GFI ClearView

Administration Guide

Find out how to set up and configure GFI ClearView in different environments and how to customize advanced features.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and GFI ClearView are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI ClearView is a copyright of GFI Software. All rights reserved.
Document Version: 1.0

Last updated (month/day/year): 30/09/2023

Contents

1. Introduction

Every day critical business network traffic and recreational network traffic compete for bandwidth on strained networks. GFI ClearView inspects, monitors and manages network traffic, maximizing speed and data flow efficiency, giving priority to mission critical business applications across your LANs and WANs.

1.1 ClearView system components

ClearView includes a number of required and optional components that can be installed in your organization's infrastructure.

1.1.1 ClearView Appliance

The ClearView product line includes a series of virtual network appliances designed to plug directly into your environment with minimal effort. Appliances come in a range of sizes to handle every networking scenario and size, from small offices with dozens of users to very large data centers that support hundreds of thousands.

For more information, refer to The ClearView product line.

1.1.2 ClearView Web UI

GFI ClearView offers to user and administrator a Web User Interface that allows users to configure policies and monitor the appliances performances through a variety of dashboard and reports.

1.1.3 ClearView Solution Center

The ClearView Solution Center provides a series of predefined monitors you can run to generate network performance reports for applications like FTP, SSH, Salesforce.com, Microsoft Office365, VoIP, and many more.

For more information, refer to Monitoring applications with the ClearView Solution Center.

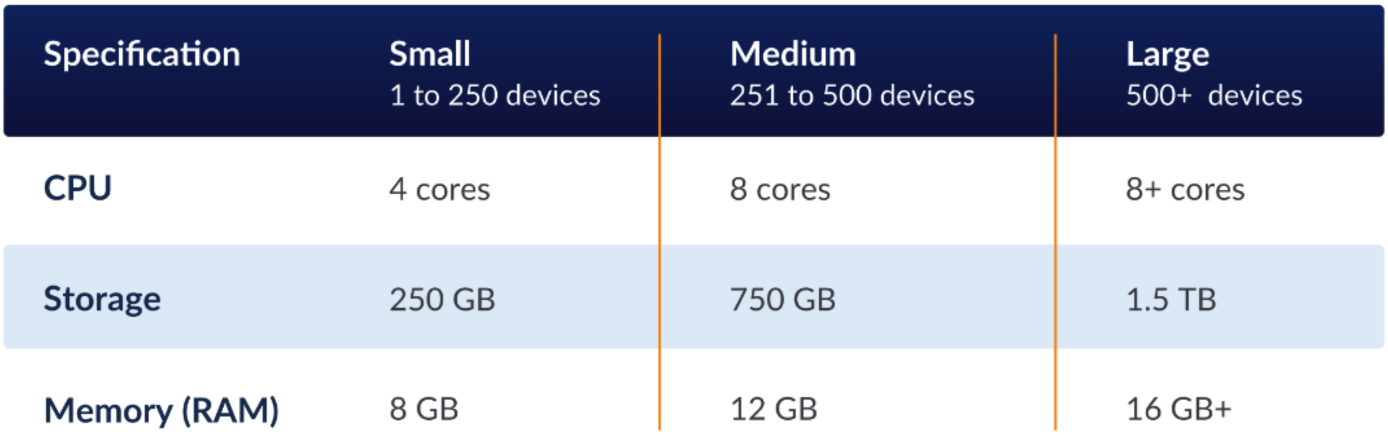
1.2 The ClearView product line

The ClearView product line includes a series of hardware and virtual network appliances designed to plug directly into your environment with minimal effort. Appliances come in a range of sizes to handle every networking scenario and size, from small offices with dozens of users to very large data centers that support hundreds of thousands.

1.2.1 ClearView virtual appliances

ClearView provides the same monitoring, reporting and control features. Capacity is determined by a combination of licensing and underlying hardware.

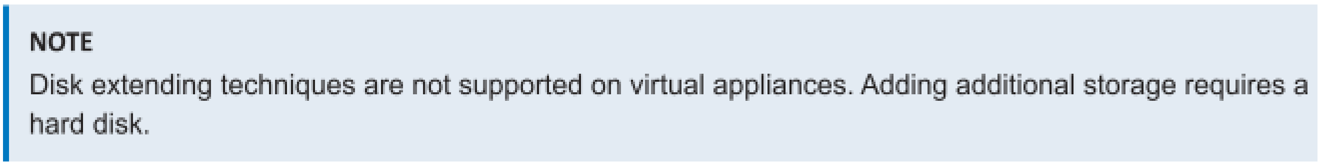
ClearView runs on a host machine under a hypervisor, using dedicated resources. The minimum dedicated hypervisor hardware requirements are listed in the table below:



Specification	Small 1 to 250 devices	Medium 251 to 500 devices	Large 500+ devices
CPU	4 cores	8 cores	8+ cores
Storage	250 GB	750 GB	1.5 TB
Memory (RAM)	8 GB	12 GB	16 GB+

Requirements:

- Intel Xeon class, 64-bit CPU with VT
- Enabled Hard drive space on a single disk



NOTE

Disk extending techniques are not supported on virtual appliances. Adding additional storage requires a hard disk.

2. ClearView Deployment Guide

This getting started guide steps through the basic process of installing, configuring and using your ClearView.

2.1 Deployment options

GFI ClearView Appliance fits almost anywhere in your network environment. As a general rule, anywhere network packets move from one device to another, whether via physical cables or virtualization, you can plug in a GFI ClearView Appliance.

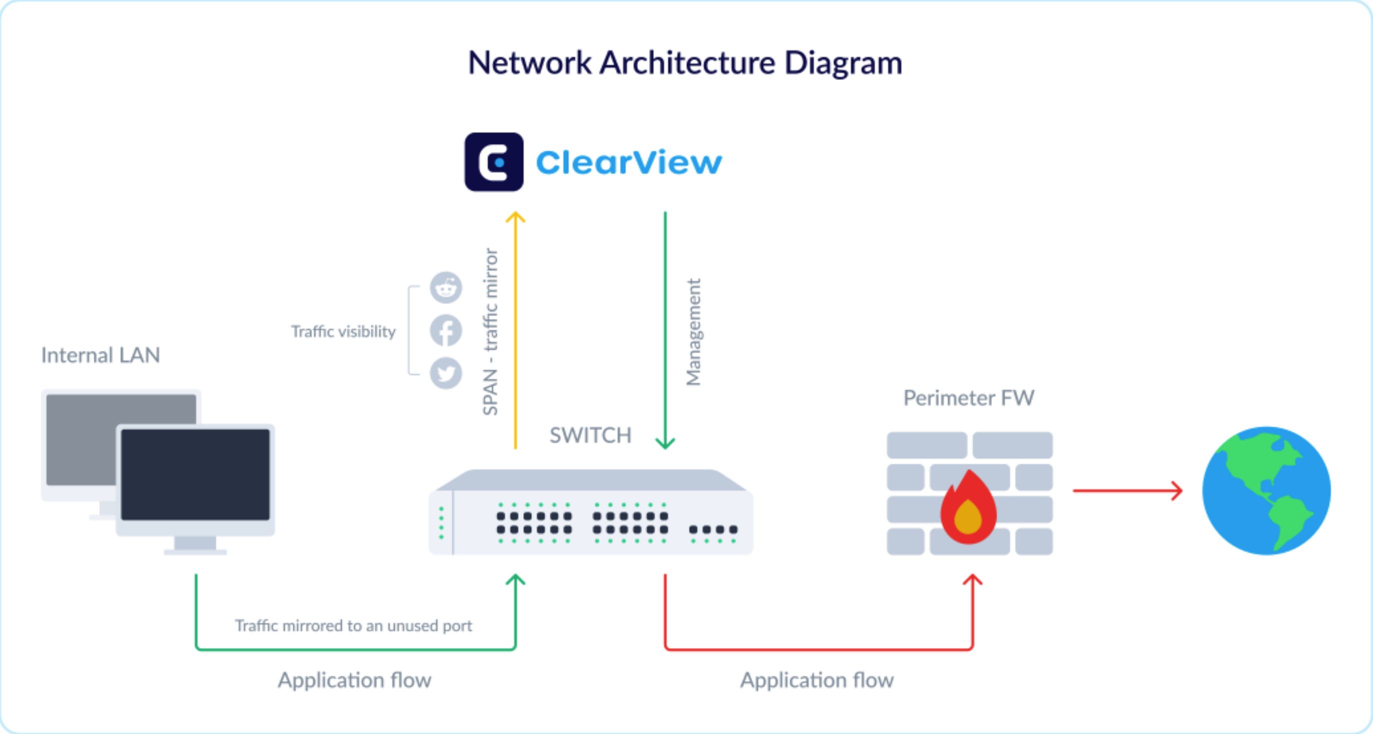
In this section of the guide, you'll walk-through the most common GFI ClearView Appliance deployments.

2.1.1 Pre-requisites:

- Hypervisor
  - VMware | OVA File | Installation guide video
  - HyperV | ISO file | Installation guide video | HyperV port mirroring settings guide
  - VirtualBox | OVA File | Installation guide video

- Port mirroring / SPAN port Configuration
  [Example] Video guide

2.1.2 Network Architecture Diagram:



2.1.3 How to Deploy:

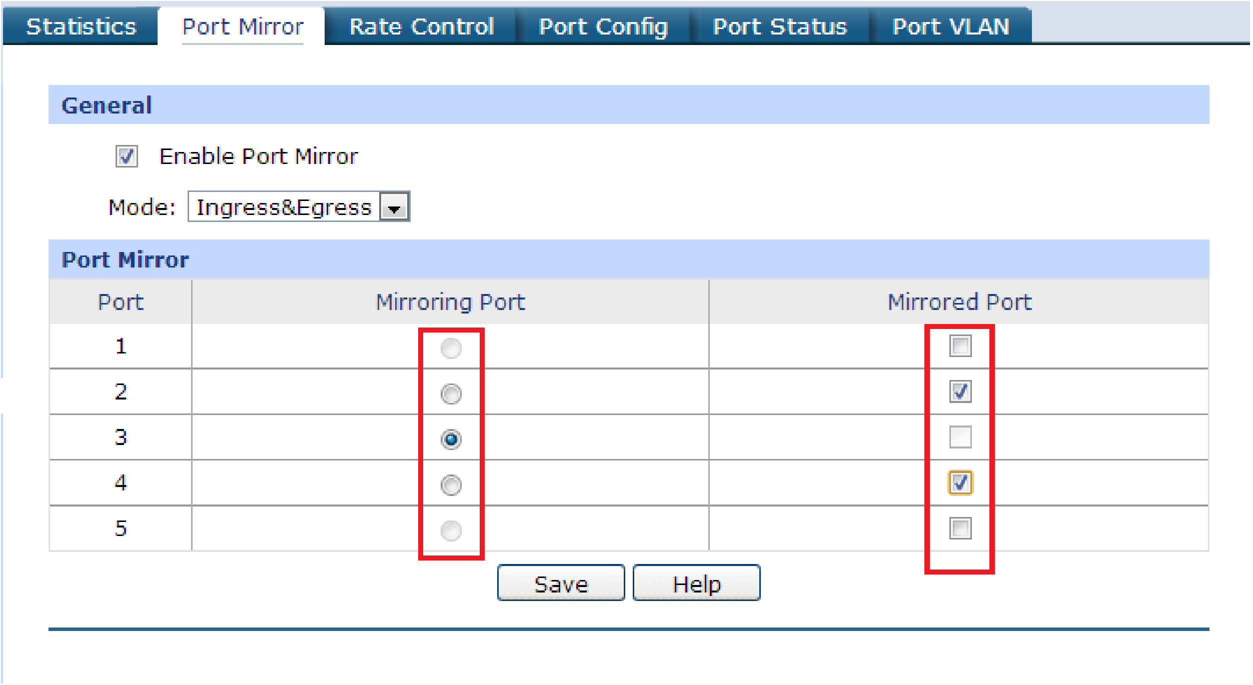
1. Download the Installer Image.
2. Load the image in the hypervisor. Adjust the hardware specifications as per your needs and deployment scenario.
3. Power on the machine.
4. Log in to GFI ClearView with **username=**admin and **password=**exinda
5. Read and accept the End User License Agreement (EULA).
6. Complete the steps in the Jumpstart Wizard.
7. Using the IP assigned to the management interface (eth0), you can access the web-based user interface by navigating to **https://<ip address>**
   Note: You can check the IPs assigned to interfaces with the following command: ***show interfaces summary***
8. Open the Web UI. Navigate to **Dashboard > System** tab, find the **Host ID**, and send that to your GFI partner.
9. Once you receive the key from the partner, please perform the following steps.

   a. Navigate to the GFI ClearView Web UI.
   b. To view the status of your license, select System > Setup and switch to the License tab.
   c. Click “Check for License Online”. Accept the license key that appears and save changes.
      Note: Please ensure that the Management Interface (eth0) has Internet Access.
   d. Alternatively, paste the license key provided in the email.
   e. Click Add License.

2.2.1 How to Configure:

For GFI ClearView to be able to detect the network traffic, you need to enable mirroring on the switch and the ClearView appliance:

- Enable Mirror/SPAN port mirroring from the switch onto an unused port. Connect that port to the GFI ClearView appliance. Here's an example where traffic on Port 2 and 4 is mirrored to Port 3. In this example, Port 3 would be connected to the GFI ClearView appliance:



General

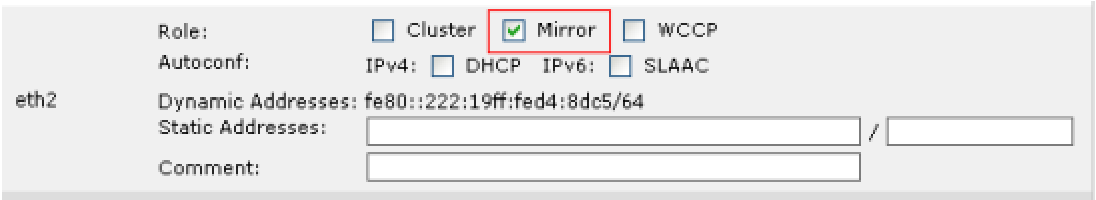
☑ Enable Port Mirror

Mode: Ingress&Egress

Port Mirror

Port	Mirroring Port	Mirrored Port
1	○	□
2	○	☑
3	●	□
4	○	☑
5	○	□

- Enable the mirror option on the GFI ClearView interface to monitor its traffic. From the Web UI:
    - Click System > Network > IP Address.
    - To use an interface as a Mirror port, select the Mirror check box.



eth2

Role: □ Cluster ☑ Mirror □ WCCP

Autoconf: IPv4: □ DHCP IPv6: □ SLAAC

Dynamic Addresses: fe80::222:19ff:fed4:8dc5/64

Static Addresses: /

Comment:

- Click "Apply Changes".

2.2.2 Related Topics

Review the following topics after completing the VM deployment:

- Adjusting the RAM available to the Virtual Machine
- Adjusting the NICs available to the Virtual Machine
- Add Storage to the VMware Virtual Machine

To improve the performance of the virtual appliance, change the number of CPUs, the RAM, networking, and storage allocated to the virtual machine.

> **NOTE**
> You will need to shut the virtual appliance down before you can modify its configuration.

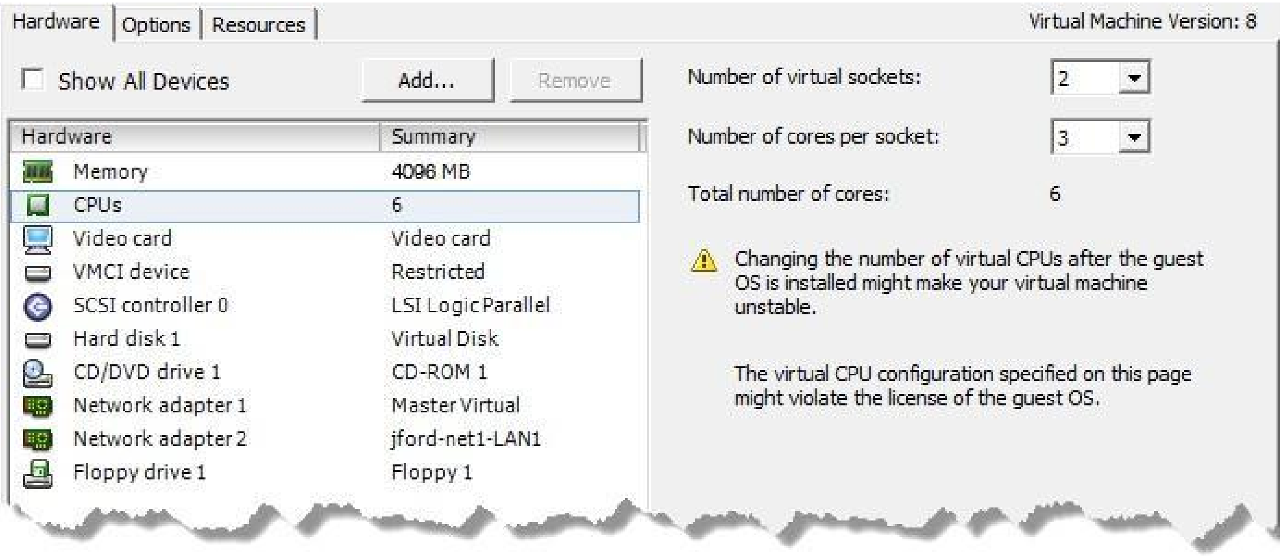
2.2.3 Related Topics

- Adjusting the number of CPUs available to the Virtual Machine
- Adjusting the RAM available to the Virtual Machine
- Adjusting the NICs available to the Virtual Machine
- Add Storage to the VMware Virtual Machine

Adjusting the number of CPUs available to the Virtual Machine

By default, all Virtual Appliances come configured with two virtual CPUs. Increase the number of CPUs to suit your requirements.

1. Open the VMware vSphere Client.
2. Right-click on the GFI ClearView Virtual Appliance, and select Edit Settings.
3. On the Hardware tab, select CPUs.
4. Select the Number of virtual sockets.
5. Select the Number of cores per socket. The resulting total number of cores is a number equal to or less than the num- ber of logical CPUs on the host. For example, if the Number of virtual sockets is 2, and the Number of cores per socket is 3, the total number of cores will be
6. Show Image...



Hardware	Summary
Memory	4096 MB
CPUs	6
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
CD/DVD drive 1	CD-ROM 1
Network adapter 1	Master Virtual
Network adapter 2	jford-net1-LAN1
Floppy drive 1	Floppy 1

Number of virtual sockets: 2

Number of cores per socket: 3

Total number of cores: 6

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

7. Click OK.

Adjusting the RAM available to the Virtual Machine

By default, all Virtual Appliances come configured with 4GB of RAM. Increase the amount of RAM to suit your requirements.

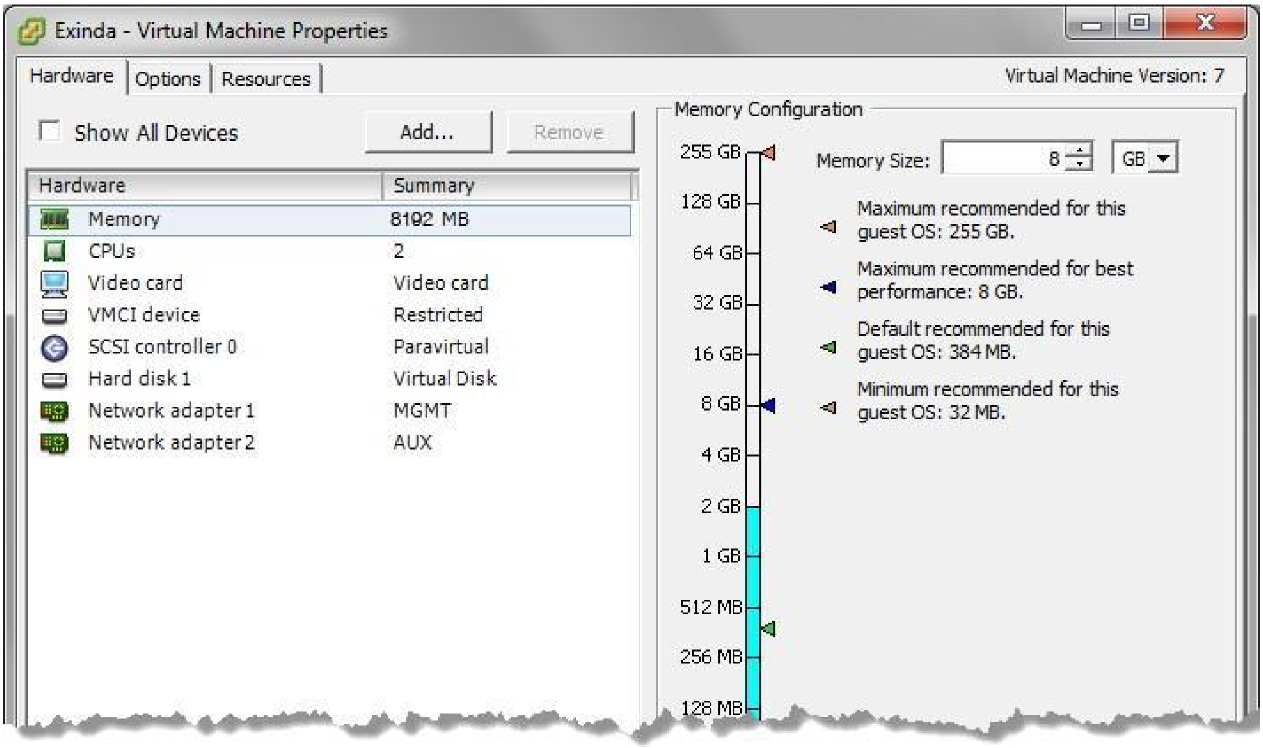
1. Open the VMware vSphere Client.

2. Right-click the GFI ClearView Virtual Appliance, and select Edit Settings.

3. On the Hardware tab, select Memory.

4. Click OK.

5. Select the desired Memory Size



Hardware	Summary
Memory	8192 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	Paravirtual
Hard disk 1	Virtual Disk
Network adapter 1	MGMT
Network adapter 2	AUX

Memory Size: 8 GB

Maximum recommended for this guest OS: 255 GB.

Maximum recommended for best performance: 8 GB.

Default recommended for this guest OS: 384 MB.

Minimum recommended for this guest OS: 32 MB.

Adjusting the NICs available to the Virtual Machine

By default, all GFI ClearView Virtual Appliances come with two NICs. Of these, the first NIC is the Management Interface (for managing the Virtual Appliance), the second NIC is the Auxiliary Interface (for HA topologies, clustering and out-of-path deployments) and is mainly used to connect to the host machine interface that receives mirrored traffic from the switch.

If there is a need to add more NICs, you can do it by following the below steps:

1. Open the VMware vSphere Client.

2. Right-click the GFI ClearView Virtual Appliance, and select Properties.

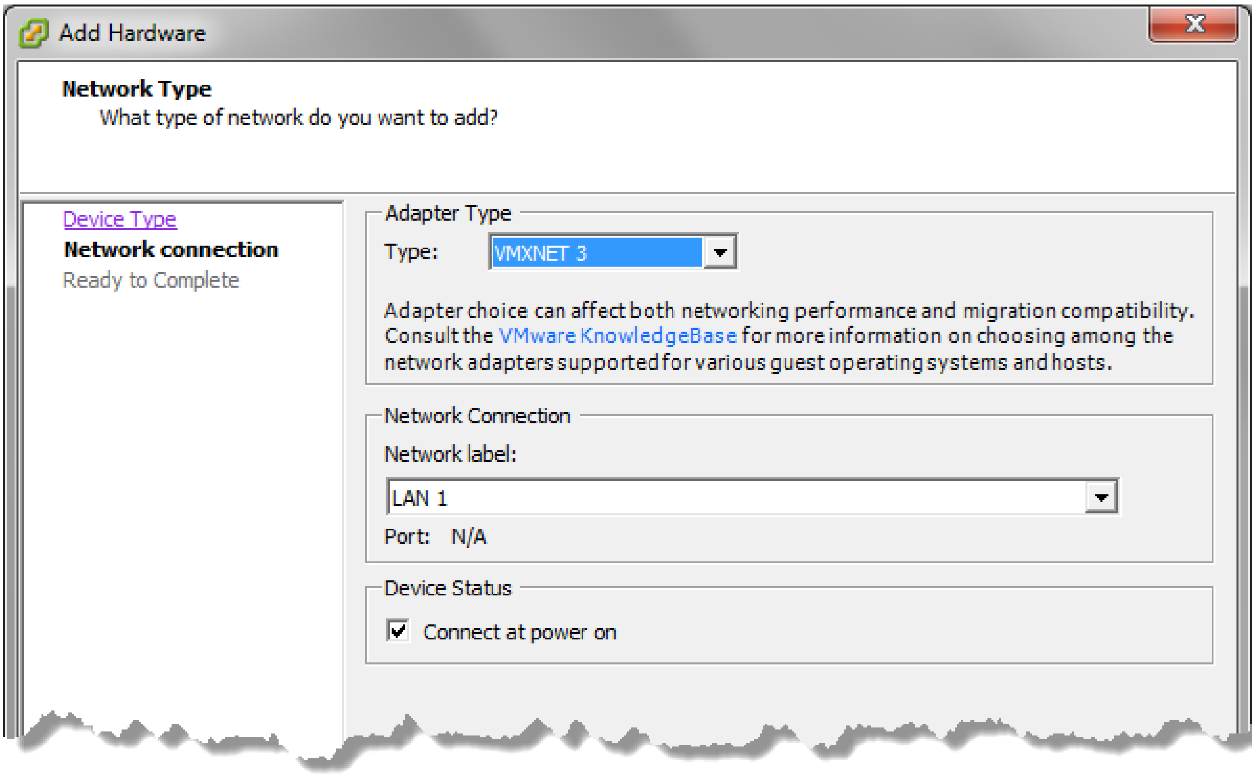
3. Switch to the Hardware tab.

4. Click Add.

5. From the Device Type list, select Ethernet Adaptor and click Next.

6. In the Adapter Type list, select VMXNET 3.

7. Select the network to map the NIC to.



Add Hardware

Network Type

What type of network do you want to add?

Adapter Type

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

Network label: LAN 1

Port: N/A

Device Status

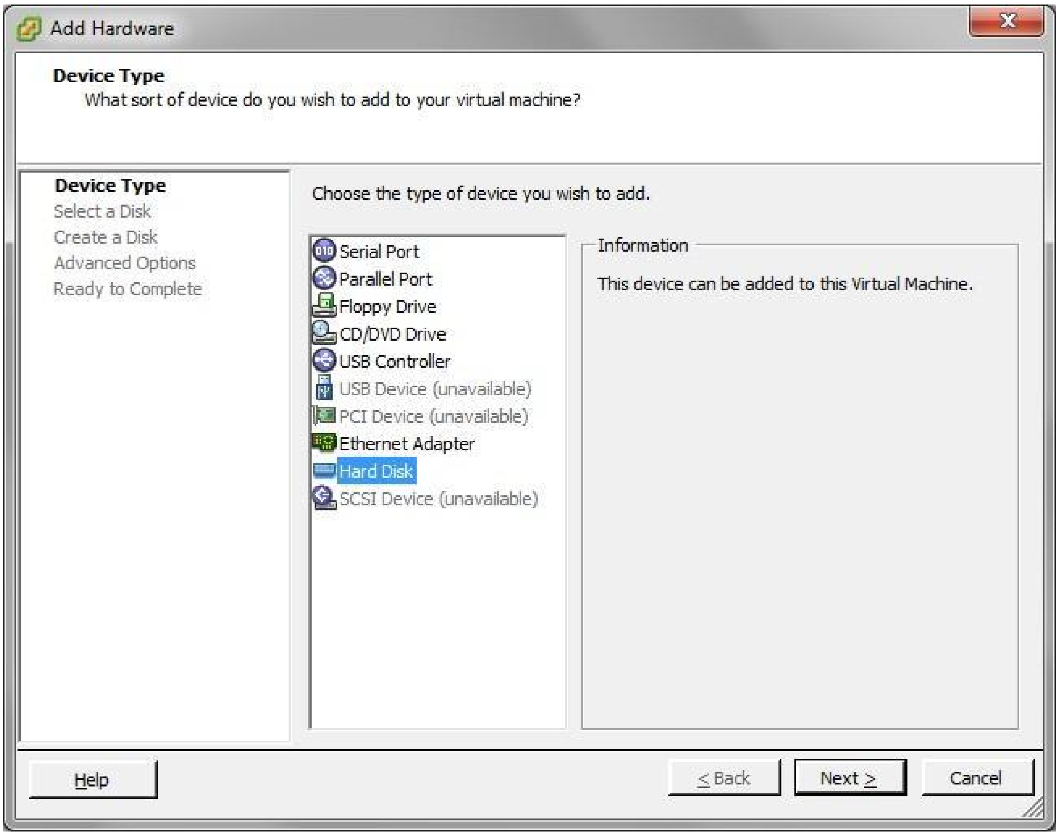
☑ Connect at power on

8. Click Next.
9. Review the information and click Finish to add the NIC
10. Restart the virtual appliance. The new NICs are automatically detected.

Add Storage to the VMware Virtual Machine

By default, all GFI ClearView Virtual Appliances come with a single 50GB (fixed-size) disk. Depending on your reporting needs, you can add more by following the below process:

1. Open the VMware vSphere Client.
2. From the Hardware tab in the GFI ClearView Virtual Appliance Properties screen, click Add.



Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

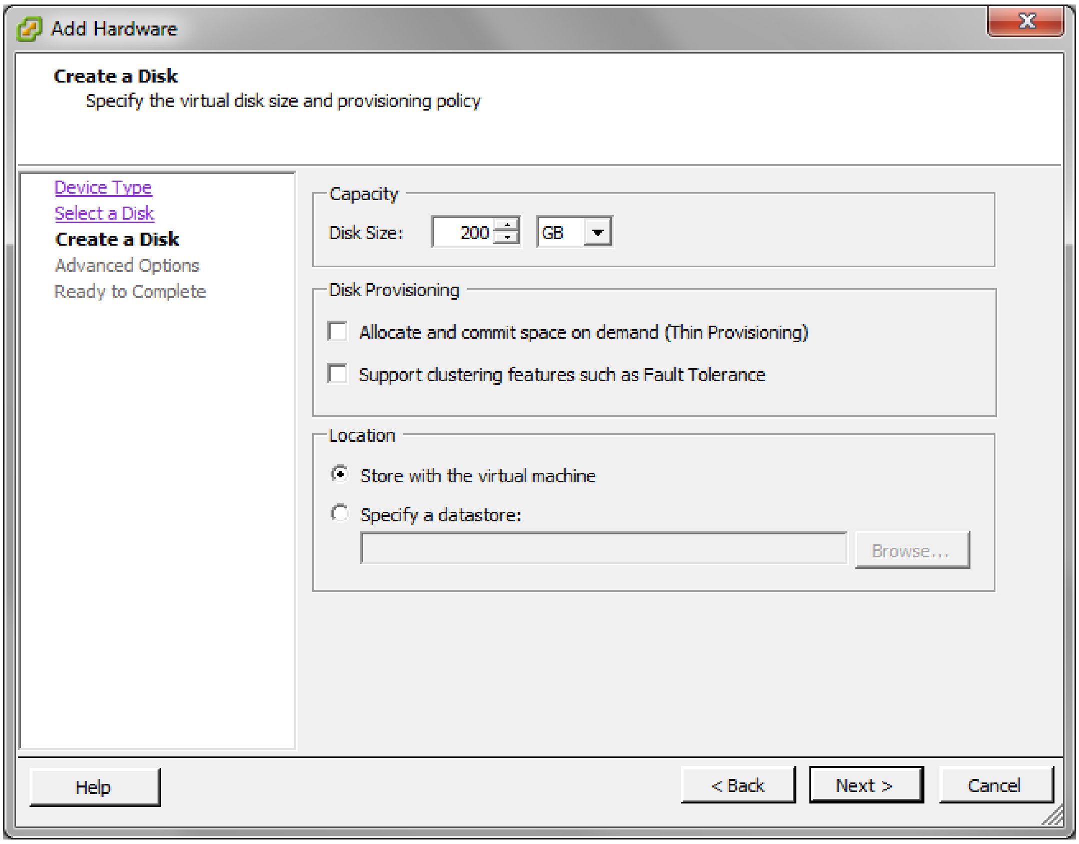
- Serial Port
- Parallel Port
- Floppy Drive
- CD/DVD Drive
- USB Controller
- USB Device (unavailable)
- PCI Device (unavailable)
- Ethernet Adapter
- Hard Disk
- SCSI Device (unavailable)

Information

This device can be added to this Virtual Machine.

3. Select Hard Disk, then click Next.

4. Specify the size of the additional disk to create. This space will be added to the default 50GB that comes with the Virtual Appliance. So if you add a 200GB disk here, the total storage for the Virtual Appliance will be 250GB.



Add Hardware

Create a Disk

Specify the virtual disk size and provisioning policy

Capacity

Disk Size: 200 GB

Disk Provisioning

☐ Allocate and commit space on demand (Thin Provisioning)

☐ Support clustering features such as Fault Tolerance

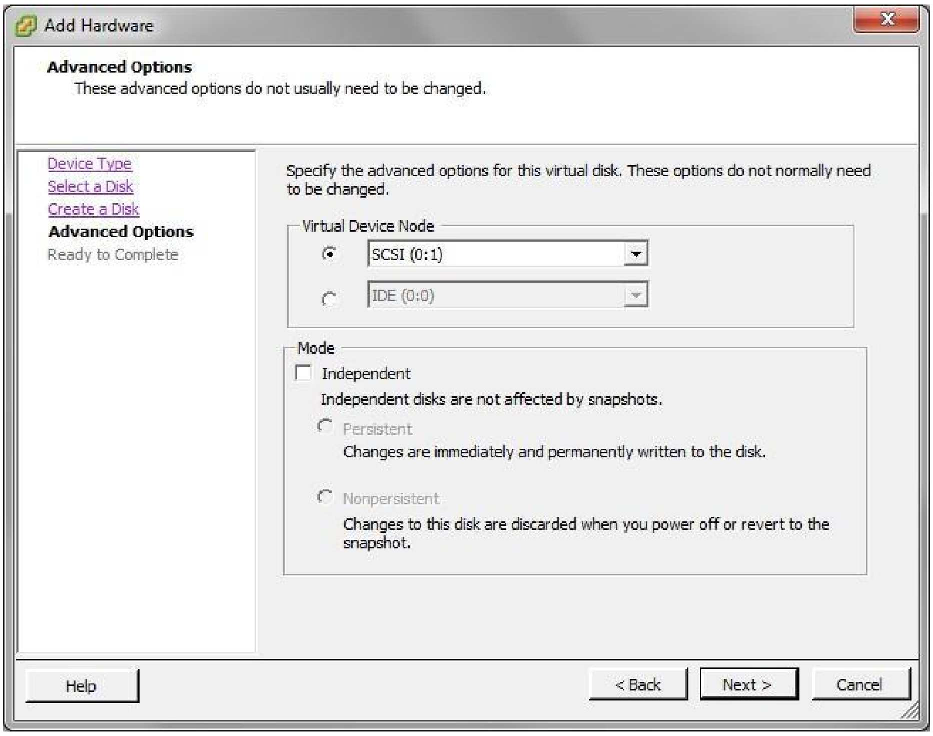
Location

● Store with the virtual machine

○ Specify a datastore:

5. Click Next.

6. Attach the new disk to the next available SCSI node for best performance



Add Hardware

Advanced Options

These advanced options do not usually need to be changed.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node

● SCSI (0:1)

○ IDE (0:0)

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

7. Click Next.

8. Review the information and click Finish to add the disk.

9. When the Virtual Appliance is next booted, you can use the storage commands in the CLI to provision the new storage. The `show storage` command lists the current storage allocations as well as the Virtual Appliance's disks.

```
(config) # show storage
Services:
 cifs: available - 3743.46M free of 3876M total
 edge-cache: available - 3723.53M free of 3872M
 total monitor: available - 9882.83M free of 10G
 total users: available - 974.62M free of 1024M
 total
 wan-memory: available - 17.21G free of 17.65G total

Disks:
 sda10(internal): in use - 36.22 GB
 sdb: not in use - 214.7 GB

Total: 36.22
Unallocated: 0
```

10. The output shows that our new 200G disk is called 'sdb' and it's currently not in use. The `storage disk add` command is used to provision the new disk.

```
(config) # storage disk add sdb
This will erase all data on the disk. Do you really want to do this (Y/N)?
[N] Y
```

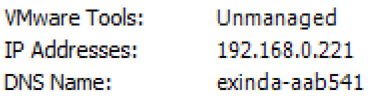
11. After this command has executed, another look at `show storage` shows that the new disk is now in use and our 200G is ready for allocation.

```
(config) # show storage
Services:
 cifs: available - 3743.46M free of 3876M total
 edge-cache: available - 3723.53M free of 3872M
 total monitor: available - 9882.83M free of 10G
 total users: available - 974.62M free of 1024M
 total
 wan-memory: available - 17.21G free of 17.65G total

Disks:
 sda10(internal): in use - 36.22 GB
 sdb: in use - 200.00 GB

Total: 236.21G
Unallocated: 200G
```

Starting the VMware Virtual Appliance

When you are ready to start the virtual appliance for the first time, Power it on. The Virtual Appliance boots, and displays a login prompt on the VMware console. At this point, you can login with the default username admin and password exinda.

If the first NIC is connected to a network that provides addresses using DHCP, the Virtual Appliance should have picked up an IP address. On the Virtual Appliance summary screen, VMware tools should display the IP address that the Virtual Appliance has obtained.



VMware Tools:	Unmanaged
IP Addresses:	192.168.0.221
DNS Name:	exinda-aab541

If the first NIC is not able to obtain an address using DHCP, you'll need to use the VMware console to enter the following CLI commands to set a static IP address.

```
> en
# conf t
(config) # interface eth0 ip address <ip> <netmask>
(config) # ip default-gateway <default gateway>
(config) # ip name-server <dns server>
```

Once you have determined the IP address or set a static IP address, you can access the web-based user interface by navigating to https://<ip address>.

2.2.4 Related Topics

At this point, the following tasks should be completed before using the Virtual Appliance:

- Add extra NICs (if required) and deploy the Virtual Appliance either in line or out-of-path.

- Add and provision extra storage (if required).
- Obtain a license for this Virtual Appliance.

Running on Microsoft Hyper-V

The following sections describe how to deploy GFI ClearView Virtual Appliance as well as to customize the virtual hardware to suit your requirements.

The GFI ClearView Virtual Appliance are available for Microsoft Hyper-V hypervisors.

Install the Virtual Machine on Hyper-V

The GFI ClearView Virtual Appliances have been prepared to run in a variety of virtual environments. Hyper-V provides support for hosting the GFI ClearView Virtual Appliances in Microsoft Server 2012 (R2) and above. The detailed installation steps can be found in the Installation guide video along with HyperV port mirroring settings guide. To install the appliance you would also need the ISO file.

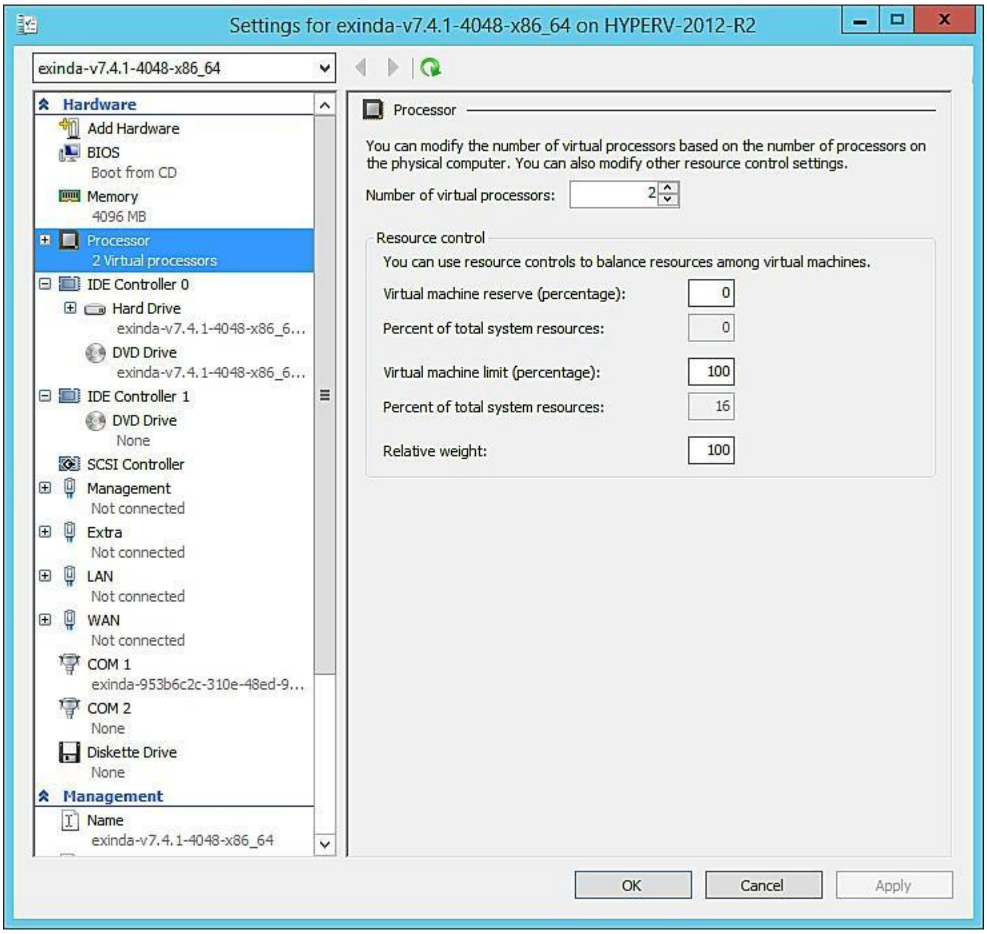
The Virtual Machine, as supplied by GFI, may not have all of the configuration options you prefer. For example, the disk storage is confined to 50GB, which is unlikely to be sufficient for your needs. When preparing the ISO file Virtual Appliance for download, it is not possible to know just what hardware is available on the host machine. After you have installed the virtual machine, you will need to make some adjustments to the configuration using the controls in the Hyper-V Manager. See the following related tasks.

2.2.5 Related Topics

Adjusting the number of CPUs available to the Virtual Machine

After installing the virtual machine, you may need to adjust the number of CPUs that are available to the GFI ClearView Virtual Appliance. The basic virtual machine configuration includes a minimal number of CPUs, but if you have spare CPUs on the host machine, you may want to make these available to the virtual machine. You make adjustments to the number of CPUs in the Hyper-V Manager.

1. Open the Hyper-V Manager.
2. In the left pane, right-click on the virtual machine you need to edit and select **Settings**. The Settings dialog box for the virtual machine opens.
3. In the left pane, under **Hardware**, select the **Processor** item. The processor settings open in the right pane.



Settings for exinda-v7.4.1-4048-x86_64 on HYPERV-2012-R2

exinda-v7.4.1-4048-x86_64

- Hardware
  - Add Hardware
  - BIOS: Boot from CD
  - Memory: 4096 MB
  - Processor: 2 Virtual processors
  - IDE Controller 0
    - Hard Drive: exinda-v7.4.1-4048-x86_6...
    - DVD Drive: exinda-v7.4.1-4048-x86_6...
  - IDE Controller 1
    - DVD Drive: None
  - SCSI Controller
  - Management: Not connected
  - Extra: Not connected
  - LAN: Not connected
  - WAN: Not connected
  - COM 1: exinda-953b6c2c-310e-48ed-9...
  - COM 2: None
  - Diskette Drive: None
- Management
  - Name: exinda-v7.4.1-4048-x86_64

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 2

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

Percent of total system resources: 16

Relative weight: 100

4. In the **Number of virtual processors** spinbox, click the up- or down-arrows to adjust the number of CPUs.

> **NOTE**
>
> In this pane you can also adjust several other settings to balance resources among any other virtual machines. Consult the Hyper-V documentation for more information on these settings.

5. Click **OK**. The number of CPUs available to the virtual machine is immediately adjusted.

> **NOTE**
>
> These instructions also apply to changing the configuration after the virtual appliance has entered service.

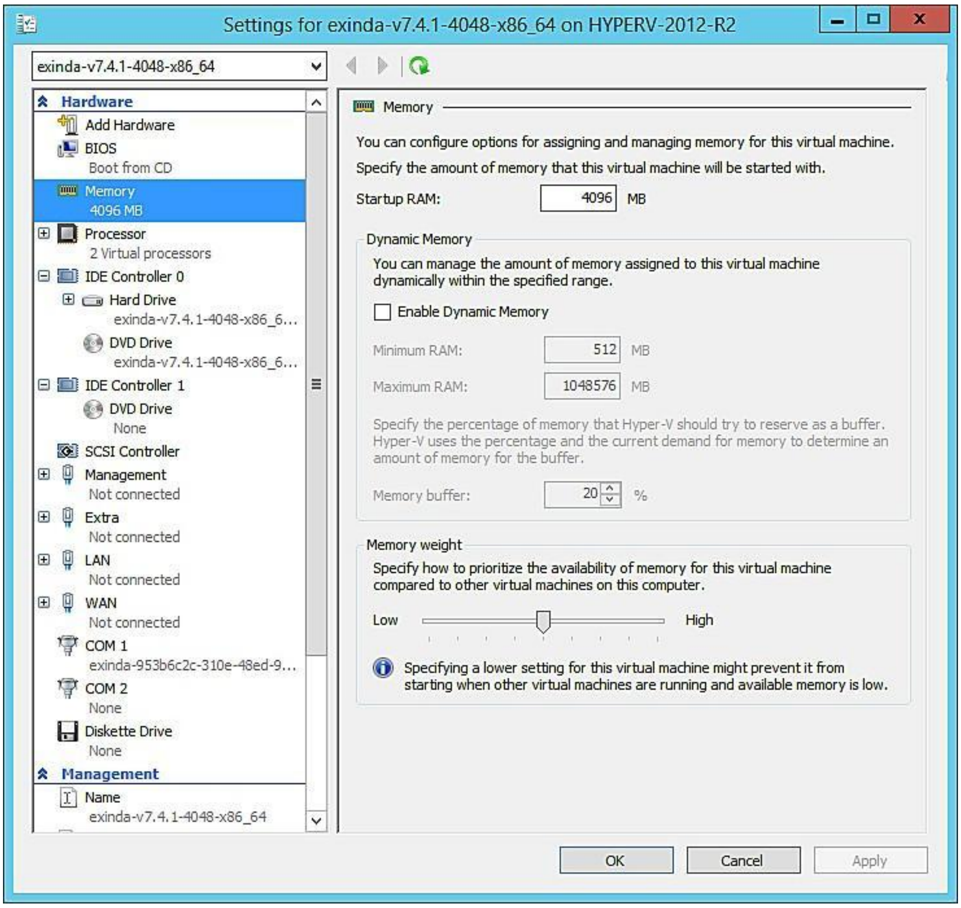
2.2.6 Related Topics

Adjusting the RAM available to the Virtual Machine

After installing the virtual machine, you may need to adjust the amount of RAM that is available to the GFI ClearView Virtual Appliance. There is a basic amount of RAM provided in the GFI ClearView Virtual Appliance, but if you have spare RAM on the host machine, you may want to make this available to the virtual machine. You make adjustments to the amount of RAM in the Hyper-V Manager.

1. Open the Hyper-V Manager.
2. In the left pane, right-click on the virtual machine you need to edit and select **Settings**. The Settings dialog box for the virtual machine opens.

3. In the left pane, under **Hardware**, select the **Memory** item. The memory settings open in the right pane.



Settings for exinda-v7.4.1-4048-x86_64 on HYPERV-2012-R2

exinda-v7.4.1-4048-x86_64

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  4096 MB
- Processor
  2 Virtual processors
- IDE Controller 0
  - Hard Drive
    exinda-v7.4.1-4048-x86_6...
  - DVD Drive
    exinda-v7.4.1-4048-x86_6...
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Management
  Not connected
- Extra
  Not connected
- LAN
  Not connected
- WAN
  Not connected
- COM 1
  exinda-953b6c2c-310e-48ed-9...
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  exinda-v7.4.1-4048-x86_64

Memory

You can configure options for assigning and managing memory for this virtual machine.

Specify the amount of memory that this virtual machine will be started with.

Startup RAM: 4096 MB

Dynamic Memory

You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

□ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight

Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

Low High

Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.

4. In the **Startup RAM** field, type a new amount for the quantity of RAM.

> **NOTE**
> These instructions also apply to changing the configuration after the virtual appliance has entered service.

5. Click **OK**. The amount of RAM available to the virtual machine is immediately adjusted.

2.2.7 Related Topics

Increase storage by adding new virtual drives

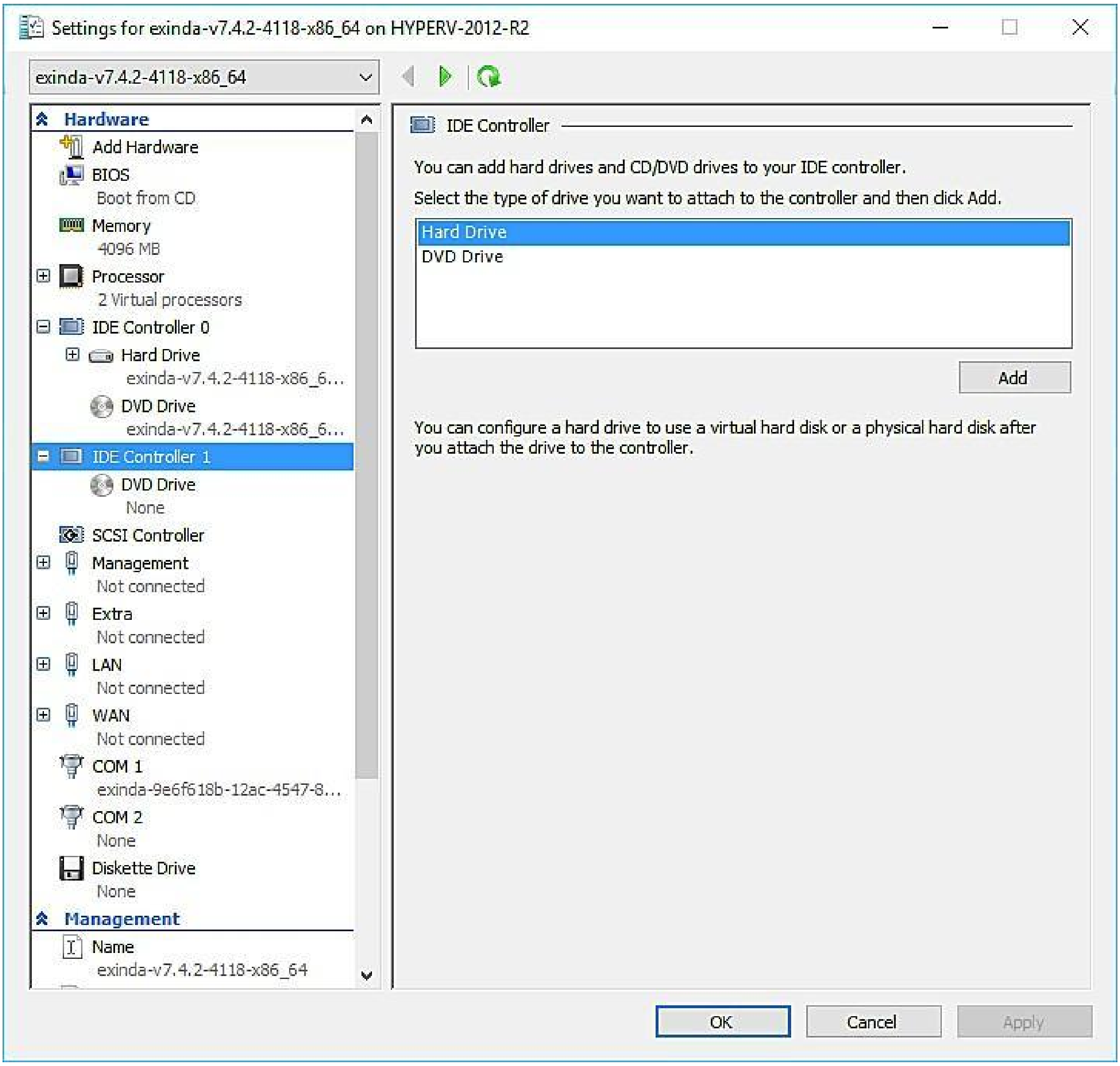
During the process of installing the virtual machine, you needed to connect the virtual hard drive (VHD) to the GFI ClearView Virtual Appliance. Prior to powering the VM on for the first time, it is likely that you should need to increase the size of the VHD. You can also make this adjustment after bringing the GFI ClearView Virtual Appliance into service. You make adjustments to the size of the VHD in the Hyper-V Manager by adding additional hard drives to the VM.

Prerequisites

Before starting this task, ensure that the virtual machine is switched off.

Procedure

1. Open the Hyper-V Manager.In the left pane, right-click on the virtual machine you need to edit and select **Settings**. The Settings dialog box for the virtual machine opens.
2. In the left pane, under **Hardware**, select any IDE Controller item. The Hard Drive settings open in the right pane.
3. Select the **Hard Drive** option in the right panel and click **Add**.



Settings for exinda-v7.4.2-4118-x86_64 on HYPERV-2012-R2

IDE Controller

You can add hard drives and CD/DVD drives to your IDE controller.

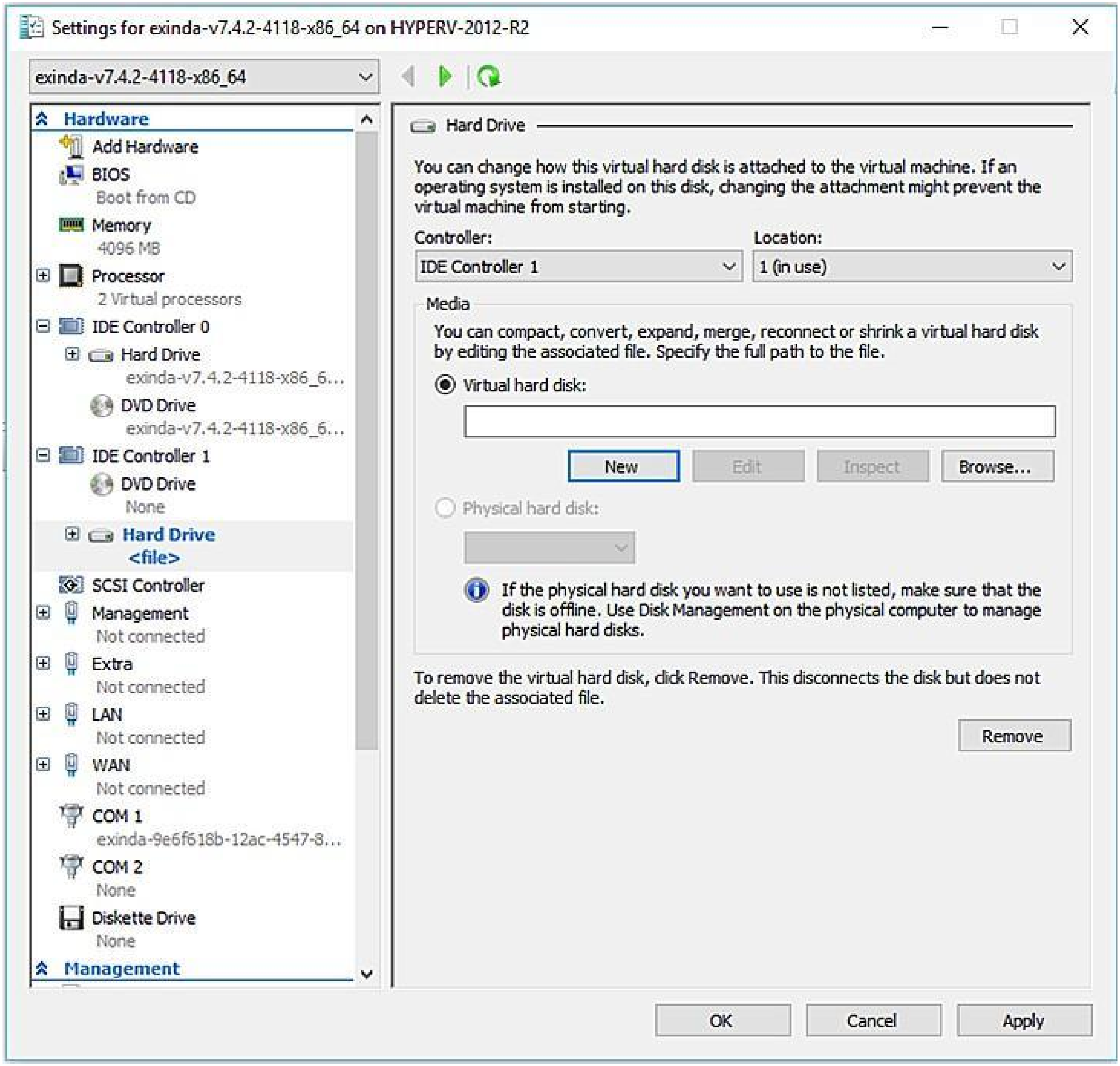
Select the type of drive you want to attach to the controller and then click Add.

Hard Drive

DVD Drive

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

4. In the Hard Drive section, select “IDE Controller 1” as the Controller and “1 (in use)” as the location. By default, this is the only slot available in the virtual machine to which to insert a new Virtual Hard Drive. However, if more hard drives are needed in the future, you could remove the DVD Drives present by default given that these are not needed in the appli- ance. In such a case, Controller 0: Location 1 and Controller 1: Location 0 will also be available for further use.



Settings for exinda-v7.4.2-4118-x86_64 on HYPERV-2012-R2

exinda-v7.4.2-4118-x86_64

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  4096 MB
- Processor
  2 Virtual processors
- IDE Controller 0
  - Hard Drive
    exinda-v7.4.2-4118-x86_6...
  - DVD Drive
    exinda-v7.4.2-4118-x86_6...
- IDE Controller 1
  - DVD Drive
    None
  - **Hard Drive**
    <file>
- SCSI Controller
- Management
  Not connected
- Extra
  Not connected
- LAN
  Not connected
- WAN
  Not connected
- COM 1
  exinda-9e6f618b-12ac-4547-8...
- COM 2
  None
- Diskette Drive
  None

Management

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 1

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

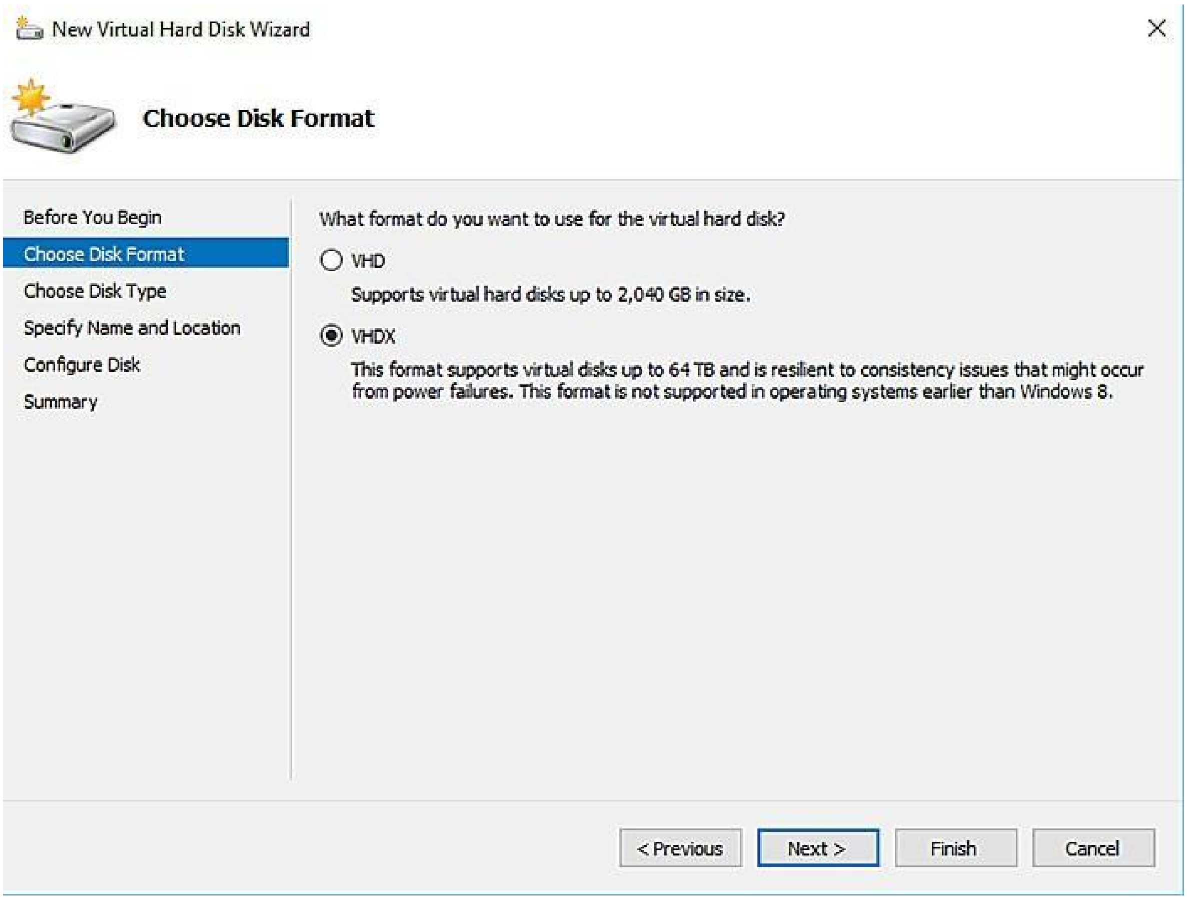
● Virtual hard disk:

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

5. Click **New**. The New Virtual Hard Disk wizard opens.


New Virtual Hard Disk Wizard

Choose Disk Format

What format do you want to use for the virtual hard disk?

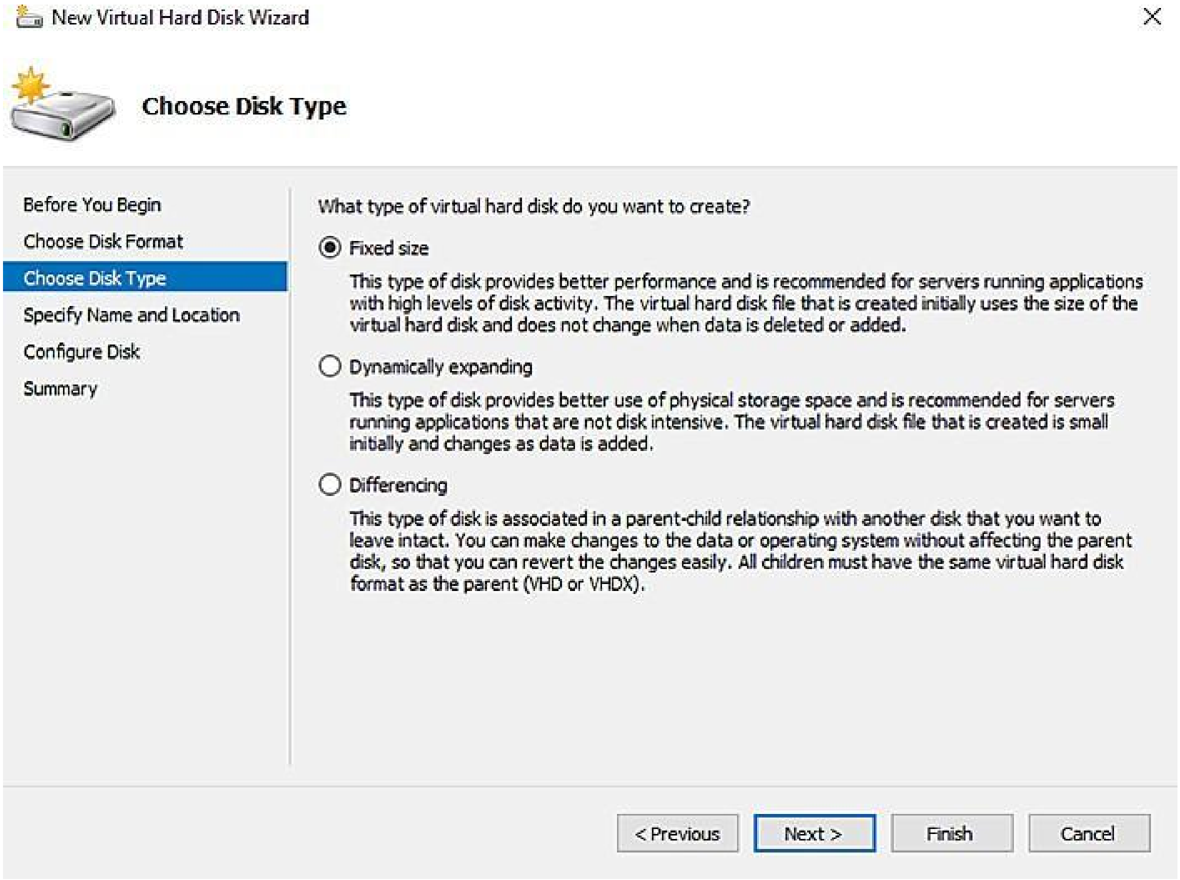
○ VHD

Supports virtual hard disks up to 2,040 GB in size.

● VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows 8.

6. Select VHDX as the Disk Format type and click **Next**.


New Virtual Hard Disk Wizard

Choose Disk Type

What type of virtual hard disk do you want to create?

● Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

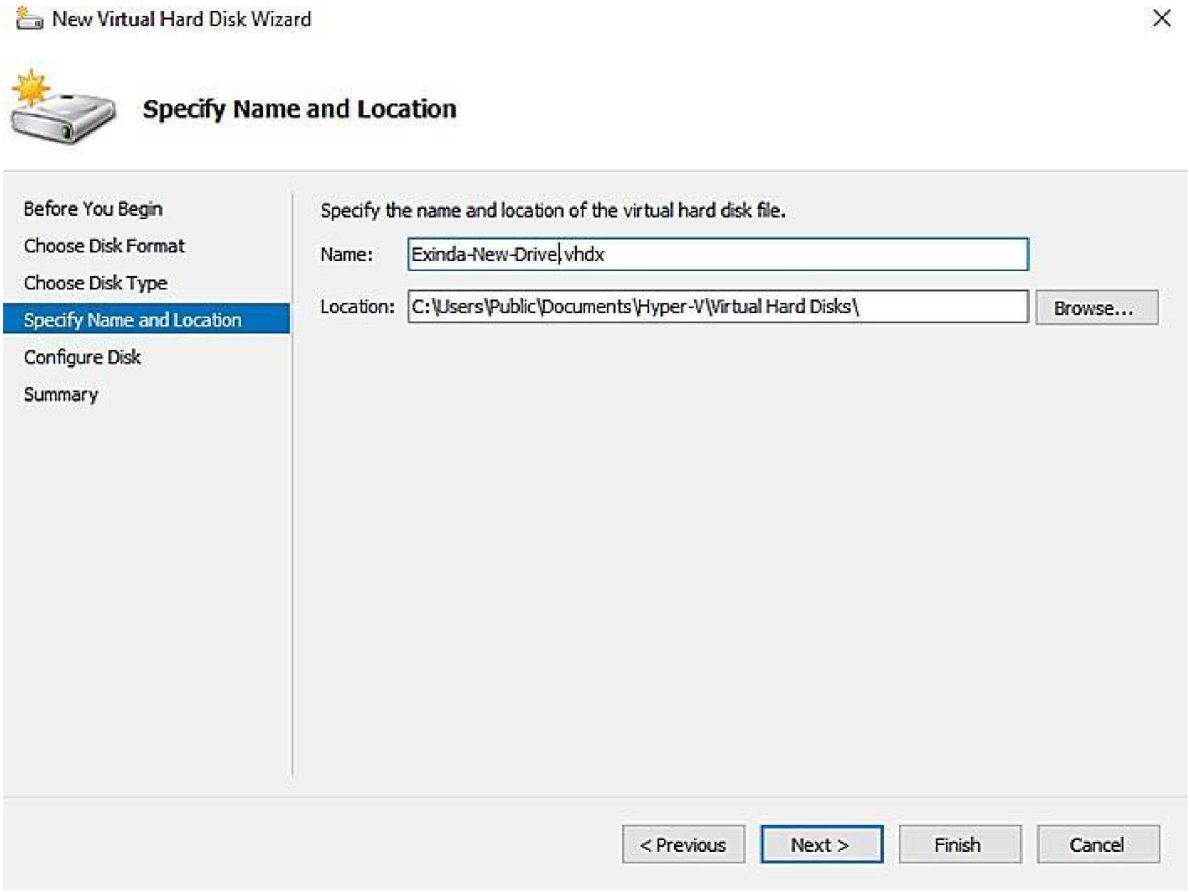
○ Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

○ Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

7. In the **Choose Disk Type** section, select the **Fixed Size** option and click **Next**.


New Virtual Hard Disk Wizard

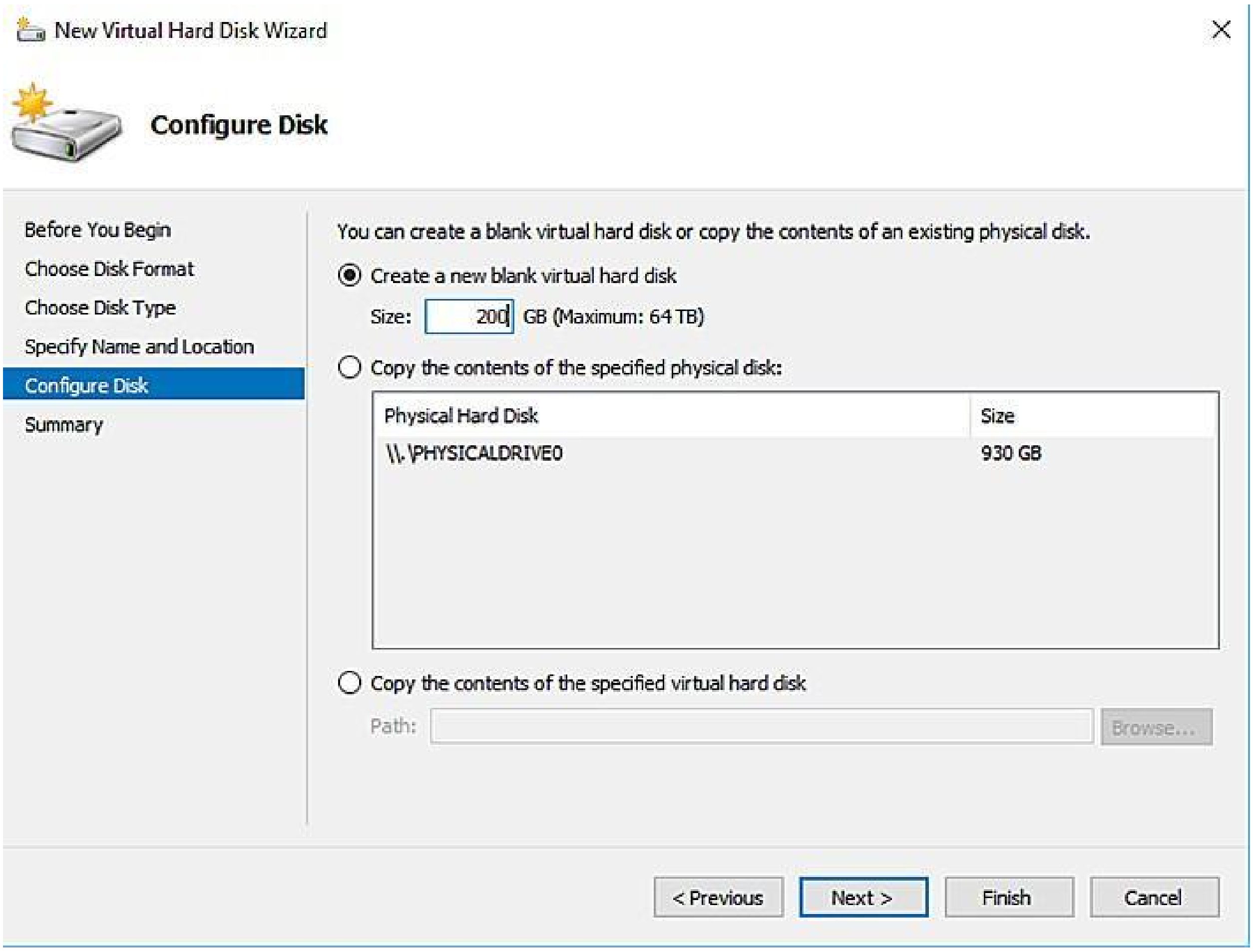
Specify Name and Location

Specify the name and location of the virtual hard disk file.

Name: Exinda-New-Drive.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

8. Specify a **Name** and **Location** for the virtual hard drive, and click **Next**.


New Virtual Hard Disk Wizard

Configure Disk

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

● Create a new blank virtual hard disk

Size: 200 GB (Maximum: 64 TB)

○ Copy the contents of the specified physical disk:

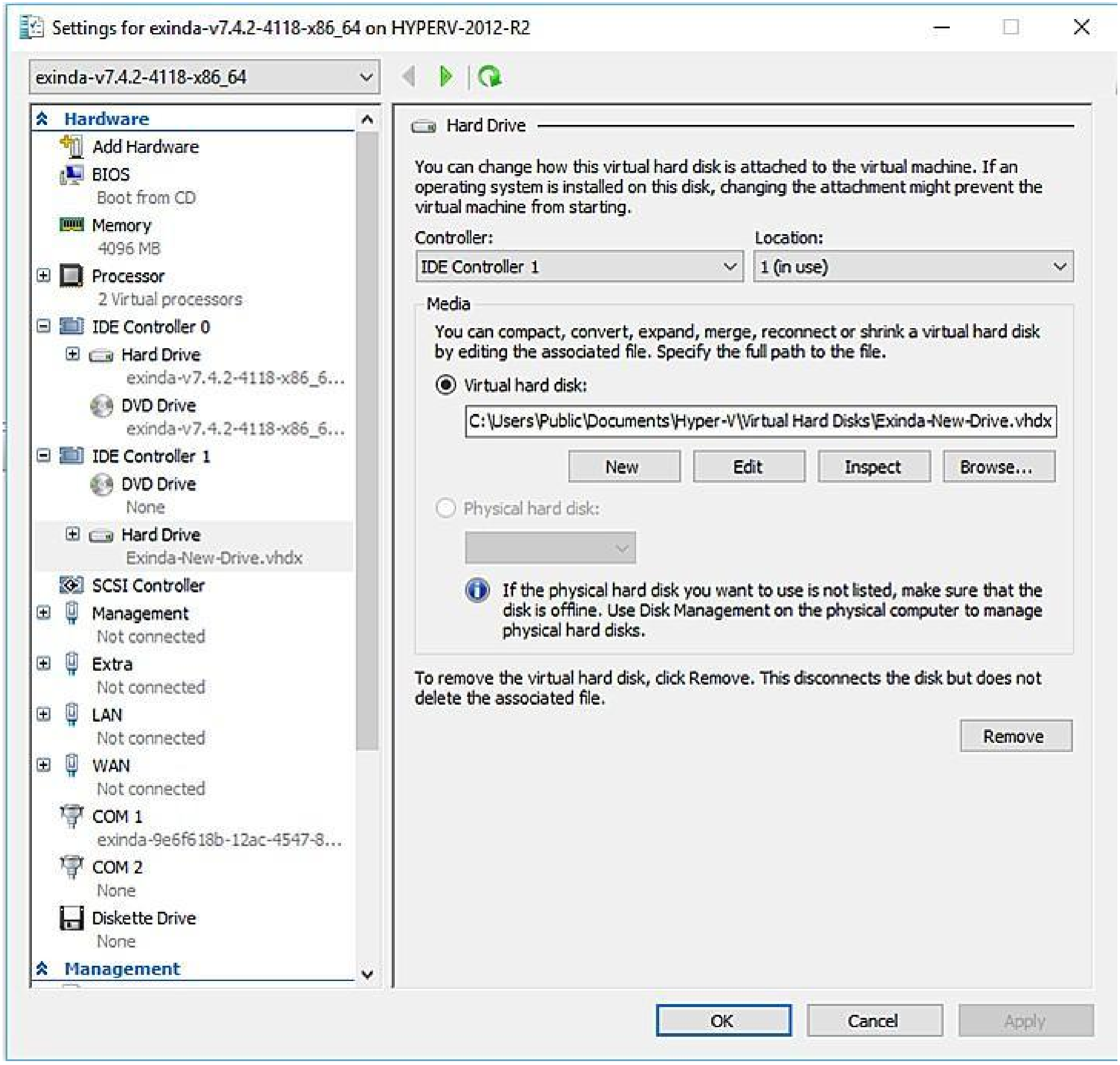
Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	930 GB

○ Copy the contents of the specified virtual hard disk

Path:

9. Set the **Disk Size** then click **Next**.

10. Click **Finish** to create the hard drive. This can take a few minutes.



Settings for exinda-v7.4.2-4118-x86_64 on HYPERV-2012-R2

exinda-v7.4.2-4118-x86_64

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 1

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\Exinda-New-Drive.vhdx

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

11. When the Hard Drive settings page for the newly created drive opens, click **OK**.

12. Start the virtual machine. When the VM starts, it will automatically recognize the new drive, but the new storage must be manually added the virtual appliance.

NOTE

Before connecting, the management interface must already have been configured with an IP address or will obtain an IP address using DHCP. You need to make sure that the Management Interface is connected to the proper Virtual Switch in your Hyper-V environment.

13. Find the IP address assigned to the management interface by right-clicking on the VM and selecting the **Connect** option. This provides console access.

14. Log on to the appliance using the default credentials (username: admin, password: exinda). You might need to accept the EULA before proceeding.

15. Apply the following commands. The output contains the IP address you need to access the appliance web user interface.

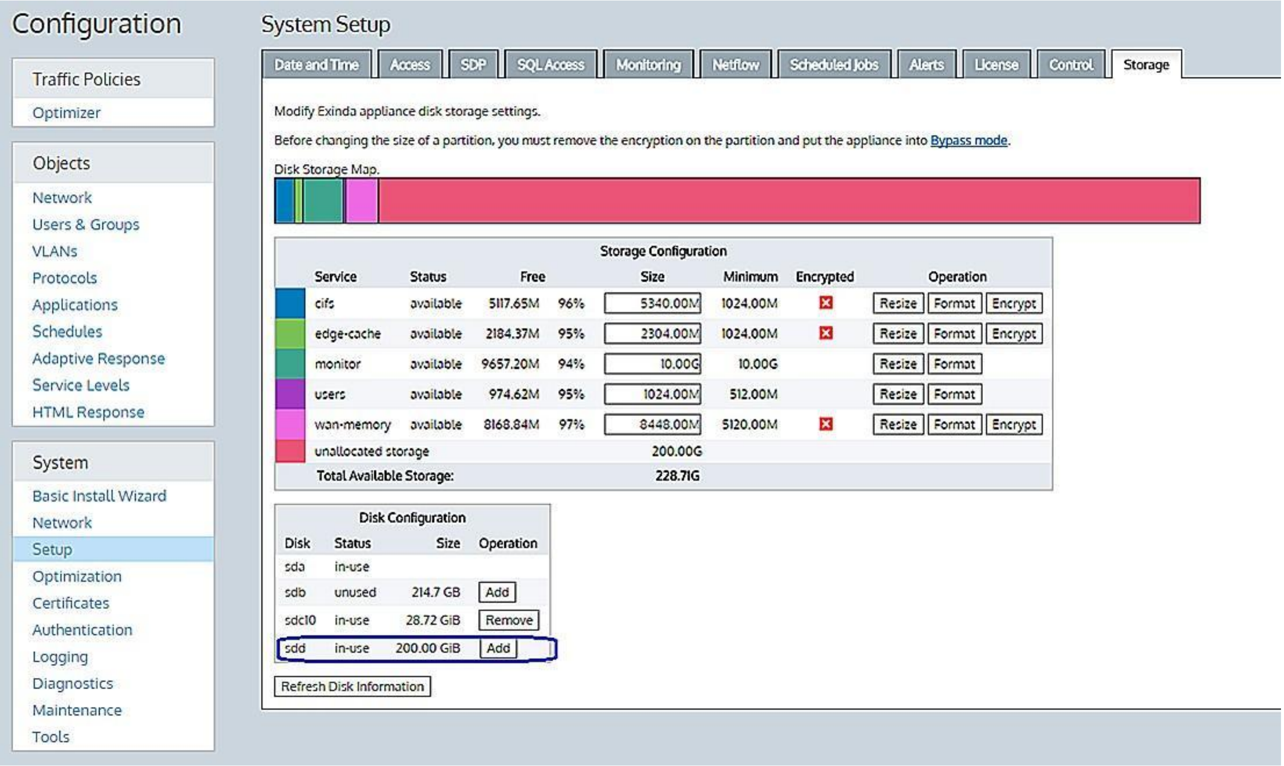
```
exinda> en
exinda># show int eth0
```

16. Connect through HTTPS to the GFI ClearView appliance using a browser.

17. Once logged on, click **Configuration > System > Setup > Storage**.

18. Add the new drive.

> **NOTE**
>
> The following screenshot assumes that the chosen controller was **1**, and the location was **0**, so the new drive is **sdd**.



Modify Exinda appliance disk storage settings.

Before changing the size of a partition, you must remove the encryption on the partition and put the appliance into Bypass mode.

Storage Configuration

	Service	Status	Free		Size	Minimum	Encrypted	Operation
🟦	cifs	available	5117.65M	96%	5340.00M	1024.00M	☒	Resize Format Encrypt
🟩	edge-cache	available	2184.37M	95%	2304.00M	1024.00M	☒	Resize Format Encrypt
🟩	monitor	available	9657.20M	94%	10.00G	10.00G		Resize Format
🟪	users	available	974.62M	95%	1024.00M	512.00M		Resize Format
🟪	wan-memory	available	8168.84M	97%	8448.00M	5120.00M	☒	Resize Format Encrypt
🟥	unallocated storage				200.00G			
	Total Available Storage:				228.71G			

Disk Configuration

Disk	Status	Size	Operation
sda	in-use		
sdb	unused	214.7 GB	Add
sdc10	in-use	28.72 GiB	Remove
sdd	in-use	200.00 GiB	Add

The new space appears as “unallocated storage” inside the “Storage Configuration” section.

19. Allocate the storage as appropriate.

2.2.8 Related Topics

Customizing a Hyper-V Virtual Machine

As supplied, the GFI ClearView Virtual Appliances will require some configuration changes before you introduce them to your network. For example, the virtual hard drives are limited to 50GB, which would be unlikely to be sufficient for your needs. The virtual machines available are sized with minimal configuration as it is not possible to know just what hardware is available on any host machine. To edit the configuration, you need to open the settings for the virtual machine in the Hyper-V Manager.

There are many settings that you can change, but for the purposes of configuring the GFI ClearView Virtual Appliance, these task instructions are limited to what is necessary for bringing the appliance into an operational state. If you need more information, please consult the documentation for Hyper-V. This topic deals with changes to the configuration related to the number of CPUs, the available RAM, the NICs, and adjusting the storage for the virtual machine.

The configuration changes are required before your initial use of the virtual machine. You can also make further changes to your virtual machine at any later time. If over time you require more resources for the virtual machine, as long as those resources are available on the host, you can make them available to the guest.

2.2.9 Creating an initial configuration using the Basic Wizard

The initial configuration wizard steps you through configuring the appliance's interfaces, IP settings, HTTP proxy settings, basic system information, license information, and storage volume. It also provides the option to upgrade the firmware and create the initial set of traffic policies.

1. The GFI ClearView appliance by default picks up an IP Address from DHCP. The IP address is available on the management interface.

Note: If a DHCP address is not picked up, the GFI ClearView appliance defaults to the IP Address 172.14.1.57. Open a web browser and connect to the Web User Interface by typing https://172.14.1.57 in the address field. To connect, configure the IP address of your PC to the same subnet as the GFI ClearView appliance. For example, set your IP address to 172.14.1.58, netmask 255.255.255.0.

2. From a web browser go to the following website http://findmy.exinda.com/. This will download an applet and automatically find the recently installed GFI ClearView.

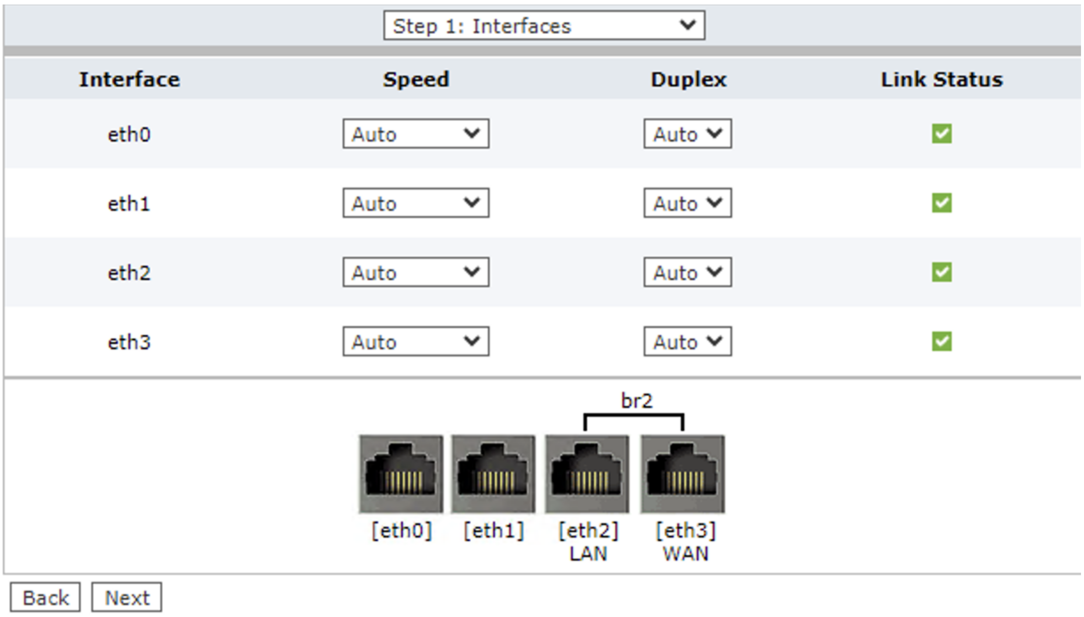
Note: The applet at findmyexinda.com uses a multicast packet to find local GFI ClearView appliances. The PC running the applet must be on the same physical LAN for the applet to work.

