Exinda User Manual

Exinda ExOS Version 6.3

Table of Contents

Part

1 Introduction

Exinda User Manual

Exinda Firmware Version: 6.3

1.1 Using This Manual

This user manual provides detailed instructions on how to use the Exinda appliance. Specific instructions are given for the configuration and use of the device.

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

1.2 Product Family

The Exinda appliance product family is outlined below:

Exinda 2061 (1RU):

Exinda 4061 (1RU):

Exinda 6060 (1RU):

Exinda 8060 (2RU):

Exinda 10060 (2RU):

Each product is available with either a x700 or x800 license (except the 1060, which is only available as an x700).

x700	Includes monitoring, reporting, optimization (bandwidth management and QoS).
x800	Includes all x700 features plus Application Acceleration.

The following table shows how the product naming convention and licensing works.

Series	Software License	Hardware Version	Hardware Version	BW Opt OR BW Accel / BW Opt
6	7	6	0	45

Series	Software License	Hardware Version	Hardware Version	BW Opt OR BW Accel / BW Opt
8	8	6	0	100 / 500

Example 1: 6760-45
- Series: 6000
- License: x700 (visibility and QoS control)
- HW Version: 60 hardware platform
- Bandwidth: 45Mbps for visibility and QoS

Example 2: 8860-100/500
- Series: 8000
- License: x800 (visibility, QoS control and acceleration)
- HW Version: 60 hardware platform
- Bandwidth: 100Mbps for acceleration and 500Mbps for visibility and QoS

1.3 Further Reading

In addition to this User Manual, the following additional user documentation is available:

- Exinda Quick Start Guides
- Exinda CLI Reference Guide
- Exinda Topologies Guide
- Exinda "How To" Guides
- Exinda Applications List

Please visit http://www.exinda.com for more information.

1.4 Safety and Compliance

Note: This safety and compliance information only applies to 2x61 appliances.

Compliance

Safety Guidelines

EMC Notice

1.4.1 Compliance

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure.

In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

1.4.2 Safety Guidelines

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

LITHIUM BATTERY CAUTION:

Risk of Explosion if Battery is replaced by an incorrect type. Dispose of used batteries according to the instructions

Operating Safety

Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.

Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.

Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

1.4.3 EMC Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

Part II

2 License

Please find below the End User License Agreement (EULA). This agreement must be accepted before logging into the Exinda appliance for the first time and prior to installing a new firmware update.

Portions of software within the Exinda appliance use Open Source licensing such as the GPL. We are required to provide a copy of these licenses (Appendix D) and in some cases make the software packages available.

For a copy of the GPL licensed software packages used in the Exinda appliance, please contact support@exinda.com and request a GPL CD. Shipping and handling charges may apply.

2.1 End User License Agreement (EULA)

Exinda Networks Pty Ltd, 13 Harper Street, Abbotsford, Victoria, 3067, Australia www.exinda.com EXINDA NETWORKS PTY LTD

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 QUESTION CONCERNING THIS AGREEMENT CONTACT Exinda Networks, 13 Harper Street, Abbotsford, Victoria, 3067, Australia OR by email: legal@exinda.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, Exinda Networks Pty Ltd ("EXINDA"), 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. You may terminate it at any point by destroying the SOFTWARE together with all copies of the SOFTWARE. EXINDA 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 EXINDA. The SOFTWARE is protected by copyright laws and International treaty provisions. The SOFTWARE is Copyright (C) 2002 Exinda Networks Pty Ltd, Australia, All rights reserved. The software remains the sole and exclusive property of EXINDA at all times.

4. LIMITED WARRANTY: EXINDA warrants that for a period of thirty (30) days from the date of shipment from EXINDA: (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 EXINDA, or any of its affiliates, subsidiaries or suppliers (each an "EXINDA Party" and together the "EXINDA Parties") 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 such EXINDA Party 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.

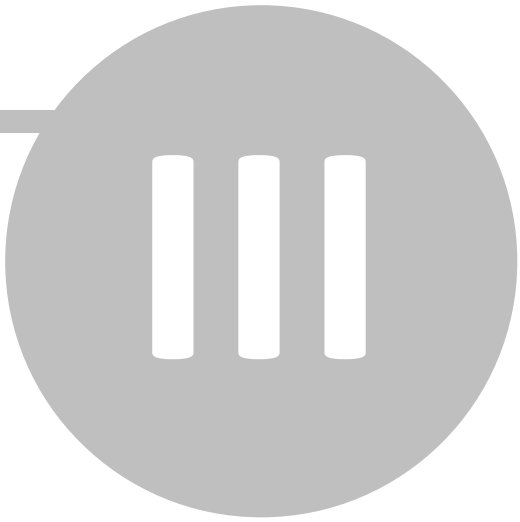
5. NO OTHER WARRANTIES: NONE OF THE EXINDA PARTIES WARRANT THAT THE SOFTWARE IS ERROR FREE. EXCEPT FOR THE "LIMITED WARRANTY" IN SECTION 4 ("LIMITED WARRANTY"), THE EXINDA PARTIES DISCLAIM ALL OTHER WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED. INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATION 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 WHICH 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: This license will be governed by the laws of the State of Victoria, Australia. 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 Victoria, Australia.

8. ENTIRE AGREEMENT: This is the entire agreement between you and EXINDA which supersedes any prior agreement or understanding, whether written or oral, relating to the subject matter of this license.

Part



3 Installation and Deployment

This chapter is designed to assist first-time users in deployment and configuration of the Exinda appliance.

3.1 Package Contents

Package contents varies slightly depending on model. In general, the following items are included:

- Exinda Appliance
- Quick Start Guide
- AC Power Cable
- Straight CAT5 Ethernet Cable (usually blue)
- Cross CAT5 Ethernet Cable (usually red)
- Serial Console Cable

3.2 Pre-Installation Checklist

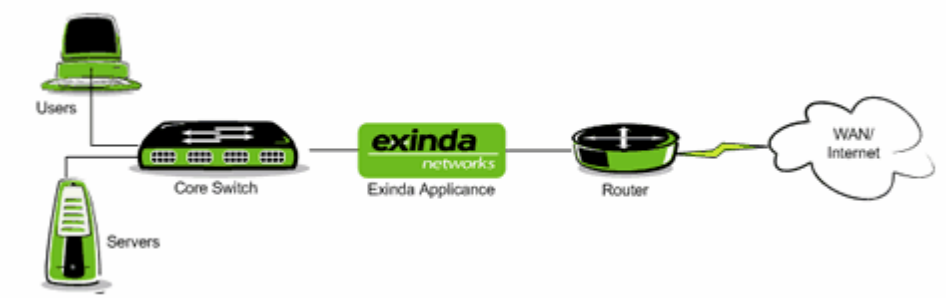
Before deploying the Exinda appliance, it is recommended that the following basic information is collected:

Host Name	Specify a host name to assign to the Exinda appliance.
Ethernet Negotiation Settings	Any Ethernet negotiation settings - does any equipment that the Exinda appliance will be connected to require and hard-coded Ethernet speed and/or duplex settings?
IP Address and Netmask	An available IP address and netmask is required.
Default Gateway	The default gateway is required.
DNS Server(s)	At least 1 DNS server is required, so that the Exinda appliance can resolve hostnames.
SMTP Server	An SMTP server needs to be specified, if you wish to receive e-mail notifications from the Exinda appliance.
Time Zone	The Exinda appliance's time zone should be correctly set.

These settings will be configured during the initial stages of deployment.

3.3 Deployment

Typically, Exinda appliances are deployed in-line, between the core switch and the WAN/ Internet router:



All models come with at least 1 hardware bypass port pair, marked LAN and WAN. These ports are designed to fail-over to pass-though mode in the event of system failure or loss of power.

Exinda appliances should be deployed with the appliance powered off. This will ensure hardware bypass is working correctly. Usually, the Exinda appliance's WAN port is cabled to the WAN/Internet router using the supplied cross-over Ethernet cable. The Exinda appliance's LAN port is cabled to the core switch using the supplied straight Ethernet cable. If your appliance has a dedicated management port, this will also need to be cabled to an internal switch using an Ethernet cable. For specific information about your model, see the supplied Quick Start Guide.

Once all Ethernet cables are in place, ensure there is still network connectivity with the Exinda appliance powered off. Then, power on the Exinda appliance. Again, ensure there is network connectivity after the appliance has booted.

Note: There may be a short interruption to network connectivity while the Exinda appliance switches out of bypass mode during boot-up. Although switching in and out of bypass takes less than 1 millisecond, this may force neighboring equipment to renegotiate their layer 2 topology, which may take several seconds.

Troubleshooting:

Q. *My network traffic is blocked after deploying the Exinda appliance in-line.*
A. Ensure you have used the correct cables for your environment. Some environments may require 2x straight Ethernet cables, while others may require 2x cross-over Ethernet cables.

Q. *My network traffic is blocked after deploying the Exinda appliance in-line, after i have booted it up.*
A. Ensure the speed/duplex settings are correct on both the Exinda appliance and any neighboring equipment.

Q. *I am experiencing significant packet loss after deploying the Exinda appliance in-line, after i have booted it up.*
A. See above regarding speed/duplex configuration. Also check Ethernet cables for defects.

Note: For further information, including additional topology examples, consult the Exinda Topologies Guide.

3.4 Acessing the Appliance

There are 2 ways to access the appliance:

- Command Line Interface (CLI)
- Web User Interface (Web UI)

By default, the Exinda appliance will attempt to automatically obtain an IP address on it's management interface using DHCP. Unless a valid DHCP address is obtained, the appliance will be assigned a default IP address of 172.14.1.57. If DHCP is unavailable or fails, you will need to change the IP address on your PC to 172.14.1.X in order to connect to the Exinda appliance on it's default IP.

If DHCP is available, you will need to know the IP address that has been assigned to the appliance (unless physically accessing the appliance with a monitor/keyboard or serial console). A convenient way to determine the appliance's IP is to visit the www.findmyexinda.com website. This site loads a small Java client that interrogates your local LAN, looking for Exinda appliances.

By default, there are 2 predefined user accounts:

Username	Default Password	Privileges
admin	exinda	read-write
monitor	exinda	read-only

When logging into the appliance for the first time using either method, you will be required to accept the End User License Agreement (EULA) before continuing.

3.4.1 Command Line Interface (CLI)

There are 4 ways to access the Command Line Interface (CLI):

- VGA Monitor / USB Keyboard
- Serial Console
- Secure Shell (SSH)
- Telnet (disabled by default)

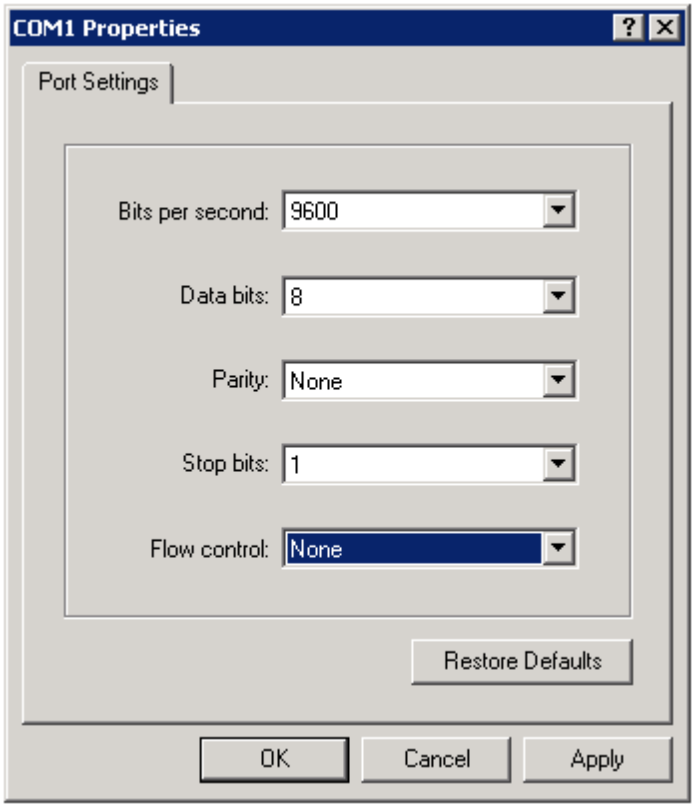
Monitor and Keyboard

It is possible to access the CLI directly by plugging in a VGA monitor and USB keyboard into the appliance itself.

Serial Console

Using a serial console, you can connect to the CLI without network connectivity. You'll need to connect a PC with a serial port (or a USB to serial adaptor) to the Exinda appliance's serial port using the supplied serial console cable. Then, using a suitable client, such as Hyper Terminal on Windows XP, you can connect to the CLI.

Use the following settings when defining a serial console connection to an Exinda appliance:



Secure Shell (SSH)

A SSH client is required to access the appliance. PuTTY is a good, free SSH client that can be used.

Using a SSH client, connect to the IP of the Exinda appliance. By default, the Exinda's SSH server runs on the default SSH port, 22.

Telnet

To enable Telnet access, navigate to the System | Setup | Access page on the Web UI, advanced mode.

Using a telnet client, connect to the IP of the Exinda appliance. By default, the Exinda's telnet server runs on the default telnet port, 23.

Note: For more information about configuring the appliance using the CLI, consult the CLI Reference Guide.

3.4.2 Web User Interface (Web UI)

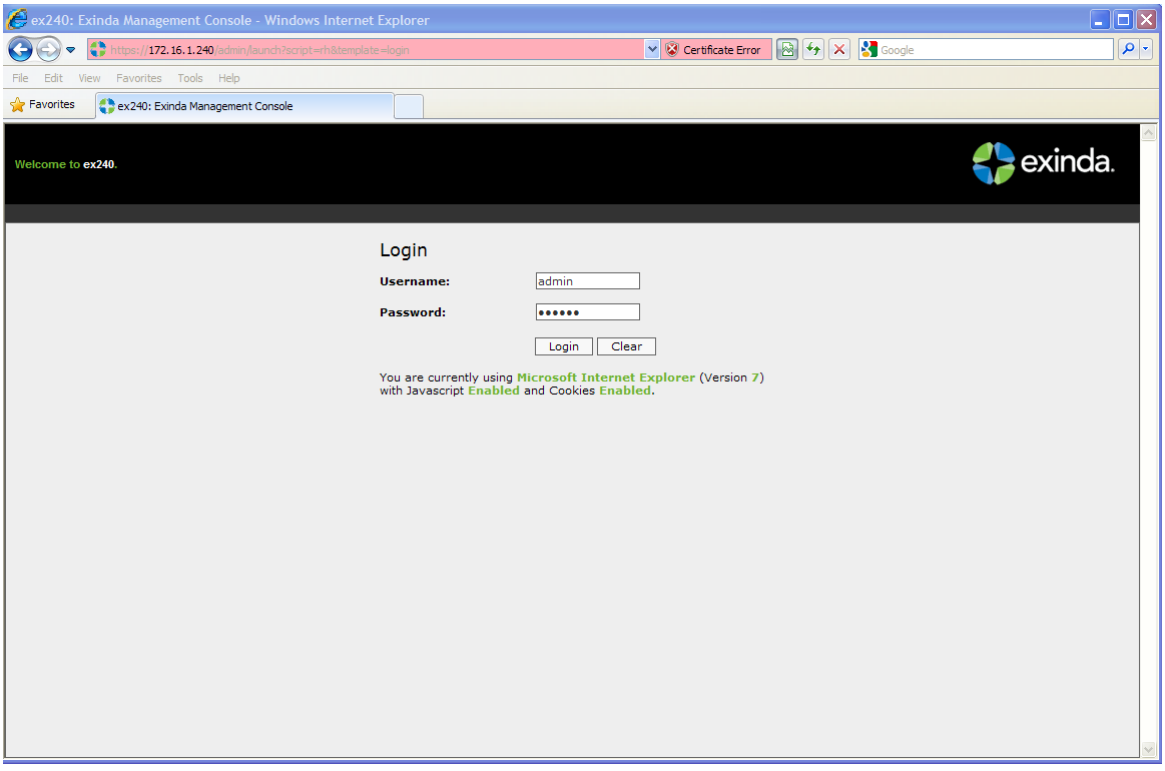
Access to the Exinda appliance's Web UI is available via a compatible Web browser. Currently, the following browsers are supported:

- Windows Internet Explorer 7 or 8
- Mozilla Firefox 3.x

By default, only https access to the appliance is enabled. You'll need to enter the following address into your browser's address bar in order to connect to the appliance:

https://<IP address of appliance>

After accepting the default security certificate, you will presented with the login screen.



The first time you access the Web UI, you will enter 'basic' mode. This mode allows you to view the appliance dashboards as well as complete the initial configuration wizard. You can also switch to 'advanced' mode, which will present you with the full user interface. The next time you login, you will enter the mode chosen last. You can always switch modes after you have logged in.

Note: To enable regular http access, navigate to the System | Setup | Access page on the Web UI, advanced mode.

3.5 Initial Configuration

When you login to the CLI or Web UI for the first time, you will be presented with an option to run a configuration wizard in order to assist with initial setup.

3.5.1 CLI Configuration Jumpstart

When you login to the CLI for the first time, you will be presented with the option to run the CLI jump-start wizard. This is a guided wizard that will help with the initial configuration of the Exinda 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.

```
Enable IPv6?

Enable IPv6 autoconfig (SLAAC) on eth1 interface?
```

These questions allow you to enable IPv6 support for the entire system. If your network supports IPv6 then enter 'Y', otherwise enter 'N'. If you enable IPv6, you have the option of enabling IPv6 SLAAC autoconfiguration. Enter 'Y' if you wish to have an address and netmask automatically configured and your network supports this option.

```
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 enter static IP connectivity settings, such as IP address and netmask, default gateway and DNS servers.

```
Enable br10 (Y/N)?

Use DHCP on br10 (Y/N)?
```

These questions allow you to enable bridges and optionally configure an address manually or by using DHCP.

```
Hostname?
```

This question is asking you to configure a hostname for the appliance.

```
Enter SMTP server address:
```

In order to receive system alerts and reports, the Exinda appliance requires an SMTP server be configured so that emails can be sent.

```
Enter an email address for reports and alerts:
```

If you wish to receive system alerts and reports, enter an email address here.

```
Admin password (Enter to leave unchanged): (unchanged)
```

This question is asking you if you wish to change the password of the Exinda 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.

```
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.

```
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):
```

If you entered 'Y', these questions will step through each interface on the Exinda appliance and ask for interface speed and duplex settings.

```
Do you want to check for a new license online (Y/N):
```

Enter 'Y' to have the Exinda appliance check for a newer license on the Exinda website (if the Exinda 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.

```
Do you want to configure optimization policies (Y/N):
```

Answering 'Y' here will take you through a text-based version of the Optimizer Wizard. For more information about the Optimizer policy wizard, see the Optimizer | Optimizer Wizard page.

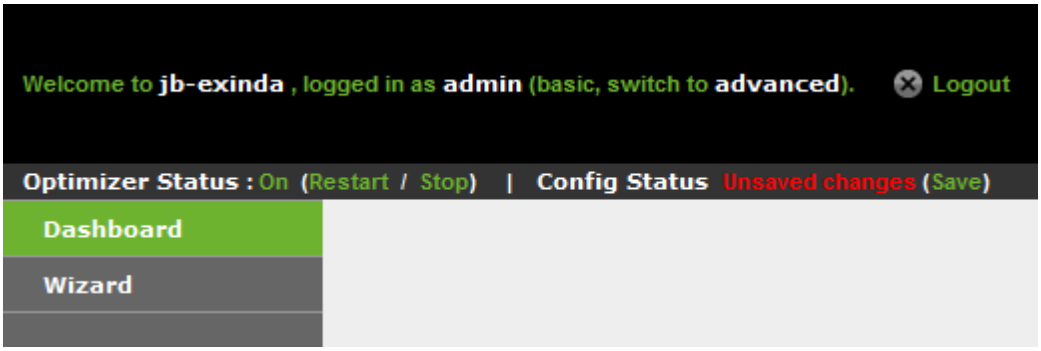
```
Check for new firmware (Y/N):
```

Answering 'Y' here will make the Exinda appliance check for a newer firmware version on the Exinda website (if the Exinda 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`

3.5.2 Web UI Basic Wizard

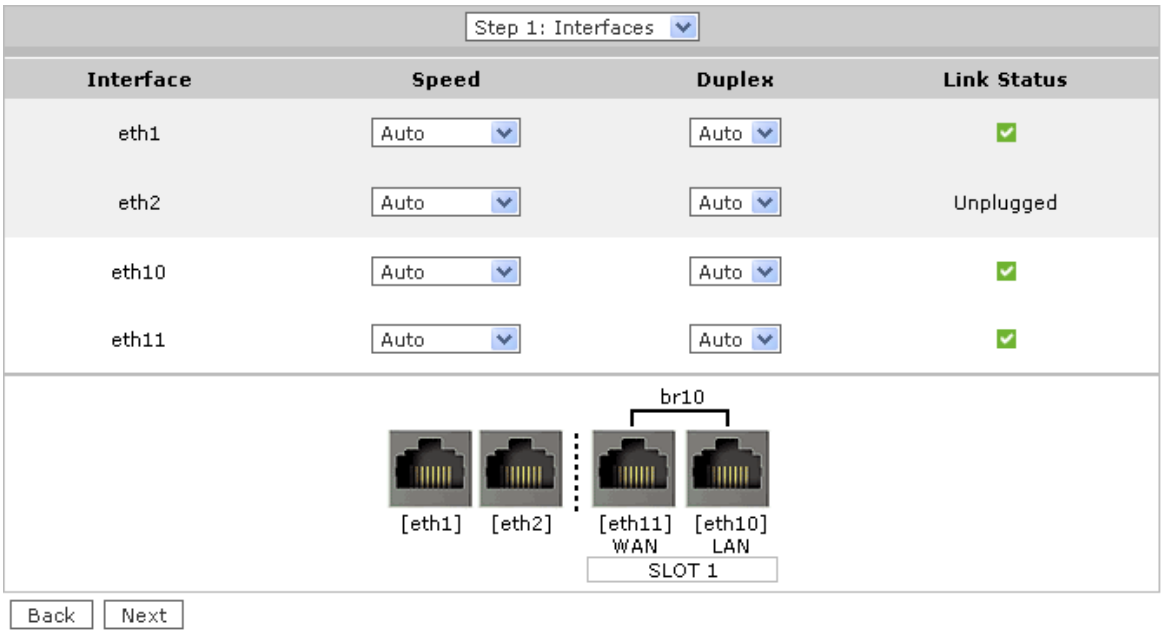
When you login to the Web UI for the first time, you will enter the 'basic' mode. In this mode, you have access to the appliance dashboards as well as the initial configuration wizard.



To access the wizard, click on the 'Wizard' link on the left-hand-side menu. The wizard will assist you to get the appliance up and running in 6 steps:

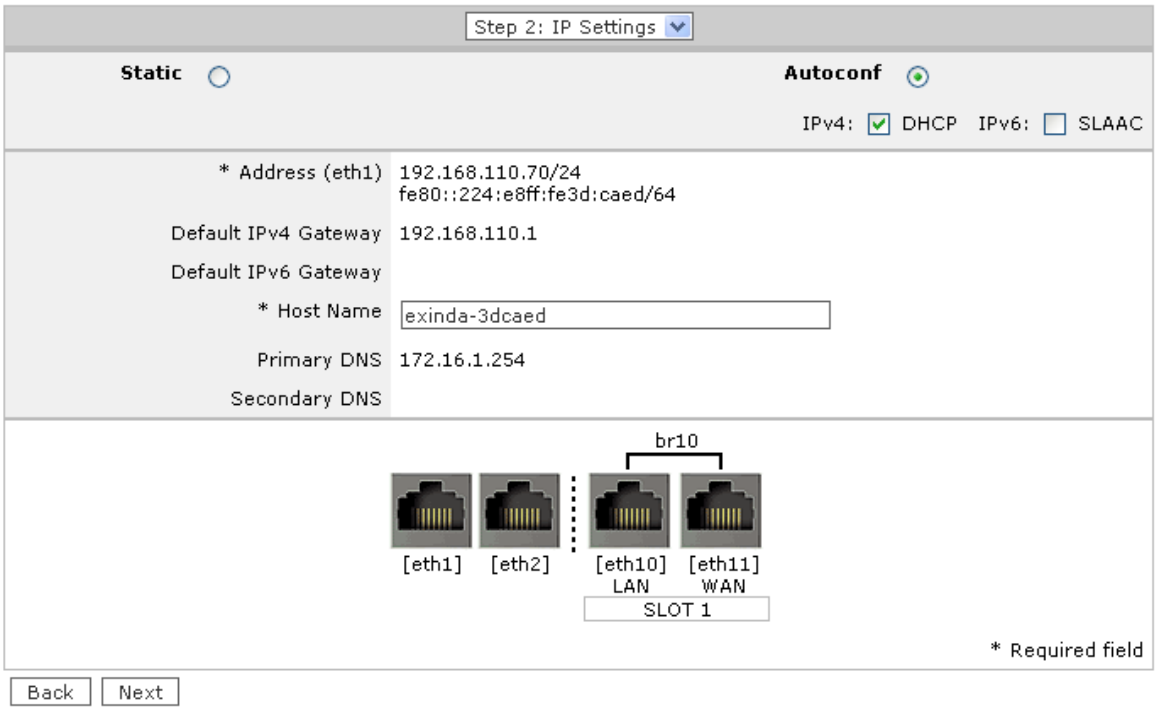
Step 1: Interfaces

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.



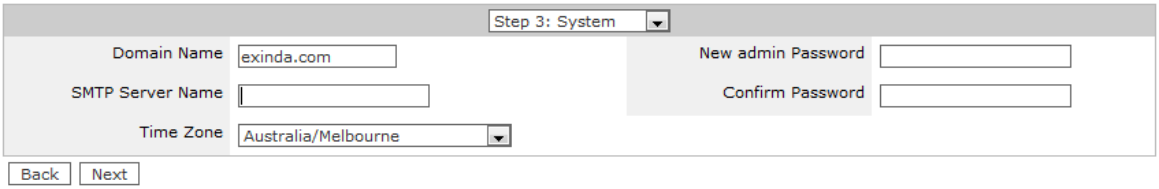
Step 2: IP Settings

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 will depend on your network. For IPv4 networks select DHCP, for IPv6 use SLAAC.



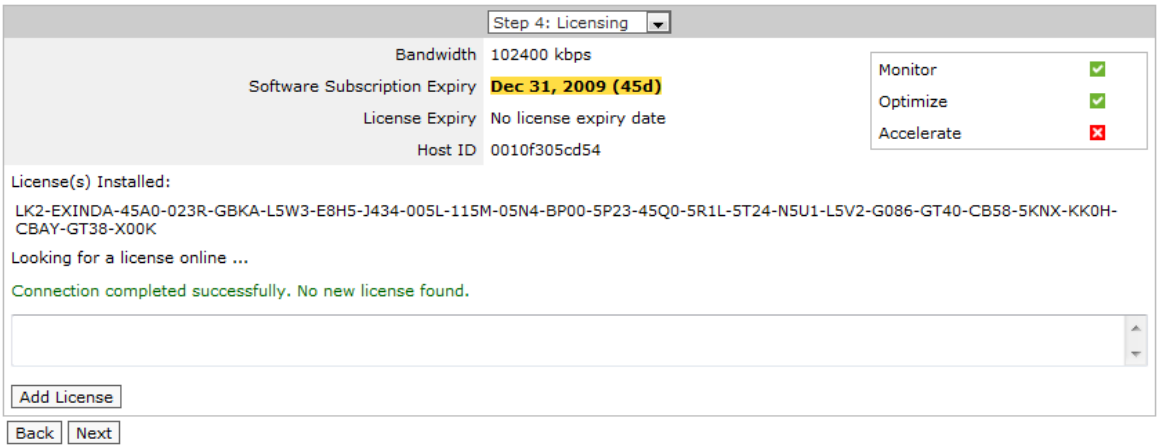
Step 3: System

This screen allows to configure basic system settings.



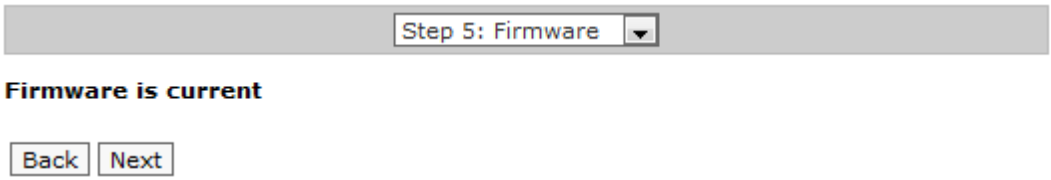
Step 4: Licensing

This screen allows you to configure the system's license. When you enter the screen, the Exinda appliance will attempt to contact the Exinda licensing server on the Internet. If the appliance has Internet connectivity and a new or updated license can be found, it will be displayed in the text-box at the bottom of the screen. You can add this license to the system by clicking the 'Add License' button.



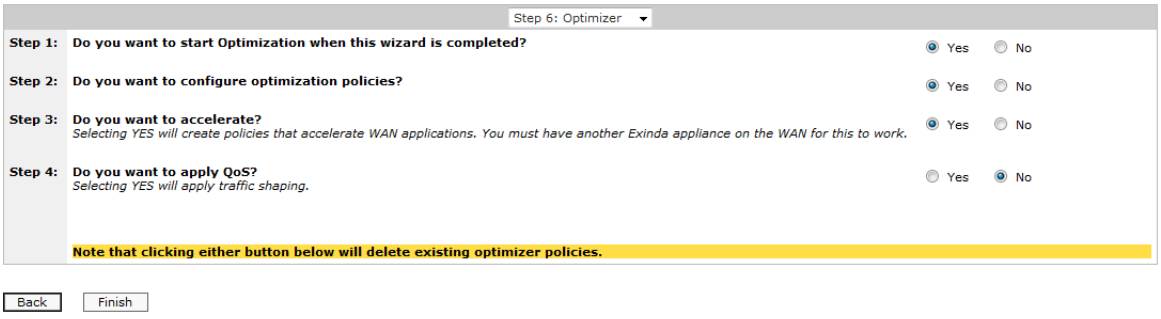
Step 5: Firmware

This screen displays the status of the firmware running on the Exinda appliance. If the appliance has Internet connectivity, the system will check for any newer firmware that may have been released. If a newer firmware image is available, you will be asked if you want to download and install it.



Step 6: Optimization

The final screen allows to configure default Optimizer policies.



For more information about the Optimizer policy wizard, see the Optimizer | Optimizer Wizard page.

Note: Settings on each step are automatically applied when clicking the 'Back' or 'Next' buttons.

3.6 Dashboards

There are 2 types of dashboards available to view on the Exinda appliance:

- System Dashboard: Shows system information.
- Benefits Dashboard: Show performance information.

3.6.1 System Dashboard

The System Dashboard shows System Information, the state of System Alarms as well as a summary of other Exinda appliances and their respective reduction statistics.

Hostname: ex240	
Hardware Series:	4060
Licensed Model:	Exinda 4860 10Mbps
SS Expiry Date:	Dec 31, 2011
Host ID:	00e0ed13e792
Serial Number:	2282PJ1
Timezone:	Australia/Melbourne
System Uptime:	1h 56m 16.050s
Scheduled Jobs:	No scheduled jobs.
Memory Usage:	59.67% of 2007MB
CPU Usage:	2%

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		
CIFS Signed Connections	OK		
Redundant Power	Not Available		
Redundant Storage	Not Available		
Accelerated Connections	OK		

WAN Reduction per Peer

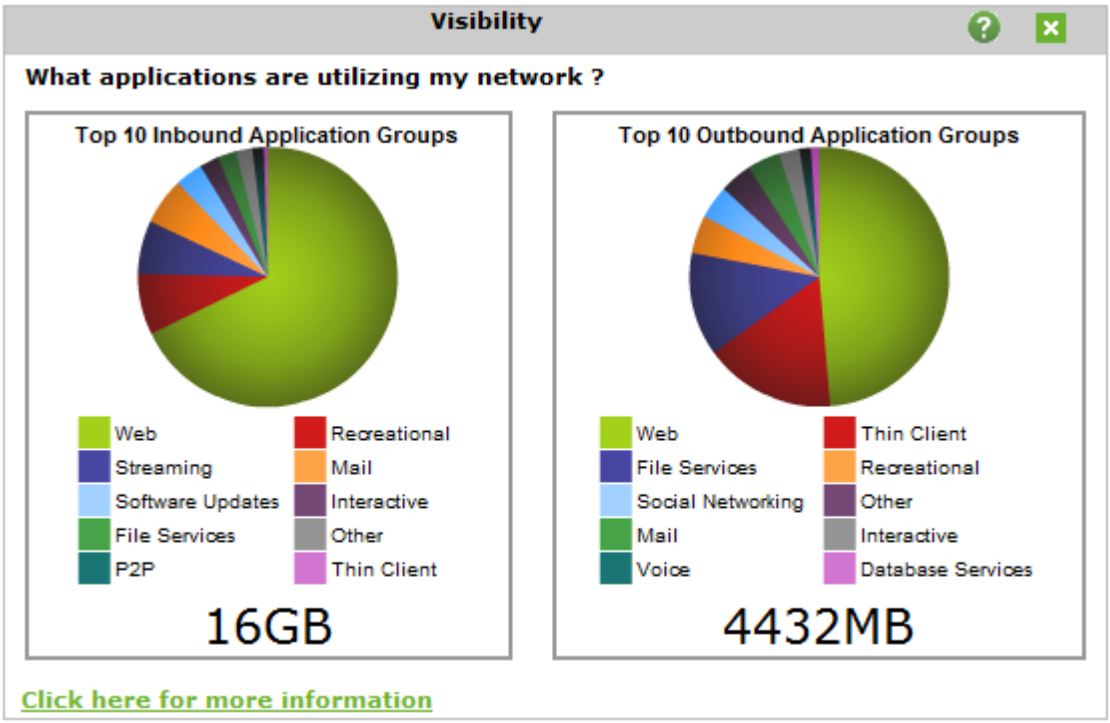
Hostname	IP Address(es)	Version	Status	LAN Data	WAN Data	Reduction Ratio (%)
				16MB	12MB	21.48
jl-home	172.16.20.130	5.3.0.11508	ONLINE	3MB	1MB	59.44
beavers42	172.16.100.57	5.3.0.11642	ONLINE	0MB	0MB	38.03
con-home3	172.16.102.119	5.3.0.11358	ONLINE	0MB	0MB	46.94
forta-home	172.16.109.57	5.2.0.10384	ONLINE	12MB	11MB	9.28

3.6.2 Benefits Dashboard

The Benefits Dashboard exposes a set of widgets, arranged on a dashboard that shows you exactly what the Exinda appliance is doing. Each widget can be hidden so you can customize the display to only include the widget that are relevant to you. To add a hidden widget click on 'Add More'. The widget settings are retained between logins. The dashboard can also be converted to PDF by clicking on the PDF icon in the top, right-hand corner of the interface.

Visibility

Visibility is an essential ingredient to maintaining clean network pipes. These graphs show the applications that are utilizing the network. This information is critical to the IT Manager to better manage the network and to make informed decisions.

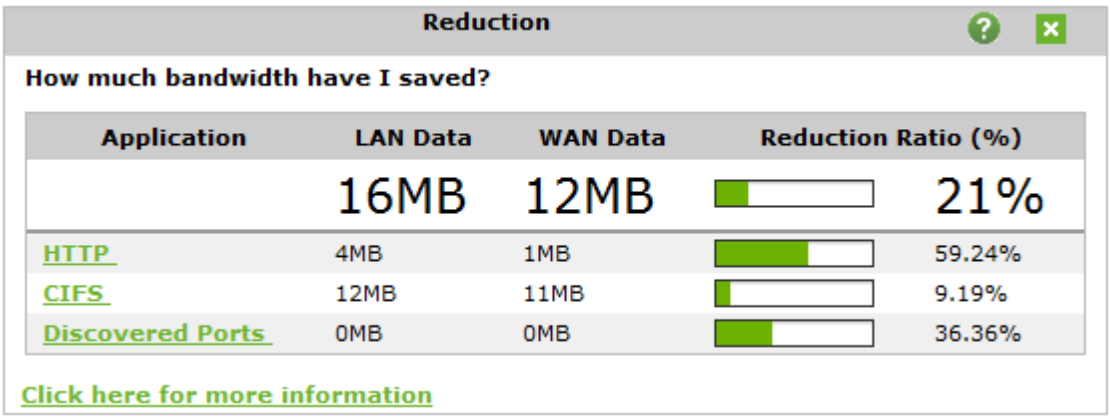


Example: This graph can tell you if the network is being miss-used. Users downloading music and videos are choking the network; miss-configured user profiles are being downloaded every day from the wrong location causing congestion and delays; data backups are running overtime and into normal business hours.

Reduction

Amount of redundant data that has been removed from the network and has therefore increased free capacity. It is a ratio that compares After Exinda (AE) to Before Exinda (BE). Data previously seen by the system is "remembered" and delivered from the local appliance rather than end-to-end from server to client resulting in a reduction in the amount of data sent across the network.

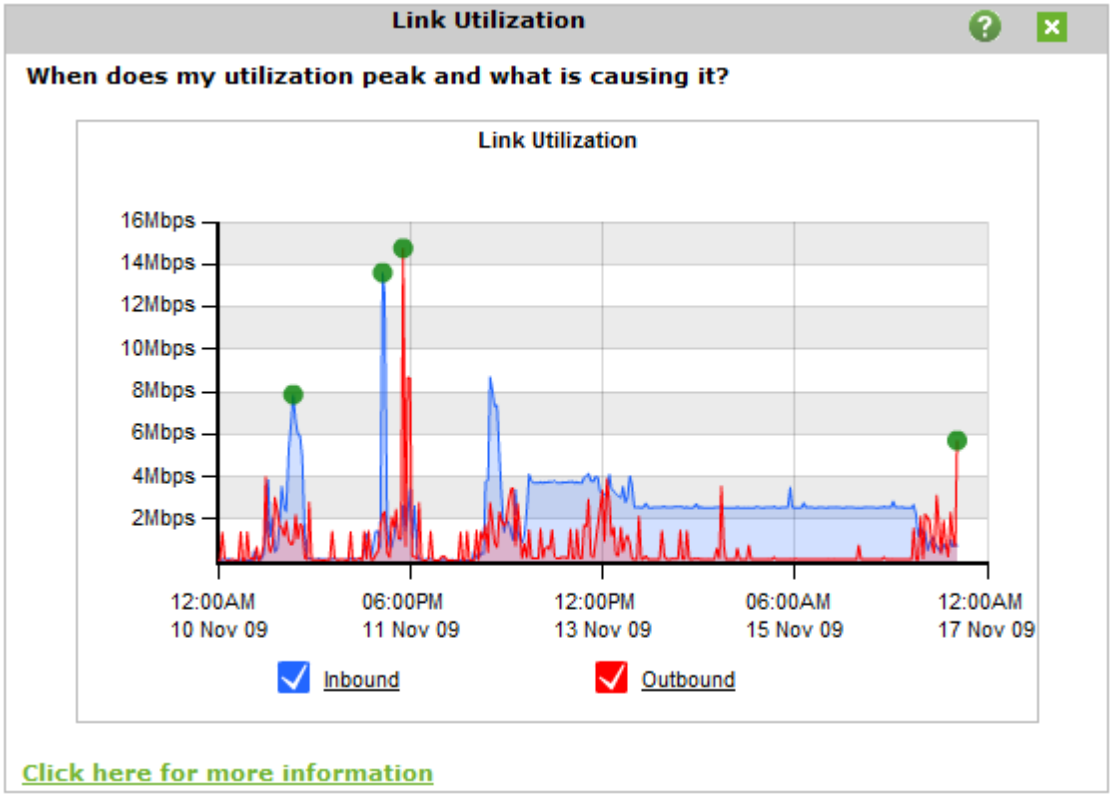
```
Reduction Ratio = (Data Transfer Size BE - Data Transfer Size AE) / Data Transfer Size BE.
```



Example: A ratio of 40% means a transfer that used to put 100MB of load onto the WAN, now puts 60MB of load on the WAN. I.e. 40% less.

Link Utilization

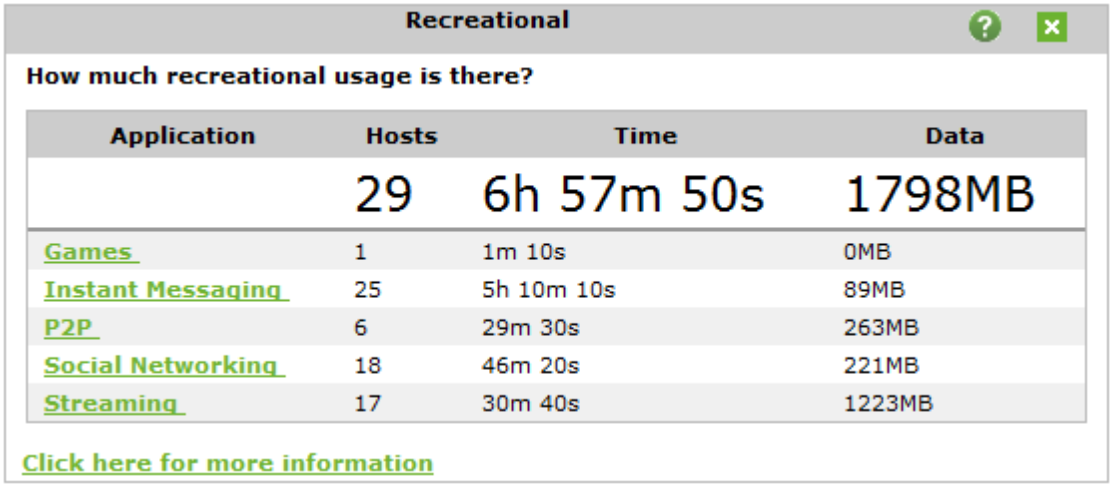
Without the right visibility and drill down capability it is very difficult to provide effective capacity planning for your network. It is important to know that the bandwidth you are paying for is what is actually being delivered, to know when the network utilization peeks and the causes of bottlenecks on your network.



Utilization graphs with conversation drill down allows you to see in one glance the symptom and causes of network bottlenecks. Without this level of visibility IT professionals may mistakenly treat the symptoms (e.g. buy more bandwidth) instead of addressing the cause which is a short term solution at best.

Recreational

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.



Prioritization

This ratio tells you how often critical applications were prioritized (also referred to re-ordering or re-queuing). A high percentage means that the system is prioritizing more often to ensure performance of your applications. A high percentage also means that by turning off optimization there is a higher probability that your critical applications will suffer.

```
Prioritization Ratio = Number of Packets Re-ordered / Number of Total Packets
```

Example: A ratio of 40% means 40% of the packets on your network were re-ordered. That means that non critical data was queued so that business critical data could jump the queue and be delivered in the order that the business requires.

Part IV

4 System Settings, Configuration and Diagnostics

More advanced system settings, configuration and diagnostics are available by using the Web UI in Advanced Mode.

This chapter covers the various configuration pages and what each setting means.

4.1 Network Settings

The Network Settings section of the Exinda appliance System Setup allows you to configure basic and advanced network settings. The various configuration pages include:

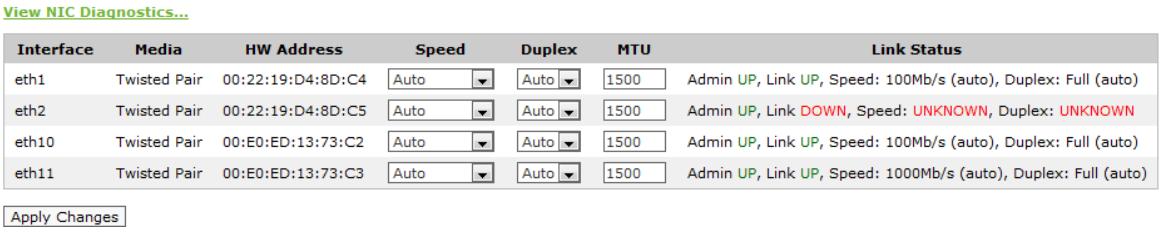
- NIC Settings: Configure network interface cards settings.
- IP Address: Configure an IP mode, IP address and gateway.
- Routes: Configure a static route.
- DNS: Configure a hostname, DNS and domain name.
- HTTP Proxy: Configure HTTP proxy settings.
- Email: Configure SMTP sever settings and email address.
- SNMP: Configure SNMP settings.
- Active Directory: Enable and fine-tune Active Directory.
- IPMI: Enable and configure IPMI on selected hardware.

4.1.1 NIC Settings

Interface Settings

Use the form below to set the speed/duplex and MTU of the System NICs. In most cases the default settings will work as the Exinda is setup to auto-negotiate. However, some equipment is not compatible with this. If there are collisions and/or errors, then it is an indication that the Exinda is not auto negotiating with neighboring equipment. As a result you might notice packet loss and network delays. To resolve this check if the router or switch is hard-coded to a speed or duplex setting. If hard-coded then set the Exinda device to a desirable speed/duplex

Note: Collisions, errors and dropped packets on the Exinda NICs will set the System health status to "Warning" and the offending interface(s) will be highlighted. For further troubleshooting click on the system warning or view the NIC Diagnostics.



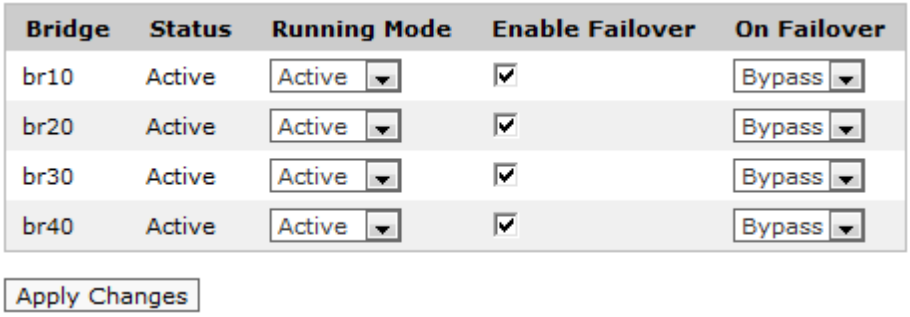
Interface	This is the interface number. Each interface corresponds to a physical port.
Media	Specifies the interface media. This could be Twisted pair or Fibre.
HW Address	This is the MAC address of the interface.
Speed	This is the speed at which the Exinda will negotiate with neighboring equipment.
Duplex	This is the duplex at which the Exinda will negotiate with neighboring equipment.
MTU	This is the maximum transmission unit size in bytes.
Link Status	The status of the interface shows wether the interface is up/down, the link is up/down as well as the speed/duplex that has been negotiated with the neighboring equipment.

Note: Ensure that the devices connected to the Exinda appliance have the same speed/duplex settings for their network interfaces (auto-negotiation is acceptable). If they are different, and the Exinda appliance is in bypass mode, the devices may not communicate and traffic may be dropped. It is recommended you set all your devices, including the Exinda, to either auto-negotiate or fixed to the same speed/duplex mode.

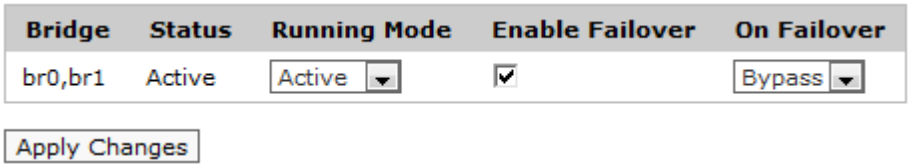
Fail to Wire (bypass)

The Fail to Wire (bypass) settings control the behaviour of the Exinda appliance's bridges in the event of failure, power outage or reboot.

Depending on the hardware appliance and the type of interface cards installed, fail to wire or bypass settings may be configured globally or per bridge. The image below shows independently controllable bypass bridges.



The image below show globally controllable bypass bridges.



Bridge	The bridge that the bypass settings apply to. Where available, bridges can be controlled independently, otherwise they will be controlled globally.
Status	The current status of the bridge - see below for definitions.
Running Mode	Specify the current status of the bridge. This allows you to change the current status of the bridge on the fly (e.g. manually put the bridge in and out of bypass) - see below for definitions.
Enable Failover	Enable failover in the event of failure, power outage or reboot. If not enabled, no action will be taken on failover.
On Failover	If failover is enabled, specify what action to take when failing over - see below for definitions.

The table below lists the various statuses and failover modes that are available. Depending on your hardware, the following options may or may not be available.

Active	The bridge is active (not in bypass) and traffic is been intercepted by the Exinda appliance.
Bypass	The bridge is in bypass and traffic is NOT been intercepted by the Exinda appliance.
Nolink	The bridge interfaces are both forced to link state down (as if the cables are not plugged into the interfaces).

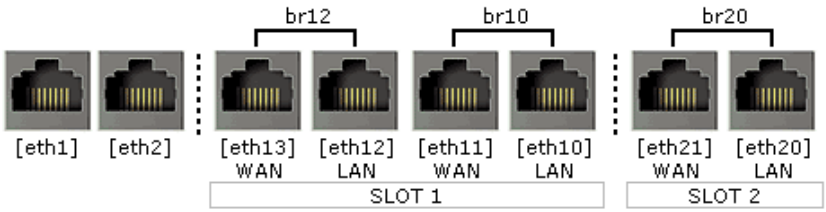
Link State Mirroring

With link state mirroring, the Exinda appliance will bring down the second port of a bridge if

the first port goes down. This feature allows the Exinda appliance to sit between a WAN router and a switch without blocking detection of switch outages by the router. This is a global setting that is applied to all enabled bridges. Use the form below to enable or disable link state mirroring.

4.1.2 IP Address

The Exinda appliance allows you to configure bridges and network interfaces as required. The form displays an image showing the available physical interfaces, physical interface to I/O slot and physical interface to bridge assignments. Bridges can be enabled, roles assigned to an interface (Cluster, Mirror or WCCP) and IP settings applied.



Interface Settings

eth1	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::222:19ff:fed4:8dc4/64
	Static Addresses:	172.16.1.240 / 23
		/
	Comment:	
eth2	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::222:19ff:fed4:8dc5/64
	Static Addresses:	/
	Comment:	
br10 ☑	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::2e0:edff:fe16:be36/64
	Static Addresses:	/
	Comment:	
br12 ☑	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::2e0:edff:fe16:be38/64
	Static Addresses:	/
	Comment:	
br20 ☐		
eth20	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::2e0:edff:fe13:73c2/64
	Static Addresses:	/
	Comment:	
eth21	Role:	☐ Cluster ☐ Mirror ☐ WCCP
	Autoconf:	IPv4: ☐ DHCP IPv6: ☐ SLAAC
	Dynamic Addresses:	fe80::2e0:edff:fe13:73c3/64
	Static Addresses:	/
	Comment:	

Gateway Settings

IPv4:	172.16.1.254
IPv6:	

Apply Changes

A bridge consists of a LAN and WAN interface. To enable a bridge, select the brXX checkbox above the interface pair.

Interfaces that are not assigned to a bridge may have the following roles configured:

Cluster	One interface may be configured for Cluster internal use in High Availability (HA) environments. An interface and Cluster Master address should also be configured.
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.
WCCP	One interface may be configured in WCCP mode. WCCP allows out of path Application Acceleration.

To configure an interfaces address and netmask automatically, select either the DHCP checkbox for IPv4 networks or SLAAC for IPv6 networks. When SLAAC is selected for IPv6 networks, the following options are available:

Privacy Address	Enable SLAAC privacy extensions. Selecting this option will periodically change the automatically assigned IPv6 address.
Gateway	Assign an IPv6 gateway dynamically.

To configure a static address, enter an IPv4 or IPv6 address and netmask.

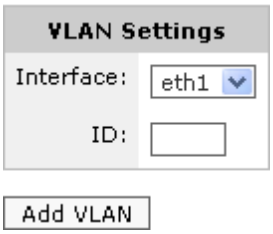
Enter the address of your networks default IPv4 and IPv6 gateways.

You can optionally add a comment describing how the interface is to be used in the Comment field.

