PerleVIEW

Device Management System

User's Guide

Version 1.2

Part #5500320-12

May 2013

PerleVIEW V1.2

Table of Contents

1 Introduction

User Guide

This user guide is provided to help you understand the management features of PerleVIEW. PerleVIEW is a Network Management System designed to help you maintain, control, configure, update and track the health of devices on your network. PerleVIEW can discover devices, automatically respond to events from these devices and track your device hardware and software inventory.

PerleVIEW User Guide Layout

- **Getting Started**

This chapter contains the information you will need to set up PerleVIEW on your server. It describes the processes for installing PerleVIEW, logging into PerleVIEW, using a web browser and Getting Started with the PerleVIEW Wizard.

- **Groups of Devices, Hardware and Events**

This chapter contains information you will need to view, manage and monitor your device groups, hardware groups and to monitor and manage events within your network.

- **Working with Device Operations**

This chapter contains information you will need to create task instances for discovering devices on your network, device scripting, backup and restore of device lists, backup and restore of device configuration, setting PerleVIEW Server parameters and creating custom device groups.

- **Hardware Activities**

This chapter contains information on how to add task instances to collect statistics, check for firmware updates, deploy firmware and create custom hardware groups.

- **Events**

This chapter contains information on how to create tasks instances for automatic event handling, event filtering, event cleanup and create custom event groups.

- **Tasks**

This chapter contains information on working with tasks. It includes information on adding new tasks, editing tasks, controlling and deleting existing tasks as well as displaying task results.

- **Administration**

This chapter contains information on configuring PerleVIEW server settings, PerleVIEW User Accounts, File Transfer Settings, PerleVIEW software updates, Audit Trail Log, Internet Proxy Settings, E-mail Account Settings and Configuring Twitter Users.

- **Admin Utility**

This utility can be used to configure parameters used by PerleView if you are having problems connecting to PerleVIEW using your web browser. This utility allows you to stop or start the PerleVIEW server, configure SQL connection parameters, define Web connection parameters, modify the PerleVIEW Administrator (master) account and lastly update the PerleVIEW software running on this server.

Typeface Conventions

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Typeface Example	Usage
`Next button`	This typeface indicates a **button** or **tab**.
Devices -> Discovering Devices	This typeface and arrow indicates a path you should follow through the menus. In this example, you select **Discovering Devices** from the **Devices** menu.
IOLAN User's Guide	This typeface indicates a book or document title.
User Guide	This typeface indicates a cross-reference to another chapter or section. You can click on the link to jump to that chapter or section.

PerleVIEW Features

This chart contains the functions that PerleVIEW supports.

Feature	Description
Device Discovery	Device discovery allows PerleVIEW to discover new devices on your network. Once discovered, PerleVIEW will interrogate the device to discover information about it such as software levels, specific hardware information, valid user credentials and the current status of the hardware components.
Automatic Event Handling	Automatic event handing tasks enables you to define an action that PerleVIEW performs when an event occurs. PerleVIEW can perform automatic event handling on the health of a device or groups of devices.You can also create event tasks instances to monitor all events within the network or the severity of an event. Automatic event handling can include any of the following actions. Notification of event via generation of a E-mail, SMS text message (via E-mail), tweet or SNMP trap.
Backup/Restore	This feature allows you to backup and restore device lists and device configuration. Backups can be stored "offsite" incase of a database corruption or a server failure.
Users and Groups	PerleVIEW allows you to create users and groups within its database. You can then give these users and groups privileges and rights to access certain devices or to become a PerleVIEW Administrator.

8

Feature	Description
Device Scripting	Device scripting allows you to create tasks with embedded scripts files that you can deploy to all your devices or a single device. This can save time in that you do not have to connect to each device and send it the same script file.
PerleVIEW Updates	PerleVIEW can notify you of any PerleVIEW software updates required or automatically download these updates to the PerleVIEW server. These updates can then be applied at a later date.
Firmware Updates	PerleVIEW can notify you of any PerleVIEW firmware updates required for the hardware it manages or automatically download these updates to the PerleVIEW respository. These updates can then be applied at a later date.
Statistics Collection	PerleVIEW can collect statistic information from your devices. This information can be used to assess network problems or network uptime.
Collection of Health Statuses	PerleVIEW can give you health statuses for your devices. These status can be used to determine if a action needs to be taken on this device (For example: critical - device unreachable means that this device needs immediate attention). These events can range from critical, major, minor, normal or suspended.

Prerequisites

PerleVIEW Server Requirements

One of these operating systems or a virtual system.

- Windows Server 2003 and 2003 R2
- Windows Server 2008 and 2008 R2
- Windows Server 2012
- VMWare ESX, ESXI
- Microsoft Hyper-V

PerleVIEW will enable these services on your PerleVIEW server. Any missing components will be activated or installed at PerleVIEW installation time.

- Microsoft Windows Internet Information Service (IIS) 6.x or higher
- Microsoft SQL Server 2005 Express or higher
- .NET framework 4.x or higher
- WinSNMP Service
- WinSNMP Client

PerleVIEW Web Client Requirements

One of these Web browsers

- Internet Explorer 7 or higher
- Mozilla Firefox 4.0 or higher

9

- Chrome 8.x or higher
- Safari 5 or higher

2 Basic Concepts

PerleVIEW is a Device Management System designed to provide you with information and control of a large number of devices deployed throughout your network. A device is an IP addressable, manageable control point. PerleVIEW supports the Perle Managed Media Convertor family. Management of these modules is provided via the MCR-MGT management module.

PerleVIEW server software will allow you to locate devices on your network, monitor the status of these devices and all associated modules controlled by these devices. It will inform you, and take action if configured to do so when any status change occurs on the device or the associated managed modules. PerleVIEW system software can also be used to deploy changes in devices such as updating the version of firmware running on your devices, deploying mass configuration changes to all your devices or saving the configuration of your devices so that it can be restored in a disaster recovery situation just to name a few. You access the system using a standard Internet browser. No special software is required on the client side.

All information collected by PerleVIEW is stored in an SQL database. The SQL database can reside on the same server as PerleVIEW or on a remote server. The GUI provides a number of statuses based on the information found in the database. However, if you wish to compile your own custom collection of data, you can use any number of SQL tools available. These tools allow you to access any of the SQL fields and incorporate them into your custom reports.

This chapter provides you with some basic concepts you may need to understand to explore the full features of PerleVIEW.

- Guided Tour of the PerleVIEW Interface
- Health Status Panel
- Entering Licensing Information
- Help

11

Guided Tour of the PerleVIEW User Interface

The first time you log into PerleVIEW you will see the Getting Started Wizard. This Wizard will help you set up and configure the parameters to be used with PerleVIEW. See *Getting Started Wizard* for more information.

Each time thereafter you connect you will see the Home page. The Home page provides links to frequently used features.This section of the screen is also used as the PerleVIEW workspace to display your latest task results, configuration options, audit log, event log, display hardware/software inventory and group views.
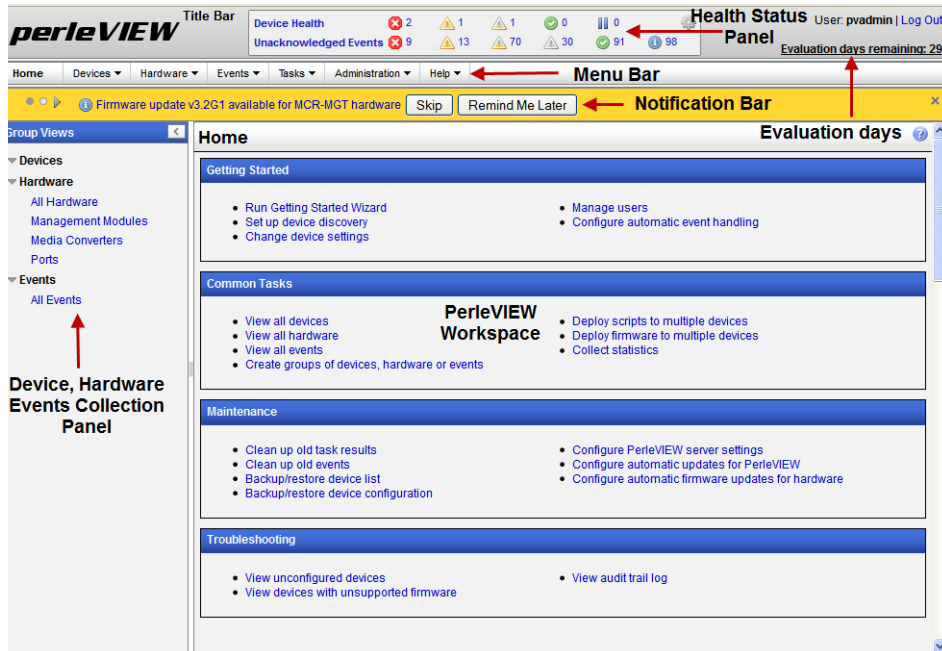
The top **Menu Bar** is used for action options or configuring devices settings. The Menu Bar is primarily used by users who administer the PerleVIEW software. If you lack administrator rights to use these tools, you might not be able to view certain menus.

Below the menu bar is a **Notification Bar**. The notification bar is for PerleVIEW messages only. To see all PerleVIEW generated events see *Appendix B, "Event Information"*. If there are no outstanding PerleVIEW messages then this bar will not appear. This notification bar does not display the health status or information regarding devices on your network. See for more health status information.

The **PerleVIEW Workspace** area displays the results of your latest request. It can contain a view, a collection, a configuration tool or the results of logs.

The **Health Status Panel** allows you to view all devices grouped by their current health status. The health status of a device can be one of the following: critical, major, minor, normal or suspended. If a device has more then one health status, only the most serious status will be counted in the device totals. In other words, the sum of the critical, major, minor, normal and suspended counts will add up to the total number of devices that you are monitoring.

This panel also provides unacknowledged event statuses for all devices. At a quick glance, you can see if there are unacknowledged events for any of your devices. This will alert you to potential issues with devices which require your attention. To manage the specific events, you can click on the "Unacknowledged Events" text to bring up a list of all unacknowledged events or you can click on any of the icons to bring up a list of unacknowledged events for a specific severity level. See *Health Status Panel* for more information.

12

Navigating PerleVIEW

The left-hand side of this screen is referred to as the "Navigation" panel. Using this panel you can quickly and easily see views for the Devices, Hardware and Events found in your managed network. You can drill down though submenus to focus in on a device, hardware or events. For each category, you can select from an existing PerleVIEW group or a custom group if you have created any. From these submenus you can manage and control most features of your devices, as well, you can view and edit your installed hardware modules such as management modules, media converter modules and individual media converter ports. Events or alerts on your system can be easily acknowledged or deleted to help you keep on top of the more critical events within your network. Custom device, hardware and event groups can be created to sort and maintain your own custom views.

Navigating the Options

The left-hand navigation tree allows you to quickly and easily navigate the various group views for your devices. Selecting the right arrow beside any of the options will further expand what options are available to you. To collapse a section, click on the down arrow. For devices, clicking on a specific device listed will bring up device specific information in the PerleVIEW workspace area allowing you to obtain device specific information as well as perform some actions on this device.
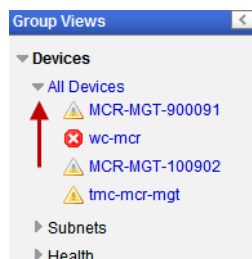
Health Status Panel

On PerleVIEW startup, the health statuses of devices in this view are populated with the last known statuses from the PerleVIEW database. PerleVIEW will automatically launch a task to obtain the current device statuses and health information when it is re-started. From that point on, it will largely rely on traps being sent from the device to report events and periodic checks by the "Poll Device Reachable" task to maintain the current health status of the device. The health status of a device can be one of the following; critical, major, minor, normal or suspended. If a device has more then one health status, only the most serious status will be counted. The sum of the critical, major, minor, normal and suspended counts will add up to the total number of devices that you are monitoring on your network.

See *Appendix B, "Event Information"* for more information on health statuses.

## Health Icons

|	
⚙	Selecting the gearbox will give you a legend of the meanings of the health icons. Click on the Show notifications button to show any hidden notifications.

13

Licensing Information

PerleVIEW is provided to you with a free, 30 day evaluation period. During the free trial period, you can use all the features of PerleVIEW. The current status of your free trial will be displayed to the right of the Device health box on the title bar. Once the 30 day trial period expires, you are required to purchase PerleVIEW if you intend to keep using the application. Information about purchasing PerleVIEW can be obtained from your Perle reseller or the Perle web site. A link to the Perle Web site location is provided by the software (see screen below).

Entering a Licensing Key

Help->License
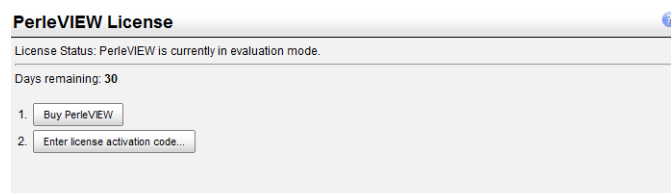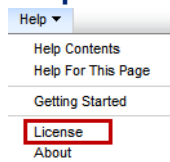
If you have not already purchased PerleVIEW, you may do so via this screen. If you click on the `Buy PerleVIEW button`, you will be directed to the Perle website where you can purchase PerleVIEW and obtain a License Activation Key. If you have already purchased PerleVIEW, you can click on the "`Enter license activation code" button` to enter your licensing information.
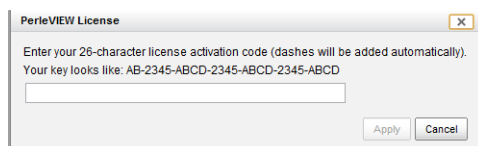
Your `license activation code` consists of 26 character which are grouped and separated by dashes. You need to only enter the digits of the activation code, the dashes will appear automatically as you type. Once you are done entering the activation code, click the `Apply button`.

If you have successfully entered the activation code, the status of PerleVIEW should now indicate "Licensed".
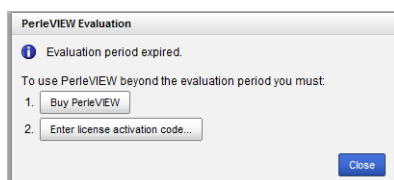
If your evaluation copy has ended you will see this screen, click on the `Buy PerleVIEW button` to purchase a copy of PerleVIEW or click on the link to enter the license activation code.

14

Online Help

Online help is provided in PerleVIEW. You can click on the ( ) icon to get page level help. You can also get help from the PerleVIEW *User's Guide* online by selecting **Help -> Help Contents**.
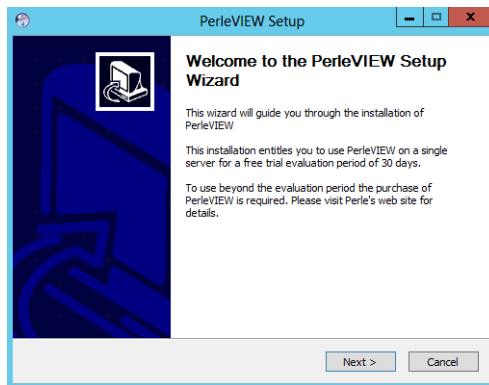
3 Getting Started

Installing PerleVIEW on your Server

The PerleVIEW Setup Wizard installs PerleVIEW on your Windows Server and helps you setup the operating parameters to be used with PerleVIEW.

To Begin

Double-click on the PerleVIEW-setup.exe to launch the installation of PerleVIEW. This must be executed on the server you wish to install PerleVIEW.
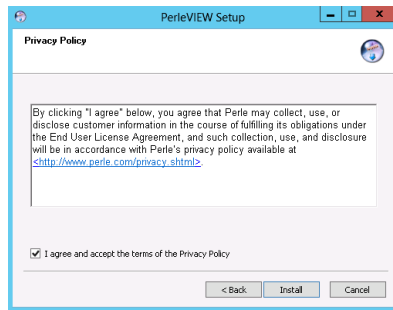

Click the **Next button** to continue.

PerleVIEW will perform some basic checks before running the install. The first check performed by PerleVIEW is to ensure that you are installing the software on a server which is running one of the supported Windows Operating Systems (see PerleVIEW Server Requirements). If this is an upgrade, the installer checks the version of PerleVIEW being installed to ensure that it is not older than the version of PerleVIEW currently installed on the server. If either of the above checks detect an issue, an appropriate message will be displayed and the install will not be allowed to proceed.

You must accept the Licensing Agreement to install PerleVIEW. Read the License Agreement, then select the checkbox to indicate that you agree to the terms of the License Agreement.


16
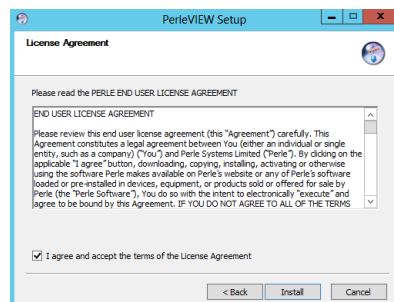
Then click on the **Install button** to continue.

Next, read the Privacy Policy and again, check the **I Agree** checkbox, then click on the **Install button** to continue.

By default, PerleVIEW will be installed in this destination folder C:\Program Files (x86)\Perle Systems Limited\PerleVIEW. To change the destination folder either type in the path to be used or click the **Browse button** to browse to a new location.
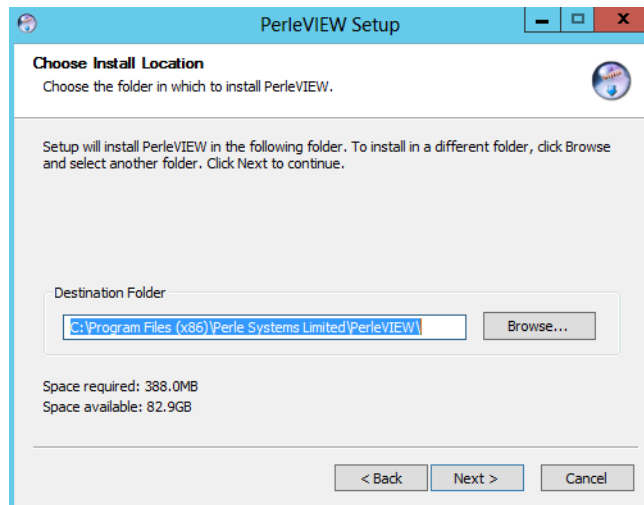

Click the **Next button** to continue the installation.

Select the Start Menu folder in which you would like to create a new folder. PerleVIEW will install both the PerleView Admin Utility and the PerleVIEW uninstall program see PVAdmin (PerleVIEW Administrator) for more information.

Click the **Install button** to continue.

PerleView requires access to an SQL server installation. You can either have PerleVIEW install a version of SQL server on this server or use an existing installation of SQL Server either locally or remotely. If you plan on using a remote installation of SQL Server, Click on the **No button.** If your intentions are to run a local copy of the SQL Server (on the PerleVIEW server), then click on the **Yes button.**

In order to run, PerleVIEW needs an SQL Server to be installed either locally or remotely.

17
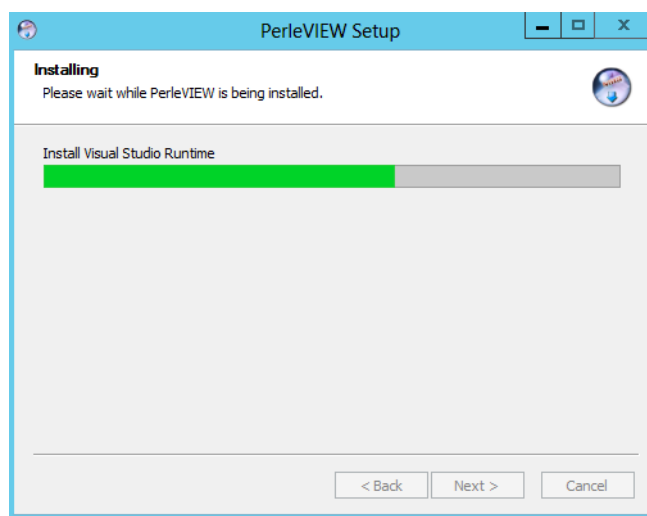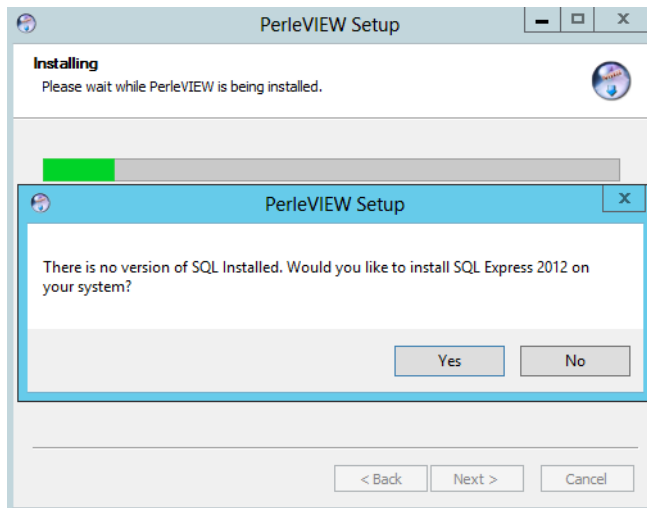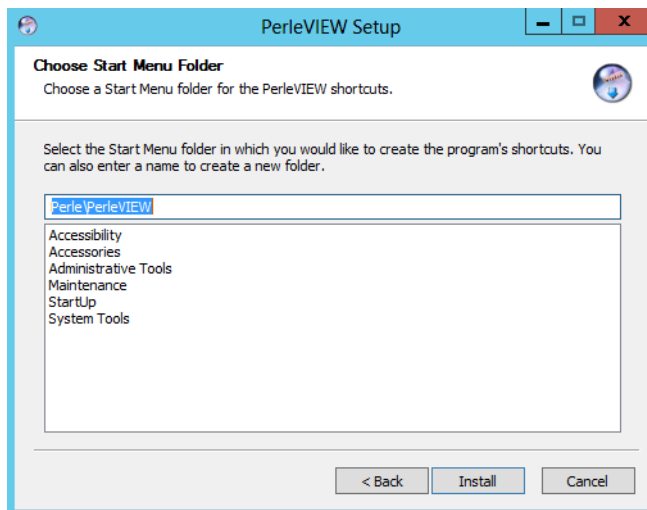
PerleVIEW is installing.
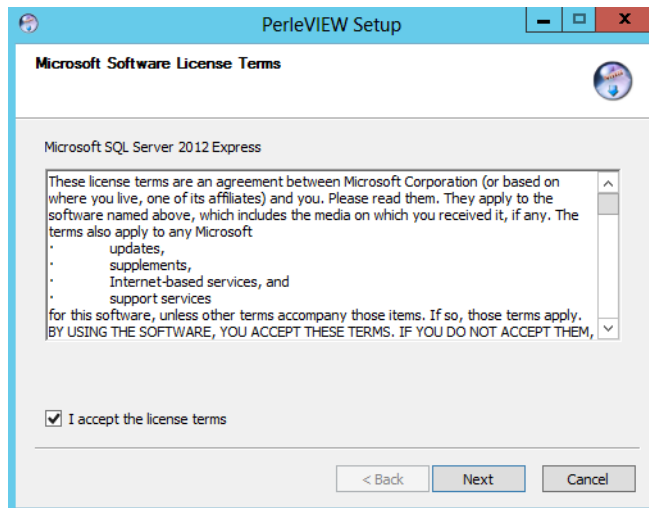
You must accept the licensing agreement to install Microsoft SQL Server. Read the license agreement, then select the checkbox to indicate that you agree to the terms of the license agreement.

