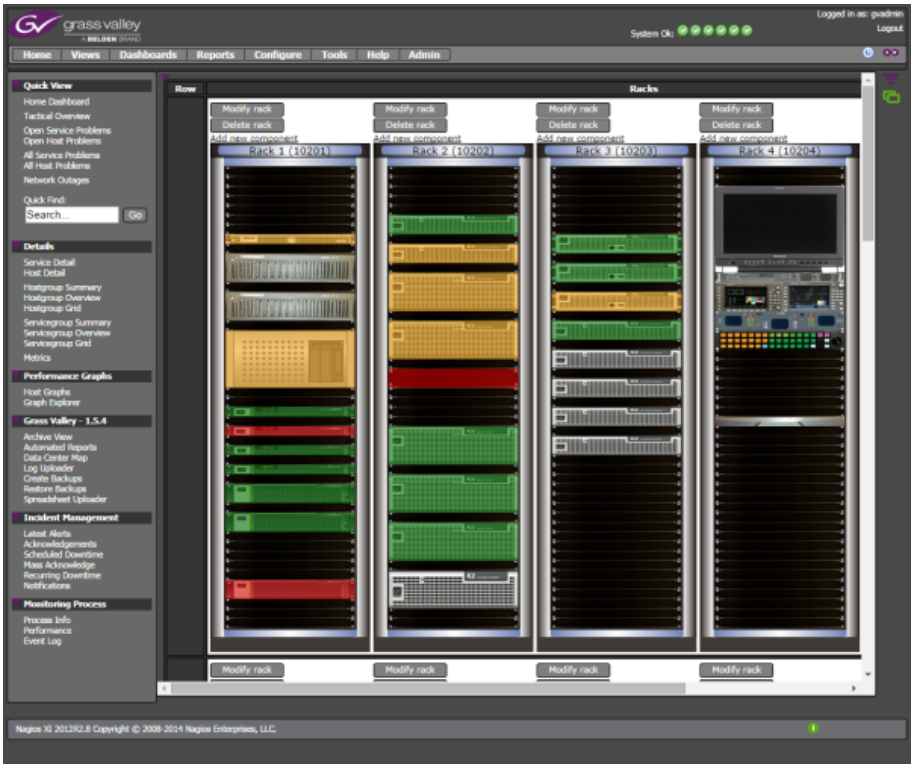
GV GUARDIAN 2.0

Infrastructure Monitoring System



www.grassvalley.com

2017 10 20

CERTIFICATE

Certificate Number: 510040.001

The Quality System of:

Grass Valley, A Belden Brand and its Grass Valley Affiliates

Headquarters: **3499 Douglas-B Floreani** **St. Laurent, Quebec H4S 2C6** **Canada**	**3030 NW Aloclek Drive** **Hillsboro, OR 97124** **United States**
Street Bergschot 69 **4817 PA Breda** **The Netherlands**	**125 Crown Point Court** **Grass Valley, CA 95945** **United States**

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

Scope:
St. Laurent HQ: The design, manufacture and support of video and audio products and systems.

Grass Valley and Hillsboro: Design, outsource manufacture and support.

Breda: Design, manufacture, including outsource manufacture, and support.

This Certificate is valid until: June 14, 2018
This Certificate is valid as of: June 14, 2015
Certified for the first time: June 14, 2000

Dr. Cem O. Onus
Managing Director, Business Assurance
DEKRA Certification, Inc.

The method of operation for quality certification is defined in the DEKRA Master Services Agreement. Integral publication of this certificate is allowed.

DEKRA Certification, Inc.
1120 Welsh Road, Suite 210
North Wales, PA 19454
USA
Ph: (215)997-4519
Fax: (215)997-3810
ISO 9001 Cert 03/09/2015 Rev C

Accredited By:
ANAB

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

grass valley
A BELDEN BRAND

GV GUARDIAN 2.0

Infrastructure Monitoring System

www.grassvalley.com

2017 10 20

Copyright & Trademark Notice

Copyright © 2017, Grass Valley Canada. All rights reserved.

Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Grass Valley is a trademark or registered trademarks of Grass Valley Canada. Belden Inc., Grass Valley Canada, and other parties may also have trademark rights in other terms used herein.

Grass Valley Web Site

The Grass Valley Web (www.grassvalley.com) site offers the following:

Online User Documentation — Current versions of product catalogs, brochures, data sheets, ordering guides, planning guides, manuals, and release notes are available.

FAQ Database — Solutions to problems and troubleshooting efforts can be found by searching our Frequently Asked Questions (FAQ) database.

Software Downloads — Download software updates, drivers, and patches.

Grass Valley Technical Support

For technical assistance, contact our international support center, at 1-800-547-8949 (US and Canada) or +1 530 478 4148.

To obtain a local phone number for the support center nearest you, please consult the Contact Us section of Grass Valley's Web site (www.grassvalley.com).

An online form for e-mail contact is also available from the Web site.

Recycling

Visit www.grassvalley.com for recycling information.

Contents

Topic Library....9
About GV GUARDIAN....10
Release Notes....10
GV GUARDIAN Version 2.0....10
Changes and features in previous releases....11
GV GUARDIAN Known Problems....11
Creating Users / Contacts....13
Managing Permissions....14
Administrator Privileges....15
User Privileges....15
Example User Privileges....16
User Security Settings....17
Grass Valley device monitoring....17
Profile Manager....18
Profile Manager Service Template configuration and arguments....18
Creating a Profile Manager Service Template....19
Creating a Profile Manager Service....20
Creating a Profile Manager Profile....20
Exporting Profile Manager Profiles....22
Importing Profile Manager Profiles....22
Applying Profile Manager configuration....23
Spreadsheet upload....24
Uploading a spreadsheet....24
Enable WMI....27
Monitor using WMI....29
Monitor using SNMP....36
Monitor Windows processes....40
Configure monitoring wizard....42
Map Data Center Rack configuration....46
Data Center rack indicators....48
Views overview....49
Access Views....49
Stop View rotation....49
Adjust View rotation speed....50
Add new Views....51
Delete Views....51
Edit Views....52
Managing Hosts....52
Add/modify a host....53
Delete a host....57
Copy a host....59
Display host information....61
Managing Services....63
Add/modify a service....63
Delete a service....67
Remove a host's dependent services....68
Copy a service....69
Display service information....71
Dashboards overview....72
Access Dashboards....72
Add Dashboards....73
Edit Dashboards....73

Delete Dashboards....73
Expand Dashboards....74
Add Dashlets....74
Manipulate Dashlets....75
Home Page Dashboard....76
Dashboards and Views....76
Clone Dashboards....76
Relationships between users and contacts....77
Multi-Tenancy Overview....79
Permissions and Multi-Tenancy....79
Creating Users / Contacts....80
Defining Contact Groups....81
Configuring Hosts and Services....84
Defining Host Groups....86
Service Groups....87
Multi-Tenancy example....87
Email notifications for alerts....91
Configure user notifications....91
Configure contact notification....93
Mail Routing....97
Simple email troubleshooting....97
The host check command 98
Change the host check command....98
Edit host templates to change the host check command....100
Send reports automatically....100
Upload logs....102
Enable Traps on Windows Devices....102
Manage GV GUARDIAN System Status....103
Manage GV GUARDIAN Monitoring Engine Status....105
License GV GUARDIAN....108
License considerations....109
Schedule a backup....109
Change VPN credentials on GV GUARDIAN server....111
Create VPN user on GV GUARDIAN cloud instance....112
Change VPN credentials on GV GUARDIAN cloud instance....113
Upgrading GV GUARDIAN....113

Glossary....115

Grass Valley Knowledge Base....125

Safety Summary....127
Safety Summary....127
Safety terms and symbols....127
Warnings....128
Cautions....128
Sicherheit – Überblick....129
Sicherheit – Begriffe und Symbole....129
Warnungen....130
Vorsicht....131
Consignes de sécurité....132
Consignes et symboles de sécurité....132
Avertissements....133
Mises en garde....134
Certifications and compliances....135
Laser compliance....136
Safety certification....136
ESD Protection....136
Recommended ESD Guidelines....137

Sources of ESD and Risks....137
Grounding Requirements for Personnel....138

Trademarks and Agreements....139
Trademarks....139
JPEG acknowledgment....139

Topic Library

The Topic Library provides several options for finding information and taking it with you. Toolbar buttons provide access to these options. The toolbar is located in the upper right corner of the Topic Library.

The Topic Library is qualified with the Internet Explorer® browser and with the Chrome™ browser.

- Print topics:
  a) In the left panel view, identify the single topic or group of topics to print.
     A group of topics to print must be a parent topic and its sub-topics.
  b) Select the single topic or parent topic so it is displayed in your browser.
  c) In the Topic Library toolbar, click one of the following:
     - **Print topic**
     - **Print topic and sub-topics**
  d) Select your printer options.

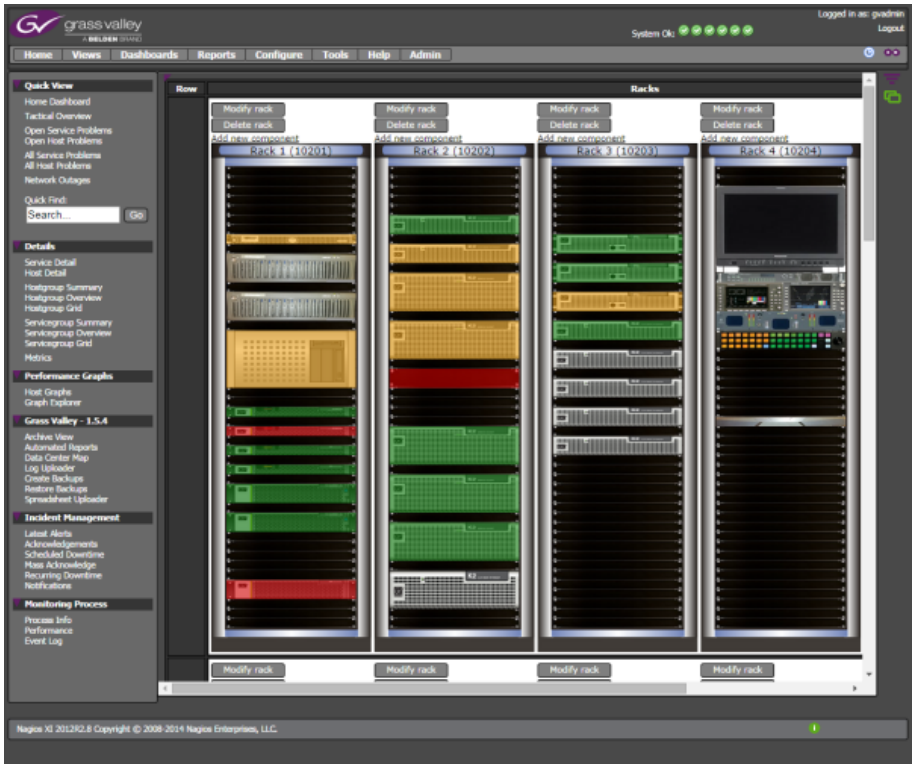
     NOTE: If your printer options support creating a pdf file, you can create a pdf file rather than printing.

     Consider your bandwidth and system resources if you select a large number of topics. It can take several minutes to create a large pdf file.
  e) Print or create a pdf file of the topic or topics.
- Download the Topic Library as:
  - : Supported on all systems with a PDF reader application, such as the free Adobe Reader® application.
  - : This single file contains the entire Topic Library.

  Once downloaded, these version of the Topic Library are uncontrolled and are not tracked for updates. For the most current and up-to-date information refer to the online Topic Library.
- Navigate the online Topic Library:
  - Browse the left panel view of topics.
  - In the toolbar located in the upper right corner of the Topic Library, click **Previous topic** and **Next topic** to navigate sequentially.
  - In the toolbar, click **Hide Navigation** to close the left panel and allow a wider reading area for your topic. Click again to open the left panel.
  - Use the links at the bottom of a topic to view related topics:
    - **Related Topics** link to topics related by subject.
    - **Parent Topic** and child topics, such as those below, link to topics related by topic hierarchy.

About GV GUARDIAN

GV GUARDIAN is Grass Valley's Infrastructure Monitoring System.



Release Notes

GV GUARDIAN Version 2.0

- **Bug fixes** — This release consists of bug fixes to improve the reliability and performance of the GV GUARDIAN application.
- **Documentation** — The following changes have been updated to the GV GUARDIAN 2.0 Topic Library:
  - Updates to GV GUARDIAN list of known problems. For more details, refer to *GV GUARDIAN Known Problems* on page 11.

Changes and features in previous releases

The following sections describe changes and features in past releases.

GV GUARDIAN Version 1.5

- **Profile Manager** — Creates reusable profiles for monitored device types. Works in conjunction with the Spreadsheet Uploader to configure devices monitored.
- **User Interface** — Logos and colors updated for Grass Valley, a Belden Brand.
- Stability improvements and bug fixes.

GV GUARDIAN Known Problems

The following limitations are present in this release of software. If you wish to obtain more information about these limitations, please mention the reference numbers.

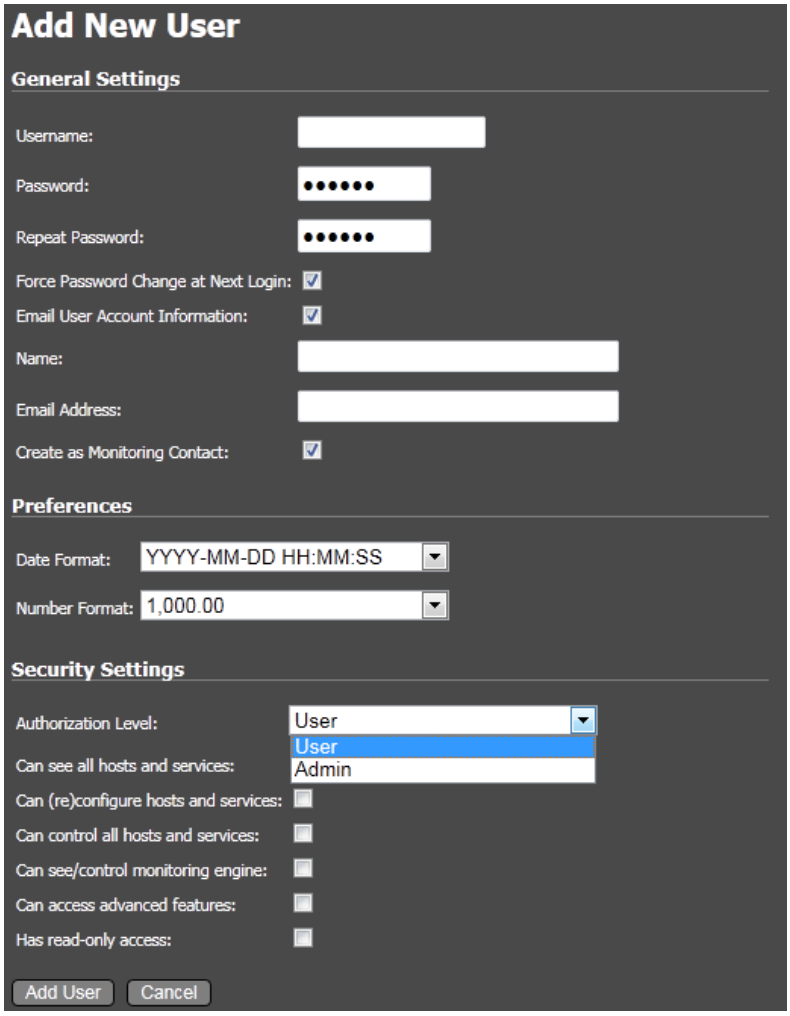
DE8090	Description:	When adding a host discovered using the SNMP Walk function to a hostgroup, the addition fails.
	Workaround:	None
DE9203	Description:	You cannot monitor the expected seven hosts using the free license, which is granted after the sixty day trial license expires. A "You have exceeded your license limits..." message appears and hosts cannot be monitored.
	Workaround:	None
DE10021	Description:	Adding a hostgroup to a template does not send alert notifications.
	Workaround:	Use Service groups notifications.
DE10023	Description:	SNMP OIDs for "Serial Number" returning null data for all device types. This occurs when using a "Type" from the spreadsheet uploader that contains a field for "Serial Number" or by adding a regular device manually.
	Workaround:	None
DE10787	Description:	Modifying an existing automated report deletes other reports. This occurs occasionally.
	Workaround:	None
DE7491	Description:	When logged on as the generic user, sending a report from the reports page fails.
	Workaround:	None
DE7932	Description:	Deleting a view causes a spinning icon to display continuously, incorrectly indicating that the GV GUARDIAN interface is not available for operations.
	Workaround:	Navigate to a different page in GV GUARDIAN.

DE10020	Description:	An alert notification references the alias of the machine having the error rather than the formal hostname. This occurs on alert notifications sent via templates assigned to hosts.
	Workaround:	None
DE10022	Description:	Alert notification cannot be sent for a user/monitoring contact with Admin privileges, if the user/monitoring contact is not the first and only user with Admin privileges.
	Workaround:	None
DE10391	Description:	The **Details	Metrics** page is not available. A "You have exceeded your license limits...." message incorrectly displays.
	Workaround:	None
DE10420	Description:	Creating a new scheduled report fails. A "Scheduled reports are only available in the Enterprise Edition" message incorrectly displays.
	Workaround:	None
DE10498	Description:	The GV GUARDIAN interface lacks a report of trial license days remaining.
	Workaround:	None
DE10504	Description:	A device that exceeds the rack size can be added to a rack.
	Workaround:	Add devices that fit the rack size.
DE10532	Description:	Availability and Notifications reports are difficult to read. White text is displayed on a gray background.
	Workaround:	None
DE10784	Description:	When modifying a report, the information presented to modify is incorrect.
	Workaround:	None
DE10785	Description:	When modifying an existing scheduled report and changing the time it runs, a new report is created that runs at the changed time. The report that runs at the previous time is retained, rather than being deleted as expected.
	Workaround:	Manually delete the report that runs at the previous time.
DE10527	Description:	The error log has repeated "It is not safe to rely on the system's timezone settings..." messages.
	Workaround:	None
DE10803	Description:	The Renaming tool fails. A "This feature requires a GV Guardian Enterprise Edition license" message incorrectly displays.
	Workaround:	None

Creating Users / Contacts

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to **Admin | Users | Manage Users | Add New User**.



2. Enter the username and the password for logging on to GV GUARDIAN.
3. Make selections to specify if you want the user to be forced to create a new password on activation or if you want to email the user the login, or both.
4. Select **Create as Monitoring Contact** if you want the user to receive notification when there are host and service alerts.
5. Select the appropriate Date and Number format.
6. Make security settings as explained in related topics.
7. Click **Add User**.

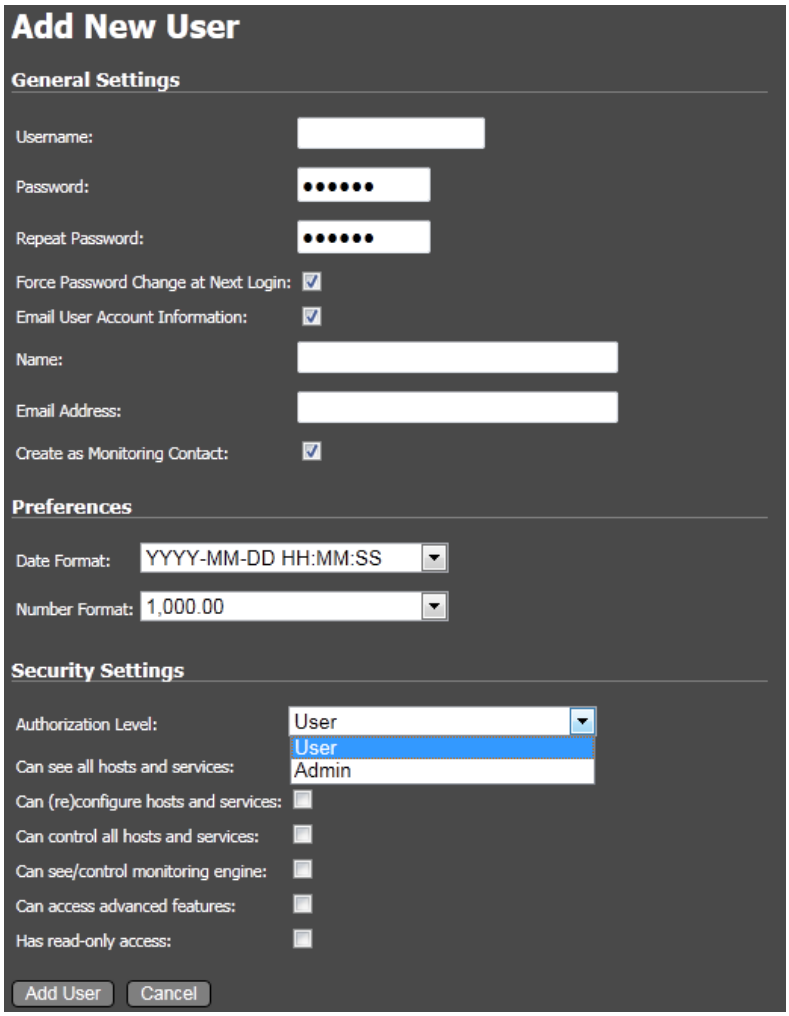
Each user that you create is automatically added as a monitoring contact that can be referenced in later configuration steps.

Related Topics

Managing Permissions on page 14
Relationships between users and contacts on page 77

Managing Permissions

Permissions for individual users can be configured or changed when adding a new user account to GV GUARDIAN or editing an existing user. To determine permissions, navigate to **Admin | Users | Manage Users**, add or edit a user, and select security settings.



When configuring security settings for an individual user account, you have the ability to configure that user as an administrator or a normal user.

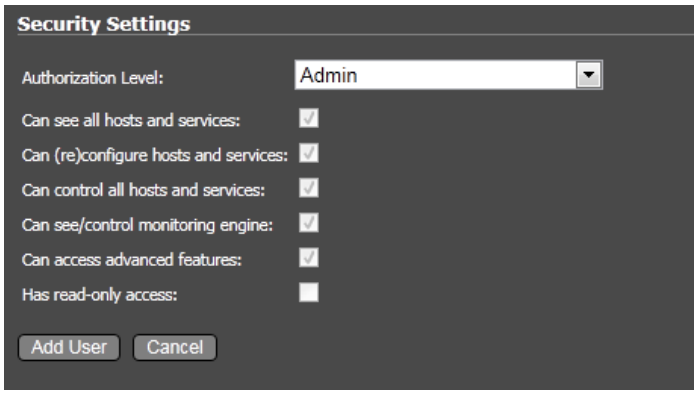
Related Topics

Example User Privileges on page 16
User Security Settings on page 17

Administrator Privileges

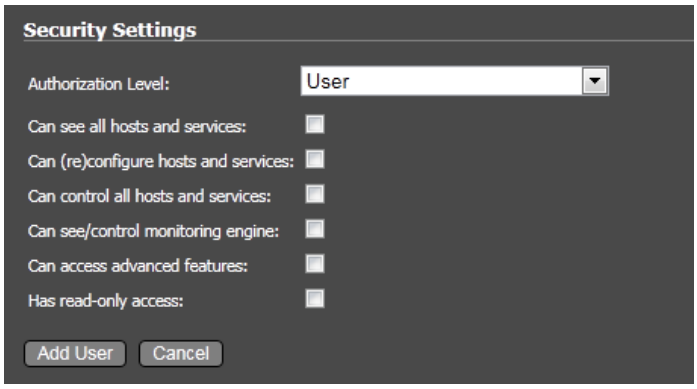
Users that are configured with an Authorization Level of Admin will have the ability to access, add, and re-configure:

Users	A user account with some level of permission to access GV GUARDIAN.
Hosts	A physical server, workstation, device, etc. that resides on your network.
Services	A service that runs on a host. The term "service" is used very loosely. It can mean an actual service that runs on the host (POP, SMTP, HTTP, etc.) or some other type of metric associated with the host (response to a ping, number of logged in users, free disk space, etc.).
Components	Optional extensions to GV GUARDIAN that can be installed by administrators to provide enhanced functionality to both end-users and administrators alike.
Configuration Wizards	A user-friendly means of monitoring new devices, services, and applications.
Dashlets	Visual elements that can be added to GV GUARDIAN dashboards and customized on a per-user basis.
Program Settings	Settings for notifications and other GV GUARDIAN parameters.
Security Credentials	Permission levels assigned to users.



User Privileges

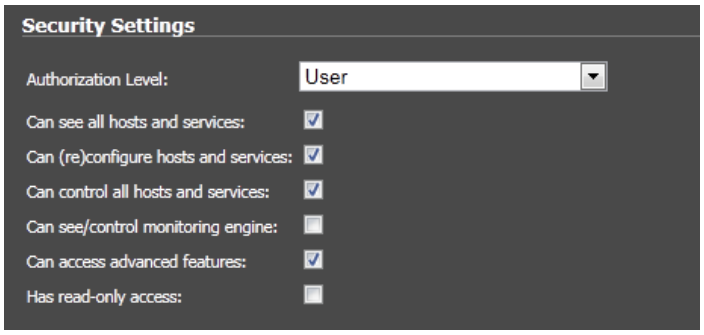
By default, users with an Authorization Level of User will only be able to see and modify hosts and services for which they are a notification contact.



Example User Privileges

Advanced User With Change Control

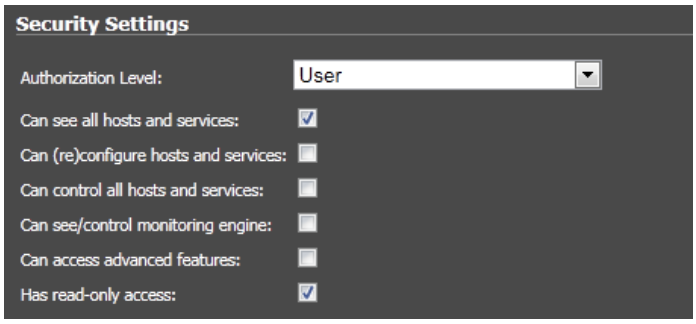
Common settings for an advanced user who should have rights to see, control, and re-configure monitored hosts and services, as well as add new hosts and services to the monitoring configuration is shown.



A user with these settings has access to advanced information and commands relating to hosts and services that are being monitored, but does not have access to control (shutdown, start, etc) the monitoring engine.

Basic Read-Only User

Common settings for a basic user who can see all hosts and services that are being monitored, but who cannot re- configure anything or submit commands to the monitoring engine is shown.



These settings are often used when configuring access for IT managers or decision makers that should be granted access to view monitoring information, but do not need access to modify anything.

User Security Settings

Administrators may grant users additional rights beyond the default permissions they have in GV GUARDIAN. A description of each individual security setting option is given in the table below.

Table 1:

Setting	Description
Can see all hosts and services	The user can see all hosts and services that are being monitored – not just the ones for which they are notification contacts.
Can (re)configure hosts and services	The user can re-configure and delete existing hosts and services (which they can see) from the monitoring configuration, and add new hosts and services to the monitoring configuration.
Can control all hosts and services	The user can see and submit commands (e.g. disable notifications) for hosts and services.
Can see/control monitoring engine	The user can see and control (e.g. shutdown or restart) the monitoring engine. Not recommended unless the user is advanced.
Can access advanced features	The user can see the Advanced tab when viewing the details of hosts and services, and can see some menu items and options that are not usually suitable for basic users.
Has read-only access	This option removes the user's ability to submit commands (e.g. disable notifications) for hosts and services and prevents them from re-configuring existing or adding new hosts and services.

Grass Valley device monitoring

Grass Valley provides the following for monitoring Grass Valley devices:

- Grass Valley device profiles: These are preconfigured by Grass Valley to monitor recommended services for each type of device.
- Grass Valley spreadsheet: This is a template for capturing the device-specific information for each of your devices and applying this information to the profile for each type of device. When you fill in the spreadsheet and upload it, your GV GUARDIAN system is automatically configured to monitor your devices.

After your GV GUARDIAN system is installed and operating at your site, Grass Valley recommends that you use profiles and the spreadsheet as follows:

1. Import Grass Valley device profiles into your GV GUARDIAN system.

   You can find the latest Grass Valley device profiles attached to Knowledge Base article KB 15707.
2. If you must monitor device types for which a Grass Valley profile is not provided, create a profile for each device type.
3. Fill in the spreadsheet template with the information for each device and specify the device type profile for each device.
4. Upload the spreadsheet to your GV GUARDIAN system.

   Your GV GUARDIAN system is now configured to monitor your devices.
5. If your requirements for monitoring a device type change, modify the device type profile for new or modified service monitoring.

   All devices currently monitored that use the profile are automatically updated to the changed monitoring requirements.

Related Topics

Importing Profile Manager Profiles on page 22
Creating a Profile Manager Profile on page 20
Uploading a spreadsheet on page 24

Profile Manager

The Profile Manager associates services with specific types of systems and devices to define monitoring for a device type. This monitoring definition becomes a reusable profile for application to all the monitored devices of that type. The Spreadsheet Uploader associates hosts and devices with the profiles created by the Profile Manager.

Grass Valley creates profiles for monitoring Grass Valley devices and provides the profiles for import into GV GUARDIAN systems at customer sites.

To access the Profile Manager, log into the GV GUARDIAN system with Administrator Privileges and navigate to **Configure | Profile Manager**.

Profile Manager Service Template configuration and arguments

Service Templates become the basis for multiple GV GUARDIAN services. Templates contain the base configuration for the service. Arguments can be added to the configuration so that different services using the templates can specify different values.

When creating a Service Template:

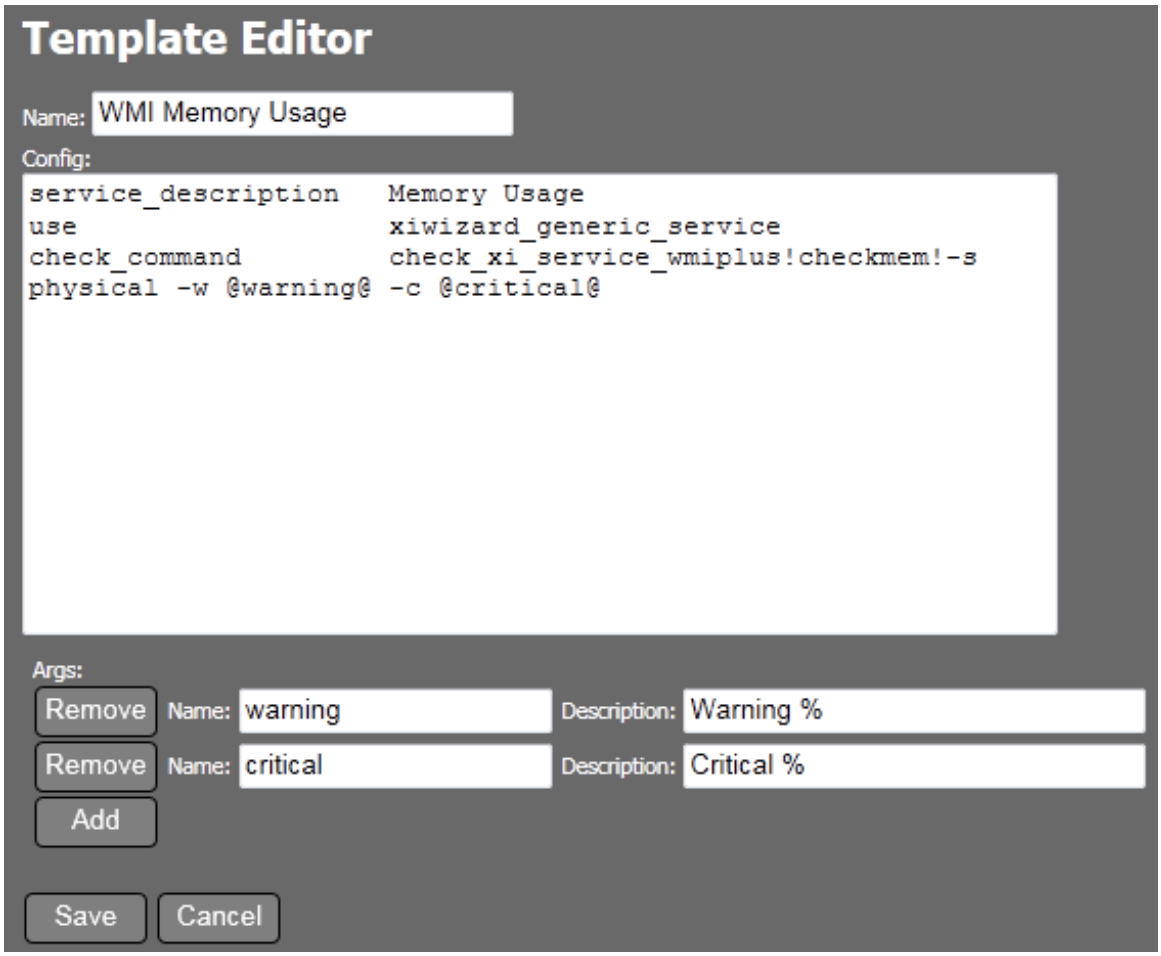
- To get the service configuration, use a monitoring wizard to create the service and then find the configuration on local PC at `/usr/local/nagios/etc/services/<hostname>.cfg`.
- Don't add hostgroups to the configuration. The Profile Manager adds hostgroups when writing out the configuration. Profiles use hostgroups to associate services to hosts in profiles.

- Arguments have a title and description. Arguments are referenced in the template configuration by adding '@'s to both the front and back of the argument title. The argument description gives context to the argument and is displayed when creating services from the template.

Creating a Profile Manager Service Template

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to **Configure | Profile Manager | Templates**.
2. Click **Add New**.



3. Enter a template name.
4. Fill in the configuration.
5. Add any desired arguments.
6. Click **Save**.

Related Topics

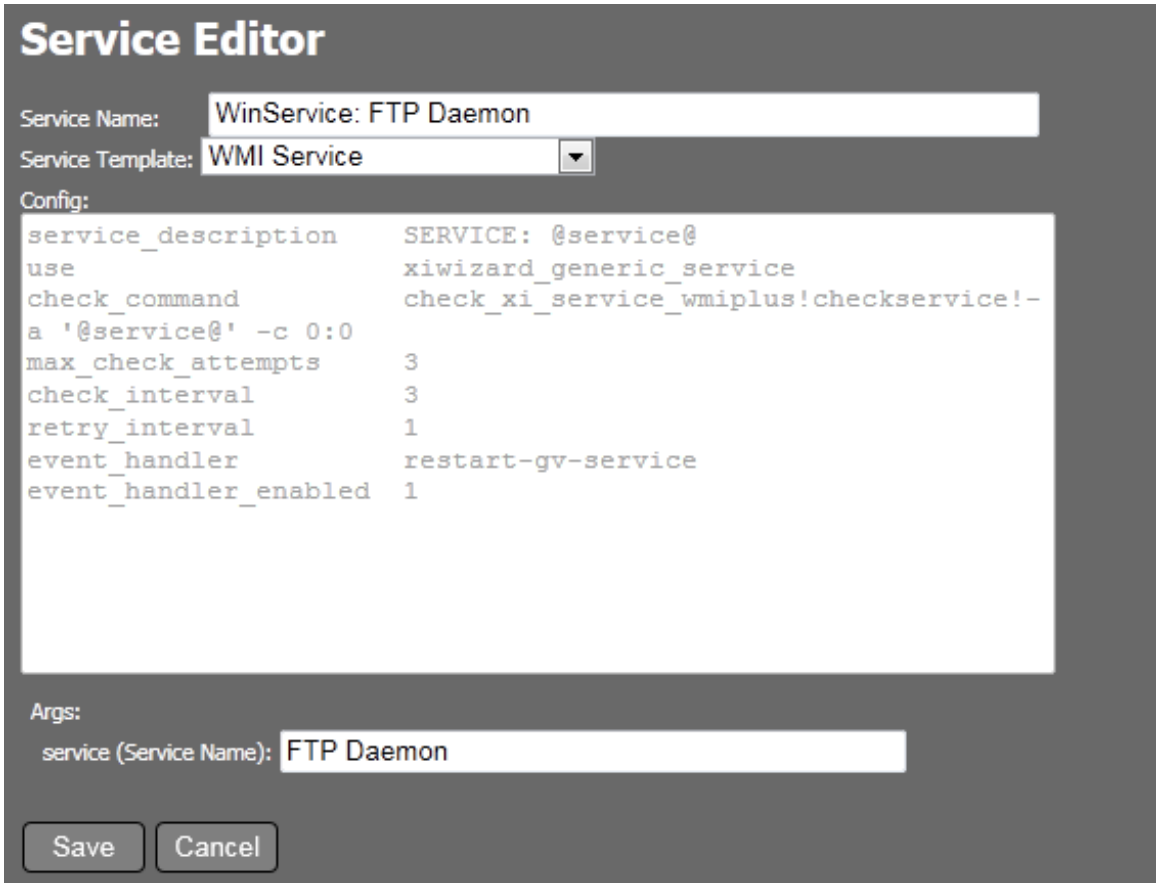
Profile Manager Service Template configuration and arguments on page 18

Creating a Profile Manager Service

- You must be logged on to the GV GUARDIAN system with administrator privileges.

A service is the actual GV GUARDIAN service that runs on the monitored system or device. A service uses a template. The service fills in any arguments that the template requires. There can be multiple services that use the same template.

1. Navigate to **Configure | Profile Manager | Services**.
2. Click **Add New**.



3. Enter a service name.
4. Add any desired arguments.
5. Click **Save**.

Related Topics

Profile Manager Service Template configuration and arguments on page 18

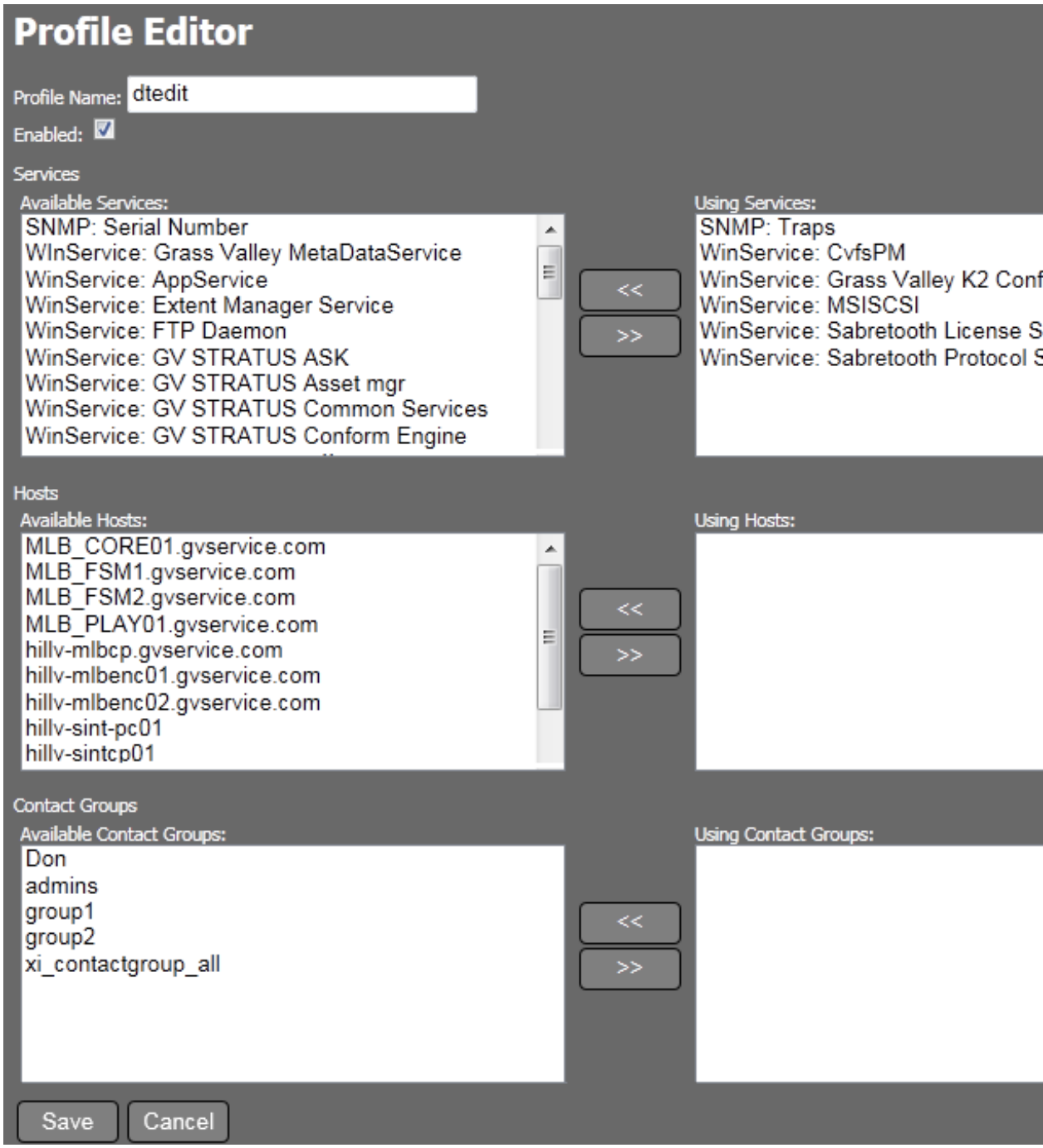
Creating a Profile Manager Profile

- You must be logged on to the GV GUARDIAN system with administrator privileges.