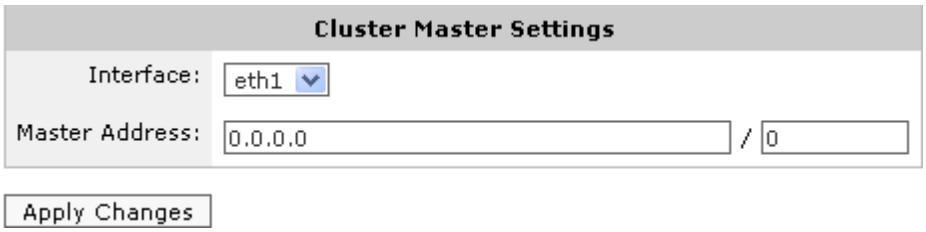
The DHCP option is enabled by default on the Exinda appliance. If a DHCP server is available, an IP address will be automatically assigned. From a web browser go to http://www.findmyexinda.com. This will download a Java applet and automatically find the Exinda appliance. Click on the Exinda appliance that has been found to access it. If a DHCP address is not picked up, the Exinda will default to the IP address of 172.14.1.57.

Model	Factory default DHCP enabled interface
2000, 4000	br1
6000	eth0
2060, 2061, 4060, 4061, 6060, 8060, 10060	eth1

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.



The Cluster Master address is the external address used to access an appliance in HA environments.



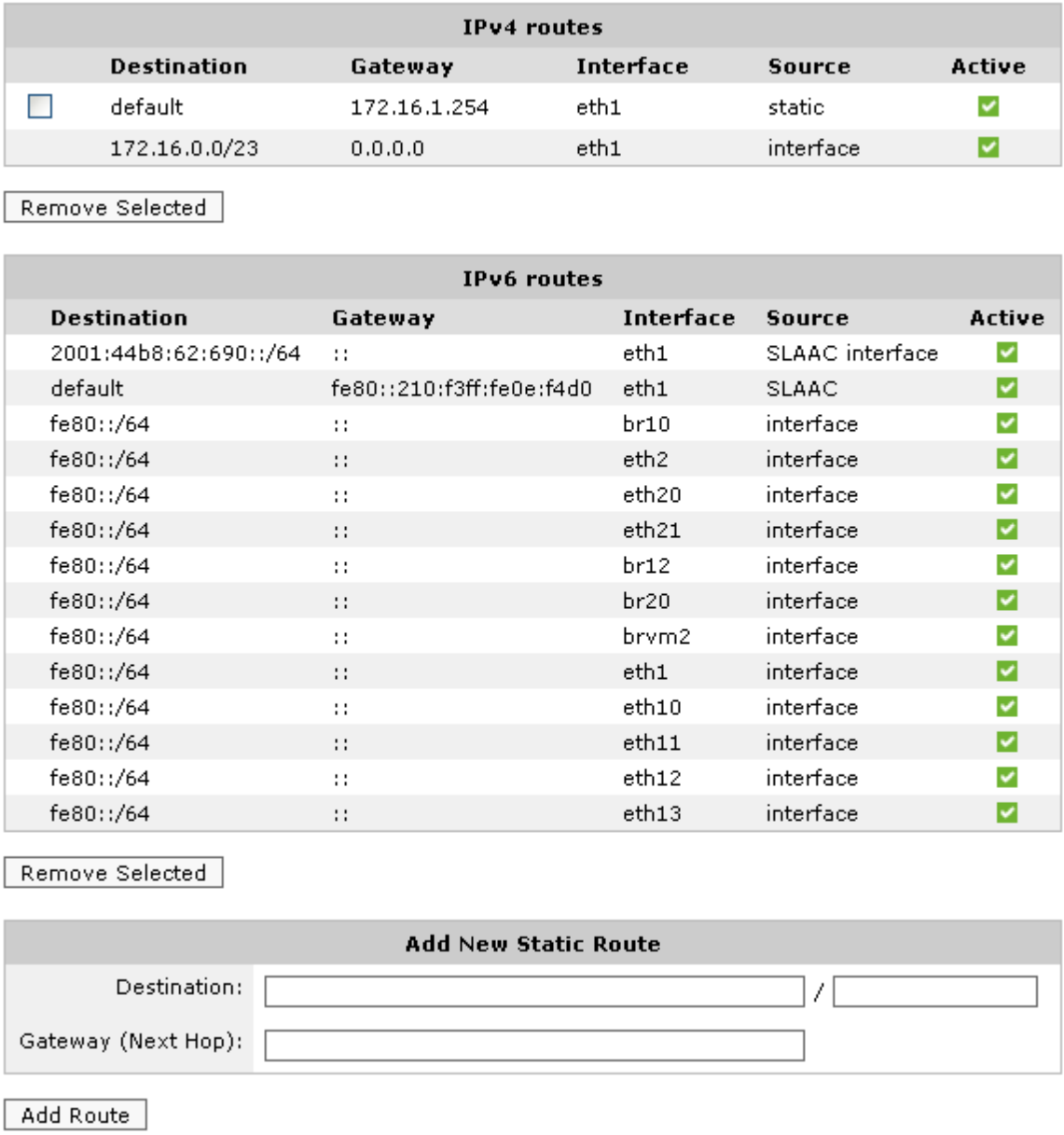
Note: Further information on Clustering/HA, Mirroring and WCCP is available in the associated How To guides.

4.1.3 Routes

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	☑

Remove Selected

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	☑

Remove Selected

Add New Static Route

Destination: /

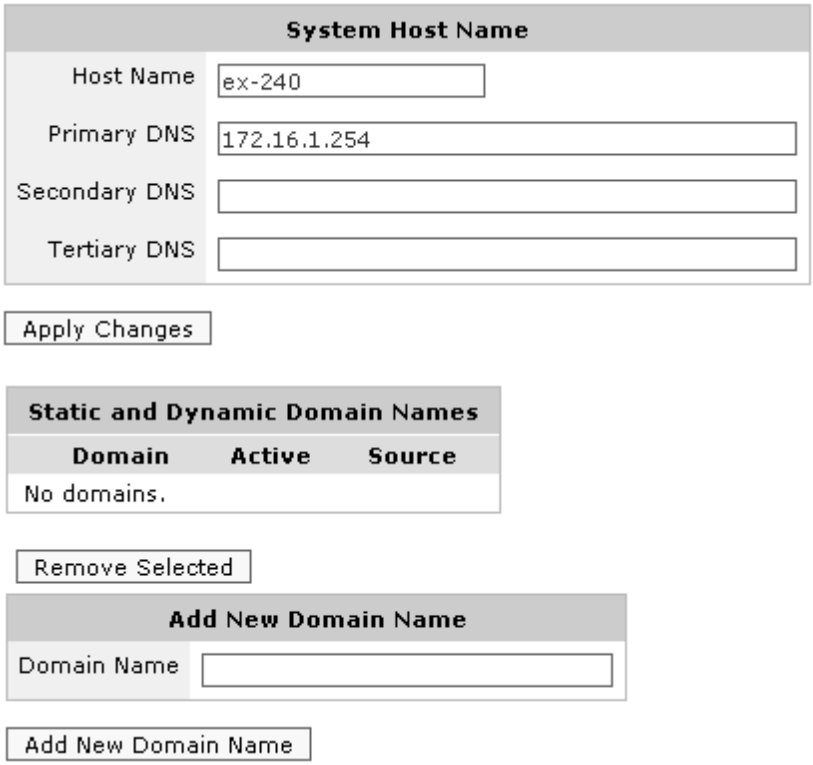
Gateway (Next Hop):

Add Route

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

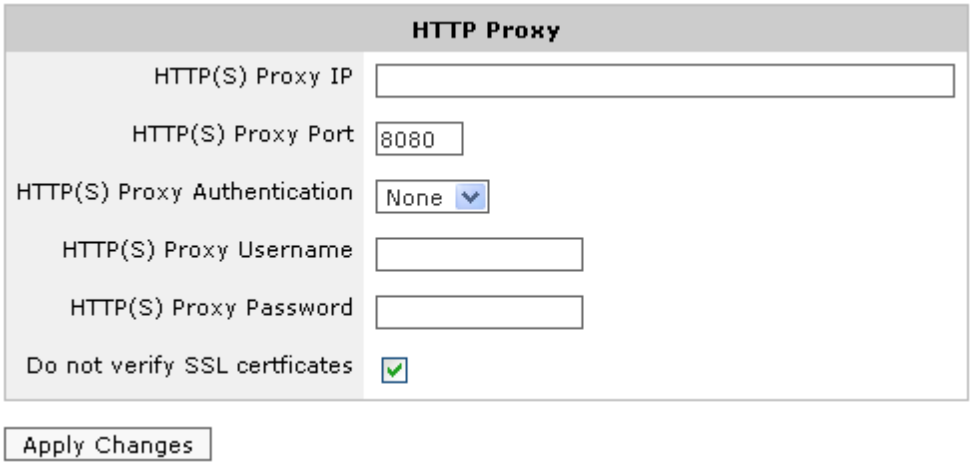
Use the form below to enter a Host Name for your Exinda appliance and configure the DNS servers and domain names. The hostname should be unique to this appliance on the network.



Note: A valid DNS server is required for Edge Cache, system alerts, scheduled reports, firmware updates, license updates and Anonymous Proxy updates.

4.1.5 HTTP Proxy

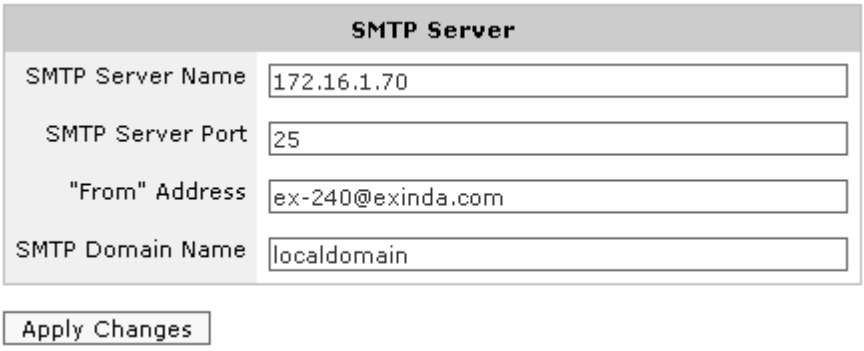
Specify a HTTP proxy if you would like the appliance to access Exinda's server via HTTP proxy. Access to Exinda's HTTP server is required for firmware updates, license updates and Anonymous Proxy updates. If you have SDP enabled, please ensure your proxy supports HTTPS.



HTTP(S) Proxy IP	The IPv4 or IPv6 address of the HTTP or HTTPS proxy server.
HTTP(S) Proxy Port	This is the port number that is used by the proxy server for client connections. The default is 8080.
HTTP(S) Proxy Authentication	Authentication type - options are none or basic.
HTTP(S) Proxy Username	The proxy server username.
HTTP(S) Proxy Password	The proxy server password.
Do not verify SSL certificates	Disable this option if you wish to verify SSL certificates.

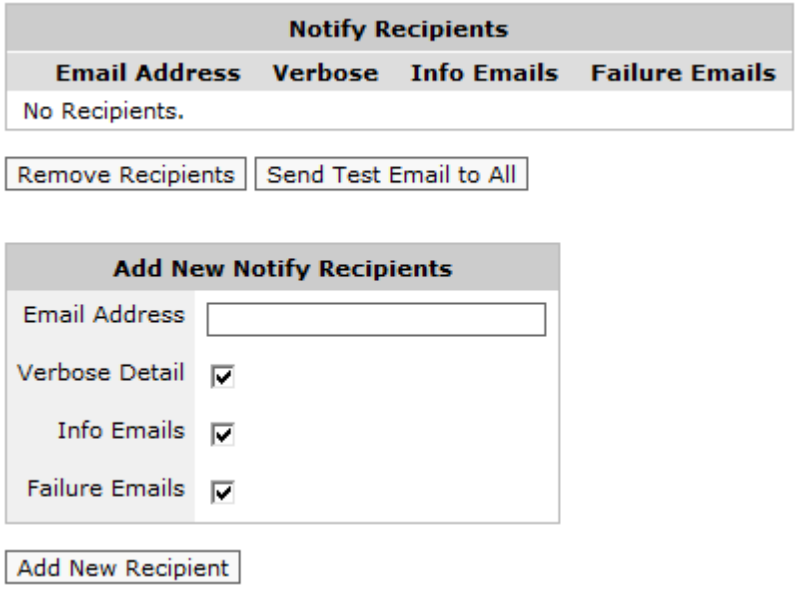
4.1.6 Email

Use the form below to configure the SMTP server settings. An SMTP server is required for receiving scheduled reports, system alerts and auto-support notifications.



SMTP Server Name	The SMTP server name, IPv4 or IPv6 address. e.g. smtp.example.com
SMTP Server Port	The SMTP server port. The default is 25.
"From" Address	This will appear as the "From" email address for system alerts and reports. e.g. exinda@example.com.
SMTP Domain Name	This is the SMTP domain name.

Use the form below to add email recipients.

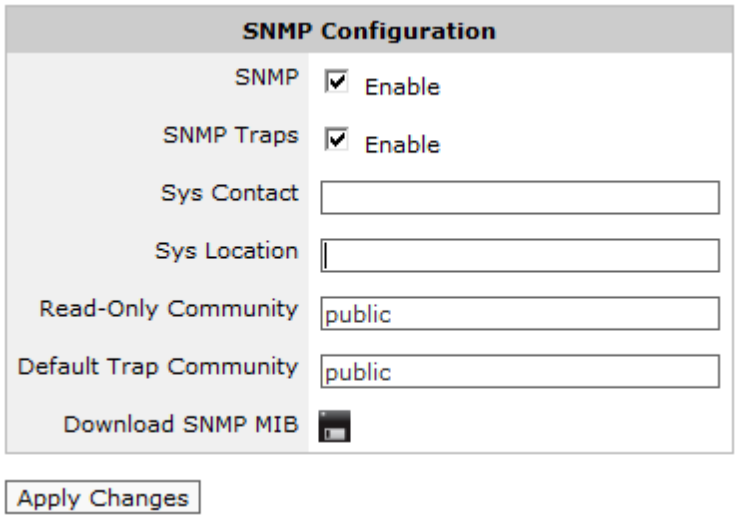


Email Address	Email address for receiving system alerts. Multiple addresses can be configured.
Verbose	Send detailed event emails to this recipient.
Info Emails	Send informational events to this recipient.
Failure Emails	Send failure events to this recipient.

Note: Use the 'Send Test Email to All' option to test that your SMTP settings are correct.

4.1.7 SNMP

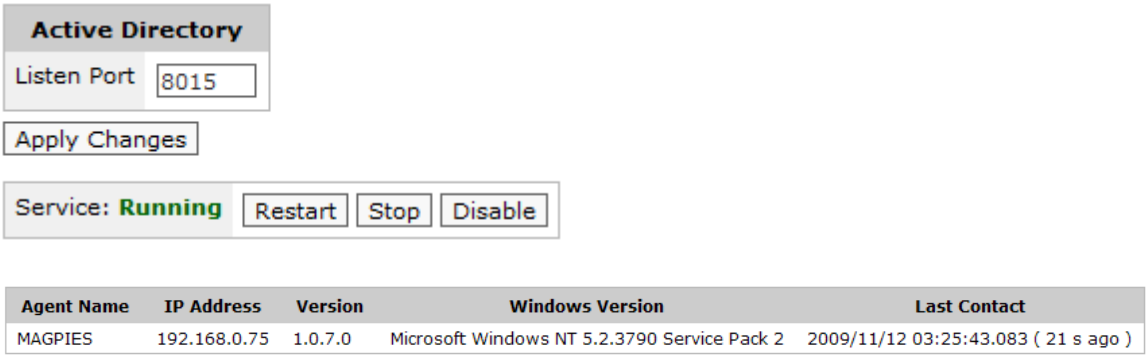
The Exinda appliance allows data export to SNMP systems. Use the form below to configure the SNMP settings. To download the Exinda SNMP MIB click on the Download icon.



Note: To disable/enable SNMP traps for system alerts, navigate to 'System | Setup | Alerts' on the Web UI, advanced mode.

4.1.8 Active Directory

The Active Directory service can be enabled/disabled on this page. The Domain Controller or Active Directory (AD) Server details will be available If the Exinda Active Directory Windows client has been installed and communicated successfully.



Listen Port	This is the port number that is used for communication between the Exinda and the AD server. This has to be the same on both the Exinda and the AD windows client for successful communication.
Agent Name	The AD server name.
IP Address	The IP address of the AD server.
Version	The Exinda AD Windows client version.
Windows Version	The AD server Windows version.
Last Contact	The time the AD server was last contacted.
Renumerate	Refresh the entire list of users and logins.

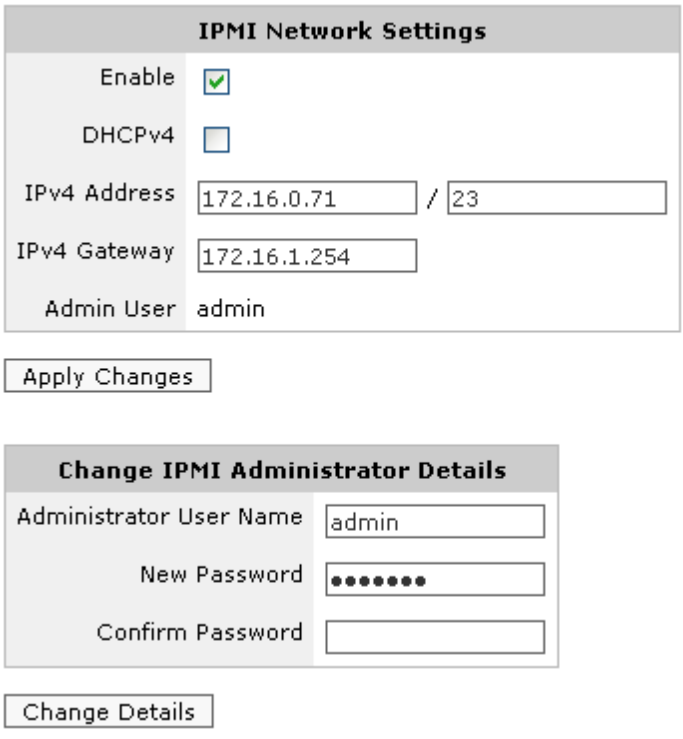
Note: For further information, consult the Active Directory How to Guide.

4.1.9 IPMI

IPMI is used to access the appliance's baseboard management controller (BMC) to perform operations such as remote power off / power on, or to access the console (serial-over-LAN)

The appliance's eth1 interface must be connected to the network and a dedicated IP address is required.

Use the form below to enable IPMI and configure IPv4 address details. You can either automatically assign an IPv4 address using DHCP (if your network supports this) or specify a static address and default gateway.



You can also update the default admin password. The default password is 'exinda'.

Once IPMI has been enabled and an IPv4 address has been configured, you can access the web-based UI by navigating to https://<ipmi-ip>. On models[1] that do not support a web-based UI, IPMI functions may be accessed using a command line utility such as ipmitool

Example: print the system event log (SEL) on an appliance that has enabled IPMI, with address 192.168.10.5

```
# ipmitool -l lan -H 192.168.10.5 -U admin -P exinda sel
```

Example: access the serial console using serial-over-LAN

```
# ipmitool -I lanplus -H 192.168.10.5 -U admin -P exinda sol activate
```

Note: Only Exinda 406X, 606X, 806X and 1006X series hardware support IPMI.

[1] 406X does not support a web-based UI for IPMI

4.2 System Setup

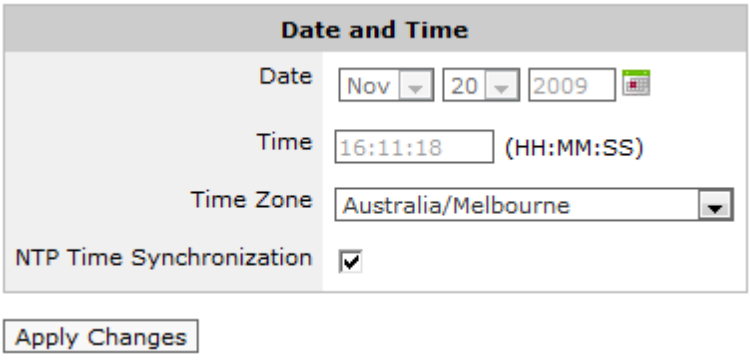
The System Setup section of the Exinda appliance allows you to configure basic and advanced system settings. The various configuration pages include:

- Date and Time Configuration: Configure Date and Time on the Exinda appliance.
- UI Configuration: Configure Web UI and CLI settings.
- SDP Configuration: Enable SDP.
- SQL Export: Configure remote SQL access.
- Monitoring Configuration: Fine-tune monitoring settings.
- Netflow Configuration: Configure netflow parameters and items to export.
- Scheduled Jobs: View and remove scheduled jobs.
- Alerts: Enable/Disable system alerts.
- License: Install a new license.
- QoS configuration: Change Optimizer mode.

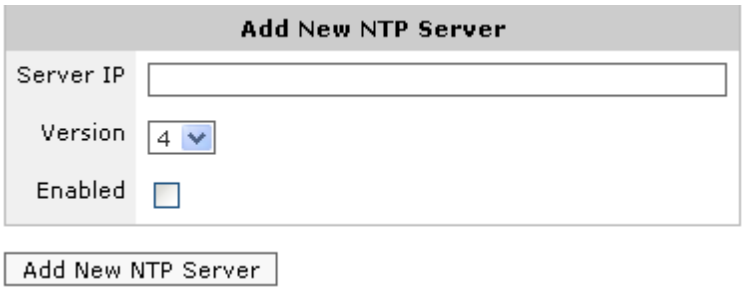
4.2.1 Date and Time Configuration

Use the form below to set the time, date and time zone on the Exinda appliance.

Note: If NTP time synchronization is enabled, the date and time cannot be manually configured.



Use the form below to configure NTP servers that the Exinda appliance will use to set its time and date. To use the configured NTP server tick the 'NTP time Synchronization' box in the form above.

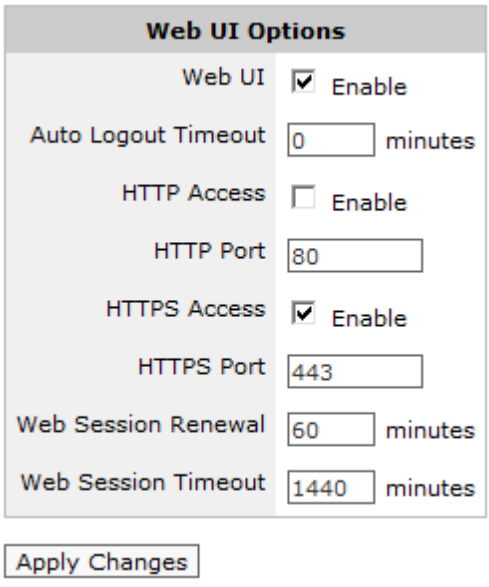


Server IP	The IPv4 or IPv6 address of the NTP server.
Version	The NTP version that the server supports.
Enabled	Enable or disable this NTP server.

4.2.2 UI Configuration

Use the form below to enable/disable the Web User Interface as well as configure Web UI options.

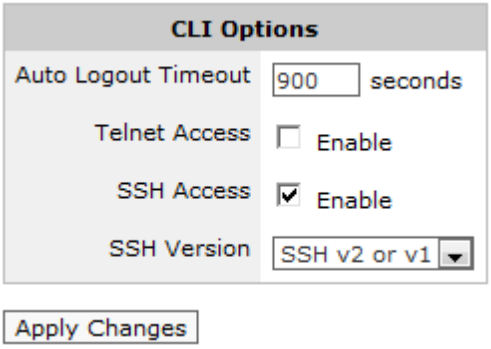
Warning: Once you disable the Web UI, you can only re-enable it via the CLI.



Web UI	Enable web access to the Exinda appliance.

Auto Logout Timeout	The time (in minutes) before the web session is automatically logs out. A value of '0' means the Web UI will never auto-logout.
HTTP Access	Enable HTTP access to the Exinda appliance. This is disabled by default.
HTTP Port	Configure the HTTP port. The default is 80.
HTTPS Access	Enable HTTPS access to the Exinda appliance. This is enabled by default.
HTTPS port	Configure the HTTPS port. The default is 443.
Web Session Renewal	Web session renewal time in minutes. This cannot be more than the Web Session Timeout.
Web Session Timeout	Web session timeout in minutes. This cannot be less than the Web session renewal.

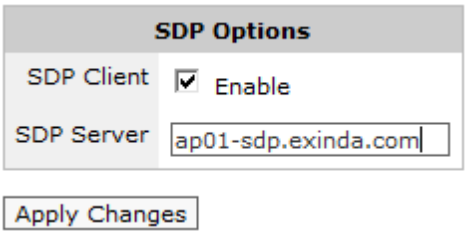
Use the form below to enable/disable the CLI as well as configure CLI options.



Auto Logout Timeout	The time (in seconds) before the CLI session automatically logs out.
Telnet Access	Enable telnet access to the Exinda appliance. This is disabled by default.
SSH Access	Enable SSH. This is enabled by default.
SSH version	Configure a SSH version. This can be set to 'SSH v2 or v1' or 'SSH v2 only'

4.2.3 SDP Configuration

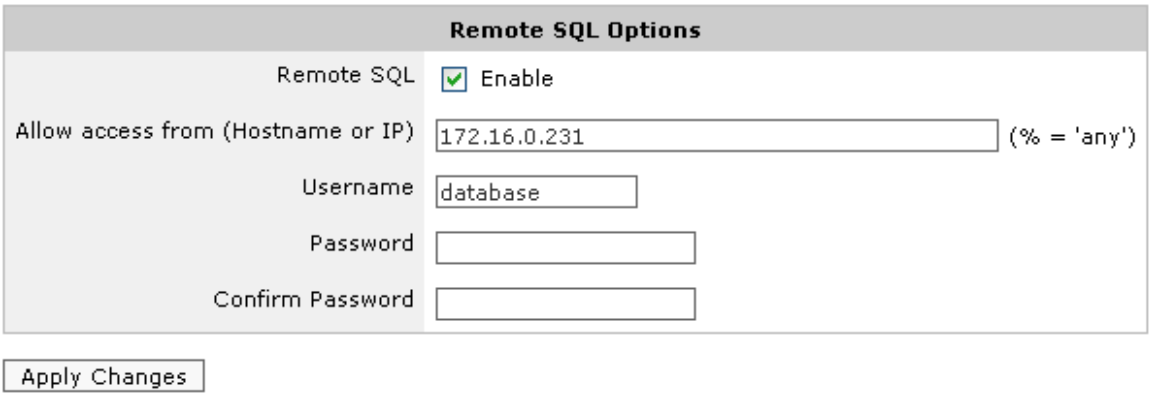
Use the form below for to enable the SDP service on the Exinda appliance and change the SDP server address if required. This will enable communication between the Exinda appliance and the SDP server. A SDP subscription is required in order to use the Exinda SDP feature.



Note: For further information, consult the SDP User Manual.

4.2.4 SQL Export

Use the form below to configure remote SQL access, allowing MySQL clients to access the internal monitoring database. When creating an ODBC connection use the user account and password you setup on the Exinda appliance. The database name to connect to is 'monitor'. This ODBC entry can be used to access the Exinda's monitor database from any ODBC aware application.



Note: For further information, consult the SQL Access How to Guide.

4.2.5 Monitoring Configuration

The monitoring configuration allows you to fine-tune monitoring options and change the way graphs are displayed. Use the form below to configure monitoring settings.

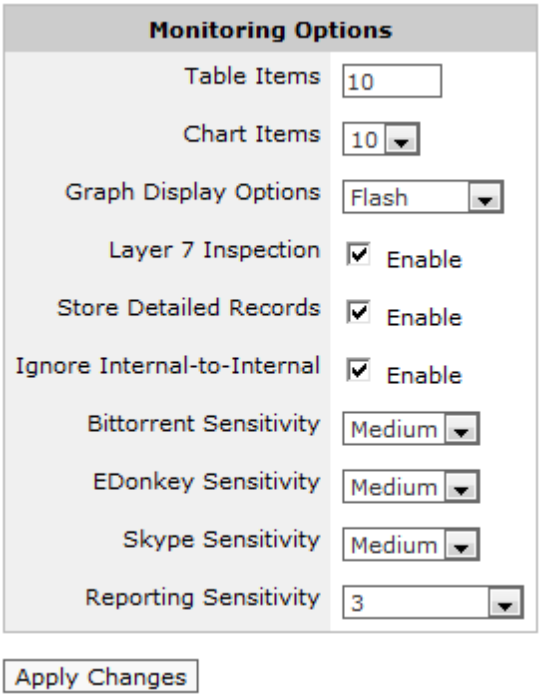
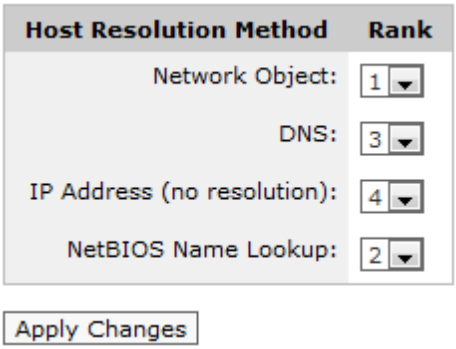


Table Items	Number of top items in the monitoring tables.
Chart Items	Number of top items in the pie chart graphs.
Graph Display Options	Graph display setting. This can be set to flash or non-flash. The default is flash.
Layer 7 Inspection	Enable Layer 7 inspection.
Store Detailed Records	Detailed Monitoring records (Applications, Hosts, URLs, Users, Conversations and Subnets) are not stored if this option is disabled. Turn this off if there are excessive traffic flows through the appliance in order to reduce CPU usage. When off there is no drill down available for Applications, Hosts, Conversations.
Ignore Internal-to-Internal	Enable the ignore internal to internal traffic option. If this is enabled all traffic between Network Objects marked as 'Internal' will be ignored and pass through the Exinda appliance.
Bittorent Sensitivity	Set the Bittorent sensitivity level. Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.

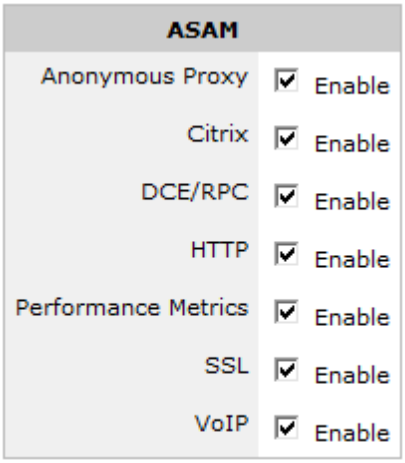
EDonkey Sensitivity	Set the EDonkey sensitivity level. Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.
Skype Sensitivity	Set the Skype sensitivity level. Setting this to 'high' is recommended for most service provider environments.
Reporting Sensitivity	This controls the sensitivity of the monitoring reports. Setting this to a high value is not recommended in high load environments.

Use the form below to control how IP addresses are resolved to hostnames. The hostnames are used in the monitoring pages and PDF reports.



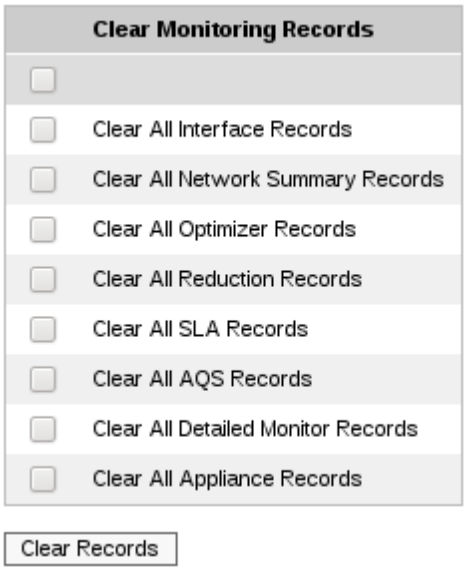
Network Object	The IP addresses will be resolved according to the configured network objects. To configure network objects, navigate to Objects | Network | Network Objects, on the Web UI, Advanced mode.
DNS	The IP addresses will be resolved according to the DNS mappings.
IP Address	The IP addresses will be not be resolved to hostnames.
NetBIOS Name Lookup	The IP addresses will be resolved to NetBIOS names.

Use the form below to enable/disable an Application Specific Analysis Module (ASAM).



Anonymous Proxy	Enable/disable Anonymous Proxy site detection.
Citrix	Enable/disable Citrix session metadata (published application name and username) detection.
DCE/RPC	Enable/disable DCE/RPC metadata (MAPI, DFS, FRS, etc) detection.
HTTP	Enable/disable HTTP metadata (host, user-agent and content-type) detection. This setting also applies to Flash and Windows Media metadata detection.
Performance Metrics	Enable/disable Performance Metric calculations (RTT, Network/Server Delay, Loss/Efficiency and TCP Health).
SSL	Enable/disable SSL metadata (common name and organization unit) detection.
VoIP	Enable/disable VoIP performance calculations (MoS and rFactor scoring).

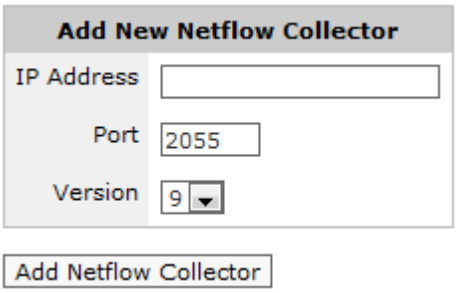
Use the form below to clear ALL or specific monitor statistics.



Warning: This will permanently delete the selected records from the monitoring database.

4.2.6 Netflow Configuration

Netflow allows the Exinda appliance to export flow records to 3rd party monitoring devices. Use the form below to configure these Netflow targets.



IP Address	Specify the IP Address of the Netflow target. The Exinda appliance will export Netflow data to this IP Address.
Port	Specify the Port number of the Netflow target. The Exinda appliance currently supports Netflow export on UDP ports.
Version	Specify the Netflow version to export. Current supported versions are v1, v5 and v9.

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

Common Options	
Active Flow Timeout	Specify how often long-term, persistent flows are exported. By default, flows are exported within 10 seconds of the flow terminating (this approach does not work well for long-term or persistent flows). This setting allows you to specify how often these long-term flows should be exported.
Netflow v9 Options	
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	
Export L7 Application ID	Export Application identification information. The Application ID to Name mappings are exported as an options template.
Export Policy ID	Export Optimizer Policy IDs and names.
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	
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.

4.2.7 Scheduled Jobs

Reboots and firmware installations can be scheduled for a specific date and time. The table below lists any jobs that have been scheduled. To cancel a job, select it form the list and click 'Remove Selected'. For more information on scheduling a firmware installation ore reboot, consult the respective pages.

	ID	Name	Description	Executes On	Status
☐	1	Reload	Scheduled reload from web user interface.	2009/12/31 00:00:00	Pending

Remove Selected

ID	Scheduled job id.
Name	Scheduled job name.
Description	Scheduled job description.
Executes on	Schedule time.
Status	Schedule status.

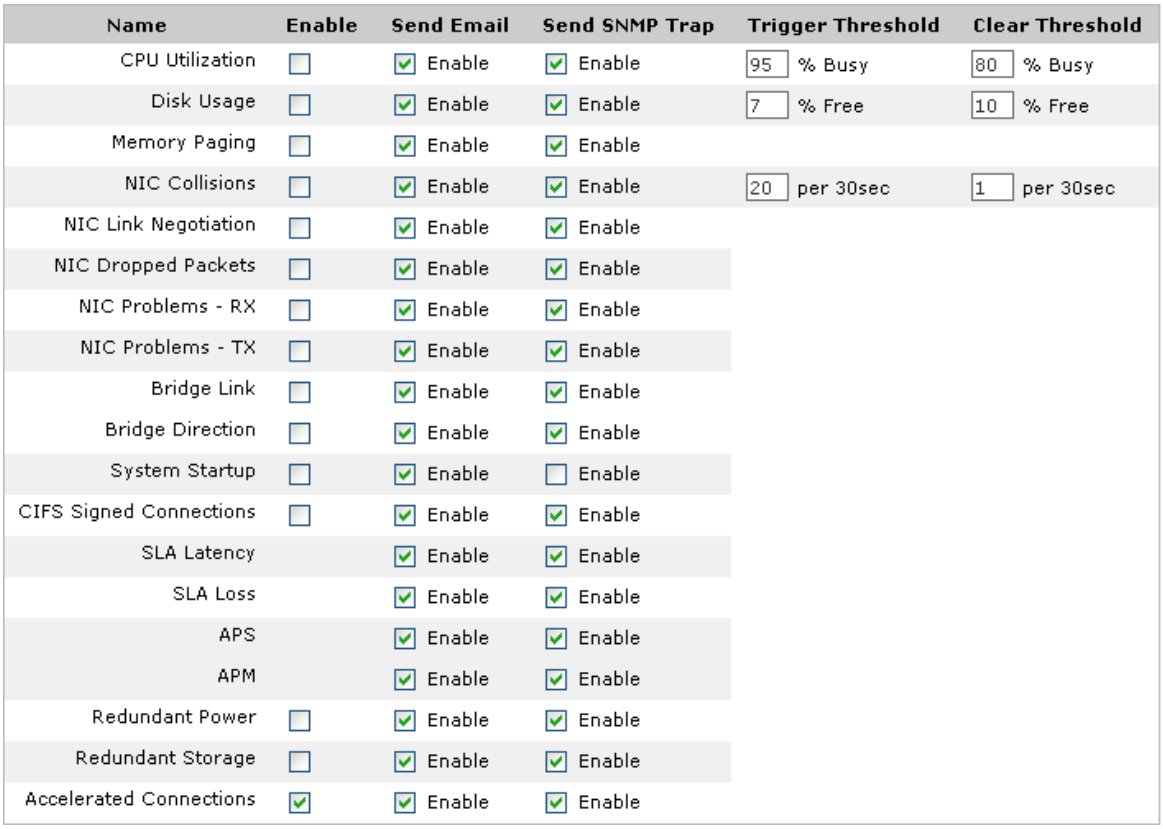
4.2.8 Alerts

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. SLA and APS email alerts are sent when the set limits are exceeded. Use the form below to disable alerts that you do not wish to trigger and/or receive emails and SNMP traps for.

Note: To create SLA, APS and APM objects, navigate to 'Objects | Service Levels' on the Web UI, advanced mode.

Note: To configure SNMP settings, navigate to 'System | Network | SNMP' on the Web UI, advanced mode.

Note: Valid SMTP and DNS settings need to be configured prior to receiving email alerts.



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	20 per 30sec	1 per 30sec
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		
CIFS 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		
Accelerated Connections	☑	☑ Enable	☑ Enable		

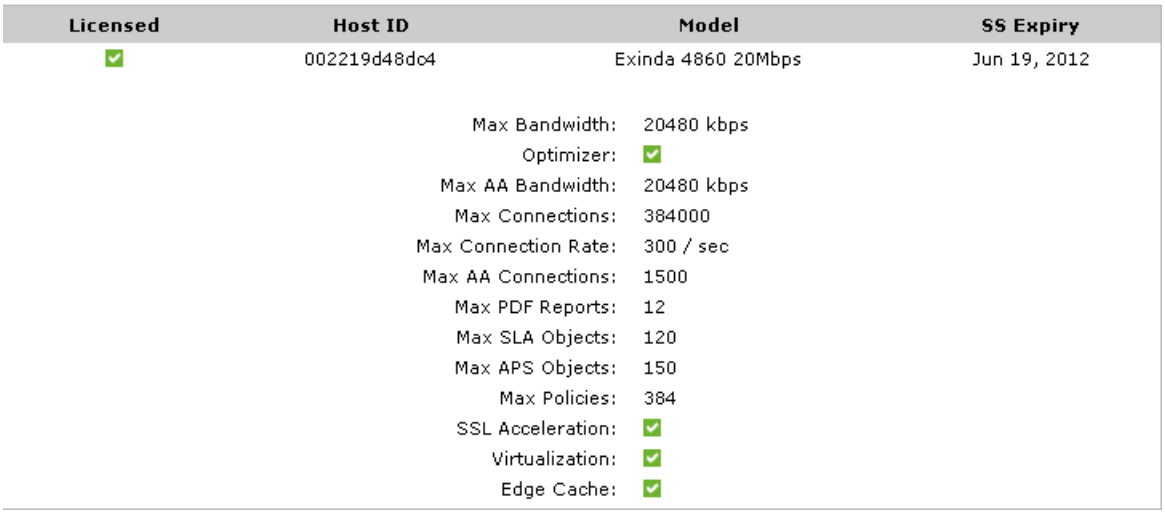
CPU Utilization	Alert raised when the CPU utilization threshold is reached. The trigger and clear thresholds can be altered. The defaults are 95% and 80% busy respectively.
Disk Usage	Alert raised when the used disk space threshold is reached. The trigger and clear thresholds can be altered. The defaults are 7% and 10% free respectively.
Memory Paging	Alert for memory use and paging.
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 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.
Bridge Link	Alert raised when one of the links on an enabled bridge is down.
Bridge Direction	Alert raised when the appliance cabling is incorrect. In most cases, it indicates the Exinda WAN interface has been incorrectly plugged into the LAN and vice versa.
System Startup	Alert raised when the Exinda appliance boots up.
CIFS signed connections	Alert raised when CIFS signed connections are present.
SLA Latency	Alert raised when the set latency for a SLA object is exceeded.
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.
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).
Accelerated Connections	Alert raised when the number of accelerated connections exceeds the licensed limit. Connections over the licensed limit pass through not accelerated.

4.2.9 License

Licensing Exinda appliances is simple. A single License Key is required to enable features. Multiple License Keys on the same appliance are also supported. The appliance will use the license that provides the highest specification limits. The license is automatically fetched and installed on first bootup. The auto license service checks for new licenses every 24 hours, if a new license is found it is automatically installed. The table below shows the time since the Auto License Service checked for a new license and the time since a new license was found. The Exinda appliance allows you to Stop, Restart or Disable the Auto License Service.

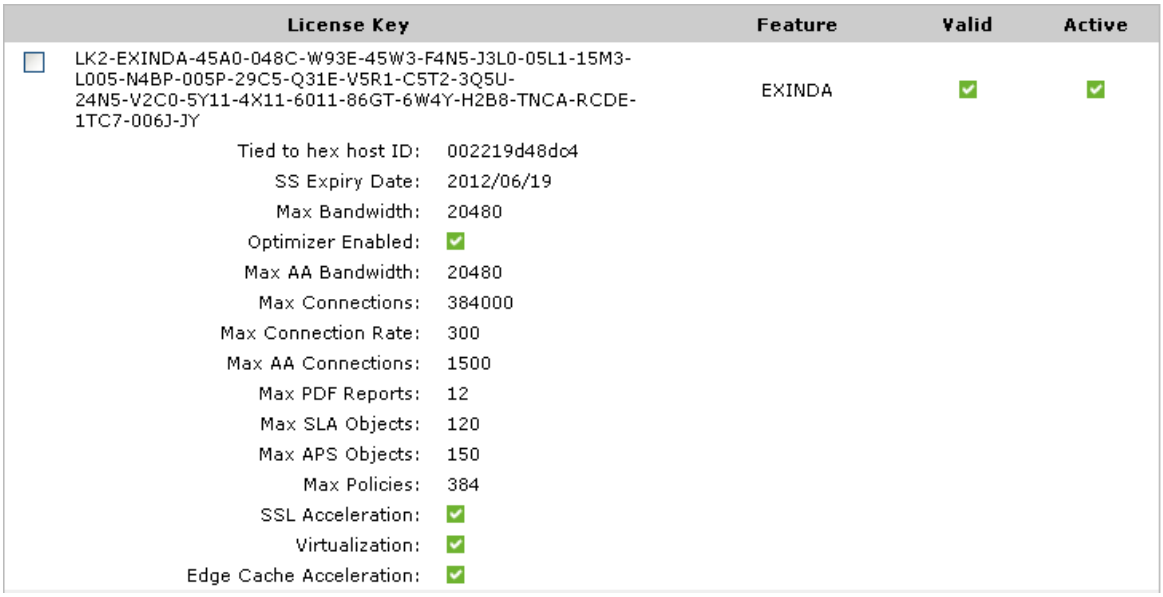
The Current System License Status displays the "effective" license limits and enabled features. These are the limits that are currently effective on the appliance. These effective limits can change depending on the license key or combination of keys installed.



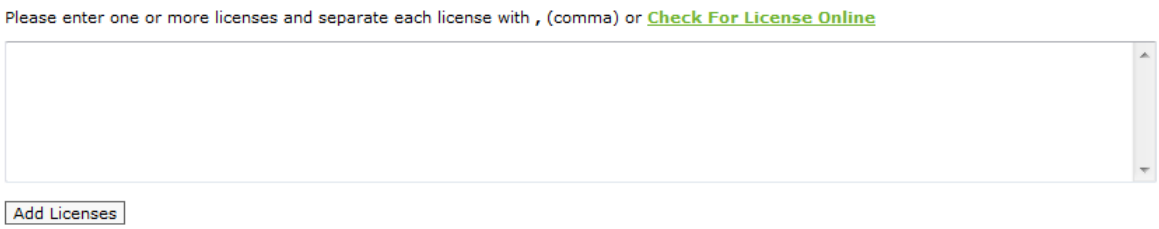
Licensed	License status.
Host ID	The Host ID is unique to each Exinda appliance.
Model	Exinda appliance model.
End Date	Expiry date of a temporary key.
SS Expiry	Expiry date of Exinda Software Subscription. After this date no updates can be installed on the appliance.
Max Bandwidth	Maximum monitoring and QoS bandwidth.
Optimizer	QoS and Acceleration module status.
Max AA bandwidth	Maximum acceleration bandwidth (WAN side).
Max Connections	Maximum concurrent connections through the appliance.
Max Connection Rate	Maximum number of new connections per second. Exceeding this will cause the network problems as any more connections will get dropped at setup time.
Max AA Connections	Maximum number of connections that can be accelerated. Exceeding this limit will mean the any new connections are not accelerated.
Max PDF reports	Maximum number of PDF reports that can be automatically generated and emailed.
Max SLA Objects	Maximum Service Level Agreement objects.
Max APS Objects	Maximum Application Performance Score objects.

Max Policies	Maximum number of optimization policies. Regardless of Circuit and VC.
SSL Acceleration	SSL Acceleration license feature status.
Virtualization	Virtualization license feature status.
Edge Cache	Edge Cache Acceleration license feature status.

The available license keys are listed along with their respective limits. License keys can also be removed from the system by clicking 'Remove'. Before removing ensure that you keep a copy of the license key.



The Exinda appliance allows you to manually check the Exinda license server, at any time, for updated licenses by clicking 'Check For License Online' . If you already have a license, you can copy and paste it in the below text box. Click 'Add Licenses' to add the newly found or manually entered license key.

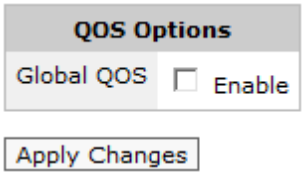


4.2.10 QoS Configuration

There are 2 Optimizer modes that affect the behaviour of how Optimizer policies are treated in a multi-bridge deployments.

Note: To change QoS Configuration, navigate to 'System | System Setup | QoS Configuration' on the Web UI, advanced mode.

The form below is used to enable/Disable Global QoS:



Independent QoS (Global QoS disabled) (Default): QoS policies are applied to each bridge (LAN and WAN pair) independently. For example, if there ware a single policy to restrict all traffic to 1Mbps, this would be applied independently to all bridges. So, the traffic through each bridge would not exceed 1Mbps.

Global QoS (enabled): QoS policies are applied globally, to the entire system. For example, if there were a single policy to restrict all traffic to 1Mbps, this would be applied across all bridges. So, the sum of all traffic through all the bridges would not exceed 1Mbps. This is typically used when you are using multiple bridges and wish to QoS everything as one link.

Note: Global QoS cannot be enabled if Dynamic Virtual Circuits are in use.

Note: In Clustering/HA deployments, Optimizer policies are implemented globally, so this setting only affects how traffic through multiple bridges are treated. For example, a policy to restrict to 1Mbps on an Independent QoS system would allow 1Mbps through on each bridge, shared across all appliances (so all the Bridge 0's would share 1Mbps, and all the Bridge 1's would share another 1Mbps, and so on for each bridge). A policy to restrict to 1Mbps on a Global QoS system would allow 1Mbps through system wide across all bridges on all appliances.

4.3 Optimization

Exinda's Application Acceleration technology provides protocol optimization and data reduction, enabling applications to run faster over the WAN. This technology is provided by the following services:

Exinda Community	Provides appliance auto-discovery and acceleration capability services between all Exinda appliances in the WAN.
TCP Acceleration	Provides layer 4 (TCP) protocol optimization.

WAN Memory	Provides data reduction using de-duplication and compression technology.
CIFS Acceleration	Provides layer 7 CIFS (Windows File Sharing) protocol optimization.
NCP Acceleration	Provides layer 7 NCP (Netware Core Protocol over TCP port 524) protocol optimization.
SSL Acceleration	Provides acceleration for SSL encrypted connections. The SSL Acceleration feature is a separately licensed component, please contact your local Exinda representative if you wish to enable this feature.
Edge Cache Acceleration	Provides acceleration of static web content such as HTML, GIF, JPEG, ZIP, RAR, ISO as well as dynamic content including YouTube, Google Video, Vimeo.

The Application Acceleration section of the Exinda appliance System Setup allows you to configure and fine-tune various Acceleration related parameters. The configuration pages include:

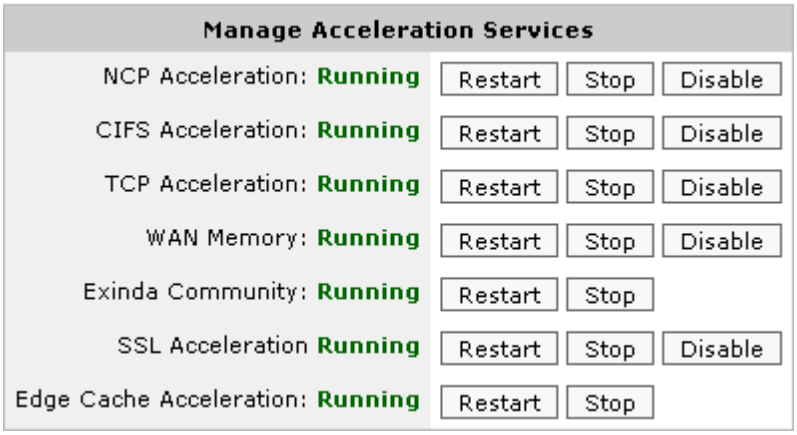
- Services: Start/Stop/Disable Application Acceleration services.
- Community: Configure Exinda Community settings.
- TCP Acceleration: Configure and fine-tune TCP Acceleration settings.
- WAN Memory: Configure and fine-tune WAN Memory settings.
- CIFS Acceleration: Configure and fine-tune CIFS Acceleration settings.
- SSL Acceleration: Configure SSL Acceleration settings.
- Edge Cache Acceleration: Configure Edge Cache settings.

4.3.1 Services

The Acceleration Services page allows you to Start/Stop/Disable the Application Acceleration Services running on the Exinda appliance.

Note: To control Acceleration Services, navigate to 'System | Acceleration | Services' on the Web UI, advanced mode.

The table below lists all the Application Acceleration Services running on the Exinda appliance and allows you to Start, Restart (if already running), Stop and Disable them.



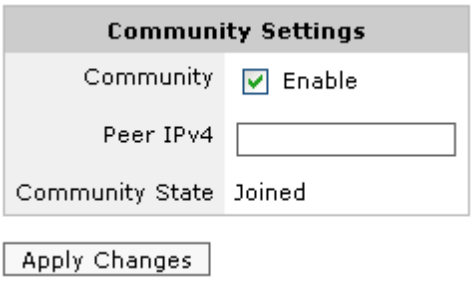
Note: Stopping or restarting running Acceleration Services may impact connections that are currently accelerated.

4.3.2 Community

The Exinda Community is referred to as the collection of Exinda appliances in a user's network. Exinda appliances that are part of the same community can accelerate to/from each other.

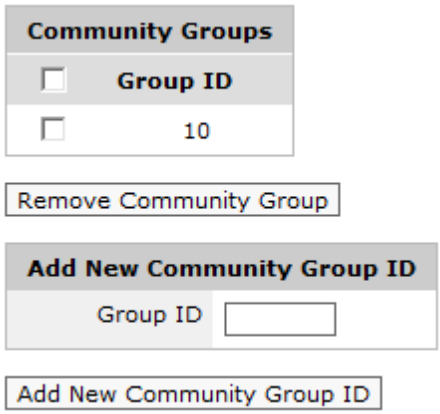
Note: To configure the Exinda Community, navigate to 'System | Acceleration | Community' on the Web UI, advanced mode.