SQL Connection Parameters

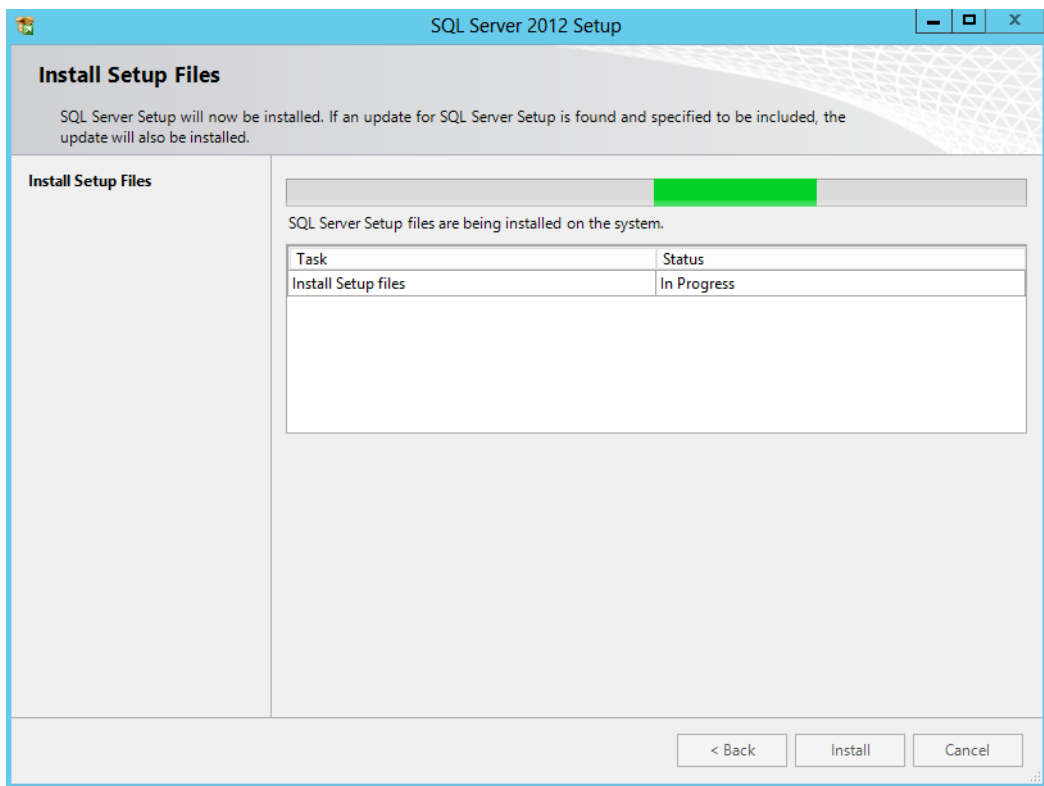If this is a new SQL connection, PerleVIEW will only require you to configure the SQL Server Name and the Database User.

If you are using a existing SQL Server, then the following screen will appear.

Click on the **Yes button** after you have completed the fields.

| SQL Server	The Server Name consists of two parts separated by a backslash (\). The first part of the name is the hostname or IP address. The second part of the Server Name is the SQL Instance Name. If during installation PerleVIEW installs the SQL server for you, then by default, PerleVIEW uses localhost\SQLEXPRESS as the Server Name**.** However, if SQL Server is already installed on this server then you must provide the server name information here**.**
User	If you are using Windows Authentication Mode, type in the Windows user name (FQDN if required) as defined within your Windows Server Users environment. If you selected SQL Authentication mode you will need to provide the user name you configured for this user in the SQL Server configuration. If the SQL Server does not have a login account set for this user, authentication will fail and the user will receive an error message.
Password	If you are using Windows Authentication Mode, type in the Windows password as defined within your Windows Server environment. If you selected SQL Authentication mode you will need to provide the password you configured for this user in the SQL server configuration.
Authentication	By default, PerleVIEW will install "Use Windows Authentication Mode". Use the SQL Authentication method if on installation of your SQL server software, you selected mixed mode or SQL server authentication.

                                        Values: Windows Authentication

                                                      SQL Authentication

                                        Default: Windows Authentication

Network Protocol	SQL Server Resolution Protocol will be used to determine how to connect to the selected SQL instance. If the SQL instance is local then the connection will use "Shared Memory". If the SQL instance selected is remote then TCP/IP will be used and SQL Server Resolution Protocol (UDP port 1434) to obtain the connection information (i.e the port number) from the remote instance. If the connection fails and the SQL instance is remote, this may be due to the inability to communicate with the SQL server. This could be caused by a firewall or the SQL Server Resolution Protocol service may not be running on the SQL server. If this is the case, you will need to use the TCP option and configure the TCP port which the SQL is listening on. **Default:** Auto
TCP Port	If your SQL server is remote to PerleVIEW, this will be the TCP port to send and receive messages between PerleVIEW and the SQL Server. **Values:** 1-65535 **Default:** 1433
Network Packet	This the size of the TCP packet that PerleVIEW will use to communicate to the SQL server. **Values:** 512-32767 bytes **Default:** 4096 bytes
Connect Timeout	The time that PerleVIEW will wait for a connection to the SQL server before PerleVIEW times out. **Values:** 0 means never times out **Max:** 30000 seconds **Default:** 15 seconds
Encrypt Connection	PerleVIEW will force the data between PerleVIEW and the SQL server to be encrypted. This is recommended when the SQL Server is remote to PerleVIEW.

At this time, the installation program will attempt to establish a connection to the SQL Server using the parameters entered on this screen. If this operation does not succeed, an error message will be displayed and the install will return to this screen to allow the you to modify the parameters and try again

21
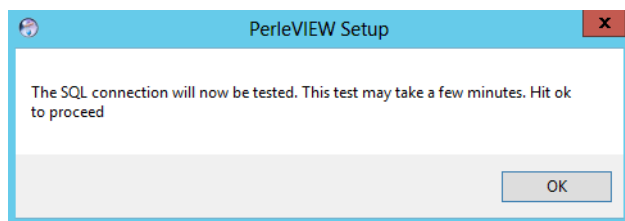
Next you will be asked to setup the parameters that PerleVIEW will use when communicating with a Web Client (browser). This includes enabling/disabling HTTP/HTTPS, the TCP ports that will used for these protocols and the name of the PerleVIEW master admin user. Please note that the master admin user must also exist in the server's Windows user list. By default, this is set to the same user who is installing PerleVIEW.

When completed, click the **Next button** to continue.

|	
Enable HTTP	Web clients (browsers) will be able to connect to PerleVIEW using the HTTP protocol. **Default Port:** 50000 **Values:** 1-65535
Enable HTTPS	Web clients (browsers) will be able to connect to PerleVIEW using the HTTPS protocol. **Default port:** 60000 **Values:** 1-65535
PerleVIEW Admin User	Type in the name of the master admin user to be used by PerleVIEW. This user can not be deleted. The master user can be reset by using the PerleVIEW Admin Utility which is installed during this installation.
Domain	Type in a domain name if required by your network.
Administrator Full Name	Type in Administrators Full Name (optional).

If your server resides behind a firewall, you will need to poke a hole in the firewall for the TCP ports configured above.

22

After entering the parameters, PerleVIEW will now create the PerleVIEW website on IIS
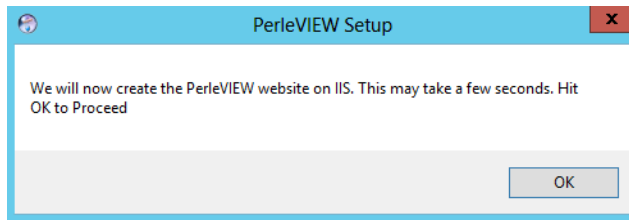
Click the `Ok button` proceed.

PerleVIEW has successfully been installed on your server.
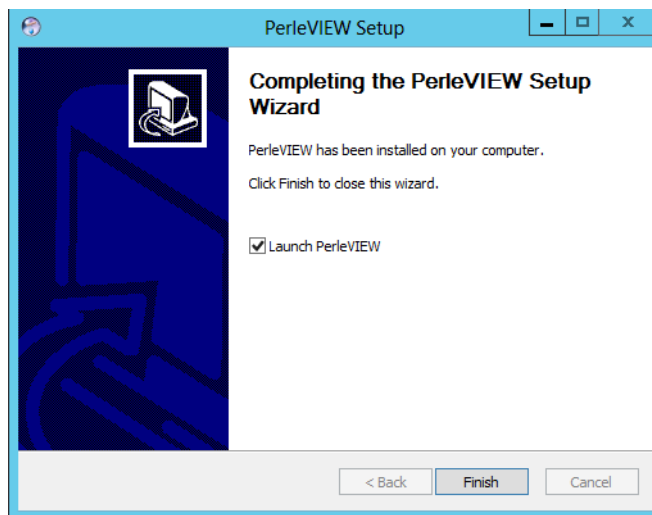
Click the `Finish button`.

Logging into PerleVIEW

Login

You can connect to PerleVIEW using any of the supported Web browsers. See PerleVIEW Web Client Requirements for list of supported Web Browsers.
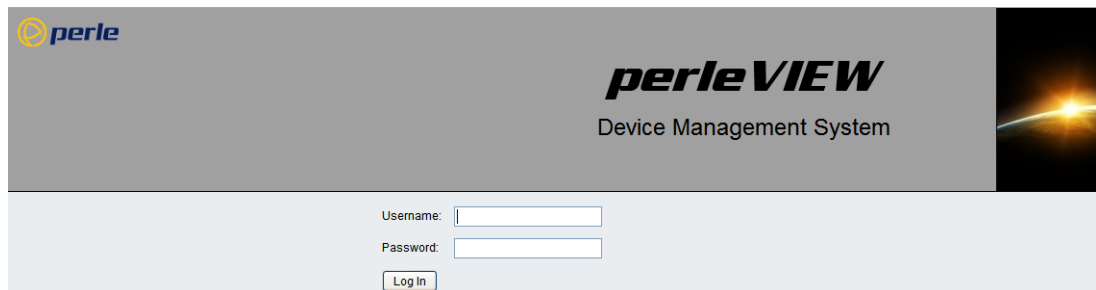
1. Open your web browser and type in the IP address of the server where you installed PerleVIEW followed by a colon (:) and the port number to connect on, then press **Enter**. For example:

   http://123.123.123.123:50000

   https://123.123.123.123:60000

   NOTE: *If you modified the default TCP ports for HTTP or HTTPS during the installation, you will need to substitute the correct TCP port in the above example.*

2. If you successfully connect to PerleVIEW, a login screen will appear.

3. Type in the "master admin" user name (and his associated password) you entered when you installed PerleVIEW.


If your server resides behind a firewall, you will need to poke a hole in the firewall for the TCP ports being used for HTTP and/or HTTPS.

Getting Started Wizard

The first time you connect to PerleVIEW, you will see the Getting Started Wizard screen.

The Getting Started wizard will guide you through the initial setup of discovering devices, setting up user security, checking your Internet connection, checking for software updates and setting the parameters to be used for file transfers.

You can run the "Getting Started" Wizard at any time by selecting "Getting Started" under the "Help" pull down menu.
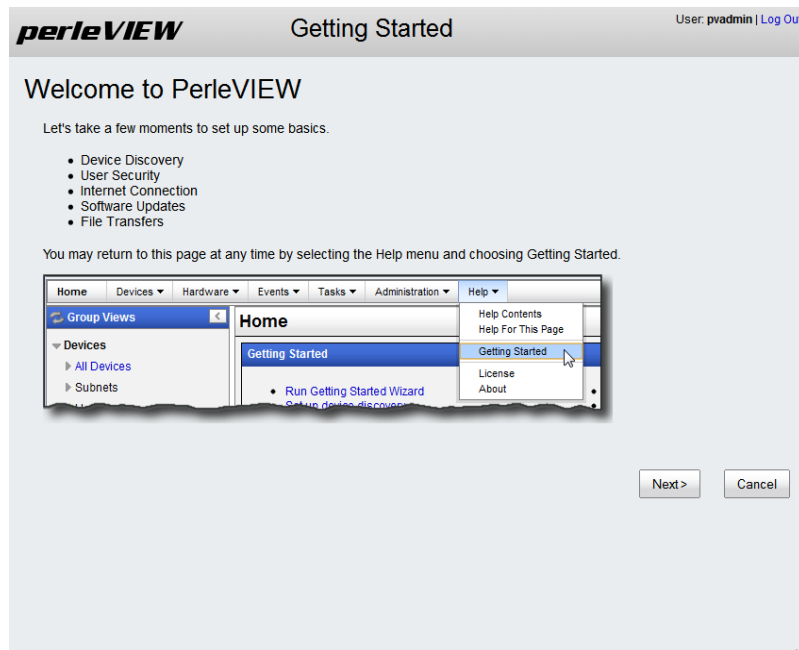
Click on the `Next button` to continue.

You can click on the `Cancel button` at any time to abort this process. All changes you made will not take effect.

On following screens, click on the `Previous button` to go back to the screen you just came from.

25

Discovering Devices

This part of the wizard will guide you through setting up the default device discovery task. PerleVIEW uses device discovery as the method by which it adds devices to its internal database. Before a device can be monitored or controlled, it must first be added to the PerleVIEW device database. To see more information on the Device Discovery task see **_Discovering Devices_** .

Click on the `Next button` to continue.

Discover devices immediately	Run the default discovery task instance immediately after completing the Getting Started Wizard.
Automatically discover devices on local network	If you have devices on the same physical subnet as the PerleVIEW server, this will allow PerleVIEW to automatically discover all of these devices. If your devices reside on a different subnet then the PerleVIEW server, you can disable this option.
Specify device addresses manually	When the default device discovery task is run, this list will be used to discover devices by hostnames, specific IP addresses, range of IP addresses or an IP subnet. Depending on the scope of the discovery, the process may take a long time to complete.
Use default device credentials	Device Credentials are used by PerleVIEW to gain access to the device in order to retrieve information from the device or write information to the device.
	Select this checkbox if you want to use the "global" device credentials for the default discovery task instance.
	If this option is unchecked, you can enter the device credentials to be used with the default discovery task instance. These values will be tried first, if they are not valid, the task will attempt the "global" credentials.
Automatically discover device when SNMP trap is received from that device	If PerleVIEW is configured as an SNMP trap host for this device, when the device sends a trap to PerleVIEW, this will cause PerleVIEW to add the device to its database (i.e. automatically discover the device). When this happens, the global parameters are used for protocol timers and credential validation.

26

User Security

In order to log into PerleVIEW, you must be a valid Windows user on the PerleVIEW server. By default, PerleVIEW is configured such that you also have to be configured on the PerleVIEW application as a user before you can successfully log into PerleVIEW. This gives you an extra level of control as to which Windows users will be allowed to access the PerleVIEW application.

For more information about User Security and Configuring Users see *PerleVIEW User Accounts* .
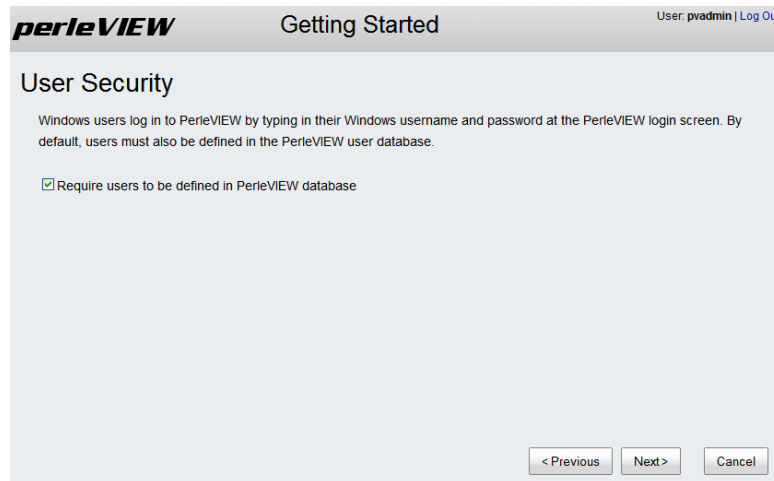
Click on the `Next button` to continue.

Require users to be defined in the PerleVIEW database	PerleVIEW users must be defined in the Windows Server User Accounts as well as within the PerleVIEW Database in order to gain access to the PerleVIEW application. Uncheck this option if you want any valid Windows user to have access to PerleVIEW.
Automatically discover device when SNMP trap is received from that device	If PerleVIEW is configured as an SNMP trap host for this device, when the device sends a trap to PerleVIEW, this will cause PerleVIEW to add the device to its database (i.e. automatically discover the device). When this happens, the global parameters are used for protocol timers and credential validation.

27

Internet Connection

On some networks, access to the Internet is provided via a proxy server. PerleVIEW needs to reach the Internet for some of its functions to work such as sending Tweets and looking for software updates. If a proxy server is being used on your network, you should enter its access information here.

Click on the `Next button` to continue.

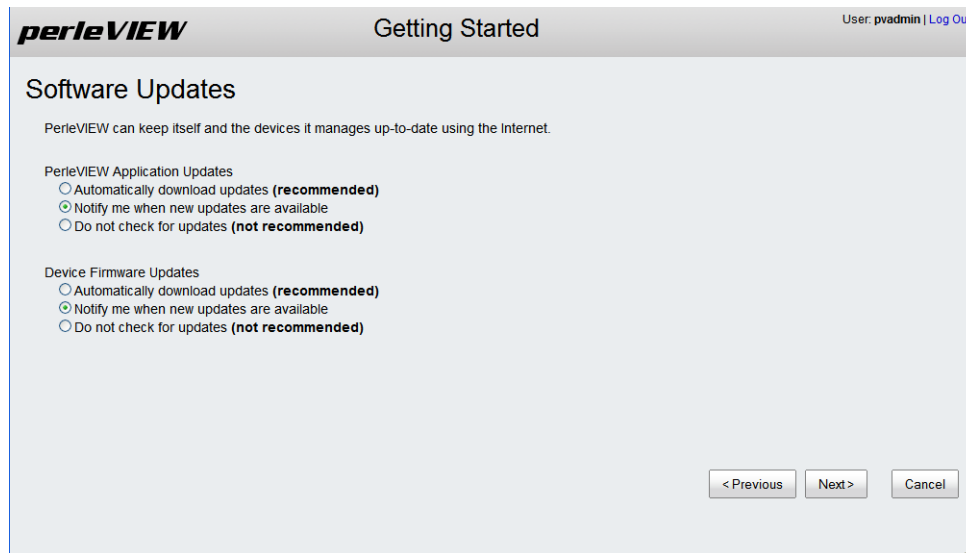|	
Use Proxy Server (HTTP/HTTPS)	Select use Proxy server if you need a Proxy server to reach the Internet. See your administrator for the parameters to set up your network Proxy Server.
Proxy Server	Enter the IP address of the Proxy Server.
Port	Enter the port number that the Proxy Server uses for client connection. **Default:** 80
Server Requires Authentication	Some Proxy Servers require user authentication. See your administrator for the authentication parameters.
Username	Enter the username to be used to authenticate to the Proxy Server.
Password	Enter the password to be used to authenticate to the Proxy Server.
Domain	If needed, enter a Domain name to be used to authenticated to the Proxy Server.

28

Software Updates

By default, PerleVIEW will notify the administrator of any new updates for itself or for any firmware for devices it manages. PerleVIEW will update the notification bar with a download pending message when an update is available. PerleVIEW can also be configured to automatically download software updates to the PerleVIEW server and firmware updates to the PerleVIEW repository. This is the recommended setting since it will ensure that PerleVIEW is always kept up to date.

To apply software updates to PerleVIEW see PerleView Software Update . To apply device firmware see *Deploying Firmware* .

Click on the `Next button` to continue.

File Transfers

PerleVIEW uses file transfers for a number of functions. This includes, but is not limited to downloading firmware updates, downloading/uploading device configuration, deploying scripts (only if file transfer mode is used). PerleVIEW can use HTTP (or HTTPS) to transfer files or alternatively it can use TFTP.

PerleVIEW comes with TFTP server software. You can define how TFTP is used on PerleVIEW in the "File Transfers" screen. See *PerleVIEW File Transfer Settings* .

PerleVIEW keeps firmware updates which it downloads or device configuration file which it uploads from the devices in a directory. You can manage the location of this directory by selecting "Choose location". Doing this will allow you to perform manual backups of the information if you want to.

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

| Repository Location	The Repository location is the location on your PerleVIEW server where your downloaded software and configuration files will be stored. Select "Let PerleVIEW manage location" unless you want to perform manual backups of this data. If you choose to specify your own software location to store your updates the server path needs to be in Microsoft Windows UNC format (Universal Naming Convention). Example \\ComputerName\SharedFolder\Resource. If you specify your own location to store the files, you will need to provide your Windows network credentials that have rights to this path.

TFTP Server	By default, PerleVIEW will install its TFTP server on port 69. PerleVIEW will use its TFTP server to transfer all files. Select use existing TFTP server and Window File Sharing if you have an existing setup for file transfer. PerleVIEW will use Windows file transfer to transfer files between PerleVIEW and the TFTP server. Configured your TFTP server and port number to transfer files between target devices and your TFTP server. If you specify this method, you will need to provide your Windows network credentials that have rights to the Windows network location specified.
	Note: To use an existing Windows File server, specify the Windows Network Location in Microsoft Windows UNC format (Universal Naming Convention).
	Example: \\ComputerName\SharedFolder\Resource
Windows Network Credentials	Specify your Windows Network Credentials of username, password and domain name (if required).
	If you have entered you own location for the repository and for the TFTP server, the credentials must be valid for both of these.

Apply Settings
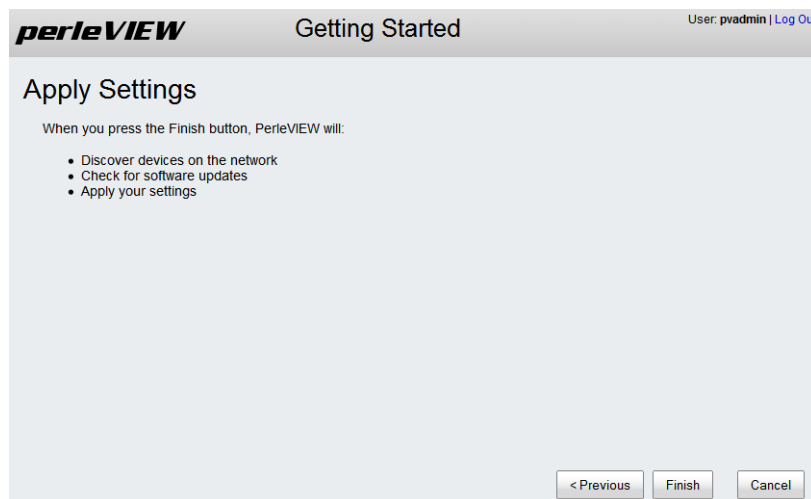
Click on the `Finish button` to continue.

The Default Discovery Task will now start to collect information from your network. For more information on this task see PerleVIEW Default Tasks .

4 Working with Device Operations

Discovering Devices

Menu Selection: Discovering Devices

Required Authorization: PerleVIEW Administrator

PerleVIEW needs to add devices to its internal database in order to provide statuses on these devices. The way that PerleVIEW adds devices to it's database is by running a device discovery task. PerleVIEW will also add devices to its database if it receives a trap message from a device not in its database. PerleVIEW uses management protocols such as its own proprietary protocol, as well as SNMP to discover and add new devices.

By default, PerleVIEW uses broadcast packets to discover local devices on its network. In order to discover remote devices, proper routing needs to be configured on servers and routers. Also the default device discovery task needs to be modified (or a new device discovery task created) so that you can specify host names, IP addresses, ranges of IP addresses or IP subnet of these devices.

The Default Device Discovery task can not be deleted as it is a PerleVIEW system task, however you can disable or enable this task and change it's operating parameters.

Discovered devices can be viewed under;

Working with Device Views or

Group Views -> All Devices within the left-hand navigation panel.

PerleVIEW provides two methods that can be used to discover devices on your network.

Method	Description
Automatically discover devices on local network	By default, PerleVIEW uses its proprietary discovery method to discover devices on its local network.
Enable Device Discovery using IP addresses	Use this method, if you need to discover devices outside of your local network. You will need to provide host names, IP addresses, IP ranges or an IP subnet.

Device Credentials

When dealing with a large number of devices, it is impossible for you to remember the user name and password associated with each device. PerleVIEW provides the ability to discover and record which credentials are valid for each device. This credential validation process takes place during device discovery. When a device discovery instance is defined, you can specify which credentials PerleVIEW should attempt to validate. In addition, you can configure specific credentials to be used with this discovery instance. There are also a set of global device credentials which are configured in PerleVIEW. If the credentials specified with the discovery task instance are not valid for the device, PerleVIEW will attempt to find valid credentials using the global credentials. Once a valid credential

32

is found, it will be saved as the working credential for that device. If possible group devices with similar credentials into the same device discovery task instance.

Launching Discovering Devices

Devices ->Discovering Devices

Working with Discovering Devices Tasks

PerleVIEW provides the following discovery task functions.

- Run Device Discovery task instance now
- Enable/Disable Device Discovery task instance
- Add a Device Discovery task instance to our PerleVIEW database
- Edit a Device Discovery task instance
- Delete a Device Discovery task instance

Run Now

To run an existing Device Discovery task instance immediately, select the task from the list, then click on the **Run Now button.**

33

Add a Device Discovery Task

Each device discovery task instance can have unique operating parameters.

Add

Click the **Add button** to create a new Device Discovery Task instance.

Task name	Use a meaningful name to uniquely identify this device discovery task instance.
Schedule	**Manual -** do not automatically run this task. This task can only be run from the **Run Now button.**
	Run Once - Run this task only once based on the configured "Start on" date
	Periodic - Run this task periodically at the configured period.
Automatically discover devices	By default, PerleVIEW uses a proprietary broadcast message to discover devices on the local network.
Enable Device Discovery using IP addresses	When the Device Discovery task is run, this list will be used to discover devices by host names, specific IP addresses, lists of IP addresses, range of IP addresses or an IP subnet.
Optimize Discovery	
All devices and networks support UDP messages on ports 33815 and 33816	If all your remote devices and networks are reachable using UDP port 33816 and UDP port 33815, then select this checkbox to optimize the discovery of devices on your network. PerleVIEW will first send a directed message using UDP port 33816 to see if the device is reachable before sending requests to gather information about this device. The device will respond using UDP port 33815.