Profiles allow different types of services to be grouped with different types of monitored systems or devices. A profile has a list of services and a list of hosts. The profile's services are applied to

each host in the profile. Notifications for the profile's hosts and services are configured by associating contact groups with the profile.

1. Navigate to **Configure | Profile Manager | Profiles**.
2. Click **Add New**.



3. Enter a profile name.

4. Select available items and use right/left arrow buttons to configure the following lists:
   - **Using Services**: The services associated with the profile.
   - **Using Hosts**: The hosts associated with the profile.
   - **Using Contact Groups**: The contact groups associated with the profile.
5. Click **Save**.

Exporting Profile Manager Profiles

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to **Configure | Profile Manager**.
2. Click **Export**

All Profile Manager templates, services and profiles are exported to a file.

Use the Profile Manager configuration file as follows:

- To back up your Profile Manager configuration.
- To import your Profile Manager configuration into another GV GUARDIAN system.

Importing Profile Manager Profiles

- You must be logged on to the GV GUARDIAN system with administrator privileges.
- A Profile Manager configuration file must be available for import into your GV GUARDIAN system. You can find the latest Grass Valley device profiles attached to Knowledge Base article KB 15707.

Relationships between profiles, services, and service templates in the Profile Manager configuration file are preserved when the file is imported.

1. Navigate to **Configure | Profile Manager**.
2. Remove any profiles, services, and service templates that currently exist.
   a) Click **Profiles**.

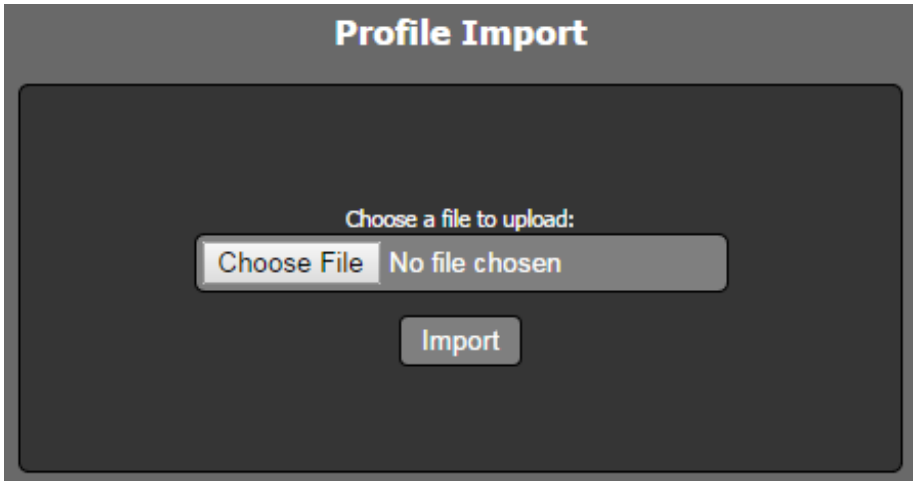
      The **Profiles** page opens.

   b) Select all the items in the list.
   c) Click **Delete Multiple**.
   d) Repeat steps for **Services** and for **Templates**.

   Removing existing profiles, services, and service templates avoids duplication and naming conflicts that can occur on import.

3. Click **Import**.

   The **Profile Import** dialog box opens.



4. Click **Choose File**, navigate to and select the Profile Manager configuration file, click **Open**, and then **Import**.

   A `Successfully...` message verifies the operation.

The Profile Manager templates, services and profiles configured in the file are imported into your GV GUARDIAN system.

Next, apply Profile Manager configuration.

Related Topics

Applying Profile Manager configuration on page 23

Applying Profile Manager configuration

- You must be logged on to the GV GUARDIAN system with administrator privileges.

In order for the profile configuration to take effect, the Profile Manager must write the configuration out to file for GV GUARDIAN to read.

1. Navigate to **Configure | Profile Manager**.
2. Evaluate and apply changes for profiles, services, and service templates.
   a) Click **Profiles**.

      The **Profiles** page opens and lists profiles. If multiple pages, consider items on all pages.

   b) Evaluate the **Sync Status** messages informing you of the changes to apply.
   c) As appropriate, select list items and click **Apply Configuration**.

      Configuration is applied for profiles, services, and service templates.

      A `Successfully...` message verifies the operation.

   d) Repeat steps for **Services** and for **Templates** to verify.

Spreadsheet upload

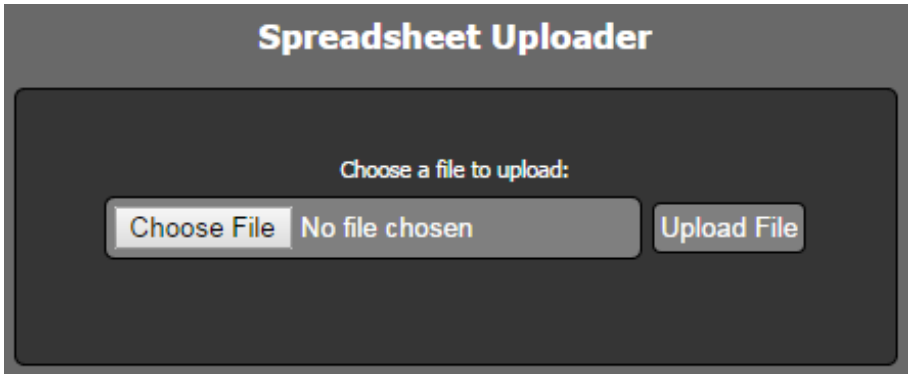
By uploading a spreadsheet that contains information for monitored devices, you can reduce the amount of time it takes to configure the GV GUARDIAN application to monitor the devices. The device information in the spreadsheet includes the following:

- Device Hostname
- Device IP address
- Notification contact information
- Profile: Assigns a predetermine list of GV GUARDIAN services to be monitored by hardware platform.

Uploading a spreadsheet

- You must be logged on to the GV GUARDIAN system with administrator privileges.
- A completed spreadsheet must be available for upload to your GV GUARDIAN system.
- Any profile specified in the spreadsheet must be present on the GV GUARDIAN system to which the spreadsheet is being uploaded.

1. Navigate to **Configure | Profile Manager | Spreadsheet Uploader**.



2. Click **Choose File**, navigate to and select a completed spreadsheet, click **Open**, and then **Import**.

   Data to be uploaded is displayed.

3. Click **Import**.

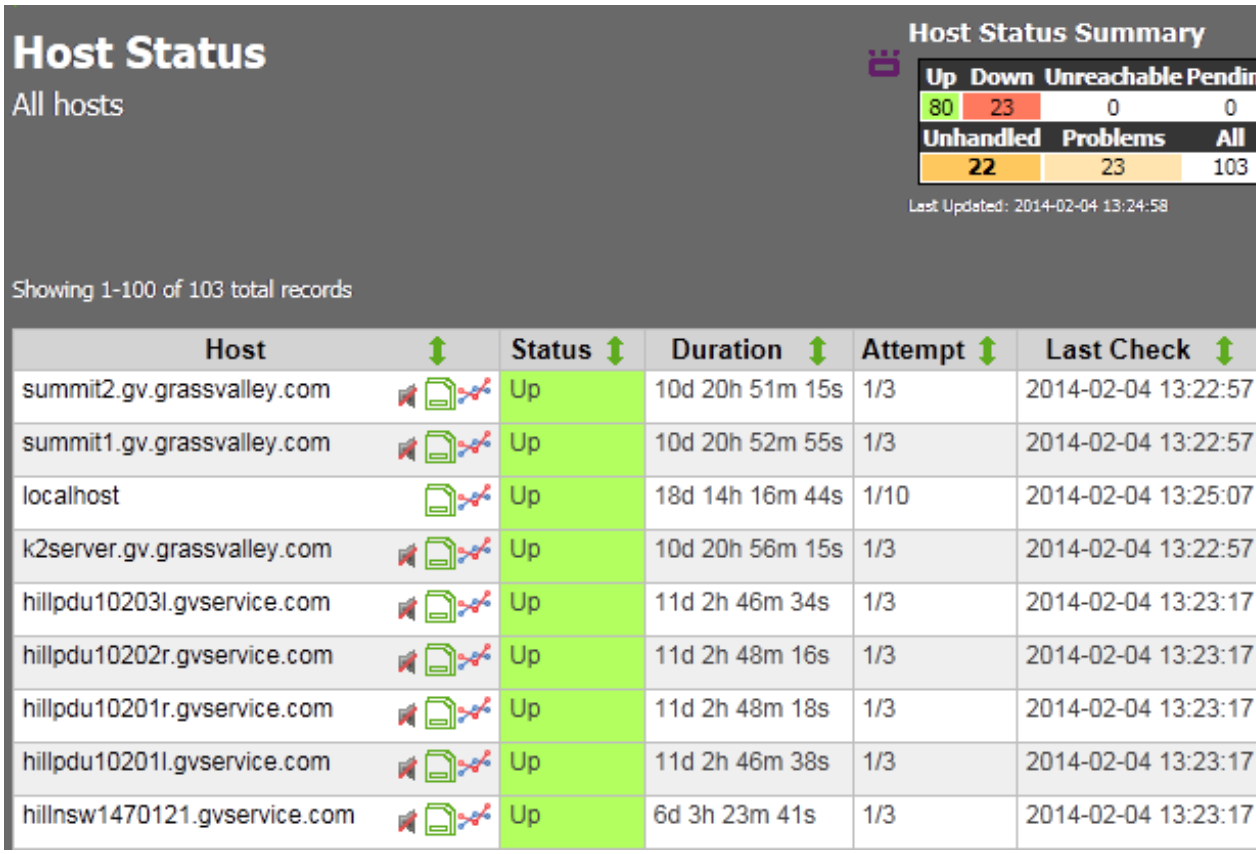
   A `Successfully...` message verifies the operation.

4. Verify data submitted as instructed in the following steps.

   Data can take some time to populate the database as polling of the devices begins.

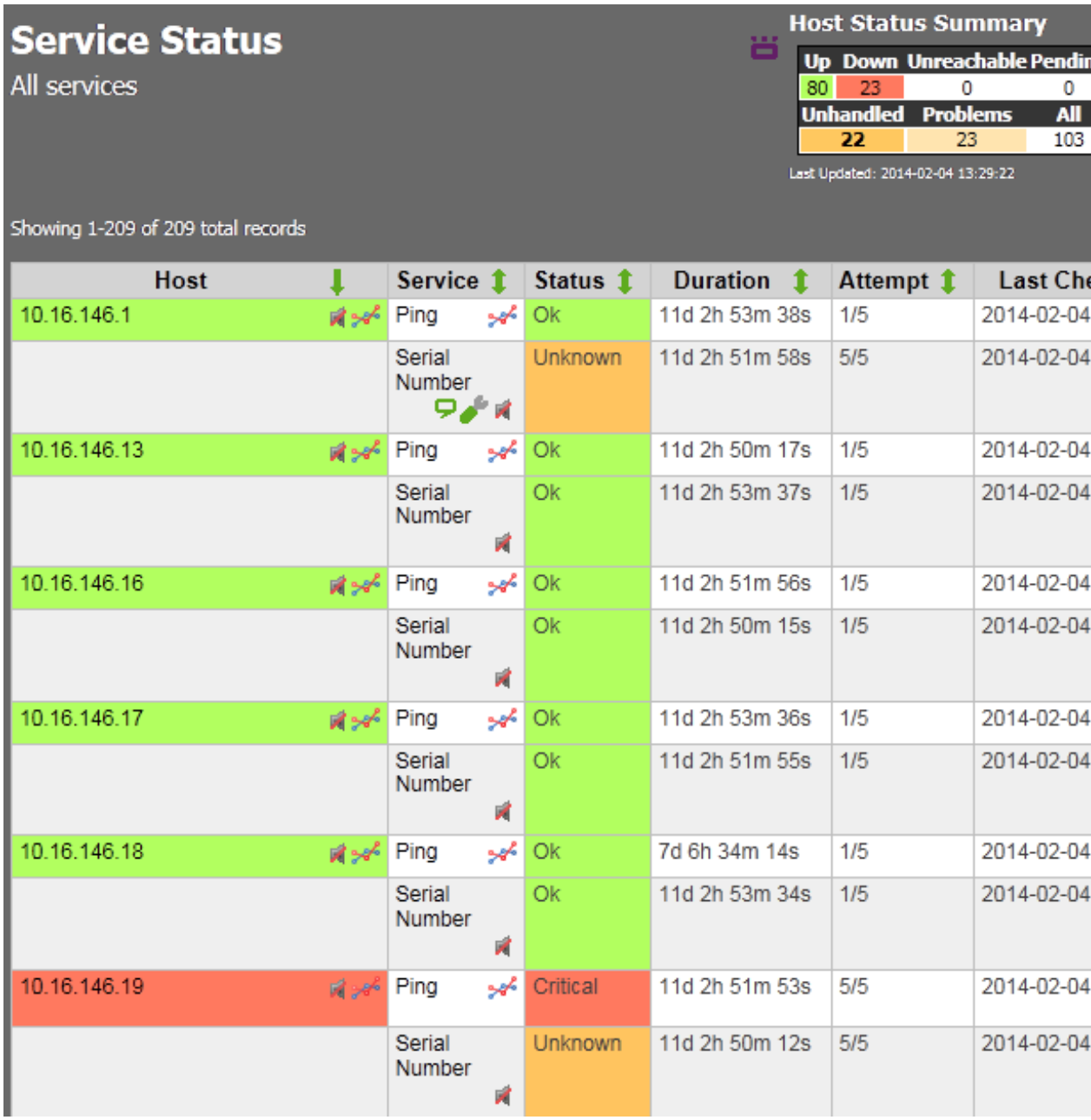
5. To verify all hosts are configured, click **Home | Details | Host Detail**.

   Device Host status starts updating. This can take a few minutes to complete the polling process depending on the amount of hosts configured.



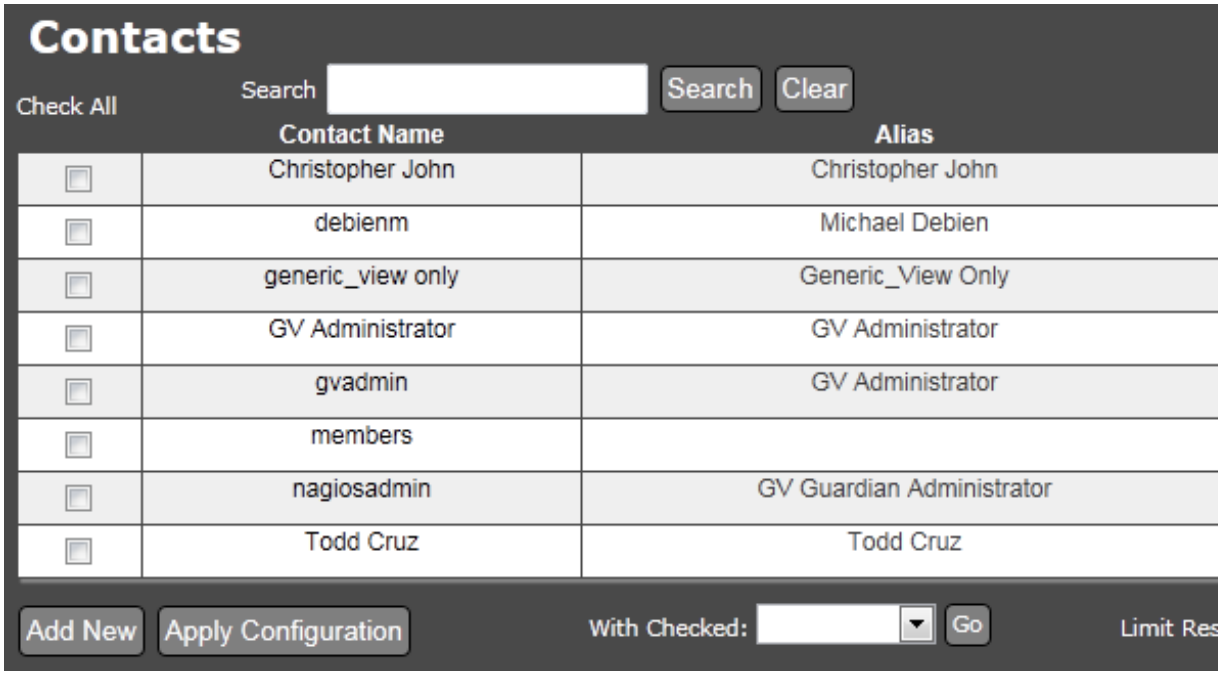
6. To verify all services have been configured, click **Home | Details | Service Detail**.

   Device Service status starts updating. This can take a few minutes to complete the polling process depending on the number of Services configured.



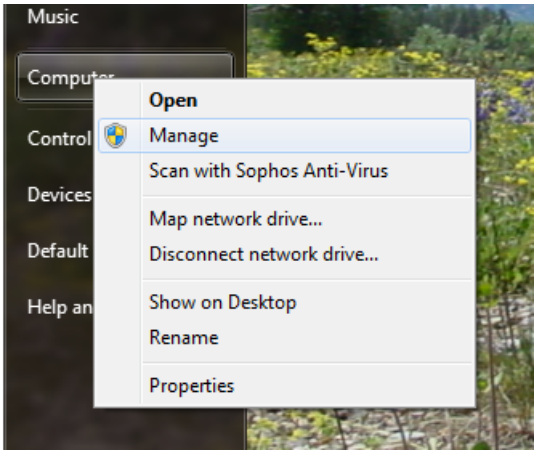
Host	Service	Status	Duration	Attempt	Last Che
10.16.146.1	Ping	Ok	11d 2h 53m 38s	1/5	2014-02-04
	Serial Number	Unknown	11d 2h 51m 58s	5/5	2014-02-04
10.16.146.13	Ping	Ok	11d 2h 50m 17s	1/5	2014-02-04
	Serial Number	Ok	11d 2h 53m 37s	1/5	2014-02-04
10.16.146.16	Ping	Ok	11d 2h 51m 56s	1/5	2014-02-04
	Serial Number	Ok	11d 2h 50m 15s	1/5	2014-02-04
10.16.146.17	Ping	Ok	11d 2h 53m 36s	1/5	2014-02-04
	Serial Number	Ok	11d 2h 51m 55s	1/5	2014-02-04
10.16.146.18	Ping	Ok	7d 6h 34m 14s	1/5	2014-02-04
	Serial Number	Ok	11d 2h 53m 34s	1/5	2014-02-04
10.16.146.19	Ping	Critical	11d 2h 51m 53s	5/5	2014-02-04
	Serial Number	Unknown	11d 2h 50m 12s	5/5	2014-02-04

7. To verify all Notification Contacts have been configured, do the following:
   a) Click **Configure | Advanced Configuration | Core Config Manager**.
   b) Enter Administrator username and password
   c) Click **Alerting | Contacts**.
   d) Verify all notification contacts are present

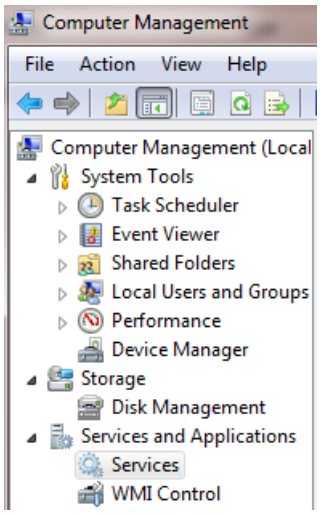


Enable WMI

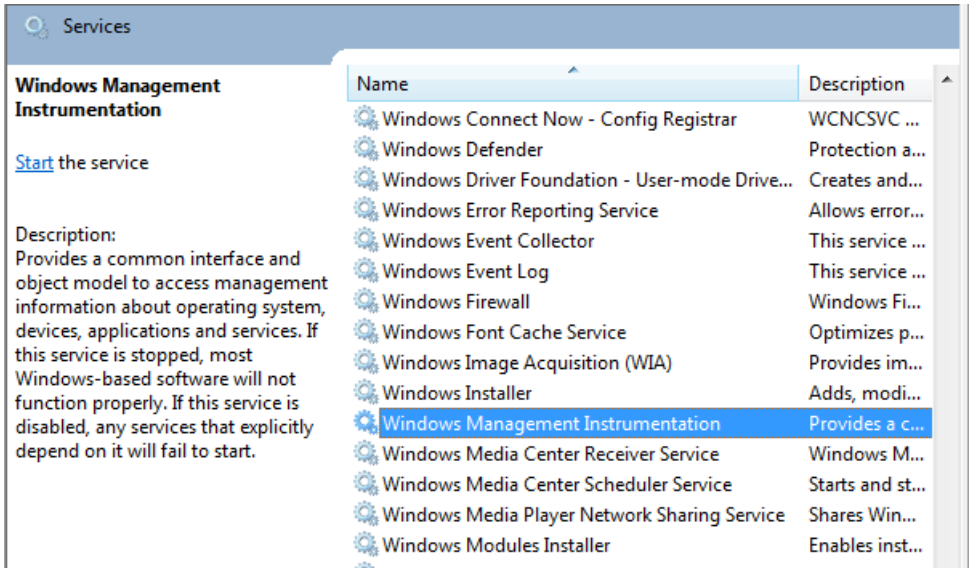
1. From the Windows desktop, click **Start**.
2. Right-click **Computer** and select **Manage**.



3. Expand **Services and Applications** and select **Services**.



4. Select **Windows Management Information** and click **Start**.

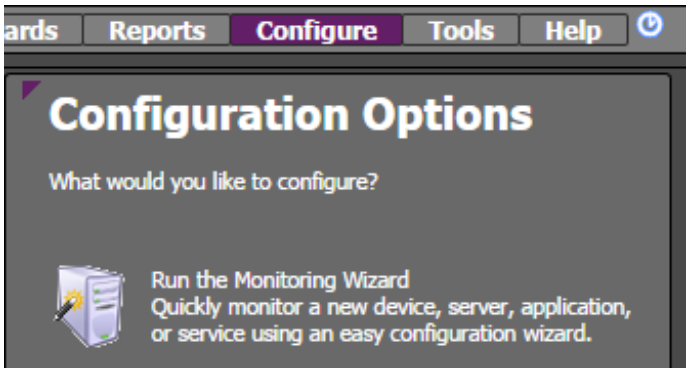


Monitor using WMI

- You must be logged on to the GV GUARDIAN system with administrator privileges.

The GV GUARDIAN Grass Valley WMI Wizard provides the ability to configure the monitoring of Server Metrics, Specific Files, Services, Processes, and Event Logs.

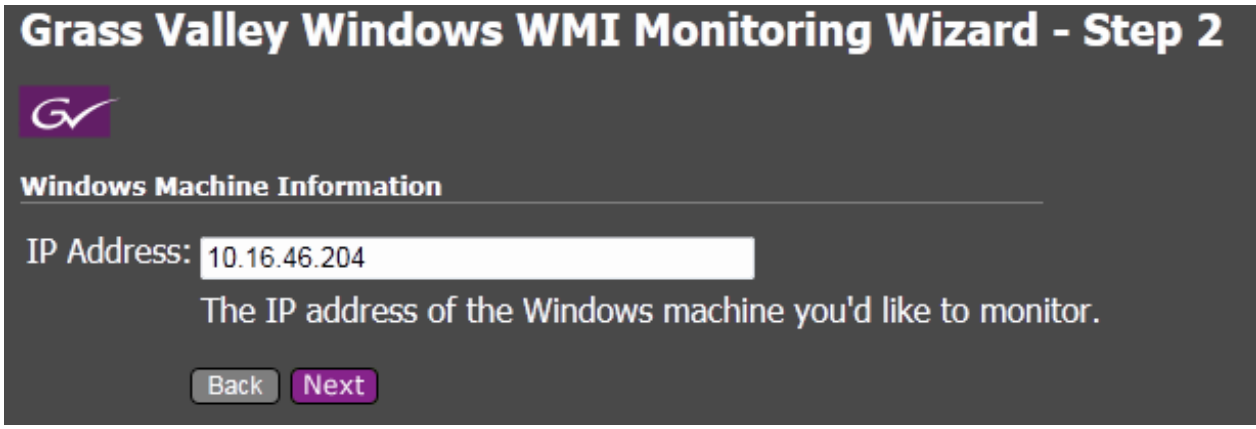
1. Click **Configure | Run the Monitoring Wizard**.



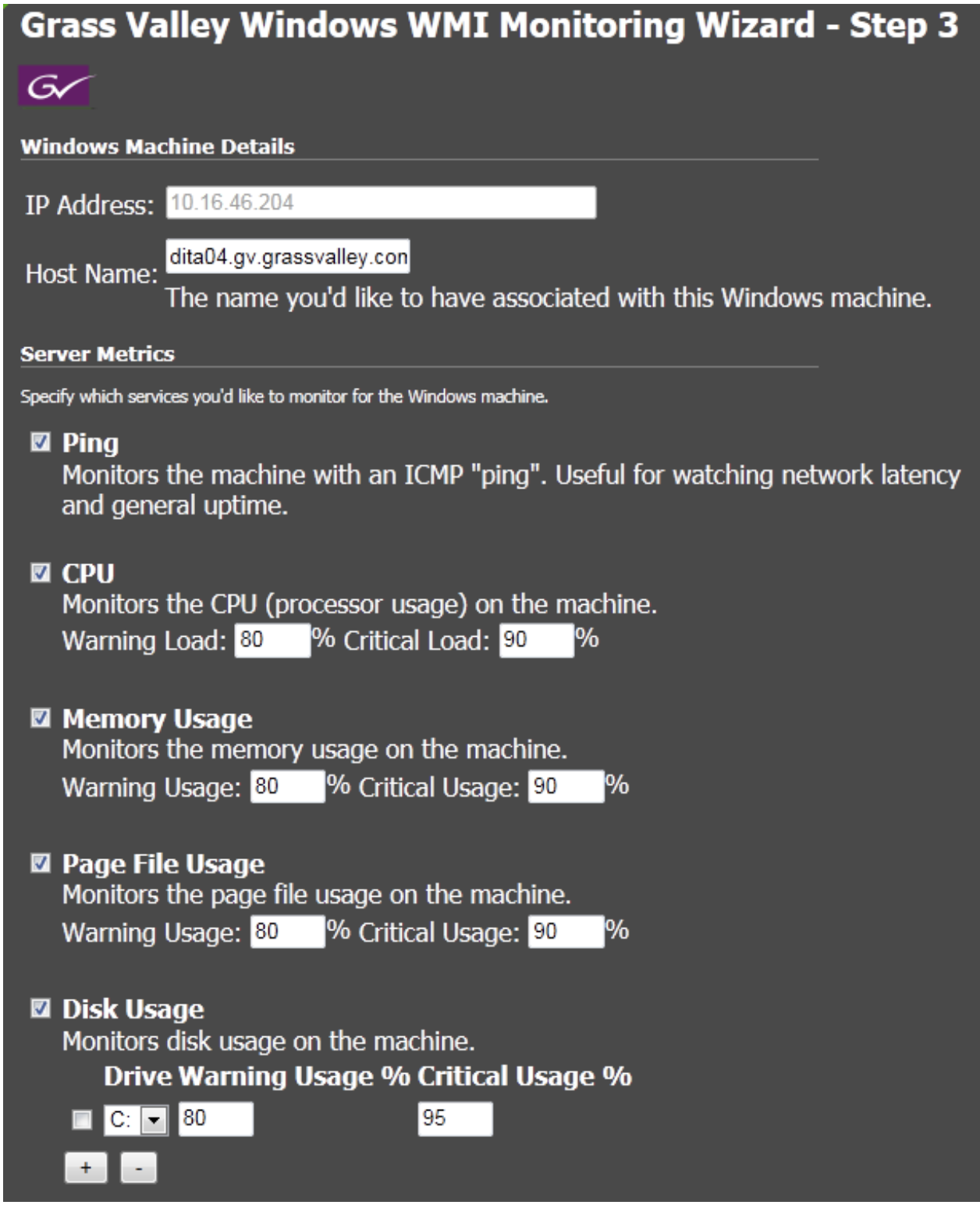
2. Select **Grass Valley Windows WMI**.

3. Scroll to the bottom of the page and click **Next**.

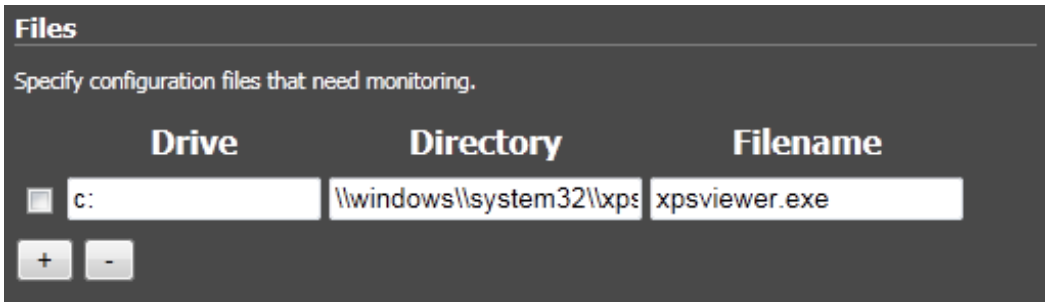
4. Enter the IP address of the workstation or server machine to be monitored and click **Next**.



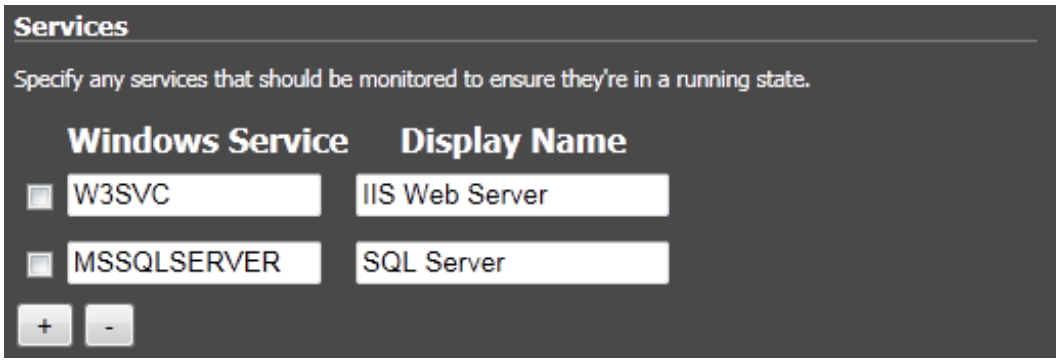
5. Configure the name and server metrics to be monitored.
   a) Enter the name to be associated with the machine you are monitoring.
   b) Select the checkbox for the metrics you want to monitor. Adjust alarm thresholds for both warning and critical percentages.
   c) For **Disk Usage**, select the checkbox and define the drive you want to monitor. Click **+** to add drives. Adjust alarm thresholds for both warning and critical percentages.


Grass Valley Windows WMI Monitoring Wizard - Step 3
Windows Machine Details
IP Address: 10.16.46.204
Host Name: dita04.gv.grassvalley.con
The name you'd like to have associated with this Windows machine.
Server Metrics
Specify which services you'd like to monitor for the Windows machine.
Ping
Monitors the machine with an ICMP "ping". Useful for watching network latency and general uptime.
CPU
Monitors the CPU (processor usage) on the machine.
Warning Load: 80 % Critical Load: 90 %
Memory Usage
Monitors the memory usage on the machine.
Warning Usage: 80 % Critical Usage: 90 %
Page File Usage
Monitors the page file usage on the machine.
Warning Usage: 80 % Critical Usage: 90 %
Disk Usage
Monitors disk usage on the machine.
Drive Warning Usage % Critical Usage %
C: 80 95
+ -

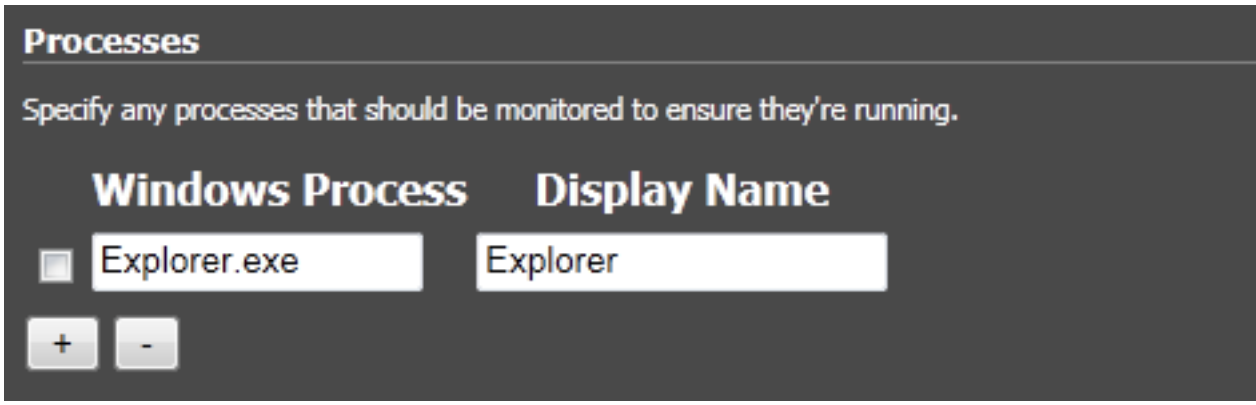
6. Scroll down and configure files to be monitored.
   a) Select the checkbox for the file you want to monitor.
   b) Select the drive with files to be monitored.
   c) Select the directory with files to be monitored.
   d) Select the filename of the file to be monitored.
   e) Click **+** to add files.



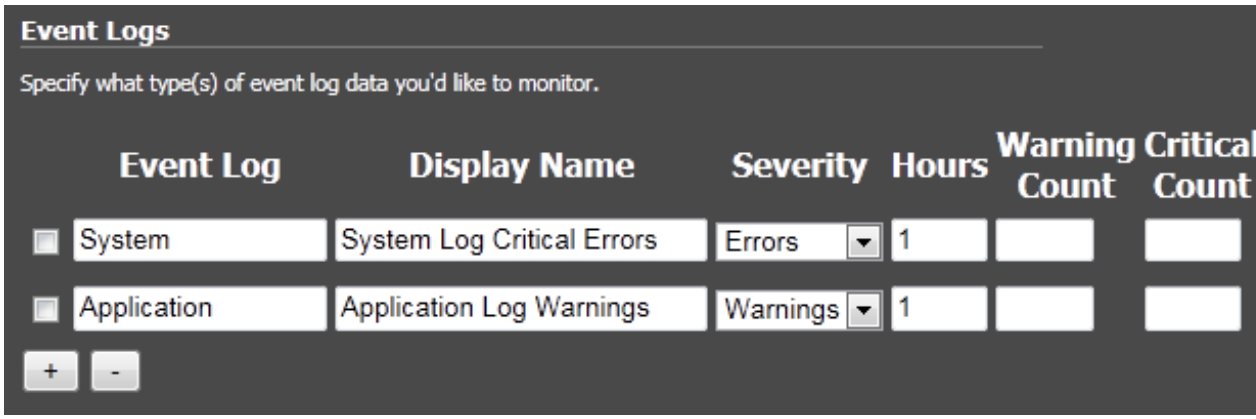
7. Scroll down and configure services to be monitored.
   a) Select the checkbox for the service you want to monitor.
   b) Define the Windows Service.
   c) Add display name.



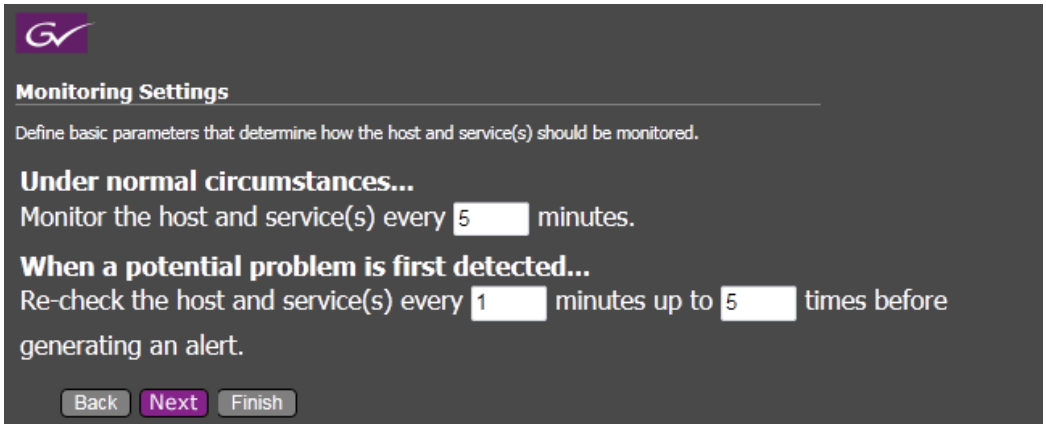
8. Scroll down and configure processes to be monitored.
   a) Select the checkbox for the Windows Process you want to monitor.
   b) Define the Windows Process.
   c) Add display name.



9. Scroll down and configure Event Logs to be monitored.
   a) Select the checkbox for the Event Log you want to monitor.
   b) Define Event Log.
   c) Define Display Name.
   d) Define notification severity.
   e) Define the alarm notification window (in hours).
   f) Define how many alarms within the notification window generate a warning notification.
   g) Define how many alarms within the notification window generate a critical warning



10. Scroll down and click **Next**.
11. Set the time intervals you want monitoring to poll the device. Default values are shown.

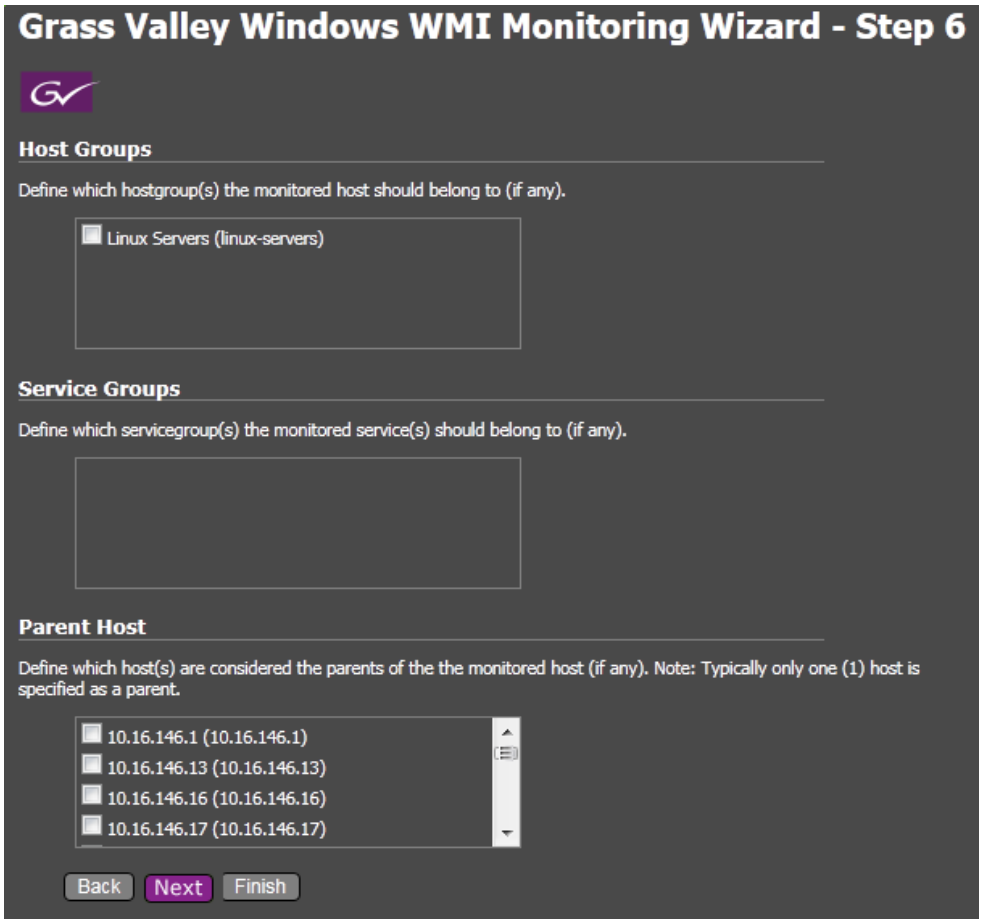


12. Click **Next**.

13. Select the timing and frequency of notifications and the individuals or groups that receive the notifications.

14. Click **Next**.

15. If the services are part of a host group, service group, or parent host, configure as shown.



16. Click **Next** and **Apply** to save the settings.

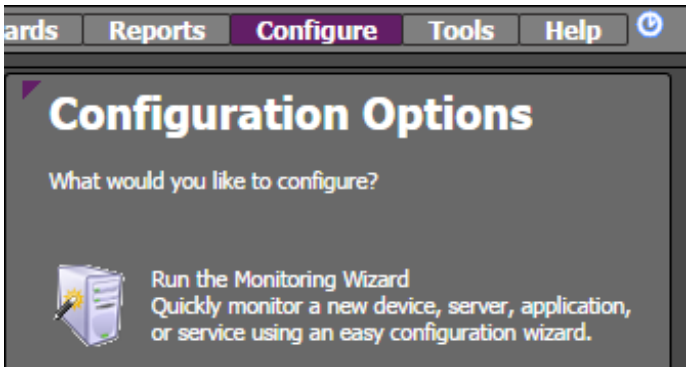
Monitor using SNMP

- You must be logged on to the GV GUARDIAN system with administrator privileges.
- The IP address of the device you intend to monitor must be known.