The form below allows you to optionally specify the IPv4 address of any other Exinda appliance in your Exinda Community. Generally, Exinda appliances automatically discover each other when attempting Application Acceleration, however, if auto-discovery is not working, you may manually specify the IPv4 address of another Exinda appliance here.



Note: If you need to manually specify the IP address of another Exinda appliance, try to use the same appliance for all Exinda appliances. For example, specify the IP address of a Head Office or Datacenter Exinda appliance.

Community Groups allow you to create multiple, separate Exinda Communities in the same network. You may wish to isolate Application Acceleration between several Exinda appliances in your network. Use the form below to add/remove the Exinda appliance to Community Groups by specifying an ID. An Exinda appliance can belong to multiple Community Groups. The default Community id is 0.



As a security measure, the Community Group ID can be used like a PIN to restrict access to any other Exinda appliance from joining your community.

Example: In a network, there are 2 WANs. A VPN-based WAN and a MPLS-based WAN. I want all the Exinda appliances in the VPN-based WAN to accelerate to each other and I want all Exinda appliances in the MPLS-based WAN to accelerate to each other. But I don't want the VPN-based Exinda appliances accelerating with the MPLS-based Exinda appliances. The 2 WANs also both access a Datacenter where there is a single Exinda appliance:

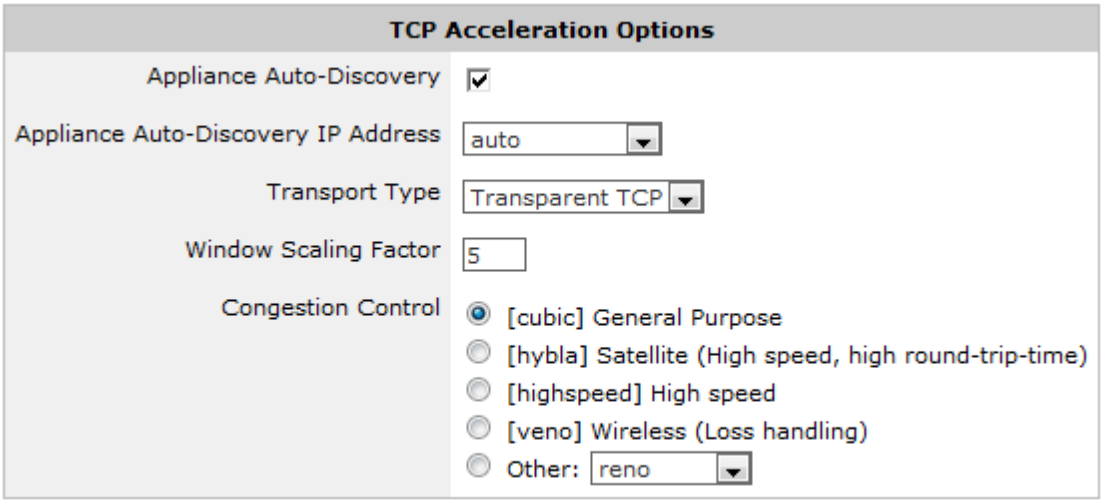
Exinda appliances at VPN-based sites: Community Group ID: 10
Exinda appliances at MPLS-based sites: Community Group ID: 20
Exinda appliance at Datacenter Community Group ID: 10 and 20

4.3.3 TCP Acceleration

TCP Acceleration is the heart of Exinda's Application Acceleration technology. All accelerated connections will be passed through TCP Acceleration.

Note: To configure the TCP Acceleration settings, navigate to 'System | Acceleration | TCP' on the Web UI, advanced mode.

Use the form below to configure various TCP Acceleration settings:



Auto Discovery	If enabled, the Exinda appliance will attempt to automatically discover other Exinda appliances on the network when making acceleration attempts. Exinda appliances do this by injecting TCP Option 30 into any TCP-SYN packets that the Exinda appliance is attempting to accelerate. If unknown TCP options are removed or blocked by other equipment in your network (e.g. VPN terminators, firewalls, IPS/IDS systems, etc) then auto-discover may not work or traffic may be blocked. If this setting is disabled or if TCP option 30 is stripped or blocked by other equipment on your network, you will need to manually specify the location of another Exinda appliance in your network on the 'System | Acceleration | Community' page.
Auto Discovery IP Address	This is the IP address the Exinda appliance will use when notifying other Exinda appliances about how to connect back to itself. Usually this is the management IP address or the IP address to which the default route is associated.
Transport Type	There are 2 acceleration Transport Types available. The default, Transparent TCP, ensures Exinda's Application Acceleration is fully transparent. Source and Destination IP addresses and Port numbers are maintained on all accelerated connections, so any equipment in between 2 accelerating Exinda appliances can still see correct IP and TCP headers.

	The other option, Protocol 139, still preserves the original IP header of the accelerated connection, but tunnels the connection over IP protocol 139, so it no longer appear as TCP. This mode is useful if you have equipment in between 2 accelerating Exinda appliances the strips or blocks TCP option 30.
Window Scaling Factor	The Window Scaling Factor determines how large the TCP window is allow to grow per connection. The TCP window size is calculated using the following formula: TCP Window Size (kbytes) = 64 kbytes x 2 ^ Window Scaling Factor. The default Window Scaling Factor is 5, which equates to a TCP window of 2Mbytes. Larger window sizes result in more potential memory usage, however, this value may need to be increased in high-bandwidth, high-latency environments.
Congestion Control	There are various types of congestion control algorithms that can be used depending on the type of WAN. The most common congestion control algorithms are listed together with their intended usage. Set this according to the type of WAN the Exinda appliances are deployed into. This setting only affects outbound traffic to the WAN, so the same setting should be applied to all Exinda appliances on the WAN.

Note: The Exinda appliance uses TCP Option 30 to facilitate transparent TCP Acceleration and Appliance Auto Discovery. Any equipment between the Exinda appliances must not block or strip TCP option 30 otherwise transparent TCP Acceleration and Appliance Auto Discovery will not work.

Caution: These settings are exposed for advanced users and should only be changed after consultation with an Exinda representative.

There is one additional TCP Acceleration setting that is only available via the CLI. This is an advanced setting that controls how TCP Acceleration behaves when more than one bridge is accelerating traffic and it is enabled by default.

```
[no] acceleration tcp dual-bridge-bypass
```

The Dual Bridge Bypass option should be enabled when an accelerated connection needs to pass through multiple bridges on the same appliance. For example, if the accelerated traffic arrives on br0, gets decellerated and then routed back through br1 of the same appliance, this option needs to be enabled.

The Dual Bridge Bypass option should be disabled if accelerated packets from a single connection could arrive on more than one bridge. This behaviour is typically exhibited when packet-based load balancing is used.

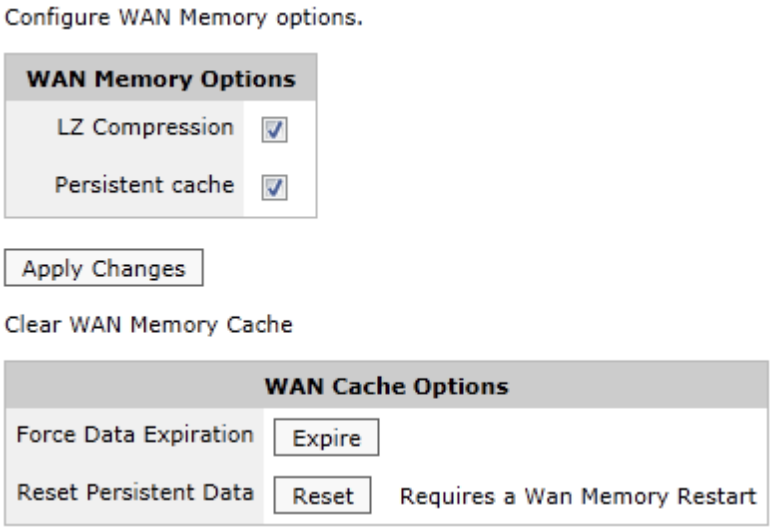
Note: For more information on TCP Acceleration, refer to Appendix A.

4.3.4 WAN Memory

WAN Memory is the data de-duplication module of Exinda's Application Acceleration Technology. It is a bi-directional and universal byte-level cache that stores repetitive patterns on the Exinda appliances's hard disk drive and uses these patterns to compress accelerated traffic between 2 or more Exinda appliances.

Note: To configure the WAN Memory settings, navigate to 'System | Acceleration | WAN Memory' on the Web UI, advanced mode.

Use the form below to configure WAN Memory settings:



LZ Compression	If selected, in addition to data de-duplication, WAN Memory will also attempt to compress accelerated traffic with a standard LZ-based compression algorithm.
Persistent Cache	If selected, the WAN Memory patterns stored on the Exinda appliance's hard disk will survive a system reboot.
Force Data Expiration	Use this button to expire the entire WAN Memory cache, thereby removing any patterns stored on the Exinda appliance's hard disk drive. This may take several minutes depending on the amount of data.
Reset Persistent Data	Use this button to tell WAN Memory NOT to load any persistent data from the hard disk next time it starts. Using this function and restarting the WAN Memory service is a quick way to clear the WAN Memory cache.

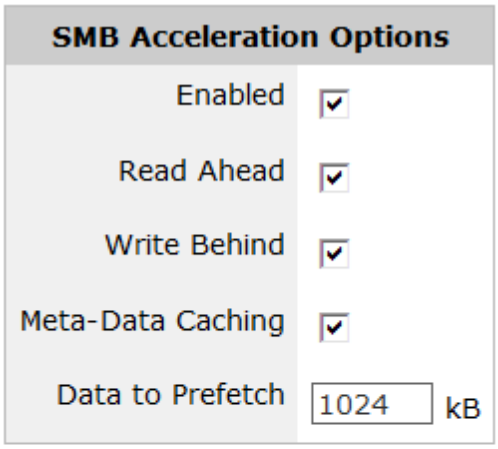
Note: Each Exinda appliance running WAN Memory will connect to each other in order to maintain cache synchronization. This communication happens over TCP port 8013, so this port must be open and available between all Exinda appliances. For security purposes, data sent across these WAN Memory synchronization connections is obfuscated.

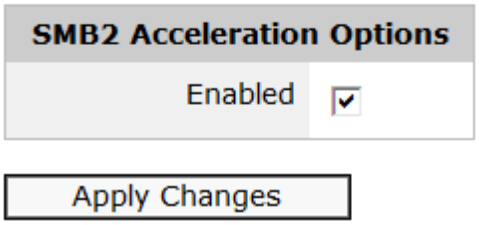
4.3.5 SMB/SMB2 Acceleration

SMB/SMB2 Acceleration is the SMB2-specific component of Exinda's Application Acceleration Technology. The SMB2 module pre-fetches and caches SMB2 requests to reduce the severe effect high network latency has on the SMB2 protocol.

Note: To configure SMB/SMB2 Acceleration settings, navigate to 'System | Acceleration | SMB/SMB2' on the Web UI, advanced mode.

Use the form below to configure the various SMB2 Acceleration settings:





Read Ahead	When enabled, SMB Acceleration will pre-fetch data for SMB reads. The Exinda appliance will fetch data from the SMB server and start transmitting it over the WAN before the client requests it.
Write Behind	When enabled, SMB Acceleration will buffer data for SMB writes.

Meta-Data Caching	When enabled, SMB Acceleration will cache SMB metadata.
Pre-fetch Data	This is the amount of data CIFS Acceleration should pre-fetch when performing read-ahead or write-ahead pre-fetching. This value should only be increased if network latency is very large (> 500 msec).

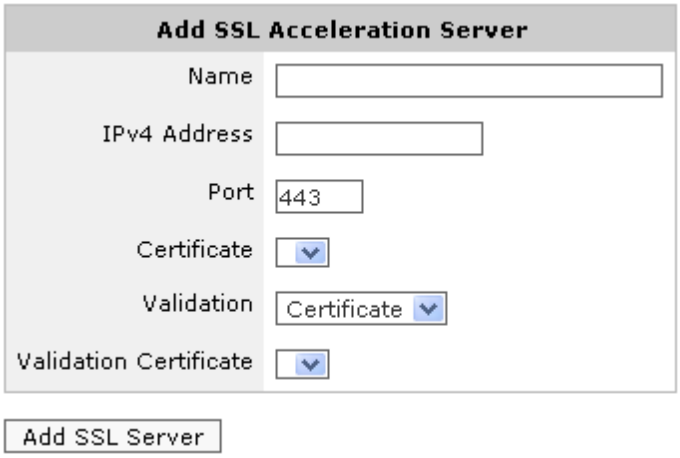
Note: For more information on SMB/SMB2 Acceleration, refer to Appendix B.

4.3.6 SSL Acceleration

SSL Acceleration provides acceleration of SSL encrypted TCP sessions by intercepting SSL connections to configured servers and decrypting them, performing acceleration techniques, then re-encrypting them again.

Note: The SSL Acceleration feature is a separately licensed component, please contact your local Exinda representative if you wish to enable this feature.

The table at the top of the page shows the current configured SSL Acceleration Servers. You can Edit or Delete these as required. Use the form below to add a new SSL Acceleration Server.



Name	Specify a name for the server/application you wish to enable for SSL Acceleration.
IPv4 Address	Specify the IPv4 address of the server running the SSL enabled application.
Port	Specify the port number running the SSL enabled application on the server.

Certificate	Select the Certificate to use for re-encryption of the SSL session. The certificates available here are those that are configured in the Certificates section.
Validation	Select the type of validation to apply to the server's certificate. Options are None, Certificate or Reject. • **None** means that SSL Acceleration will accept and process the connection even if the server's SSL certificate is invalid or expired. • **Reject** means that SSL Acceleration will not process the connection if the server's SSL certificate is invalid or expired. The connection will still be accelerated, but not SSL accelerated. • **Certificate** means that SSL Acceleration will accept and process the connection only if the server's certificate matches the validation certificate, specified below. Otherwise, the connection is not processed.
Validation Certificate	If 'Certificate' is selected as the validation method above, this is the certificate that's used to validate against the server's certificate.

Note: For further information, consult the SSL Acceleration How to Guide.

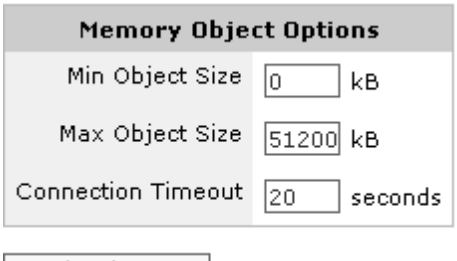
4.3.7 Edge Cache

Edge Cache provides acceleration of HTTP based applications by caching objects in memory and on disk. Edge Cache acceleration is single-sided - acceleration requires only one Exinda appliance.

Note: To configure Edge Cache Acceleration settings, navigate to 'System | Acceleration | Edge Cache' on the Web UI, advanced mode.

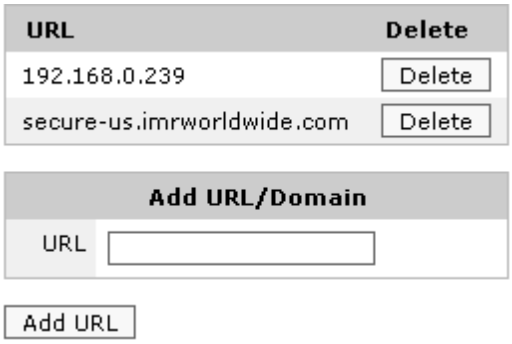
Note: The Edge Cache Acceleration feature is a separately licensed component, please contact your local Exinda representative if you wish to enable this feature.

Use the form below to configure Edge Cache. To see throughput and other Edge Cache statistics, navigate to Monitor | Acceleration | Edge Cache.

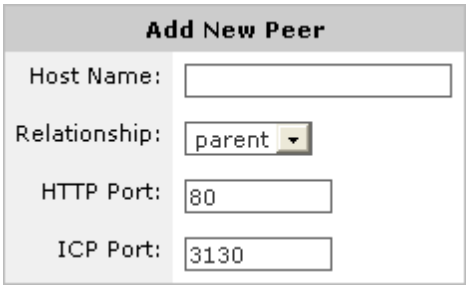


Min Object Size	Objects with a size less then this value will not be cached.
Max Object Size	Objects with a size larger then this value will not be cached.
Connection Timeout	The amount of time Edge Cache will wait for a response from the WAN when loading objects.

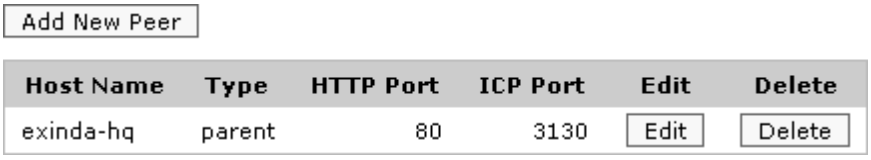
Use the form below to configure URL's that should never be cached.



Exinda appliances with Edge Cache can establish a community of peers in order to share objects between caches. Currently configured peers are shown in the table below:



Click on 'Add New Peer' or 'Edit' to add a new peer or edit an existing peer.



Host Name	The hostname of the peer
Relationship	Peer relationship. Only Parent is supported at present.
HTTP Port	The peer HTTP port
ICP Port	The peer ICP port

Note: For more information refer to the Edge Cache HowTo Guide.

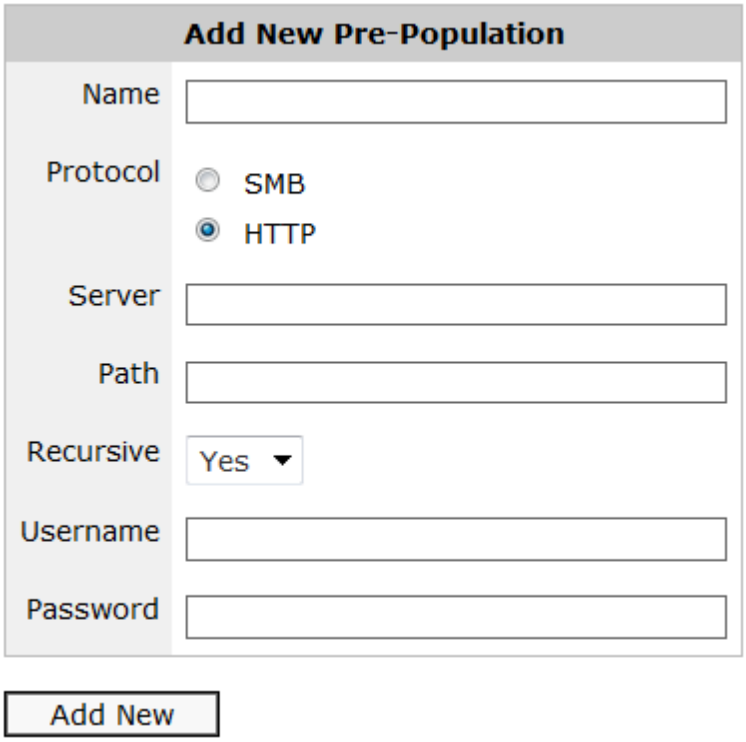
4.3.8 Pre Population

SMB/HTTP Pre Population & Object Cache

The Object Cache works like Edge Cache for SMB and HTTP traffic. It is independent of WAN Memory and uses the same resources without duplication for both SMB and SMB2 traffic.

With data in the cache, the Exinda appliance handles read and write requests as “warm” data transfers, sending only new or modified data even though complete files may have been requested, thereby reducing the overall traffic volumes and significantly increasing the rate of data transfer over the WAN.

Pre-population of Object Cache with SMB and/or HTTP data allows customers to make sure their cache is ready to go before any traffic passes through the Exinda appliance. Either specific files or entire directory structures can be specified and fed into the Object Cache. Pre-population can even be scheduled to occur at a future time convenient to the network, reducing network strain and making better use of less utilized “off-hour” bandwidth.



Name	The name of the Pre-Population job.
Protocol	The protocol of the files to be Pre-Populated. HTTP and SMB/SMB2 protocols are supported.
Server	The server from which the Pre-Population data will be retrieved. (For example, "www.exinda.com")
Path	The path to the Pre-Population data on the server. (For example, "/data/resources")
Recursive	Select "Yes" to Pre-Populate content from subfolders as well as the root folder.
Username	The username for access to the server.
Password	The password for access to the server.

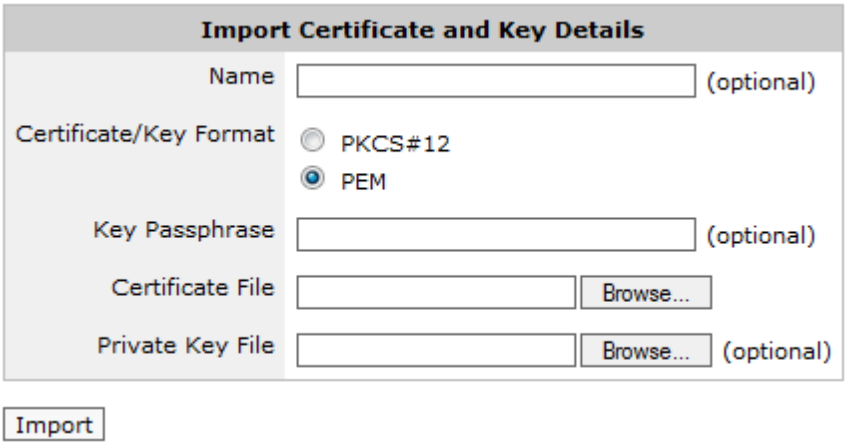
4.4 Certificates

The Certificates section allows you to import SSL Certificates and Private Keys for use in SSL Acceleration.

Note: The SSL Acceleration feature is a separately licensed component, please contact your local Exinda representative if you wish to enable this feature.

The table at the top of the page shows the current configured Certificates and Private Keys. The Validity cell will be highlighted yellow if the certificate is due to expire within 30 days, or it will be highlighted red if the certificate has already expired. You can View or Delete these as required.

Use the form below to import Certificates and Private Keys.



Name	Specify a new for the Certificate/Private Key pair. If no name is supplied, the filename of the uploaded certificate file is used.
Certificate/Key Format	Select either PKCS#12 or PEM as the format.
Key Passphrase	If the the Certificate/Private Key is password protected, specify the pass phrase here.
Certificate File	Choose the Certificate file to upload.
Private Key File	If the Private Key is not embedded in the Certificate file, specify the matching Private Key file to upload.

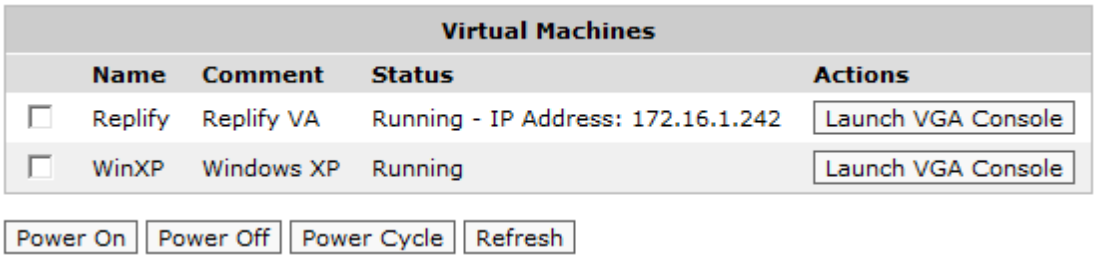
Note: For further information, consult the SSL Acceleration How to Guide.

4.5 Virtualization

The Virtualization feature allows Virtual Machines to be run on the the Exinda appliance.

Note: Virtualization requires an additional, optional license before this feature can be configured and used. Please contact Exinda TAC or your local Exinda representative if you do not have this license and you wish to use this feature.

Most of the Virtualization configuration is performed using the "virt" CLI command. The table below show all configured Virtual Machines and provides the ability to Power them ON, OFF or restart (cycle) them. You can also view the VGA console for each Virtual Machine. The VA console uses a Java-based applet to launch secure SSH-based protocol to encrypt the session. You will need to have Java installed and enabled as well as direct SSH access to the Exinda appliance in order to use this feature. You will also need to authenticate with your username and password.



Note: For further information, consult the Virtualization How to Guide.

4.6 Authentication

The Authentication section of the Exinda appliance System Setup allows you to configure Local User Accounts, as well as remote authentication mechanisms such as LDAP (including Active Directory), Radius or TACACS+. The various configuration pages include:

- Active Users: View a list of currently logged in users.
- Local User Accounts: Configure local usernames and passwords.
- AAA: Specify how users are authenticated and authorized on the Exinda appliance.
- LDAP: Configure remote LDAP authentication servers.
- Radius: Configure remote Radius authentication servers.
- TACACS+: Configure remote TACACS+ authentication servers.

4.6.1 Active Users

Active Users lists the users currently logged into either the Web UI or the CLI.

Note: To view the users currently logged in, navigate to 'System | Authentication | Active Users' on the Web UI, advanced mode.

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

4.6.2 Local User Accounts

Local User Accounts allows you to add/remove local user accounts as well as change local user's passwords.

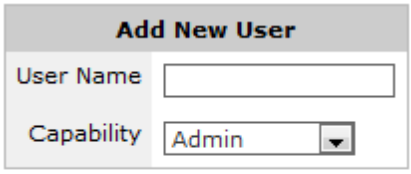
Note: To configure Local User Accounts, navigate to 'System | Authentication | Local User Accounts' on the Web UI, advanced mode.

The table at the top of the page lists the configured local users and their capabilities. You can use this to remove local user accounts from the Exinda appliance or to temporarily disable an account.

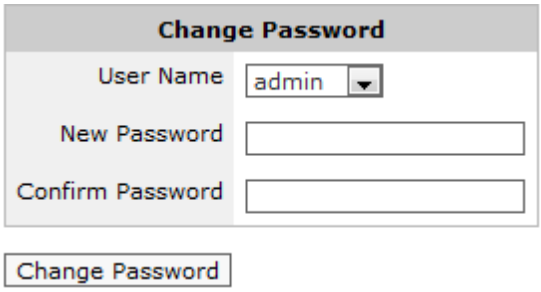
Local Users			
	User	**Capability**	**Enabled**
☐	admin	admin	☑
☐	monitor	monitor	☑

Remove User | Enable User | Disable User

To add a new Local User Account, use the form below. Specify a username and select a capability. Admin users have full read-write access to the Exinda appliance. Monitor users have read-only access.



By default, new users are created without a password. Use the form below to create a password for a new user, or change the password for an existing user.



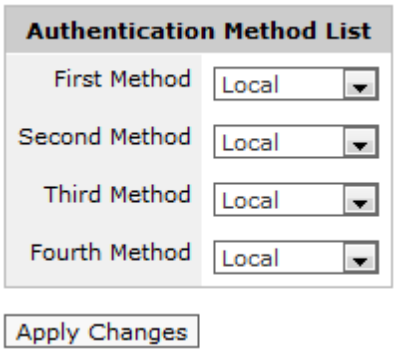
Select the username you wish to create/change the password for and enter their new password.

4.6.3 AAA

AAA configures how remote users should authenticate to the Exinda appliance and what privileges they should receive.

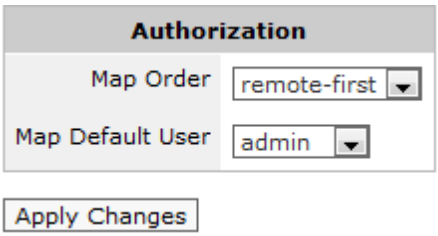
Note: To configure AAA, navigate to 'System | Authentication | AAA' on the Web UI, advanced mode.

The form below should be used to specify the order in which users are authenticated. When a user logs in, the Exinda appliance will try to authenticate them using the authentication methods specified here, in the order they are configured.



Note: This setting is required if you are using a remote access mechanism such as LDAP, Radius or TACACS+.

Use the following form to control what privileges remotely authenticated users receive when they login to the Exinda appliance.



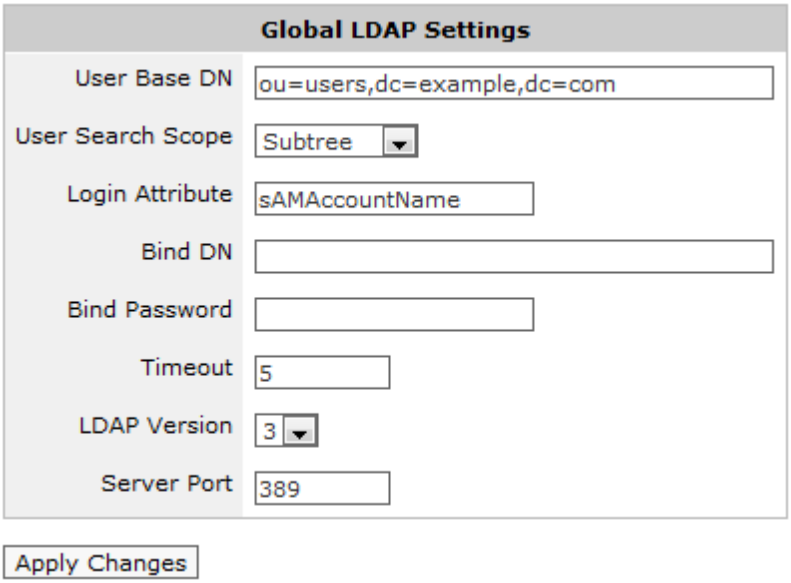
Map Order	remote-first	Apply user privileges supplied by the remote authentication mechanism first. If that fails, use the 'Map Default User' setting below.
	remote-only	Apply user privileges supplied by the remote authentication mechanism first. If that fails, the user will not be authenticated.
	local-only	Use the 'Map Default User' setting below.
Map Default User		If the 'local-only' option is selected above, the user will be given the same privileges as the local user account selected here.

4.6.4 LDAP Authentication

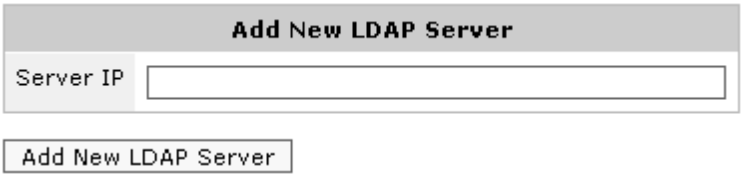
LDAP authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote LDAP (including Active Directory) server.

Note: To configure LDAP Authentication, navigate to 'System | Authentication | LDAP' on the Web UI, advanced mode.

Use the form below to define global LDAP authentication options.



Use the form below to specify connection details to the remote LDAP server. IPv4 or IPv6 addresses can be specified. Multiple LDAP servers may be defined. The table at the top of the page allows you to enable/disable/remove defined LDAP servers.



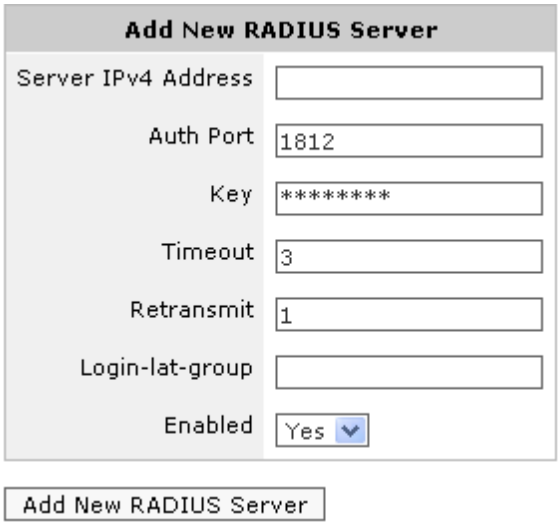
Note: 'LDAP' must be selected as an Authentication Method on the 'System | Authentication | AAA' page on the Web UI, advanced mode, in order for the Exinda appliance to attempt LDAP authentication.

4.6.5 Radius Authentication

Radius authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote Radius server.

Note: To configure Radius Authentication, navigate to 'System | Authentication | Radius' on the Web UI, advanced mode.

Use the form below to specify connection details to the remote Radius server. Multiple Radius servers may be defined. The table at the top of the page allows you to enable/disable/remove defined Radius servers. Only IPv4 addresses are supported for Radius servers.



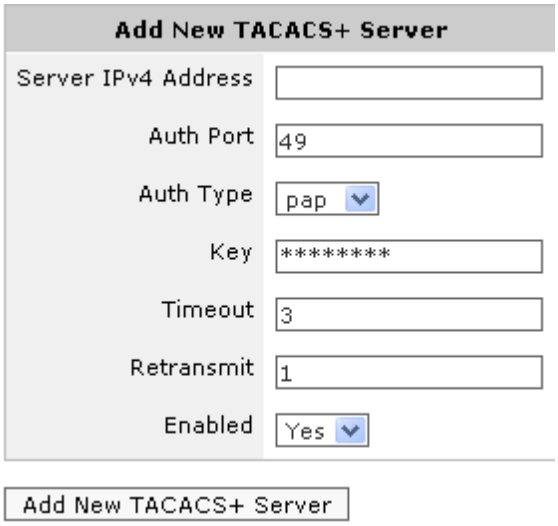
Note: 'RADIUS' must be selected as an Authentication Method on the 'System | Authentication | AAA' page on the Web UI, advanced mode, in order for the Exinda appliance to attempt Radius authentication.

4.6.6 TACACS+ Authentication

TACACS+ authentication allows you to configure the Exinda appliance to authenticate user login attempts with a remote TACACS+ server.

Note: To configure TACACS+ Authentication, navigate to 'System | Authentication | TACACS+' on the Web UI, advanced mode.

Use the form below to specify connection details to the remote TACACS+ server. Multiple TACACS+ servers may be defined. The table at the top of the page allows you to enable/ disable/remove defined TACACS+ servers. Only IPv4 addresses are supported for TACACS+ servers.



Note: 'TACACS+' must be selected as an Authentication Method on the 'System | Authentication | AAA' page on the Web UI, advanced mode, in order for the Exinda appliance to attempt TACACS+ authentication.

4.7 System Logging

The System Logging section of the Exinda appliance System Setup allows you to view and configure the System Log files.

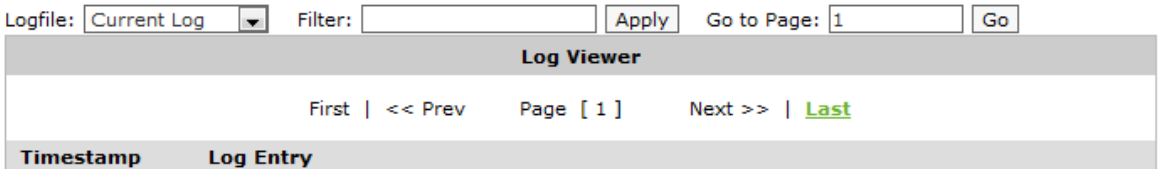
- View Log Files: View and search the System Log files.
- Live Log: View real-time entries to the System Log file.
- Tail Log: View the most recent entries to the System Log file.
- System Logging Configuration: Configure various System Logging settings, including remote syslog servers.

4.7.1 View Log Files

The View Log Files page allows you to view the System Log files and filter out various log messages. Log files provide an inside into the Exinda appliance's operation and aid in troubleshooting.

Note: To View the System Log, navigate to 'System | Logging | View' on the Web UI, advanced mode.

The form below allows you to navigate through the log files as well as enter a filter to narrow down the entries displayed.



Note: By default, the 'Current Log' is displayed. The Exinda appliance will also periodically archive log files. These archived log files can also be viewed by selecting them from the 'Logfile' drop-down.

4.7.2 Live Log

The Live Log page allows you to view new entries to the System Log in real-time.

Note: To view the Live Log, navigate to 'System | Logging | Live Log' on the Web UI, advanced mode.

A dot/period (.) character will be displayed after a few seconds of inactivity to indicate the Live Log is still active.

4.7.3 Tail Log

The Tail Log page allows you to view the most recent entries in the system log file.

Note: To Tail the System Log, navigate to 'System | Logging | Tail Log' on the Web UI, advanced mode.

The form below allows you to configure how many lines to view and in which order to display the log entries.

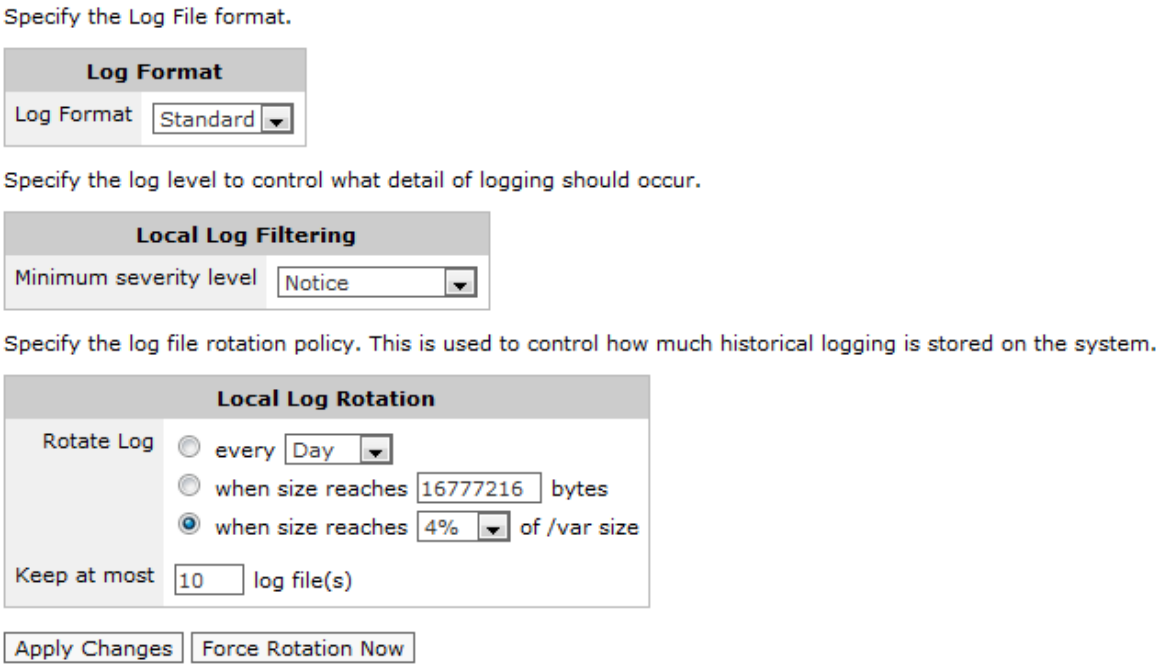
Clicking the 'Go' button will refresh this page and will ensure any new log entries since the list time this page was refreshed are displayed.

4.7.4 System Logging Configuration

The System Logging Configuration page allows you customize various aspect of System Logging, including exporting to remote syslog servers.

Note: To configure System Logging, navigate to 'System | Logging | Setup' on the Web UI, advanced mode.

The form below allows you configure System Logging properties.



Log Format	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.
Minimum severity level	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.
Rotate Log	Select the desired log rotation policy.
Keep at most	Specify how many rotated/archived log files should be kept before they are permanently removed from the Exinda appliance.

You can also force System Log rotation immediately, by clicking the 'Force Rotation Now' button.

The form below is used to add remote syslog servers to the Exinda appliance. This allows you to forward system log entries at a defined severity level to one or more remote syslog servers. Only IPv4 addresses are supported for remote sinks.

IP address	Enter the IP Address of the remote syslog server.
Minimum Severity	Select the severity level of log entries that should be sent to the remote syslog server. Any log entry with this severity level or lower r will be sent.

4.8 System Diagnostics

System Diagnostics provide troubleshooting assistance in cases of system and network issues. The various diagnostics pages include:

- Alerts Status: View status of system alerts.
- Diagnostics Files: Generate and download diagnostics files.
- TCP Dump: Run and download a TCP dump.
- Community Diagnostics: View community diagnostics.
- Acceleration Diagnostics: View TCP acceleration, WAN memory and CIFS acceleration diagnostics.
- Monitor Diagnostics: View monitoring diagnostics.
- Optimizer Diagnostics: View optimizer diagnostics.
- NIC Diagnostics: View NIC diagnostics.
- RAID Diagnostics: View RAID adapter, logical and physical drive information.

4.8.1 Alert Status

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. Click on the 'Warning' to view the alert that has triggered it. The table below lists the alerts and specifies the status, the time it was last triggered and how many times. Resetting the alert will change the system health status to 'OK'. For further troubleshooting click on the offending alarm.

Note: To disable/enable system alerts, navigate to 'System | Setup | Alerts' on the Web UI, advanced mode.

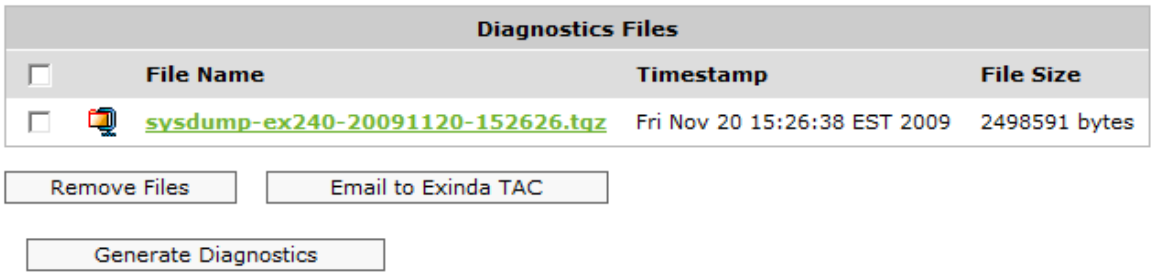
Alarm	Status	Last Triggered	Count	
CPU Utilization	OK			Reset
System Disk Full	OK			Reset
Memory Paging	OK			Reset
Bridge Link	OK	Wed Apr 11 13:38:29 EST 2012	2	Reset
Bridge Direction	OK			Reset
Link Negotiation	DISABLED			Reset
NIC Problems	OK			Reset
NIC Collisions	OK			Reset
NIC Dropped Packets	OK	Wed Apr 11 13:40:00 EST 2012	1	Reset
Redundant Power	Not Available			Reset
Redundant Storage	Not Available			Reset
Accelerated Connections	OK			Reset
Asymmetric Route Detection	OK			Reset

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
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.
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	Alert raised when errors are present on the interfaces.

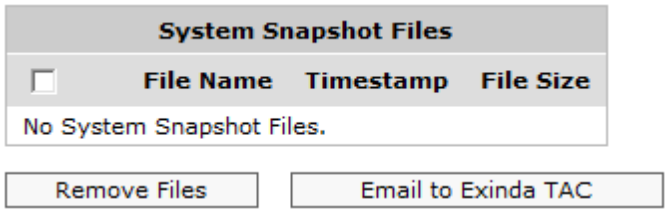
Bridge Link	Alert raised when one of the links of an enabled bridge is down.
Bridge Direction	Alert raised when the appliance cabling is incorrect. In most cases, it indicates the Exinda WAN interface has been incorrectly plugged into the LAN and vice versa.
CIFS signed connections	Alert raised when CIFS 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).
Accelerated Connections	Alert raised when the number of accelerated connections exceeds the licensed limit. Connections over the licensed limit pass through not accelerated.
Asymmetric Route Detection	alert raised when asymmetric routing is detected.

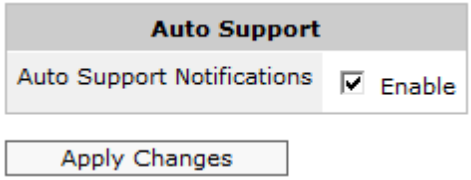
4.8.2 Diagnostics Files

Diagnostics files contain system state information and can aid in troubleshooting. Diagnostics files may be requested by Exinda TAC and can be generated and downloaded using the form below.



System snapshots are automatically generated when a process fails. If the 'Auto Support Notifications' option is enabled, they are automatically sent to Exinda TAC for further troubleshooting.

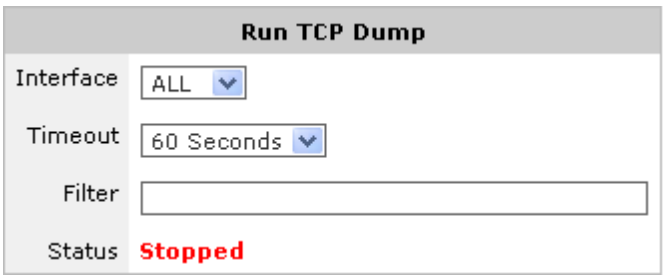




Note: Valid SMTP and DNS settings are required for diagnostics to be sent to Exinda TAC.

4.8.3 TCP Dump

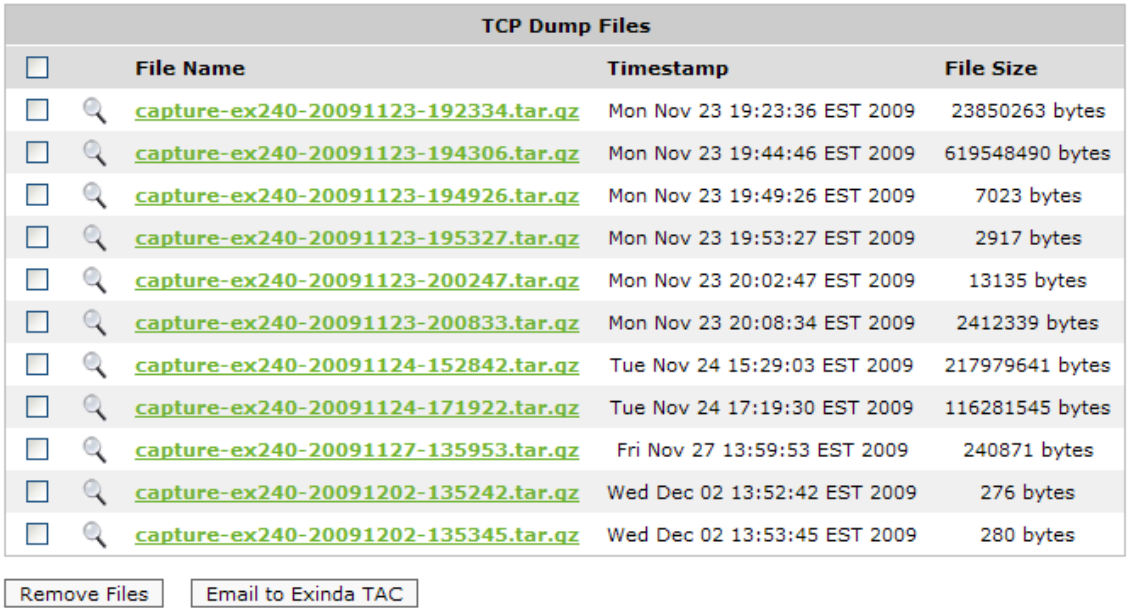
The following form can be used to generate a TCP Dump on the Exinda appliance. A TCP Dump captures packets being transmitted or received from the specified interfaces and can assist in troubleshooting. A TCP Dump may be requested by Exinda TAC.



Note: when ALL is selected for the Interface, only those interfaces which are link up will be included.

Interface	Select an interface to run the TCP dump on. Select ALL to capture packets on all (link up) interfaces.
Timeout	Select the time for which the TCP Dump will run.
Filter	Set a filter if required. More information on tcpdump filters is available at www.tcpdump.org
Status	Shows the status of a running TCP Dump

Saved TCP Dumps can then be downloaded and/or emailed to Exinda TAC using the form below.



TCP Dump Files

	File Name	Timestamp	File Size
	capture-ex240-20091123-192334.tar.gz	Mon Nov 23 19:23:36 EST 2009	23850263 bytes
	capture-ex240-20091123-194306.tar.gz	Mon Nov 23 19:44:46 EST 2009	619548490 bytes
	capture-ex240-20091123-194926.tar.gz	Mon Nov 23 19:49:26 EST 2009	7023 bytes
	capture-ex240-20091123-195327.tar.gz	Mon Nov 23 19:53:27 EST 2009	2917 bytes
	capture-ex240-20091123-200247.tar.gz	Mon Nov 23 20:02:47 EST 2009	13135 bytes
	capture-ex240-20091123-200833.tar.gz	Mon Nov 23 20:08:34 EST 2009	2412339 bytes
	capture-ex240-20091124-152842.tar.gz	Tue Nov 24 15:29:03 EST 2009	217979641 bytes
	capture-ex240-20091124-171922.tar.gz	Tue Nov 24 17:19:30 EST 2009	116281545 bytes
	capture-ex240-20091127-135953.tar.gz	Fri Nov 27 13:59:53 EST 2009	240871 bytes
	capture-ex240-20091202-135242.tar.gz	Wed Dec 02 13:52:42 EST 2009	276 bytes
	capture-ex240-20091202-135345.tar.gz	Wed Dec 02 13:53:45 EST 2009	280 bytes

Remove Files Email to Exinda TAC

Note: Valid SMTP and DNS settings are required for TCP Dumps to be sent to Exinda TAC.

4.8.4 Community Diagnostics

The community diagnostics display the state of the community and details of the individual hosts that have joined.

Note: To configure Community settings, navigate to 'System | Acceleration | Community' on the Web UI, advanced mode.

```
State:              Joined
Enabled:            true
Network Forwarding: true
Community Group:    10

Global Settings

Nodes
   Host ID:      00e0ed13e792
   IP Address:   172.16.1.240
   Lost State:   found
   Last Contact: N/A
   Hostname:     ex240
   Version:      5.5.0.12115

   Host ID:      0060e0e1c49c
   IP Address:   172.16.101.3
   Lost State:   found
   Last Contact: 2009/12/02 14:29:37 (18s ago)
   Hostname:     jb-exinda
   Version:      5.5.0.12035
```

4.8.5 Acceleration Diagnostics

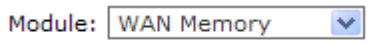
Acceleration diagnostics aid in troubleshooting TCP Acceleration, CIFS Acceleration and WAN Memory issues. To view acceleration diagnostic select the relative module from the drop down list.

The TCP Acceleration diagnostics display the current configuration settings as well as the number of new and concurrent accelerated connections.

```
Configuration
   Congestion Control Algorithm: bic
   Transport Mode:               transparent
   Window Scale:                 5
   Appliance Discovery Enabled:  yes

Concurrent Accelerated Connections:      85
New connections per second:              0
Peak Concurrent Accelerated Connections: 162
```

Note: To configure TCP acceleration settings, navigate to 'System | Acceleration | TCP' on the Web UI, advanced mode.

Note: To view the licensed limit of accelerated connections, navigate to 'System | Setup | License' on the Web UI, advanced mode.

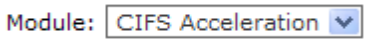


The WAN memory Acceleration diagnostics display the current configuration settings as well as reduction statistics for the individual hosts.

View WAN Memory Logs

```
Configuration
   Reduction LZ compression on:           yes
   Reduction small matching on:           no
   Reduction small matcher always list:   Lotus Notes
   Persistence enabled:                   yes

Statistics
   Disk available:              262.71G
   Disk used:                   2218.98M (0.825%)
   Persistence active:          yes
   Persistence loading:         no
   Persistence clear pending:   no

   TX reduction:                51.53%
   TX bytes in:                 71.03M
   TX bytes out:                34.43M
   TX small matcher bytes in:   0
   TX small matcher bytes out:  0

   RX reduction:                27.32%
   RX bytes in:                 831.57k
   RX bytes out:                1144.08k

Peer 0060e0e22eb8 state
   Status:               ONLINE
   Last status change:   2011/05/25 12:33:10 (23h 42m 27s)
   IP address:           172.16.20.130
   Connections:          0
   Disk cache status:    Active
   Version info:         0k/24 (local:23-24 remote:23-24)

   TX reduction:         34.35%
   TX bytes in:          1000.17k
   TX bytes out:         656.6k

   RX reduction:         32.22%
   RX bytes in:          167.53k
   RX bytes out:         247.16k
```

Note: To configure WAN memory acceleration settings, navigate to 'System | Acceleration | WAN memory' on the Web UI, advanced mode.



The CIFS Acceleration diagnostics display the current configuration settings as well as the number of new and concurrent accelerated connections. If CIFS signed connection are present, the total number of signed connections will be also displayed.

```
Configuration
   Enabled:                    yes
   Read-ahead enabled:         yes
   Write-ahead ahead:          yes
   Transaction acceleration:   yes
   Disk temporary file cache: 536870912B
   Data to prefetch:           1024 kB

Concurrent connections:  1
Accelerated connections: 1
Signed connections:      0

No signed servers detected
```

Note: To configure CIFS acceleration settings, navigate to 'System | Acceleration | CIFS on the Web UI, advanced mode.

4.8.6 Monitor Diagnostics

The monitor diagnostics display the current monitor settings and the status of monitor and collector processes.