3. Click on the GFI ClearView appliance that has been found.

4. Login with **username=admin** and **password=exinda**.

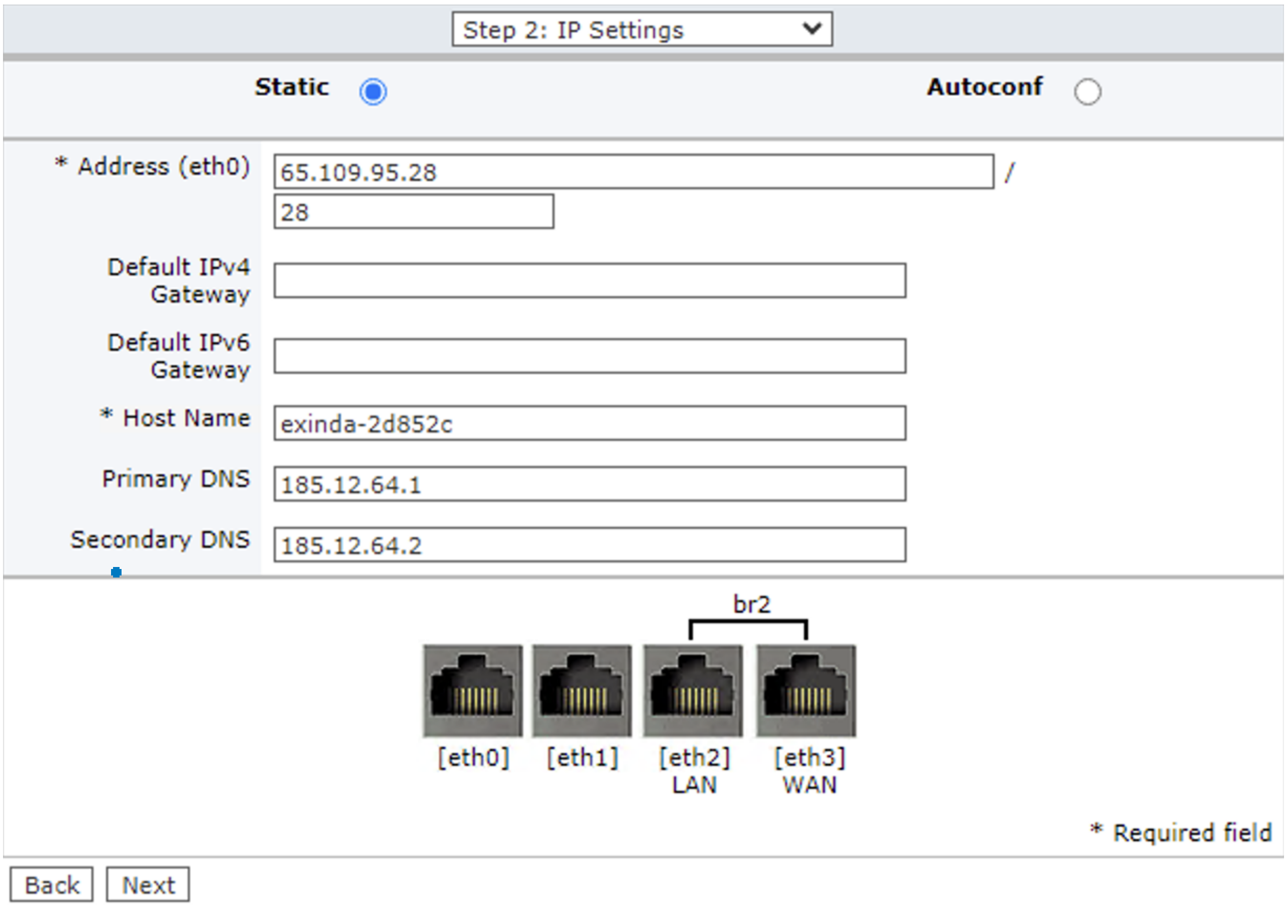
5. Select **Configuration**> **Basic Install Wizard** to start the configuration wizard .

    - **Basic Wizard Step 1 - Interfaces**: This screen lists all the system interfaces, as well as reports any problem with the interfaces. You can set interface speed and duplex settings from this screen.



Interface	Speed	Duplex	Link Status
eth0	Auto	Auto	✓
eth1	Auto	Auto	✓
eth2	Auto	Auto	✓
eth3	Auto	Auto	✓

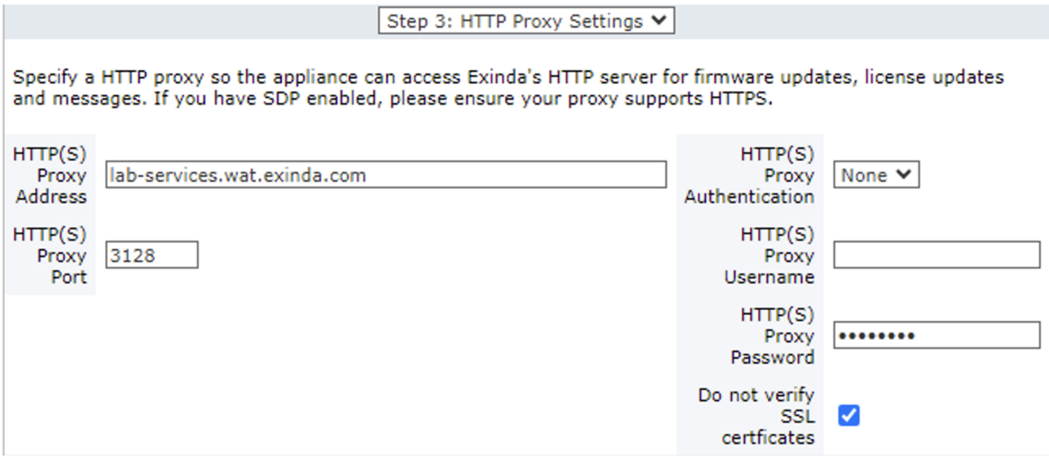
Basic Wizard Step 2 - IPSettings: This screen allows you to configure basic network connectivity settings. You can either manually specify these settings or select **Autoconf** to automatically acquire these settings. The type of auto configuration selected depends on your network. For IPv4 networks select **DHCP**, for IPv6 use **SLAAC**.



Static ● Autoconf ○

* Address (eth0)	65.109.95.28 / 28
Default IPv4 Gateway	
Default IPv6 Gateway	
* Host Name	exinda-2d852c
Primary DNS	185.12.64.1
Secondary DNS	185.12.64.2

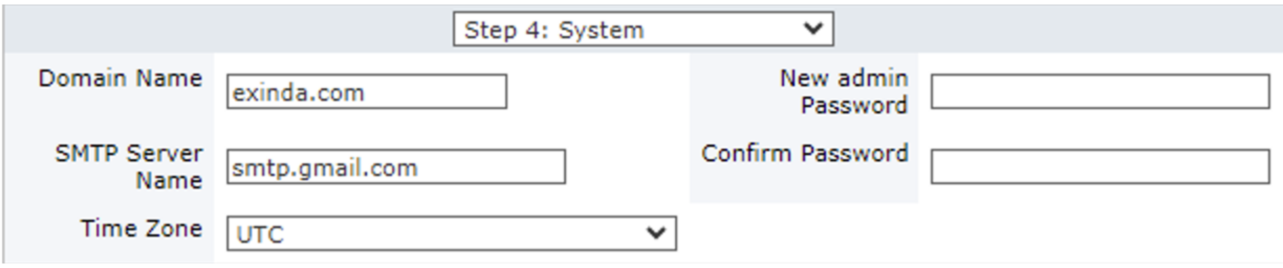
Basic Wizard Step 3 - HTTPProxy Settings: To allow the appliance to access GFI ClearView's HTTP server for firmware updates, license updates, and messages, specify an HTTP proxy. If you have SDP enabled, ensure your proxy supports HTTPS.



Specify a HTTP proxy so the appliance can access Exinda's HTTP server for firmware updates, license updates and messages. If you have SDP enabled, please ensure your proxy supports HTTPS.

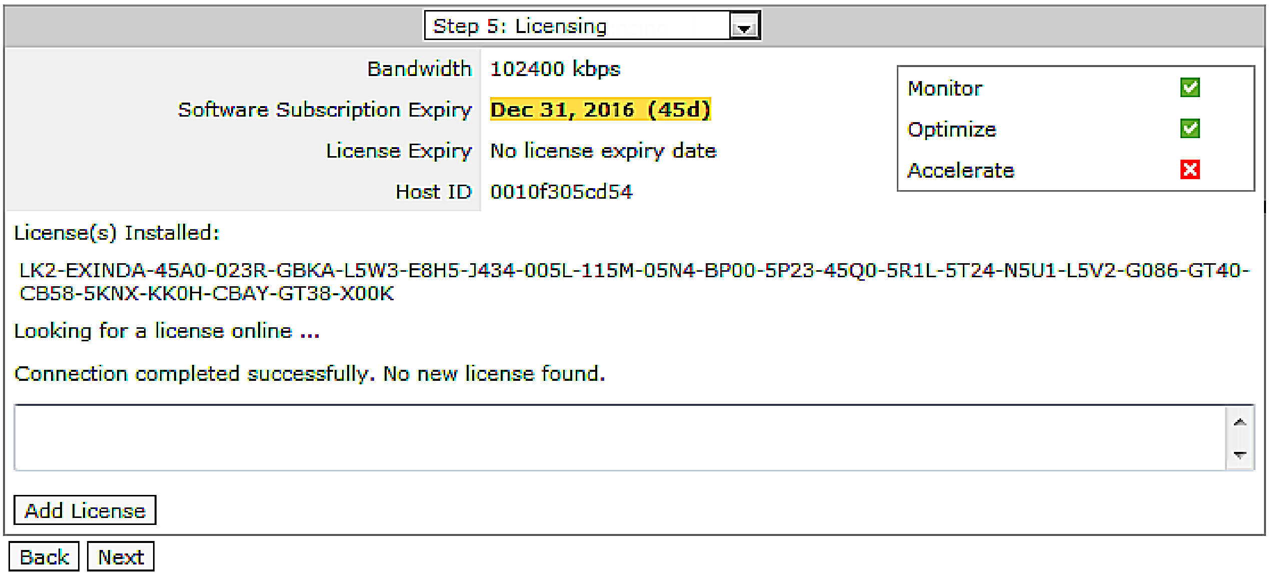
HTTP(S) Proxy Address	lab-services.wat.exinda.com	HTTP(S) Proxy Authentication	None
HTTP(S) Proxy Port	3128	HTTP(S) Proxy Username	
		HTTP(S) Proxy Password	••••••••
		Do not verify SSL certficates	☑

- **Basic Wizard Step 4 - System**: This screen allows to configure basic system settings.



Domain Name	exinda.com	New admin Password	
SMTP Server Name	smtp.gmail.com	Confirm Password	
Time Zone	UTC		

- **Basic Wizard Step 5 - Licensing**:This screen allows you to configure the system's license. When you enter the screen, the GFI ClearView appliance attempts to contact the GFI ClearView licensing server on the Internet. If the appliance has Internet connectivity and a new or updated license can be found, it is displayed in the text-box at the bot- tom of the screen. You can add this license to the system by clicking the **Add License** button.



Bandwidth	102400 kbps
Software Subscription Expiry	Dec 31, 2016 (45d)
License Expiry	No license expiry date
Host ID	0010f305cd54

Monitor	☑
Optimize	☑
Accelerate	☒

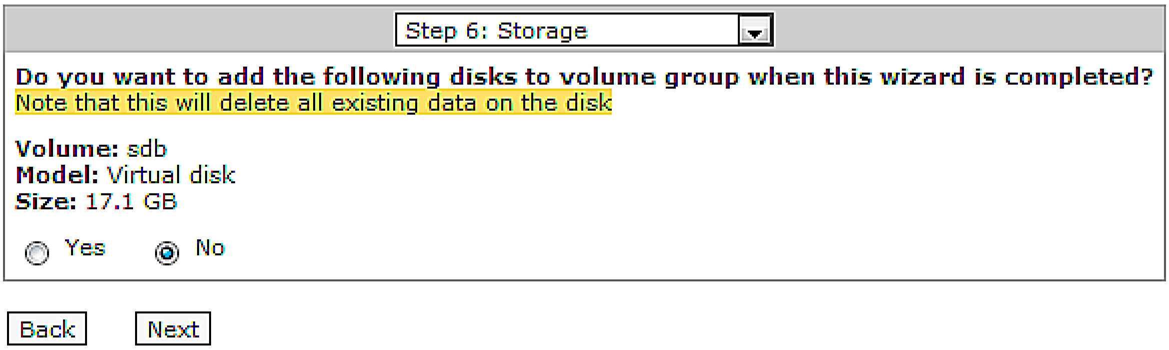
License(s) Installed:

LK2-EXINDA-45A0-023R-GBKA-L5W3-E8H5-J434-005L-115M-05N4-BP00-5P23-45Q0-5R1L-5T24-N5U1-L5V2-G086-GT40-CB58-5KNX-KK0H-CBAY-GT38-X00K

Looking for a license online ...

Connection completed successfully. No new license found.

- **Basic Wizard Step 6 - Storage**: This screen displays the available disks that can be added to the volume group.



Do you want to add the following disks to volume group when this wizard is completed?
Note that this will delete all existing data on the disk

Volume: sdb
Model: Virtual disk
Size: 17.1 GB

○ Yes ● No

- **Basic Wizard Step 7 - Firmware**: This screen displays the status of the firmware running on the GFI ClearView appli- ance. If the appliance has Internet connectivity, the system checks for any newer firmware that may have been released. If a newer firmware image is available, you are asked if you want to download and install it.

3 Using

This topic focuses on the day-to-day use of your GFI ClearView Appliance like setting alerts, monitoring performance, monitoring traffic, and understanding solutions and recommendations.

3.1 Defining a network environment

One of the first things you do after connecting an GFI ClearView to your network, is define how the GFI ClearView sees your network and its components.

As an analogy, imagine walking around your office or data center and placing sticky notes on all the servers, cables and racks to identify them and note what they do. That's essentially what you do when you define objects in GFI ClearView.

There are a variety of object types available, representing almost every physical, virtual and logical network component in your environment.

3.1.1 Adding network objects

Network objects represent hosts on a network and can include subnets, single hosts, or groups of both. Once defined, a network object may be used throughout the GFI ClearView Appliance for monitoring purposes.

Network objects are in the configurations of other objects, such as applications, adaptive response rules, application performance score objects, and application performance metric objects.

Network objects are also used to determine which traffic is considered inbound to your network and which traffic is outbound.

The location of a network object determines the direction of traffic. If one end of the conversation is defined in an external network object and the other is defined in an internal network object, then traffic from an external network object to an internal network object is considered inbound traffic.

Conversely, traffic from an internal network object to an external network object is considered outbound traffic.

You can indicate whether you want to report on the traffic relative to the network object, that is chart the traffic in and out of a given network object.

Adding network objects in the GFI ClearView Web UI

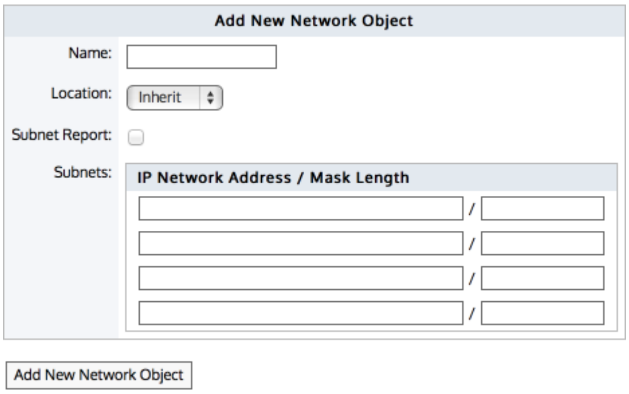
By checking the Subnet Report checkbox, the data for the network object will be shown on the subnet monitor page. This setting only affects the display of the data. The data will be collected regardless of this setting.

Some network objects are automatically created by the appliance: **ALL**, **private net** and **local**

» **All**— Represents all traffic on the network. This network object is not editable and cannot be deleted.

» **private net**— Represents all possible non-routable, private IP addresses.

» **local**— Created when an IP address is assigned to one or more bridge interfaces.



Screenshot 49: Adding a new network object.

Where to configure it

Go to **Configuration > Objects> Network Object > Network Objects**.

To create a new network object

1. Specify a name for the network object.

2. Select the location of the network object - internal, external, or inherit Packets are matched to a network object, and the closest subnet within that network object determines the location. See examples below.

   - **Internal**— All subnets and hosts defined by the network object will be considered on the LAN side of the appliance.
   - **External**— All subnets and hosts defined by the network object will be considered to be on the WAN side of the appliance.
   - **Inherit**— The locations of the subnets and hosts defined by the network object is determined or inherited by closest match to other network objects.
     - If all the subnets in this network object are contained in other network objects that are internal, then the location of this network object will inherit the internal location.
     - Similarly, if all the subnets in this network objects are contained in other network objects that are external, then the location of this network object will inherit the external location.
     - If some subnets in this network object are contained in other internal network objects and some are contained in other external network objects, then the location of this network object will be mixed.

- If no network objects match, then the location defaults to external.

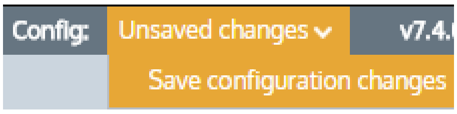
> **NOTE**
> When creating network objects that have location set to "inherit", you can use the CLI command `show network-object <name>` to show the location.

3. Select whether the traffic for this network object should be shown on the Subnet reports. See For more information, refer to Monitoring subnets.

4. Specify the network IP address and netmask length of the subnet. IPv4 and IPv6 addresses are accepted. Although only four lines for IP addresses are displayed for a new object, add more IP addresses by saving the network object and click **Edit** to be presented with an extra 4 lines.

5. Click **Add new Network Object**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



Examples of network object definitions

> **EXAMPLE – Network object defining two internal proxy servers**
> Create a network object that defines two internal proxy servers, 192.168.1.10 and 192.168.1.11:

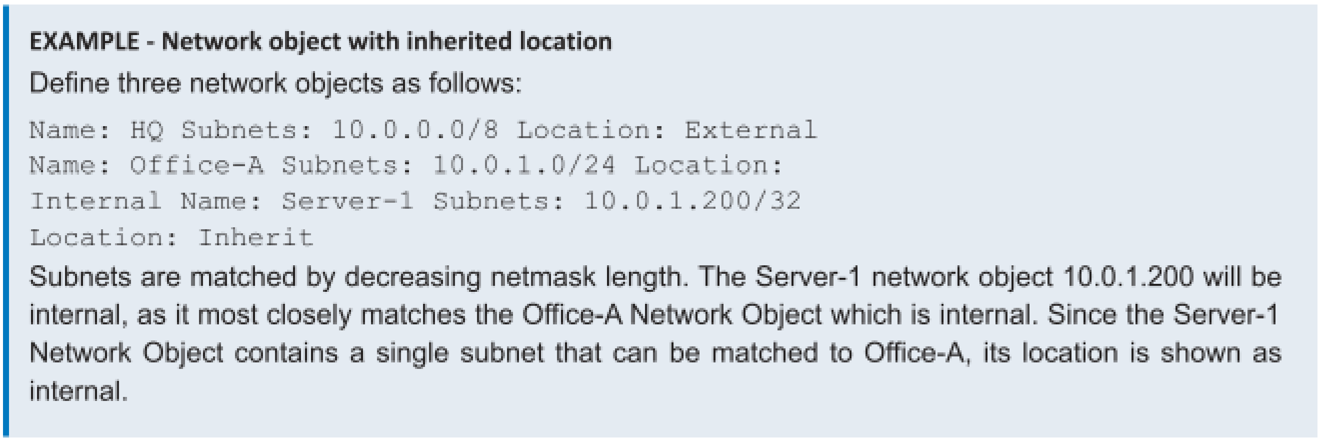
```
Name: Web Proxies
Location: Internal
Subnets: 192.168.1.10 /32
Subnets: 192.168.1.11 /32
```

> **EXAMPLE – Head office defining a network object for a remote branch**
> Create a network object that defines the Head Office location, that has a subnet 10.0.100.0/24, where this Exinda appliance is NOT deployed:

```
Name: Head Office
Location: External
Subnets: 10.0.100.0 /24
```

> **EXAMPLE – Network object defining an internal IPv6 server**
> Create a network object that defines the internal IPv6 server at 2001:db8::1234:5678

```
Name: FileServer6
Location: Internal
Subnets: 2001:db8::1234:5678 /128
```



EXAMPLE - Network object with inherited location

Define three network objects as follows:

```
Name: HQ Subnets: 10.0.0.0/8 Location: External
Name: Office-A Subnets: 10.0.1.0/24 Location:
Internal Name: Server-1 Subnets: 10.0.1.200/32
Location: Inherit
```

Subnets are matched by decreasing netmask length. The Server-1 network object 10.0.1.200 will be internal, as it most closely matches the Office-A Network Object which is internal. Since the Server-1 Network Object contains a single subnet that can be matched to Office-A, its location is shown as internal.

What about internal-to-internal or external-to-external traffic?

When the **Ignore Internal-to-Internal** option is set on the Monitoring configuration page, all traffic between network objects marked as internal is ignored and passed through the GFI ClearView appliance unaffected. See For more information, refer to Monitoring Configuration.

How to know whether a network object with location 'inherit' resolved to internal or external location?

You can use the CLI command to see what location the network object resolved to:

```
show network-object <name>
```

Creating Network Objects based on FQDN?

It is possible to configure network objects using fully-qualified-domain-names instead of IP addresses. Should it later become necessary to change network settings on application servers, the GFI ClearView appliance can then automatically detect the change through DNS.

To configure a network object based on a fully qualified domain name, use the following commands:

```
>en #conf t(config) # network-object <NAME> fqdn <fully qualified
domain name>
```

An GFI ClearView appliance must be configured with a DNS server if it is to perform name resolution using FQDN. Each record retrieved has a life cycle equal to the TTL (Time to live) defined for such a record. When the TTL is exceeded, GFI ClearView automatically refreshes the record to verify that the IP address has not changed. When appliance reboots occur, or changes to DNS configuration, interface configurations, or link states on any interface, this causes an automatic refresh of the network object. Should you need to perform a refresh, you can use the following command:

```
(config) # network-object <NAME> refresh
```

When the TTL is lower than 5 minutes, GFI ClearView waits the full five minutes before attempting a refresh in order to avoid DNS flooding.

3.1.2 Working with users and groups as objects

Users and groups objects are used to define pre-populated users and groups such that they can be used for monitoring and optimization.

There are two ways the GFI ClearView Appliance can learn about user and group information:

1. Active Directory: The GFI ClearView Appliance can receive user and group information using the GFI ClearView Active Directory Ser- vice, installed on Active Directory Servers.

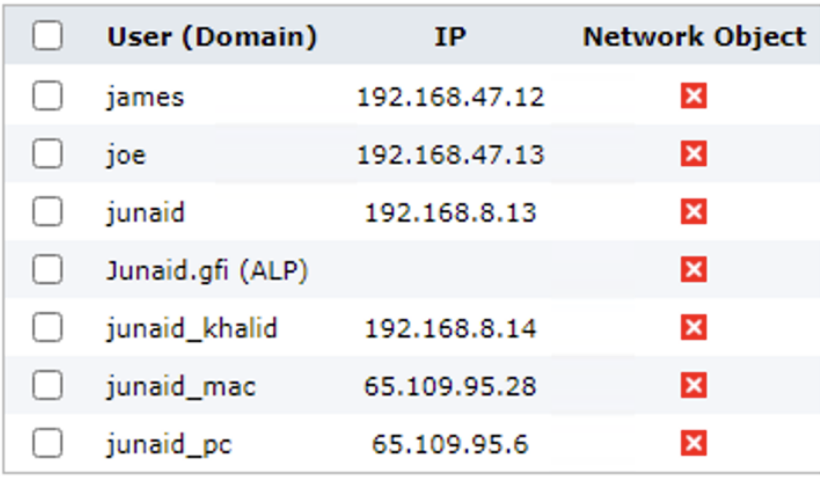
2. Static Users and Groups: Static users and group information can be only entered using the CLI "network user" command.

Once the appliance has learned about users and groups, you can use the users and groups pages to define which users and groups to expose as Dynamic Network Objects, for use in monitoring and optimization.

- To define users as Dynamic Network Objects, see Create Network User Objects.
- To define groups as Dynamic Network Objects, see Create Network Group Objects.

Defining network user objects

The Network Users page displays a pre-populated list of users (and their associated IP addresses) from either the GFI ClearView AD Connector, or from static users entered using the CLI. Select which individual users you want to define as dynamic network objects.



□	User (Domain)	IP	Network Object
□	james	192.168.47.12	☒
□	joe	192.168.47.13	☒
□	junaid	192.168.8.13	☒
□	Junaid.gfi (ALP)		☒
□	junaid_khalid	192.168.8.14	☒
□	junaid_mac	65.109.95.28	☒
□	junaid_pc	65.109.95.6	☒

Screenshot 56: A list of network users displayed on the Network Users page.

Defining and removing users as dynamic network objects

Use the following instructions to define users as dynamic network objects and to stop identifying them as necessary. The instructions focus on dealing with one user at a time, but you can define or remove many users by selecting multiple checkboxes.

1. Go to Configuration > Objects> Users& Groups> Network Users.

2. Find the user in the listing.

> **TIP**
>
> If you have many users, use the links at the top of the page to help find the user.

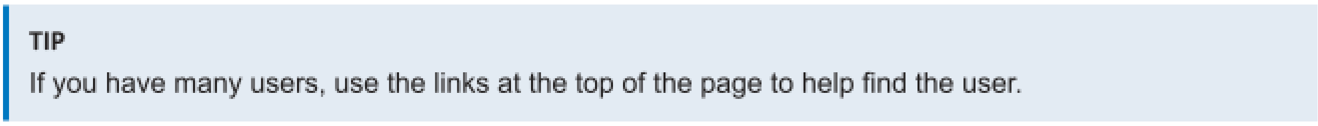
3. Select the checkbox for the user.

4. At the bottom of the page, click **Add Network Object**. The Network Status icon for the user changes to ☑, indicating it is a network object.

To stop identifying (remove) a user as a dynamic network object

1. Go to Configuration > Objects> Users& Groups> Network Users.

2. Find the user in the listing.



TIP

If you have many users, use the links at the top of the page to help find the user.

3. Select the checkbox for the user.

4. At the bottom of the page, click **Remove Network Object**. The Network Status icon for the user changes to ☒, indicating it is no longer a network object.

Configuring network user group objects

The Network Groups page displays a pre-populated list of groups from either the GFI ClearView AD Connector, or from static groups entered using the CLI. This page allows you to select which groups you want to define as dynamic network objects.

Defining and removing user groups as dynamic network objects

To define a group as a dynamic network object

Use the following instructions to define a user group object.

1. Go to Configuration > Objects> Users& Groups> Network Groups

2. Find the group in the list, and click **Edit**.

3. To map all users within the selected network group to the network object, select **Map to Network Object**.

4. Select **Ignore Domain** to exclude the domain prefix.

5. Click **Apply**. The Network Status icon for the group changes to ☑, which indicates it is now a network object. If the dynamic network object is created from multiple groups, the groups are combined into a single entry and each domain is identified after the group name.

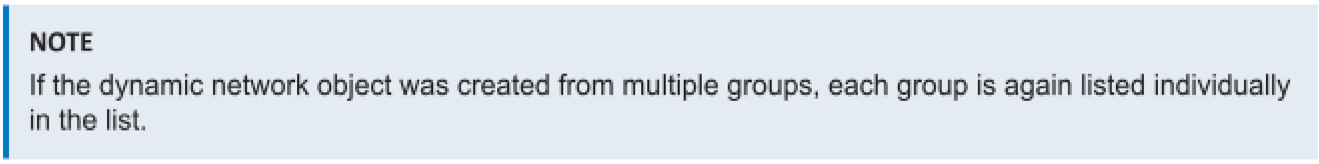
To remove a group as a dynamic network object

1. Go to Configuration > Objects> Users& Groups> Network Groups

2. Locate the group in the list, and click **Edit**.

3. Clear the **Map to Network Object** checkbox.

4. Click **Apply**. The Network Status icon for the user group changes to ☒, which indicates it is no longer a network object.



NOTE

If the dynamic network object was created from multiple groups, each group is again listed individually in the list.

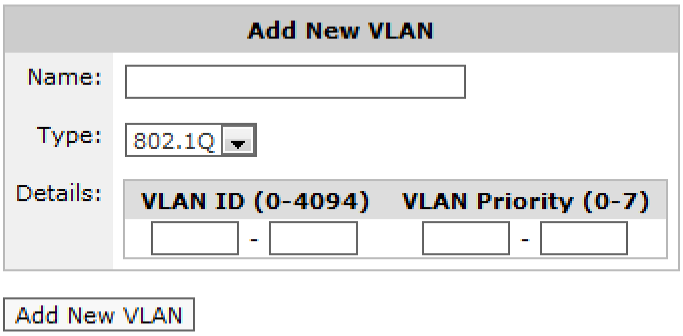
3.1.3 Configuring VLAN objects

Virtual LAN (VLAN) objects are used to logically separate hosts (or groups of hosts) on a functional basis rather than on a physical basis.

Configuring VLAN objects in the GFI ClearView Web UI

By default, the GFI ClearView Appliance has a single VLAN defined called "ALL", which matches all traffic (regardless if that traffic is part of a VLAN or not). Additional VLAN Objects can easily be added.

All the defined VLAN objects are shown in the table. Each VLAN object can be edited or deleted by clicking the appropriate button in the table. The **ALL** VLAN object is protected and cannot be edited or deleted.



Add New VLAN

Name:

Type: 802.1Q

Details:

VLAN ID (0-4094)	VLAN Priority (0-7)
-	-

Screenshot 57: Adding a new VLAN.

To add a new VLAN object:

1. Go to Configuration > Objects> VLANs.

2. Enter a meaningful name for the VLAN object.

3. Specify the type of VLAN to define. Currently only 802.1Q VLANs are available.

4. Specify the range of VLAN IDs to define. To define all VLAN IDs, leave this field blank or type 0 - 4094. A single VLAN ID can be defined by entering the same value in both fields.

5. Specify the VLAN Priority range to define. To define all VLAN Priorities, leave this field blank or type 0 - 7. A single VLAN Priority can be defined by entering the same value in both fields.

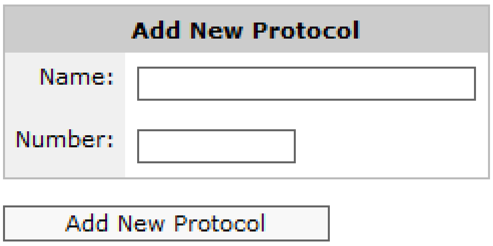
6. Click the **Add New VLAN** button. The VLAN will be added to the list of VLANs in the table.

3.1.4 Adding protocol objects

Protocol objects are used to define IPv4 protocol numbers that can then be used to define application objects. By default, the appliance factory setting includes all major Internet Protocol (IPv4) related protocols, including ICMP (Internet Control Message Protocol), TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Additional IPv4 protocols can easily be added by simply specifying IPv4 protocol number.

> **NOTE**
>
> Protocol numbers are unique and can only be defined once.

All the defined protocol objects are shown in the table. Each protocol object can be edited or deleted by clicking the appropriate button in the table. Some protocols are protected and cannot be edited or deleted.



Screenshot 58: Adding a new protocol.

To configure protocol objects:

1. Go to Configuration > Objects> Protocols.
2. Enter a meaningful name for the protocol.
3. In the **Number** field, specify the IPv4 protocol number.
4. Click the **Add New Protocol** button. The protocol will be added to the list of protocols in the table.

> **EXAMPLE**
>
> Consider where SCTP (Stream Control Transport Protocol) is undefined by default and need to be defined.
>
> ```
> Name: SCTP
> Number:
> 132
> ```

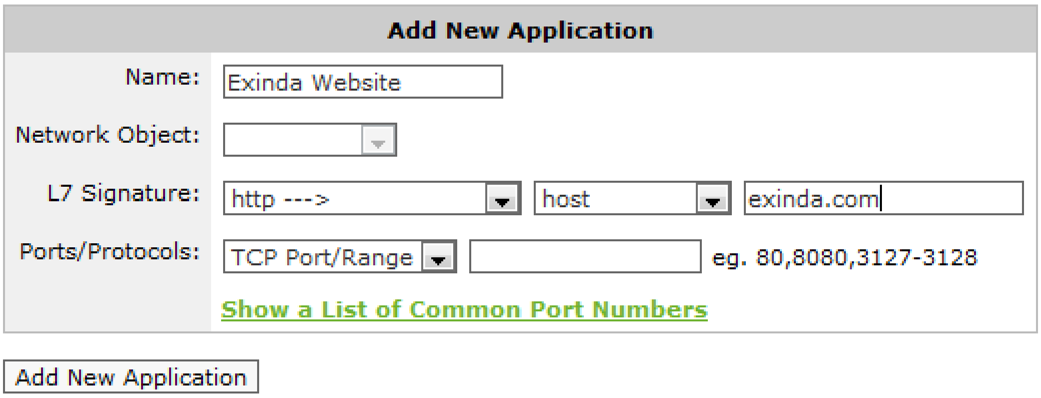
3.1.5 Adding application objects

Application objects are used to classify traffic on the network and are made up of layer 7 signatures or TCP/UDP port numbers and port ranges. Application classification can be used to monitor traffic or to create application-specific policy. There are many predefined applications on the appliance. You can add any applications that are not already in the list.

Applications can be created from various combinations of L7 signatures, TCP/UDP port numbers or ranges, and network object. The following are valid combinations.

- Applications based on L7 signatures. For example, you can create an application for a particular website by selecting http, host, and entering the domain of the website.
- Applications based on L7 signature and TCP/UDP port numbers or ranges, which are OR'd together. For example, you could define HTTP based on TCP port 80 OR 'http' L7 signature.
- Applications based on network object and TCP/UDP port numbers or ranges, which are added together. For example, you could define an application based on a particular port number on a particular server (specified by network object).
- Applications based on only network object. For example, you could define an application based on a particular application server (specified by network object).
- Applications based on only TCP/UDP port number or ranges. For example, you could create an application based on a particular port.

Network objects cannot be used in conjunction with a layer 7 signature.


Add New Application

Name:	Exinda Website
Network Object:	
L7 Signature:	http ---> · host · exinda.com
Ports/Protocols:	TCP Port/Range · eg. 80,8080,3127-3128

Screenshot 59: Adding a new application object.

> **NOTE**
>
> When creating applications based on ports, any given port number can only be defined once for TCP and once for UDP. The same port number can be defined for TCP and UDP. For example, if you define an application object with a port range TCP 500-510, you cannot then define another application object on TCP port 505. However, you can define another application object with UDP port 505.
>
> You can define duplicate ports/port ranges if a network object is also specified.

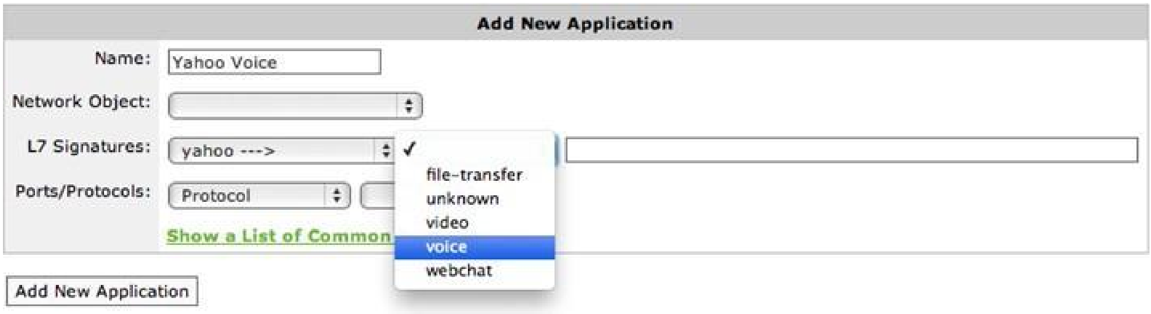
Many of the L7 signatures have sub-type classifications, which makes layer 7 visibility much more granular. For instance, for reporting on specific web applications, most vendors can only report on port 80 traffic. GFI ClearView allows a deeper look into Layer 7 applications. For example, by comparison:

- Layer 4 reporting tools report on web applications
- as: port 80 or HTTP Layer 7 reporting tools report

  on web applications as: Yahoo or Skype
- Layer 7 with subtype classification report on web applications as: Yahoo video, Yahoo voice, or Yahoo webchat.

This allows you to monitor at a much more granular level.

Adding application objects in the GFI ClearView Web UI



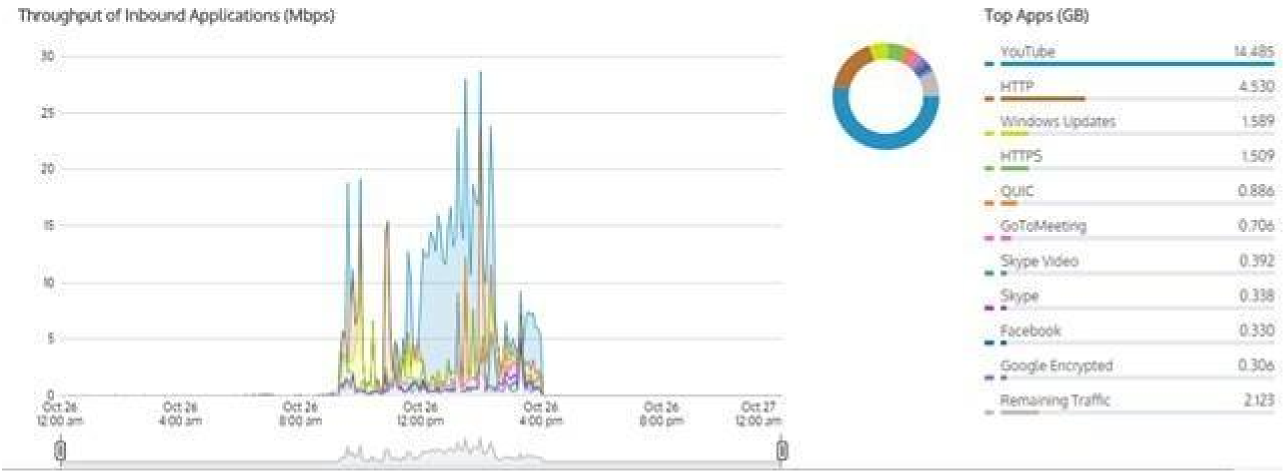
Add New Application

Name: Yahoo Voice

Network Object:

L7 Signatures: yahoo ---> ✓ voice

Ports/Protocols: Protocol



Screenshot 60: Chart displaying bandwidth throughput for applications.

3.1.6 Adding and updating application group objects

To properly classify applications on your network it is important to understanding what is happening and for controlling or protecting a particular type of traffic.

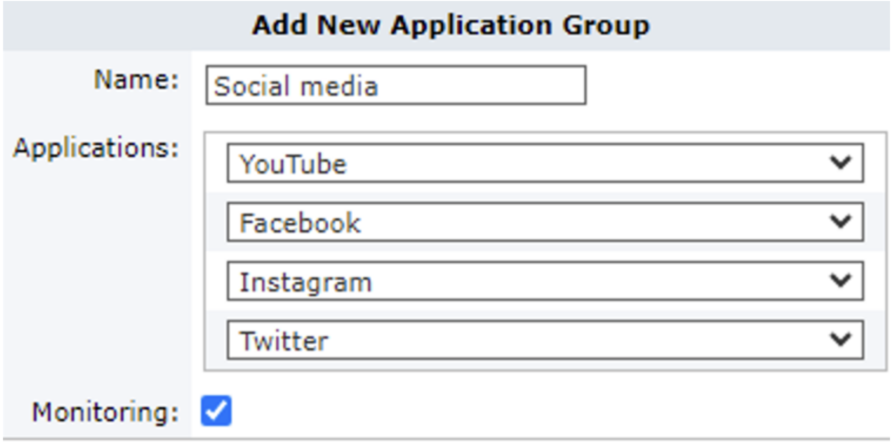
The GFI ClearView Appliance comes with a long list of predefined applications used to classify your network traffic. If, however, you want to create your own application, you can create new applications based on L7 signatures, TCP/UDP port numbers and port ranges, or network objects.

You may also want to monitor, control, or protect your traffic by grouping a set of applications. For instance, controlling social networking applications as a group in most cases provides adequate granularity. The GFI ClearView Appliance comes with a default set of application groups. You can add new applications to these groups, or create new groups, or delete existing groups.

There are several predefined application groups, such as Mail, P2P, Voice, etc. You can edit existing application groups or create new ones.

> **NOTE**
> A given application can exist in multiple application groups. However, monitored groups must not contain applications which are already a member of another group being monitored. Any given application can only be monitored within a single application group.

Adding application group objects in the GFI ClearView Web UI



Add New Application Group

Name: Social media

Applications: YouTube, Facebook, Instagram, Twitter

Monitoring: ☑

Screenshot 61: Adding a new application group.

To add a new application group

1. Go to Configuration > Objects> Applications> Application Groups.

2. In the **Add New Application Group** area type a name for the new group.

3. Select the applications that belong in the new group. By default, there are four drop-downs available to add Applic- ation Objects. If you need to add more, save the application group object, then select the **Edit** button next to the newly created application group. You will be presented with four additional drop-downs to add more applications.

4. If you want this application group to be monitored in the Application Group report, select the **Monitoring** checkbox.

5. Click **Add New Application Group**.

To update an application group

1. Go to Configuration > Objects> Applications> Application Groups.

2. Locate the group from which to add or delete applications and click **Edit**.

3. Select a new application from a blank drop-down list. Or to remove an application, open the drop-down list with the application to remove and select the blank row at the top.

4. Click **Apply Changes**.

What application groups are predefined?

For more information, refer to Predefined Application Groups.

3.1.7 Configuring anonymous proxy detection and monitoring

Anonymous proxies are typically used to circumvent security policies, allowing users to access prohibited recreational, adult or other non-business sites by tunneling this traffic over a regular or encrypted HTTP session. Anonymous Proxies also provide anonymity; users accessing websites through an Anonymous Proxy cannot easily be traced back to their original IP.

GFI ClearView Appliances have built-in support for anonymous proxy detection. The GFI

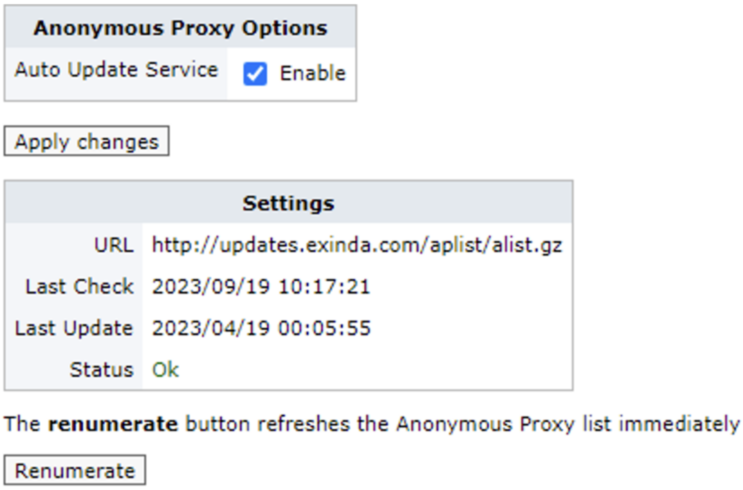
ClearView Appliance receives daily updates containing updated anonymous proxy definitions, much like anti-virus applications receive daily threat updates.

The anonymous proxy application is a special application object that is used to detect anonymous proxy websites and services. However, the anonymous proxy service is disabled by default.

If the anonymous proxy service is enabled, the GFI ClearView appliance fetches a list of anonymous proxy definitions from the GFI web servers on a daily basis.

An application object called 'Anonymous Proxy' is automatically created. The Anonymous Proxy application tracks all traffic sent through one of the anonymous proxies in the list. This application object is displayed in the monitoring reports like any other application object.

> **NOTE**
>
> » Anonymous Proxy classification only occurs if the Anonymous Proxy ASAM module is enabled on the **Configuration > System > Setup > Monitoring** page.
>
> » In order to receive daily Anonymous Proxy definition updates, the GFI ClearView appliance must be able to contact the GFI web servers and the appliance must also have a valid software subscription.



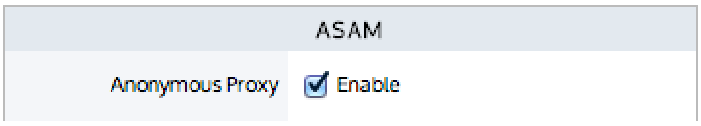
Anonymous Proxy Options

Auto Update Service ☑ Enable

Settings	
URL	http://updates.exinda.com/aplist/alist.gz
Last Check	2023/09/19 10:17:21
Last Update	2023/04/19 00:05:55
Status	Ok

The **renumerate** button refreshes the Anonymous Proxy list immediately

Screenshot 62: The form to enable the Anonymous Proxy service to keep a list of anonymous proxy sites.



ASAM

Anonymous Proxy ☑ Enable

Screenshot 63: The form to enable/disable the Anonymous Proxy ASAM required for classification.

Where to configure it

- To enable the anonymous proxy service, go to **Configuration > Objects> Applications>**
- **Anonymous Proxy**. To enable the anonymous proxy traffic classification, go to

  Configuration > System > Setup > Monitoring.

To enable the anonymous proxy traffic classification

1. Check the Auto Update Service **Enable** checkbox. The appliance will communicate with the GFI web servers daily and fetch any new anonymous proxy definitions.

2. Ensure that the Anonymous Proxy ASAM module is enabled by going to the **Configuration > System > Setup > Monitoring** page and ensuring the **Anonymous Proxy** checkbox is checked in the **ASAM** section. The Anonymous Proxy ASAM is **on** by default. The appliance will classify traffic by matching the traffic against the anonymous proxy list.

To see when the appliance last updated the anonymous proxy definitions

1. Look at the **Settings** section.

2. The **Last Check** field indicates the last time that the appliance checked the GFI service for new anonymous proxy definitions.

3. The **Last Update** field indicates the last time new anonymous proxy definitions were found and updated.

To force a check of the anonymous proxy definitions

Click the **Renumerate** button. The appliance will check the GFI web servers immediately to check for new anonymous proxy information.

To disable the anonymous proxy traffic classification

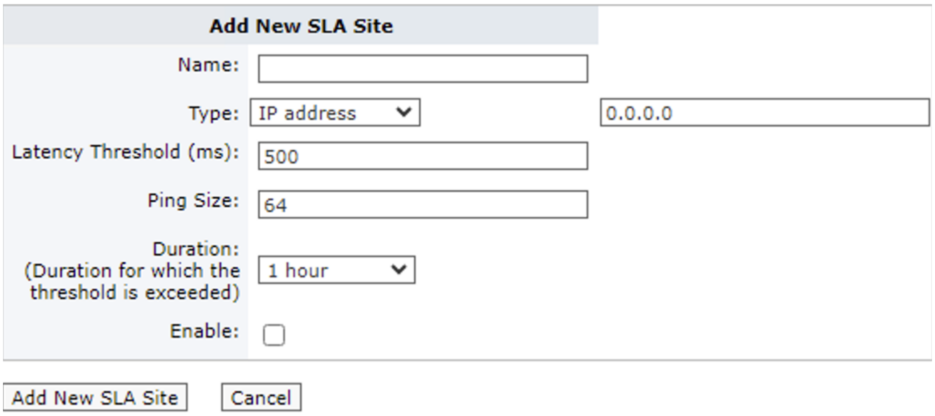
1. Uncheck the Auto Update Service **Disable** checkbox.

2. Disable the Anonymous Proxy ASAM by going to the **Configuration > System > Setup > Monitoring** page, uncheck- ing the **Anonymous Proxy** checkbox in the **ASAM** section, and clicking the **Apply Changes** button. Disabling the ASAM will clear the existing anonymous proxy definitions.

3.1.8 Configuring service level agreement objects

The Service Level Agreement (SLA) objects are used to monitor the availability of a particular IP site. By creating a SLA object, you indicate which IP site to monitor. The GFI ClearView appliance will send one ICMP ping every 10 seconds to the IP address. You can specify the ping packet size to use. You can also specify when an alert will be triggered by specifying the ping latency threshold and the duration that the ping latency threshold was exceeded. An alert is triggered when the latency of the SLA site exceeds the latency threshold for longer than the specified duration.

Configuring service level agreement objects in the GFI ClearView Web UI



Add New SLA Site

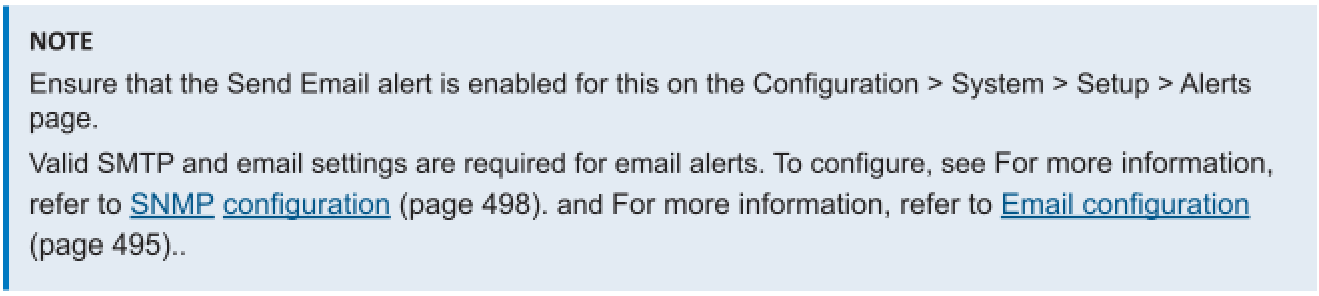
Name:		
Type:	IP address	0.0.0.0
Latency Threshold (ms):	500	
Ping Size:	64	
Duration: (Duration for which the threshold is exceeded)	1 hour	
Enable:	□	

Screenshot 64: Adding an SLAsite.

To access this configuration, go to **Configuration > Objects> Service Levels> Service**

Level Agreements. To create a Service Level Agreement (SLA) object:

1. Click the **Add New SLA Object** button.
2. Type a name for the SLA object.
3. Type a IP address in the **Destination IP** field that will be pinged.
4. Type the **Latency Threshold**(in ms), such that you want to be notified if this threshold is consistently exceeded. The default is 500 milliseconds.
5. Enter the ping packet size (in bytes) to use in the **Ping Size** field.The default is 64 bytes.
6. Select the duration, that is the amount of time that the latency threshold needs to be exceeded before the alert is sent. The options are:
   - 30 seconds
   - 60 seconds
   - 5 minutes
   - 30 minutes
   - 1 hour (Default)
   - 0 - (Disable), which disables the alert.
7. Select the **Enable** checkbox to enable the SLA object to starting pinging the IP site.
8. Click the **Apply Changes** button. The object is added to the list of configured SLA objects.



NOTE

Ensure that the Send Email alert is enabled for this on the Configuration > System > Setup > Alerts page.

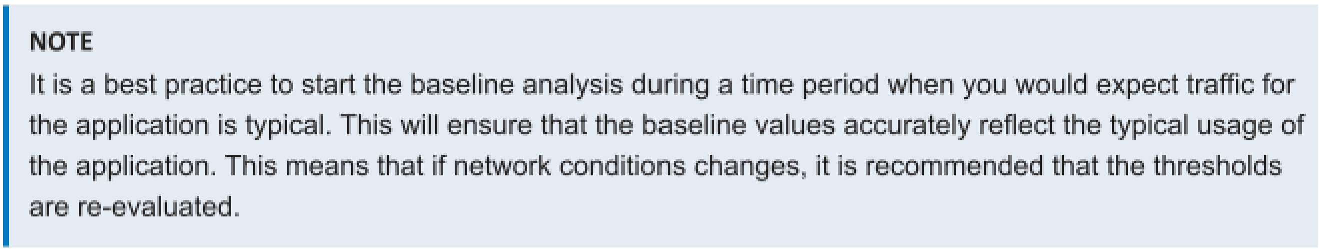
Valid SMTP and email settings are required for email alerts. To configure, see For more information, refer to SNMP configuration (page 498). and For more information, refer to Email configuration (page 495)..

3.1.9 Configuring application performance score objects

The application performance score (APS) object is used to assess how network users enjoy the network performance experience of business-critical applications. The score, ranging between 0 and 10, where 0 is poor and 10 is excellent, indicates whether the app is performing as well as expected or is performing poorly. By creating an APS object, you specify an application to monitor. Optionally, you can also specify a network object so that the application is only monitored when observed on that part of the network. You set thresholds on one or more network metrics. Later, traffic for that application is assessed against those thresholds to determine how well the application is performing.

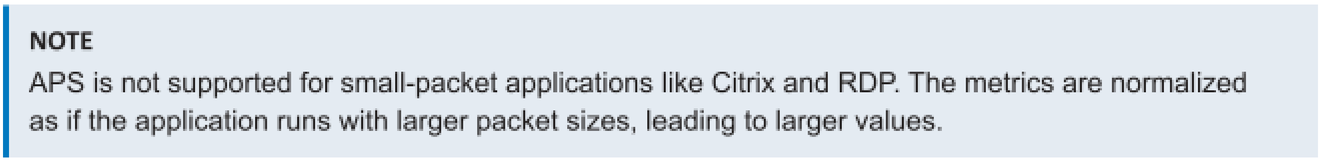
The appropriate thresholds for an application is unique for each network environment. You can manually set the thresholds for the network metrics or you can have the system automatically create threshold values by having the system observe traffic to determine reasonable baseline values. The metrics include network delay, server delay, round trip time, jitter, and network loss. Note that you can manually set the network loss metric, however, it will not be automatically be calculated during the baseline analysis. You can use one or more of these metrics in your APS object. Most applications use transactional protocols. Applications like Citrix XenApp server or Microsoft Remote Desktop use non-transactional protocols that send information between the client and server at arbitrary times. With these types of applications, the standard method of calculating the network delays and server delays does not produce an accurate metric. If the application uses a non-transactional protocol, you must specify that when creating APS object.

For the baselining analysis, traffic is analyzed during the specified period, and a set of metric thresholds is generated. The threshold recommendations target an APS of 8.5. If the application reports an APS below 8.5, the application is performing worse than the baseline. If no traffic is observed during the baselining period, then the appliance will automatically start another the baseline analysis for the next larger time period. Email will be sent for each unsuccessful baseline analysis.



NOTE

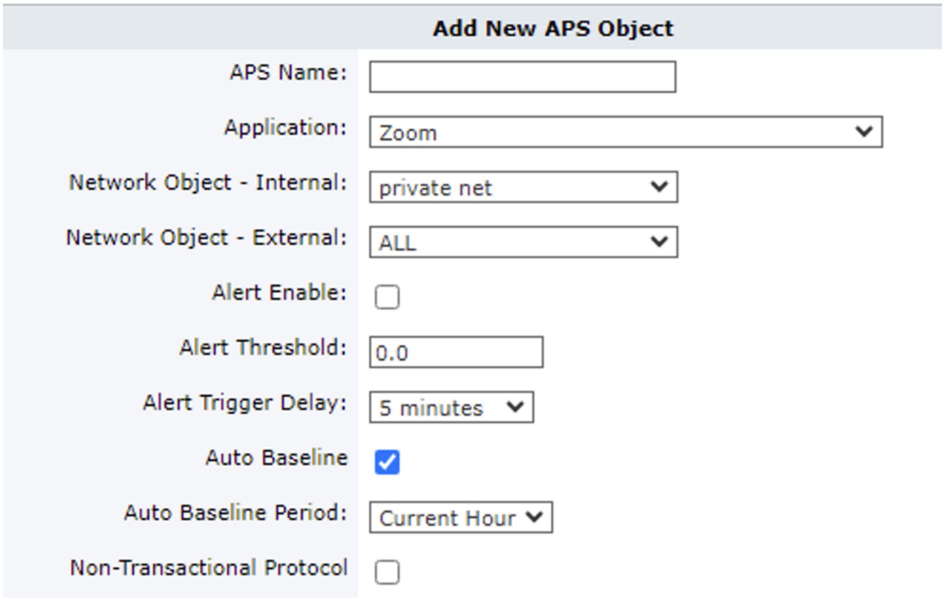
It is a best practice to start the baseline analysis during a time period when you would expect traffic for the application is typical. This will ensure that the baseline values accurately reflect the typical usage of the application. This means that if network conditions changes, it is recommended that the thresholds are re-evaluated.



NOTE

APS is not supported for small-packet applications like Citrix and RDP. The metrics are normalized as if the application runs with larger packet sizes, leading to larger values.

You can also set alerts so that you will be notified when the score drops below a certain threshold value. There is an alert trigger delay setting which requires that the score remains below the alert threshold for a specified period of time before triggering the alert. This prevents brief temporary poor scores from appearing like an emergency.

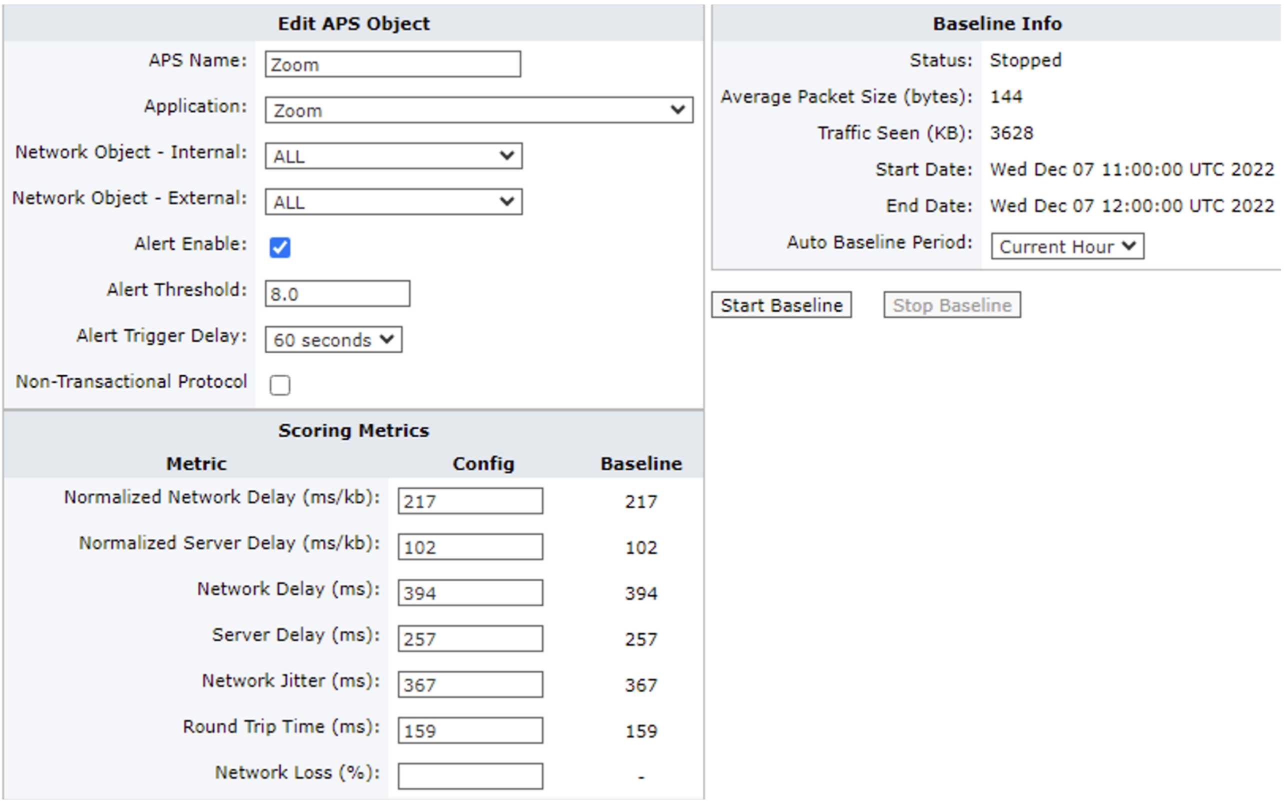


Add New APS Object

APS Name:	
Application:	Zoom
Network Object - Internal:	private net
Network Object - External:	ALL
Alert Enable:	□
Alert Threshold:	0.0
Alert Trigger Delay:	5 minutes
Auto Baseline	☑
Auto Baseline Period:	Current Hour
Non-Transactional Protocol	□

Screenshot 69: The form to add a new APS object.

When editing the APS object, you can modify the alert configuration, restart the baselining operation, and modify the threshold values. If you change the network object settings, it is recommended that you re-evaluate the metric thresholds and possibly re-start a baseline.



Edit APS Object

APS Name:	Zoom
Application:	Zoom
Network Object - Internal:	ALL
Network Object - External:	ALL
Alert Enable:	☑
Alert Threshold:	8.0
Alert Trigger Delay:	60 seconds
Non-Transactional Protocol	□

Scoring Metrics

Metric	Config	Baseline
Normalized Network Delay (ms/kb):	217	217
Normalized Server Delay (ms/kb):	102	102
Network Delay (ms):	394	394
Server Delay (ms):	257	257
Network Jitter (ms):	367	367
Round Trip Time (ms):	159	159
Network Loss (%):		-

Baseline Info

Status:	Stopped
Average Packet Size (bytes):	144
Traffic Seen (KB):	3628
Start Date:	Wed Dec 07 11:00:00 UTC 2022
End Date:	Wed Dec 07 12:00:00 UTC 2022
Auto Baseline Period:	Current Hour

Screenshot 70: Editing an APS object.

Creating an application performance score object

Use the instructions that follow to create a new APS object. During this set up, you can set a scope for the monitoring process. The scores can focus on specific internal and/or external network objects, or on ALL in one or both categories.

Before you begin…

- If you need to enable alerts, ensure that you have set Email on the **Configuration > System > Setup > Alerts** page.

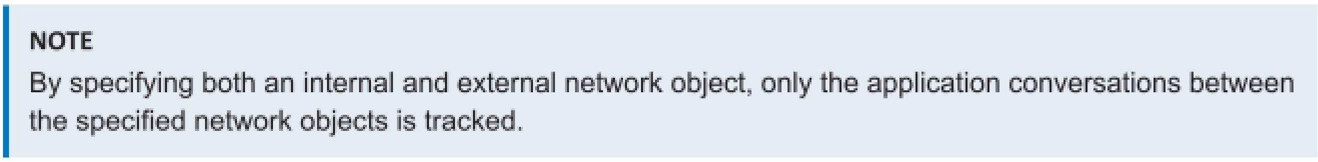
For more information, see the GFI ClearView Web UI help.

- You also need to set up SNMP on the **Configuration > System > Network> SNMP** page. for more information, see the GFI ClearView Web UI help.

Creating an application performance score object in the GFI ClearView Web UI

To create the object:

1. Go to Configuration > Objects> Service Levels> Application Performance Score.
2. Click the **Add New APS Object** button.
3. In the **APS Name** field, type a name for the score.
4. In the **Application** list, select the application traffic to monitor.
5. Open the **Network Object - Internal** drop-down and either select a specific network object or select ALL.
6. Open the **Network Object - External** drop-down and either select a specific network object or select ALL.



NOTE

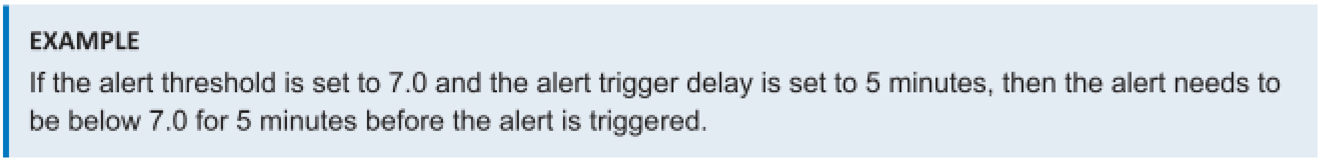
By specifying both an internal and external network object, only the application conversations between the specified network objects is tracked.

7. If you want to be alerted when the application performance score drops below a particular threshold, set the fol- lowing alert settings:

   a. Ensure the **Alert Enable** checkbox is selected.

   b. In the **APS Threshold** field, set a threshold value between 0 and 10.

   c. In the **Alert Trigger Delay** field, specify how many minutes that the APS score to be below the threshold before the notification is sent.



EXAMPLE

If the alert threshold is set to 7.0 and the alert trigger delay is set to 5 minutes, then the alert needs to be below 7.0 for 5 minutes before the alert is triggered.

8. If you need baselining to start immediately, select the **Auto Baseline** checkbox and select the **Auto Baseline Period**.

9. If the application uses a non-transactional protocol for traffic between the client and server, such as Citrix XenApp Servers or Microsoft Remote Desktop, select the **Non-Transactional Protocol** checkbox.

10. Click **Add New APS Object**. The object is added to the list of configured APS object

How performance metric thresholds are calculated

Network performance metrics are calculated based on the observed traffic. Each threshold is calculated to be 0.85 of a standard deviation above the average observation for that metric. This ensures that the calculated thresholds target is an APS of 9.0. If the application reports an APS below 9.0, the application is performing worse than the baseline.

Configuring APS thresholds manually

Metric thresholds can be set manually when initially creating the APS object or upon editing an APS object even if they were automatically determined by the baselining operation. For example, if the baselining operation set all of the thresholds and you really only care about round trip time, normalized server delay, and normalized network delay, then you can remove the threshold settings for the other metrics.

1. Go to Configuration > Objects> Service Levels> Application Performance Score.

2. On the **Add New APS Object** form, uncheck the **Auto Baseline** checkbox. Note if a baseline analysis is running, you'll need to press the **Stop Baseline** button. The threshold values are only editable if there is not a baseline running. The met- rics will appear on the screen. Or edit the APS object in the list, then on the **Edit APS Object** form, the **Scoring Metrics** appear at the bottom of the form.

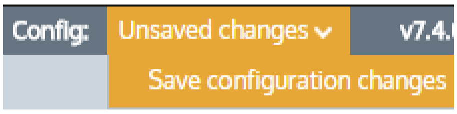
3. Enter or modify the values for the metrics that you are interested in setting thresholds for. Note that any metric that does not have a threshold set will not be analyzed when calculating the APS score.

- Network delay – the time taken for data to traverse the network (on the wire) in one direction from the client through the GFI ClearView appliance to the server (or in the opposite direction) in ms
- Server delay – the time taken for a server to respond to the request in ms
- Normalized network delay – the time taken for data to traverse the network in one direction, where the delay is measured independent of the transaction size by assuming a normalized packet size of 1024 bytes
- Normalized server delay – the time taken for a server to respond to the request, where the delay is measured independent of the transaction size by assuming a normalized packet size of 1024 bytes
- Round-trip time – the time taken for a packet to travel from a client through the GFI ClearView appliance to the server and back
- Jitter – the measure of variability of network delay, defined as one standard deviation of normalized network delay
- Inbound loss – the percentage of packet loss on
- inbound traffic Outbound loss – the percentage of

  packet loss on outbound traffic

4. Click **Apply Changes**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



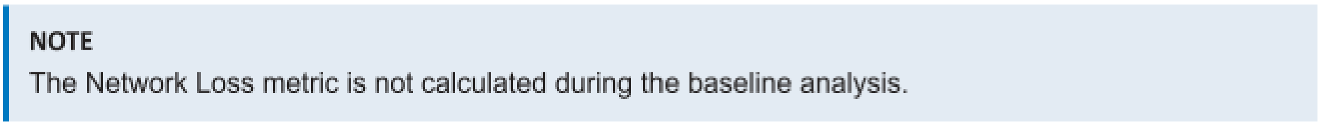
Configuring automatic APS threshold calculation

The baselining process can be started when initially creating the APS object or upon editing an APS object. At any time you can restart the baselining process if you would like the system to recalculate the thresholds.

1. Go to Configuration > Objects> Service Levels> Application Performance Score.

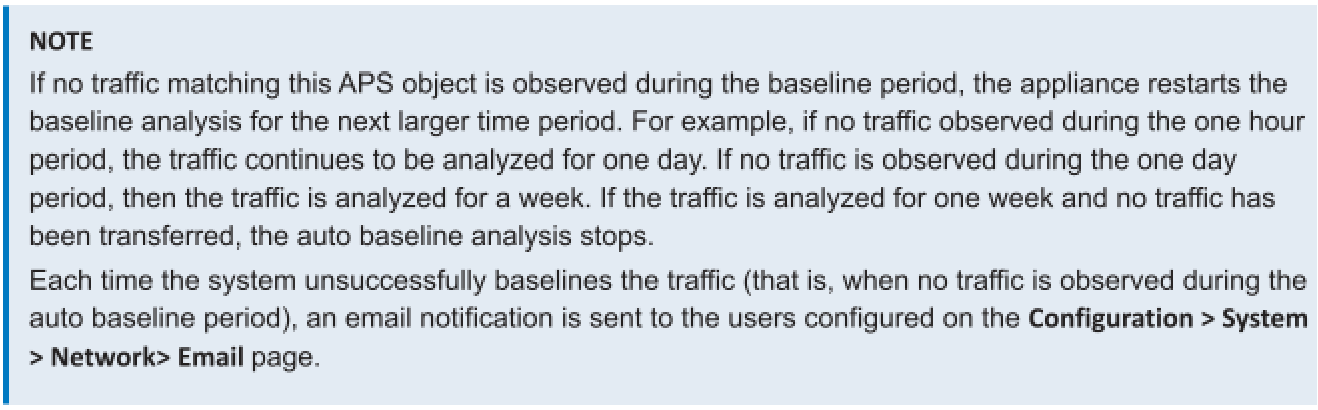
2. On the **Add New APS Object** form, ensure that the **Auto Baseline** checkbox is checked and set how long you want the system to observe traffic when calculating the thresholds by using the **Auto Baseline Period** drop-down list. Select the time period for the baseline based on how popular the application is. For example, if there is a lot of HTTP traffic on the network, the 1 hour period will be long enough to analyze traffic and create an accurate baseline. For an application that is not used very often, use the 1 week baseline period to ensure that enough traffic is analyzed to generate baseline recommendations.

3. Or on the **Edit APS Object** form, set the **Auto Baseline Period** and click **Start Baseline**.



NOTE

The Network Loss metric is not calculated during the baseline analysis.



NOTE

If no traffic matching this APS object is observed during the baseline period, the appliance restarts the baseline analysis for the next larger time period. For example, if no traffic observed during the one hour period, the traffic continues to be analyzed for one day. If no traffic is observed during the one day period, then the traffic is analyzed for a week. If the traffic is analyzed for one week and no traffic has been transferred, the auto baseline analysis stops.

Each time the system unsuccessfully baselines the traffic (that is, when no traffic is observed during the auto baseline period), an email notification is sent to the users configured on the **Configuration > System > Network> Email** page.

Checking if baselining is in progress

On the **Application Performance Score** configuration tab, the list of APS objects is shown. If the APS is currently baselining the application traffic, there will be a green checkmark in the **Auto Baseline** column.

Press the **Edit** button for the APS object. The **Baseline Info** section specifies the status (Running or Stopped) and the Start and End Date and time of the baseline period. Note that it also shows the average packet size and the amount of traffic seen.

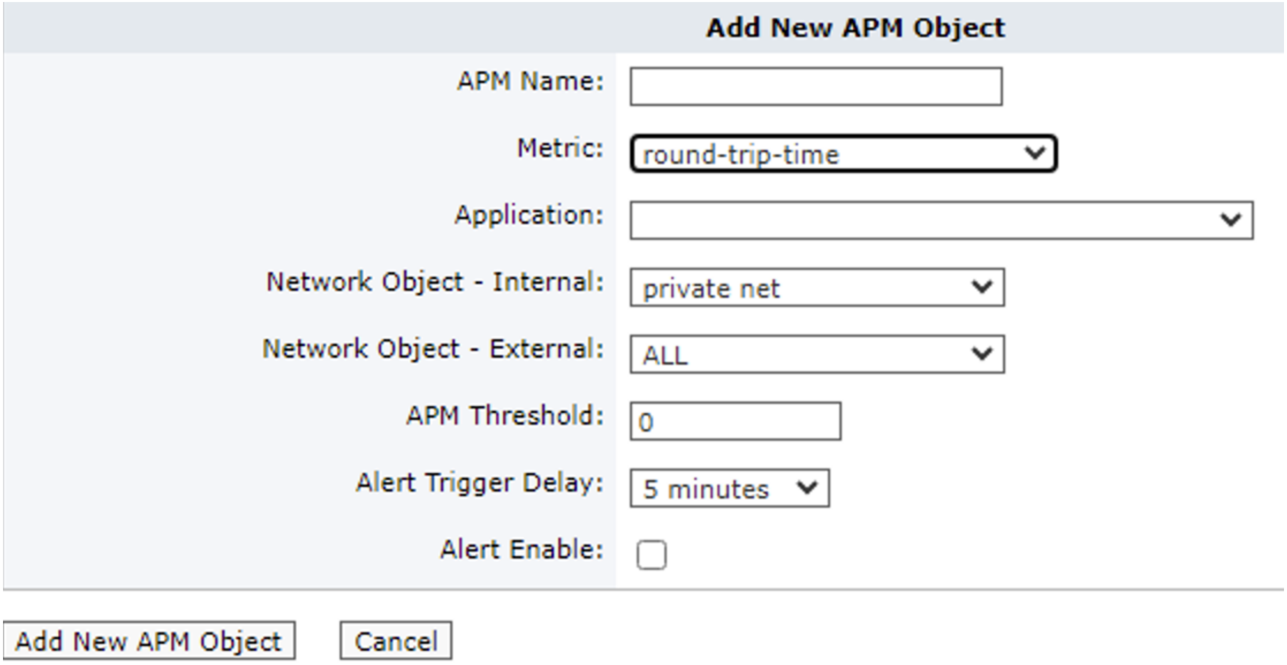
3.1.10 Configuring an application performance metric object

The Application Performance Metric (APM) objects are used to monitor particular application performance metrics. By creating an APM object, you indicate which application to monitor. Optionally, you can also specify a network object so that the application is only monitored when observed on that part of the network. You set a threshold on a single network metric. Later, traffic for that application is assessed against that threshold to determine how well the application is performing. An alert is triggered when the threshold is exceeded for a given length of time.

The following metrics are available:

- bytes lost
- network delay
- server delay
- transaction delay
- normalized network delay
- normalized server delay
- normalized transaction delay
- round trip time
- tcp connections aborted
- tcp connections ignored
- tcp connections refused

- tcp connected started.



Add New APM Object

APM Name:	
Metric:	round-trip-time
Application:	
Network Object - Internal:	private net
Network Object - External:	ALL
APM Threshold:	0
Alert Trigger Delay:	5 minutes
Alert Enable:	□

Screenshot 79: Adding a new APM object.

> **NOTE**
> APM values are not shown on any report; they are used solely to generate alerts.

Use the following instructions to create an APM object.

Before you begin...

» If you need to enable alerts, ensure that you have set Email on the **Configuration > System > Setup > Alerts** page.

For more information, see the GFI ClearView Web UI help.

» You also need to set up SNMP on the **Configuration > System > Network> SNMP** page. for more information, see the GFI ClearView Web UI help.

To create an APM object

1. Go to **Configuration > Objects> Service Levels> Application Performance Metric**.
2. Click the **Add New APM Object** button.
3. Type a name for the APM object.
4. Select the metric that you need to monitor. The following metrics are available:
    - **bytes-lost** — Bytes lost due to retransmissions.
    - **network-delay** — The time taken for data to traverse the network.
    - **server-delay** — The time taken for a server to respond to a request.
    - **transaction-delay** — The total time for a transaction (network delay + server delay)
    - **normalized-network-delay** — The time taken for data to traverse the network where the packet size is nor- malized to 1024 bytes.
    - **normalized-server-delay** — The normalized measure of the time taken for a server to

respond to a trans- action request.

- **normalized-transaction-delay** — The normalized measure of the time taken for a client request to be sent to a server, and the server's reply to be received by the client.
- **round-trip-time** — The time taken for a packet to travel from a device, cross a network, and return.
- **tcp-connections-aborted** — The number TCP connections reset after the connection is established. (RST from client or server)
- **tcp-connections-ignored** — The number TCP connections that expire in the SYN-SENT state. No response is received from the server.
- **tcp-connections- refused** — The number TCP connections that are reset before the connection is established. (RST in SYN-SENT state)
- **tcp-connections-started** — The number of TCP connections initiated.

5. In the **Application** list, select the application traffic to monitor.

6. If you want to just monitor the application for a particular internal network object, specify the desired internal network object; otherwise select ALL.

7. If you want to just monitor the application for a particular external network object, specify the desired external net- work object; otherwise select ALL. By specifying both the internal and external network object, only the application con- versations between the specified network objects will be tracked.

8. Select the **Alert Enable** checkbox.

9. In the **APM Threshold** field, type the threshold that will trigger an alert if the score drops below that value.

10. In the **Alert Trigger Delay** list, select how long the metric needs to remain below the threshold before the alert is sent. For example, if the alert is tracking the number of bytes lost, the threshold is set to 100, and the alert trigger delay is set to 5 minutes, then the number of bytes lost needs to be above 100 for 5 minutes before the alert is triggered.

11. Set the threshold for the APM metric. The units of the threshold is relative to the metric being measured. That is, delays and round trip time are measured in milliseconds, tcp connections and bytes lost are counts.

12. Click **Add New APM Object**. The object is added to the list of configured APM objects.

3.2 Monitoring your network

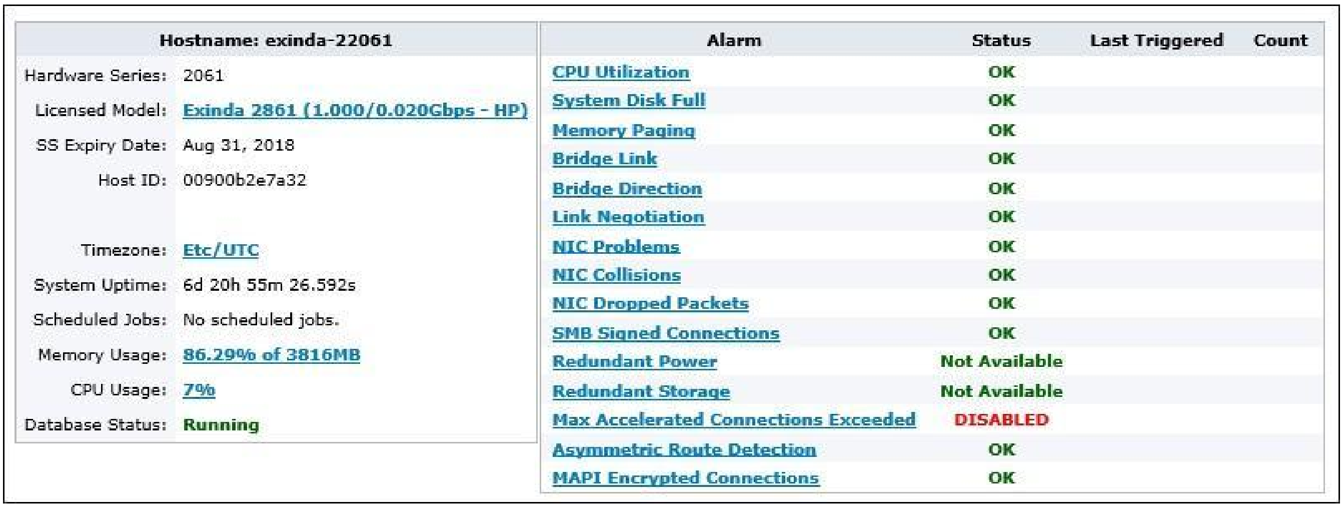
After installing and configuring your GFI ClearView Appliance you can monitor your network, gaining full visibility into the applications users access, inbound traffic, outbound traffic and network throughput.

3.2.1 Dashboards

The GFI ClearView Web UI provides dashboards you can use to monitor the operation of an GFI ClearView Appliance. One dashboard displays system health and status information about the GFI ClearView Appliance. The other dashboard provides statistical data to show the benefits and impact of the GFI ClearView Appliance in your network.

System dashboard

The System dashboard shows system information, the state of system alarms as well as a summary of other GFI ClearView appliances and their respective reduction statistics. The dashboard answers questions, such as "Are there any issues with the NICs, or CPU utilization, etc? What is this appliance licensed for? What is this appliance's host ID?"



Hostname: exinda-22061	
Hardware Series:	2061
Licensed Model:	Exinda 2861 (1.000/0.020Gbps - HP)
SS Expiry Date:	Aug 31, 2018
Host ID:	00900b2e7a32
Timezone:	Etc/UTC
System Uptime:	6d 20h 55m 26.592s
Scheduled Jobs:	No scheduled jobs.
Memory Usage:	86.29% of 3816MB
CPU Usage:	7%
Database Status:	Running

Alarm	Status	Last Triggered	Count
CPU Utilization	OK		
System Disk Full	OK		
Memory Paging	OK		
Bridge Link	OK		
Bridge Direction	OK		
Link Negotiation	OK		
NIC Problems	OK		
NIC Collisions	OK		
NIC Dropped Packets	OK		
SMB Signed Connections	OK		
Redundant Power	Not Available		
Redundant Storage	Not Available		
Max Accelerated Connections Exceeded	DISABLED		
Asymmetric Route Detection	OK		
MAPI Encrypted Connections	OK		

Screenshot 80: The system dashboard displays information about a GFI ClearView Appliance.

The status of the appliance database is displayed as **Database Status**. The possible statuses

- include: **Starting**—The database is initializing, and it is waiting for a response from the
- system on available storage. **Running**—The database is operating.
- **Upgrading**—The database has started, but is being upgraded.
- **Downgrading**—The database has started, but is being upgraded.
- **Stopped**—The database is stopped.
- **Error**—The database cannot be accessed. This typically appears when there is a problem with the upgrade or down- grade of the database.
- **Unknown**—The state of the database is unknown.

Benefits Dashboard

The Benefits Dashboard exposes a set of widgets arranged on a dashboard that shows high level information about your network traffic. The dashboard answers questions, such as "What are the dominant application groups on my network? Are recreational apps using a large amount of my bandwidth? Is my link saturated? " The dashboard may also show a recommendation. The GFI ClearView Appliance analyzes network traffic and makes recommendations based on what it learns.

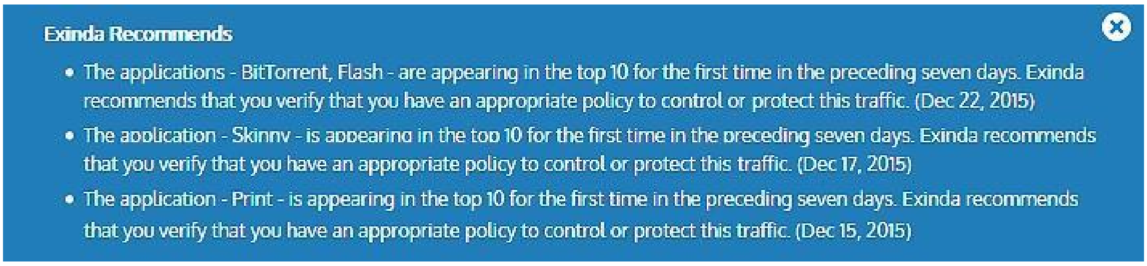
Widgets can be hidden to customize the dashboard to only include widget(s) relevant to you. To add a hidden widget, click the '**Add More**' link at the top right of the dashboard. If the '**Add More**' link is not visible, then all available widgets are displayed. Widget settings and layouts are retained between log-ins.

The dashboard can be captured and converted to PDF by clicking on the PDF icon at the top-right of the interface.

GFI ClearView recommends

Every night after midnight, your GFI ClearView Appliance analyzes the traffic it saw during the previous day and, if there was something remarkable or unusual, it makes a recommendation, displays it on the dashboard and sends it to the email addresses configured in **Network Setup > Email**.

Each recommendation includes the date of the traffic data. Dismiss the recommendation by clicking the close button. To view the last three recommendations made, double-click the GFI ClearView logo in the header bar on the dashboard.



Exinda Recommends

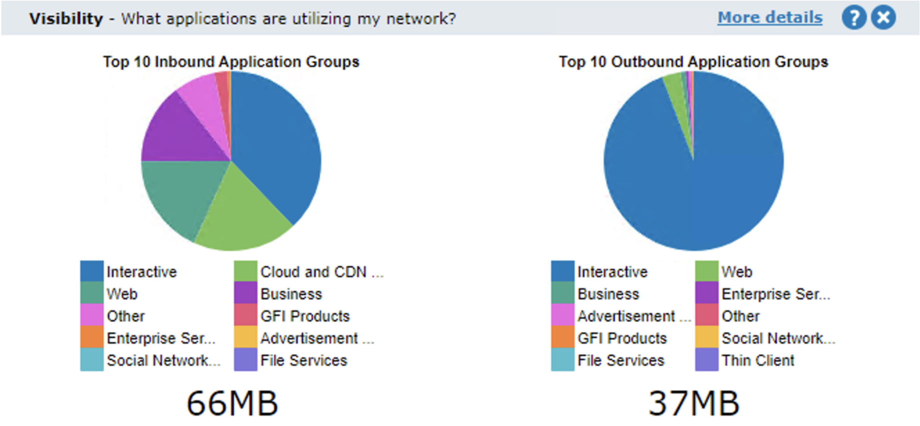
- The applications - BitTorrent, Flash - are appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 22, 2015)
- The application - Skinny - is appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 17, 2015)
- The application - Print - is appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 15, 2015)

Screenshot 81: Example of GFI ClearView recommendation messages in the dashboard

Visibility

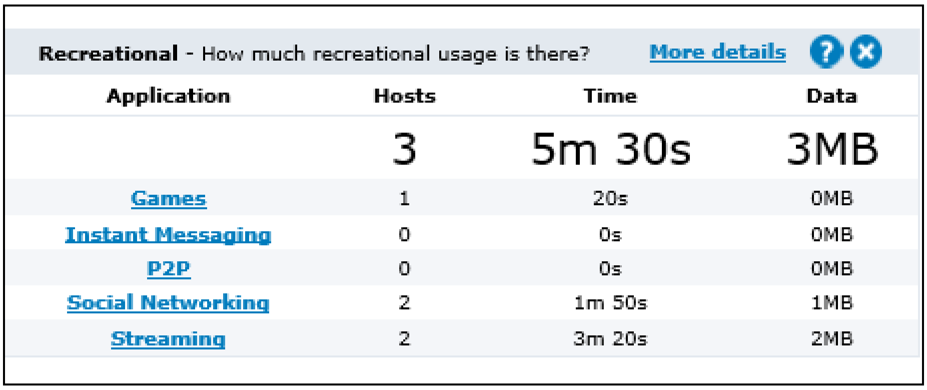
Visibility gives you insight into the traffic on your network so you can effectively control or protect it. The visibility graphs show application groups utilizing the network. These graphs answer questions such as, "Are streaming applications for music and videos choking the network? Are data backups overrunning the network?"

Click the drill down link to see which apps are in an application group.



Recreational

Having visibility into key recreational applications is the first step to managing them. These applications are generally undesirable because they can impact the performance of key business applications, negatively impact customer experiences, reduce productivity, introduce viruses to the network and enable downloading of illegal or copyrighted material.