The SNMP Walk Wizard provides the ability to configure active SNMP scans to poll devices at predetermined intervals.

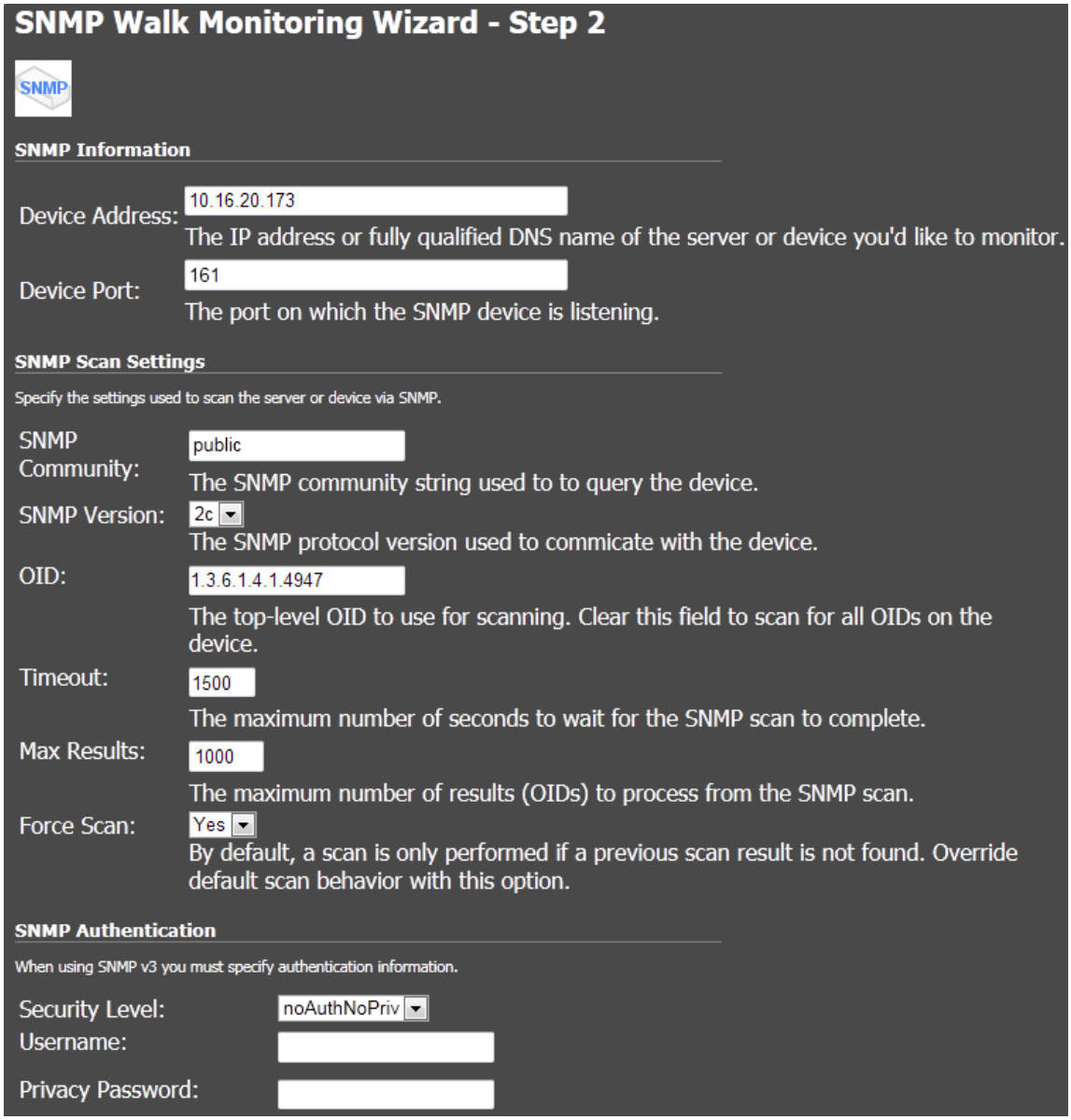
This task uses a Grass Valley 4ME Kayenne Panel as the example of the device monitored. Apply your knowledge of SNMP to monitor a different device, using these steps as a guideline.

1. Click **Configure | Run the Monitoring Wizard**.



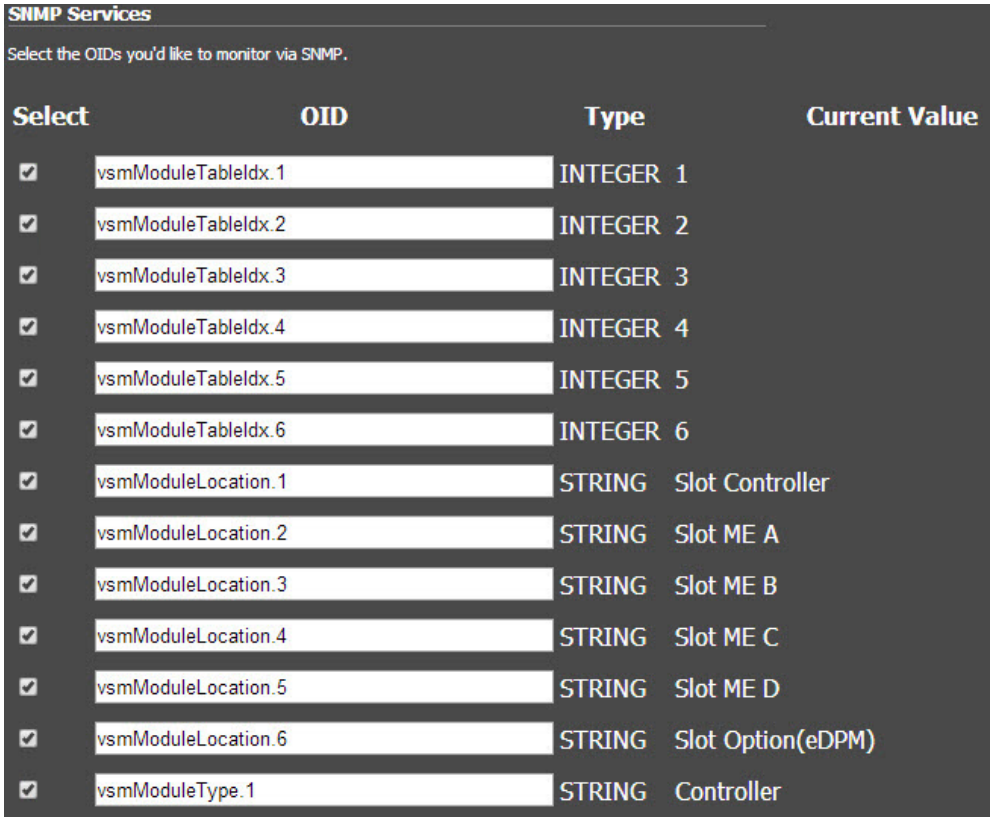
2. Select **SNMP Walk**.

3. Scroll to the bottom of the page and click **Next**.
   The Step 2 page opens.



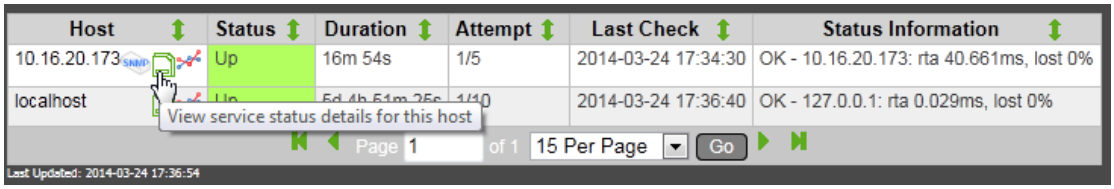
4. For **Device Address**, enter the IP address of the device to be monitored.
5. For **OID**, enter `1.3.6.1.4.1.4947`.
   This is the main OID for Grass Valley products.
6. For **Timeout**, enter `1500`.
7. For **Max Results**, enter `1000`.
8. For **Force Scan**, select **Yes**.
9. Click **Next**.
   GV GUARDIAN scans the device.
   The Step 3 page opens and displays a list of OIDs.

10. In the right-most **MIB To Use** column, find the rows for **GVG-VSM-MIB**.
11. In the left-most column, select the OIDs for the **GVG-VSM-MIB** rows.



12. Click **Next** and **Finish**.
13. Observe the progress of configuration and verification processes and verify that `Configuration applied successfully` is reported.
14. Navigate to **Home | Details | Host Detail**.

    The Host Status page opens and displays a list of monitored hosts.
15. On the row for the device you added with the SNMP Walk Wizard, click **View service status details for this host**.



The Service Status page opens.

16. Identify the Services that report `SNMP OK - No Such Instance currently exists at this OID` in the **Status Information** column.

Showing 1-111 of 111 total records

Host	Service	Status	Duration	Attempt	Last Check	Status Information
10.16.20.170	vsmModuleLocation.1	Ok	1d 3h 45m 7s	1/5	2014-03-21 16:29:13	SNMP OK - Slot ME A
	vsmModuleId.6	Ok	1d 3h 45m 10s	1/5	2014-03-21 16:29:10	SNMP OK - No Such Instanc
	vsmModuleId.5	Ok	1d 3h 45m 13s	1/5	2014-03-21 16:29:07	SNMP OK - 5
	vsmModuleId.4	Ok	1d 3h 45m 15s	1/5	2014-03-21 16:29:05	SNMP OK - 5
	vsmModuleId.3	Ok	1d 3h 45m 18s	1/5	2014-03-21 16:29:02	SNMP OK - 5
	vsmModuleId.2	Ok	1d 3h 45m 21s	1/5	2014-03-21 16:28:59	SNMP OK - 5
	vsmModuleId.1	Ok	1d 3h 45m 24s	1/5	2014-03-21 16:28:56	SNMP OK - 5
	vsmModuleHwRev.6	Ok	1d 3h 45m 27s	1/5	2014-03-21 16:28:53	SNMP OK - No Such Instanc
	vsmModuleHwRev.5	Ok	1d 3h 45m 30s	1/5	2014-03-21 16:28:50	SNMP OK - (FW 31 HW 0)

This indicates that this OID is not needed to monitor the device, as what it is configured to monitor does not exist.

17. For the OIDs not needed, delete the service. Refer to related topics in this Topic Library.

Related Topics

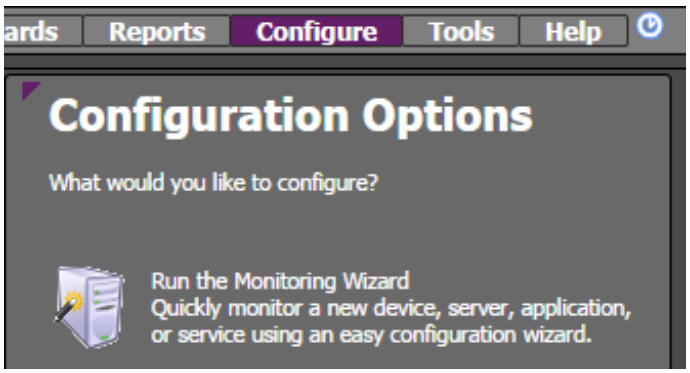
Delete a service on page 67

Monitor Windows processes

To do this task you must be logged in with administrator privileges.

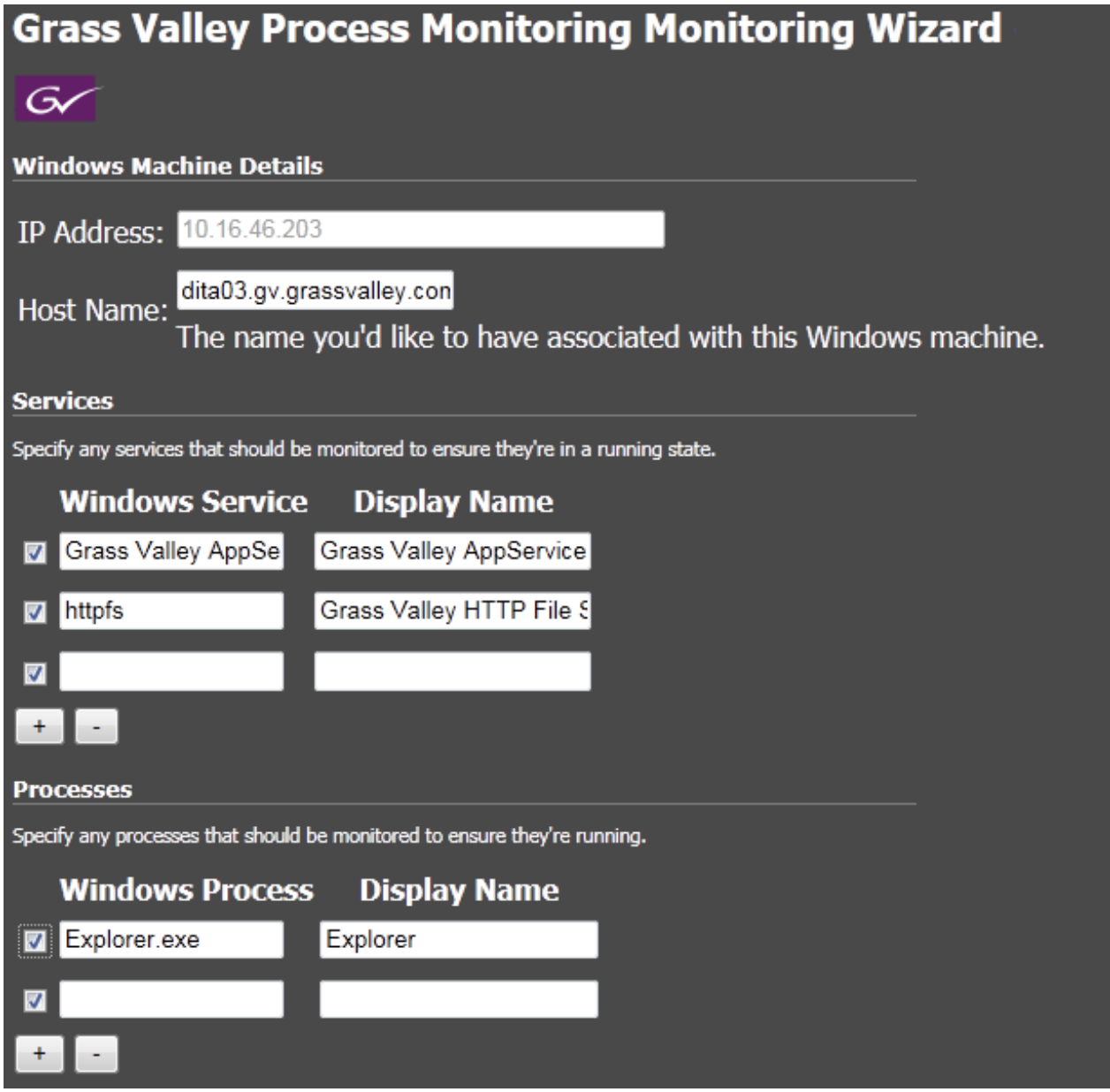
The GV GUARDIAN Grass Valley Process Monitoring Wizard ensures that services and process continue to run. The wizard monitors the service or process and if it finds that it is not running, starts the process automatically.

1. Click **Configure | Run the Monitoring Wizard**.



2. Select **Grass Valley Process Monitoring**.
3. Scroll to the bottom of the page and click **Next**.

4. Enter the IP address of the Windows machine to be monitored and click **Next**.



5. If the Windows machine has a host name that resolves on the network, it is automatically filled in. If the machine does not yet have a host name, enter a unique host name.
6. Configure the services to monitor as follows:
   a) Select each service to monitor.
   b) If desired, change the **Display Name**.
      The name you enter here is displayed in GV GUARDIAN.
   c) Click **+** or **-** to add or remove services.

7. Configure the processes to monitor as follows:

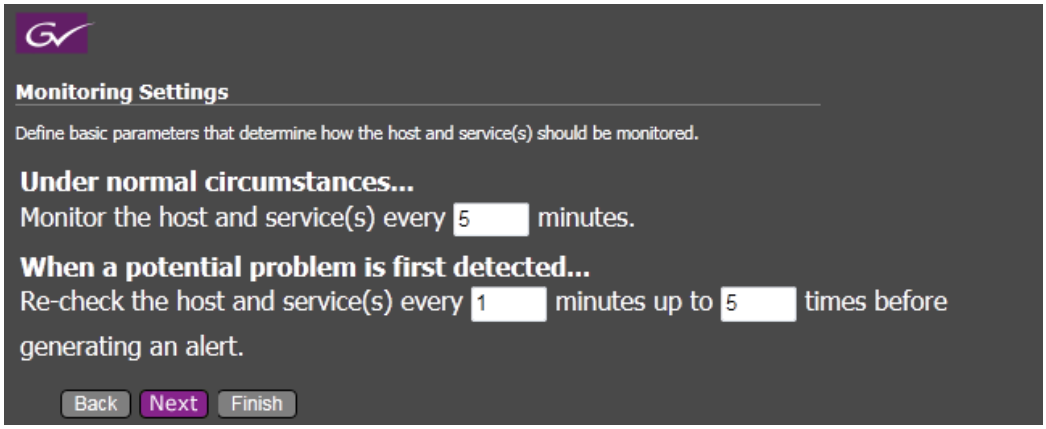
   Processes are applications that run on the Windows machine. They typically have a `.exe` file name extension.

   a) Select each process to monitor.
   b) If desired, change the **Display Name**.

      The name you enter here is displayed in GV GUARDIAN.

   c) Click **+** or **-** to add or remove processes.

8. Click **Next**.
9. Set the time intervals you want monitoring to poll the device. Default values are shown.



10. Click **Next**.
11. Observe the progress of configuration and verification processes and verify that `Configuration applied successfully` is reported.

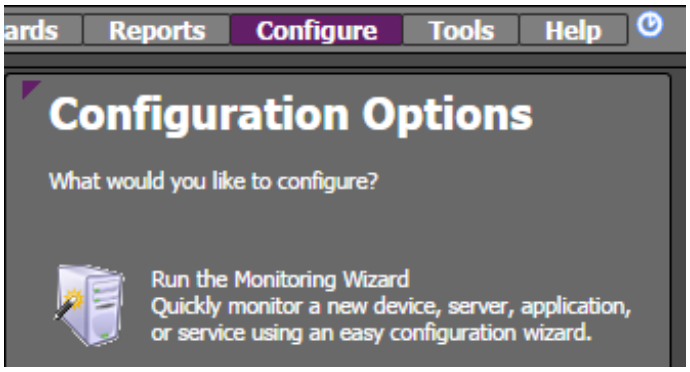
Configure monitoring wizard

- You must be logged on to the GV GUARDIAN system with administrator privileges.

Monitoring wizards provide you with a method of monitoring new devices, services, and applications. This topic provides an example of the Website monitoring wizard.

1. Navigate to **Configure | Configuration Wizards | Monitoring Wizard**, select the Website Monitoring Wizard and click **Next**.

2. Click **Configure | Run the Monitoring Wizard**.

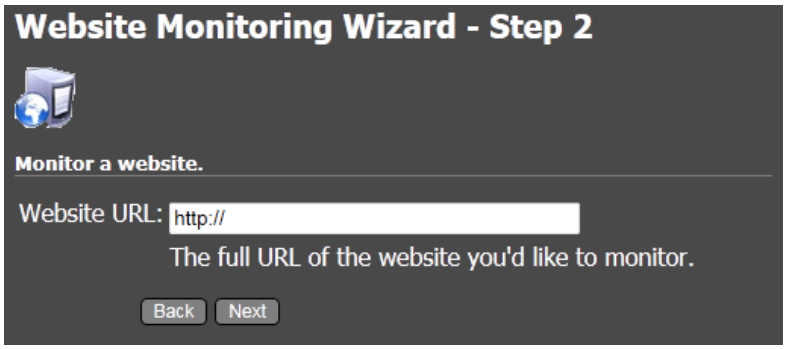


The **Monitoring Wizard - Step 1** page opens and displays a list of available wizards.

3. Select the Website Monitoring Wizard.

4. Scroll to the bottom of the page and click **Next**.

   The **Website Monitoring Wizard - Step 2** page opens.



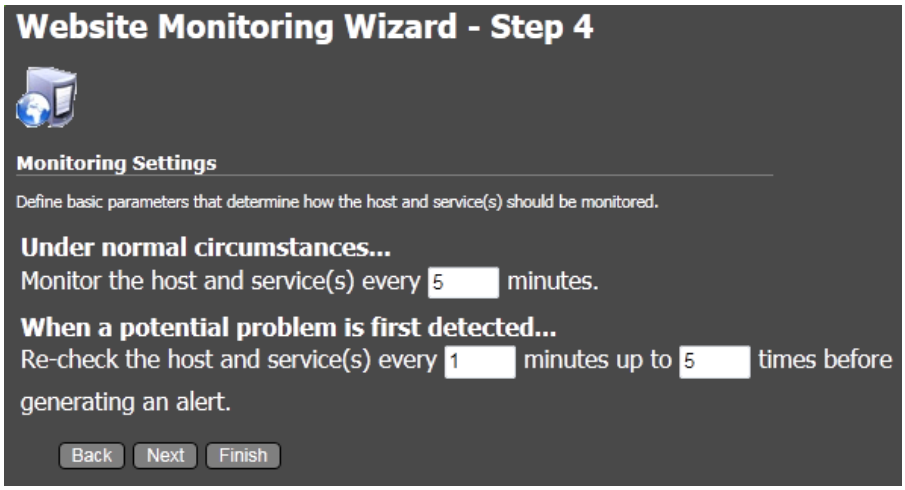
5. Enter the URL of the site to be monitored.

   The host information you enter on this page varies depending the type of monitor you're setting up.

6. Click **Next**.
   The **Website Monitoring Wizard - Step 3** page opens.

7. Configure the information relevant to the services you can monitor for the selected host.
8. Click **Next**.

   The **Website Monitoring Wizard - Step 4** page opens.



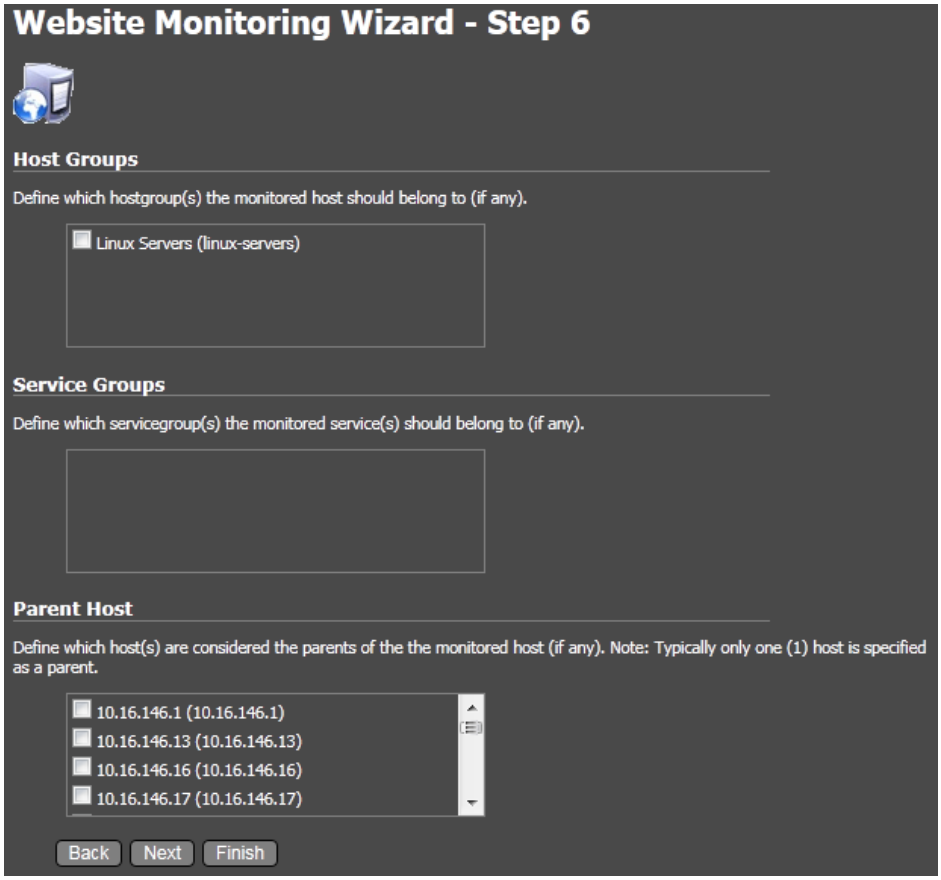
9. Configure the time increments for monitoring the host and services.
10. Click **Next**.

    The **Website Monitoring Wizard - Step 5** page opens.

11. Specify the circumstances and contacts for notifications relating to the hosts and services.

12. Click **Next**.

    The **Website Monitoring Wizard - Step 6** page opens.



13. Configure any final settings that may be necessary to monitor the hosts and services.
14. Click **Next** and **Apply** to submit the items you selected to monitor to the underlying monitoring engine.

The new devices, services, and applications you chose to monitor with the wizard will now be available in the GV GUARDIAN interface.

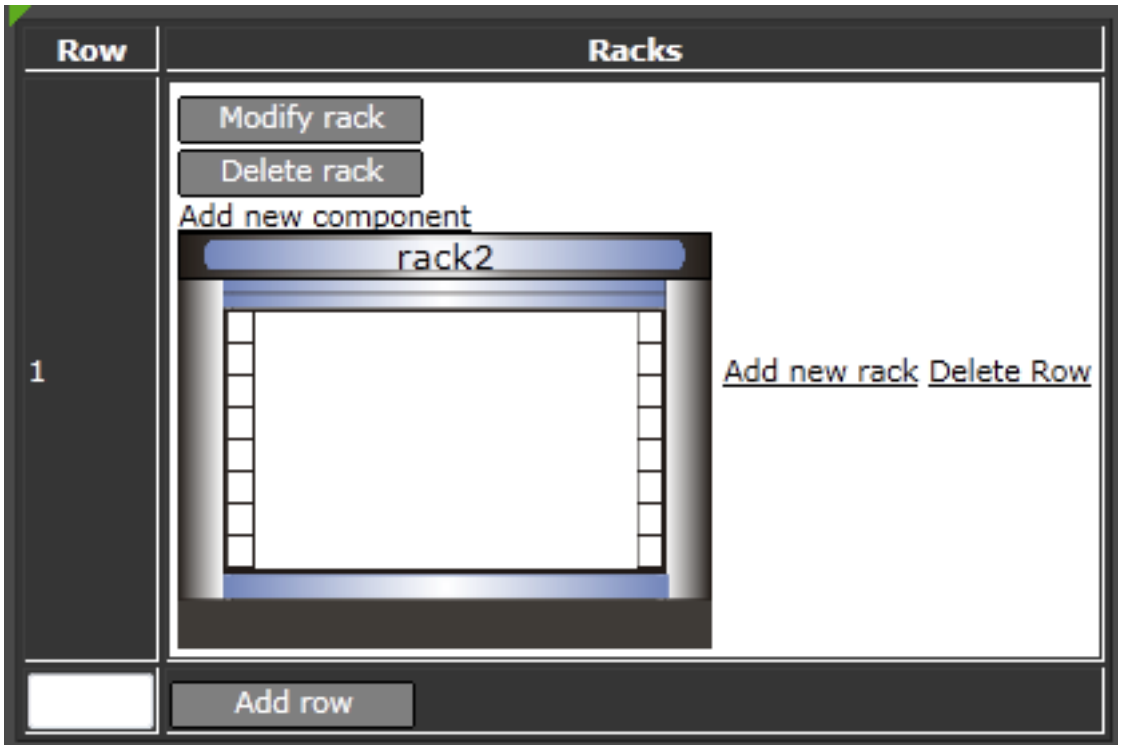
Map Data Center Rack configuration

A Data Center with its racks and servers can be mapped out by going to the Data Center's GV GUARDIAN page.

1. On the GV GUARDIAN home page, under **Grass Valley** click **Data Center Map**.

   A Data Center consists of zero or more rows of racks, a rack consists of zero or more components, and a component consists of zero or more hosts.

2. To add a row, type the row index in the input box on the bottom left and click **Add row**.



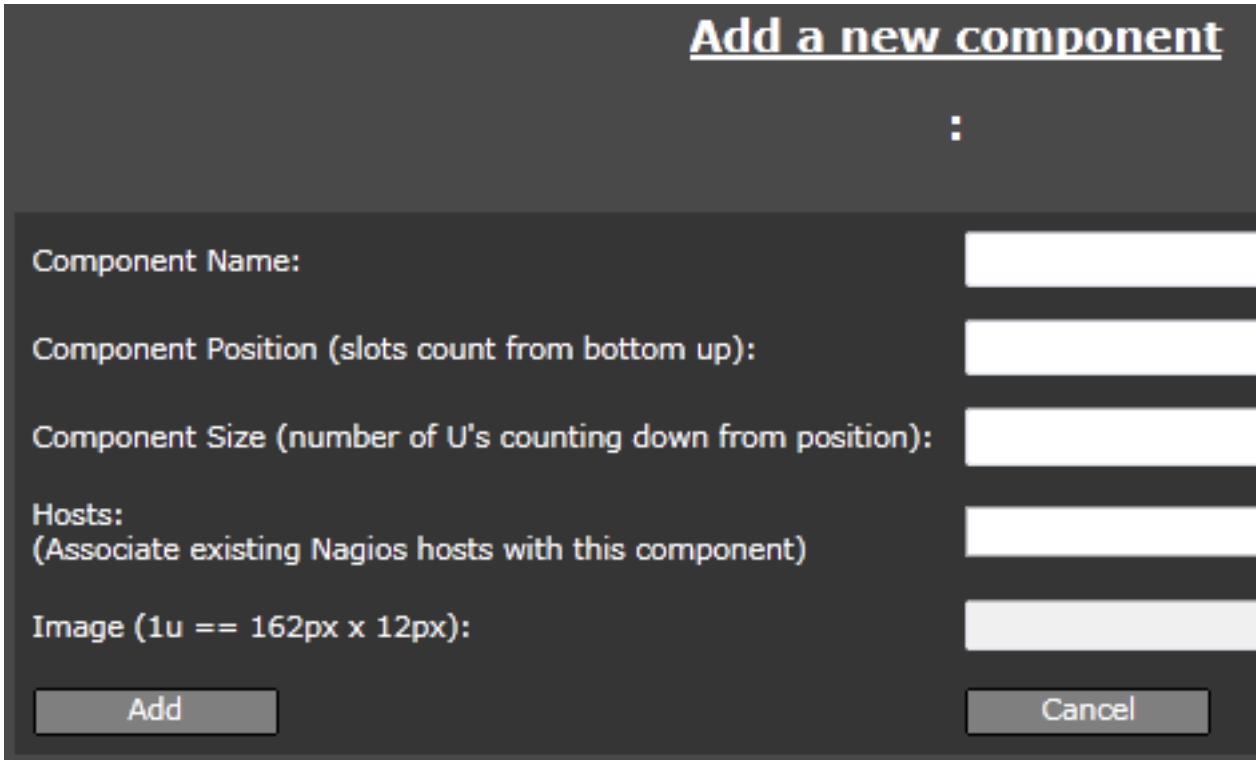
3. To add racks to the row, click **Add new rack**.
4. Fill out information about the rack as follows:

- **Rack Index**: The position of rack in the row. This setting is optional.
- **Name**: Appears as a label above the rack.
- **Rack Height**: The number of rack units in the rack.

5. Click **Add Rack**.
6. Use the buttons above the rack as desired:

- **Modify rack**
- **Delete rack**

7. Click **Add new component** to add components to the rack.
8. Fill out information about the component as follows:



- **Component Name**: The name displayed for the component.
- **Component Position**: Specifies the upper most slot of where the component exists in the rack. A rack's slots count from the bottom up.
- **Component Size**: The number of slots down the component occupies from the component's position.
- **Hosts**: Specifies which hosts are associated with this component. To add a host, select the host in the drop-down list and click **Add**.
- **Image**: You can add an image of the component. An image is rendered so that the width is 162px and the height is 12px for each rack unit. If the image is not at these dimensions, it is scaled to fit these dimensions.

Data Center rack indicators

In a Data Center rack, component states are indicated by color overlays as follows:

- Unknown: Black
- Critical: Red
- Warning: Yellow

Clicking on a component displays a page with each of the component's hosts, with the option to modify or delete the component. Clicking on a host displays a GV GUARDIAN page with the host and its services.

Views overview

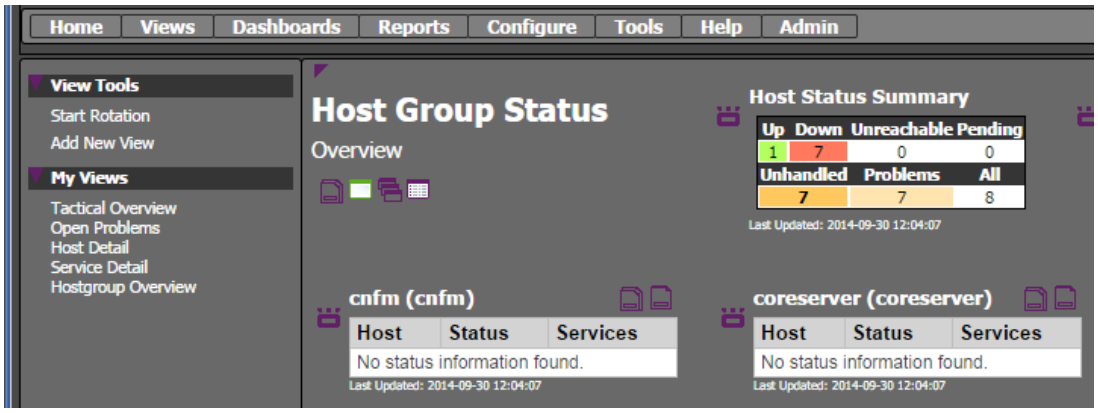
Views are designed to provide individual users with quick access to GV GUARDIAN pages and external websites they find useful. Views are often used by network administrators who wish to display important information on wall monitors in network operations centers (NOCs) or public locations.

Views are specific to individual GV GUARDIAN users. Each user can create their own unique set of views.

Access Views

Click **Views**.

The Views page opens.

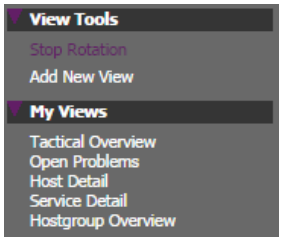


The Views page automatically cycles, or rotates, through each of the views you have defined, as listed under **My Views**.

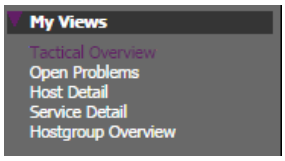
Stop View rotation

By default the Views page rotates through the different views you have defined. You can stop this rotation at any time by doing one of the following:

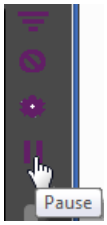
- Click **Stop Rotation**.



- Select a view.



- Click **Pause**.



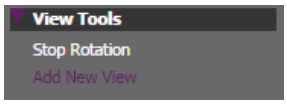
Adjust View rotation speed

Drag the view rotation slider upwards for longer viewing times, downwards for shorter viewing times.

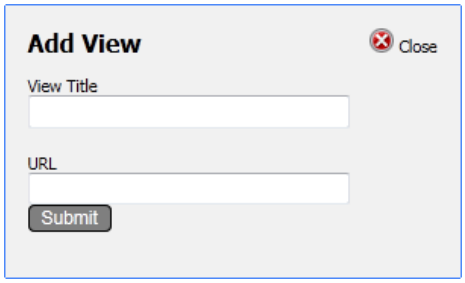
While the slider is at it's lowest, the rotation time will be the fastest (approximately 10 seconds).

Add new Views

1. Open the **Add View** dialog box as follows:
   - From the **Home** and **Dashboard** pages, click **Add to My Views**.
   - From the **Views** page, click **Add New View**.



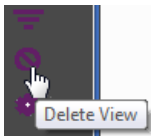
   The **Add View** dialog box opens.



2. Enter a title and any URL to display as a View.
   URLs can either be internal GV GUARDIAN pages or external URLs.

Delete Views

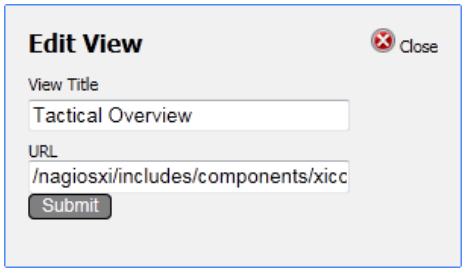
From the **Views** page, click **Delete View**.



Edit Views

1. From the **Views** page, click **Edit View**.

The **Edit View** dialog box opens.



2. Edit the title and URL and click **Submit**.

   URLs can either be internal GV GUARDIAN pages or external URLs.

Managing Hosts

You have the following options for managing a host:

- The Monitoring Wizard on the main Configure page: Allows easy setup.
- Core Config Manager: Provides precise control over host monitoring, notifications, and configurations.

Add/modify a host

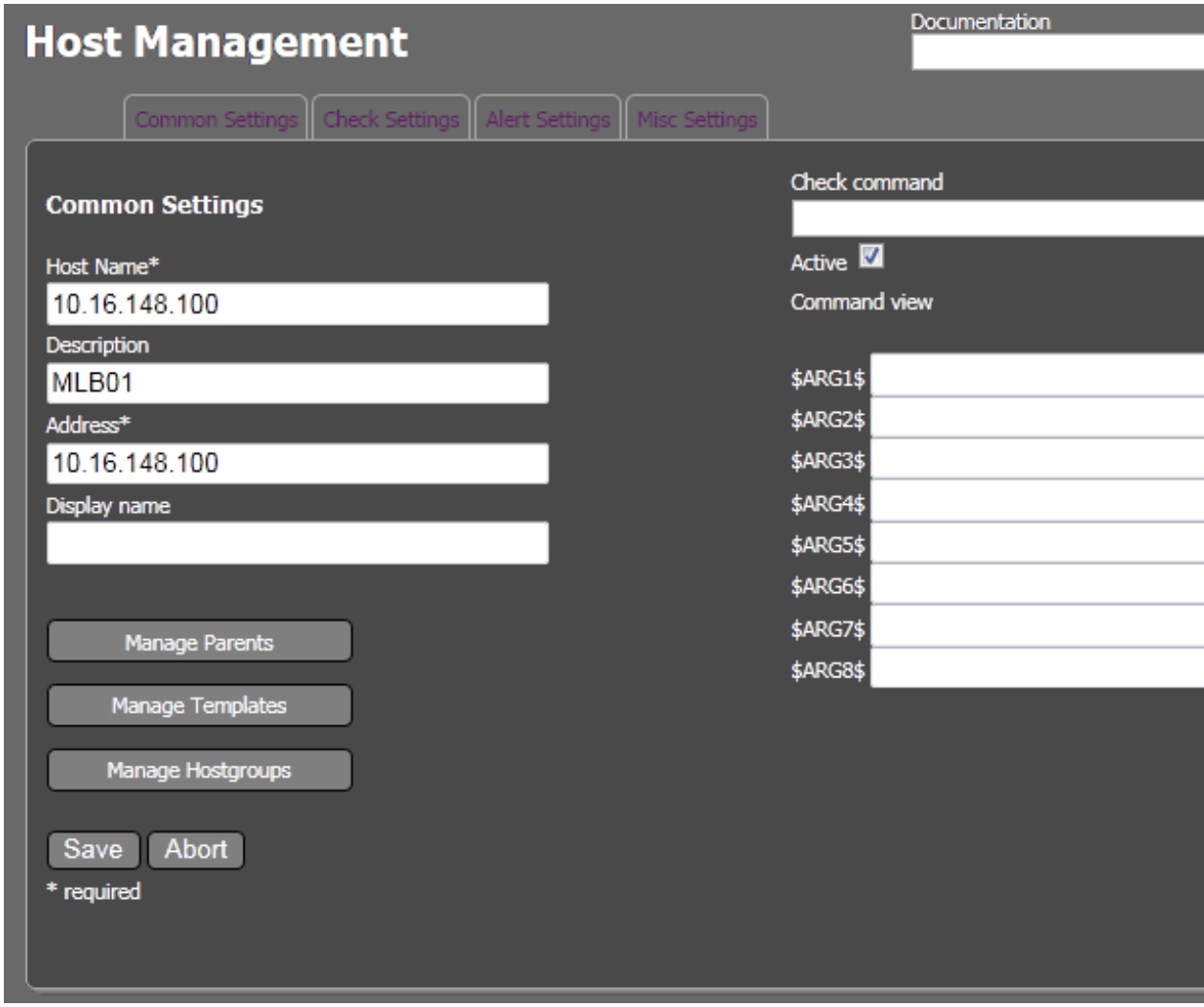
- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Hosts** page.
   The list of hosts currently monitored opens.