Note: To configure Monitor settings, navigate to '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
```

4.8.7 Optimizer Diagnostics

The optimizer diagnostics display the current optimizer status and the optimizer configuration.

```
Optimizer Status: Started
Restart Required: no
Show VC Totals:   no
Global QOS:   no

Optimizer Configuration:

Chain PREROUTING (policy ACCEPT 9538K packets, 3714M bytes)
 pkts bytes target     prot opt in     out     source               destination
  76M   36G ACCEPT     !icmp --  *      *       0.0.0.0/0            0.0.0.0/0           NET match ignore
  20M   16G BRIDGE_PORT  all  --  br+    *       0.0.0.0/0            0.0.0.0/0

Chain INPUT (policy ACCEPT 13M packets, 13G bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 83M packets, 39G bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 8366K packets, 5121M bytes)
 pkts bytes target     prot opt in     out     source               destination
1336K  422M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           NET match ignore
    0     0 LOCAL_OUT  all  --  *      br+     0.0.0.0/0            0.0.0.0/0           DIR match inbound
1715K 1183M LOCAL_OUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0           AA match accel DIR match inbound

Chain POSTROUTING (policy ACCEPT 93M packets, 45G bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain ACTION (1 references)
 pkts bytes target     prot opt in     out     source               destination
8583K   12G AA         all  --  *      *       0.0.0.0/0            0.0.0.0/0           socket transparent AA target
 872K  779M AA         all  --  *      *       0.0.0.0/0            0.0.0.0/0           EXPOLICY match accel AA target port 9998
    0     0 COMPRESS_OLD  all  --  *      *       0.0.0.0/0            0.0.0.0/0           EXPOLICY match compress COMPRESS algorithm 48 set-protocol 138

Chain BRIDGE_PORT (1 references)
 pkts bytes target     prot opt in     out     source               destination
  20M   16G DIR_MARK   all  --  *      *       0.0.0.0/0            0.0.0.0/0
  20M   16G HA         all  --  *      *       0.0.0.0/0            0.0.0.0/0
  20M   16G SETAPP     all  --  *      *       0.0.0.0/0            0.0.0.0/0           SETAPP
6581K 3290M UNACCEL    all  --  *      *       0.0.0.0/0            0.0.0.0/0           DIR match inbound
73440 6289K ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           NET match ignore
  17M   15G MON        all  --  *      *       0.0.0.0/0            0.0.0.0/0
  13M   13G ACTION     all  --  *      *       0.0.0.0/0            0.0.0.0/0           DIR match outbound

Chain DIR_MARK (1 references)
 pkts bytes target     prot opt in     out     source               destination
6581K 3290M MARK       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match --physdev-in eth11 MARK xset 0x1001/0xffffffff
  13M   13G MARK       all  --  *      *       0.0.0.0/0            0.0.0.0/0           PHYSDEV match --physdev-in eth10 MARK xset 0x1000/0xffffffff
```

4.8.8 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 '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
```

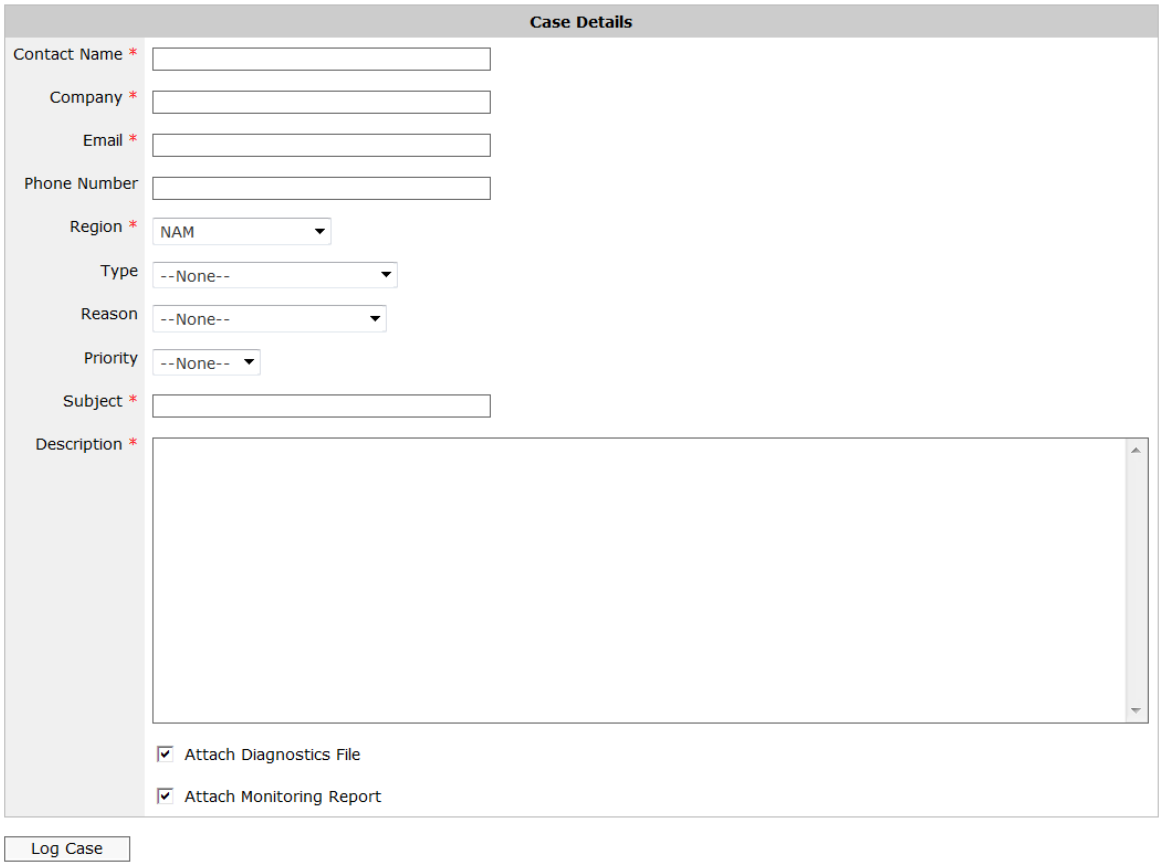
4.8.9 RAID Diagnostics

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]
```

4.8.10 Log a Case

The Log a Case page allows you to log a case with Exinda Support.



Contact Name	Your full name.
Company	The name of your company.
Email	Your email address.
Phone Number	Your phone number.
Region	Your geographical region.
Type	The type of support case.
Reason	The functionality your question relates to.
Priority	Select the appropriate priority from the drop-down list.
Subject	Enter a brief summary of the problem or question.
Description	Enter a detailed description of the problem or question.
Attach Diagnostics File	Keep this option checked to automatically attach a Diagnostics File to your case (recommended).

Attach Monitoring Report	Keep this option checked to automatically attach a Monitoring Report to your case (recommended).

4.9 Maintenance

The Maintenance section of the Exinda appliance System Setup allows you to perform various system maintenance tasks. These include:

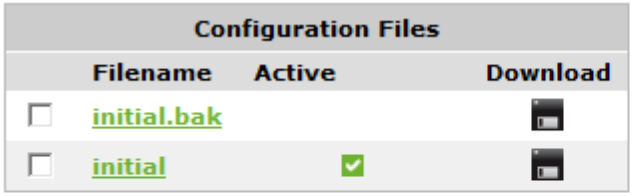
- Manage System Configuration: Allows you to save, activate, switch, revert and delete system configuration files.
- Import System Configuration: Allows you to import previously saved or backed-up system configuration files.
- Clustering / High Availability: View the status of Exinda clustering.
- Firmware Update: Upgrade the ExOS software on the Exinda appliance.
- Factory Defaults: Restore the Exinda appliance to factory default settings.
- Reboot / Shutdown: Reboot or Shutdown the Exinda appliance.

4.9.1 Manage System Configuration

The Manage System Configuration screen allows you to download, save, switch, revert and delete system configuration files.

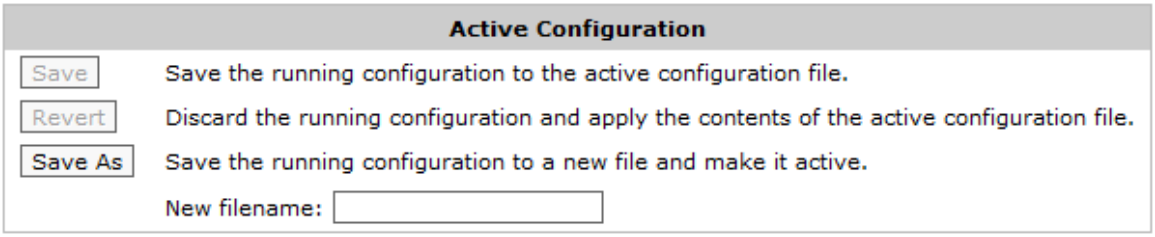
Note: To Manage System Configuration, navigate to 'System | Maintenance | Manage Config' on the Web UI, advanced mode.

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.



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'.



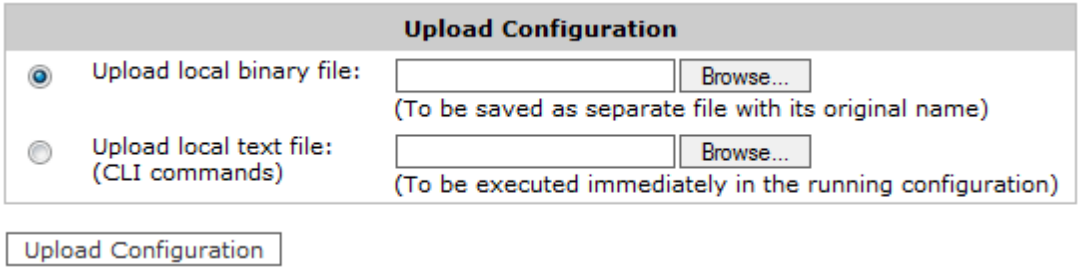
You can save the running configuration and make it the active configuration, revert the running configuration back to the previously saved state of the active configuration, or save the running configuration to a new configuration file and make that the new active configuration.

4.9.2 Import System Configuration

The Import System Configuration screen allows you to import previously saved or backed-up system configuration files.

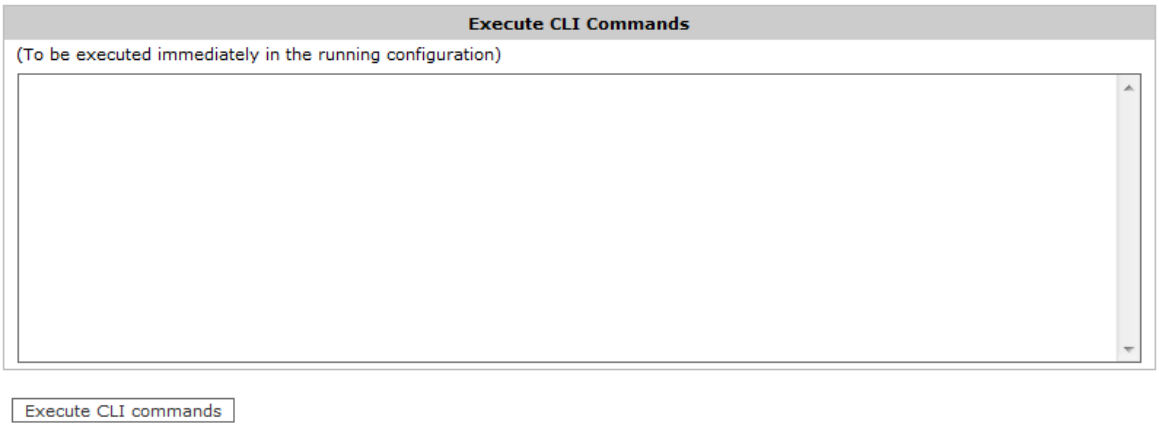
Note: To Import System Configuration, navigate to 'System | Maintenance | Import Config' on the Web UI, advanced mode.

The form below can be used to upload system configurations that have been saved locally on the PC.



Upload local binary file	Use this option to upload a saved binary configuration file. This file would have been downloaded as a binary file from the 'System | Maintenance | Manage Config' page. Once this file is uploaded, it will appear in the list of available configuration files on the System | Maintenance | Manage Config' page.
Upload local text file	Use this option to upload a text file containing CLI commands. The CLI commands will be executed in order and any configuration changes will be applied to the running configuration. This text file can contain one or more CLI commands or could be a complete text-based system configuration file downloaded from the 'System | Maintenance | Manage Config' 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.

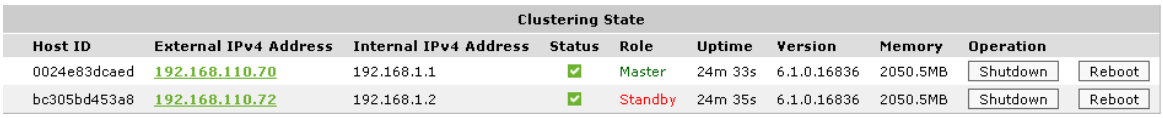


4.9.3 Clustering / High Availability

The Clustering screen allows you to view the status of all Exinda appliances in a cluster.

Note: To view the Clustering status, navigate to 'System | Maintenance | Clustering' on the Web UI, advanced mode.

The table on this page lists all the Exinda appliances in the cluster as well as additional information about each appliance.



Clustering State

Host ID	External IPv4 Address	Internal IPv4 Address	Status	Role	Uptime	Version	Memory	Operation	
0024e83dcaed	192.168.110.70	192.168.1.1	✓	Master	24m 33s	6.1.0.16836	2050.5MB	Shutdown	Reboot
bc305bd453a8	192.168.110.72	192.168.1.2	✓	Standby	24m 35s	6.1.0.16836	2050.5MB	Shutdown	Reboot

Host ID	The unique host id of the Exinda appliance.
External IPv4 Address	The cluster virtual IP address (cluster alias address).
Internal IPv4 Address	The cluster node's internal IP address.
Status	The status of the Exinda appliance. Online or offline.
Role	The role of the Exinda appliance in the HA setup. Master or standby.
Uptime	Total uptime of the Exinda appliance.
Version	ExOS version on the Exinda appliance.
Memory	Total memory size on the Exinda appliance.
Operation	You can also Shutdown or Reboot individual Exinda appliances in the cluster.

Note: For further information regarding Clustering and High Availability, consult the Clustering and HA How to Guide.

4.9.4 Firmware Update

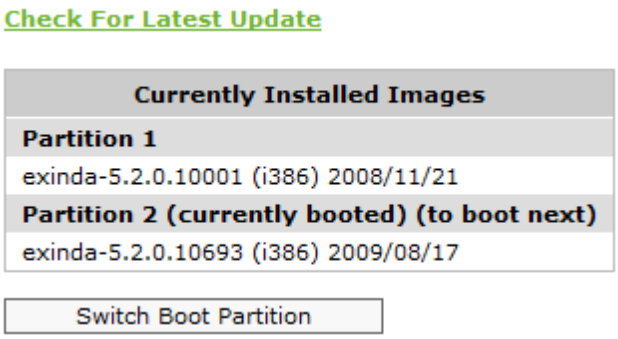
The Firmware Update screen allows you to update the software on your Exinda appliance. Exinda software is called ExOS and is updated regularly with new product features as well as system and performance improvements.

Note: To perform a Firmware Update, navigate to 'System | Maintenance | Firmware Update' on the Web UI, advanced mode.

Exinda appliances have 2 partitions for installing ExOS updates. The current, running ExOS version will be installed on one partition, which means you can install a newer ExOS update on the other, unused partition.

Note: Valid Software Subscription (SS) is required to install new ExOS updates. You can view your SS expiry date at the top of this page.

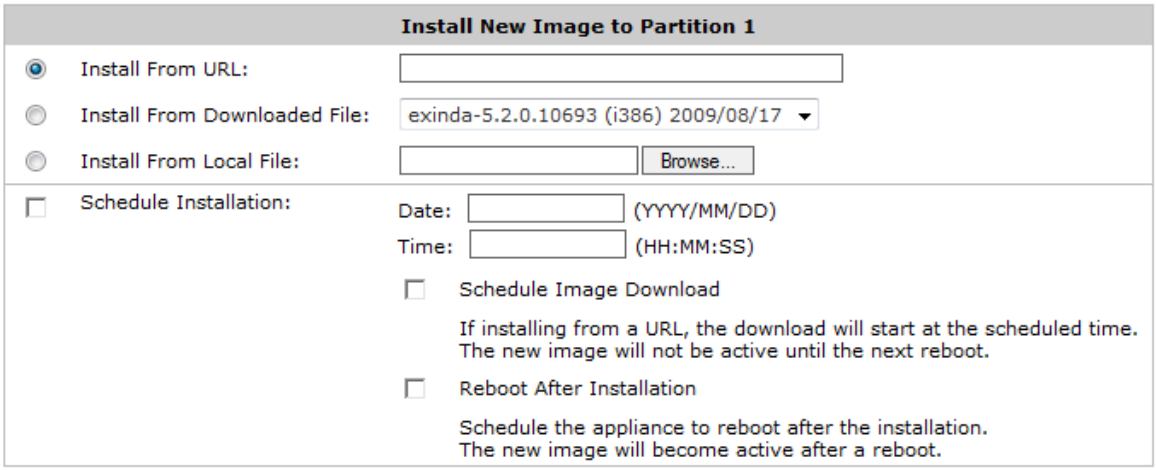
If the Exinda appliance has connectivity to the Internet, you can click on the 'Check for Latest Update' link which will contact the Exinda website and determine if a suitable new ExOS update is available.



You can also use this form to rollback the ExOS version to the previously installed version by clicking the 'Switch Boot Partition' button. You will need to reboot the Exinda appliance for this change to take effect.

Note: When rolling back to a previous ExOS version, the system configuration will be changed to the state that it was in, last time you were running the older version. If you've made changes to the system configuration since upgrading from the older version, they will be lost when the Exinda appliance is rolled back.

The form below is used to download and install an ExOS update on the Exinda appliance:



Install from URL	Specify the URL to fetch the ExOS update from. This URL will usually be published in the Release Notes as part of an ExOS release. If you used the 'Check for Latest Update' link above, this field will be populated automatically if a newer ExOS software update is available.
Install from Downloaded File	If an ExOS image has been previously downloaded onto the Exinda appliance (e.g. via the CLI), it will appear in the drop-down here and can be used for installation.
Install from Local File	If an ExOS image is available on your PC, you can upload it to the Exinda appliance.

Schedule Installation	Optionally schedule the download and/or installation of the ExOS update for a later date/time. Select the 'Schedule Installation' checkbox and specify a suitable Date and Time. By default, the download of the image will happen straight away and only the installation will be scheduled. You can optionally schedule the download of the ExOS image to happen at the scheduled time as well. By default, the Exinda appliance will not reboot following a scheduled installation. You can optionally automatically reboot the Exinda appliance after the scheduled installation.

Before installing or scheduling a new ExOS update, you will need to accept the End User License Agreement (EULA).

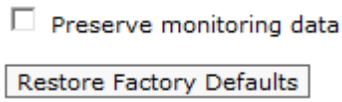
Note: After an ExOS update has been installed, a reboot of the Exinda appliance is required.

4.9.5 Factory Defaults

The Factory Defaults screen allows you to restore the Exinda appliance's configuration back to factory default settings. This includes removing any system logs, WAN Memory cache and monitoring statistics.

Note: To restore Factory Defaults, navigate to '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.



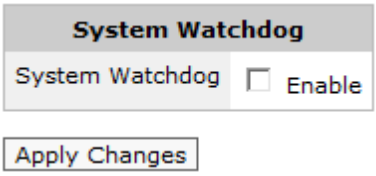
After performing a Factory Defaults, the Exinda appliance will automatically reboot.

4.9.6 Reboot / Shutdown

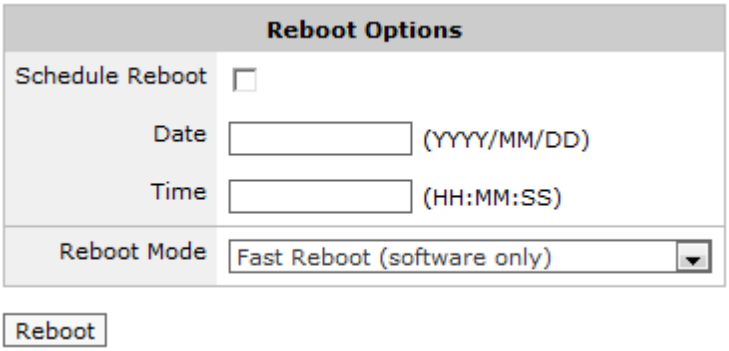
The Reboot / Shutdown screen allows you to configure Reboot options as well as gracefully shutdown the Exinda appliance in order to reboot it or power it down.

Note: To Reboot or Shutdown the Exinda appliance, navigate to 'System | Maintenance | Reboot / Shutdown' on the Web UI, advanced mode.

The System Watchdog feature will automatically reboot the Exinda appliance if it becomes unresponsive.



Use the following form to reboot the Exinda appliance.



Reboots can be scheduled by clicking on the 'Schedule Reboot' checkbox and specifying a Date and Time for the reboot to occur.

There are also 2 reboot modes to choose from.

Fast Reboot	This is a soft reboot and will reboot the operating system only. This does not reboot the hardware 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.

Caution: Any unsaved configuration changes will be lost if the Exinda appliance is Reboot or Shutdown without saving the changes first.

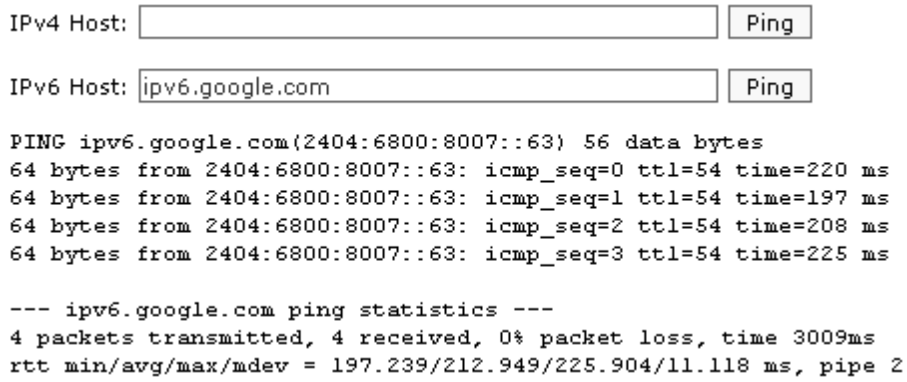
4.10 Tools

There are a set of tools installed on the Exinda appliance to assist with configuration and troubleshooting. These tools include:

- Ping: A tool to ping a network host from the Exinda appliance.
- Traceroute: A tool to perform a traceroute to a network host from the Exinda appliance.
- NS Lookup: A tool to query the configured DNS servers from the Exinda appliance.
- Console: A tool to connect to the Exinda appliance's CLI from the Web UI.
- IPMI: A tool to issue remote power commands to an IPMI enabled appliance.

4.10.1 Ping

Use the Ping Tool to test network connectivity from the Exinda appliance to other hosts on the WAN or Internet.

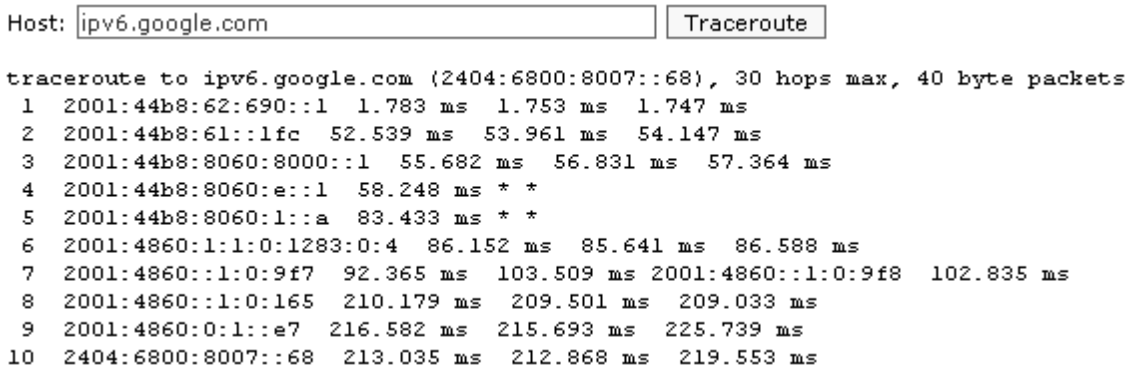


IPv4 Host	Specify an IPv4 Address or Fully Qualified Domain Name to attempt to ping.
IPv6 Host	Specify an IPv6 Address or Fully Qualified Domain Name to attempt to ping.

Note: After the 'Ping' button is pressed, it may take a few seconds for the ping operation to complete and display the results.

4.10.2 Traceroute

Use the Traceroute Tool to determine the network hops from the Exinda appliance to other hosts on the WAN or Internet.

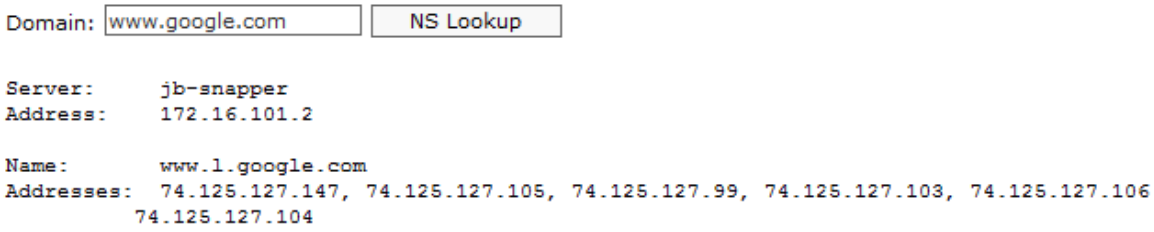


Host	Specify an IPv4 or IPv6 Address, or Fully Qualified Domain Name to attempt to traceroute.

Note: After the 'Traceroute' button is pressed, it may take a few seconds for the operation to complete and display the results.

4.10.3 DNS Lookup

Use the NS Lookup Tool to have the Exinda appliance query it's configured DNS servers to resolve the specified domain name.



Domain	Specify a Fully Qualified Domain Name to lookup.

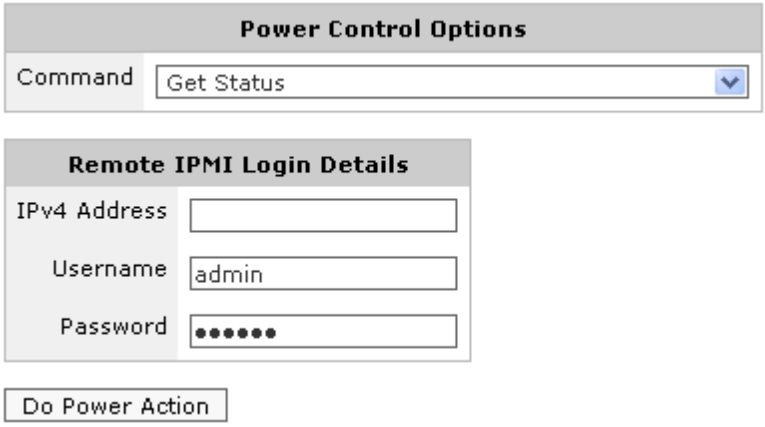
Note: After the 'NS Lookup' button is pressed, it may take a few seconds for the operation to complete and display the results.

4.10.4 Console

Use this tool to connect to the Exinda 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.

4.10.5 IPMI

Use the IPMI Tool to query the power status, power cycle/power off or reset a remote Exinda appliance via IPMI. The remote appliance must have enabled IPMI access. Select the desired action from the drop down selection, enter the IPMI authentication details for the remote appliance and click on the Do Power Action button.



IPv4 Address	The IPMI IPv4 address of the remote appliance
Username	The IPMI username for the remote appliance (default: admin)
Password	The IPMI password for the remote appliance (default: exinda)

Part V

5 Object Definitions

Objects are used by the Exinda appliance to define various items of interest such as IP addresses, Users/Groups, Applications, VLANs, Schedules, etc. These Objects are then often used in the Monitoring reports or in the Optimizer policies. The following Objects can be defined:

- Network Objects: Used to define IP addresses and subnets.
- User and Group Objects: Used to define users and groups.
- VLAN Objects: Used to define 802.1Q VLANs.
- Protocol Objects: Used to define network layer protocols.
- Application Objects: Used to define applications.
- Schedule Objects: Used to define times during days of the week.
- Adaptive Response Objects: Used to define and manage user data transfer quota.

5.1 Network Objects

Network objects are used to represent hosts, subnets and groups for monitoring and optimization. Thus, a network object can either be a single addressable network host, or a subnet of network hosts or a combination of both. Once defined, a network object may be used throughout the Exinda appliance for monitoring, optimization, and configuration purposes.

There are 2 types of Network Objects:

- Static: These are user-defined Network Objects. Users must manually specify subnets and/or IP addresses to define the Network Object.
- Dynamic: These Network Objects are automatically created and maintained by the Exinda appliance.

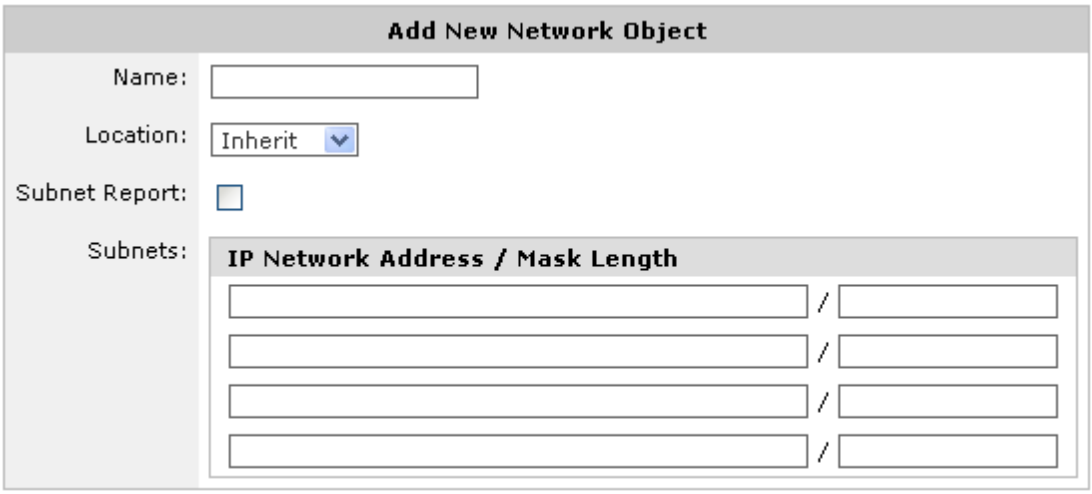
5.1.1 Static Network Objects

The **ALL**, **private net** and **local** Network Objects are automatically created by the appliance.

Name	IP Address	Netmask	Subnet Report	Location	Edit	Delete
ALL			✓	external		
	0.0.0.0	0.0.0.0				
private net			✗	external	Edit	
	10.0.0.0	255.0.0.0				Delete
	172.16.0.0	255.240.0.0				Delete
	192.168.0.0	255.255.0.0				Delete
local			✓	internal	Edit	Delete
	172.16.0.0	255.255.254.0				Delete

ALL	This Network Object can be used to represent all traffic on the network. When used in Optimizer Policies, it will match all traffic. This Network Object is not editable and cannot be deleted.
private net	This Network Object represents all possible non-routable, private IP addresses.
local	This Network Object is created when an IP address is assigned to one or more bridge interfaces. The object will contain the IP address and subnet mask of each bridge interface.

Additional Network Objects can be added by using the form at the top of the page.



Name	Specify a name for the Network Object.

Location	The location field is used when determining if a particular subnet is on the LAN side of the appliance (internal) or the WAN side (external). Packets are matched to a Network Object, and the closest subnet (see Example below) within that Network Object determines the location. There are 3 options for the location field. Inherit, Internal and External. **Internal** means all subnets/hosts defined by this Network Object exist on the LAN side of the appliance. **External** means all subnets/hosts defined by this Network Object exist on the WAN side of the appliance. **Inherit** means that a subnet/hosts location is determined by closest match to other Network Objects. If no Network Objects match then the location defaults to external.
Subnet Report	If enabled, traffic matching this Network Object will be included in Subnet Monitoring Reports.
Subnets	This is the network IP address and mask length of the subnet. IPv4 and IPv6 addresses are accepted.

Note: When creating or editing a network object, you will be presented with 4 input lines. To add more than 4 objects, you need to save and then re-edit to be presented with an extra 4 lines.

When the 'Ignore Internal-to-Internal' option is set on the System | Setup | Monitoring page, all traffic between Network Objects marked as 'Internal' will be ignored and pass-through the Exinda appliance.

Example: Create a Network Object that defines my 2 internal proxy servers, 192.168.1.10 and 192.168.1.11:

Name: Web Proxies
Location: Internal
Subnet Report: Yes

Subnets: 192.168.1.10 /32
Subnets: 192.168.1.11 /32

Example: Create a Network Object that defines my Head Office location, that has a subnet 10.0.100.0/24, where this Exinda appliance is NOT deployed:

Name: Head Office
Location: External
Subnet Report: Yes

Subnets: 10.0.100.0 /24

Example: Create a Network Object that defines my internal IPv6 server at 2001:db8::1234:5678

Name: FileServer6
Location: Internal

Subnet Report: Yes
Subnets: 2001:db8::1234:5678 /128

Note: When creating Network Objects that have location set to "Inherit", use the CLI "show network-object" command to show the location. When all subnets in the Network Object are contained within another Network Object that is internal, the location will be internal. If all subnets match a Network Object that is external, the location will be external. If some subnets match a Network Object that is internal, and some match a Network Object that is external, the location will be shown as mixed.

Example: We 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: User-1 Subnets: 10.0.1.200/32 Location: Inherit

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

```
(config) # show network-object User-1

Network Object: User-1
   Location:       internal (inherited)
   Subnet Report: no
   Subsystem:      static