Recreational - How much recreational usage is there? More details

Application	Hosts	Time	Data
	3	5m 30s	3MB
Games	1	20s	0MB
Instant Messaging	0	0s	0MB
P2P	0	0s	0MB
Social Networking	2	1m 50s	1MB
Streaming	2	3m 20s	2MB

3.2.2 Monitoring network traffic in real time

This section describes real-time reporting with the GFI ClearView Web UI. The real-time monitors display information related to traffic that has passed through monitored links with granularity levels of up to 1 second.

There are several views to help you understand real-time network traffic. These include traffic by applications, by hosts (and users), by conversations, and by reduction per application. Typically, conversations in real time are the most valuable view, as each conversation is shown separately rather than collapsing across an application or host. Also the conversation view allows you to filter the view by IP address or subnet.

When investigating a current issue, the real time monitors allow you to answer questions like:

- My link is congested; which conversations, applications, or hosts may be contributing to the congestion?
- I know I have an issue with a particular host or subnet; what traffic is that host handling?

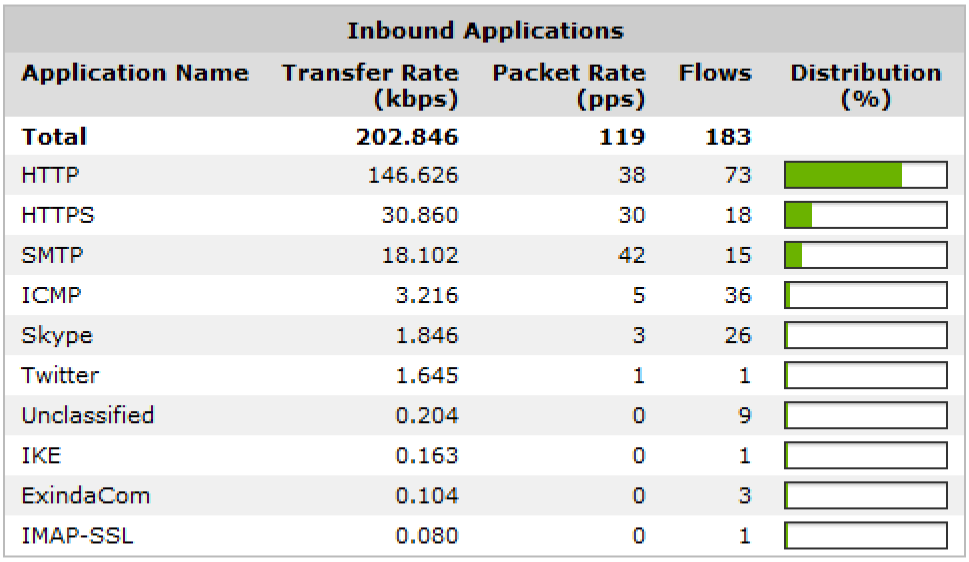
Monitoring network applications in real time

The Applications in Real Time monitor shows the top applications by throughput observed during the last 1 second to 1 minute. This report answers questions such as:

- My link is congested; which applications are on my network right now?
- How much bandwidth is BitTorrent using right now?

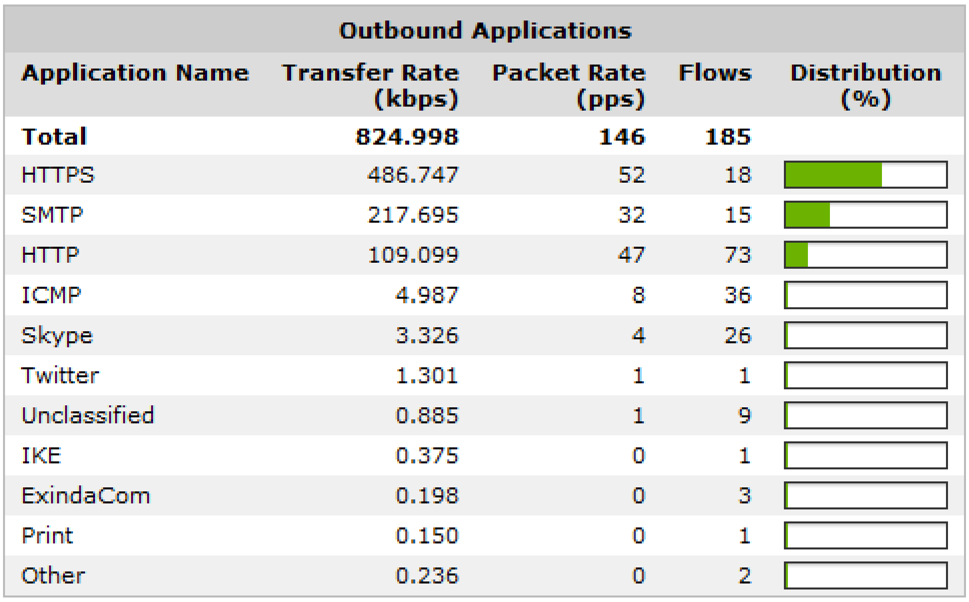
The Applications in Real Time monitor shows inbound application traffic separately from outbound application traffic. Traffic is sorted by transfer rate. The packet rate and a number of flows for each application in that period are also shown. The Distribution percentage shows the proportion of bandwidth consumption of each application relative to all applications.

You can set the chart to refresh frequently or infrequently or not at all. Each refresh shows the data for the selected time range.



Inbound Applications				
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**202.846**	**119**	**183**	
HTTP	146.626	38	73	
HTTPS	30.860	30	18	
SMTP	18.102	42	15	
ICMP	3.216	5	36	
Skype	1.846	3	26	
Twitter	1.645	1	1	
Unclassified	0.204	0	9	
IKE	0.163	0	1	
ExindaCom	0.104	0	3	
IMAP-SSL	0.080	0	1	

Screenshot 82: The Inbound Applications monitor



Outbound Applications				
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**824.998**	**146**	**185**	
HTTPS	486.747	52	18	
SMTP	217.695	32	15	
HTTP	109.099	47	73	
ICMP	4.987	8	36	
Skype	3.326	4	26	
Twitter	1.301	1	1	
Unclassified	0.885	1	9	
IKE	0.375	0	1	
ExindaCom	0.198	0	3	
Print	0.150	0	1	
Other	0.236	0	2	

Screenshot 83: The Outbound Applications monitor

To find this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Real Time > Applications.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

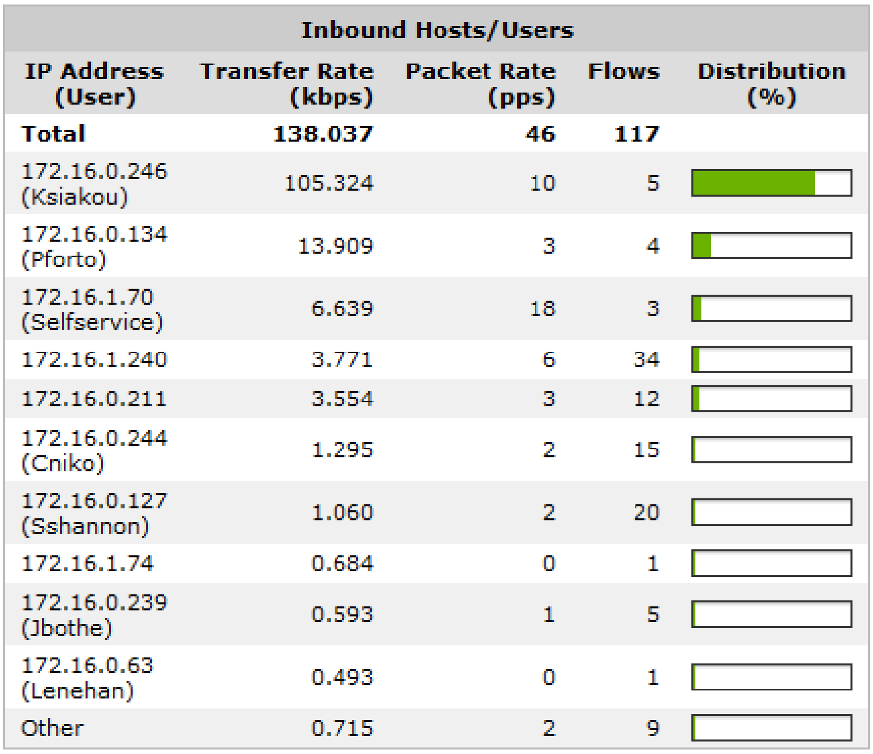
Monitoring hosts and users in real time

The Hosts/Users widgets in the Realtime Monitor shows the top internal hosts by bandwidth consumption observed during the selected period (1 second to up to 60 seconds). The data displayed answers questions such as:

- My link is congested. Which hosts are on my network right now?

The Realtime Monitor separates inbound and outbound host/user traffic. The traffic is sorted by transfer rate. The packet rate and a number of flows in the preceding period are shown. The user name of the internal hosts will also be displayed if configured.

The Distribution percentage shows the proportion of bandwidth consumption of each host relative to all hosts for the period. You can set the chart to refresh frequently or infrequently or not at all.



Inbound Hosts/Users

IP Address (User)	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	**138.037**	**46**	**117**	
172.16.0.246 (Ksiakou)	105.324	10	5	
172.16.0.134 (Pforto)	13.909	3	4	
172.16.1.70 (Selfservice)	6.639	18	3	
172.16.1.240	3.771	6	34	
172.16.0.211	3.554	3	12	
172.16.0.244 (Cniko)	1.295	2	15	
172.16.0.127 (Sshannon)	1.060	2	20	
172.16.1.74	0.684	0	1	
172.16.0.239 (Jbothe)	0.593	1	5	
172.16.0.63 (Lenehan)	0.493	0	1	
Other	0.715	2	9	

Screenshot 84: Monitoring inbound hosts/users report

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to Monitor> Real Time > Hosts/Users.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To show the user associated with the internal hosts, check the **Show Users** checkbox.

> **NOTE**
>
> Active Directory must be configured on the GFI ClearView Appliances before usernames can be displayed in reports. See
> For more information, refer to Integrate with Active Directory (page 503).

Monitoring conversations in real time

The Realtime Conversations monitor shows the top conversations by throughput observed by the GFI ClearView Appliance during the selected period (1 second to up to 60 seconds). This report answers questions such as:

- My link is congested; who's doing what on my network right now?
- I think I have a problem with a particular host or subnet; what is that host or subnet doing right now?

Inbound and outbound conversation traffic is displayed separately. Conversations are represented by external IP address, internal IP address, and application. Some traffic types show extra information (like URL) in square brackets following the application.

Traffic is sorted by transfer rate. The packet rate and number of flows for each conversation in the preceding (selected) period is shown. You can set the chart to refresh frequently or infrequently or not at all.

The Realtime Conversations monitor helps you diagnose issues by:

- Filtering the conversations by IP address or subnet
- Showing the user name associated with the internal IP address
- Allowing connections within a flow to either be shown individually or to be grouped together
- Highlighting accelerated conversations in yellow and indicating the acceleration technique used
- Highlighting conversations processed by Edge Cache (in blue)
- Indicating how the conversations is flowing through the high availability cluster
- Indicating asymmetric traffic

Monitoring application response in real time

The Realtime Application Response monitor shows the slowest applications by round-trip-time observed by the GFI ClearView Appliance during the selected period.

This report can answer questions such as:

1. Which applications may be having problems?
2. What are my poorest performing applications?
3. Why is the application performing poorly; could it be due to network delay or server delay?

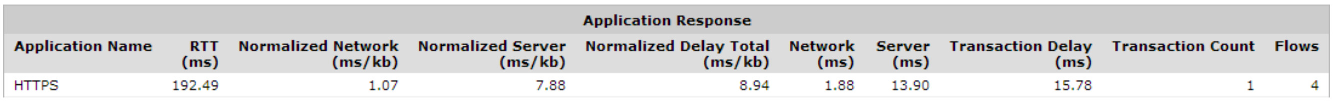
To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Real Time > Application Response.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

The monitor shows application response metrics like round-trip time (RTT), normalized network delay, normalized server delay, normalized total delay, network delay, server delay, transaction delay, transaction count, and flow count by application. Traffic is sorted by round-trip-time.

You can set the chart to refresh frequently or infrequently or not at all.



Application Response

Application Name	RTT (ms)	Normalized Network (ms/kb)	Normalized Server (ms/kb)	Normalized Delay Total (ms/kb)	Network (ms)	Server (ms)	Transaction Delay (ms)	Transaction Count	Flows
HTTPS	192.49	1.07	7.88	8.94	1.88	13.90	15.78	1	4

Screenshot 88: The Application Response monitordisplays response by RTT.

> **NOTE**
>
> These statistics are only available if the Performance Metrics ASAM Module is enabled on the System > Setup > Monitoring page.

Monitoring real time application response

The APM values are available as a real time display. The real time display shows the APM values by application for the selected time period. As well as the APM values, the number of flows and the number of transactions are shown.

Display the report in the GFI ClearView Web UI

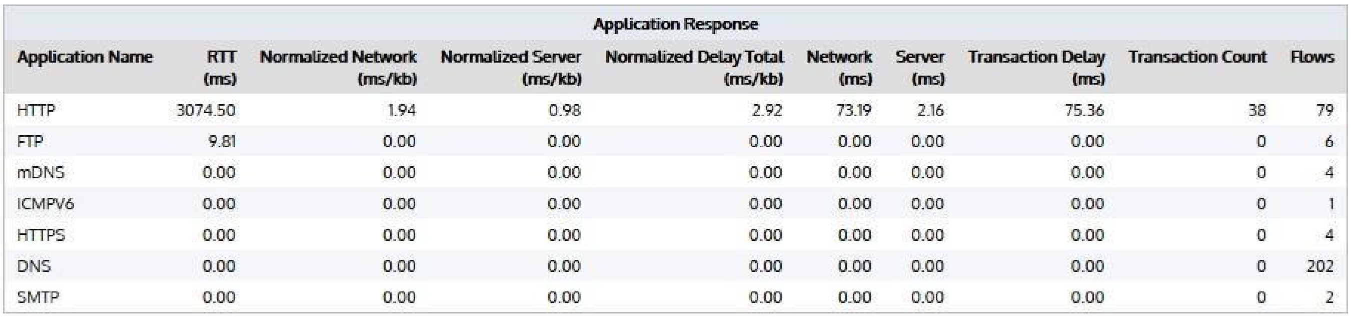
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Monitor> Real Time** and switch to the

Application Response tab. The following report opens:



Application Response

Application Name	RTT (ms)	Normalized Network (ms/kb)	Normalized Server (ms/kb)	Normalized Delay Total (ms/kb)	Network (ms)	Server (ms)	Transaction Delay (ms)	Transaction Count	Flows
HTTP	3074.50	1.94	0.98	2.92	73.19	2.16	75.36	38	79
FTP	9.81	0.00	0.00	0.00	0.00	0.00	0.00	0	6
mDNS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	4
ICMPV6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	1
HTTPS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	4
DNS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	202
SMTP	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	2

6. To change how often the table is refreshed, select an **Auto-Refresh Rate** from the list.

Display the report in the GFI ClearView CLI

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Click Configuration > System > Tools> Console.

5. Type the appliance username and password at the prompts. Do one of the following:

- To enter privileged EXEC (enable) mode, at the prompt run the command: `hostname > enable`

  The `hostname #` prompt appears.

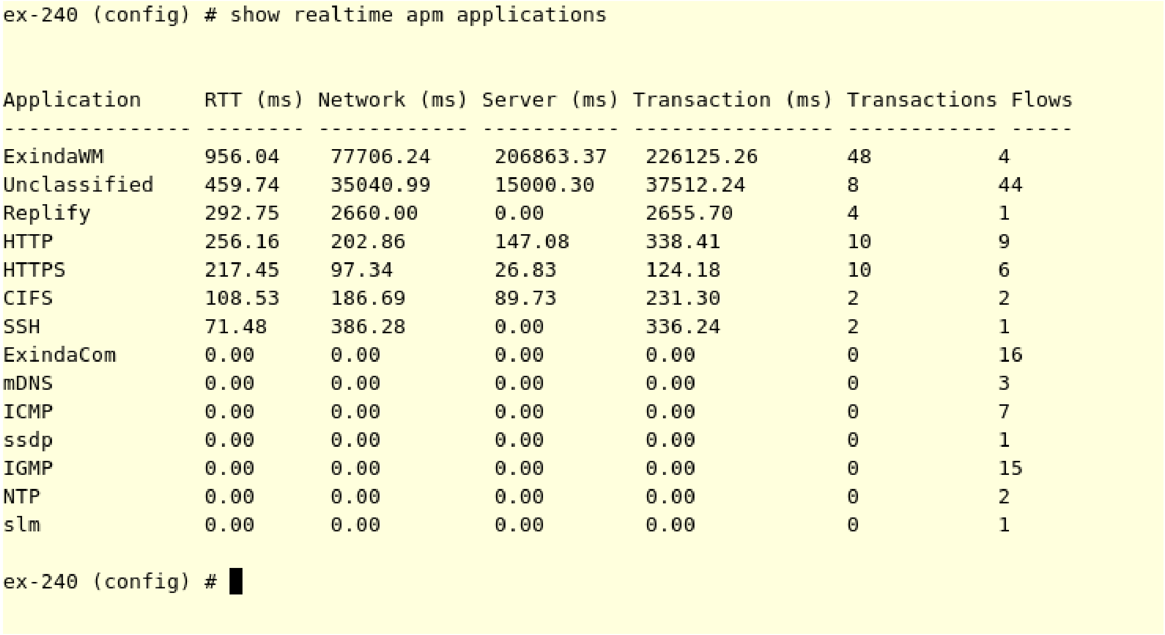
- To enter configuration (config) mode, at the prompt run the commands: `hostname # configure terminal`

The `hostname (config)#` prompt appears.

7. To display real time APM data from the CLI, use the following command:

```
(config) # show realtime apm applications
```

The following results are displayed:



```
ex-240 (config) # show realtime apm applications


Application     RTT (ms) Network (ms) Server (ms) Transaction (ms) Transactions Flows
--------------- -------- ------------ ----------- ---------------- ------------ -----
ExindaWM        956.04    77706.24     206863.37   226125.26        48           4
Unclassified    459.74    35040.99     15000.30    37512.24         8            44
Replify         292.75    2660.00      0.00        2655.70          4            1
HTTP            256.16    202.86       147.08      338.41           10           9
HTTPS           217.45    97.34        26.83       124.18           10           6
CIFS            108.53    186.69       89.73       231.30           2            2
SSH             71.48     386.28       0.00        336.24           2            1
ExindaCom       0.00      0.00         0.00        0.00             0            16
mDNS            0.00      0.00         0.00        0.00             0            3
ICMP            0.00      0.00         0.00        0.00             0            7
ssdp            0.00      0.00         0.00        0.00             0            1
IGMP            0.00      0.00         0.00        0.00             0            15
NTP             0.00      0.00         0.00        0.00             0            2
slm             0.00      0.00         0.00        0.00             0            1

ex-240 (config) # █
```

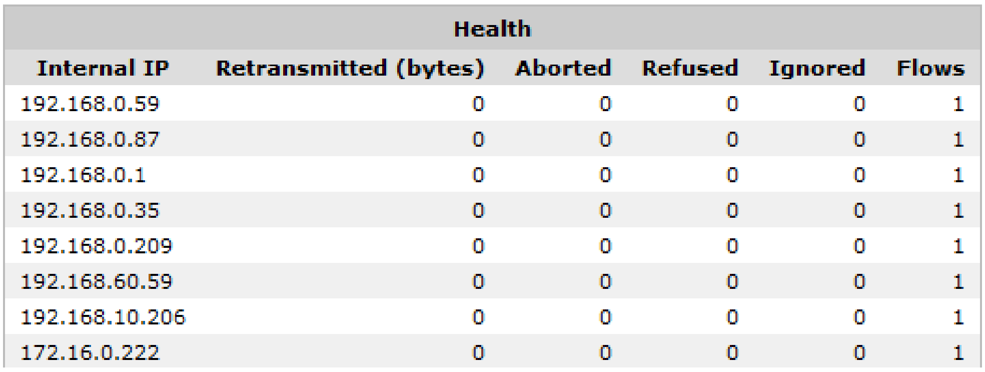
Monitoring host health in real time

The Realtime Host Health monitor shows unhealthy hosts as measured by the number of retransmitted bytes during the selected period (1 second to up to 60 seconds). This report answers questions such as:

- Which internal hosts are having the most difficulty with successfully transmitting traffic?

The monitor separates internal and external hosts and displays metrics like number of retransmitted bytes, number of aborted connections, number of refused connections, number of ignored connections, and the flow count for each internal and external host monitored during the selected period.

Traffic is sorted by the amount of retransmitted bytes. You can set the chart to refresh frequently or infrequently or not at all.



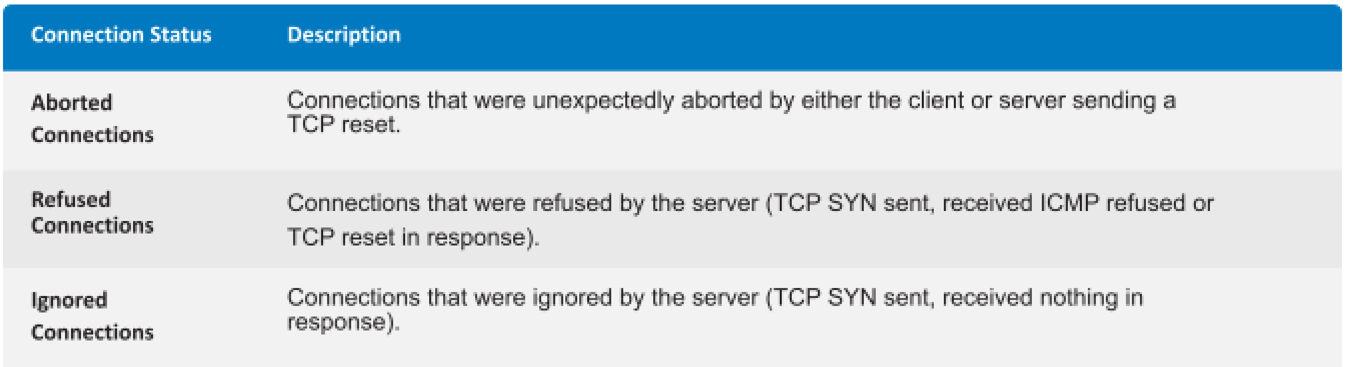
Health					
Internal IP	Retransmitted (bytes)	Aborted	Refused	Ignored	Flows
192.168.0.59	0	0	0	0	1
192.168.0.87	0	0	0	0	1
192.168.0.1	0	0	0	0	1
192.168.0.35	0	0	0	0	1
192.168.0.209	0	0	0	0	1
192.168.60.59	0	0	0	0	1
192.168.10.206	0	0	0	0	1
172.16.0.222	0	0	0	0	1

Screenshot 89: The Realtime Host Health report displays the number of retransmitted bytes.

> **NOTE**
>
> These statistics are only available if the Performance Metrics ASAM Module is enabled on the System > Setup > Monitoring page.

Display the report in the GFI ClearView Web UI

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Click **Monitor> Real Time>Host Health**. The reports contains the following status:
5. To change how often the table is refreshed, select an **Auto-Refresh Rate** from the list.



Connection Status	Description
Aborted Connections	Connections that were unexpectedly aborted by either the client or server sending a TCP reset.
Refused Connections	Connections that were refused by the server (TCP SYN sent, received ICMP refused or TCP reset in response).
Ignored Connections	Connections that were ignored by the server (TCP SYN sent, received nothing in response).

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

Display the report in the GFI ClearView CLI

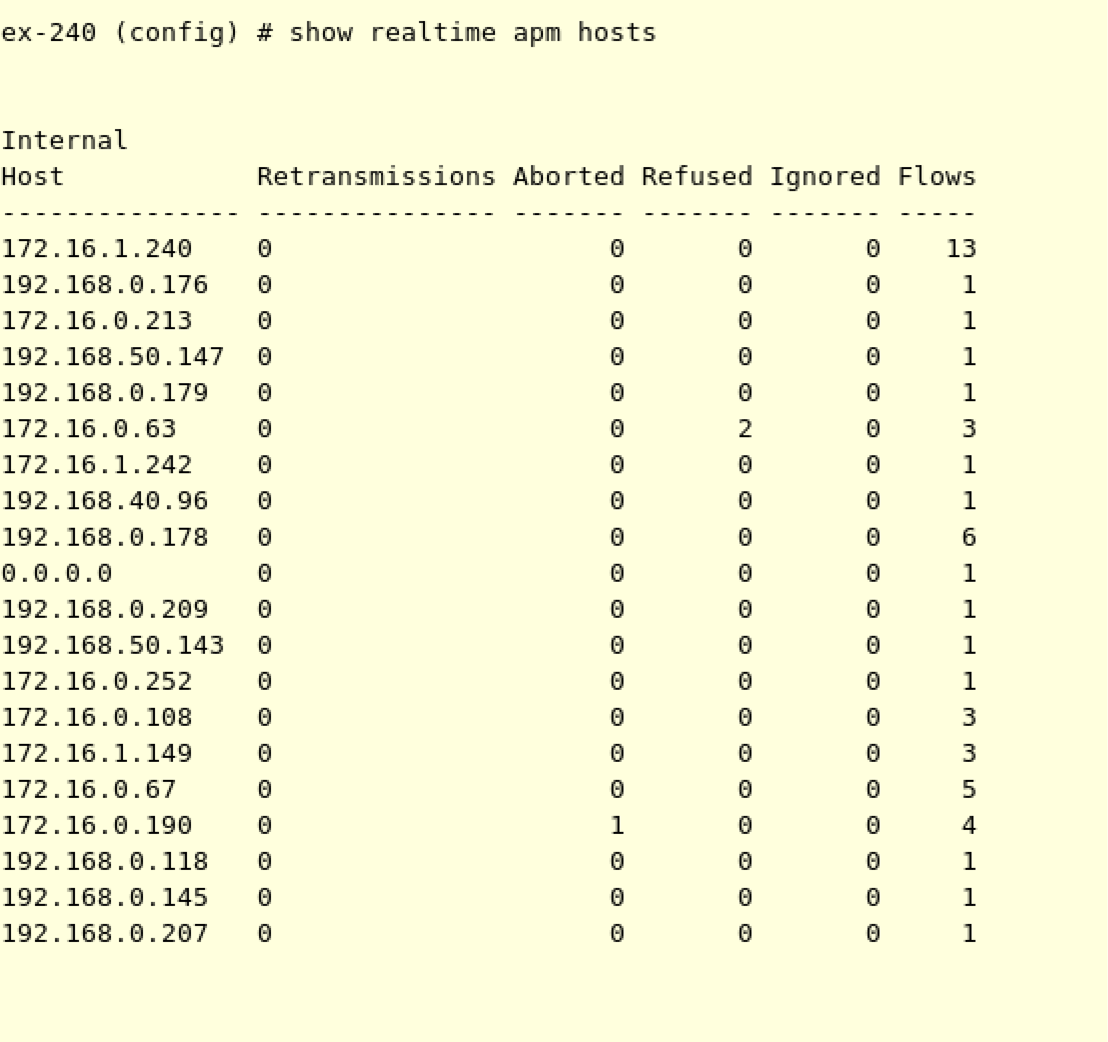
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Click Configuration > System > Tools> Console.
5. Type the appliance username and password at the prompts. Do one of the following:
    - To enter privileged EXEC (enable) mode, at the prompt run the command: `hostname > enable`

      The `hostname #` prompt appears.
    - To enter configuration (config) mode, at the prompt run the commands: `hostname # configure terminal`

      The `hostname (config)#` prompt appears.
6. To display realtime TCP health from the CLI, use the following command:

```
(config) # show realtime apm hosts
```

The following results are displayed:



```
ex-240 (config) # show realtime apm hosts


Internal
Host            Retransmissions Aborted Refused Ignored Flows
--------------- --------------- ------- ------- ------- -----
172.16.1.240    0                     0       0       0    13
192.168.0.176   0                     0       0       0     1
172.16.0.213    0                     0       0       0     1
192.168.50.147  0                     0       0       0     1
192.168.0.179   0                     0       0       0     1
172.16.0.63     0                     0       2       0     3
172.16.1.242    0                     0       0       0     1
192.168.40.96   0                     0       0       0     1
192.168.0.178   0                     0       0       0     6
0.0.0.0         0                     0       0       0     1
192.168.0.209   0                     0       0       0     1
192.168.50.143  0                     0       0       0     1
172.16.0.252    0                     0       0       0     1
172.16.0.108    0                     0       0       0     3
172.16.1.149    0                     0       0       0     3
172.16.0.67     0                     0       0       0     5
172.16.0.190    0                     1       0       0     4
192.168.0.118   0                     0       0       0     1
192.168.0.145   0                     0       0       0     1
192.168.0.207   0                     0       0       0     1
```

Screenshot 90: Realtime TCP health from the CLI.

3.2.3 Monitoring network throughput

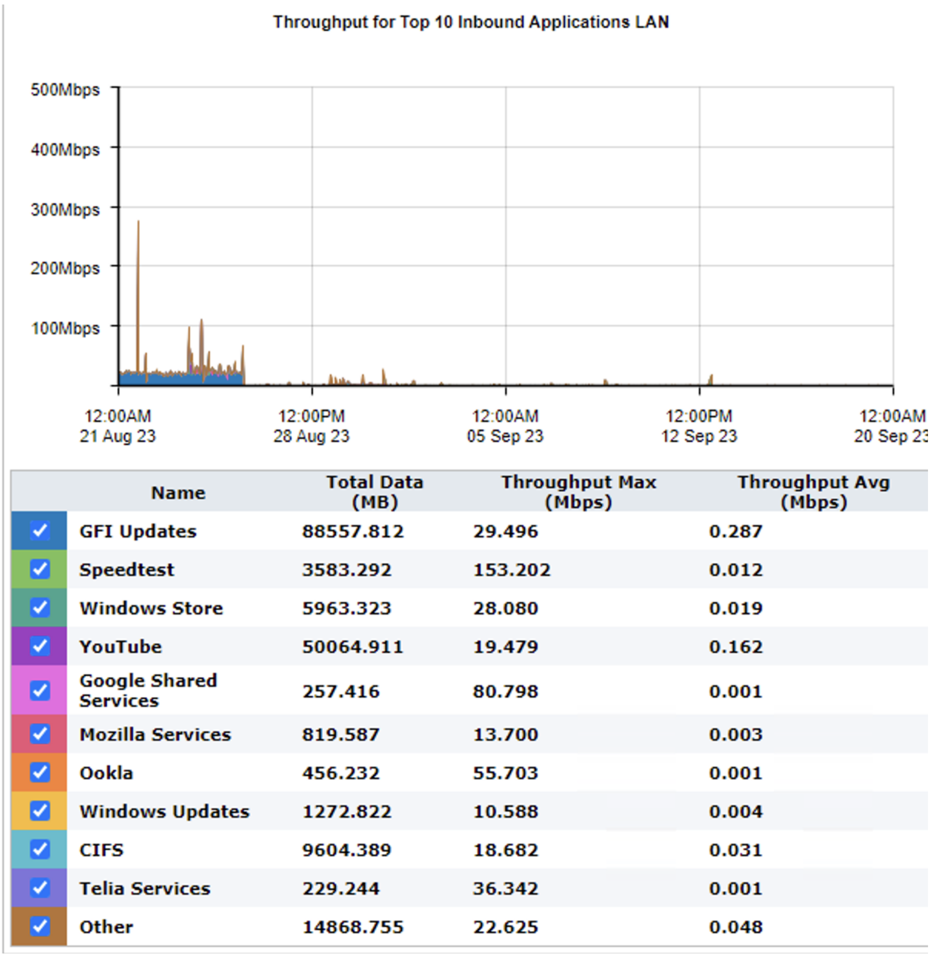
The Network Summary report shows traffic throughput over time by application, application groups, internal or external hosts, internal or external users, conversations, or URLS. You can remove items from the chart to isolate traffic patterns and sources.

This report answers questions such as:

- What is the pattern of throughput for particular apps, app groups, users, hosts, etc.?
- Are there any spikes and what type of traffic may be causing the spikes?
- What would happen to the throughput if I created a policy to block a particular app, application group, user, or host?

The charts help you diagnose issues and perform what-if scenarios to determine the right size of your network.

The report shows LAN-side and WAN-side charts for both inbound traffic and outbound traffic. The total data volume, maximum throughput, and average throughput is also shown in tables below each chart. The charts aggregate data outside the top 10 in a category named "Other".



	Name	Total Data (MB)	Throughput Max (Mbps)	Throughput Avg (Mbps)
☑	GFI Updates	88557.812	29.496	0.287
☑	Speedtest	3583.292	153.202	0.012
☑	Windows Store	5963.323	28.080	0.019
☑	YouTube	50064.911	19.479	0.162
☑	Google Shared Services	257.416	80.798	0.001
☑	Mozilla Services	819.587	13.700	0.003
☑	Ookla	456.232	55.703	0.001
☑	Windows Updates	1272.822	10.588	0.004
☑	CIFS	9604.389	18.682	0.031
☑	Telia Services	229.244	36.342	0.001
☑	Other	14868.755	22.625	0.048

Screenshot 93: The Network Summary report displays LAN traffic volume for the top 10 inbound applications.

Where do I find this report?

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to **Monitor> Network**.

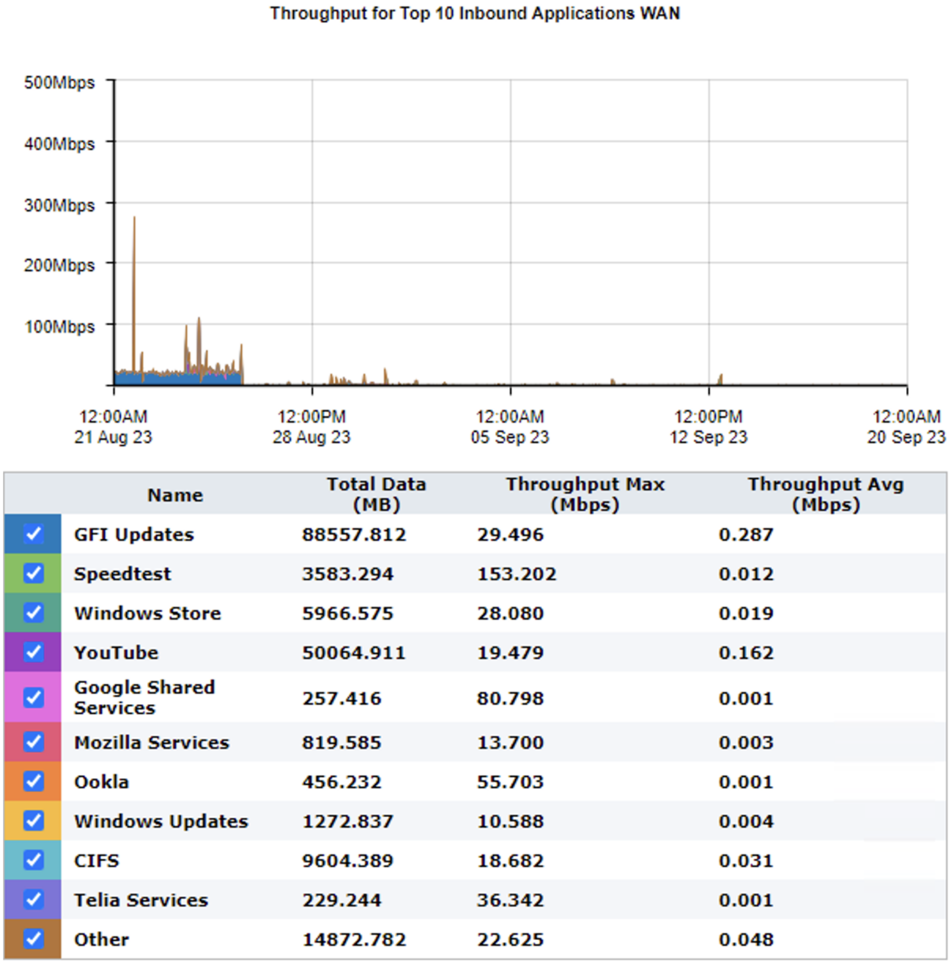
Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To determine the right size of your network (i.e. remove items from the chart)

Remove specific types of traffic from the graph by deselecting their checkbox in the legend below the graph. The remaining traffic models what your network traffic would look like if you blocked that type of traffic. You can then determine an appropriate amount of bandwidth required.

To identify which throughput falls above a specific percentile

Select the desired percentile level from the **Select Percentile Marker to Display** selector.



	Name	Total Data (MB)	Throughput Max (Mbps)	Throughput Avg (Mbps)
☑	GFI Updates	88557.812	29.496	0.287
☑	Speedtest	3583.294	153.202	0.012
☑	Windows Store	5966.575	28.080	0.019
☑	YouTube	50064.911	19.479	0.162
☑	Google Shared Services	257.416	80.798	0.001
☑	Mozilla Services	819.585	13.700	0.003
☑	Ookla	456.232	55.703	0.001
☑	Windows Updates	1272.837	10.588	0.004
☑	CIFS	9604.389	18.682	0.031
☑	Telia Services	229.244	36.342	0.001
☑	Other	14872.782	22.625	0.048

Screenshot 94: The Network Summary report displays WAN traffic volume for the top 10 inbound applications.

How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Interactive Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling

Reports.

3.2.4 Monitoring service levels

Learn how to view application performance reports, the availability of your ISP, and the health and efficiency of TCP traffic.

Monitoring application performance scores

The Application Performance Score (APS) report shows scores that assess network performance and user experience when using business-critical applications.

These charts can answer questions such as:

- Are my important applications performing well from a network perspective for
- my network users? Has this been a persistent problem or is it getting worse?
- If an application is not performing well, what might be causing the problem?

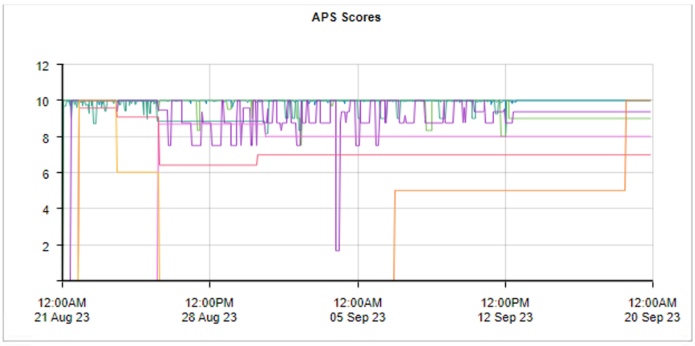
To access the report:

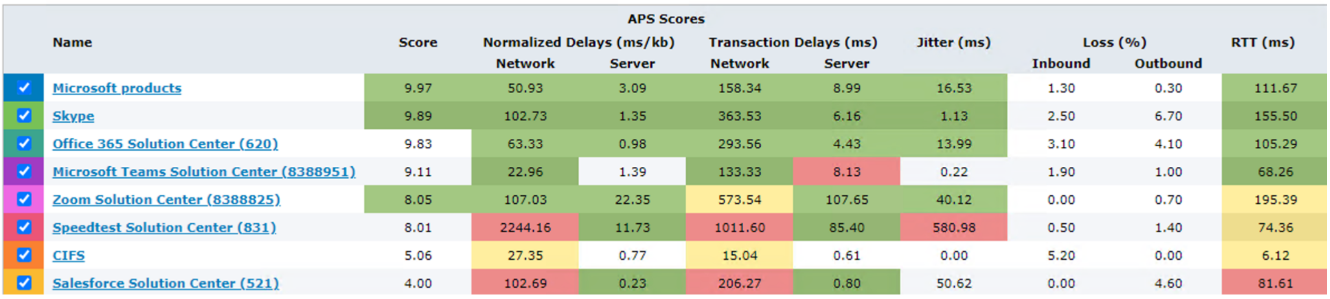
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Service Levels> Application Performance Score (APS).

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

A score between 0 and 10, where 0 is poor and 10 is excellent, indicates whether the app is performing well or poorly.

Scores are graphed over time to show how the scores changes and trends. The underlying metrics and measures used to calculate scores are shown in the table below the graph. You can drill into the details of the APS by clicking an application name.





APS Scores

	Name	Score	Normalized Delays (ms/kb)		Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
			Network	Server	Network	Server		Inbound	Outbound	
☑	Microsoft products	9.97	50.93	3.09	158.34	8.99	16.53	1.30	0.30	111.67
☑	Skype	9.89	102.73	1.35	363.53	6.16	1.13	2.50	6.70	155.50
☑	Office 365 Solution Center (620)	9.83	63.33	0.98	293.56	4.43	13.99	3.10	4.10	105.29
☑	Microsoft Teams Solution Center (8388951)	9.11	22.96	1.39	133.33	8.13	0.22	1.90	1.00	68.26
☑	Zoom Solution Center (8388825)	8.05	107.03	22.35	573.54	107.65	40.12	0.00	0.70	195.39
☑	Speedtest Solution Center (831)	8.01	2244.16	11.73	1011.60	85.40	580.98	0.50	1.40	74.36
☑	CIFS	5.06	27.35	0.77	15.04	0.61	0.00	5.20	0.00	6.12
☑	Salesforce Solution Center (521)	4.00	102.69	0.23	206.27	0.80	50.62	0.00	4.60	81.61

Screenshot 95: The Application Performance Score displays scores from 0 - 10 over time.

A score includes input from one or more of the following metrics:

- Network delay – the time taken for data to traverse the network
- (on the wire) Server delay – the time taken for a server to

  respond to the request
- Normalized network delay – the time taken for data to traverse the network, where the delay is measured inde- pendent of the transaction size by assuming a normalized packet size of 1024 bytes
- Normalized server delay – the time taken for a server to respond to the request, where the delay is measured inde- pendently of the transaction size, by assuming a normalized packet size of 1024 bytes
- Round-trip time – the time taken for
- Jitter – the measure of variability of network delay, defined as one standard
- deviation of network delay Inbound loss – the percentage of packet loss on

  inbound traffic
- Outbound loss – the percentage of packet loss on outbound traffic

Each metric that contributes to the score has a threshold value set. The threshold may have been set manually or may have been determined automatically by the GFI ClearView Appliance observing the traffic for the period of time to determine a baseline threshold values. The table below the chart indicates the current observed values for these metrics and whether that value is considered good or not.

- If the observed traffic is within the threshold, it is considered good and is colored green in the APS Scores table.
- If the observed traffic is above the threshold but not above 4 x the threshold, it is considered tolerable and is colored yellow.
- If the observed traffic is above 4 x the threshold, it is considered poor and is colored red.
- If there is no color in the table for a particular metric, it indicates that the metric is not contributing to the calculation of the APS score.

Use this information to determine which metrics contribute to an application's performance score.

Generate a PDF report of APS results

Create a report that contains the APS, TCP health, and TCP efficiency for a specified period of time.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
5. Click **Report** and switch to the **PDF Reports** tab.
6. Click **Add New PDF Report**.
7. In the Report Selection area select **APS**, **TCPHealth**, and **TCPEfficiency**.
8. In the Report Details area, type a name for the report.
9. Specify how often the report will be generated.
10. Click **Add New Report**.
11. To generate the report, locate the report in the list and click **PDF**.

What to expect

If an APS report is not showing data

Either the APS object does not have thresholds set and therefore the score cannot be calculated or there is no traffic for the specified application on the network for the period that is shown on the screen.

If the thresholds were set by using the baselining feature

You should get an application performance score of 9.0 if the same traffic were to be observed.

Evaluating the APS

If the thresholds were set by using the baselining feature, a score of 8.5 or higher is considered a good score. The thresholds are automatically set to be slightly higher than the average observed measures so that good would be at the top end of the range of scores.

If you set the thresholds manually such that your thresholds lie at the boundary of what you consider good or not good, then you should consider APS scores greater than 5.0 good, as statistically half the time you would expect the observed values to be slightly above your threshold and half the time the observed values would be slightly below the threshold.

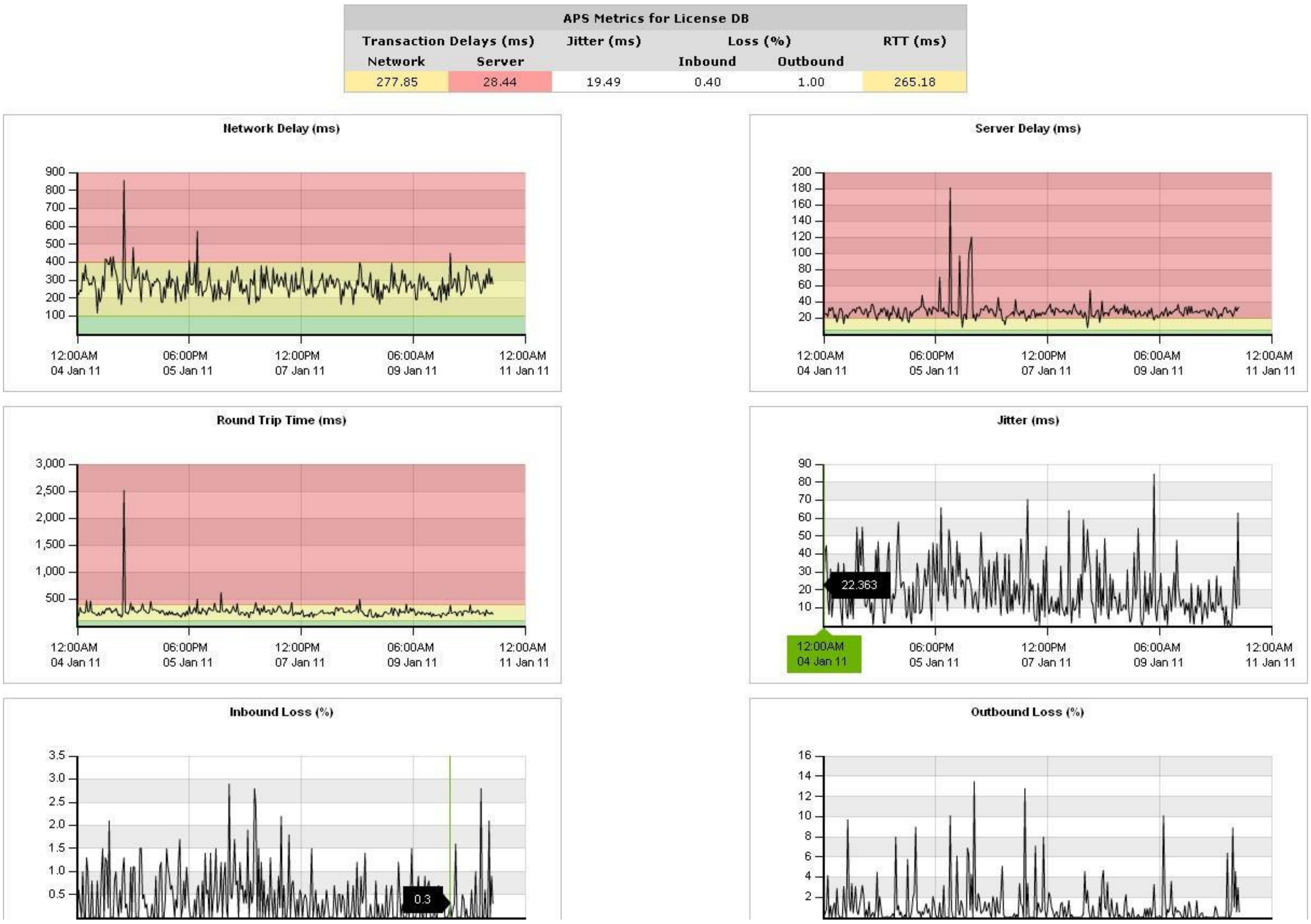
Looking at the results

Determining what might be causing a low APS score

Click the APS name in the table. A new screen that shows charts for each underlying metric appears. The background of each chart is colored to represent value within threshold, within 4 x threshold, and above.

If the background of the chart is not colored, that metric does not contribute to the calculation of the APS score. You can zoom into these charts by clicking and dragging within a chart to zoom into the x-axis range. All other charts will synchronize their zoom ranges to the specified zoom range.

The metrics showing poor values could indicate a problem to investigate. For example, if the network delay is good, but the server delay is poor, you know that the network is not to blame and that the server administrator should take a look at the application server.



APS Metrics for License DB

Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
Network	Server		Inbound	Outbound	
277.85	28.44	19.49	0.40	1.00	265.18

Network Delay (ms)

Server Delay (ms)

Round Trip Time (ms)

Jitter (ms)

Inbound Loss (%)

Outbound Loss (%)

Determining if a problem has been persistent

Look at the APS score timeline. If the score has been low for an extended period or if it looks like the score is dropping, you'll know that this is a persistent problem that needs addressing.

Determining if you should pay attention to the normalized delays or the transaction delays

Generally, you should use the transaction delays unless the protocol that is being monitored has large or variable sized packets. The normalized delay measure normalizes the score to reflect a 1024 packet size allowing you to more easily compare delays when the packets are variable in size.

Configuring the system to notify you if the APS score drops too low

You can configure the system to send an email if the APS score drops below an APS value you specify and remains below that value for a specified duration. For example, you can set it to notify you if it drops below 7.0 and stays below 7.0 for 5 minutes.

Making the APS chart easier to read by removing score lines

» You can temporarily remove lines from the APS Scores chart by clearing the checkboxes next to the APS name in the table.

» You can zoom into an area of interest by clicking and dragging in the chart to select a smaller time range. This often has the effect of flattening the lines so that it appears less cluttered.

Calculating an application performance score

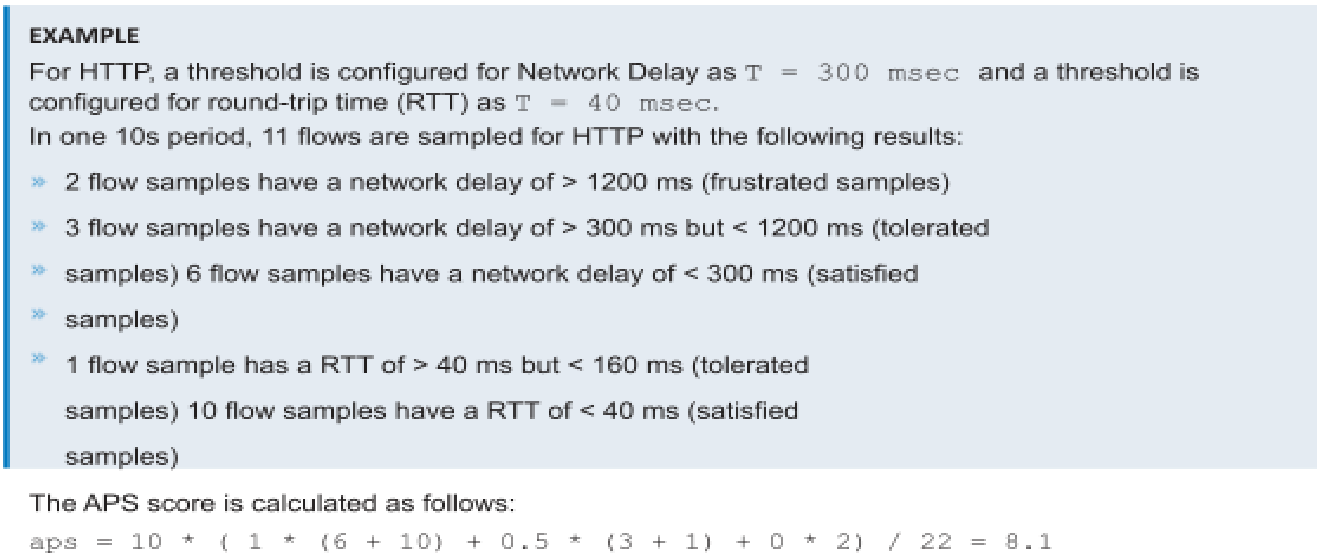
The Application Performance Score object defines the application traffic that will be monitored and which application performance metrics to evaluate. It also provides application performance thresholds to be used in the evaluation.

For each metric, the observed traffic is compared against the threshold and is classified into one of three categories:

- Good — The baseline for the application is good, which indicates that the application is performing within the expected levels (below the threshold). Users should be happy with application performance.
- Tolerated — The performance of the application is less than expected, but still performing within a range that users should be able to tolerate (between the threshold and four times the threshold).
- Frustrated — The application is performing poorly (more than four times the threshold). Users will be frustrated.

The number of good observations for all metrics with a threshold are totaled and given a full weighting; the number of tolerated observations for all metrics with a threshold are totaled and given a half weighting; and all frustrated observations are given a zero weighting. These weighted totals are summed and divided by the total observations.

```
aps = 10 * ((1 x number of satisfied samples) + (0.5 x number of tolerated
samples)
+ (0 x number of frustrated samples)) / total samples
```



EXAMPLE

For HTTP, a threshold is configured for Network Delay as `T = 300 msec` and a threshold is configured for round-trip time (RTT) as `T = 40 msec.`

In one 10s period, 11 flows are sampled for HTTP with the following results:

- 2 flow samples have a network delay of > 1200 ms (frustrated samples)
- 3 flow samples have a network delay of > 300 ms but < 1200 ms (tolerated
- samples) 6 flow samples have a network delay of < 300 ms (satisfied
- samples)
- 1 flow sample has a RTT of > 40 ms but < 160 ms (tolerated

  samples) 10 flow samples have a RTT of < 40 ms (satisfied

  samples)

The APS score is calculated as follows:

```
aps = 10 * ( 1 * (6 + 10) + 0.5 * (3 + 1) + 0 * 2) / 22 = 8.1
```

Setting thresholds

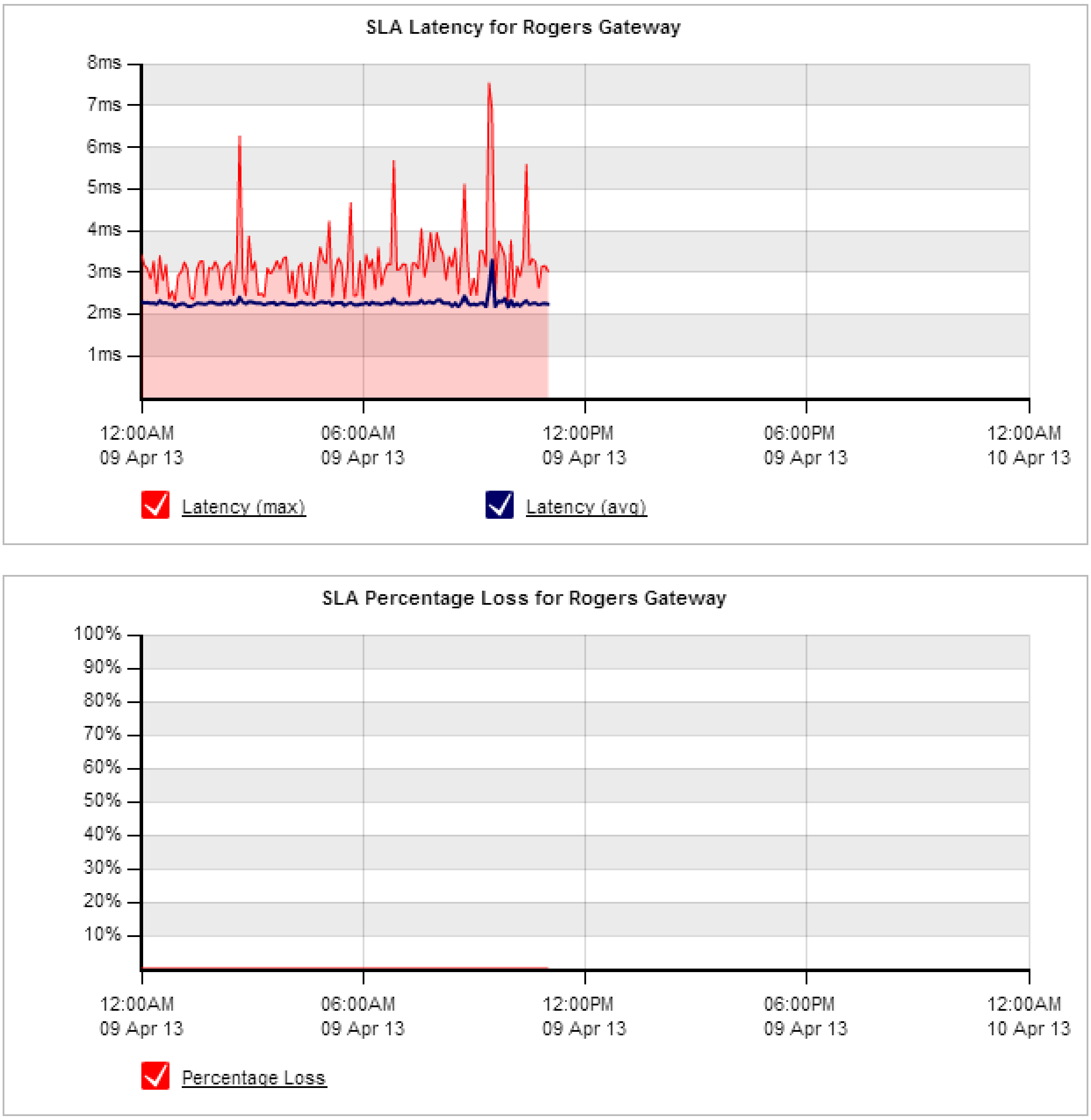
The appropriate thresholds for an application is unique for each network environment. Thresholds can be set manually when configuring an APS object or the GFI ClearView appliance can analyze the traffic for an application for a baseline period and create a recommended set of thresholds.

For more information, refer to Configuring application performance score objects.

Monitoring network response SLA

The SLA monitor reports the performance of your ISP against a set of predefined criteria. The SLA monitor sends 1 64-bit long ICMP ping every 10 seconds to the remote site. It reports the maximum and average latency and the percentage loss of the pings over time. This report answers questions such as:

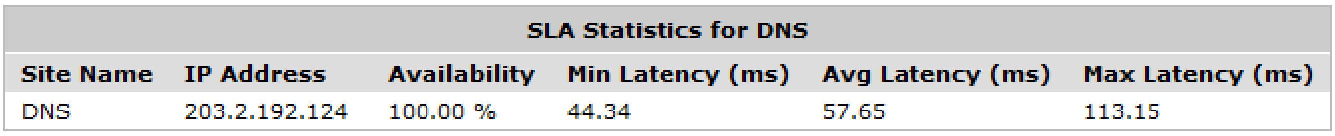
- Is my ISP always available?
- What is the latency of my ISP?



Screenshot 96: The SLAmonitortracks latency and percentage loss over time.

For each SLA object, the GFI ClearView tracks the IP address, percentage of availability, minimum and maximum and average latency in the table below the charts.

- Availability is the percentage of time a resource is reachable by the GFI ClearView appliance.
- Latency is the delay in getting an ICMP echo reply for an ICMP echo request generated from the GFI ClearView appliance. It represents both the delay from the local GFI ClearView appliance to a remote host and back again.



SLA Statistics for DNS					
Site Name	IP Address	Availability	Min Latency (ms)	Avg Latency (ms)	Max Latency (ms)
DNS	203.2.192.124	100.00 %	44.34	57.65	113.15

Where do I find this report?

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Service Levels> Network Response (SLA).

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To add an SLA Site

Click the **Add/Edit SLA Site...** link. See TO-DO for details of configuring an SLA object.

To view the chart for a different SLA Site

Select the desired site from the **SLA Sites** selector.

How do I interact with the interactive flash time graphs?

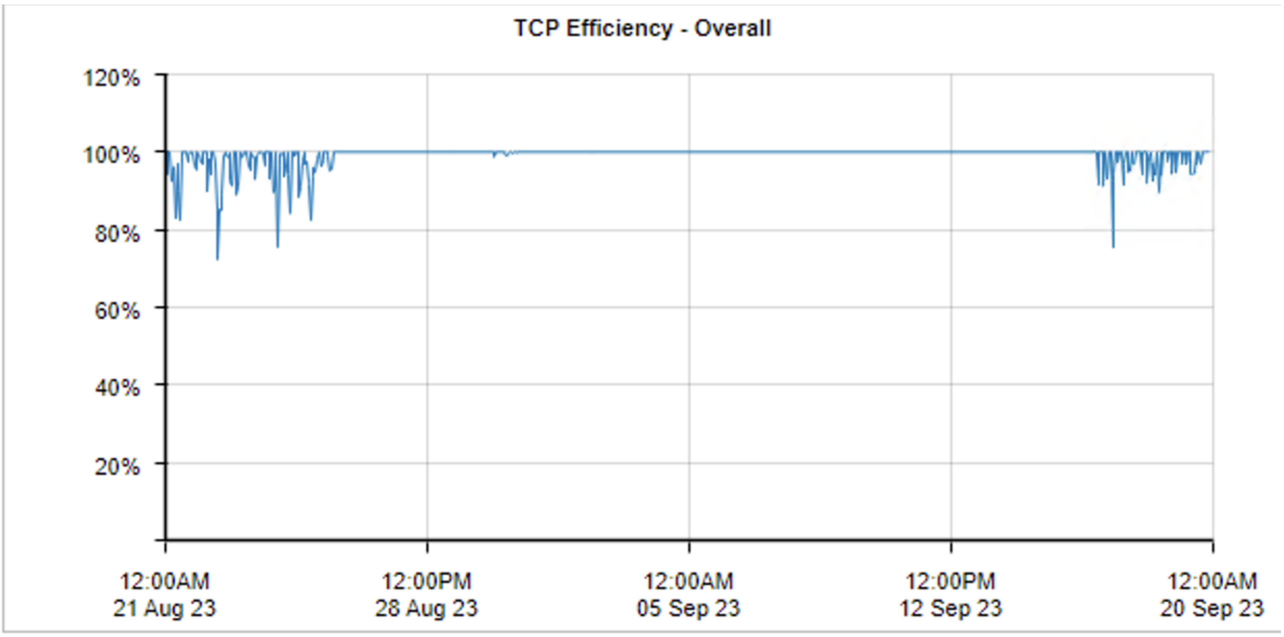
- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring TCP efficiency

The TCP Efficiency report shows the total efficiency of all TCP connections over time. The report data can be categorized by applications, internal hosts or external hosts. You can drill into particular apps or hosts to view the efficiency for particular traffic.

This report answers questions such as:

- Are we experiencing network delays due to TCP inefficiencies?
- Is a particular application or host having troubles due to retransmissions?

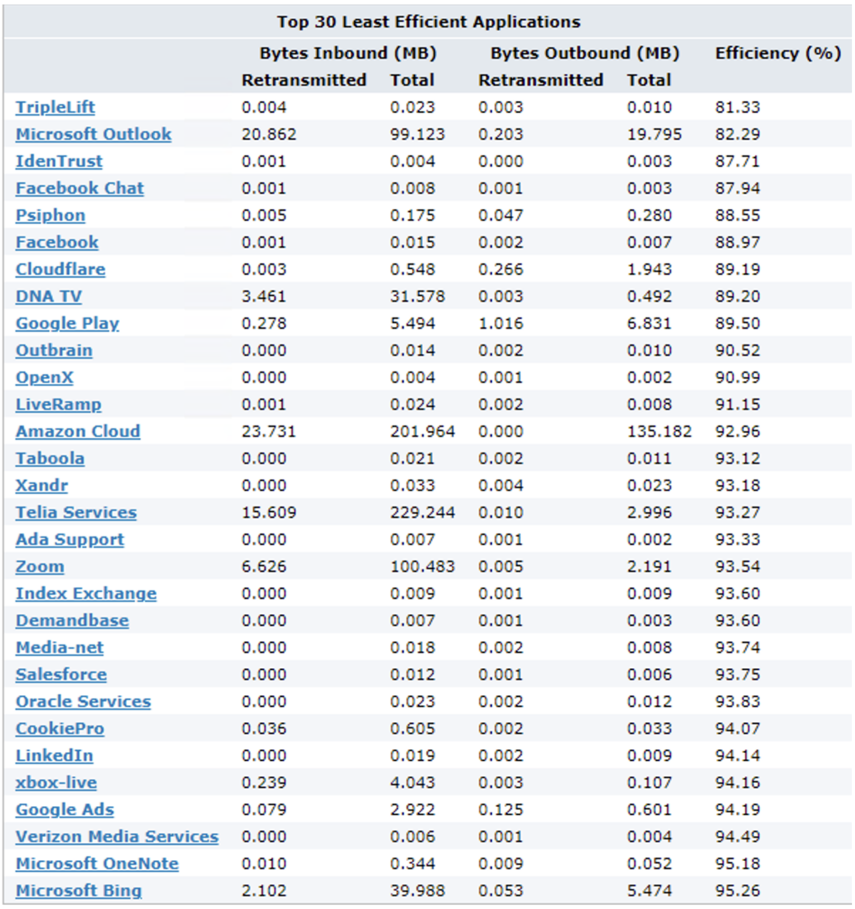


Screenshot 97: The TCP Efficiency report displays TCP connection efficiency over time.

TCP Efficiency is calculated using the formula below:

```
TCP Efficiency = (Total Bytes - Bytes Retransmitted) / Total Bytes
```

The table below shows both retransmitted bytes and efficiency per Application or Host. Each item in the table below can be drilled down to view TCP Efficiency details and a graph for that item.



Top 30 Least Efficient Applications

	Bytes Inbound (MB)		Bytes Outbound (MB)		Efficiency (%)
	Retransmitted	Total	Retransmitted	Total	
TripleLift	0.004	0.023	0.003	0.010	81.33
Microsoft Outlook	20.862	99.123	0.203	19.795	82.29
IdenTrust	0.001	0.004	0.000	0.003	87.71
Facebook Chat	0.001	0.008	0.001	0.003	87.94
Psiphon	0.005	0.175	0.047	0.280	88.55
Facebook	0.001	0.015	0.002	0.007	88.97
Cloudflare	0.003	0.548	0.266	1.943	89.19
DNA TV	3.461	31.578	0.003	0.492	89.20
Google Play	0.278	5.494	1.016	6.831	89.50
Outbrain	0.000	0.014	0.002	0.010	90.52
OpenX	0.000	0.004	0.001	0.002	90.99
LiveRamp	0.001	0.024	0.002	0.008	91.15
Amazon Cloud	23.731	201.964	0.000	135.182	92.96
Taboola	0.000	0.021	0.002	0.011	93.12
Xandr	0.000	0.033	0.004	0.023	93.18
Telia Services	15.609	229.244	0.010	2.996	93.27
Ada Support	0.000	0.007	0.001	0.002	93.33
Zoom	6.626	100.483	0.005	2.191	93.54
Index Exchange	0.000	0.009	0.001	0.009	93.60
Demandbase	0.000	0.007	0.001	0.003	93.60
Media-net	0.000	0.018	0.002	0.008	93.74
Salesforce	0.000	0.012	0.001	0.006	93.75
Oracle Services	0.000	0.023	0.002	0.012	93.83
CookiePro	0.036	0.605	0.002	0.033	94.07
LinkedIn	0.000	0.019	0.002	0.009	94.14
xbox-live	0.239	4.043	0.003	0.107	94.16
Google Ads	0.079	2.922	0.125	0.601	94.19
Verizon Media Services	0.000	0.006	0.001	0.004	94.49
Microsoft OneNote	0.010	0.344	0.009	0.052	95.18
Microsoft Bing	2.102	39.988	0.053	5.474	95.26

Screenshot 98: The TCP Efficiency report displays the 50 least efficient applications.

Where do I find this report?

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

4. Go to Monitor> Service Levels> TCP Efficiency.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring TCP health

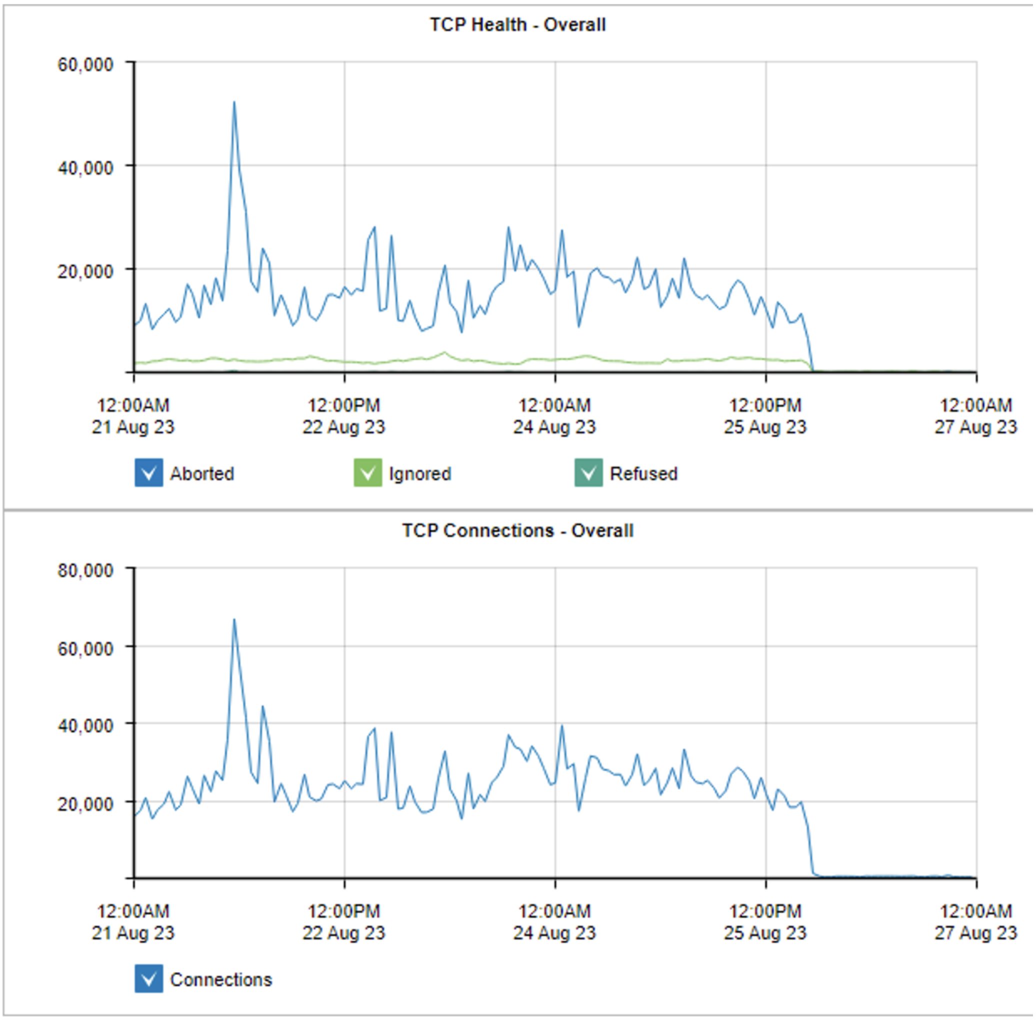
The TCP Health report shows the number of aborted, refused, and ignored connections over time. The report can be categorized by applications, internal hosts, or external hosts. You can drill into particular apps or hosts to view the health for particular traffic.

This report can answers questions such as:

- Why are there so many retransmissions for a particular application or host?"

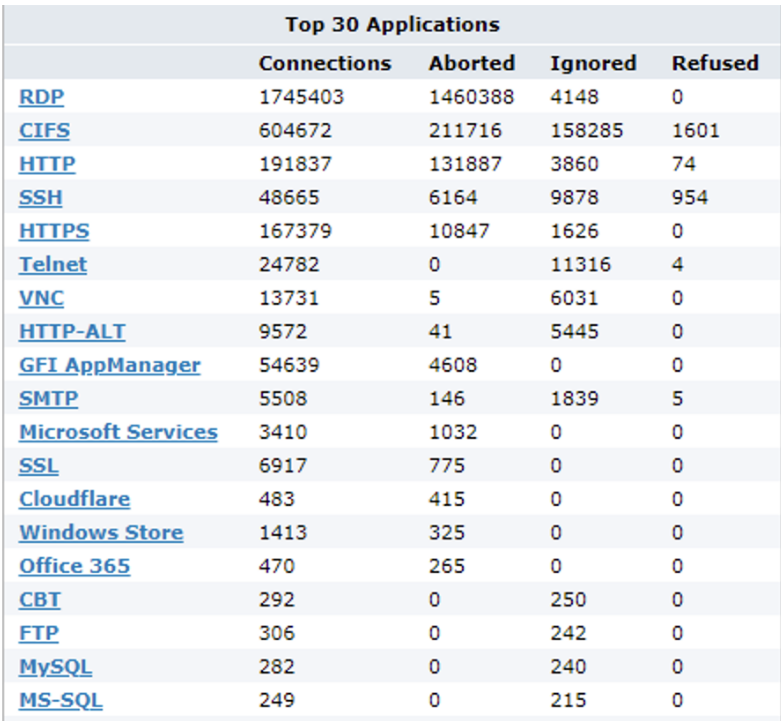
The definitions of aborted, refused and ignored connections used by the TCP Health report:

- **Aborted**— Connections were established, but were closed by a RST (reset) issued by either the client or server rather than a clean close. High numbers of aborted connections can point to network or server problems.
- **Refused**— A SYN packet was observed and a RST or ICMP "connection refused" message was received in response. This usually means the server is up, but the application is unavailable or not working correctly. It can also indicate a TCP port scan is occurring.
- **Ignored**— A SYN packet was observed, but no SYN-ACK response was received. This usually means the server is not responding, does not exist, is not accessible, or is ignoring the connection request. It can also indicate a TCP port scan is occurring.



Screenshot 99: The TCP Health report displays data about connections over time.

The most unhealthy applications or hosts are shown in the table below the charts. The table shows the number of connections, number of aborted, ignored, and refused connections. You can click the name of the application or host to view the TCP Health details and a graph for that item.



Top 30 Applications				
	Connections	Aborted	Ignored	Refused
RDP	1745403	1460388	4148	0
CIFS	604672	211716	158285	1601
HTTP	191837	131887	3860	74
SSH	48665	6164	9878	954
HTTPS	167379	10847	1626	0
Telnet	24782	0	11316	4
VNC	13731	5	6031	0
HTTP-ALT	9572	41	5445	0
GFI AppManager	54639	4608	0	0
SMTP	5508	146	1839	5
Microsoft Services	3410	1032	0	0
SSL	6917	775	0	0
Cloudflare	483	415	0	0
Windows Store	1413	325	0	0
Office 365	470	265	0	0
CBT	292	0	250	0
FTP	306	0	242	0
MySQL	282	0	240	0
MS-SQL	249	0	215	0

Screenshot 100: The TCP Health report displays the applications with the most connections.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to Monitor> Service Levels> TCPHealth.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

» To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.

» To understand how to set the desired time range for a chart, see Setting the Time Range.

» To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

3.2.5 Monitoring applications

This section provides information about various reports that deal with the performance of your application groups, individual applications, unclassified applications, and URLs.

Monitoring application performance on the network

Analyzing the performance of networked applications is a common task for network administrators because every organization relies on these applications to conduct business operations. Too often, the root causes of poor application performance are misunderstood. And when the root cause is unknown or misdiagnosed, solutions typically involve expensive upgrades to increase and enhance network capacity.

The GFI ClearView Appliance is designed to detect network problems, show them to you and help you uncover root causes, so you can take full advantage of the network hardware and capacity your have and only invest in more when it's truly required.

GFI ClearView Appliances monitors and collects several properties of TCP flows of an application converts them to metrics. These metrics are compared to an established threshold and given a score between one and ten, known as the Application Performance Score (APS). The appliance also monitors single metric values within TCP flows for a specified application, known as Application Performance Metrics (APM).

This allows IT departments to use the Application Performance Score (APS) to determine what is performing well, and what is not. APS and APM have thresholds that identify acceptable performance levels for the applications. When the metric values cross the configured threshold, notifications are sent alerting the necessary users so they can review the issue and make the necessary modifications to allow the applications to perform within the threshold level.

Application Performance Score reports can be easily communicated to senior management and to users to help explain how the applications are performing. The reports can also be used to diagnose and determine where issues are in the network. For each APS score, the results for the metrics can identify the specific area within the network that is affecting the performance of the application, for instance server delays, network delays, or jitter. This makes it easier to fix any network issues and get the application back to optimum performance levels.

Monitoring application groups traffic

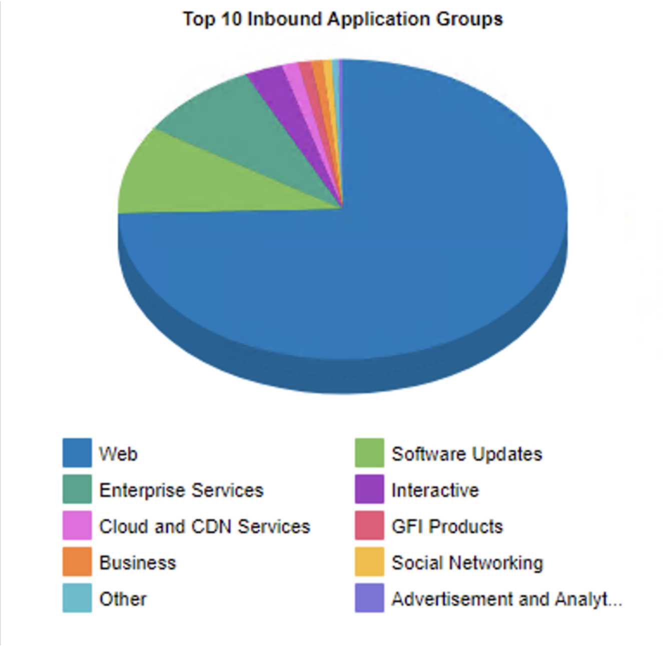
The Traffic Analysis Applications Groups report shows the top application groups by data volume for a selected time period. Inbound and outbound traffic are shown separately.

This report answers questions such as:

- Which application groups may be overrunning my network?
- Is the proportion of traffic for a particular application group what I expect?

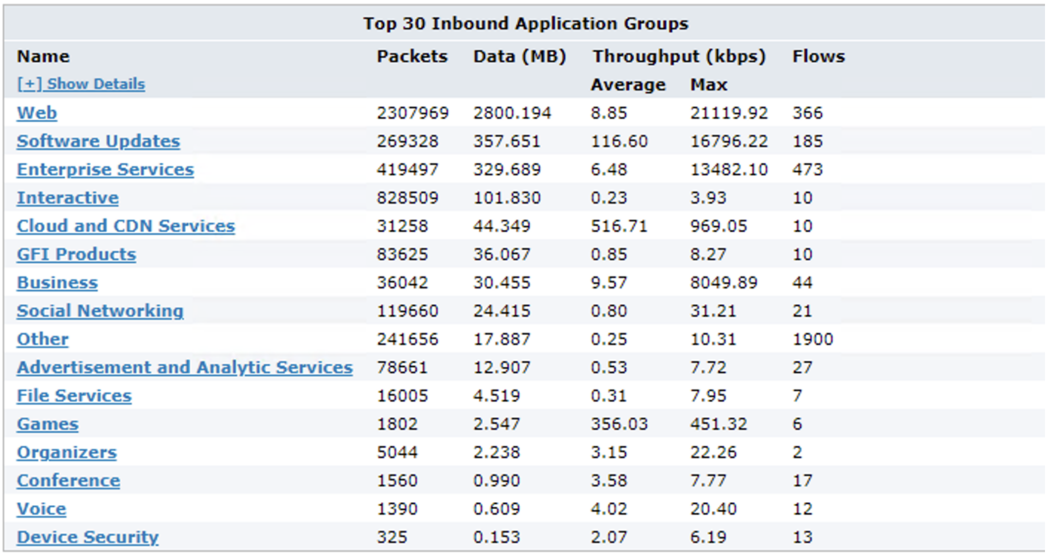
Use this information to determine if you need to create policies to control or protect high data volume application groups.

You can drill into the application group by clicking on the application group name in the tables below the charts. This shows the Hosts Report which lists hosts in the selected application group. You can then drill into a particular application to see the hosts using that application.



Screenshot 101: The Applications Group report displays the top 10 inbound application groups.

The tables at the bottom of the report show for each of the top application groups, the total amount of data, and the maximum and average throughput rates, the number of packets, and the number of flows for the selected time period. More network metrics, such as, round-trip time (RTT), network and server delays, and TCP efficiency can be shown by clicking on the **Show Details** link in the tables.



Top 30 Inbound Application Groups

Name	Packets	Data (MB)	Throughput (kbps)		Flows
[+] Show Details			Average	Max	
Web	2307969	2800.194	8.85	21119.92	366
Software Updates	269328	357.651	116.60	16796.22	185
Enterprise Services	419497	329.689	6.48	13482.10	473
Interactive	828509	101.830	0.23	3.93	10
Cloud and CDN Services	31258	44.349	516.71	969.05	10
GFI Products	83625	36.067	0.85	8.27	10
Business	36042	30.455	9.57	8049.89	44
Social Networking	119660	24.415	0.80	31.21	21
Other	241656	17.887	0.25	10.31	1900
Advertisement and Analytic Services	78661	12.907	0.53	7.72	27
File Services	16005	4.519	0.31	7.95	7
Games	1802	2.547	356.03	451.32	6
Organizers	5044	2.238	3.15	22.26	2
Conference	1560	0.990	3.58	7.77	17
Voice	1390	0.609	4.02	20.40	12
Device Security	325	0.153	2.07	6.19	13

Screenshot 102: The Application Groups report displays traffic volume from the top application groups.

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Applications> Application Groups.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

You can customize the applications objects included in an application group. For more information, refer to Adding and updating application group objects.

To interact with the pie-based reports, you can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic, that means it is 50% of the top items, not 50% through the appliance.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Viewing a network summary of application groups

Each table shows the top application groups together with the number of packets, number of flows data transferred and throughput statistics.

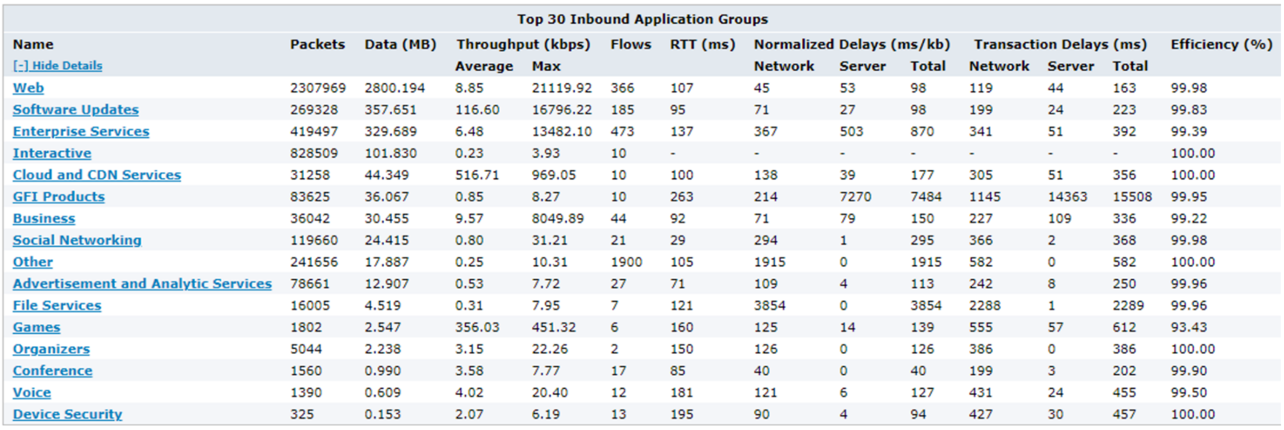
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Monitor> Application Groups**.

6. To expose Round trip time, Normalized Delays, Transaction Delays, and Efficiency statistics for each Application Group, click **Show Details**.



Top 30 Inbound Application Groups

Name	Packets	Data (MB)	Throughput (kbps)		Flows	RTT (ms)	Normalized Delays (ms/kb)			Transaction Delays (ms)			Efficiency (%)
[-] Hide Details			Average	Max			Network	Server	Total	Network	Server	Total	
Web	2307969	2800.194	8.85	21119.92	366	107	45	53	98	119	44	163	99.98
Software Updates	269328	357.651	116.60	16796.22	185	95	71	27	98	199	24	223	99.83
Enterprise Services	419497	329.689	6.48	13482.10	473	137	367	503	870	341	51	392	99.39
Interactive	828509	101.830	0.23	3.93	10	-	-	-	-	-	-	-	100.00
Cloud and CDN Services	31258	44.349	516.71	969.05	10	100	138	39	177	305	51	356	100.00
GFI Products	83625	36.067	0.85	8.27	10	263	214	7270	7484	1145	14363	15508	99.95
Business	36042	30.455	9.57	8049.89	44	92	71	79	150	227	109	336	99.22
Social Networking	119660	24.415	0.80	31.21	21	29	294	1	295	366	2	368	99.98
Other	241656	17.887	0.25	10.31	1900	105	1915	0	1915	582	0	582	100.00
Advertisement and Analytic Services	78661	12.907	0.53	7.72	27	71	109	4	113	242	8	250	99.96
File Services	16005	4.519	0.31	7.95	7	121	3854	0	3854	2288	1	2289	99.96
Games	1802	2.547	356.03	451.32	6	160	125	14	139	555	57	612	93.43
Organizers	5044	2.238	3.15	22.26	2	150	126	0	126	386	0	386	100.00
Conference	1560	0.990	3.58	7.77	17	85	40	0	40	199	3	202	99.90
Voice	1390	0.609	4.02	20.40	12	181	121	6	127	431	24	455	99.50
Device Security	325	0.153	2.07	6.19	13	195	90	4	94	427	30	457	100.00

7. To view the data for individual applications within a group, click the application group name.

Viewing application traffic volume

The Applications report shows the top applications by volume and their average throughput. Volume and throughput data for single applications can be graphed by clicking the filter icon for the desired application in the data table below the graphs. Inbound and outbound LAN application traffic is reported separately.

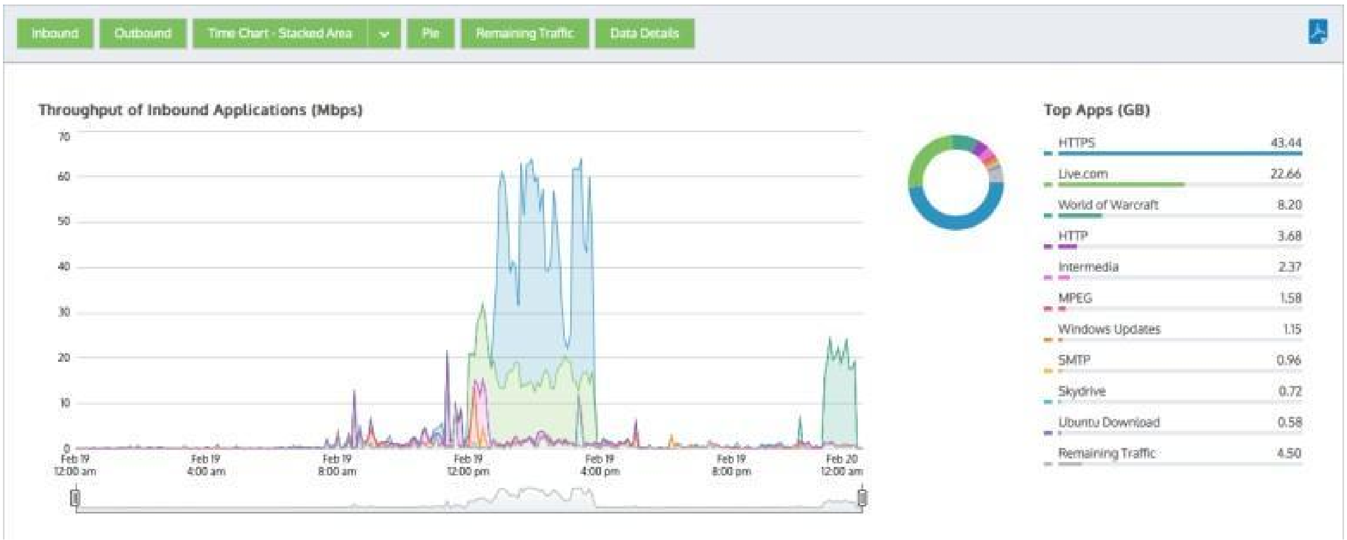
To show all application traffic, add a category to represent the remaining application traffic on your network. Doing this allows the cumulative stack on the throughput chart to represent all the application traffic moving through the appliance.