2. Do one of the following:
   - Click **Add New** to add a host.
   - On the row for the desired host, click **Modify**.

   Host Management settings open.

3. On the **Common Settings** tab, enter information as appropriate for the host you are monitoring. Fields marked with an asterisk are required.



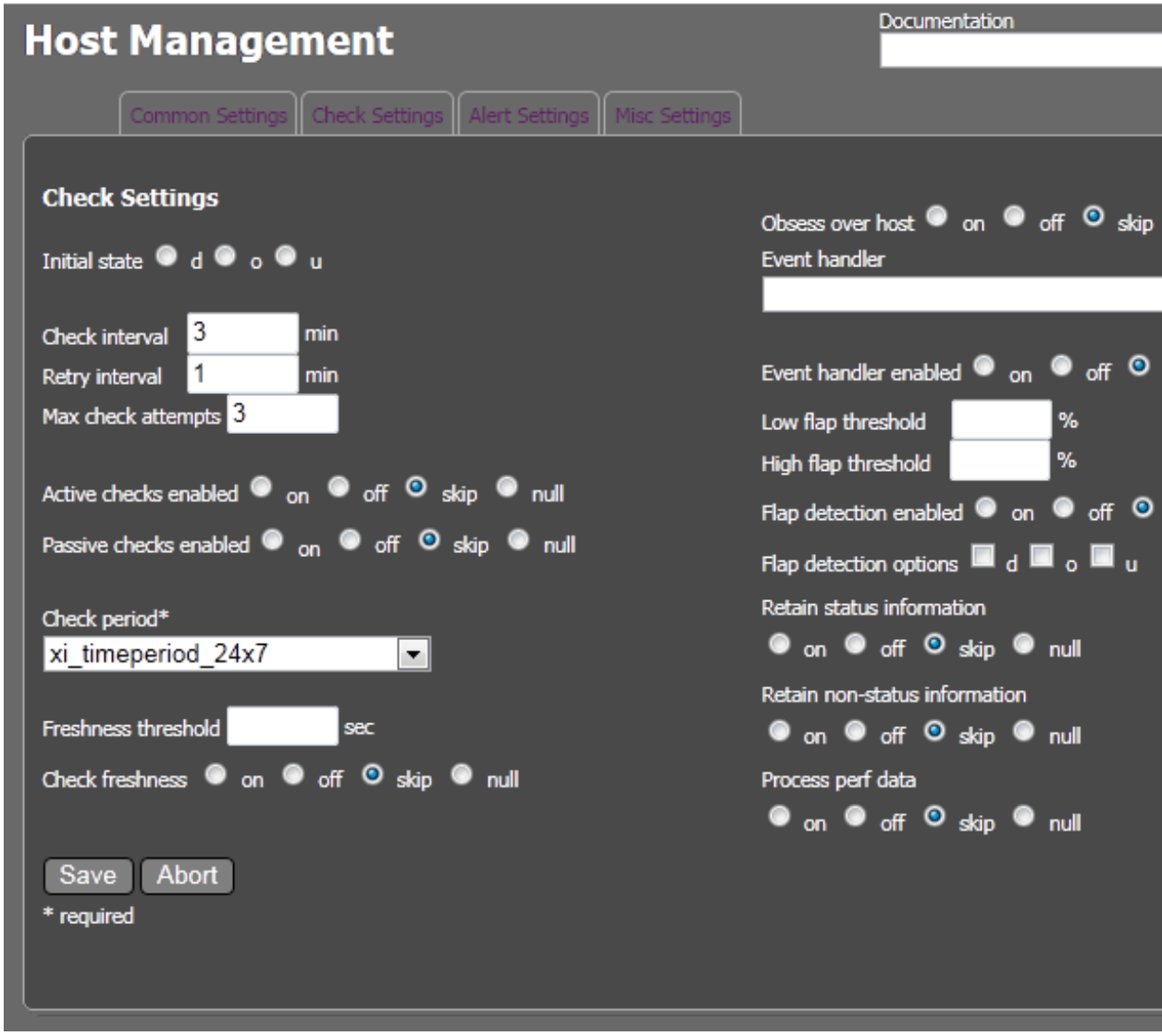
a) From the **Check command** drop-down list, select the method GV GUARDIAN uses to check if the host is operational.

   Each list item is associated with a set of GV GUARDIAN Core commands and arguments.

4. On the **Check Settings** tab, specify the settings for frequency of checks and the host state.

   If a problem is detected with a connection, you can specify the details of how GV GUARDIAN responds.

   Fields marked with an asterisk are required.

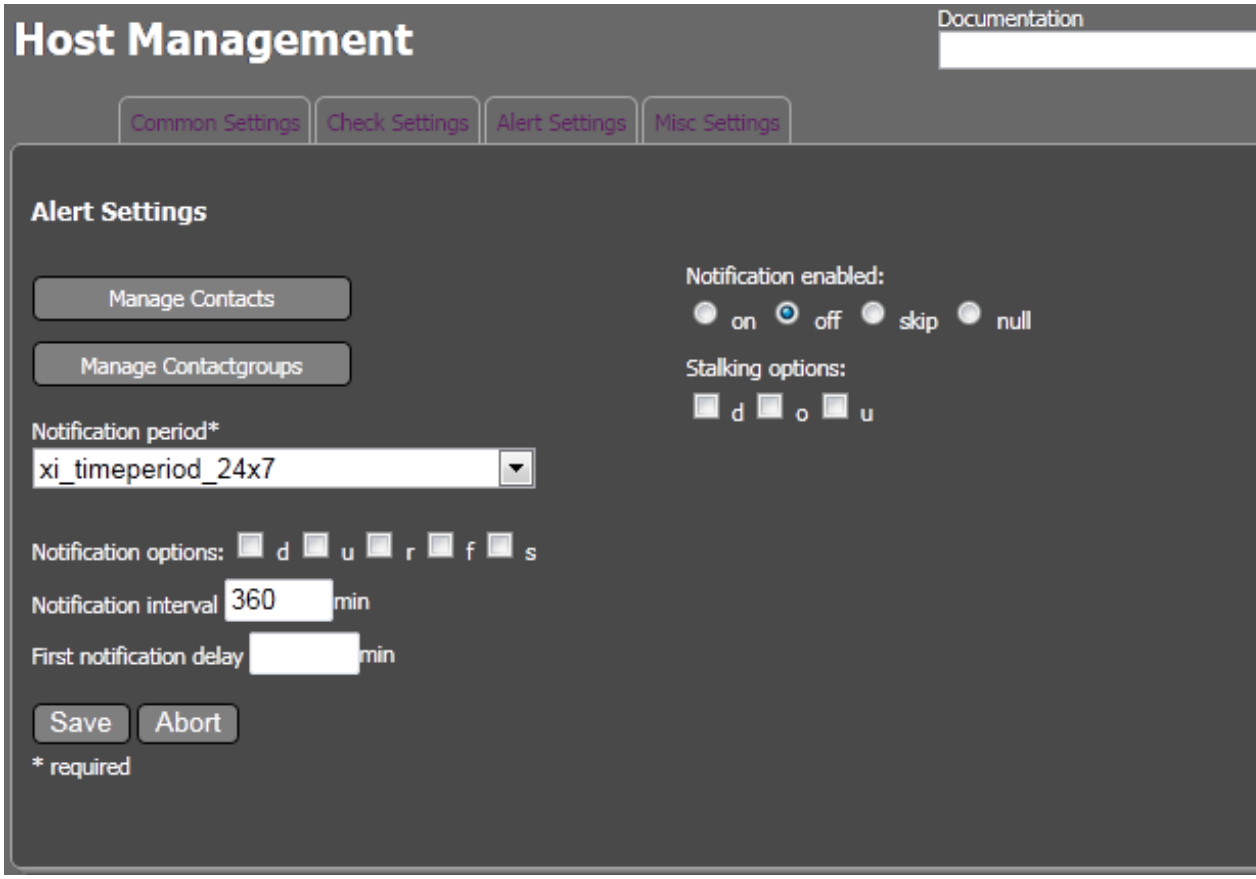


   a) For **Check interval**, enter the time between checks.
   b) For **Retry interval**, enter the time delay before GV GUARDIAN checks again if a problem is detected.
   c) For **Max check attempts**, enter the number of problem states that trigger a GV GUARDIAN notification.
   d) Select a check period.

5. On the **Alert Settings** tab, specify your notification settings using your existing contacts and contact groups.

   If a problem is detected with a connection, you can specify the details of how GV GUARDIAN sends alerts.

   Fields marked with an asterisk are required.



   a) Assign a contact or contact group to the host.
   b) Select a notification period.
   c) Select a notification interval.

6. If desired, on the **Misc Settings** tab, define additional host information, add notes, icon images, and make other settings.

   Place a 40x40 pixel icon image in the `ls /usr/local/nagios/share/images/logos/` directory to make it available for use in GV GUARDIAN.

7. Click **Save** and **Apply Configuration**.

Delete a host

- You must be logged on to the GV GUARDIAN system with administrator privileges.

Before you can delete a host, you must remove any dependent services.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Hosts** page.
   The list of hosts currently monitored opens.

2. On the row for the host you are deleting, click **Info**.
   Host information opens.

3. If the host has dependent services, as indicated in the host information, remove the dependent services.

   Refer to related topics in this Topic Library.

4. On the row for the host you are deleting, click **Delete**.

   GV GUARDIAN reports the result of the delete operation at the bottom of the page. If there are unresolved dependencies, GV GUARDIAN displays an error message in red.

5. If the delete operation succeeds, click **Apply Configuration**.

Related Topics

Remove a host's dependent services on page 68

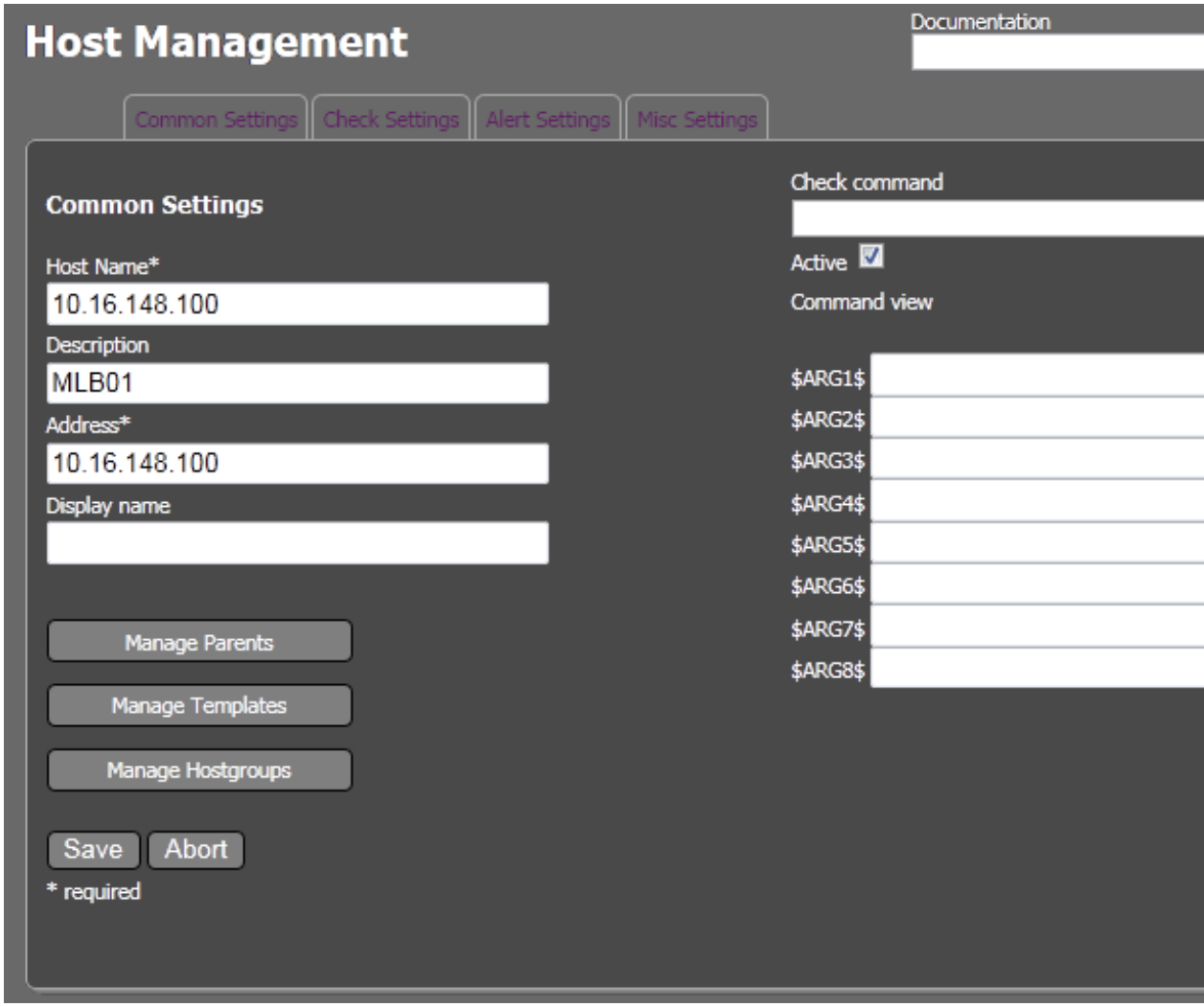
Copy a host

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Hosts** page.
   The list of hosts currently monitored opens.

2. On the row for the host you are copying, click **Copy**.
   The duplicate host is added to the list.
3. On the row for the duplicate host, click **Modify**.
   Host Management settings open.

4. On the **Common Settings** tab, enter information as appropriate for the host you are monitoring. Fields marked with an asterisk are required.



   a) Enter a valid host name and address.
   b) Select **Active**.

5. Click **Save** and **Apply Configuration**.

Display host information

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Hosts** page.
   The list of hosts currently monitored opens.

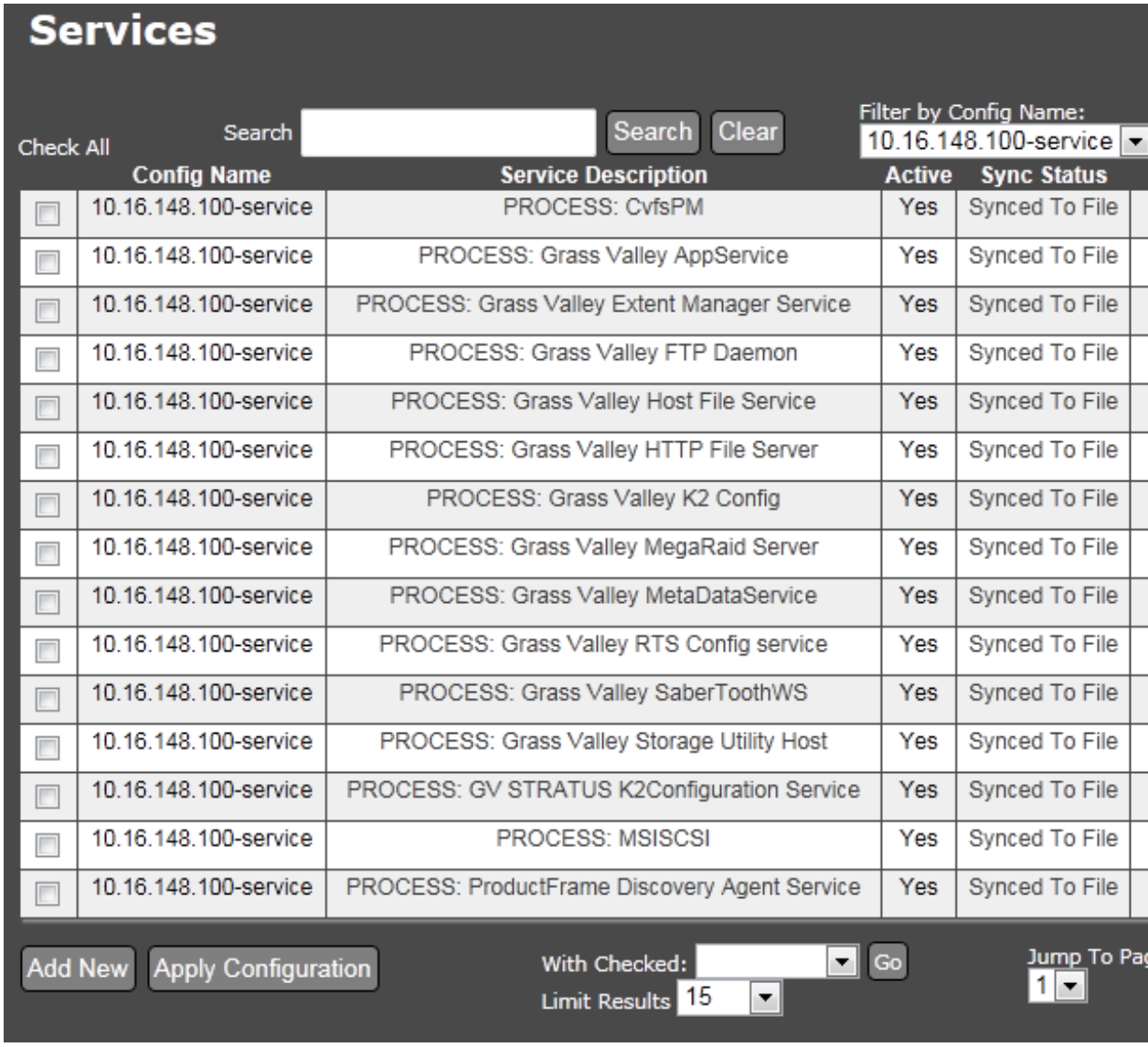
2. On the row for the desired host, click **Info**.
   Host information opens. Relationships are listed.

Managing Services

Add/modify a service

- You must be logged on to the GV GUARDIAN system with administrator privileges.

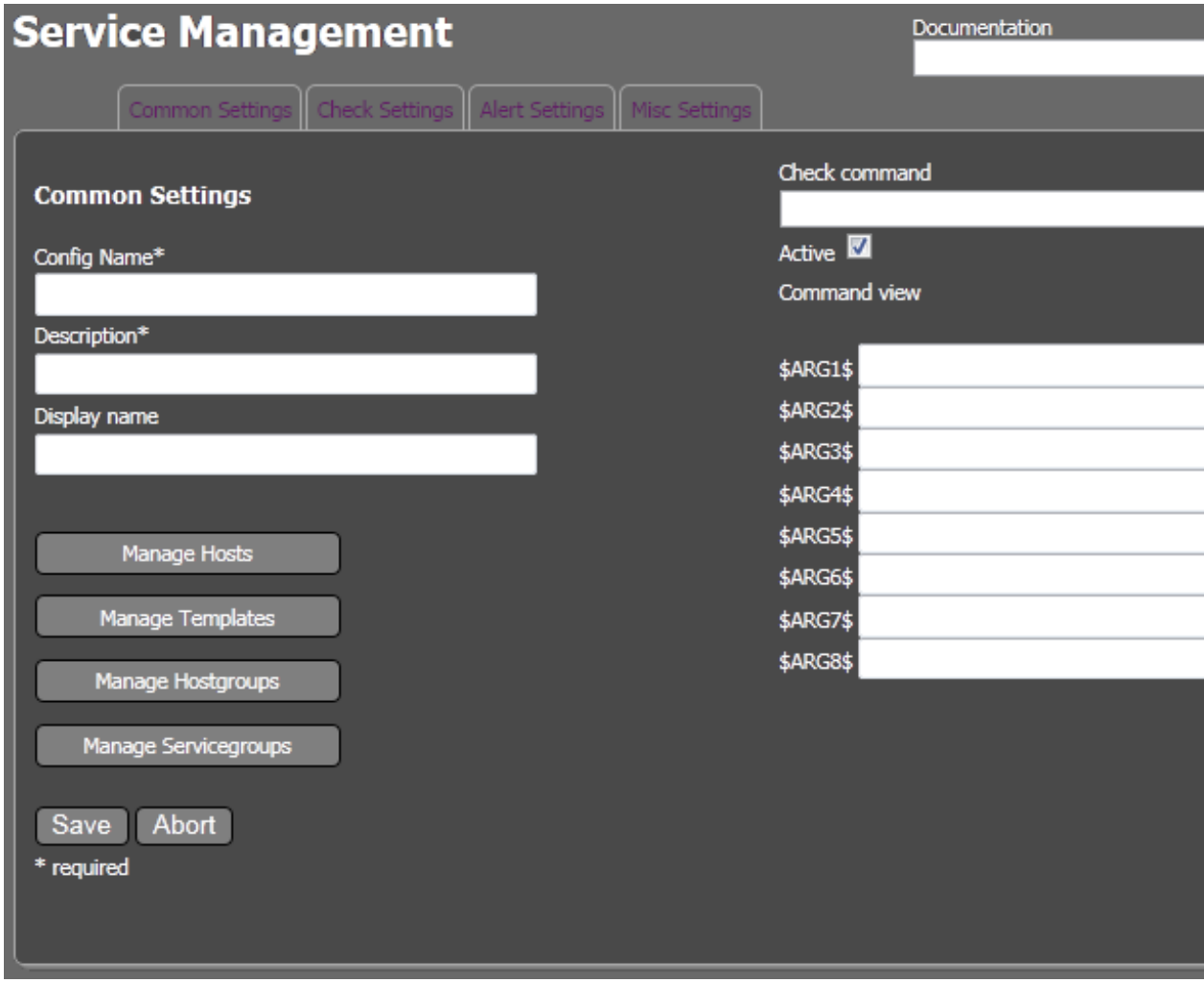
1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Services** page.
   A list opens and displays the services GV GUARDIAN is checking.



Config Name	Service Description	Active	Sync Status
10.16.148.100-service	PROCESS: CvfsPM	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley AppService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Extent Manager Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley FTP Daemon	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Host File Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley HTTP File Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley K2 Config	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MegaRaid Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MetaDataService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley RTS Config service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley SaberToothWS	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Storage Utility Host	Yes	Synced To File
10.16.148.100-service	PROCESS: GV STRATUS K2Configuration Service	Yes	Synced To File
10.16.148.100-service	PROCESS: MSISCSI	Yes	Synced To File
10.16.148.100-service	PROCESS: ProductFrame Discovery Agent Service	Yes	Synced To File

2. Do one of the following:
   - Click **Add New** to add a service.
   - On the row for the desired service, click **Modify**.

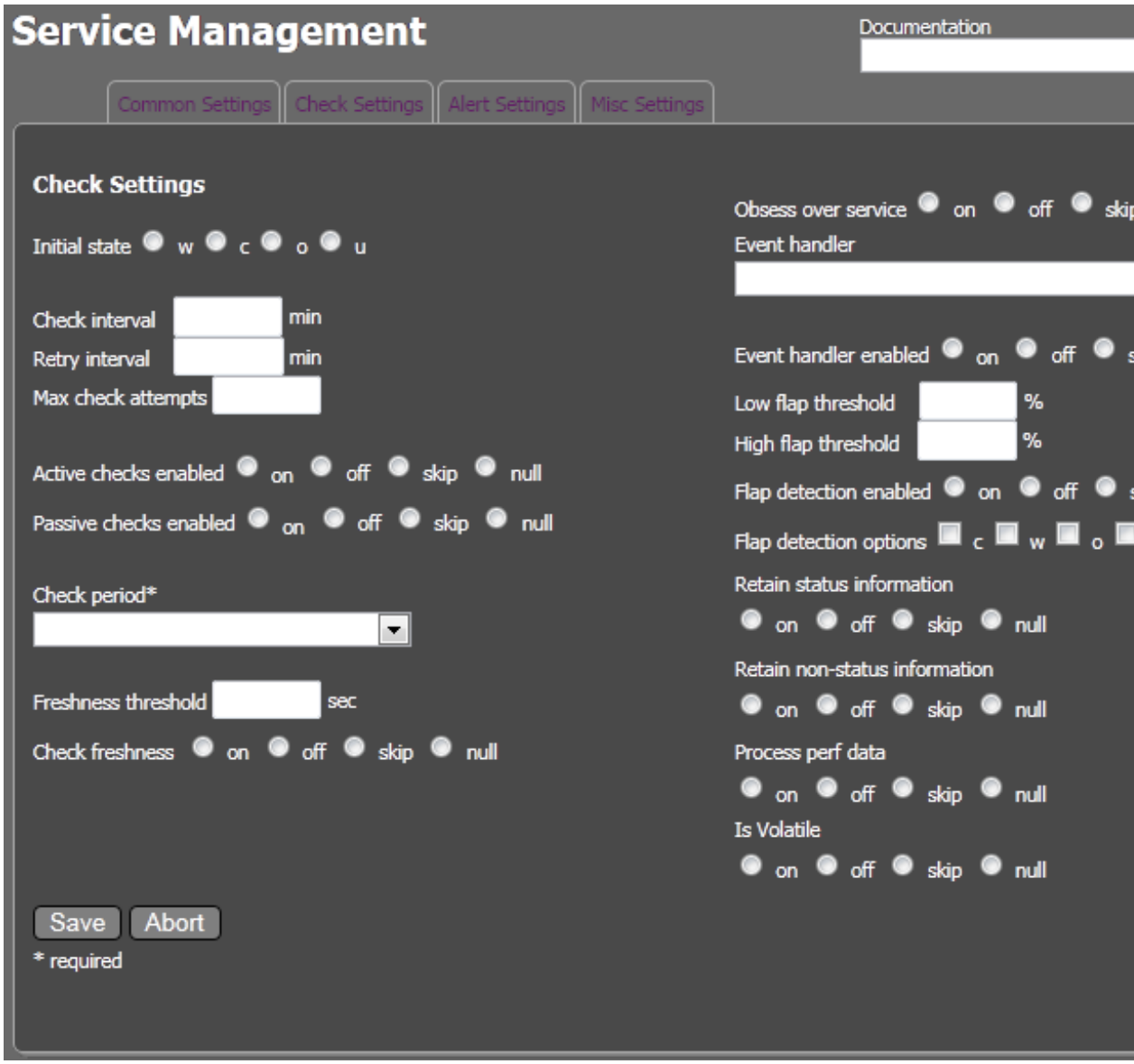
   Service Management settings open.
3. On the **Common Settings** tab, enter information as appropriate for the service.
   Fields marked with an asterisk are required.



   a) Enter a config name and description for display in GV GUARDIAN.
   b) Attach the service check to hosts using **Manage Hosts** or **Manage Hostgroups**.
   c) From the **Check command** drop-down list, select the method GV GUARDIAN uses to check the service.

      Each list item is associated with a set of GV GUARDIAN Core commands and arguments.

4. On the **Check Settings** tab, specify the settings for frequency of checks and the service state. If a problem is detected, you can specify the details of how GV GUARDIAN responds. Fields marked with an asterisk are required.

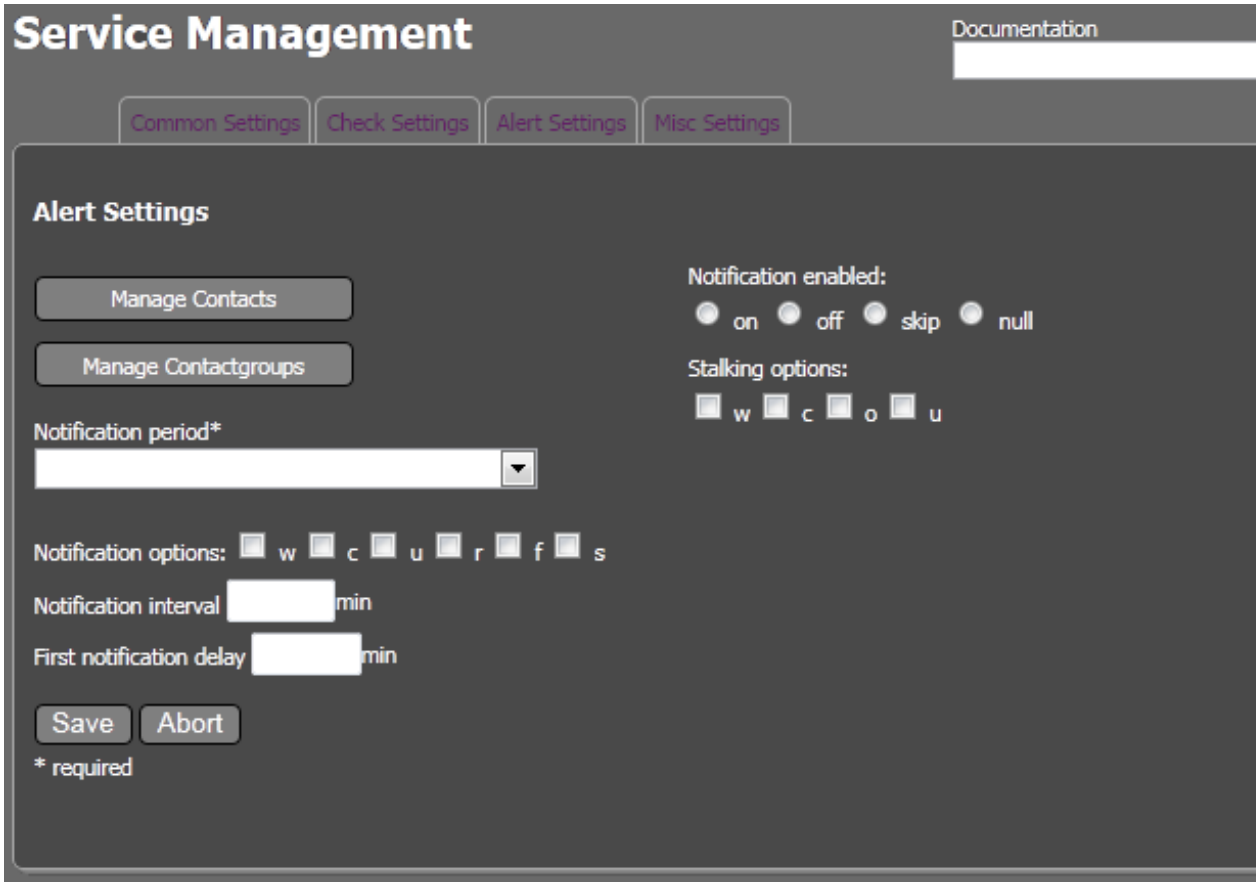


a) For **Check interval**, enter the time between checks.
b) For **Retry interval**, enter the time delay before GV GUARDIAN checks again if a problem is detected.
c) For **Max check attempts**, enter the number of problem states that trigger a GV GUARDIAN notification.
d) Select a check period.

5. On the **Alert Settings** tab, specify your notification settings using your existing contacts and contact groups.

   If a problem is detected, you can specify the details of how GV GUARDIAN sends alerts.

   Fields marked with an asterisk are required.



   a) Assign a contact or contact group.
   b) Select a notification period.
   c) Select a notification interval.

6. If desired, on the **Misc Settings** tab, define additional information, add notes, icon images, and make other settings.

   Place a 40x40 pixel icon image in the `ls /usr/local/nagios/share/images/logos/` directory to make it available for use in GV GUARDIAN.

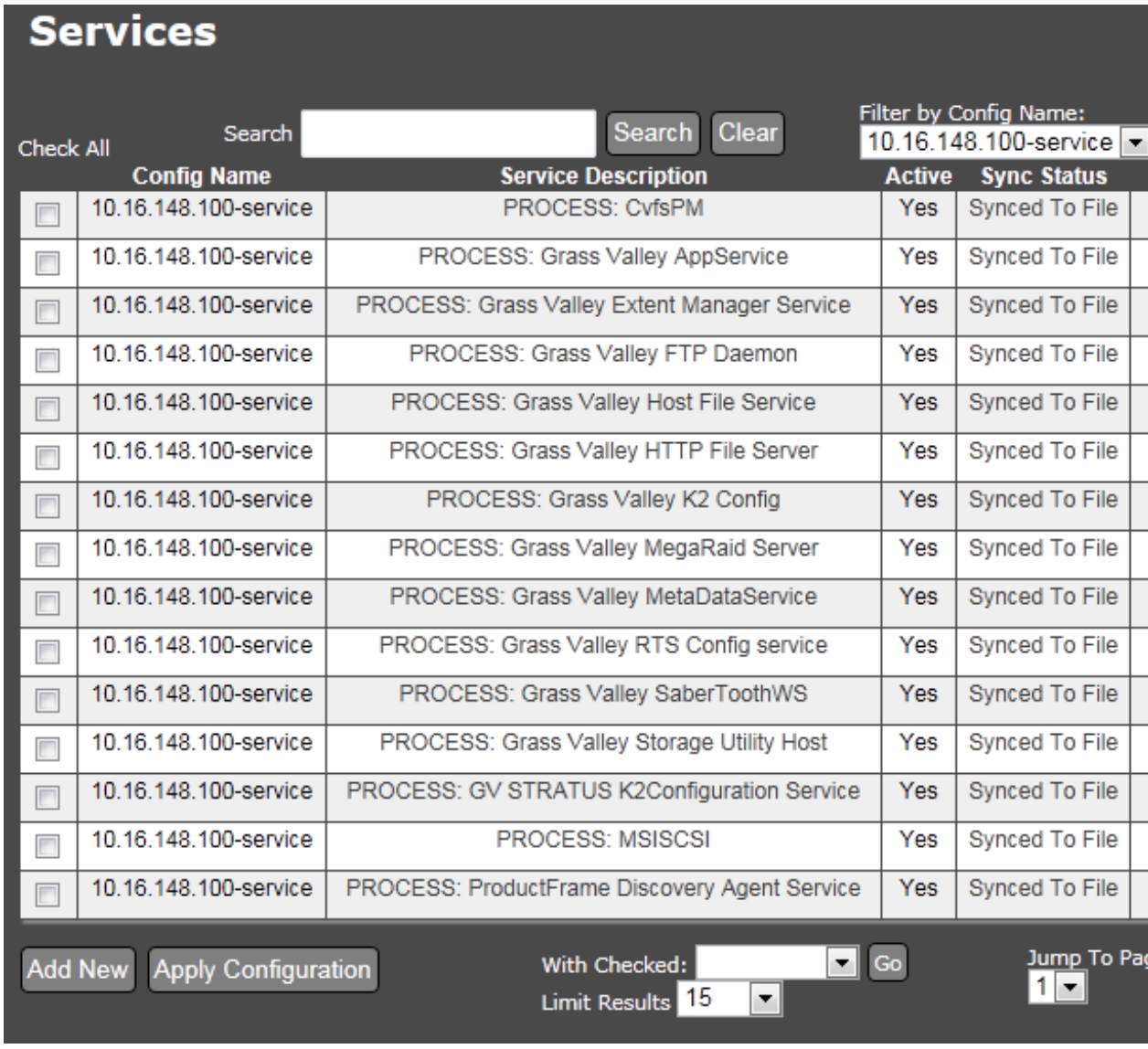
7. Click **Save** and **Apply Configuration**.

Delete a service

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Services** page.

   A list opens and displays the services GV GUARDIAN is checking.



Config Name	Service Description	Active	Sync Status
10.16.148.100-service	PROCESS: CvfsPM	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley AppService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Extent Manager Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley FTP Daemon	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Host File Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley HTTP File Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley K2 Config	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MegaRaid Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MetaDataService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley RTS Config service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley SaberToothWS	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Storage Utility Host	Yes	Synced To File
10.16.148.100-service	PROCESS: GV STRATUS K2Configuration Service	Yes	Synced To File
10.16.148.100-service	PROCESS: MSISCSI	Yes	Synced To File
10.16.148.100-service	PROCESS: ProductFrame Discovery Agent Service	Yes	Synced To File

2. On the row for the service you are deleting, click **Delete**.

   GV GUARDIAN reports the result of the delete operation at the bottom of the page. If there are unresolved dependencies, GV GUARDIAN displays an error message in red.

3. If the delete operation succeeds, click **Apply Configuration**.

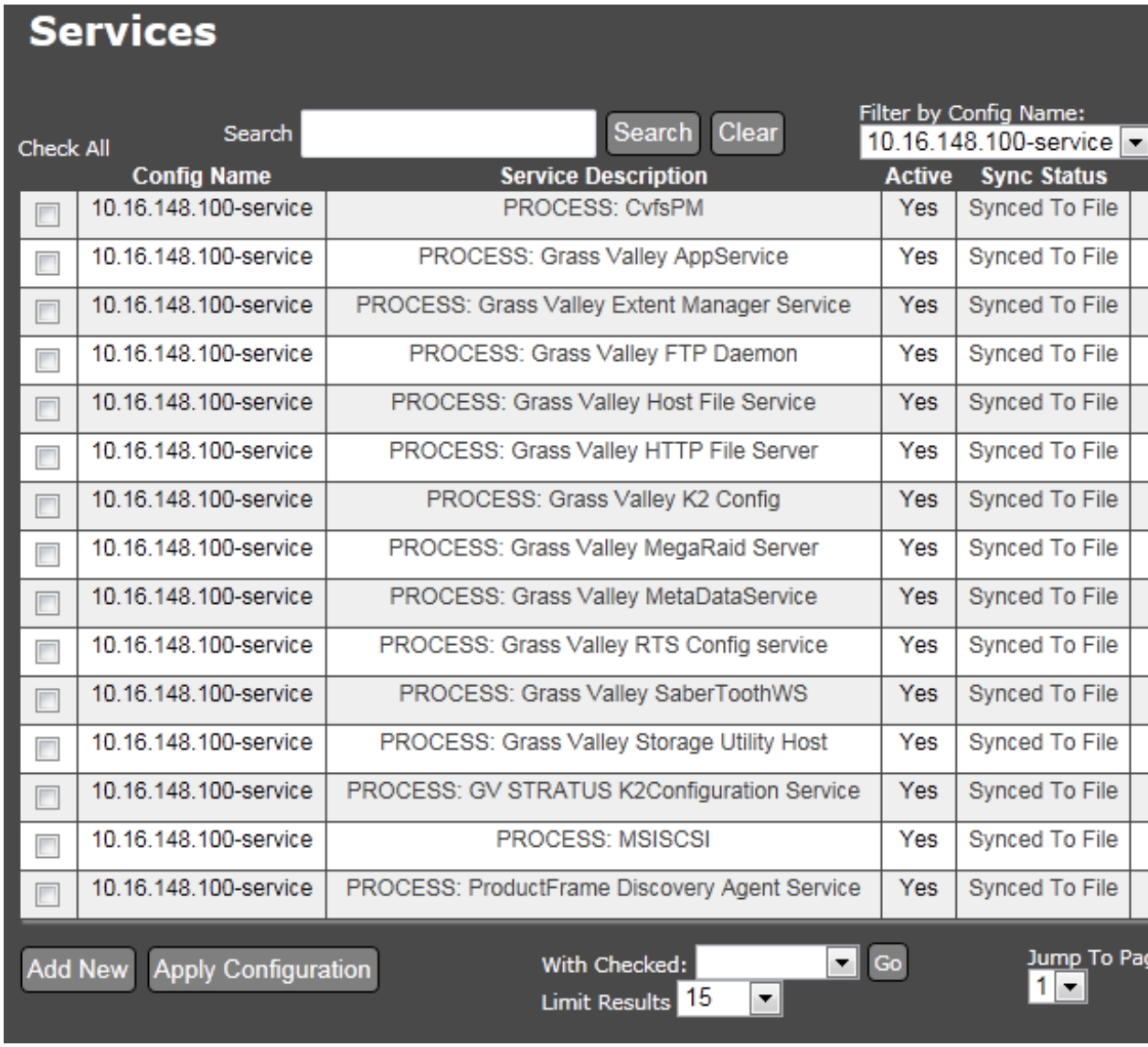
Remove a host's dependent services

- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can remove all of service checks that are dependent on a host. This is a prerequisite to deleting the host.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Services** page.

   A list opens and displays the services GV GUARDIAN is checking.



2. In the **Filter by Config Name** drop-down list, select the desired host.

   The list of services used by the host opens.

3. Select **Check All**.
4. In the **With Checked** drop-down list, select **Delete**.

The dependent services are removed from the host.