   Subnets:
      10.0.1.200/32
```

5.1.2 Dynamic Network Objects

Dynamic Network Objects are Network Objects that are automatically updated and maintained by the Exinda appliance. They can be used anywhere Static Network Objects are used, however, they cannot be manually modified. This page allows you to view the contents of a Dynamic Network Object by selecting it from the drop-down at the top of the page. It displays the IP addresses, usernames (if applicable) and the date/time the specific address was dynamically added.

Currently there are 2 types of Dynamic Network Objects.

1. Adaptive Response Dynamic Network Objects

   When Adaptive Response rules are created, a corresponding Dynamic Network Object is automatically created. This Dynamic Network Object is populated by the hosts that have exceeded their Adaptive Response quota. For further information, see the Adaptive Response page.

2. Active Directory Dynamic Network Objects

   When Active Directory users or groups are defined, a corresponding Dynamic Network Object is automatically created. This Dynamic Network Object is populated by the hosts that make up that particular Active Directory user or group. For further information, see the System | Network | Active Directory page and the Objects | Users and Groups page.

5.2 Users and Groups

Users and Groups Objects are used to define pre-populated Users and Groups such that they can be used for Monitoring and Optimization.

Currently, there are 2 ways the Exinda appliance can learn about User and Group information:

1. Active Directory: The Exinda appliance can receive User and Group information using the Exinda Active Directory Service, installed on Active Directory Servers.

2. Static Users and Groups: Static Users and Group information can be only entered using the CLI "networkuser" 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.

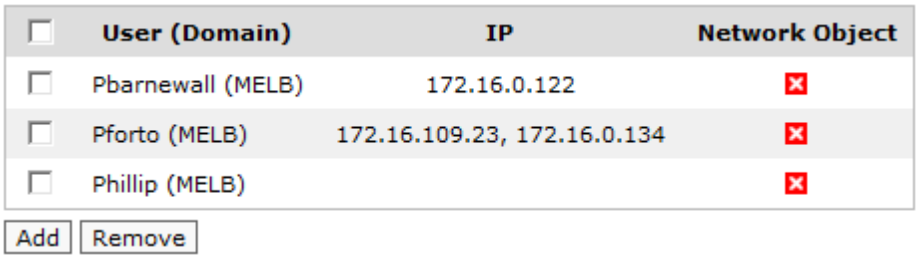
- To define Users as Dynamic Network Objects, see the Network Users page.
- To define Groups as Dynamic Network Objects, see the Network Groups page.

Note: For further information, consult the Active Directory How to Guide.

5.2.1 Network Users

Network Users displays a pre-populated list of Users (and their associated IP addresses) from either the Exinda Active Directory Service, or from static users entered using the CLI.

This page allows you to select which individual users you want to define as Dynamic Network Objects. Once a user is defined as a Dynamic Network Object, it can be used in the Optimizer policies.

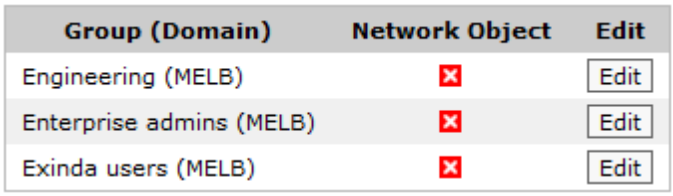


To define a user as a Dynamic Network Object, check the box next to their name, and click the 'Add' button.

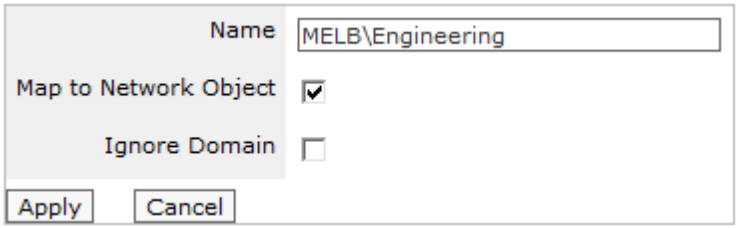
5.2.2 Network Groups

Network Groups displays a pre-populated list of Groups from either the Exinda Active Directory Service, or from static groups entered using the CLI.

This page allows you to select which groups you want to define as Dynamic Network Objects. Once a group is defined as a Dynamic Network Object, it can be used in the Optimizer policies.



To define a group as a Dynamic Network Object, click the 'Edit' button next to the group name.



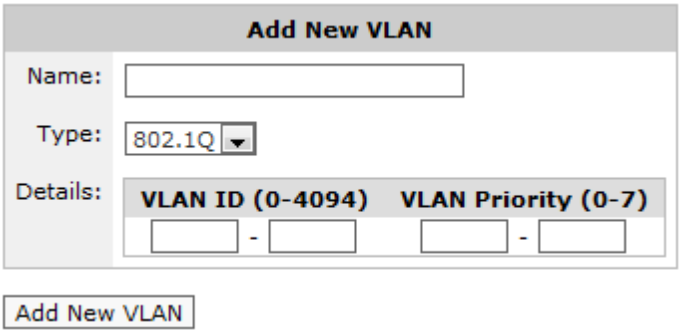
Make sure the 'Map to Network Object' option is selected. The group name can either be prefixed with the domain or without the domain. To exclude the prefixed domain tick the 'Ignore Domain' box. When ready, click the 'Save' button.

5.3 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. Once VLAN Objects are defined, they can be used in Optimizer policies to filter traffic.

By default, the Exinda 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 by using the form at the top of the page.



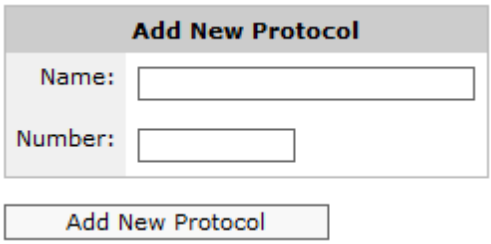
Name	Specify a meaningful name for the VLAN Object.
Type	Specify the type of VLAN to define. Currently only 802.1Q VLANs are available.
VLAN ID	Specify the range of VLAN IDs to define. To define all VLAN IDs, leave this field blank or enter 0 - 4094. A single VLAN ID can be defined by entering the same value in both fields.
VLAN Priority	Specify the VLAN Priority range to define. To define all VLAN Priorities, leave this field blank or enter 0 - 7. A single VLAN Priority can be defined by entering the same value in both fields.

Example: If VoIP traffic has a VLAN ID of 10, you'll need to create a VLAN object with this ID. This object can then be used to prioritize VoIP traffic using the Optimizer.

Name: VoIP
Type: 802.1Q
VLAN ID: 10 - 10
VLAN Priority: 0 - 7 (or leave this field blank)

5.4 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 be defined using the form at the top of the page.



Name	Give the protocol a meaningful name.
Number	Specify the IPv4 protocol number.

Note: Protocol numbers are unique and can only be defined once.

All the defined Protocol Objects are available to view in the table on this page. Each Protocol Object can be Edited or Deleted by clicking the appropriate button in the table. Some Protocol Objects are protected and cannot be edited or deleted.

Example: SCTP (Stream Control Transport Protocol) is undefined by default and needs to be defined in the Exinda appliance.

Name: SCTP
Number: 132

5.5 Application Objects

Application Objects are used to represent applications for monitoring and optimization. They are used to define applications that run over the network and are made up of TCP/UDP port numbers/ranges and layer 7 signatures. A Network Object can also be specified which can be used to tie an Application to a specific IP address/subnet. Application Objects can also be grouped together to form Application Groups.

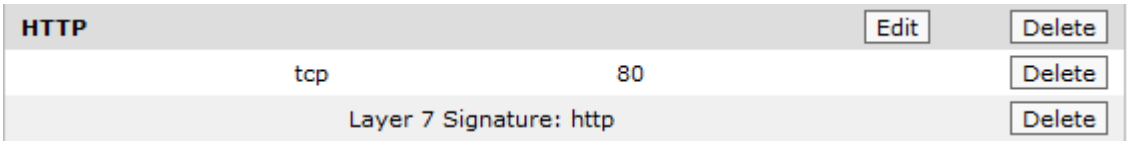
There are 3 Application Object sub-sections:

- Individual Applications: This is where all applications are defined.
- Application Groups: This is where Individual Applications can be grouped together to form Application Groups.

- Anonymous Proxy Application: This is a special Application Object used to detect anonymous proxy type applications.

5.5.1 Individual Applications

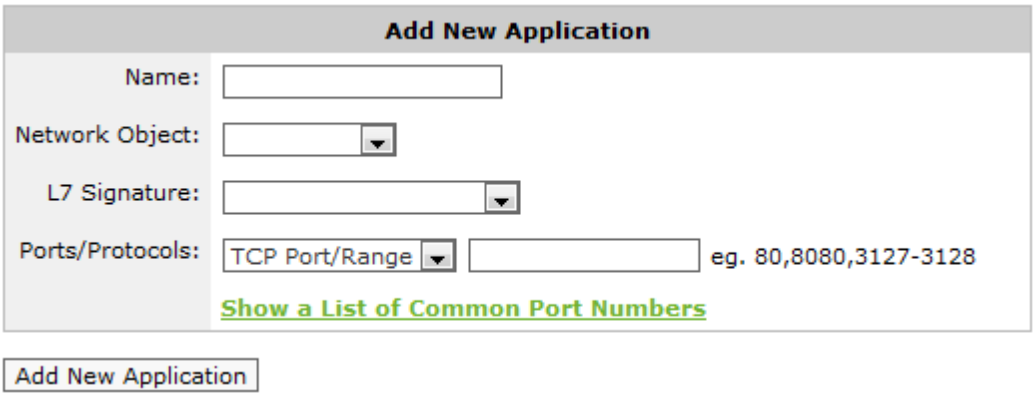
Applications are used to define applications that run over the network and are made up of TCP/UDP port numbers/ranges and layer 7 signatures. For example the **HTTP** application will match any traffic over TCP port 80 OR any traffic that matches the inbuilt 'http' layer 7 signature.



A Network Object can also be specified which can be used to tie an Application to a specific IP address/subnet. Network Objects can only be combined with TCP/UDP port numbers/ranges, not with Layer 7 signatures, and are logically AND'd to create a match. An *external* Network Object is matched as external and an *internal* Network Object is matched as internal. If a TCP/UDP port number/range is specified,it is always matched against the host matching the network object.

Example: If the network object is 192.168.0.20 (external) and the port is 8080, then only *outbound* packets with 192.168.0.20:8080 as a *destination* will be matched and *inbound* packets with 192.168.0.20:8080 as a *source* will be matched.

There are 100s of predefined Applications built into the Exinda appliance. To add a new Application, use the form at the top of the page:



Name	Give the Application Object a meaningful name.
Network Object	Specify a Network Object if you want to match all traffic to/from a particular server/subnet as an Application.

Ports/Protocols	Specify either TCP ports/port ranges, UDP ports/port ranges or a layer 3 protocol. Multiple ports and port ranges can be specified at the same time by comma separating values.
L7 Signature	Specify a Layer 7 signature that the application uses. See below for custom properties that can be specified for some L7 signatures.

Note: Ports, Port Ranges and L7 Signatures are OR'd together, that is, traffic only has to match one of the conditions for it to be considered a match. Take the HTTP example above. Traffic needs to be on TCP port 80 OR match the 'http' L7 signature for the appliance to classify it as HTTP. If a Network Object is specified, it is AND'd with any specified ports or port ranges.

Note: Network Objects and Layer 7 Signatures are mutually exclusive - only one or the other can be specified.

Note: TCP and UDP port pairs can only be defined once. So if you define an Application Object with a port range TCP 500 -> 510, you cannot then define another Application Object on TCP port 505. You can however, define UDP port 505 as TCP and UDP are treated separately. You can also define duplicate ports/port ranges if a Network Object is also specified.

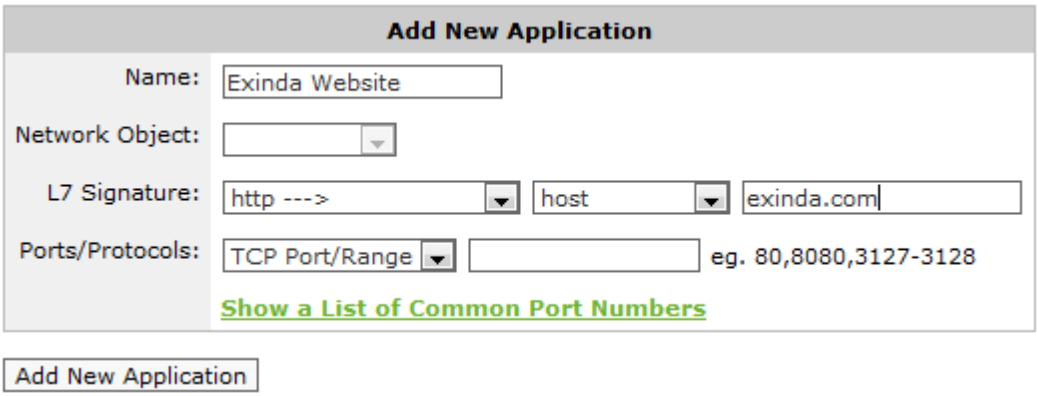
Some Layer 7 signatures have additional options that allow you to define Application Objects based on specific parts of that L7 Signature. The following table explains the various options available:

citrix	application	Allows you to define an Application Object based on a published Citrix application name.
	priority ^	Allows you to define an Application Object based on a published Citrix priority. Citrix priorities are 0=High, 1=Medium, 2=Low, 3=Background.
	user	Allows you to define an Application Object based on the user running the Citrix published application.
flash	host	Allows you to define an Application Object based on the 'host' field in the HTTP header (where flash is running over http).
http	content_type	Allows you to define an Application Object based on the 'content-type' field in the HTTP header.
	file	Allows you to define an Application Object based on the filename requested in the HTTP URL.
	host	Allows you to define an Application Object based on the 'host' field in the HTTP header.
	method	Allows you to define an Application Object based on the HTTP method (e.g. GET PUT HEAD DELETE).

	user_agent	Allows you to define an Application Object based on the 'user-agent' field in the HTTP header.
ssl	common_name	Allows you to define an Application Object based on the 'common name' field in the SSL certificate.
	organization_name	Allows you to define an Application Object based on the 'organization name' field in the SSL certificate.
rtp	codec	Allows you to define an Application Object based on the 'codec' used in a RTP stream.
windowsmedia	host	Allows you to define an Application Object based on the 'host' field in the HTTP header (where windowsmedia is running over http).

^ **Note**: The Citrix priority detection will only work if Citrix is running without session-reliability, over TCP port 1494.

Example: Create an Application Object that matches traffic to/from the Exinda website (HTTP traffic to/from *exinda.com*).



Note: For more information, consult the Exinda Applications List.

5.5.2 Application sub-types

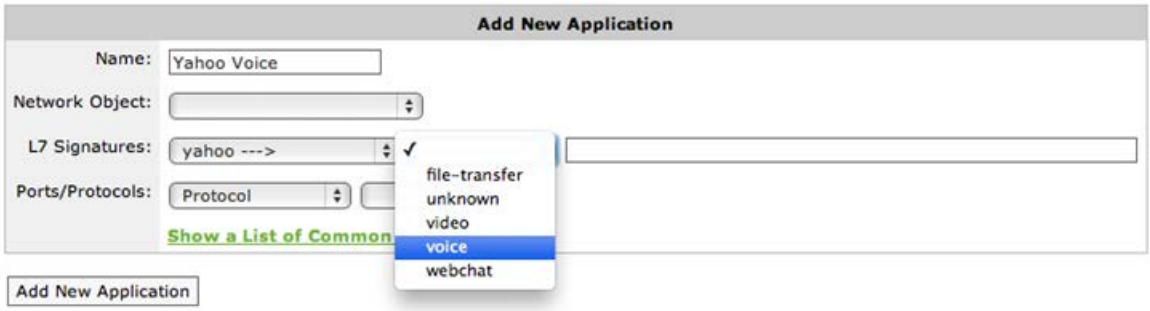
Sub-type classification takes reporting and Layer 7 visibility to a whole new level of granularity. Just like reporting on specific web applications where most vendors can only report on “port 80” traffic, Exinda allows a deeper look into Layer 7 applications.

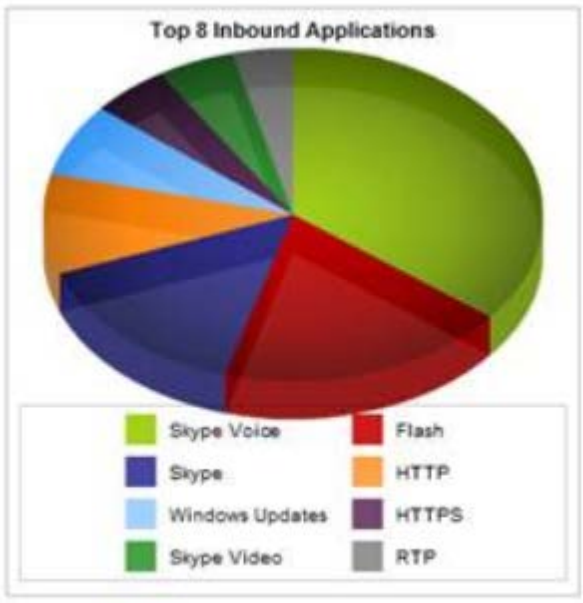
By comparison:

- Layer 4 reporting tools will report on web applications as: “port 80” or “HTTP”
- Layer 7 reporting tools will report on web applications as: “Yahoo” or “Skype”

- Exinda's Layer 7 with Sub-type classification will report on web applications as: "Yahoo video", "Yahoo voice", or "Yahoo webchat". Similarly it will break down other applications into their piece parts.

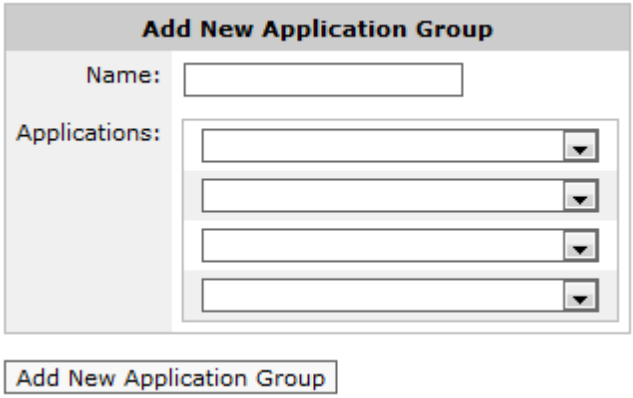
The following two graphics show the simplified configuration screen used by the Exinda to identify an applications' sub-type and, following, what a report on a sub-type classification may look like (notice Skype video and Skype voice broken out as separate reportable entries).





5.5.3 Application Groups

Application Groups are used to group together Individual Application Objects into a logical group. There are several predefined Application Groups, such as Mail, P2P, Voice, etc. Using this page, you can edit existing Application Groups or create new ones.



Name	Specify a name for the Application Group.
Applications	Select the Application Objects from the drop-downs that you want to include in this Application Group.

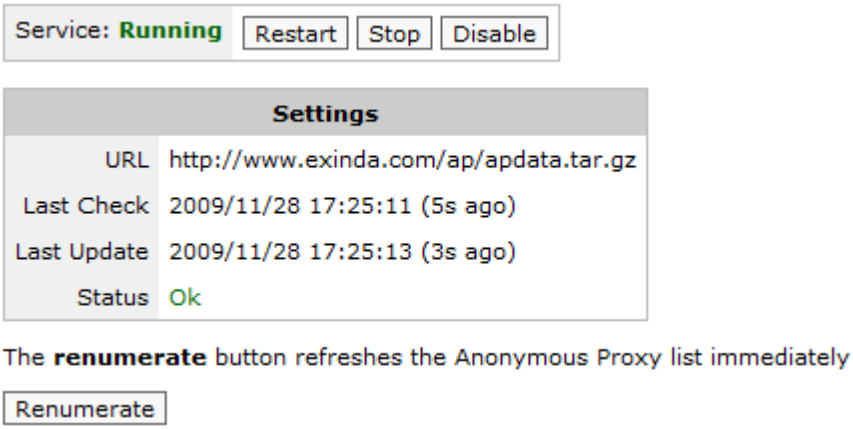
Note: By default, there are 4 drop-downs available to add Application Objects. If you need to add more, save the Application Group, then select the Edit button next to the newly created Application Group. You will be presented with 4 additional drop-downs to add more Application Objects.

Once defined, Application Objects are automatically used in various monitoring reports and can also be used in the Optimizer policies.

Note: For more information, consult the Exinda Applications List.

5.5.4 Anonymous Proxy Application

The Anonymous Proxy Application is a special Application Object that is used to detect Anonymous Proxy websites and services.



If the Anonymous Proxy Service is enabled, the Exinda appliance will fetch a list of Anonymous Proxy definitions from the www.exinda.com website on a daily basis. An Application Object called 'Anonymous Proxy' will automatically be created. This Application Object will show up in the monitoring reports like any other Application Object and can also be used in the Optimizer policies.

Note: Anonymous Proxy classification will only occur if the Anonymous Proxy ASAM module is enabled on the 'System | Setup | Monitoring' page.

The 'Renumerate' button can be used to force the Anonymous Proxy Service to fetch the Anonymous Proxy definitions immediately.

Note: For more information, consult the Anonymous Proxy How to Guide.

Note: Valid Software Subscription (SS) is required in order to fetch the Anonymous Proxy list form the Exinda website. The Exinda appliance will also require access to www.exinda.com to fetch new Anonymous Proxy definitions either via a direct Internet connection or via a HTTP Proxy.

5.6 Schedules

The Exinda appliance allows you to automate your network optimization polices for different times of the day and different days of the week.

For example, you may wish to lock down your network at night to improve security, whilst still allowing automated backup services and email to function.

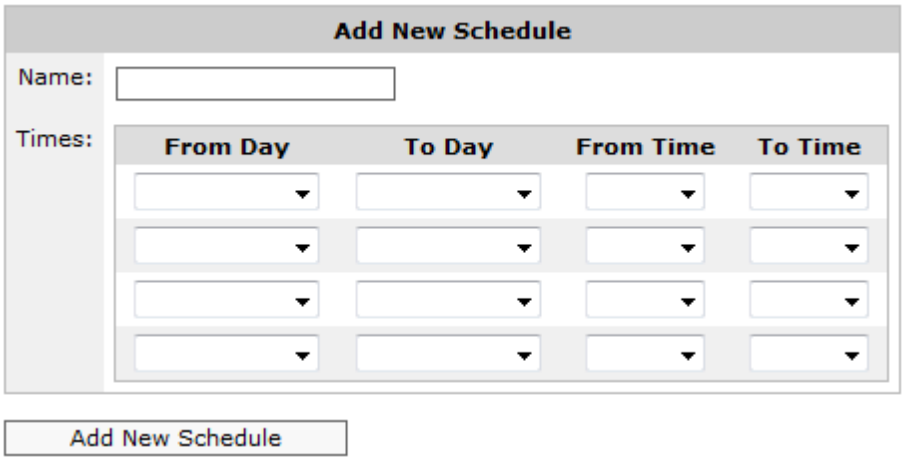
By default, there are 3 Schedule Objects defined.

Name	From Day	To Day	From Time	To Time	Edit	Delete
After Hours					Edit	Delete
	Monday	Friday	0:00	08:00		Delete
	Monday	Friday	18:00	24:00		Delete
	Saturday	Saturday	0:00	24:00		Delete
	Sunday	Sunday	0:00	24:00		Delete
ALWAYS						
	Sunday	Saturday	0:00	24:00		
Work Hours					Edit	Delete
	Monday	Friday	08:00	18:00		Delete

ALWAYS	This Schedule Object defines an 'Always On' schedule. This schedule is active 24 hours a day, 7 days a week. This Schedule is not editable and cannot be deleted.

After Hours	This Schedule Object defines a typical after hours schedule. It is active all day on Saturday and Sunday and from 6pm to 8am on Mondays to Fridays.
Work Hours	This Schedule Object defines a typical working hours schedule. It is active from 8am to 6pm on Mondays to Fridays.

Additional Schedule Objects can easily be added by using the form at the top of the page.



Name	Give the Schedule Object a meaningful name.
Times	Specify one or more times this Schedule Object is to be active for.
From Day	Specify a day of the week this Schedule Object should begin.
To Day	Specify a day of the week this Schedule Object should end.
From Time	Specify a time this Schedule Object should begin.
To Time	Specify a time this Schedule Object should end.

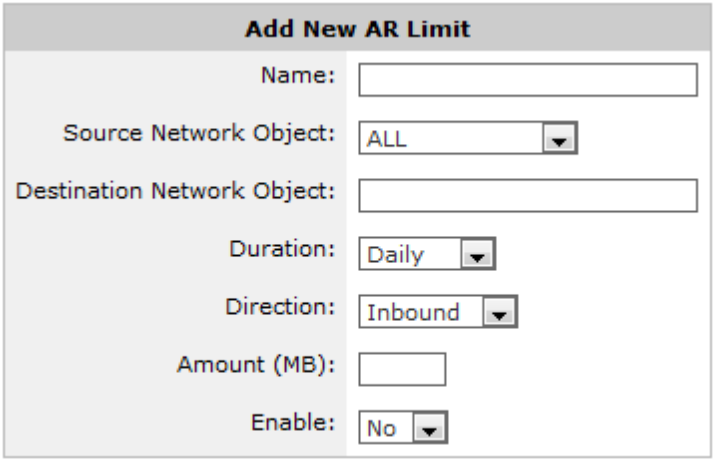
Note: A single Schedule Object cannot specify different times that overlap. Time must be unique within the same Schedule Object.

Note: The 'Start Time' and 'End Time' values must fall within the same day. In order to specify a time from one day to the next, use two lines: one from 'Start Time' to 24:00 on the first day, and the other from 00:00 to 'End Time' on the next day.

Note: By default, there are 4 drop-downs available to add schedule times. If you need to add more, save the Schedule, then select the Edit button next to the newly created Schedule. You will be presented with 4 additional drop-downs to add more schedule times.

5.7 Adaptive Response

Adaptive Response Objects are used to define and manage user data transfer quotas. You can use Adaptive Response Objects to create a limit on how much data users transfer per day, week or month. Use the form at the top of the page to create a new Adaptive Response Object.



Name	The name of the Adaptive Response object
Source Network Object	Specify a source Network Object to use as a list of users for whom to apply the quota. This can be a Static Network Object (such as a subnet) or a Dynamic Network Object (such as an Active Directory group).
Destination Network Object	Specify a name for the Dynamic Network Object that will be created, which will hold the list of users that have exceeded their quota.
Duration	Specify the duration to use when accounting the quota. Daily, weekly or monthly.
Direction	Specify which direction should be used when accounting the quota. Inbound, outbound or both.
Amount	Specify the quota amount (in MB) for this rule.
Enable	Specify if this rule should be enabled or not.

Any users from the 'Source Network Object' who have exceeded their quota within the 'Duration' period, will be placed into the 'Destination Network Object', which can then be used in the Optimizer policies. To view a list of the users who have exceeded their quota, see the Objects | Network | Dynamic page.

Note: For further information, consult the Adaptive Response How to Guide.

5.8 Service Levels

The Service Levels section allows you to configure parameters and alerts for Application Performance Score, Application Performance Metrics and Service Level Agreement Objects.

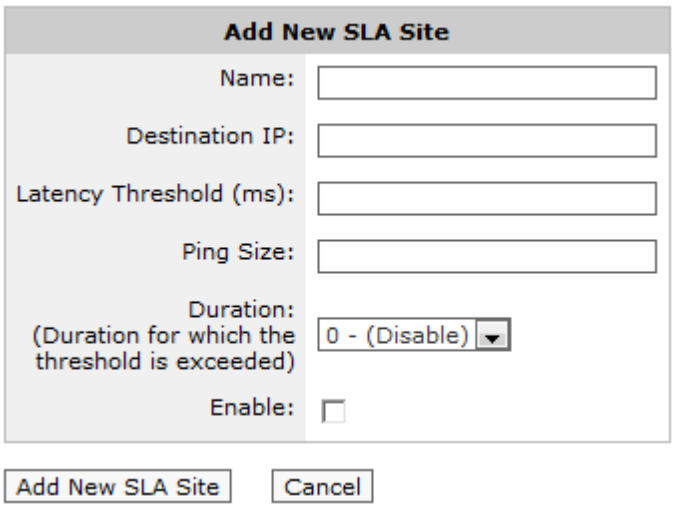
- Service Level Agreements
- Application Performance Score
- Application Performance Metrics

5.8.1 Service Level Agreements

Service Level Agreement (SLA) Objects can be configured on this page.

Note: To configure SLA Sites, navigate to 'Objects | Service Levels | Service Level Agreements' on the Web UI, advanced mode.

The table at the top of this page lists the currently defined SLA Objects, from here, you can edit/delete them. To configure new SLA Objects, click on the 'Add New SLA Object...' link.



Name	Specify a meaningful name for the SLA Site.
Destination IP	Specify an IP Address to use as the host to ping.
Latency Threshold	Specify a Latency Threshold. An alert will be triggered when the latency for the SLA Site exceeds the Latency Threshold for longer then the Duration.
Ping Size	Specify the ping packet size to use. The default is 64 bytes.

Duration	Specify a Duration. An alert will be triggered when the latency for the SLA Site exceeds the Latency Threshold for longer then the Duration.
Enable	Make this SLA Site active by clicking 'Enable'.

Note: Email alerts are sent when the specified threshold is exceeded for the set duration. Valid SMTP and email settings are required for email alerts. To configure, navigate to 'System | Network | Email' on the Web UI, advanced mode.

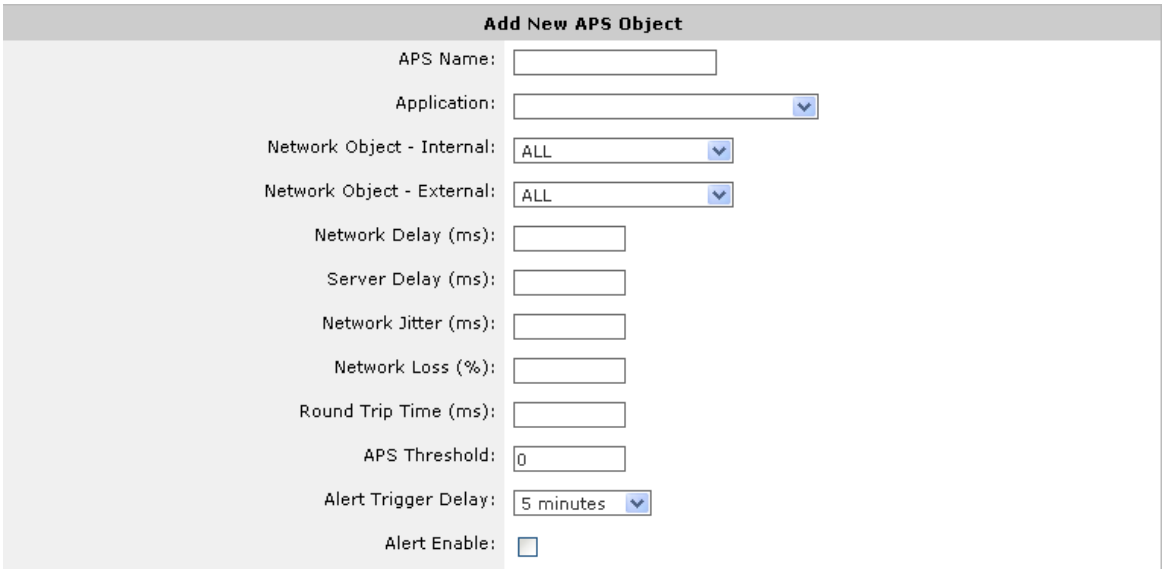
5.8.2 Application Performance Score

Application Performance Score (APS) Objects can be configured on this page.

Note: To configure APS Objects, navigate to 'Objects | Service Levels | Application Performance Score' on the Web UI, advanced mode.

APS is a score between 0 and 10 that is given to each APS Object based on how close the traffic that makes up the APS Object matches pre-defined thresholds. Each APS Object is made up of a name, a filter, a set of thresholds and alert settings.

The table at the top of this page lists the currently defined APS Objects, from here, you can edit/delete them. To configure new APS Objects, click on the 'Add New APS Object...' button.



APS Name	Specify a name for the APS Object.
Application	Specify an Application to filter.
Network Object - Internal	Specify an Internal Network Object to filter.
Network Object - External	Specify an External Network Object to filter.

Network Delay	Specify a Network Delay (in ms) threshold to apply to this APS Object (optional).
Server Delay	Specify a Server Delay (in ms) threshold to apply to this APS Object (optional).
Network Jitter	Specify a Network Jitter (in ms) threshold to apply to this APS Object (optional).
Network Loss	Specify a Network Loss (in %) threshold to apply to this APS Object (optional).
Round Trip Time	Specify a Round Trip Time (in ms) threshold to apply to this APS Object (optional).
APS Threshold	Specify an APS threshold to apply to this APS Object (optional).
Alert Trigger Delay	Specify an Alert Trigger Delay to apply to this APS Object. If the APS Object's score falls below the APS Threshold for longer than this time an alert will be generated.
Alert Enabled	Enable or Disable alerting on this APS Object.

Note: Email alerts and/or SNMP traps are sent when the APS falls below the threshold for the trigger delay time. Valid SMTP and email settings are required for email alerts. To configure, navigate to 'System | Network | Email' on the Web UI, advanced mode.

Note: For more information, consult the APS How to Guide.

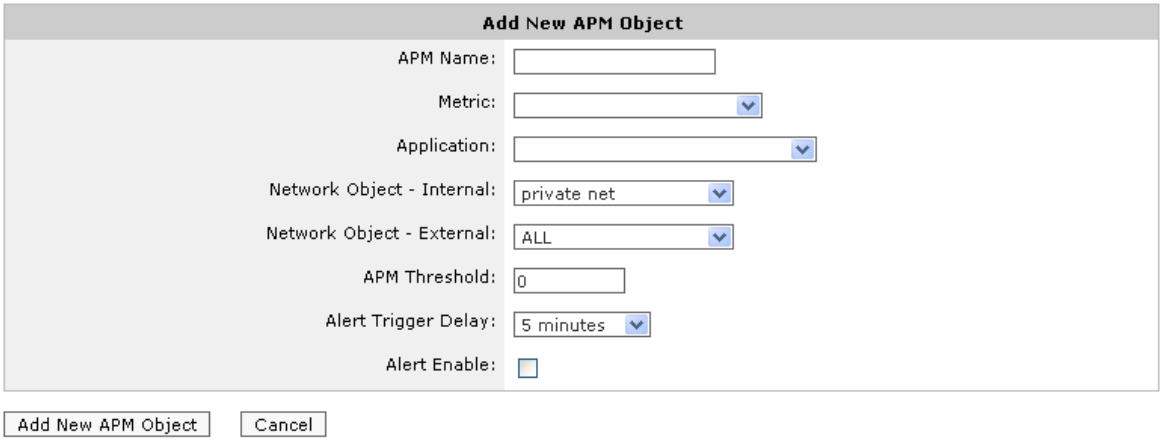
5.8.3 Application Performance Metrics

Application Performance Metrics (APM) Objects can be configured on this page.

Note: To configure APM Objects, navigate to 'Objects | Service Levels | Application Performance Metrics' on the Web UI, advanced mode.

APM objects allow a finer grained monitoring of application performance then APS.

The table at the top of this page lists the currently defined APM Objects, from here, you can edit/delete objects. To configure new APM Objects, click on the 'Add New APM Object...' button.



APM Name	The APM object name
Metric	The APM metric (see table below)
Application	Specify the traffic that the APM object should monitor
Network Object - Internal	Specify an internal Network Object to filter traffic
Network Object - External	Specify an external Network Object to filter traffic
APM Threshold	Specify the threshold that will trigger an alert.
Alert Trigger Delay	Specify the delay. An alert is only generated when the metric remains above the threshold for this length of time
Alert Enable	Enable or disable an alert when the metric rises above a configured threshold for a specified delay.

The following metrics are available:

network-delay	The time taken for data to traverse the network
server-delay	The time taken for a server to respond to a request

round-trip-time	The time taken for a packet to travel from a device, cross a network and return.
transaction-time	The total time for a transaction (network + server)
bytes-lost	Bytes lost due to retransmissions
tcp-connections-started	The number of TCP connections initiated
tcp-connections-aborted	A TCP connection reset after being established (RST from client or server)
tcp-connections-ignored	A TCP connection that expires in the SYN-SENT state. No response was received from the server.
tcp-connections-refused	A TCP connection that was reset before being established (RST in SYN-SENT state)

Note: for more information on Application Performance Metrics, refer to the Application Performance Score How To Guide.

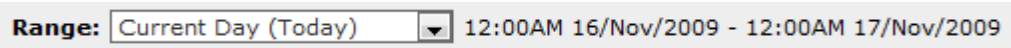
Part VI

6 Monitoring and Reporting

After installing and configuring your Exinda appliance you can start monitoring your network. You will have full visibility into the applications that users are accessing and the amount of inbound and outbound throughput that they reach . It's recommended that you monitor your network for an adequate period before customizing Optimizer policies.

6.1 Report Time Ranges

The 'Range' drop down at the top of most Monitoring Reports allows you to view common date/time ranges.



These are broken down into the following ranges:

- Last 5 Minutes
- Last 60 Minutes
- Current Hour
- Last Hour
- Last 24 Hours
- Today
- Yesterday
- Last 7 Days
- This Week
- Last Week
- Last 30 Days
- This Month
- Last Month
- Last 12 Months
- This Year
- Last Year

Custom Ranges

There is also a custom option that allows you choose your own date/time range. You can create a custom date/time range by either selecting "Custom" from the range drop down, or by clicking the date/time range.

Note: The further back in history you select, the less resolution is available. Your selection will be validated prior to displaying the report.

Data Granularity

Monitoring Reports can be defined by the time range option. The Exinda keeps:

- 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:

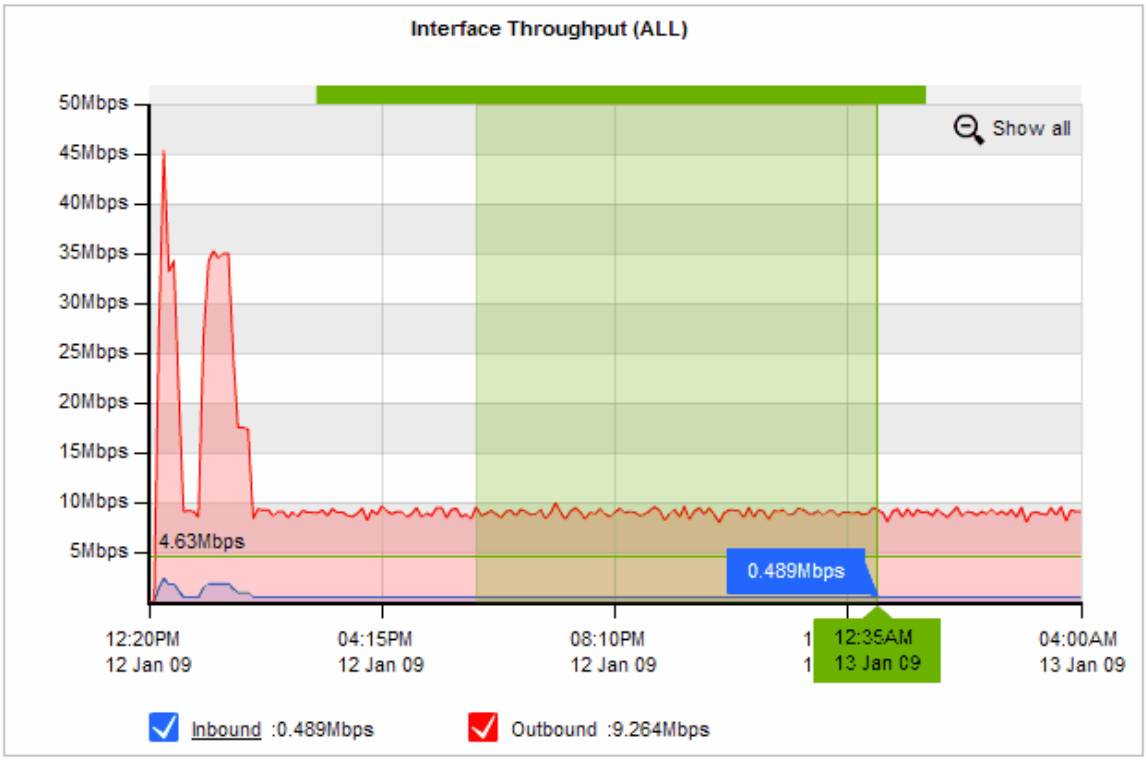
- Hourly granularity for up to 2 days (today, yesterday, this hour, previous hour)
- Daily granularity for up to 2 months (this week, last week, this month and last month)
- Monthly granularity for up to 2 years (this year, last year)

For the Interface, Network, Reduction, Optimizer, 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

6.2 Interactive Reports

The time graphs allow you to zoom in to a custom time range. Drag your mouse over the top of the graph and select the desired time range. To return to the initial time range click the magnifier glass icon.



Note: Any tabular data displayed below these interactive graphs will automatically be updated with the data for the selected time range.

Note: The interactive feature is only applicable to flash graphs. To change the graph display option navigate to System|Setup|Monitoring on the Web UI, advanced mode.

6.3 Printable Reports

All Monitoring Reports can be exported as a PDF document or can be printed directly from the Web UI. The following icons appear on the top, right-hand corner of the interface.

Print: Clicking on the Printer icon will open a new browser window and format the current report suitable for printing. It will then prompt you to select a printer.

PDF: Clicking on the PDF icon will instruct the Exinda appliance to 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 to the reports displayed on the Web UI.

6.4 Real Time Monitoring

The Real Time Monitoring Report displays a breakdown of the traffic that passed through your monitored links during the last 10 seconds. There are 6 Real Time Reports available:

- Inbound and Outbound Applications
- Internal and External Hosts/Users
- Inbound and Outbound Conversations
- Reduction
- Application Response
- Host Health

It is useful during times of network congestion to know exactly what is going through the link just as it happens. Use these reports to see which internal and external hosts and/or applications are currently using the link the most and at what speeds they are doing so.

6.4.1 Applications

The Real Time Applications Report shows a breakdown of the Applications monitored by the Exinda appliance during the last 10 seconds. Applications are divided into Inbound and Outbound directions. The menu at the top of the report allows you to adjust the report auto-refresh rate (every 30 seconds by default).

Applications are sorted by throughput. You can also see the packet rate and number of flows for each Application. The Distribution shows the percentage of throughput an Application consumed relative to all the other Applications.

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	

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	

6.4.2 Hosts / Users

The Real Time Hosts/Users Report shows a breakdown of the Hosts/Users monitored by the Exinda appliance during the last 10 seconds. Hosts/Users are divided into Internal and External Hosts/Users. The menu at the top of the report allows you to adjust the report auto-refresh rate (every 30 seconds by default) as well as an option to show/hide users in the report (hide Users by default). The 'show users' options allows to view the available username mappings as configured on the Network Users page. Users are shown below the Internal or External IP if available.

Hosts/Users are sorted by throughput. You can also see the packet rate and number of flows for each Host/User. The Distribution shows the percentage of throughput a Host/User consumed relative to all the other Hosts/Users.

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	

6.4.3 Conversations

The Real Time Conversations Report shows a breakdown of the Conversations monitored by the Exinda appliance during the last 10 seconds. Conversations are divided into Inbound and Outbound directions. The menu at the top of the report allows you to:

- Adjust the report auto-refresh rate of the report (every 30 seconds by default).
- Filter the report by an IPv4 or IPv6 address or subnet (no filter by default).

- Show/hide Optimizer Policies in the report (hide Optimizer Policies by default).
- Show/hide Users in the report (hide Users by default).
- Group individual connections within a flow as a single line item or show each connection as a separate line item (group connections by default).

By default, the Real Time Conversations Report looks like the example below. Conversations are sorted by throughput. You can also see the packet rate and number of flows for each Conversation. Any extra information about a Conversation (a URL for example) will be shown in square brackets next to the Application.

Inbound Conversations					
External IP	**Internal IP**	**Application**	**Transfer Rate (kbps)**	**Packet Rate (pps)**	**Flows**
Total			**351.001**	**121**	**108**
66.102.11.104	172.16.0.239	HTTP[www.google.com.au]	143.126	16	3
66.102.11.132	172.16.0.239	Anonymous Proxy	89.327	14	12
204.14.234.41	172.16.1.85	HTTPS	38.867	8	9
78.141.177.73	172.16.0.239	Skype	19.107	19	1
38.97.76.70	172.16.1.70	HTTPS	10.875	35	1
207.5.72.97	172.16.0.154	IMAP	10.643	7	7
209.160.58.87	172.16.0.239	HTTP[img.tfd.com]	9.512	1	2
207.5.72.97	172.16.0.177	HTTPS	7.248	2	2
168.143.162.52	172.16.0.244	HTTPS	5.847	2	3
66.102.11.101	172.16.0.239	HTTP[www.google-analytics.com]	1.654	1	1
Other			14.795	17	52

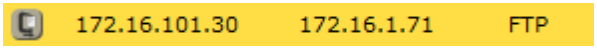
When Optimizer Policies are shown, the Real Time Conversations Report looks like the example below. Conversations are grouped by the Optimizer Policy they fall into.

Inbound Conversations					
External IP	Internal IP	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
Total			**120.677**	**65**	**86**
WAN inbound: Interactive and Secure - Guarantee High 10%-100%					
207.5.72.97	172.16.0.206	IMAP-SSL	52.031	11	1
207.5.72.97	172.16.0.211	HTTPS	7.467	2	4
69.49.191.53	172.16.0.101	HTTPS	6.463	1	1
207.5.72.97	172.16.0.63	IMAP-SSL	1.296	0	1
WAN inbound: Web - Guarantee Med 8%-100%					
74.125.153.104	172.16.0.177	HTTP[www.google.com.au]	15.665	2	1
66.102.11.100	172.16.0.177	HTTP[clients1.google.com.au]	8.682	5	4
74.125.153.103	172.16.0.101	HTTP[www.google.com.au]	8.043	1	2
67.228.80.250	172.16.0.101	HTTP[cct.clickable.net]	2.643	0	1
WAN inbound: copy (cn) of Recreational_backup - Limit Low 2%-10%					
38.97.76.70	172.16.1.70	HTTPS	10.122	30	3
121.141.99.13	172.16.0.115	udp ports 56553 -> 12816	0.375	0	1
Other					
Other			7.891	12	58

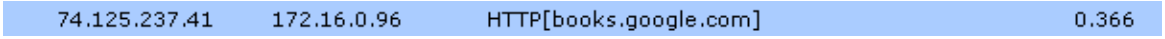
When Users are shown, the Real Time Conversations Report looks like the example below. The 'show users' options allows to view the available username mappings as configured on the Network Users page. Users are shown below the Internal or External IP if available.

Inbound Conversations					
External IP (User)	Internal IP (User)	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
Total			**272.198**	**109**	**107**
207.5.72.97	172.16.0.206 (stephen-ubuntu)	IMAP-SSL	151.511	29	1
204.14.234.41	172.16.1.85 (Confluence)	HTTPS	62.619	8	4
78.141.177.73	172.16.0.239 (Jbothe)	Skype	18.980	21	2
210.8.186.60	172.16.0.178 (chili)	HTTP[www.bom.gov.au]	10.931	3	6

When a conversation has been accelerated by the Exinda appliance, the Conversation will be highlighted in yellow and the Application Acceleration technologies being applied to that conversation will be displayed on the left-hand side as a series on icons. For example, the FTP connection below is accelerated and is also been process by WAN Memory.



When a conversation has been processed by Edge Cache it will be highlighted in blue.



The following legend describes the meaning of each icon.

	WAN Memory: The connection is been processed by WAN Memory.
	CIFS Acceleration: The connection is been processed by CIFS Acceleration.
	SSL Acceleration: The connection is been processed by SSL Acceleration.
	NCP Acceleration: The connection is been processed by NCP Acceleration.

When an appliance is deployed in a High Availability (HA) or Clustering mode, the following icons may also appear next to each conversation.

L	Local: The connection is passing through this appliance in the cluster.
R	Remote: The connection is passing through another appliance in the cluster.
L R	Local/Remote: The connection is passing though both this and other appliances in the cluster.

6.4.4 Reduction

The Real Time Reduction Report shows a breakdown of the Reduction Ratio by Application achieved by the Exinda appliance during the last 5 minutes. The menu at the top of the report allows you to adjust the report auto-refresh rate (every 30 seconds by default) as well as an option to view the inbound, outbound or bi-directional traffic reduction ratio (bi-directional by default).

Reduction Statistics (Last 5 Minutes)

	Application	LAN Data (MB)	WAN Data (MB)	Reduction Ratio (%)
1	URL	0.0008	0.0007	12.50
2	EMC Replication	255.71	211.34	17.35
3	HTTP	0.82	0.48	41.46
4	Oracle	0.0010	0.0009	10.00
5	LotusNotes	0.05	0.03	40.00

Reduction Ratio is a ratio that compares After Exinda (AE) to Before Exinda (BE).

```
Reduction Ratio = (Data Transfer Size BE - Data Transfer Size AE) / Data Transfer Size BE.
```

6.4.5 Application Reponse

The Real Time Application Response Report shows the Round-trip Time, Network Delay, Server Delay, Transaction Delay, Transaction Count and Flow Count for each application monitored by the Exinda appliance during the last 10 seconds. The menu at the top of the report allows you to adjust the report auto-refresh rate (every 30 seconds by default).

The Applications are sorted by Round-trip Time.

Application Response						
Application Name	RTT (ms)	Network (ms)	Server (ms)	Transaction Delay (ms)	Transaction Count	Flows
SMTP	462.70	44.65	0.00	44.65	1	1

Note: These statistics are only available if the Performance Metrics ASAM Module is enabled on the System | Setup | Monitoring page.

6.4.6 Host Health

The Real Time Host Health Report shows the Retransmitted Bytes, Aborted Connections, Refused Connections, Ignored Connections and Flow Count for each Internal and External Host monitored by the Exinda appliance during the last 10 seconds. The menu at the top of the report allows you to adjust the report auto-refresh rate (every 30 seconds by default).

The Hosts are sorted by Retransmitted Bytes.

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

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).

Note: These statistics are only available if the Performance Metrics ASAM Module is enabled on the System | Setup | Monitoring page.

6.5 Interface Reports

The Interface Reports show information about the traffic seen on the wire for each WAN interface on the Exinda appliance. The following Interface Reports are available on all models:

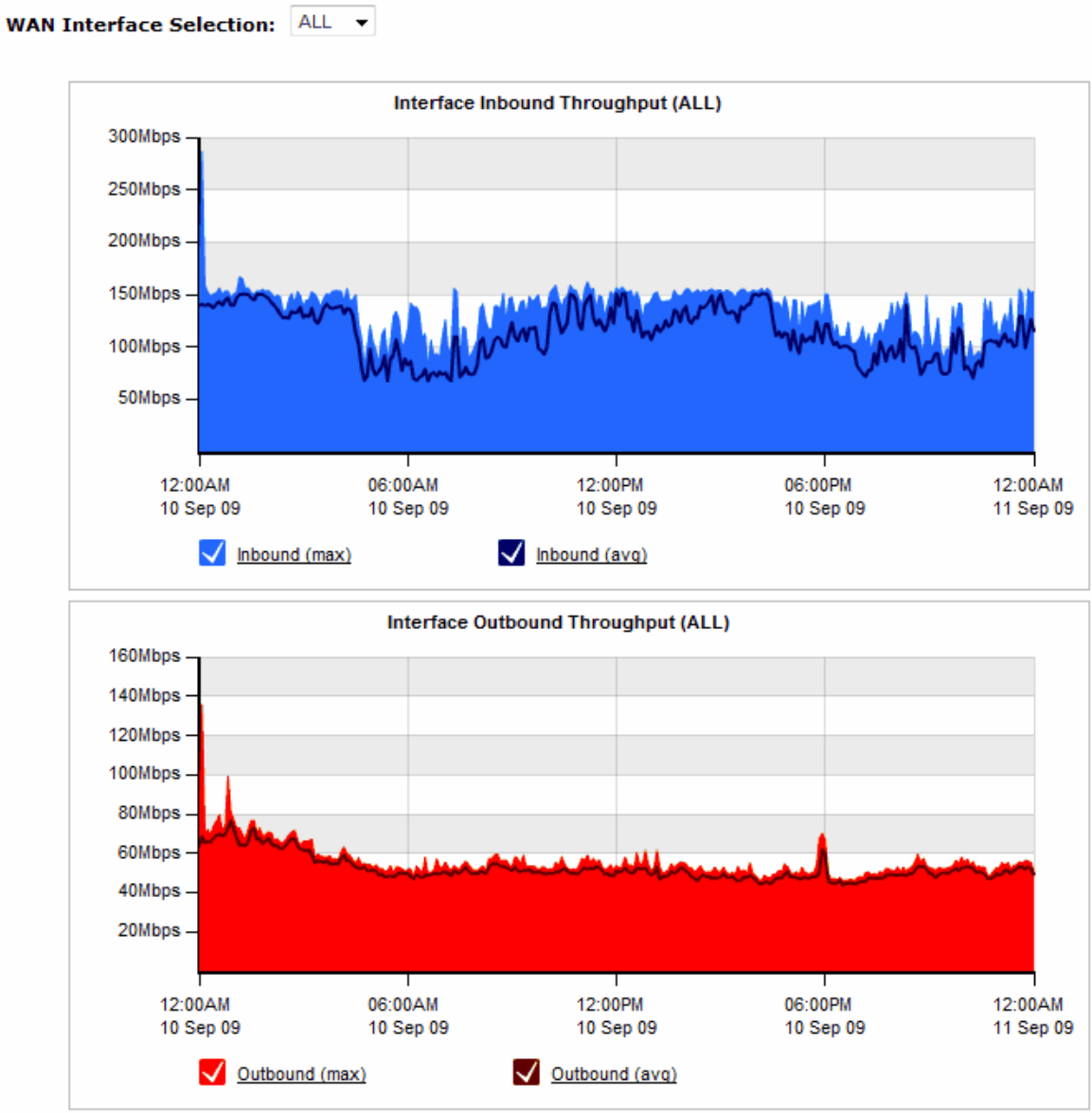
- Interface Throughput Reports
- Interface Packets Per Second (PPS) Reports

6.5.1 Interface Throughput Report

The Interface Throughput Report provides you with statistics of the total data that has passed through each WAN interface on each bridge. This report allows you to see the inbound and outbound throughput for all traffic on the wire, over time.

The WAN interface of each bridge is monitored and can be selected using the 'WAN Interface Selection' drop-down. There is also an option to report on the aggregate of all WAN ports by selecting 'ALL' from this drop-down.

Note: To view the Interface Throughput Report, navigate to 'Monitor | Interfaces | Throughput' on the Web UI, advanced mode.



WAN Interface Throughput Summary (ALL)			
Data Direction	**Total Data (MB)**	**Throughput Avg (Mbps)**	**Throughput Max (Mbps)**
Inbound	1200094.45	113.39	286.88
Outbound	553478.38	52.30	136.31

The table at the bottom of the report shows the total amount of data transferred into and out of the WAN interface(s), and also the maximum and average throughput values for the selected time period. The values in the table are automatically updated when the interactive flash graphs are manipulated.

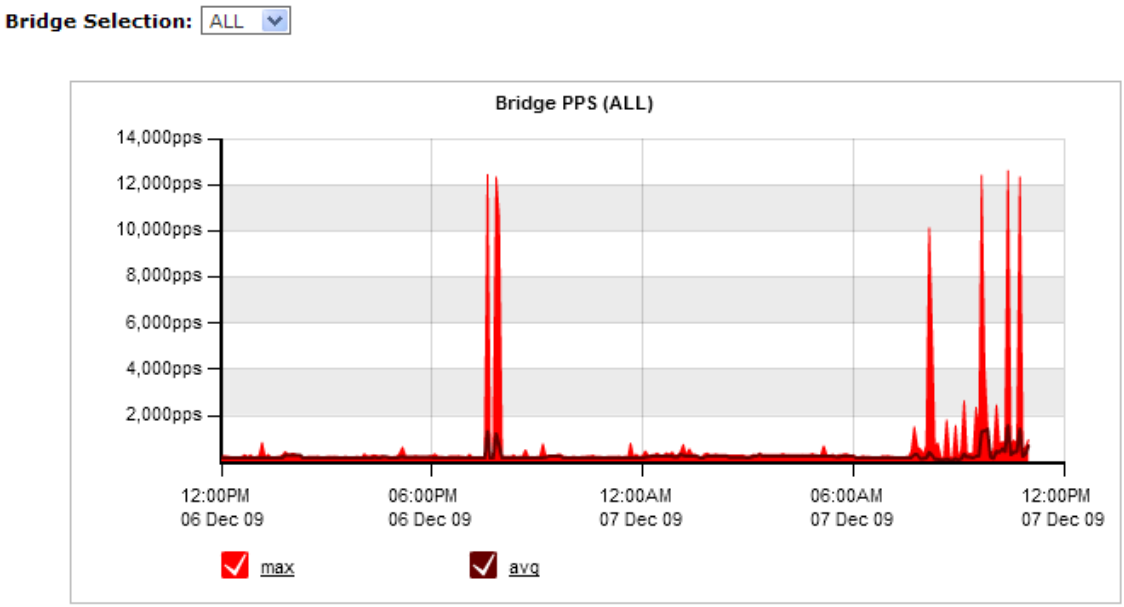
Note: Given that this report shows all data on the wire, the report may also include traffic that is not seen on the WAN, such as local LAN broadcasts, etc.

6.5.2 Interface Packets Per Second (PPS) Report

The Interface PPS Report provides you with the packet rate that has passed through each bridge on the Exinda appliance. This report allows you to see the outbound packet rate for all traffic on the wire, over time.

Each bridge is monitored and can be selected using the 'Bridge Selection' drop-down. There is also an option to report on the aggregate of all bridges by selecting 'ALL' from this drop-down.

Note: To view the Interface PPS Report, navigate to 'Monitor | Interfaces | Packets Per Second' on the Web UI, advanced mode.



Bridge PPS Summary (ALL)		
Data Direction	**Packets Per Second (Avg)**	**Packets Per Second (Max)**
Outbound	215	12,629

The table at the bottom of the report shows the maximum and average PPS values through the bridge for the selected time period. The values in the table are automatically updated when the interactive flash graphs are manipulated.

Note: Given that this report shows all data on the wire, the report may also include traffic that is not seen on the WAN, such as local LAN broadcasts, etc.

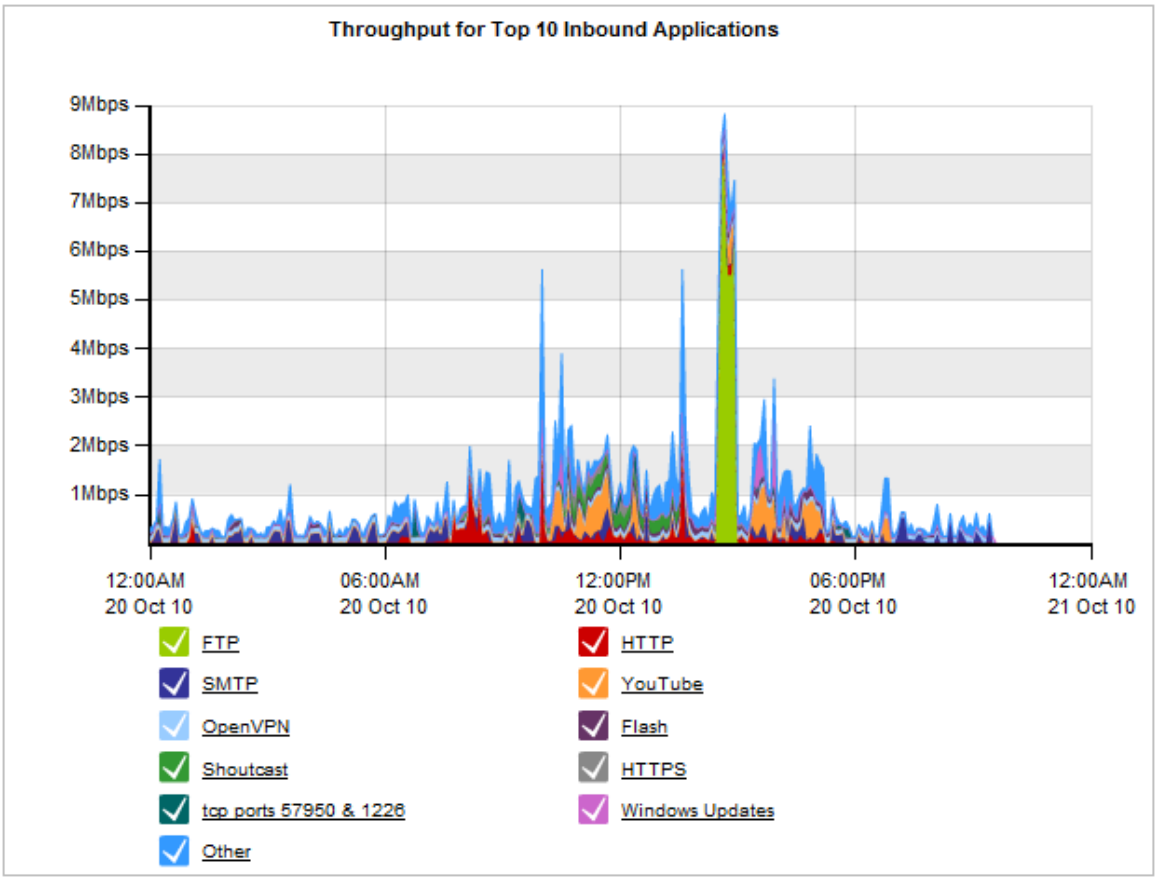
6.6 Network Throughput Reports

The Network Reports display a time series of the top 10 inbound and outbound Applications, Hosts, Conversations, URLs or Users on the network. The Applications series bundles applications not in the top 10 in an "Other" category.

Note: To view the Network Reports, navigate to 'Monitor | Network' on the Web UI, advanced mode.

Select the graph you wish to view from the 'Select graph to display' drop-down.

It is also possible to "zoom in" to a particular time period using the interactive flash-based graphs and disable certain plots by de-selecting their checkbox in the legend.



6.7 Optimization Reports

The Optimizer page shows how each Circuit, Virtual Circuit and Policy performs over time. You can see how well your policies are performing, how much bandwidth each policy is served, how much data is blocked and what the prioritization statistic are.

There are 3 Optimizer Reports available:

- Optimizer Shaping (QoS): Shows Optimizer Circuit, Virtual Circuit and Policy throughput over time.
- Optimizer Discard: Shows Optimizer discard (block) statistics over time.

- Optimizer Prioritization: Show Optimizer Policy prioritization statistics over time.

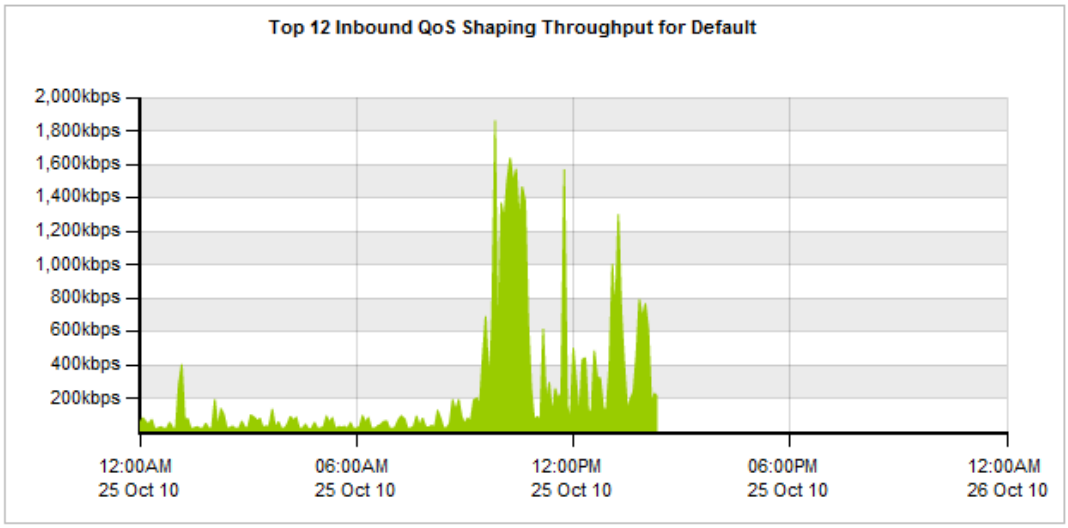
6.7.1 Optimizer Shaping (QoS) Report

The Optimizer Shaping Report shows how each Circuit, Virtual Circuit, Dynamic Virtual Circuit and Policy performs over time. You can see how well your Policies are performing and exactly how much bandwidth each Policy is served.

Note: To view the Optimizer Shaping (QoS) Report, navigate to 'Monitor | Optimization | Shaping' on the Web UI, advanced mode.

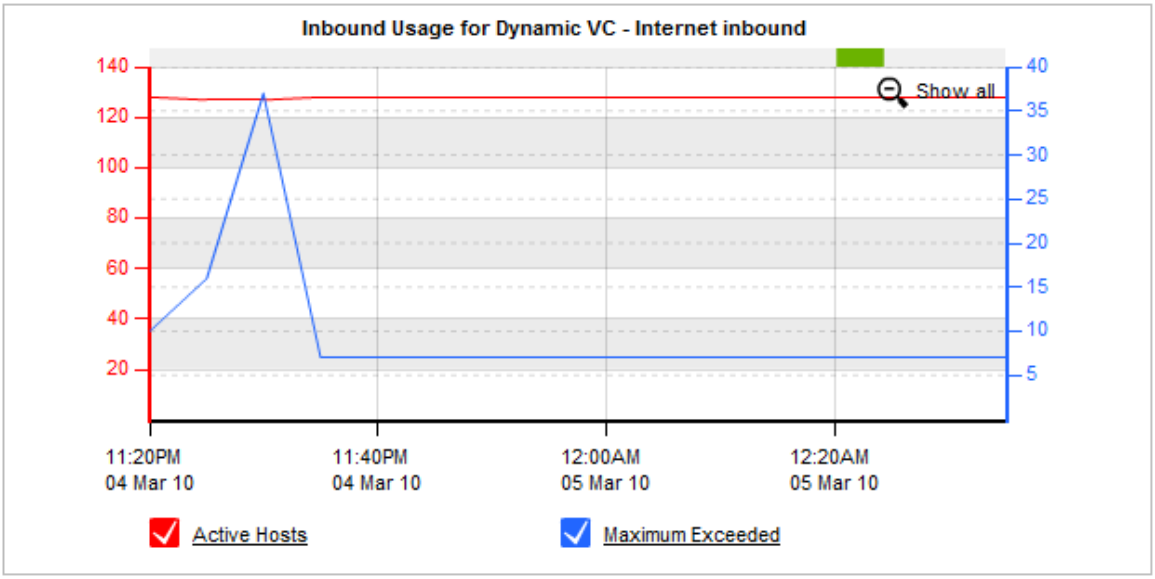
The menu at the top of the report allows you to filter the report by Circuit, Virtual Circuit or Policy.

When viewing Circuits, the report shows all Virtual Circuits within the selected Circuit, in both the graph and the table.



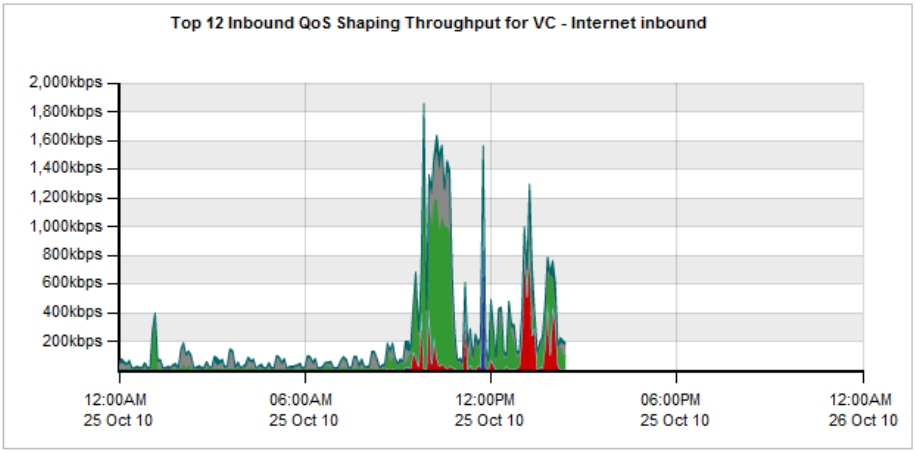
Optimizer Inbound QoS Summary (Default)				
VC Name	Maximum BW	Avg Rate / Max Rate (kbps)	Current Rate (kbps) / Utilization (%)	
Internet inbound	10000kbps	237.00 / 1,861.00		484.00 / 4.84

If the Virtual Circuit selected is a Dynamic Virtual Circuit, then the following graph will appear above the QoS Shaping graph.



The 'Active Hosts' line shows the number of Active Hosts for this Dynamic Virtual Circuit. The 'Maximum Exceeded' line shows the number of Hosts that have exceeded the Hosts limit for this Dynamic Virtual Circuit.

If a Virtual Circuit is selected, the report shows all Policies within the selected Virtual Circuit in both the graph and the table.



Optimizer Inbound QoS Summary (Internet inbound)				
	Policy Name [+] Show Details	Avg Rate / Max Rate (kbps)	Current Rate (kbps)	/ Utilization (%)
☑	10 - P2P - Choke 1%-3%	0.00 / 0.00		0.00 / 0.00
☑	20 - Recreational - Limit Low 2%-10%	40.00 / 915.00		0.00 / 0.00
☑	30 - Software Updates - Limit Med 3%-50%	7.00 / 1,258.00		0.00 / 0.00
☑	40 - Voice - Guarantee Critical 15%-100%	0.00 / 22.00		0.00 / 0.00
☑	50 - Thin Client - Guarantee High 10%-100%	0.00 / 1.00		0.00 / 0.00
☑	60 - Files - Guarantee Med 8%-100%	0.00 / 0.00		0.00 / 0.00
☑	70 - Web - Guarantee High 10%-100%	118.00 / 1,547.00		57.00 / 0.57
☑	80 - Mail - Guarantee Med 8%-100%	44.00 / 472.00		93.00 / 0.93
☑	200 - ALL - Guarantee Low 5%-100%	23.00 / 223.00		23.00 / 0.23

The table underneath the graph shows some additional information for the selected time period. The 'Average Rate' is the average policy throughput for the time specified in the time range. The 'Current Rate' is the Policy throughput averaged over the last 10 seconds.

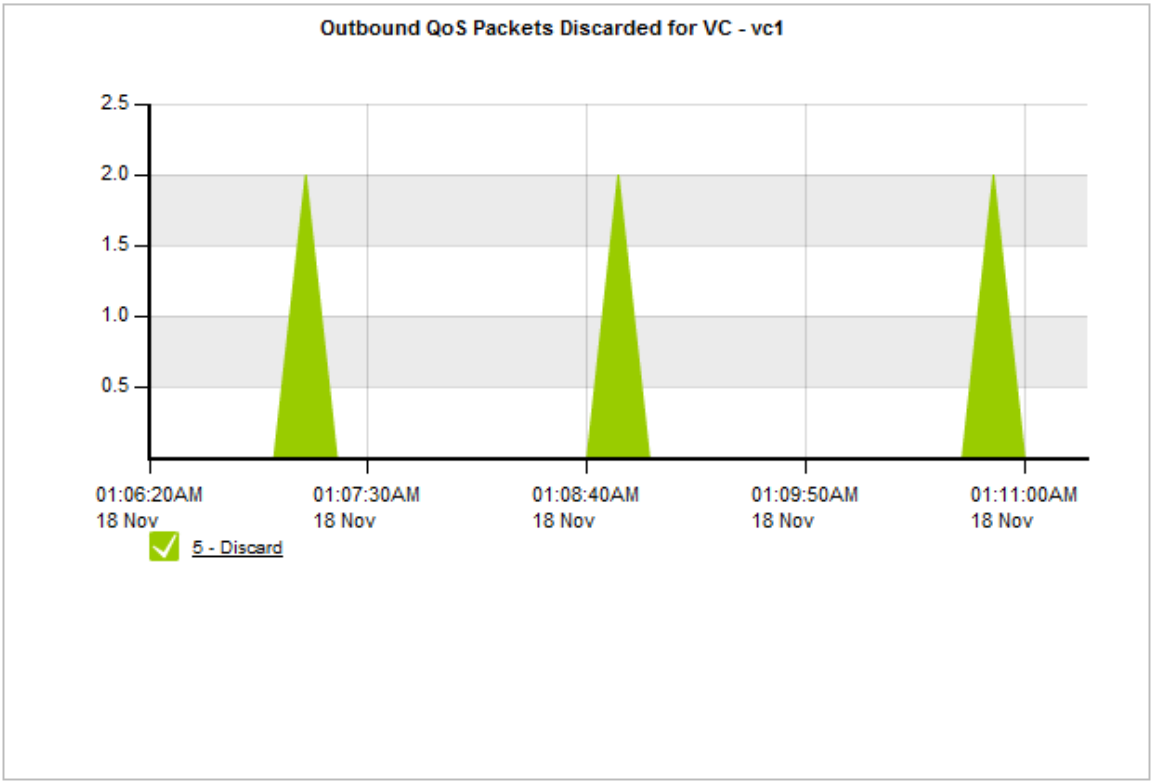
6.7.2 Optimizer Discard Report

The Optimizer Discard Report shows how many packets were discarded as a result of Optimizer Discard Policies.

Note: To view the Optimizer Discard Report, navigate to 'Monitor | Optimization | Discard' on the Web UI, advanced mode.

Using the menu at the top of the Report, you can filter the Report by Virtual Circuit or Policy. Only Virtual Circuits and Polices that contain discard actions are displayed.

The graph shows the number of packets discarded over time. The table below show the total number of discarded packets over the selected time period.



Optimizer Outbound Discarded Summary	
Policy Name	**Total Packets Discarded**
5 - Discard	6

It is also possible to "zoom in" to a particular time period using the interactive flash-based graphs and disable certain plots by de-selecting their checkbox in the legend.

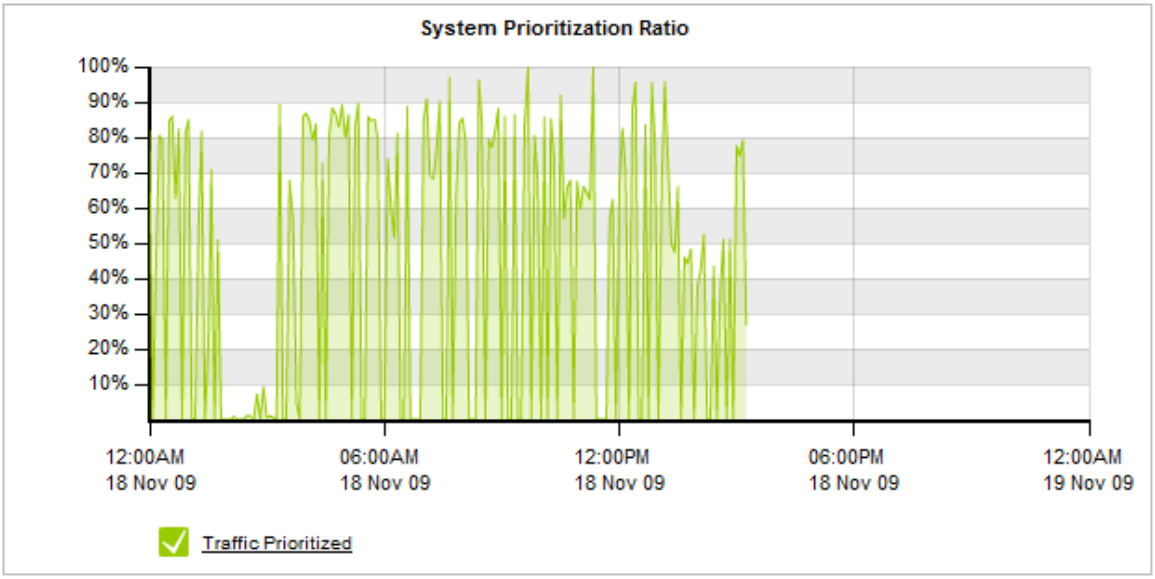
6.7.3 Optimizer Prioritization Report

The Optimizer Prioritization Report tells you how often critical applications were prioritized (also referred to re-ordering or re-queuing).

Note: To view the Optimizer Prioritization Report, navigate to 'Monitor | Optimization | Prioritization Ratio' on the Web UI, advanced mode.

A high percentage means that the system is prioritizing more often to ensure performance of your applications. A high percentage also means that by turning off optimization there is a higher probability that your critical applications will suffer.