34

Support ICMP ping messages	If all devices in your network are reachable by sending an ICMP message, then select this checkbox to optimize the discovery of these devices. PerleVIEW will first send a ICMP message to see if the device is reachable before sending requests to gather information about this device.
Protocol Timeout	Specify how long to wait for a reply from the device after sending either a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery message. This field should contain the value in seconds of the device which has the longest response time.
	Default: 3 seconds
	Values: 1-255
	(*) denotes - leave blank to use global parameter
Protocol Retries	Specify how many retries to attempt when no response received from a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery message.
	Default: 2
	Values: 0-255
	(*) denotes - leave blank to use global parameter
Select Credential Types	Put a check mark in front of each type of credential that you want PerleVIEW to validate for devices discovered by this discovery task instance. Since PerleVIEW uses SNMP to collect information from devices as well as control the devices, at least one of the SNMP credentials must be checked.
	The credentials used by PerleVIEW are as follows;
	• SMNP read community - Used to get statuses from the device.
	• SMNP read/write community - Used to get statuses and control the device (example: reboot the device).
	• Operator login/Admin login - These credentials are used by PerleVIEW to log into the device when needed. For example, when managing the device via Web Manager or Web Terminal, PerleVIEW will automatically log you into the device using the device's login credentials.
	• SSH keys - If SSH keys are used on the device, the SSH private/public key pair will be used by PerleVIEW to login to that device when performing an SSH connection or managing the device via a secured (HTTPS) Web Manager session.
Select Credential Data	For the credential types you selected, you can now specify where PerleVIEW will obtain the credential values to be attempted on the device. By default, PerleVIEW will attempt the credential values configured in it's global credential tables. If you wish to use a specific credential value with this discovery task, you can do so by checking the "Specify additional credentials" checkbox. If both "Use global credentials" and "Specify additional credentials" are checked, PerleVIEW will attempt to use the credentials specified with this discovery task instance first. If they fail, it will attempt to find valid credentials using the global credentials. See global *Credentials* for more information.

Settings for All Discovery Tasks

Click on the **Settings for All Discovery Tasks button** to view and configure global parameters which apply to all discovery task instances. For more information see *Configure Device Settings* .

35

Show All Devices

Click on the **Show All Devices button** to shows all of the devices which are present in the PerleVIEW device database. See *Groups Views* for more information.

Task Details/Last Run Results

This panel displays the task details of the selected discovery task instance. It shows the Last Run Results for the current task that was run, the name of the task, who submitted the task, status of the task, schedule and the start and end times. The All Results button, View Log button and Target Results button gives you more in depth information about every time this task has been run and also individual task results.

All Results

The **All Results button** will show you the results for every time this task has been run.

View Log

```
Task Result Log                                                    [X]
┌──────────────────────────────────────────────────────────────────┐
│ 10/05/2012 11:18:08 PM Starting Discovery                      [▲] │
│ 10/05/2012 11:18:08 PM Trying to Automatically Discover Devices... │
│ 10/05/2012 11:18:09 PM Device 1:2:3:4:5:6:23:40 Responded         │
│ 10/05/2012 11:18:09 PM Device 172.16.23.40 Responded             │
│ 10/05/2012 11:18:09 PM Device 172.16.54.106 Responded            │
│ 10/05/2012 11:18:09 PM Device 1:2:3:4:5:6:22:30 Responded        │
│ 10/05/2012 11:18:09 PM Device 172.16.54.55 Responded             │
│ 10/05/2012 11:18:09 PM Device 172.16.22.30 Responded             │
│ 10/05/2012 11:18:09 PM Device 172.16.23.40 Responded             │
│ 10/05/2012 11:18:10 PM Device 172.16.54.106 Responded            │
│ 10/05/2012 11:18:10 PM Device 172.16.54.55 Responded             │
│ 10/05/2012 11:18:10 PM Device 172.16.22.30 Responded             │
│ 10/05/2012 11:18:16 PM Devices Discovered: 4                     │
│ 10/05/2012 11:18:16 PM Subtask Protocols Starting               │
│ 10/05/2012 11:18:21 PM SubTask Protocols Ended                  │
│ 10/05/2012 11:18:22 PM Subtask Credentials Starting             │
│ 10/05/2012 11:18:33 PM Subtask Credentials Ended                │
│ 10/05/2012 11:18:34 PM Subtask Device Identity Starting         │
│ 10/05/2012 11:18:36 PM Subtask Device Identity Ended            │
│ 10/05/2012 11:18:37 PM Hardware Inventory Collection Starting   │
│ 10/05/2012 11:18:54 PM Subtask Media Port Status Starting     [▼] │
│                                                                    │
│                                                     [  Close  ]    │
└──────────────────────────────────────────────────────────────────┘
```

The **View Log button** will display PerleVIEW related messages for this task. To see the full list of PerleVIEW generated messages see Appendix B, "Event Information".

Target Results

```
Task Target Results                                              [X]
┌────────────────────────────────────────────────────────────────┐
│ Target          │ Type    │ Status    │ Log                     │
│ 172.16.22.50    │ Device  │ Running   │ Yes                     │
│ 172.16.22.30    │ Device  │ Running   │ Yes                     │
│                                                                  │
│ << first  < prev   1   next >  last >>                           │
│                                              [  View Log  ]       │
│                                              [   Close   ]        │
└────────────────────────────────────────────────────────────────┘
```
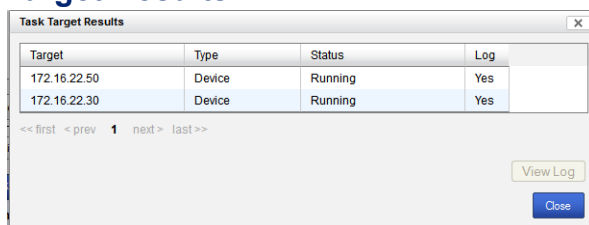
The **Target Results button** will display the results from the target devices.

Device Scripting

Menu Selection: Device scripting

Minimum Required Authorization: Device Operator

PerleVIEW allows you to create Device scripts (which are lists of CLI commands) that can be sent to one or many devices. Scripts will be executed on each device and the results be will logged. You can find these logs under "**Tasks --> Task Results**" under the associated task name.

CLI commands for the Perle MCR-MGT management Module can be found on our website at `http://www.perle.com/downloads/`

More information on Device Scripting can be found in Appendix C, *Device Scripts*.

Launching Device Scripting

Device->Device Scripting
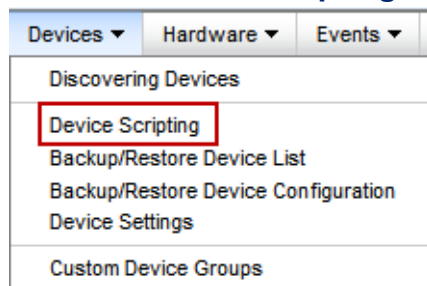
Working with Device Scripts

PerleVIEW provides the following device script task options. Select the device script you want to run and then click the **Run Now button.** PerleVIEW provides one default device script to reboot all target devices which is useful after a deployment of firmware to multiple target devices.

- Run Device Script task now
- Disable/Enable Device Script task instance
- Add a Device Script task instance to your PerleVIEW database
- Edit a Device Script task instance
- Delete a Device Script task instance

Run Now
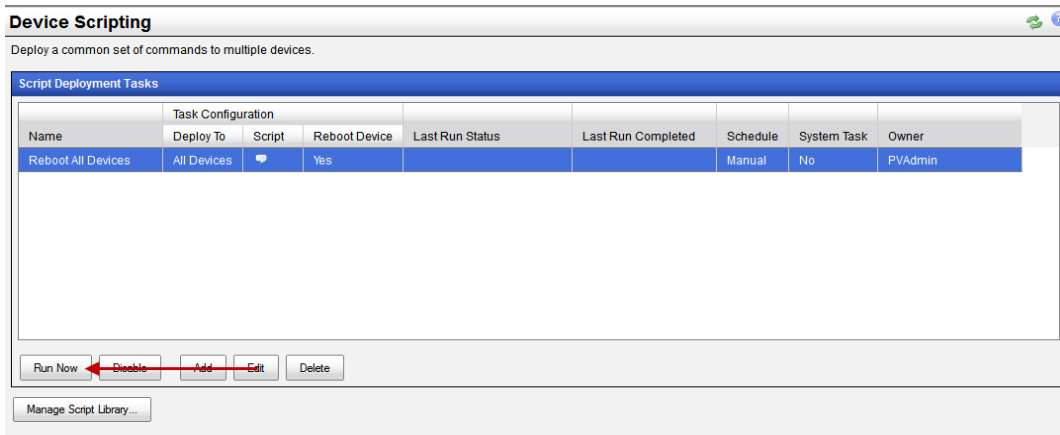
To run a existing Device Script task instance immediately, select the task from the list, then click on the **Run Now button.**

Each deploy script task instance can have unique operating parameters.

Add

Click the **Add button** to create a new Deploy Script task instance.

Task Name	Enter a name to uniquely identify this device script task instance.
Targets	Select the device(s) to which you want to deploy this script. Scripts can be deployed to Device groups, Custom Groups or selected individual devices.
Schedule	See *Add a Device Discovery Task* for configuration parameters.
Script	This window can be used to enter CLI commands directly. Standard editing functions such as cut or paste can be used. Simply right click to bring up selection menu or use editing keystrokes (i.e. "CTRL+C" to copy highlighted text).
Insert Script from Library	The script library holds previously saved scripts. This button allows you to insert one of these saved scripts in the edit script window at the current cursor position. You can insert more than one script if you want to, but you must insert each script individually. Once inserted, this script becomes part of the current deploy script task. The original inserted script is unaffected by any changes made in this copy.
Reboot target device after executing script	Checking this option will cause PerleVIEW to reboot the target device after the device script has finished processing.
Operate in file transfer mode	Use this mode if you do not want PerleVIEW to send the script to the device using Telnet or SSH. When selected, this will cause PerleVIEW to initiate a file transfer via HTTP or TFTP to the device, transfer the script to the device and once execution of the script is completed, the results will be file transferred back to PerleVIEW.
Apply	When the **Apply button** is clicked, the device script task will be created with a copy of the script which was typed in or inserted in the above dialog. You can edit the script associated with this task by selecting the task and clicking the **Edit button**.

39

Manage Script Library

These scripts are used by the "Deploy Script" tasks.
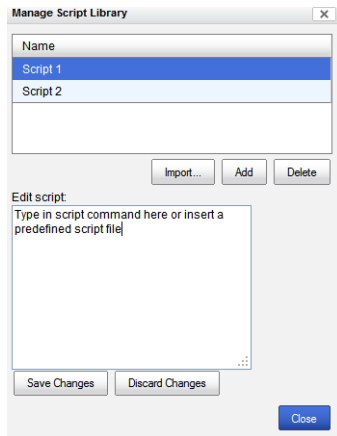
Click on the **Manage Script Library button** to add new script files to the script library, delete existing script files or import existing script files from a different location.

Import	Import a file from another location into the script library. The script is displayed in the "Edit script" window and can be edited if needed.
Add	Add a new script file to the Script Library. Enter the CLI commands for the newly added script in the "Edit script" window.
Delete	Delete the selected script file from the library.

Backup/Restore Device List

Menu Selection: Backup/Restore Device List

Minimum Run Authorization: PerleVIEW Administrator

If you ever lose the contents of the PerleVIEW database, you can use this backup feature to restore the lists of devices to the PerleVIEW database. The restore device list feature would launch a discovery task instance with all the IP addresses of your previously discovered (and backed up) devices defined for that instance. The backup is stored outside of the PerleVIEW database so that it would not be lost in the event of a database corruption or loss. The backup device list can also be exported to a different PC for additional safe keeping.

Launching Backup/Restore Device List

Devices ->Backup and Restore
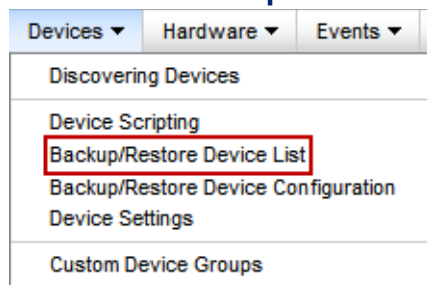
Working with Backup Device Lists

To save your current Device List to a directory on the PerleVIEW server, click the **Backup to Server button**.

Backup Now
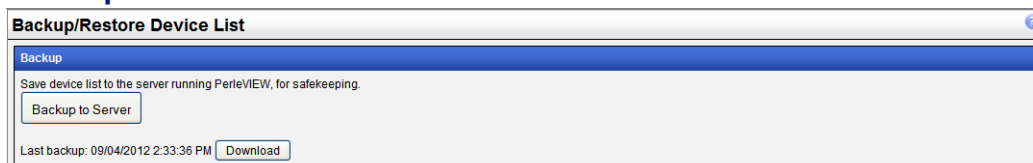
After the backup is completed you can click the **Download button** if you want to save your Device List to a different location for added safe keeping.

Working with Restore Device List

PerleVIEW will run a new discovery task using the device list as its list of IP addresses to discover. If a device already exists in the database, the device information will be updated with any new information collected during the discovery. PerleVIEW can create a device discovery task using the "Last Backed" list or a list which was previously downloaded (saved) after a backup operation.

Restore

41
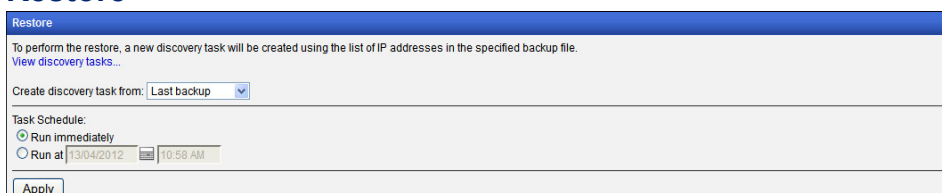
You can either select to run the **Restore immediately** or have it run at a later time by selecting the "**Run at**" option. Click the **Apply button** to create the discovery task instance for this restore operation.

Backup/Restore Device Configuration

Menu Selection: Backup/Restore Device Configuration

Minimum Run Authorization: PerleVIEW Administrator

PerleVIEW provides the ability to backup and restore individual device configurations to the PerleVIEW repository. Each device's configuration will be saved to a separate file which will be permanently associated with that device. Once backed up, if a need ever arises, you will be able to restore the configuration to that device.

Launching Backup/Restore Device Configuration

Backup/Restore Device Configuration

Working with Backup Device Configuration

PerleVIEW provides the following backup/restore device configuration functions.

- Run a Backup Device Configuration task instance now
- Enable/Disable Backup Device Configuration task instance
- Add a Backup Device Configuration task instance to your PerleVIEW database.
- Edit a Backup Device Configuration task instance
- Delete a Backup Device Configuration task instance

Each Backup/Restore task instance can have unique operating parameters such as which devices it will operate on as well as unique scheduling parameters

43

Run Now

To run a existing Backup Device Configuration task immediately, select the task from the list, then click on the **Run Now button.**

Add

Click on the **Add button** to create a new Backup Device Configuration task instance.

Task name	Enter a name to uniquely identify this backup task instance.
Targets	Choose which devices to back up. This can be done by selecting individual devices or by selecting a device group.
Schedule	See *Add a Device Discovery Task* for configuration parameters.

Working with Restore Device Configuration

PerleVIEW provides the following Restore Device Configuration functions.

- Run a Restore Device Configuration task instance now
- Enable/Disable a Restore Device Configuration task instance
- Add a Restore Device Configuration task instance to your PerleVIEW database.
- Edit a Restore Device Configuration task instance.
- Delete Restore Device Configuration task instance.

Each Restore Device Configuration task instance can have unique operating parameters.

44

Run Now

To run an existing Restore Device Configuration task instance immediately, select the task from the list, then click on the **Run Now button.**

Add

Click the **Add button** to create a new Restore Device Configuration task instance.

Task name	Enter a name to uniquely identify this Restore Device Configuration task instance.
Targets	Choose which devices to you wish to restore the configuration for. This can be done by selecting individual devices or by selecting a device group.
Schedule	See *Add a Device Discovery Task* for configuration parameters.
Reboot	PerleVIEW will reboot the device after the configuration has been restored. Since many configuration parameters only take place after a reboot, this option is on by default.

45

Task Details

This window displays the current task details of the selected Backup Device Configuration task instance.

To delete device configuration from the PerleVIEW database, click on "Device with Saved Configuration" option.

Devices with saved configuration

For each device on the list, you are presented with some basic information on the device. This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view

Select the device with the saved configuration that you want to delete from the PerleVIEW repository, then click the **Delete saved configuration button** to delete.

Configure Device Settings

Menu Selection: Device Settings

Minimum Run Authorization: PerleVIEW Administrator
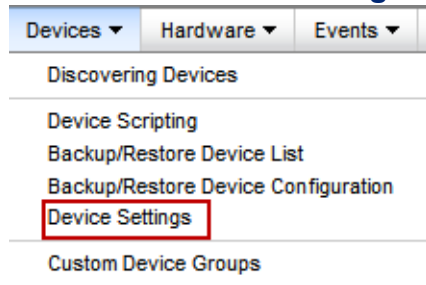
This function allows you to change a number of device related, global parameters. These include settings for Device Discovery tasks, Device credentials, Polling timers and Network protocol settings.

Launching Device Settings

Devices ->Device Settings

Working with Device Settings
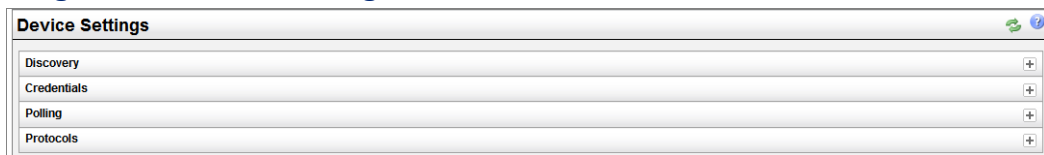
Discovery

The Device Settings screen allows you to change global parameters for the device discovery task. You can create filters to limit the scope of the device discovery task. This is done by configuring which specific IP addresses or range of addresses you want to exclude from the discovery.

Additionally, you can configure the default setting for the "automatically discover devices when SNMP trap is received from that device".

Lastly, at the time of device discovery, you can have the PerleVIEW add its IP address to the device's list of SNMP trap hosts. This will ensure that PerleVIEW receives notifications whenever a trap is generated by the device.

These changes do not affect existing device discovery task instances. They will be used the next time you set up a new device discovery task instance.

Click the **Apply button** to save the changes.

47

Exclude the following IP addresses and ranges from device discover.	To exclude certain IP addresses or IP ranges from the device discovery task, add entries to the table. Valid options are IP addresses and IP ranges. Exclude a single IP address or a range of IP addresses. examples: 172.16.1.5 (excludes a single IP address) 172.16.10.1 - 172.16.10.100 (excludes addresses 1-100 in the specified subnet of 172.16.10)
Automatically discover device when a SNMP trap is received from that device.	If PerleVIEW is configured as an SNMP trap host for this device, when the device sends a trap to PerleVIEW, this will cause PerleVIEW to add the device to its database (i.e. automatically discover the device) if it is not already in the database. When this happens, the global parameters are used for protocol timers and credential validation for this device.
At time of discovery, set PerleVIEW as a trap host for the discovered device.	If this option is set, when PerleVIEW discovers a new device, it will modify the configuration of that device to add PerleVIEW's server address to the device's SNMP trap host table.

Credentials

These credentials are the global settings used when PerleVIEW attempts to discover valid credentials for a devices. PerleVIEW will attempt each of the configured **SNMP credentials**, configured **Login credentials** and configured **SSH keys**. If credentials are specified with the discovery task instance, they will be attempted first. If they fail, the global credentials will be attempted.
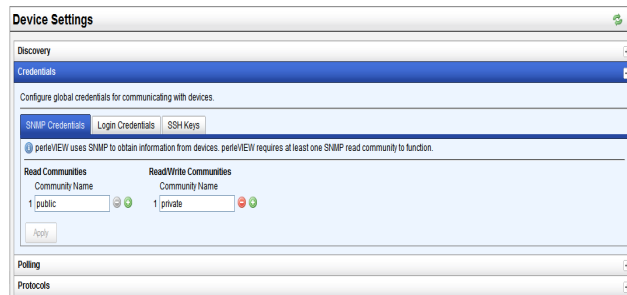
You can configure up to 10 SNMP Read and Read/Write communities within PerleVIEW. These configured SNMP communities need to match the configured SNMP Read and Read/Write communities configured on one or more of your devices. SNMP Read Only communities allow you to only read from the devices to get status information whereas Read/Write communities allow you to also control the target device (example: reboot the device).

You can configured up to 10 login id's for administrator and operator under Login credentials These configured administrator and operator login id's must match users configured within the devices user database. PerleVIEW will use these login credentials whenever it needs to log into a device. Examples of this is when PerleVIEW needs to Telnet to a device to deploy a "device script" or when a user is performing a Web Management session with the device.

You can configure up to 10 SSH keys under SSH Keys. These will be used when PerleVIEW needs to SSH to a device and the device has been set up to use SSH keys. The devices must have the correct SSH public key configured for you to be logged into this device using this SSH private/public key pair.

48

SNMP Credentials

As each device is discovered, the credentials configured will be tried on it until one set is found to work. This set will be saved as the working credentials for that device.

| Read SNMP Communities	You can configure up to 10 SNMP Read communities within PerleVIEW. These configured SNMP communities need to match the configured SNMP Read communities configured on one or more of your devices. SNMP Read Only communities allow you to only read from the devices to get status information. Each configured community will be tried against each device until a valid match is found. This set will be saved as the working credentials for that device.
Read/Write SNMP Communities	You can configure up to 10 SNMP Read/Write communities within PerleVIEW. These configured SNMP Read/Wrote communities need to match the configured SNMP Read/Write communities configured on one or more of your devices. Read/Write communities also allow you to control the target device (example: reboot the device). Each configured community will be tried against each device until a valid match is found. This set will be saved as the working credentials for that device.

To access all of PerleVIEW's features at least one Read or Read/Write community must be configured within PerleVIEW to match a SNMP community configured on the target device.

Login Credentials

As each device is discovered, the credentials listed will be tried on it until one set is found to work. This set will be saved as the working credentials for that device.
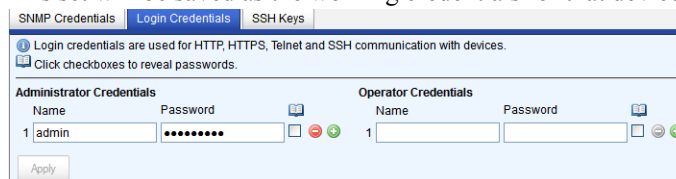
Administrator Credentials	Use Administrator login depending on the privilege level that the users has on the target device. These credentials are used to log into the device. (for example: Direct management of the device using Telnet) or to run some PerleVIEW functions (for example: Device Scripting).
	Configure up to 10 Administrator user names and passwords that PerleVIEW will validate against the device until a valid pair is found.

49

Operator Credentials	Use operator login depending on the privilege level that the users has on the target device. These credentials are used to log into the device. (example Direct management of the device using Telnet).
	Configure up to 10 Operator user names and passwords that PerleVIEW will validate against the device until a valid pair is found.

SSH Keys

As each device is discovered, the credentials listed will be tried on it until one set is found to work. This set will be saved as the working credentials for that device.

Administrator/ Operator Private Key	The target device must have SSH keys enabled in order to use SSH Keys. You would then be logged into the device using a SSH private/public key pair. PerleVIEW will SSH to each device using each of the configured SSH user and associated private key until a valid match is found. The device must have the correct SSH public key configured for successful authentication.

Polling

Polling parameters allow you to customize how often a device or hardware within PerleVIEW's database will be polled for status, health or reachability.

Device reachability	The device polling task will run immediately with the startup of PerleVIEW. You can set how often PerleVIEW will attempt to communicate to the device to see if the device is still reachable.
Hardware health	Sets how often PerleVIEW checks for any outstanding alarm conditions on each device. See *Health Status Panel* for more information.
Media converter port link status	Sets how often PerleVIEW checks the Media converter port link status for each hardware port. The media converter link port status results (up or down) can be viewed under **Group Views -> Hardware -> Ports.**
Rediscover devices	Set the time to run a Rediscover devices task on all devices and hardware. The re-discovery task will go through all existing devices in the database and attempt to re-validate credentials, collect hardware health, reachability and link statuses. This task will not discover new devices. To discover new devices run a Device Discovery task instance.