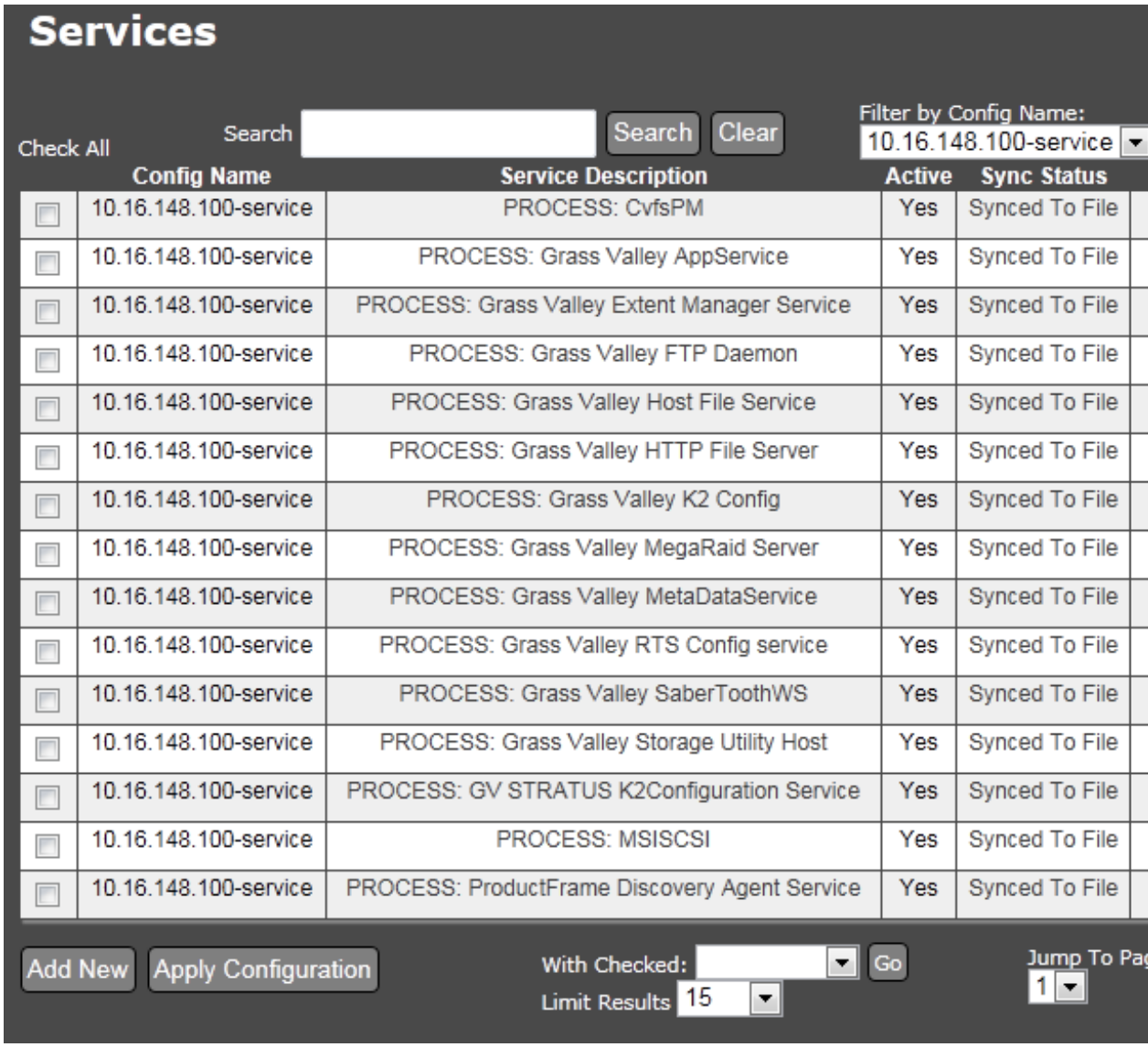
Related Topics

Delete a host on page 57

Copy a service

- You must be logged on to the GV GUARDIAN system with administrator privileges.

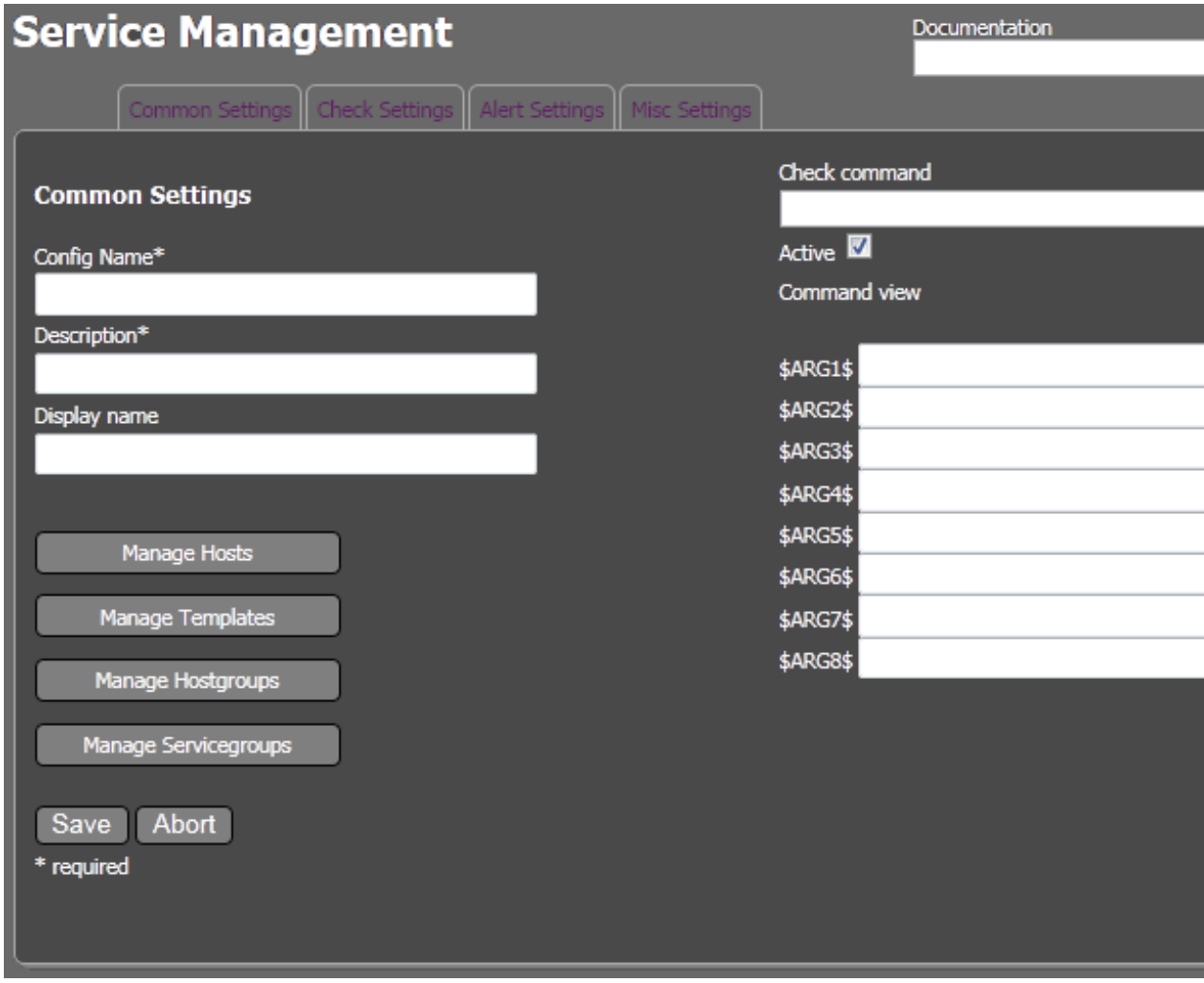
1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Services** page.
   A list opens and displays the services GV GUARDIAN is checking.



Config Name	Service Description	Active	Sync Status
10.16.148.100-service	PROCESS: CvfsPM	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley AppService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Extent Manager Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley FTP Daemon	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Host File Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley HTTP File Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley K2 Config	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MegaRaid Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MetaDataService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley RTS Config service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley SaberToothWS	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Storage Utility Host	Yes	Synced To File
10.16.148.100-service	PROCESS: GV STRATUS K2Configuration Service	Yes	Synced To File
10.16.148.100-service	PROCESS: MSISCSI	Yes	Synced To File
10.16.148.100-service	PROCESS: ProductFrame Discovery Agent Service	Yes	Synced To File

2. On the row for the service you are copying, click **Copy**.
   The duplicate service is added to the list.

3. On the **Common Settings** tab, enter information as appropriate for the service.
   Fields marked with an asterisk are required.



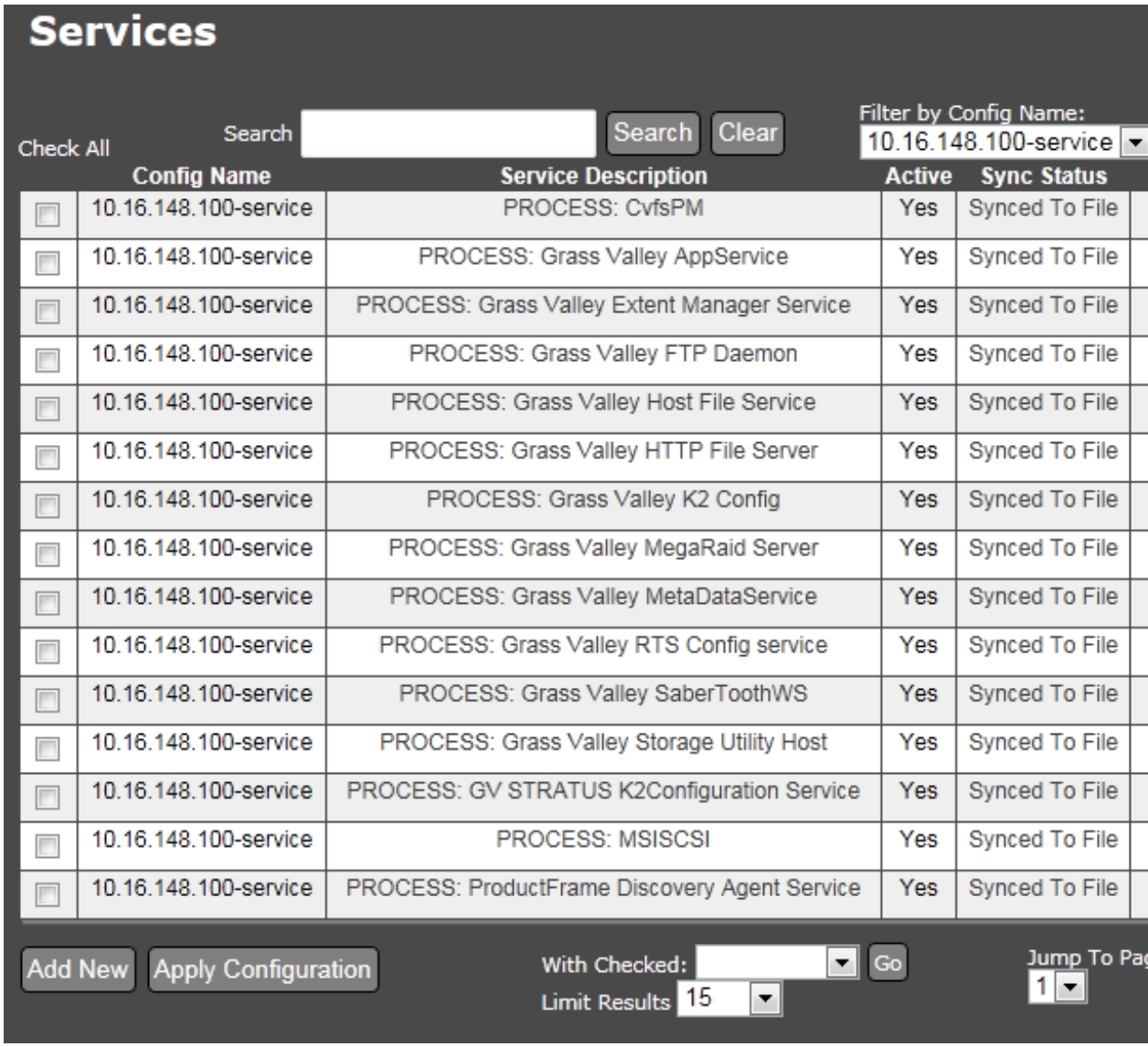
   a) Enter a config name and description for display in GV GUARDIAN.
   b) Attach the service check to hosts using **Manage Hosts** or **Manage Hostgroups**.
   c) From the **Check command** drop-down list, select the method GV GUARDIAN uses to check the service.
      Each list item is associated with a set of GV GUARDIAN Core commands and arguments.
   d) Select **Active**.

4. Click **Save** and **Apply Configuration**.

Display service information

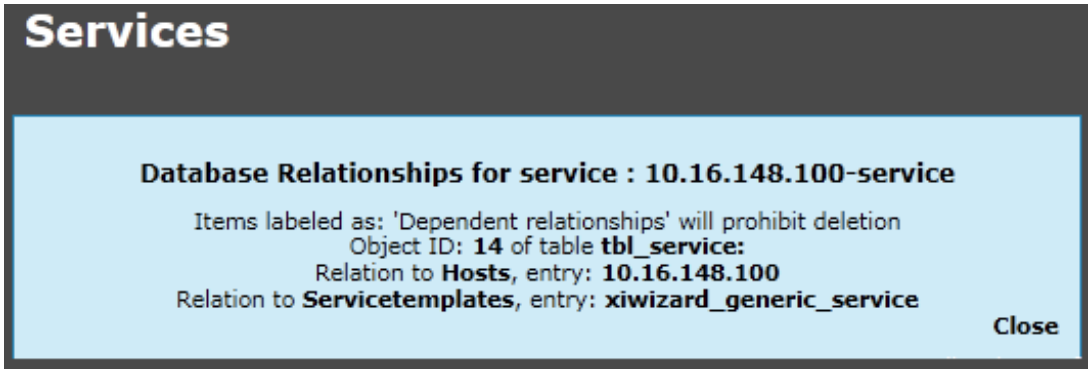
- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Services** page.
   A list opens and displays the services GV GUARDIAN is checking.



Config Name	Service Description	Active	Sync Status
10.16.148.100-service	PROCESS: CvfsPM	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley AppService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Extent Manager Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley FTP Daemon	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Host File Service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley HTTP File Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley K2 Config	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MegaRaid Server	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley MetaDataService	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley RTS Config service	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley SaberToothWS	Yes	Synced To File
10.16.148.100-service	PROCESS: Grass Valley Storage Utility Host	Yes	Synced To File
10.16.148.100-service	PROCESS: GV STRATUS K2Configuration Service	Yes	Synced To File
10.16.148.100-service	PROCESS: MSISCSI	Yes	Synced To File
10.16.148.100-service	PROCESS: ProductFrame Discovery Agent Service	Yes	Synced To File

2. On the row for the desired service, click **Info**.
   Service information opens. Relationships are listed.



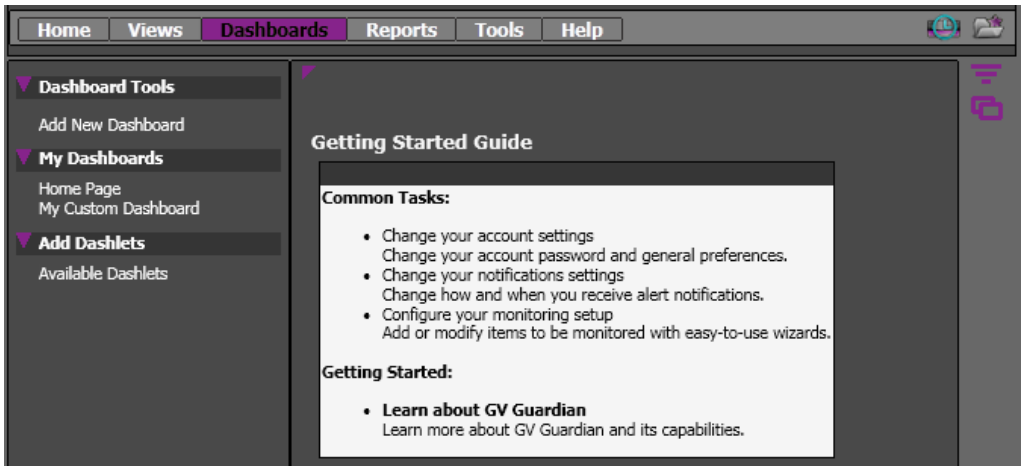
Dashboards overview

Dashboards are a powerful feature of GV GUARDIAN designed to provide individual users with customized information they find useful. Dashboards are often used to display important, relevant information where it is needed most.

Dashboards are specific to individual GV GUARDIAN users. Each user can create their own unique set of dashboards to customize GV GUARDIAN to fit their needs.

Access Dashboards

1. Click **Dashboards**.



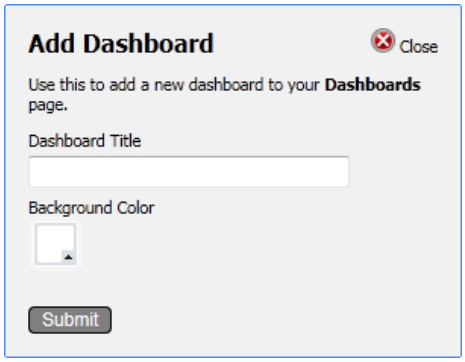
   The Home Page dashboard loads by default.

2. Under **My Dashboards** select a dashboard.

Add Dashboards

GV GUARDIAN allows users to create multiple customized dashboards.

1. Navigate to **Dashboard | Dashboard Tools | Add New Dashboard**.
   The **Add Dashboard** dialog box opens.

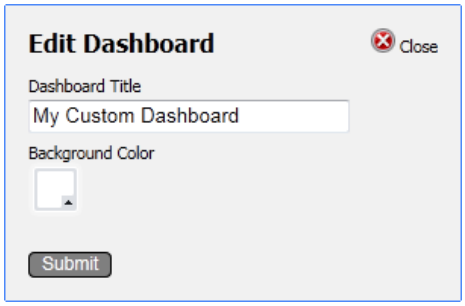


2. Enter a Title and background color and click **Submit**.
3. Under **My Dashboards** select the new dashboard.

Edit Dashboards

1. On the **Dashboard** page, under **My Dashboards**, select the dashboard you are editing.
2. Click **Edit Dashboard**.

The **Edit Dashboard** dialog box opens.

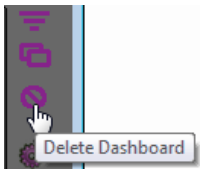


3. Edit the title and background color as desired and then click **Submit**.

Delete Dashboards

1. On the **Dashboard** page, under **My Dashboards**, select the dashboard you are deleting.

2. Click **Delete Dashboard**.

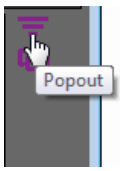


3. When prompted to confirm deletion, click **Delete**.

Expand Dashboards

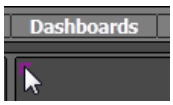
You can expand a Dashboard to fill the browser window in the following ways.

- Click **Popout**.



  The selected dashboard opens in a new browser tab.

- Click the expand control.



  The selected dashboard expands to fill the current browser window.

  Click the expand control again to return to the Dashboard page view.

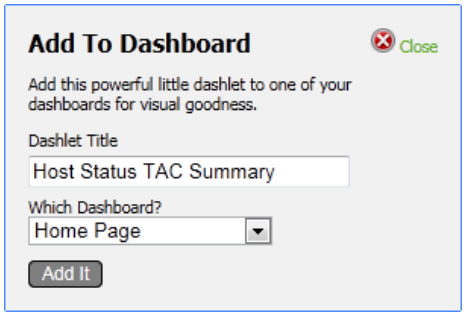
Add Dashlets

GV GUARDIAN allows you to add dashlets to your dashboard. A dashlet can be added from the Dashboard page or from other GV GUARDIAN pages. Any summary, graph, or chart that has **Add This To A Dashboard** can be added as a dashlet to your dashboard.

1. Find the desired dashlet in one of the following locations:
   - Navigate to **Dashboard | Add Dashlets | Available Dashlets**.

     Dashlet titles, images, and descriptions are displayed in a list.
   - Browse a GV GUARDIAN page that contains dashlets.

2. Next to the desired dashlet, click **Add This To A Dashboard**.
   The **Add To Dashboard** dialog box opens.

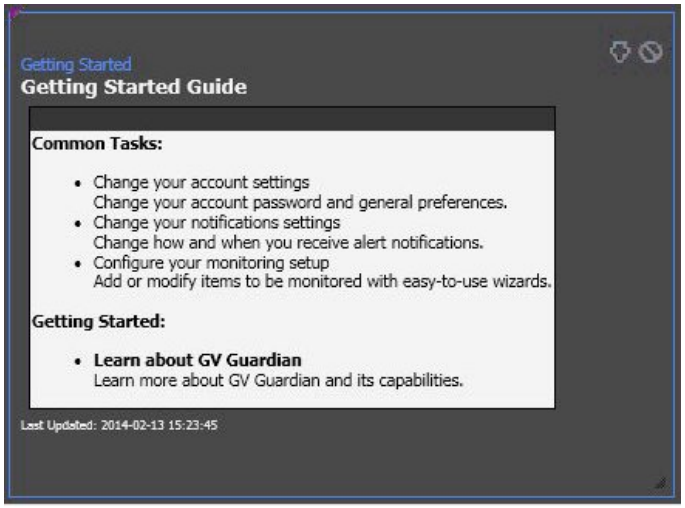


3. Specify the title of the dashlet, select the dashboard to which the dashlet is added, and click **Add It**.

Manipulate Dashlets

You can move and resize dashlets within the dashboard to create a custom layout to fit your needs.

1. Hover over a dashlet it to reveal a blue border and a set of buttons.



2. Adjust the dashlet's position as follows:
   a) Toggle the **Pin / Float Dashlet** button to allow the dashlet to be moved.
   b) Drag the dashlet into position.
   c) Toggle the **Pin / Float Dashlet** button to affix the dashlet in place.
3. Adjust the dashlet's size at the bottom right corner of the dashlet.

Home Page Dashboard

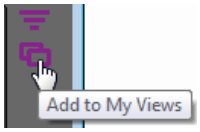
When you log on, GV GUARDIAN displays your unique home page dashboard.

Navigate to **Dashboards | My Dashboard | Home Page** to modify your home page dashboard and add, manipulate, and remove dashlets.

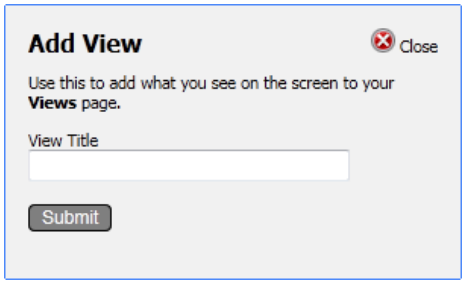
Dashboards and Views

You can add a dashboard to a view page.

1. On the **Dashboard** page, under **My Dashboards**, select the dashboard you are adding to a view.
2. Click **Add To My Views**.



The **Add View** dialog box opens.



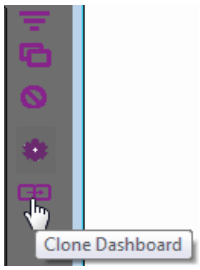
3. Enter the view title and click **Submit**.

Clone Dashboards

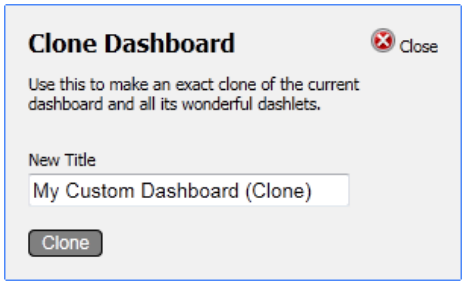
When you want to create a new dashboard by making modifications to an existing dashboard, GV GUARDIAN allows you to clone a dashboard.

1. On the **Dashboard** page, under **My Dashboards**, select the dashboard you are cloning.

2. Click **Clone Dashboard**.



The **Clone Dashboard** dialog box opens.



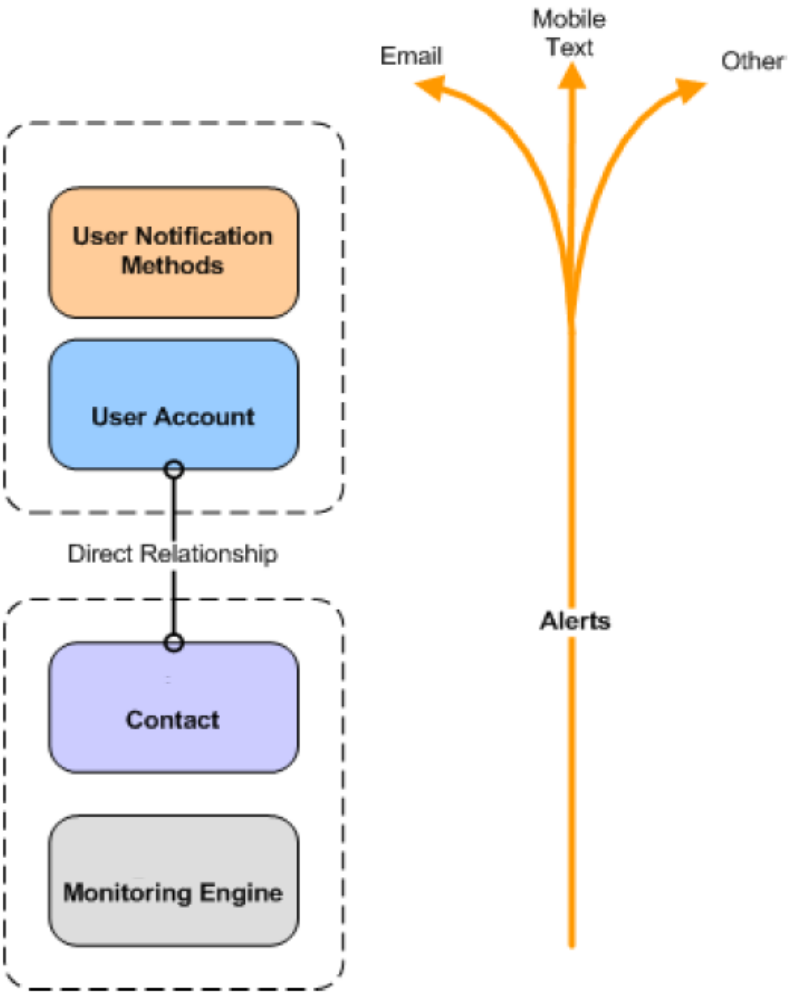
3. Enter the title of your new dashboard and click **Clone**.

Relationships between users and contacts

Users and contacts have relationships and differences as follows:

- Users correspond to user accounts that are used to login to the web interface. A user is typically "connected" to a contact for the purposes of both enabling notifications and obtaining permission to see and modify hosts and services.
- Contacts are definitions that are normally used for directing host and service alerts to specific individuals. While contacts are not required to have a relationship with a user, they typically do have have a relationship with a user. This ensures that the user can use the web interface.

In normal operation, users are directly associated to contacts with a one-to-one relationship. Admins create this relationship when they check the **Create as Monitoring Contact** option when adding new user accounts. This direct correlation allows the management of alert notifications from the monitoring engine on a per-user basis. Users can easily manage their notification preferences and methods using the web interface without having to understand the complexities of the underlying contact definitions. When a user account is directly related to a contact, the user account is automatically granted permission to see and modify all hosts and services the underlying contact receives notifications for.



By default users are allowed to manage their notification preferences, notification times, and notification messages through the web interface. This requires that each user has a direct relationship with a corresponding contact. The relationship between a user and a contact is established with the following configuration:

- There is a contact with the same short name (e.g. jdoe) as the user's username (e.g. jdoe).
- The contact that corresponds to the user account must have the following properties:
  - Host notification command is `xi_host_notification_handler`
  - Service notification command is `xi_service_notification_handler`
  - Host and service notification time periods are both set to `<username>_notification_times` (e.g. `jdoe_notification_times`)

To define a relationship between a pre-existing contact and a new user, modify the contact's configuration information using the Core Configuration Manager. This is useful when constructing relationships after migrating. If you wish to break an existing user/contact relationship, change the contact's configuration details to use values other than those described above.

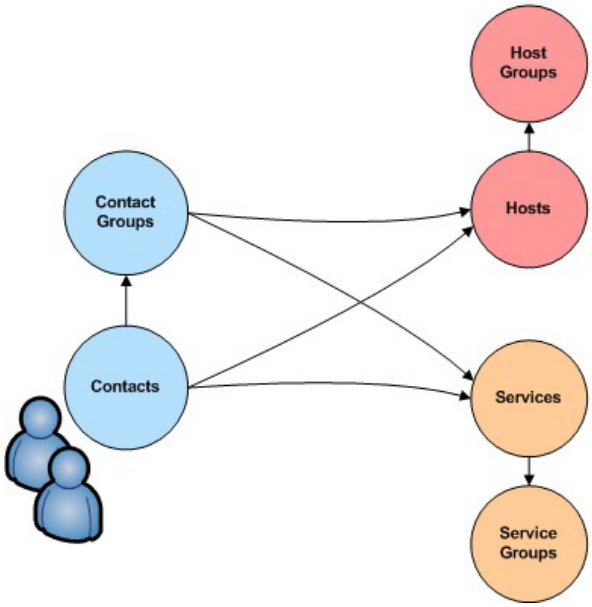
Multi-Tenancy Overview

Multi-tenancy allows administrators to configure GV GUARDIAN in such a way that the following criteria can be met:

- A single GV GUARDIAN instance can monitor hosts and services for multiple users
- Each user (client) can only see the hosts and services for which they are authorized.

Permissions and Multi-Tenancy

A key component of multi-tenancy is the ability to restrict a given user's permissions to allow them to see and control only hosts and services they are authorized for. GV GUARDIAN automatically determines what hosts and services a user is authorized to see based on their relationship to those hosts and services.



By default, GV GUARDIAN grants users permission to see and control hosts and services that are configured to:

- Send alerts to the user (contact)
- Send alerts to a contact group the user (contact) is a member of

Objects are all the elements that are involved in the monitoring and notification logic. Types of objects include:

- Services
- Service Groups
- Hosts
- Host Groups
- Contacts
- Contact Groups

- Commands
- Time Periods
- Notification Escalations
- Notification and Execution Dependencies

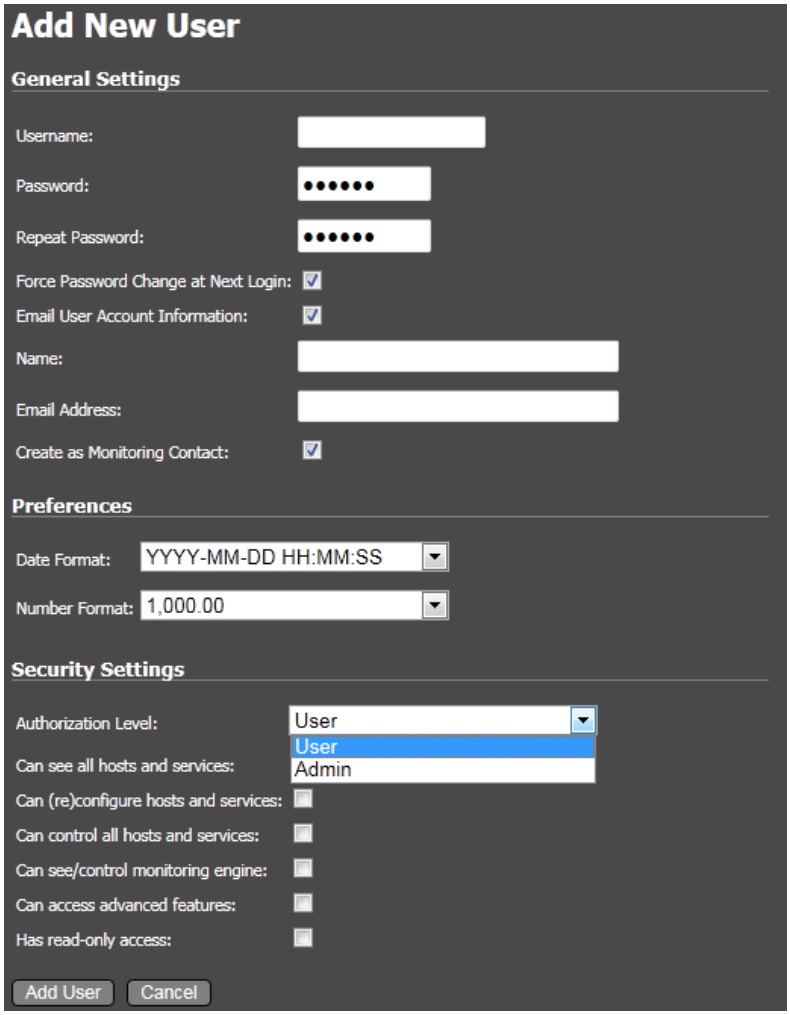
A key to understanding the relationships between objects and the corresponding permissions that contacts have is knowing how different types of objects relate to each other:

- Users (contacts) may belong to one or more contact groups
- Hosts and services may be configured to send alerts to multiple contacts or contact groups
- Hosts and services may be members of one or more host groups or service groups, respectively

Creating Users / Contacts

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to **Admin | Users | Manage Users | Add New User**.



2. Enter the username and the password for logging on to GV GUARDIAN.

3. Make selections to specify if you want the user to be forced to create a new password on activation or if you want to email the user the login, or both.
4. Select **Create as Monitoring Contact** if you want the user to receive notification when there are host and service alerts.
5. Select the appropriate Date and Number format.
6. Make security settings as explained in related topics.
7. Click **Add User**.

Each user that you create is automatically added as a monitoring contact that can be referenced in later configuration steps.

Related Topics

Managing Permissions on page 14

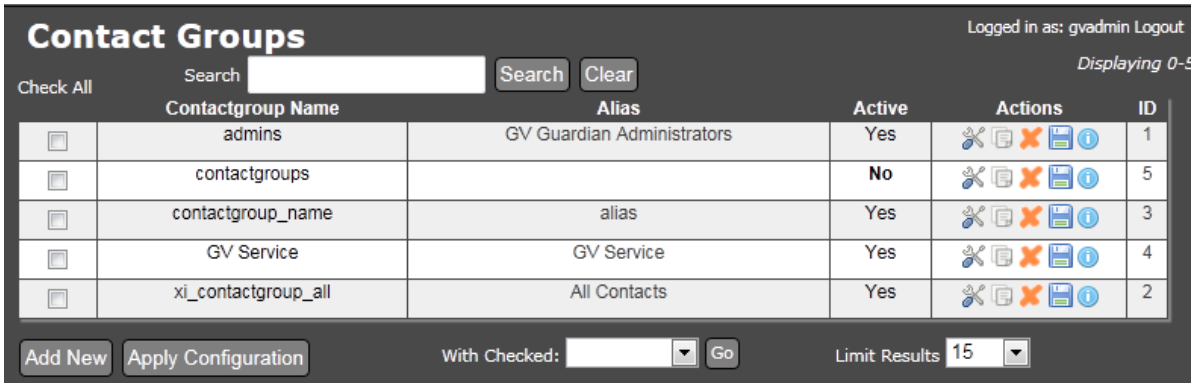
Relationships between users and contacts on page 77

Defining Contact Groups

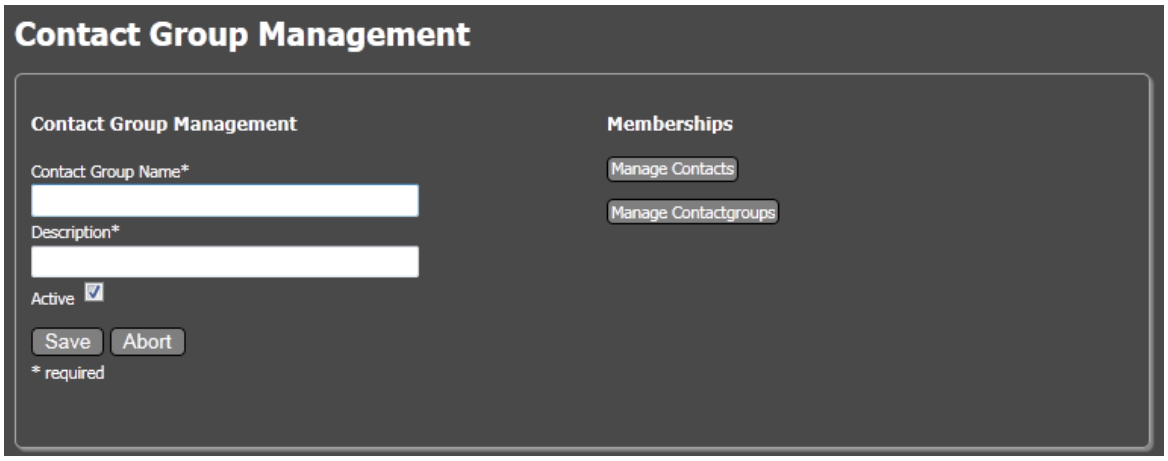
- You must be logged on to the GV GUARDIAN system with administrator privileges.

It is considered best practice to define one or more contact groups that can be used to categorize the contacts you create. Contact groups can be used to group contacts by company/client, department, team, or other logical grouping.

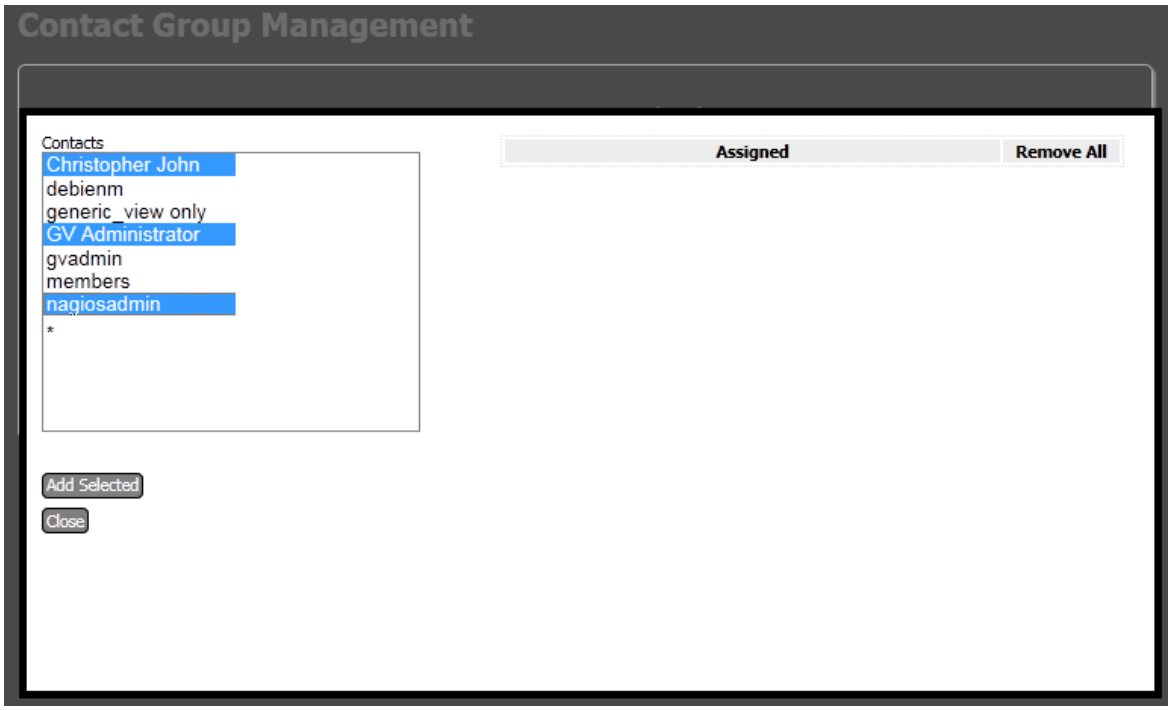
1. Navigate to **Configure | Advanced Configuration | Core Config Manager** and logon with administrator privileges.
2. Navigate to **Alerting | Contact Groups**,
3. Click **Add New**.