```
Prioritization Ratio = 100 x Number of Packets Re-ordered / Number of Total Packets
```



Example: A ratio of 40% means 40% of the packets on your network were re-ordered. That means that non critical data was queued so that business critical data could jump the queue and be delivered in the order that the business requires.

6.8 Reduction Report

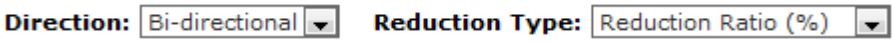
The Reduction Report shows the WAN Memory reduction throughput and percentage, the reduction statistics and peers (remote sites) and Applications with reduced traffic. You can choose to view a particular time period using the time range selection bar at the top of the page.

Note: To view the Reduction Report, navigate to 'Monitor | Reduction' on the Web UI, advanced mode.

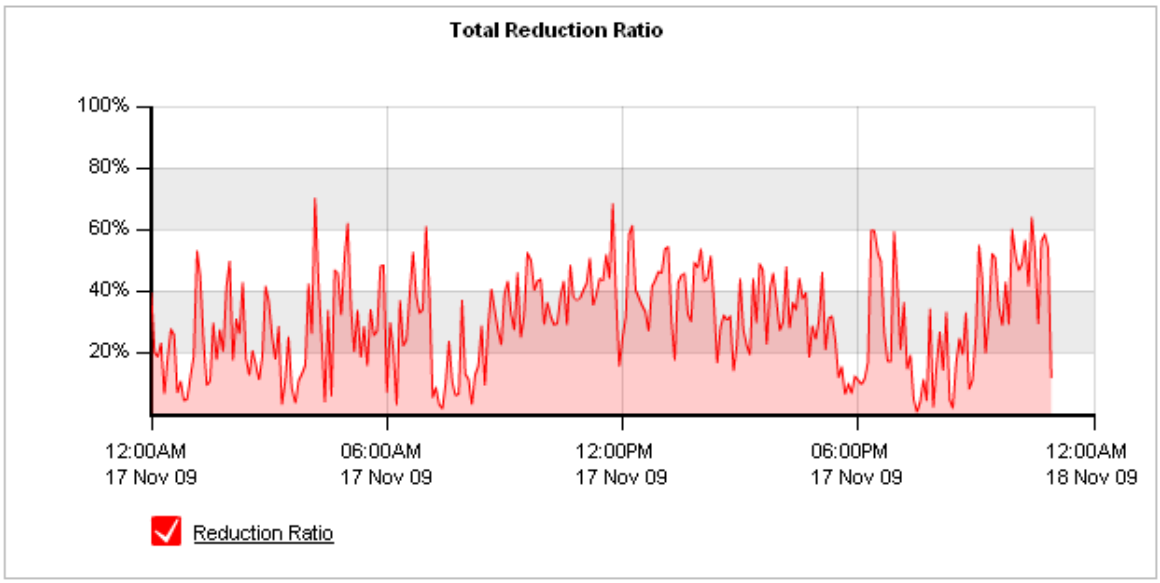
There are 2 options when it comes to configuring the Reduction Report.

- Direction: Choose which direction you wish to view reduction statistics. Choices are Bi-directional, Inbound or Outbound.
- Reduction Type: Choose how you want reduction statistics to be displayed. Choices are Percentage and Throughput.

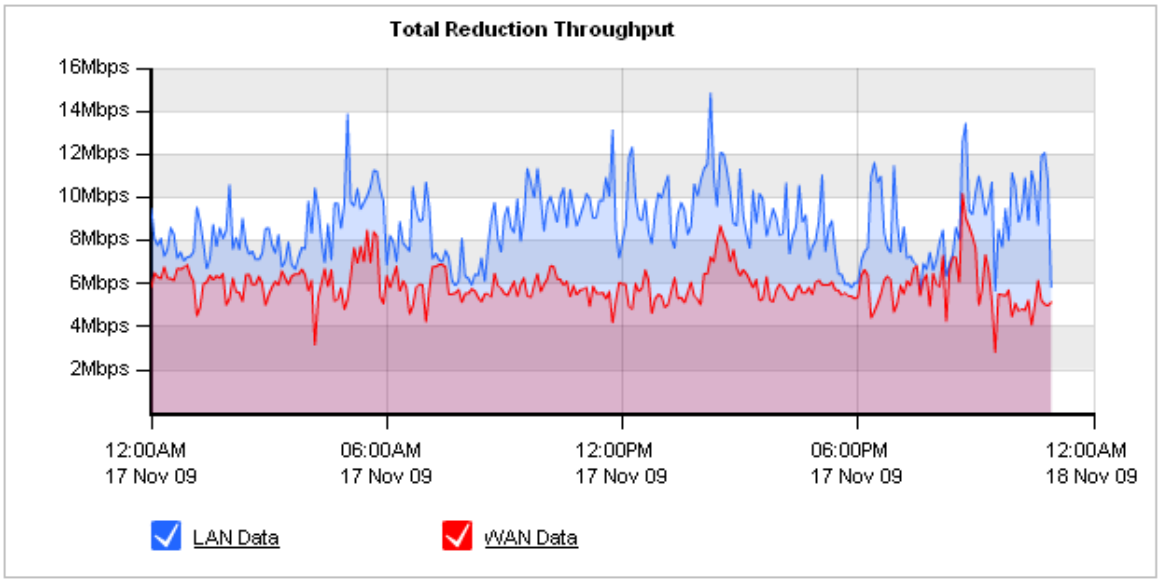
The drop-down menus at the top of this report allow you to configure these options.



When reduction statistics are displayed as a percentage, the following graph will be visible:



When reduction statistics are displayed as throughput, the following graph will be visible:



You can choose to view a particular time period using the time range selection bar at the top of the page. It is also possible to "zoom in" to a particular time period using the interactive flash-based graphs and disable certain plots by de-selecting their checkbox in the legend.

The table below the graphs show reduction statistics broken down by peer (remote Exinda appliance) as well as by Application.

Reduction Statistics by Peer				
	Peer	LAN Data (MB)	WAN Data (MB)	Reduction Ratio (%)
1	will	374.01	286.44	23.41
2	war	2,762.56	872.18	68.43
3	bhl	230.23	171.05	25.70
4	wbri	374.16	222.65	40.49
5	man	76,821.56	54,609.32	28.91
6	tops	247.85	137.24	44.63
7	bed	186.72	136.68	26.80
8	bos	44.7	32.6	27.07
9	hol	420.65	189.31	55.00
10	rh	3,764.34	1,888.74	49.83
11	wor	106.46	89.48	15.95
12	wilt	906.41	478.35	47.23
13	wes	2,591.56	843.86	67.44
	Total	**88,831.21**	**59,957.9**	**32.50**

Reduction Statistics by Application				
	Application	LAN Data (MB)	WAN Data (MB)	Reduction Ratio (%)
1	Discovered Ports	0.11	0.08	27.27
2	URL	93.68	28.3	69.79
3	URL 1	1.1	0.67	39.09
4	http file	24.07	17.67	26.59
5	EMC Replication	75,027.27	53,135.1	29.18
6	ZCM	0.01	0.01	0.00
7	HTTP	6,777.73	1,984.65	70.72
8	CIFS	4,978.02	3,399.93	31.70
9	LotusNotes	1,681.82	1,360.8	19.09
10	MS-SQL	247.01	30.46	87.67
11	Oracle	0.02	0.02	0.00
12	NFS	0.09	0.05	44.44

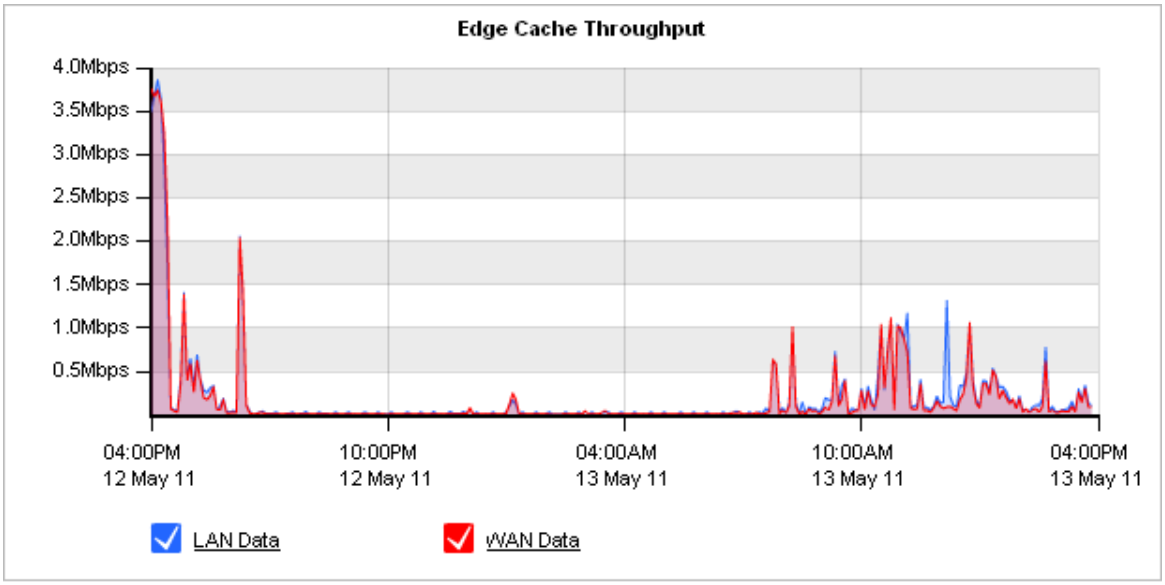
Reduction Ratio is a ratio that compares After Exinda (AE) to Before Exinda (BE).

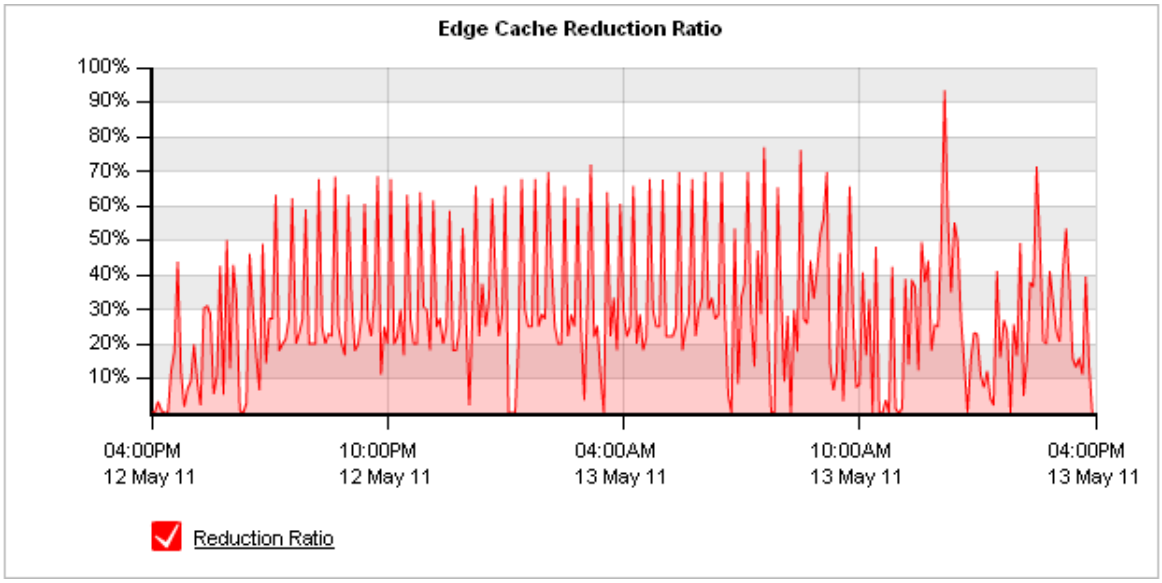
```
Reduction Ratio = (Data Transfer Size BE - Data Transfer Size AE) / Data Transfer Size BE.
```

6.9 Edge Cache Report

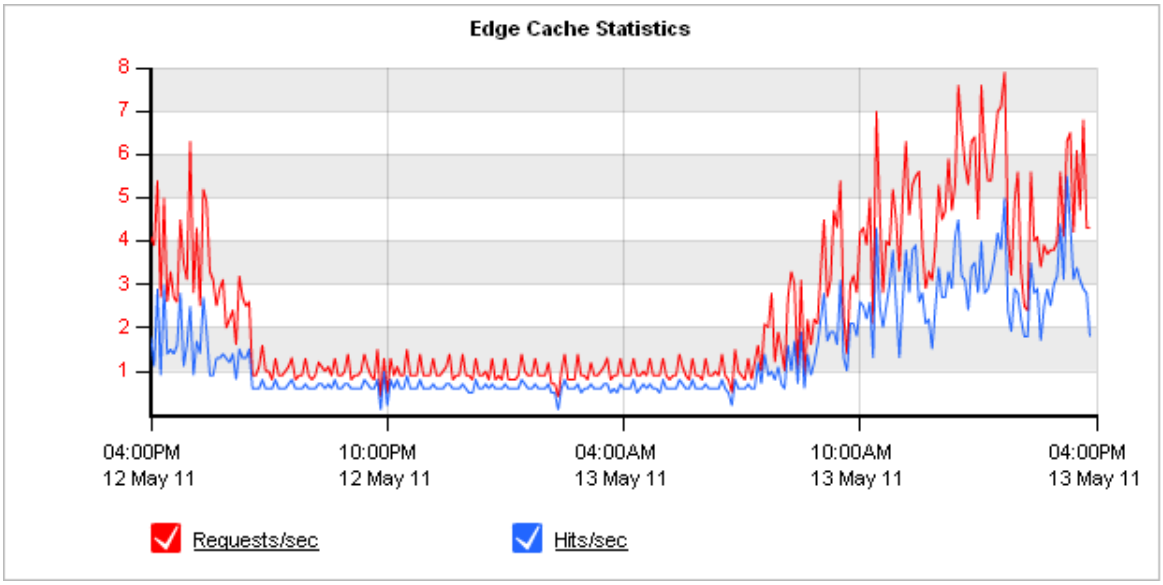
The Edge Cache report shows the amount of data reduced.

Two reduction graphs are available - 1. Edge Cache throughput (LAN and WAN) and 2. Ratio of WAN to LAN throughput in percent.





The graph below shows the number of requests per second and the number of "hits" per second. A hit occurs when a request is made for an object stored in the Edge Cache memory.



The table below shows a summary of Edge Cache reduction for the selected time period.

LAN (MB)	WAN (MB)	Reduction Ratio (%)	Requests	Hits	Hit Ratio (%)
2138.61	1930.90	9.71	204030	120030	58.83

6.10 Service Level Reports

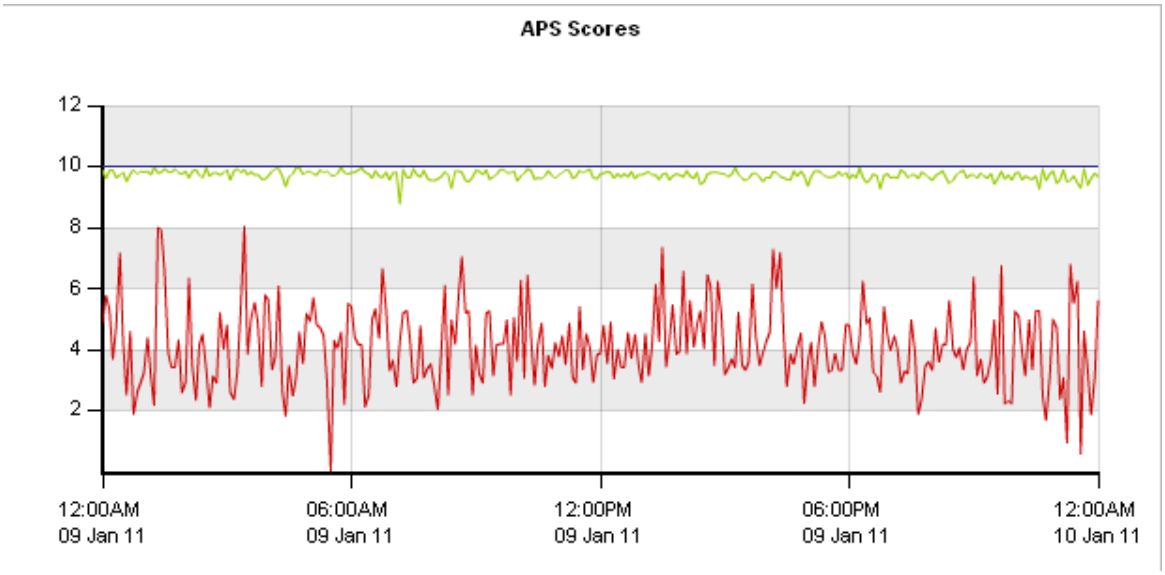
The Exinda appliance provides various ways of measuring Application Performance and Network Service Levels:

- APS: Application Performance Score passively measures application response times and scores application performance against preset criteria.
- SLA: Service Level monitoring actively measures network response times.
- TCP Efficiency: Passively measures TCP retransmissions and calculates TCP Efficiency.
- TCP Health: Passively measures TCP connection states and calculates TCP Health.

6.10.1 Application Performance Score (APS) Reports

Application Performance Score (APS) provides a single data point for the overall health and performance of an application. This report show the score for each APS Object over time.

Note: To configure APS Objects, navigate to 'Objects | Service Levels | Application Performance Score' on the Web UI, advanced mode.



The table below lists each APS Object and also shows the individual metrics used to calculate the score. Each item in the table can be drilled down to view APS details and a graph for that item.

APS Scores

Name	Score	Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
		Network	Server		Inbound	Outbound	
HTTP	9.72	95.89	57.89	32.90	0.10	0.40	100.62
License DB	4.10	263.37	26.66	15.09	0.30	0.70	238.84
SMTP	10.00	19.98	0.32	0.02	2.10	0.00	273.50

The highlighting of the cells indicates how close the results were to the predefined thresholds of the APS Object.

White (No Threshold)	No threshold defined for this metric.
Green (Good)	This results for this metric were below the predefined threshold.
Yellow (Tolerable)	This results for this metric were between 1 and 4 times the predefined threshold.
Red (Frustrated)	This results for this metric were greater than 4 times the predefined threshold.

Note: For more information, consult the APS How to Guide.

6.10.2 Network Response (SLA) Reports

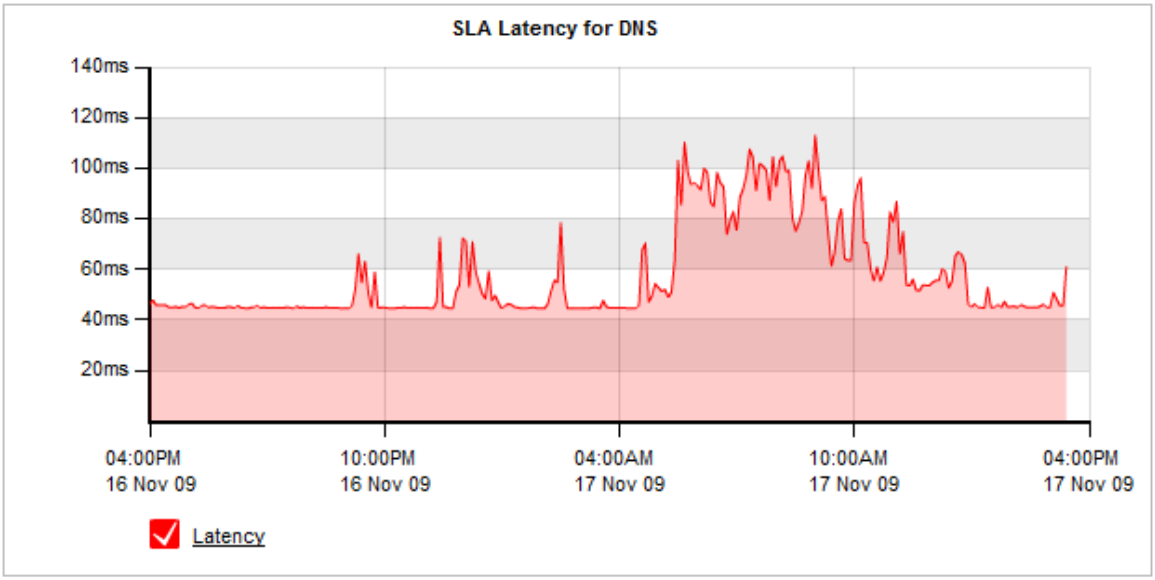
SLA monitoring is a valuable tool for ensuring the performance of your IP provider against predefined criteria.

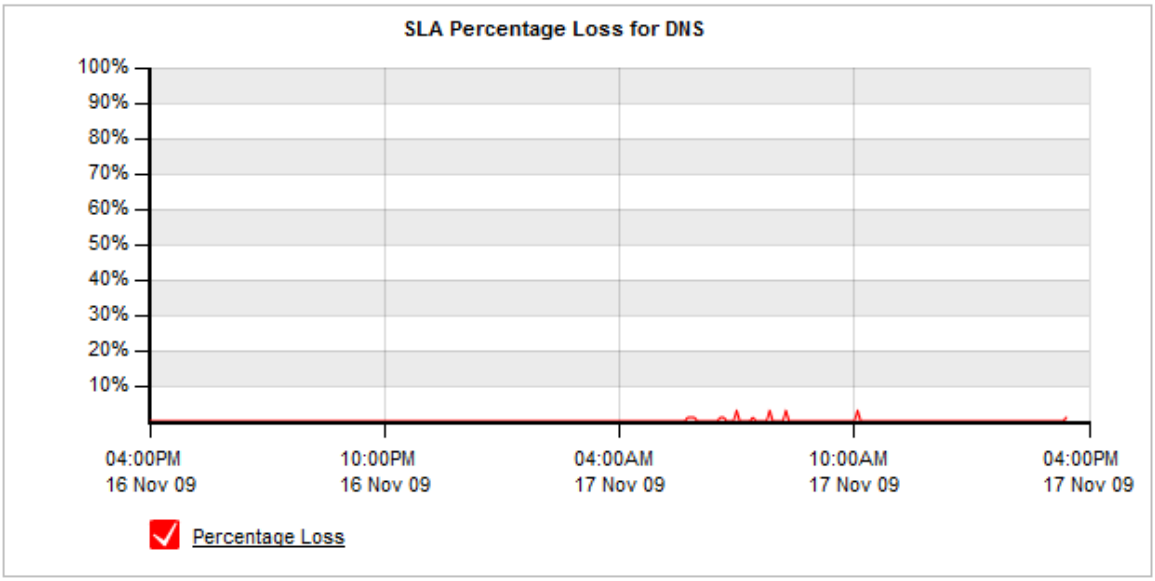
The SLA monitoring works by sending 1 ICMP ping every 10 seconds (each of 64-bits length by default) to the remote site to collect statistics.

To add an SLA Site, click the 'Add/Edit SLA Site...' link.

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

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

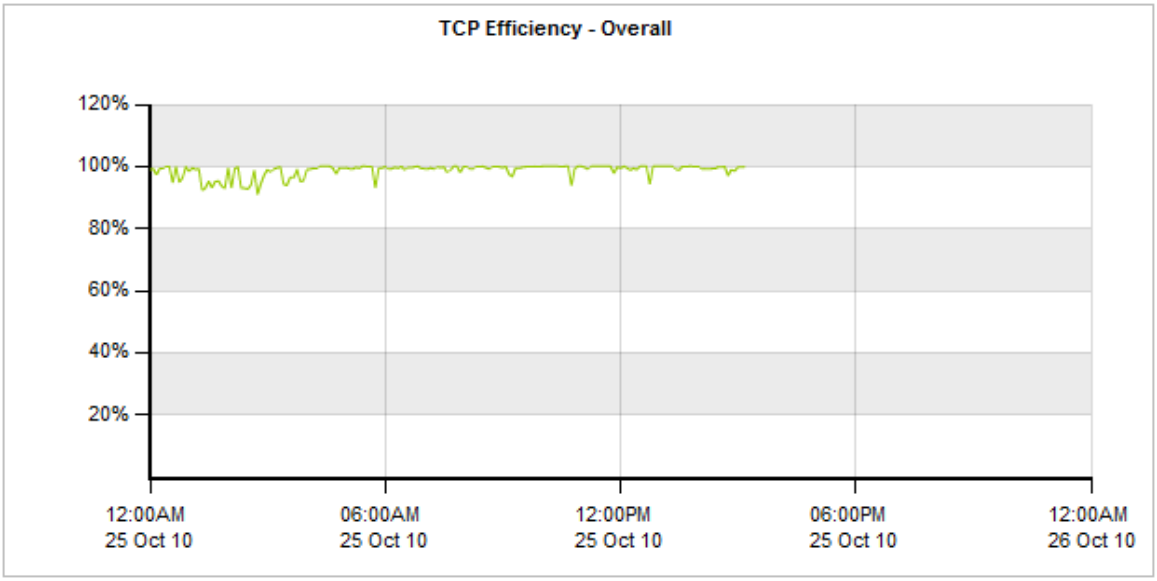




6.10.3 TCP Efficiency Report

The TCP Efficiency Report shows the total efficiency of all TCP connections over time.

The Report can be viewed by Applications, Internal Hosts or External Hosts and the view can be changed by selecting the desired category from the drop-down at the top of the page.



TCP Efficiency is calculated using the formula below:

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

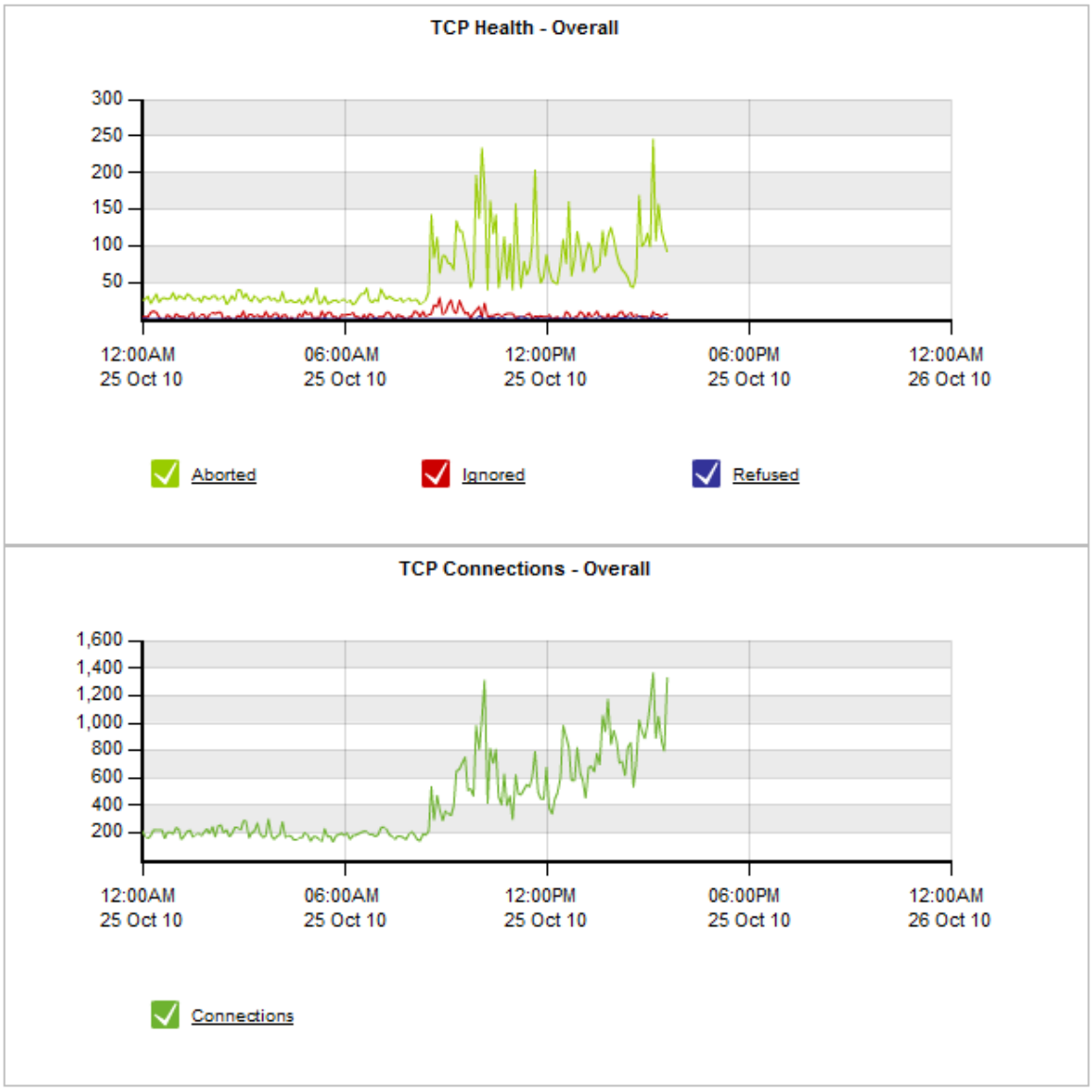
The table below shows both retransmitted bytes and efficiency per Application or Host. Each item in the table below can be drilled down to view TCP Efficiency details and a graph for that item.

Top 50 Least Efficient Applications					
	Bytes Inbound (MB)		Bytes Outbound (MB)		Efficiency (%)
	Retransmitted	Total	Retransmitted	Total	
SSH	0.007	10.254	2.627	98.108	97.57
ICMP	0.000	0.001	0.000	0.002	98.51
RDP	0.000	0.075	0.025	1.656	98.52
Replify	0.000	0.337	0.100	7.769	98.76
SMTP	1.315	107.018	0.024	14.494	98.90
Quicktime	0.231	22.299	0.000	0.385	98.98
HTTP	1.745	388.939	7.281	540.749	99.03
LinkedIn	0.015	2.740	0.007	0.687	99.38
Facebook	0.031	6.423	0.006	0.990	99.50
Jabber	0.000	0.038	0.000	0.033	99.56
Twitter	0.002	0.582	0.001	0.361	99.73
HTTP-ALT	0.000	0.074	0.001	0.161	99.73
Skype	0.001	0.533	0.000	0.031	99.75
SalesForce	0.006	3.245	0.000	0.433	99.84

6.10.4 TCP Health Report

The TCP Health Report shows the number of Aborted, Ignored and Refused TCP connections over time.

The Report can be viewed by Applications, Internal Hosts or External Hosts and the view can be changed by selecting the desired category from the drop-down at the top of the page.



Aborted	Aborted connections are TCP connections that were established, but were closed by a RESET issues by either the client or server rather than a clean close. High numbers of aborted connections can point to network or server problems.

Ignored	Ignored connections are TCP connections where 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.
Refused	Refused connections are TCP connections where a SYN packet was observed and a RESET or ICMP connection refused message was seen 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.

The table below shows the total, aborted, ignored and refused connection counts per Application or Host. Each item in the table below can be drilled down to view TCP Health details and a graph for that item.

Top 50 Applications				
	Connections	Aborted	Ignored	Refused
HTTP	34263	5172	1	6
HTTPS	21925	4941	8	1
ExindaCom	4440	0	822	0
Flash	820	233	0	0
HTTP-ALT	695	0	112	0
POP-SSL	147	110	0	0
LinkedIn	371	93	0	0
MAPI	674	91	0	0
Facebook	688	89	0	0
CIFS	64	3	61	0
SMTP	517	32	0	0
Replify	769	0	0	31
Windows Updates	58	26	0	0
SalesForce	198	21	0	0

6.11 System Reports

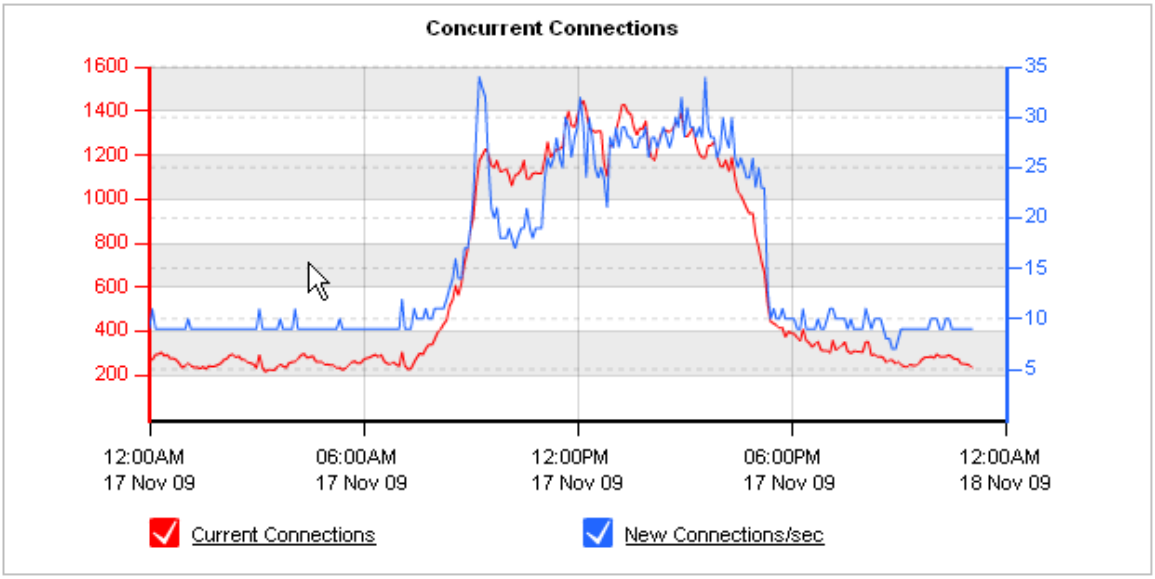
The System Reports show various statistics about system performance and health. There are 6 System Reports available:

- Connections Report: Shows the number of concurrent and new connections.
- Accelerated Connections Report: Shows the number of concurrent and new accelerated connections.

- CPU Usage Report: Shows the CPU usage over time.
- CPU Temperature Report: Shows the CPU temperature over time.
- RAM Usage Report: Shows the RAM usage over time.
- Swap Usage Report: Shows the Swap usage over time.

6.11.1 Connections Report

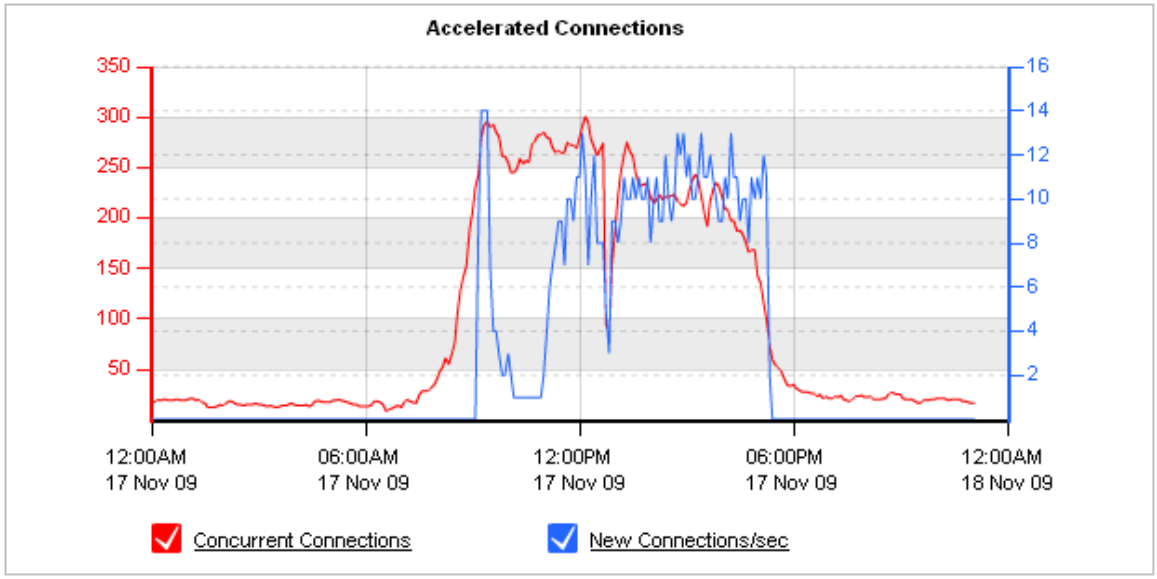
This report shows the number of concurrent connections as well as the connection establishment rate through the Exinda appliance over time.



Systems that report unusually high spikes in the number of connections or the connection rate may be experiencing some form of DoS attack or network problem.

6.11.2 Accelerated Connections Report

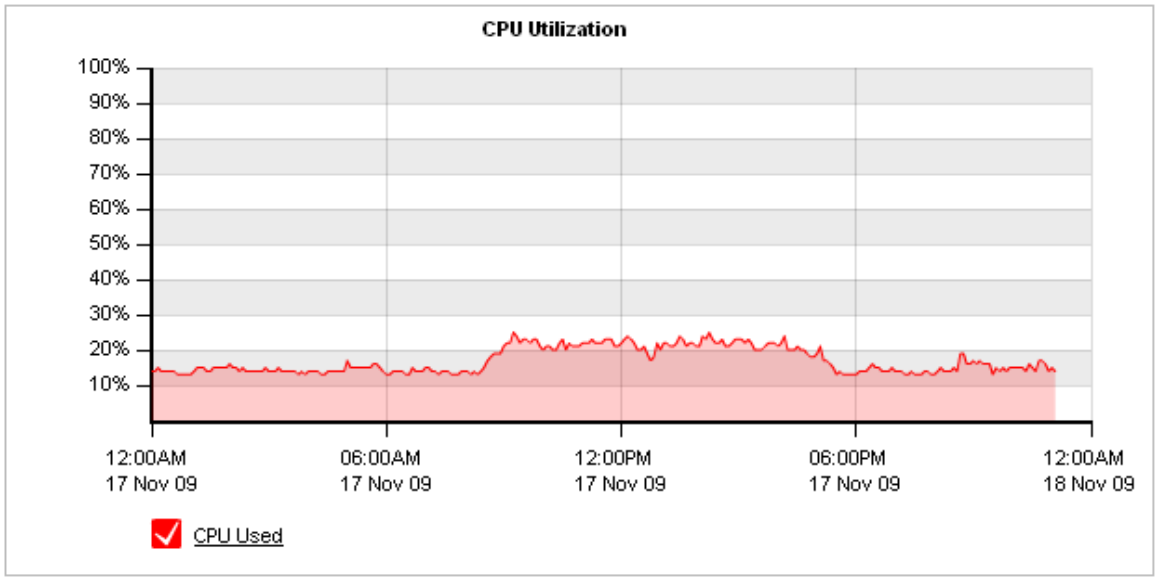
This report shows the number of concurrent accelerated connections as well as the accelerated connection establishment rate through the Exinda appliance over time.



The second graph shows the number of connections through each of the specific application acceleration modules, such as CIFS Acceleration, SSL Acceleration and NCP Acceleration.

6.11.3 CPU Usage Report

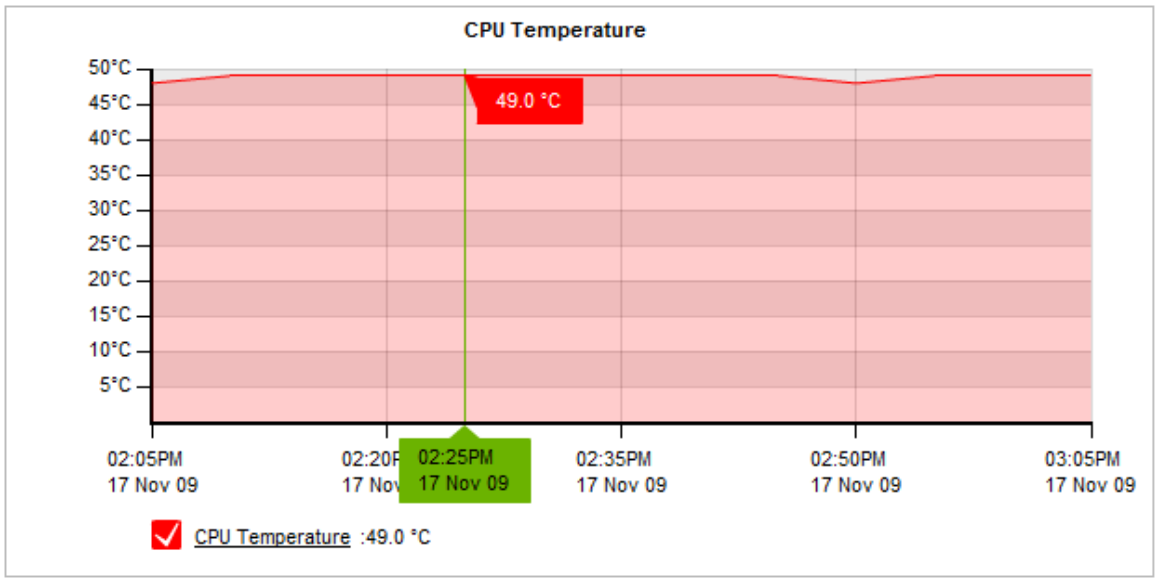
This reports shows the Exinda appliance's CPU usage over time.



Systems running at high CPU usage for long periods of time may be overloaded or may be experiencing a problem. Contact Exinda TAC if the CPU usage constantly reports close to 100%.

6.11.4 CPU Temperature Report

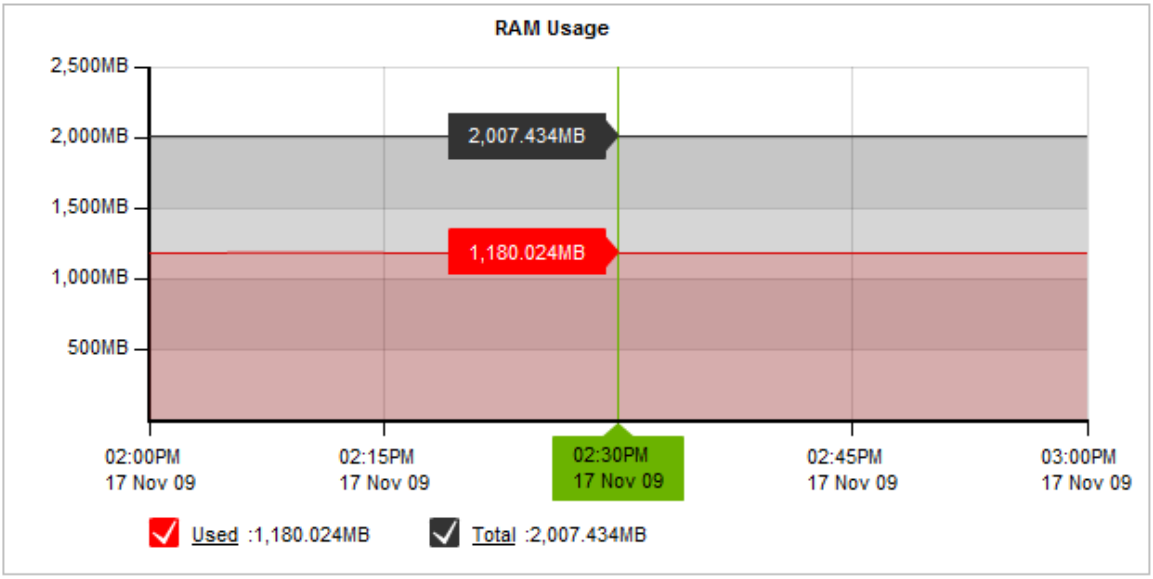
This report show the CPU temperature over time in degrees Celsius.



Systems running at very high temperatures may be experiencing a problem and system performance may be affected. Contact Exinda TAC if the CPU temperature constantly reports hot.

6.11.5 RAM Usage Report

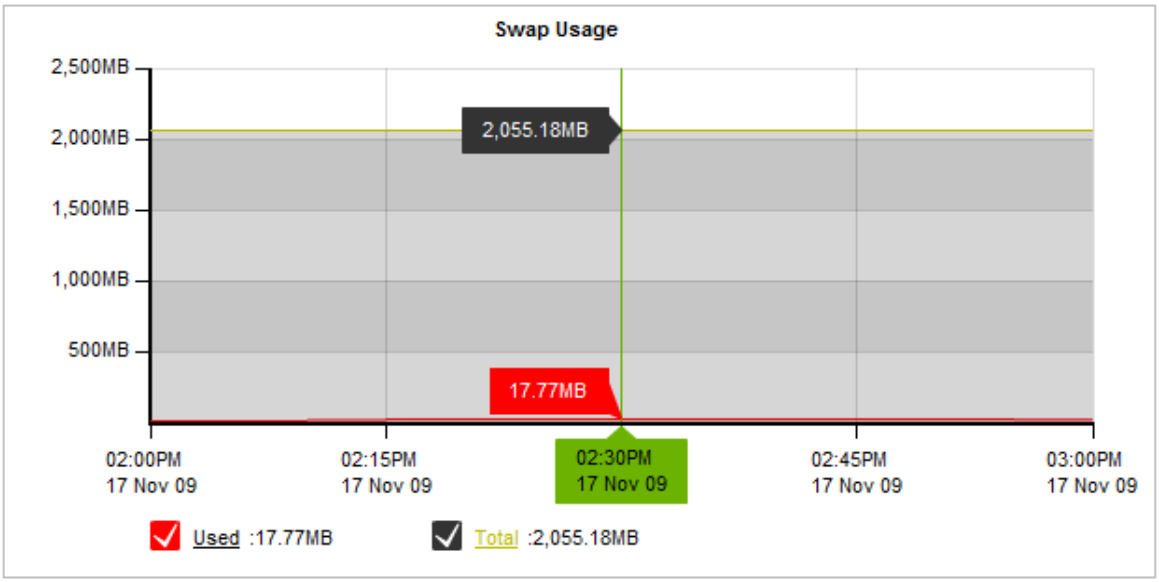
This report shows how much system RAM the Exinda appliance is consuming over time.



Systems that are running low on RAM may experience performance problems. Contact Exinda TAC if RAM usage increases close to the maximum.

6.11.6 Swap Usage Report

This report shows the swap or page file usage of the Exinda appliance over time.



Excessive amounts of swapping may impact system performance so this report provides a way to determine how much swapping the Exinda appliance is doing.

6.12 Applications Report

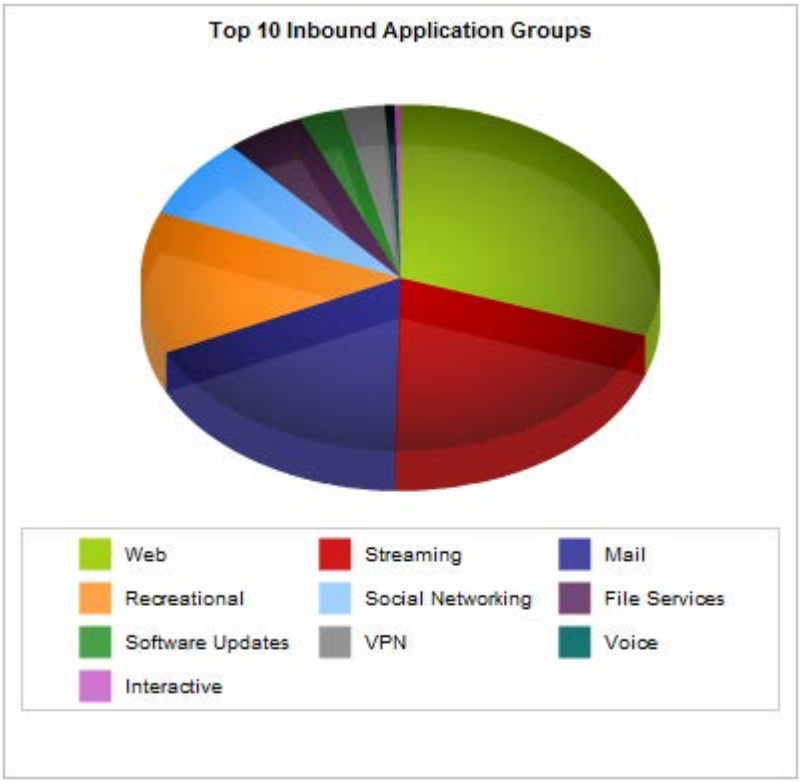
The Application Reports displays a breakdown of the traffic that has passed through the monitored links by Application Object or Application Group. There are also special Application Reports for URLs and VoIP. Use the Application Reports to determine what applications are using the link the most and at what speeds.

There are 4 Application Reports:

- Application Groups Report: Shows the top Application Groups.
- Individual Applications Report: Shows the top Application Objects.
- URLs Report: Shows the top URLs.
- VoIP Report: Shows VoIP flows and MOS information.

6.12.1 Application Groups Report

The Top 10 Application Groups are shown in a pie chart. You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie.



Each table shows the top Application Groups together with the number of packets, number of flows data transferred and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each Application Group.

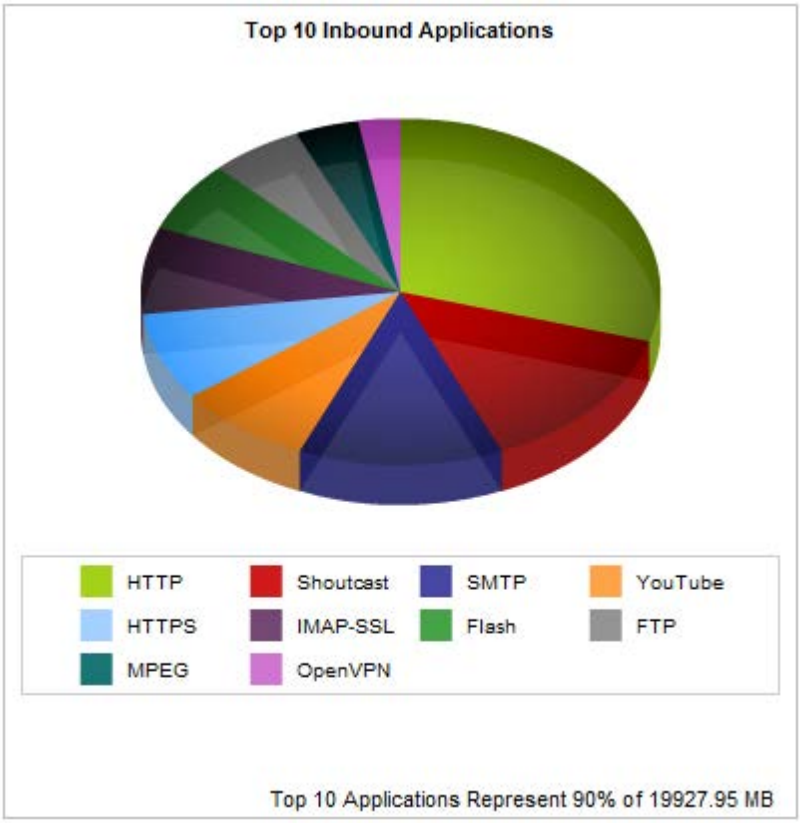
Click on the Application Group name to drill-down into the Individual Applications Report, filtered by that particular Application Group.

Top 50 Inbound Application Groups					
Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
Web	9442485	6807.044	14.25	8801.78	15165
Streaming	3331989	4439.998	152.12	930.83	1388
Mail	3951889	3930.893	54.41	3384.16	578
Recreational	2227319	2971.643	107.79	1377.49	2501
Social Networking...	1266370	1690.538	126.17	1377.49	1296
File Services	1338624	1096.368	494.85	7970.57	32
Software Updates	431603	604.262	788.23	4346.87	181
VPN	736575	596.622	31.05	1326.80	30
Voice	1069909	140.829	11.51	409.92	85
Interactive	859128	81.518	4.22	448.42	119

Note: To customize the Individual Application Objects that make up an Application Group, see the Objects | Applications | Application Groups page.

6.12.2 Individual Applications Report

The Top 10 Application Objects are shown in a pie chart. You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie.



Each table shows the top Application Objects together with the number of packets, number of flows, data transferred and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each Application.

Click on the Application Object name to drill-down into the Hosts Report, filtered by that particular Application Object. You have the option to view Internal or External hosts in the drill-down.

Top 50 Inbound Applications					
Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
HTTP	6817611	5334.422	18.45	8801.78	12960
Shoutcast	1873255	2523.348	258.10	307.57	9
SMTP	1927337	2297.050	297.60	2584.53	291
YouTube	1088274	1512.809	367.74	1377.49	300
HTTPS	2619277	1472.302	7.89	1407.26	2197
IMAP-SSL	1769795	1459.845	26.97	534.73	186
Flash	914997	1199.138	76.21	828.16	1354
FTP	728912	1034.463	5432.26	7970.57	12
MPEG	542279	716.296	203.89	930.83	14
OpenVPN	372946	471.839	96.49	148.52	19

Note: If a previously defined Application Object has been deleted, it will appear in these reports as 'Deleted Application'.

The Applications Report may also contain links to 'Discovered Ports'. These are links to inbound and outbound applications which have not been classified. By clicking 'Discovered Ports', a new report is loaded showing details about the unclassified applications. Source and destination ports for each application are shown in the inbound and outbound tables. Each discovered port can be broken down to the internal/external host by clicking on the link. This helps to drill down and understand what the application really is and what it should be classified as.

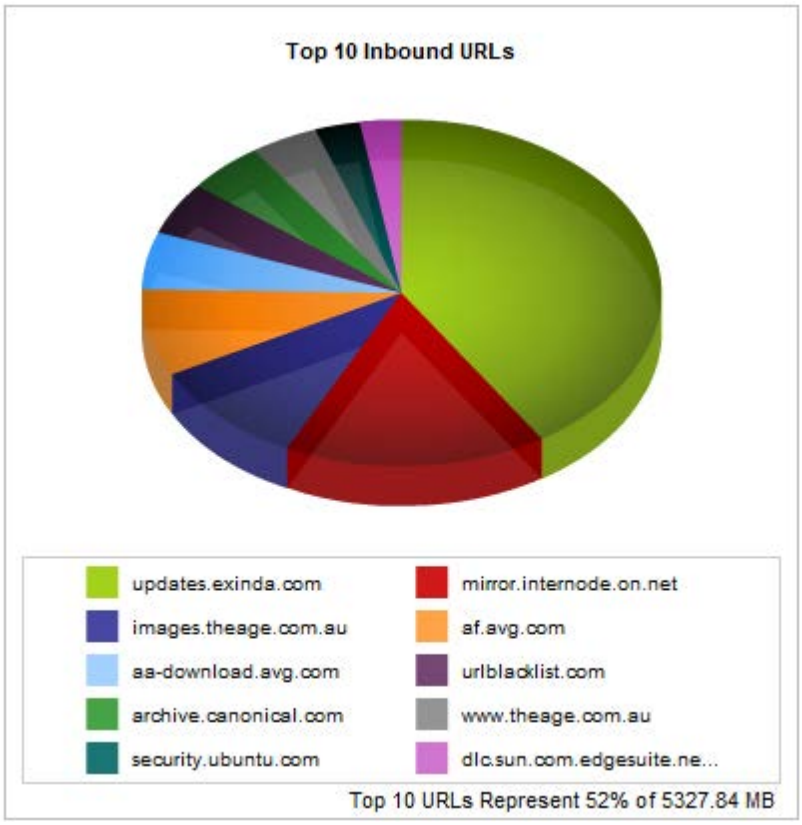
Top 10 Inbound Discovered Ports					
	Application	Packets	Data (MB)	Throughput Avg (kbps)	Throughput Max (kbps)
1	tcp ports 49471 & 6323	366	0.028	0.21	0.30
2	tcp ports 1794 & 41686	257	0.018	0.20	0.30
3	tcp ports 4443 & 6030	186	0.015	0.92	1.74
4	tcp ports 44371 & 10752	152	0.012	0.20	0.30
5	tcp ports 34688 & 33192	129	0.010	0.22	0.33
6	tcp ports 2800 & 10752	158	0.009	0.16	0.32
7	tcp ports 4692 & 48537	161	0.009	0.13	0.21
8	tcp ports 55099 & 19029	107	0.009	0.21	0.28
9	tcp ports 1283 & 62371	59	0.005	0.24	0.33
10	tcp ports 50236 & 48537	18	0.002	0.21	0.37

Note: When deciding how to classify a discovered port, look for a common destination port. If more than two entries appear with the same destination port, the chances are that by adding that port to an Application Object, the application will be classified correctly.

6.12.3 URLs Report

URLs are requested when users visit HTTP sites. They are stored in the form of a domain/host name on the Exinda appliance.

The Top 10 URLs are shown in a pie chart for inbound and outbound traffic. You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie.



Each table shows the top URLs together with the amount of data transferred, number of packets, number of flows and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each URL.

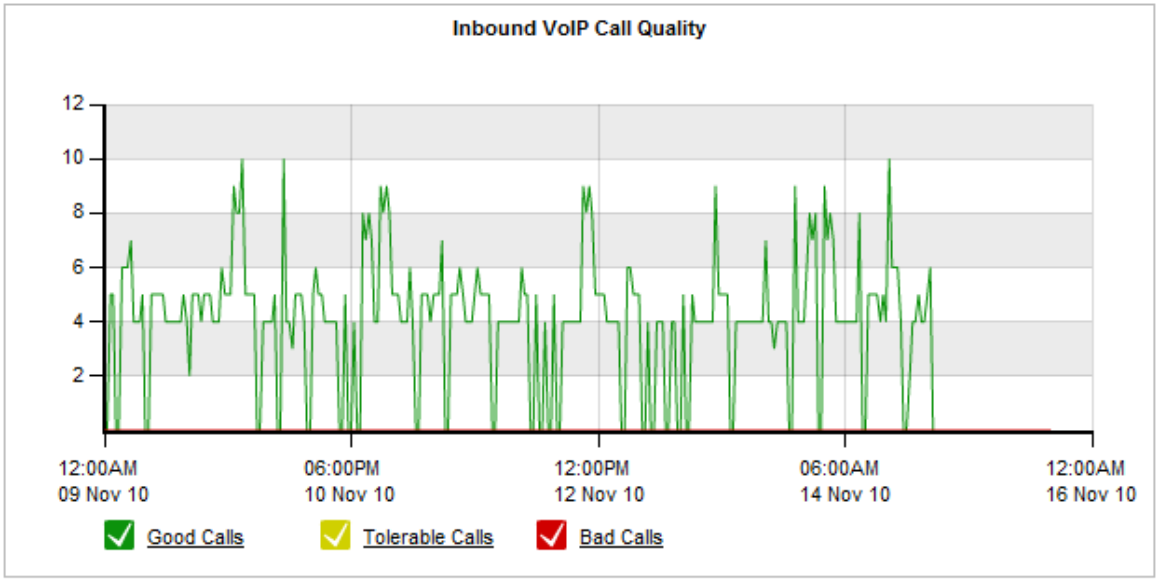
Click on a specific URL to drill-down into the Hosts Report, filtered by that particular URL. You have the option to view Internal or External hosts in the drill-down.

Top 50 Inbound URLs					
Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
updates.exinda.com	815189	1124.869	4981.04	8175.02	7
mirror.internode.on.net	317642	449.981	2595.95	7900.50	72
images.theage.com.au	448747	273.494	83.35	745.06	309
af.avg.com	158276	222.598	2762.92	8295.91	40
aa-download.avg.com	118371	147.128	1883.24	1617.50	2
urlblacklist.com	98498	136.172	672.00	782.32	7
archive.canonical.com	92519	131.373	417.13	2834.83	24
www.theage.com.au	91250	115.655	55.37	101.83	315
security.ubuntu.com	54822	77.100	168.43	2422.13	50
dlc.sun.com.edgesuite.net	50849	71.411	823.94	713.44	1

6.12.4 VoIP Report

The VoIP Report shows call quality over time. The VoIP Report automatically includes any RTP-based VoIP call, including SIP, H.323 and Cisco Skinny.

The graph shows 3 series, the number of "Good", "Tolerable" and "Bad" calls over time. The table below lists the worst quality inbound and outbound VoIP calls over the selected time period.



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

Green (Good)	Number of calls with a MoS greater than 4.
Yellow (Tolerable)	Number of calls with a MoS between 2 and 4.

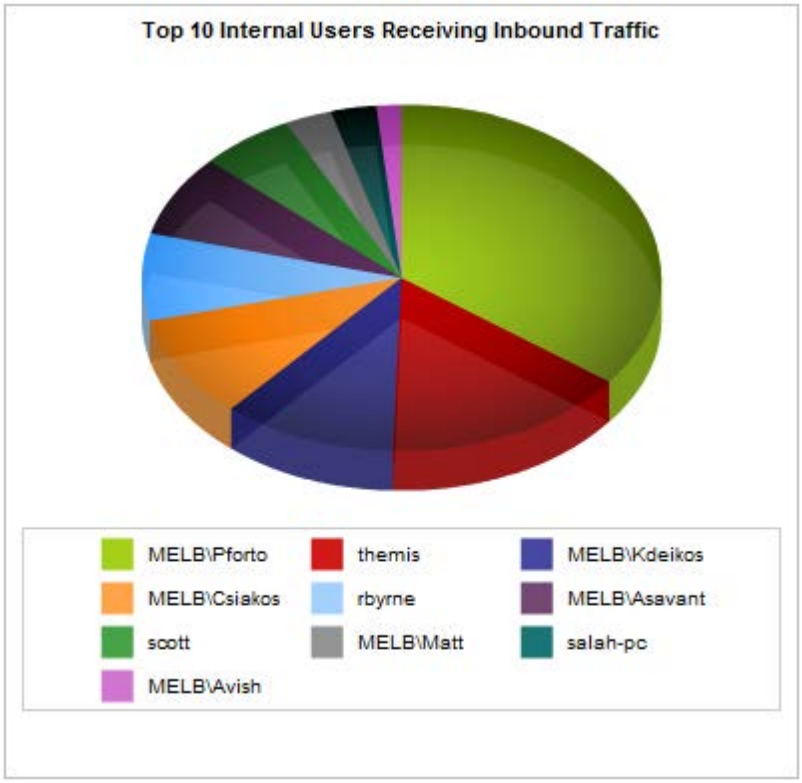
Red (Bad)	Number of calls with a MoS less than 2.

6.13 Users Report

Users are automatically monitored when the Exinda Active Directory Service is installed on a Domain Controller or AD Server.

The Top 10 Users are shown in a pie chart for inbound and outbound traffic. You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie.

You can choose to view either Internal or External Users in this Report by using the drop-down at the top of the page. You can choose to view a particular time period using the time range selection bar at the top of the page.



Each table shows the top Users together with the amount of data transferred, number of packets, number of flows and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each User.

Click on the 'User Name' to drill-down into the Applications Report, filtered by that particular User. You have the option to view Applications, URLs, Hosts and Conversations in the drill-down.

Top 50 Internal Users Receiving Inbound Traffic					
Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
MELB\Pforto	256599	328.319	264.20	4034.39	224
themis	224420	142.290	28.87	1656.61	1194
MELB\Kdeikos	76578	101.077	79.85	887.10	433
MELB\Csiakos	90826	89.588	21.56	3961.84	564
rbyrne	55507	75.806	167.84	946.30	84
MELB\Asavant	110339	71.434	7.47	612.92	1124
scott	60506	54.297	12.48	695.97	689
MELB\Matt	33342	27.351	9.67	1854.87	455
salah-pc	34944	26.560	11.65	855.17	498
MELB\Avish	41831	14.614	1.58	172.73	2243

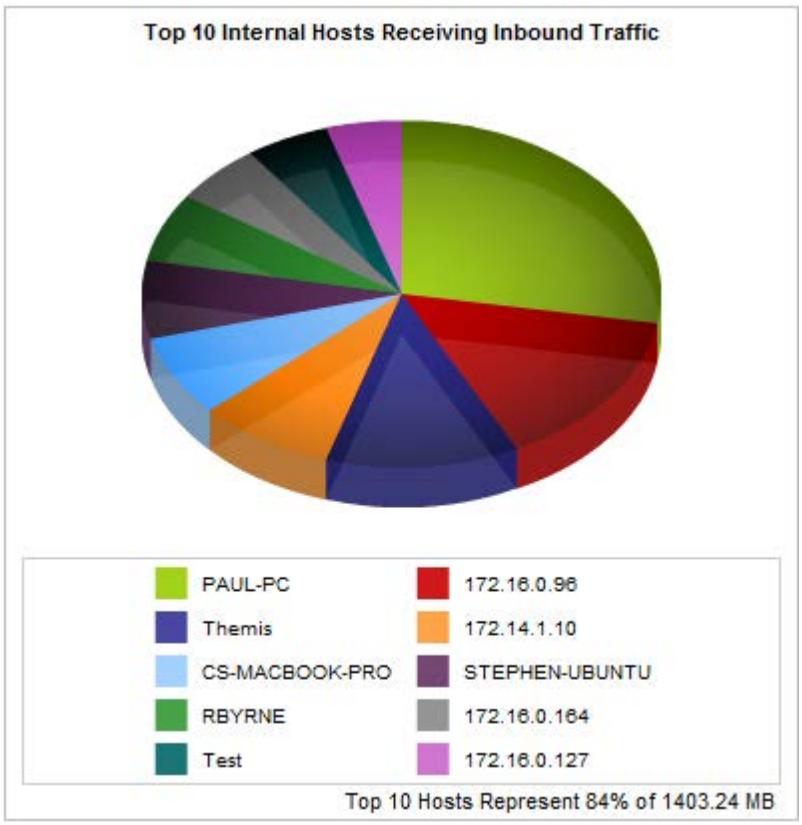
Note: For further information, see the System | Network | Active Directory page and the Objects | Users and Groups page.

6.14 Hosts Report

Hosts are IP address endpoint's in IP transactions and are usually client PCs or servers.

The Top 10 Hosts are shown in a pie chart for inbound and outbound traffic. You can hover over the pie slices to view the amount of data transferred as well as view the percentage of the pie.

You can choose to view either Internal or External Hosts in this Report by using the drop-down at the top of the page. You can choose to view a particular time period using the time range selection bar at the top of the page.



Each table shows the top Hosts together with the amount of data transferred, number of packets, number of flows and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each Host.

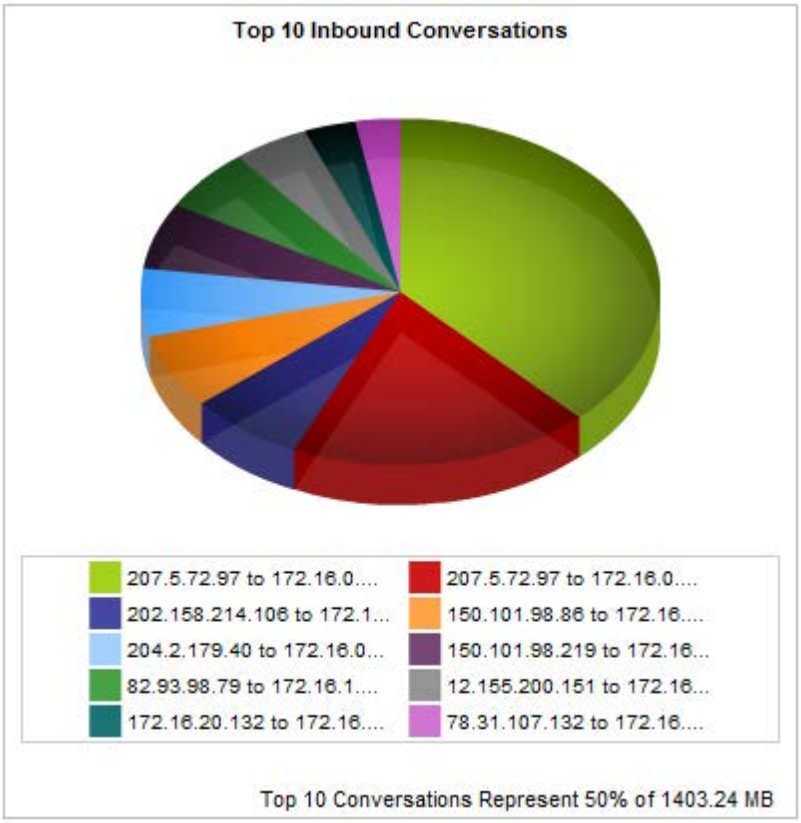
Click on the 'Host Name' to drill-down into the Applications Report, filtered by that particular Host. You have the option to view Applications, URLs, Hosts and Conversations in the drill-down.

Top 50 Internal Hosts Receiving Inbound Traffic						
Hostname [+] Show Details	Address	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
PAUL-PC	172.16.0.67	256679	328.333	263.18	4034.39	224
172.16.0.96	172.16.0.96	170136	176.929	63.93	4916.38	342
Themis	172.16.1.85	224508	142.331	28.80	1656.61	1198
172.14.1.10	172.14.1.10	76604	101.079	79.24	887.10	433
CS-MACBOOK-PRO	172.16.0.182	90826	89.588	21.56	3961.84	564
STEPHEN-UBUNTU	172.16.0.114	170381	86.534	24.67	4830.92	456
RBYRNE	172.16.0.213	55507	75.806	167.84	946.30	84
172.16.0.164	172.16.0.164	56105	66.111	48.40	6803.19	406
Test	172.16.0.236	74463	61.797	15.66	612.92	934
172.16.0.127	172.16.0.127	61851	55.486	12.57	695.97	708

6.15 Conversations Report

A conversation is defined as data that is transacted between two hosts using the same application within the specified time period. Conversations can also be referred to as sessions.

The pie chart shows the top 10 inbound and outbound Conversations that have occurred on your monitored interfaces. You can choose to view a particular time period using the time range selection bar at the top.



Each table shows the top Conversations together with the amount of data transferred, number of packets, number of flows and throughput statistics. Click on the 'Show Details' link to expose RTT, Transaction Delay and Efficiency statistics for each Conversation.

Click on the 'Host Name' to drill-down into the Hosts Report, filtered by that particular Host. You have the option to view Applications, URLs, Hosts and Conversations in the drill-down.

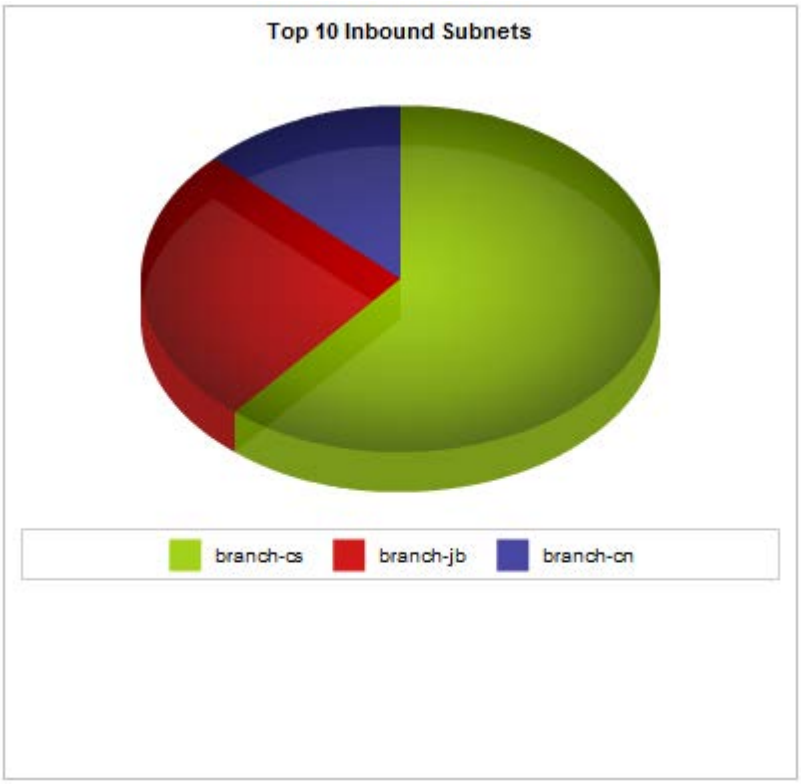
Click on the Application Object name to drill-down into the Applications Report, filtered by that particular Application Object. You have the option to view Internal or External Hosts in the drill-down.

Top 50 Inbound Conversations						
External Host [+] Show Details	Internal Host	Application	Data (MB)	Throughput (kbps) Average	Max	Flows
207.5.72.97	172.16.0.67	HTTPS	264.435	461.89	828.50	5
207.5.72.97	172.16.0.96	IMAP-SSL	131.470	185.05	454.53	6
202.158.214.106	172.16.0.164	HTTP	49.833	5831.85	6803.19	2
150.101.98.86	172.16.0.213	Flash	48.308	842.00	946.30	1
204.2.179.40	172.16.0.67	Adobe Updates	44.323	4034.39	4034.39	1
150.101.98.219	172.16.0.114	YouTube	43.571	830.07	857.89	1
82.93.98.79	172.16.1.85	SMTP	40.777	175.81	257.79	15
12.155.200.151	172.16.1.85	SMTP	33.122	343.46	1000.48	15