This will help you understand the significance of the top applications relative to the whole. In addition to showing a stacked cumulative view, you can display the throughput as a line chart with a common zero baseline. You can also display the application volumes as a pie chart.

These charts can answer questions such as:

- What are the top applications on my network?
- Are those top applications significant relative to the entire traffic?
- How much bandwidth does my FTP application typically take?
- Could one application be choking out the other application traffic?
- Do any of my top applications appear to be limited?

Using this information, you can determine if you need to create policies for high data volume applications and applications that tend to have large data volume spikes. You may want to create protection policies for your business critical apps and limiting policies for high volume non-business critical applications like recreational applications.



Top Apps (GB)

HTTPS	43.44
Live.com	22.66
World of Warcraft	8.20
HTTP	3.68
Intermedia	2.37
MPEG	1.58
Windows Updates	1.15
SMTP	0.96
Skydrive	0.72
Ubuntu Download	0.58
Remaining Traffic	4.50

Screenshot 103: The Applications report shows traffic volume graphed over time.

> **NOTE**
>
> Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

If you drilled into the applications chart from any of the virtual circuit, subnets, or hosts charts, then the relevant virtual circuit, subnet, or host will be shown on the filter bar below the button bar. To turn off the filtering, click on the close 'x' in the filter tag.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> Applications> Applications.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To filter the report data

Various components on the screen can be toggled on and off by clicking buttons above the charts. Note that when generating a pdf report of this screen, the toggle states are taken into account. That is, if you had toggled off the outbound charts, they will not be present in the pdf.

- **Host Type:** When you first load the Hosts report, Internal hosts are graphed by default. Click the Internal hosts button and then select External hosts to change the type. Note that you cannot graph both internal and external hosts at the same time.
- **Traffic Type (Inbound/Outbound):** By default, both Inbound and Outbound traffic is graphed. Click either the Inbound or Outbound option to hide the data, including all the carts and the data tables below the charts.
- **Chart Type:** Toggles on or off the time series charts and allows selecting stacked area display versus a line chart dis- play.
- **Pie:** Toggles on or off a colour-coded Pie chart to the left of the Top Listeners and Top Talkers list.
- **Remaining Traffic:** Append or hide the Remaining Traffic category below the Top Listeners and Top Talkers lists.

This option toggles on or off the presence of a category for all the remaining applications summed together.

- **Data Details:** Toggles on or off the data tables below the time series charts.
- **Mouse Hover:** Hover the mouse pointer over the graph to view data throughput at a given date and time.

Turning on or off the remaining traffic category

Toggle the Remaining Traffic button on the button bar. When toggled on, a grey chart series will appear in all charts (throughput, pie, top applications) representing all the applications on your network that are not explicitly represented in the top applications. If the remaining applications show vastly more data volume than the top applications, then the top applications may look insignificant relative to the total, and so you may need to toggle off the remaining traffic category to see the relative differences and usage patterns of the top applications.

Changing the throughput chart to stacked area charts or line charts

Press the down arrow next to the dropdown list at the top of the page and choose which chart type to show. The line chart shows the applications against the common zero baseline so they can be compared to each other and the pattern of a specific application is clearer. You can look for particular patterns such as spikes or flat tops.

Determining if one or more applications may be choking out the other application traffic

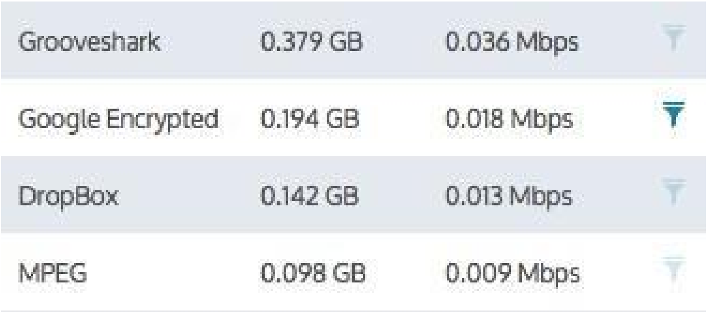
View the throughput charts with the remaining traffic category toggled on. For any periods where the cumulative throughput is especially high (compared to the pipe size that this appliance is managing) is there an application or two that is consuming a significant portion of the bandwidth. If so, that application may be choking out other applications and would be a candidate for control. Please note that you may need to go to the virtual circuit chart and filter the applications by the individual virtual circuits to understand whether an application is choking out others since the virtual circuits share bandwidth and an application may overrun one virtual circuit but not others.

Determining if any of the top applications appear to be limited

View the throughput charts as a line chart with the remaining traffic category toggled off. If any of the lines representing the applications have raised flat tops, this may represent that the application is being limited by the capacity of your pipe.

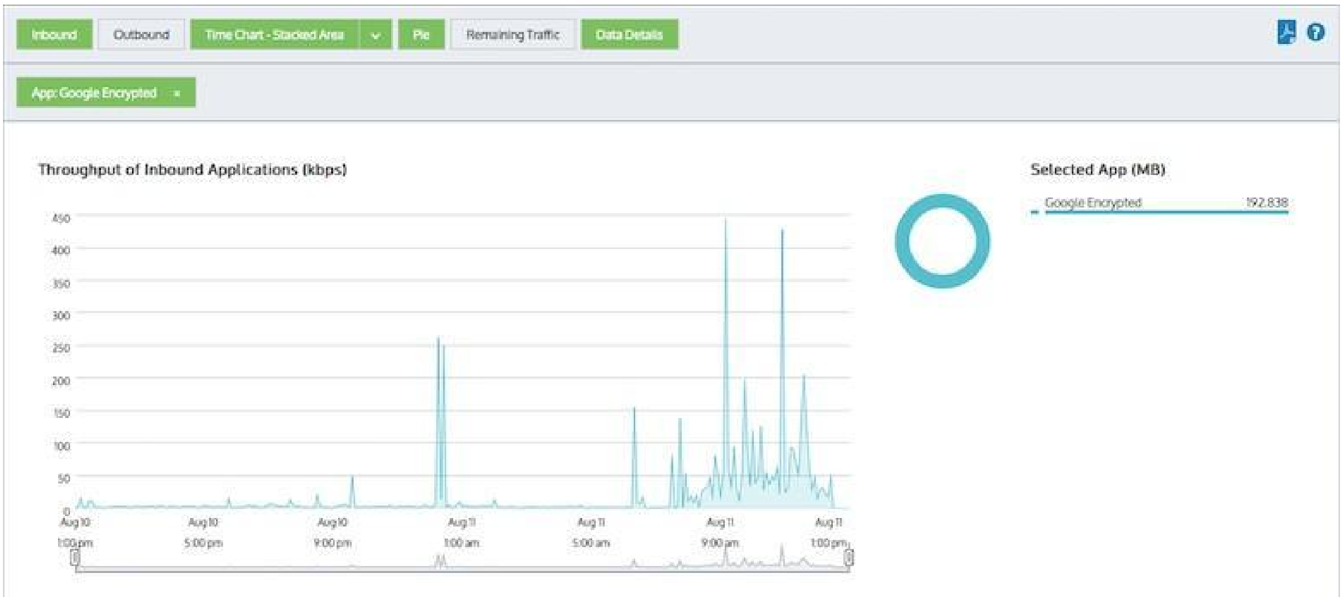
Charting any single application

In the data table, each application has a filter icon on the right-hand-side of the row. By clicking on the filter icon, as shown below for Google Encrypted, only the selected application will be charted.



Grooveshark	0.379 GB	0.036 Mbps	▼
Google Encrypted	0.194 GB	0.018 Mbps	▼
DropBox	0.142 GB	0.013 Mbps	▼
MPEG	0.098 GB	0.009 Mbps	▼

Screenshot 104: Click filter icon beside desired application to chart that application.



Screenshot 105: Applications are filtered to only show 'Google Encrypted'

While in filter mode, any other application filter icon can be clicked to change which application is charted.

To remove this filter and return to the top application set, click the 'x' on the green 'App: Google Encrypted' filter tag.

To show more applications or fewer applications in the top applications chart and the throughput chart

The number of applications shown are configurable by using the **Chart Items** setting on the **Configuration > System > Setup > Monitoring** page. Please note that this configuration applies to all charts on the appliance. See Monitoring Configuration.

How do I interact with the new time-series & bar chart reports?

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how the charts interact and what the toggle buttons do, see Understanding How Charts Relate.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand the difference between inbound and outbound traffic, see Understanding Traffic Direction.
- To understand how many data points are shown for each time period, see Understanding Traffic Granularity.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

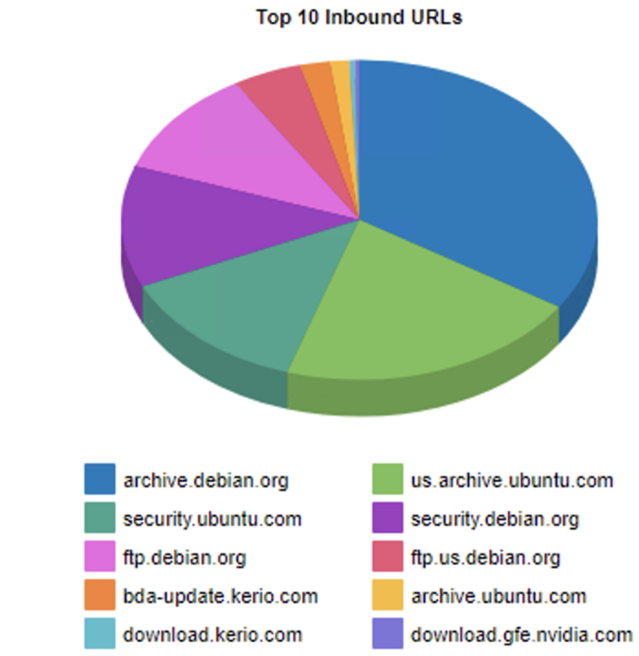
Monitoring URLs visited

The URLs report shows the top URLs visited by data volume for the selected time period. The URLs report shows inbound traffic separately from outbound traffic. This report answers questions such as:

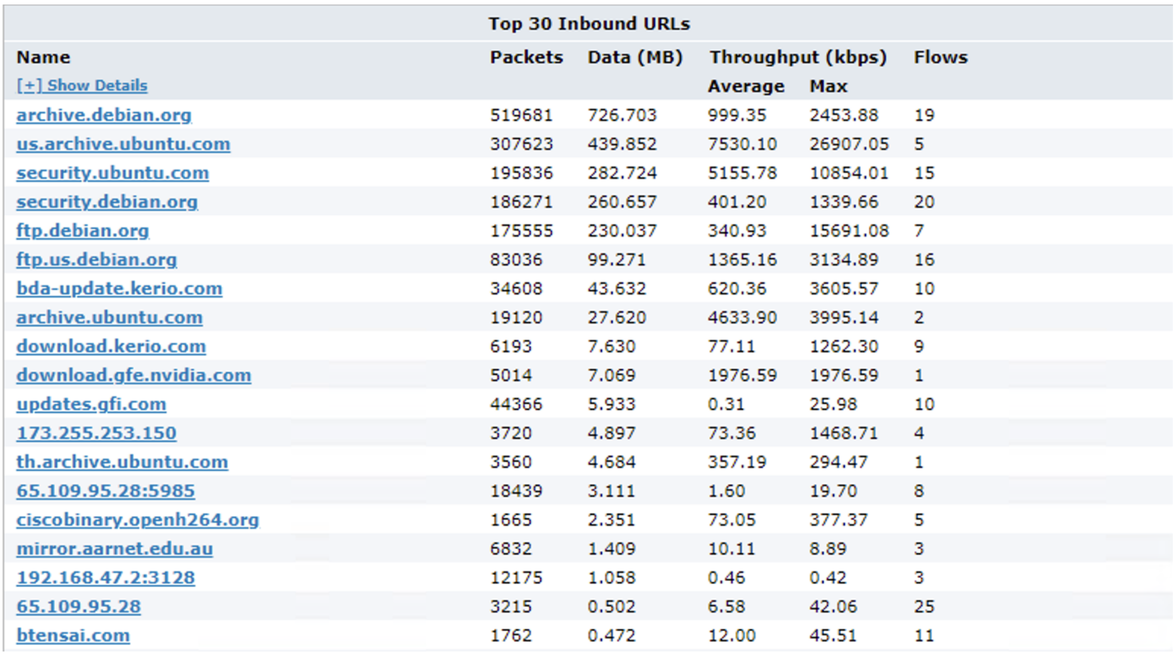
- Which websites are generating the most traffic?

Using this information you can determine if you need to create applications based on URLs and create policies to control or protect high data volume URLs.

The URL names are represented as a domain/host name. Drill into the URLs by clicking on the URL name in the tables below the charts. This will show the Hosts Report which lists hoists that visited the URL.



The tables at the bottom of the report displays the total amount of data and the maximum and average throughput rates, the number of packets, and the number of flows for the selected time period for the top URLs. More network metrics like round-trip time (RTT), network and server delays, and TCP efficiency can be shown by clicking on the **Show Details** link in the tables.



Top 30 Inbound URLs					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
[+] Show Details			Average	Max	
archive.debian.org	519681	726.703	999.35	2453.88	19
us.archive.ubuntu.com	307623	439.852	7530.10	26907.05	5
security.ubuntu.com	195836	282.724	5155.78	10854.01	15
security.debian.org	186271	260.657	401.20	1339.66	20
ftp.debian.org	175555	230.037	340.93	15691.08	7
ftp.us.debian.org	83036	99.271	1365.16	3134.89	16
bda-update.kerio.com	34608	43.632	620.36	3605.57	10
archive.ubuntu.com	19120	27.620	4633.90	3995.14	2
download.kerio.com	6193	7.630	77.11	1262.30	9
download.gfe.nvidia.com	5014	7.069	1976.59	1976.59	1
updates.gfi.com	44366	5.933	0.31	25.98	10
173.255.253.150	3720	4.897	73.36	1468.71	4
th.archive.ubuntu.com	3560	4.684	357.19	294.47	1
65.109.95.28:5985	18439	3.111	1.60	19.70	8
ciscobinary.openh264.org	1665	2.351	73.05	377.37	5
mirror.aarnet.edu.au	6832	1.409	10.11	8.89	3
192.168.47.2:3128	12175	1.058	0.46	0.42	3
65.109.95.28	3215	0.502	6.58	42.06	25
btensai.com	1762	0.472	12.00	45.51	11

Screenshot 106: The URLs report displays traffic volume by inbound URL.

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://`ClearView`_IP_address`).

2. Key-in the **User Name** and **Password**.

3. Click **Login**.

Go to **Monitor> Applications> URLs**.

To interact with the pie-based reports, you can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic, that means it is 50% of the top items, not 50% through the appliance.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

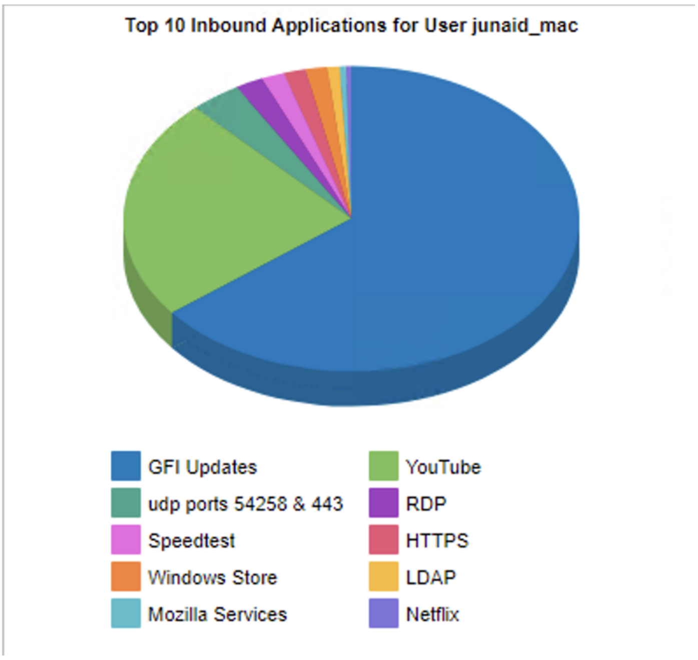
Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

Drilling into application data

The Application Drill-in report shows application specific traffic data volume for a selected time period. Inbound and outbound traffic are shown separately. This report answers questions such as:

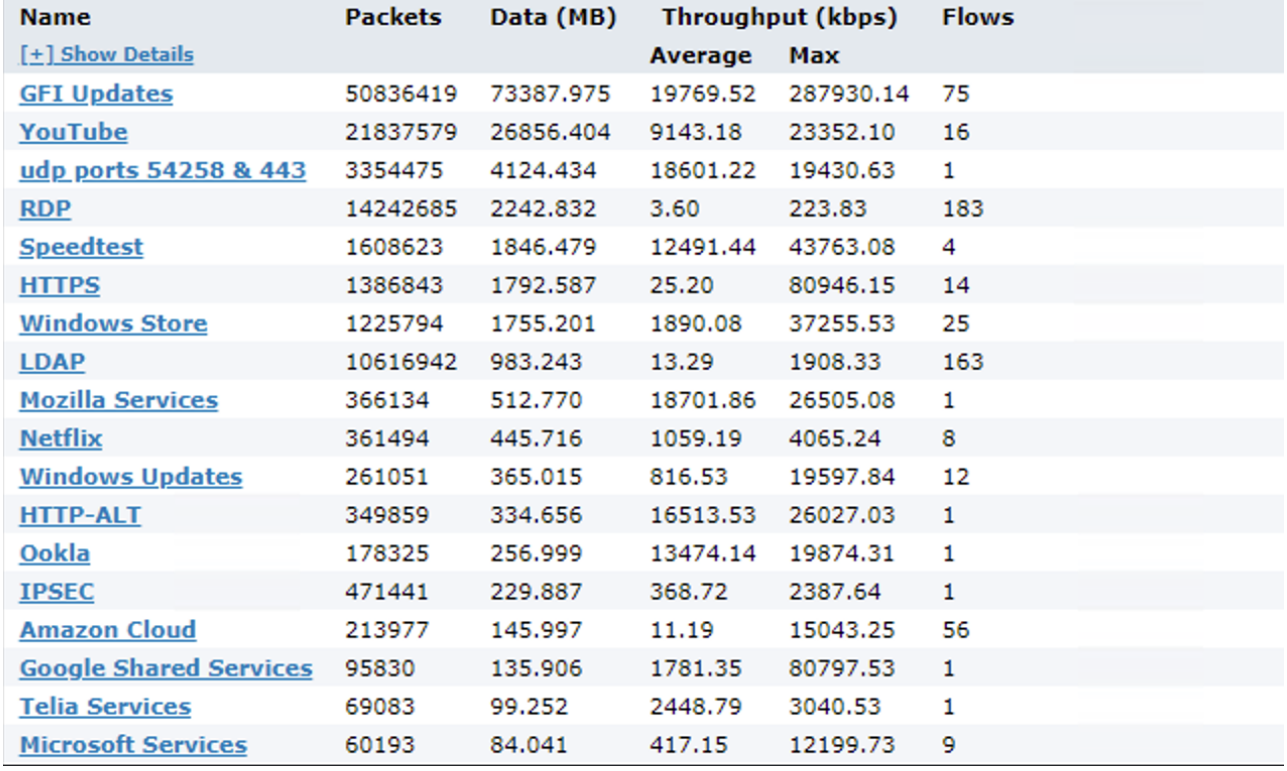
- Which applications are part of the application group that I clicked on?
- Which applications did a particular user or host use?

You can drill into the application by clicking on the application name in the tables below the charts. This will show the Hosts Report which lists hosts that used the application.



Screenshot 107: The Applications report displays a graph of traffic volume by application.

The tables at the bottom of the report show the total amount of data, the maximum and average throughput rates, the number of packets, and the number of flows by application for the selected time period. Click on the **Show Details** link in the Name column to see more metrics like round-trip time (RTT), network and server delays, and TCP efficiency.



Name	Packets	Data (MB)	Throughput (kbps)		Flows
[+] Show Details			Average	Max	
GFI Updates	50836419	73387.975	19769.52	287930.14	75
YouTube	21837579	26856.404	9143.18	23352.10	16
udp ports 54258 & 443	3354475	4124.434	18601.22	19430.63	1
RDP	14242685	2242.832	3.60	223.83	183
Speedtest	1608623	1846.479	12491.44	43763.08	4
HTTPS	1386843	1792.587	25.20	80946.15	14
Windows Store	1225794	1755.201	1890.08	37255.53	25
LDAP	10616942	983.243	13.29	1908.33	163
Mozilla Services	366134	512.770	18701.86	26505.08	1
Netflix	361494	445.716	1059.19	4065.24	8
Windows Updates	261051	365.015	816.53	19597.84	12
HTTP-ALT	349859	334.656	16513.53	26027.03	1
Ookla	178325	256.999	13474.14	19874.31	1
IPSEC	471441	229.887	368.72	2387.64	1
Amazon Cloud	213977	145.997	11.19	15043.25	56
Google Shared Services	95830	135.906	1781.35	80797.53	1
Telia Services	69083	99.252	2448.79	3040.53	1
Microsoft Services	60193	84.041	417.15	12199.73	9

Access this report by drilling in from other reports, such as application group, hosts, users, conversations, subnets.

To interact with the pie-based reports, you can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic, that means it is 50% of the top items, not 50% through the appliance.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Disabling calculations of application performance metrics

Stop the GFI ClearView Appliance from calculating Round Trip Time (RTT), Network and Server Delay, Loss and Efficiency, and TCP Health.

> **IMPORTANT**
> Application performance metrics must be enabled to calculate Application Performance Scores.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Configuration > System > Setup** and switch to the **Monitoring** tab.

6. In the ASAM section, uncheck the **Performance Metrics** checkbox.

7. Click **Apply Changes**.

8. To save the changes to the configuration file, in the status bar click the **Unsaved changes** menu and select **Save configuration changes**.

3.2.6 Monitoring network users

The Users report shows the top users by data volume for a selected time period. Inbound and outbound traffic are reported separately. You can view internal and external users in the report, answering questions such as:

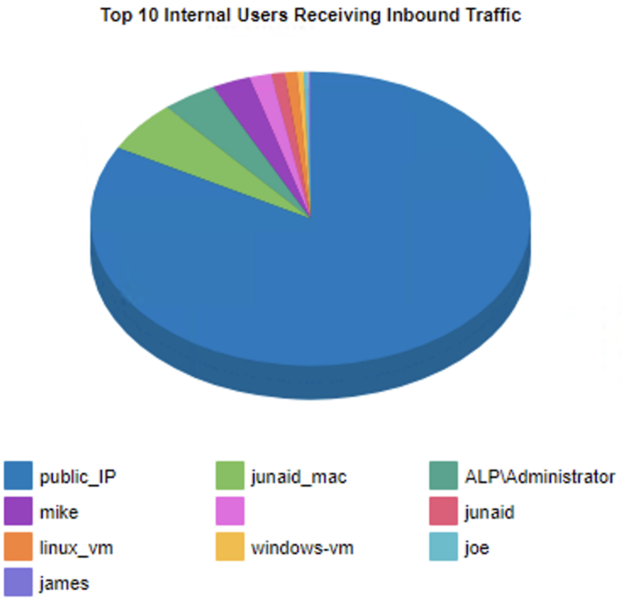
- What internal users are the top talkers and top listeners?
- Which external users are top talkers?
- Which external users are top listeners?
- Is one user choking the network?

Using this information, you can determine if you need to create policies for these high data volume users. You may want to create protection policies for your important users, like your CEO or finance department, or create control policies to limit users who are abusing the network.

In this report, users are associated with IP addresses. Network traffic flows from one host to another and typically, one host is considered internal to your network while the other is considered external.

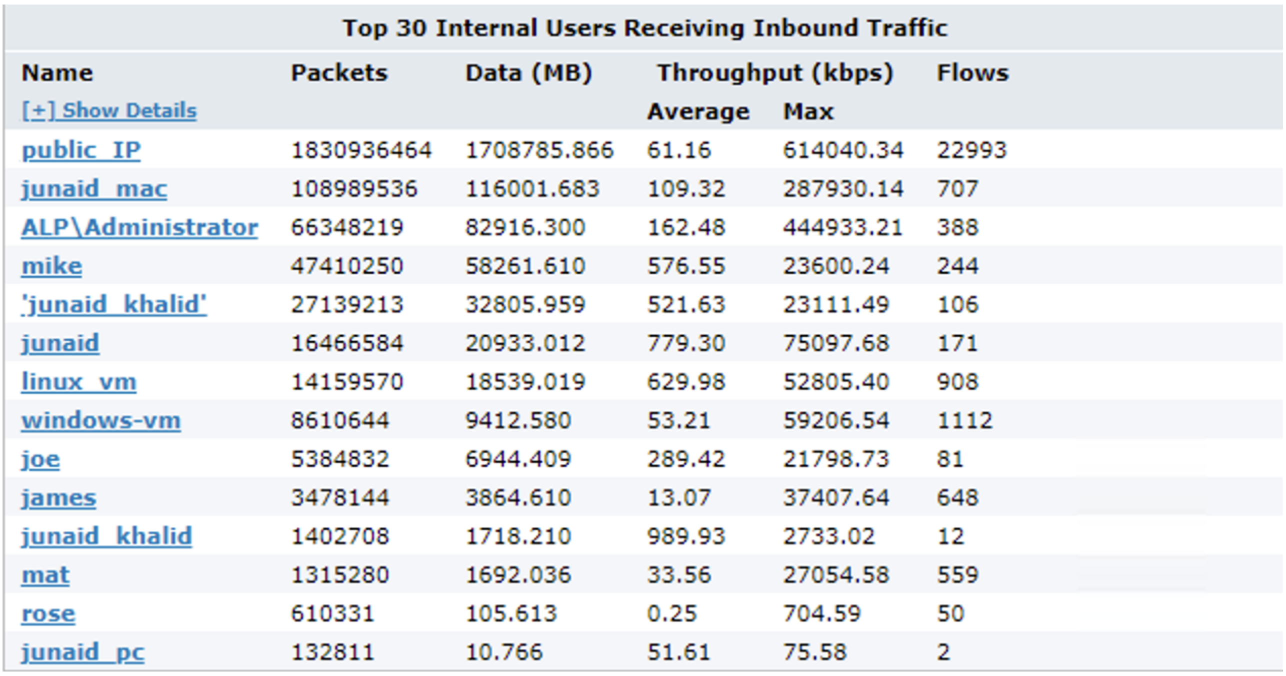
Hosts that fall into a network object defined as internal are considered internal to your network. Hosts that fall into a network object defined as external are considered external to your network. Keep in mind that the traffic is inbound and outbound relative to your LAN – not relative to the host or user. Inbound traffic for an external user means a user was sending data into your network.

You can drill into the user by clicking on the user name in the tables below the charts. This will show the Applications Report for the user that you drilled into. You can then use the selector on the Applications report page to show URLs or conversations or hosts that involved the user.



Screenshot 108: The Users report displays traffic volume by user.

The tables at the bottom of the report shows for each of the top users, the total amount of data, and the maximum and average throughput rates, the number of packets, and the number of flows for the selected time period. More network metrics, such as, round-trip time (RTT), network and server delays, and TCP efficiency can be shown by clicking on the **Show Details** link in the tables.



Top 30 Internal Users Receiving Inbound Traffic

Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	 Max	Flows
public_IP	1830936464	1708785.866	61.16	614040.34	22993
junaid_mac	108989536	116001.683	109.32	287930.14	707
ALP\Administrator	66348219	82916.300	162.48	444933.21	388
mike	47410250	58261.610	576.55	23600.24	244
'junaid_khalid'	27139213	32805.959	521.63	23111.49	106
junaid	16466584	20933.012	779.30	75097.68	171
linux_vm	14159570	18539.019	629.98	52805.40	908
windows-vm	8610644	9412.580	53.21	59206.54	1112
joe	5384832	6944.409	289.42	21798.73	81
james	3478144	3864.610	13.07	37407.64	648
junaid_khalid	1402708	1718.210	989.93	2733.02	12
mat	1315280	1692.036	33.56	27054.58	559
rose	610331	105.613	0.25	704.59	50
junaid_pc	132811	10.766	51.61	75.58	2

Screenshot 109: The table on the Users report shows traffic volume metrics broken down by user.

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> Users**.

To show only internal users or external users, use the **Select Users To View** selector at the top of the page.

To interact with the pie-based reports, you can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic, that means it is 50% of the top items, not 50% through the appliance.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

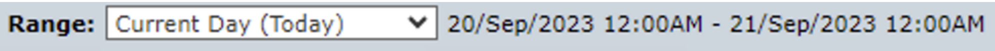
Setting the time period for a report

To limit report data to specific periods of time, set the date range. Viewing reports by date range is available on all reports except Realtime reports.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

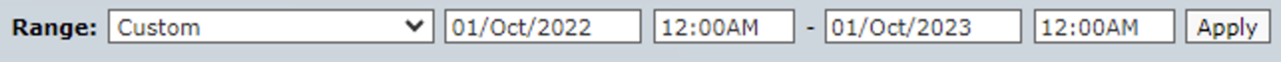
5. Select a report from the Monitor list.

6. Beside the title of the report, select the desired date range from the drop down list.



Range: Current Day (Today) 20/Sep/2023 12:00AM - 21/Sep/2023 12:00AM

7. To specify a custom date range, in the drop down list select **Custom**. Select the start and end date and time to include in the report. After the date range is selected, the graphs and charts are immediately updated.



Range: Custom 01/Oct/2022 12:00AM - 01/Oct/2023 12:00AM

Temporal granularity of stored data

The GFI ClearView Appliance stores data for the following time intervals:

- 2 years of data - this year, previous year & last 12 months
- 2 months of data - this month, previous month & last 30 days
- 2 weeks of data - this week, previous week & last 7 days
- 2 days of data - today, yesterday & last 24 hours
- 1 day of data - this hour, last hour & last 60 minutes, last 5 minutes

For the Applications, URLs, Users, Hosts, Conversations and Subnets Reports, the data is stored at:

- Hourly granularity for up to 2 days (today, yesterday, this hour, previous hour)
- Daily granularity for up to 2 months (this week, last week, this month and last month)
- Monthly granularity for up to 2 years (this year, last year)

For the Interface, Network, Service Levels, System the data is stored at: » 10 second granularity for 1 day (except Network)

- 5 minute granularity for 2 weeks
- 30 minute granularity for 2 months
- 60 minute granularity for 6 months
- 24 hour granularity for 2 years

3.2.7 Monitoring hosts traffic volume

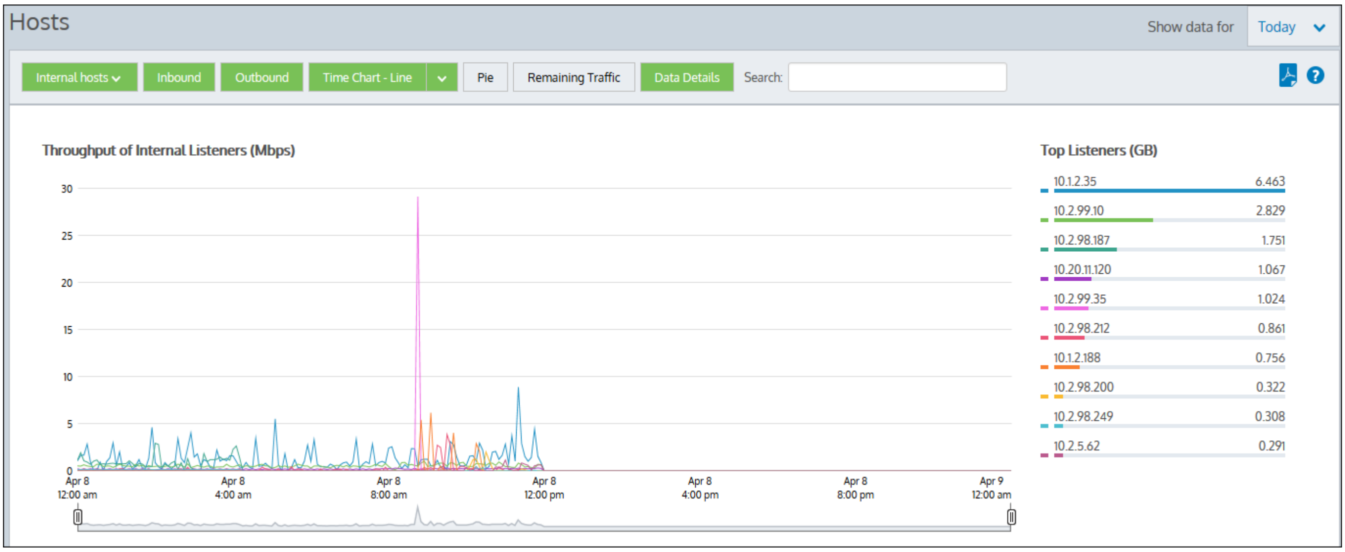
The Hosts report shows the top hosts by data volume for the selected time period. For more information, refer to Setting the time period for a report.

Traffic inbound into your LAN is reported separately from the outbound traffic. You can view internal and external hosts and data is graphed separately for Top Listeners and Top Talkers. This allows multi-site enterprises to monitor corporate systems while excluding Internet servers.

This report answers questions such as:

- What internal hosts are the top talkers and top listeners?
- Which external hosts are top talkers from which internal hosts are retrieving information?
- Which external hosts are top listeners from which internal hosts are sending information to?
- Could one host be choking out my network?

Use this information to determine if you need to create policies for these high data volume hosts. You may want to create protection policies for your business critical server machines or create control policies to limit hosts that are abusing the network.



Top Listeners (GB)

10.1.2.35	6.463
10.2.99.10	2.829
10.2.98.187	1.751
10.20.11.120	1.067
10.2.99.35	1.024
10.2.98.212	0.861
10.1.2.188	0.756
10.2.98.200	0.322
10.2.98.249	0.308
10.2.5.62	0.291

Screenshot 110: The Hosts report displays traffic volume over time and top listeners.

> **AVERAGE BANDWIDTH**
>
> Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

What are hosts?

Hosts are IP Address endpoint's in IP transactions and are usually client PCs or servers. During a flow, traffic flows from one host to another. Typically, one host is considered internal to your network; the other is external:

- Hosts that fall into a network object that was defined as internal are considered internal to your network
- Hosts that fall into a network object that was defined as external are considered external to your network

Traffic is inbound and outbound relative to your LAN – not relative to the host. Therefore, inbound traffic for an external host means that host was sending data inbound into your network.

Where do I find this report?

To access the report:

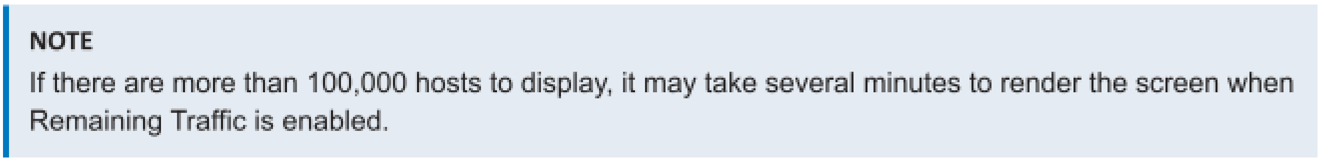
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> Hosts**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To filter the report data

Toggle various chart elements on and off by clicking the buttons above the charts. Note that when generating a PDF report of this screen, the toggle states are taken into account. That is, if you had toggled off the outbound charts, they will not be present in the PDF.

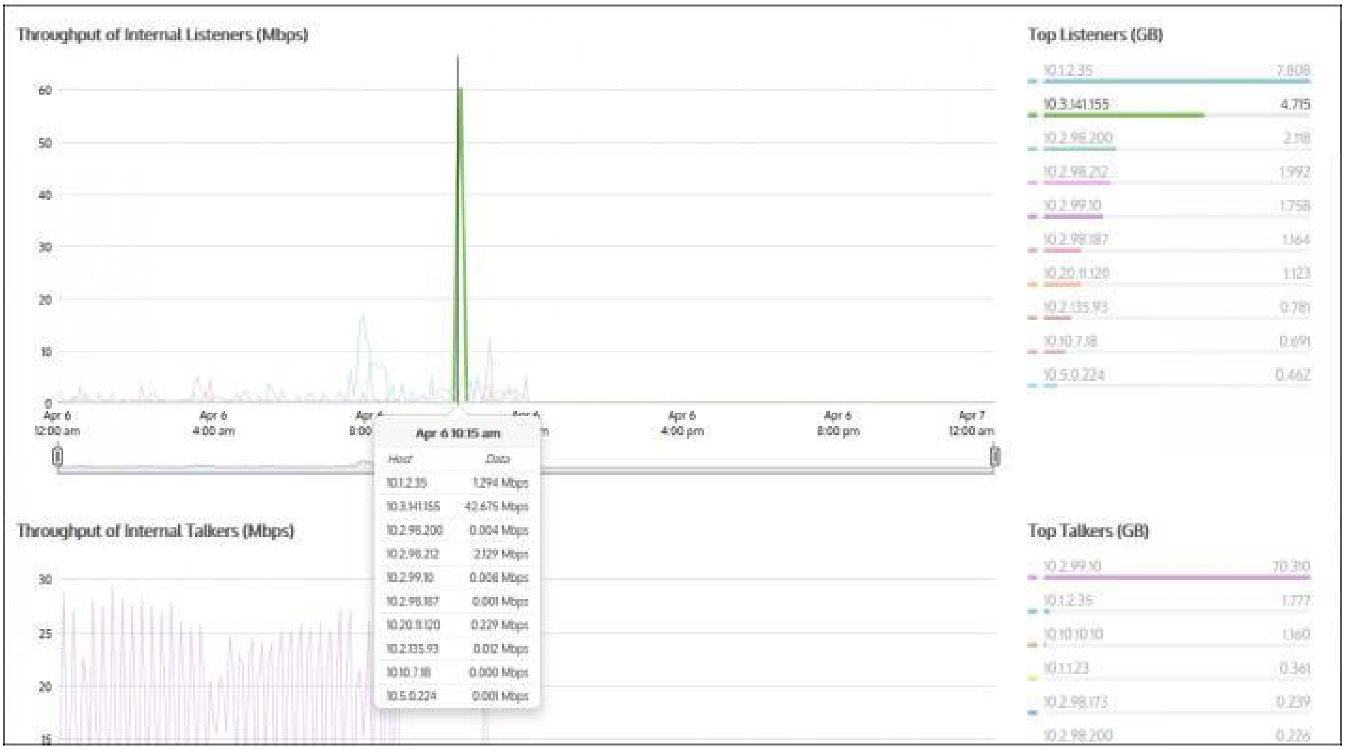
- **Host Type:** When you first load the Hosts report, Internal hosts are graphed by default. Click the Internal hosts button and then select External hosts to change the type. Note that you cannot graph both internal and external hosts at the same time.
- **Traffic Type (Inbound/Outbound):** By default, both Inbound and Outbound traffic is graphed. Click either the Inbound or Outbound option to hide the data. When viewing Internal hosts, hiding the Inbound data toggles off the Top Listeners data from the graphs, whereas hiding the Outbound data toggles off the Top Talkers data. When viewing External hosts, the opposite is true.
- **Chart Type:** The chart is initially mapped as a Stacked Area , but you can change the format to Line Chart if necessary.
- **Pie:** Toggles on or off a colour-coded Pie chart to the left of the Top Listeners and Top Talkers list.
- **Remaining Traffic:** Append or hide the Remaining Traffic data below the Top Listeners and Top Talkers lists. Reamin- ing traffic represents the remaining application traffic on your network and the cumulative stack on the throughput chart represents all the hosts communicating through the appliance. If the remaining traffic show vastly more data volume than the top hosts, then the top hosts may look insignificant relative to the total, and so you may need to toggle off the remaining traffic category to see the relative differences and usage patterns of the top hosts.



NOTE

If there are more than 100,000 hosts to display, it may take several minutes to render the screen when Remaining Traffic is enabled.

- **Data Details:** Toggles on or off the data tables below the time series charts.
- **Mouse Hover:** Hover the mouse pointer over the graph to view data throughput at a given date and time. Refer to Chart Interactions - Drill in & Data brush in WUI Guided Tour for details.



Apr 6 10:15 am

Host	Data
10.1.2.35	1.294 Mbps
10.3.141.155	42.675 Mbps
10.2.98.200	0.004 Mbps
10.2.98.212	2.129 Mbps
10.2.99.10	0.008 Mbps
10.2.98.187	0.001 Mbps
10.20.11.120	0.229 Mbps
10.2.135.93	0.012 Mbps
10.10.7.18	0.000 Mbps
10.5.0.224	0.001 Mbps

Top Listeners (GB)

10.1.2.35	7.808
10.3.141.155	4.715
10.2.98.200	2.118
10.2.98.212	1.992
10.2.99.10	1.758
10.2.98.187	1.164
10.20.11.120	1.123
10.2.135.93	0.781
10.10.7.18	0.691
10.5.0.224	0.462

Top Talkers (GB)

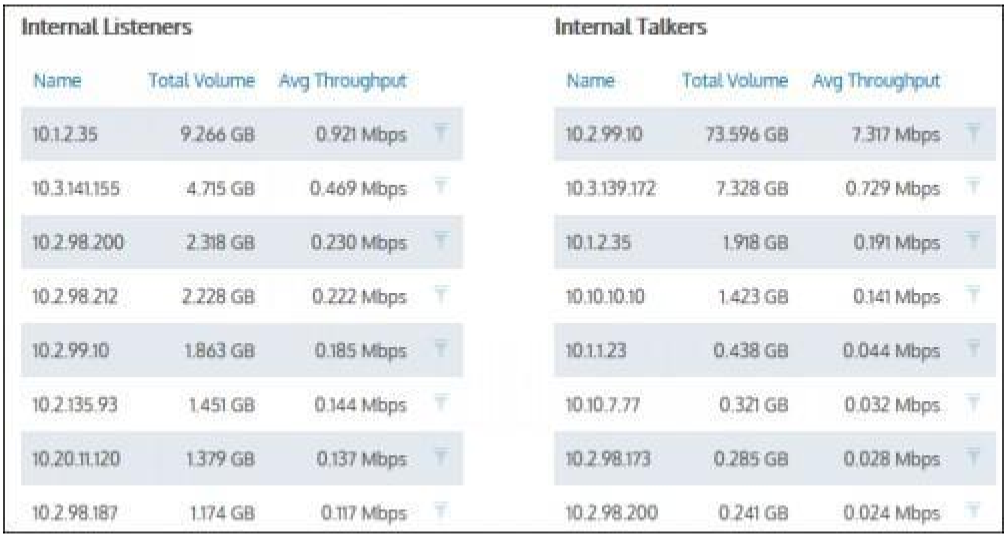
10.2.99.10	70.310
10.1.2.35	1.777
10.10.10.10	1.160
10.1.1.23	0.361
10.2.98.173	0.239
10.2.98.200	0.226

Screenshot 111: The Hosts report displays throughput by internal listeners over time broken down by top listeners and talkers.

Drilling down into report data

Drill into the host data by clicking on a host in the Top Listeners or Top Talkers list (located to the right of the graphs). Click a particular host to view the Applications Report for the host that you selected. You can then use the selector on the Applications Report page to show URLs or conversations that involve the host.

The tables at the bottom of the Hosts report information for the top listeners and talkers and include the IP Address, the Total Volume of data, and the Average Throughput rates. Click on any entry in the table to open the Applications Report for that specific host.



Internal Listeners

Name	Total Volume	Avg Throughput
10.1.2.35	9.266 GB	0.921 Mbps
10.3.141.155	4.715 GB	0.469 Mbps
10.2.98.200	2.318 GB	0.230 Mbps
10.2.98.212	2.228 GB	0.222 Mbps
10.2.99.10	1.863 GB	0.185 Mbps
10.2.135.93	1.451 GB	0.144 Mbps
10.20.11.120	1.379 GB	0.137 Mbps
10.2.98.187	1.174 GB	0.117 Mbps

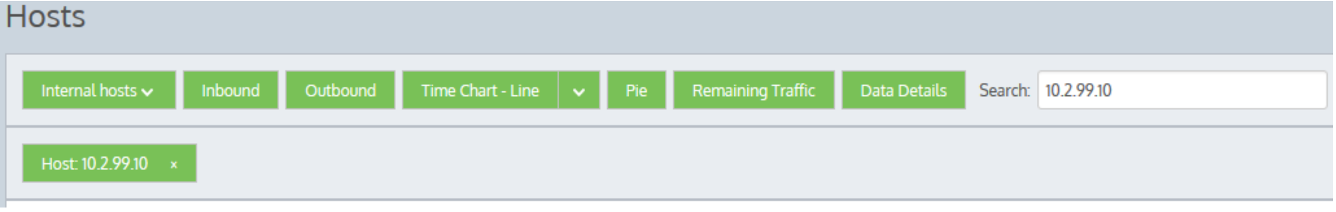
Internal Talkers

Name	Total Volume	Avg Throughput
10.2.99.10	73.596 GB	7.317 Mbps
10.3.139.172	7.328 GB	0.729 Mbps
10.1.2.35	1.918 GB	0.191 Mbps
10.10.10.10	1.423 GB	0.141 Mbps
10.1.1.23	0.438 GB	0.044 Mbps
10.10.7.77	0.321 GB	0.032 Mbps
10.2.98.173	0.285 GB	0.028 Mbps
10.2.98.200	0.241 GB	0.024 Mbps

Screenshot 112: Drilling down into hosts data.

Searching for a specific host

If the host you are looking for is not listed in the Top hosts, you can use the search function to locate data for a single host only. Type a single IP Address in the Search field to locate data for a particular host. If entering an IPv6 host, use the full IPv6 address only. When the data is retrieved, the individual host is shown on the filter bar below the button bar. To turn off the filtering, click on the close 'x' in the filter tag.



How do I interact with the new time-series & bar chart reports?

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how the charts interact and what the toggle buttons do, see Understanding
- How Charts Relate. To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand the difference between inbound and outbound traffic, see Understanding
- Traffic Direction. To understand how many data points are shown for each time period,
- see Understanding Traffic Granularity. To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

3.2.9 Monitoring network conversations

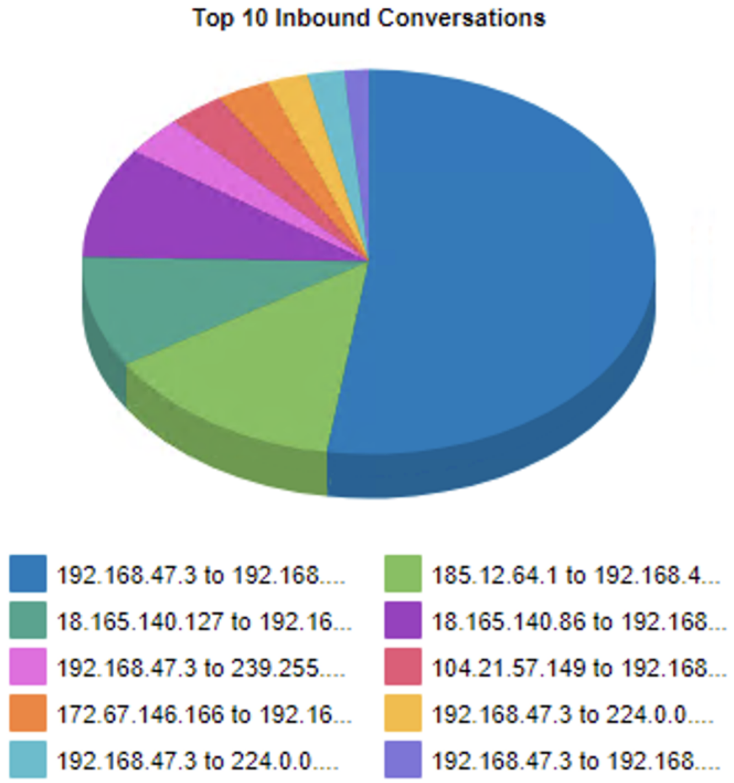
The Conversations report shows top conversations by data volume for a selected time period. Traffic inbound to your LAN is reported separately from the outbound traffic.

This report answer questions such as:

- What are the top conversations on my network?
- Could one conversation be choking out the other application traffic?

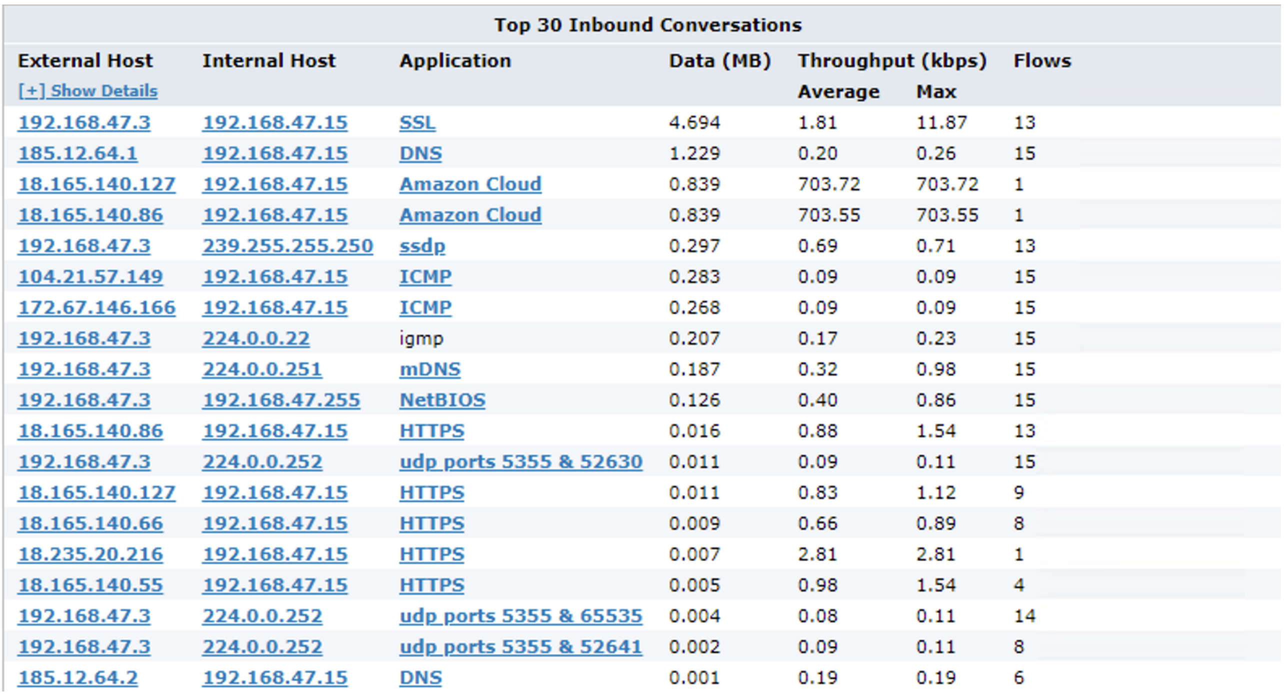
Use this information to determine if you need to create policies for high data volume conversations. You may want to create limiting policies for particular hosts or users accessing particular applications.

A conversation is defined as data transacted between two host machines using the same application within a specified time period. Conversations may also be referred to as sessions.



Screenshot 113: The Conversations report displays traffic volume data by conversation.

The tables at the bottom of the report shows for each of the top conversations, the total amount of data, and the maximum and average throughput rates, the number of packets, and the number of flows for the selected time period. More network metrics, such as, round-trip time (RTT), network and server delays, and TCP efficiency can be shown by clicking on the **Show Details** link in the tables.



Top 30 Inbound Conversations

External Host	Internal Host	Application	Data (MB)	Throughput (kbps)		Flows
[+] Show Details				Average	Max	
192.168.47.3	192.168.47.15	SSL	4.694	1.81	11.87	13
185.12.64.1	192.168.47.15	DNS	1.229	0.20	0.26	15
18.165.140.127	192.168.47.15	Amazon Cloud	0.839	703.72	703.72	1
18.165.140.86	192.168.47.15	Amazon Cloud	0.839	703.55	703.55	1
192.168.47.3	239.255.255.250	ssdp	0.297	0.69	0.71	13
104.21.57.149	192.168.47.15	ICMP	0.283	0.09	0.09	15
172.67.146.166	192.168.47.15	ICMP	0.268	0.09	0.09	15
192.168.47.3	224.0.0.22	igmp	0.207	0.17	0.23	15
192.168.47.3	224.0.0.251	mDNS	0.187	0.32	0.98	15
192.168.47.3	192.168.47.255	NetBIOS	0.126	0.40	0.86	15
18.165.140.86	192.168.47.15	HTTPS	0.016	0.88	1.54	13
192.168.47.3	224.0.0.252	udp ports 5355 & 52630	0.011	0.09	0.11	15
18.165.140.127	192.168.47.15	HTTPS	0.011	0.83	1.12	9
18.165.140.66	192.168.47.15	HTTPS	0.009	0.66	0.89	8
18.235.20.216	192.168.47.15	HTTPS	0.007	2.81	2.81	1
18.165.140.55	192.168.47.15	HTTPS	0.005	0.98	1.54	4
192.168.47.3	224.0.0.252	udp ports 5355 & 65535	0.004	0.08	0.11	14
192.168.47.3	224.0.0.252	udp ports 5355 & 52641	0.002	0.09	0.11	8
185.12.64.2	192.168.47.15	DNS	0.001	0.19	0.19	6

To access this report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to **Monitor> Conversations**.

To interact with the pie-based reports, you can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie. Note that the pie is showing only the top items, so the proportion is relative to the top items - not relative to all the traffic through the appliance. That is, if one wedge showed 50% of the traffic, that means it is 50% of the top items, not 50% through the appliance.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

3.2.9 Monitoring subnets

A subnet, a type of network object, can include multiple network subnets and/or multiple IP addresses. The Subnets report shows the top subnets by volume and their average throughput for the selected time period.

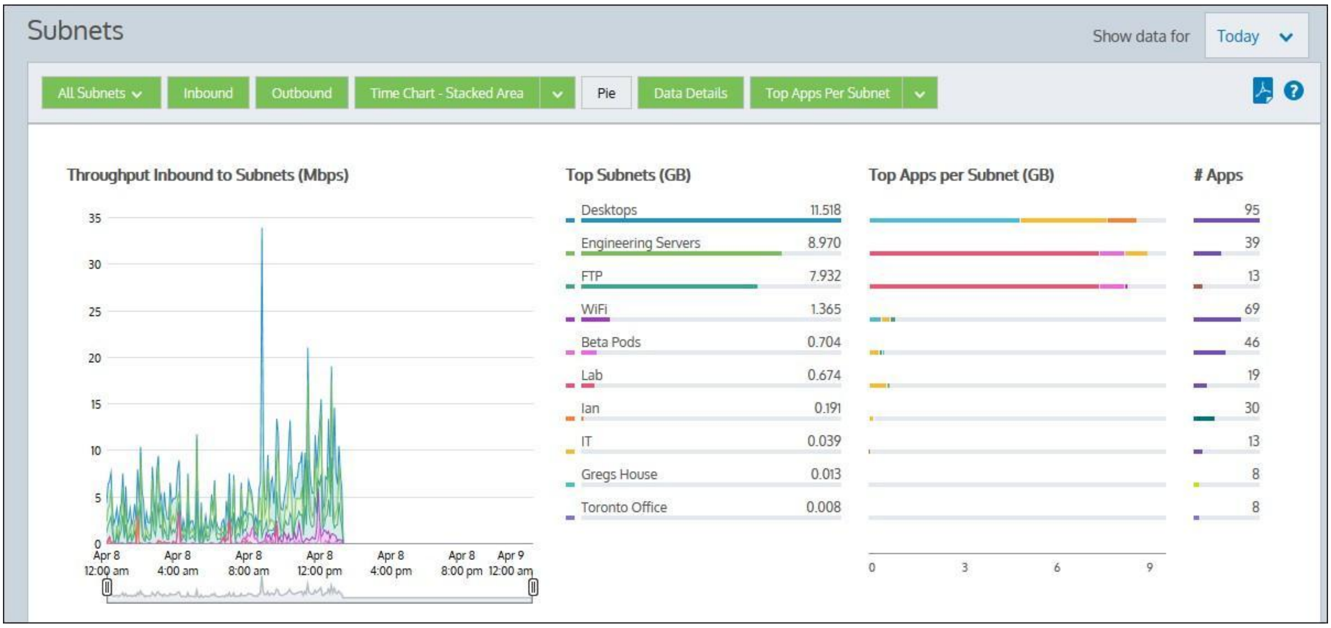
When subnets are defined, they can be specified as internal or external to your network. Inbound and outbound traffic for these subnets are reported separately. Inbound and outbound traffic is relative to the subnet, not relative to the GFI ClearView Appliance.

Subnets are not required to be mutually exclusive. Traffic may be reported in more than one subnet. You can optionally show the top three applications for each of the top subnets.

These charts can answer questions such as:

- What are the top subnets in my network?
- How much bandwidth does my subnet for the New York branch or for my finance department or for my PBX phones typically consume?
- Do each of my branches or departments (partitioned by subnet) have the same top applications?

Toggle chart components on and off by clicking the buttons at the top of the report. Note when generating a PDF report of this screen, toggle states are taken into account.



Top Subnets (GB)		# Apps
Desktops	11.518	95
Engineering Servers	8.970	39
FTP	7.932	13
WiFi	1.365	69
Beta Pods	0.704	46
Lab	0.674	19
Ian	0.191	30
IT	0.039	13
Gregs House	0.013	8
Toronto Office	0.008	8

> **NOTE**
>
> Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to **Monitor> Subnets**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

To configure a subnet for monitoring

Create a network object. See For more information, refer to Adding network objects.

I do not see my subnet data

If Network Object/Subnet statistics collection is disabled, the Subnets report will not include application data for the time period the collection was disabled. For more information, refer to Adding network objects.

If the Subnet Report checkbox is not enabled on the definition of the subnet, then the data will not be included in the report. If the data was collected, then enabling the Subnet Report will immediately show the data in the chart.

To change the throughput chart to stacked area charts or line charts

Press the down arrow next to the Stacked Chart button to select Line Chart to switch to the line chart. Conversely, press the down arrow next to the Line Chart button to select Stacked Chart and switch to the stacked area chart. The line chart shows the subnets against the common zero baseline so that the throughput of the subnets can be compared with one another and the pattern of a specific subnet is clearer. You can look for particular patterns such as spikes or flat tops. If your subnets are not defined to be mutually exclusive, displaying the throughput in a line chart with a common zero baseline may make the most sense, as the cumulative values chart will double count some data and may not be meaningful. However, if you have defined your subnets to be mutually exclusive then stacked area charts is an option.

To show the data volume of the subnets as a pie chart

Toggle on the pie chart by clicking the Pie button. Note that if your subnets are not defined to be mutually exclusive, that is, data is captured in more than one subnet, then the pie chart does not hold much meaning.

To show more or fewer subnets in the top subnets chart and the throughput chart

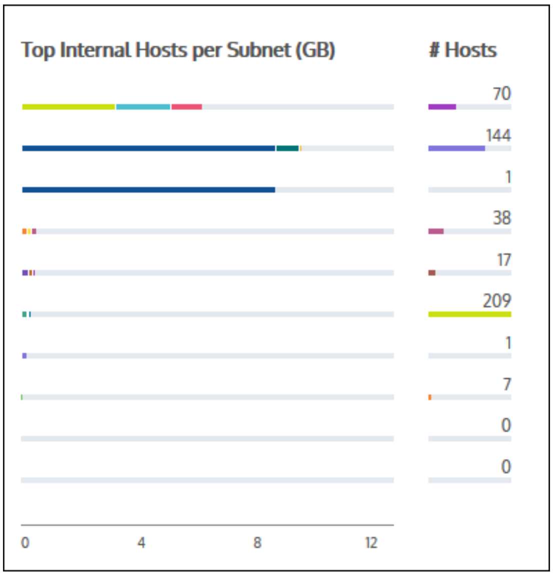
The number of subnets shown are configurable. Note that this configuration applies to all charts on the appliance. For more information, refer to Monitoring Configuration.

Should subnet totals match virtual circuit totals when the virtual circuit and subnet are based on the same network object?

In general, yes. However, there are some cases where the traffic direction is different for subnets versus virtual circuits and so the totals will not match. For more information, refer to Determining traffic direction and the implications of directional flow on reports.

Can I view the Top Internal or External Hosts per Subnet in this report?

By default, this report displays the Top Apps per subnet, but you can change the view to Top Internal or Top External Hosts per Subnet. Click the drop-down arrow beside the Top Apps per Subnet button to view these other options. When the display updates, the Top hosts data is mapped to a bar graph. You can brush over any host to view it's IP Address and throughput data.



How can I drill down in this report?

You can drill into the applications for a specific subnet by clicking on the subnet name in the Top Subnets chart or by clicking on the subnet name in the table below the charts. You can also drill into the hosts, or users, or conversations for a particular subnet by clicking on the **View Users**, **View Conversations**, **View URLs** links in the table. The applications, hosts, users, conversations, or URLs graph will be shown filtered for the specified subnet.

How do I interact with the new time-series & bar chart reports?

- To understand how to set the desired time range for a chart, see Setting the Time Range.

- To understand how the charts interact and what the toggle buttons do, see Understanding How Charts Relate.

- To understand how to drill into the data to find particular filtered data, see Drilling into the Data.

- To understand the difference between inbound and outbound traffic, see Understanding Traffic Direction.

- To understand how many data points are shown for each time period, see Understanding Traffic Granularity.

- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Creating a detailed subnet activity report

Create a PDF report that lists all network activity for Applications, Conversations, Hosts, URLs, and Users on the selected subnets.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Report > PDF Reports**.

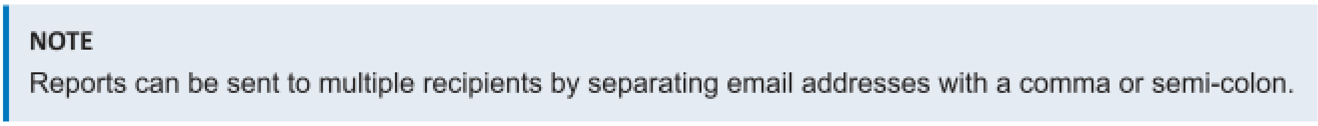
6. Click **Add New PDF Report**.

7. In the Reports Selection area, select **Detailed Subnet Reports**.

8. From the subnet list, select a subnet to add to the report and click **Add subnet to report**. Repeat this for each subnet to include in the report.

9. In the Subnets Selected area, select the network traffic to include in the report.

10. In the Report Details area, specify the name of the report, what time period the report should reflect, and an email address where the report can be sent.



NOTE

Reports can be sent to multiple recipients by separating email addresses with a comma or semi-colon.

11. Click **Add New Report**.

3.2.11 Monitoring GFI ClearView Appliance system performance

Learn about the reports that provide feedback on the performance of your GFI ClearView Appliance. The reports cover aspects of operational performance like number of concurrent connections, CPU utilization, CPU temperature, memory usage, disk IO and swap space usage.

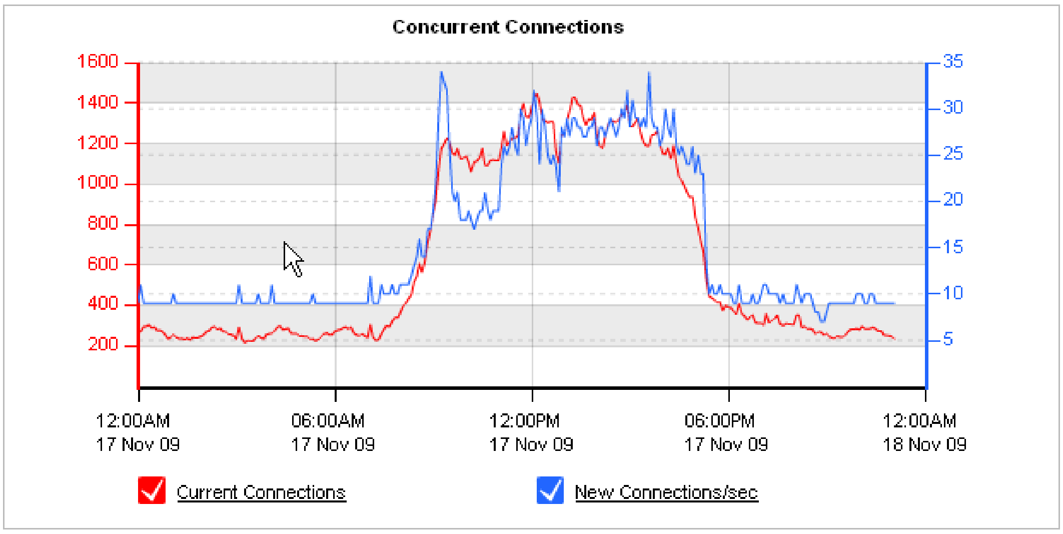
Monitoring connections to an GFI ClearView Appliance

The Connections report shows the number of concurrent connections as well as the connection establishment rate over time for the selected time period.

This report answers questions such as:

- Is there an unusual number of connections or is the connection rate particularly high?
- Could I be experiencing some form of denial of service attack or network problem?”

> NOTE
> Systems reporting unusually high spikes in the number of connections or rate of connections may be experiencing a denial of service attack or network problem.



Screenshot 128: The Concurrent Connections graph displays connection statistics over time.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Monitor> System > Connections.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring GFI ClearView Appliance CPU usage

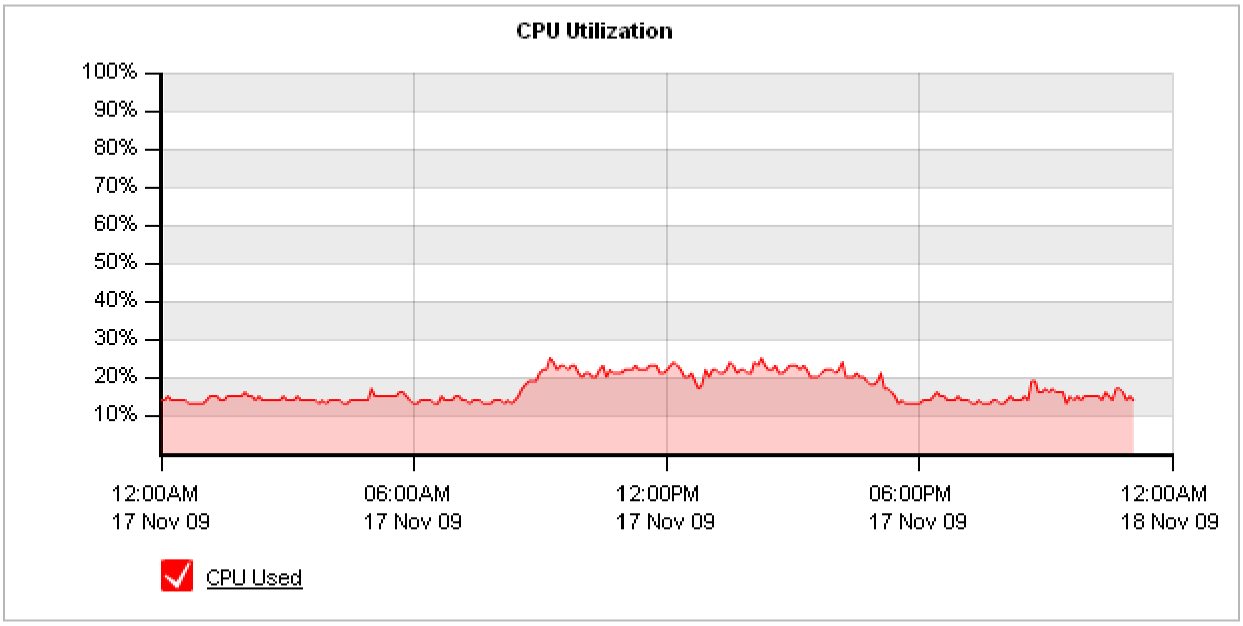
The CPU Usage report shows how hard the CPU is working over time. This report answers questions such as:

- Are some of the other issues I'm seeing with my traffic due to overworking the appliance?
- I see the appliance's CPU is highly utilized. What traffic issues could cause this to be happening?

High CPU usage may be due to a variety of processing intensive traffic characteristics:

- The number of new connections per second is high
- The number of accelerated connections is high
- The appliance is encountering more accelerated traffic than it can handle. If this is the case, latency can be introduced when the appliance queues the packets for acceleration and cannot process them fast enough. Using virtual circuits, you can limit the amount of accelerated traffic to process.
- The appliance is encountering more analysis-intensive traffic than it can handle. For instance, VoIP traffic is CPU intensive due to the processing required to compute the metrics such as rFactor, MOS, jitter, etc.

To diagnose a CPU usage problem, for each period where the CPU usage is high, compare with the Connections report, the Accelerated Connections report, the Reduction report, and the VoIP Solution report.



Screenshot 131: The CPU utilization graph shows howhard the GFI ClearView Appliance works over time.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> System > CPU Usage**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

Where do I find the other reports for diagnosing the reason for high CPU usage?

- The report for the number of new connections can be found at **Monitor> System > Connections**. For more inform- ation, refer to Monitoring connections to a GFI ClearView Appliance.
- The report for the number of accelerated connections can be found at **Monitor> System > Accelerated Connections**. For more information, refer to Monitoring accelerated connections.
- The report for the amount of accelerated traffic can be found at **Monitor> Optimization > Reduction**. For more information, refer to Monitoring traffic reduction.
- The report for VoIP traffic can be found in the Solution Center (**Solution Center> Show Solution Center**). For more information, refer to Using the Application Performance Monitor VoIP report.

How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Interactive Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring GFI ClearView Appliance CPU temperature

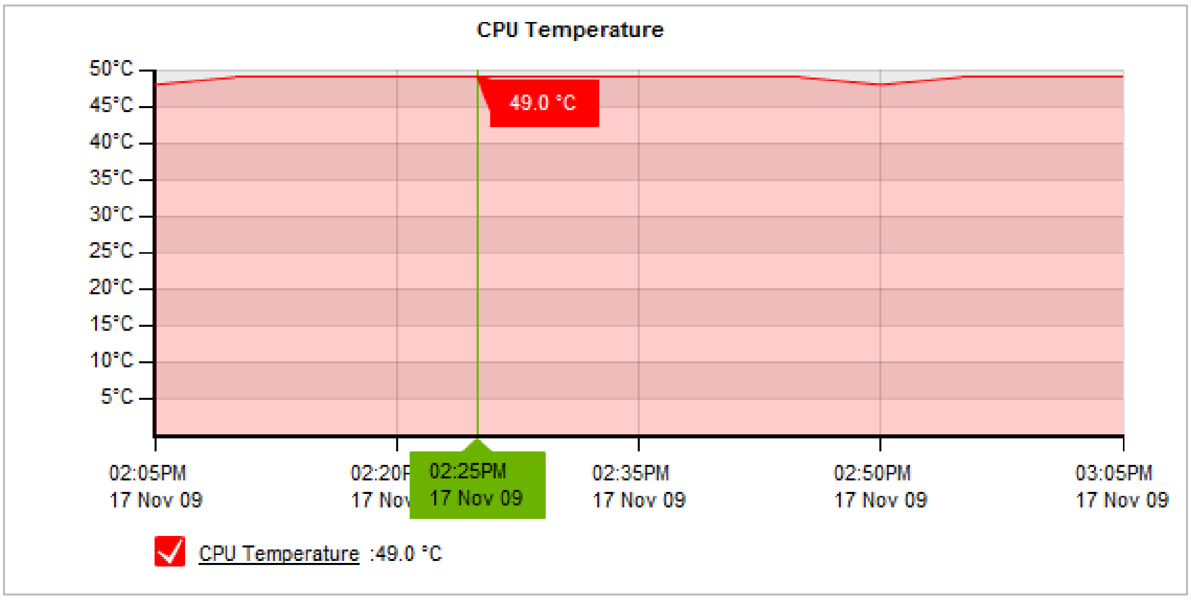
The CPU Temperature report shows the temperature in degrees Celsius of the appliance CPU over time for the selected time period.

This report answers questions such as:

- Are some of the other issues I'm seeing with my traffic due to overworking the appliance?
- I see the appliance's CPU temperature is high. Is it due to high CPU usage or is the ambient temperature around the GFI ClearView Appliance too warm?

You should expect the CPU temperature to be considerably lower than 80 degrees Celsius, usually between 35-50 degrees. Systems running at very high temperatures may be experiencing a problem and system performance may be affected. Once the temperature gets too high (80-90 degrees) the appliance will throttle its processing speed to reduce heat emissions.

See the **CPU Usage** report to see if the temperature correlates with the processing activity on the appliance.



Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Go to Monitor> System > CPU Temperature.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

Where do I find the CPU Usage report?

The report for CPU usage can be found at **Monitor> System > CPU Usage**. For more information, refer to Monitoring GFI ClearView Appliance CPU usage.

How do I interact with the interactive flash time graphs?

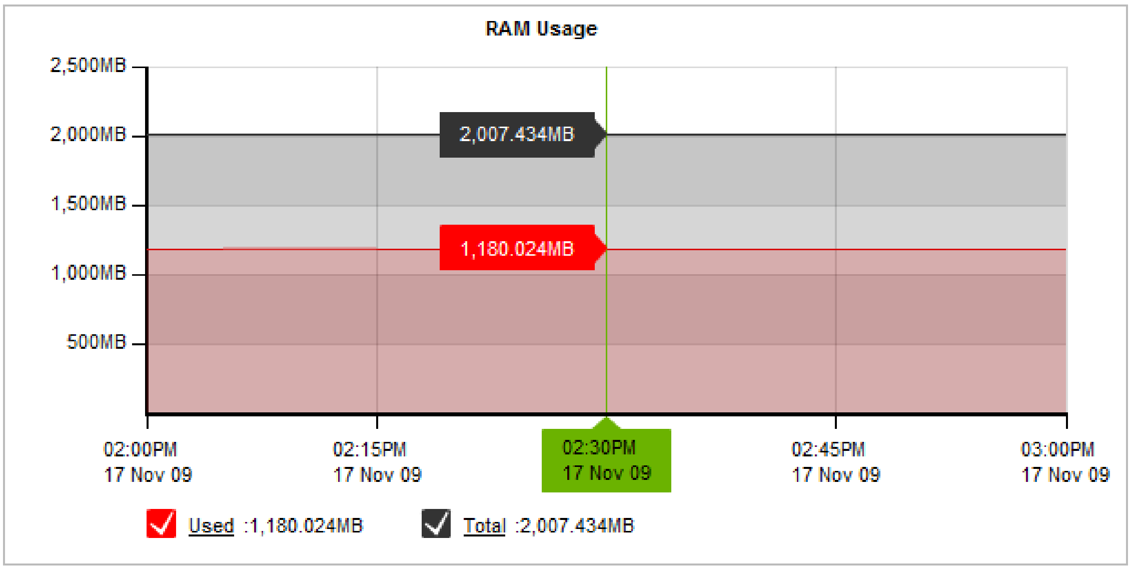
- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring GFI ClearView Appliance RAM usage

The RAM Usage report shows how much memory the appliance is using relative to the amount of memory available for the selected time period.

This report answers questions such as:

- Could the performance of my appliance be affected by insufficient RAM?



Screenshot 132: The RAM Usage chart displays memory consumption over time.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> System > RAM Usage**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Interactive Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring GFI ClearView Appliance Disk IO

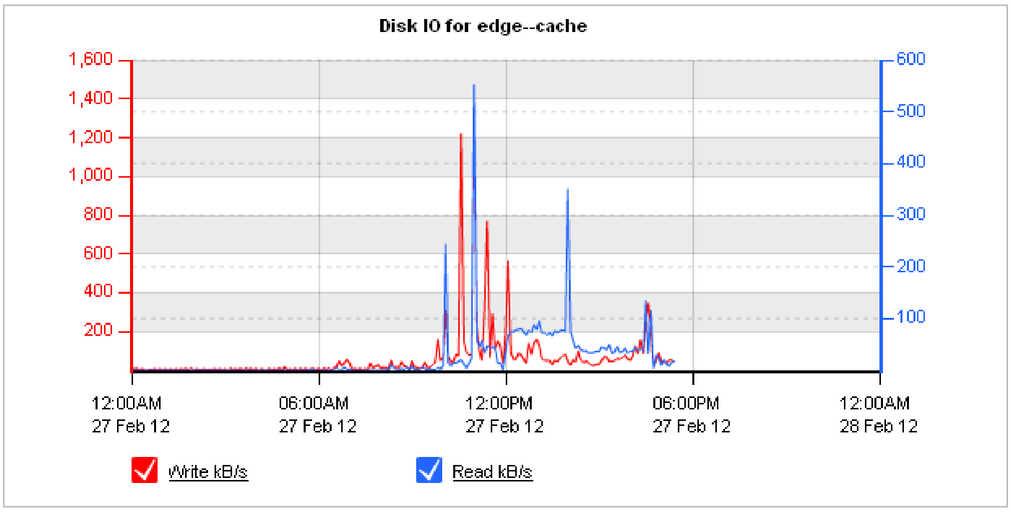
The Disk IO report shows read and write disk usage for each service in kB/s over time for the selected time period. This report answers questions such as:

- Has my disk I/O usage suddenly increased or over time? If so, which subsystem is responsible for the increased disk I/O usage?
- If WAN memory acceleration, or CIFS acceleration, or edge cache performance is suffering, was there a decrease in its I/O load?
- Was that decreased I/O load due to another subsystem's increased I/O load?

» I swapped an appliance and loaded the same configuration and it seems slower. If all the I/O rates look lower, then maybe this is a physical disk issue.

The disk usage for each of the following services can be shown by selecting the desired service from the Service selector.

- **System (vda)** – Total disk usage for all services combined for the single disk; Note that there may be two disks.
- **monitor** – Disk usage required for storing the monitoring data
- **swap** – Disk usage required for swapping/paging
- **users** – Disk usage required to store the username information (i.e. data sent by the AD connector, manually con- figured users and groups, details of dynamic network objects)
- **wan** – memory - Disk usage required for WAN memory acceleration techniques
- **edge-cache** – Disk usage required for storing cached content for Edge Cache
- **cifs** – Disk usage required for CIFS acceleration techniques



Screenshot 133: The Disk IO graph displays IO used by edge cache.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> System > Disk IO**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

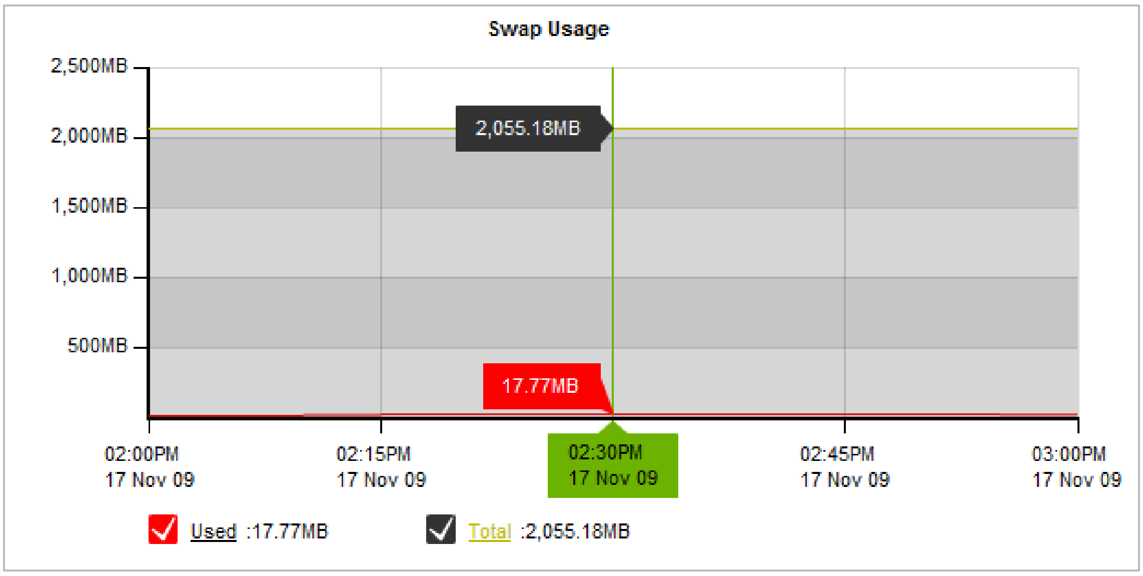
» To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Inter- active Time Graphs.

- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Monitoring GFI ClearView Appliance swap space usage

The Swap Usage report shows how much the appliance is swapping over time for the selected time period. This report answers questions such as:

- Could excessive swapping be affecting the performance of my appliance?



Screenshot 134: The Swap Usage graph displays system swap space utilization over time.

Where do I find this report?

To access the report:

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to **Monitor> System > Swap Usage**.

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. For more information, refer to Exporting, printing and scheduling reports.

How do I interact with the interactive flash time graphs?

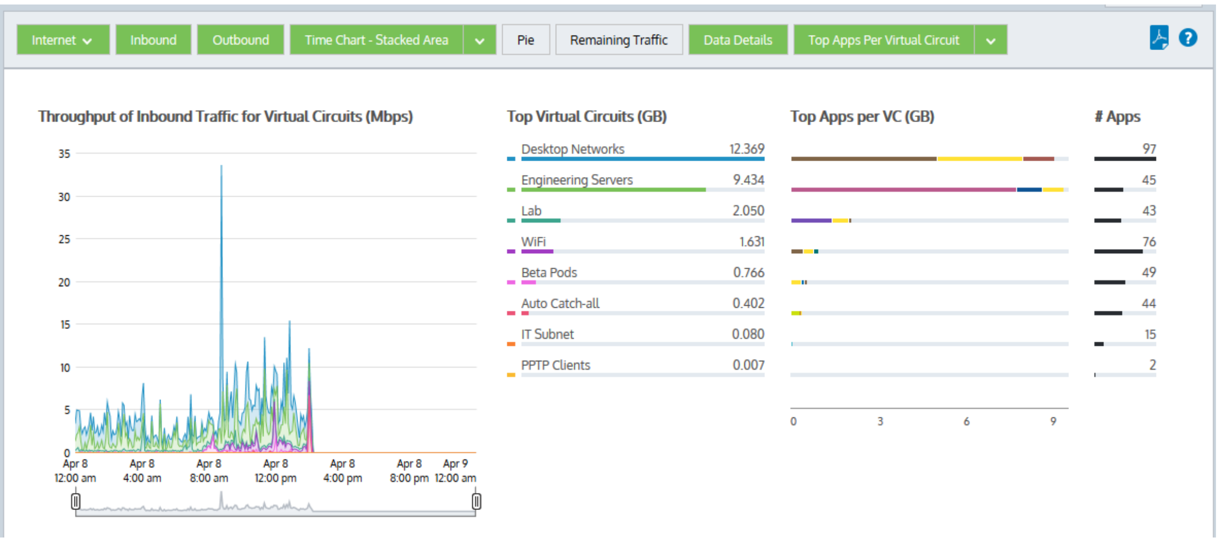
- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Interactive Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

3.2.12 Viewing monitoring statistics

Your GFI ClearView Appliance provides several ways to view the statistics gathered from monitoring your network. This section provides information about accessing those statistics and interpreting the information provided.

Understanding the relationships between charts and data

On the new time series monitoring screens, there will be a pie chart and a bar chart showing the top data by volume for the specified time period and a time chart showing the same top times. There will be one set of these charts for inbound traffic and one for outbound traffic. In some instances, another chart that shows the top three items of another application type for each of the top data elements. For example, if looking at the virtual circuits chart, you will see the top virtual circuits as a bar chart. Then beside the bar chart, there will be a stacked horizontal bar chart which shows the top three applications for each of the top virtual circuits.



Top Virtual Circuits (GB)		# Apps
Desktop Networks	12.369	97
Engineering Servers	9.434	45
Lab	2.050	43
WiFi	1.631	76
Beta Pods	0.766	49
Auto Catch-all	0.402	44
IT Subnet	0.080	15
PPTP Clients	0.007	2

Screenshot 135: Virtual circuit details

When you brush over an item in any of these charts, the item is highlighted in all the charts.

There are toggle buttons at the top of the chart which you can use to turn on and off different chart elements.

- **Inbound** button – Toggles on or off all reporting for inbound traffic including all the charts and the data tables below the charts.

- **Outbound** button – Toggles on or off all reporting for outbound traffic including all the charts and the data table below the charts.

- **Stacked Chart** or **Line Chart** button – Toggles on or off the time series charts or selects a different view of the data. Press the down arrow next to the Stacked Chart button to select Line Chart to switch to the line chart. Conversely, press the down arrow next to the Line Chart button to select Stacked Chart and switch to the stacked area chart. The line chart shows the virtual circuits against the common zero baseline so that the throughput of the virtual circuits can be compared with one another and the pattern of a specific virtual circuit is clearer. You can look for particular patterns such as spikes or flat tops.

- **Pie** button – Toggles on or off the data volume pie charts.

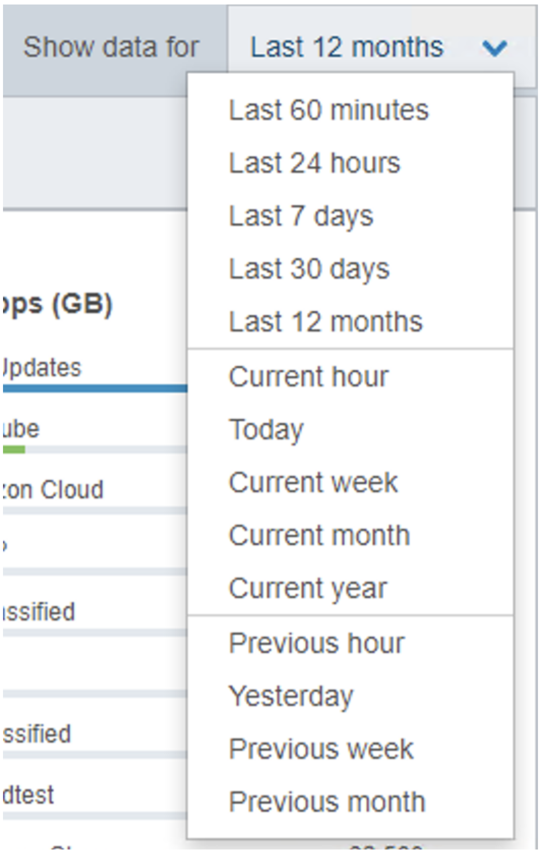
- **Remaining Traffic** button – Toggles on or off the rest of the data that is not represented in the top virtual circuits.