50

Protocol Settings

HTTP/HTTPS
Telnet, SSH

Connection Timeout   Specify the maximum time to wait when establishing various types of connections between PerleVIEW and the device.

SNMP, ICMP and Perle Discovery protocol

Timeout   Specify how long to wait for a reply from the device after sending either a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery request. This field should contain the value in seconds of the device which has the longest response time.

Default: 3 seconds

Values: 1-255

(*) denotes - leave blank to use global parameter

Retries   Specify how many retries to attempt when no response received from a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery request.

Default: 2

Values: 0-255

(*) denotes - leave blank to use global parameter

Custom Device Groups

For more information on Custom Device Groups see *Creating Custom Views by Groups* .

51

5 Groups of Devices, Hardware, and Events

Groups Views

Group Views allows you to quickly and easily see the Devices, Hardware and Events found in your managed network. You can quickly drill down though submenus to get details about these devices, hardware or events. From these submenus you can manage and control most features of your devices as well, you can view and edit your installed hardware modules such as management modules, media converter modules and individual media converter ports. Events or alerts on your system can be easily acknowledged or deleted to help you keep on top of the more critical events within your network. Custom device, hardware and event groups can be created to sort and maintain your own custom views. See *Creating Custom Views by Groups* .

PerleVIEW supplies you with four pre-defined Group Views under the submenu **Devices.** Each group will display all devices which have been discovered on your network but will group them based on different criteria.

The groupings are as follows:

- All Devices - View all discovered devices on your network. From the left-hand navigation panel select **Devices -> All Devices**

- Subnets - View all discovered devices grouped by IP subnets. From the left-hand navigation panel select **Devices -> Subnets**

- Health - View all discovered devices grouped by their current health status. From the left-hand navigation panel select **Devices -> Health.**

- Limited Functionality - View all discovered devices with limited functionality. From the left-hand navigation panel select **Devices -> Limited Functionality.** Limited functionality devices are devices that are not configured (example: do not have an IP address) or devices that need to update their firmware level. If no devices exist for this category, the group will not show up in the left-hand navigation panel.

Launching Groups Views

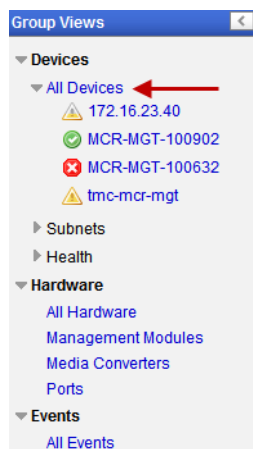From the left-hand side navigation panel, select Group Views.

Select Group Views

52
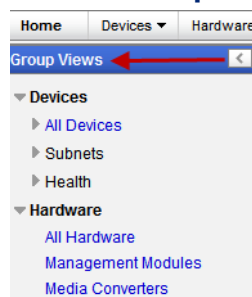
Working with Device Views

To View All Devices select **Devices -> All Devices** from the left navigation panel.

Devices ->All Devices

This view shows all of the devices which are present in the PerleVIEW device database.

At the top of the screen there is a count for the number of devices in the list which fall into each health category. For an "All Device" view, this count will match the count on the title bar.

For each device on the list, you are presented with some basic information on the device. This view can be customized by clicking on the "Columns" button on the top, right hand of the table.

You can select one or more devices by selecting the checkbox to the left of the device. Once selected, you can click on one of the buttons at the bottom to perform an action on the device(s) selected.
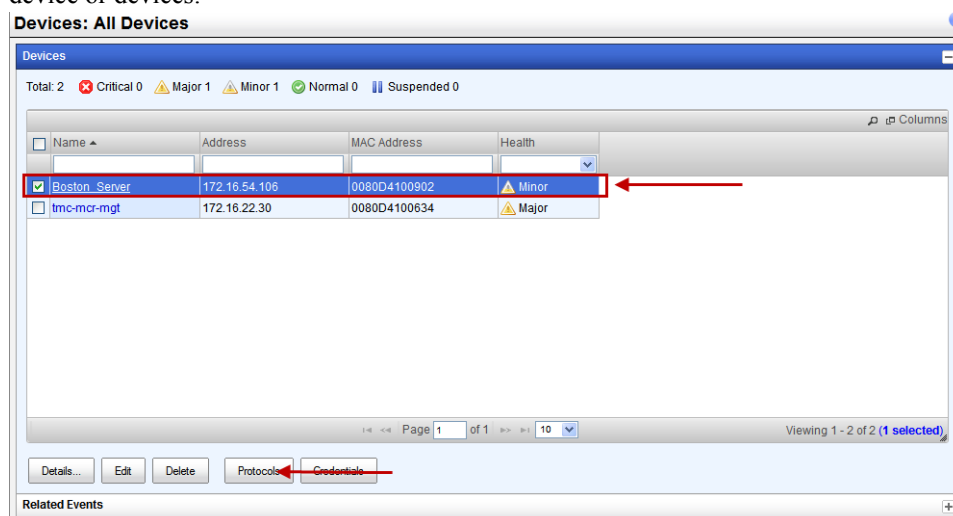
All Devices

For each device on the list, you are presented with some basic information on the device. This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view
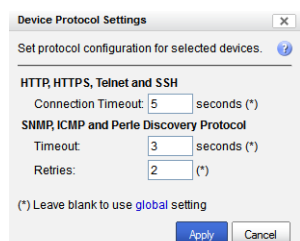
53

Details
Use the Details button to bring up a table with various information and actions that can be performed on the selected device. The same can be achieved simply by clicking on the device name. For more information see *Working with Device Views* .

Delete
Use the Delete button to remove a device or devices from the PerleVIEW database. All information for the device will be lost.

Edit
Use the edit button to change parameters for this device or devices. For more information see *Working with Device Views* .

Protocols (Device)

Click on this button to change the parameters related to protocol timeouts and retries for the selected device or devices.

Protocol Settings

HTTP, HTTPS, Telnet and SSH

    Connection Timeout
Specify the maximum time to wait when establishing various types of connections between PerleVIEW and the device.

SNMP, ICMP and Perle Discovery protocol

54

Timeout   Specify how long to wait for a reply from the device after sending either a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery request. This field should contain the value in seconds of the device which has the longest response time.

Default: 3 seconds

Values: 1-255

(*) denotes - leave blank to use global parameter

Retries   Specify how many retries to attempt when no response received from a UDP message on port 33816, an SNMP message, a ping message or a Perle Discovery request.

Default: 2

Values: 0-255

(*) denotes - leave blank to use global parameter

Credentials (Device/s)

Select the **Credential button** to delete or override credentials for this device or devices.

Credentials (Device/s)

To access all of PerleVIEW's features at least one Read or Read/Write community must be configured within PerleVIEW to match a SNMP community configured on the target device.

Select credentials to delete

SNMP Read Community	Select the checkbox for SNMP Read community if you do not want to attempt SNMP Read credentials for this device.
SNMP Read/Write Community	Select the checkbox for SNMP Read/Write community if you do not want to attempt SNMP Read/Write credentials for this device.
Operator Login	Select the checkbox for Operator Login if you do not want to attempt Operator Login credentials for this device.
Admin Login	Select the checkbox for Admin Login if you do not want to attempt Admin Login credentials for this device.
Operator SSH Key	Select the checkbox for Operator SSH Key if you do not want to attempt Operator SSH Key credentials for this device.
Admin SSH Key	Select the checkbox for Admin SSH Key if you do not want to attempt Admin SSH Key credentials for this device.

Add/Remove override

SNMP Read	Select the checkbox to enter in your own SNMP Read credentials. These credentials will be used when attempting to validate credentials on this device/s.
SNMP Read/Write	Select the checkbox to enter in your own SNMP Read/Write credentials. These credentials will be used when attempting to validate credentials on this device/s.
Operator Login	Select the check box to enter in your own Operator Login credentials. These credentials will be used when attempting to validate credentials on this device/s.

56

Admin Login	Select the check box to enter in your own Admin Login credentials. These credentials will be used when attempting to validate credentials on this device/s.
Operator SSH Key	Select the check box to enter in your own Admin Operator SSH Keys. These credentials will be used when attempting to validate credentials on this device/s.
Admin SSH Key	Select the check box to enter in your own Admin SSH Key. These credentials will be used when attempting to validate credentials on this device/s.

This panel displays the device details. This is the same view you would get if you were to select a specific device from the Devices section on the left-hand navigation panel or double click on the device from the "All Device" view.

Device -> Details

Monitor Enable	PerleVIEW will monitor and maintain the device status and if needed will react to any events generated by the device. All tasks will run as scheduled.
Monitor Suspend	PerleVIEW will no longer monitor and maintain the current status of the device. Any events received from the device will be ignored. The following tasks will no longer run if scheduled. - Device Discovery, Device Rediscovery, Poll Hardware Health Status, Poll Media Converter Port Link Status and Poll Device Reachable task. The automatic event handler will not log entries to the log file and the event handler will not act on traps received from the device. However, tasks such as deploy firmware, device script, backup/restore device list and backup/restore device configuration will continue to run as scheduled.
Name	The name given to this device.
Health	See *Health Status Panel* for more information.

57

Health Details	This is the current health status of this device. To see more information on device generated messages (see your MCR-MGT users guide for Device messages).
User Access Level	This is the device access level for this device for the current user logged into PerleVIEW. Valid user access levels are Device View, Device Admin and Device Operator. For more information on user access levels see *PerleVIEW User Accounts* .
Address	This is what PerleVIEW will use when communicating with the device. It can be the hostname, IPV4 address or IPV6 address of the device.
IPV4 address/subnet	This is the current IPV4 address of this device and its subnet. (only available if configured/used on the device).
IPV6 Addresses	This is the current IPV6 address of this device. (only available if configure/used on the device).
Mac Address	This is the Mac Address associated with this device.
Description	This is a description retrieved from the device.
Location	This is the SNMP location information retrieved from the device.
Contact	This is the SNMP contact name retrieved from the device.
Uptime	How long this device has been powered on.
Management protocols	These are the management protocols configured on your target device. These management protocols will be used by PerleVIEW to communicate with your target device. If a protocol is not accessible, it will be marked with a red "X". One reason why a protocol may not be accessible is a firewall which is preventing access.

The information in this table is collected from the PerleVIEW database. When the table is being displayed, the information is updated every minute. Not all columns are applicable to all hardware. If not applicable, the entry will be left blank. For information on Rediscover this device see *Rediscover devices*.

58

Device Details -> Hardware

Device Details: MCR-MGT-100902

| Device | Hardware | Events | Protocols | Credentials | Tools |

□ Columns

Type	Health	Slot	📊	Power	Link	Port #	Port Type	Name	Model	Description
▼ Chassis	✅ Normal		No					MCR-MGT-100902	MCR1900	19 Slot C
Power Supply	✅ Normal	A	No						MCR-ACPWR	AC Powe
▼ Media Converter	✅ Normal	1	No	⚪ On				CM-1110-SFP	CM-1110-SFP	10/100/1
Port	✅ Normal	1	No		⚪ Down	1	Copper	Copper 1		
▼ Port	✅ Normal	1	No		⚪ Down	2	Fiber	Fiber 2		
SFP Module	✅ Normal	1	No							
Management Module	✅ Normal	3	No	⚪ On				MCR-MGT-100902	MCR-MGT	Managen
▼ Media Converter	✅ Normal	6	No	⚪ On				CM-110-M2SC2	CM-110-M2SC2	10/100 F
Port	✅ Normal	6	No		⚪ Down	1	Copper	Copper1		
Port	✅ Normal	6	No		⚪ Down	2	Fiber	Fiber 2		

Viewing 1 - 25 of 25

Edit...

Details

Click on a row to see more details...

> For each device on the list, you are presented with some basic information on the device. This view can be customized by clicking on the "Columns" button on the top, right hand of the table.

Column Details

Type
This is the type of hardware inserted in this chassis slot.

Health
This is the current health status for this device.To see more information on health statuses see *Health Status Panel* .

Slot
This is the physical slot location in the chassis where this module resides.

Statistics Collected
Indicates that statistics have been collected for this device. Depending on the hardware installed some devices will not have statistics associated with them. See here for more information on hardware statistics *Collecting Statistics* .

Power
The status of the power on this hardware.

Link
If applicable to the hardware type this will either be link up or down. Typically only applicable to a "port".

Port #
This is the port number for this port.

Port Type
This is the port type. Known values are copper, fiber or unknown (SFP port with no SFP inserted).

Model
Displays the model name for each hardware where applicable (i.e. ports don't have model names).

Description
The description of the hardware.

Serial number
The serial number of the hardware where applicable.

Firmware Version
The current version of firmware running on this hardware.

Connector Type
The connector type for this hardware. (RJ45, SC, ST, SFP). Typically only applicable to hardware of type "port".

Bootloader Version
The current version of bootloader firmware running on this hardware.

59

Preferred Name   The name the you typed in the Preferred field for this hardware.

Use Preferred Name   Check this box to use the Preferred Name from the above Name field. This would override a name retrieved from the hardware.

Custom 1, 2, 3   These field can be used to save information about this hardware to be used in logs, views and reports.

Device Details -> Hardware -> Edit

For each device on the list, you are presented with some basic information on the device. This view can be customized by clicking on the "Columns" button on the top, right hand of the table.

Select the hardware you want to edit, then click the **Edit button**.

Edit Hardware

Type   This is a non edit field. This is the internal name of the hardware type.

Name   This is the name retrieved from the hardware.

Preferred Name   Edit this field to replace the Name field for this hardware. You can enter a name here which better describes the selected hardware.

Use Preferred Name   Check this box to use the Preferred Name instead of the Name field. When checked, the preferred name will be used in all views, event logs and reports for this hardware.

60

Custom 1, 2, 3   These field can be used to save information about this hardware to be used in logs, views and reports.

Events Details

From this screen you are able to add a comment to an event, set an event as acknowledged or not, or delete the event from the database. By managing events on your network you will be able to view the events that are critical and deal with those events first.

Click on the Events tab to see the list of events associated with this device.

At the top of the screen there is a total of the number of events for each event severity.

Device Details -> Events

For each event on the list, you are presented with some basic information on the event. This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view

Column Details

Acknowledged   Displays whether this event has been acknowledged. Marking an event as "Acknowledged" simply indicates to you that you have seen and dealt with this event. The drop down acknowledged box allows you to sort by acknowledged yes or no.

Severity   Displays the severity of each event.

Time   Displays the time the event was received.

Description   This is a brief description of the event.

Action Taken   When an associated action exists for a given event, this column will display a link called "details....". Click on this link to obtain more information on the action performed. To view more information about events and Automatic Event handling see *Automatic Event Handling* .

Comment   Displays the comment that you specified in this field.

Log   This is the message entered into the log file. It contains detailed information about the event.

61

Click on any of the buttons below to change the details for a selected event.

Comment	Enter a comment about this event.
Mark as acknowledged	Mark an event as acknowledged if you have viewed or have no further action for this event.
Mark as unacknowledged	Unmark a previously marked acknowledged event as unacknowledged so that you are aware that an action is needed for this event. To help manage events, you can set up *Automatic Event Handling* or *Event Filter Settings* .
Delete	Permanently delete this event from the PerleVIEW event database.

Device Protocols

You can enter specific values to be used during communication with this device. These values will overwrite the values saved for this device during discovery. A blank value will cause the "global" value to be saved for this device. See global *Protocol Settings* for more information.

Click on the Protocol tab to edit the Protocol timers and Protocol retry counts for this device.

Device Details -> Protocols

HTTP, HTTPS, Telnet and SSH	
Connection Timeout	Specify the maximum time to wait when establishing various types of connections between PerleVIEW and the device.

62

SNMP, ICMP and Perle Discovery protocol	
Timeout	Specify how long to wait for a reply from the device after sending either a UDP message on port 33816, an SNMP message, a ping message or a Perle proprietary message. This field should contain the value in seconds of the device which has the longest response time.
	Default: 3 seconds
	Values: 1-255
	(*) denotes - leave blank to use global parameter
Retries	Specify how many retries to attempt when no response is received for a UDP message sent on port 33816 (response is on port 33815), any SNMP message, a ping request or a Perle proprietary message.
	Default: 2
	Values: 0-255
	(*) denotes - leave blank to use global parameter

Device Credentials

Configure **SNMP credentials**, **Login credentials** and **SSH keys** to be associated with the selected device or devices. Credential information entered here will be stored in the database for the selected device/s. These will be the credentials that PerleVIEW will attempt to use the next time it needs to access the device/s. If these credentials are tried and found not to work, an error will be logged in the log file. Global credentials will not be tried on this device/s.

Click on the **Credentials tab** to edit device credentials for SNMP communities, Login accounts and SSH Keys.

To edit a specific credential, select the checkbox to the left of the credential to enable the field for entry. Blank entries cannot be saved.

Click the **Apply button** to save the changes.

63

Device Details -> Credentials

Device Details: Boston_Server

| Device | Hardware | Events | Protocols | Credentials | Tools |

Attempted Credentials:

✓ SNMP Read   [Delete...]
✓ SNMP Read/Write   [Delete...]
✓ Operator Login   [Delete...]
✓ Admin Login   [Delete...]
✗ SSH Key Operator [Delete...]
✗ SSH Key Admin   [Delete...]

Override Credentials:

☐ SNMP Read Community   [_____]
☐ SNMP Read/Write Community [_____]

                          Username   Password
☐ Operator Login   [_____]   [_____]
☐ Admin Login   [_____]   [_____]

                          Username   SSH Key
☐ Operator SSH Key   [_____]   [_____] [Browse...]
☐ Admin SSH Key   [_____]   [_____] [Browse...]

[Apply]

> To access all of PerleVIEW's features at least one Read or Read/Write community must be configured within PerleVIEW to match a SNMP community configured on the target device.

Attempted Credentials

SNMP Read

The check mark indicates that a SNMP Read community was found for this device during the discovery process, these credentials were tried and were found to be successful. A red "X" next to the credential indicates that this specific credential could not be validated for this device.

SNMP Read/Write

The check mark indicates that a SNMP Read/Write community was found for this device during the discovery process, these credentials were tried and were found to be successful. A red "X" next to the credential indicates that this specific credential could not be validated for this device.

Operator Login

The check mark indicates that a Operator Login was found for this device during the discovery process, these credentials were tried and were found to be successful. A red "X" next to the credential indicates that this specific credential could not be validated for this device.

SSH Key Operator

The check mark indicates that a SSH Key Operator was found for this device during the discovery process, these credentials were tried and were found to be successful. A red "X" next to the credential indicates that this specific credential could not be validated for this device.

Admin SSH Key

The check mark indicates that a SSH Admin Key was found for this device during the discovery process, these credentials were tried and were found to be successful. A red "X" next to the credential indicates that this specific credential could not be validated for this device.

Override Credentials

SNMP Read

Select the checkbox to enter in your own SNMP Read credentials. These will be used when attempting to validate credentials on this device.

SNMP Read/Write

Select the checkbox to enter in your own SNMP Read/Write credentials. These will be used when attempting to validate credentials on this device.
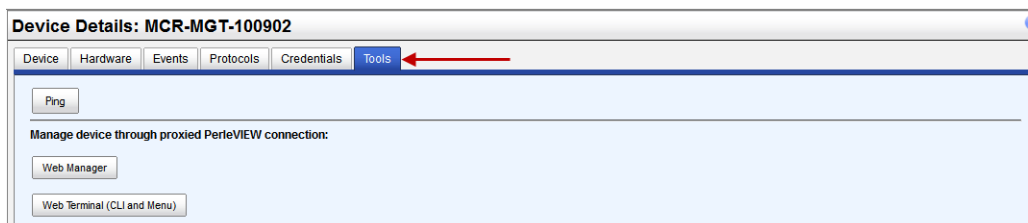
64

Operator Login	Select the check box to enter in your own Operator Login credentials. These will be used when attempting to validate credentials on this device.
Admin Login	Select the check box to enter in your own Admin Login credentials. These will be used when attempting to validate credentials on this device.
Operator SSH Key	Select the check box to enter in your own Operator SSH Key credentials. These will be used when attempting to validate credentials on this device.
Admin SSH Key	Select the check box to enter in your own Admin SSH Key credentials. These will be used when attempting to validate credentials on this device.

Device Details Tools

The Device details "Tools" tab allows you perform actions directly on the device. These include pinging the device to see if it is still reachable or to access the device via a Web or Terminal interface. Even though you are accessing the device, PerleVIEW is still involved in the connection. If login is required to access the device, PerleVIEW will automatically perform this action on your behalf. The connection to the device is via PerleVIEW which allows you to access the device event if it is not directly accessible to the client PC. This is because the client PC is communicating directly with PerleVIEW. The PerleVIEW software re-directs the client messages to the device.

To use Web Manager, the target device must have HTTP or HTTPS enabled. If both HTTP and HTTPS are enable, HTTP will be tried first. To use Web Terminal the target device must have Telnet or SSH enabled. If both SSH and Telnet are enable, Telnet will be tried first unless PerleVIEW is configured to only use secure connections. To enable secure connections only, see *Working with Server Settings* for more information.

Device Details -> Tools

Ping	The **Ping button** will send 10 ICMP echo request packets to the device to test for reachability.
Web Manager	The **Web Manager button** allows PerleVIEW to connect to your target device acting like a transparent proxy server. The web browser communicates directly to PerleVIEW and PerleVIEW either HTTP or HTTPS to the target device. HTTP requests will be send on TCP port 80 and HTTPS requests will be send on TCP port 443. The target device must have these ports enabled for successful communication.
Web Terminal (CLI or Menu)	The **Web Terminal button**, allows you to connect to your device using Telnet or SSH. Telnet will establish a session to TCP port 23 and SSH will establish a session to TCP port 22. The target device must have these services enabled for successful communication.

65

View Devices by Subnets

View Devices by subnets groups your devices based on the subnet they reside on. You can choose to view all devices on a particular subnet or use the subnet information to drill down to a specific device on that subnet.

To view device by subnets select **Devices -> Subnets** from the left navigation panel.

Devices -> Subnets
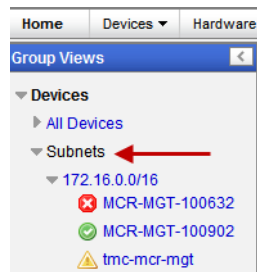
To view details see *Groups Views* .

View Devices by Health

This view allows you to view all devices grouped by their current health status. The health status of a device can be one of the following statuses: critical, major, minor, normal or suspended. A device may have a number of outstanding issue. The health status represents the most severe condition which currently exists.

To view Devices by Health select **Devices -> Health** from the left navigation panel.

Devices -> Health
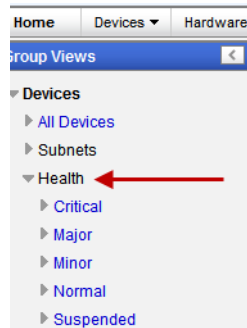
To view device details see *Groups Views* .

66

Limited Functionality

Devices that show up under the "Limited Functionality" grouping are devices that meet one of the following criteria;

Unsupported firmware

These devices are running firmware which is the pre v1.5 which is required in order to be fully supported by PerleVIEW. These devices need to be upgraded to the latest version of software available.

You can have PerleVIEW automatically retrieve the latest device firmware by enabling the "Check for Firmware Updates" feature. See *Check for Firmware Update* . Alternatively, you can download the latest firmware from the Perle Web site at `http://www.perle.com/downloads/`

Once you have obtained the latest firmware, you must now deploy it to the device. See *Deploying Firmware* .

Factory Default

These devices have never been configured. They contain the default IP address of 10.0.0.10. Before PerleVIEW can access these devices, you must assign a valid IP address to them. For more information see *Device -> Not Configured* .

This grouping may or may not show up on the left hand navigation panel. It only appears if there are devices that meet the criteria for this group.

To view Limited Functionality devices select **Devices -> Limited Functionality** from the left navigation panel.

Limited Functionality

67

Device -> Not Configured

Select the device you are interested in working with from the list, then click one of the action buttons. To work with this device, click on the **Details button**, **Edit button** or **Delete button**.

These are the details of this unconfigured device. Click on the **Assign IP Address Button** to assign an IP address.

Assign IP Address

Successful

Device - Unsupported Firmware

Select the device you are interested in working with from the list, then click one of the action buttons. To work with this device, click on the **Details button**, **Edit button** or **Delete button**.

69

To update this device with the latest firmware see *Check for Firmware Update* and *Deploying Firmware* .

Working with Hardware Views

PerleVIEW supplies you with four pre-defined Group Views under the submenu **Hardware.** These groups represent distinct hardware in your system.