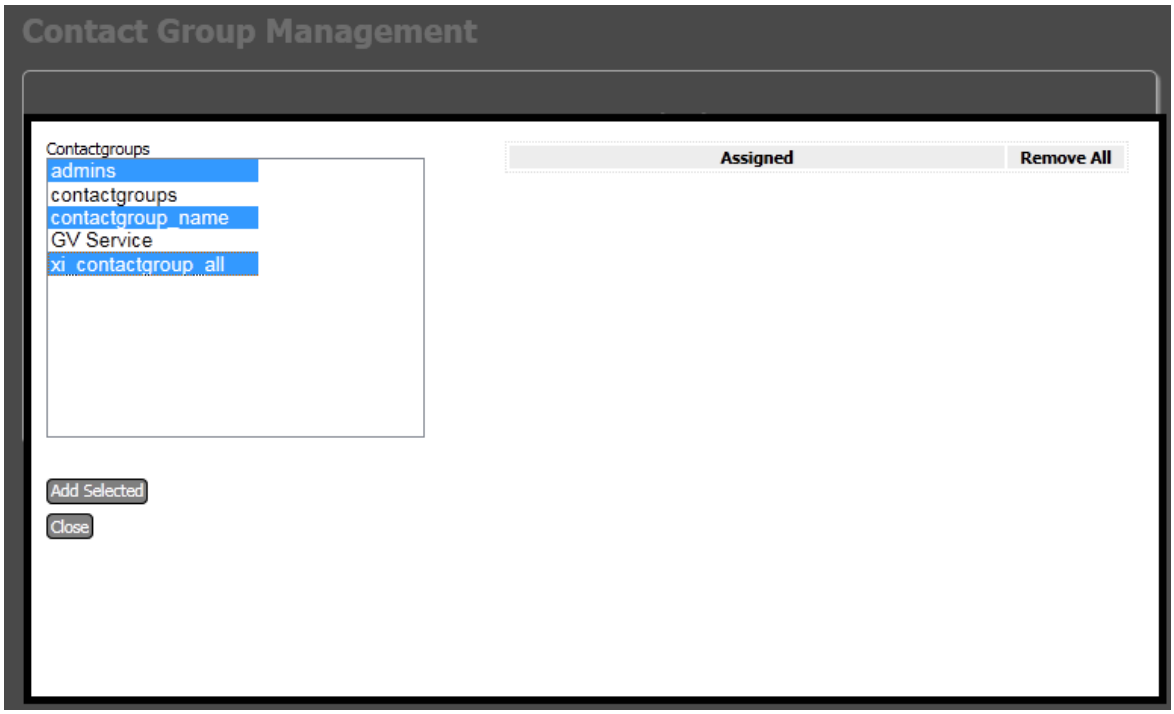
4. Define a name and description for the group.



5. Click **Manage Contacts** and add individual members as appropriate.



6. Click **Manage Contact Groups** and add group members as appropriate.



Groups members are other contact groups that are themselves a member of this group (a sub-group, but allowing for multiple group relationships on different levels).

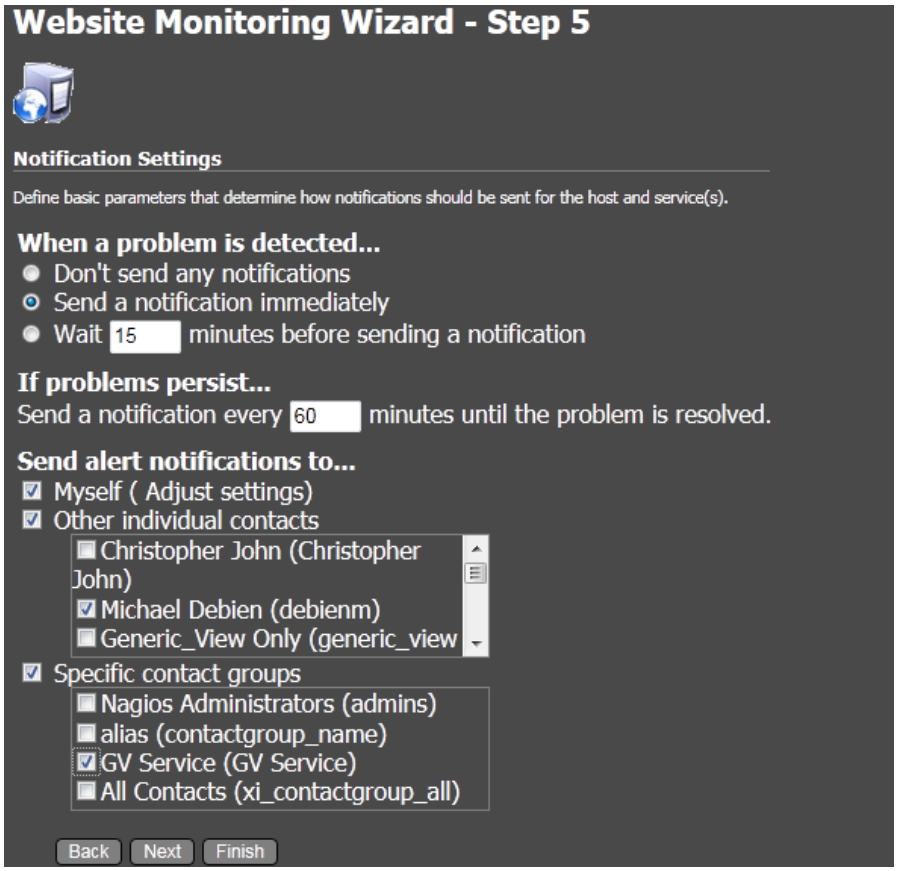
7. Save your settings and apply the configuration.

Configuring Hosts and Services

- You must be logged on to the GV GUARDIAN system with administrator privileges.

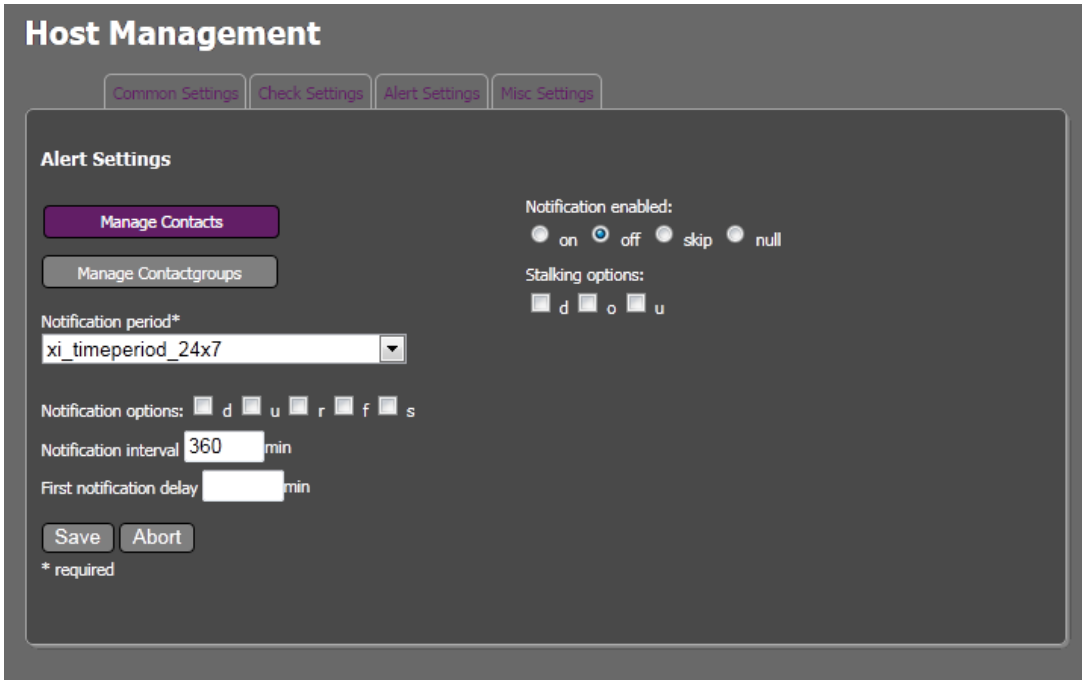
In order to grant users permission to see specific hosts and services, you must configure that user to be a notification contact for those hosts and services.

1. To configure the user with the Website Monitoring Wizard, do the following:
   a) Navigate to **Configure | Configuration Wizards | Monitoring Wizard**, select the Website Monitoring Wizard and click **Next**.
   b) On the Notification Settings page, select the appropriate contact(s) and/or contact group(s) to receive notifications for the host and services.



The contacts and contact groups you select on this screen will have the ability to view the status of these hosts and services when they login to GV GUARDIAN.

2. To re-configure the hosts or services to use new contacts and/or contact groups, do the following:
   a) Navigate to **Configure | Advanced Configuration | Core Config Manager | Hosts**.
   b) Select a host to view the **Host Management** page.
   c) Click the **Alert Settings** tab.
   d) Click **Configure**.



   e) Click **Manage Contacts**.

Defining Host Groups

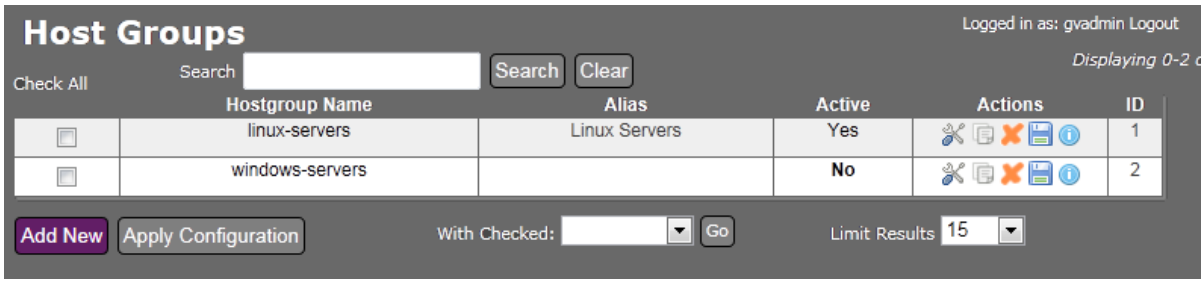
- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can group hosts in a logical manner for the following purposes:

- Allow users to get a quick and understandable view of their network infrastructure.
- Allow administrator to quickly pinpoint where problems are occurring.

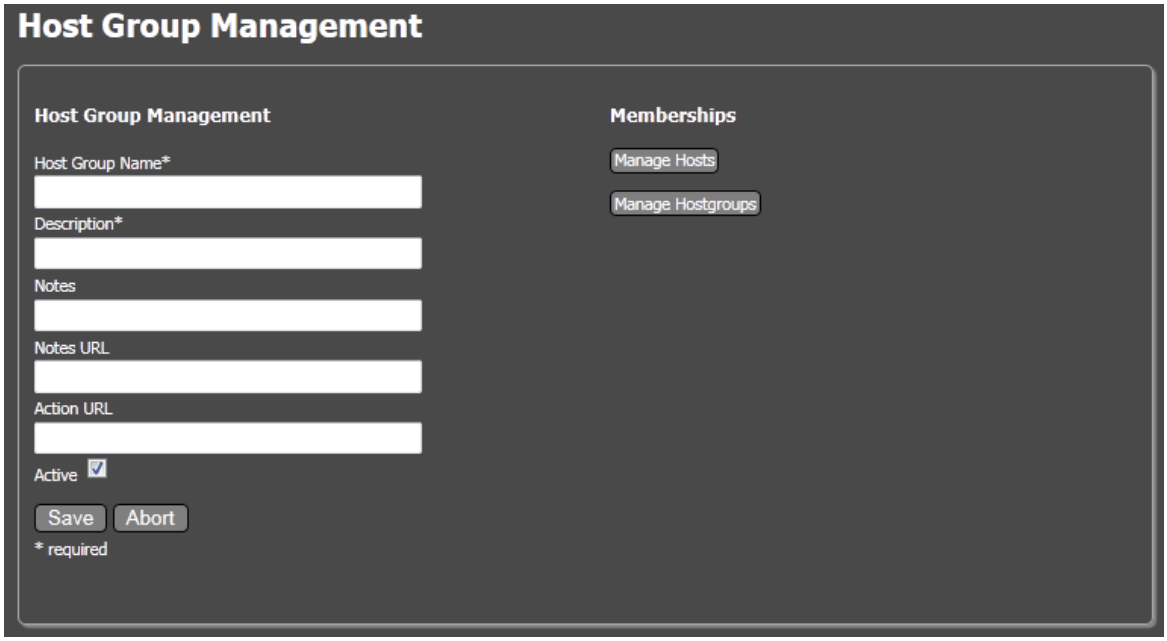
Host groups do not have an impact on the notifications or access control.

1. Navigate to **Configure | Advanced Configuration | Core Config Manager**.
2. Click **Monitoring | Host Groups**.
   The Host Groups page opens.
3. On the Host Groups page, click **Add New.**



   The Host Group Management page opens.

4. Define a name and description for the host group.



5. Click **Manage Hosts** and **Manage Hosts Groups** as appropriate to create host groups that have individual hosts and other host groups as their members.
6. Save your settings and apply the configuration.

Service Groups

- You must be logged on to the GV GUARDIAN system with administrator privileges.

Service groups work in a similar way to host groups, in that they allow you to group services together in a way that makes sense for users who need to view the status of your infrastructure. The process for creating service groups is similar to that of creating host groups.

1. Navigate to **Configure | Advanced Configuration | Core Config Manager**.
2. Click **Monitoring | Service Groups**.

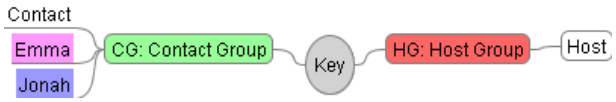
   The Service Groups page opens.
3. On the Service Groups page, click **Add New.**

   The Service Group Management page opens.
4. Define a name and description for the service group.
5. Click **Manage Services** and **Manage Service Groups** as appropriate to create service groups that have individual host services and other service groups as their members.
6. Save your settings and apply the configuration.

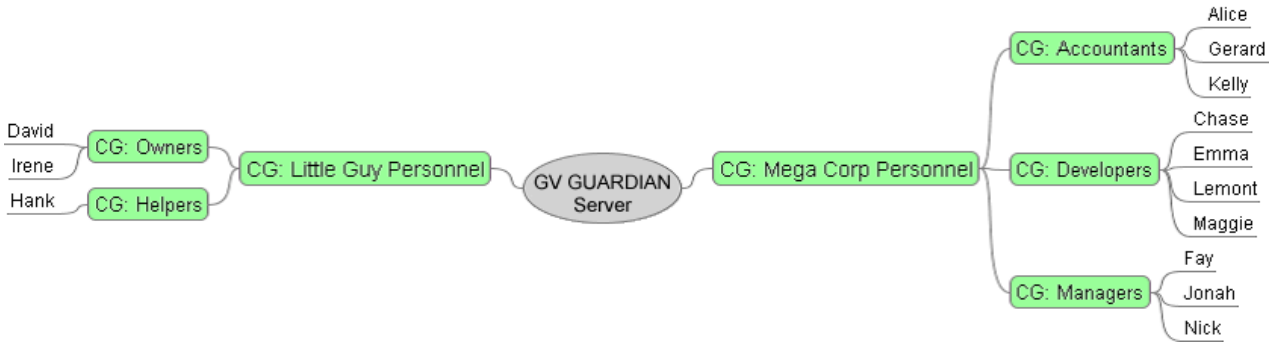
Multi-Tenancy example

GV GUARDIAN can be configured with a sample setup to demonstrate the multi-tenancy features available. These topics describe how to setup the GV GUARDIAN instance and the end-result of the configuration.

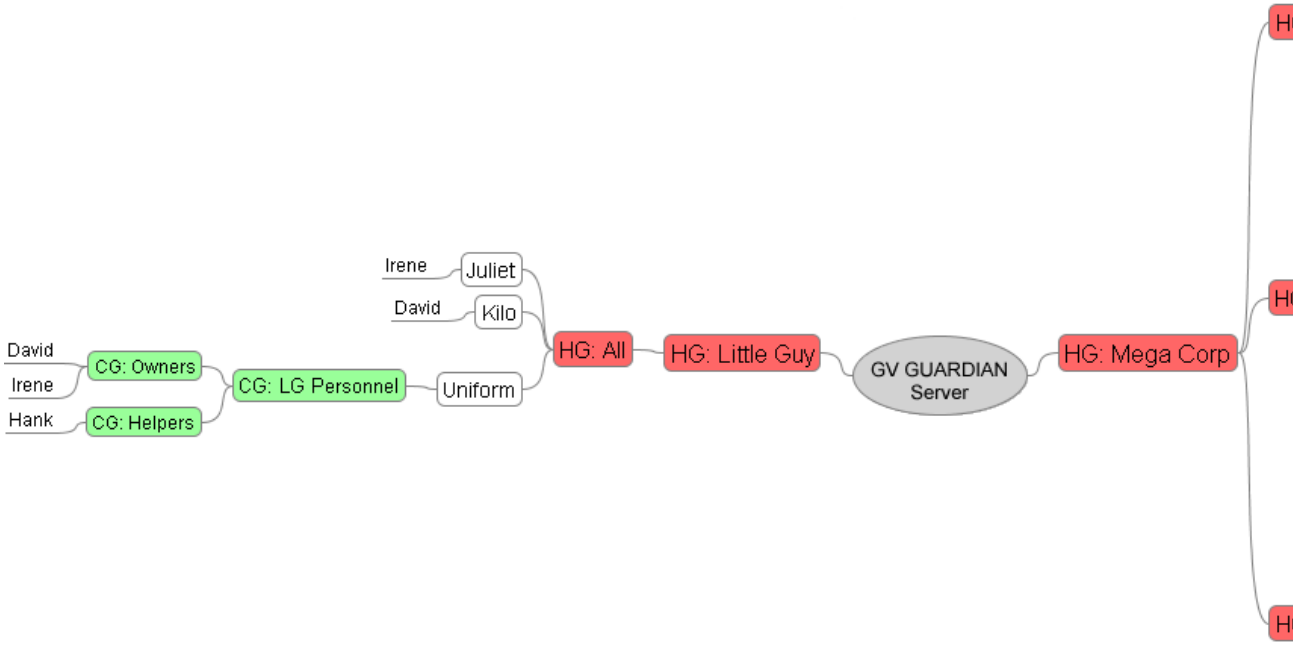
Elements of the following diagrams show the relationships between hosts, host groups, contacts, and contact groups.



Two client companies are defined - Little Guy and Mega Corp - each of which has a single top-level contact group covering their entire company. Those top-level contact groups then have other sub-groups as their members, which are used to define roles or departments within the company. The sub-groups then have individual employees as their members. The illustrations represents the configuration.

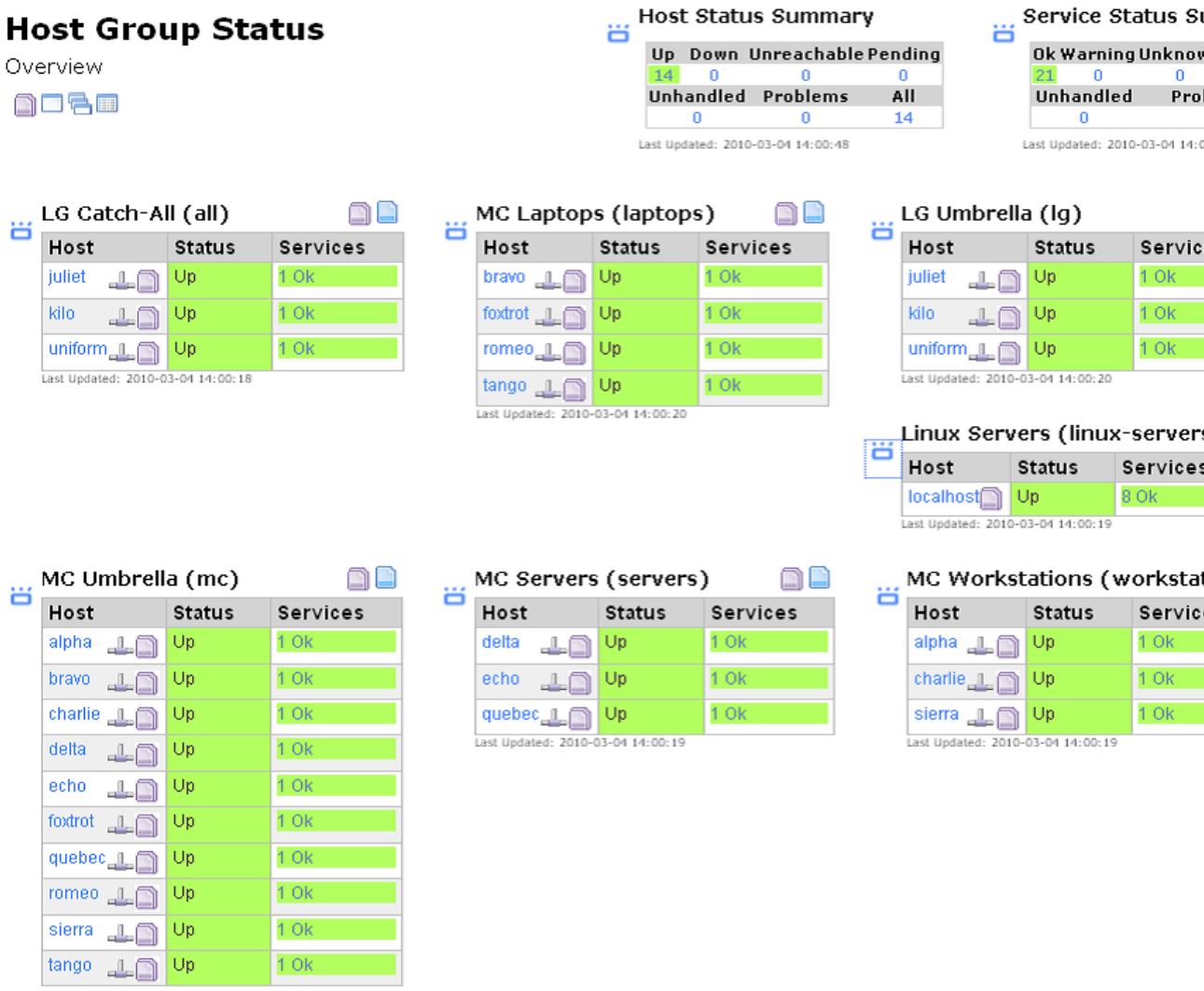


Top-level host groups are configured to contain each company's respective infrastructure elements. Sub-level host groups are defined to narrow the scope of included infrastructure elements for Mega Corp. The illustration shows the hosts that are defined as members of various hostgroups, along with the the contact(s) and/or contact group(s) that are assigned to each host for notification purposes.



Multi-Tenancy example administrator view

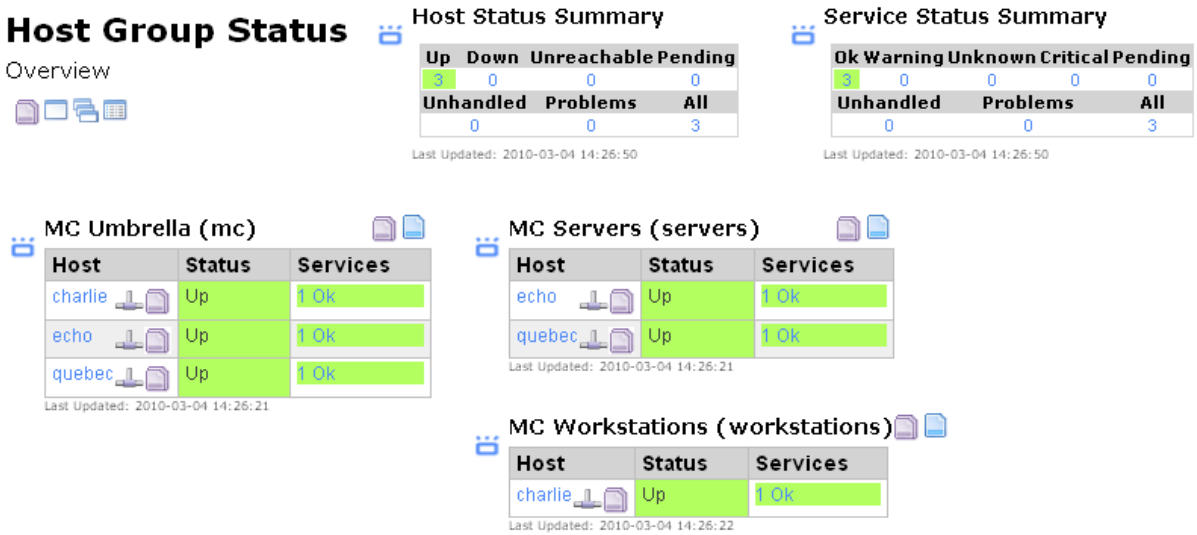
GV GUARDIAN is configured using the `gvguardianadmin` account. This account is an administrator, so it has permission to view all hosts, services, and groups that are defined. The following illustrations show the hostgroups that are visible to the administrator once configuration is complete.



Multi-Tenancy example non-admin view #1: Jonah

The user "Jonah" appears in three different places. Jonah is configured as a direct notification contact for the hosts Echo and Quebec, and indirectly as a notification contact for Charlie via his membership in the Managers contact group. These relationships are summarized in the following diagram.

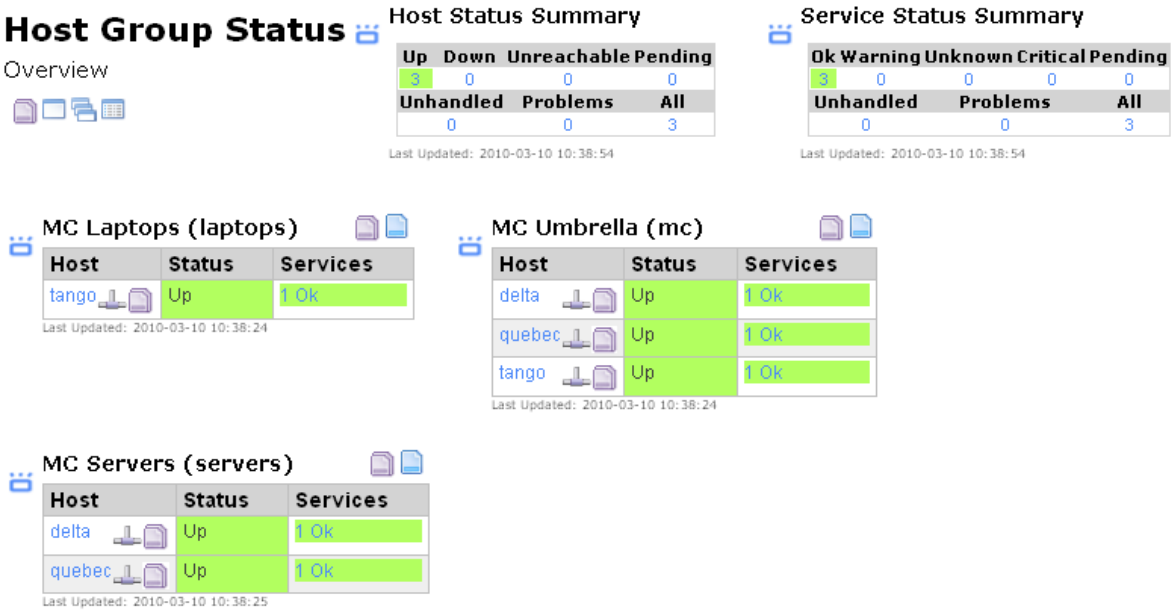
When logged into GV GUARDIAN as Jonah, the following illustration shows that Jonah's view is limited to include only the hosts Echo, Quebec, and Charlie.



Multi-Tenancy example non-admin view #2: Emma

Another user, Emma, is directly defined as the notification contact for the host Tango and indirectly for Delta and Quebec through her membership in the Developers contact group.

As illustrated, Emma can only see the Delta, Tango, and Quebec servers when she is logged in.



Multi-Tenancy example conclusion

In this example, Jonah and Emma only see the hosts to which they have permission. Neither sees the other company (Little Guy), its assets, or things within their own company to which they have not been assigned as a notification contact. This provides security from the administrator's perspective and simplicity from the end user's perspective.

You can configure GV GUARDIAN to support this same type of host grouping and user-specific permissions to enable effective multi-tenancy features.

Email notifications for alerts

You can enable email notifications as follows:

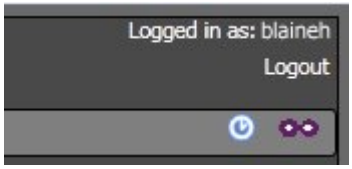
- Configure a user's notification preferences so that they are when alerts occur.
- Create a contact, either as a standalone contact or as a contact linked to a user, and then assign specific objects “Hosts/Services etc..” and control specific notification options through the contact's configuration.

Related Topics

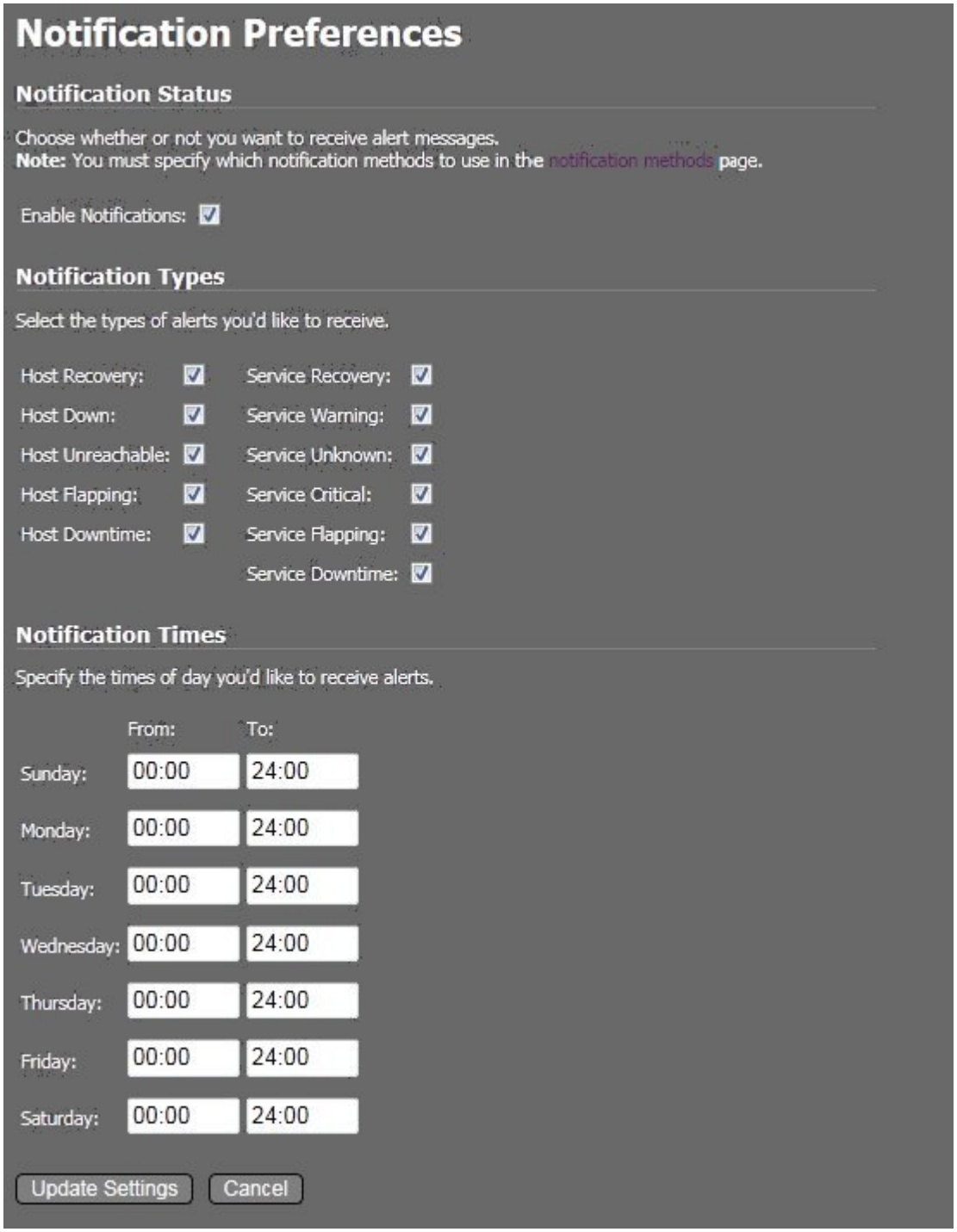
Relationships between users and contacts on page 77

Configure user notifications

1. Log in as the user for which you are configuring notifications.
2. Click the user name in the upper right hand corner of the main web page.



3. Select **Notification Preferences** from the list on the left hand side.
   The **Notification Preferences page** opens.



4. Select the notification types to receive.
5. Specify the times of the day, and the days of the week to receive notifications.
6. Open the **Notification Methods** page.

7. From the **Notification Methods** page, select the different methods to send notifications to you. Methods include email and mobile text.
8. Open the **Notification Messages** page.
9. From the **Notification Messages** page, alter the format of notifications sent to you. You can alter or remove the variables which dynamically pull their information based on the notification object and event.
10. Open the **Send Test Notifications** page.

11. Send test notifications in the ways you defined on the **Notification Methods** page.

Configure contact notification

- You must be logged on to the GV GUARDIAN system with administrator privileges.

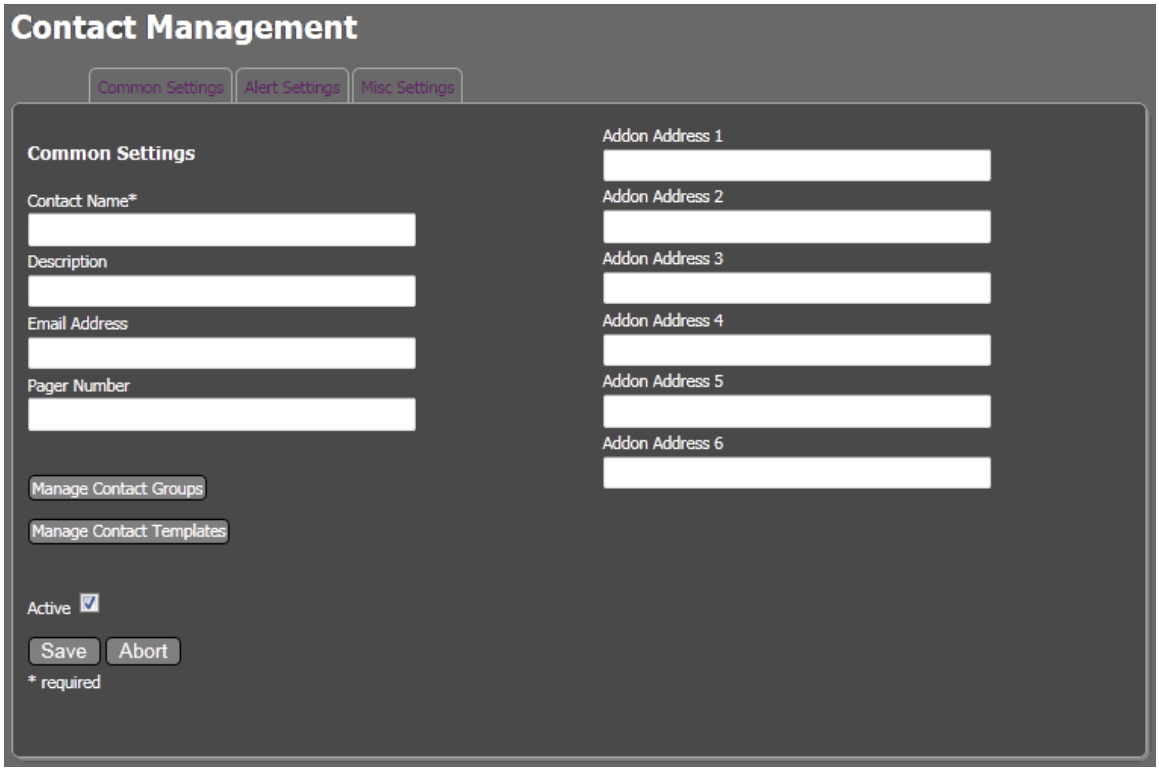
The most popular form of setting up notifications is the use of contacts. Contacts are defined in one of the following ways:

- When a user is first created
- Defined manually in the Core Configuration Manager.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Alerting | Contacts** page.

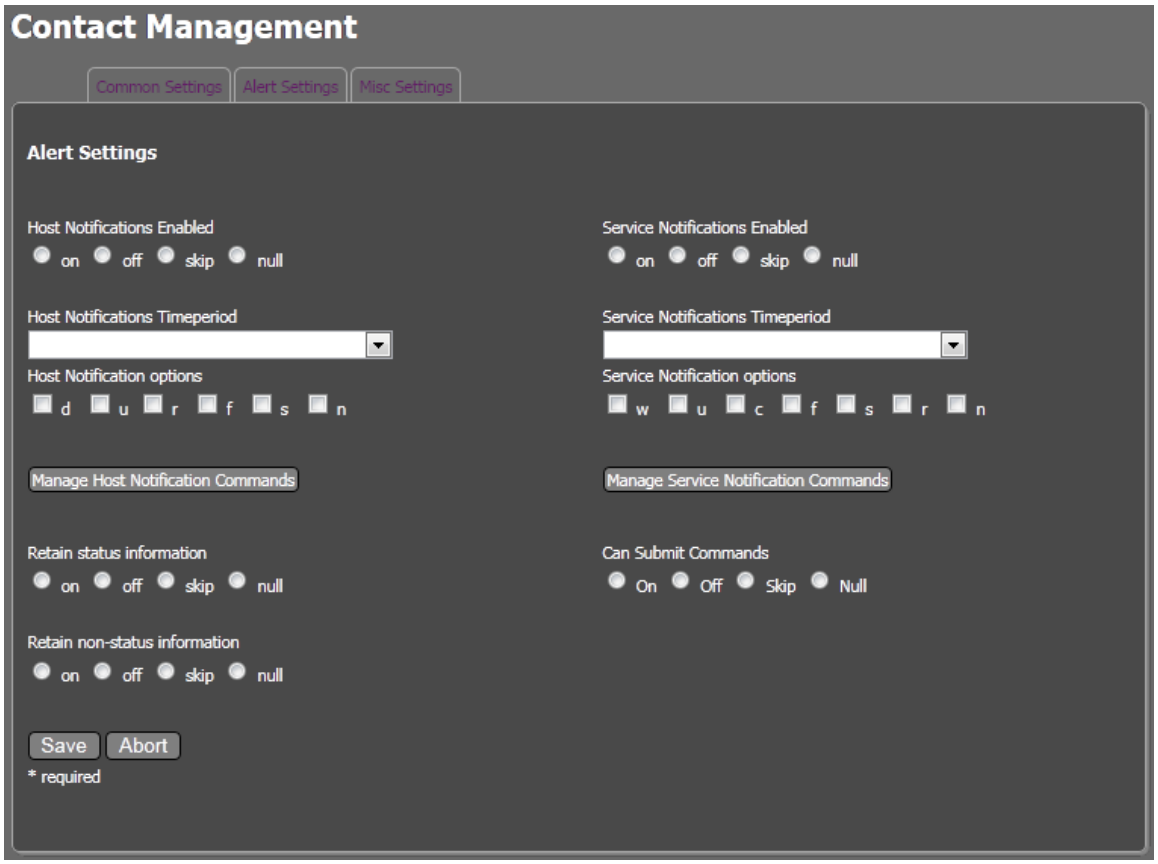
2. Do one of the following to select a contact:
   - If the contact exists, select it. Skip ahead to the next step.
   - If the contact does not exist, click **Add New** to add the contact and enter the following information:

   a) On the **Common Settings** tab:



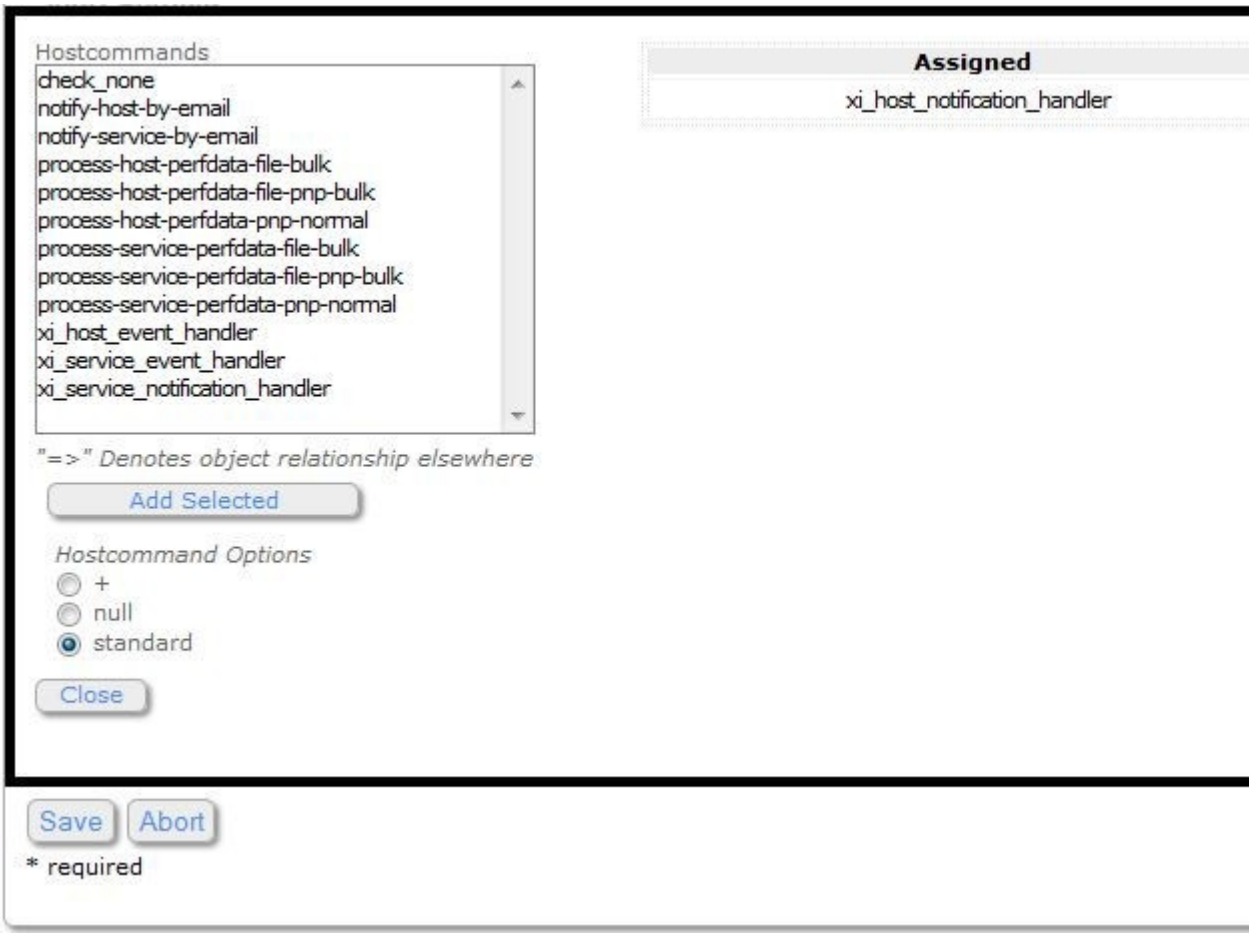
   - Contact name
   - Email address
   - Pager number
   - Add-on addresses, such as a mobile phone number for text messaging, or additional email addresses

   b) On the **Alert Settings** tab:



- Host notification time period
- Host notification options for state changes, as follows:
  - d - down
  - u - unknown
  - r - recovery
  - f - flapping
  - s - scheduled downtime
  - n - no host notifications
- Service notification time period
- Service notification options for state changes, as follows:
  - w - warning
  - u - unknown
  - c - critical
  - f - flapping
  - s - scheduled downtime
  - n - no service notifications
- Select the **On** or **Skip** radio buttons to enable host and service notifications.