When toggled on, a gray chart series will appear in all charts (throughput, pie, top virtual circuits) representing all the virtual circuits in your network that are not explicitly represented in the top virtual circuits. If the remaining virtual circuits show vastly more data volume than the top virtual circuits, then the top virtual circuits may look insignificant relative to the total, and so you may need to toggle off the remaining traffic category to see the relative differences and usage patterns of the top virtual circuits.

- **Data Details** button – Toggles on or off the tables of data below the charts.
- **Top Apps Per X**(bar chart row) button –Toggles on or off extra charts showing the top 3 apps for each row in the bar chart and the number of apps for each row in the bar chart.

Zooming into a time Interval on the time graphs

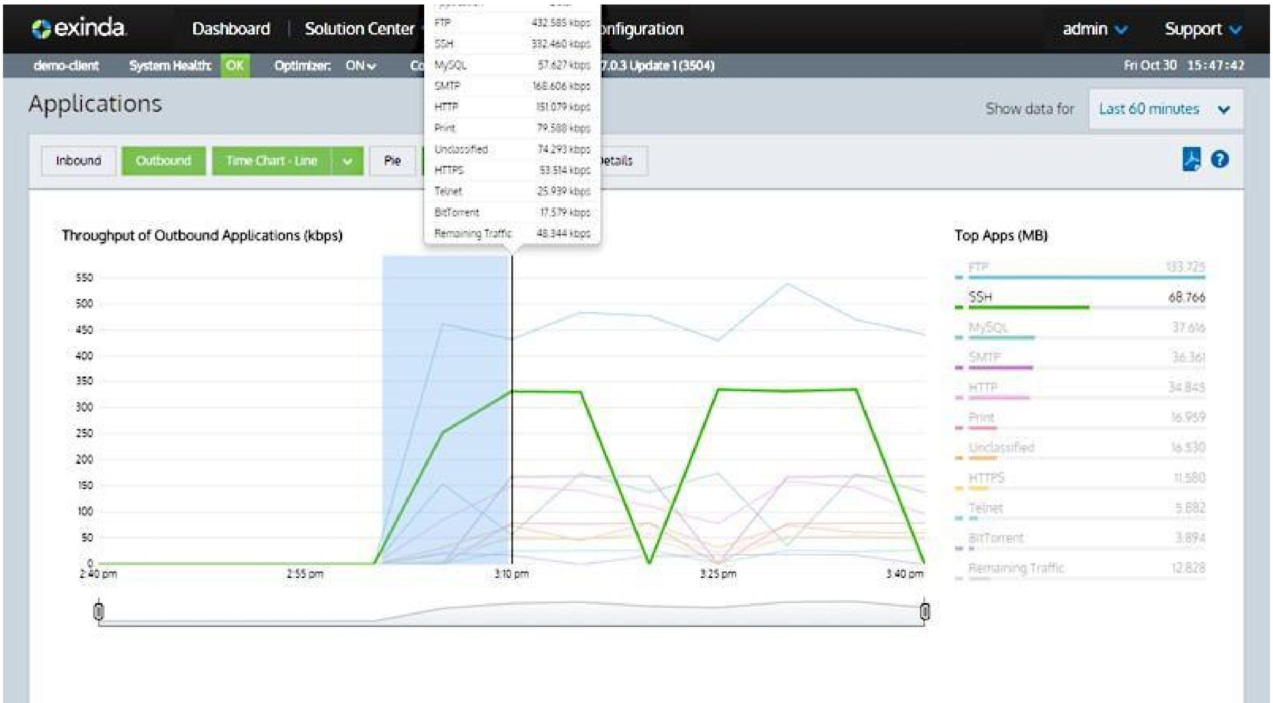
To view data within a time range, you can use the **Show data for** drop-down list to narrow the range. If it does not provide the detail you need, you can narrow the search further by clicking and dragging within the graph or by using the zoom control below the graph. These methods allow you to define a custom time range.



Show data for Last 12 months

Screenshot 136: The "Showdata for" drop-down list

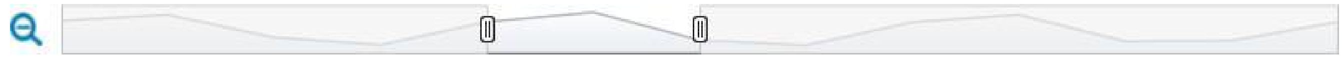
Click and drag your mouse on the chart to select the desired time range.
Drag the handles on the zoom controller to modify the time range. As you drag, the area between the drag points becomes shaded. When you release, the shaded area expands to occupy the entire graph. To return to the initial time range, click on the Zoom Out button to the left of the zoom controller.



FTP	432.585 kbps
SSH	332.460 kbps
MySQL	57.627 kbps
SMTP	168.606 kbps
HTTP	151.079 kbps
Print	79.588 kbps
Unclassified	74.293 kbps
HTTPS	53.514 kbps
Telnet	25.939 kbps
BitTorrent	17.579 kbps
Remaining Traffic	48.344 kbps

Top Apps (MB)	
FTP	133.725
SSH	68.766
MySQL	37.616
SMTP	36.361
HTTP	34.845
Print	16.959
Unclassified	16.530
HTTPS	11.580
Telnet	5.882
BitTorrent	3.894
Remaining Traffic	12.828

You can also use the zoom controls that appear below the graph. Drag the handles in from the left and/or the right to isolate the data you need. The graph is dynamic, so you can immediately view the data. The handles remain in the positions you left them, so the scope of the initial report remains evident.. When finished click on the Zoom Out 🔍 button.

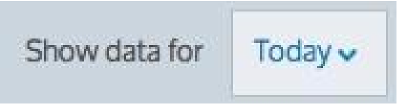


Screenshot 137: The Zoom controls

Setting time ranges for charts and graphs

For each chart, you can set the time range that is reported in the chart.

At the upper-right of the report, select the desired date range from the drop down list. Custom time ranges are not supported.



After the date range is selected, the graphs and charts are immediately updated.

Drilling into the chart data

Charts that show the data, such as applications, application groups, users, hosts, URLs, subnets, virtual circuits, allow you to drill into a particular item to explore the details filtered by that item.

To drill-down:

- For charts, click on an item in the table below the charts.
- For bar charts, click on an item in the bar chart.

You can drill-down into the following details for each of the application types:

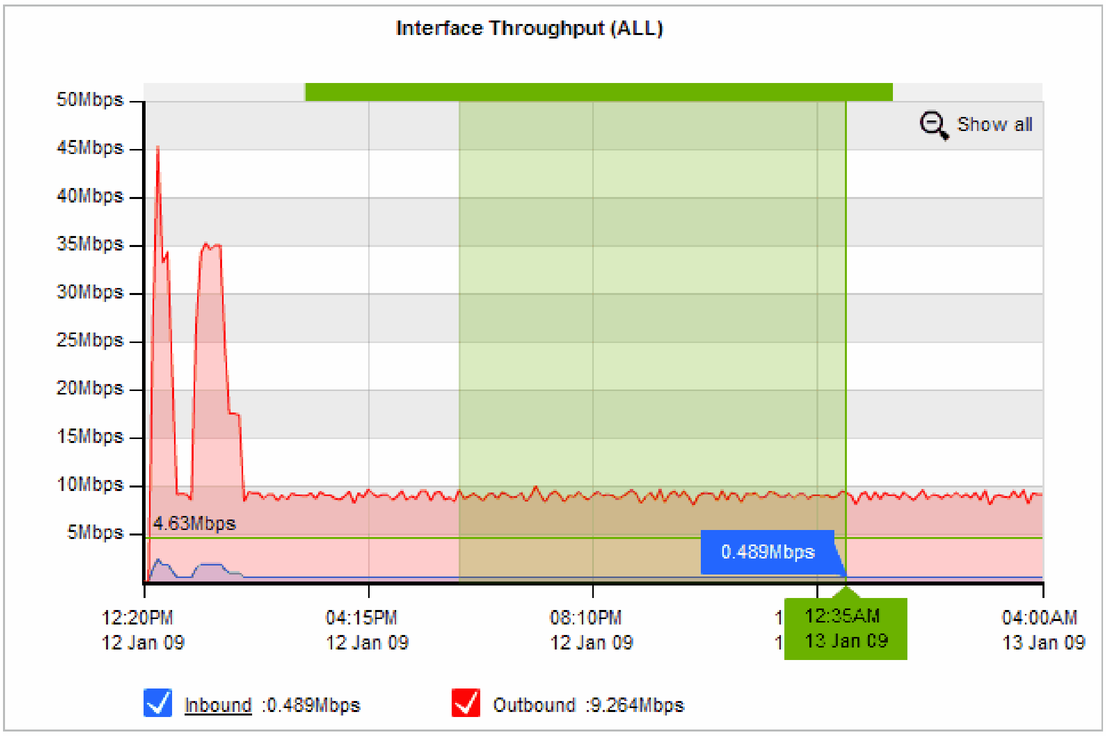
- Application groups > applications > hosts
- Applications > hosts URLs > hosts
- Users > applications or conversations or URLs or hosts
- Hosts > applications or conversations or URLs
- Subnets > applications > hosts
- Subnets > hosts > applications or conversations or URLs
- Subnets > users > applications or hosts or conversations or URLs
- Subnets > conversations
- Subnets > URLs
- Virtual Circuits > applications

Drilling past these levels widens the filter. For example, drilling from users to applications filters the applications for that user, however, if you then drill into one of the applications for that users, it shows all hosts using that application.

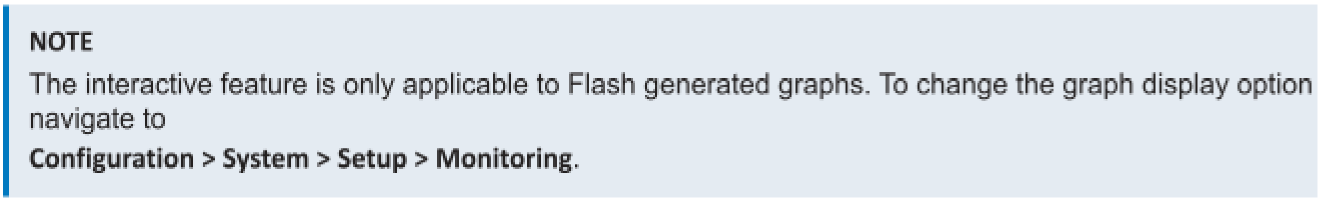
Using interactive time graphs

If you want a better look at a traffic pattern or if the chart is too cluttered, you can zoom in to a custom time range and remove time series lines that you are not interested in on the time graphs.

To zoom into a custom time range, click and drag your mouse on the chart to select the desired time range. To return to the initial time range click the 'Show all' magnifying glass icon. Any data displayed below these interactive graphs will automatically be updated with the data for the selected time range.



To remove a time series line, click on the check in the graph legend or in some cases the table below the chart to toggle off the display of that line.



NOTE

The interactive feature is only applicable to Flash generated graphs. To change the graph display option navigate to

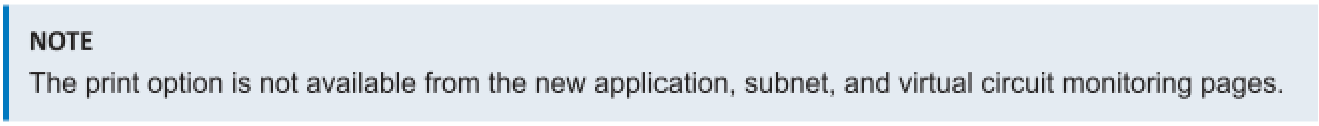
Configuration > System > Setup > Monitoring.

Exporting, printing and scheduling reports

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. The following icons appear on the top-right of the interface:

🖨 📅 📄

- **Print**: Clicking on the Printer icon will open a new browser window and format the current report suitable for print- ing. It will then prompt you to select a printer.

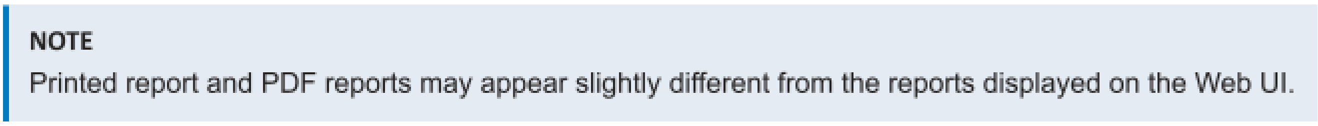


NOTE

The print option is not available from the new application, subnet, and virtual circuit monitoring pages.

- **Schedule PDF**: Clicking on the schedule icon will save the report configuration to the scheduled reports. It will prompt you for a report name, the scheduled frequency, the email addresses to send it to, and optionally a password if you choose to password protect the PDF.

- **PDF**: Clicking on the PDF icon will render the current report as a PDF document and prompt you to save or open the PDF file once complete.



NOTE

Printed report and PDF reports may appear slightly different from the reports displayed on the Web UI.

Generating PDF reports

PDF reports can be generated and downloaded on demand or generated and emailed at scheduled intervals. The content of the PDF reports can be configured in two ways:

- exploring the data in the monitor screens and
- requesting a report going to the Report page to

  configure the details of the PDF report

The following PDF report generation scenarios are supported:

- Explore the data in the monitor screens and generate an ad hoc PDF report of what is shown on the screen. Explore the data in the monitor screens and schedule a PDF report to be
- generated using the configuration and filters shown on the screen.

- Configure a PDF report using the Report page .
- Configure a PDF report using the Report page and request an on-demand generation of the PDF report.

Scheduled reports can be emailed to one or more email addresses by comma separating or semicolon separating the email addresses in the appropriate field.

Scheduled reports can be generated hourly, daily, weekly, or monthly. The time range included in the report matches the frequency, that is, daily reports report on a day’s worth of data and is generated once a day.

> **NOTE**
>
> - Hourly scheduled reports are emailed to users at 22 minutes past
> - the hour. Hourly reports cannot be generated on-demand.
> - Daily scheduled PDF Reports are generated every morning at 1 a.m.

On-demand reports from the monitor pages can include any time range available to the monitoring screens, including custom time ranges.

Scheduled PDF reports can be branded by uploading your logo to be displayed on the title page of the reports. Reports scheduled from the report page, can contain one or more charts in the PDF by selecting any number of charts.

To generate an on-demand PDF report from a monitor screen

1. Go to any monitor screen (except the Real Time screen) and configure it according to the available controls, such as the date range selector, the Internal or External selector for hosts and user charts and subnets, drilling into the data by selecting the links in the data tables under the charts, and so on.

2. Click on the Adobe PDF icon in the upper-right of the screen.

3. The system will generate and present a PDF report that corresponds to what you see on the screen.

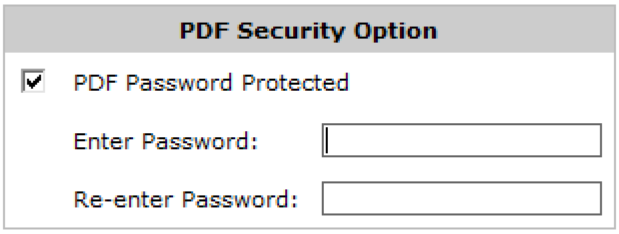
To schedule a PDF report from a monitor screen

1. Go to any monitor screen (except the Real Time screen) and configure it according to the available controls, such as the date range selector, the Internal or External selector for hosts and user charts and subnets, drilling into the data by selecting the links in the data tables under the charts, and so on.

> **NOTE**
> When you use this method to generate a report, the time range that appears on the front page of the report is updated to reflect the scheduled time range:"last 60 minutes" is updated to "last hour", " last 24 hours is updated to "yesterday", etc. For example, the time range may be mapped to the following: 'Report Time Range 04:55PM 07 April 2015 to 05:55PM 07 April 2015'.

1. Click on the schedule PDF icon in the upper-right of the screen.

2. Optionally protect PDF documents by specifying a password.



PDF Security Option

☑ PDF Password Protected

Enter Password:

Re-enter Password:

3. On the Report Details page, specify the report name, the report frequency, and email addresses to send the report to.

    - **Report Name**— a meaningful name for the new PDF Report.

- **Report Frequency**— This option is disabled when you click the Schedule button from a Monitor screen because the system assumes you want to use the time range obtained from the Monitoring screen. If you need to change the time range, click the Add New PDF Report link at the top of the page.
- **Email Addresses**— one or more email addresses for scheduled PDF Reports. Email addresses are optional for on-demand PDF Reports. To specify multiple email addresses, comma or semicolon separate the addresses.

4. The system will add this scheduled report to the Reporting page (**Monitor> Schedule Reports**)

> NOTE
>
> PDF reports that were scheduled from a monitoring page cannot be edited. Ensure that you specify all the email addresses that you need it emailed to.

To schedule a new PDF report from the Reporting page

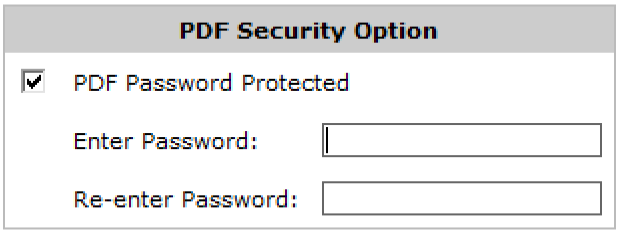
1. Go to Monitor> Schedule Reports > PDF Reports.

2. Click on the **Add New PDF Report** link at the top of the page.

3. Select the various reports you wish to include in the PDF report. Many of the reports available from the Web UI are available as PDF reports.

- **Interface Throughput Summary**– can select a specific interface(s), WCCP,or all WAN interfaces Bridge PPS (Packets per Second)
- **Summary** – can select specific bridge(s), WCCP, or all bridges
- **Network Summary**
- **Subnets Summary**
- **Detailed Subnet Reports**– can select specific subnet(s) and specific details for each subnet (i.e. application detail, conversation detail, host detail, URL detail, and user detail)
- **APS**
- **SLA**
- **TCPHealth**
- **TCPEfficiency**
- **VoIP**
- **Appliance Statistics**– can select specific appliance system statistics (i.e. Concurrent Connections, CPU Usage, CPU Temperature, RAM Usage, SWAP Usage, Disk IO)

4. Optionally protect PDF documents by specifying a password.



PDF Security Option

☑ PDF Password Protected

Enter Password:

Re-enter Password:

5. On the Report Details page, specify the report name, the report frequency, and email addresses to

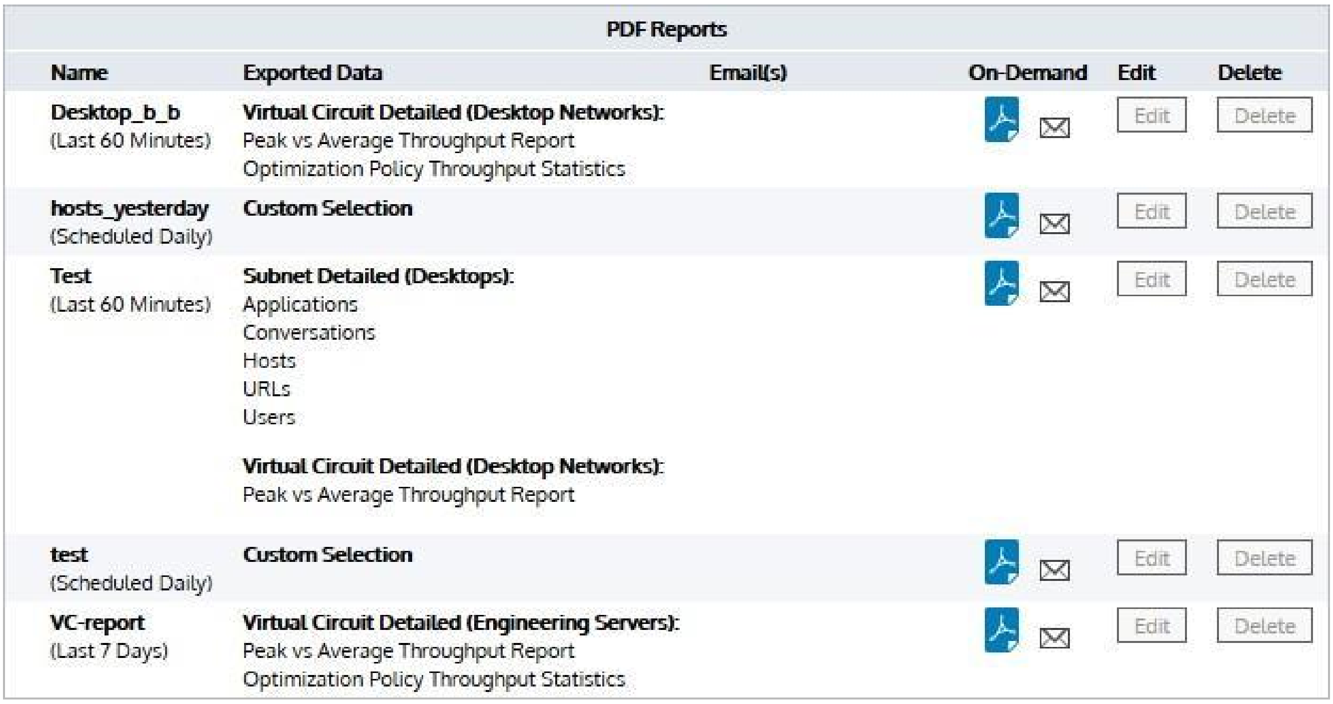
send the report to.

- **Report Name**— a meaningful name for the new PDF Report.
- **Report Frequency**— the time range of the report and the frequency that it is sent. For example, daily frequency presents a day's worth of data and is emailed once a day.
- **Email Addresses**— one or more email addresses for scheduled PDF Reports. Email addresses are optional for on-demand PDF Reports. To specify multiple email addresses, comma or semicolon separate the addresses.

6. The system will add this scheduled report to the scheduled report list.

To view a scheduled report on demand or edit or delete a report

1. Go to Monitor> Schedule Reports > PDF Reports.
2. The scheduled PDF reports are listed with a description of the charts that will be included in the report and the list of email addresses it will be sent to.



PDF Reports

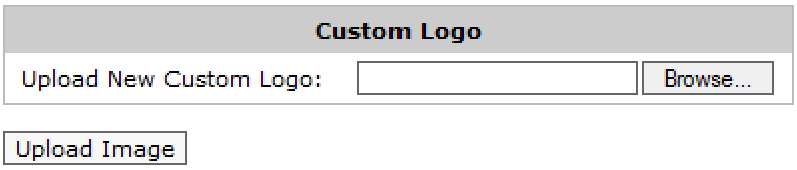
Name	Exported Data	Email(s)	On-Demand	Edit	Delete
Desktop_b_b (Last 60 Minutes)	**Virtual Circuit Detailed (Desktop Networks):** Peak vs Average Throughput Report Optimization Policy Throughput Statistics		✉	Edit	Delete
hosts_yesterday (Scheduled Daily)	**Custom Selection**		✉	Edit	Delete
Test (Last 60 Minutes)	**Subnet Detailed (Desktops):** Applications Conversations Hosts URLs Users **Virtual Circuit Detailed (Desktop Networks):** Peak vs Average Throughput Report		✉	Edit	Delete
test (Scheduled Daily)	**Custom Selection**		✉	Edit	Delete
VC-report (Last 7 Days)	**Virtual Circuit Detailed (Engineering Servers):** Peak vs Average Throughput Report Optimization Policy Throughput Statistics		✉	Edit	Delete

3. To view the report, click the Adobe PDF icon.
4. To email the report to email recipients on demand, click the mail icon.
5. To edit or delete a configured PDF report, click on the appropriate button next to the report in the table.

> **NOTE**
>
> PDF reports that were scheduled from a monitoring page cannot be edited. Ensure that you specify all the email addresses that you need it emailed to.
>
> PDF reports can only be emailed on-demand if the report was configured with one or more email addresses.

To add a custom logo to the cover of the scheduled reports

1. Go to Monitor> Schedule Reports > Custom Logo
2. Upload your custom logo.
3. The system will insert the logo on the cover page of any scheduled PDF report.



Custom Logo

Upload New Custom Logo: [ ] Browse...

Upload Image

> **NOTE**
> Files should be no more than 300px wide by 300px high and must be in PNG format with maximum file size of 3MB.

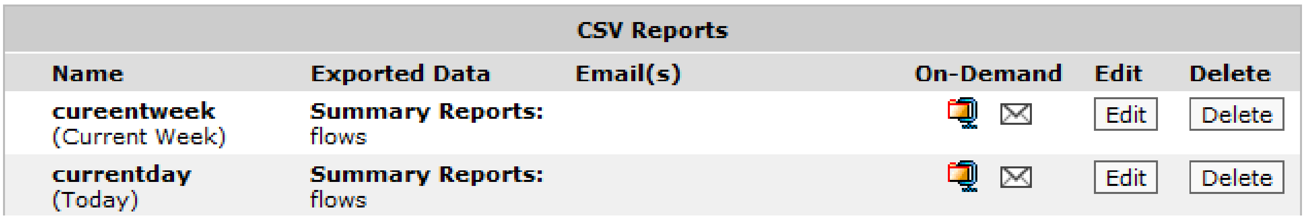
CSV Reporting

CSV Reporting allows you to configure the export of raw CSV data to be emailed or downloaded either on demand or at scheduled intervals. Exported data can be sent to multiple recipients by comma or semicolon separating email addresses.

> **NOTE**
> To configure a CSV Report, navigate to Report | CSV Reports on the Web UI, advanced mode.

CSV Reports are listed in the table on this page. CSV Report can be generated and either emailed or downloaded on- demand by clicking either the ZIP icon (to generate and download) or the envelope icon (to generate and email). CSV Reports can only be emailed on-demand if the report was configured with one or more email addresses.

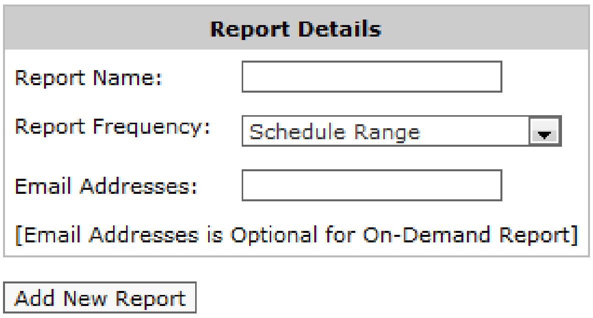
You can also Edit or Delete a configured CSV Report by clicking on the appropriate button next to the report in the table.



CSV Reports

Name	Exported Data	Email(s)	On-Demand	Edit	Delete
cureentweek (Current Week)	**Summary Reports:** flows		🗜 ✉	Edit	Delete
currentday (Today)	**Summary Reports:** flows		🗜 ✉	Edit	Delete

New CSV Reports can be added by using the form at the top of the page.



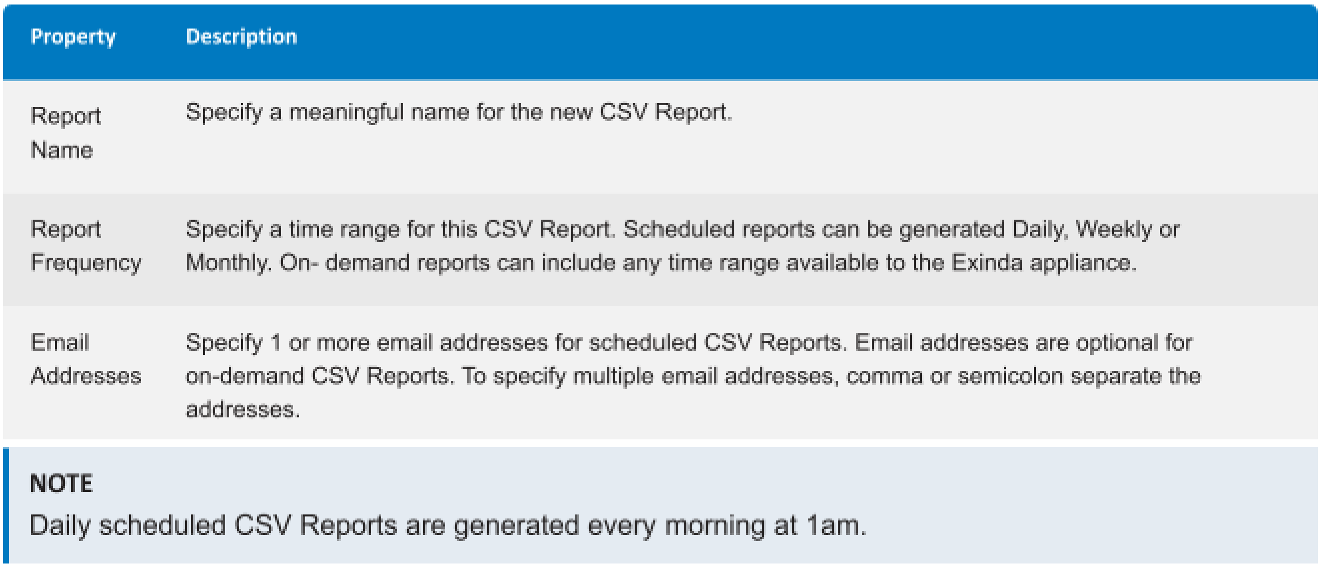
Report Details

Report Name:	
Report Frequency:	Schedule Range
Email Addresses:	

[Email Addresses is Optional for On-Demand Report]

Add New Report

Screenshot 138: Report Details



Property	Description
Report Name	Specify a meaningful name for the new CSV Report.
Report Frequency	Specify a time range for this CSV Report. Scheduled reports can be generated Daily, Weekly or Monthly. On- demand reports can include any time range available to the Exinda appliance.
Email Addresses	Specify 1 or more email addresses for scheduled CSV Reports. Email addresses are optional for on-demand CSV Reports. To specify multiple email addresses, comma or semicolon separate the addresses.

NOTE

Daily scheduled CSV Reports are generated every morning at 1am.

For information about the schema used in CSV Reports, consult the SQL Access using ODBC How to Guide. To find this functionality, go to **Monitor> Schedule Reports > CSVReports.**

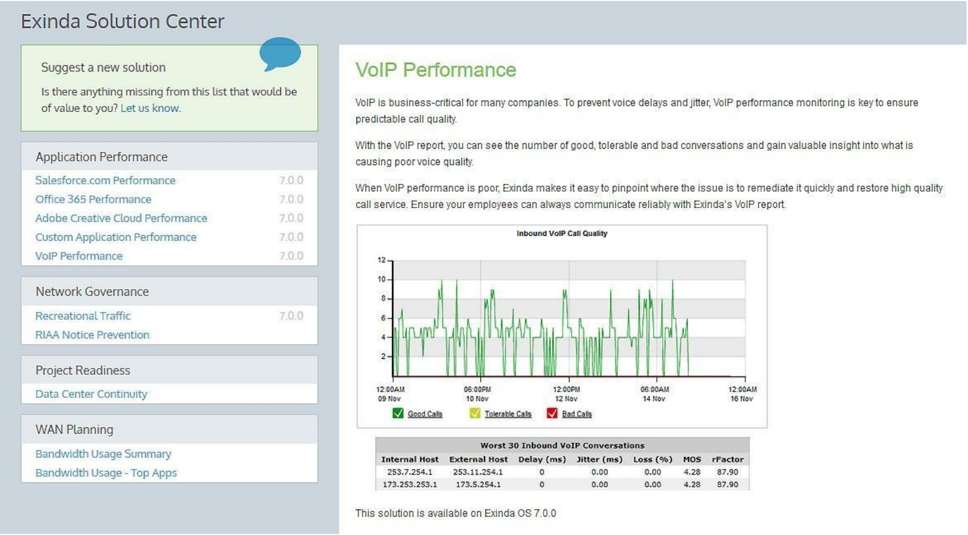
3.3 Monitoring applications with the ClearView Solution Center

The ClearView Solution Center provides a series of predefined monitors you can run to generate network performance reports for applications like FTP, SSH, Salesforce.com, Office365 VoIP and many more.

The generated reports answer questions, such as:

- How is salesforce.com performing for network users?
- How are critical applications performing on the network?
- How can I best mitigate data center disasters?

Each solution description indicates which GFI ClearView OS version is required to run the solution, shown both in the solution list and in each solution description. You may need to upgrade your GFI ClearView OS version to take advantage of the desired solutions. Some solutions may not yet be available and are shown as ‘Coming soon’.



Is there anything missing from this list that would be of value to you? Let us know.

VoIP Performance

VoIP is business-critical for many companies. To prevent voice delays and jitter, VoIP performance monitoring is key to ensure predictable call quality.

With the VoIP report, you can see the number of good, tolerable and bad conversations and gain valuable insight into what is causing poor voice quality.

When VoIP performance is poor, Exinda makes it easy to pinpoint where the issue is to remediate it quickly and restore high quality call service. Ensure your employees can always communicate reliably with Exinda's VoIP report.

Worst 30 Inbound VoIP Conversations

Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

This solution is available on Exinda OS 7.0.0

Screenshot 139: The GFI ClearView Solution Center

Performance monitors are divided into four solution categories: Application Performance, Network Governance, Project Readiness and WAN Planning.

Each monitor has a description you can display by clicking its link in the left panel. Descriptions detail usage information and which GFI ClearView OS version is required to run the monitor. Some monitors also have short video descriptions.

3.3.1 How performance reports work

An GFI ClearView Appliance continuously collects network traffic data. Performance reports in the GFI ClearView Solution Center provide insight into that data by grouping it in meaningful ways and displaying it in charts, tables and graphs.

The process starts by analyzing traffic and computing initial threshold values to create a baseline. A baseline requires an hour's worth of network traffic data. If no traffic is observed for an application during a baselining period, the process continues until enough data is collected.

The baseline process may not take an hour. If an GFI ClearView Appliance has observed and stored traffic for the application within the hour the baseline process starts, the baseline process uses that stored information and only waits enough time for a total hour of data to be collected.

For example, if you create an application monitor with ten minutes left in an hour and the GFI ClearView captured network traffic for the application in that hour, the baseline process analyzes the previous fifty minutes of collected traffic data and completes the baseline period with data collected in the remaining ten minutes.

3.3.2 Using Application Performance reports

Application Performance monitors generate reports that display information about application users, application performance, application bandwidth consumption, and the amount of reduction achieved (if applicable).

Application Performance solutions provide a predefined set of application monitors. Except for VoIP, application monitors generate similar reports.

You can choose a monitor from the main GFI ClearView Solution Center screen or click the **Custom Application Performance** link to bring up a list of applications to choose from.

> **NOTE**
>
> The report description lists the minimum version of GFI ClearView OS required to run the report. If your GFI ClearView OS does not meet or exceed the requirement, the Run button will not be available.

Running an Application Performance report

The GFI ClearView Solution Center lists a set of predefined reports on the Solution Center main screen. You can choose to run one of those or you can choose to run one of the dozens of other reports by clicking **Custom Application Performance**.

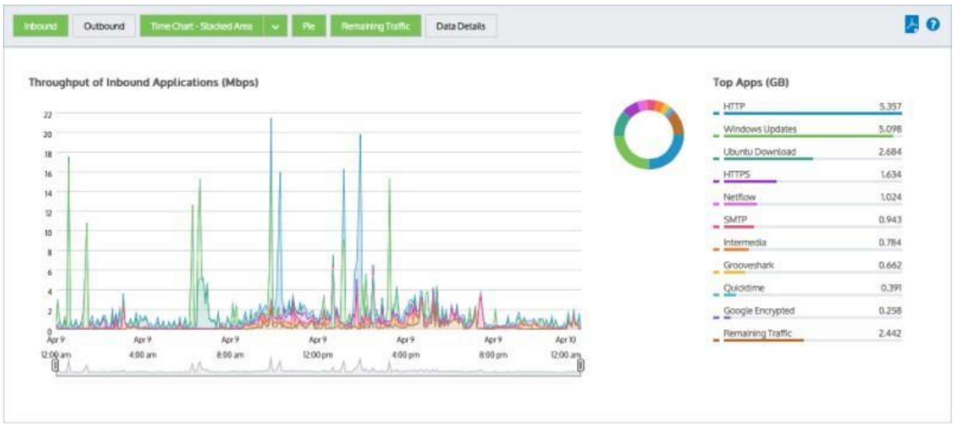
1. Go to Solution Center> Show Solution Center.
2. Under **Application Performance**, click the name of the report to run
3. Click **Run**. A confirmation screen opens.
4. Click **Ok**.

> **NOTE**
>
> After the initial run, you can access the report by clicking **Solution Center**, hovering over **Applications** and clicking the report name.

Understanding the data displayed in an Application Performance report

An Application Performance report shows the network user experience of an application through a series of charts, tables and graphs.

The Inbound and Outbound Bandwidth charts show how much bandwidth an application uses. Chart lines typically show spikes instead of raised flat tops. Flat tops may indicate traffic limitations imposed by policy rules.



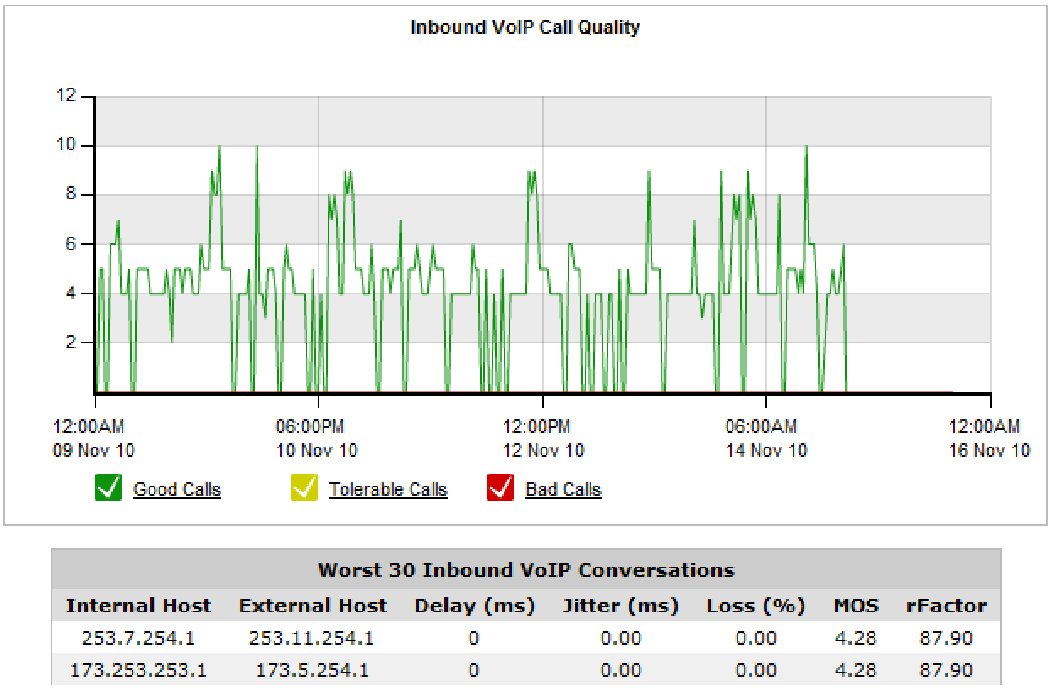
Top Apps (GB)

HTTP	5.357
Windows Updates	5.098
Ubuntu Download	2.684
HTTPS	1.634
Netflow	1.024
SMTP	0.943
Intermedia	0.784
Grooveshark	0.662
Quicktime	0.391
Google Encrypted	0.258
Remaining Traffic	2.442

Screenshot 142: Users and hosts barcharts.

Users and Hosts bar charts display bandwidth volume by top listeners and talkers. Multi-user applications typically show an even distribution among top users or hosts. If a user or host displays more bandwidth volume than other users and hosts, that situation may warrant investigation.

You can choose to show internal endpoints (LAN-side of an GFI ClearView Appliance), external endpoints (WAN-side of an GFI ClearView Appliance), users only or hosts only. For more information, refer to Monitoring real time application response.



Worst 30 Inbound VoIP Conversations

Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

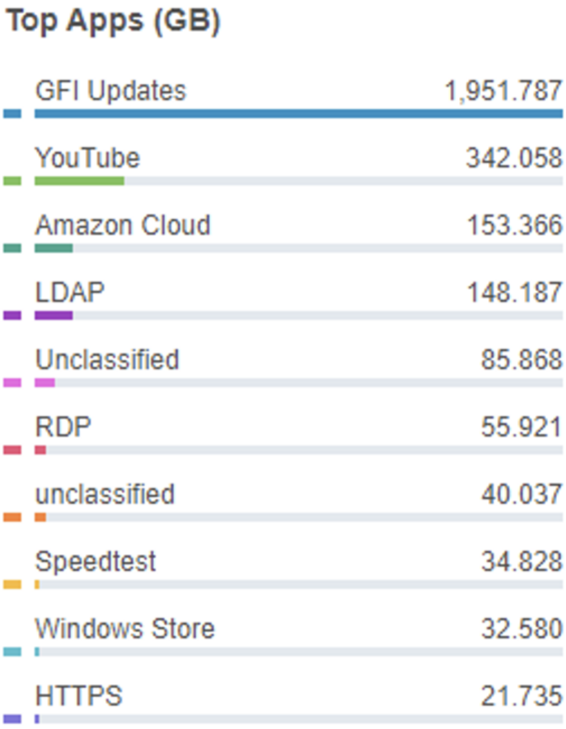
Screenshot 143: The Application Performance Scores and Metrics table.

Application Performance Scores and Metrics displays the APS score for the application. A good score is between 8.5 and 10.0. A score less than 7.0 may warrant an investigation.

3.3.3 Bandwidth usage

bandwidth usage - top apps

Knowing how much bandwidth your top applications consume can provide insight into weather controlling particular apps could help effectively reduce your throughput.



Top Apps (GB)

GFI Updates	1,951.787
YouTube	342.058
Amazon Cloud	153.366
LDAP	148.187
Unclassified	85.868
RDP	55.921
unclassified	40.037
Speedtest	34.828
Windows Store	32.580
HTTPS	21.735

Screenshot 144: Top App usage graph

To see how much bandwidth your top application are using go to **Monitor> Applications**. For more information, refer to Viewing application traffic volume.

bandwidth usage - top summary

Knowing how much bandwidth your users are consuming is crucial to managing your network. If your link is congested, you need to know whether to plan for a bandwidth upgrade, or if policy-based shaping can effectively reduce your throughput instead.

To see how much of your network's bandwidth is in use, go to **Monitor> Interfaces**. For more information, refer to Monitoring interface throughput.

3.3.4 Using the Application Performance Monitor VoIP report

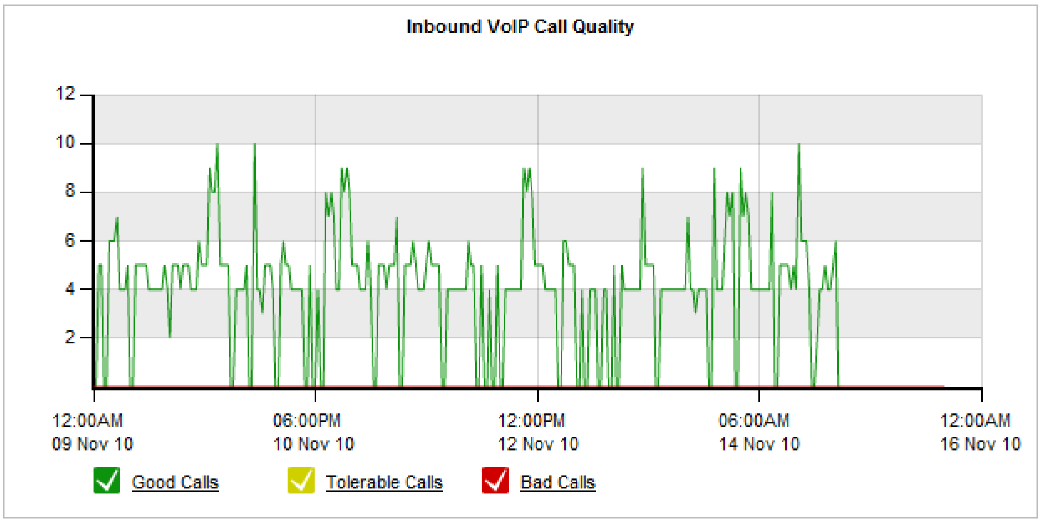
The VoIP report monitors and reports on the quality of VoIP transactions in a network. It displays data using telecommunication industry standard measures like MOS and rFactor.

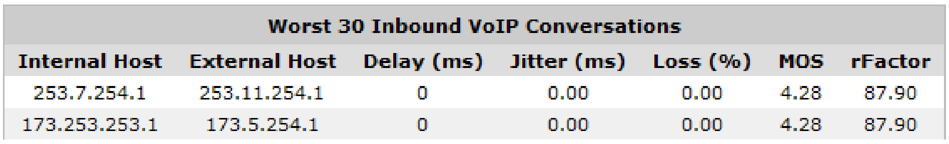
Running the Application Performance VoIP report

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
4. Go to Solution Center> Show Solution Center.
5. Under **Application Performance**, click **VoIP Performance > Run**. A confirmation screen opens.
6. Click **Ok**. The report opens.

> **NOTE**
> After the initial run, you can access the report by clicking **Solution Center> VoIP Performance**.

Understanding the data displayed in an Application Performance VoIP report





Worst 30 Inbound VoIP Conversations

Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

The graph shows three series, representing the number of "Good", "Tolerable" and "Bad" calls over time. The table below the chart lists the worst quality inbound and outbound VoIP calls for the specified time period.

The meanings of the colors:

- Good (green) - MOS greater than 4.
- Tolerable (yellow) - MOS between 2 and 4.
- Bad (red) - MOS less than 2.

What is MOS?

MOS, or Mean Opinion Score, is a measure of all quality. Historically, users would rate their call experience on a five point scale.

An GFI ClearView Appliance automates MOS ratings, taking into account network dependency conditions. The scores have the following meanings.

5 - Perfect, like face-to-face conversations or radio reception.

4 - Fair, imperfections perceived, but the sound is clear. Cell phone calls are typically rated fair.

3 - Annoying.

2 - Very annoying, nearly impossible to communicate.

1 - Impossible to communicate.

What is rFactor?

rFactor is a measure of the call quality in IP networks taking into account network delay and impairments. rFactor ranges from 0 (extremely poor quality) to 100 (high quality). Any rFactor less than 50 is not acceptable.

3.3.5 Recreational Traffic

The Recreational Traffic Report shows the usage of recreational application groups over time for the specified time period. It shows information for games, instant messaging, peer-to-peer, social networking, and streaming. This report can answer questions such as:

- How much data is going over my network for recreational applications?
- How many hosts are involved?
- How much time is spent transferring the data over the network?

Having visibility into key recreational applications is the first step in being able to manage them. These applications are generally undesirable because they can impact the performance of key business applications, negatively impact customer experience, reduce the productivity of users, introduce viruses to the network, and enable downloading of illegal or copyrighted material.

How to set up this report?

The report for recreational traffic can be created by visiting the GFI ClearView Solution Center

1. Go to Solution Center> Show Solution Center.
2. Under **Network Governance**, click **Recreational Traffic > Run**. A confirmation screen opens.

3. Click **Ok**.

> **NOTE**
> Once the report has been set up, you can access it by clicking Solution Center > Recreational Traffic.

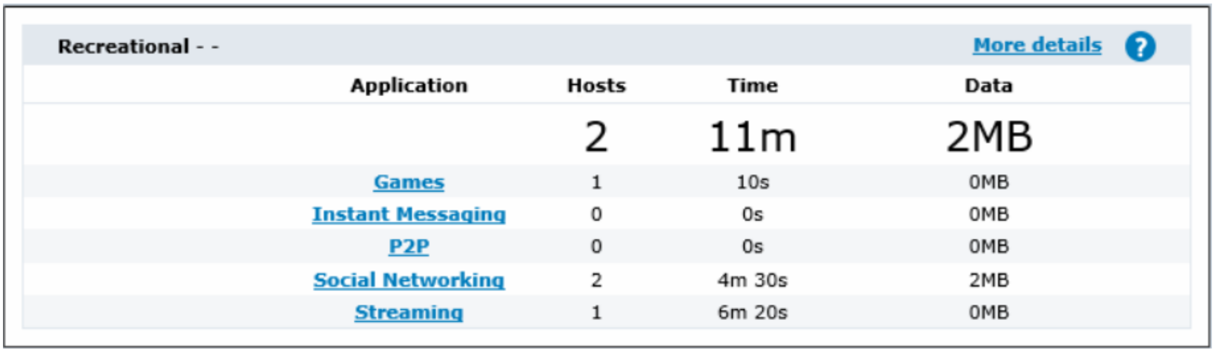
3.3.6 Using Network Governance reports

Network Governance reports provide data that allow you to manage your network resources according to ethical boundaries set by your organization. Solution categories include Recreational Traffic and RIAA Notice Prevention.

Understanding the data displayed in the Recreational Traffic report

The Recreational Traffic Report shows the bandwidth consumption of recreational applications for a specified time period. It shows network traffic data for games, instant messaging, peer-to-peer, social networking, and streaming.

Recreational applications are generally deemed undesirable on business networks because they impact the performance of key business applications, negatively impact customer experience, reduce user productivity, introduce viruses to the network, and enable downloading of illegal or copyrighted material.



Recreational - -

Application	Hosts	Time	Data
	2	11m	2MB
Games	1	10s	0MB
Instant Messaging	0	0s	0MB
P2P	0	0s	0MB
Social Networking	2	4m 30s	2MB
Streaming	1	6m 20s	0MB

Screenshot 146: The Recreational Traffic report.

Running the Recreational Traffic report

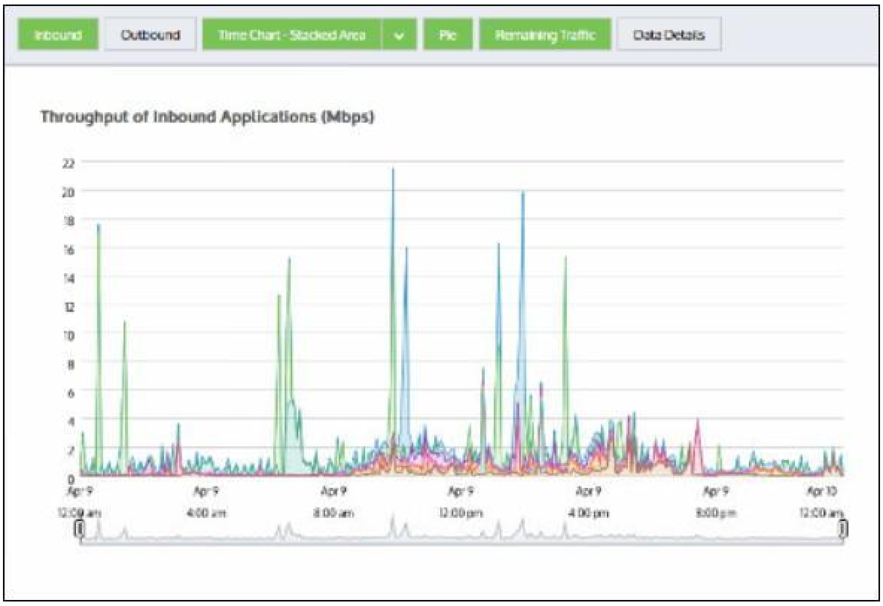
1. Go to Solution Center> Show Solution Center.
2. Under **Network Governance**, click **Recreational Traffic**.
3. Specify any details that the wizard requires.
4. Click **Ok**.

> **NOTE**
> After the initial run, you can access the report by clicking **Solution Center> Recreational Traffic**.

3.3.7 Answers to common questions about Solution Center Application Performance

What type of data is available in an Application Performance report?

An Application Performance report shows the network user experience of an application through a series of charts, tables and graphs.



Screenshot 147: Inbound bandwidth application

The Inbound and Outbound Bandwidth charts show how much bandwidth the application is using. You should expect the bandwidth to show spikes instead of raised flat tops.

The chart shows data measured on the WAN-side of the appliance before accelerated traffic is decompressed for inbound traffic and after acceleration and traffic shaping policies have been applied for outbound traffic.

You can overlay the data measured on the LAN-side of the appliance to show the amount of reduction achieved due to acceleration and traffic shaping.

The users and hosts bar charts show the WAN-side data volumes consumed by the top users and hosts for the application. Typically, applications are used by multiple users or hosts and the traffic distribution is fairly even amongst the top users or hosts.

If one user or host shows considerably more data volume than the other users, it may be reasonable behavior or it may indicate a problem worthy of further investigation. Also, you can choose to show just internal endpoints, that is, hosts and users on the LAN-side of your appliance, or just external endpoints, that is, hosts and users on the WAN-side of your appliance. You can also choose to show just users, just hosts, or both. Application Performance Score Metrics You should expect a good score (between 8.5 and 10.0). If the score is less than 7.0, you may want to investigate.

What is Application Performance report baselining?

An Application Performance monitor requires a baseline understanding of observed traffic for an application in your network. The process of collecting data and setting a baseline is called baselining.

Once you create a monitor, the baselining operation starts automatically analyzing traffic and begins the process of computing initial threshold values. This process requires an hour's worth of network traffic data.

If no traffic is observed for an application during a baselining period, the baselining process repeats until traffic is observed and thresholds are calculated.

The baselining process may not always take an hour if an GFI ClearView Appliance has observed and stored traffic for the application within the hour the baselining process starts.

For example, if you create an application monitor with ten minutes left in an hour and the GFI ClearView captured network traffic for the application in that hour, the baselining process analyzes the previous fifty minutes of collected traffic data. It then completes the baseline period in the remaining 10 minutes of the hour.

What if the Solution Center indicates there are no solutions?

The solution descriptions are served up from an GFI ClearView hosted server. If your GFI ClearView Solution Center indicates there are no solutions, check for Internet connectivity and connectivity to the GFI ClearView hosted server. If the GFI ClearView hosted server is down, previously instantiated solutions will still be available in your Solution Center.

What if a solution requires a higher GFI ClearView OS version?

The solution's **Run** button won't be available until you upgrade your GFI ClearView OS to the appropriate version or higher.

Can I run a solution more than once?

Yes. You can run a solution multiple times if the solution takes configuration parameters. For instance, you can create multiple Custom Application Performance monitors where each report monitors a different application. For solutions without configuration parameters, such as VoIP Performance, you cannot create the solution more than once.

3.3.8 Adding and deleting Solutions

Use the instructions that follow to add GFI ClearView Solutions to your configuration , and later, if necessary, delete them. When defined, the solutions provide access to reports that focus on the specified applications.

To add a solution

The GFI ClearView Solution Center includes several predefined solutions, but you can also define you own.

1. Go to **Solution Center> Show Solution Center**. The solutions, broken into categories, are accessible through the vari- ous links on the left.

2. Select the desired solution from the list.

3. Click the **Run** button.

4. Specify any details that the wizard requires. The final page of the wizard specifies where to find the report.

5. Clicking **Ok** will take you to your report.

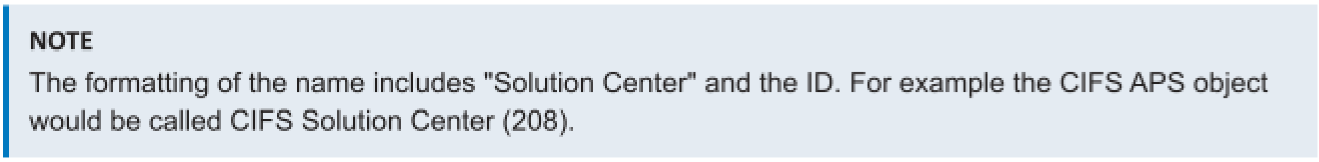
NOTE
Once a report has been set up, a link to it is available from the main task bar at the top of the page. Click **Solution Center> Report Name**.

To delete a solution

The only way to delete a solution is through the command line. However, for some solutions you need the determine the solution ID from the Web UI before you can remove the solution.

1. Go to Configuration > Objects> Service Levels> Application Performance Scores.

2. Find the application in the **APS Name** column.



NOTE
The formatting of the name includes "Solution Center" and the ID. For example the CIFS APS object would be called CIFS Solution Center (208).

3. Make a note of the solution ID.

4. Open the CLI.

5. At the prompt, type `no solutionc <id>`. Examples:

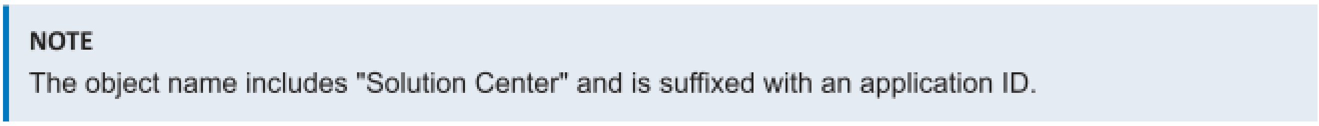
   - `no solutionc 208`
   - `no solutionc VoIPPerformance`
   - `no solutionc RecreationalTraffic`

3.3.9 Setting a new baseline

Use the following instructions to set a new baseline for an application performance score. If you need to set a new baseline, you should do this when you expect the application to perform reasonably well.

1. Go to Configuration > Objects> Service Levels> Application Performance Score (APS).

2. Find and select the APS object.

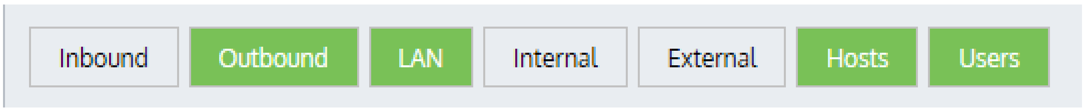


NOTE
The object name includes "Solution Center" and is suffixed with an application ID.

3. Select **Auto Baseline Period** and click **Start Baseline**.

3.3.10 Working with Application Performance charts

You can filter the data displayed on the page by toggling on and off the various charts. Click the buttons at the top of the page to switch between the views. If a button is green, the data appears on the page.



Determining throughput values for specific points in time in the throughput chart

Hover your cursor over the chart. A data brush will appear showing average throughput for the specific point in time.

3.3.11 Investigating a poor application performance score (APS)

From an application performance chart, click **Show details**. A new screen charts the measures contributing to the APS:

- Network delay and normalized network delay – the amount of time for data to traverse the network (on the wire)
- Server delay and normalized server delay – the amount of time for a server to respond to a request
- Round trip time – the amount of time for data to travel from a device across a network and return
- Jitter – a measure of the variability of Network Delay. We define it as one standard deviation of the Network Delay.
- Inbound loss and outbound loss – the amount of data retransmitted

Inspect the charts to determine which attribute caused the poor APS score. For example, if the server delay measures are good but the network delay measures are bad, then you know that the network is to blame and perhaps you can do something about it. If the network delay measures are good but the server delay measures are bad, then you should have someone investigate why the server is performing poorly.

Note that if the baselining period was not typical, then the calculated thresholds may be overly high or low. For example, if the application was baselined on a weekend when there was very little traffic, then the thresholds may be much lower than would be expected when the network is in a typical use scenario. Similarly, if the application was base-lined during an extremely busy time, such as when most employees are watching an online CEO webcast, then the thresholds may be much higher than would be expected when the network is in a typical use scenario.

3.3.12 Investigating unusual performance

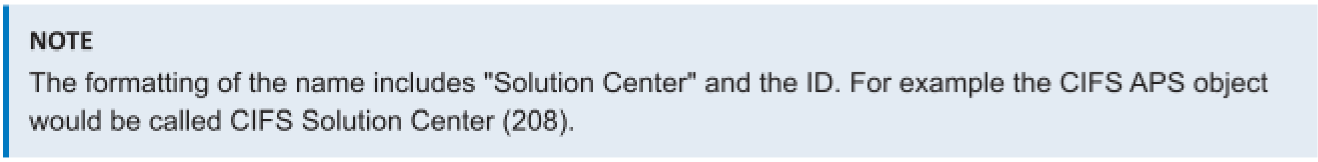
Zoom into the area of interest by opening the **Show data for** drop-down list and selecting one of the defined time spans. If necessary, use the slider controls below the chart to further refine the period. All the time series charts on this screen (inbound throughput, outbound throughput) will synchronize so that you can look for correlations in the data.

If any flat tops correspond to drops in application performance score, you likely have an issue that relates to a policy (or policies) that control the application. The policy environment may not guarantee the application sufficient bandwidth, or that less important apps, such as recreational apps, have too much bandwidth. To determine your best course of action you may need to look at the charts for other applications or application groups to see if the allowed bandwidth is appropriate.

3.3.13 Deleting an Application Performance report

The only way to delete a solution is through the command line. However, for some solutions you need to determine the solution ID from the Web UI before you can remove the solution.

1. Go to Configuration > Objects> Service Levels> Application Performance Scores.
2. Find the application in the **APS Name** column.



NOTE

The formatting of the name includes "Solution Center" and the ID. For example the CIFS APS object would be called CIFS Solution Center (208).

3. Make a note of the solution ID.
4. Open the CLI.
5. At the prompt, type `no solutionc <id>`. Examples:
   - `no solutionc 208`
   - `no solutionc VoIPPerformance`
   - `no solutionc RecreationalTraffic`

4 Settings

Learn how to configure GFI ClearView Appliance to meet your requirements.

4.1 Network settings

Learn how to configure the network setting for your GFI ClearView Appliance(s).

4.1.1 NIC configuration

The NIC settings page is used to set the speed, duplex, and MTU of the System NICs.

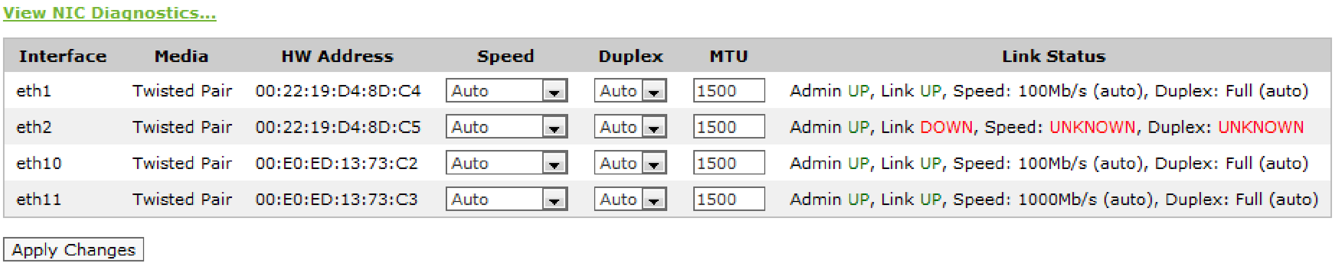
Interface Settings

You need the GFI ClearView appliance and devices that are connected to the appliance to have the same speed and duplex settings for their network interfaces. In most cases the default settings will work as the GFI ClearView is setup to auto-negotiate. However, some equipment is not compatible with this.

If the appliance and connected devices are using different speeds and duplex settings, the devices may not communicate and traffic may be dropped. In this case, you may notice collisions, errors, packet loss, and network delays on the GFI ClearView NICs, which will cause the System health status to show as "Warning" and the offending interface(s) will be highlighted.

To resolve this, check if the router or switch is hard-coded to a speed or duplex setting. If hard-coded, then either set all devices to auto-negotiate or set the GFI ClearView device to the same speed and duplex mode.

> **NOTE**
> For further troubleshooting, click on the system warning or view the NIC Diagnostics by clicking on the View NIC Diagnostics link.



Interface	Media	HW Address	Speed	Duplex	MTU	Link Status
eth1	Twisted Pair	00:22:19:D4:8D:C4	Auto	Auto	1500	Admin UP, Link UP, Speed: 100Mb/s (auto), Duplex: Full (auto)
eth2	Twisted Pair	00:22:19:D4:8D:C5	Auto	Auto	1500	Admin UP, Link DOWN, Speed: UNKNOWN, Duplex: UNKNOWN
eth10	Twisted Pair	00:E0:ED:13:73:C2	Auto	Auto	1500	Admin UP, Link UP, Speed: 100Mb/s (auto), Duplex: Full (auto)
eth11	Twisted Pair	00:E0:ED:13:73:C3	Auto	Auto	1500	Admin UP, Link UP, Speed: 1000Mb/s (auto), Duplex: Full (auto)

Screenshot 205: Set and view the speed, duplex, MTU of NIC interfaces

Where do I find this configuration?

Go to **Configuration** > **System** > **Network> NICs**.

To configure the NIC interfaces

1. In the interface table, you will see:

   - **Interface** - Each interface corresponds to a physical port.
   - (e.g. eth1, eth2) **Media** - Indicates the interface media. The
   - options are Twisted pair or Fibre. **HW Address** - Indicates the

     MAC address of the interface.

2. Specify the **Speed** and **Duplex** at which the GFI ClearView will negotiate with neighboring equipment. Use **Auto** speed to allow the GFI ClearView appliance to auto-negotiate the speed with neighboring equipment. Use **Auto** duplex to allow the GFI ClearView appliance to auto-negotiate the duplex with neighboring equipment.

3. Specify the **MTU** (maximum transmission unit) size in bytes.

4. View the **Link Status**.The link status shows whether the interface is up/down, the link is up/down, as well as the speed/duplex that has been negotiated with the neighboring equipment.

5. Click **Apply Changes**.

4.1.2 IP address configuration

The GFI ClearView appliance allows you to configure network interfaces as required, and roles can be assigned to an interface (Mirror) and IP settings applied.

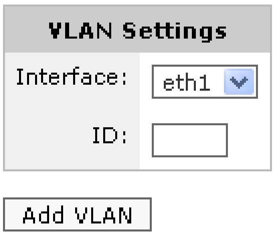
> **NOTE**
> For GFI ClearView, only the “Mirror” option is relevant, the other options are for the optimization-enabled version of GFI ClearView i.e. Exinda Network Orchestrator.”

For GFI ClearView, only a single role is required:

» **Mirror**- One or more interfaces may be configured in Mirror mode. This mode of operation is used for out of path monitoring using a hub or switch mirror/SPAN port.

The DHCP option is enabled by default on the GFI ClearView appliance. If a DHCP server is available, an IP address will be automatically assigned. From a web browser go to http://findmy.exinda.com/. This will download a Java applet and automatically find the GFI ClearView appliance. Click on the GFI ClearView appliance that has been found to access it. If a DHCP address is not picked up, the GFI ClearView will default to the IP address of 172.14.1.57.

The VLAN configuration allows an An 802.1Q VLAN ID to be set on an interface. The VLAN ID can be between 1 and 4094.



VLAN Settings

Interface: eth1

ID:

Further information on Clustering/HA, Mirroring and WCCP is available in the associated How To guides.

Where do I find this configuration?

Go to **Configuration > System > Network> IP Address**.

To configure an interface address and netmask automatically

1. For the given interface or bridge, select either the **DHCP** checkbox for IPv4 networks or **SLAAC** for IPv6 networks.
2. If **DHCP** is selected, an IP address will be automatically assigned.
3. If **SLAAC** is selected for IPv6 networks, the following additional options are shown:
   - **Privacy Address**- Enable SLAAC privacy extension. Selecting this option will periodically change the auto- matically assigned IPv6 address.
   - **Gateway**- Assign an IPv6 gateway dynamically.

To configure a static address

1. Enter an IPv4 or IPv6 address and netmask.
2. You can optionally add a comment describing how the interface is to be used in the **Comment** field.

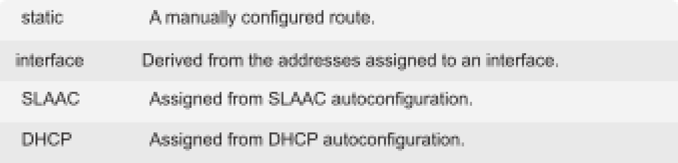
To configure the gateway settings

Enter the address of your network's default IPv4 and IPv6 gateways.

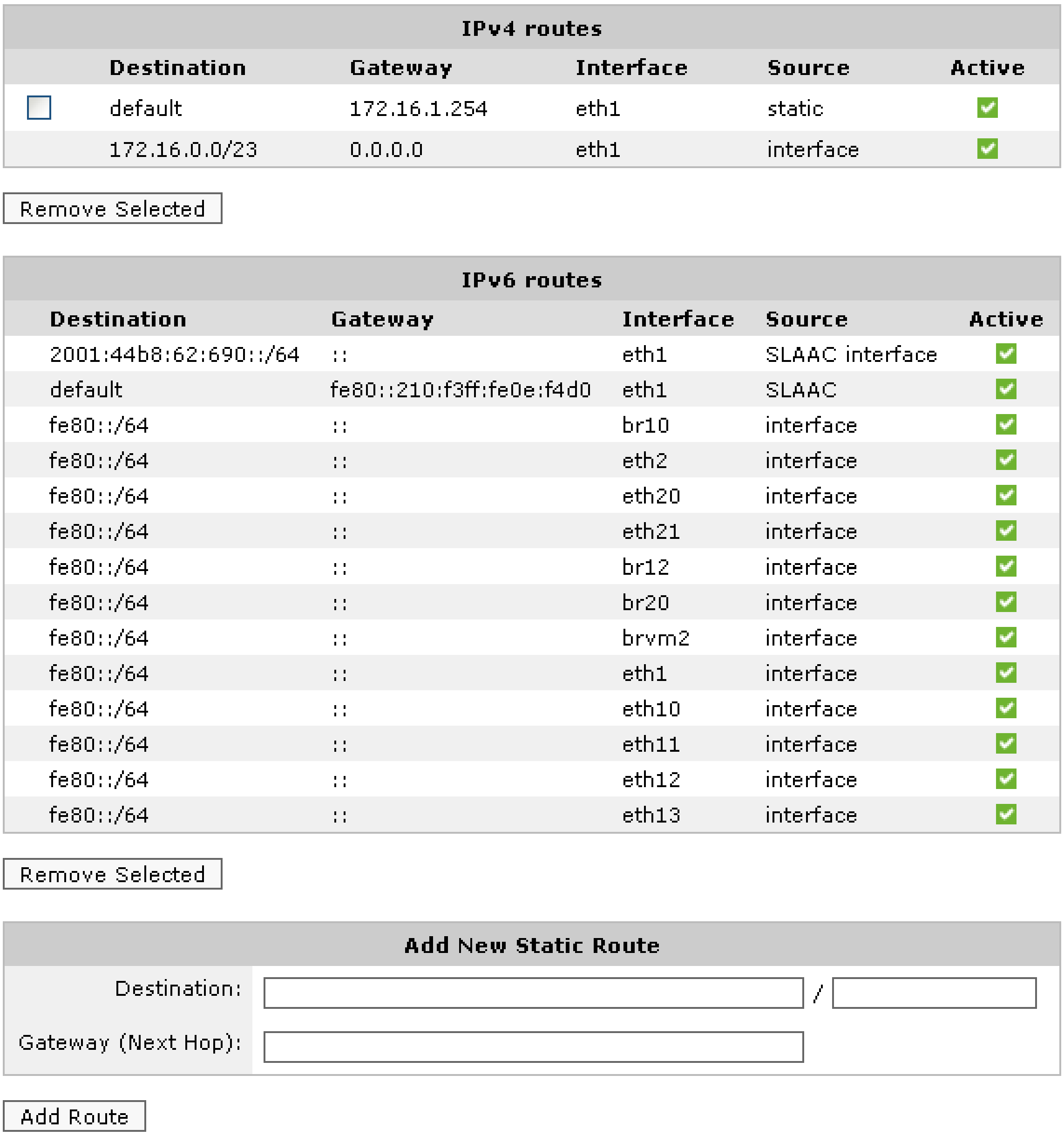
4.1.3 Routes configuration

Static routes may need to be defined when access to external networks cannot be reached via the default gateway. This may be necessary so the appliance can connect to services such as DNS or NTP.

Routing table entries are shown for IPv4 and IPv6 networks. The destination, gateway, interface, source and state is shown for each route. Routing table entries can have multiple sources:



static	A manually configured route.
interface	Derived from the addresses assigned to an interface.
SLAAC	Assigned from SLAAC autoconfiguration.
DHCP	Assigned from DHCP autoconfiguration.



IPv4 routes

	Destination	Gateway	Interface	Source	Active
☐	default	172.16.1.254	eth1	static	✓
	172.16.0.0/23	0.0.0.0	eth1	interface	✓

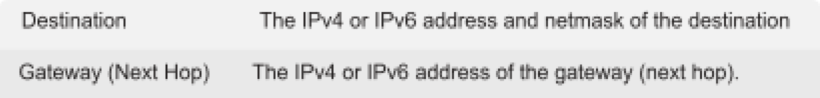
IPv6 routes

Destination	Gateway	Interface	Source	Active
2001:44b8:62:690::/64	::	eth1	SLAAC interface	✓
default	fe80::210:f3ff:fe0e:f4d0	eth1	SLAAC	✓
fe80::/64	::	br10	interface	✓
fe80::/64	::	eth2	interface	✓
fe80::/64	::	eth20	interface	✓
fe80::/64	::	eth21	interface	✓
fe80::/64	::	br12	interface	✓
fe80::/64	::	br20	interface	✓
fe80::/64	::	brvm2	interface	✓
fe80::/64	::	eth1	interface	✓
fe80::/64	::	eth10	interface	✓
fe80::/64	::	eth11	interface	✓
fe80::/64	::	eth12	interface	✓
fe80::/64	::	eth13	interface	✓

Add New Static Route

Destination:	/
Gateway (Next Hop):	

Screenshot 209: Routes configuration

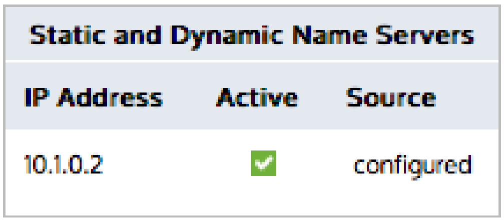


Destination	The IPv4 or IPv6 address and netmask of the destination
Gateway (Next Hop)	The IPv4 or IPv6 address of the gateway (next hop).

4.1.4 DNS and domain names configuration

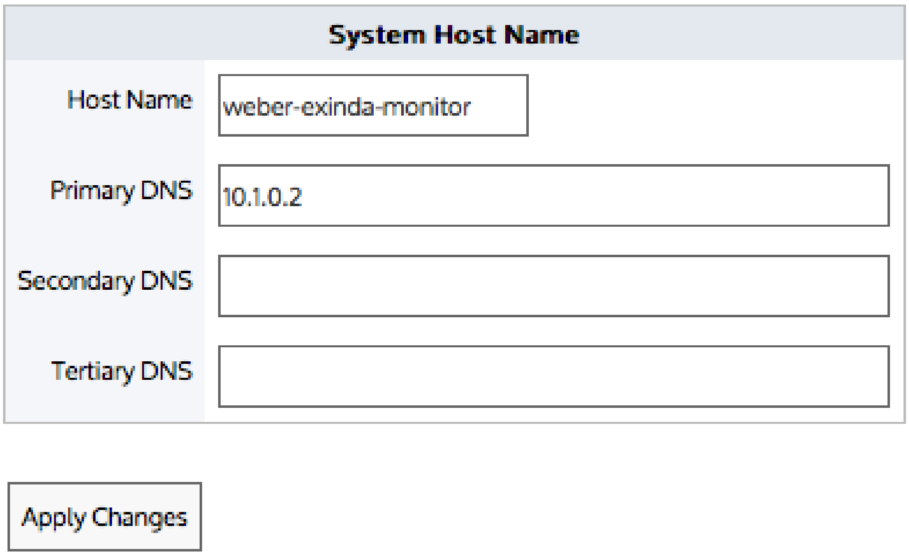
The DNS page is used to set a host name for your GFI ClearView appliance and to configure the location of your DNS server(s). You can also configure domain names that can be used to resolve hostnames in other configuration screens.

The GFI ClearView appliance hostname should be unique on the network. The DNS server setting may be dynamic, configured by the DHCP server, or it could be configured by entering one or more IP addresses of your DNS server(s).



Static and Dynamic Name Servers

IP Address	Active	Source
10.1.0.2	✓	configured

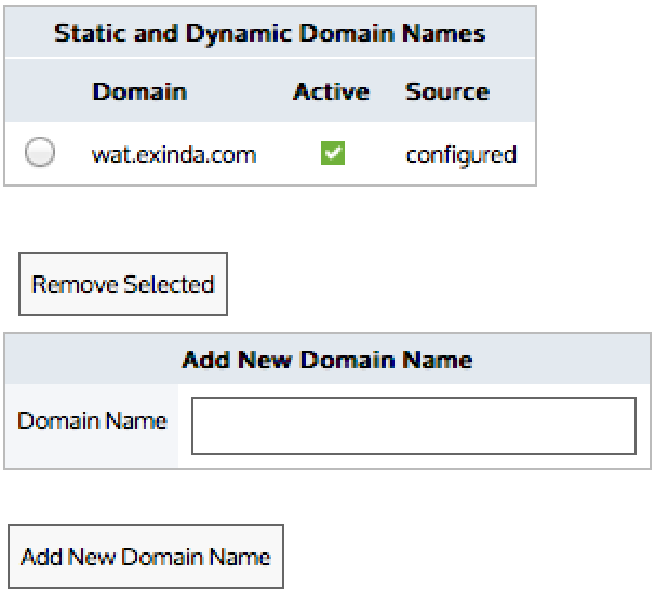


System Host Name

Host Name	weber-exinda-monitor
Primary DNS	10.1.0.2
Secondary DNS	
Tertiary DNS	

NOTE

A valid DNS server is required for system alerts, scheduled reports, firmware updates, license updates, and Anonymous Proxy updates



Static and Dynamic Domain Names			
	Domain	Active	Source
○	wat.exinda.com	✓	configured

Add New Domain Name	
Domain Name	

Where do I find this configuration?

Go to **Configuration > System > Network> DNS**.

To configure the appliance's hostname

1. In the **System Host Name** section, in the **Host Name** field, type the name for this appliance.
2. Click **Apply Changes**.

How to know if the DNS was configured by the DHCP server?

In the Static and Dynamic Name Servers section, there will be an IP address where the source is indicated to be dynamic. Dynamic means it was configured by the DHCP server.

To configure the location of the DNS servers

1. In the **System Host Name** section, type the IP addresses of your DNS servers in one or more of the **Primary DNS** field,
Secondary DNS field, and **Tertiary DNS** field.

2. Click **Apply Changes**. The IP addresses entered will appear in the Static and Dynamic Name Servers section as con- figured.

To add a domain name

1. In the **Add New Domain Name** area, type the new domain name.

2. Click **Add New Domain Name**. The domain name is added to the Static and Dynamic Domain Names list. All manu- ally added domain names are static.

To remove a domain name

1. In the **Static and Dynamic Domain Names** list, select the domain to remove. Only manually added domain names can be removed.

2. Click **Remove Selected**.

4.1.5 HTTP proxy configuration

Specify a HTTP proxy if you would like the appliance to access GFI ClearView’s server via HTTP proxy. Access to GFI ClearView's HTTP server is required for firmware updates, license updates, and Anonymous Proxy updates. If you have SDP enabled, please ensure your proxy supports HTTPS.

Where do I find this configuration?

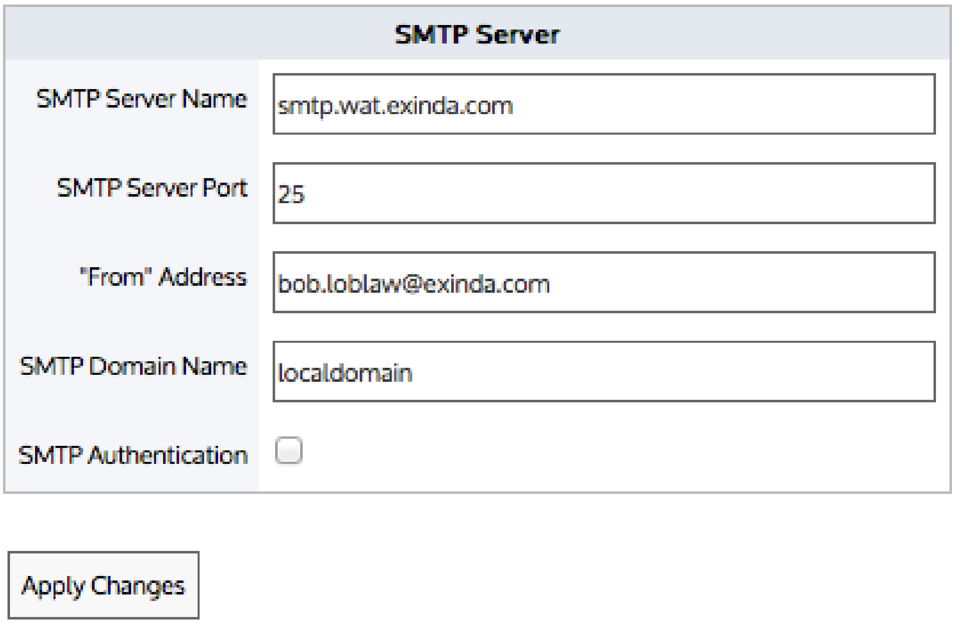
Go to **Configuration > System > Network> HTTPProxy**.

To configure access to GFI ClearView's server via HTTP proxy

1. Specify the hostname or IP address and HTTP proxy port of the HTTP proxy. IPv4 or IPv6 addresses can be specified.
2. Select the type of authentication for the HTTP proxy.
3. Type the **Username** and **Password** for the HTTP proxy.
4. To verify SSL certificates, clear the **Do not verify SSL certificates** checkbox.
5. Click **Apply Changes**.

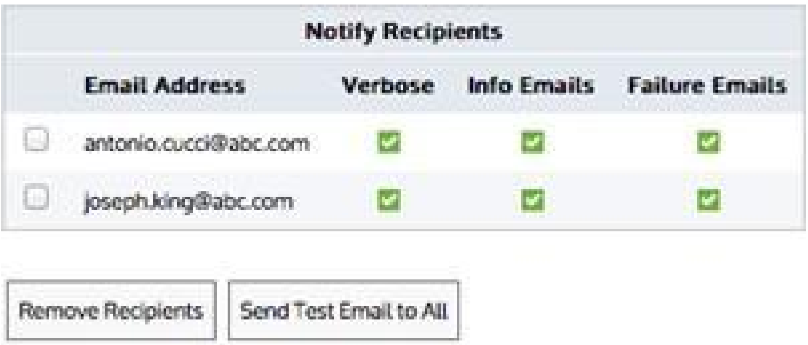
4.1.6 Email configuration

An SMTP server is required for sending email from the GFI ClearView appliance. The appliance can email scheduled reports, system alerts, and auto-support notifications. Initially, you must configure the connection to the SMTP server, and then manage the users who receive the system notifications.

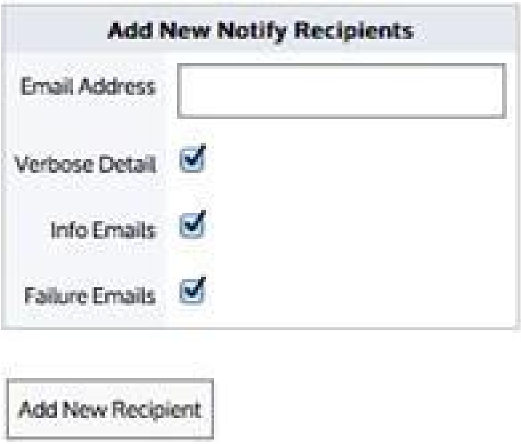


SMTP Server

SMTP Server Name	smtp.wat.exinda.com
SMTP Server Port	25
"From" Address	bob.loblaw@exinda.com
SMTP Domain Name	localdomain
SMTP Authentication	□



Notify Recipients				
	Email Address	Verbose	Info Emails	Failure Emails
□	antonio.cucci@abc.com	☑	☑	☑
□	joseph.king@abc.com	☑	☑	☑



Add New Notify Recipients

Email Address

Verbose Detail ☑

Info Emails ☑

Failure Emails ☑

Configuring SMTP server settings

Use the following instruction to configure the SMTP server settings.

1. Go to Configuration > System > Network> Email > SMTPServer.
2. In the **SMTPServer Name** field, type the name.

> **NOTE**
> You can use IPv4 or IPv6 addresses, or DNS names.

3. In the **SMTPServer Port** field, type the port number.

> **NOTE**
> The default port number is 25.

4. In the **"From" Address** field, type the email address from which the system alerts and report notifications should be sent.
5. If authentication is required, select the **SMTP Authentication** checkbox, and provide the **Username** and **Password**.
6. If necessary, select the **Use Secure Sockets Layer (SSL)** checkbox.
7. Click **Apply Changes**.

Testing the SMTP configuration

Use the following instructions to test the SMTP configuration.

1. Go to Configuration > System > Network> Email > Add New Notify Recipients.

2. Add your own email address and click **Add New Recipient**. The list in the "Notify Recipients" section above updates.

3. In the **Notify Recipients** section, click **Send Test Email to All**.

Adding notification email recipients

Use the following instructions to add new notification email recipients.

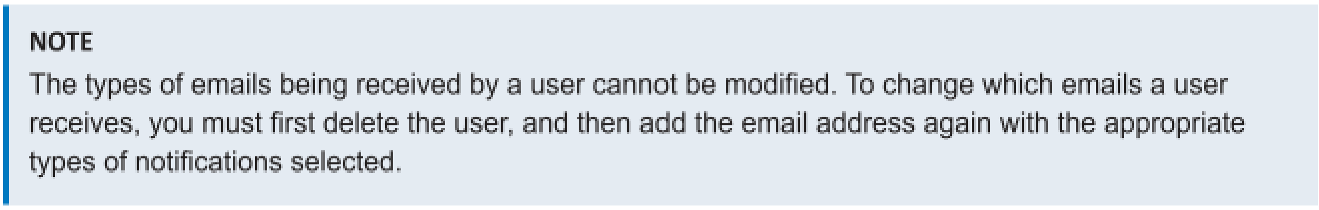
1. Go to Configuration > System > Network> Email > Add New Notify Recipients.

2. In the **Email Address** field, type the email address.

3. Select the types of notifications the user should receive:

    - **Verbose Detail**—Send detailed event emails to the user.
    - **Info Emails**—Send informational emails to the user.
    - **Failure Emails**—Send failure emails to the recipient.

4. Click **Add New Recipient**. The new recipients are added to the Notify Recipients list above.



NOTE

The types of emails being received by a user cannot be modified. To change which emails a user receives, you must first delete the user, and then add the email address again with the appropriate types of notifications selected.

Removing notification email recipients

Use the following instructions to remove users from the list of notification email recipients.