They are as follows:

- All Hardware - View all discovered hardware on your network. From the left-hand navigation panel select **Hardware -> All Hardware**

- Management Modules - View all discovered Management Modules discovered on your network. From the left-hand navigation panel select **Hardware -> Management Modules**

- Media Converters - View all discovered Media Converter Modules on your network. From the left-hand navigation panel select **Hardware -> Media Converter Modules**

- Ports - View all discovered Media Converter Ports on your network. From the left-hand navigation panel select **Hardware -> Ports**

All Hardware

The information in this table is populated from information within the PerleVIEW database. When the table is displayed, the information is updated every minute.

To view All Hardware select **Hardware -> All Hardware** from the left navigation panel.

Hardware->All Hardware

All Hardware -> Edit

For this example select the chassis (device named tmc-mcr-mgt), then click the **Edit button.** To edit multiple media converters, select the boxes beside the fields to be edited. The text entered in these fields will be added to all selected hardware.

See *Working with Device Views* for more information.

Specifying The Type Of Hardware To View

You can select from any of the following hardware types to get a view of only this type of hardware.

To view all Management Modules discovered on your network select **Hardware -> Management Modules** from the left navigation panel.

71

Hardware->Management Modules
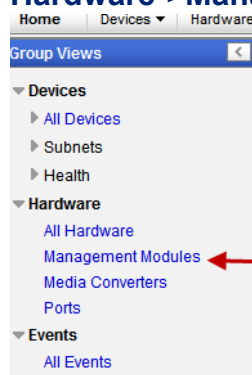
To view all Media Converters select **Hardware -> Media Converters** from the left navigation panel.

Hardware->Media Converters
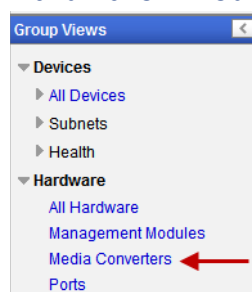
To view all Port select **Hardware ->Ports** from the left navigation panel.

Hardware->Ports
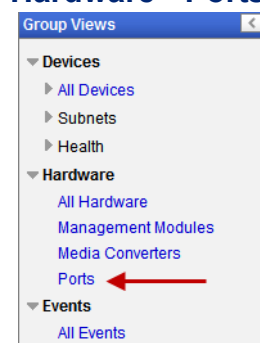
See *Groups Views* for more information.

Working with Event Views

PerleVIEW supplies you with one pre-defined Group View under the submenu **Events.**

● All Events - View all events generated by your devices or PerleVIEW.

Events

The events in this view can come from two sources. One is a trap received from a device which is being monitored by PerleVIEW. The second is an event which is generated by PerleVIEW itself (i.e. PerleVIEW detects that a device is no longer reachable). The column labeled "Source" provides information as to which of the above caused the event to be generated.

72

Managed devices must be configured to send events (traps) to PerleVIEW. After PerleVIEW receives the event, it applies any configured filters to the event, it then performs any actions configured under Automatic event handling and lastly the event is added to the PerleVIEW database for later viewing. For more information on Events and Automatic Event handling see *Automatic Event Handling* .

To view events select **Group Views -> Events** from the left navigation panel

Events->All Events
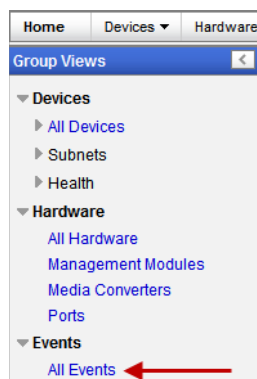
See *Working with Device Views* for more information.

6 Hardware Activities

Collecting Statistics

Menu Selection: Collect Statistics

Minimum Required Authorization: Device Operator

PerleVIEW provides you with the ability to create tasks to collect statistics from media converter ports on your devices. Statistics are only available on rate converting media converter module ports.

Launching Collecting Statistics

Select Hardware -> Collecting Statistics
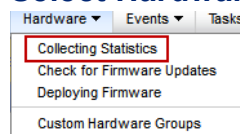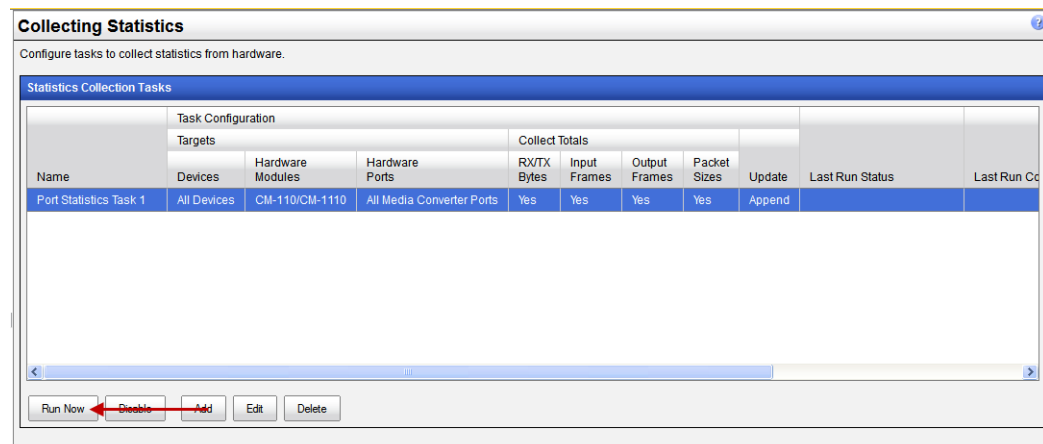
Working with Statistics Collection Tasks

PerleVIEW provides the following statistics collection task functions.

- Run a statistics collection task instance now
- Enable/Disable statistics collection task instance
- Add a statistics collection task instance to our PerleVIEW database
- Edit a statistics collection task instance
- Delete a statistics collection task instance

Run Now

74

To run an existing statistics collection task instance immediately, select the task from the list, then click on the **Run Now button.**

Add a Statistics Collection Task

Each Statistics Collection task instance can have unique operating parameters.

Add

To Add a new Statistics Collection instance, click on the **Add button**.

Task Name	Use a meaningful name to uniquely identify this statistics collection task.
Targets	Choose from the drop down boxes the Devices, Hardware and Media converter ports that you want to collect Statistical information from. The valid options are:

Devices:

- Select an existing "Devices" group.
- Select individual Devices from a list.

Hardware:

- Select all rate converting Media Converter Modules
- Select all CM-110 Media Converter Modules
- Select all CM-1110 Media Converter Modules
- Select all ex-1CM Media Converter Modules

Hardware Ports:

- MCR Media Converter
  - All Media Converter Ports
  - Fiber Media Converter Ports
  - Copper Media Converter Ports

Schedule	For more information see *Add a Device Discovery Task*.
Collect Totals	
RX/TX Bytes	Number of good bytes received, bytes received in error and number of bytes transmitted.

75

Input Frames	Number of good frames received in the following categories; • Unicast frames • Broadcast frames • Multicast frames • Pause frames Number of bad frames received in the following categories; • Undersized frames • Fragmented frames • Oversized frames • Jabber frames • MAC receive error frames • FCS error

Output Frames	Number of good frames transmitted in the following categories;
	• Unicast frames
	• Broadcast frames
	• Multicast frames
	• Pause frames
	Number of bad frames transmitted in the following categories;
	• FCS error
	• Deferred frames
	• Collision frames
	    • Excluding late and excessive
	    • Late
	    • Excessive
	    • Single
	    • Multiple

Packet Sizes	Number of frames which fall into the following categories; • 64 Bytes • 65 - 127 Bytes • 128 - 255 Bytes • 256 - 511 Bytes • 512 - 1023 Bytes • Over 1024 Bytes
Update Mode	**Append -** Each new sample collected is added to existing statistic samples already collected by this task. **Overwrite -** Each new sample collected replaces the previously collected sample. Only one sample (the latest) will be maintained.

Edit a Statistics Collection Task

Once the task has been run, only the Statistics Collection task instance name can be edited. To change target devices and parameters, you must create a new statistics collection task instance.

76

Edit

To Edit a Statistics Collection task instance, click on the **Edit button**.

Task Details

This panel displays the current task details of this task instance as well as the Last Run Results. See *Working with Device Views* for more details on logs, details and results.

77

Check for Firmware Update

Menu Selection: Check for Firmware Updates

Required Authorization: PerleVIEW Administrator

PerleVIEW can check the Perle Web site for new firmware updates for the devices that it manages. There are two options with regards to the action taken by PerleVIEW if an update is available. The first is to only have PerleVIEW notify the administrator that new firmware updates are available for its target devices. An administrator of PerleVIEW can then download the updates at their leisure. The second way is to have PerleVIEW automatically download firmware updates to its PerleVIEW repository when it detects that an update is available. The frequency for checking for updates is user configurable. To deploy firmware to the target devices see *Deploying Firmware*.

Launching Check for Firmware Updates

Hardware->Check for Firmware Updates
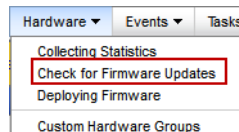
Working with Check for Firmware Updates

PerleVIEW provides the following configurable parameters for the "Check for Firmware Updates" function.

- User can set how often (in days) to check for firmware updates
- Action to take when updates are available;
  - Notify the administrator for any firmware updates
  - Notify and Automatically download any firmware updates

Check Now

Click the **Apply button** to save any changes.

Click the **Check Now button** to check the Perle Web site for any updates.

78

Check Now Results

Download Now Download Now indicates that there is a download pending. Highlight the entry and then select the **Download Now button**. The firmware will be transferred from the Perle Web site to the PerleVIEW repository.

Deploy Update Deploy Update will create a new Add Task Deploy Firmware task instance. For configuration parameters see *Add a Deploying Firmware Task*.

Delete Update Highlight the update to be deleted then select the **Delete Update button.** The selected firmware is now deleted from the PerleVIEW repository.

Changelog Provides a description of what is new or changed in this version of the firmware.

Bundled Firmware Provides details about the Media Converter Module firmware which is bundled within the Device firmware image.

Internet Proxy

Internet Proxy If your network uses a proxy for accessing the Internet, you can configure the proxy settings by clicking on this button. See your network administrator for Internet proxy parameter settings. See *Internet Proxy Server* to setup these parameters within PerleVIEW.

79

Firmware Deployment Tasks

Check for Firmware Updates

PerleVIEW can automatically check for updates to hardware it manages.

☑ Check for updates every 7 days

Action: Notify administrator of new updates ▾   Configure location for downloaded firmware

Apply

Check Now...   Internet Proxy...   Firmware Deployment Tasks ◄

Firmware Updates

No updates available.

Firmware Deployment Tasks

After the firmware has been download to the PerleVIEW repository or a directory location created by you, this firmware needs to be deployed to the target devices. To deploy firmware you need to create firmware deployment tasks instances. See *Deploying Firmware*.

80

Deploying Firmware

Menu Selection: Deploying Firmware

Required Authorization: Device Administrator

PerleVIEW manages it's firmware within the PerleVIEW's repository. Firmware images are uploaded into the repository. You can create firmware deployment tasks instances to download the firmware to target devices.

Launching Deploying Firmware

Hardware->Deploying Firmware
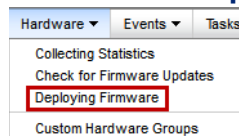
Working with Deploying Firmware

PerleVIEW provides the following task functions for Deploying Firmware.

- Run a existing Deploying Firmware task instance now
- Disable/Enable Deploying Firmware task instance
- Add a Deploying Firmware task instance to your PerleVIEW database
- Edit a Deploying Firmware task instance
- Delete a Deploying Firmware task instance

Run Now

To run an existing Deploying firmware task instance immediately, select the task from the list, then click on the **Run Now button.**

Add a Deploying Firmware Task

To create a task to deploy firmware to devices that are managed by PerleVIEW, click on the **Add button**. When you are done, click the **Apply button** to add the task to the PerleVIEW database.

You will be prompted to accept the licensing agreement in order to continue. Specify your country. If you reside in Germany you must select "Germany" as your country. Germany has unique licensing requirements. After selecting your country, click the **I Agree** button. Then click the **I Agree** to accept the Privacy Policy and continue the download.

Task Name	Use a meaningful name to uniquely identify this deploying firmware task instance.
Targets	Firmware can be deployed to Device groups, Custom Groups or selected individual devices.
Schedule	See *Add a Device Discovery Task* for configuration parameters.
Choose MCR-MGT firmware	Select the MCR-MGT firmware you wish to be downloaded to your target devices.
Reboot Management Module	This option causes PerleVIEW to reboot the device after the firmware has been downloaded to it. This will cause the new firmware to be executed. This is the default setting for this parameter.

This window displays the filename, source, date and version of all firmware in the PerleVIEW repository.

Manage Firmware

Use the **Import** button to if you wish to upload firmware images from other locations to the PerleVIEW repository.

Custom Hardware Groups

For more information on Custom Hardware Groups see Appendix A, Custom Views by Groups.

7 Tasks

Task

PerleVIEW provides you with the ability to create task instances for common functions you need to perform on your devices. By creating tasks this gives you the ability to control and schedule when certain functions will be performed (example: discovering devices or deploying software).

PerleVIEW Common Tasks

- Discovering Devices
- Collecting Statistics
- Device Scripting
- Deploying Firmware
- Backup/Restore Device Configuration

When you install PerleVIEW, it will automatically create some "system" tasks which it needs in order to properly function. You can edit the parameters for these default tasks instances, however they cannot be deleted.

PerleVIEW Default Tasks

- Default Device Discovery (see *Discovering Devices*)
- Default Device Rediscovery (see *Polling*)
- Events Cleanup (see *Event Cleanup*)
- Poll Hardware Health Status (see *Polling*)
- Poll Media Converter Port Status (see *Polling*)
- Poll Device Reachable (see *Polling*)
- Task Results Cleanup (see *Task Results Cleanup*)
- Application Update Notifier (see *PerleVIEW Updates*)
- Firmware Update Notifier (see *Check for Firmware Update*)

Tasks

Menu Selection: Tasks

Minimum Required Authorization: Depending on the task

Tasks are used by PerleVIEW to perform a variety of functions. If you need to perform an action which is different from the one being performed by the default system task, you can create your own instance of task using this menu. As an example, you may be going through an expansion which will be adding devices over the next month in a particular subnet. In order to have PerleVIEW detect these devices quickly, you may wish to create a discovery task instance which only polls this subnet for any new devices. You could set this task to run every day in order to make sure that you detect any devices added during the day.

Creating new tasks allows you to deploy your specific parameters and scheduling for each instance of the task.

You can create tasks from many of the other menus as well. The end result is the same regardless of which menu item was used to create the task instance. For example creating a "Device Scripting" task from the "Devices" menu is the same as creating it from the "Tasks" menu.

Launching Tasks

Tasks ->Tasks
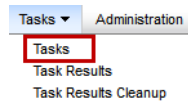
Working with Tasks

PerleVIEW provides the following task selections.

- Run a task instance immediately
- Enable/Disable a task instance
- Add a task instance
- Edit a task instance
- Delete a task instance

Each task instance can have unique operating parameters. PerleVIEW also provides options to enable/disable, delete and edit existing task instances.

Run Now

To run a task immediately, select a task from the task list, then click on the **Run Now button.**That task will execute immediately using the parameters configured for that task instance. Once run, the task will resume its normal schedule.

Add

To create a new task, click on the **Add button,** then select a task from the drop down list.

To create a Discovering Device task instance see *Discovering Devices*.

To create a Collecting Statistics task instance see *Collecting Statistics*.

To create a Device Scripting task instance see *Device Scripting*.

To create a Deploying Firmware task instance see *Deploying Firmware*.

To create a Backup/Restore Device Configuration see *Backup/Restore Device Configuration*.

Last Run Results

To view All Results, View Log, or Target Results see *Working with Device Views*.

86

Task Results

Menu Selection: Task Results

Minimum Required Authorization: None

This menu item provides access to the task results for all task instances which have been run by PerleVIEW.

Launching Task Results

Task -> Task Results
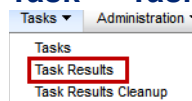
Working with Task Results

PerleVIEW provides the following actions which can be performed on a specific task result.

- Stop a Task instance (only available if the task is currently running)
- Delete a Task instance
- View the Log for that task instance
- View the Target Results for that task instance

Task Results

Result ID	Task Name	Status	Log	Target Results	End Time	Start Time	User
625	Poll Device Reachable	Complete	Yes	Yes	04/05/2012 2:18 PM	04/05/2012 2:18 PM	PVAdmin
624	Poll Media Converter Port Status	Complete	Yes	Yes	04/05/2012 2:13 PM	04/05/2012 2:13 PM	PVAdmin
623	Poll Device Reachable	Complete	Yes	Yes	04/05/2012 2:13 PM	04/05/2012 2:13 PM	PVAdmin
622	Poll Device Reachable	Complete	Yes	Yes	04/05/2012 2:08 PM	04/05/2012 2:08 PM	PVAdmin
621	Poll Hardware Health Status	Complete	Yes	Yes	04/05/2012 2:03 PM	04/05/2012 2:03 PM	PVAdmin
620	Poll Media Converter Port Status	Complete	Yes	Yes	04/05/2012 2:03 PM	04/05/2012 2:03 PM	PVAdmin
619	Poll Device Reachable	Complete	Yes	Yes	04/05/2012 2:03 PM	04/05/2012 2:03 PM	PVAdmin
618	Poll Device Reachable	Complete	Yes	Yes	04/05/2012 1:58 PM	04/05/2012 1:58 PM	PVAdmin
617	Poll Media Converter Port Status	Complete	Yes	Yes	04/05/2012 1:53 PM	04/05/2012 1:53 PM	PVAdmin

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

[Stop] [Delete] [View Log] [Target Results]

Results ID	This is a PerleVIEW's internal task ID.
Task Name	This is the task name you gave this task when you created it or the default task name.
Status	The following statuses are valid:

- In progress - Task is currently executing
- Completed - Task has completed running
- Cancelling - Task is the process of being cancelled.
- Cancelled - Task was cancelled by PerleVIEW before it completed.
- Stopped - Task was cancelled by user before it completed.
- Failed - Task completed with a failure.

Log	Displays whether there are any messages in the log.
Target Results	Displays whether there are any target specific results for this task instance.

87

End Time   Shows the time when this task instance finished running.

Start Time   Shows the time when this task instance started running.

User   This is the user that created this task.

To view the Log or Target Results see *Working with Device Views*

Task Results Cleanup

Menu Selection: Task Results Cleanup

Minimum Required Authorization: PerleVIEW Administrator

The purpose if this clean up task is to remove old task results which are no longer needed from the PerleVIEW database. PerleVIEW will perform the clean up operation periodically in an attempt to maintain the number of task results in the database to the configured level. Doing this will keep the size of the database down as well as provide you with a more relevant list of task results.

This Cleanup Task will delete from the PerleVIEW database:

- Older scheduled Tasks results
- "Run Now" Task results
- Target Task results

PerleView will log the total number of each task results removed from the database.

You can configure parameters to schedule this cleanup task to run at a later time or click the **Run Now button** to perform a cleanup of task results now.

Launching Task Results Cleanup

Tasks ->Tasks Results Cleanup
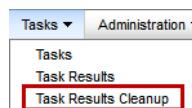
Task Results Cleanup

Scheduled Results	This subsection defines the criteria for removing task results associated with scheduled tasks (as opposed to tasks which were manually run).

You can set the number of task results to keep for each task. The latest results will be kept.

Default: 10 (last 10 task results for each scheduled task)

Values: 1- 99999 task results

You can optionally delete task results which are older than the specified number of days.

Default: 30 days

Values: 1-999 days

89

Run Now Results   This subsection defines the criteria for removing task results associated with manually run tasks (as opposed to scheduled tasks).

You can set the maximum number of task results to keep for all run now task instances. The latest results will be kept.

Default: 200 task results

Values: 1- 99999 task results

You can optionally delete "run now" task results which are older than the specified number of hours.

Default: 24 hours

Values: 1-999 hours

Click the **Apply button** to save your changes.

To run a clean up task immediately, click on the **Run Now button.**

90

8 Events

Events

Events can come from two sources. One is an SNMP trap received from a managed device which is being monitored by PerleVIEW. The second is an event which is generated by PerleVIEW itself (for example: PerleVIEW detects that a device is no longer reachable). After PerleVIEW receives the event, it applies any configured filters to the event, it then performs any actions configured under Automatic Event Handling and lastly the event is added to the PerleVIEW database for viewing.

By default, PerleVIEW will capture all events (Critical, Major, Minor, Warning, Normal and Informational). You can modify which type of events you want PerleVIEW to process by setting the Global Event filters (see *Event Filter Settings*). You can also specify what type of action you want PerleVIEW to take for a given event severity. PerleVIEW also allows you to configure the source of the event(s) you wish to take action on (see *Automatic Event Handling*). If an event is filtered out via the global filters, it will be discarded and no further activity will be performed on that event. The only exception is the "Automatically discover device when SNMP trap is received from that device" function. If enabled, this will be performed on all events received from devices regardless of the global filter settings.

It is important to manage the events on your system in order to properly see the overall health and statuses of devices on your network. PerleVIEW allows you to put handling in place which will perform the desired activity when an event occurs. It also provides facilities for periodically cleaning up the event database.

Automatic Event Handling

Menu Selection: Automatic Event Handling

Minimum Required Authorization: Device Operator

PerleView has the capability of configuring Automatic Event Handling task instances to automatically inform you of events generated from your devices or from PerleVIEW itself.

Launching Automatic Event Handling

Events ->Automatic Event Handling

91
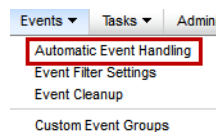
Working with Automatic Event Handling

PerleVIEW provides the following automatic event handling task functions.

- Enable/Disable an automatic event handling task instance
- Add an automatic event handling task instance
- Delete an automatic event handling task instance
- Edit an automatic event handling task instance

Each Automatic Event Handling task instance can have unique operating parameters.

Automatic Event Handling
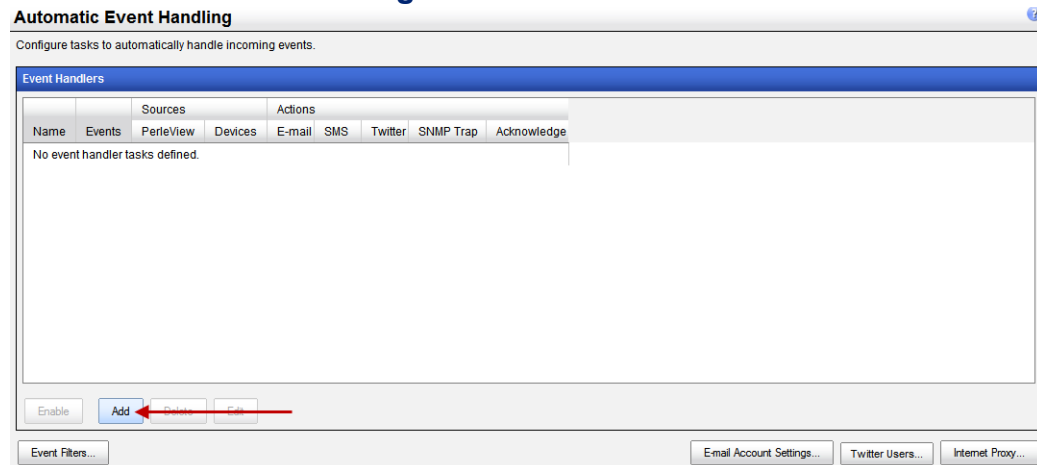
To create a task to automatically handle an event, click on the **Add button**.

Add

| Task name | Use a meaningful name to uniquely identify this event handling task instance. |

Targets

Events	Select the "type" of events you want this automatic event handling task instance to act upon. You can select all events or select the severity level of an event. Valid options are Critical, Major, Minor, Warning, Normal, Informational and Important Events (Important Events are the grouping of Critical, Major and Minor events).
Sources	Select the source from which the event is generated. Sources can either be a PerleVIEW application or/and a Device event. When selecting devices, you can select from any of the "device" groups as the source for the event.

Actions

Select the action that you want PerleVIEW to perform if it receives this event. You can select multiple actions.

The following actions are available:

- Send an E-mail. See *Send E-mail* .
- Send an SMS text message (via E-mail). See *Send SMS Text Message (via E-mail)* .
- Send a Tweet on Twitter. See *Send Tweet on Twitter* .
- Send a SNMP Trap message. See *Send SNMP Trap Message* .
- Acknowledge the event (PerleVIEW Administrator only). See *Acknowledge Event* .

Send E-mail

Send E-mail	
To	Configure the user's E-mail address to receive this E-Mail message.
CC	Configure the user's E-mail to sent a carbon copy of this E-Mail message.