3. Make sure users and contacts are set up with the proper notification handlers. To change, click **Manage Host Notification Commands** and **Manage Service Notification Commands**.



4. If you are using users, which are also contacts (you've added a contact to them), do the following:
   a) Under **Manage Host Notification Commands** select `xi_host_notification_handler`.
   b) Under **Manage Service Notification Commands** select `xi_service_notification_handler`.
5. If you are using contacts only, do the following:
   a) Under **Manage Host Notification Commands** select `notify-host-by-email`.
   b) Under **Manage Service Notification Commands** select `notify-service-by-email`.
6. Verified all settings correct.
7. Click **Save** and **Apply Configuration**.

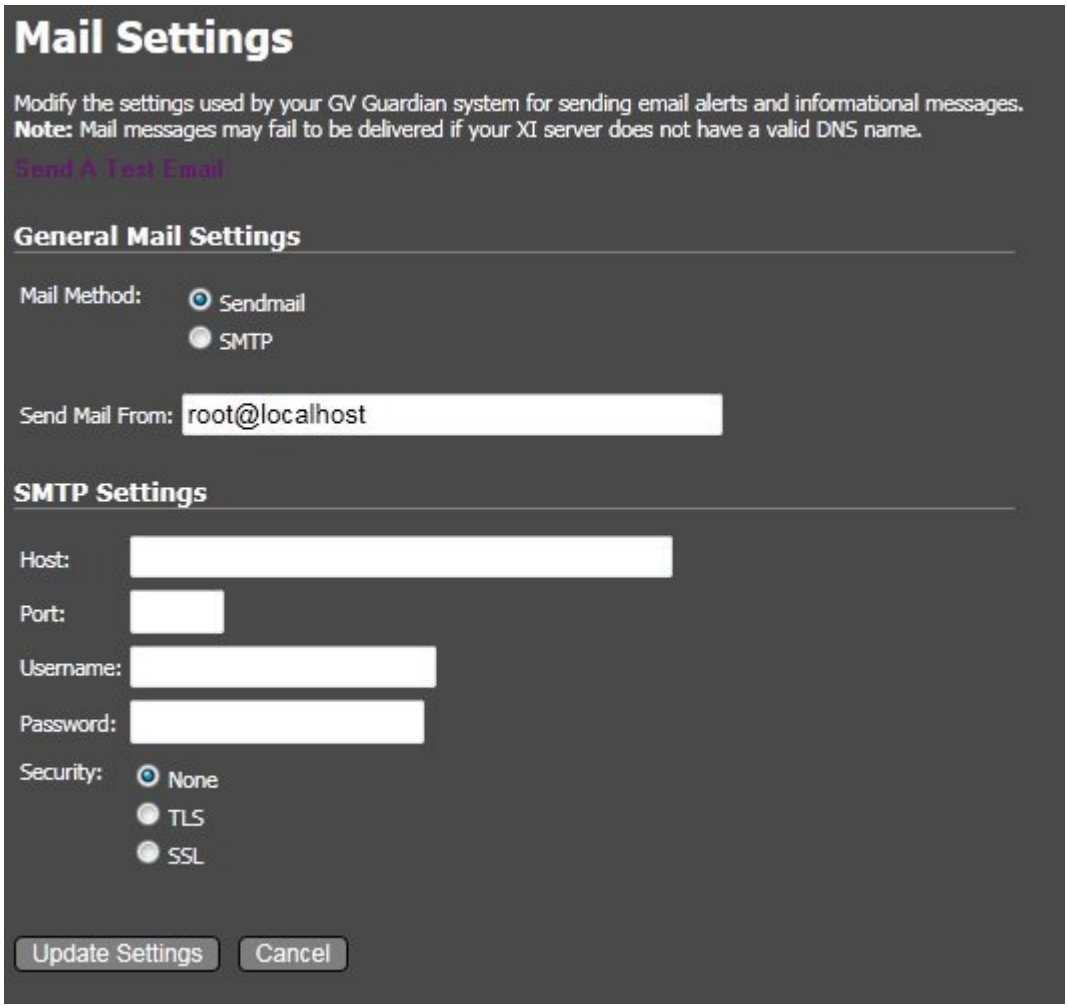
Add the contact to existing host or service configurations through their respective Core Configuration Manager pages, or select them when running a Monitoring Wizard.

Mail Routing

- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can control the way email notifications are routed through the server's Mail Transfer agent. Sendmail is used by default.

1. Navigate to **Admin | Manage Email Settings**.



2. Switch to SMTP if required by your site.
3. Verify the address and authentication information.
4. Click **Update Settings**.

Simple email troubleshooting

1. Navigate to the **Home | Notifications** page to see all notifications sent.

2. Verify that the handler is correct for your mode of email handling.

Date / Time	Host	Service	Reason	Escalated	State	Contact	Dispatche
2013-05-31 10:48:43	10.16.148.20	CPU Usage	Service Problem	No	CRITICAL	gvadmin	Nagios XI

3. Identify the contact and the dispatcher.
4. Verify that the handler is correct for the contact.

The host check command

You can refuse ICMP Ping requests and require a different schema for determining if a particular host is truly down. An example of a host that is functional, but is considered “Down” is illustrated as follows. The host “Backroom MOKEEFE” has a firewall rule that does not allow ICMP.

Host	Service	Status	Duration	Attempt	Last Check
Backroom MOKEEFE	/ Disk Usage	Ok	2d 15h 57m 2s	1/5	2011-07-08 11:2
	CPU Stats	Ok	2d 15h 56m 24s	1/5	2011-07-08 11:2
	Cron Scheduling Daemon	Ok	2d 15h 55m 46s	1/5	2011-07-08 11:2
	Load	Ok	2d 15h 55m 8s	1/5	2011-07-08 11:2
	Memory Usage	Warning	6h 11m 44s	5/5	2011-07-08 11:2
	Open Files	Ok	2d 15h 53m 52s	1/5	2011-07-08 11:2
	Ping	Critical	54s	2/5	2011-07-08 11:2
	SSH Server	Ok	2d 15h 52m 33s	1/5	2011-07-08 11:2
	Swap Usage	Ok	2d 15h 57m 0s	1/5	2011-07-08 11:2
	System Logging Daemon	Critical	2d 15h 56m 22s	5/5	2011-07-08 11:2
	Total Processes	Warning	2d 15h 55m 44s	5/5	2011-07-08 11:2
	Users	Ok	2d 15h 55m 5s	1/5	2011-07-08 11:2
	Yum Updates	Warning	2d 15h 51m 19s	5/5	2011-07-08 11:2

If you are running a server that is not allowed to respond to ping, consider alternatives. A baseline service provided is often a good choice. For instance, if you are running a web server, set the `check-host-alive` check to be a `check-host-alive-http` on the host.

Change the host check command

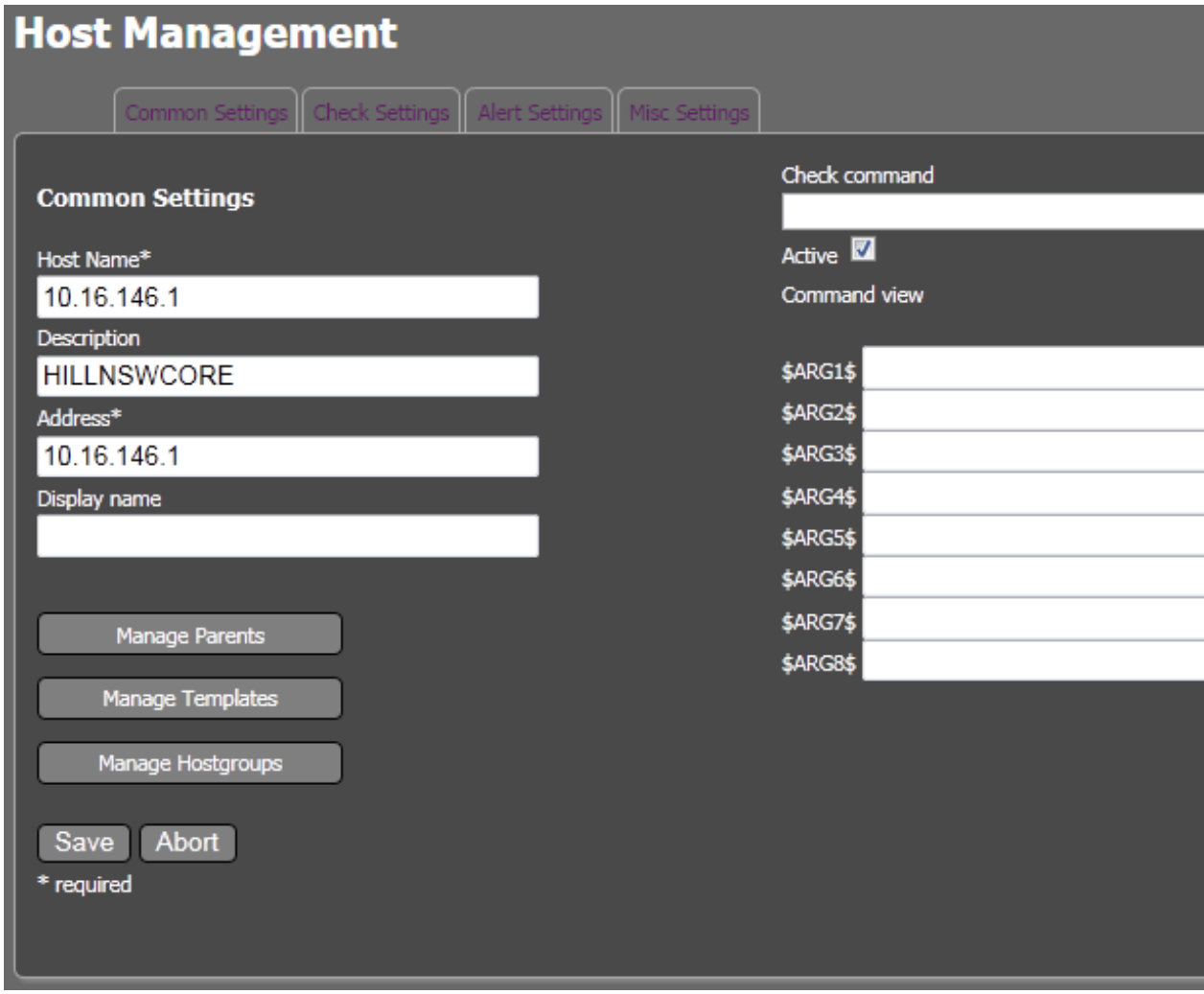
- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Monitoring | Hosts** page.
2. Enter the Core Config Manager.

3. Identify the host in the list and click the **Modify** button. .

	Host Name	Alias	Active	Sync Status	Actions	ID
	10.16.146.1	HILLNSWCORE	Yes	Synced To File		4
	10.16.146.13	hillpdu10202L	Yes	Synced To File		5

The **Host Management** page opens.



4. Evaluate the **Check command** drop-down list and proceed as follows:
   - If the desired command is already defined, it is on the list. Select the command.
   - If the desired command is not yet defined and so is not on the list, you must define a new command.
   - If the list field is blank, a template is referenced for this host and the host check is referenced in that template. Change the host check command in the template. You can see a list of templates by clicking **Manage Templates**.
5. If you changed a setting, click **Save**.
6. Repeat steps for any other hosts to change the host check command.

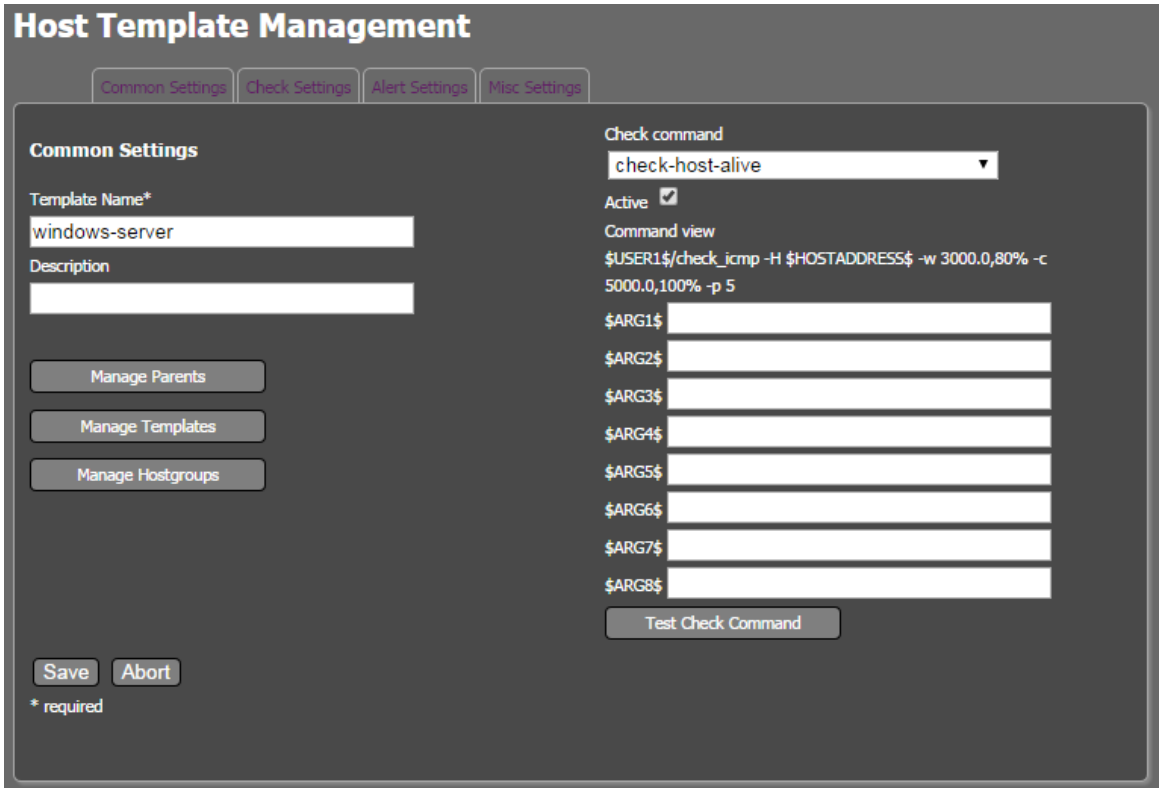
7. On the **Hosts** page, click **Apply Configuration**.

If you need to edit multiple hosts to use a check, edit the check command in the template. Editing a template affects all the hosts that are using the template.

Edit host templates to change the host check command

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Navigate to the **Configure | Advanced Configuration | Core Config Manager | Templates | Host Templates** page.
2. In the list, identify the template you are editing.
3. Click the template's **Modify** button. .



Changes to the template apply to all hosts referencing the template.

4. In the **Check command** drop-down list, select the desired command.

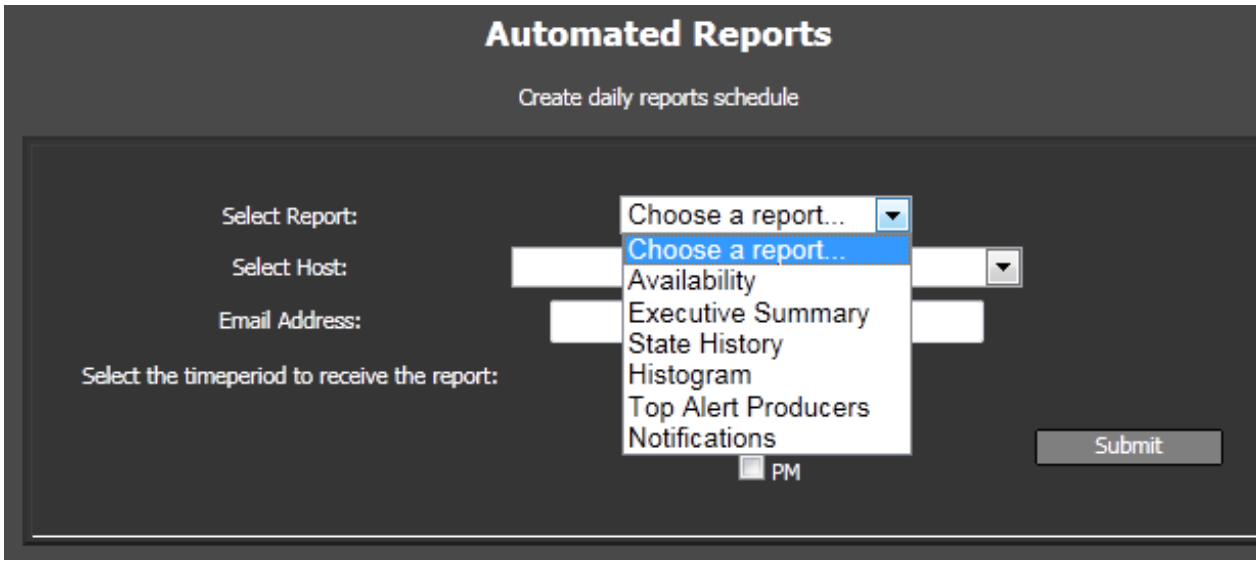
Send reports automatically

- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can configure the GV GUARDIAN application to send reports automatically via email.

1. Click **Home | Grass Valley | Automated Reports**.

2. Choose a report from the **Select Report** drop-down list:



Options	Description
Availability	A PDF document which provides a graphical display indicating Host availability and service availability for a particular device/host.
Executive Summary	A web link to a graphical display representing one or all hosts/services. Provides availability, top alert producers, average host up time, average service up time, alert histrogram and latest alerts, all in one easy to read location.
State History	A PDF document which provides a spreadsheet based indication of Events, Service state and additional SNMP information for one or all hosts
Histogram	A PDF document which provides a graphical display of alerts for one or all hosts.
Top Alert Producers	A PDF document which provides a spreadsheet based data set representing the top ten alert producing hosts in the system. Indications of number of alerts/host, type of service alert and date/time of alert.
Notifications	A PDF document which provides a spreadsheet based data set representing the alert notification details for all hosts in the system. Includes date/time, host, service, reason, state, contact and SNMP information.

3. Add the following specific data to each report:
   a) Host name/IP address
   b) Delivery email address
   c) Time period of report
   d) Hour of day that report is emailed

4. The report displays below **Current Reports Schedules**.

Report	Hostname	Email Address	Time		
Top Alert Producers		cj@oijed.vp,	Weekly - 1 am MON	Delete	Modify

5. Modify or delete as needed.

Upload logs

- The GV GUARDIAN system must be configured for connectivity to the cloud system and must be authorized by Grass Valley to have access.
- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can send logs to the long term archive in the cloud.

1. Click **Home | Grass Valley| Log Uploader**.
2. Select start and end dates/times to push to the cloud long term storage.

   The network path to the long term storage is not visible for security reasons.

Enable Traps on Windows Devices

You can enable Traps on Windows Devices to work with Grass Valley remote management.

1. Open the Windows **Services** Control Panel.
2. Verify that **SNMP Services** is displayed and proceed as follows:

SMS Task Sequen...	SMS client a...		Manual	Local Syste...
SNMP Service	Enables Sim...	Started	Automatic	Local Syste...
SNMP Trap	Receives tra...		Manual	Local Service

   - If **SNMP Services** is displayed, skip ahead to the next step.
   - If **SNMP Services** is not displayed, you must install it. Continue with the following substeps.

   a) Open the Windows **Programs and Features** Control Panel.
   b) Select **Turn Windows Features on or off**.

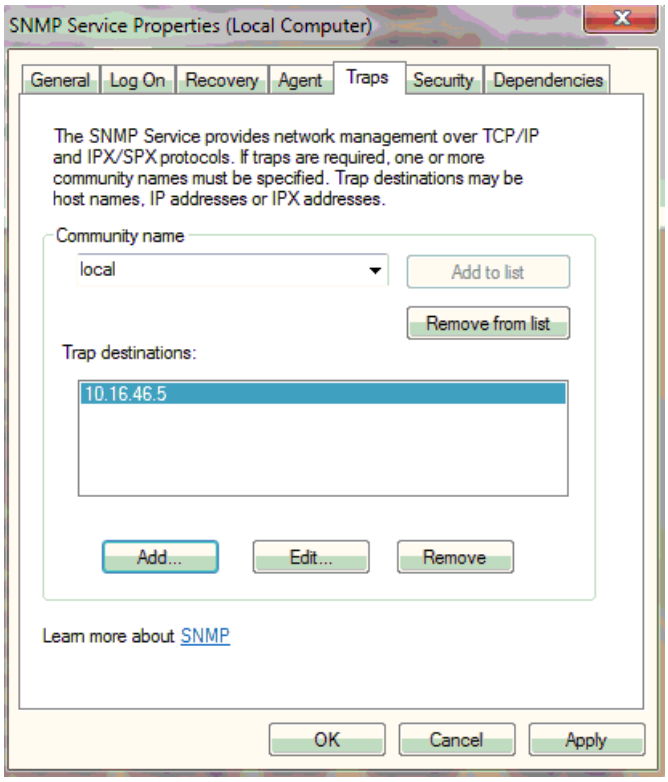
      The **Windows Features** dialog box opens.

   c) Select **Simple Network Management Protocol (SNMP)**.
   d) Click **OK**.

3. In Windows **Services** Control Panel, double-click **SNMP Services**.

   The **SNMP Service Properties** dialog box opens.

4. Select the **Traps** tab.



5. Enter the community name (user group) and then click **Add to list**.
6. In the **Trap destinations** field, click **Add** and then enter the IP address (trap destination) of the GV GUARDIAN SNMP Monitoring Server.
7. Click **Apply** and **OK** to save settings and close.

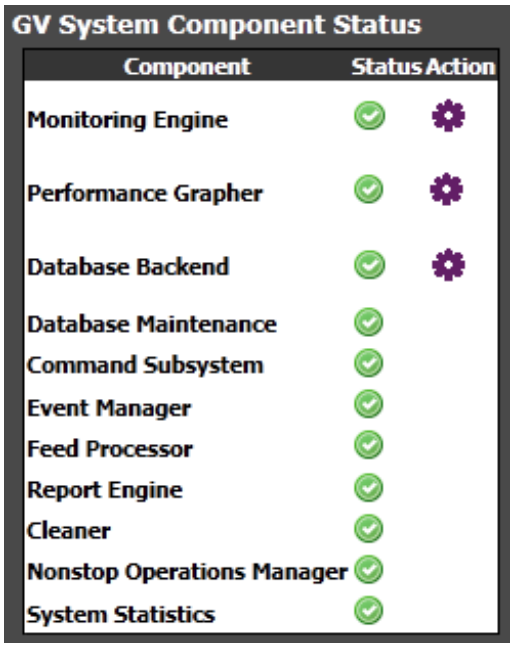
Manage GV GUARDIAN System Status

- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can start/stop components and view information regarding the current health of your GV GUARDIAN system and the load on system resources.

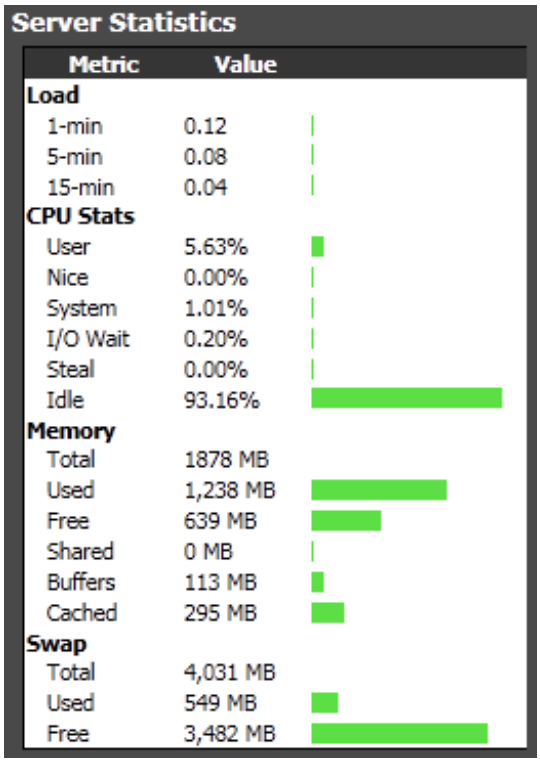
1. Navigate to **Admin | System Information | System Status**.

2. Manage GV System Component Status as follows:



a) :Hover over a **Status** indicator to view status information.
b) Click the **Action** button and select **Restart** or **Stop**.

3. Interpret Server Statistics information as follows:



Server Statistics

Metric	Value
Load	
1-min	0.12
5-min	0.08
15-min	0.04
CPU Stats	
User	5.63%
Nice	0.00%
System	1.01%
I/O Wait	0.20%
Steal	0.00%
Idle	93.16%
Memory	
Total	1878 MB
Used	1,238 MB
Free	639 MB
Shared	0 MB
Buffers	113 MB
Cached	295 MB
Swap	
Total	4,031 MB
Used	549 MB
Free	3,482 MB

- Loads are relative to CPU cores available so 2.0 load is equal to 100% usage of 2 cores while 8.0 is equal to 100% usage of 8 cores.
- The CPU States display horizontal bars as a reference on how each aspect is used.
- Analyze Memory and Swap values to ensure plenty of free memory is available, with Swap used at a minimum.

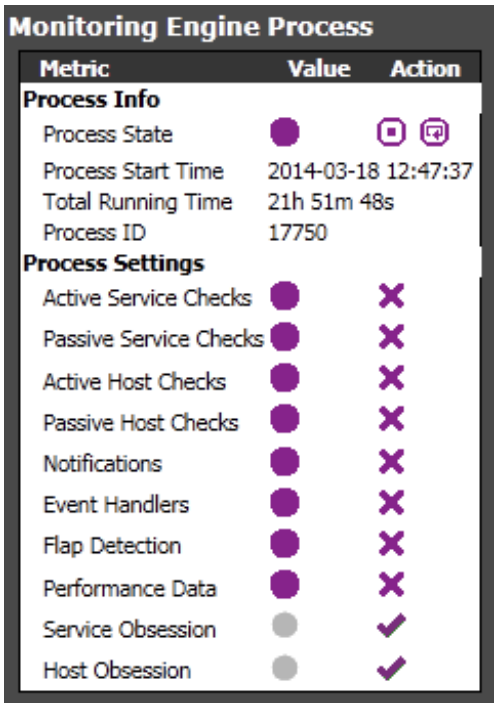
Manage GV GUARDIAN Monitoring Engine Status

- You must be logged on to the GV GUARDIAN system with administrator privileges.

You can start/stop process state and settings and view information regarding the current performance of your GV GUARDIAN Monitoring Engine.

1. Navigate to **Admin | System Information | Monitoring Engine Status**.

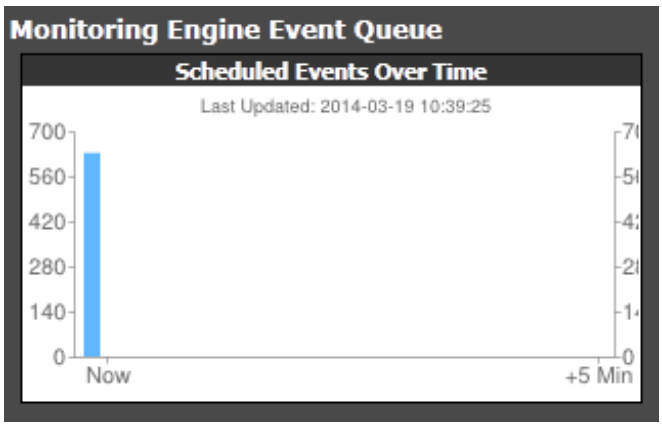
2. Manage Monitoring Engine Process as follows:



a) :Hover over a **Value** indicator to view process information.
b) Hover over an **Action** button to determine its function and click to execute one of the following functions:

- Stop
- Restart
- Disable
- Enable

3. Interpret Monitoring Engine Event Queue information as follows:



The graph illustrates the number of checks scheduled to occur over the next 5 minutes.

4. Interpret Monitoring Engine Check Statistics as follows:

Monitoring Engine Check Statistics

Metric	Value
Active Host Checks	
1-min	0
5-min	0
15-min	0
Passive Host Checks	
1-min	0
5-min	0
15-min	0
Active Service Checks	
1-min	0
5-min	0
15-min	0
Passive Service Checks	
1-min	0
5-min	0
15-min	0

Review the number of host and service checks.

5. Interpret Monitoring Engine Performance information as follows:

Monitoring Engine Performance

Metric	Value
Host Check Latency	
Min	0.00 sec
Max	0.23 sec
Avg	0.00 sec
Host Check Execution Time	
Min	0.00 sec
Max	0.02 sec
Avg	0.00 sec
Service Check Latency	
Min	0.00 sec
Max	1.04 sec
Avg	0.03 sec
Service Check Execution Time	
Min	0.00 sec
Max	4.01 sec
Avg	0.01 sec

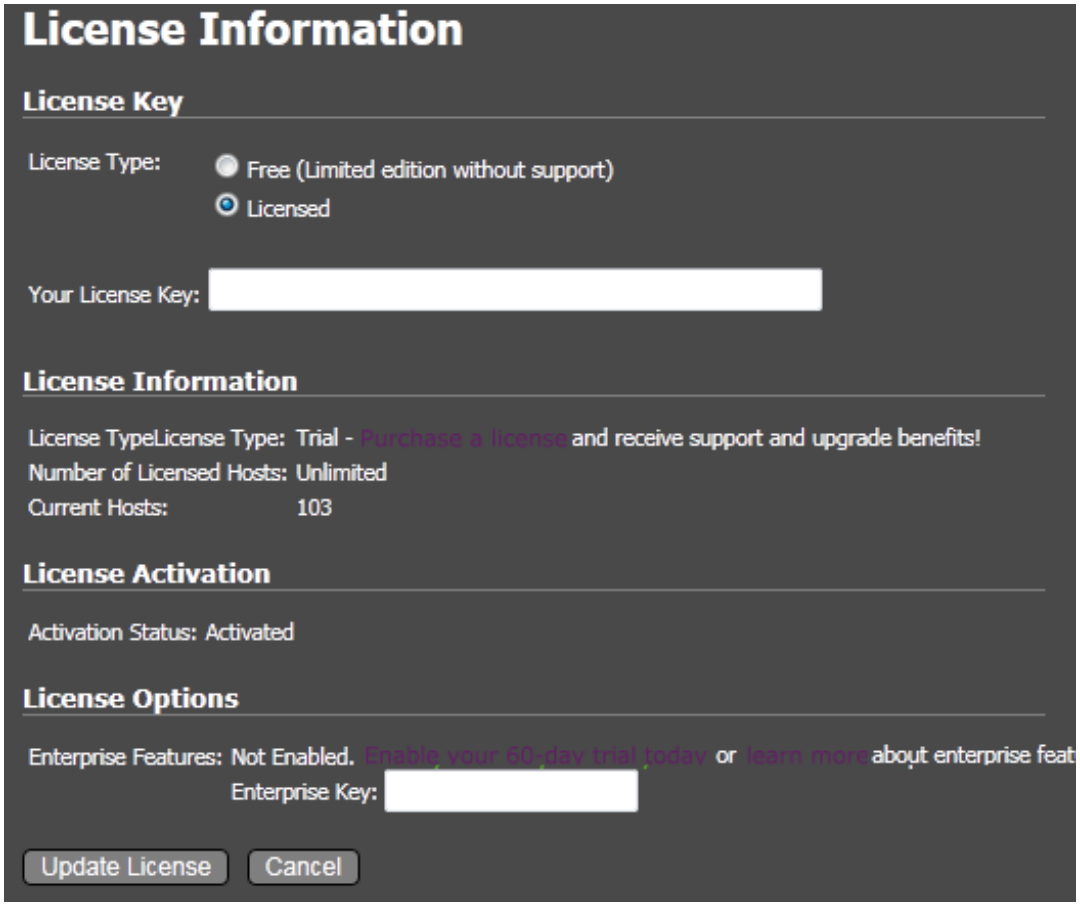
When average latency goes over 1 second (1.0), the interface slows down, checks time out, and the entire system degrades. Add CPU core and RAM to mitigate the problem.

License GV GUARDIAN

- You must be logged on to the GV GUARDIAN system with administrator privileges.

1. Find your license key as follows:
   - On the GV GUARDIAN Recovery Image USB Flash Drive that you received from Grass Valley with your GV GUARDIAN server, in the file `GV GUARDIAN License Key Information`.
   - On the printed GV GUARDIAN License Document that you received from Grass Valley after purchase.
2. Navigate to **Admin | System Config | License Information**.

   The **License Information** page opens.



3. Select **Licensed** and enter your license key.
4. Click **Update License**.

Your GV GUARDIAN system is licensed.

License considerations

When you start using GV GUARDIAN at your site, it is licensed with a free trial license by default. You can continue to operate GV GUARDIAN for test purposes under this license for 60 days of use. Only the days that you actually use GV GUARDIAN are counted in this 60 day total.

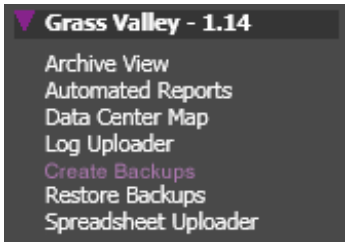
When you enter the GV GUARDIAN license key that you receive from Grass Valley, your GV GUARDIAN system is updated to a permanent license. This license key is associated with the IP address of the GV GUARDIAN server on which GV GUARDIAN is currently installed. If the IP address changes, you must re-enter and update the license on the GV GUARDIAN server. The GV GUARDIAN system allows three such licensing updates using the same license key. If the IP address changes a fourth time, the license update fails.

If you plan to change the IP address several times during your initial GV GUARDIAN testing, do so using the default trial license. Wait until the GV GUARDIAN server has its final IP address before entering the license key. This retains your ability to change the server IP address in the future. If you exceed the number of license updates allowed by the GV GUARDIAN system, contact Grass Valley Support for a new license key.

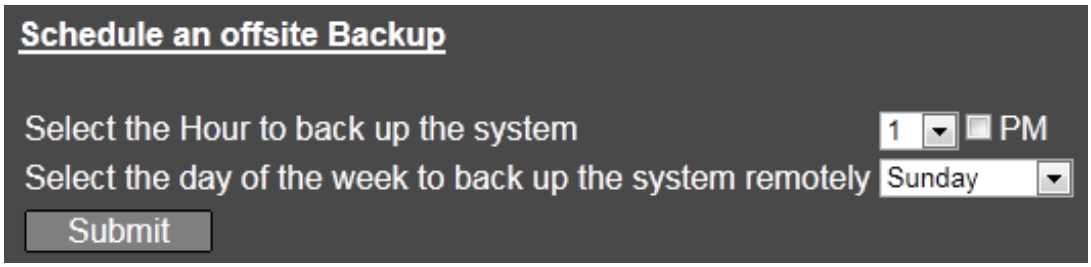
Schedule a backup

You can perform a backup of the GV GUARDIAN Application data and the MySQL database. The backup can be used for system recovery after a catastrophic failure. There are two methods of data backup; immediate and scheduled. There are two options for back up folder locations; local and offsite.

1. Click **Home | Grass Valley| Create Backups**.



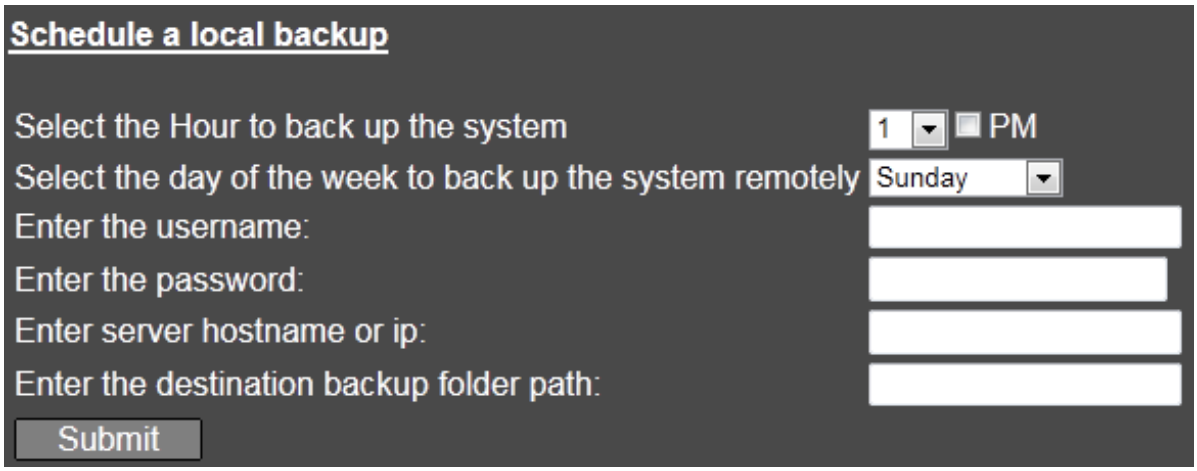
2. To schedule an offsite backup, do the following:



   a) Enter the time of day you would like to execute the backup. Consider network impact when scheduling.
   b) Enter the day of the week you would like to execute the backup
   c) Click **Submit**.

   NOTE: This occurs via port 22, Secure Key Copy.

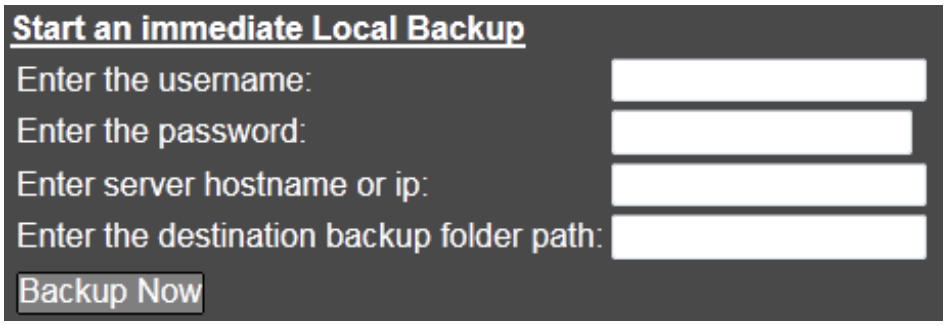
3. To schedule a local backup, do the following:



   a) Enter the time of day you would like to execute the backup. Consider network impact when scheduling.
   b) Enter the day of the week you would like to execute the backup
   c) Enter user name of file transfer destination machine
   d) Enter the password of the file transfer destination machine
   e) Enter the hostname or IP address of the file transfer destination machine
   f) Enter the folder network path for the file transfer destination machine.
   g) Click **Submit**.

4. To start an immediate offsite backup, do the following:
   a) Click **Backup Now** to start an immediate backup to the GV Long Term storage archive.
   NOTE: This occurs via port 22, Secure Key Copy.

5. Start an immediate local backup, do the following:



   a) Enter user name of file transfer destination machine
   b) Enter the Password of the file transfer destination machine
   c) Enter the hostname or IP address of the file transfer destination machine
   d) Enter the folder network path for the file transfer destination machine.
   e) Click **Backup Now**.