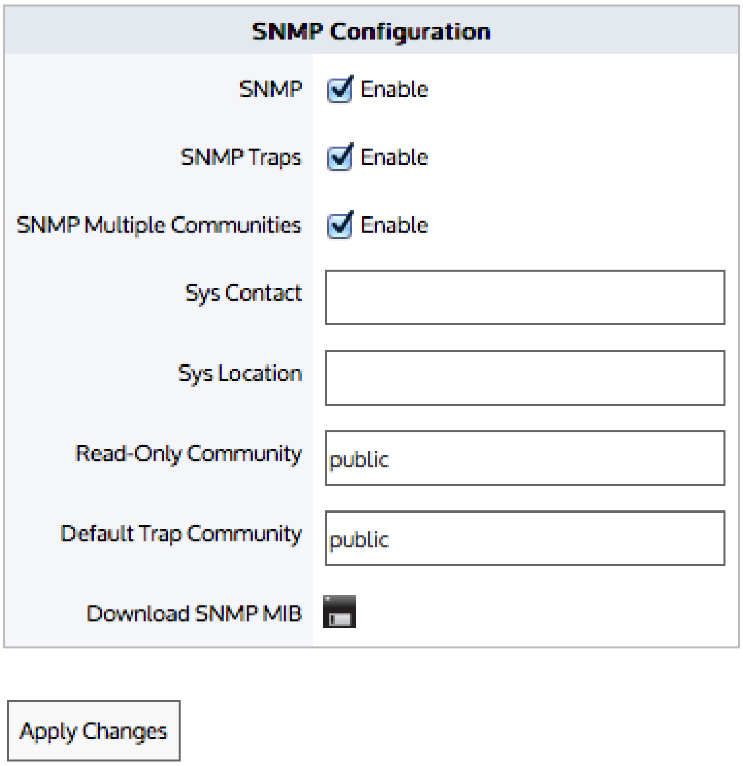
1. Go to Configuration > System > Network> Email > Notify Recipients.

2. In the list, select the user to be deleted.

3. Click **Remove Recipients**. The user is removed from the list, and will no longer receive email notifications.

4.1.7 SNMP configuration

The GFI ClearView appliance allows data export to SNMP systems. Configure the SNMP settings or download the GFI ClearView SNMP MIB.



SNMP Configuration

SNMP	☑ Enable
SNMP Traps	☑ Enable
SNMP Multiple Communities	☑ Enable
Sys Contact	
Sys Location	
Read-Only Community	public
Default Trap Community	public
Download SNMP MIB	💾

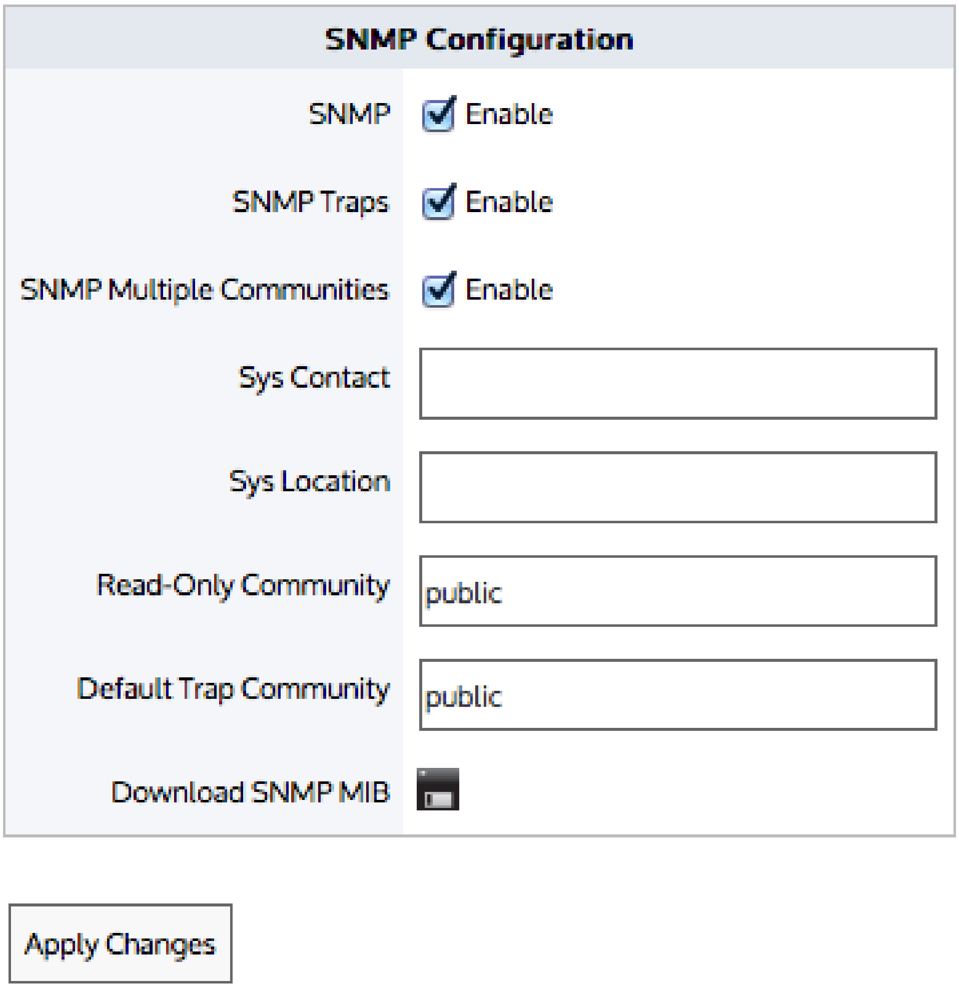
NOTE

To disable or enable SNMP traps for system alerts, see For more information, refer to Alerts (page 581)..

Configuring SNMP

Use the following instructions to configure SNMP.

1. Go to Configuration > System > Network> SNMP> SNMPConfiguration.



SNMP Configuration

SNMP ☑ Enable

SNMP Traps ☑ Enable

SNMP Multiple Communities ☑ Enable

Sys Contact

Sys Location

Read-Only Community: public

Default Trap Community: public

Download SNMP MIB

2. Enable the following, as needed:

   - SNMP
   - SNMP Traps
   - SNMP Multiple Communities

> **NOTE**
> When the Multiple Communities option is disabled, the Community list area does not appear.

4. In the **Sys Contact** field, specify the syscontact variable in MIB-II.

5. In the **Sys Location** field, specify the syslocation variable in MIB-II.

6. Type the **Read-only** and **Default Trap** community string.

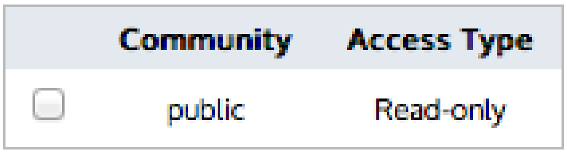
> **NOTE**
> When the Read-only community is changed to have a value that does not match an existing community, a new SNMP community is added to the list.

7. Click **Apply Changes**.

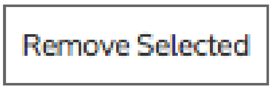
Removing an unwanted SNMP Community

Use the following instructions to remove an unwanted SNMP community.

1. Go to Configuration > System > Network> SNMP> List of configured SNMPCommunities.



	Community	Access Type
□	public	Read-only



2. In the list of **SNMPCommunities** area, select the checkbox next to community entry and click **Remove Selected**.

Downloading the SNMP MIB file

Use the following instructions to download the SNMP MIB file. The file contains additional monitoring information.

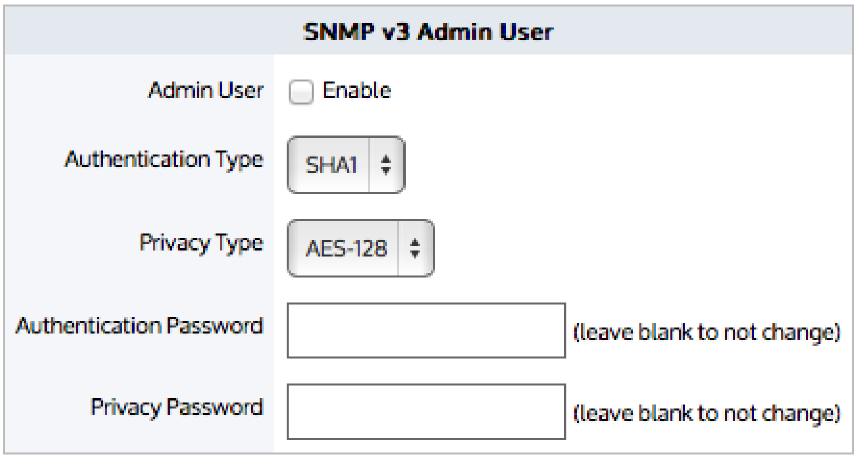
1. Go to Configuration > System > Network> SNMP.

2. Under **SNMPConfiguration**, click **Download SNMPMIB** 💾 . The `EXINDA-MIB.txt` file downloads to the location you specify.

Changing SNMP authentication for Admin user

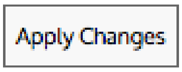
Use the following instructions to change the SNMP authentication for the Admin user.

1. Go to Configuration > System > Network> SNMP> SNMPv3 Admin User.



SNMP v3 Admin User

Admin User	□ Enable
Authentication Type	SHA1
Privacy Type	AES-128
Authentication Password	(leave blank to not change)
Privacy Password	(leave blank to not change)



2. If you need to enable **Admin User**, select the checkbox.

3. From the **Authentication Type** spin-box, select either SHA1 or MD5.

4. From the **Privacy Type** spin-box, select either AES-128 or DES.

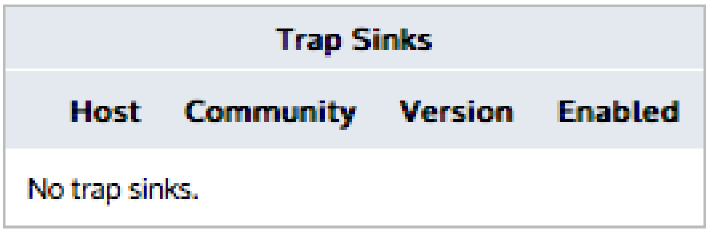
5. If necessary, change the **Authentication Password** by typing the new password.

6. If necessary, change the **Privacy Password** by typing the new password.

7. Click **Apply Changes**.

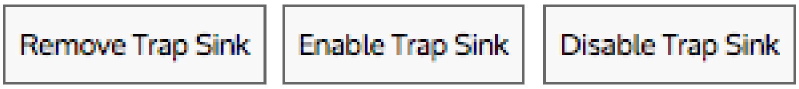
Temporarily stopping the sending of SNMP traps

Use the following instructions to disable the sending of SNMP traps to the sink server.



Trap Sinks

Host	Community	Version	Enabled
No trap sinks.			



1. Go to Configuration > System > Network> SNMP> Trap Sinks.
2. In the list, select the checkbox for server and click **Disable Trap Sink**.
3. To re-enable the server, select the server from the list and click or **Enable Trap Sink**.

Removing Trap Sink servers

Use the following instruction to remove a trap sink server.

1. Go to Configuration > System > Network> SNMP.

Trap Sinks

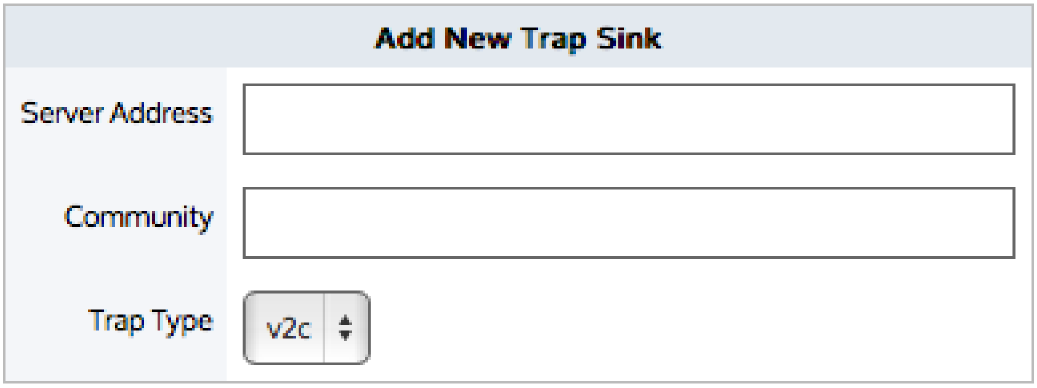
Host	Community	Version	Enabled
No trap sinks.			

2. In the **Trap Sinks** area, select the server from the list and click **Remove Server**.

Defining SNMP trap destinations

Use the following instructions to define where SNMP traps are sent.

1. Go to Configuration > System > Network> SNMP.



Add New Trap Sink

Server Address

Community

Trap Type v2c

2. In the **Add New Trap Sink** area, specify the hostname or IP address of the SNMP trap sink server.

> **TIP**
> You can specify IPv4 or IPv6 addresses, or a hostname.

3. Type the **Community** string for the SNMP trap sink server.
4. Select the appropriate SNMP trap type to send to the sink server.
5. Click **Add New Trap Sink**.

4.1.8 Integrate with Active Directory

> **NOTE**
> You can configure the options in the Active Directory tab only after the GFI ClearView AD Connector is installed and configured on a designated network server that has access to the Active Directory Server. You will see the Active Directory Server details on this tab only when the configuration is completed successfully.

Configuring Active Directory allows the GFI ClearView Appliance to accept network users and groups from Active Directory (e.g logins, IP address, group membership) resulting in the ability to:

- Expose Active Directory usernames in monitoring and reporting, no longer having to view
- users as IP addresses. Use Active Directory groups and usernames in optimization policies,

thereby implementing QoS and Optimization

Polices based on individual users or entire groups.

To configure Active Directory, you need to install the GFI ClearView AD Connector on a designated network server, configure various settings, and then proceed to configure the port and password settings on the Active Directory tab on each GFI ClearView Appliance.

How Active Directory Integration Works

Active Directory integration allows you to expose AD usernames within monitoring and reporting on the GFI ClearView Appliance, rather than viewing the default IP Addresses. You can also use AD groups and usernames within optimization policies, allowing you to implement QoS and Optimization Policies based on individual users or entire groups.

Integration requires a proprietary GFI ClearView AD Connector service installed onto a server in the network that has access to the Active Directory server. After configuration, the Connector functions as a gateway between the Active Directory Server and the GFI ClearView Appliances to supply user and group information. As each user logs in using their Active Directory credentials, the information is gathered by the Connector and passed to the GFI ClearView Appliances. Within the Monitor reports, IP Addresses are replaced by the user and group names where obtained from Active Directory.

Integration Process

Complete the following tasks to connect the GFI ClearView AD Connector to the Active Directory server, and to select the individual GFI ClearView Appliances that will receive the AD information

> **NOTE**
>
> Each installation of the Active Directory Connector can have a maximum of 20 GFI ClearView Appliances connected to it.
>
> If there are more than 20 GFI ClearView Appliances, you will need to install the connector on multiple Windows servers and divide the appliances across multiple instances of the Active Directory Connector. The instructions below step you through configuring a single Connector. Repeat these instructions if you are installing more than one instance of the Active Directory Connector.

1. Install the GFI ClearView AD Connector. For more information, refer to Install the GFI ClearView AD Connector.

   a. Add the GFI ClearView Appliances to the GFI ClearView AD Connector. For more information, refer to Add the GFI ClearView Appliances to the GFI ClearView AD Connector.

   b. Identify the Active Directory Server. For more information, refer to Identify the Active Directory Server.

   c. Select the information sent between the GFI ClearView appliance and the Active Directory server. For more inform- ation, refer to Select the information sent between the GFI ClearView appliance and the Active Directory server .

   d. The GFI ClearView AD Connector port number. For more information, refer to The GFI ClearView AD Connector port number.

2. Identifying users. For more information, refer to Identifying users.

3. Verify communication between the Active Directory server and the GFI ClearView Appliance. For more information, refer to Verify communication between the Active Directory server and the GFI ClearView Appliance.

> **NOTE**
>
> If you encounter any issues, see Troubleshoot issues with Active Directory configuration.

Configuration Options

After the integration process is successful, you can complete the following tasks to expose user names in monitoring reports, and to implement optimization policies based on user groups.

- View top Internal and External Users on the Network
- Controlling Traffic Based on Users

Install the GFI ClearView AD Connector

To integrate Active Directory with the GFI ClearView Appliance, you need to install the GFI ClearView AD Connector service on a Windows server that can then connect to the Active Directory server. Each GFI ClearView AD Connector can talk to up to 20 GFI ClearView appliances.

You can download the Active Directory Connector from the **Configuration > System > Network> Active Directory** tab on the GFI ClearView Appliance. Click on the Microsoft Installer Executable link and save the installer to a location that can be accessed by all Windows servers in the network.

Installation Requirements

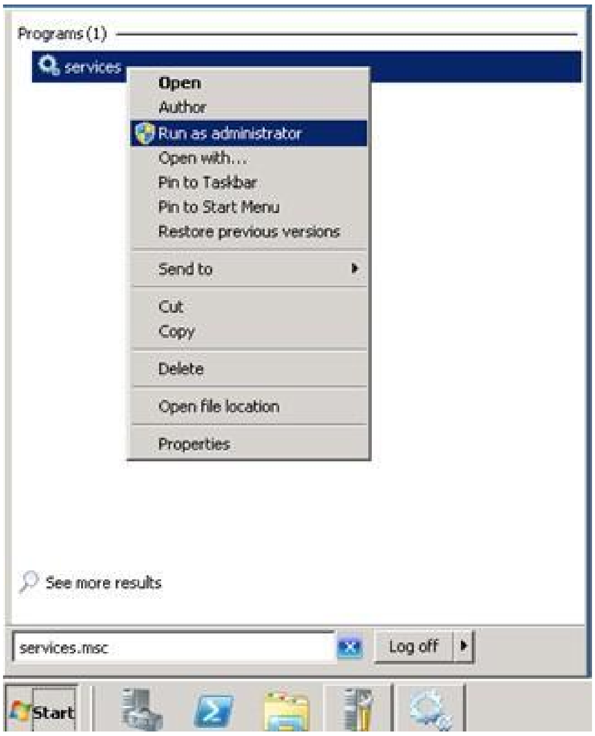
- The GFI ClearView AD Connector is supported on the following platforms:
    - Windows Server 2019 and earlier versions
- The GFI ClearView AD Connector requires .NET Framework 4.0.
- Logon Auditing must be enabled on the Active Directory server to install the GFI ClearView AD Connector.
- The WMI service must be started on the Active Directory server and on the server where the GFI ClearView AD Connector is installed.
- The Active Directory server and the server where the GFI ClearView AD Connector is installed require the RPC Endpoint Mapper and LDAP ports open in your firewall. These ports are open by default. To verify your settings, see http://sup- port.microsoft.com/kb/179442.

Providing the required permissions to the GFI ClearView AD service

When installing the ClearView AD Connector on a server that is not a domain controller, ensure that the account in charge of running the service is an Active Directory domain admin account.

To provide the required permissions

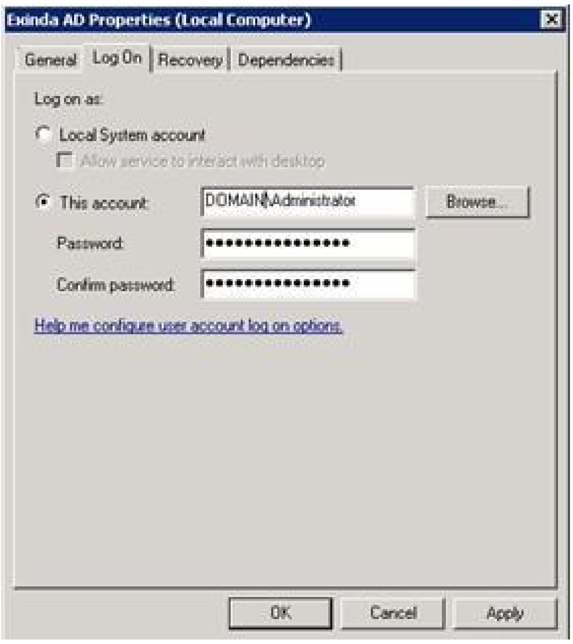
1. Run **Services.msc** as an Administrator.



2. Find the entry for the **GFI ClearView AD** service.
3. Right click on it and select **Properties**.
4. On the **Log On** tab, click **Browse** and select the domain and administrator account.

> **NOTE**
> The domain and slash (\) are required.

5. Type the **Password** and confirm.


Exinda AD Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
OK
Cancel
Apply

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: DOMAIN\Administrator

Password: ••••••••••••••••

Confirm password: ••••••••••••••••

6. Click **OK** or **Apply** to save the changes.
7. Restart the service.

Installing the GFI ClearView AD Connector

Use the following instructions to install the GFI ClearView AD Connector.

Before you begin

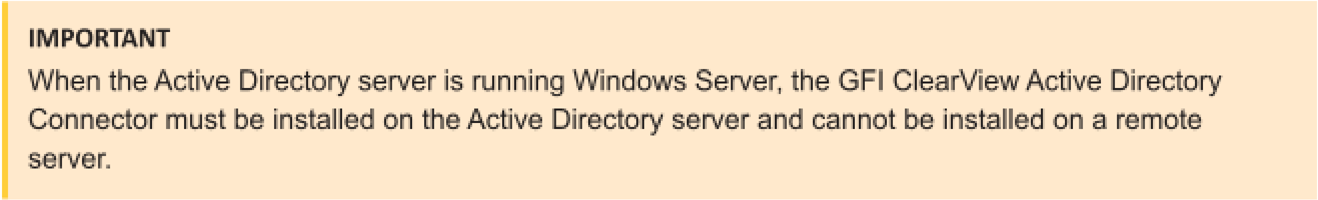
Ensure that you have followed the Installation Requirements. For more information, refer to Install the GFI ClearView AD Connector.

To install the Connector Service

1. On the server where the GFI ClearView Active Directory Connector should be installed, run the installation file.

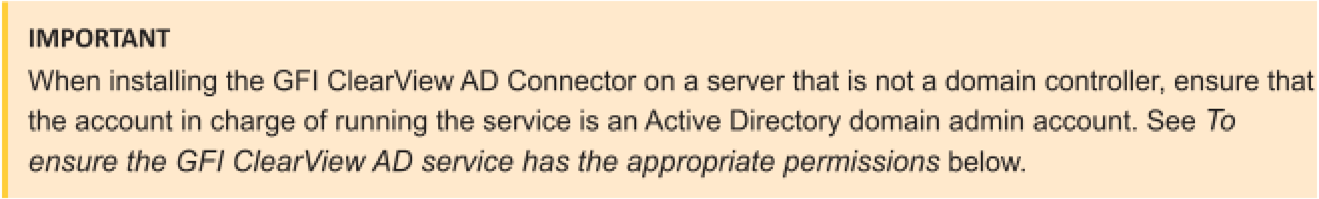
2. Read and accept the end-user license agreement, and then proceed through the screens, making the selections indicated below, and clicking Next where needed:

   - Specify the directory where the GFI ClearView Active Directory Connector should be installed.
   - Select whether the Active Directory server is on **this server** or **another server**. If the connector is not installed on the server with Active Directory, type the IP address or hostname of the Active Directory server, and type the username and password of the Administrator account on the Active Directory server.



IMPORTANT

When the Active Directory server is running Windows Server, the GFI ClearView Active Directory Connector must be installed on the Active Directory server and cannot be installed on a remote server.



IMPORTANT

When installing the GFI ClearView AD Connector on a server that is not a domain controller, ensure that the account in charge of running the service is an Active Directory domain admin account. See *To ensure the GFI ClearView AD service has the appropriate permissions* below.

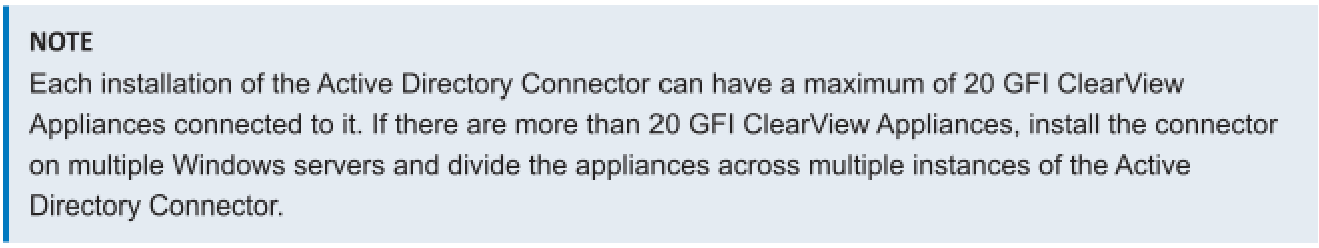
- Optionally, type the GFI ClearView appliance IP address or hostname, port number, and administrator password. This step is optional because you can add an GFI ClearView Appliance after the GFI ClearView Active Directory Connector is installed.
- In the **Include log entries newer than the specified age** field, specify the maximum age of log entries (in seconds) to be analyzed and sent to the GFI ClearView Appliance when the GFI ClearView Active Directory Connector service starts.

3. If any warnings are displayed, resolve the issues as specified in the dialog.
4. Click **Install**. Ensure **Launch GFI ClearView Active Directory Connector** is selected, and click **Finish**.

After the installation is finished, the GFI ClearView Active Directory Connector starts automatically and attempts to communicate with the configured GFI ClearView appliance. When you first install the GFI ClearView Active Directory Connector, it may take 24 hours or longer to obtain all user to IP address mappings as users progressively login.

Add the GFI ClearView Appliances to the GFI ClearView AD Connector

Identify the GFI ClearView Appliance using this GFI ClearView AD Connector to retrieve user and group information.



NOTE

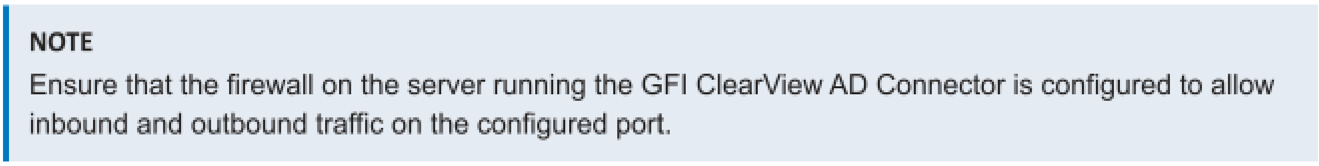
Each installation of the Active Directory Connector can have a maximum of 20 GFI ClearView Appliances connected to it. If there are more than 20 GFI ClearView Appliances, install the connector on multiple Windows servers and divide the appliances across multiple instances of the Active Directory Connector.

In the **GFI ClearView ADConfiguration Utility**, on the **GFI ClearView Appliances** tab, type the IP Address and hostname of each appliance into an empty row. You will also need to type the Admin **password** for each appliance. The port number refers to the port that the GFI ClearView AD Connector is using to communicate with the clients, and the GFI ClearView Appliance must all use the same port number. The default port number of the Active Directory Client is 8015. For more information, refer to The GFI ClearView AD Connector port number.

In the **Sync interval** field, identify how frequently the GFI ClearView AD Connector contacts the GFI ClearView Appliances to synchronize Active Directory user and group information. The default is 5 minutes.

The GFI ClearView AD Connector port number

By default, port 8015 is used to communicate Active Directory information between the GFI ClearView AD Connector and the connected GFI ClearView Appliances. You should change the port number only if a conflict necessitates the change. If you change the port on the Connector, you must also change the port on each of the GFI ClearView Appliances.



NOTE

Ensure that the firewall on the server running the GFI ClearView AD Connector is configured to allow inbound and outbound traffic on the configured port.

Changing the GFI ClearView AD Connector port number

If necessary, you can change the AD Connector port number using the following instructions. Changing the port number requires that you do this on both the server hosting the AD Connector, and each of the GFI ClearView appliances.

To change the port number on the GFI ClearView AD Connector

1. Launch the **GFI ClearView ADConfiguration Utility**.
2. Select the **GFI ClearView Appliances** tab.
3. Type a new port number in the field. The default port number is 8015.

To change the port number on each GFI ClearView Appliance

1. Log into the GFI ClearView Web UI.
2. Click **Configuration**, and from the System group, select **Network> Active Directory**.
3. Type the same port number you set above in the GFI ClearView AD Configuration Utility.
4. Apply the changes.
5. Repeat these steps for each GFI ClearView Appliance that communicates with this instance of the GFI ClearView AD Connector.

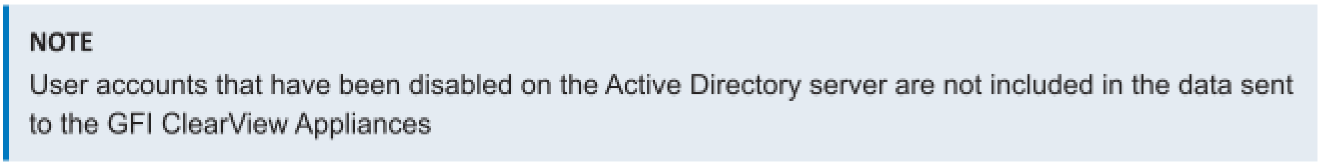
To determine if the port change was successful on the GFI ClearView Appliance

Wait a few moments to ensure the information on the Active Directory tab updates with new information:

- **IPAddress**– The IP address of the server running the GFI ClearView AD Connector.
- **Windows Version**– The version of Windows on the Active Directory server.
- **Version**– The GFI ClearView AD Connector version.
- **Agent Name**– The GFI ClearView AD Connector name.
- **Last Contact**– The last time the Active Directory server was contacted.

Select the information sent between the GFI ClearView appliance and the Active Directory server

Specify what information is sent between the Active Directory server and the GFI ClearView appliance. When you first install the GFI ClearView AD Connector, it may take a while to complete all user to IP address mappings as each user needs to logon.

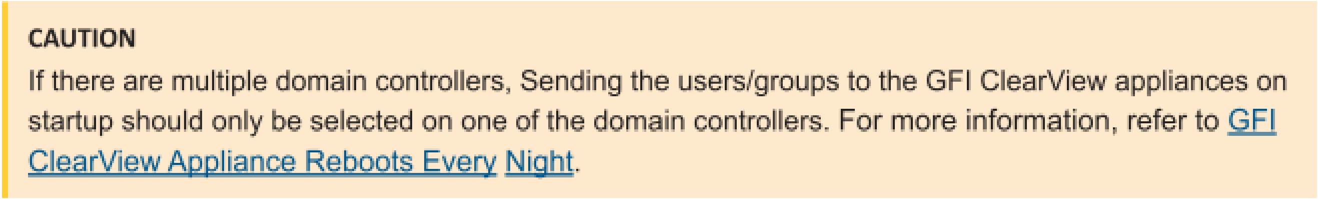


NOTE

User accounts that have been disabled on the Active Directory server are not included in the data sent to the GFI ClearView Appliances

1. In the GFI ClearView AD Connector, switch to the **ADServer** tab.

2. To send a list of users and groups to GFI ClearView appliances when the service starts, select **Send Active Directoryuserand group information to GFI ClearView appliances**. If this is not selected, only logged on users will be available to your GFI ClearView appliances. Information about groups will not be available. This information is obtained through an LDAP query against the Active Directory server.



CAUTION

If there are multiple domain controllers, Sending the users/groups to the GFI ClearView appliances on startup should only be selected on one of the domain controllers. For more information, refer to GFI ClearView Appliance Reboots Every Night.

3. To include user names in monitoring reports, allow the login history to be analyzed.

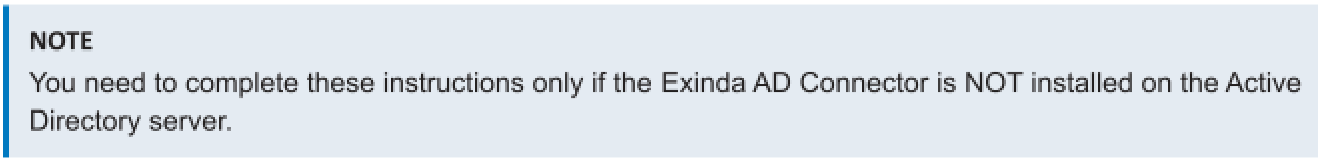
   a. To enable this option, select **Analyze login history and send to GFI ClearView appliance**. This information is obtained through a Windows Event Log query against the Active Directory server.

   b. In the **Include log entries newer than the specified age** field, specify the maximum age of log entries (in seconds) to be analyzed and sent to the GFI ClearView Appliance when the GFI ClearView AD Connector service starts.

4. Click **OK**.

Identify the Active Directory Server

The GFI ClearView AD Connector can be installed on any server in the network that has access to the Active Directory server. If the Connector is installed somewhere other than on the Active Directory server, you must specify the location and authentication credentials of the Active Directory server.



NOTE

You need to complete these instructions only if the Exinda AD Connector is NOT installed on the Active Directory server.

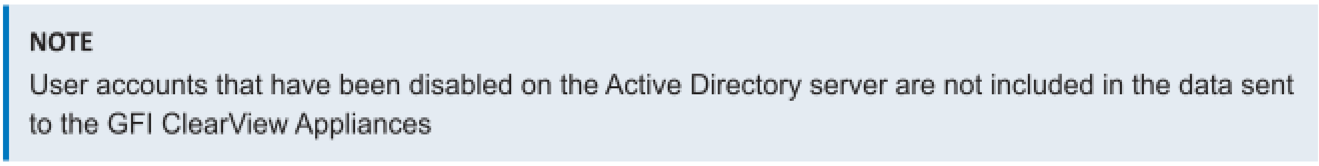
1. Launch the GFI ClearView AD configuration utility, and switch to the AD Server tab.

2. Select **another server**, and then type the **IPAddress** or the **hostname** of the Active Directory server.

3. To authenticate against the server, type the **username** and **password** of the Administrator account on the Active Directory server.

Verify communication between the Active Directory server and the ClearView Appliance

To ensure the communication between the Active Directory server and the GFI ClearView Appliance is successful, you can quickly check the Active Directory tab on the GFI ClearView Appliance. Login to the GFI ClearView Web UI. Click **Configuration**, and from the System group, select **Network> Active Directory**.



NOTE

User accounts that have been disabled on the Active Directory server are not included in the data sent to the GFI ClearView Appliances

Verify the Active Directory server is listed, and that the service is **Running**.

When the GFI ClearView Appliance successfully communicates with the Active Directory Client, the following information is displayed in the table:

- Agent Name– The Active Directory server name.
- IPAddress– The IP address of the Active Directory server.
- Version– The GFI ClearView Active Directory Windows client version.
- Windows Version– The Active Directory server Windows version.
- Last Contact– The last time the Active Directory server was contacted.

If the service is not visible on the list, run the Event Viewer program on your Active Directory server, and examine Windows logs:

1. From the **Start** menu select **Control Panel > Administrative Tools**.
2. Double-click **Services**, and verify the status of the **GFI ClearView AD** service. If the service is stopped, restart the service.

3. In the **Windows Logs> Application** area, a “Service started successfully” message should be displayed from GFI ClearView Networks Active Directory Connector.

If communications between the Active Director and the GFI ClearView Appliance are failing, an error message from the GFI ClearView Networks Active Directory Connector appears in these logs.

Request updated user and group information from the Active Directory server

If the list of users and groups using the Active Directory client appears to be out of date, erase all username to IP address mappings and refresh the list sent from the Active Directory server.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

5. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
6. To clear user, group, and login data from the appliance and requests an update from the Active Directory clients click **Renumerate**.

Change the state of the GFI ClearView AD Connector

Temporarily stop or disable the Active Directory integration to help with troubleshooting and to avoid errors when modifying the GFI ClearView AD Connector settings.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

5. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
6. Modify the state of the Active Directory service.

- To temporarily stop the GFI ClearView AD Connector, click Stop.
- If you are experiencing issues with the ClearView AD Connector, Restart the service.
- If you no longer need the GFI ClearView AD Connector running, click Disable.
- If the service has been disabled, to start it again click Enable.

Exclude specific usernames from reports

You may have user accounts that should not be linked to IP addresses when reporting on the GFI ClearView appliance, such as the account used for signing SMB traffic. Configure the GFI ClearView AD Connector to prevent the IP address to username mapping being sent to the GFI ClearView Appliance.

Before you begin…

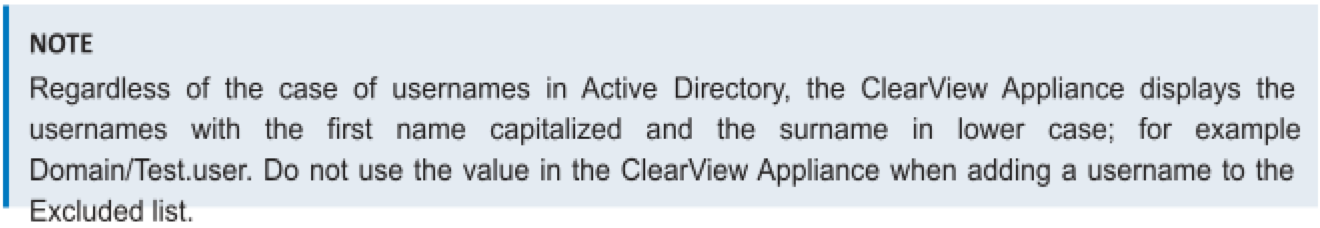
You need to understand the process of:

» Requesting updated user and group from Active Directory. For more information, refer to Request updated user and group information from the Active Directory server.

» Restarting the Active Directory service. For more information, refer to Change the state of the GFI ClearView AD Con- nector.

To exclude usernames

1. From the **Start** menu, click **All Programs> ClearView Networks > ClearView ADConfiguration Utility**.
2. Select the **Excluded Users** tab.
3. Click in the **Ignored User** s area and type the full username of each user to ignore. Usernames are case sensitive. If the Active Directory has the user Domain/Test.User, and the excluded list has the user as Domain/test.user, the traffic is not excluded.



NOTE

Regardless of the case of usernames in Active Directory, the ClearView Appliance displays the usernames with the first name capitalized and the surname in lower case; for example Domain/Test.user. Do not use the value in the ClearView Appliance when adding a username to the Excluded list.

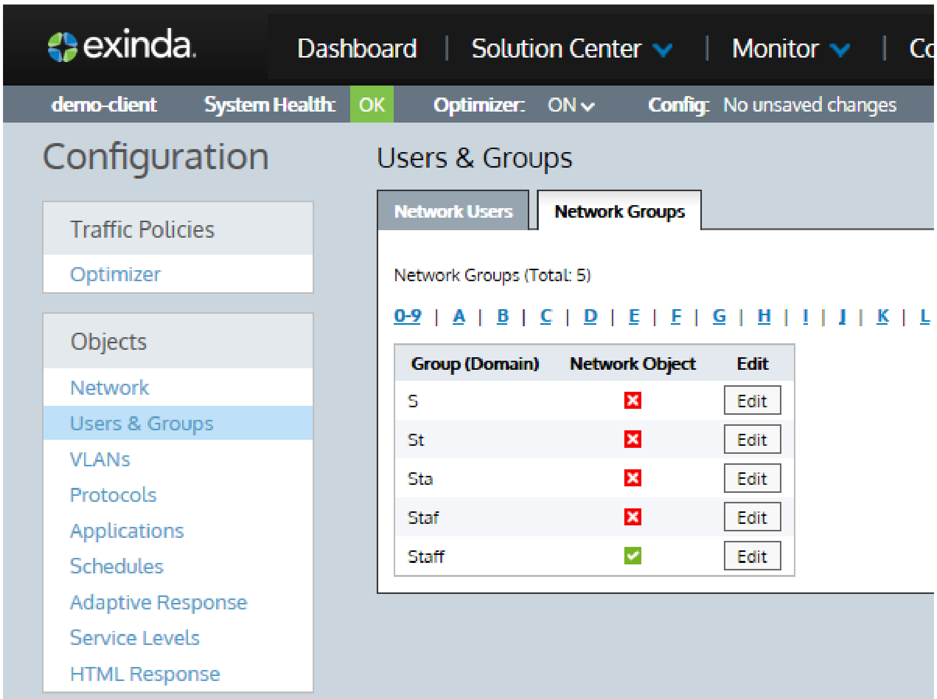
4. Click **Apply**.
5. Request updated user and group information from the Active Directory server.
6. Restart the Active Directory service.

Use Adaptive Response with Active Directory

In the last example, a static Network Object was used as the source of IPs. It is also possible to use a Dynamic Network Object mapped from an Active Directory group as a source.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

5. Click **Configuration > Objects> Users & Groups**.
6. Click **Edit** to edit the required user group.



demo-client System Health: OK Optimizer: ON Config: No unsaved changes

Users & Groups

Network Groups (Total: 5)

Group (Domain)	Network Object	Edit
S	☒	Edit
St	☒	Edit
Sta	☒	Edit
Staf	☒	Edit
Staff	✓	Edit

7. Check **Map to Network Object** and **Ignore Domain** options.

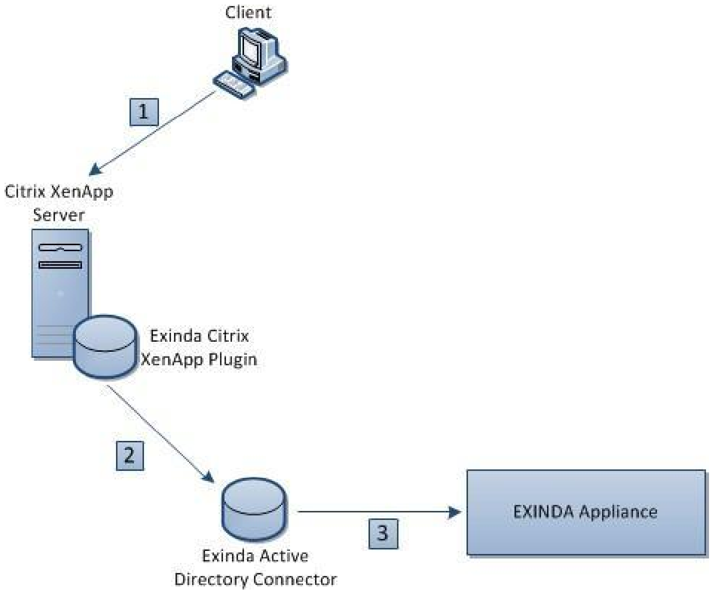
8. Click **Apply**.

A Network Object named similar to the user group name is created that contains all IPs in the Active Directory 'Student' group. This Network Object can be used when creating an Adaptive Response rule exactly as for the previous example.

Identifying users

A Citrix XenApp server hosts a virtual desktop with pre-installed software that users with the correct credentials can access as needed. This allows the company to provide access to commonly used software without having to maintain and upgrade installations on each client computer in the network.

Because the Citrix XenApp server is treated as a single IP address by the GFI ClearView appliance, and the IP address of the clients connecting to the server are ignored, the GFI ClearView Appliance cannot include the names of users who are accessing the applications on the XenApp server.


Client
1
Citrix XenApp Server
Exinda Citrix XenApp Plugin
2
Exinda Active Directory Connector
3
EXINDA Appliance

When a user on a client computer logs into a Citrix XenApp server (1), their IP address and user name are captured by the GFI ClearView Citrix XenApp Plugin and sent on to the GFI ClearView AD Connector (2). The connector then sends the user name and IP address of the XenApp user to the GFI ClearView Appliance to include in reports (3).

Install and configure the GFI ClearView Citrix XenApp Plugin to identify activity by specific users on the XenApp server.

Install the GFI ClearView Citrix XenApp Plugin

The GFI ClearView Citrix XenApp Plugin sends the IP address and username of the user using the application on the XenApp server to the GFI ClearView AD Connector so the user names can be displayed in reports on the GFI ClearView Appliances. The GFI ClearView Citrix XenApp Plugin must be installed on each Citrix XenApp server in the network.

> **NOTE**
> The GFI ClearView Citrix XenApp Plugin is supported on Citrix XenApp Servers version 6.0.

1. Download the installer the GFI ClearView Appliance.
    a. Click **Configuration > System > Network**, and switch to the **Active Directory** tab.
    b. Download the **Microsoft Installer Executable**.
2. Save the GFI ClearView Citrix XenApp Plugin install to a location that can be accessed by the Citrix XenApp server.
3. On the server where the GFI ClearView Citrix XenApp Plugin should be installed, locate and double-click installation file.
4. At the Welcome dialog, click **Next**.
5. Specify the directory where the GFI ClearView Citrix XenApp Plugin should be installed and click **Next**.
6. Read the End-User License Agreement. Select **I Agree** and click **Next**.
7. To confirm the installation, click **Next**. The GFI ClearView Citrix XenApp Plugin is installed.
8. When the installation is completed, click **Close**.

Add the GFI ClearView AD Connector to the GFI ClearView Citrix XenApp Plugin

To ensure that user activity on the Citrix XenApp server is reported on the GFI ClearView appliance, add the connection details for the GFI ClearView AD Connector to the GFI ClearView Citrix XenApp Plugin.

1. Open the GFI ClearView Citrix XenApp Plugin.
2. Select the **Synchronization** tab and double-click in the **Location** area of the first blank line.
3. Type the IP address or hostname and port number of the computer where the GFI ClearView AD Connector is installed.

> **NOTE**
> The port number used to communicate between the GFI ClearView AD Connector and the GFI ClearView Citrix XenApp Plugin cannot be the same as the port number used to communicate between the GFI ClearView AD Connector and the GFI ClearView Appliances.

4. In the **Sync Interval** field, define how frequently the GFI ClearView AD Connector sends

XenApp server user information to the GFI ClearView AD Connector. The default is 1 minute.

5. Click **Apply**.

Capture the GFI ClearView Citrix XenApp Plugin Activity in a Log File

Depending on the logging level selected, the GFI ClearView Citrix XenApp Plugin records various types of data in a log file. The available log levels include Error, Warning, Info, and Verbose. By default, the log sensitivity is Warning. The location of the log file and the level of detail recorded in the log file are configurable.

1. Open the GFI ClearView Citrix XenApp Plugin.
2. On the **ADServer** tab, specify the location where log files should be stored.
3. Switch to the **Console** tab and select the level of messages that are recorded in the log file from the **Log Sensitivity**
list.
4. Click **Apply**.
5. To view the contents of the log, on the **Console** tab click **Open Log**.

Change the GFI ClearView Citrix XenApp Plugin Port Number

Identify the port on which the GFI ClearView AD Connector is communicating to the connected GFI ClearView Citrix XenApp Plugins. The default port number is 8016.

Step 1: Change the port number on the GFI ClearView Citrix XenApp Plugin.

1. From the **Start** menu click **All Programs> ClearView Networks > ClearView Citrix XenApp Plugin Configuration**.
2. Switch to the **Synchronization** tab.
3. Double-click the port number for the appropriate GFI ClearView AD Connector and type the new port number in the field.
4. Click **OK**.

Step 2: Change the port number on the GFI ClearView AD Connector.

1. From the **Start** menu click **All Programs> ClearView Networks > ClearView ADConfiguration Utility**.
2. Switch to the **XenApp** tab.
3. Type the port number in the field.
4. Click **OK**.

Request Updated User Information from the GFI ClearView Citrix XenApp Plugin

If the synchronizations of the user data between the GFI ClearView Citrix XenApp Plugin and the GFI ClearView AD Connector are infrequent, trigger the GFI ClearView Citrix XenApp Plugin to send the data to the GFI ClearView AD Connector immediately.

1. From the **Start** menu, click **All Programs> ClearView Networks > ClearView ADConfiguration Utility**.
2. Switch to the **XenApp** tab.
3. Click **Renumerate**.

The latest data is sent from the GFI ClearView Citrix XenApp Plugin to the GFI ClearView AD Connector.

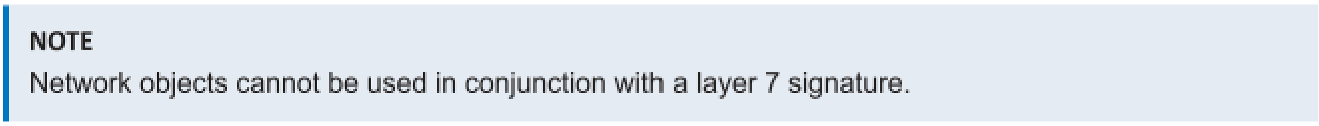
Adding a new application

Use the following instruction to add a new application.

1. Click Configuration > Objects> Applications> Applications.
2. In the **Add New Application** area, type a name for the new application.

   Define an application to be based on one of the following:

   - L7 signature
   - L7 signature + ports or protocols
   - Network object + ports or protocols
   - Network object
   - Ports or protocols

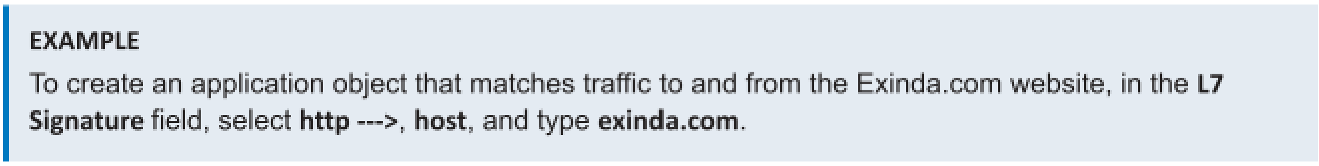


NOTE

Network objects cannot be used in conjunction with a layer 7 signature.

3. Select the **Network Object** for the application. If the network object is internal, then traffic inbound to the LAN with the network object as a destination will be matched to this application, and traffic outbound from the LAN with the net- work object as the source will be matched to this application. If the network object is external, then traffic inbound to the LAN with the network object as a source will be matched to this application, and traffic outbound from the LAN with the network object as the destination will be matched to this application.

4. Select the **L7 Signature** for the application. Some layer 7 signatures have additional options that allow you to define application objects based on specific parts of that L7 signature. If a layer 7 signature is selected, specify the parameters for the signature.



EXAMPLE

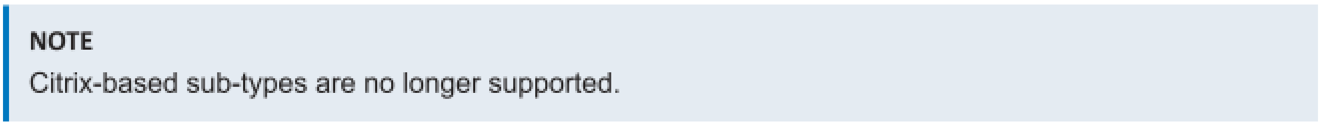
To create an application object that matches traffic to and from the Exinda.com website, in the **L7 Signature** field, select **http --->**, **host**, and type **exinda.com**.

5. In the **Ports/Protocols** controls, specify either TCP ports/port ranges, UDP ports/port ranges, or a layer 3 protocol. Mul- tiple ports and port ranges can be specified at the same time by comma separating values.

6. Click the **Add New Application** button.

What L7 signature options are there?

Some Layer 7 signatures have additional options that allow you to define application objects based on specific parts of that L7 Signature. When configuring a new application object, the L7 signatures followed by '--->' in the drop-down list have additional options. Most provide options that you simply select from. Some require a selection plus additional information. The following table explains the various options that require more than simply picking an option.



NOTE

Citrix-based sub-types are no longer supported.

Layer 7 Signature	Sub-Type	Description
(direct	host	Allows you to define an Application Object based on the 'host' field in the
flash	host	Allows you to define an Application Object based on the 'host' field in the HTTP header (where flash is running over http).

<table>
<tr><th>Layer 7 Signature</th><th>Sub-Type</th><th>Description</th></tr>
<tr><td>http</td><td>content_type</td><td>Allows you to define an Application Object based on the 'content-type' field in the HTTP header.</td></tr>
<tr><td></td><td>file</td><td>Allows you to define an Application Object based on the filename requested in the HTTP URL.</td></tr>
<tr><td></td><td>host</td><td>Allows you to define an Application Object based on the 'host' field in the HTTP header.</td></tr>
<tr><td></td><td>method</td><td>Allows you to define an Application Object based on the HTTP method (e.g. GET PUT HEAD DELETE).</td></tr>
<tr><td></td><td>user_agent</td><td>Allows you to define an Application Object based on the 'user-agent' field in the HTTP header.</td></tr>
<tr><td></td><td>advanced</td><td>Define custom criteria with the following syntax:
» A string literal is enclosed in quotes (").
» A backslash can be included in the string by escaping it with another backslash (\\).
» Keywords are bare (common_name) with no quotes.
» Keywords are bare (host) with no quotes.
» Grouping is supporting using parenthesis
» Operators supported are or and andand has higher precedence than or
» The comparison operators that are available are:
<table>
<tr><th>Description</th><th>Syntax</th><th>Example</th></tr>
<tr><td>equals</td><td><keyword> = <value></td><td>host = "example.com"</td></tr>
<tr><td>does not equal</td><td><keyword> != <value></td><td>host != "example.com"</td></tr>
<tr><td>contains substring</td><td><keyword> =% <value></td><td>host =% "example.com"</td></tr>
<tr><td>does not contain substring</td><td><keyword> !% <value></td><td>host !% "example.com"</td></tr>
<tr><td>Right side is a regular expression and it matches the full left side</td><td><keyword> =~ <value></td><td>host =~ "example.*"</td></tr>
<tr><td>Right side is a regular expression and it does not match the full left side</td><td><keyword> !~ <value></td><td>host !~ "example.*"</td></tr>
</table>
» Regular expressions use the perl syntax
» The keywords for HTTP are: host, file, user_agent, content_type, method, content_len and encoding

Examples:
» (url =% "index" or file =% "login") and host =% "example.org" and content_type.case = "MyContentType"
» (host =% "facebook.com" and file !% "cgi-bin/abcd") or host =% "facebook2.com"</td></tr>
</table>

<table>
<tr><th>Layer 7 Signature</th><th>Sub-Type</th><th>Description</th></tr>
<tr><td>mpeg</td><td>host</td><td>Allows you to define an Application Object based on the 'host' field in the HTTP header (where mpeg is running over http).</td></tr>
<tr><td>quicktime</td><td>host</td><td>Allows you to define an Application Object based on the 'host' field in the HTTP header (where quicktime is running over http).</td></tr>
<tr><td>silverlight</td><td>host</td><td>Allows you to define an Application Object based on the 'host' field in the HTTP header (where silverlight is running over http).</td></tr>
<tr><td>ssl</td><td>common_ name</td><td>Allows you to define an Application Object based on the 'common name' field in the SSL certificate.</td></tr>
<tr><td></td><td>advanced</td><td>Define custom criteria with the following syntax:
» A string literal is enclosed in quotes (").
» Internal quotes can be escaped with the backslash (\") character.
» A backslash can be included in the string by escaping it with another backslash (\\).
» Keywords are bare (common_name) with no quotes.
» Grouping is supporting using parenthesis
» Operators supported are OR and AND. AND has higher precedence than OR.
» The keywords for SSL are common_name (cn) and organization_name (o)
» The comparison operators that are available are:
<table>
<tr><th>Description</th><th>Syntax</th><th>Example</th></tr>
<tr><td>equals</td><td><keyword> = <value></td><td>common_name = "John"</td></tr>
<tr><td>does not equal</td><td><keyword> != <value></td><td>common_name != "John"</td></tr>
<tr><td>contains substring</td><td><keyword> =% <value></td><td>common_name =% "John"</td></tr>
<tr><td>does not contain substring</td><td><keyword> !% <value></td><td>common_name !% "John"</td></tr>
<tr><td>Right side is a regular expression and it matches the full left side</td><td><keyword> =~ <value></td><td>common_name =~ "John*"</td></tr>
<tr><td>Right side is a regular expression and it does not match the full left side</td><td><keyword> !~ <value></td><td>common_name !~ "John*"</td></tr>
</table>
» Regular expressions use the perl syntax</td></tr>
<tr><td></td><td>organization_ name</td><td>Allows you to define an Application Object based on the 'organization' name field in the SSL certificate.</td></tr>
<tr><td></td><td>spdy</td><td>This field should remain empty as any values typed here are ignored.</td></tr>
<tr><td>rtp</td><td>codec</td><td>Allows you to define an Application Object based on the 'codec' used in a RTP stream.</td></tr>
<tr><td>windowsmedia</td><td>host</td><td>Allows you to define an Application Object based on the 'host' field in the HTTP header (where windowsmedia is running over http).</td></tr>
</table>

Example: How to create a custom application based on the HTTPS protocol

Get the common name of the (https) SaaS site and create an application using the ssl L7 signature with the common name.

1. Go to the site that you are interested in.
2. In the address bar of most browsers, click on https or the lock symbol.
3. Show the certificate details.
4. Copy the common name shown in the certificate details.
5. Go to Configuration > Objects> Applications.
6. In the **L7 Signature** field, select **'ssl --->'**
7. In the field beside the L7 Signature, select **common name**.
8. Enter the common name of the site that you got from the certificate in the browser.

Top Internal and External Users on the Network

The Network - Users (Internal) and Users (External) reports displays the top users sending traffic through the network.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

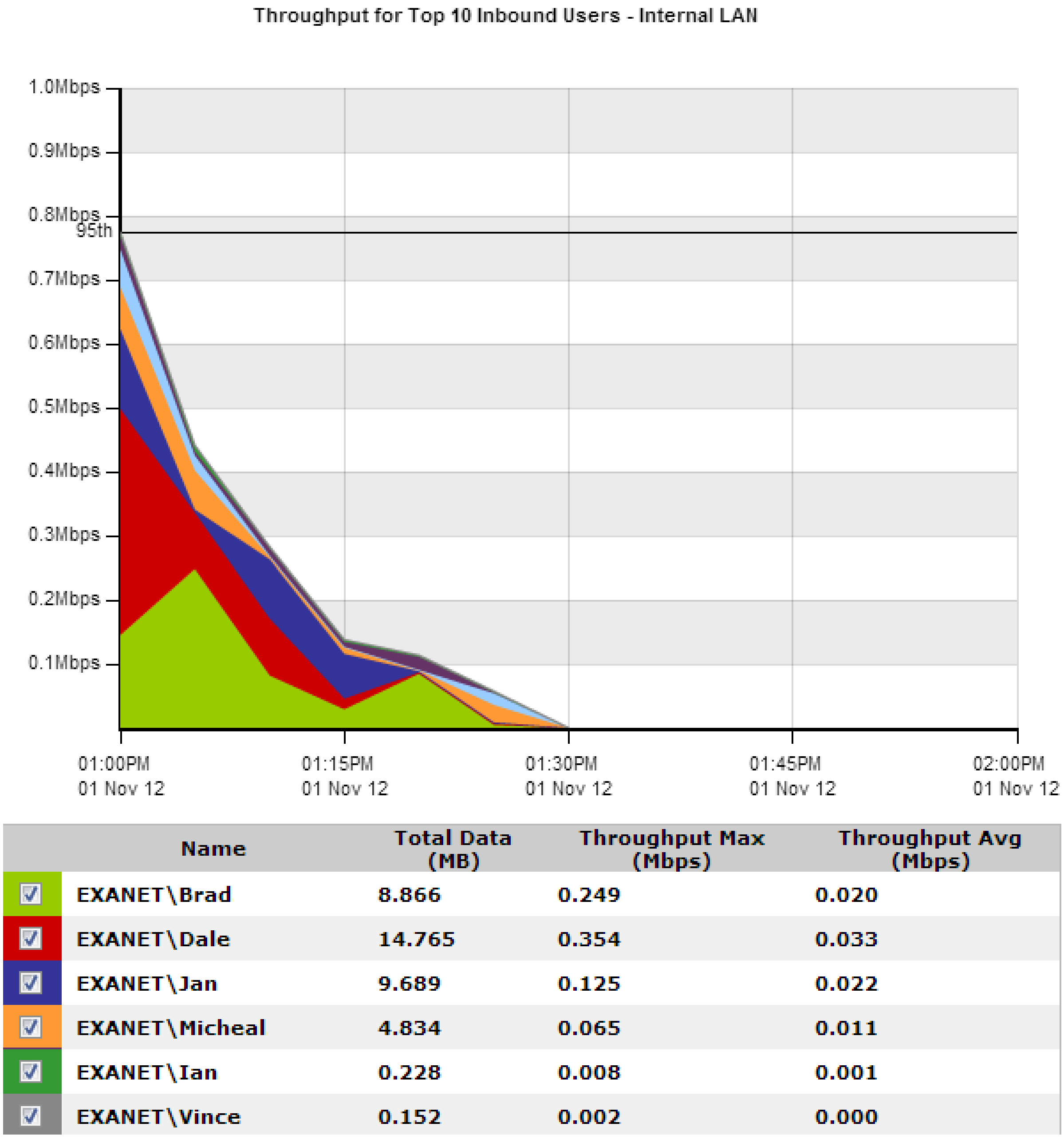
5. Click **Monitor> Network**.
6. In the Select Graph to Display list, select **Users- Internal** or **Users- External**.

7. Set the Time Period Reflected in the Report. For more information, refer to Setting the time period for a report. After the date range is select, the graphs and charts are immediately updated.

8. Remove specific types of traffic from the graph by deselecting their checkbox in the legend below the graph.
9. To determine what the size of your WAN link should be configured to, from the **Select Percentile Marker to Display**

select **95th**.

Use the 95th percentile mark for throughput speed to configure your WAN link.



	Name	Total Data (MB)	Throughput Max (Mbps)	Throughput Avg (Mbps)
🟩 ☑	EXANET\Brad	8.866	0.249	0.020
🟥 ☑	EXANET\Dale	14.765	0.354	0.033
🟦 ☑	EXANET\Jan	9.689	0.125	0.022
🟧 ☑	EXANET\Micheal	4.834	0.065	0.011
🟩 ☑	EXANET\Ian	0.228	0.008	0.001
⬛ ☑	EXANET\Vince	0.152	0.002	0.000

4.2 System Setup

Learn how to set up your GFI ClearView Appliance(s). The configuration information provided focuses on the appliance and not upon the GFI ClearView firmware.

4.2.1 Date and Time Configuration

It is important to accurately set the date and time of your GFI ClearView appliance so that all time-based functions use the appropriate time. It is highly recommended to set the date and time using an NTP server. This is particularly important if you have multiple GFI ClearView appliances where you need to correlate or aggregate the monitoring data or if you need the exported NetFlow records to be synchronized with NetFlow records from other network appliances.

It is recommended to set the date and time using one or more NTP servers. The more NTP servers that are configured, the more accurate the time will be. It is generally accepted that four

NTP servers is the optimal number of servers for extremely accurate time. To explain why four NTP servers is considered an optimal number of servers, see http://www.ntp.org/ntpfaq/NTP-s-algo-real.htm

A great source for NTP servers is the NTP Pool Project at http://www.pool.ntp.org/en/use.html

The date and time setting has implications for the following functions:

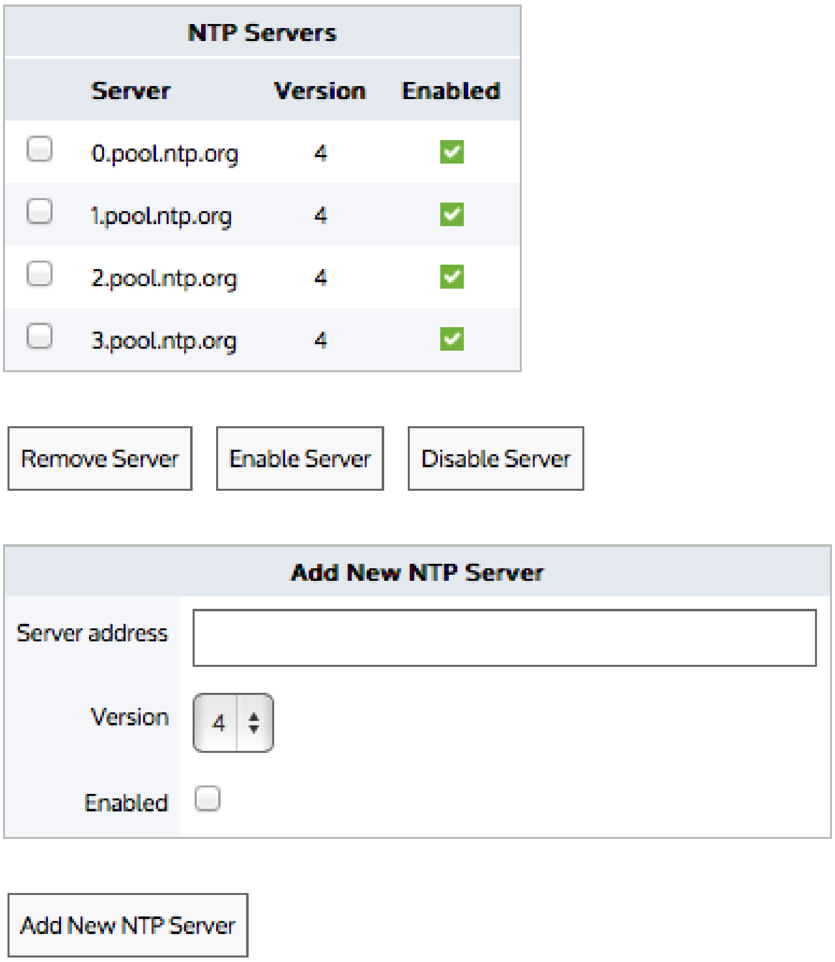
- Monitoring data have time stamps and the monitor charts will be reported relative to these
- time stamps Exported NetFlow records have time stamps
- Schedule-based policies need to take effect at the appropriate times
- Scheduled events, such as scheduled reports or scheduled jobs, need to occur at appropriate times.

Note that when the current time on the appliance is out of sync with the date-time provided by the NTP servers, the NTP servers will slowly adjust the clock time. If the appliance's time is significantly out of sync with the NTP servers (say, 1000 seconds or approximately 15 minutes), then it is recommended that you force the appliance to jump to the correct time using the ntpd command from the command line.

Where do I find this configuration?

Go to **Configuration >System > Setup > Date and Time**.

To set the date & time using an NTP server



NTP Servers

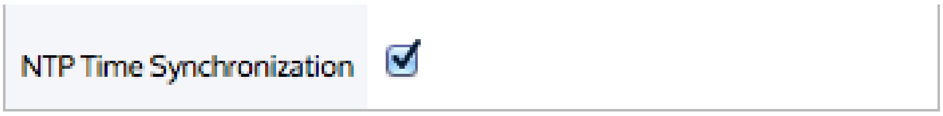
	Server	Version	Enabled
□	0.pool.ntp.org	4	☑
□	1.pool.ntp.org	4	☑
□	2.pool.ntp.org	4	☑
□	3.pool.ntp.org	4	☑

Add New NTP Server

Server address	
Version	4
Enabled	□

1. Add one or more NTP servers by entering the IP address or hostname of the NTP server, the version of NTP supported by the server, and enabling it by checking the enable checkbox in the Add New NTP Server area, Only hostnames and IPv4 addresses are supported.

2. In the Date and Time area, select the **NTPTime Synchronization** checkbox and **Apply Changes**.

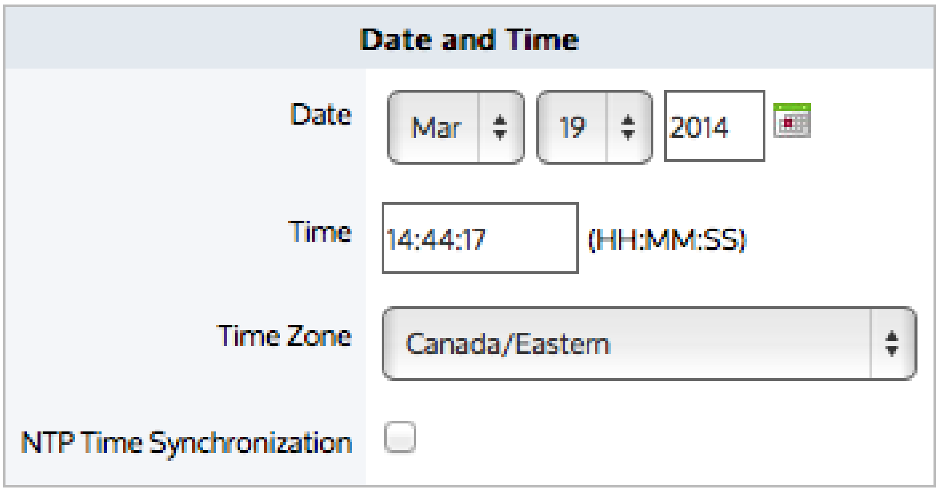


NTP Time Synchronization ☑

The change is applied only if you accept the Restart Message to restart the UI.

Any of the NTP servers can be disabled, re-enabled, or removed by clicking the appropriate button - **Disable Server**, **Enable Server**, **Remove Server**.

To set the date & time manually



Date and Time

Date	Mar 19 2014
Time	14:44:17 (HH:MM:SS)
Time Zone	Canada/Eastern
NTP Time Synchronization	□

1. In the Date and Time area, ensure that the **NTPTime Synchronization** checkbox is not checked.

2. Set the desired date, time, and timezone and click **Apply Changes**.

> **WARNING**
>
> If you change the time manually, you will be prompted to restart the UI. If you do not accept the Restart, the configuration change is not applied. If the NTP Time Synchronization checkbox is checked, then the manual date-time setting will not be applied.

To force a time reset when the time is significantly out of sync

On the command line, type: `ntpd <ntp-server-address>`

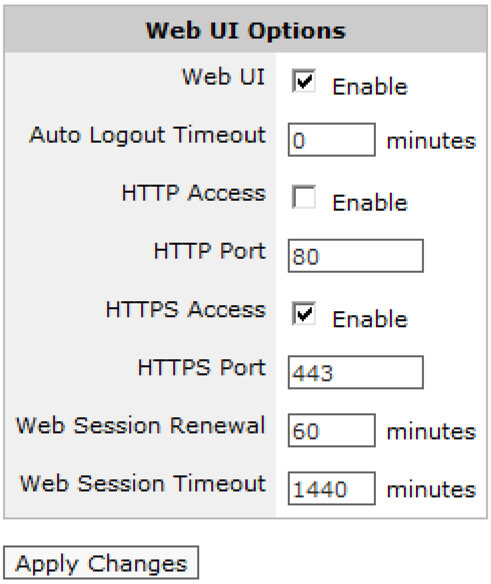
- `<ntp-server-address>` - The location of an NTP server specified as hostname or IPv4/IPv6 address.

This command is similar to the deprecated `ntpdate` command.

4.2.2 UI Access Configuration

The Access page allows you to specify how long the appliance web user interface can be idle before the user is automatically logged out. Similarly you can specify how long the CLI can be idle before being logged out. You can specify whether to enable http or https access and which port numbers to use. If desired, you can also choose to disable the web UI altogether. You can specify whether CLI access is through telnet or SSH.

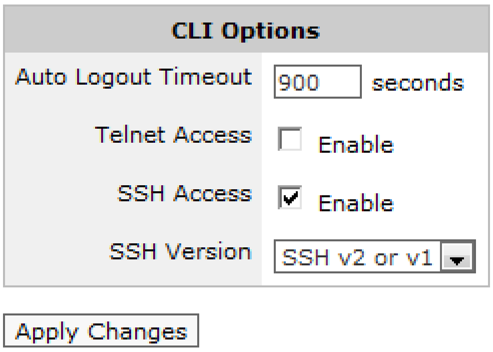
> **NOTE**
> Once you disable the Web UI, you can only re-enable it via the CLI.



Web UI Options

Web UI	☑ Enable
Auto Logout Timeout	0 minutes
HTTP Access	□ Enable
HTTP Port	80
HTTPS Access	☑ Enable
HTTPS Port	443
Web Session Renewal	60 minutes
Web Session Timeout	1440 minutes

Screenshot 224: Web UIoptions for setting HTTP or HTTPS access, auto-logout time period, and disabling the Web UI



CLI Options

Auto Logout Timeout	900 seconds
Telnet Access	□ Enable
SSH Access	☑ Enable
SSH Version	SSH v2 or v1

Screenshot 225: CLIoptions for setting Telnet or SSH access, and the auto-logout timeout period

To configure the Web UI to auto-logout after a specified idle period

1. Ensure the **Web UI Enable** checkbox is checked.

2. Set the **Auto Logout Timeout** period to the specified number of minutes that the user can be idle before the user gets automatically logged out. To configure the system to never automatically log out, set the field to **0** minutes. It is not recommended to change the values in the **Web Session Renewal** field or the **Web Session Timeout** field.

3. Click **Apply Changes**.

To enable HTTP or HTTPS web access

1. Ensure the **Web UI Enable** checkbox is checked.
2. To enable HTTP access, check the **HTTPAccess** checkbox and specify the **HTTPPort** number to use. The default port number is 80.
3. To enable HTTPS access, check the **HTTPS Access** checkbox and specify the **HTTPS Port** number to use. The default port number is 443.
4. Click **Apply Changes**.

To disable the Web UI

1. Uncheck the **Web UI Enable** checkbox.
2. Click **Apply Changes**.

To re-enable the Web UI

From the CLI type: `web enable`

To configure CLI to be accessed via Telnet or SSH

1. To enable Telnet access, check the **Telnet Access** checkbox.
2. To enable SSH access, check the **SSH Access** checkbox and select the **SSH Version** to use.
3. Click **Apply Changes**.

To configure CLI to auto-logout after a specified idle period

1. Set the **Auto Logout Timeout** period to the specified number of seconds that the user can be idle before the user gets automatically logged out. To configure the system to never automatically log out, set the field to **0** minutes.
2. Click **Apply Changes**.

4.2.3 Configure SQL Access

The SQL Access feature on an GFI ClearView appliance provides access to the traffic monitoring database from any ODBC compliant application.

In order to use this feature, SQL access needs to be configured on the GFI ClearView appliance, and an ODBC driver needs to be installed and configured on a client. ODBC aware applications running on the client will then be able to query the GFI ClearView appliance's internal monitoring database.

This How to Guide explains how to configure the GFI ClearView appliance to accept remote SQL connections, as well as setting up the ODBC driver on Windows 8 and Windows 10 clients.

Download the ODBC Driver

Download the ODBC driver version that corresponds to your client operating system. Follow the instructions on this site for installing the ODBC driver on your client operating system.

The ODBC driver can be downloaded from:

http://dev.mysql.com/downloads/connector/odbc/

Set Remote SQL Options

To allow the GFI ClearView appliance to accept remote SQL connections from an external ODBC connector, you must configure the settings in **Configuration > System > Setup > SQL Access**.

- **Remote SQL:** Select this option to allow the GFI ClearView appliance to accept remote SQL connections from external ODBC connectors.

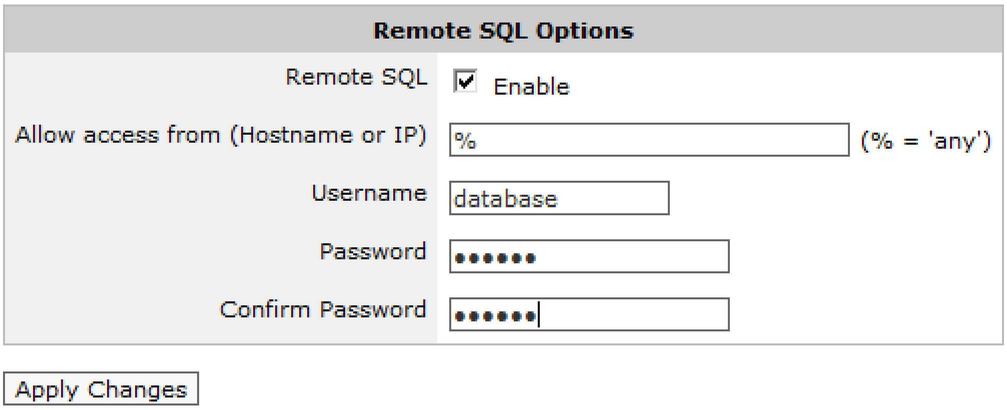
- **Allow access from (Hostname or IP):** Use this option to restrict the hosts that can connect to the SQL database. Spe- cify '%' to allow any hosts to connect or type an IP address or Hostname of a specified host to restrict access.

- **Username:** Specify a username to use for authentication (E.g. 'database').

- **Password:** Specify a password to use for authentication.

- **Confirm Password:** Retype the password specified above.

Apply the changes. The SQL access will be made available immediately. A successfully configured appliance would look something like:

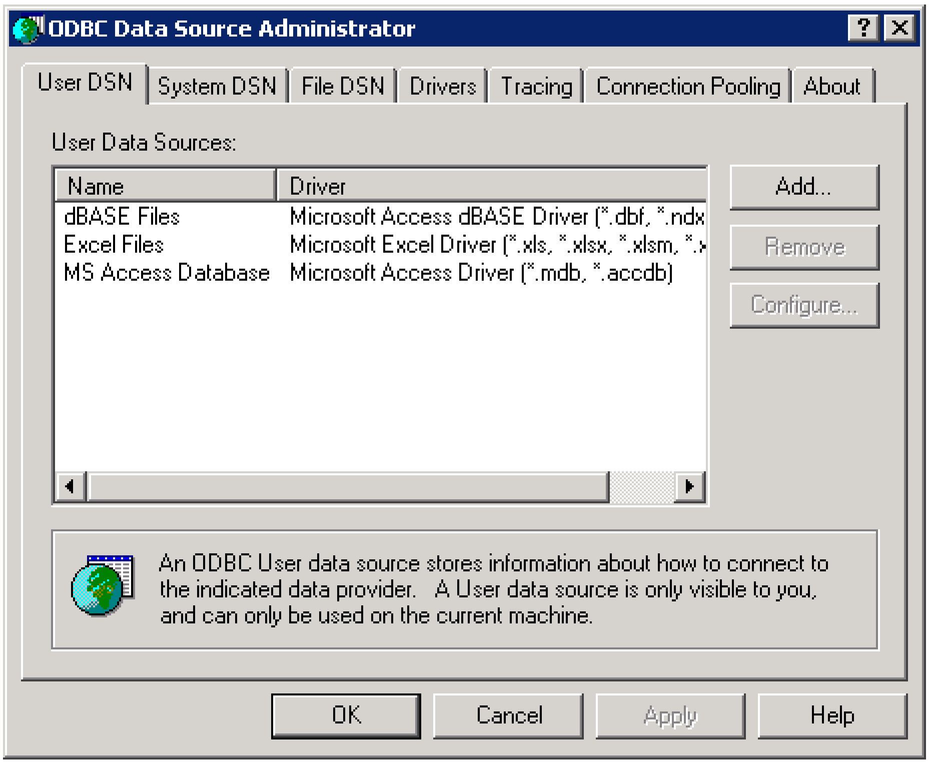


Remote SQL Options

Remote SQL	☑ Enable
Allow access from (Hostname or IP)	% (% = 'any')
Username	database
Password	••••••
Confirm Password	••••••

Once remote SQL access has been configured on the GFI ClearView appliance, the next step is to create an ODBC data source on the client.

1. Open **Administrative Tools** and select **Data Sources(ODBC)**. You should be presented with the following dialog.

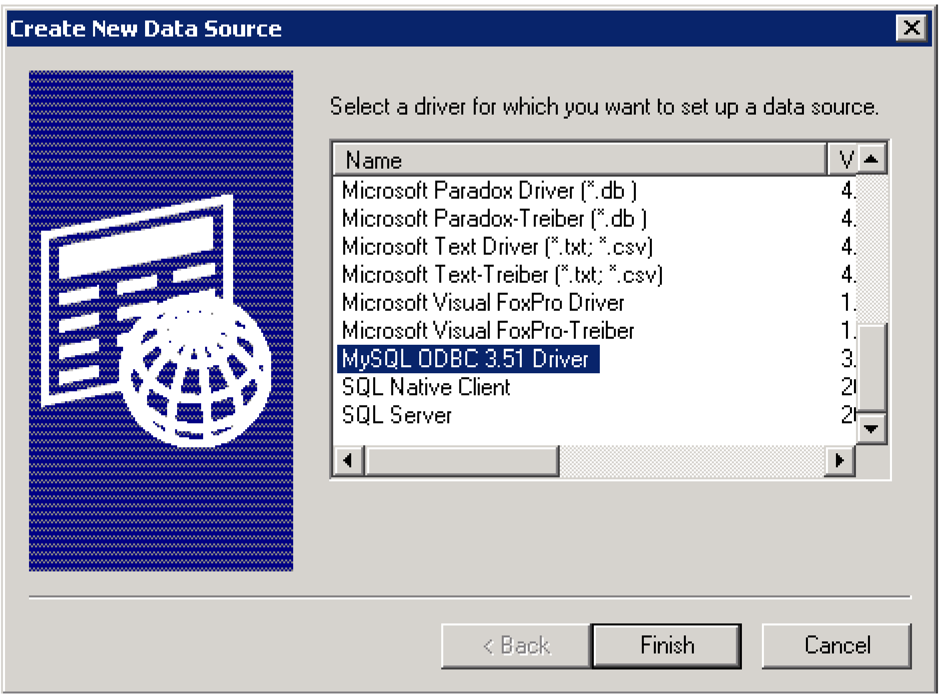


User Data Sources:

Name	Driver
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.x
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)

An ODBC User data source stores information about how to connect to the indicated data provider.   A User data source is only visible to you, and can only be used on the current machine.

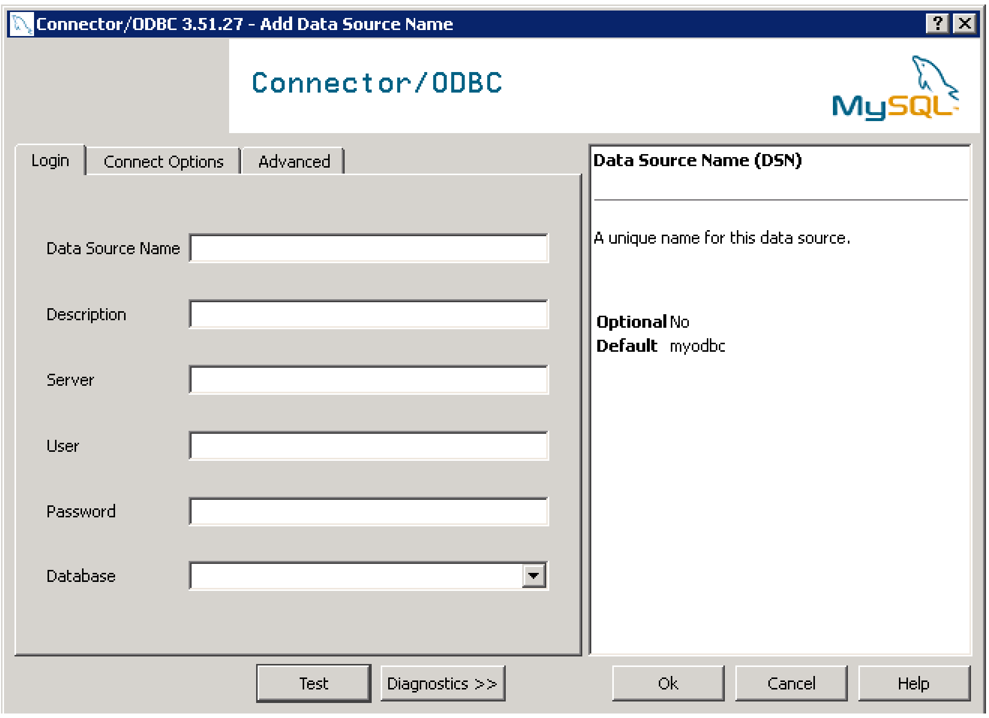
2.	Select the **User DSN** tab or the **System DSN** tab depending on whether you wish the SQL data to be made available to only the current user (User DSN) or all users (System DSN). Then click **Add** This will start a wizard that allows you to create a new data source.



Select a driver for which you want to set up a data source.

Name	V
Microsoft Paradox Driver (*.db)	4.
Microsoft Paradox-Treiber (*.db)	4.
Microsoft Text Driver (*.txt; *.csv)	4.
Microsoft Text-Treiber (*.txt; *.csv)	4.
Microsoft Visual FoxPro Driver	1.
Microsoft Visual FoxPro-Treiber	1.
MySQL ODBC 3.51 Driver	3.
SQL Native Client	2(
SQL Server	2(

3.	Select **MySQL ODBC Driver** and click **Finish**. You will be prompted to enter details about the SQL access using the form below:



Data Source Name

Description

Server

User

Password

Database

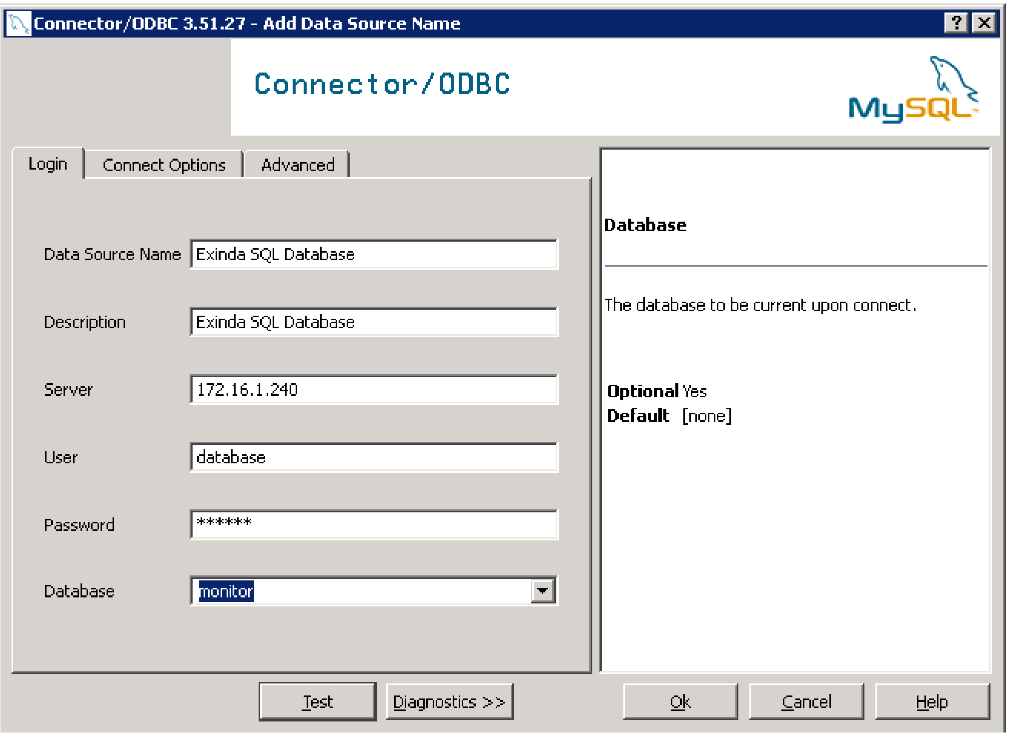
Data Source Name (DSN)

A unique name for this data source.

Optional No
Default myodbc

Data Source Name / Description	Enter a descriptive name for the DSN. E.g. GFI ClearView SQL Database'.
Server	Enter the IP address of the GFI ClearView appliance.
User	Enter the username you specified when enabling SQL access on ClearView appliance.
Password	Enter the password you specified when enabling SQL access on ClearView appliance.
Database	Once the above fields are configured, press the 'Test' button. If the connection attempt is successful, the 'Database' drop down will be populated with a list of available databases. Select 'monitor'.