93

Subject	Type in a message for the subject that is meaningful to you.
	By default, PerleVIEW uses internal macros to configure the subject message as:
	Event on ${DeviceName} at IP address ${DeviceIPAddress}
	Where ${DeviceName} is the actual Device Name or the Preferred Name if configured.
	${DeviceIPAddress} is the IP address of the device.
Body	Type in a body message that is meaningful to you.
	By default, PerleVIEW uses internal macros to configure the body message as:
	Event occurred on ${DeviceName} at IP address ${DeviceIPAddress}.
	${EventMessage}
	Where ${DeviceName} is the actual Device Name or the Preferred Name if configured.
	${DeviceIPAddress} is the IP address of the device.
	${EventMessage} is the text of a PerleVIEW generated message, see Appendix B, "Event Information" or a Device generated message (see your MCR-MGT users guide for Device messages).

After completing the fields, you can click on the **Test button** to test the connection to the E-Mail server. PerleVIEW will send a test message of "PerleVIEW event action handler test E-mail message". If the test E-Mail is received at the destination, the test is successful. If not successful, then correct the parameters in error and retry the test.

If you do not wish to add any other actions to this event, then click on the **Apply button** to save the task instance.

Send SMS Text Message (via E-mail)

Send SMS Text Message (via E-mail)	
Phone number	Configure the cellular phone number where the SMS message will be sent. For example: 9054770000

Carrier Domain	Configure a Carrier Domain.
	For example: @txt.bell.ca

Subject	Type in a message for the subject that is meaningful to you.
	By default, PerleVIEW configures the subject message as:
	Event on ${DeviceName}
	where ${DeviceName} is the actual Device Name or the Preferred Name if configured.

Body	Type in a body message that is meaningful to you.
	By default, PerleVIEW configures the Body message as:
	${EventMessage} where ${EventMessage} is either a PerleVIEW generated message see Appendix B, "Event Information" or a Device generated message (see your MCR-MGT users guide for Device messages).

Any SMS text messages over 140 characters will be sent as multiple messages.

After completing the fields, click on the **Test button** to test the SMS connection. PerleVIEW will send a test message of "PerleVIEW event action handler test SMS text message". If the SMS is received at the destination, the test is successful. If not successful, then correct the parameters in error and retry the test.

If you do not wish to add any other actions to this event, then click on the **Apply button** to save the task instance.

Send Tweet on Twitter

Send Tweet on Twitter	

User	Choose a "previously authorized" user from the drop down box or click on Authorize user to create a new authorized user. To authorize a user, PerleVIEW will take you to the twitter site where you will be asked to log in (you need a twitter account for this). Once logged in, you will be asked to authorize PerleVIEW to tweet via your account. Click the refresh link to update any new Twitter users after they have been added.

95

Message
Type in a message that is meaningful to you.

$[{DeviceName}]${EventMessage}

where ${DeviceName} is the actual Device Name or the Preferred Name if configured.

${EventMessage} where ${EventMessage} is either a PerleVIEW generated message see Appendix B, "Event Information" or a Device generated message (see your MCR-MGT users guide for Device messages).

> Any tweets over 140 characters will be sent as multiple messages. The Twitter API only allows clients (like PerleVIEW) to make a limited number of tweets in a given hour/day. PerleVIEW will not exceed that limit. Carefully select what severity level of events you want PerleVIEW to tweet for you. See www.twitter.com for more information on rate limiting.

After completing the fields, click on the **Test button** to have PerleVIEW send a test tweet using the authorized user's Twitter account. PerleVIEW will send a test message of "PerleVIEW event action handler test Twitter message". If the tweet is issued, the test is successful. If not successful, then correct the parameters in error and retry the test.

If you do not wish to add any other actions to this event, then click on the **Apply button** to save the task instance.

Send SNMP Trap Message

Edit Task: Automatic Event Handler

Task Name: Event Handler 3
ⓘ This task requires Device Operator rights
Targets
Events: All Events ▾
Sources: ☑ PerleView
☑ Devices All Devices ▾
Actions
☐ Send E-mail
☐ Send SMS Text Message (via E-mail)
☐ Send Tweet on Twitter
☑ Send SNMP Trap [Test]
Host: _Hostname/IP address_
Port: 162
Community: public
Mode: v2c ▾
☐ Acknowledge Event

[Apply] [Cancel]

Send SNMP Trap

Host
Specify the host name or IP address where this SNMP trap message will be sent. This host is known as the listening Trap Receiver.

Port
Specify the SNMP port number that the Trap Receiver is listening on.
Default: 162
Values: 1-65535

Community
Specify the community name that is used by the Trap Receiver.

Mode
Select the SNMP mode V1 or Vc2.
Default: Vc2

96

> To view SNMP traps on the Trap Receiver, you must load both the MCR-MGT Management Module MIB and the PerleVIEW MIB into the Trap Receiver (both these MIBs can be found on the Perle Web site **http://www.perle.com/downloads/**

After completing the fields, click on the **Test button** to have PerleVIEW send a test trap to the trap receiver. PerleVIEW will send a test message of "Trap being sent indicates that a PerleVIEW user has issued a test trap in order to verify his event handler trap configuration". If the trap is received by the trap receiver, the test is successful. If not successful, then correct the parameters in error and retry the test.

If you do not wish to add any other actions to this event, then click on the **Apply button** to save the task instance.

Acknowledge Event

Acknowledge Event

For some events, you may want to automatically have PerleVIEW mark them as acknowledged. Marking an event as "Acknowledged" simply indicates to you that you have dealt with this event. It is used to help you sort which events need your immediate attention and which ones have already been dealt with.

Global Settings

See *Event Filter Settings* for more information on Event Filters.

See *E-mail Account Settings* for more information on E-mail account settings.

See *Twitter Users* for more information on Twitter Users settings.

See *Internet Proxy Server* for more information on Internet Proxy Server settings.

97

Automatic Event Handling

Configure tasks to automatically handle incoming events.

		Sources		Actions				
Name	Events	PerleView	Devices	E-mail	SMS	Twitter	SNMP Trap	Acknowledge
Event Handler 1	All Events	No	All Devices	No	No	No	Yes	Yes

[Disable] [Add] [Delete] [Edit]

[Event Filters...]   [E-mail Account Settings...] [Twitter Users...] [Internet Proxy...]

98

Event Filter Settings

Menu Selection: Event Filter Settings

Minimum Required Authorization: PerleVIEW Administrator

By default, PerleVIEW will capture events of all severity levels (Critical, Major, Minor, Warning, Normal and Informational) sent from devices as well as ones generated by the PerleVIEW application. This configuration lets you select which severity levels you want PerleVIEW to process. By applying filters to certain events this will allow you to see the events that are important to you.

Launching Event Filter Settings

Event->Event Filter Settings
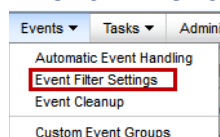
Event Filter Settings
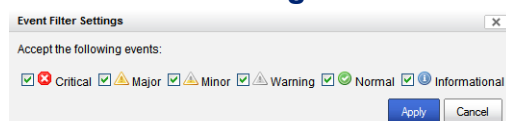
Event Filter Settings	By default, all event severities are checked. Uncheck the checkboxes for the severity of events you do not want PerleVIEW to process.

Event Cleanup

Menu Selection: Event Cleanup

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW provides an event cleanup task that will remove old and/or acknowledged events from the PerleVIEW database. This task can be run manually at any time or periodically on a configured schedule.

By scheduling a regular cleanup task, this allows you to maintain only the events that are current and relevant on your system.

Launching Event Cleanup

Event->Event Cleanup
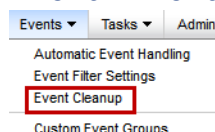
Event Cleanup

Click on the **Apply button** to save this configuration.

Click on the **Run Now button** to run the clean up task immediately. PerleVIEW will use the parameters specified on this screen for Run Now.

Clean up old events every	Defines how often the event clean up task should be run by PerleVIEW. **Default:** 7 days **Values:** 1-999 days or hours
Remove events older than	Sets the criteria for removing old events. All events that are older than the number of days defined by the parameter will be removed from the database when the event cleanup task runs. **Default:** 90 days **Values:** 1-9999 days
Also remove acknowledged events	If this option is checked, all acknowledged events will be removed from the database when the event cleanup task runs. **Default:** Not checked.

Custom Event Groups

For more information on Custom Event Groups see *Creating Custom Views by Groups* .

100

9 Administration

Administration

PerleVIEW administration tasks enables you to set up PerleVIEW global configuration parameters, user account settings, view or export the Audit logs and configure when software updates to PerleVIEW will be performed.

Working with Administration Functions

The Administration drop down menu allows for the configuration or viewing of the following items;

- PerleVIEW Server Settings
- PerleVIEW User Accounts
- File Transfer Settings
- PerleVIEW software updates
- Audit Trail Log
- Internet Proxy Server Settings
- E-mail account settings for sending event alerts
- Twitter users settings for sending event alerts

PerleVIEW Server Settings

Menu Selection: PerleView Server Settings

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW server settings options allow you to change parameters within the PerleVIEW server such as Force Secure Connections between PerleVIEW and devices, validate certificates and configure WEB Terminal TCP listening ports.

Launching PerleVIEW Server Settings

Administration->PerleVIEW Server Settings

Administration ▼	Help ▼
PerleVIEW Server Settings	
PerleVIEW User Accounts	
File Transfer Settings	
PerleVIEW Updates	
Audit Trail Log	
Internet Proxy Settings	
E-mail Account Settings	
Twitter Users	

101
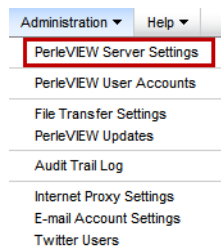
Working with Server Settings

PerleVIEW provides the following options for Server Settings.

- Force Secure Connections to devices (HTTPS/SSH)
- Validate CA certificates
- Configure Web Terminal TCP Listening ports

PerleVIEW Server Setting

PerleVIEW Server Settings

PerleVIEW Device Management
☑ Force secure connection to device (HTTPS/SSH)
☐ Validate certificates

Web Terminal - TCP Listening Ports
ⓘ The following TCP ports are for internal use only. They do not need to be changed unless they conflict with other network services on the PerleVIEW server.

SSH Listening Port: 4201
Telnet Listening Port: 4200

[Apply]

Force Secure Connections to device (HTTPS/SSH)	Select the Force Secure Connections to device if you want Web Manager and Web Terminal connections between PerleVIEW and the target device to be secure connections only. For HTTPS, PerleVIEW will communicate on TCP port 443 and for SSH communication will be on port 22. The target devices need to have HTTPS and SSH enabled.
Validate certificate	Select this option if you want HTTPS connections to validate certificates. A valid certificate must be downloaded or exist on the target device (example MCR-MGT Management module). Common certificate Authorities (CAs) such as Verisign, COST, GTE, CyberTrust etc. issue certificates that are normally already stored within your Microsoft Windows Server environment. If you need to use a self-signed certificate or a CA certificate is not found within the Window Server environment then you will need add the CA certificate to your Microsoft Windows Server. See your Microsoft Windows Server documentation for more information on how to add CA certificates.
Web Terminal TCP Listening Ports	The following TCP ports are for internal use only. They do not need to be changed unless they conflict with other network services on the PerleVIEW server.
SSH Listening Port	**Default:** 4201 **Values:** 1-65535
Telnet Listening Port	**Default:** 4200 **Values:** 1-65535

PerleVIEW User Accounts

Menu Selection: PerleVIEW User Accounts

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW uses a concept of authentication for logging users into PerleVIEW and a concept of authorization for giving users and groups access rights to target devices. PerleVIEW uses Windows authentication to control users logging into PerleVIEW. Authorization for accessing target devices is done through adding a user or group and assigning (PerleVIEW Administrator, Device Admin, Device Operator, Device View) rights to that user or group. By giving users or groups PerleVIEW Administrator privileges, these users and groups will automatically have Device Admin access to target devices.

Authentication

Authentication is based on the mode of operation you select. PerleVIEW can operate in one of two modes for authentication of users.

Windows Mode

In this mode, the username and password which you enter on the login screen will be authenticated against the Windows Server User Accounts. If successfully authenticated, you will be granted access to PerleVIEW.

Once authenticated, PerleVIEW will create a "*virtual*" user record in its database for this username (if a record does not already exist). A virtual user is a user which was dynamically added by PerleVIEW as opposed to one that was manually configured by the PerleVIEW administrator. *"Virtual users"* are shown in italics in the User Account log and they will have Device View Access only, unless they are associated with a user group or groups. If this is the case, they will be given the authorization which is associated with this group or groups. PerleVIEW administrators will have access to see *virtual user's* attributes, log the user out or convert the *virtual user* to a normal user.

PerleVIEW/Windows Mode

In this mode, in order to be granted access to PerleVIEW the username/password must first be authenticated by the Windows Server. If this is successful, PerleVIEW will next verify that the username also exists in the PerleVIEW user database. If both conditions are valid, only then is the user granted access to PerleVIEW. This mode of operation allows the PerleVIEW administrator to control which Windows users will be granted access to PerleVIEW.

Authorization

Authorization is the process of assigning PerleVIEW and device rights (PerleVIEW Administrator, Device Admin, Device Operator, Device View) to individual users or to a group. The easiest way to add and maintain authorization rights to target devices is to create groups. Creating groups within PerleVIEW will allow you to assign PerleVIEW and device access (PerleVIEW, Device View, Device Operator or Device Administrator) to that group. Assigning a user to a group is done via the Windows Server User Account settings. Create the same group name under the Windows Server User Accounts then you can add or delete members from this group on your Window Server. When a user logs in, the Windows Server will notify PerleVIEW as to which groups this user is associated with. PerleVIEW will use that information to look for these groups on its database and extract the associated PerleVIEW and device access rights from that group definition and assign them to the user.

Rights	Device Access
PerleVIEW Administrator	This is the highest access level available on PerleVIEW. It provides access to all PerleVIEW administrator functions as well as Device Admin access. If a user is not a PerleVIEW administrator, they are a PerleVIEW operator. A PerleVIEW operator can not make any changes that would affect the configuration or operation of PerleVIEW.
Device Administrator	Access to all Device access functions for target devices such as: Firmware Updates and configuration.
Device Operator	Access to operator functions for target devices. This includes retrieving status as well as operating the device (i.e. reboot of device).
Device View	Access to view target devices. Can retrieve status of devices and perform such operation as collecting statistics from devices.

PerleVIEW always requires one PerleVIEW administrator in order to operate. This "master" administrator user is the user you configured during your installation of PerleVIEW. The PerleVIEW Master administrator cannot be deleted through the PerleVIEW web interface, however the name, domain and full name can be edited using the PerleVIEW Admin Utility see *PVAdmin (PerleVIEW Administrator)* .

Launching PerleVIEW User Accounts

Administration->PerleVIEW User Accounts
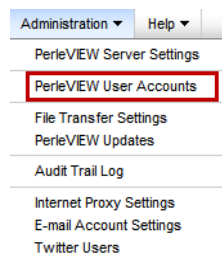
Working with PerleVIEW User Accounts

PerleVIEW provides the following User Account functions.

- Add a User to PerleVIEW's database
- Add a Group to PerleVIEW's database
- Edit User or Group from the PerleVIEW database
- Delete User or Group from the PerleVIEW database
- Log Off a User

PerleVIEW User Accounts (Add)

User Accounts

Configure users and groups to control access to PerleView and managed devices/hardware.

ⓘ PerleVIEW uses Windows authentication to control login access.
Authorizations for PerleVIEW, devices and hardware are defined by adding users/groups below.

Users and Groups:

Domain\Name	Type	PerleVIEW Administrator	Logged On	Description/Full Name
everyone	Group	☐		Windows everyone group
GroupA	Group	☑		Test GroupA
GroupB	Group	☐		Test GroupB
GroupC	Group	☐		Test GroupC
PVAdmin	User (Master Administrator)	☑	☑	
user2	User	☐	☐	Test user2
mydomain\user1	Virtual User	☑	☐	Test user1

[Add User] [Add Group] [Edit] [Delete]   [Log User Off]

PerleVIEW login restrictions:
◉ PerleVIEW/Windows Mode
  ⓘ Users must pass Windows authentication and exist in the PerleVIEW user/group list (not including virtual users)
○ Windows Mode
  ⓘ Users must pass Windows authentication

[Apply]

To Add a new User to the PerleVIEW database, click on the **Add User button**. To Add a new Group to the PerleVIEW database, click on the **Add Group button**.

Add User

Edit User [×]

Type:	User
Name:	test-user
Domain:	
Full Name:	

☐ PerleVIEW Administrator

Windows Group Membership:

☑ Inherit device access permissions from groups

Device Access:

Name	Type	Permissions	Inherited From User Group
All Devices	Device Group	Device View	✖

[Add...] [Delete]

[Apply] [Cancel]

Click the **Apply button** to save your changes.

Name	Type in the name the user will use to log on.
Domain	If required type in the domain name to fully qualify the user.
Full Name	Type in the users full name.
PerleVIEW Administrator	Select the checkbox, if this user will have PerleVIEW Administrator rights.
Inherit device access permissions from groups	By default, this checkbox will be selected so if this user is part of a group, then device access permissions will come from that group. If you uncheck this option then this user will be assigned the device access rights as configured in this user record. By default, the user is granted "Device View access" to all devices. You can add Device access rules for this user by selecting the **Add button**.

105

Click the **Add button** to Add device access rules for this user. You can add multiple "device access" rules for the same user.

Add Device Access Rule (User)

Access Level	This selects the device access level which will be assigned for this user for the devices selected below. Valid device access levels are Device Admin, Device Operator and Device View. For more information on device access levels see *PerleVIEW User Accounts* .
Devices	Choose a device group or select individual devices to which this user will be assigned the "Access Level" selected above.

Add User Group

Click the **Apply button** to save your changes.

Name	Enter the name for this group. This must match the group name configured on the Windows Server.
Domain	If required, enter the domain name.
Description	Enter a description for this Group.
PerleVIEW Administrator	Check the checkbox if all members of this group will have PerleVIEW Administrator rights.

Click the **Add button** to add device access rules for this group. You can add multiple "device access" rules for the same group.

106

Add Device Access Rule (Group)

Access Level   Select the device access level which will be assigned to this group for the devices selected below. Valid device access levels are Device Admin, Device Operator and Device View. For more information on device access levels see *PerleVIEW User Accounts* .

Devices   Choose a device group or select individual devices to which this user group will be assigned the "Access Level" selected above.

User Accounts (Edit)

Edit User

The "Window Group Membership" area shows groups that this user belongs to. These groups must be configured on the Windows Server User Accounts as well as on the PerleVIEW database.

107

The "Device access" area shows the device access that this user has. The device access can be obtained in two ways. First the user can inherit the device access by belonging to a group and any access for that group will be inherited. Secondly, device access can be added for a user by selecting the **Add button** and selecting device groups or individual devices you want to add for this user.

This example shows that user "lyn-test" is part of the Windows Server group "perleview-group" as well as existing in the PerleVIEW database user group "perleview-group". The device access list shows the device access for this user "lyn-test".

User Accounts (Delete)

Delete User

Take ownership of user's tasks	All tasks associated with this user will become "owned" by the PerleVIEW administrator who deleted this user.
Delete user's tasks	All tasks associated with this user will be deleted when this user is deleted.

If a user deletes themselves, then the tasks associated with this user can either be deleted along with the user or the user has the option of assigning their tasks to the PerleVIEW master administrator.

PerleVIEW File Transfer Settings

Menu Selection: File Transfer Settings

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW uses file transfers for a number of functions. This includes but is not limited to downloading firmware updates, downloading/uploading device configuration, deploying scripts (only if file transfer mode is used). PerleVIEW can use HTTP (or HTTPS) to transfer files or alternatively it can use TFTP.

PerleVIEW keeps firmware updates which it downloads or device configuration file which it uploads from the devices in a directory which is called "the repository". This menu item will allow you to manage the location of the repository. You may want to manage this location if you wish to perform manual backups on its contents.

PerleVIEW comes with TFTP server software. This menu item will let you can define how TFTP is used on PerleVIEW.

Launching PerleVIEW File Transfer Settings

Administration->PerleVIEW File Transfer Settings
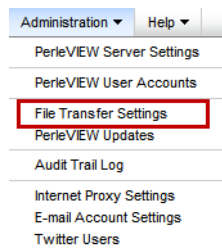
Working with File Transfer Settings

File Transfer Settings allow you to configure the following items;

- Location for downloaded software updates and configuration
- Settings for TFTP transfers
- Windows Network Credentials for accessing UNC paths

File Transfer Settings

Click the **Apply button** to save your changes.

109

Repository Location	The Repository location is the location on your PerleVIEW server where your downloaded software and configuration files will be stored. If you choose to specify your own software location to store your updates the server path needs to be in Microsoft Windows UNC format (Universal Naming Convention). Example \\ComputerName\SharedFolder\Resource. If you specify your own location to store the files, you will need to provide your Windows network credentials that have rights to this path.
	PerleVIEW does provides the option for you to let PerleVIEW manage the download location. If this options is selected, no additional information is required for this item.
TFTP Server	By default, PerleVIEW will install its TFTP server on port 69. PerleVIEW will use its TFTP server to transfer all files. Select use existing TFTP server and Window File Sharing if you have an existing setup for file transfer. PerleVIEW will use Windows file transfer to transfer files between PerleVIEW and the TFTP server. Configured your TFTP server and port number to transfer files between target devices and your TFTP server. If you specify this method, you will need to provide your Windows network credentials that have rights to the Windows network location specified.
	Note: To use an existing Windows File server, specify the Windows Network Location in Microsoft Windows UNC format (Universal Naming Convention).
	Example: \\ComputerName\SharedFolder\Resource
Windows Network Credentials	Specify your Windows Network Credentials of username, password and domain name (if required).

110

PerleVIEW Updates

Menu Selection: PerleVIEW Updates

Required Authorization: PerleVIEW Administrator

PerleVIEW can be set to automatically check for firmware updates to itself. PerleVIEW can either notify the administrator that updates are available or automatically download the updates to the PerleVIEW server. After the software has been downloaded from the Internet, you can then update PerleVIEW by using the PerleVIEW Admin Utility. See *PVAdmin (PerleVIEW Administrator)* for more information.

Launching PerleVIEW Updates

Administration->PerleVIEW Updates
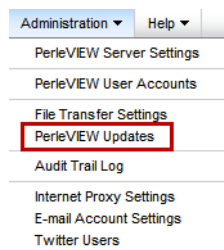
Working with PerleVIEW Updates

PerleVIEW Updates allows you to configure or view the following items;

- Set the frequency to check for software updates to PerleVIEW
- Select action to take when a software update is available
- Manually initiate a check to look for a software update

PerleVIEW Updates
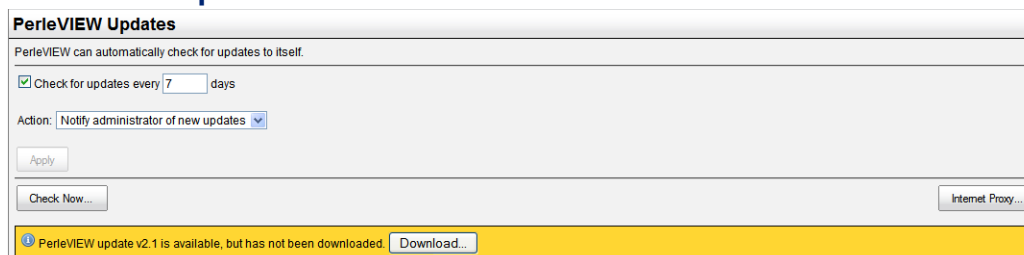
Check the Internet for updates	This parameter defines how often PerleVIEW will check whether an update is available. By default, PerleVIEW will check for software updates every 7 days. Valid options are 1 - 999 days.
Action	This parameter defines what action PerleVIEW will take if an update to the PerleVIEW software is found. By default, PerleVIEW will notify the administrator of any new software updates by updating the status in the notification bar. See *Guided Tour of the PerleVIEW User Interface* for more information on the notification bar. PerleVIEW can be configured to also automatically download updates to the PerleVIEW server. To apply these updates to PerleVIEW see *PVAdmin (PerleVIEW Administrator)* .

Check Now

To Check for PerleVIEW Updates now, click on the **Check Now button.**

Results of Check Now

The yellow banner on the bottom of the screen will display any available downloads for PerleVIEW. Click the **Download Button** to have the updates saved to the PerleVIEW server.

Internet Proxy Button

On some networks, access to the internet is provided via a proxy server. PerleVIEW needs to access the Perle Web site in order to check for software updates. If a proxy server is being used on your network, you can click on this button to access the screen for entering your proxy server information. See *Internet Proxy Server* on page 115 on how to setup these parameters within PerleVIEW.

PerleVIEW Audit Trail Log

Menu Selection: Audit Trail Log

Minimum Required Authorization: PerleVIEW Administrator

This is a log of PerleVIEW activities done by system tasks, services, or by users via the web application. The Audit Log records all internal PerleView application messages. It allows you to monitor what the PerleVIEW application is doing.