172.16.20.132	172.16.0.63	OpenVPN	22.522	104.24	148.52	15
78.31.107.132	172.16.1.85	HTTP	19.458	797.01	817.33	1

6.16 Subnets Report

The Exinda appliance allows you to monitor and filter traffic by subnet. This will allow you to see the network usage of each of your business departments, branch offices or groups providing they are implemented in separate network subnets. To configure a subnet for monitoring, you must create a Network Object. Network Objects that are marked as 'Subnet Report' will appear in this section.

The traffic distribution of all subnets is displayed in a pie chart, broken down into inbound and outbound traffic. Internal and external subnets can be selected by using the drop-down at the top of the page.



Each table shows the amount of inbound and outbound data transferred and throughput statistics for each subnet. Click on the appropriate link to further drill-down into the Applications Report, Hosts Report, Conversations Report, URLs Report or Users Report for each subnet.

	branch-cs	Inbound	Outbound	Total
View Applications	**Average Throughput (kbps):**	0.37	0.72	
View Hosts	**Maximum Throughput (kbps):**	6.68	26.00	
View Conversations	**Data Transfer (MB):**	0.393	0.766	**1.159**
View URLs				
View Users				

	branch-jb	Inbound	Outbound	Total
View Applications	**Average Throughput (kbps):**	5.53	6.26	
View Hosts	**Maximum Throughput (kbps):**	21.26	156.77	
View Conversations	**Data Transfer (MB):**	0.169	0.833	**1.002**
View URLs				
View Users				

	branch-cn	Inbound	Outbound	Total
View Applications	**Average Throughput (kbps):**	0.56	0.61	
View Hosts	**Maximum Throughput (kbps):**	4.51	30.17	
View Conversations	**Data Transfer (MB):**	0.082	0.089	**0.171**
View URLs				
View Users				

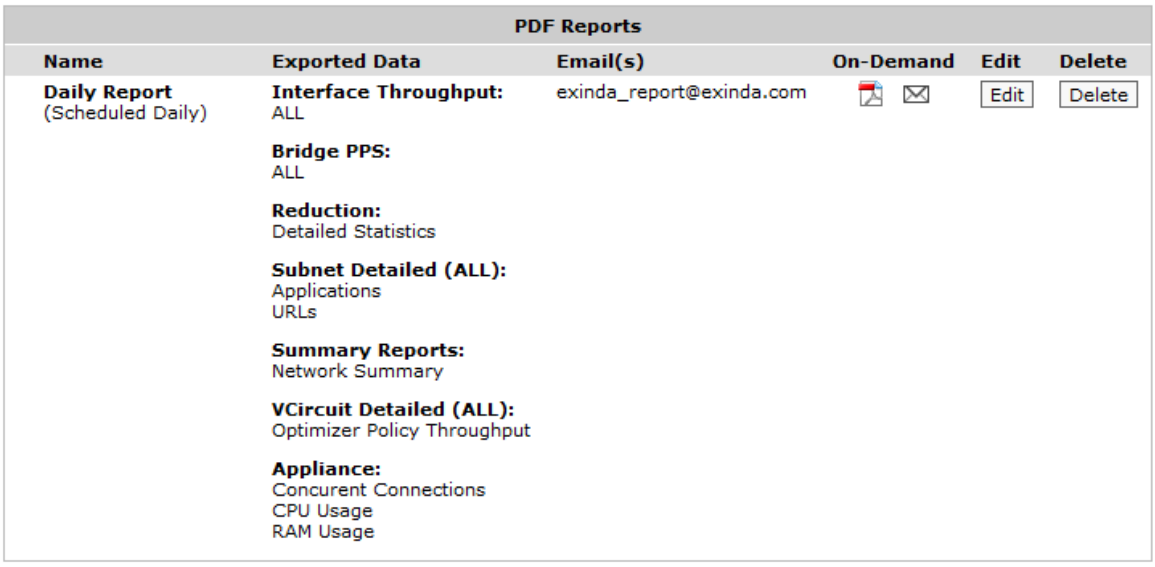
6.17 PDF Reporting

PDF Reporting allows you to configure PDF versions of the monitoring reports to be emailed or downloaded either on demand or at scheduled intervals. PDF Reports can be sent to multiple recipients by comma or semi-colon separating email addresses.

Note: To configure a PDF Report, navigate to 'Report | PDF Reports' on the Web UI, advanced mode.

PDF Reports are listed in the table on this page. PDF Reports can be generated and either emailed or downloaded on-demand by clicking either the PDF icon (to generate and download) or the envelope icon (to generate and email). PDF 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 PDF Report by clicking on the appropriate button next to the report in the table.

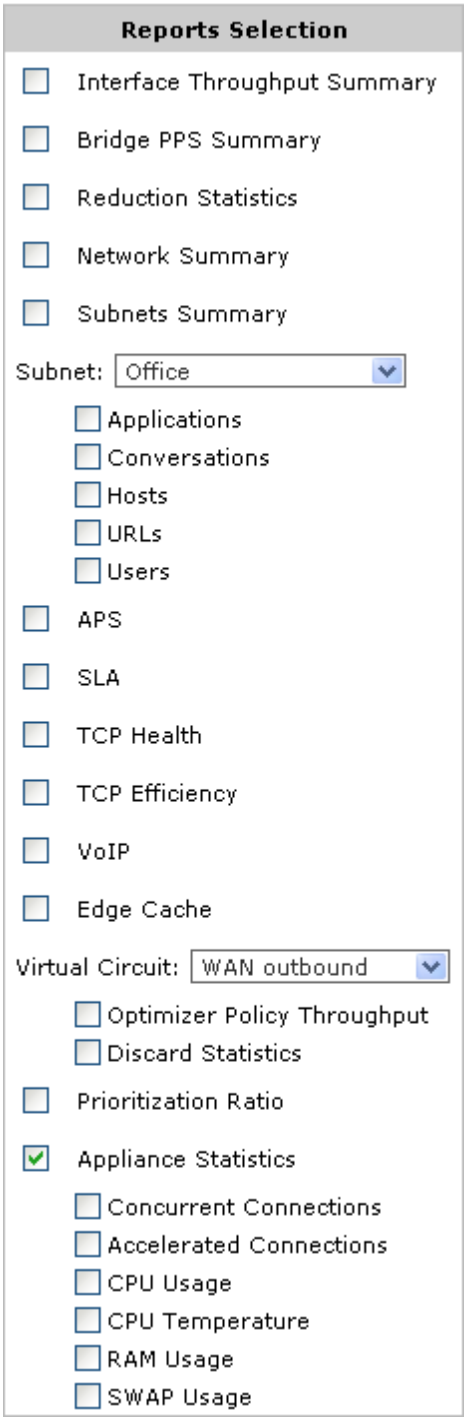


PDF Reports

Name	Exported Data	Email(s)	On-Demand	Edit	Delete
Daily Report (Scheduled Daily)	**Interface Throughput:** ALL **Bridge PPS:** ALL **Reduction:** Detailed Statistics **Subnet Detailed (ALL):** Applications, URLs **Summary Reports:** Network Summary **VCircuit Detailed (ALL):** Optimizer Policy Throughput **Appliance:** Concurent Connections, CPU Usage, RAM Usage	exinda_report@exinda.com		Edit	Delete

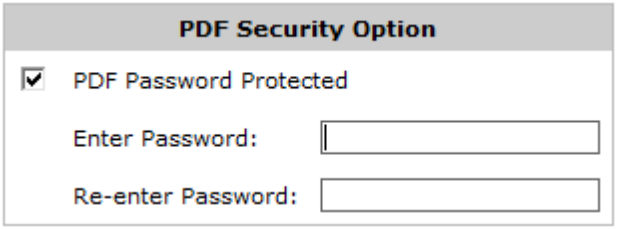
New PDF Reports can be added by clicking on the 'Add New PDF Report' link at the top of the page. There are 3 steps involved in configuring a PDF Report.

Step 1: Reports Selection



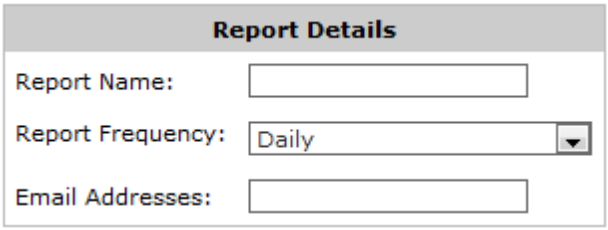
Select the various reports you wish to include in the PDF Report. Most of the reports available from the Web UI are available as PDF Reports.

Step 2: PDF Security



You can optionally password protect PDF documents by specifying a password at Step 2.

Step 3: Report Details

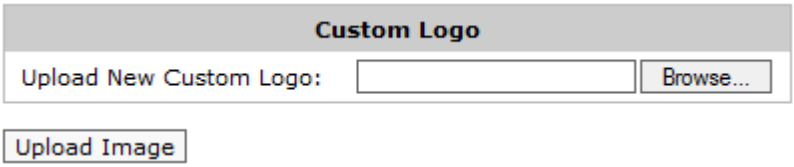


Report Name	Specify a meaningful name for the new PDF Report.
Report Frequency	Specify a time range for this PDF Report. Scheduled reports can be generated Daily, Weekly or Monthly. On-demand reports can include any time range available to the Exinda appliance, including custom time ranges.
Email Addresses	Specify 1 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.

Note: Daily scheduled PDF Reports are generated every morning at 1am.

6.17.1 Custom Report Logo

This form allows you to upload a custom logo that will be inserted onto the cover page of any PDF Report generated by the Exinda appliance.



Note: Files should be no more than 300px wide by 300px high and must be in PNG format with maximum file size of 3MB.

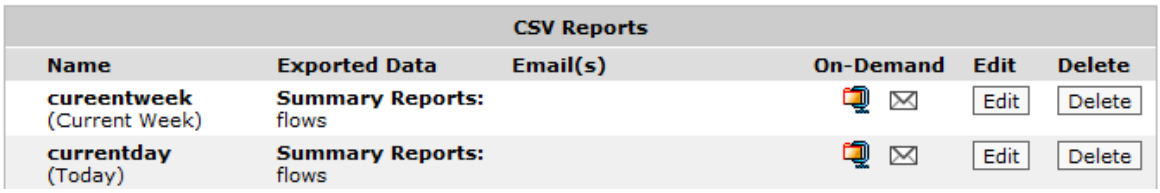
6.18 CSV Reporting

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.

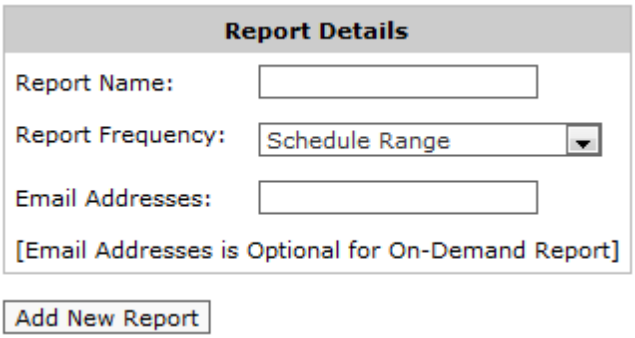
Note: To configure a CSV Report, navigate to 'Report | CSV Reports' on the Web UI, advanced mode.

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.



New CSV Reports can be added by using the form at the top of the page.



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: For information about the schema used in CSV Reports, consult the SQL Access using ODBC How to Guide.

Note: Daily scheduled CSV Reports are generated every morning at 1am.

Part VII

7 Optimizer Configuration

The Optimizer delivers Quality of Service and Application Acceleration (x800 series only) mechanisms to improve application performance on the network. The intuitive, policy-based management helps match network behaviour to business objectives.

As an analogy, vehicle traffic on road systems can be dramatically slowed by disorganized control of traffic. Through intelligent traffic flow co-ordination techniques (such as allocating road lanes for particular types of vehicles), road traffic efficiency can be dramatically increased. Similarly, the efficiency of data flow on an IP network can be significantly improved using an intelligent optimization system powered by custom defined optimization rules.

As each network link has a fixed amount of bandwidth limiting the amount of data it may carry, optimum performance can be achieved by pre-sorting the data before it reaches the bottleneck links (typically the link between your network and the internet). Therefore "mission-critical" data is given priority over non-time sensitive data flow, such as SMTP mail or FTP traffic.

A Vehicle Traffic Analogy to Optimization

Using the vehicle analogy, if you have a number of people you need to get from point A to point B, via a freeway which passes over a bridge with a reduced number of lanes, the best way to get the most urgent passengers there first, is to:

- Sort the passengers into different vehicles so that the urgent passengers are grouped together in the fast cars;
- Identify these urgent car groups and allocate them to the first lanes;
- Similarly, sort the other groups of cars from fast (high priority to low priority);
- Give permission to certain slower groups to be allowed in the fast lanes, if and only, there is no fast car traffic;
- If there are certain groups which need a dedicated lane, then allocate the lane on the bridge as such.

By pre-determining these rules and queuing cars before they reach the bottleneck, it is possible to dramatically increase the traffic capacity of the road towards its theoretical maximum. To optimize the efficiency of your IP network, you need to carefully set the queuing or "optimizer" rules to meet the network requirements.

The optimizer provides:

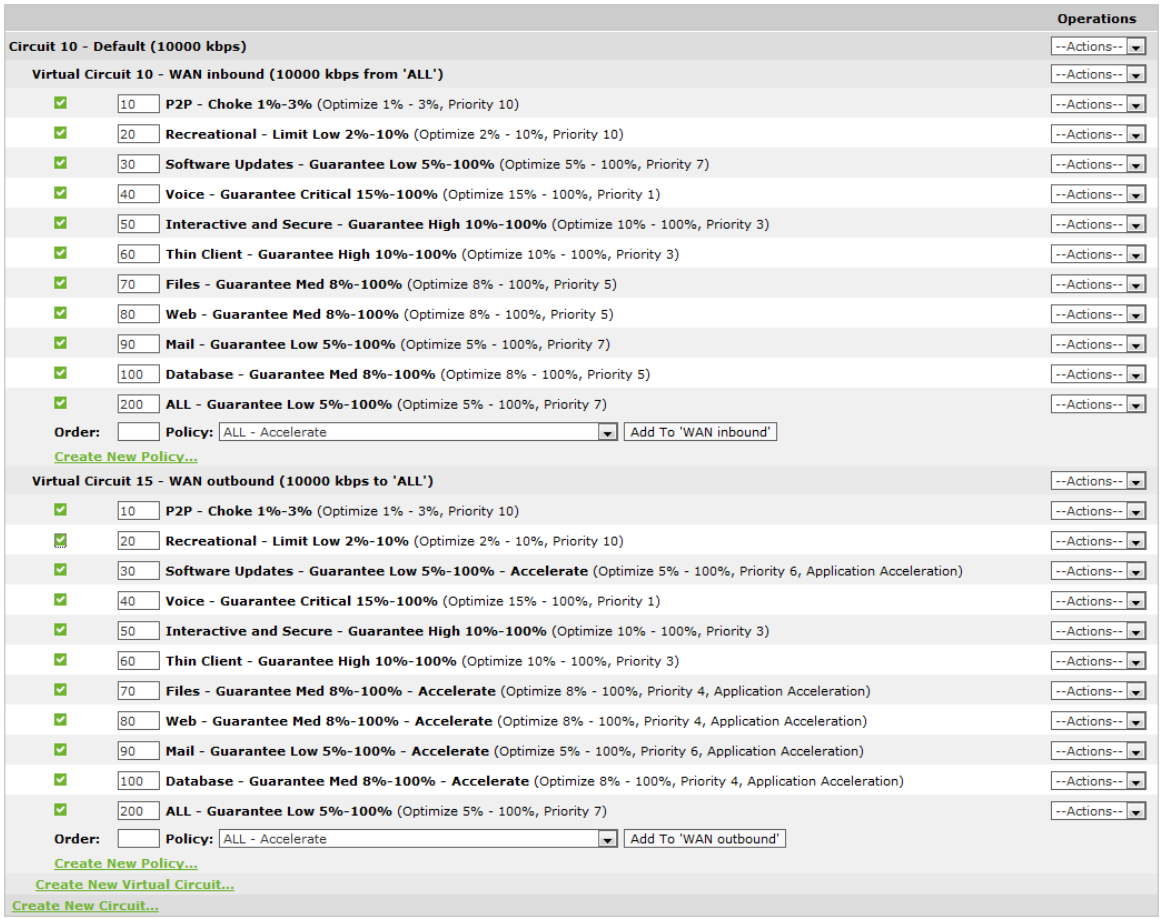
- Rate shaping
- Traffic prioritization

- Application Acceleration
- Per Host QoS
- ToS/DSCP tagging
- Traffic blocking
- Time-based policies

7.1 Optimizer Policy Tree

Optimizer Policies are organized in a tree structure, and traffic is matched top-down, first by Virtual Circuits (VC), then by Policies. As traffic flows through the Exinda appliance, it is first matched to a Virtual Circuit (in order of Virtual Circuit number), then by a Policy within that Virtual Circuit (by order of Policy number).

Once traffic falls into a Virtual Circuit, it will never leave, so it must be captured by a policy within that Virtual Circuit. Similarly, once traffic is matched by a Policy, it never leaves. The means, more specific Virtual Circuits and Policies should be configured higher in order (towards the top) whereas more general Virtual Circuits and Polices should be last.



Circuits, Virtual Circuits and Policies can be manipulated by selecting various options from the drop-down to the right of the respective item.

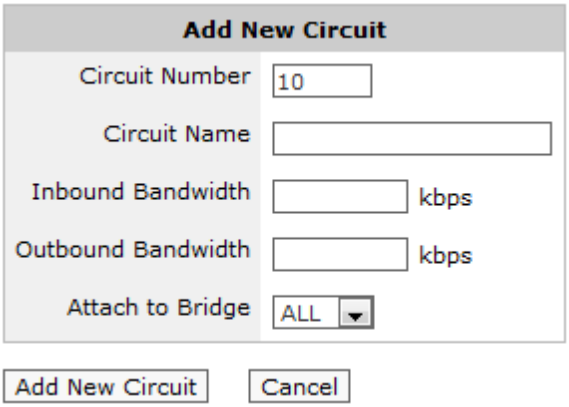
Note: System default Policies cannot be edited. Instead, they can be cloned, then customized.

The Optimizer service is controlled by clicking on the Optimizer links in the main toolbar.

Note: To view/change additional Optimizer configuration options, navigate to 'System | System Setup | QoS Configuration' on the Web UI, advanced mode.

7.1.1 Circuits

Circuits define physical connections to the WAN/Internet. If you have more than 1 bridge configured, you can bind different Circuits to each bridge.

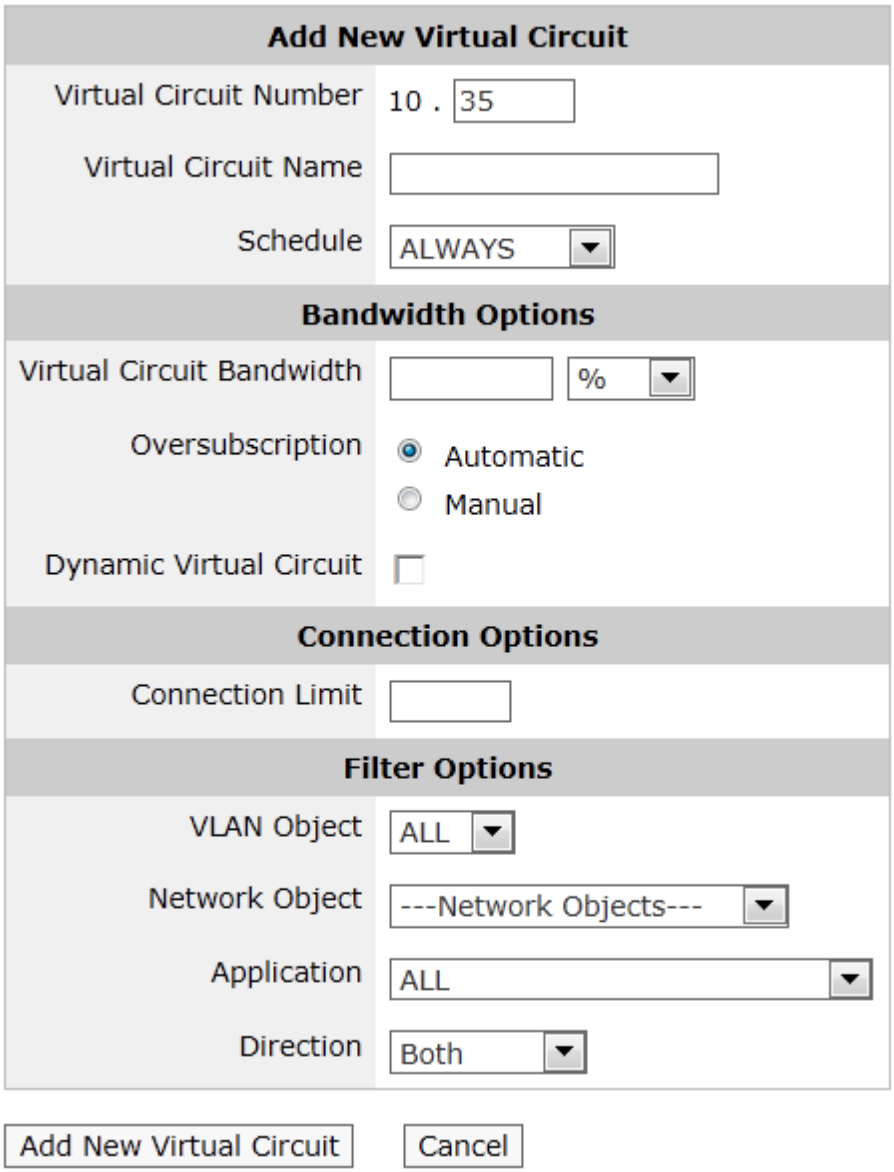


Number	The order of the Circuit relative to other Circuits.
Name	A logical name that represents the Circuit.
Inbound / Outbound Bandwidth	The available bandwidth of the Circuit. If the Circuit is synchronous, the inbound and outbound bandwidth values should be the same.
Attach to Bridge	Specify the bridge to bind the Circuit to.

Typically, one Circuit would be created for each physical link to the WAN/Internet for which the Exinda appliance is placed in-line with. Circuits whose traffic can be filtered out by VCs, or by attaching it to a specific bridge, should be configured first; whereas the Internet Circuit (which contains a “Catch All” Virtual Circuit) must be configured last.

7.1.2 Virtual Circuits

Virtual Circuits (VCs) are created within Circuits and are used to logically divide/partition the Circuit. For example, a Virtual Circuit may be configured for each branch office or, one Virtual Circuit for WAN data and one Virtual Circuit for Internet data. Each Virtual Circuit can contain different policies, which allows each Virtual Circuit to be treated differently.



Number	The order of the Virtual Circuit relative to other Virtual Circuits within the same Circuit.
Name	A logical name that represents the Virtual Circuit.
Schedule	A schedule that defines when the Virtual Circuit should be active.
Bandwidth	The maximum bandwidth used by the Virtual Circuit.

Oversubscription	Specify the behaviour when multiple Virtual Circuits are oversubscribed (the sum of the Virtual Circuit bandwidths exceed the parent Circuit bandwidth). The Exinda appliance can automatically calculate the oversubscription bandwidths or you can specify them manually. For more information, see the Virtual Circuit Oversubscription page.
Dynamic Virtual Circuit	This option allows you to specify per host QoS for each host that falls into this Virtual Circuit. For more information, see the Dynamic Virtual Circuit page.
VLAN Object	VLAN tags or priorities used to filter out what traffic falls into the Virtual Circuit.
Network Object	Subnets/hosts/users/groups used to filter out what traffic falls into the Virtual Circuit.
Application	Application or Application Group used to filter out what traffic falls into the Virtual Circuit.
Direction	The traffic direction the Virtual Circuit should apply to.

The Filter Options are used to define what traffic falls into the Virtual Circuit. Filters can consist of VLAN Objects, Network Objects, Application/Application Groups and Direction. These filters are AND'd together.

Example: A Virtual Circuit with a Network Object 'Email Server' and an Application Group 'Mail' will catch all Mail traffic to/from the Email Server.

Network Objects are typically used when Virtual Circuits are created for specific branch office locations or user group. Each branch office location or user group would be represented by a Static Network Object (typically 1 or more subnets) or a Dynamic Network Object (such as an Active Directory Group) and these Network Objects are defined in the Virtual Circuit. Only traffic to/from the subnets/users defined by the Network Object in the Virtual Circuit fall into the Virtual Circuit itself, all other traffic is evaluated by the next Virtual Circuit, and so on.

A default Network Object, Private Net, exists which defines all non-routable subnets. This can be used to create a Virtual Circuit for all WAN data. Another default Network Object, ALL, when used in a Virtual Circuit, will capture all traffic. This is called a “Catch All” Virtual Circuit and is typically the last (or only) configured Virtual Circuit.

The direction is used to ensure that the Virtual Circuit only captures traffic in a certain direction. This is useful for asynchronous circuits, as these generally require that at least 2 Virtual Circuits are defined, one for the inbound bandwidth and one for the outbound bandwidth.

If a network object is used in conjunction with a direction, the following rules apply:

Network Object	Direction	Captured Traffic
All	Both	All traffic, both inbound and outbound.
All	Inbound	All inbound traffic.
All	Outbound	All outbound traffic.
Not All	Both	Only inbound and outbound traffic to and from the subnets defined by the Network Object.
Not All	Inbound	Only inbound traffic **to** the subnets defined as 'internal' by the Network Object and **from** the subnets defined as 'external' by the Network Object.
Not All	Outbound	Only outbound traffic **from** the subnets defined as 'internal' by the Network Object and **to** the subnets defined as 'external' by the Network Object.

Note: The bandwidth used by a single Virtual Circuit must not exceed the parent Circuit bandwidth in either direction, but the sum of all Virtual Circuit bandwidths in either direction can exceed the parent Circuit bandwidth. This is called oversubscription and more information is available on the Virtual Circuit Oversubscription page.

7.1.2.1 Virtual Circuit Oversubscription

Over-subscription is where the sum of the Virtual Circuit bandwidths exceeds the sum of the parent Circuit bandwidth. This is the case in the following situation:

Circuit Bandwidth = 2Mbps

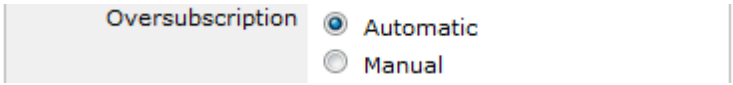
Virtual Circuit Bandwidth = 1Mbps

Virtual Circuit Bandwidth = 1Mbps

Virtual Circuit Bandwidth = 1Mbps

This means, the sum of the 3 Virtual Circuits is 3Mpbs, but the Circuit bandwidth is only 2Mbps. The Virtual Circuits are oversubscribed.

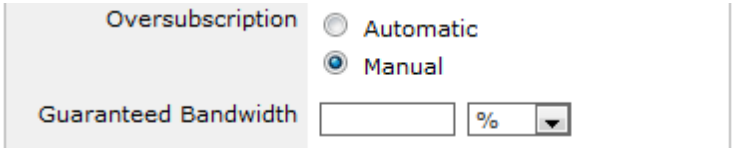
There are 2 ways of dealing with oversubscribed Virtual Circuits, Automatic and Manual.



What happens in the ***Automatic*** case is that each Virtual Circuit will be guaranteed bandwidth on a pro-rata basis, 2/3Mbps (= .66Mbps) each and will be able to burst up to the specified bandwidth of 1Mbps (if this bandwidth is available). Under congestion (each Virtual Circuit under load) they will each share the Circuit's 2Mbps. If only 1 Virtual Circuit is under load, it will get the full 1Mbps. If only 2 Virtual Circuits are under load, they will both get 1Mbps.

The same pro-rata calculation is applied to all policies within an oversubscribed Virtual Circuit automatically.

In the ***Manual*** case you can specify a Guaranteed Bandwidth for each Virtual Circuit.



So using the example above, you can create the Virtual Circuits as follows:

Circuit Bandwidth = 2Mbps

Virtual Circuit Bandwidth = 1Mbps, Guarantee: 1Mbps

Virtual Circuit Bandwidth = 1Mbps, Guarantee: 512kbps

Virtual Circuit Bandwidth = 1Mbps, Guarantee: 512kbps

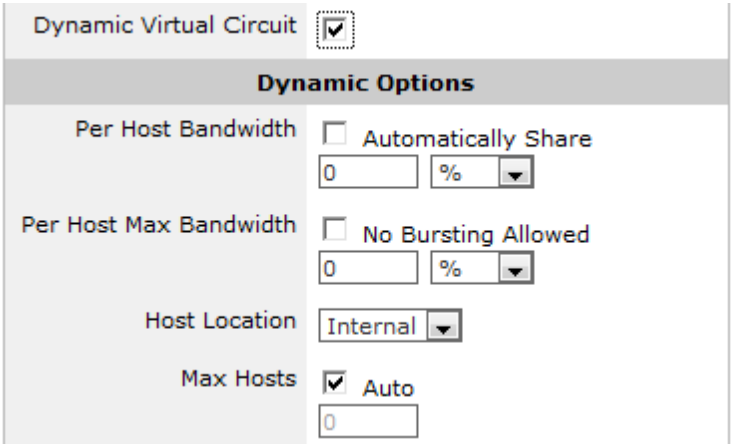
Note: The sum of all the Virtual Circuit Guaranteed Bandwidths must not exceed the parent's Circuits bandwidth in both directions.

In this case, we've decided that the 1st Virtual Circuit will always receive the full 1Mbps if it needs it. The other 2 Virtual Circuits will receive 512kbps each. If the first Virtual Circuit is not using all of it's 1Mbps, the other 2 Virtual Circuits can burst up to the full 1Mbps. The priority by which Virtual Circuits consume the burst bandwidth is determined by the priority of the policies within the Virtual Circuits.

Note: There can be a mixture of Automatic and Manual Virtual Circuits in the same Circuit. The Guaranteed Bandwidths for each Manual Virtual Circuit are allocated first, then the Automatic calculations are made of the remaining bandwidth.

7.1.2.2 Dynamic Virtual Circuits

Dynamic Virtual Circuits allow administrators to allocate bandwidth to each host that matches the Virtual Circuit.



When the 'Dynamic Virtual Circuit' checkbox is selected on the Virtual Circuit configuration page, the following options will become available.

Per Host Bandwidth	Specify the amount of bandwidth (in kbps or percentage of the Virtual Circuit bandwidth) that each Host will receive. This bandwidth is guaranteed, so it will be available to each host if required. If 'Automatically Share' is selected the amount of bandwidth each Host receives is calculated by dividing the Virtual Circuit bandwidth by the number of active Hosts.
Per Host Max Bandwidth	Specify the maximum amount of bandwidth (in kbps or percentage of the Virtual Circuit bandwidth) that each Host can burst to. If 'No Bursting Allowed' is selected, then each Host will get no more bandwidth than what they have been allocated above.
Host Location	Specify the location of the hosts to allocate bandwidth to. Internal Hosts are those that are on the Internal (or LAN) side of the Exinda appliance. External Hosts are those that are on the External (or WAN) side of the Exinda appliance.

Max Hosts	Specify the maximum number of Hosts that can fall into this Dynamic Virtual Circuit. If 'Auto' is selected, the maximum number of Hosts is calculated by assuming each host gets it's allocated bandwidth. So if you specify 1,000kbps as the VC bandwidth, and specify 100kbps per Host, then the maximum number of Hosts is automatically calculated as 10. If the 'Automatically Share' option is selected, the maximum number of Hosts is calculated by assuming each Host is entitled to minimum bandwidth, which is 10kbps. Any Host that comes along after the maximum number of Hosts is exceeded will not fall into this Virtual Circuit and should be captured in another Virtual Circuit.

Note: The maximum number of Hosts multiplied by the Per Host Bandwidth cannot exceed the Virtual Circuit bandwidth.

Example: See the following examples for various Dynamic Virtual Circuit configurations.

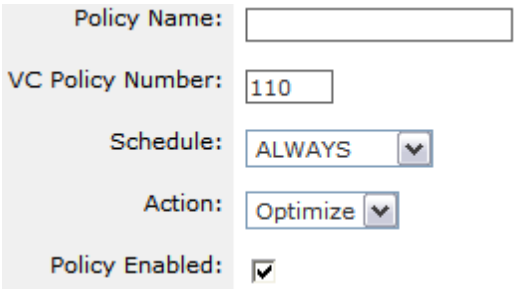
Name: Example 1 **Bandwidth**: 1024kbps **Direction**: Both **Network Object**: Internal Users **Dynamic Virtual Circuits Enabled**: Yes **Per Host Bandwidth**: Auto **Per User Max Bandwidth**: 100% **Host Location**: Internal **Max Hosts**: Auto	"Internal Users" is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get the full 1024kbps. If there are 2 users, they each get 512kbps and can burst up to the full 1024kbps (if the other user is not using their guaranteed 512kbps). If there are 10 users, they each get 102kbps and can burst up to the full 1024kbps (if the other users are not using their guaranteed 102kbps).
Name: Example 2 **Bandwidth**: 1024kbps **Direction**: Both **Network Object**: Internal Users **Dynamic Virtual Circuits Enabled**: Yes **Per Host Bandwidth**: 10% **Per User Max Bandwidth**: No **Host Location**: Internal **Max Hosts**: Auto	"Internal Users" is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get 102kbps and cannot burst. If there are 10 users, they each get 102kbps and cannot burst.

	If there are 100 users, the first 10 users each get 102kbps and cannot burst. The remaining 90 users will not match this VC.
Name: Example 3 **Bandwidth**: 1024kbps **Direction**: Both **Network Object**: Internal Users **Dynamic Virtual Circuits Enabled**: Yes **Per Host Bandwidth**: 64kbps **Per User Max Bandwidth**: 50% **Host Location**: Internal **Max Hosts**: 16	"Internal Users" is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get 64kbps and can burst up to 512kbps. If there are 16 users, they each get 64kbps and can burst up to 512kbps (if the other users are not using their guaranteed 64kbps). If there are 30 users, the first 16 users each get 64kbps and can burst up to 512kbps (if the other users are not using their guaranteed 64kbps). The remaining 14 users will not match this VC.
Name: Example 4 **Bandwidth**: 1024kbps **Direction**: Both **Network Object**: Internal Users **Application**: Citrix **Dynamic Virtual Circuits Enabled**: Yes **Per Host Bandwidth**: 64kbps **Per User Max Bandwidth**: No **Host Location**: Internal **Max Hosts**: 16	"Internal Users" is a Network Object that defines all hosts on the LAN side of the Exinda appliance. "Citrix" is an Application that defines Citrix traffic. This VC will match all Internal User's Citrix traffic. If there is 1 user, they get 64kbps for their Citrix traffic and cannot burst. If there are 16 users, they each get 64kbps for their Citrix traffic and cannot burst. If there are 30 users, the first 16 users each get 64kbps for their Citrix traffic and cannot burst. The remaining 14 users will not match this VC.

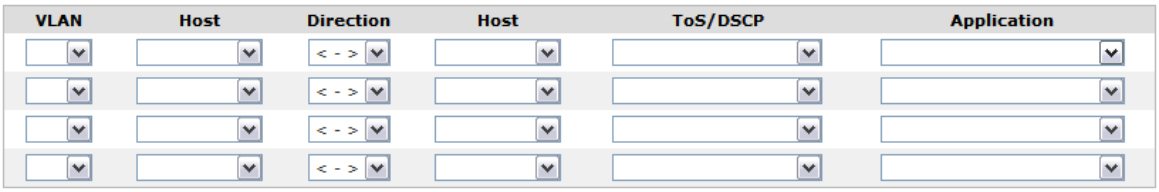
Note: For further information on Per Host QoS, consult the Per Host QoS How to Guide.

7.1.3 Policies

Policies are used to filter specific traffic and apply one or more actions to that traffic. The following properties can be configured on all policies:



Filter rule are used to define which traffic matches a policy. Use the form below to add or modify filter properties:



VLAN	A pre-defined VLAN Object, which can select traffic based on 802.1Q VLAN ID and/or 802.1P VLAN priority tag.
Host / Direction / Host	A predefined Network Object (static or dynamic), which can select traffic to/from specific subnets or addresses.
ToS / DSCP [2]	Select traffic based on DSCP/ToS marks in the IP header.
Application	Select traffic based on a predefined Application Object or Application Group.

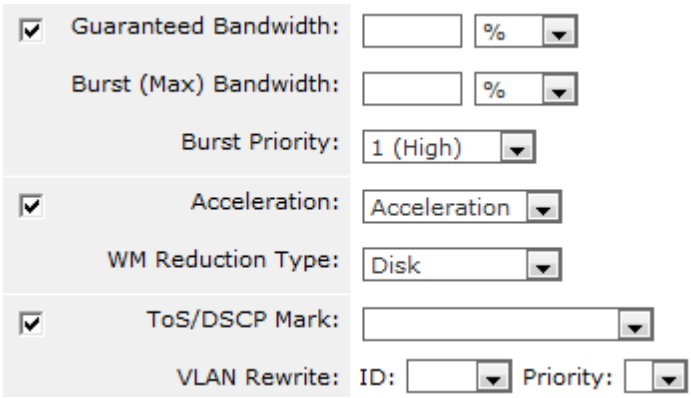
One or all of these properties can be set to capture traffic for the policy. If each item is set to “All”, the policy will capture all traffic. This is called a “Catch All Policy”.

Note: Selecting an entry in only one drop down, will default all the other items to “All”, for example, if you want to configure a Filter Rule for all HTTP traffic, you can select HTTP from the 'Application' drop down and save the policy without selecting anything else from the other drop downs.

Note: By default, 4 Filter Rules can be created per policy. If more are required, fill out the first 4, save the Policy, then edit the Policy and 4 more lines will become available.

Note: To delete individual Filter Rules, set all the fields for that Filter Rule to blank or use the Optimizer | Policies page on the Web UI, advanced mode.

If the “Optimize” action is selected, the following options will appear:



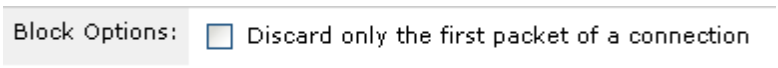
QoS	**Allocate bandwidth to the policy so that QoS can be applied to any matching traffic. All bandwidth allocations are relative to the parent VC bandwidth. The following options are available as a percentage of the parent VC bandwidth or as an explicit value in kbps.**
Guaranteed Bandwidth [1]	The minimum bandwidth made available for the policy. **This is not reserved bandwidth** – if no traffic is matched to this policy, the guaranteed bandwidth is available for use by other policies.
Burst (Max) Bandwidth [1]	The maximum bandwidth made available for the policy. Once all guaranteed bandwidth is allocated, the remaining (excess) bandwidth is made available for burst usage. This value is the maximum burst bandwidth that will be allocated to a policy.
Burst Priority	The burst priority is used to decide how excess bandwidth is distributed. Policies with a higher burst priority will be preferred when allocating excess bandwidth for burst usage.
Acceleration	**All traffic matching the policy will attempt to be accelerated. The following options define what kind of acceleration is applied to the matching traffic.**
Acceleration	Specify the type of acceleration to apply to the matching traffic. Available options are 'Acceleration' and 'Edge Cache'. 'Acceleration' is TCP-based Application Acceleration and is only available on x800 licensed appliances. Only outbound TCP traffic is accelerated. Edge Cache is Asymmetric Object Memory - a WAN reduction technology applied to outbound HTTP traffic. Edge Cache can be used with a single appliance.

WM Reduction Type	Specify the type of WM reduction technology to apply to the matching traffic. If the 'Acceleration' option is selected above, the available options here are 'Disk', 'Compression' and 'None'. 'Disk' reduction uses the HDD in the Exinda appliance to store de-duplication patterns. It also uses 'Compression' reduction. 'Compression' reduction uses a network optimized LZ compression algorithm rather than de-duplication. 'None' means that the traffic will not attempted to be reduced but will still be accelerated.
Packet Marking	**Mark individual packets matching this policy. The following packet marking options are available.**
DSCP / ToS Mark [2]	Set a DSCP/ToS mark in the IP header of all packets matching the policy.
VLAN Rewrite	Rewrite the 802.1Q VLAN ID and/or Priority only if an existing VLAN header is present. This is a packet based VLAN rewrite feature. Only packets matching this policy will be rewritten. Other packets that do not match this policy may be required to be rewritten in order for this feature to work (including non-IP packets such as ARP, which are not even processed by the Optimizer). Ensure that your topology supports this method of rewriting VLAN IDs before using this feature.

If the “Ignore” action is selected, traffic that matches the policy is still monitored, but will be ignored by the optimizer and pass through the appliance with no restriction on bandwidth. Typically this option is used for local traffic.

Note: The "Ignore" option should not be used for policies within Dynamic Virtual Circuits.

If the "Discard" action is selected, traffic that matches the policy is dropped by the appliance. The following option is available:



Discard only the first packet	This option can be used in conjunction with a uni-directional Virtual Circuit to discard connections originating from a specific side (WAN or LAN) of the appliance. For example, when used with an inbound Virtual Circuit, the first (SYN) packet will be discarded - effectively blocking connection establishment from the WAN but allowing traffic from established connections.

[1] The guaranteed bandwidth of a single Policy must not exceed the parent Virtual Circuit bandwidth and the sum of all guaranteed bandwidths in each policy within a Virtual Circuit must not exceed the virtual Circuit bandwidth. In addition, the burst bandwidth must be greater than the guaranteed bandwidth, and less than or equal to the parent Virtual Circuit bandwidth.

[2] For more information, refer to the DSCP / ToS How to Guide.

Note: Any changes made to a Policy definition are global and will affect all Virtual Circuits that use that Policy.

7.2 Optimizer Policies

Polices can be created and edited independently of the Optimizer Policy Tree. The Optimizer | Policies page on the Web UI, advanced mode, lists all the system default and custom Policies. By default, there are no policies available. After running the Optimizer Wizard, a set of default policies will be installed.

The form at the top of the page allows you to create custom Policies.

Note: See the Optimizer Policy Tree | Policies page for more information regarding creating custom Policies.

You can also use this page to delete individual Filter Rules from within Policies.

Note: Any changes made to Policies will affect all instances of that policy if it is in use by more than one Virtual Circuit.

The following tables shows the policies that will be available to some of the default Application Groups after running the Optimizer wizard.

Num	Name	Min BW%	Max BW%	Priority	Accelerate
1	Ignore	-	-	-	-
2	Accelerate	-	-	-	X
3	Choke 1%-3%	1	3	10	-
4	Limit Low 2%-10%	2	10	10	-
5	Limit Med 3%-50%	3	50	9	-
6	Limit High 4%-70%	4	70	8	-
7	Guarantee Low 5%-100%	5	100	7	-
8	Guarantee Med 8%-100%	8	100	5	-
9	Guarantee High 10%-100%	10	100	3	-

Num	Name	Min BW%	Max BW%	Priority	Accelerate
10	Guarantee Critical 15%-100%	15	100	1	-
11	Guarantee Low 5%-100% - Accelerate	5	100	6	X
12	Guarantee Med 8%-100% - Accelerate	8	100	4	X
13	Guarantee High 10%-100% - Accelerate	10	100	2	X

The following matrix shows the combination of default Application Groups and policies (above) that will be made available as default policies.

Application Group	Policy Number												
	1	2	3	4	5	6	7	8	9	10	11	12	13
ALL		X					X	X					
Database						X	X	X				X	X
Files							X	X	X			X	X
Interactive	X							X	X	X			
Mail						X	X	X			X	X	
P2P			X	X	X								
Recreational			X	X	X	X	X						
Secure	X												
Software Updates				X	X	X	X				X		
Streaming				X	X	X	X	X					
Thin Client	X							X	X	X			
Voice	X								X	X			
Web							X	X	X		X	X	X

7.3 Optimizer Wizard

The Optimizer Wizard is a convenient way to populate the Optimizer with some default Policies.

Caution: Running the Optimizer Wizard will delete any existing Optimizer Policies and Optimizer Configuration.

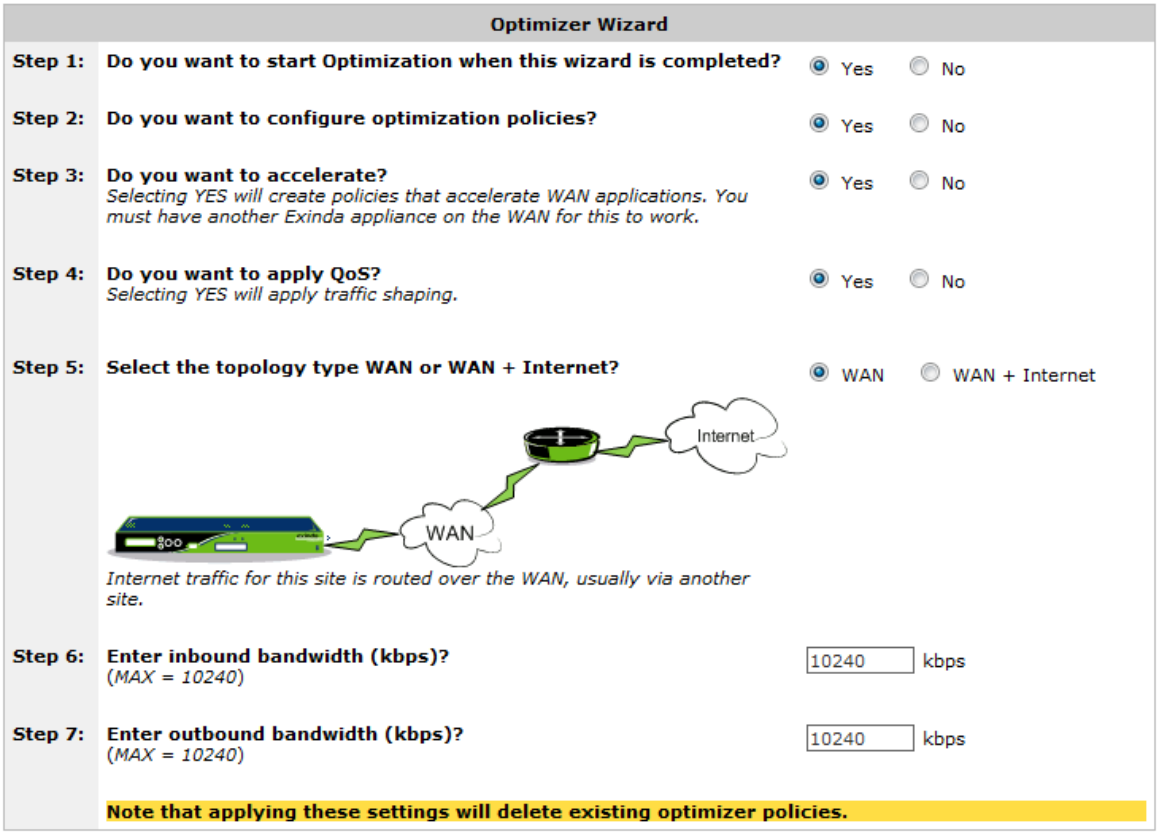
The fist 4 questions are always the same:

Do you want to start Optimization when this wizard is completed?	Selecting YES will start the Optimizer service automatically when you compete all the steps in the wizard.
Do you want to configure optimization policies?	Selecting YES will cause Questions 2 and 3 to appear.
Do you want to accelerate?	Selecting YES will create policies that accelerate WAN applications. You must have another Exinda appliance on the WAN for this to work.
Do you want to apply QoS?	Selecting YES will apply traffic shaping.

Depending on your answers to Questions 2 and 3, the following scenarios are possible.

Scenario 1:

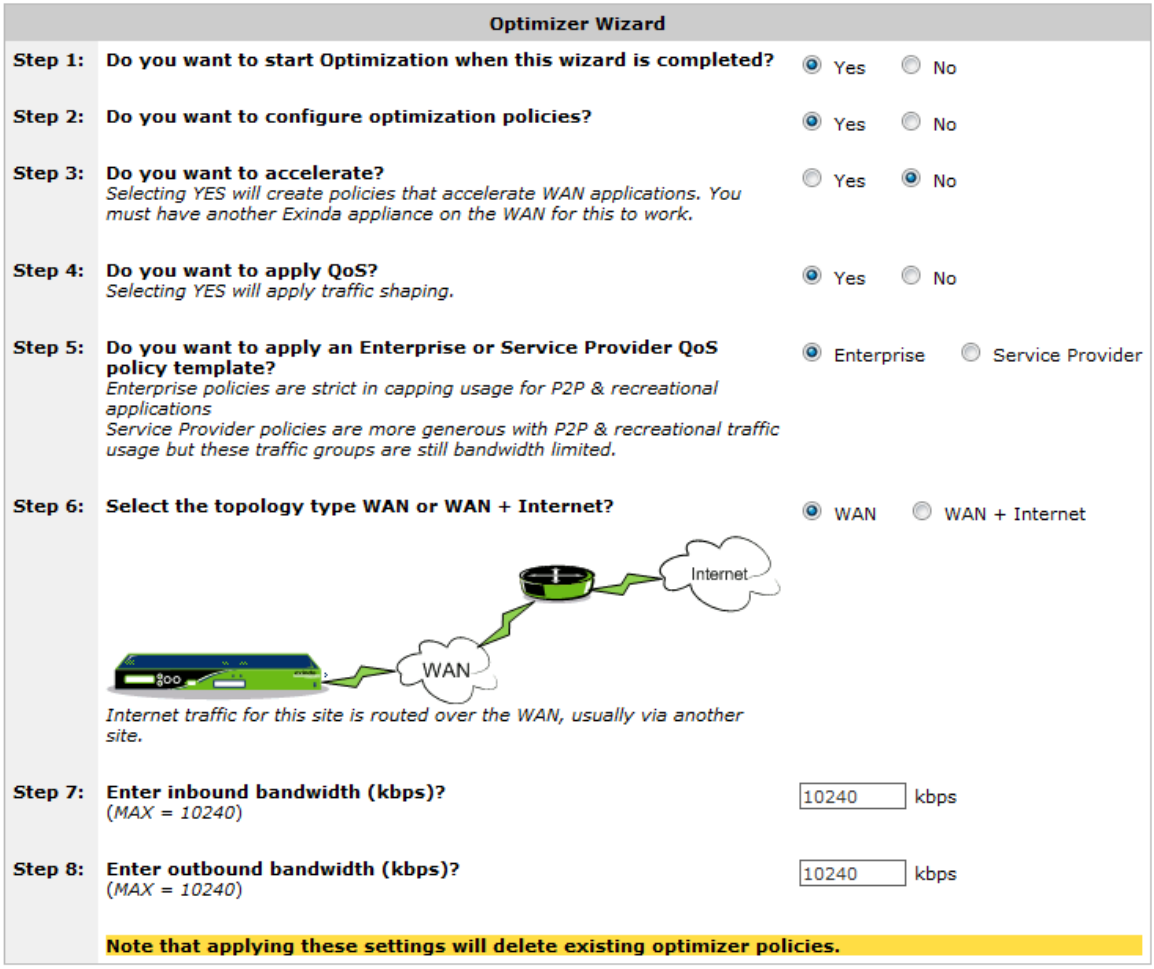
*Do you want to accelerate?***YES**
*Do you want to apply QoS?***YES**



This will enable both QoS (traffic shaping) and Application Acceleration. You will need to select the WAN topology that bests represents your deployment and also enter the inbound and outbound bandwidths for this Exinda appliance.

Scenario 2:

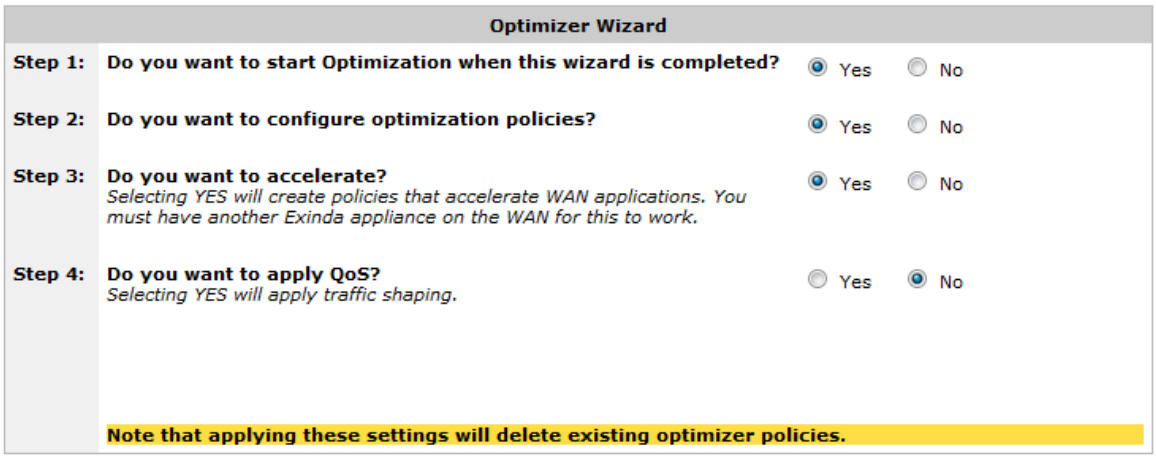
*Do you want to accelerate?***NO**
*Do you want to apply QoS?***YES**



This will enable QoS (traffic shaping) only. You have the choice of the type of default Policy template to apply. There is a template better suited to Enterprise or one better suited to Service Providers. You will also need to select the WAN topology that bests represents your deployment and also enter the inbound and outbound bandwidths for this Exinda appliance.

Scenario 3:

*Do you want to accelerate?***YES**
*Do you want to apply QoS?***NO**



This will enable Application Acceleration only.

Part VIII

8 Appendices

Appendix A - TCP Acceleration

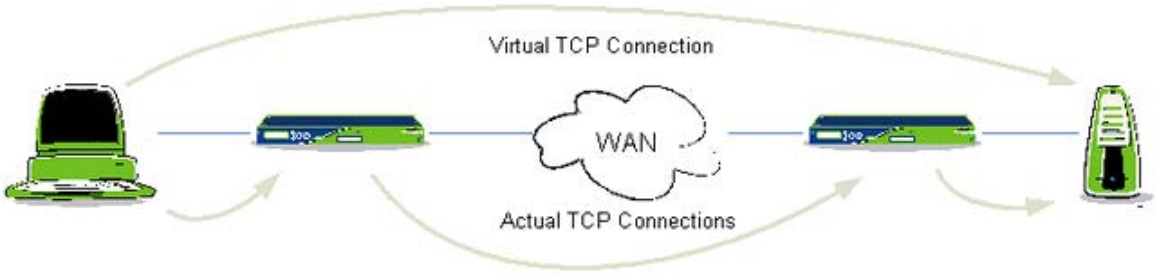
Appendix B - CIFS Acceleration

Appendix C - Auto Discovery

Appendix D - Licenses

8.1 Appendix A - TCP Acceleration

In order to accelerate traffic over the WAN, Exinda transparently proxies TCP connections at each end. Both the client and server think they have established a connection with each other; however, they have connected with their local Exinda devices.



By transparently proxying TCP connections like this, Exinda has full control of the TCP connection over the WAN. It is this WAN connection that TCP Acceleration technologies are applied.

In addition to facilitating other acceleration technologies like WAN Memory and CIFS acceleration, TCP acceleration also provides performance improvements over and above regular TCP, whilst been fully compliant with TCP.

- *Window Scaling* increases the TCP window size which allows more data to be in-flight before TCP requires acknowledgements. This means higher throughput can be achieved on large WAN links with latency.
- *Selectable Congestion Control Algorithms* can be chosen to match the WAN environment. For long-fat links, something like High Speed TCP should be used. For Satellite links, or other high-latency links, something like Hybla should be used. This allows for better TCP performance over different WAN technologies.
- *Delayed and Selective Acknowledgements* are used to acknowledge the receipt of packets in batches, instead of acknowledging every single packet. This reduces the amount of return data on the wire.

- *Explicit Congestion Notification* (ECN) allows end-to-end (between the Exinda appliances) notification of network congestion without dropping packets. Traditionally, TCP/IP networks signal congestion by dropping packets. When ECN is enabled, an ECN-aware router may set a mark in the IP header instead of dropping a packet in order to signal impending congestion.

- *Adaptive Initial Congestion Window* allows automatic adjustment of the Initial Window size depending on the connectivity properties of the end-to-end link (between the Exinda appliances).

- Slow Start with Congestion Avoidance is used when TCP uses a combination of the slow start and congestion avoidance algorithms to reset the send window size temporarily, to avoid congestion.

Modes of Operation

Exinda's default mode of acceleration is called 'Transparent Mode'. In this mode the source and destination addresses and ports of the client and server are maintained to provide the least intrusive network implementation.

A secondary supported mode of acceleration is called 'Protocol Mode'. In Protocol Mode the Exinda solution does not use traditional TCP connections to send traffic and dynamically sends the TCP connections over a different protocol. Once a connection is setup via the protocol, subsequent connections can use the protocol connection and avoid the 3-way TCP handshake. The benefit of Protocol Mode is that it reduces the number of TCP connections traversing the WAN and also reduces the TCP connection setup time. Protocol Mode is also used to bypass connectivity issues that can be caused by Firewalls and Intrusion Detection systems.

8.2 Appendix B - CIFS Acceleration

Overview

Common Internet File System (CIFS) is a remote file access protocol that forms the basis for Windows file sharing. It is a de facto standard and comes pre-bundled with all Microsoft-based client (e.g. XP) and server (e.g. Server 2003) platforms. Various CIFS implementations (e.g. Samba) are also available for other operating systems such as Linux.

CIFS defines both a client and server: the CIFS client is used to access files on a CIFS server. For example, each time you browse or access files on a Windows server using Windows Explorer, the CIFS protocol is used to transport information (files or directory information) back and forth between your computer and the server you are accessing.

Anyone who has ever copied a file from a mapped drive and seen the dialog box in Figure 1 has used the CIFS protocol, perhaps without actually knowing it.

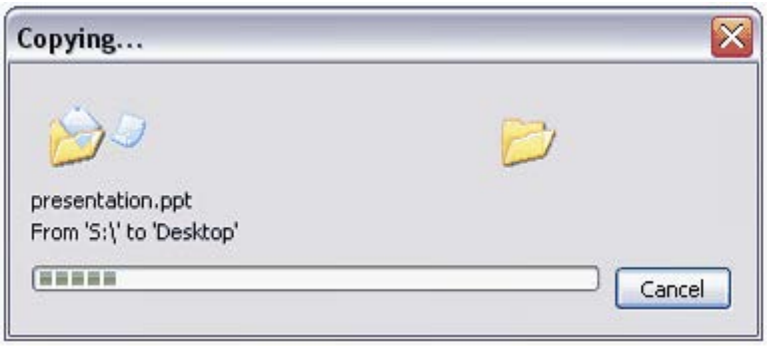


Figure 1: Windows File Sharing (CIFS transfer).

In addition to file sharing, CIFS is also used as a transport protocol for various higher level Microsoft communications protocols, as well as for network printing, resource location services, remote management/administration, network authentication (secure establishment services) and RPC (Remote Procedure Calls).

CIFS was designed back in the 1980s (formally known as SMB) when the networking paradigm was quite different from today. At that time, no consideration was made for how CIFS would operate over a high latency WAN link. As many network managers have discovered, CIFS operates very poorly over such a link. The fundamental reason is because by design CIFS is a very "chatty" protocol, meaning a large number of back and forth transactions are required to complete a request. For example, the largest chunk of data that CIFS can transfer in a single round trip between client and server is 61,440 bytes (61KB). As illustrated in Figure 2, each CIFS request requires a response before the next request is sent to the CIFS server. Therefore CIFS is a latency-bound protocol meaning that as latency increases the performance of CIFS decreases.

To put this in perspective, in order to transfer a single 30MB file, the CIFS protocol would have to make hundreds of round trips between client and server. On a typical LAN this would take a few seconds but on a 2 Mbps WAN link with 300msec latency it would take around 7.5 minutes! Clearly this level of performance degradation has a severe negative impact on productivity. With Exinda's x800 Acceleration products, this same transaction can be reduced to less than 2.5 minutes, for a greater than 3x improvement on the first (cold) pass and where the file can't be compressed. On subsequent transfers of this same 30MB file, the transfer time reduces to less than 30 seconds as CIFS Acceleration and Exinda's WAN Memory network caching work together. As the bandwidth and latency of a WAN link increases, the benefit of Exinda's CIFS acceleration increases as well.

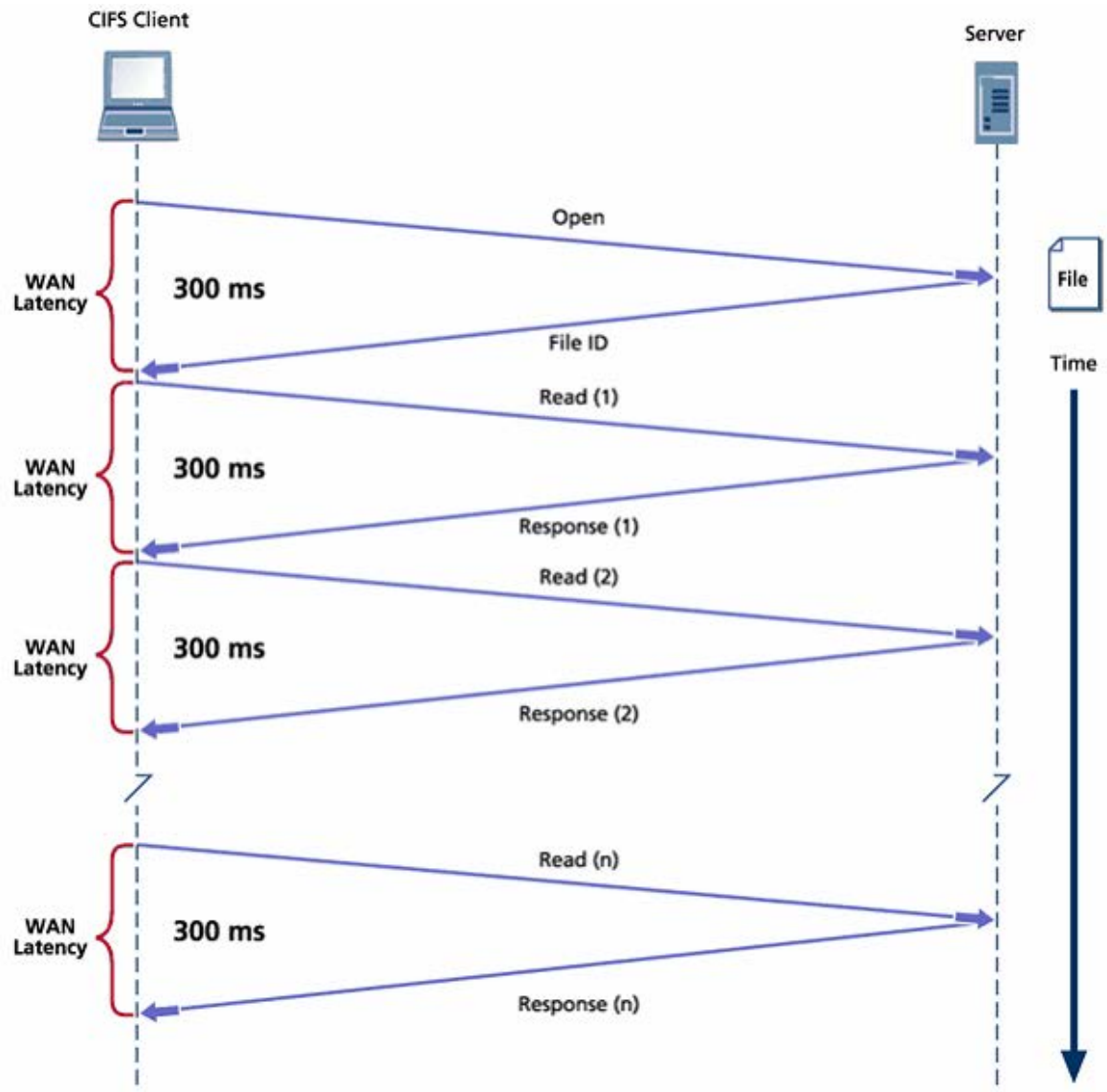


Figure 2: CIFS inefficiency over a high latency WAN link.

How does Exinda improve CIFS performance?

Each Exinda appliance has a deep understanding of the CIFS protocol and can therefore act on behalf of a CIFS client (e.g. Microsoft XP computer) and server (e.g. Windows Server 2003 server) to make the interaction between the two much more efficient. The result is dramatic improvement in activities such as file download (read), file upload (write) and remote access (e.g. open a PowerPoint file on a remote CIFS share).

Exinda maintains a state machine and database of CIFS behaviors that it relies upon to reliably anticipate future CIFS related transactions. When Exinda determines that a certain CIFS transaction is likely to occur, it pre-fetches data (e.g. a file) and temporarily stores it in the remote (client) Exinda's system memory for future reference. Once the pre-fetched data is referenced (transaction successfully predicted) it is deleted from the memory. No file caching is involved; just transient storage of data to facilitate improved CIFS response time.

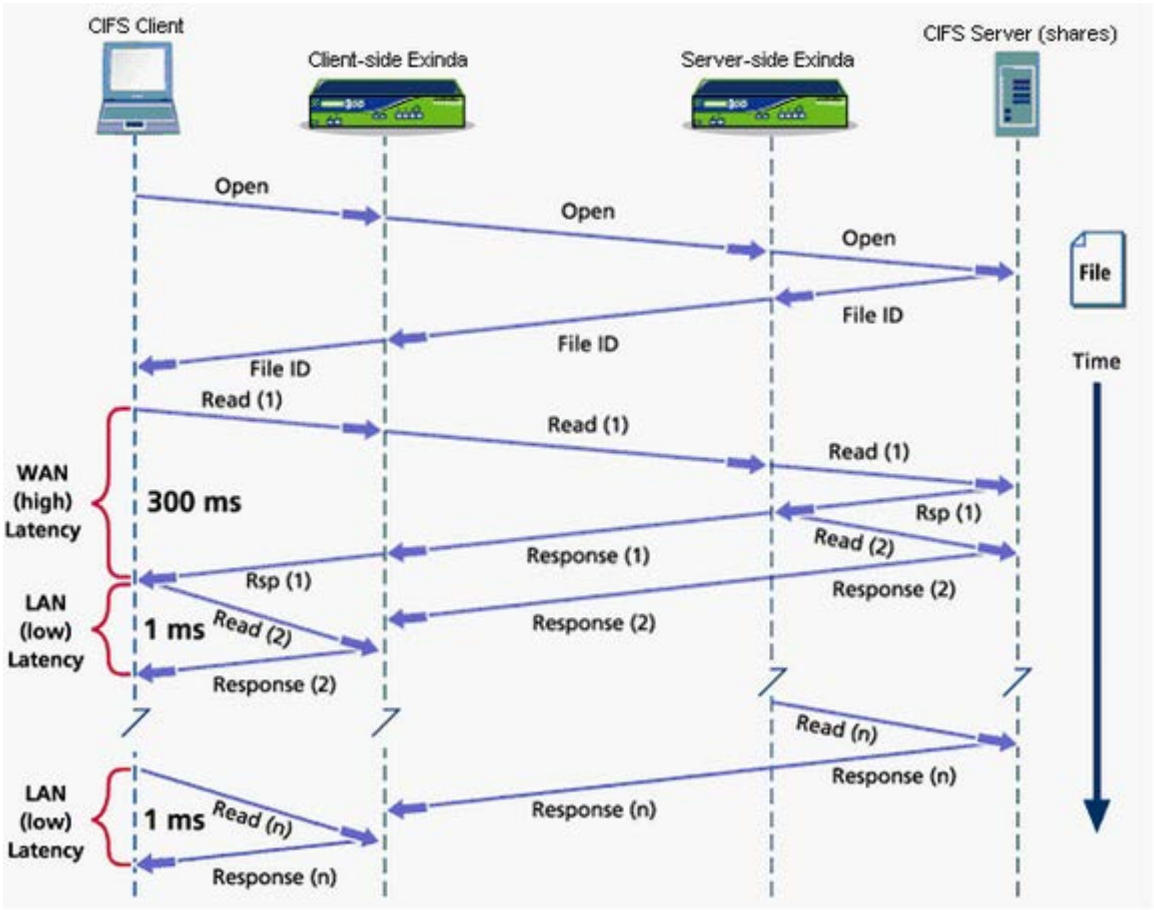


Figure 3: CIFS file download (read) example.

Figure 3 illustrates the primary goal of Exinda CIFS Acceleration: reduce the latency experienced by the CIFS client (e.g. Microsoft XP computer) from WAN latency (i.e. high) to LAN (i.e. low) latency.

The sequence of events that transpire when Exinda accelerates a CIFS file download (read) request is as follows:

1. CIFS client opens a file for reading.

2. CIFS server responds with a file ID.

3. CIFS client issues the first read request and CIFS server responds with data. This first transaction takes a relatively long time because the read request and response are bound by the WAN latency (e.g. 300ms).

4. Once the Exinda systems see the initial transactions, they can determine that the CIFS client is attempting a file download. At this point, the server side Exinda begins pre-fetching data by generating read requests locally to the server at a rate that will keep the WAN link full. If this is a repeat transfer or the file contains repeated data, then the server side will use WAN Memory and therefore transfer only a small amount of data across the WAN link. This will in turn further speed up the CIFS transfer.

5. The pre-fetched data is sent to the client side Exinda and stored temporarily in anticipation of requests from the CIFS client. As the CIFS client requests the file data, instead of getting each 61k bytes from the server (and hence going across a high latency WAN) it now gets the replies locally from the client side Exinda at LAN speeds (e.g. 1 ms or less). This will in turn vastly improve CIFS download performance.

CIFS acceleration works seamlessly with Exinda's TCP Acceleration, WAN Memory and Compression and will benefit from WAN Memory's ability to reduce data traversing the WAN just as other applications such as FTP, HTTP or email do.

There is also no risk of serving stale data using this approach and no file permissions, access lists or user security is ever compromised.

Other Common CIFS Use Cases

A file download was used to illustrate how Exinda performs CIFS acceleration. However, CIFS acceleration uses similar mechanisms to achieve greatly improved performance for many other scenarios. Below are a few examples:

File Upload (Write)

This is conceptually very similar to a file download with the obvious difference being that a CIFS client is writing a file to a CIFS server instead of reading it. In this case, the client side Exinda responds locally to the CIFS client's write requests and passes the data to the server side Exinda at WAN link speed to complete the write operation.

Remote Access of Microsoft Office Files

Microsoft office files (e.g. MS Word, PowerPoint, Excel, etc.) which reside on a remote CIFS server are often opened from a CIFS client. This action suffers from all of the CIFS related problems that are described in this paper because the file data is retrieved serially, 61k bytes at a time. The result is a long wait time to open the file, browse or perform any type of action (e.g. save). Exinda's CIFS Acceleration addresses these problems by pre-fetching the file data and populating it on the client side Exinda. Consequently all CIFS client requests for the file data are served from the client side Exinda at LAN speeds.

Directory Browsing

When browsing a remote file system using Windows Explorer, the CIFS protocol transfers various bits of information about the files you are browsing. This metadata is transferred in special CIFS instructions called transactions. The Exinda appliance also caches these transactions such that they can be served locally, from the client-side Exinda appliance. This significantly improves the performance of directory browsing using the CIFS protocol.

8.3 Appendix C - Auto Discovery

The Exinda auto-discovery process is used for two purposes:

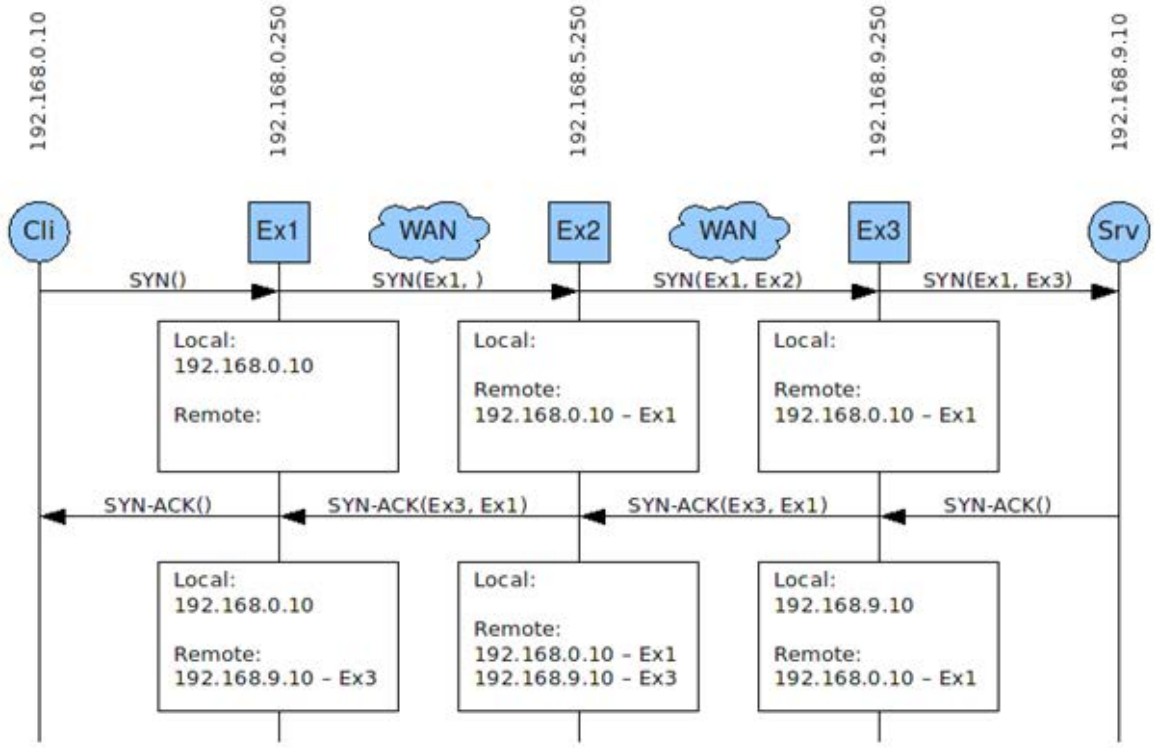
1. The discovery of which connections can be accelerated.
2. The discovery of new Exinda appliances on the network.

To achieve this, some extra information is included in the SYN, SYN-ACK and first ACK packets of each new connection. This information is in the form of a TCP option. The required information is the:

1. Source Appliance ID
2. Destination Appliance ID
3. Acceleration Module Map

Optionally an IP address corresponding to one of the appliances will also be sent.

In addition to this, each appliance must keep a list of host/appliance id pairs.



The connection discovery process is as follows:

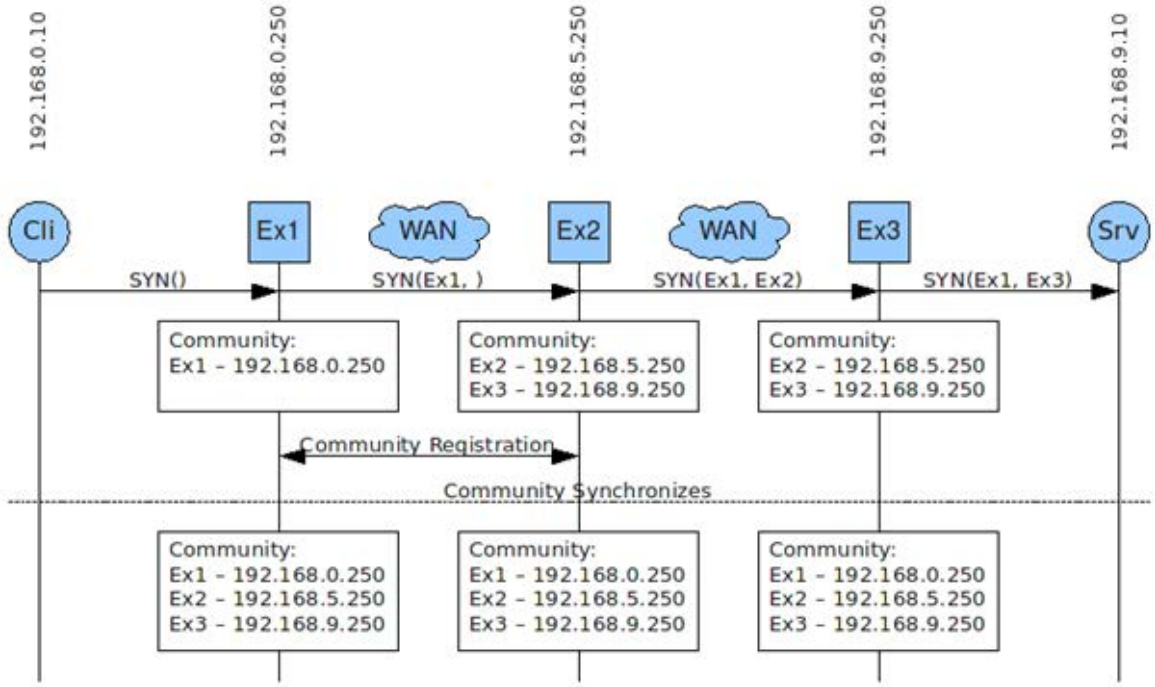
1. When an appliance receives a packet SYN from a client, it adds the client's IP to its local list. It adds the auto-discovery option to the packet, filling out the source details. If the server exists in the appliances remote list, then the destination field is filled out with that appliances details, otherwise the destination is left blank.

2. When an appliance receives a SYN packet containing the auto-discovery option, it will record the client IP address and source appliance id in its remote list. It will then fill out the destination details and forward the packet on.

3. The end appliance can be determined by receiving a SYN-ACK from the server without any auto-discovery option. This appliance will add an auto-discovery option with both the source and destination details filled out.

4. When another appliance receives the SYN-ACK, it will add the server IP address and source appliance id will be added to the remote list. If it finds that the destination does not refer to itself, then it will ignore all packets further packets that are part of that connection.

5. After the SYN-ACK has passed through, both end devices know who they are accelerating between and any appliances have a record of who to accelerate to if they have a connection to either the client or the server.



This process also allows for the discovery of new Exinda appliances on the network. When an appliance receives an auto-discovery option from a source that the Exinda community doesn't know about, it can notify the community which will establish a connection to that appliance, and add it to the community. This may also cause two existing communities to join together.

The Auto Discovery process is very lightweight - it adds negligible latency/delay to packets as they pass through the Exinda appliance.

8.4 Appendix D - Licenses

GNU Public License (GPL)

BSD 2.0

8.4.1 GNU Public License (GPL)

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            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.

TERMS AND CONDITIONS

0. 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), accompanied 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), accompanied 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 software 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 noncommercially, 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 accord 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 satisfy simultaneously 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.

END OF TERMS AND CONDITIONS

8.4.2 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 disclaimer.

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.