Here is what a successful configuration looks like:



Data Source Name Exinda SQL Database

Description Exinda SQL Database

Server 172.16.1.240

User database

Password *******

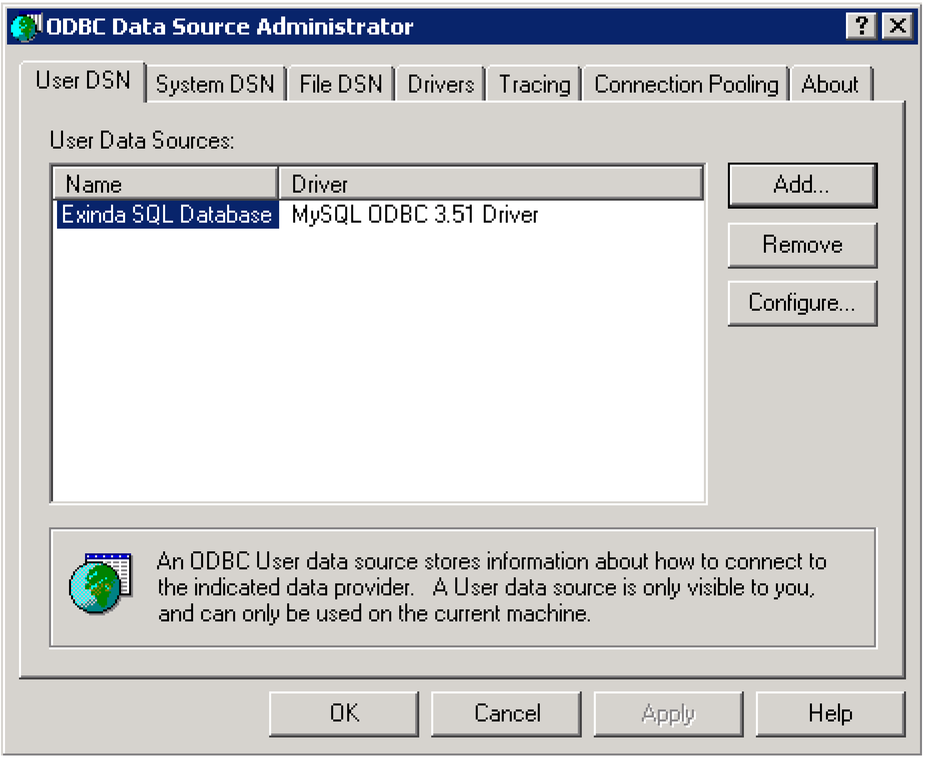
Database monitor

Database

The database to be current upon connect.

Optional Yes
Default [none]

Click **OK**. This will add the GFI ClearView SQL Database' to the list of available data sources that can be used by 3rd party applications on this client.

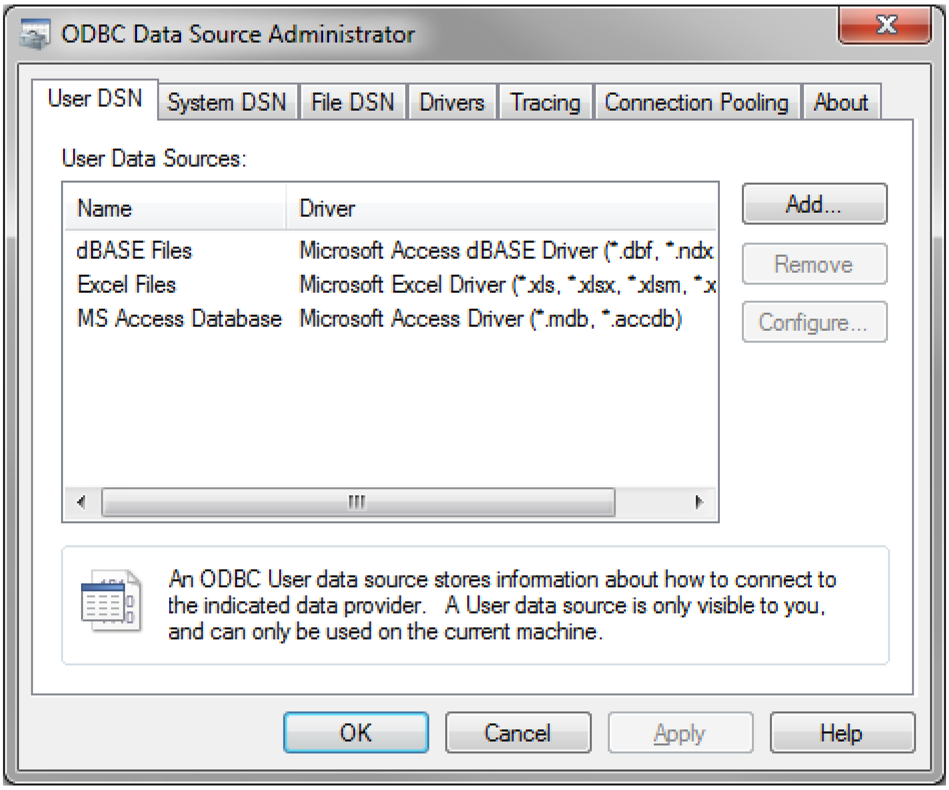


Name	Driver
Exinda SQL Database	MySQL ODBC 3.51 Driver

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

Create ODBC Data Source on Windows 7

Open **Administrative Tools** and select **Data Sources(ODBC)**. You should be presented with the following dialog.

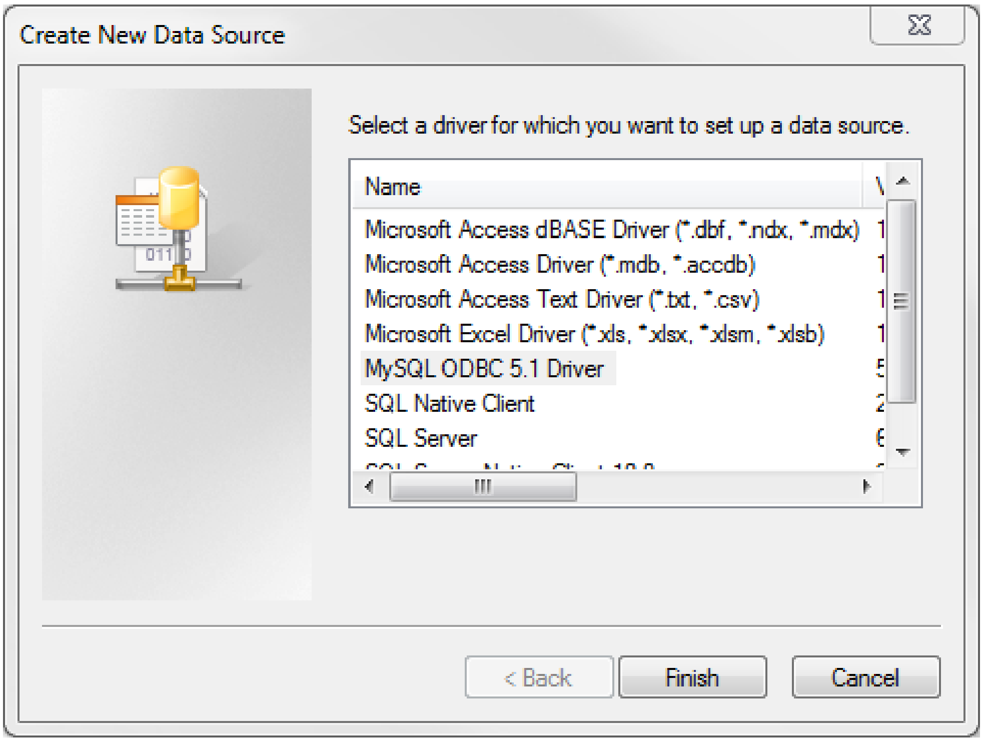


Name	Driver
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.x
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

Select the User DSN tab or the System DSN tab depending on weather you wish the SQL data to be made available to only the current user (User DSN) or all users (System DSN).

Then click **Add.** This will start a wizard that allows you to create a new data source.

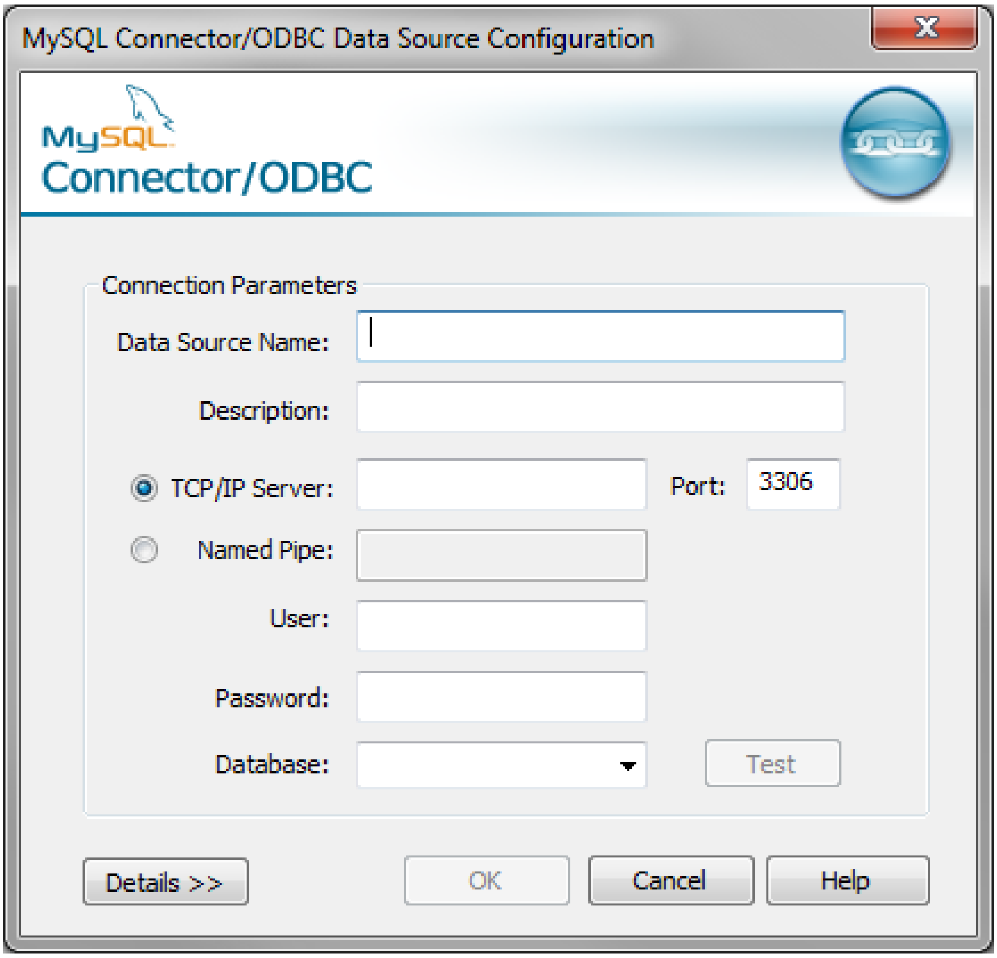


Create New Data Source

Select a driver for which you want to set up a data source.

Name
Microsoft Access dBASE Driver (*.dbf, *.ndx, *.mdx)
Microsoft Access Driver (*.mdb, *.accdb)
Microsoft Access Text Driver (*.txt, *.csv)
Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.xlsb)
MySQL ODBC 5.1 Driver
SQL Native Client
SQL Server

Select **MySQL ODBC Driver** and click **Finish**. You will be prompted to enter details about the SQL access using the form below:



MySQL Connector/ODBC Data Source Configuration

Connection Parameters

Data Source Name:

Description:

● TCP/IP Server: Port: 3306

○ Named Pipe:

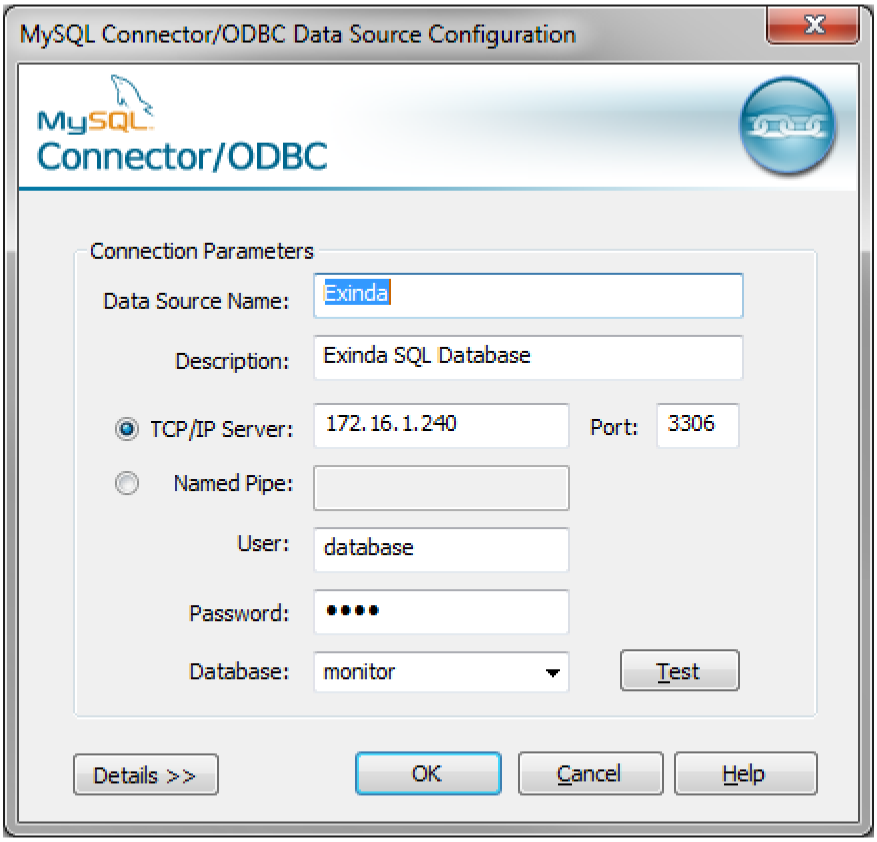
User:

Password:

Database:

Data Source Name / Description	Enter a descriptive name for the DSN. E.g. GFI ClearView SQL Database'.
Server	Enter the IP address of the GFI ClearView appliance.
User	Enter the username you specified when enabling SQL access on the ClearView appliance.
Password	Enter the password you specified when enabling SQL access on the ClearView appliance.
Database	Once the above fields are configured, press the 'Test' button. If the connection attempt is successful, the 'Database' drop down will be populated with a list of available databases. Select 'monitor'.

Here is what a successful configuration looks like:



MySQL Connector/ODBC Data Source Configuration

Connection Parameters

Data Source Name: Exinda

Description: Exinda SQL Database

● TCP/IP Server: 172.16.1.240 Port: 3306

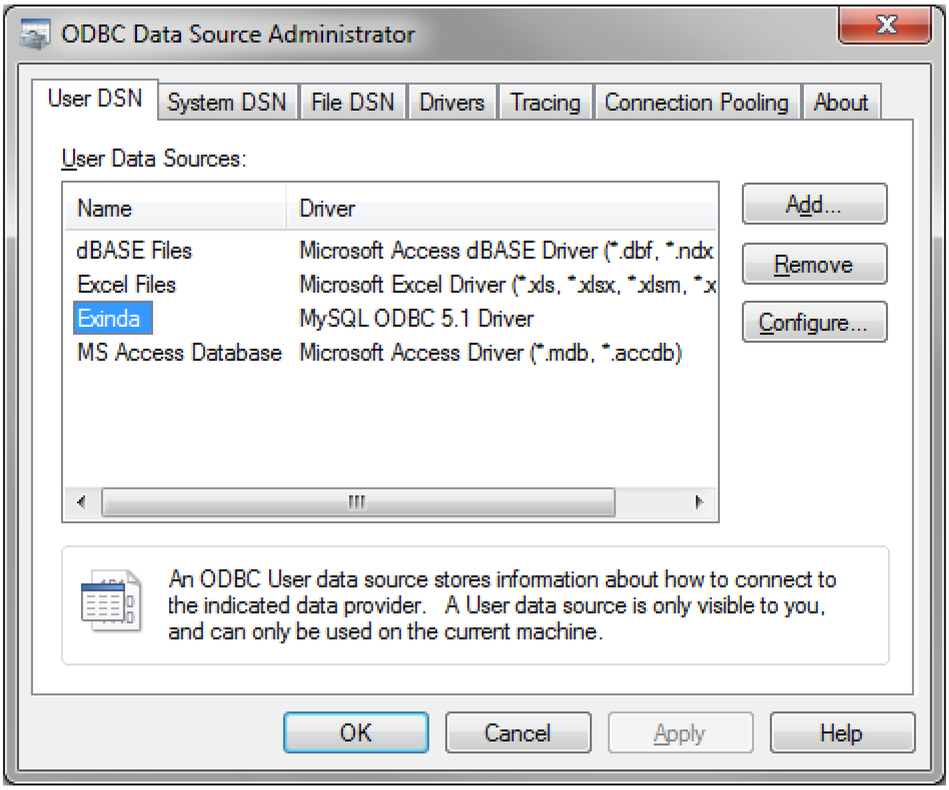
○ Named Pipe:

User: database

Password: ••••

Database: monitor

Click **OK**. This will add the GFI ClearView SQL Database' to the list of available data sources that can be used by 3rd party applications on this client.



User Data Sources:

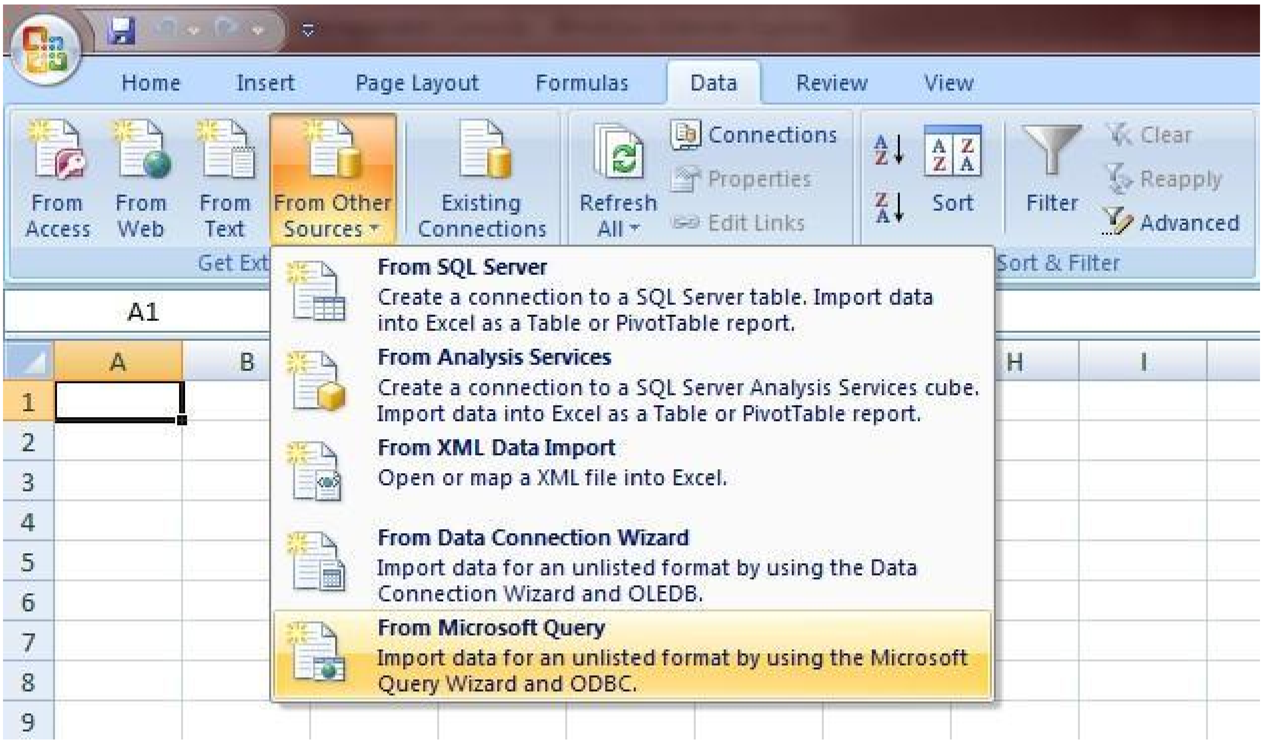
Name	Driver
dBASE Files	Microsoft Access dBASE Driver (*.dbf, *.ndx
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.x
Exinda	MySQL ODBC 5.1 Driver
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

View SQL Access data in Microsoft Excel

You will need a 3rd party application that is capable of accessing data from ODBC data sources. For the purposes of this How to Guide, we will use Microsoft Excel as an example.

From the **Data** tab in Excel, select **From Other Sources> From Microsoft Query**.



From SQL Server
Create a connection to a SQL Server table. Import data into Excel as a Table or PivotTable report.

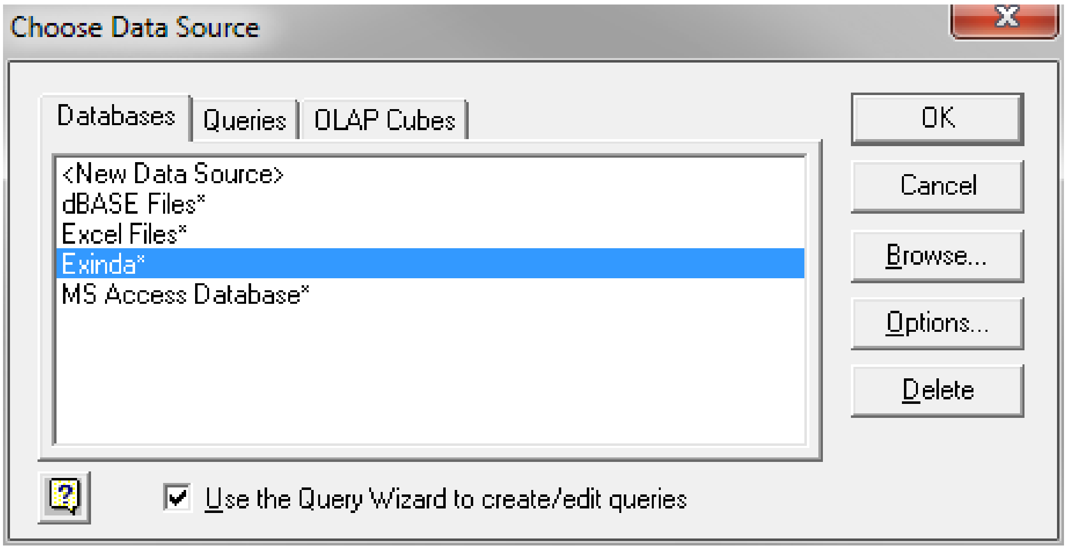
From Analysis Services
Create a connection to a SQL Server Analysis Services cube. Import data into Excel as a Table or PivotTable report.

From XML Data Import
Open or map a XML file into Excel.

From Data Connection Wizard
Import data for an unlisted format by using the Data Connection Wizard and OLEDB.

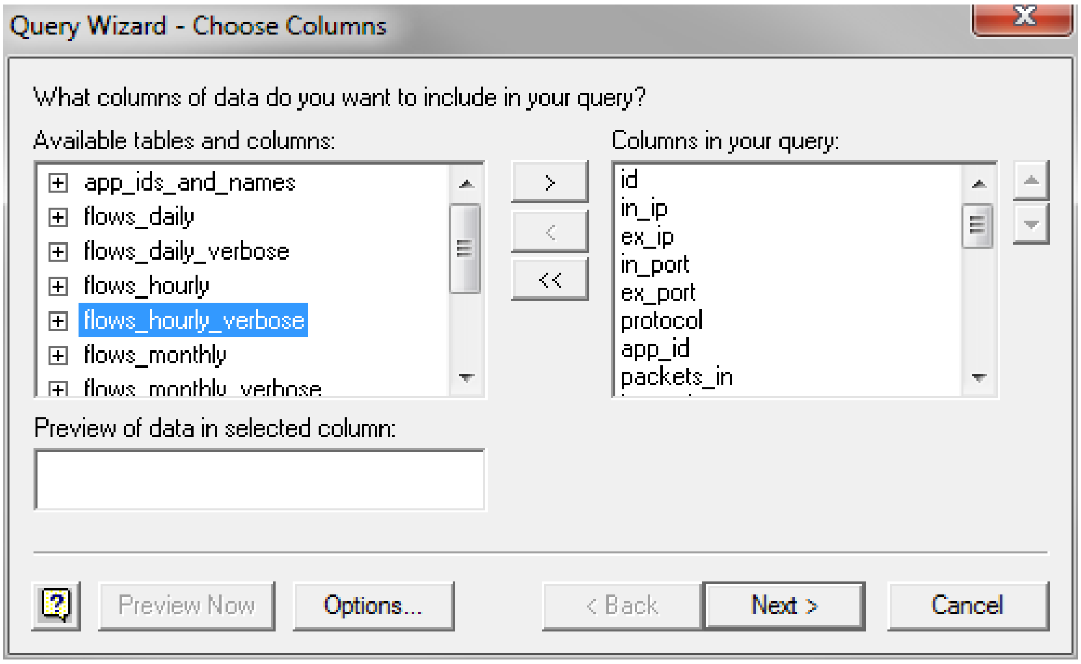
From Microsoft Query
Import data for an unlisted format by using the Microsoft Query Wizard and ODBC.

You will be presented with a dialog box that allows you to select the DSN you created in the previous chapter.

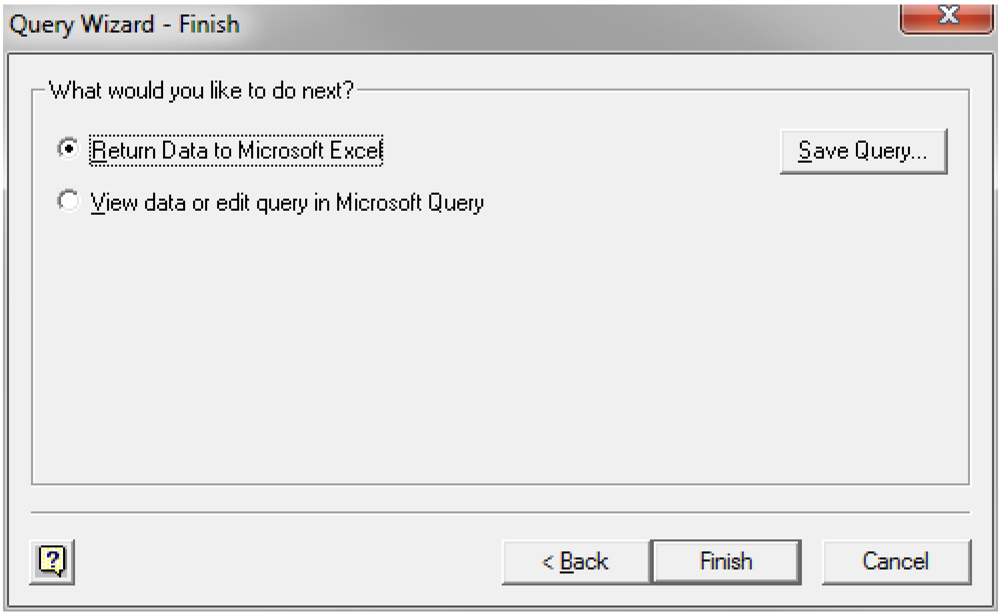


☑ Use the Query Wizard to create/edit queries

Select the **GFI ClearView SQL Database** DSN. This will allow you to choose from the available tables and select the columns to query. Select a table and click the **>** button to move that table's fields into the list of columns to query.



Click through the wizard, optionally specifying columns to filter or sort by. Then click Finish to return the data to Excel.



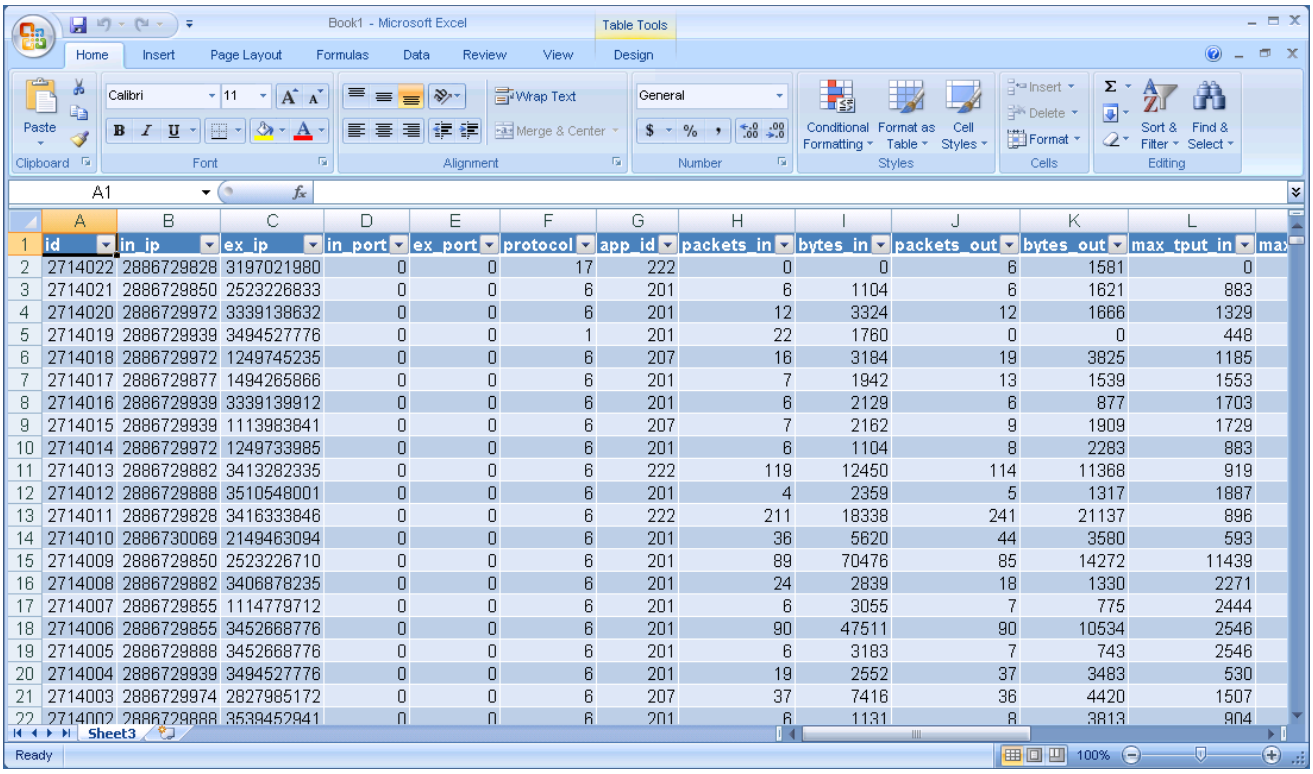
Query Wizard - Finish

What would you like to do next?

● Return Data to Microsoft Excel

○ View data or edit query in Microsoft Query

The GFI ClearView appliance will now be queried and the data will be returned to the Excel spreadsheet.



	id	in_ip	ex_ip	in_port	ex_port	protocol	app_id	packets_in	bytes_in	packets_out	bytes_out	max_tput_in
2	2714022	2886729828	3197021980	0	0	17	222	0	0	6	1581	0
3	2714021	2886729850	2523226833	0	0	6	201	6	1104	6	1621	883
4	2714020	2886729972	3339138632	0	0	6	201	12	3324	12	1666	1329
5	2714019	2886729939	3494527776	0	0	1	201	22	1760	0	0	448
6	2714018	2886729972	1249745235	0	0	6	207	16	3184	19	3825	1185
7	2714017	2886729877	1494265866	0	0	6	201	7	1942	13	1539	1553
8	2714016	2886729939	3339139912	0	0	6	201	6	2129	6	877	1703
9	2714015	2886729939	1113983841	0	0	6	207	7	2162	9	1909	1729
10	2714014	2886729972	1249733985	0	0	6	201	6	1104	8	2283	883
11	2714013	2886729882	3413282335	0	0	6	222	119	12450	114	11368	919
12	2714012	2886729888	3510548001	0	0	6	201	4	2359	5	1317	1887
13	2714011	2886729828	3416333846	0	0	6	222	211	18338	241	21137	896
14	2714010	2886730069	2149463094	0	0	6	201	36	5620	44	3580	593
15	2714009	2886729850	2523226710	0	0	6	201	89	70476	85	14272	11439
16	2714008	2886729882	3406878235	0	0	6	201	24	2839	18	1330	2271
17	2714007	2886729855	1114779712	0	0	6	201	6	3055	7	775	2444
18	2714006	2886729855	3452668776	0	0	6	201	90	47511	90	10534	2546
19	2714005	2886729888	3452668776	0	0	6	201	6	3183	7	743	2546
20	2714004	2886729939	3494527776	0	0	6	201	19	2552	37	3483	530
21	2714003	2886729974	2827985172	0	0	6	207	37	7416	36	4420	1507
22	2714002	2886729888	3539452941	0	0	6	201	6	1131	8	3813	904

SQL Schema

There are a total of 10 tables available for access via SQL.

Name	Description
flows_hourly	Flow records at an hourly resolution, that is, information for each flow is stored hourly, on the hour
flows_daily	Flow records at daily resolution, that is, information for each flow is stored daily, on the day at midnight.
flows_ monthly	Flow records at monthly resolution, that is, information for each flow is stored monthly, on the 1st day of the month at midnight.
urls_hourly	URL records for each flow record that contain 1 or more urls at hourly resolution, that is, information for each url is stored hourly, on the hour.
urls_daily	URL records for each flow record that contain 1 or more urls at daily resolution, that is, information for each url is stored daily, on the day at midnight.
urls_monthly	URL records for each flow record that contain 1 or more urls at monthly resolution, that is, information for each url is stored monthly, on the 1st day of the month at midnight.
app_ids_ and_names	Application records. The record contains a name, id and a flag to indicate if the application has been deleted. Deleted applications are used when labeling historical data.
summary_ applications	Flow records summarized by application. Each record contains information gathered over a 5 minute period.
summary_ hosts_ex	Flow records summarized by external host. Each record contains information gathered over a 5 minute period.
summary_ hosts_in	Flow records summarized by internal host. Each record contains information gathered over a 5 minute period.

flows Table

The following table describes the schema of the flows_* SQL tables.

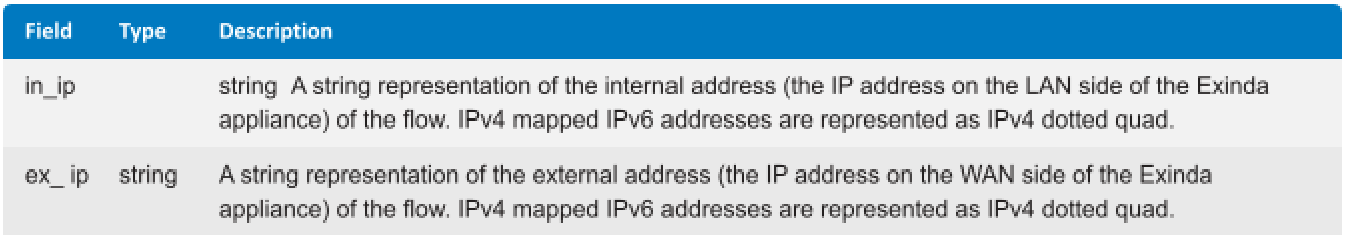
Field	Type	Description
id	unsigned 32-bit integer	A unique id that defines this record. This is the primary key.
in_ip	binary (128 bit)	A 16 byte (128 bit) representation of the internal IPv6 address (the IP address on the LAN side of the GFI ClearView appliance) of the flow. IPv4 addresses are represented as IPv4 mapped formats.
ex_ip	binary (128 bit)	A 16 byte (128 bit) representation of the external IPv6 address (the IP address on the WAN side of the GFI ClearView appliance) of the flow. IPv4 addresses are represented as IPv4 mapped formats.
in_port	unsigned 24-bit integer	The TCP or UDP port number on the internal side (the LAN side of the GFI ClearView appliance) of the flow.1
ex_port	unsigned 24-bit integer	The TCP or UDP port number on the external side (the WAN side of the GFI ClearView appliance) of the flow.1
protocol	unsigned 24-bit integer	The IANA assigned IP protocol number of the flow. See http://www.iana.org/assignments/protocol-numbers/ for more information.
app_id	unsigned 24-bit integer	The internal GFI ClearView Application ID assigned to this flow.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.

Field	Type	Description
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.
packets_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period.
max_tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample period.
intervals_in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period (bps).
intervals_out	unsigned 24-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this flow during the sample period (bps).
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.
in_username	string	A string representation of the username that was assigned to the internal IP of this flow when it was created (if available).
ex_username	string	A string representation of the username that was assigned to the external IP of this flow when it was created (if available).1
rtt	unsigned 32-bit integer	Round Trip Time in milliseconds. A measure if the time a packet takes to leave a device, cross a network and return.2
network_delay	unsigned 32-bit integer	A normalized measure of the time taken for transaction data to traverse the network.2
network_jitter	unsigned 32-bit integer	A normalized measure of the network_delay variability.2
server_delay	unsigned 32-bit integer	A normalized measure of the time taken for a server to respond to a transaction request.2
bytes_lost_in	unsigned 64-bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).2
bytes_lost_out	unsigned 64-bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).2
aps	unsigned 64-bit integer	Application Performance Score. A measure of an applications performance on the network.2

» `in_port` and `ex_port` are only defined when the IP protocol is TCP (6) or UDP (17) and the GFI ClearView was unable to classify the flow (so the app_id is 0).

» For more information, refer to Using Application Performance reports.

The flows_* tables are available as views that represent the binary IPv6 addresses in string format. The views tables are flows_*_verbose (e.g. flows_hourly_verbose). The fields are identical to the above except for the following:



Field	Type	Description
in_ip		string A string representation of the internal address (the IP address on the LAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.
ex_ ip	string	A string representation of the external address (the IP address on the WAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.

app_ids_and_names Table

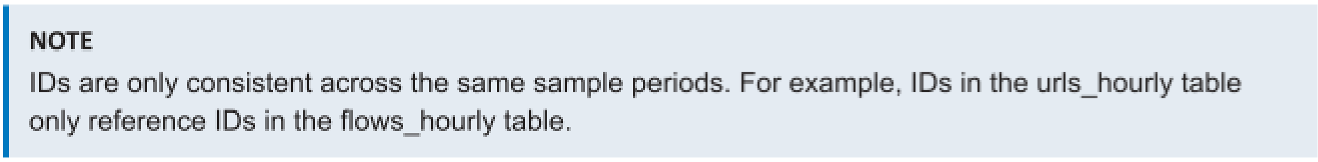
The following table describes the schema of the app_ids_and_names SQL table.

Field	Type	Description
app_id	unsigned 24-bit integer	A unique id that defines the Application. This is the primary key.
app_name	string	The Application name (e.g HTTP, Hotmail)
deleted_ flag	unsigned 8-bit integer	A flag indicating if the Application has been deleted from the appliance (0 = no, 1 = yes)

urls Table

The following table describes the schema of the urls_* SQL tables.

Field	Type	Description
id	unsigned 32-bit integer	This id references an id in the corresponding parent flows_* table. There can be multiple url records referencing the same flow id, so this field is not unique.
url	string	The URL (host) extracted from the HTTP header of the parent flow.
packets_ in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this URL over the sample period.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this URL over the sample period.
packets_ out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this URL over the sample period.
bytes_ out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this URL over the sample period.
max_ tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this URL during the sample period.
max_ tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this URL during the sample period.
intervals_in	unsigned 16-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this URL during the sample period.
intervals_out	unsigned 16-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this URLduring the sample period.



NOTE

IDs are only consistent across the same sample periods. For example, IDs in the urls_hourly table only reference IDs in the flows_hourly table.

summary_applications Table

The summary_application table summarizes the aggregated data from the GFI ClearView. The following table describes the schema of the summary_applications SQL table.

Field	Type	Description
in_port	unsigned 24-bit integer	The TCP or UDP port number on the internal side (the LAN side of the GFI ClearView appliance)1
ex_port	unsigned 24-bit integer	The TCP or UDP port number on the external side (the WAN side of the GFI ClearView appliance)1
protocol	unsigned 24-bit integer	The IANA assigned IP protocol number of the flow. See http://www.iana.org/assignments/protocol- numbers/ for more information.
app_id	unsigned 24-bit integer	The internal GFI ClearView Application ID assigned to this flow. This represents GFI ClearView'S classification of the flow. A zero value should be interpreted as unclassified.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.
packets_ out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
intervals_ in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period.
intervals_ out	unsigned 24-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this flow during the sample period.
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period (bps).
max_tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample period (bps).
rtt	unsigned 32-bit integer	Round Trip Time in milliseconds. A measure of the time a packet takes to leave a device, cross a network and return.2
network_ delay	unsigned 32-bit integer	A normalized measure of the time taken for transaction data to traverse the network.2
network_ jitter	unsigned 32-bit integer	A normalized measure of the network_delay variability.2
server_ delay	unsigned 32-bit integer	A normalized measure of the time taken for a server to respond to a transaction request.2
bytes_ lost_in	unsigned 64-bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).2
bytes_ lost_out	unsigned 64-bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).2

» `in_port` and `ex_port` are only defined when the IP protocol is TCP (6) or UDP (17) and the GFI ClearView was unable to classify the flow (so the app_id is 0).

» For more information, refer to Using Application Performance reports.

summary_hosts Table

The following table describes the schema of the summary_hosts_in and summary_hosts_ex SQL tables. The table fields are identical apart from the ip field - this field represents the IPv4 or IPv6 address of an internal host (summary_hosts_in) or an external host (summary_hosts_ex).

A host is internal if it is on the LAN side of the appliance and external when on the WAN side.

Field	Type	Description
ip	binary string	A string representation of the internal or external IPv4 or IPv6 address of the host.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.
packets_ out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
intervals_in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period (bps).
intervals_ out	unsigned 24-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this flow during the sample period (bps).
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period.
max_tput_	unsigned 64-bit	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample
rtt	unsigned 32- bit integer	Round Trip Time in milliseconds. A measure of the time a packet takes to leave a device, cross a network and return.1
network_ delay	unsigned 32- bit integer	A normalized measure of the time taken for transaction data to traverse the network.1
network_ jitter	unsigned 32- bit integer	A normalized measure of the network_delay variability.1
server_ delay	unsigned 32- bit integer	A normalized measure of the time taken for a server to respond to a transaction request.1
bytes_ lost_in	unsigned 64- bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).1
bytes_ lost_out	unsigned 64- bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).1

For more information, refer to Using Application Performance reports.

4.2.4 Monitoring Configuration

You can configure details relevant to monitoring charts and the monitoring data that is collected. You can configure how the data is displayed, how the traffic is analyzed for monitoring purposes, which order of resolution methods are tried when resolving IP addresses to hostnames, whether data is collected, and whether collected data is deleted.

For configuring how data is to display, you can specify how many items are shown in the data tables, how many items are shown in the pie charts, and how many characters to show in the URLs.

For analyzing traffic, you can specify whether to recognize traffic according to layer 7 or layer 3 definitions, and how sensitive (or aggressive) to be when attempting to recognize BitTorrent, eDonkey, Skype, and flow detection.

For analyzing traffic for specific application types (Application Specific Analysis Modules (ASAM)), you can specify whether to extract data from Citrix, http, and SSL traffic, whether to identify anonymous proxies in the traffic, whether to analyze VoIP traffic, whether to calculate the performance and health of connections, whether to collect connection symmetry information, and whether to log every URL seen in the traffic.

For resolving IP addresses to hostnames, you can specify which methods are tried first, second and so on: network object, DSN, NetBios name lookup, and IP address.

For collection of monitoring data, you can specify whether to collect data for subnets and virtual circuits, and whether to collect detailed records for applications, hosts, URLs, users, conversations and subnets, and whether to collect data for traffic between internal network objects.

For deleting monitoring data, you can selectively delete various types of data collected by the appliance.

To configure monitoring charts display options

Go to **Configuration > System > Setup > Monitoring tab - Monitoring Options** form. The following fields allow you to modify display options.

- **Table Items** - Sets the maximum number of top items displayed in the monitoring tables. Acceptable values are 1- 1000.
- **Chart Items** - Sets the maximum number of top items to be displayed in the chart and graphs. Acceptable values are 1-10. Note that this value will apply universally to ALL options on the Monitor menu.
- **Maximum URL Size** - Sets the maximum length of URLs displayed on the Real Time report tables.
- **Graph Display Options** - Specifies whether the graphs display in Flash or non-Flash format. The default is flash.
- **Display for Application details per subnet** - In a scheduled report, specifies whether the application chart within a subnet displays as a Time series chart (line chart), or as a Pie graph. When this option is selected, the Applications per subnet chart displays in the scheduled report as a line chart whereas all other charts continue to display as a pie graph. The default is Time series chart.
- **Sort Subnetsby Name** - Subnets are sorted by name within scheduled reports if the Enable checkbox is checked; otherwise the subnets are sorted by data volume.

To configure how traffic is monitored

Go to **Configuration > System > Setup > Monitoring** tab - **Monitoring Options** form.

The following fields allow you to specify how sensitive the traffic classification analysis should be.

- **Layer 7 Inspection** - Controls whether to analyze the application signatures within a packet to further classify the traffic within the reports. For example, when analyzing HTTP and FTP traffic and an MPEG file is detected within the packets, the application associated with the connection is changed to MPEG. When disabled, the Layer 7 signatures within packets are not analyzed and any application detection objects with Layer 7 rules are ignored.

- **Monitor IPv6 Link Local Traffic** - Indicates whether to monitor IPv6 link local traffic, that is, non-routable traffic that is only valid on the single network segment. The default is to not monitor this traffic as it is not representative of your net- work user's traffic. It is mostly used for network discovery.

- **OpenVPN Detection** - Indicates the sensitivity for detecting OpenVPN traffic. Setting this to 'aggressive' is the default, however, may result in some false positives. Setting this to 'safe' may result in false negatives.

- **Bittorrent Sensitivity** - Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.

- **EDonkey Sensitivity** - Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.

- **Skype Sensitivity** - Setting this to 'high' is recommended for most service provider environments.

- **Reporting Sensitivity** - Controls the minimum number of packets needed to be seen on a flow before it is recorded in the database. Acceptable values are between 1 and 10, with 10 being the lowest sensitivity. Setting this to a low value is not recommended in high load environments. When the sensitivity is set to a low value such as 9, flows that contain less than nine packets over a five minute period are not stored in the database. This prevents port scans from loading hundreds of unnecessary rows of data into the database.

To enable or disable Application Specific Analysis Modules (ASAM)

Go to **Configuration > System > Setup > Monitoring** tab - **ASAM** form.

The GFI ClearView appliance analyzes traffic and attempts to match it against criteria specific to the traffic type. The criteria for matching traffic is defined within Application Specific Analysis Modules (ASAM). Enable and disable the modules that are important for your network.

The following ASAM modules are available:

- **Anonymous Proxy** - When enabled, the system attempts to use anonymous proxies by matching the HTTP hostname and SSL common name against the list of anonymous proxy URLs downloaded by the appliance daily. Disable this module if it appears that an application is being misclassified as an anonymous proxy.

- **Citrix** - When enabled, the appliance attempts to extract user names and applications names from Citrix connections.

Disable this module to stop the appliance in locations where privacy policy does not permit this type of user iden- tification.

- **DCE/RPC** - When enabled, this module categorizes client requests for Microsoft services such as MAPI and SMB. This should always be enabled.

- **HTTP** - When enabled, this module attempts to further analyze connections identified as HTTP and attempts to extract information such as the host, URL, request type, and content type.

- **Performance Metrics** - When enabled, this module calculates the network delay, server delay, round trip time (RTT), loss, efficiency, and TCP health for TCP connections. Disable this module if the RAM or CPU usage is increasing and affecting the performance of the appliance. For more information refer to RAM Usage Report and CPU Usage Report.

- **SSL** - When enabled, this module extracts public certificates from connections identified as SSL and decodes the information from those certificates (such as common name and organization unit).

- **VoIP** - When enabled, this module extracts VoIP related information such as code type and call quality information (MoS and rFactor scoring) from connections identified as RTP.
- **Asymmetric route** - When enabled, this module collects connection symmetry information. Disable this module if the network regularly has asymmetric routes, as it is unnecessary to alert administrators that asymmetrical connections are occurring.
- **URL Logging** - When enabled, every URL seen by the appliance is logged to the database. Specify how long (in days) the data will be saved. This module is disabled by default.

To control the order of resolution methods tried when resolving IP addresses to hostnames

Go to **Configuration > System > Setup > Monitoring** tab - **Host Resolution Method** form.

There are multiple host resolution methods that can be used to resolve IP addresses to hostnames. The system will attempt to resolve the hostname using one of the methods. If that method fails it will try another method. You can determine the order of host resolution methods that the system will use by ranking the first method as 1, the next as 2, and so on.

The options for host resolution methods are the following:

- **Network Object** - The IP addresses will be resolved according to the configured network objects.
- **DNS** - The IP addresses will be resolved according to the DNS mappings.
- **IPAddress(no resolution)** - The IP addresses will NOT be resolved to hostnames.
- **NetBIOS Name Lookup** - The IP addresses will be resolved to NetBIOS names.

To enable or disable collection of monitoring data

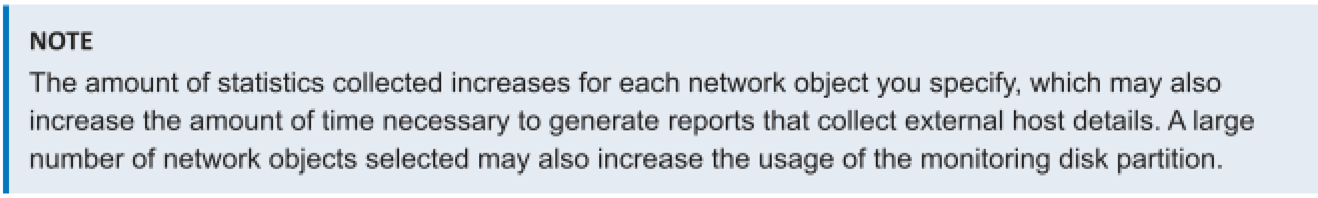
Go to Configuration > System > Setup > Monitoring tab

Various types of data are collected for traffic passing through the network. If the appliance is not performing as expected, data collection can be disabled to improve performance.

The following data collection can be disabled:

- **Subnets**(shown in the **Statistics Collection** form) - If disabled, data is not collected for subnet reporting.
- **Virtual Circuits**(and Applications) (shown in the **Statistics Collection** form) - If disabled, data is not collected for virtual circuit reporting. The collection of global application statistics also will not be collected since the global application statistics are derived from the virtual circuit stats. Note that application reporting within a subnet is not affected by this setting. That is, if data collection is enabled for subnets and is disabled for virtual circuits, then the applications within a subnet will reported, but the applications reported across the entire appliance or within a virtual circuit will not be repor- ted.
- **Internal Hosts**(shown in the **Statistics Collection** form) - If disabled, data is not collected for internal hosts. You can disable this option to control the amount of data collected in situations where you have many hosts and want to ensure you do not run out of storage room. To view the amount of storage space allocated and how much is free, see Allocate Disk Storage for System Services. Ensure you enable this option if you want to monitor or produce reports for internal host data or to display internal host data on the Application Performance screens in the Solution Center.
- **External Hosts For Subnets**(shown in the **Statistics Collection form)** - Specify one or more network objects to col- lect external host data for specific network objects only. In cases where you have created a custom network object related to a specific set of IP Addresses, you can

choose the network object to collect only the required data, rather than extraneous data from all objects.



NOTE

The amount of statistics collected increases for each network object you specify, which may also increase the amount of time necessary to generate reports that collect external host details. A large number of network objects selected may also increase the usage of the monitoring disk partition.

- **Detailed Record Retention**(shown in the **Monitoring Options** form) - Controls whether detailed monitoring records (Applications, Hosts, URLs, Users, Conversations and Subnets) are stored. If there are excessive traffic flows through the appliance, disabling this option will reduce CPU usage. However, the detailed records will no longer be collected and drill down information for Applications, Hosts, Conversations will no longer be available.Summary information, that is totals for the entire appliance, will be available for Applications, Hosts, and Conversations.
- **Ignore Internal-to-Internal**(shown in the **Monitoring Options** form) - Your network may have network objects on the WAN side of the appliance that have been configured as Internal objects, for example a router or firewall. Enabling the Ignore Internal-to-Internal option prevents traffic between internal network objects being included in the reports.

To delete collected monitoring data

Go to **Configuration > System > Setup > Monitoring tab - Clear Monitoring Records** form.
If the appliance is running out of disk space, you can delete collected data.

The following record types can be deleted:

- **All Interface Records** - Deletes all data associated with the Interfaces charts - Interface Throughput and Interface Packets Per Second charts.
- **All Network Summary Records** - Deletes all data associated with the Network Summary charts.
- **All Control/Policy Records** - Deletes all data associated with the Control charts - Policies, Discard, and Prioritization Ratio charts.
- **All Optimization Records** - Deletes all data associated with the Optimization charts - Reduction and Edge Cache charts.
- **All SLA Records** - Deletes all data associated with Network Response (SLA) chart.
- **All APS Records** - Deletes all data associated with Application Performance Score (APS) summary chart.
- **All APM Records** - Deletes all data associated with Application Performance Metric (APM) charts, which are the detailed metric charts for the APS monitor.
- **All Detailed Monitor Records** - Deletes all detailed data, that is, deletes all the drill down data for applications, hosts, URLs, users, conversations. Summary information, that is, the totals for the entire appliance will still be available.

- **All Appliance Records** - Deletes all data associated with the system charts - Connections, Accelerated Connections, CPU Usage, CPU Temperature, RAM Usage, Disk IO, and Swap Usage charts.
- **All Subnet Records** - Deletes all data associated with subnet charts.

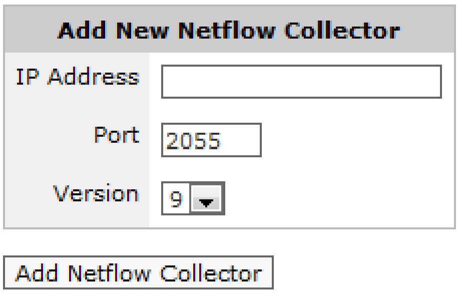
All check boxes can be selected by clicking in the checkbox in the header area.

> **CAUTION**
> This will permanently delete the selected records from the monitoring database.

4.2.5 Netflow Configuration

Netflow allows the GFI ClearView appliance to export flow records to 3rd party monitoring devices.

1. Use the form below to configure these Netflow targets.



Add New Netflow Collector

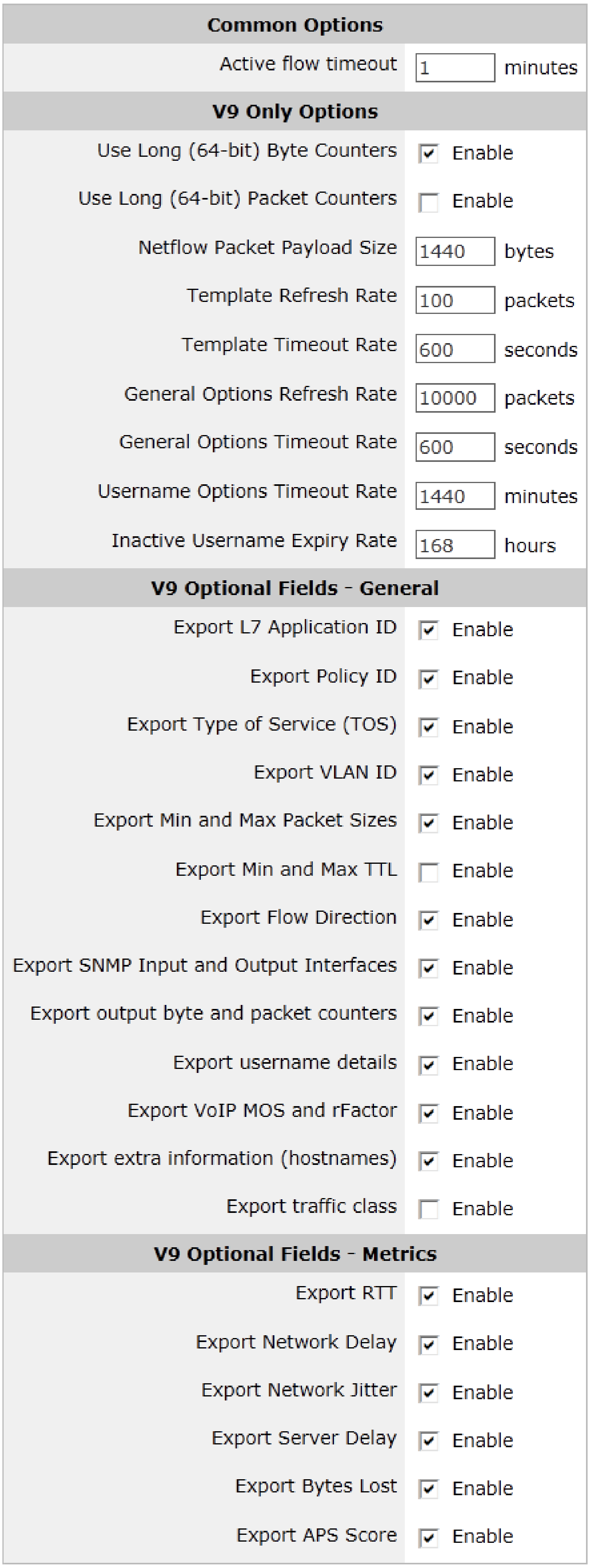
IP Address:

Port: 2055

Version: 9

Property	Description
IP Address	Specify the IP Address of the Netflow target. The GFI ClearView appliance will export Netflow data to this IP Address.
Port	Specify the Port number of the Netflow target. The GFI ClearView appliance currently supports Netflow export on UDP ports.
Version	Specify the Netflow version to export. Current supported versions are v1, v5 and v9.

2. The form below allows customization of the flow records sent by Netflow.



Common Options

Active flow timeout	1 minutes

V9 Only Options

Use Long (64-bit) Byte Counters	☑ Enable
Use Long (64-bit) Packet Counters	□ Enable
Netflow Packet Payload Size	1440 bytes
Template Refresh Rate	100 packets
Template Timeout Rate	600 seconds
General Options Refresh Rate	10000 packets
General Options Timeout Rate	600 seconds
Username Options Timeout Rate	1440 minutes
Inactive Username Expiry Rate	168 hours

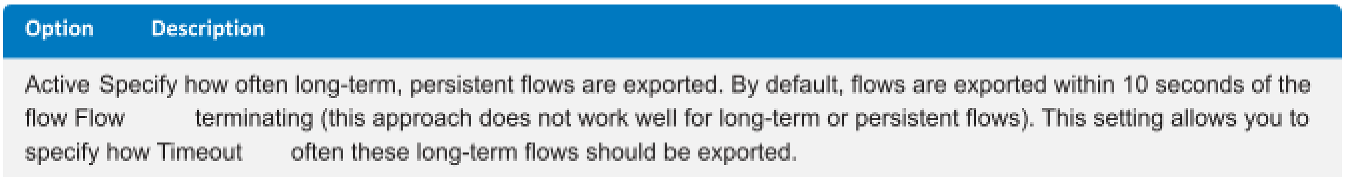
V9 Optional Fields - General

Export L7 Application ID	☑ Enable
Export Policy ID	☑ Enable
Export Type of Service (TOS)	☑ Enable
Export VLAN ID	☑ Enable
Export Min and Max Packet Sizes	☑ Enable
Export Min and Max TTL	□ Enable
Export Flow Direction	☑ Enable
Export SNMP Input and Output Interfaces	☑ Enable
Export output byte and packet counters	☑ Enable
Export username details	☑ Enable
Export VoIP MOS and rFactor	☑ Enable
Export extra information (hostnames)	☑ Enable
Export traffic class	□ Enable

V9 Optional Fields - Metrics

Export RTT	☑ Enable
Export Network Delay	☑ Enable
Export Network Jitter	☑ Enable
Export Server Delay	☑ Enable
Export Bytes Lost	☑ Enable
Export APS Score	☑ Enable

Common Options:



Option	Description
Active Specify how often long-term, persistent flows are exported. By default, flows are exported within 10 seconds of the flow Flow terminating (this approach does not work well for long-term or persistent flows). This setting allows you to specify how Timeout often these long-term flows should be exported.	

Netflow v9 Options:

Option	Description
Use Long Byte Counters	Export byte counters as 64bit values instead of 32bit.
Use Long Packet Counters	Export packet counters as 64bit values instead of 32bit.
Netflow Packet Payload Size	Set maximum Netflow packet payload size.
Template Refresh Rate	Configure the maximum number of packets between exporting of templates.
Template Timeout Rate	Configure the maximum number of seconds between exporting of templates.
Options Refresh Rate	Configure the maximum number of packets between exporting of options.
Options Timeout Rate	Configure the maximum number of seconds between exporting of options.
Username Options Timeout	Configure maximum number of minutes between exporting of username options.
Inactive Username Expiry Rate	Configure the maximum time to remember inactive usernames.

Netflow v9 Optional Fields - General:

Option	Description
Export L7 Application ID	Export Application identification information. The Application ID to Name mappings are exported as an options template.
Export Type of Service (TOS)	Export minimum and maximum Type of Service (TOS).
Export VLAN ID	Export VLAN identifier.
Export Packet Sizes	Export minimum and maximum packet sizes.
Export Min and Max TTL	Export minimum and maximum time-to-live (TTL).
Export Flow Direction	Export flow direction.
Export SNMP Interfaces	Export SNMP input and output interfaces.
Export Output Counters	Export output packet and byte counters, these can be compared to input byte and packet counters to calculate reduction.
Export Username Details	Export AD usernames.
Export VoIP MoS and rFactor	Export MoS and rFactor values for VoIP calls.
Export Extra Information	Exports extra flow information, such as domain name for HTTP flows, published application name for Citrix.
Export traffic class	Export traffic class.

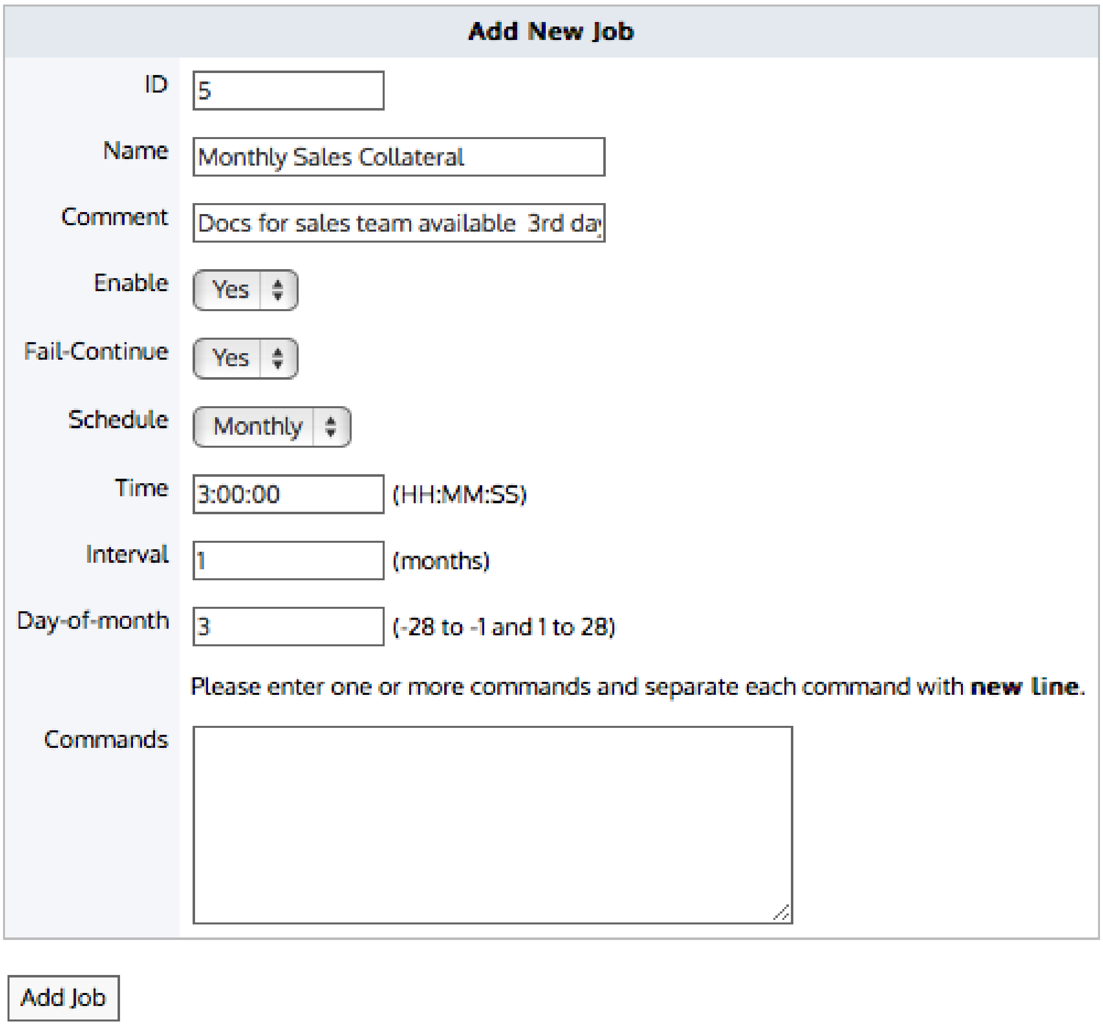
Netflow v9 Optional Fields - Metrics:

Option	Description

Export RTT	Export round trip time (RTT).
Export Network Delay	Export network delay.
Export Network Jitter	Export network jitter.
Export Server Delay	Export server delay.
Export Bytes Lost	Export lost bytes count.
Export APS Score	Export APS score.

4.2.6 Create a Scheduled Job

Cache pre-population, reboots, and firmware installations can be scheduled to run at a specific date and time, and at a set frequency.



Add New Job

ID	5
Name	Monthly Sales Collateral
Comment	Docs for sales team available 3rd day
Enable	Yes
Fail-Continue	Yes
Schedule	Monthly
Time	3:00:00 (HH:MM:SS)
Interval	1 (months)
Day-of-month	3 (-28 to -1 and 1 to 28)
	Please enter one or more commands and separate each command with **new line**.
Commands	

Screenshot 226: Create the schedule

Where do I find this configuration?

Go to **Configuration > System > Setup > Scheduled Jobs**.

To schedule a job

1. In the **Add New Job** area, type a unique **ID** for the job.
2. Type a **Name** for the job.
3. [Optional] In the **Comment** field, type a description for the job.
4. To enable the job to execute upon the next scheduled time, **Enable** the job.
5. If the job should be completed, even if one or more commands fail to execute, set **Fail-Continue** to **Yes**.
6. Set the schedule of the job. Jobs can be set to run Once, Daily, Weekly, Monthly, or Periodically.
   - **Once:** Set the time and date when this job should be executed.
   - **Daily:** Set the time that this job will execute every day.
   - **Weekly:** Set the time and the day of the week that this job will execute.
   - **Monthly:** Set the time of day, how frequently it recurs measured in intervals of months, and the day of the month. The day of the month is specified as 1 through 28 (E.g. March 23 would have a day of the month as 23), or the day of the month can be specified as -1 through -28, where it counts from the last day of the month (E.g. March 31 would have a day of the month as -1 and March 23 could be -9.)
   - **Periodic:** Set the start time and date and how frequently it recurs as an interval. Start time is specified as `HH:MM:SS`, start date is entered as YYYY/MM/DD, interval is entered as 2h3m4s.

7. After selecting the schedule of the job, specify the parameters for the schedule. For example, set the time, date, inter- val, or day-of-the-week when the job runs.

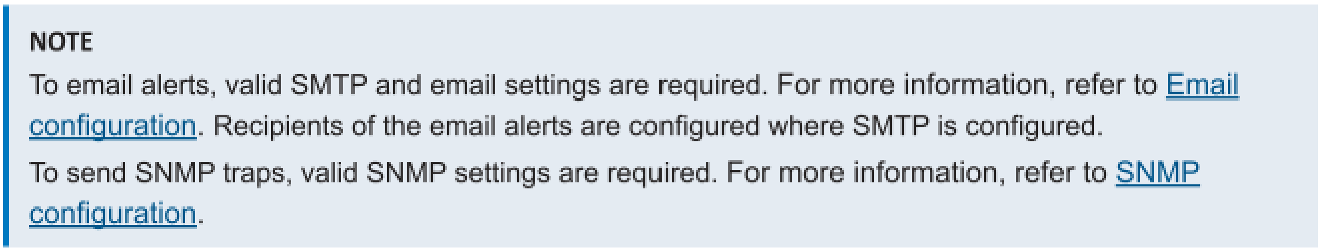
8. In the **Commands** field, type the necessary commands for the job you want to run. Each command must be on a new line. For scheduled pre-population jobs, leave the commands field blank. When creating the pre-population object, specify this scheduled job. The CLI for the pre-population object will automatically populate this commands field.

9. Click **Add Job**.

The job is added to the list, and is now available for selection in the Pre-population Object, if desired.

4.2.7 Alerts

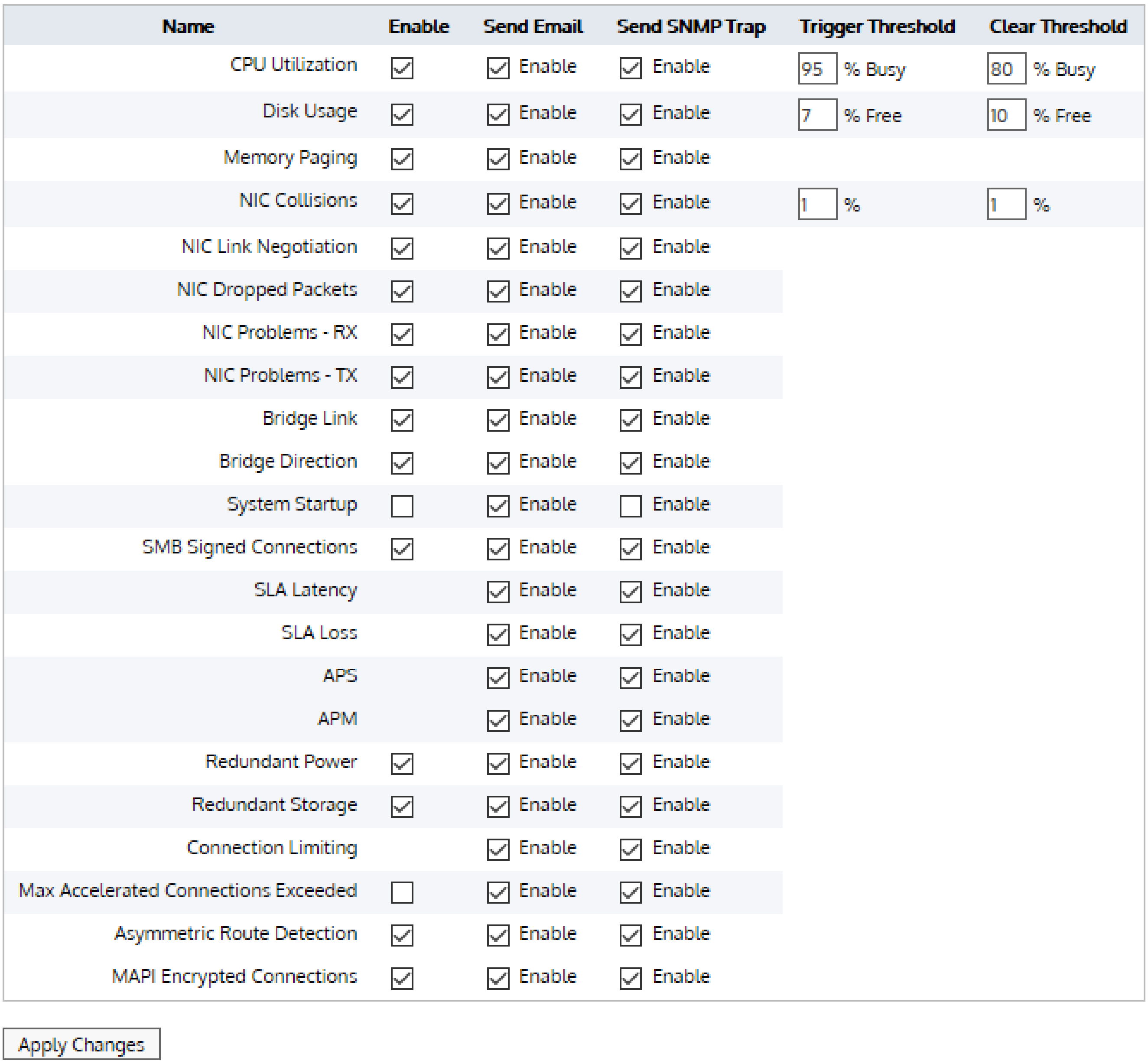
Alerts will notify you when there are issues or potential issues with either the GFI ClearView appliance system (such as CPU utilization and memory paging) or with your traffic (such as an application performance score dropped).The alerts can either be sent by email or by SNMP traps. Use the alerts to ensure the system and your network is operating the way you need it to.



NOTE

To email alerts, valid SMTP and email settings are required. For more information, refer to Email configuration. Recipients of the email alerts are configured where SMTP is configured.

To send SNMP traps, valid SNMP settings are required. For more information, refer to SNMP configuration.



Name	Enable	Send Email	Send SNMP Trap	Trigger Threshold	Clear Threshold
CPU Utilization	☑	☑ Enable	☑ Enable	95 % Busy	80 % Busy
Disk Usage	☑	☑ Enable	☑ Enable	7 % Free	10 % Free
Memory Paging	☑	☑ Enable	☑ Enable		
NIC Collisions	☑	☑ Enable	☑ Enable	1 %	1 %
NIC Link Negotiation	☑	☑ Enable	☑ Enable		
NIC Dropped Packets	☑	☑ Enable	☑ Enable		
NIC Problems - RX	☑	☑ Enable	☑ Enable		
NIC Problems - TX	☑	☑ Enable	☑ Enable		
Bridge Link	☑	☑ Enable	☑ Enable		
Bridge Direction	☑	☑ Enable	☑ Enable		
System Startup	□	☑ Enable	□ Enable		
SMB Signed Connections	☑	☑ Enable	☑ Enable		
SLA Latency		☑ Enable	☑ Enable		
SLA Loss		☑ Enable	☑ Enable		
APS		☑ Enable	☑ Enable		
APM		☑ Enable	☑ Enable		
Redundant Power	☑	☑ Enable	☑ Enable		
Redundant Storage	☑	☑ Enable	☑ Enable		
Connection Limiting		☑ Enable	☑ Enable		
Max Accelerated Connections Exceeded	□	☑ Enable	☑ Enable		
Asymmetric Route Detection	☑	☑ Enable	☑ Enable		
MAPI Encrypted Connections	☑	☑ Enable	☑ Enable		

Some alerts are enabled with no option to disable, but for all alerts you need to decide if you want email notifications and/or SNMP traps. For some alerts, you can specify operational thresholds to trigger or clear the alerts.

Specified Thresholds Exceeded

- **SLA Latency** – Alert raised when the specified latency for an SLA object is exceeded.For more information, refer to Configuring service level agreement objects.
- **SLA Loss** – Alert raised when there is loss for a SLA.
- **APS** – Alert raised when the defined threshold for an APS object is exceeded.
- **APM** – Alert raised when the defined threshold for an APM object is exceeded.
- **Connection Limiting** – Alert raised when one or more Virtual Circuits has connection limits enabled, and the threshold was reached.

Appliance Issues

- **CPU Utilization** – Alert raised when the CPU utilization threshold is reached. The defaults are 95% and 80% busy respectively.
- **Disk Usage** – Alert raised when the used disk space threshold is reached. The defaults are 7% and 10% free respectively.
- **Memory Paging** – Alert for memory use and paging.
- **NIC Collisions** – Alert raised when collisions are present on the interfaces. The defaults are 20 and 1 per 30 sec respectively.
- **NIC Link Negotiation** – Alert raised when the speed/duplex on an interface is set to auto, but it is negotiating at half duplex and/or 10Mbps.
- **NIC Dropped packets** – Alert raised when dropped packets are present on the interfaces.
- **NIC Problems- RX** – Alert raised when RX errors are present
- on the interfaces. **NIC Problems- TX** - Alert raised when TX
- errors are present on the interfaces. **System Startup** – Alert

  raised when the GFI ClearView appliance boots up.

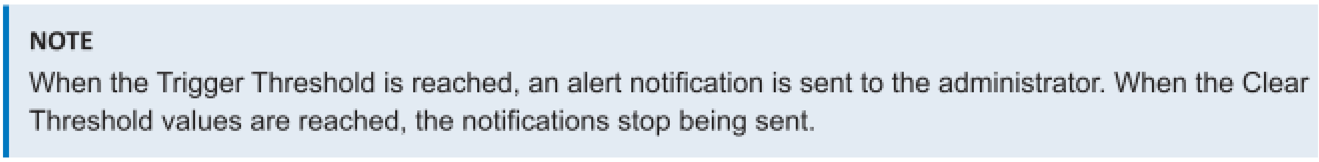
- **Redundant Power** – Alert raised when one of the power supplies fails (only available on platforms with power redundancy).
- **Redundant Storage** – Alert raised when one of the hard disks fails (only available on platforms with storage redundancy).

Enabling System Alerts

Use the following instructions to enable the system alerts.

Before you begin, read through Alerts for an understanding of what each of the alerts does.

1. Go to Configuration > System > Setup > Alerts.
2. For each of the listed alerts, decide upon which you need **Enabled**.
3. For each of the enabled alerts, select the types of notification to receive: **Send Email**, **Send SNMPTrap**, or both.
4. If selecting **CPU Utilization**, **Disk Usage**, or **NIC Collisions** alerts, specify the **Trigger Threshold** and **Clear Threshold** levels that cause the notifications to be sent.



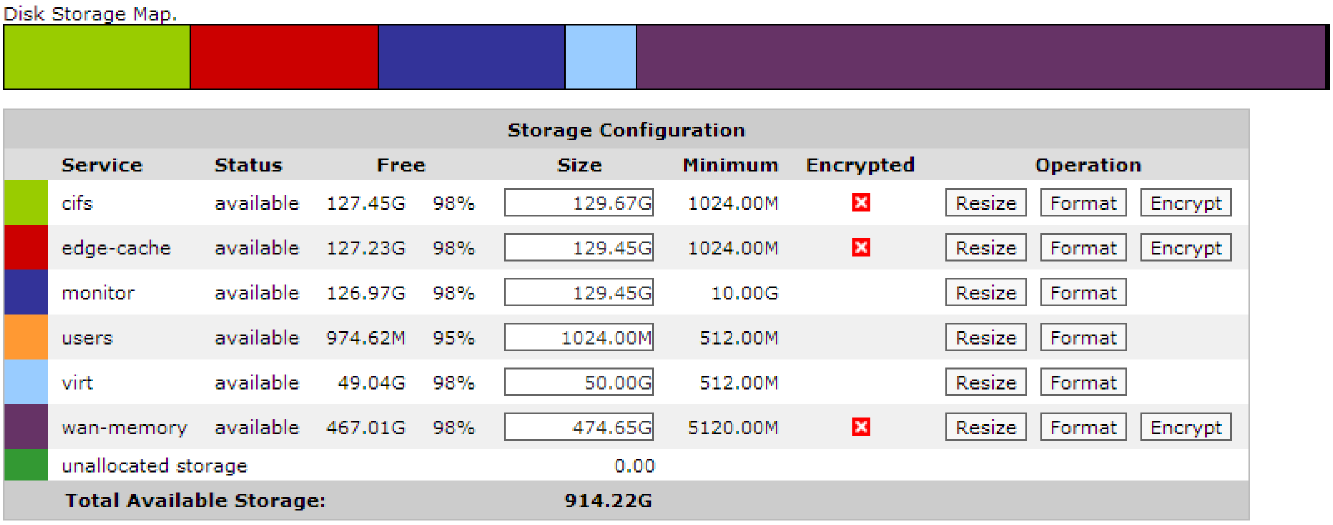
NOTE

When the Trigger Threshold is reached, an alert notification is sent to the administrator. When the Clear Threshold values are reached, the notifications stop being sent.

5. Click **Apply Changes**..

4.2.8 Diskstorage explained

The GFI ClearView appliance has the capability to dynamically change the amount of storage allocated to system services. The Storage configuration page allows you to see how much disk storage is currently allocated to each system service, as well as the amount currently in use. Users can re-size and reallocate disk space as required.



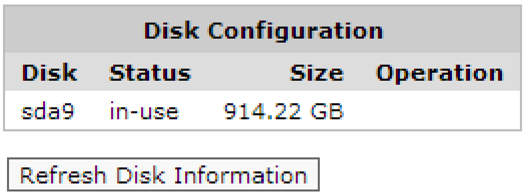
Disk Storage Map.

Storage Configuration

	Service	Status	Free		Size	Minimum	Encrypted	Operation		
🟩	cifs	available	127.45G	98%	129.67G	1024.00M	☒	Resize	Format	Encrypt
🟥	edge-cache	available	127.23G	98%	129.45G	1024.00M	☒	Resize	Format	Encrypt
🟦	monitor	available	126.97G	98%	129.45G	10.00G		Resize	Format	
🟧	users	available	974.62M	95%	1024.00M	512.00M		Resize	Format	
🟦	virt	available	49.04G	98%	50.00G	512.00M		Resize	Format	
🟪	wan-memory	available	467.01G	98%	474.65G	5120.00M	☒	Resize	Format	Encrypt
🟩	unallocated storage				0.00					
	Total Available Storage:				**914.22G**					

The disk storage map shows which services are using disk storage and their current status. It also shows the amount of storage allocated to each service with their amount of free space and minimum storage requirements. Particular services have the capability to be encrypted. Whether the storage for those services are currently encrypted is also indicated.

The Disk Configuration section shows a summary of storage by disk partition.



Disk Configuration

Disk	Status	Size	Operation
sda9	in-use	914.22 GB	

Refresh Disk Information

The Disk Storage Map

- **Service** – the services using disk storage
- **Status** – the status of that storage; the disk storage may be in one of several states, depending on which operation has been selected:
  - **available** – The storage is online and available to the service.
  - **growing** – The storage size was increased, and the file system is being reconfigured to use the newly cre- ated space.
  - **shrinking** – The storage size was decreased, and the file system is being reconfigured to use the decreased amount of storage available.
  - **formatting** – The storage is being formatted.
  - **checking** – The storage file system is being checked for consistency.
  - **error** – The storage is in an error state. Further information about the error will be displayed in a status mes- sage at the top of the form.
  - **unavailable** – The storage is not available.
- **Free** – the amount of free storage available, shown as the number of bytes as well as a

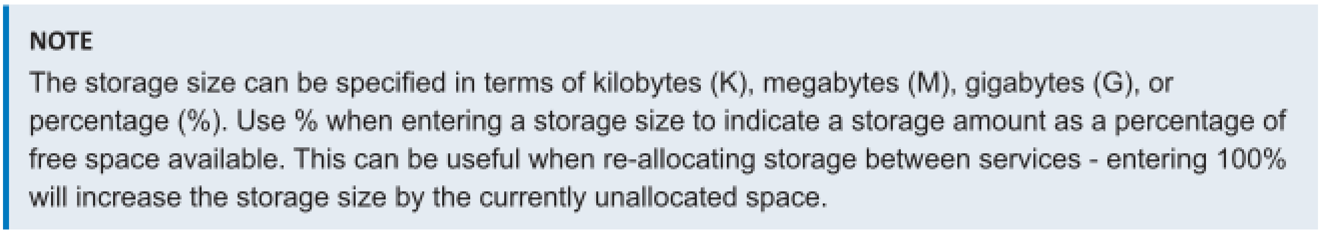
percentage of available space

- **Size** – the total amount of storage allocated for this service
- **Minimum** – the minimum amount of storage required for this service
- **Encrypted** – identifies whether the storage for the service is currently encrypted or not
- **Operation** – options to perform operations on the storage (resize, format, encrypt).

Resizing disk storage for a service

Use the following instructions to resize the disk storage for a service. These instructions apply to each service.

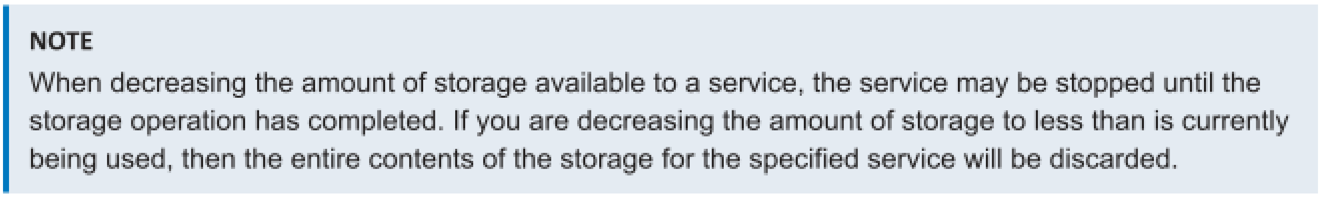
1. Go to Configuration > System > Setup > Storage.
2. Find the entry for the service in the table.
3. In the Size column, edit the amount of storage available to a service.



NOTE

The storage size can be specified in terms of kilobytes (K), megabytes (M), gigabytes (G), or percentage (%). Use % when entering a storage size to indicate a storage amount as a percentage of free space available. This can be useful when re-allocating storage between services - entering 100% will increase the storage size by the currently unallocated space.

4. On the same row, click **Resize**.

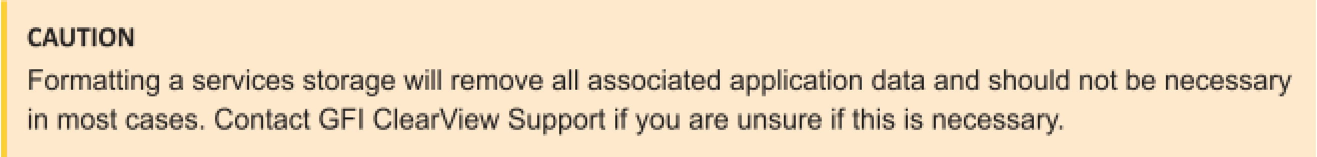


NOTE

When decreasing the amount of storage available to a service, the service may be stopped until the storage operation has completed. If you are decreasing the amount of storage to less than is currently being used, then the entire contents of the storage for the specified service will be discarded.

Deleting all data stored for a service

Use the following instructions to delete all data from the disk storage for a service. These instructions apply to all services



CAUTION

Formatting a services storage will remove all associated application data and should not be necessary in most cases. Contact GFI ClearView Support if you are unsure if this is necessary.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
5. Click Configuration > System > Setup > Storage.
6. Find the entry for the service in the table.
7. On the same row, click **Format**.

4.3 Authentication

Learn the process of authenticating users and user groups on your network.

4.3.1 Display a List of Active Users

Active Users lists the users currently logged into either the Web UI or the CLI.