The Audit Trail Log will not exceed 1 Megabyte in size. When this limit is reached, the oldest entries will get deleted to allow for new entries to be added.

Launching PerleVIEW Audit Trail Log

Administration->Audit Trail Log
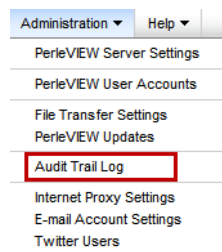
Working with PerleVIEW Audit Trail Log

The PerleVIEW Audit Trail Log menu selection allows you to:

- View all events within the PerleVIEW application
- Export the log to a .CSV file for external manipulation of the data.

PerleVIEW Audit Trail Log

The log contains the following information.

Date	This is the date and time the message was recorded to the log file.
Message	This is the contents of the message.
Event Type	This is the event type. Valid event types are Error, Warning, Information, SuccessAudit and FailureAudit.
Category	General category that this message falls into.

113

Source Type	Provides information on what originated the message.
Action	Provides an indication of what action was performed.
Result	Provides information on the results of the action taken. Valid results include Successful, Failure, Cancelled, Stopped or Pending.
User	This is the name of the user that performed the task that created the entry in the audit log file. If the user field is blank that means that this task was started by PerleView.
Index	This is a sequential counter which is incremented for each entry in the log. If many entries are occurring at the same second in time, this index may be helpful in determining the order of the entries.
Process ID	This is the internal task ID of the task which generated the message.

Internet Proxy Server

Menu Selection: Internet Proxy Server

Minimum Required Authorization: PerleVIEW Administrator

On some networks, access to the Internet is provided via a proxy server. PerleVIEW needs to reach the Internet for some of its functions to work such as sending Tweets, E-mails and looking for software updates. If a proxy server is being used on your network, you should enter its access information here.

PerleVIEW does not need the Internet to discover target devices or communicate with target devices.

Launching PerleVIEW Internet Proxy Server

Administration->Internet Proxy Server
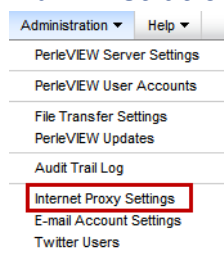
Internet Proxy Server

Click the **Apply button** to save your changes.

Use Proxy Server (HTTP/HTTPS)	Select "use Proxy server" if you need a Proxy server to reach the Internet. See your network administrator for the parameters required to set up your network Proxy Server.
Proxy Server	Enter the IP address of the Proxy Server.
Port	Enter the port number that the Proxy Server uses for client connection. **Default:** 8080
Server Requires Authentication	Some Proxy Servers require user authentication. See your network administrator for the authentication parameters.
Username	Enter the username to be used to authenticate with the Proxy Server.
Password	Enter the password to be used to authenticate with the Proxy Server.
Domain	If needed, enter a Domain name to be used to authenticated with the Proxy Server.

E-mail Account Settings

Menu Selection: E-mail Account Settings

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW has the capabilities of notifying you via E-mail of events occurring on your network. These events could be generated by devices or by PerleVIEW when it detects a status change (i.e. loss of communication with a device) or other non-device related events. Use this feature if you need to be notified via E-mail of certain events which occur in your network. To set up an E-mail notification see *Automatic Event Handling* .

Launching E-mail Account Settings

Administration->E-mail Account Settings
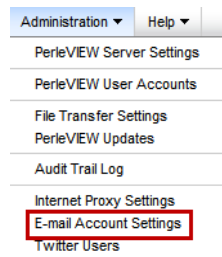
E-mail Account Settings

Click the **Apply button** to save your changes.

To delete the account information. click on the **Delete Account Info button.**

E-mail address (From)	Specify the E-mail address you want to see in the "From" field for E-mails originating from PerleVIEW.
Outgoing E-mail Server (SMTP)	Specify the IP address or Hostname of the E-mail server.
Encryption	Specify whether to use SSL or STARTTLS encryption for this connection. Check your E-mail server for information on what it requires. **Default:** Disabled
Port	Specify the smtp (Simple Mail Transfer Protocol) port number to use to communicate with the E-mail server. **Default:** 25 when encryption is disabled or using STARTTLS. Use port 465 when using SSL.
Use Authentication	Check this field if the E-mail server requires authentication.
Username	Specify a username for authentication.

116

Password   Specify a password for authentication.

Confirm   Type the password again to confirm.
password

Domain   Specify a domain name if the E-mail server requires it.
(optional)

117

Twitter Users

Menu Selection: Twitter Users

Minimum Required Authorization: PerleVIEW Administrator

PerleVIEW has the capabilities of notifying you via tweets on your Twitter account of events occurring on your target devices or on PerleVIEW itself. To setup for tweets, you need to follow these steps.

1. Have an existing Twitter user account or add a new user account at `www.twitter.com`.

2. If your network uses a Proxy to access the Internet, you must configure the Proxy settings see *Internet Proxy Server* .

3. You must authorize PerleVIEW to send tweets on your behalf. This is done by adding a twitter user using this menu.

Launching Twitter Users

Administration->Twitter Users
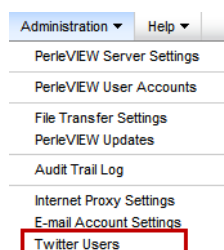
Adding a Twitter User

Click the **Add/Reauthorize User button** to allow PerleVIEW to send tweets on your behalf.

Authorize User
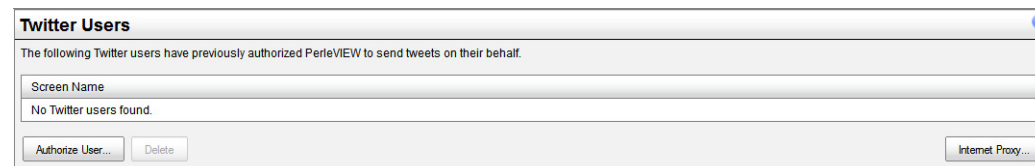
Click on the Twitter link
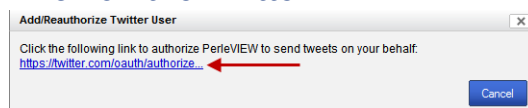
Clicking on the link above will take you to the "Twitter" web site. This is where you can authorize PerleVIEW to tweet on your behalf (i.e. using your twitter account).

118

Enter your Twitter userid and password, then click the **Authorize app button.**

Success

You should receive a message indicating that PerleVIEW is now authorized to post tweets on behalf for this user.

10 PerleVIEW Admin Utility

PerleVIEW Admin Utility

This utility can be used to configure parameters used by PerleView if you are having problems connecting to PerleVIEW using your web browser. An example would be the configuration of the HTTP port which PerleVIEW listens on for client connections.

This utility also allows you to stop or start the PerleVIEW server. Using the utility to do so will ensure that an orderly and complete shutdown occurs. When starting up PerleVIEW, it will ensure that all required components are activated.

PerleVIEW Admin Utility is also used if a software update of the PerleVIEW needs to be performed.

This utility is installed on your server when PerleVIEW is installed.

Launching PerleVIEW Admin Utility

This utility is installed on the Windows Server where PerleVIEW resides.

Start->All Programs->Perle->PerleVIEW
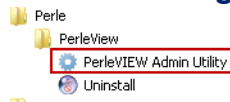
Working with PerleView Administration tasks

PerleVIEW provides the following administration functions.

- Start and Stop all PerleVIEW components.
- Modify SQL Connection parameters.
- Modify Web Connection parameters.
- Modify the PerleVIEW master admin user information.
- Update PerleVIEW software.
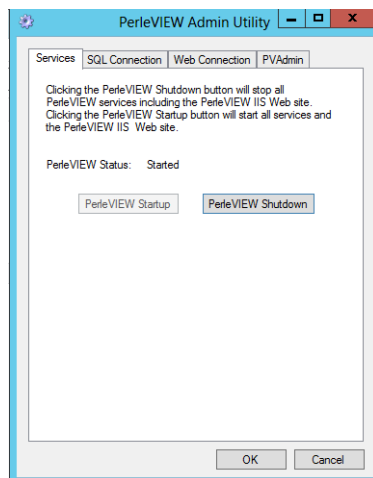
This screen allows you to stop or start the PerleVIEW server.

PerleVIEW Startup	Start up all PerleVIEW services on the Windows Server.
PerleVIEW Shutdown	Shut down all PerleVIEW services on the Windows Server.

SQL Connection

PerleVIEW uses these parameters to connect to your SQL Server. The server can be either locally (on the same server) or remote to the PerleVIEW server.
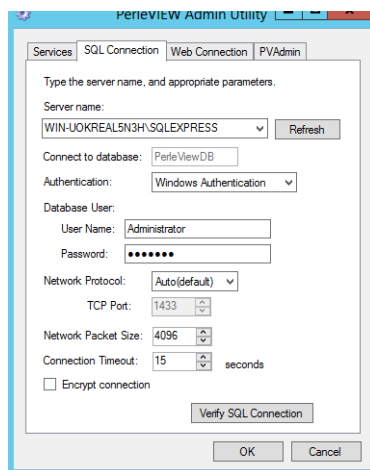
Configure the following parameters:

SQL Server	The Server Name consists of two parts separated by a backslash (\). The first part of the name is the hostname or IP address. The second part of the Server Name is the SQL Instance Name. If during installation PerleVIEW installs the SQL server for you, then by default, PerleVIEW uses localhost\SQLEXPRESS as the Server Name**.** However, if the SQL Server is already installed on this server then the server name field will need to be configured by you.

121

Connect to database	If you are using Windows Authentication Mode, type in the Windows user name (FQDN if required) as defined within your Windows Server environment. If you selected SQL Authentication mode you will need to provide the user name you configured for this user in the SQL server configuration. If the SQL server does not have a login account set for this user, authentication will fail and the user will receive an error message.
Authentication	By default, PerleVIEW will install "Use Windows Authentication Mode". Use the SQL Authentication method if on installation of your SQL server software, you selected mixed mode or SQL server authentication.

Values: Windows Authentication

SQL Authentication

Default: Windows Authentication

Database User

Username	If you are using Windows Authentication Mode, type in the Windows user name (FQDN if required) as defined within your Windows Server environment. If you selected SQL Authentication mode you will need to provide the user name you configured for this user in the SQL server configuration. If the SQL server does not have a login account set for this user, authentication will fail and the user will receive an error message.
Password	If you are using Windows Authentication Mode, type in the Windows password as defined within your Windows Server environment. If you selected SQL Authentication mode you will need to provide the password you configured for this user in the SQL server configuration.
Network Protocol	SQL Server Resolution Protocol will be used to determine how to connect to the selected SQL instance. If the SQL instance is local then the connection will use "Shared Memory". If the SQL instance selected is remote then TCP/IP will be used and SQL Server Resolution Protocol (UDP port 1434) to obtain the connection information (i.e the port number) from the remote instance. If the connection fails and the SQL instance is remote, this may be due to the inability to communicate with the SQL server. This could be caused by a firewall or the SQL Server Resolution Protocol service may not be running on the SQL server. If this is the case, you will need to use the TCP option and configure the TCP port which the SQL is listening on.

Default: Auto

TCP Port	If your SQL server is remote to PerleVIEW, this will be the TCP port to send and receive messages between PerleVIEW and the SQL Server.

Values: 1-65535
Default: 1433

Network Packet	This is the size of the TCP packet that PerleVIEW will use to communicate to the SQL server.

Values: 512-32767 bytes
Default: 4096 bytes

Connect Timeout	The time that PerleVIEW will wait for a connection to the SQL server before PerleVIEW times out.

Values: 0 - never times out
Max: 30000 seconds
Default: 15 second

122

Encrypt Connection	PerleVIEW will force the data between PerleVIEW and the SQL server to be encrypted. This is recommended if you are concerned about someone intercepting the data between the SQL Server and PerleVIEW.
Verify SQL Connection	PerleVIEW verifies that a connection can be made to the SQL server.

Web Connection

PerleVIEW uses these parameters for connections from Web browsers.
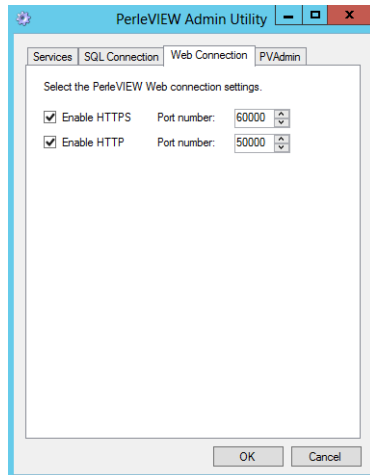
Enable HTTPS	When checked, web clients will be allowed to connect to PerleVIEW using the HTTPS protocol. You can specify the port number that PerleVIEW will listen on for this connection. **Default port:** 60000 **Values:** 1-65535
Enable HTTP	When checked, web clients will be allowed to connect to PerleVIEW using the HTTP protocol. You can specify the port number that PerleVIEW will listen on for this connection. **Default Port:** 50000 **Values:** 1-65535

> If you have an external firewall in front of your server you will need to "open" the above configured ports for HTTP and/or HTTPS connections.

123

PVAdmin (PerleVIEW Administrator)
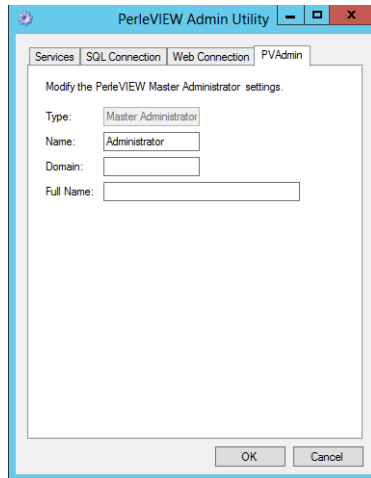
Configure the following parameters:

Type	Master Administrator.
Name	Enter a Master Administrator Name.
Domain	Type in a domain name if required by your network.
Full Name	Type in Administrators Full Name (optional).

PerleView Software Update

This utility is used to deploy software updates for PerleVIEW. Obtaining the software and placing it on the server can be performed manually or by PerleVIEW. PerleVIEW can be set to automatically check for firmware updates to itself. See *PerleVIEW Updates* to set the parameters for automatic software checking.

Once the updated software has been downloaded to PerleVIEW, use this option to perform the actual update.

If you obtain your own copy of a PerleVIEW update, you can copy it to the server PerleVIEW is running on and just execute it directly.
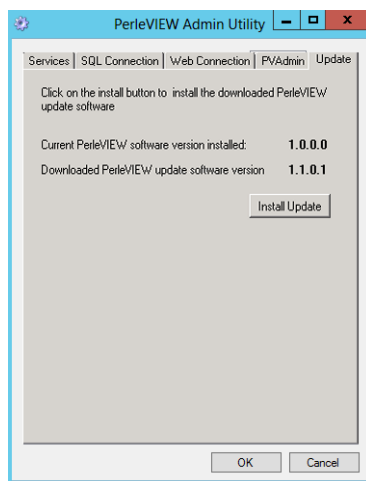
During the installation, you will be prompted to accept the licensing agreement in order to continue. Specify your country (All other Countries or Germany) then click the **I Agree** button. Next click the **I Agree** button to accept the Privacy Policy and continue the download.

Install Updates   Install the updates to PerleVIEW that have been downloaded to this server.

This utility will uninstall PerleView from this server.

Start->All Programs->Perle->PerleVIEW->Uninstall
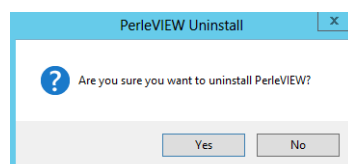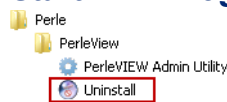
Click the **Yes button** to uninstall PerleVIEW.

125

You will be prompted on whether you want to remove the PerleVIEW database.
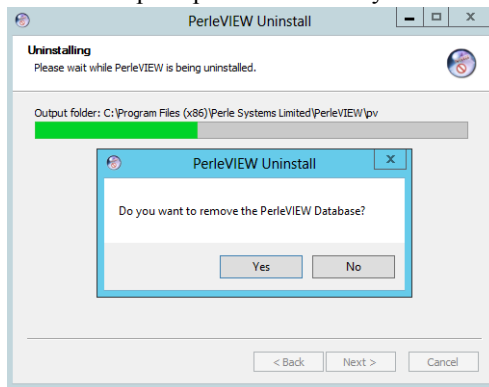
Click the **Yes button** to remove the PerleVIEW database. Click the **No button** to keep the database and continue the uninstall. PerleVIEW will now be uninstall from this server.

A Custom Views by Groups

Creating Custom Views by Groups

Menu Selection: Custom Device/Hardware/Events Groups

Minimum Run Authorization: Everyone

PerleVIEW has a very powerful grouping feature. It allows you to create custom views of devices, hardware and events. By creating group views you can clearly see the views that are important to you to maintain your devices. From within each of the Custom Groups main menu, you can create groups for any of the three groups (Devices, Hardware, and Events).

A Group View can be created in two ways. First you can select to create the group from a list of discovered devices by simply selecting the device from the list box to be added to the group. Secondly, you can create a Group View by selecting criteria that the device, hardware or event must meet in order to be added to that group. Criteria Groups use operator functions for the selection of what devices, hardware or events will be added to the group.

The list of valid operator functions are listed below.

Operator Functions

Operator	Meaning
match all	a device (hardware/event) must match the criteria. For example criteria one AND criteria two must match.
match any	at least one of the devices/hardware/events must match the criteria. For example criteria one OR criteria two must match.
is	equal to
is not	not equal to
begin with	begins with the specified letter, number or symbol
does not begin with	does not begins with the specified letter, number or symbol
ends with	ends with the specified letter, number or symbol
does not end with	does not end with the specified letter, number or symbol
contains	contain the specified letter, number or symbol
does not contain	does not contain the specified letter, number or symbol
does not exist	the field does not exist
exists	the field does exist

Here are some examples of group views

● Create a custom group view of all devices who's Name field begins with "Boston" with a health status of Major. See (*Example 1*).

● Create a custom group of hardware with selected SFP modules. See *Example 2*.

● Create a custom group of all unacknowledged events with a health status of Major. See *Example 3*.

Launching Custom Device/Hardware/Events Groups

Devices -> Custom Device/Hardware/Events Groups
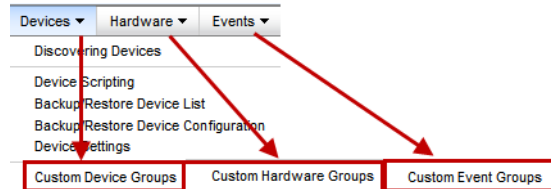
Example 1

You can create a Custom Device Group for the following scenario. You need to know if any servers in Boston have a health status of Major. Configure each device with the Name Boston (in the Use Preferred Name field) starting at Boston1 and so on. Check the Preferred name to use so that the Name field will begin with Boston.

Your two criteria are:

● all servers with the name field beginning with "Boston"

● need to know if any of these "Boston" servers have a health status of "Major"

Custom Groups
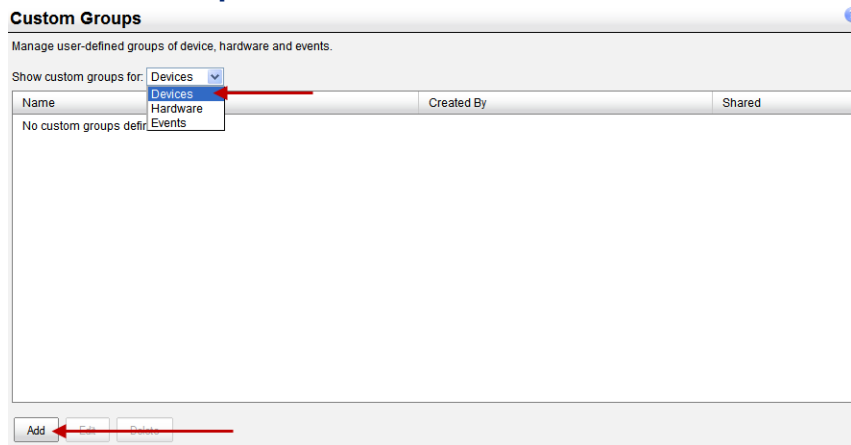
First you will need to add a Group for Devices by selecting Devices from the drop down box and then click on the `Add button`.

Add Device Group
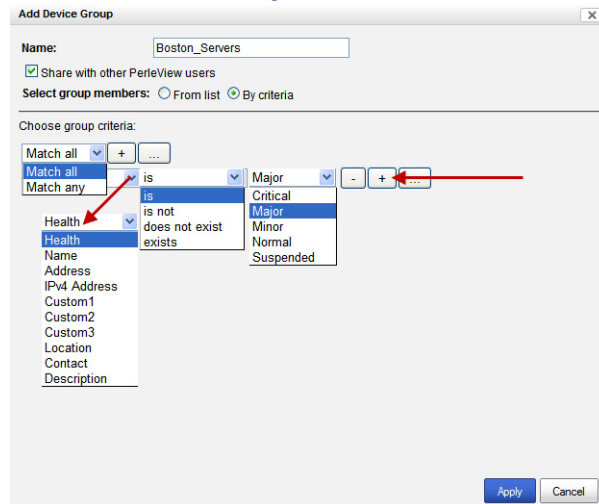
1. Type in the name of the group (Boston_Servers).

2. Select the checkbox "Share with all PerleVIEW users", if you want to share this device view with the other users of PerleVIEW.

3. Select Group members from "By criteria".

4. Choose Group criteria of:

   - Select "Match all" from the first drop down box.
   - Select "Health" from the next drop down box.
   - Select "is" for the operator.
   - Select "Major" from the third drop down box.

5. Click on the (+) `plus button` (add rule) to add a second criteria to this Custom Device Group.

6. Choose Group criteria of:

   - Select "Name" from the first drop down box.
   - Select "begins with" for the operator.
   - Type in Boston in the last field.

7. Click the `Apply button` to save this new Custom Device Group.

129
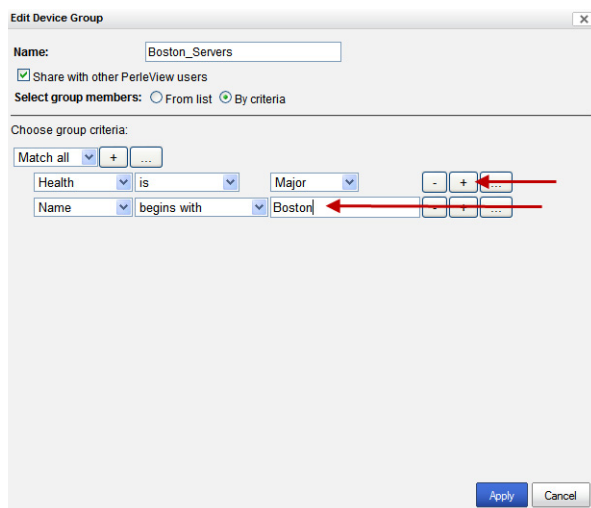
8. Your Custom Device Group will now be displayed within the left navigation panel under Group Views (Devices).

Group View of Boston_Servers
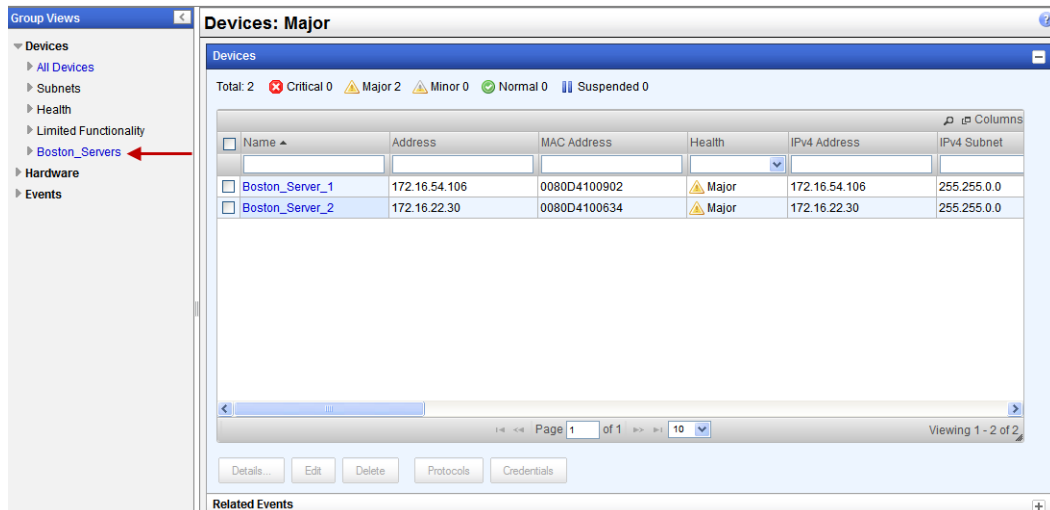
This view has the same properties as any other device view. See *Groups Views*. for more details.