Change VPN credentials on GV GUARDIAN server

1. Initiate an SSH connection to the GV GUARDIAN server and log on with administrator credentials.
2. Type the following and press **Enter**.

   ```
   cd /etc/openvpn
   ```

3. Type the following and press **Enter**.

   ```
   vim login.cfg
   ```

   The username and password are displayed. The username is on the first line, the password on the second line.

4. Change the username and password as desired.
   a) Enter `dd` twice.
   b) `I` for insert.
   c) Type the username.
   d) Press **Enter**.
   e) Type the password.
   f) Press **Escape**.
   g) Hold **Shift** and type `zz`.
5. Type the following and press **Enter**.

   ```
   service openvpn restart
   ```
6. Close the SSH connection to the GV GUARDIAN server.

Next, change or create credentials accordingly on the GV GUARDIAN cloud instance. If the user does not already exist, create it and set the password.

Create VPN user on GV GUARDIAN cloud instance

1. Initiate an SSH connection to the GV GUARDIAN cloud instance and log on with administrator credentials.
2. Create the user with the `useradd -m` command.

   For example, if the new user is `blaineh`, type the following and press **Enter**.

   ```
   useradd -m blaineh
   ```
3. Set the password for the new user with the `passwd` command.

   For example, if the password is `wrkngcrw`, type the following and press **Enter**.

   ```
   passwd wrkngcrw
   ```
4. Add a new entry in `/etc/openvpn/ccd` using the following commands:
   a) `su` to gain root access.
   b) `vi /etc/openvpn/ccd/yourusername`
   c) `I` for insert.
   d) `Ifconfig-push IPAddress Subnetmask`
   e) For example, `ifconfig-push 172.30.0.10 255.255.0.0`
   f) Press **Escape**.
   g) Hold **Shift** and type `zz`.
5. Remove the previous username using the following commands:
   a) `su` to gain root access.
   b) `rm username`
6. Type the following and press **Enter**.

   ```
   service openvpn reload
   ```
7. Close the SSH connection.

Change VPN credentials on GV GUARDIAN cloud instance

Before doing this task, the user for which you are changing the password must already exist.

1. Change the password for an existing user with the `passwd` command, entering the new password twice.

   For example, if the user is `blaineh` and the new password is `wrkngcrw`, type the following lines, pressing **Enter** at the end of each line.

   ```
   passwd blaineh
   wrkngcrw
   wrkngcrw
   ```

2. Close the SSH connection.

Upgrading GV GUARDIAN

- You must be qualified by Grass Valley Support to do this task. Do not attempt without adequate training.

These steps are for upgrading an existing installation.

1. Transfer the zip file to the GV GUARDIAN VM using WinSCP.
2. Put the zip file into the *`tmp`* folder.

   An example of the zip file name is *`nagios_auto_install-1.x`*.

3. Log in using the Putty application and do the following:
   a) Log in as root. Type the following and press **Enter**.

      `SU`

   b) Enter the following password and press **Enter**.

      `adminGV!`

4. Navigate to the *`tmp`* folder. Type the following and press **Enter**.

   `cd /tmp`

5. Verify you are in the *`tmp`* folder and that the files for the update are available. Type the following and press **Enter**.

   `ls`

6. Unzip the file. Type the following using the zip file name and press **Enter**. The following uses an example of a zip file name.

   `tar xzvf nagios_auto_install-1.10.3.tar.gz`

7. Navigate to the version. Type the following using the zip file name and press **Enter**. The following uses an example of a zip file name.

   `cd nagios_auto_install-1.10.3`

8. Start the installation process. Type the following and press **Enter**. The following uses variable indicators for the values you type.

   ```
   ./install.sh -I {ip address} -P {port number} -r {proxy user} -p {proxy
   password} -s {use https (0/1)} -w {wmi user} -p {wmi pass} -u
   ```

   - If ip address is not set, proxy information is not added.
   - If port number is not set, the default value is 80.
   - Proxy user and proxy password are required in combination or not at all.
   - If https is not set, the default value is 0.
   - If wmi_user and wmi_password are not set, the default values are wmiagent and wmiagent.
   - -u is used for update.

A "...complete..." message confirms the process is successful. This can take up to 15 minutes. Do not attempt to interrupt the process.

Glossary

Advanced Logging
The tool that creates and customizes logging of assets.

Advanced Search
The functionality provided by the Advanced Search tool, which includes the ability to search by multiple criteria.

Application Window
An application's main surrounding window, in which the application's panels are docked.

Asset
A physical or logical entity defined and managed by the Grass Valley system.

Asset List
The panel that displays the list for the item currently selected in the Navigator panel or the search results.

Asset type icon
An icon that indicates the type of asset.

Assignment List
The tool that creates placeholders for clips and coordinates with rundown stories on the Newsroom Computer System and with GV STRATUS Rundown.

Authorization Manager
Settings in the GV STRATUS Control Panel that assign licenses and permissions to users and groups.

Bin
On a K2 system, a folder that contains media.

Button Panel
The panel that creates and assigns logging buttons.

Channel Panel
The tool that includes channels and channel gangs for controlling one or more K2 channels.

Channel Panel configuration
The settings that you configure to create a Channel Panel. When the Channel Panels node is selected under the Tools item in the Navigator, the settings appear as an item in the Asset List.

Clip
A single media asset with video and/or audio, timecode, and associated metadata.

Composite panel
A panel that contains one or more panels.

Control Point PC
A network connected PC that is an optional component of the Grass Valley system. It serves as the central configuration location for the Grass Valley system. It runs applications such as the GV STRATUS Control Panel application, the SiteConfig application, the K2Config application, and an SNMP manager application.

Control Tray
The toolbar that opens on the bottom of a GV STRATUS component that displays video. The Control Tray contains buttons for transport control, markup, and other functions.

Copy
A complete copy of an asset.

Crash Record
Start a recording without specifying a clip name.

Dashboard
The tool that displays a dynamic system overview of the activity on the GV STRATUS system, such as channel usage and storage capacity.

Details view
The list view format that displays each asset as a multi-column row.

Director
The tool that controls the interface with GV Director.

Drop target
The graphic that appears when hovering an undocked panel over another panel or over the application window. The graphic indicates the area in which the panel is docked if the panel is dropped on the graphic.

Effects
Groups effects for use in the GV Director stage or program.

Event (Playlist)
A clip, trigger, or other entity that is one of the items in a playlist.

Event (Scheduler)
An item that marks the time that a recording or other action is scheduled to occur.

Feed Ingest
Operations performed by the Scheduler tool where K2 system channels are configured to record clips.

Focus
The state of a user interface component in which the component is currently receiving the input from the keyboard or mouse.

Folder
A physical or logical container. It can be a physical directory on a computer's file system or a database record managed by a Grass Valley system database.

FT server
The fault tolerant server that provides a platform for Grass Valley system devices, such as the GV STRATUS Core server.

Gang
Two or more channels that can be controlled as a single unit. A channel in a gang is referred to as a ganged channel. A channel that is not in a gang is referred to as a single channel.

Grass Valley system
The applications with their database(s) and supporting infrastructure that manage assets for one or more Grass Valley products.

GV Director
Grass Valley's nonlinear live production center .

GV Director Server
The server that supports GV Director.

House Number
The panel that populates the house number list and links assets to house numbers from the traffic system.

Ingest Database
The database for the Scheduler tool.

Inspector
The panel that displays details of the asset currently loaded.

K2Config
Grass Valley's application for configuring the K2 Storage Area Network (SAN).

K2 Media Server
The K2 Media Server product, which is a K2 SAN device. It can have the role of file system manager and other roles.

K2 Nearline SAN
A large pool of offline K2 storage to which files can be saved. Suitable for media file transfer. Does not support record or play.

K2 SAN
The K2 Storage Area Network, including K2 Media Server, K2 RAID, and K2 SAN-attached systems. This term applies to an online or production SAN except if it is specified as a nearline SAN.

K2 Solo system
The K2 Solo Media Server product.

K2 Summit SAN-attached system
A K2 Summit system with media storage on a K2 SAN. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Client products.

K2 Summit standalone system

A K2 Summit system with internal or direct-connect media storage. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Server products.

K2 Summit system

A K2 Summit system of any storage type, including standalone internal/direct-connect or SAN-attached shared media storage. Applies to K2 Summit (3G) Production Client and K2 Summit Transmission Server/Client products.

K2 system

K2 product family servers, clients, and SANs, either individually or combined as a system. This includes K2 Media Clients, K2 Summit (3G) Production Clients, K2 Summit Transmission Servers/Clients and K2 Solo Media Servers with standalone, direct-connect, or SAN storage, as appropriate for the product.

Keyword

A section of a clip that has duration, as defined by an in point and an out point, with its associated metadata.

Launch

Opening a tool or other component to expose the controls and functionality that you can use to accomplish a task.

Lease

A license that is checked out to a particular user. For the period of time that the license is checked out to that user, the user has a lease on that license.

License Management Database

The database for the assignment of GV STRATUS licenses and roles to groups and users

Marker Panel

The panel that displays keywords and markers of assets.

Marker

A specific point in a clip, as defined by timecode, with its associated metadata.

MDI

MDI is the acronym for Managed Device Interface. An MDI is a software component that provides an interface for the GV STRATUS database to access a device. Typically these are devices on which media resides, such as K2 systems, NAS devices, and archive devices. Each type of device has its own MDI. For most MDIs, the MDI software component is hosted on the GV STRATUS Core server, rather than being hosted on the same machine that it accesses.

Media ID

Metadata assigned to a disk or directory that contains a group of clips that can be imported via RMI.

MEWS Server

A customer-supplied server dedicated to MEWS functionality. It hosts MewsService, which is a Grass Valley service.

Navigator
The panel that contains the tree-view.

Panel
A UI component that can be undocked and docked in an application window.

Permissions
Access to files or directories that can be assigned to user groups.

Playback
Playing an asset, such as a clip or playlist.

Playlist
An asset type consisting of a series of events. A playlist contains only events, transitions, and other features supported on the K2 system channel.

Playlist Editor
The tool that creates and modifies playlists. This tool uses a K2 channel.

Program
Controls and monitors the GV Director program output.

Proxy server
The GV STRATUS server on an online or production K2 SAN that provides access to the low-resolution proxy media stored on the SAN. The server has the role of Proxy K2 SAN Server and SNFS file system client.

Proxy Storage
A K2 Nearline SAN that stores low-resolution proxy media for a GV STRATUS system. A GV STRATUS Core Services server takes the role of file system server for the Proxy Storage.

Proxy Storage file system server
The GV STRATUS server on a dedicated Proxy Storage system that provides access to the low-resolution proxy media stored on the system. The server has the roles of Proxy Storage Server and SNFS file system server for the Proxy Storage system.

Render Engine
A GV STRATUS server that functions as a conform server and that can function as an EDIUS XRE Server. The server hosts the GV Render Engine Service and XRE Controller software. As a conform server the GV Render Engine Service renders a complex asset, such as a GV STRATUS sequence, into a simple clip. As an EDIUS XRE Server the GV Render Engine Service and XRE Controller software render a project created in EDIUS into a simple clip. A GV STRATUS server that functions as a proxy encoder and as a conform server. As a proxy encoder, the server creates low-resolution proxy assets. If a high-resolution asset does not yet have associated proxy, the server creates it. The software that provides the proxy encoder functionality can run on a dedicated Render Engine server or on a GV STRATUS server that has other roles as well, such as a GV STRATUS Express server. As a conform server, the server hosts the Render Engine Service. The service renders a complex asset, such as a GV STRATUS sequence or a project created in EDIUS, into a simple clip.

RMI

RMI is the acronym for Removable Media Interface. It is the tool that populates and ingests files from multiple removable media devices such as P2 and XDCAM. The RMI tool requires a GV STRATUS client with access to high-resolution assets.

Role

Functionality that can be assigned. In the SiteConfig application, it is software functionality assigned to a device. In the GV STRATUS application, it is licensed functionality assigned to a user or group.

Rules Engine Database

The database for the Rules Engine. Stores the rules and the current state of the active rules. This is a SQL database. The database name is RulesEngine.

Salvo

A pre-defined and re-usable set of clips to load into a specific channel.

Scheduler

The tool that schedules events to be recorded.

Scrub bar

The control that allows you to navigate through a clip using your mouse. The scrub bar slider provides click and drag mouse operations.

Stage

Composites and previews production elements for use in the GV Director program.

SDB

SDB is the acronym for Simple Database, which is the database server component for GV STRATUS Rundown. It provides status on clips and on playlists associated with NCS rundowns.

Section

A panel's subdivision, such as the Explore section of the Navigator panel.

Segmentation Tool

The tool that creates segments from assets.

Segment Template

A collection of metadata properties, as configured in the GV STRATUS Inspector panel, that can be associated with a segment as part of the Digital Media Platform workflow.

Send Message

The tool that sends and receives messages and attachments between users logged on to GV STRATUS applications.

Sequence

An asset consisting of a series of events for EDL exchange with an editor or creating finished stories for playout.

Sequence Viewer

The tool that plays sequences and playlists.

Shortcut
The representation of an asset that operates as a copy of the asset but is actually a reference that points to the original asset.

Show/Hide button
The button that shows or hides an interface component. For example, the Show/Hide button that shows or hides transport controls in a Channel Panel.

Show/Hide tab
The tab that indicates the position of a hidden panel. When the tab is clicked, the panel slides open (shows).

Live Shotbox
Allows selection of camera inputs for use in the GV Director stage and program.

Media Shotbox
Readies clip, still, and animation production elements to use in the GV Director stage and program.

Simple Search
The functionality provided by the Simple Search tool, which is the ability to search by a single search term.

SiteConfig
Grass Valley's application for network configuration and software deployment.

Source Viewer
The tool that plays assets and provides controls for adding markers, keywords, and other features.

Storyboard Editor
The tool that creates and modifies sequences. This tool does not use a K2 channel.

GV STRATUS
Grass Valley's media workflow application framework. Applications include the GV STRATUS application and the GV STRATUS Control Panel.

GV STRATUS Common server
A GV STRATUS server with common roles, excluding the role of Core Server and Proxy Server. This server provides licensing and user preference functionality on typical GV STRATUS systems where there are multiple GV STRATUS servers.

GV STRATUS Control Panel
The GV STRATUS application that provides central configuration of the software components of the GV STRATUS system.

GV STRATUS Core server
A GV STRATUS server that has the role of Core Services on a system with multiple GV STRATUS servers. The server provides media management functionality, including the GV STRATUS database and associated software components.

GV STRATUS Core Services
The software components that provide the underlying functionality to GV STRATUS applications. The components run as services on one or more GV STRATUS Core Services servers.

GV STRATUS Database
The database that provides the core asset management functionality to the GV STRATUS system.

GV STRATUS Express server
A GV STRATUS server with all the roles necessary for a basic GV STRATUS system, including the role of Proxy Express Server. The server has larger drives than other GV STRATUS servers to accommodate the low-resolution proxy media that is stored on the local server. This server is designed for use on smaller GV STRATUS systems where no other GV STRATUS servers or proxy systems are present.

Subclip
A clip created by referencing a portion of media from a parent clip. The subclip does not contain any actual media. Rather, it points to the media in the parent clip.

Tag
A metadata entry that has no timecode information. In the GV STRATUS application this applies to an entire asset rather than to a particular point or section in an asset.

Take control
To take control of a K2 system channel that is currently being controlled by another. This can occur when two people are using the application on different PCs and one person opens or adds a channel that is in use by the other person.

Tally indicator
The colored bar or rectangle that indicates the current status (recording, playing, etc) of a channel gang or an individual channel.

Thumbnails view
The list view format that displays each asset as a small rectangular image.

Tiles view
The list view format that displays each asset as a small rectangular image with asset property information to the right.

Transition
The place between two events in a playlist or sequence. A cut and an effect are examples of a transition.

View Mode
The visual representation of a list of items. Modes include detail, tile, and thumbnail views.

Web Monitor
The tool that displays a web page.

WfPersistence Database
The database for the runtime data of the workflow engine. Stores the current state of running workpackages. This is a SQL database. The database name is WfPersistence.

Workflow Database
The database for the workflow engine. Stores the workflow templates. This is a SQL database. The database name is MediaFlow.

Workflow Server

A GV STRATUS server dedicated to hosting the Workflow Engine Service, the Rules Engine Service, and the Xcode Control Engine Service. These services support rules-based operations.

Working Bin

The bin on a K2 system into which one or more channels record.

Workspace

The layout of docked and undocked panels that are part of an application.

Xcode Control Engine

The service that controls a third-party transcode application to support rules-based transcode operations.

Grass Valley Knowledge Base

Visit the Grass Valley Knowledge Base site for technical articles and FAQs (Frequently Asked Questions) about Grass Valley systems and products.

Grass Valley Knowledge Base

Safety Summary

Safety Summary

Read and follow the important safety information below, noting especially those instructions related to risk of fire, electric shock or injury to persons. Additional specific warnings not listed here may be found throughout the manual.

⚠	***WARNING: Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.***

Safety terms and symbols

Terms in this manual

Safety-related statements may appear in this manual in the following form:

⚠	***WARNING: Warning statements identify conditions or practices that may result in personal injury or loss of life.***
⚠	***CAUTION: Caution statements identify conditions or practices that may result in damage to equipment or other property, or which may cause equipment crucial to your business environment to become temporarily non-operational.***

Terms on the product

These terms may appear on the product:

DANGER — A personal injury hazard is immediately accessible as you read the marking.

WARNING — A personal injury hazard exists but is not immediately accessible as you read the marking.

CAUTION — A hazard to property, product, and other equipment is present.

Symbols on the product

The following symbols may appear on the product:

⚠	Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
⚠	Indicates that user, operator or service technician should refer to product manual(s) for important operating, maintenance, or service instructions.
⚠	This is a prompt to note fuse rating when replacing fuse(s). The fuse referenced in the text must be replaced with one having the ratings indicated.

⏚	Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.
⏚	Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.
⚡	Indicates that static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Warnings

The following warning statements identify conditions or practices that can result in personal injury or loss of life.

Dangerous voltage or current may be present — Disconnect power and remove battery (if applicable) before removing protective panels, soldering, or replacing components.

Do not service alone — Do not internally service this product unless another person capable of rendering first aid and resuscitation is present.

Remove jewelry — Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.

Avoid exposed circuitry — Do not touch exposed connections, components or circuitry when power is present.

Use proper power cord — Use only the power cord supplied or specified for this product.

Ground product — Connect the grounding conductor of the power cord to earth ground.

Operate only with covers and enclosure panels in place — Do not operate this product when covers or enclosure panels are removed.

Use correct fuse — Use only the fuse type and rating specified for this product.

Use only in dry environment — Do not operate in wet or damp conditions.

Use only in non-explosive environment — Do not operate this product in an explosive atmosphere.

High leakage current may be present — Earth connection of product is essential before connecting power.

Dual power supplies may be present — Be certain to plug each power supply cord into a separate branch circuit employing a separate service ground. Disconnect both power supply cords prior to servicing.

Double pole neutral fusing — Disconnect mains power prior to servicing.

Use proper lift points — Do not use door latches to lift or move equipment.

Avoid mechanical hazards — Allow all rotating devices to come to a stop before servicing.

Cautions

The following caution statements identify conditions or practices that can result in damage to equipment or other property

Use correct power source — Do not operate this product from a power source that applies more than the voltage specified for the product.

Use correct voltage setting — If this product lacks auto-ranging power supplies, before applying power ensure that the each power supply is set to match the power source.

Provide proper ventilation — To prevent product overheating, provide equipment ventilation in accordance with installation instructions.

Use anti-static procedures — Static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Do not operate with suspected equipment failure — If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.

Ensure mains disconnect — If mains switch is not provided, the power cord(s) of this equipment provide the means of disconnection. The socket outlet must be installed near the equipment and must be easily accessible. Verify that all mains power is disconnected before installing or removing power supplies and/or options.

Route cable properly — Route power cords and other cables so that they ar not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.

Use correct power supply cords — Power cords for this equipment, if provided, meet all North American electrical codes. Operation of this equipment at voltages exceeding 130 VAC requires power supply cords which comply with NEMA configurations. International power cords, if provided, have the approval of the country of use.

Use correct replacement battery — This product may contain batteries. To reduce the risk of explosion, check polarity and replace only with the same or equivalent type recommended by manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Troubleshoot only to board level — Circuit boards in this product are densely populated with surface mount technology (SMT) components and application specific integrated circuits (ASICS). As a result, circuit board repair at the component level is very difficult in the field, if not impossible. For warranty compliance, do not troubleshoot systems beyond the board level.

Sicherheit – Überblick

Lesen und befolgen Sie die wichtigen Sicherheitsinformationen dieses Abschnitts. Beachten Sie insbesondere die Anweisungen bezüglich

Brand-, Stromschlag- und Verletzungsgefahren. Weitere spezifische, hier nicht aufgeführte Warnungen finden Sie im gesamten Handbuch.

⚠ ***WARNUNG: Alle Anweisungen in diesem Handbuch, die das Abnehmen der Geräteabdeckung oder des Gerätegehäuses erfordern, dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Um die Stromschlaggefahr zu verringern, führen Sie keine Wartungsarbeiten außer den in den Bedienungsanleitungen genannten Arbeiten aus, es sei denn, Sie besitzen die entsprechende Qualifikationen für diese Arbeiten.***

Sicherheit – Begriffe und Symbole

In diesem Handbuch verwendete Begriffe

Sicherheitsrelevante Hinweise können in diesem Handbuch in der folgenden Form auftauchen:

⚠	***WARNUNG: Warnungen weisen auf Situationen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen.***
⚠	***VORSICHT: Vorsichtshinweise weisen auf Situationen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen oder zum zeitweisen Ausfall wichtiger Komponenten in der Arbeitsumgebung führen können.***

Hinweise am Produkt

Die folgenden Hinweise können sich am Produkt befinden:

GEFAHR – Wenn Sie diesen Begriff lesen, besteht ein unmittelbares Verletzungsrisiko.

WARNUNG – Wenn Sie diesen Begriff lesen, besteht ein mittelbares Verletzungsrisiko.

VORSICHT – Es besteht ein Risiko für Objekte in der Umgebung, den Mixer selbst oder andere Ausrüstungskomponenten.

Symbole am Produkt

Die folgenden Symbole können sich am Produkt befinden:

⚠	Weist auf eine gefährliche Hochspannung im Gerätegehäuse hin, die stark genug sein kann, um eine Stromschlaggefahr darzustellen.
⚠	Weist darauf hin, dass der Benutzer, Bediener oder Servicetechniker wichtige Bedienungs-, Wartungs- oder Serviceanweisungen in den Produkthandbüchern lesen sollte.
⚠	Dies ist eine Aufforderung, beim Wechsel von Sicherungen auf deren Nennwert zu achten. Die im Text angegebene Sicherung muss durch eine Sicherung ersetzt werden, die die angegebenen Nennwerte besitzt.
⏚	Weist auf eine Schutzerdungsklemme hin, die mit dem Erdungskontakt verbunden werden muss, bevor weitere Ausrüstungskomponenten angeschlossen werden.
⏚	Weist auf eine externe Schutzerdungsklemme hin, die als Ergänzung zu einem internen Erdungskontakt an die Erde angeschlossen werden kann.
⚡	Weist darauf hin, dass es statisch empfindliche Komponenten gibt, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

Warnungen

Die folgenden Warnungen weisen auf Bedingungen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen:

Gefährliche Spannungen oder Ströme – Schalten Sie den Strom ab, und entfernen Sie ggf. die Batterie, bevor sie Schutzabdeckungen abnehmen, löten oder Komponenten austauschen.

Servicearbeiten nicht alleine ausführen – Führen Sie interne Servicearbeiten nur aus, wenn eine weitere Person anwesend ist, die erste Hilfe leisten und Wiederbelebungsmaßnahmen einleiten kann.

Schmuck abnehmen – Legen Sie vor Servicearbeiten Schmuck wie Ringe, Uhren und andere metallische Objekte ab.

Keine offen liegenden Leiter berühren – Berühren Sie bei eingeschalteter Stromzufuhr keine offen liegenden Leitungen, Komponenten oder Schaltungen.

Richtiges Netzkabel verwenden – Verwenden Sie nur das mitgelieferte Netzkabel oder ein Netzkabel, das den Spezifikationen für dieses Produkt entspricht.

Gerät erden – Schließen Sie den Erdleiter des Netzkabels an den Erdungskontakt an.

Gerät nur mit angebrachten Abdeckungen und Gehäuseseiten betreiben – Schalten Sie dieses Gerät nicht ein, wenn die Abdeckungen oder Gehäuseseiten entfernt wurden.

Richtige Sicherung verwenden – Verwenden Sie nur Sicherungen, deren Typ und Nennwert den Spezifikationen für dieses Produkt entsprechen.

Gerät nur in trockener Umgebung verwenden – Betreiben Sie das Gerät nicht in nassen oder feuchten Umgebungen.

Gerät nur verwenden, wenn keine Explosionsgefahr besteht – Verwenden Sie dieses Produkt nur in Umgebungen, in denen keinerlei Explosionsgefahr besteht.

Hohe Kriechströme – Das Gerät muss vor dem Einschalten unbedingt geerdet werden.

Doppelte Spannungsversorgung kann vorhanden sein – Schließen Sie die beiden Anschlußkabel an getrennte Stromkreise an. Vor Servicearbeiten sind beide Anschlußkabel vom Netz zu trennen.

Zweipolige, neutrale Sicherung – Schalten Sie den Netzstrom ab, bevor Sie mit den Servicearbeiten beginnen.

Fassen Sie das Gerät beim Transport richtig an – Halten Sie das Gerät beim Transport nicht an Türen oder anderen beweglichen Teilen fest.

Gefahr durch mechanische Teile – Warten Sie, bis der Lüfter vollständig zum Halt gekommen ist, bevor Sie mit den Servicearbeiten beginnen.

Vorsicht

Die folgenden Vorsichtshinweise weisen auf Bedingungen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen führen können:

Gerät nicht öffnen – Durch das unbefugte Öffnen wird die Garantie ungültig.

Richtige Spannungsquelle verwenden – Betreiben Sie das Gerät nicht an einer Spannungsquelle, die eine höhere Spannung liefert als in den Spezifikationen für dieses Produkt angegeben.

Gerät ausreichend belüften – Um eine Überhitzung des Geräts zu vermeiden, müssen die Ausrüstungskomponenten entsprechend den Installationsanweisungen belüftet werden. Legen Sie kein Papier unter das Gerät. Es könnte die Belüftung behindern. Platzieren Sie das Gerät auf einer ebenen Oberfläche.

Antistatische Vorkehrungen treffen – Es gibt statisch empfindliche Komponenten, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

CF-Karte nicht mit einem PC verwenden – Die CF-Karte ist speziell formatiert. Die auf der CF-Karte gespeicherte Software könnte gelöscht werden.

Gerät nicht bei eventuellem Ausrüstungsfehler betreiben – Wenn Sie einen Produktschaden oder Ausrüstungsfehler vermuten, lassen Sie die Komponente von einem qualifizierten Servicetechniker untersuchen.

Kabel richtig verlegen – Verlegen Sie Netzkabel und andere Kabel so, dass Sie nicht beschädigt werden. Stützen Sie schwere Kabelbündel ordnungsgemäß ab, damit die Anschlüsse nicht beschädigt werden.

Richtige Netzkabel verwenden – Wenn Netzkabel mitgeliefert wurden, erfüllen diese alle nationalen elektrischen Normen. Der Betrieb dieses Geräts mit Spannungen über 130 V AC erfordert Netzkabel, die NEMA-Konfigurationen entsprechen. Wenn internationale Netzkabel mitgeliefert wurden, sind diese für das Verwendungsland zugelassen.

Richtige Ersatzbatterie verwenden – Dieses Gerät enthält eine Batterie. Um die Explosionsgefahr zu verringern, prüfen Sie die Polarität und tauschen die Batterie nur gegen eine Batterie desselben Typs oder eines gleichwertigen, vom Hersteller empfohlenen Typs aus. Entsorgen Sie gebrauchte Batterien entsprechend den Anweisungen des Batterieherstellers.

Das Gerät enthält keine Teile, die vom Benutzer gewartet werden können. Wenden Sie sich bei Problemen bitte an den nächsten Händler.

Consignes de sécurité

Il est recommandé de lire, de bien comprendre et surtout de respecter les informations relatives à la sécurité qui sont exposées ci-après, notamment les consignes destinées à prévenir les risques d'incendie, les décharges électriques et les blessures aux personnes. Les avertissements complémentaires, qui ne sont pas nécessairement repris ci-dessous, mais présents dans toutes les sections du manuel, sont également à prendre en considération.

⚠ ***AVERTISSEMENT: Toutes les instructions présentes dans ce manuel qui concernent l'ouverture des capots ou des logements de cet équipement sont destinées exclusivement à des membres qualifiés du personnel de maintenance. Afin de diminuer les risques de décharges électriques, ne procédez à aucune intervention d'entretien autre que celles contenues dans le manuel de l'utilisateur, à moins que vous ne soyez habilité pour le faire.***

Consignes et symboles de sécurité

Termes utilisés dans ce manuel

Les consignes de sécurité présentées dans ce manuel peuvent apparaître sous les formes suivantes :

⚠ ***AVERTISSEMENT: Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales.***

⚠ ***MISE EN GARDE: Les mises en garde signalent des conditions ou des pratiques susceptibles d'occasionner un endommagement à l'équipement ou aux installations, ou de rendre l'équipement temporairement non opérationnel, ce qui peut porter préjudice à vos activités.***

Signalétique apposée sur le produit

La signalétique suivante peut être apposée sur le produit :

DANGER — risque de danger imminent pour l'utilisateur.

AVERTISSEMENT — Risque de danger non imminent pour l'utilisateur.

MISE EN GARDE — Risque d'endommagement du produit, des installations ou des autres équipements.

Symboles apposés sur le produit

Les symboles suivants peut être apposés sur le produit :

⚠	Signale la présence d'une tension élevée et dangereuse dans le boîtier de l'équipement ; cette tension peut être suffisante pour constituer un risque de décharge électrique.
⚠	Signale que l'utilisateur, l'opérateur ou le technicien de maintenance doit faire référence au(x) manuel(s) pour prendre connaissance des instructions d'utilisation, de maintenance ou d'entretien.
⚠	Il s'agit d'une invite à prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait référence dans le texte doit être remplacé par un fusible du même calibre.
⏚	Identifie une borne de protection de mise à la masse qui doit être raccordée correctement avant de procéder au raccordement des autres équipements.
⏚	I dentifie une borne de protection de mise à la masse qui peut être connectée en tant que borne de mise à la masse supplémentaire.
⚡	Signale la présence de composants sensibles à l'électricité statique et qui sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

Avertissements

Les avertissements suivants signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales :

Présence possible de tensions ou de courants dangereux — Mettez hors tension, débranchez et retirez la pile (le cas échéant) avant de déposer les couvercles de protection, de défaire une soudure ou de remplacer des composants.

Ne procédez pas seul à une intervention d'entretien — Ne réalisez pas une intervention d'entretien interne sur ce produit si une personne n'est pas présente pour fournir les premiers soins en cas d'accident.

Retirez tous vos bijoux — Avant de procéder à une intervention d'entretien, retirez tous vos bijoux, notamment les bagues, la montre ou tout autre objet métallique.

Évitez tout contact avec les circuits exposés — Évitez tout contact avec les connexions, les composants ou les circuits exposés s'ils sont sous tension.

Utilisez le cordon d'alimentation approprié — Utilisez exclusivement le cordon d'alimentation fourni avec ce produit ou spécifié pour ce produit.

Raccordez le produit à la masse — Raccordez le conducteur de masse du cordon d'alimentation à la borne de masse de la prise secteur.

Utilisez le produit lorsque les couvercles et les capots sont en place — N'utilisez pas ce produit si les couvercles et les capots sont déposés.

Utilisez le bon fusible — Utilisez exclusivement un fusible du type et du calibre spécifiés pour ce produit.

Utilisez ce produit exclusivement dans un environnement sec — N'utilisez pas ce produit dans un environnement humide.

Utilisez ce produit exclusivement dans un environnement non explosible — N'utilisez pas ce produit dans un environnement dont l'atmosphère est explosible.

Présence possible de courants de fuite — Un raccordement à la masse est indispensable avant la mise sous tension.

Deux alimentations peuvent être présentes dans l'équipement — Assurez vous que chaque cordon d'alimentation est raccordé à des circuits de terre séparés. Débranchez les deux cordons d'alimentation avant toute intervention.

Fusion neutre bipolaire — Débranchez l'alimentation principale avant de procéder à une intervention d'entretien.

Utilisez les points de levage appropriés — Ne pas utiliser les verrous de la porte pour lever ou déplacer l'équipement.

Évitez les dangers mécaniques — Laissez le ventilateur s'arrêter avant de procéder à une intervention d'entretien.

Mises en garde

Les mises en garde suivantes signalent les conditions et les pratiques susceptibles d'occasionner des endommagements à l'équipement et aux installations :

N'ouvrez pas l'appareil — Toute ouverture prohibée de l'appareil aura pour effet d'annuler la garantie.

Utilisez la source d'alimentation adéquate — Ne branchez pas ce produit à une source d'alimentation qui utilise une tension supérieure à la tension nominale spécifiée pour ce produit.

Assurez une ventilation adéquate — Pour éviter toute surchauffe du produit, assurez une ventilation de l'équipement conformément aux instructions d'installation. Ne déposez aucun document sous l'appareil – ils peuvent gêner la ventilation. Placez l'appareil sur une surface plane.

Utilisez des procédures antistatiques - Les composants sensibles à l'électricité statique présents dans l'équipement sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

N'utilisez pas la carte CF avec un PC — La carte CF a été spécialement formatée. Le logiciel enregistré sur la carte CF risque d'être effacé.

N'utilisez pas l'équipement si un dysfonctionnement est suspecté — Si vous suspectez un dysfonctionnement du produit, faites inspecter celui-ci par un membre qualifié du personnel d'entretien.

Acheminez les câbles correctement — Acheminez les câbles d'alimentation et les autres câbles de manière à ce qu'ils ne risquent pas d'être endommagés. Supportez correctement les enroulements de câbles afin de ne pas endommager les connecteurs.

Utilisez les cordons d'alimentation adéquats — Les cordons d'alimentation de cet équipement, s'ils sont fournis, satisfont aux exigences de toutes les réglementations régionales. L'utilisation de cet équipement à des tensions dépassant les 130 V en c.a. requiert des cordons d'alimentation qui satisfont aux exigences des configurations NEMA. Les cordons internationaux, s'ils sont fournis, ont reçu l'approbation du pays dans lequel l'équipement est utilisé.

Utilisez une pile de remplacement adéquate — Ce produit renferme une pile. Pour réduire le risque d'explosion, vérifiez la polarité et ne remplacez la pile que par une pile du même type, recommandée par le fabricant. Mettez les piles usagées au rebut conformément aux instructions du fabricant des piles.

Cette unité ne contient aucune partie qui peut faire l'objet d'un entretien par l'utilisateur. Si un problème survient, veuillez contacter votre distributeur local.

Certifications and compliances

Canadian certified power cords

Canadian approval includes the products and power cords appropriate for use in the North America power network. All other power cords supplied are approved for the country of use.

FCC emission control

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by Grass Valley can affect emission compliance and could void the user's authority to operate this equipment.

Canadian EMC Notice of Compliance

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A préscrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

EN55103 1/2 Class A warning

This product has been evaluated for Electromagnetic Compatibility under the EN 55103-1/2 standards for Emissions and Immunity and meets the requirements for E4 environment.

This product complies with Class A (E4 environment). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC emission limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

Laser compliance

Laser safety requirements

This product may contain a Class 1 certified laser device. Operating this product outside specifications or altering its original design may result in hazardous radiation exposure, and may be considered an act of modifying or new manufacturing of a laser product under U.S. regulations contained in 21CFR Chapter 1, subchapter J or CENELEC regulations in HD 482 S1. People performing such an act are required by law to recertify and reidentify this product in accordance with provisions of 21CFR subchapter J for distribution within the U.S.A., and in accordance with CENELEC HD 482 S1 for distribution within countries using the IEC 825 standard.

Laser safety

Laser safety in the United States is regulated by the Center for Devices and Radiological Health (CDRH). The laser safety regulations are published in the "Laser Product Performance Standard," Code of Federal Regulation (CFR), Title 21, Subchapter J.

The International Electrotechnical Commission (IEC) Standard 825, "Radiation of Laser Products, Equipment Classification, Requirements and User's Guide," governs laser products outside the United States. Europe and member nations of the European Free Trade Association fall under the jurisdiction of the Comité Européen de Normalization Electrotechnique (CENELEC).

Safety certification

This product has been evaluated and meets the following Safety Certification Standards:

Standard	Designed/tested for compliance with:
ANSI/UL 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
IEC 60950-1 with CB cert.	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition, 2005).
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
BS EN 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment 2006.

ESD Protection

Electronics today are more susceptible to electrostatic discharge (ESD) damage than older equipment. Damage to equipment can occur by ESD fields that are smaller than you can feel. Implementing the information in this section will help you protect the investment that you have made in purchasing Grass Valley equipment. This section contains Grass Valley's recommended ESD guidelines that should be followed when handling electrostatic discharge sensitive (ESDS) items. These minimal recommendations are based on the information in the *Sources of ESD and Risks* on page 137 area. The information in *Grounding Requirements for Personnel* on page 138 is provided to assist you in selecting an appropriate grounding method.

Recommended ESD Guidelines

Follow these guidelines when handling Grass Valley equipment:

- Only trained personnel that are connected to a grounding system should handle ESDS items.
- Do not open any protective bag, box, or special shipping packaging until you have been grounded.

  NOTE: When a Personal Grounding strap is unavailable, as an absolute minimum, touch a metal object that is touching the floor (for example, a table, frame, or rack) to discharge any static energy before touching an ESDS item.
- Open the anti-static packaging by slitting any existing adhesive tapes. Do not tear the tapes off.
- Remove the ESDS item by holding it by its edges or by a metal panel.
- Do not touch the components of an ESDS item unless it is absolutely necessary to configure or repair the item.
- Keep the ESDS work area clear of all nonessential items such as coffee cups, pens, wrappers and personal items as these items can discharge static. If you need to set an ESDS item down, place it on an anti-static mat or on the anti-static packaging.

Sources of ESD and Risks

The following information identifies possible sources of electrostatic discharge and can be used to help establish an ESD policy.

Personnel

One of the largest sources of static is personnel. The static can be released from a person's clothing and shoes.

Environment

The environment includes the humidity and floors in a work area. The humidity level must be controlled and should not be allowed to fluctuate over a broad range. Relative humidity (RH) is a major part in determining the level of static that is being generated. For example, at 10% - 20% RH a person walking across a carpeted floor can develop 35kV; yet when the relative humidity is increased to 70% - 80%, the person can only generate 1.5kV.

Static is generated as personnel move (or as equipment is moved) across a floor's surface. Carpeted and waxed vinyl floors contribute to static build up.

Work Surfaces

Painted or vinyl-covered tables, chairs, conveyor belts, racks, carts, anodized surfaces, plexiglass covers, and shelving are all static generators.

Equipment

Any equipment commonly found in an ESD work area, such as solder guns, heat guns, blowers, etc., should be grounded.

Materials

Plastic work holders, foam, plastic tote boxes, pens, packaging containers and other items commonly found at workstations can generate static electricity.

Grounding Requirements for Personnel

The information in this section is provided to assist you in selecting a grounding method. This information is taken from ANSI/ESD S20.20-2007 (Revision of ANSI/ESD S20.20-1999).

Product Qualification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ANSI/ESD S1.1 (Section 5.11)	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ANSI/ESD STM97.1	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ANSI/ESD STM97. 1ANSI/ESD STM97.2	< 10^9 ohm
	ANSI/ESD STM97.2	< 100 V

Product qualification is normally conducted during the initial selection of ESD control products and materials. Any of the following methods can be used: product specification review, independent laboratory evaluation, or internal laboratory evaluation.

Compliance Verification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ESD TR53 Wrist Strap Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 1	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 3.5 x 10^7 ohm
Flooring / Footwear System – Method 2 (both required)	ESD TR53 Flooring Section and ESD TR53 Footwear Section	< 1.0 x 10^9 ohm

* For situations where an ESD garment is used as part of the wrist strap grounding path, the total system resistance, including the person, garment, and grounding cord, must be less than 3.5 x 10^7 ohm.

Trademarks and Agreements

Trademarks

Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Grass Valley, GV STRATUS, GV Director, K2, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP and NetCentral, are trademarks or registered trademarks of Grass Valley Canada. Belden Inc., Grass Valley Canada, and other parties may also have trademark rights in other terms used herein, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom. AVCHD and the AVCHD logo are trademarks of Panasonic Corporation and Sony Corporation. Avid DNxHD is a registered trademark of Avid Technology, Inc., a Delaware corporation.

JPEG acknowledgment

This software is based in part on the work of the Independent JPEG Group.