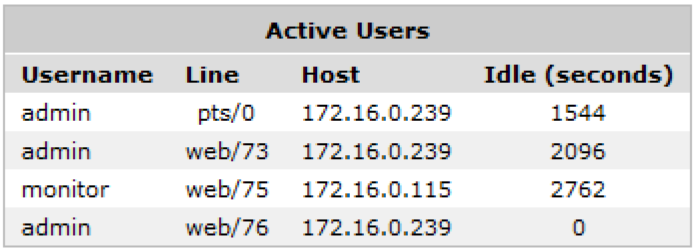
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click Configuration > System > Authentication > Active Users.

The table below shows an example of the currently logged in users along with the session type, IP address and the session idle time in seconds.



Active Users

Username	Line	Host	Idle (seconds)
admin	pts/0	172.16.0.239	1544
admin	web/73	172.16.0.239	2096
monitor	web/75	172.16.0.115	2762
admin	web/76	172.16.0.239	0

4.3.2 Local User Accounts

Local User Accounts allows you to add/remove local user accounts as well as change local user's passwords.

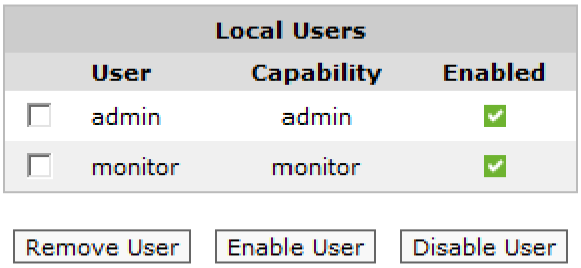
On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

1. Key-in the **Username** and **Password**.

2. Click **Login**.

5. Click Configuration > System > Authentication > Local User Accounts.

The table at the top of the page lists the configured local users and their capabilities.

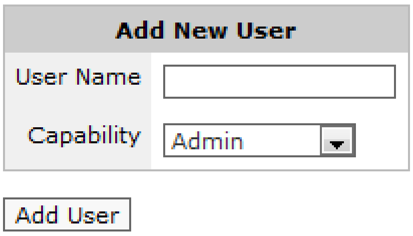


Local Users

	User	Capability	Enabled
□	admin	admin	✓
□	monitor	monitor	✓

6. To remove local user accounts from the GFI ClearView appliance or to temporarily disable an account, select the checkbox for the user and click **Remove User** or **Disable User**.

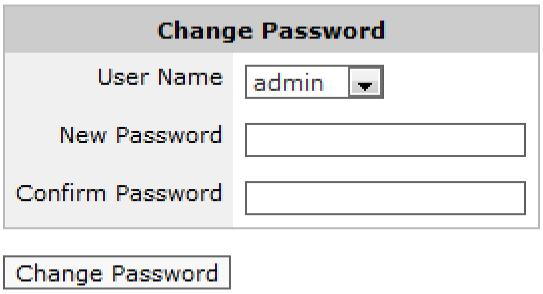
7. To add a new Local User Account, specify a username and select a capability. Click **Add User**. Admin users have full read-write access to the GFI ClearView appliance. Monitor users have read-only access.



Add New User

User Name	
Capability	Admin

8. Create a password for a new user, or change the password for an existing user by selecting the username you wish to create or change the password for and enter a new password. Click **Change Password**.



Change Password

User Name: admin

New Password:

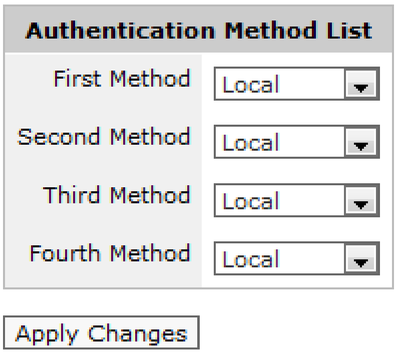
Confirm Password:

4.3.3 AAA

AAA configures how remote users should authenticate to the GFI ClearView appliance and what privileges they should receive.

1. To configure AAA, navigate to **Configuration > System > Authentication > AAA** on the Web UI, advanced mode.

2. Specify the order in which users are authenticated. When a user logs in, the GFI ClearView appliance will try to authenticate them using the authentication methods specified here, in the order they are configured.



Authentication Method List

First Method: Local

Second Method: Local

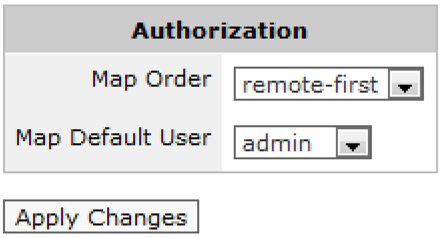
Third Method: Local

Fourth Method: Local

> **NOTE**
>
> This setting is required if you are using a remote access mechanism such as LDAP, Radius or TACACS+.

3. Click **Apply Changes**.

4. Control what privileges remotely authenticated users receive when they login to the GFI ClearView appliance.



Authorization

Map Order: remote-first

Map Default User: admin

Map Orde r	remote-first	Apply user privileges supplied by the remote authentication mechanism first. If that fails, use the 'Map Default User' setting below.
	remote - only	Apply user privileges supplied by the remote authentication mechanism first. If that fails, the user will not be authenticated.
	local-only	Use the 'Map Default User' setting below.
Map Default		

5. Click **Apply Changes**.

4.3.4 LDAP Authentication

LDAP authentication allows you to configure the GFI ClearView appliance to authenticate user login attempts with a remote LDAP (including Active Directory) server.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Ensure LDAP is selected as an Authentication Method on the AAA page.

6. Click **Configuration > System > Authentication** and switch to the **LDAP** tab.

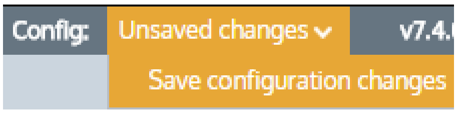
7. Define the global LDAP authentication options. Click **Apply Changes**.

8. Specify the hostname or IP address of the remote LDAP server. IPv4 or IPv6 addresses can be specified. Multiple LDAP servers may be defined.

9. Click **Add New LDAPServer**.

10. To remove an LDAP servers from the GFI ClearView appliance, select the checkbox for the server and click **Remove Server**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



4.3.5 Radius Authentication

Radius authentication allows you to configure the GFI ClearView appliance to authenticate user login attempts with a remote Radius server.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Ensure RADIUS is selected as an Authentication Method on the AAA page.

6. Click **Configuration > System > Authentication** and switch to the **Radius** tab.

7. Define the global RADIUS settings.

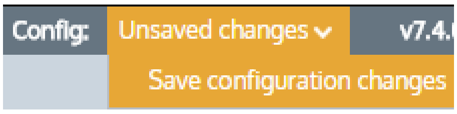
8. Click **Apply Changes**.

9. Specify the hostname or IP address of the remote Radius server. IPv4 addresses can be specified. Multiple Radius serv- ers may be defined.

10. Click **Add New RADIUS Server**.

11. To remove Radius servers from the GFI ClearView appliance, select the checkbox for the server and click **Remove Server**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



4.3.6 TACACS+ authentication

TACACS+ authentication allows you to configure the GFI ClearView appliance to authenticate user login attempts with a remote TACACS+ server.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Ensure TACACS+ is selected as an Authentication Method on the AAA page.

6. Click **Configuration > System > Authentication** and switch to the **TACACS+** tab.
7. Define global TACACS+ authentication options.

8. Click **Apply Changes**.

9. Specify the hostname or IP address of the remote TACACS+ server. IPv4 addresses can be specified. Multiple TACACS+ servers may be defined.

10. Click **Add New TACACS+ Server**.

11. To remove TACACS+ servers from the GFI ClearView appliance, select the checkbox for the server and click **Remove Server**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.

4.4 System Maintenance

Learn to maintain your GFI ClearView Appliances.

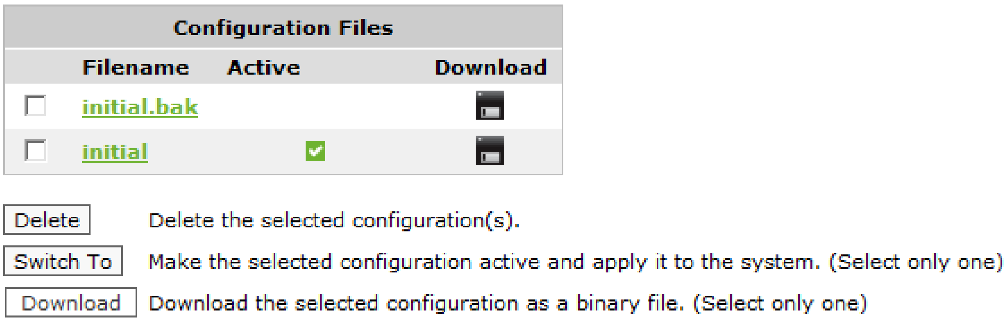
The Manage System Configuration screen allows you to download, save, switch, revert and delete system configuration files. You can learn about backing up your configuration as well as importing and exporting your config system.

4.4.1 Manage System Configuration

The Manage System Configuration screen allows you to download, save, switch, revert and delete system configuration files.

> **NOTE**
> To Manage System Configuration, navigate to **Configuration > System > Maintenance > Manage Config** on the Web UI, advanced mode.

The table below lists the available system configuration files. There will be a check mark next to the active configuration. Clicking on the configuration file name will display the text-based version of the configuration file in the window at the bottom of this page. Clicking on the 'Download' icon next to the configuration file will allow you to download and save/backup the text-based version of the configuration file.



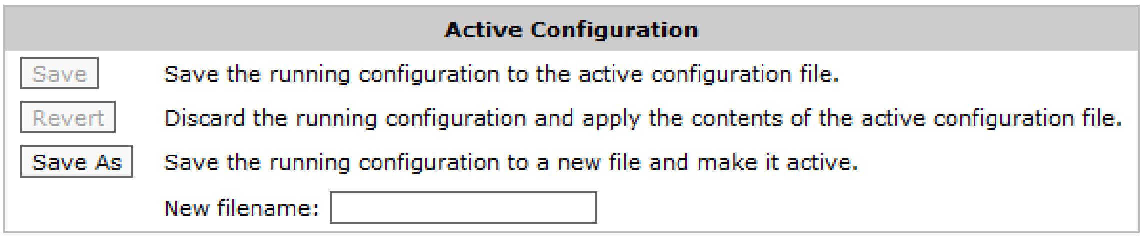
Configuration Files

	Filename	Active	Download
□	initial.bak		💾
□	initial	☑	💾

Delete	Delete the selected configuration(s).
Switch To	Make the selected configuration active and apply it to the system. (Select only one)
Download	Download the selected configuration as a binary file. (Select only one)

By selecting a configuration file and using the buttons above, you can delete the selected files from the system, switch to the selected configuration or download the selected configuration file in binary format.

The form below allows you to control the active and running configuration. If there are unsaved changes to the active configuration, this is known as the 'running configuration'.



Active Configuration

Save	Save the running configuration to the active configuration file.
Revert	Discard the running configuration and apply the contents of the active configuration file.
Save As	Save the running configuration to a new file and make it active.
	New filename:

You can save the running configuration and make it the active configuration, revert the running configuration back to the previously saved state of the active configuration, or save the running configuration to a new configuration file and make that the new active configuration.

How to backup your Appliance settings

It is recommended to take a backup of your GFI ClearView Appliance configuration during:

- Disk replacement
- Diagnostics by TAC
- Firmware upgrade

Generally users configure GFI ClearView once and the configuration file doesn't have to be changed over and over again. Hence simply use the steps below to save the configuration file locally. If for any reason a backup is required periodically, you can also schedule a job for the same. Go to **System > Setup > Scheduled Jobs**.

There are two types of GFI ClearView configuration files:

- Binary
- Text (recommended)

To download and save the configuration file:

1. Go to Configuration > System > Maintenance > Manage Config.

2. Find the configuration you wish to export. The current active configuration displays a green check mark in front of it.

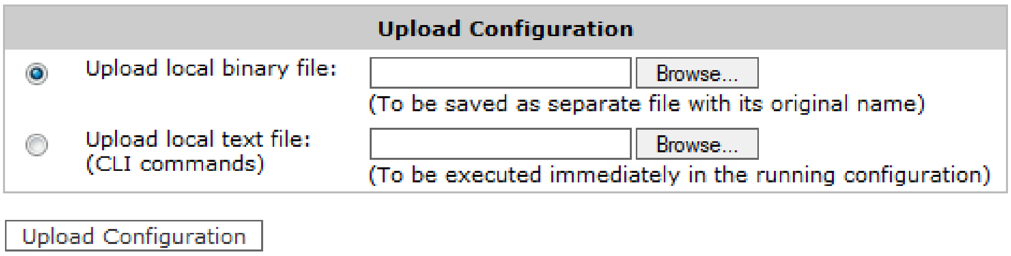
   - To save the configuration as a text file, click the save icon in the **Download** column beside it. It takes some time to generate. The generated text file contains all the CLI commands to replicate the configuration.
   - To save the configuration as a binary file, click the filename.

Import System Configuration

The Import System Configuration screen allows you to import previously saved or backed-up system configuration files.

> **NOTE**
>
> To Import System Configuration, navigate to **Configuration > System > Maintenance > Import Config** on the Web UI, advanced mode.

The form below can be used to upload system configurations that have been saved locally on the PC.



Upload Configuration

●	Upload local binary file:	Browse... (To be saved as separate file with its original name)
○	Upload local text file: (CLI commands)	Browse... (To be executed immediately in the running configuration)

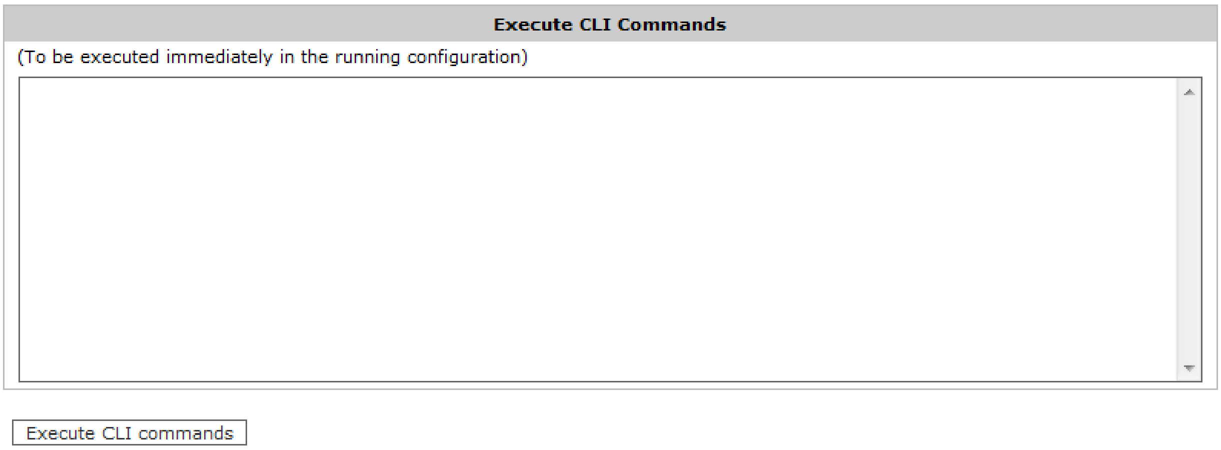
Screenshot 241: Upload system configurations

Option Description

Upload Use this option to upload a saved binary configuration file. This file would have been downloaded as a binary file from the local System > Maintenance > Manage Config page. Once this file is uploaded, it will appear in the list of available con-
binary figuration files on the System > Maintenance > Manage Config
page. file

Upload Use this option to upload a text file containing CLI commands. The CLI commands will be executed in order and any con- local figuration changes will be applied to the running configuration. This text file can contain one or more CLI commands or text could be a complete text-based system configuration file downloaded from the System > Maintenance > Manage Config file page.

Use the form below to execute a batch of CLI commands on the Web UI. The CLI commands will be executed in order and any configuration changes will be applied to the running configuration.

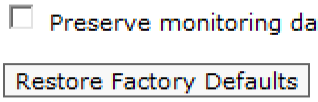


4.4.2 Factory Defaults

The Factory Defaults screen allows you to restore the configuration of the GFI ClearView appliance to factory default settings. This includes removing any system logs, and monitoring statistics.

> **NOTE**
> To restore Factory Defaults, navigate to **Configuration > System > Maintenance > Factory Defaults** on the Web UI, advanced mode.

When restoring Factory Default settings, network connectivity settings such as the IP address, DNS servers and Default Gateway are preserved. There is also an option to preserve any monitoring data. To preseve monitoring data tick the 'Preserve monitoring' box prior to restoring the factory default settings.



After performing a Factory Defaults, the GFI ClearView appliance will automatically reboot.

4.4.3 Reboot/Shutdown

The Reboot/Shutdown screen allows you to configure Reboot options as well as gracefully shutdown the GFI ClearView appliance in order to reboot it or power it down.

In this area of the GFI ClearView Web UI you can:

- Reboot the GFI ClearView Appliance
- Automatically Reboot the GFI ClearView Appliance
- Shutdown the GFI ClearView Appliance

Reboot the GFI ClearView Appliance

After a new version of the ExOS firmware is installed, you must reboot the appliance.

CAUTION
Any unsaved configuration changes will be lost if the Exinda appliance is rebooted or shutdown without saving the changes first.

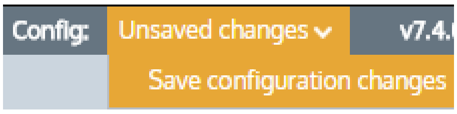
1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
5. Click **Configuration > System > Maintenance** and switch to the **Reboot / Shutdown** tab.
6. (Optional) Schedule the GFI ClearView Appliance to reboot at a specific date or time.
    a. Check **Schedule Reboot**.
    b. Enter the date and time when the appliance should reboot.
7. Select the reboot mode from the list.
    - **Fast Reboot**—This is a soft reboot and will reboot the operating system only. This does not reboot the hard- ware and does not reload the BIOS.
    - **Slow Reboot**—This is a hard reboot and will reboot the entire appliance. Use this option to access the BIOS or other start-up options.
8. Click **Reboot**. Rebooting the GFI ClearView Appliance may take a few minutes to restart.

Automatically Reboot the GFI ClearView Appliance

If the GFI ClearView Appliance becomes unresponsive, the System Watchdog can automatically reboot the appliance.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **User Name** and **Password**.
3. Click **Login**.
5. Click **Configuration > System > Maintenance** and switch to the **Reboot / Shutdown** tab.
6. In the System Watchdog area, select **Enable**.
7. Click **Apply Changes**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



Shutdown the GFI ClearView Appliance

If the GFI ClearView appliance needs to be powered off, shut it down from within the GFI ClearView Web UI.

IMPORTANT
Any unsaved configuration changes will be lost if the GFI ClearView appliance is rebooted or shutdown without saving the changes first.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
5. Click **Configuration > System > Maintenance** and switch to the **Reboot / Shutdown** tab.
6. Click **Shutdown**.

The GFI ClearView Appliance will not restart, and must be physically powered on again.

4.5 System Tools

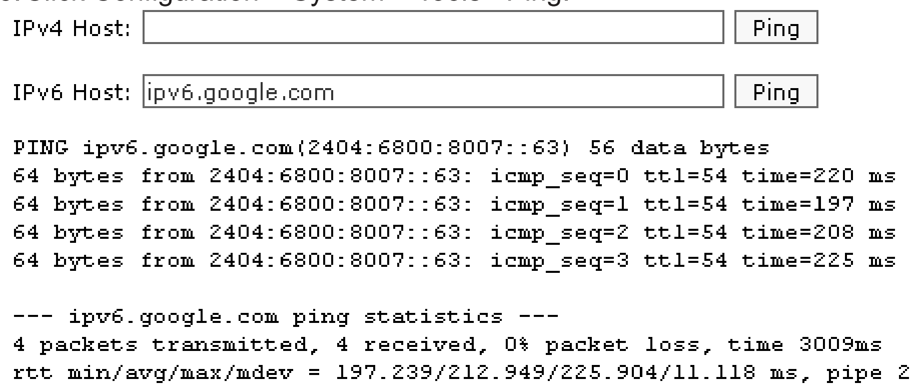
Learn about the various system tools available on your GFI ClearView Appliance to assist you in day-to-day operations.

GFI ClearView Appliance provides you with a set of network utilities that enables you to monitor network activity, gather network information and audit network devices.

4.5.1 Ping

Use the Ping Tool to test network connectivity from the GFI ClearView appliance to other hosts on the WAN or Internet.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.
5. Click Configuration > System > Tools> Ping.



IPv4 Host:

IPv6 Host: ipv6.google.com

```
PING ipv6.google.com(2404:6800:8007::63) 56 data bytes
64 bytes from 2404:6800:8007::63: icmp_seq=0 ttl=54 time=220 ms
64 bytes from 2404:6800:8007::63: icmp_seq=1 ttl=54 time=197 ms
64 bytes from 2404:6800:8007::63: icmp_seq=2 ttl=54 time=208 ms
64 bytes from 2404:6800:8007::63: icmp_seq=3 ttl=54 time=225 ms

--- ipv6.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 197.239/212.949/225.904/11.118 ms, pipe 2
```

6. In the **IPv4 host** or **IPv6 host** field, specify an IP address or fully qualified domain name to attempt to ping.
7. Click **Ping**. It may take a few seconds for the ping operation to complete and display the results.

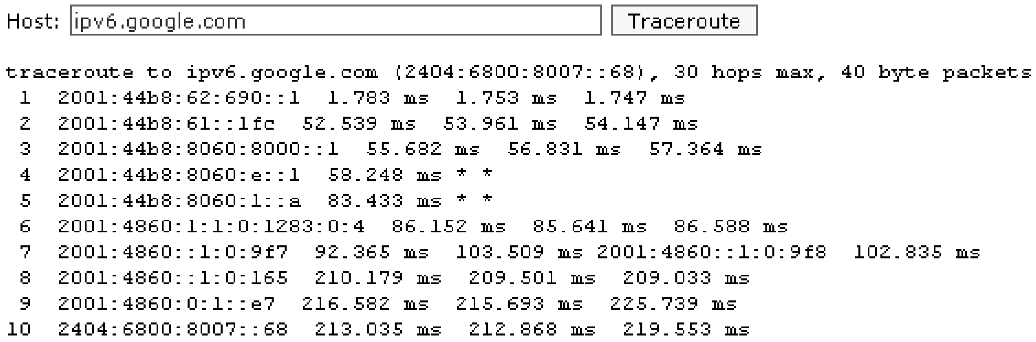
4.5.2 Traceroute

Use the Traceroute Tool to determine the network hops from the GFI ClearView appliance to other hosts on the WAN or Internet.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click Configuration > System > Tools> Traceroute.



Host: ipv6.google.com

```
traceroute to ipv6.google.com (2404:6800:8007::68), 30 hops max, 40 byte packets
 1  2001:44b8:62:690::1  1.783 ms  1.753 ms  1.747 ms
 2  2001:44b8:61::1fc  52.539 ms  53.961 ms  54.147 ms
 3  2001:44b8:8060:8000::1  55.682 ms  56.831 ms  57.364 ms
 4  2001:44b8:8060:e::1  58.248 ms * *
 5  2001:44b8:8060:1::a  83.433 ms * *
 6  2001:4860:1:1:0:1283:0:4  86.152 ms  85.641 ms  86.588 ms
 7  2001:4860::1:0:9f7  92.365 ms  103.509 ms 2001:4860::1:0:9f8  102.835 ms
 8  2001:4860::1:0:165  210.179 ms  209.501 ms  209.033 ms
 9  2001:4860:0:1::e7  216.582 ms  215.693 ms  225.739 ms
10  2404:6800:8007::68  213.035 ms  212.868 ms  219.553 ms
```

6. In the **Host** field, specify an IPv4 or IPv6 Address, or fully qualified domain name to attempt to traceroute.

7. Click **Traceroute**. It may take a few seconds for the operation to complete and display the results.

4.5.3 DNS Lookup

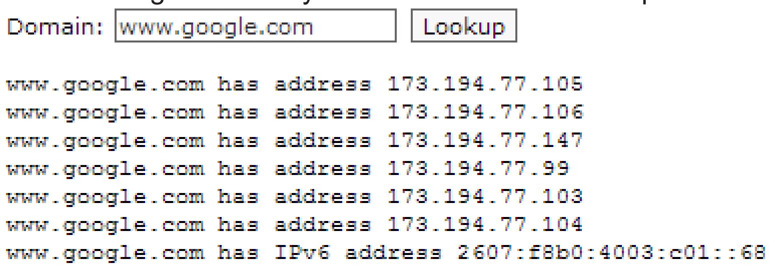
Use the DNS Lookup Tool to have the GFI ClearView appliance query the configured DNS servers to resolve the specified domain name.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click Configuration > System > Tools> DNS Lookup.



Domain: www.google.com

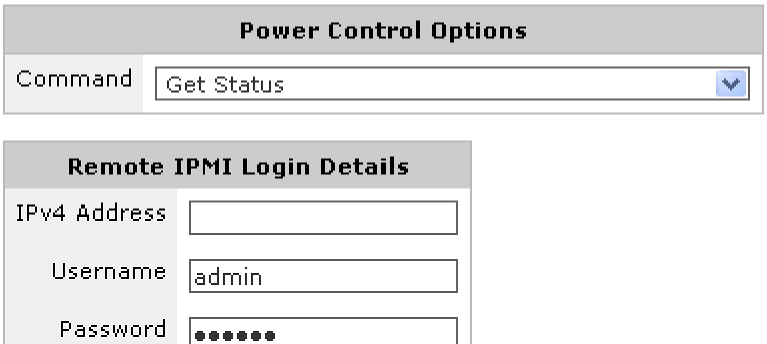
```
www.google.com has address 173.194.77.105
www.google.com has address 173.194.77.106
www.google.com has address 173.194.77.147
www.google.com has address 173.194.77.99
www.google.com has address 173.194.77.103
www.google.com has address 173.194.77.104
www.google.com has IPv6 address 2607:f8b0:4003:c01::68
```

6. In the Domain field, specify a fully qualified domain name to look up.

7. Click **Lookup**. It may take a few seconds for the operation to complete and display the results.

4.5.4 Query a remote IPMI GFI ClearView appliance

Use the IPMI Tool to query the power status, power cycle/power off, or reset a remote GFI ClearView appliance via IPMI. The remote appliance must have enabled IPMI access.



Power Control Options

Command: Get Status

Remote IPMI Login Details

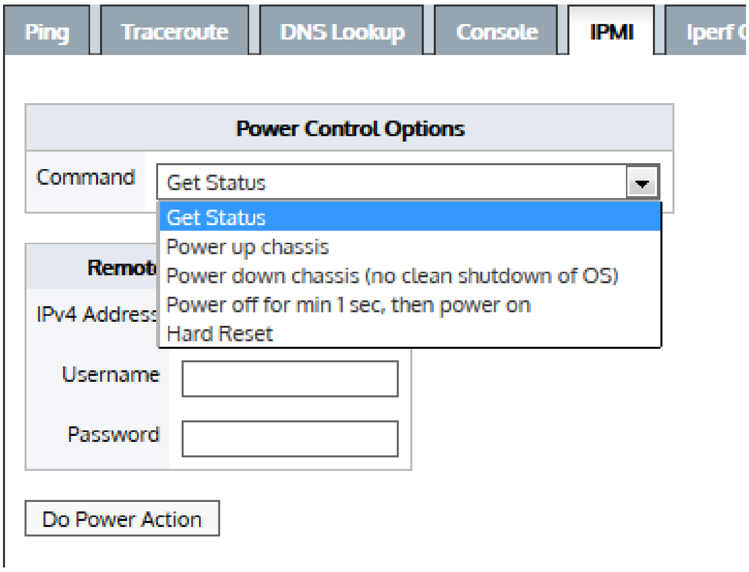
IPv4 Address:

Username: admin

Password: ••••••

To perform an IPMI action on a remote GFI ClearView appliance

1. Select the desired action from the **Power Control Options** drop down selection.



Command: Get Status

2. Enter the IPMI **IPv4 Address** of the remote appliance.

3. Enter the IPMI authentication details for the remote appliance.

   - The default username is admin.
   - The default password is exinda.

4. Click **Do Power Action**.

Example: Power cycle the GFI ClearView appliance with IPMI address 192.168.110.61 -

```
ipmi power address 192.168.110.61 username admin password exinda
control cycle
```

Example: Show the current power state of the GFI ClearView appliance with IPMI address 192.168.110.61 -

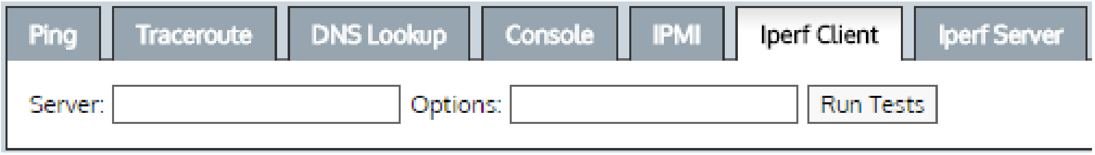
```
show ipmi power address 192.168.110.61 username admin password
exinda
```

4.5.5 iPerf Client

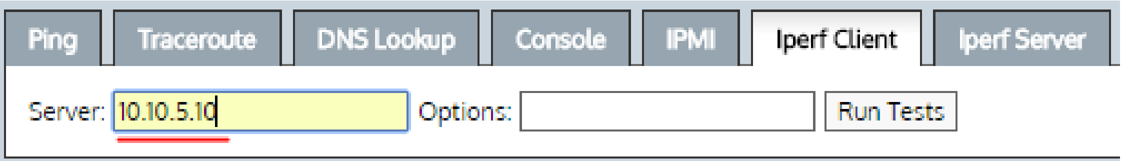
iPerf is a tool used for network throughput measurements. To function, it requires that two devices must be running the iPerf software to obtain bandwidth metrics between two endpoints. One device plays the role of the server and the other plays the role of the client. In GFI ClearView, there is a Web User Interface option to configure an GFI ClearView appliance as an iPerf client:

To configure an GFI ClearView Appliance as the iPerf client:

1. Click Configuration > System > Tools> Iperf Client.

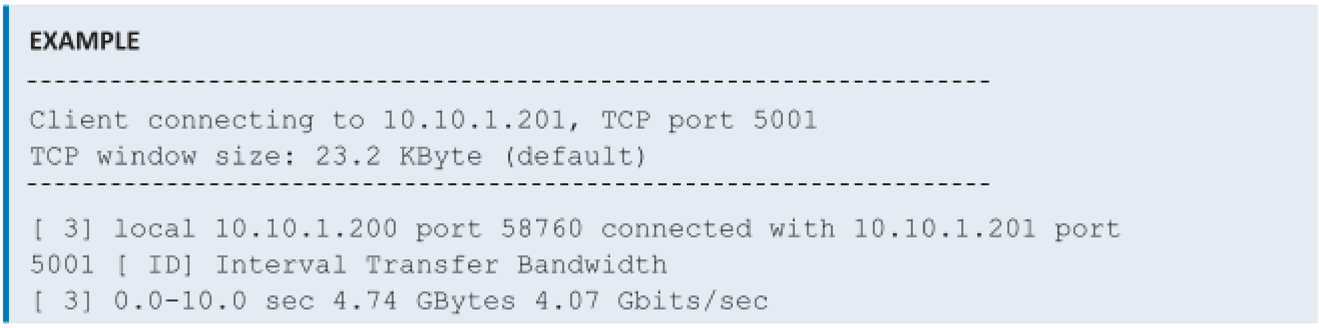


2. In the **Server** field, type the **IPaddress** or **Host Name** of an iPerf server that is already running.



Server: 10.10.5.10

3. Click Run Tests to view the test results. Example Results:



EXAMPLE

```
------------------------------------------------------------
Client connecting to 10.10.1.201, TCP port 5001
TCP window size: 23.2 KByte (default)
------------------------------------------------------------
[ 3] local 10.10.1.200 port 58760 connected with 10.10.1.201 port
5001 [ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.0 sec 4.74 GBytes 4.07 Gbits/sec
```

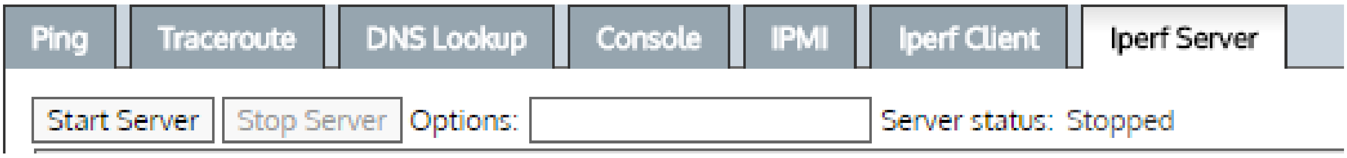
4.5.6 iPerf Server

iPerf is a tool used for network throughput measurements. To function, it requires that two devices must be running the iPerf software to obtain bandwidth metrics between two endpoints. One device plays the role of the server and the other plays the role of the client. In GFI ClearView, there is a Web User Interface option to configure an appliance as an iPerf server:

To configure an GFI ClearView Appliance as the iPerf Server:

Use the iPerf Server tab when the GFI ClearView appliance is the designated server.

1. Click Configuration > System > Tools> Iperf Server.



Options:

Server status: Stopped

2. (Optional), By default, an iPerf server listens to TCP packets on port 5001. However, you can use the following list of options to modify this condition:

Usage: `iperf [-s|-c host]`

`[options]` Example:

`iperf[-h]--help[-v|--version]`

Options for both Clients and Servers

```
-f, --format [kmKM] format to report: Kbits, Mbits, KBytes, MBytes

-i, --interval # seconds between periodic bandwidth reports
-l, --len #[KM] length of buffer to read or write (default 8 KB)

-m, --print_mss print TCP maximum segment size (MTU - TCP/IP header)

-o, --output <filename> output the report or error message to this
specified file

-p, --port # server port to listen on/connect to

-u, --udp use UDP rather than TCP

-w, --window #[KM] TCP window size (socket buffer size)

-B, --bind <host> bind to <host>, an interface or multicast address

-C, --compatibility for use with older versions does not sent extra msgs

-M, --mss # set TCP maximum segment size (MTU - 40 bytes)

-N, --nodelay set TCP no delay, disabling Nagle's Algorithm
```

```
-V, --IPv6Version Set the domain to IPv6
```

Options for Servers only

```
-s, --server run in server mode

-U, --single_udp run in single threaded UDP mode

-D, --daemon run the server as a daemon
```

Options for Clients only

```
-b, --bandwidth #[KM] for UDP, bandwidth to send at in bits/sec
(default 1 Mbit/sec, implies -u)

-c, --client <host> run in client mode, connecting to <host>

-d, --dualtest Do a bidirectional test simultaneously

-n, --num #[KM] number of bytes to transmit (instead of -t)

-r, --tradeoff Do a bidirectional test individually

-t, --time # time in seconds to transmit for (default 10 secs)

-F, --fileinput <name> input the data to be transmitted from a file

-I, --stdin input the data to be transmitted from stdin

-L, --listenport # port to receive bidirectional tests back on

-P, --parallel # number of parallel client threads to run

-T, --ttl # time-to-live, for multicast (default 1)

-Z, --linux-congestion <algo> set TCP congestion control algorithm (Linux
only)
```

Miscellaneous Options

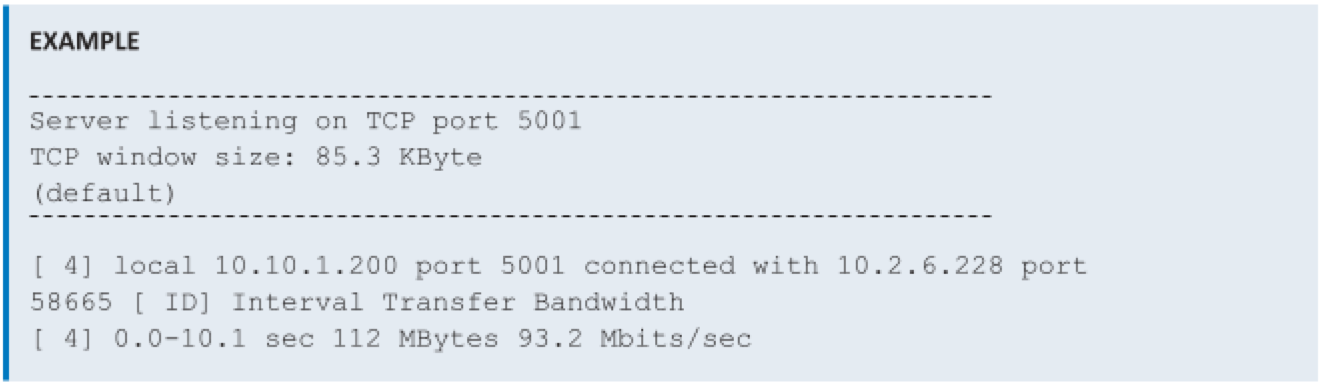
```
-x, --reportexclude [CDMSV] exclude C(connection) D(data) M(multicast)
S(settings) V(server) reports

-y, --reportstyle C report as a Comma-Separated Values

-h, --help print this message and quit

-v, --version print version information and quit
```

For instance, if the Iperf server is to listen to UDP packets on port 319, then you must use the following options:

```
-u –p 319
```

3. In the **Options** text box, type the options you need and then click the **Start Server** button. The server must be star- ted before triggering traffic from an Iperf client.

After the server is started, you can test the connection from an Iperf client by supplying the hostname as a parameter. Example Results:



EXAMPLE

```
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte
(default)
------------------------------------------------------------

[ 4] local 10.10.1.200 port 5001 connected with 10.2.6.228 port
58665 [ ID] Interval Transfer Bandwidth
[ 4] 0.0-10.1 sec 112 MBytes 93.2 Mbits/sec
```

5 Troubleshooting

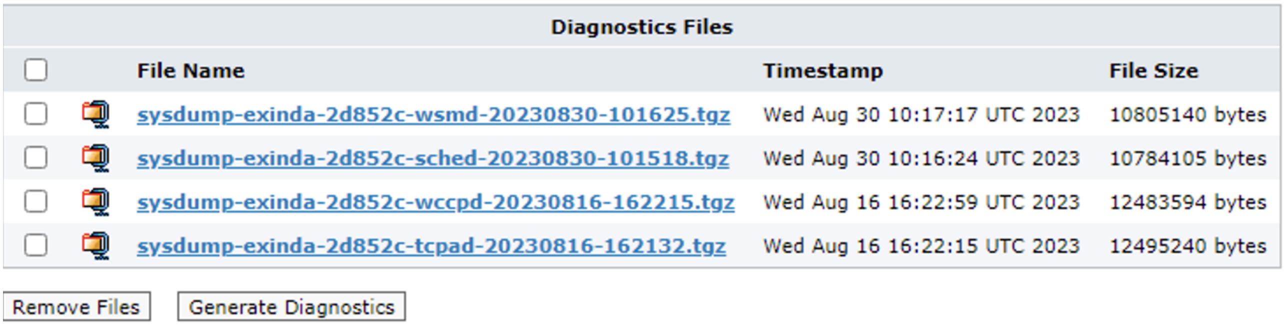
Learn how to deal with troubleshooting issues that you might have encountered when using the GFI ClearView Appliances. Much of the information here is also available elsewhere in the help, but is gathered here as a central location for accessing information about how to troubleshoot issues.

5.1 Diagnostics

Learn the various diagnostics tools available on your GFI ClearView Appliance. You can use these tools to help troubleshoot issues you might encounter.

5.1.1 Diagnostics Files

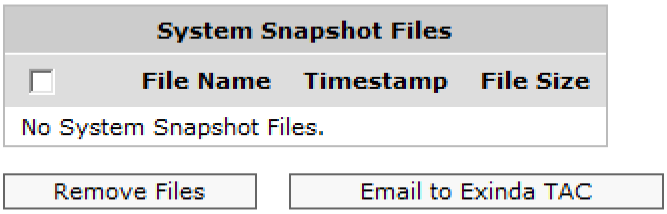
Diagnostics files contain system state information and can aid in troubleshooting. Diagnostics files may be requested by GFI ClearView TAC and can be generated and downloaded using the form below.



Diagnostics Files

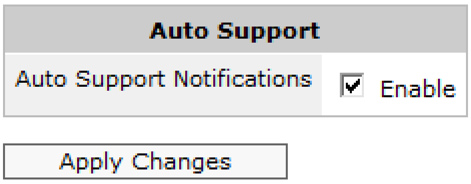
□		File Name	Timestamp	File Size
□		sysdump-exinda-2d852c-wsmd-20230830-101625.tgz	Wed Aug 30 10:17:17 UTC 2023	10805140 bytes
□		sysdump-exinda-2d852c-sched-20230830-101518.tgz	Wed Aug 30 10:16:24 UTC 2023	10784105 bytes
□		sysdump-exinda-2d852c-wccpd-20230816-162215.tgz	Wed Aug 16 16:22:59 UTC 2023	12483594 bytes
□		sysdump-exinda-2d852c-tcpad-20230816-162132.tgz	Wed Aug 16 16:22:15 UTC 2023	12495240 bytes

System snapshots are automatically generated when a process fails. If the 'Auto Support Notifications' option is enabled, they are automatically sent to GFI ClearView TAC for further troubleshooting.



System Snapshot Files

□	File Name	Timestamp	File Size
No System Snapshot Files.			



Auto Support

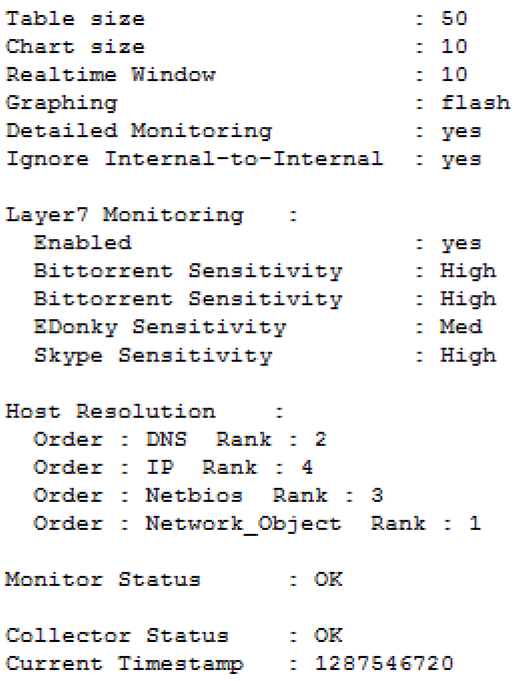
Auto Support Notifications	☑ Enable

> **NOTE**
>
> Valid SMTP and DNS settings are required for diagnostics to be sent to GFI ClearView TAC.

5.1.2 Monitor

The monitor diagnostics display the current monitor settings and the status of monitor and collector processes.

> **NOTE**
>
> To configure Monitor settings, navigate to **Configuration > System > Setup > Monitoring** on the Web UI, advanced mode.



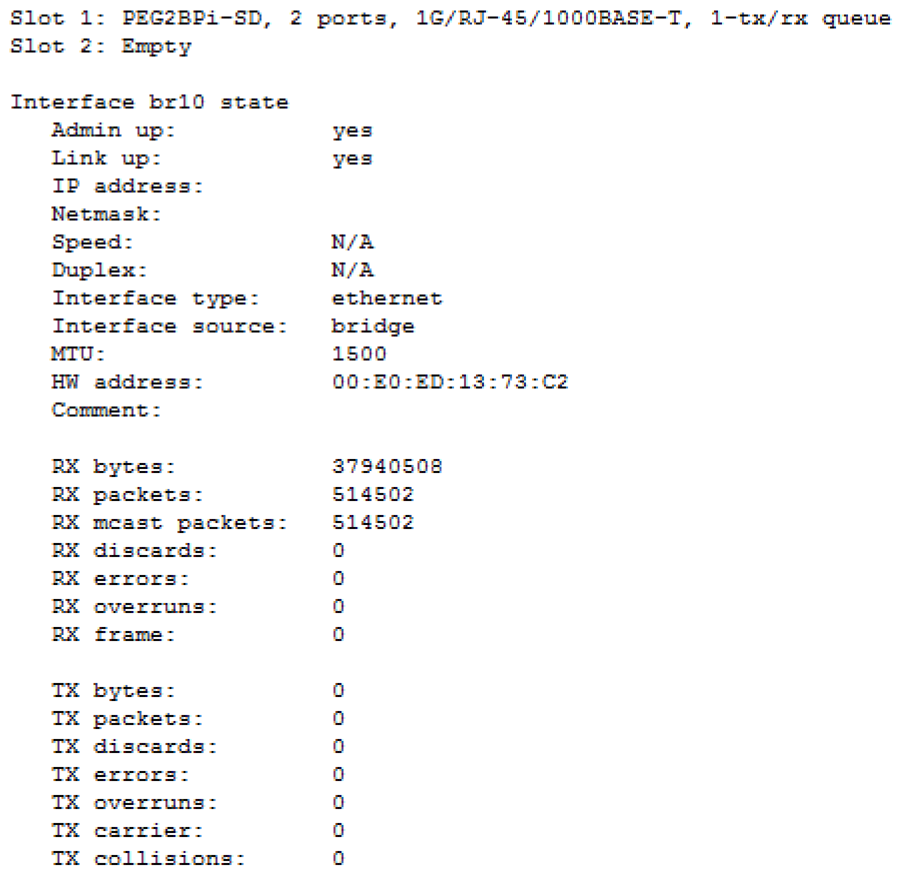
```
Table size                    : 50
Chart size                    : 10
Realtime Window               : 10
Graphing                      : flash
Detailed Monitoring           : yes
Ignore Internal-to-Internal   : yes

Layer7 Monitoring    :
  Enabled                     : yes
  Bittorrent Sensitivity      : High
  Bittorrent Sensitivity      : High
  EDonky Sensitivity          : Med
  Skype Sensitivity           : High

Host Resolution     :
  Order : DNS  Rank : 2
  Order : IP  Rank : 4
  Order : Netbios  Rank : 3
  Order : Network_Object  Rank : 1

Monitor Status       : OK

Collector Status     : OK
Current Timestamp    : 1287546720
```

5.1.3 NIC Diagnostics

The NIC diagnostics page can help when troubleshooting network delay issues. NIC errors, collisions and discards indicate a negotiation problem, which can lead to dropped packets and network delay. It is recommended that negotiation issues are addressed immediately.

The first lines show a summary of installed network adapters. Detailed information is available from the CLI "show diag" command.

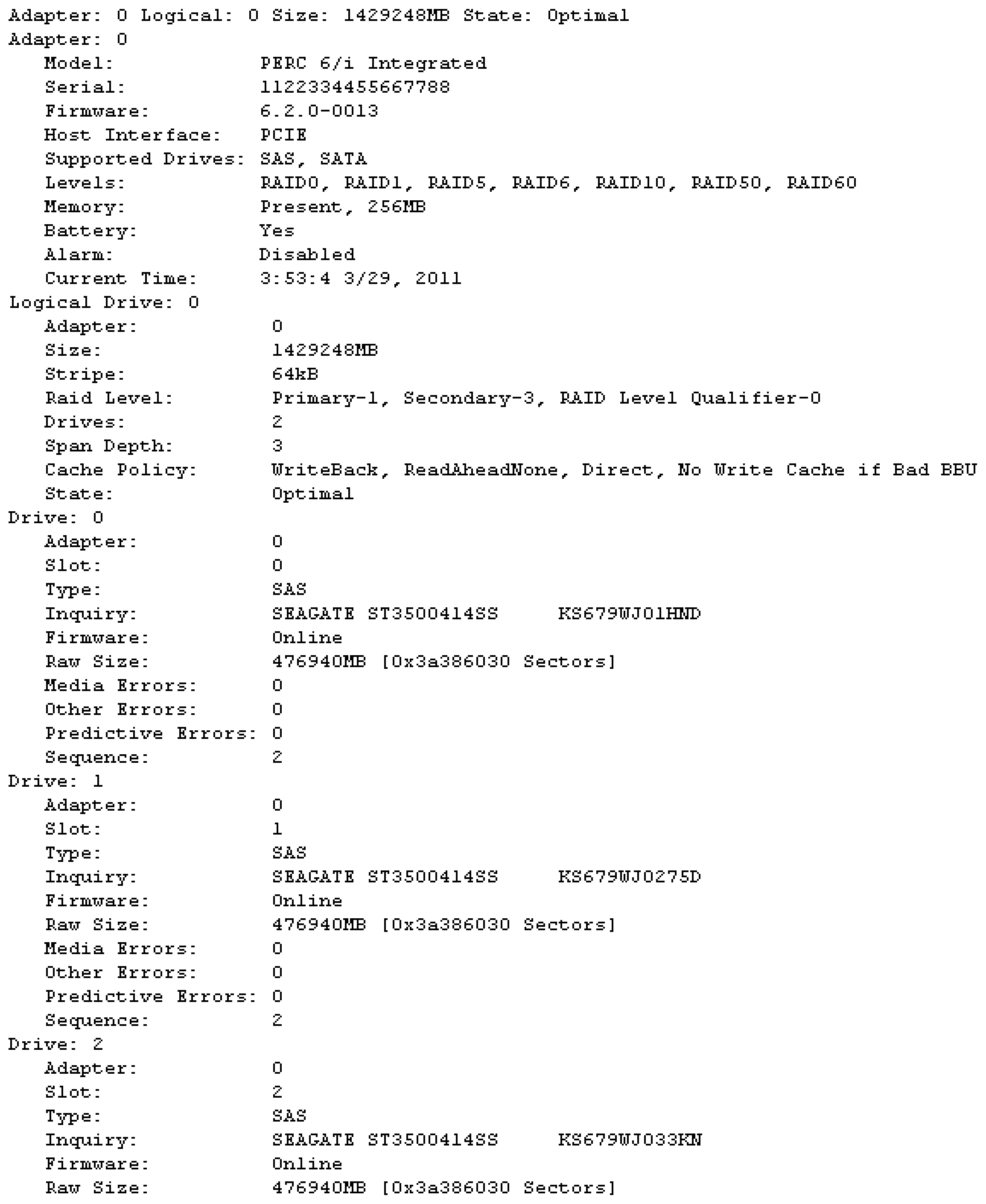
> **NOTE**
>
> To configure NIC settings, navigate to **Configuration > System > Network> NICs** on the Web UI, advanced mode.



```
Slot 1: PEG2BPi-SD, 2 ports, 1G/RJ-45/1000BASE-T, 1-tx/rx queue
Slot 2: Empty

Interface br10 state
   Admin up:             yes
   Link up:              yes
   IP address:
   Netmask:
   Speed:                N/A
   Duplex:               N/A
   Interface type:       ethernet
   Interface source:     bridge
   MTU:                  1500
   HW address:           00:E0:ED:13:73:C2
   Comment:

   RX bytes:             37940508
   RX packets:           514502
   RX mcast packets:     514502
   RX discards:          0
   RX errors:            0
   RX overruns:          0
   RX frame:             0

   TX bytes:             0
   TX packets:           0
   TX discards:          0
   TX errors:            0
   TX overruns:          0
   TX carrier:           0
   TX collisions:        0
```

5.1.4 RAID Diagnostics

The RAID diagnostics page is available on models that support Redundant Storage. A summary of the logical volume status is shown as well as details for RAID adapters, logical volumes and physical drives.



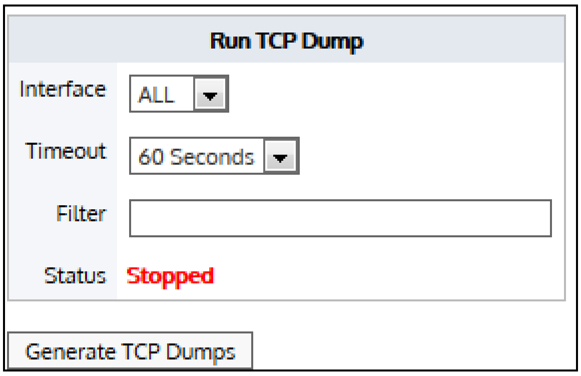
```
Adapter: 0 Logical: 0 Size: 1429248MB State: Optimal
Adapter: 0
   Model:            PERC 6/i Integrated
   Serial:           1122334455667788
   Firmware:         6.2.0-0013
   Host Interface:   PCIE
   Supported Drives: SAS, SATA
   Levels:           RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
   Memory:           Present, 256MB
   Battery:          Yes
   Alarm:            Disabled
   Current Time:     3:53:4 3/29, 2011
Logical Drive: 0
   Adapter:           0
   Size:              1429248MB
   Stripe:            64kB
   Raid Level:        Primary-1, Secondary-3, RAID Level Qualifier-0
   Drives:            2
   Span Depth:        3
   Cache Policy:      WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
   State:             Optimal
Drive: 0
   Adapter:           0
   Slot:              0
   Type:              SAS
   Inquiry:           SEAGATE ST3500414SS     KS679WJ01HND
   Firmware:          Online
   Raw Size:          476940MB [0x3a386030 Sectors]
   Media Errors:      0
   Other Errors:      0
   Predictive Errors: 0
   Sequence:          2
Drive: 1
   Adapter:           0
   Slot:              1
   Type:              SAS
   Inquiry:           SEAGATE ST3500414SS     KS679WJ0275D
   Firmware:          Online
   Raw Size:          476940MB [0x3a386030 Sectors]
   Media Errors:      0
   Other Errors:      0
   Predictive Errors: 0
   Sequence:          2
Drive: 2
   Adapter:           0
   Slot:              2
   Type:              SAS
   Inquiry:           SEAGATE ST3500414SS     KS679WJ033KN
   Firmware:          Online
   Raw Size:          476940MB [0x3a386030 Sectors]
```

5.1.5 TCP Dump

A TCP Dump captures packets being transmitted or received from the specified interfaces and can assist in troubleshooting. A TCP Dump may be requested by GFI ClearView TAC.

Run a TCP Dump from the GFI ClearView appliance

Click Configuration > Diagnostics> TCPDump.



Run TCP Dump

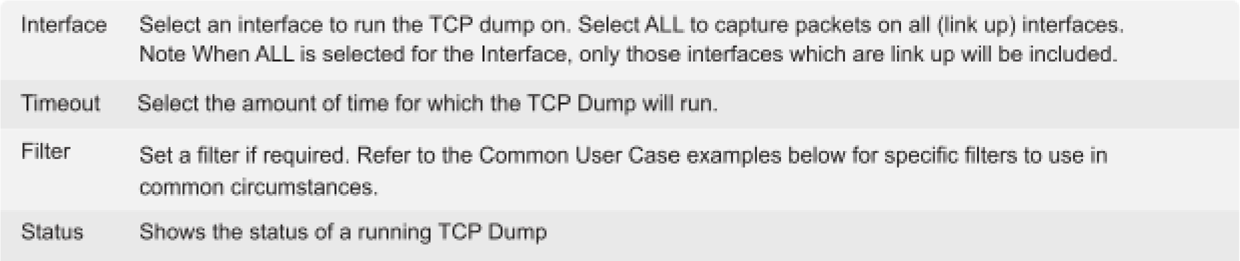
Interface: ALL

Timeout: 60 Seconds

Filter:

Status: Stopped

Make the following selections and then click Generate TCP Dumps:



Interface	Select an interface to run the TCP dump on. Select ALL to capture packets on all (link up) interfaces. Note When ALL is selected for the Interface, only those interfaces which are link up will be included.
Timeout	Select the amount of time for which the TCP Dump will run.
Filter	Set a filter if required. Refer to the Common User Case examples below for specific filters to use in common circumstances.
Status	Shows the status of a running TCP Dump

Common Use Cases

The following examples provide the syntax to enter in the Filter field to gather data from a particular source.

To collect traffic to/from a single host

`host <IP address>`

Example: `host 1.2.3.4`

To collect traffic from a single host who is the source of the traffic

`src <IP address>`

Example: `src 1.2.3.4`

To collect traffic from a single host who is the destination for the traffic

`dst <IP address>`

Example: `dst 1.2.3.4`

To collect traffic between two hosts

`host <IP address 1> and host <IP address 2>`

Example `host 1.2.3.4 and host 5.6.7.8`

To collect traffic to / from a subnet

`net <IP subnet>`

Example: `net 1.2.3.0/24`

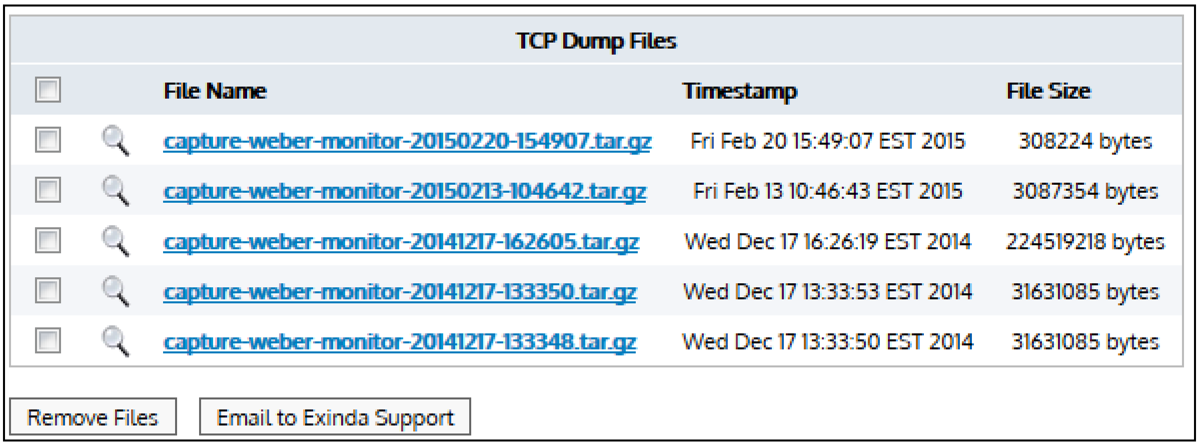
To collect traffic between two subnets

`src net <IP subnet> and dst net <IP subnet>`

Example: `src net 1.2.3.0/24 and dst net 1.2.4.0/24`

Send a TCP Dump to GFI ClearView TAC

Saved TCP Dumps can then be downloaded and/or emailed to GFI ClearView TAC using the form below.



TCP Dump Files

□		File Name	Timestamp	File Size
□	🔍	capture-weber-monitor-20150220-154907.tar.gz	Fri Feb 20 15:49:07 EST 2015	308224 bytes
□	🔍	capture-weber-monitor-20150213-104642.tar.gz	Fri Feb 13 10:46:43 EST 2015	3087354 bytes
□	🔍	capture-weber-monitor-20141217-162605.tar.gz	Wed Dec 17 16:26:19 EST 2014	224519218 bytes
□	🔍	capture-weber-monitor-20141217-133350.tar.gz	Wed Dec 17 13:33:53 EST 2014	31631085 bytes
□	🔍	capture-weber-monitor-20141217-133348.tar.gz	Wed Dec 17 13:33:50 EST 2014	31631085 bytes

For more information about TCP dump filters, refer to https://danielmiessler.com/study/tcpdump/#common.

5.1.6 View the status of an alert

System alerts notify you of any system issues that may require further attention and troubleshooting. If a system alert is raised the system health status is set to 'Warning' and an email alert is sent.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

4. Click **Configuration > System > Diagnostics**, and switch to the **System** tab. Anything that has generated alerts dis- play the last time an alert was triggered, and the total number of alerts that have been sent.

5. To view the alert that has triggered the warning, click the alarm name. Use the information in this alert to help troubleshooting the issue.

6. To remove the history for an alert, click **Reset**. The system health status is returned to OK.

Alert Name	Description
CPU Utilization	Alert raised when the CPU utilization threshold is reached. The trigger and clear thresholds can be altered. The defaults are 95% and 80% busy respectively.
System Disk Full	Alert raised when the used disk space threshold is reached. The trigger and clear thresholds can be altered. The defaults are 7% and 10% free respectively.
Memory Paging	Alert for memory use and paging. This means that the data in RAM is swapped to disk. Excessive paging alerts could indicate a system that is running low on RAM resources. Check RAM & SWAP graphs under Monitoring > System.
Link Negotiation	Alert raised when the speed/duplex on an interface is set to auto, but it is negotiating at half duplex and/or 10Mbps.

NIC Problems	Alert raised when errors are present on the interfaces.
NIC Collisions	Alert raised when collisions are present on the interfaces. The trigger and clear thresholds can be altered. The defaults are 20 and 1 per 30 sec respectively.
NIC Dropped packets	Alert raised when dropped packets are present on the interfaces.
SMB signed connections	Alert raised when SMB signed connections are present.
Redundant Power	Alert raised when one of the power supplies fails (only available on platforms with power redundancy).
Redundant Storage	Alert raised when one of the hard disks fails (only available on platforms with storage redundancy).

5.1.7 Open a case with ClearView Support Services

If you are experiencing a problem or have a question about GFI ClearView, please refer to the knowledge base or create a ticket with the customer support team using the Support Portal.

5.2 Log Files

Learn about the various log files stored on an GFI ClearView Appliance, and how you can use these logs in your efforts to troubleshoot issues that you might encounter.

5.2.1 Live Log

The Live Log page allows you to view new entries to the System Log in real-time.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.
3. Click **Login**.

5. Click **Configuration > System > Logging** and switch to the **Live Log** tab.

NOTE

A dot/period (.) character is displayed after a few seconds of inactivity to indicate the Live Log is still active.

5.2.2 Tail Log

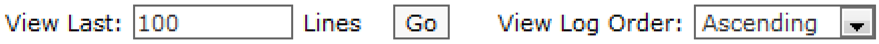
The Tail Log page allows you to view the most recent entries in the system log file.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Configuration > System > Logging** and switch to the **Tail Log** tab.

6. Configure how many lines to view and in which order to display the log entries.



View Last: 100 Lines Go View Log Order: Ascending

7. To refresh this page and ensure any new log entries since the list time this page was refreshed are displayed, click **Go**.

5.2.3 System Logging Configuration

The System Logging Configuration page allows you to customize various aspects of System Logging, including exporting to remote syslog servers.

In this area of the GFI ClearView Web UI you can:

- Configure the appliance log files
- Add a remote syslog server
- Remove a remote syslog server

Configure the appliance log files

The System Logging Configuration page allows you to customize various aspects of System Logging, including exporting to remote syslog servers.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

3. Click **Login**.

5. Click **Configuration > System > Logging** and switch to the **Setup** tab.

6. Specify the format log files should be saved in. The Standard form is usually sufficient, however some external log file parsers may prefer the log file in WELF format.

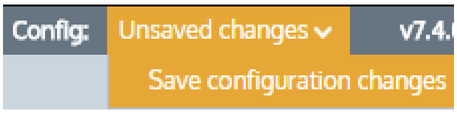
7. Select the severity level of log entries that should be saved. Any log entry with this severity level or lower will be saved to the System Log file.

8. Select when the logs are rotated. To force System Log rotation immediately, click **Force Rotation Now**.

9. Specify how many log files should be kept before they are permanently removed from the GFI ClearView appliance.

10. Click **Apply Changes**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



Add a remote syslog server

Add remote syslog servers to the GFI ClearView appliance, allowing you to forward system log entries at a defined severity level to one or more remote syslog servers.

On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

1. Key-in the **Username** and **Password**.

2. Click **Login**.

5. Click **Configuration > System > Logging** and switch to the **Setup** tab.

6. In the Add New Remote Sink area, type the Hostname or IPv4 address of the remote syslog server. IPv6 addresses are not supported for remote sinks.

7. Select the severity level of log entries that are sent to the remote syslog server. Any log entry with this severity level or lower is sent.

8. Click **Add New Remote Sink**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.

Remove a remote syslog server

To stop forwarding system log entries to a remote syslog server, remove the server from the GFI ClearView appliance.

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).

2. Key-in the **Username** and **Password**.

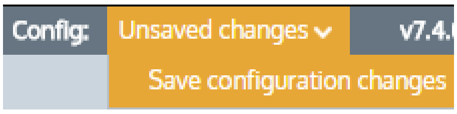
3. Click **Login**.

5. Click **Configuration > System > Logging** and switch to the **Setup** tab.

6. Select the server from the Remote Log Sinks list, and select **Remove Selected**.

7. Click **Add New Remote Sink**.

To save the changes to the configuration file, in the status bar click the Unsaved changes menu and select Save configuration changes.



Remove Events from the Appliance System Log

The BMC processor keeps a log of system events including power status, power redundancy, chassis intrusion. The following command can be used to periodically flush these events to the appliance's system log.

```
(config) # ipmi sel enable
```

5.3 Troubleshoot issues with Active Directory configuration

If you are experiencing issues with the Active Directory integration, these troubleshooting topics may help resolve the issue.

5.3.1 GFI ClearView Appliance Reboots Every Night

Problem

When multiple installations of the GFI ClearView AD Connector have the **Send Active Directoryuserand group information to GFI ClearView appliance(s) at startup** option selected, the GFI ClearView Appliance can become overwhelmed with duplicate data from the connectors, which can cause the appliance to shut down.

Solution

1. On each instance of the GFI ClearView AD Connector, check whether the **Send Active Directoryuserand group information to GFI ClearView appliance(s) at startup** option is selected.
2. If the option is selected on more than one instance, deselect the option on all GFI ClearView AD Connectors.
3. Choose one instance of the GFI ClearView AD Connector, and select the **Send Active Directoryuserand group information to GFI ClearView appliance(s) at startup** checkbox, and click **OK**.

5.3.2 WMI Service is not running

Problem

When I try to access the GFI ClearView AD Connector, a message opens that states “The installer has detected that WMI Service is not running. Consult Windows Help files to find information on how to start WMI Service.”.

Solution

This message indicates that Windows Management Information (WMI) service is disabled. The GFI ClearView AD Connector will not be able to run correctly until the WMI service is started.

To start the WMI service, at a command prompt type the following command: `net start winmgmt`

5.3.3 System account showing in traffic reports

Problem

When viewing conversations, the IP address and username of an account created for signing SMB traffic is being displayed as generating traffic rather than the actual user generating the traffic.

Solution

When SMB signing is configured and enabled, the SMB signing account is the last user account registered as using an IP address, the GFI ClearView AD Connector transfers the SMB signing account as the username that is generating the traffic. To ignore the SMB signing account and report the traffic as being generated by the actual user, configure the GFI ClearView AD Connector to ignore the SMB signing account. For more information, refer to Exclude specific usernames from reports.

5.3.4 No Communication Between the GFI ClearView AD Connector and the GFI ClearView Appliance

Problem

You see one of the following symptoms:

- A connection cannot be established between the GFI ClearView AD Connector and the GFI ClearView Appliance.
- The Last Contact status on the **Configuration > System > Network> Active Directory** tab is blank or red.

Resolution

1. Ensure your firewall allows incoming and outgoing traffic on the port configured for the GFI ClearView Appliance to com- municate with the GFI ClearView AD Connector

5.3.5 GFI ClearView AD Connector stops running

Problem

At times after restarting the GFI ClearView AD Connector or the GFI ClearView AD service, the GFI ClearView AD Connector does not continue running, and requires constant restarts.

Solution

To fix this:

1. The GFI ClearView AD Connector requires .NET version 4.0 for it to run successfully on a server other than the Active Directory server. Ensure .NET 4.0 or later is installed on the server running the GFI ClearView AD Connector.

2. If the Active Directory server is running Windows 2003 R2, ensure the GFI ClearView AD Connector is installed directly on the Active Directory server.

3. Review your event logs for .NET RunTime errors, and attempt to resolve those errors. The .NET installation may need to be reinstalled and the .NET 4.0 services and other environmental services such as WMI may need to be updated.

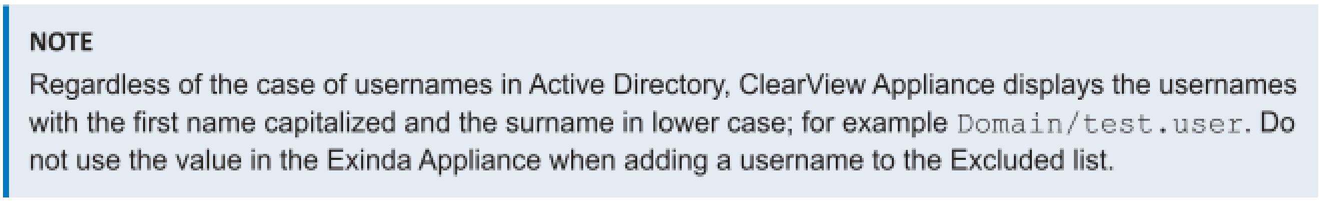
5.3.6 Excluded Users Still Appear on the GFI ClearView Appliance

Problem

Even though a user name has been added to the Excluded list on the GFI ClearView AD Connector, the username continues to appear associated with traffic on the GFI ClearView Appliance.

Solution

1. Verify that the username on the Excluded tab of the GFI ClearView AD Connector matches the username in Active Directory. The username is case sensitive. For example, if the Active Directory has the user `Domain/Test.User`, and the excluded list has the user as `Domain/test.user`, the traffic is not excluded.



NOTE

Regardless of the case of usernames in Active Directory, ClearView Appliance displays the usernames with the first name capitalized and the surname in lower case; for example `Domain/test.user`. Do not use the value in the Exinda Appliance when adding a username to the Excluded list.

2. If the case matches on the usernames, restart the AD Client Service and renumerate the GFI ClearView Appliance.

5.3.7 Changes to the GFI ClearView Active Directory Controller have no effect

Problem

After making changes to the configuration of the GFI ClearView Active Directory Controller, the information reported on the GFI ClearView Appliance appears to be the same as before the changes.

Solution

Restart the AD Client Service and renumerate the GFI ClearView Appliance to ensure the latest configuration is being used.

5.3.8 The IP addresses are not being mapped to the AD users and groups

Problem

When integrating the AD client with the GFI ClearView appliance, the IP addresses are not being mapped to the users and groups on the GFI ClearView appliance.

Solution

Logon auditing must be enabled for IP address to be mapped to the users.

You can investigate by verifying whether the domain controller is logging particular event IDs. If these events are absent then you will need to enable logon auditing.

In the Domain Controller, go to **Event Viewer > Windows Logs> Security Logs**.

- For Windows Server 2008, 2008 R2, 2012, and 2012 R2, you should see Event ID

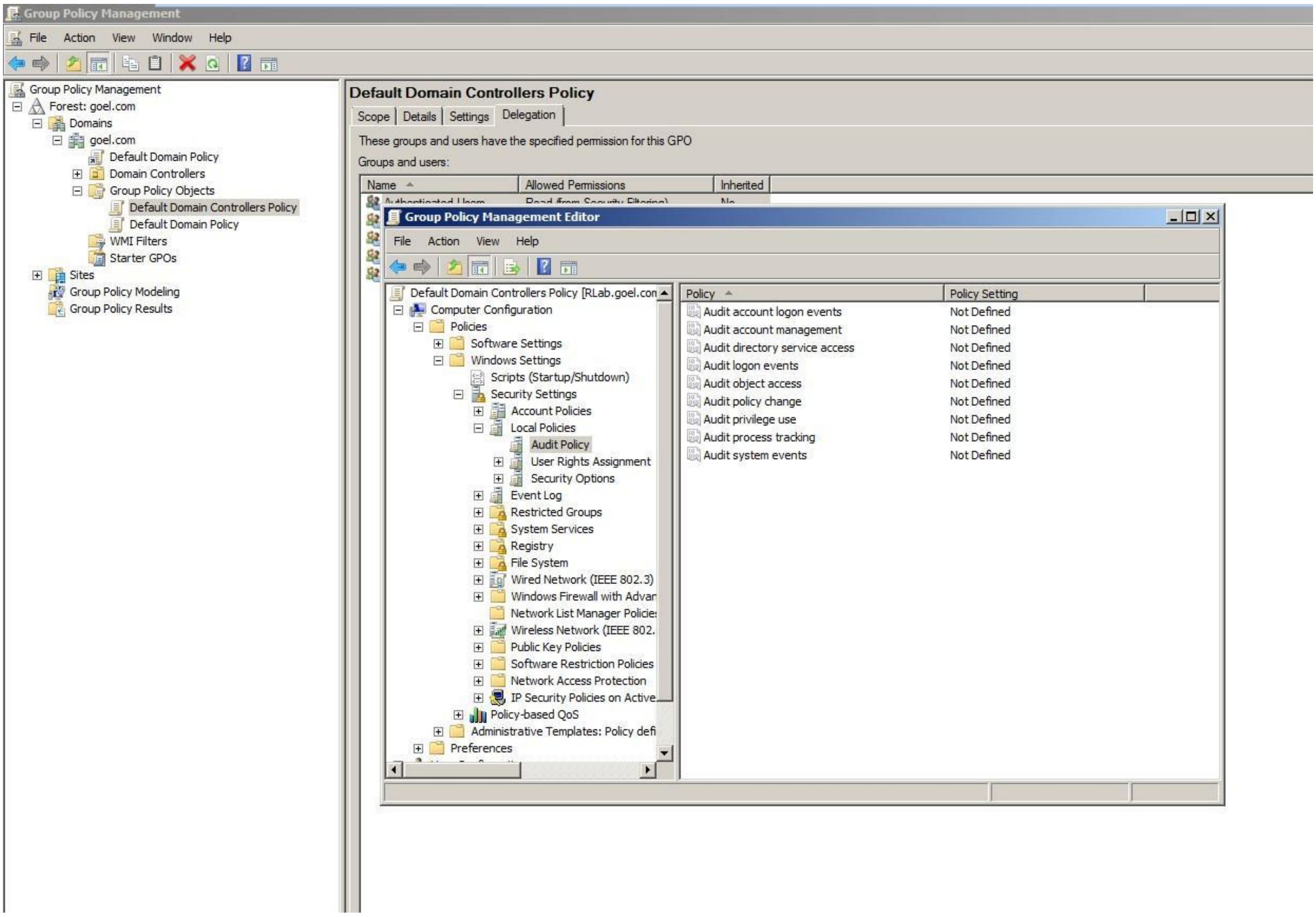
#4624

- For Windows Server 2003, 2003 R2, you should see Event ID #528 and 540.

If the Domain Controller is not logging these events, then you need to enable **logon auditing** on the domain controller and renumerate the AD client on the GFI ClearView appliance.

1. In the Domain Controller, go to **Start menu > Administrative Tools> Group Policy Management Snap-in**.

2. In the Group Policy Management tree, go to your domain, expand the **Group Policy Objects** node, and select **Default Domain Controllers Policy.**



These groups and users have the specified permission for this GPO

Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

3. Right click on **Default Domain Controllers Policy** and select **Edit** from the context menu.

4. In the **Group Policy Management Editor** dialog box, expand the tree and select **Computer Configuration > Policies> Windows Settings> Security Settings> Local Policies> Audit Policy**.

5. In the policy list on the right, click on **Audit logon events** and ensure that **Success** is checked.

6. On the GFI ClearView appliance, go to **Configuration > System > Network> Active Directory**.

7. Click the **Renumerate** button.

8. Apply the changes by executing the following command using a CMD console in the Domain Controller: `gpup- date /force`

6 ClearView Command Line Interface (CLI)

Learn how to use the GFI ClearView Command Line Interface (CLI).

6.1 Using the Command Line Interface

Many of the actions available in the GFI ClearView Web UI can also be executed through the Command Line Interface (CLI).

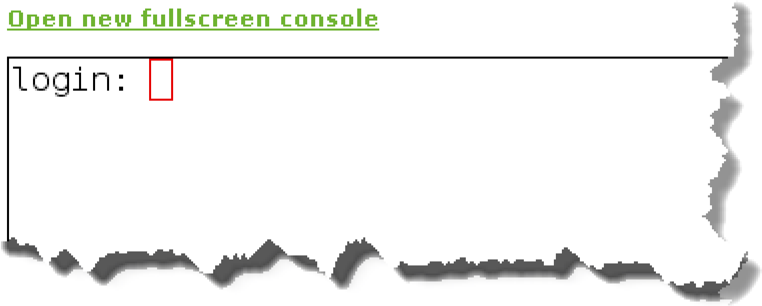
> TIP
>
> » Auto complete is available by pressing the tab key after typing the first several letters of a command. Use the tab key to view available options for any of the commands.
>
> » Use `?` at the end of a command to view available options and descriptions.
>
> » Command history is available by using the up and down arrow keys. Command line editing is available, using the left and right keys to navigate.
>
> » Use **ctrl-w** to delete from the cursor to start of line.

6.1.1 Accessing the Command Line Interface

There are four ways of accessing the GFI ClearView CLI (in order of preference):

1. Secure Shell (SSH) (recommended)
2. GFI ClearView Web UI
3. Telnet
4. Serial Console Interface

Use this tool to connect to the GFI ClearView appliance's Command Line Interface (CLI) from the Web UI. This tool connects to the appliance via the web interface and does not require SSH access.



```
login:
```

1. On your browser, open the GFI ClearView Web UI (`https://ClearView_IP_address`).
2. Key-in the **User Name** and **Password**.
3. Click **Login**.
4. Click Configuration > System > Tools> Console.
5. Type the appliance username and password at the prompts. Do one of the following:

   - To enter privileged EXEC (enable) mode, at the prompt run the command: `hostname > enable`

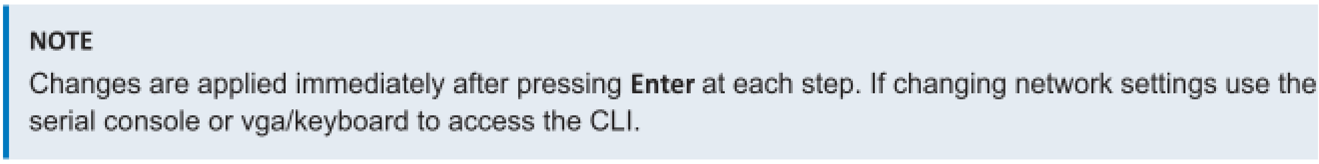
   The `hostname #` prompt appears.

   - To enter configuration (config) mode, at the prompt run the commands: `hostname # configure terminal`

The `hostname (config)#` prompt appears.

6.1.2 CLI Configuration Jumpstart

When you login to the CLI for the first time, you are presented with the option to run the CLI jump-start wizard. This is a guided wizard that helps with the initial configuration of the GFI ClearView appliance.



NOTE

Changes are applied immediately after pressing **Enter** at each step. If changing network settings use the serial console or vga/keyboard to access the CLI.

1. `Enable IPv6?` - These questions allow you to enable IPv6 support for the entire system. If your network supports IPv6 then type 'Y', otherwise type 'N'.

2. `Enable IPv6 autoconfig (SLAAC) on eth1 interface?` - If you enable IPv6, you have the option of enabling IPv6 SLAAC autoconfiguration. Type 'Y' if you wish to have an address and netmask automatically con- figured and your network supports this option.

3. `Use eth0 for management access. Note: This disables br0 (Y/N)?` - Select whether to use eth0 for accessing management functionality.

4. `Use DHCP on eth1 (Y/N)?` - This question is asking if you want to use DHCP for automatically acquiring IP connectivity settings. If you specify 'N' here, you will be prompted to type static IP connectivity settings, such as IP address and netmask, default gateway and DNS servers.

5. `Enable br10 (Y/N)?` and `Use DHCP on br10 (Y/N)?` - For GFI ClearView, select ‘N’. These questions allow you to enable bridges and optionally configure an address manually or by using DHCP.

6. `br2 IP address and netmask? [192.168.2.254/24]` - For GFI ClearView, select ‘N’. Configure the IP address and netmask for the bridge.

7. `Hostname?` - This question is asking you to configure a hostname for the appliance.

8. `SMTP server address?` - In order to receive system alerts and reports, the GFI ClearView appliance requires an SMTP server be configured so that emails can be sent.

9. `An email address for reports and alerts?` - If you wish to receive system alerts and reports, type an email address here.

10. `Admin password (Enter to leave unchanged):` - This question is asking you if you wish to change the password of the GFI ClearView appliance's 'admin' account. Press 'Enter' to leave the password unchanged or enter a new password and you'll be asked to re-enter the password again to confirm.

11. `Do you want to configure the interface speed and duplex settings? (Y/N)?` - Enter 'Y' if you wish to configure interface settings or 'N' to leave them unchanged. If you entered 'Y', these questions will step through each interface on the GFI ClearView appliance and ask for interface speed and duplex settings.

```
What is the speed of eth1 (auto, 10 or 100):

What is the duplex mode of eth1 (auto, full or half):

What is the speed of eth2 (auto, 10 or 100):
```

```
What is the duplex mode of eth2 (auto, full or half):
```

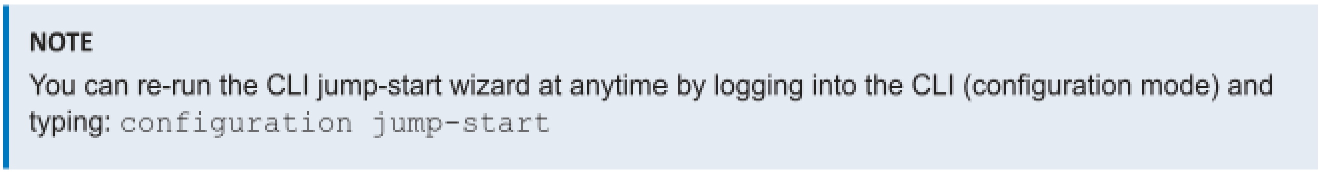
12. `Do you want to change HTTP proxy settings (Y/N)?` - If you enter Y, these questions step through the parameters of the HTTP Proxy setup.

```
HTTP proxy address (0.0.0.0 to
disable)? HTTP proxy port? [3128]
HTTP proxy authentication type (N)one or (B)asic
(N/B)? Allow insecure (unverified certificate) SSL
(Y/N)?
```

13. `Do you want to check for a new license online (Y/N)?` - Enter 'Y' to have the GFI ClearView appliance check for a newer license on the GFI ClearView website (if the GFI ClearView appliance has Internet connectivity). If a newer license is found, you will be asked if you wish to install it. If you enter 'N', you will be prompted for a license key.

14. `Do you want to configure optimization policies (Y/N):` - Answer with ‘N’ here.

15. `Check for new firmware (Y/N)?` - Answering 'Y' here will make the GFI ClearView appliance check for a newer firmware version on the GFI ClearView website (if the GFI ClearView appliance has Internet connectivity). If a newer firmware image is found, you will be asked if you want to download and install it.



NOTE

You can re-run the CLI jump-start wizard at anytime by logging into the CLI (configuration mode) and typing: `configuration jump-start`

6.1.3 Configure command line options

Configure the command line interface to meet your needs.

1. Use the following command to set the terminal character width and number of lines:

```
hostname (config)# cli session terminal width <number of
characters> hostname (config)# cli session terminal length
<number of lines>
```

2. Auto logout is enabled by default. To change the auto logout time use the following command:

```
hostname (config)# cli default auto-logout <minutes>
```

To disable auto-logout, set the minutes to `0`.

3. To enable or disable paging use the following command:

```
hostname (config)# [no] cli default paging enable
```

4. Use the `show cli` command to see current CLI settings.

5. To save the running configuration, type `configuration write`.

7 Copyright

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of their respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

7.1 GFI ClearView End User License Agreement (EULA)

NOTICE TO USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT. USE OF THE SOFTWARE PROVIDED WITH THIS AGREEMENT ("SOFTWARE") CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE COMPLETE SOFTWARE PACKAGE (AND ANY OTHER DEVICES DELIVERED WITH THIS PACKAGE) TO THE DEALER FROM WHOM YOU OBTAINED THIS PRODUCT FOR A FULL REFUND. IF YOU HAVE ANY QUESTIONS CONCERNING THIS AGREEMENT CONTACT GFI USA, LLC, 2028 E BEN WHITE BLVD, SUITE 240-2650 AUSTIN, TX 78741 OR BY EMAIL: LEGAL@GFI.COM.

1. LICENSE GRANT: The SOFTWARE is licensed, not sold. Upon the valid purchase of a license to the SOFTWARE and except as otherwise specified in an accompanying license summary, invoice, or other documents evidencing the purchase of the software license, GFI USA, LLC ("GFI"), grants you a non-exclusive, non-transferable license to use the SOFTWARE during the subscription period on servers connected to a maximum number of user computers not exceeding the number of user computers specified in the packaging accompanying the SOFTWARE or in any Supplemental Agreements. This license to use the SOFTWARE is conditioned upon your compliance with the terms of this Agreement. You agree you will only compile the SOFTWARE into any machine-readable or printed form as necessary to use it in accordance with this license or for backup purposes in support of your use of the SOFTWARE. This license is effective until terminated when the subscription period has ended. GFI has the option to terminate this Agreement if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the SOFTWARE together with all copies of the SOFTWARE.

2. REVERSE ENGINEERING. You may not reverse engineer, decompile, modify or disassemble the SOFTWARE in whole or in part.

3. COPYRIGHT: All title and copyrights in and to the SOFTWARE, and accompanying printed materials are owned by GFI. The SOFTWARE is protected by copyright laws and International treaty provisions. The SOFTWARE is Copyright (c) 2002-2023 GFI USA, LLC., All rights reserved. The software remains the sole and exclusive property of GFI at all times.

4. LIMITED WARRANTY: GFI warrants that for a period of thirty (30) days from the date of shipment from GFI: (i) the SOFTWARE will be free of defects in workmanship under normal use, and (ii) the Software substantially conforms to its published specifications. Except as expressly granted in this Agreement the SOFTWARE is provided AS IS. In no event shall GFI or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this SOFTWARE, even if GFI has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

5. NO OTHER WARRANTIES. GFI DOES NOT WARRANT THAT THE SOFTWARE IS ERROR FREE. EXCEPT FOR THE "LIMITED WARRANTY" IN SECTION 4 ("LIMITED WARRANTY), GFI DISCLAIMS ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED. INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY MAY LAST OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

6. SEVERABILITY: In the event of invalidity of any provision of this license, the parties agree that such invalidity shall not affect the validity of the remaining portions of this license.

7. APPLICABLE LAW. The laws of the State of Texas will govern this license. In the event of any dispute arising out of this Agreement the parties hereby agree to submit to the jurisdiction of the courts of the State of Texas.

8. ENTIRE AGREEMENT: This is the entire agreement between you and GFI, which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

7.2 GNU General Public License (GPL)

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

7.2.1 Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public

License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

7.2.1 TERMS AND CONDITIONS

Definitions

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities.
However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a. The work must carry prominent notices stating that you modified it, and giving a relevant date.

b. The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c. You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d. If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accom- panied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b. Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accom- panied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for soft- ware interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c. Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and non-commercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d. Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e. Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accordance with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a. Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b. Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c. Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d. Limiting the use for publicity purposes of names of licensors or authors of the material; or

e. Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f. Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or
(2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to simultaneously satisfy your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

There is no warranty for the program, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide the program “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the program is with you. Should the program prove defective, you assume the cost of all necessary servicing, repair or correction.

16. Limitation of Liability.

in no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who modifies and/or conveys the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

7.3 BSD 2.0

The BSD 2.0 License

Copyright (c) 2009 Kontron America, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following dis- claimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. Neither the name of Kontron, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by the copyright holders and contributors "as is" and any express or implied warranties, including, but not limited to, the implied Warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright owner or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Software, even if advised of the possibility of such damage.