> This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view

Example 2

You can create a Custom Hardware Group to view selected SFP modules from devices in your network.

Your criteria is:

● selected SPF modules

Custom Groups
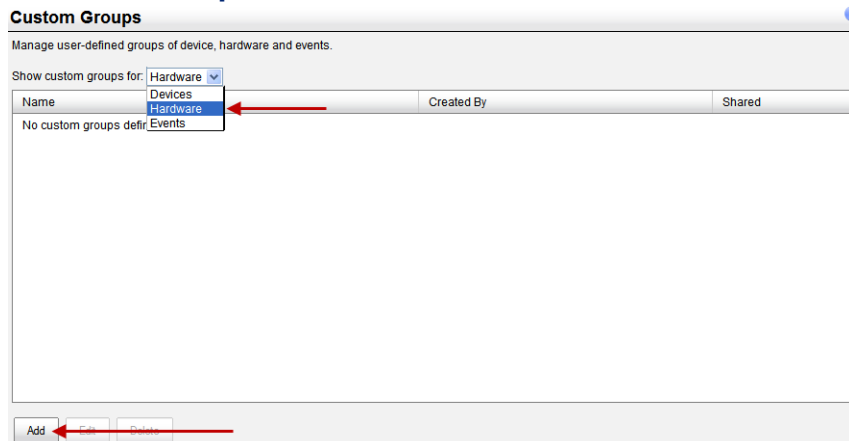
First you need to add a Group for Hardware by selecting Hardware from the drop down box and then click on the **Add button**.

Add Hardware Group
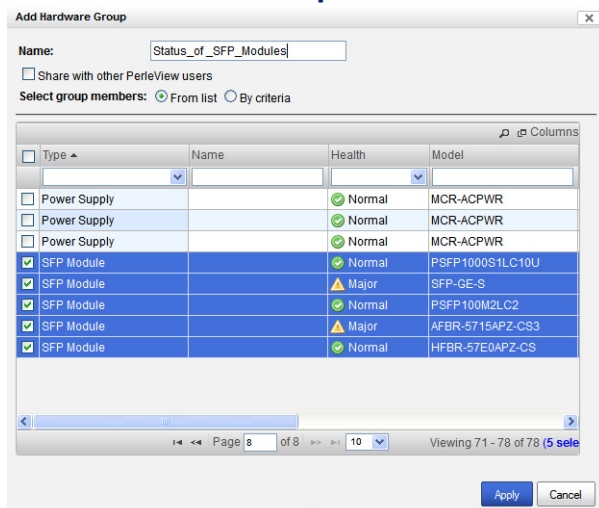
1. Type in the name of the group

2. Select the checkbox "Share with all PerleVIEW users", if you want to share this hardware view with other PerleVIEW users.

3. Select Group members from list box.

4. Select the checkbox beside all of the SFP modules you want to add to this group.

5. Click the **Apply button** to save this new Custom Hardware Group.

6. Your Custom Hardware Group will now be displayed within the left navigation panel under Group Views (Hardware).

View of Hardware SFP Modules
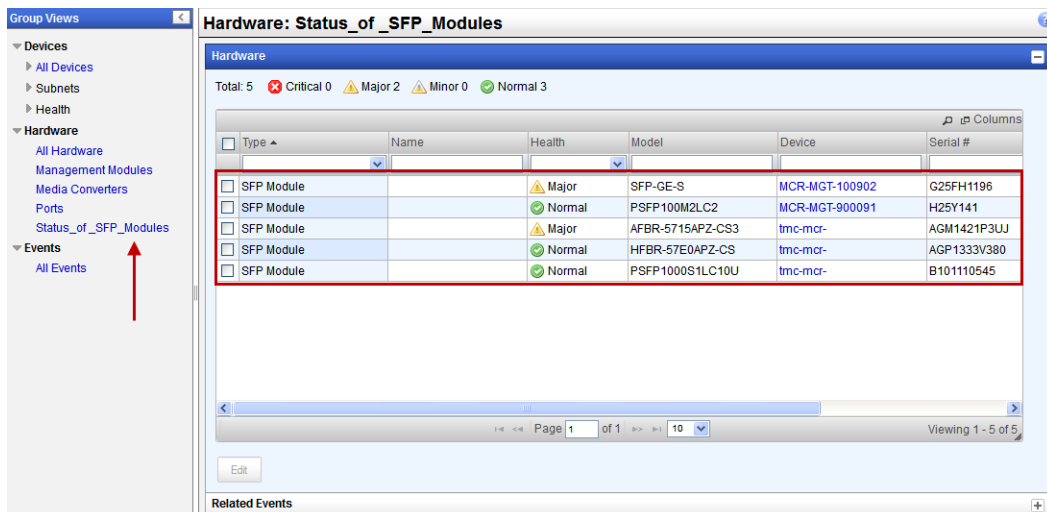
This view has the same properties as any other hardware view. See *Groups Views* for more information.

> This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view

131

Example 3

In this example you want to create a Custom Event Group to view all unacknowledged events with either a Critical or a Major health status.

Your criteria is:

● all unacknowledged events

● health status of Critical or Major

Custom Groups
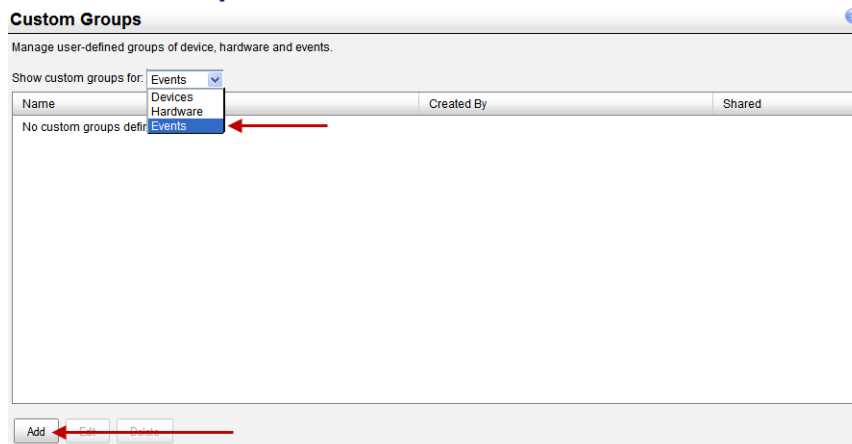
First you need to add a Group for Events by selecting Events from the drop down box and then click on the `Add button`.

Add Event Group
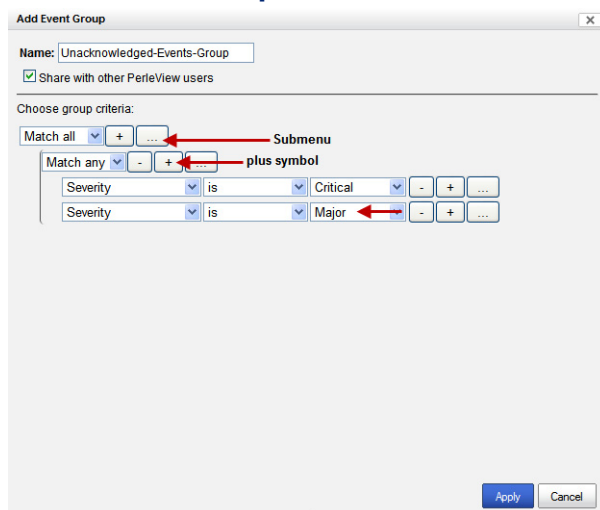
1. Type in the name of the group "Unacknowledged-Events-Group"

2. Select the checkbox "Share with all PerleVIEW users", if you want to share this event view with other PerleVIEW users.

3. Choose Group criteria of:

   ● First select the "**...**" `button` (Submenu) to create a new subgroup.

   ● Change the setting for this group to "Match any".

4. Add the criteria for the "Match any" set:

- Select "Severity" from the first drop down box.
- Select "is" for the operator.
- Select "Critical" for the last drop down box.
- Click the `Plus button` (add rule) to add the second entry for severity. Change the criteria in the last drop down box from Critical to Major.

You should now have two entries under submenu "Match any" as follows:

> Severity is Critical
>
> Severity is Major
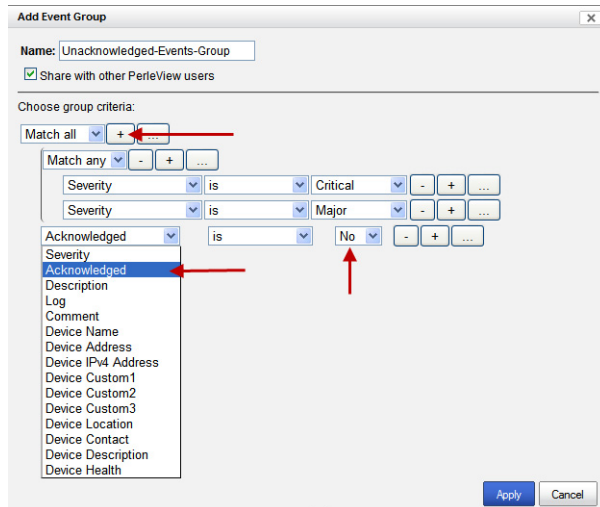
5. The next criteria you have for this group is all events must be unacknowledged. From the top "Match all" drop down box, click on the `(+) Plus button` (add rule) to add a new rule.

6. Select "Acknowledged" from the first drop down box.

7. Select "is" for the operator.

8. Select No from the last drop down box.

9. Click the `Apply button` to save this new Custom Event Group.

10. Your Custom Event Group will now be displayed within the left navigation panel under Group Views (Events).

View Group of Unacknowledged Events
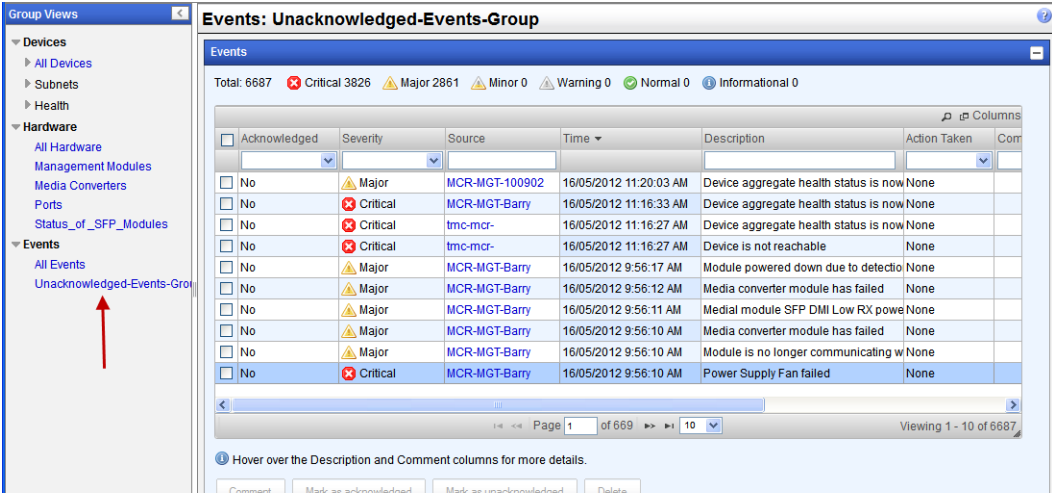
This view has the same properties as any other event view. See **Groups Views** for more information.

This view can be customized by clicking on the "Columns" button on the top, right hand of the table. Click on the magnify glass to apply filters to this view

B Event Information

PerleVIEW Generated Events

Event Severity	Health Status	Message
Critical	Critical	Device {0} at IP address {1} is not reachable.
Critical	Critical	Device {0} at IP address {1} firmware version {2} does not fully support $(SWProductName) functions. Please upgrade your Device firmware to the latest version.
Critical	Critical	New Perle factory default device {0} at IP address {1} has been discovered. Please assign a proper IP address to this device.
Critical	Critical	Existing device {0} at IP address {1} has been set to factory default. Please assign a proper IP address to this device.
Critical	Critical	Duplicate IP address has been detected on device {0} at IP address {1}. Device monitoring will be suspended.
Critical	Critical	Duplicate IP address has been resolved on device {0} at IP address {1}. Suspend state will be automatically reset for this device.
Critical	Critical	Device {0} at IP address {1} aggregate health status is now Critical. Device health status was previously {2}.
Critical	Critical	Device {0} at IP address {1} not accessible via SNMP. This may be do to either incorrect device SNMP credentials settings or the device/network not supporting SNMP.
Critical	Critical	Device {0} at IP address {1} not accessible via SNMP. This may be do to either incorrect device SNMP credential settings or the device/network not supporting SNMP protocol.
Critical	Critical	Polling for hardware inventory for the device {0} at IP address {1} failed to complete. This may be do to network or database timeout errors. Please run rediscovery on this device to retry this function.
Major	Major	Administrator login credential failed for device {0} at IP address {1}. Please run rediscovery on this device to automatically rediscover a valid credentials for this device.
Major	Major	Device {0} at IP address {1} aggregate health status is now Major. Device health status was previously {2}.

Event Severity	Health Status	Message
Major	Major	Verifying credentials for device {0} at IP address {1} failed to complete. This may be do to network or database timeout errors. Please run rediscovery on this device to retry this function.
Major	Major	Retrieving device identity for device {0} at IP address {1} failed to complete. This may be do to network or database timeout errors. Please run rediscovery on this device to retry this function.
Major	Major	Poll for hardware health statuses for device{0} at IP address {1} failed to complete. This may be do to network or database timeout errors. Please run rediscovery on this device to retry this function.
Major	Major	Poll for media converter port statuses for device {0} at IP address {1} failed to complete. This may be do to network or database timeout errors. Please run rediscovery on this device to retry this function.
Minor	Minor	Device at {0} at IP address {1} firmware version {2} is not up to date. $(SWProductName) repository contains version {3} for device model {4}. To update create and/or run a Deploy Firmware task.
Minor	Suspended	Device monitoring suspended for Device {0} at IP address.
Minor	Minor	Device {0} at IP address {1} aggregate health status is now Minor. Device health status was previously {2}.
Minor	Minor	Operator's login credentials failed for device {0} at IP address {1}. Please run rediscovery on this device to automatically discover a valid credential for this device.
Minor	Minor	The auto configuration of host trap failed for device {0} at IP address {1}. This indicates that this device has all of it's host trap entries configured.
Minor	Minor	The auto configuration of host trap successful for device {0} at IP address {1}. This device will now start sending SNMP traps for all events that occur on this device.
Minor	Minor	SSH key administrators login credentials failed for device {0} at IP address {1}. Please run rediscovery on this device to automatically discover a valid SSH key administrator login credential for this device.
Minor	Minor	SSH key operators login credentials failed for device {0} at IP address {1}. Please run device rediscovery on this device to automatically rediscover valid credentials for this device.
Minor	Minor	All SNMP read-only credentials failed verification for device {0} at IP address {1}. Please check your device credentials settings.
Minor	Minor	All SNMP read/write credentials failed verification for device {0} at IP address {1}. Please check your global credentials and discovery credentials settings.

Event Severity	Health Status	Message
Minor	Minor	All administrator credentials failed verification for device {0} at IP address {1}. Please check your device credentials settings.
Minor	Minor	All operators credentials failed verification for device {0} at IP address {1}. Please check your device credentials settings.
Minor	Minor	All SSH key administrators credentials failed verification for device {0} at IP address {1}. Please check your device credential settings.
Minor	Minor	All SSH key operator credentials failed verification for device {0} at IP address {1}. Please check your global credentials and discovery credentials settings.
Minor	Minor	Some media converter port link statuses are DOWN on device {0} at IP address {1}.
Minor	Suspended	Device Monitoring suspended for Device{0} at IP address {1}.
Warning	Warning	Bundled device firmware has been deployed to device {0} at IP address {1} with "firmware auto update" disabled. Device's module firmware will not be updated in this mode.
Warning	Warning	Deploy firmware to device {0} at IP address {1} failed.
Warning	Normal	Device {0} IP address has changed to {2}
Normal	Normal	Device {0} at IP address {1} aggregate health status is now Normal. Device health status was previously {2}.
Normal	Normal	All media converter port link statuses are now up on device {0} at IP address {1}.
Normal	Normal	Polling for hardware inventory for device {0} at IP address {1} completed successfully.
Normal	Normal	Verifying credentials for device{0} at IP address {1} completed successfully.
Normal	Normal	Retrieving device identity for device {0} at IP address {1} completed successfully.
Normal	Normal	Poll for hardware health statuses for device at {0} at IP address {1} completed successfully.
Normal	Normal	Poll for media converter port statuses for device {0} at IP address {1} completed successfully.
Informational	Normal	Device {0} at IP address {1} is reachable.
Informational	Normal	Administrator login credential successful for device {0} at IP address {1}.
Informational	Normal	Operator's login credential successful for device {0} at IP address {1}
Informational	Normal	SSH key administrators login credentials successful for device {0} at IP address {1}

Event Severity	Health Status	Message
Informational	Normal	SSH key operator login credentials successful for device {0} at IP address {1}
Informational	Normal	SNMP read-only credentials passed verification for device {0} at IP address {1}.
Informational	Normal	SNMP read/write credentials passed verification for device {0} at IP address {1}.
Informational	Normal	SSH key administrator credentials passed verification for device {0} at IP address {1}.
Informational	Normal	SSH key operators credentials passed verification for device {0} at IP address {1}.
Informational	Informational	Administrators credentials passed verification for device {0} at IP address {1}.
Informational	Informational	Operators credentials passed verification for device {0} at IP address {1}.
Informational	Informational	Duplicate IP address conflict has been resolved on device {0} at IP address {1}. Device monitoring will be resumed.
Informational	Informational	Device {0} at IP address {1} firmware has been updated to version {2}. All $SWProductName) functions are fully supported by this firmware version.
Informational	Informational	New $(SWProductName) manageable device {0} at IP address {1} has been discovered.
Informational	Informational	Deploy firmware to device {0} at IP address {1} was successful.

PerleVIEW Generated non Device Events

Event Severity	Health Status	Message
Critical	Critical	$(SWProductName) IIS web application failed to start. View the $(SWProductName) Audit log for more details.
Critical	Critical	$(SWProductName) IIS Web application is now started. View the $(SWProductName) Audit log for more details.
Critical	Critical	$(SWProductName) Event Manager Service failed to start. View the $(SWProductName) Audit log for more details.
Critical	Critical	$(SWProductName) Event Manager Service is stopped. View the $(SWProductName) Audit log for more details.
Critical	Critical	$(SWProductName) Task Manager Service failed to start. View the $(SWProductName) Audit log for more details.
Critical	Critical	$(SWProductName) Task Manager Service is stopped. View the $(SWProductName) Audit log for more details
Minor	Minor	user {0} at IP address {1} failed authentication when attempting to login the $(SWProductName) Web server application.
Minor	Minor	A new version of the device firmware is available on the Perle's web site. Please download the latest version of firmware to the repository.
Minor	Minor	Unsupported trap received from device {0} at IP address {1}. Your $(SWProductName) software may be out of date.)
Minor	Minor	$(SWProductName) TFTP Server failed to start. View the $(SWProductName) Audit log for more details.
Minor	Minor	A new version of $(SWProductName) software is available on Perle's web site. Please download and install this latest version.
Warning	Warning	Check for new device firmware updates failed. This may be due to Internet communication problems or missing/incorrect $(SWProductName) Internet proxy settings.
Warning	Warning	Check for new $(SWProductName) software updates failed. This may be due to Internet communication problems or missing/incorrect $(SWProductName) Internet proxy settings.
Warning	Warning	Trap received from supported device at IP address {0} but this device has not been discovered by $(SWProductName). Add this IP address to a discovery task or turn on auto-discovery of device on receive of trap.
Warning	Warning	The download of PerleVIEW software updates failed. View the $(SWProductName) Audit log for more details
Warning	Warning	The download of device firmware updates failed. View the $(SWProductName) Audit log for more details.
Normal	Normal	$(SWProductName) TFTP Server is stopped. View the $(SWProductName) Audit log for more details

Event Severity	Health Status	Message
Informational	Informational	user {0} at IP address {1} logged off the $(SWProductName) Web server application.
Informational	Informational	$(SWProductName) Event Manager Service started successfully.
Informational	Informational	$(SWProductName) Task Manager Service started successfully. Running $(SWProductName) Version {0}.
Informational	Informational	$(SWProductName) event action handler test {0} message
Informational	Informational	$(SWProductName) IIS Web application is now started. View the $(SWProductName) Audit log for more details.
Informational	Informational	user {0} at IP address {1} successfully logged into the $(SWProductName) Web server application.
Informational	Informational	{0} has manually cleared {1} events.
Informational	Informational	{0} user has cleared {1} events.
Informational	Informational	$(SWProductName) TFTP Server Service started successfully.
Informational	Normal	There are no newer versions of $(SWProductName) available on Perle's web site.
Informational	Informational	The download of $(SWProductName) software updates was successful. Please launch the $(SWProductName) Admin Utility on the $(SWProductName) server to install the new software.
Informational	Informational	There are no newer versions of $(SWProductName) device firmware available on Perle's web site.
Informational	Informational	The download of device firmware updates successful. To update your managed devices create and/or run a Deploy firmware task.
Informational	Informational	A new version of $(SWProductName) software has been installed. The installed ($SWProductName) version is {0}.

Remap MCR-MGT Management Module Events

MCR-MGT Management Module Traps	PerleVIEW Event
	Critical
Module Level Fault	Major
Persistent Error	Minor
One Time Error	Warning
Significant Error	Warning
Normal	Normal

C   Device Scripts

Introduction

When using the Device Scripting feature of PerleVIEW, you need to provide a script which will be deployed to each of the selected devices. This script will be composed of "CLI" (Command Line Interface) commands.

PerleVIEW provides a "slot macro" that will enable you to replace any CLI command which contains slot# as a parameter with the following macros ({CM100}, {CM1000}, {CM110}, {CM1110ANY}, {CM100MM}, {CM1000MM}, {CM1110}, {CM1110SFP}, {CM10G}, {CM10GT}, {EX-1CM} or {CM4GPT}).You can insert the "slot macro" in your script so that if the object (i.e. CM-100) exists in multiple slots on a given device, the command line will be repeated multiple times with each line having the "slot macro" replaced with the slot number corresponding to each slot the module is in.

For example:

set slot **1** cm-1110 module link-mode smart-link-passthrough would be:

set slot **{CM1110ANY}** cm-1110 module link-mode smart-link-passthrough

For a listing of the CLI commands available, please see the "MCR-MGT Management Module CLI Guide.

This appendix will describe commands for which the behavior when deployed via the PerleVIEW Device Scripting feature is slightly modified than that which is described in the guide.

Commands which are not supported will be discarded by the device.

The following commands are graphical in nature and will therefore not be supported in the Device Scripting mode of operation.

menu, screen, help

The following commands would cause the device to immediately reboot and therefore would not allow the Device Scripting function to terminate gracefully. They are not supported.

reboot, reset factory, chassis reset,

The following commands are interactive in nature and will therefore not be supported in the Device Scripting mode of operation.

admin, "?", "tab", "ESC"

Most of the commands which require the entry of a password will prompt the user for the password and then ask the user to re-enter the password to ensure that they typed it in correctly. If these commands are used within the Device Scripting feature of PerleVIEW, the interactive prompting for password would fail. To allow the command to be used in an automated scripting mode, commands which issue a prompt for passwords will be modified to add an additional parameter for the password. The command will fail if the password parameter is not included when used in conjunction with the Device Scripting function. When included, the password parameter will be used to include the password on the command line instead of having the device prompt for it. The following commands have been modified to include the new password parameter.

Command:add user

141

Parameter added:password-script <password>

Command:set user

Parameter added:password-script <password>

Command:set server

Parameter added: ssl-passphrase-script<password>

Command:set snmp v3-security readonly

Parameter added:auth-password-script <password>

Command:set snmp v3-security readwrite

Parameter added:privacy-password-script <password>

Command:add radius auth-host<host>

Parameter added:secret-script <password>

Command:add radius accounting-host<host>

Parameter added:secret-script <password>

Some commands require a "Y/N" reply. When these commands are used with the Device Scripting feature of PerleVIEW, the following behavior will be applied with no user interaction required.

save – would do the save.

netload firmware – Will not reboot of chassis.

netload text-config - Will perform the save config. Will not perform the reboot.

slot reset [factory] – Will perform the resetting of slot or config

set config-to-factory-default - Will perform the setting of current config to as the factory default configuration.

set chassis management_module_slot - Will not perform the reboot.

netload media-converter - If 'automatically updating of media module firmware' is enabled, then display message that this cannot be over-ridden in script mode otherwise, go ahead and save file.

During netload commands, the CLI will not output the progress messages. This takes time, bandwidth and will be of no use in a Device Scripting implementation. A series of dots are output to provide the batch mode with periodic traffic to prevent the process from timing out.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com