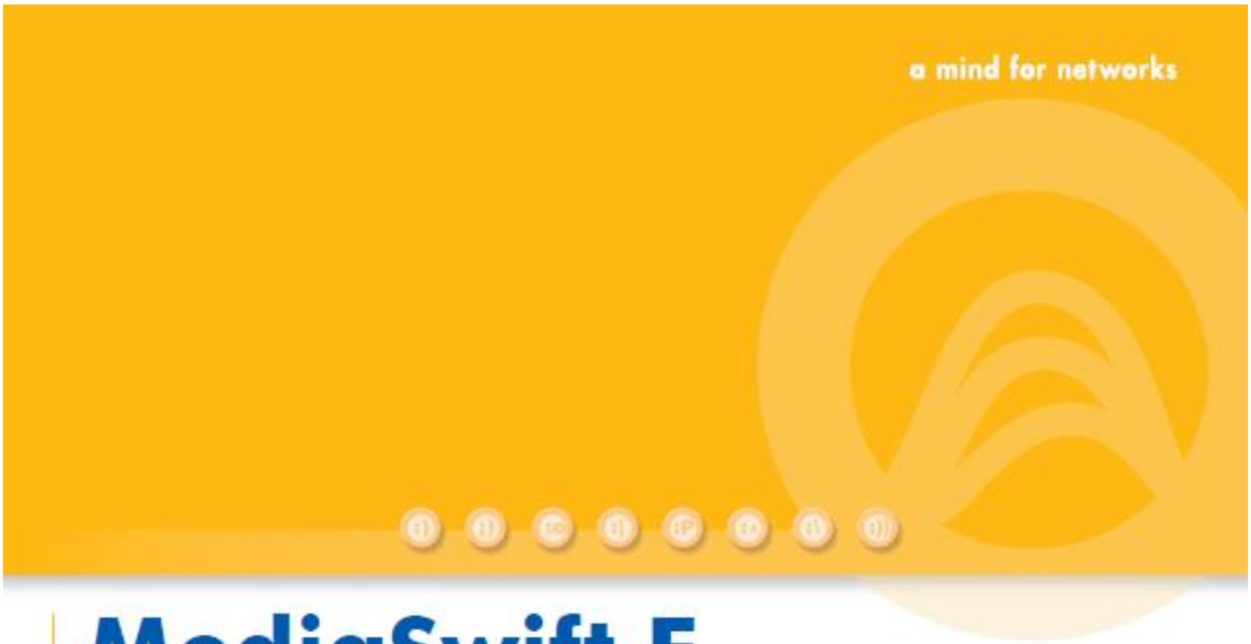


a mind for networks

MediaSwift E

Operation Guide

Allot communications

MediaSwift E

Operation Guide

P/N D351016 R1

Important Notice

Allot Communications Ltd. ("Allot") is not a party to the purchase agreement under which Service Gateway was purchased, and will not be liable for any damages of any kind whatsoever caused to the end users using this manual, regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ALLOT OR ANY OF ITS SUBSIDIARIES. ALLOT ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Please read the End User License Agreement and Warranty Certificate provided with this product before using the product. Please note that using the products indicates that you accept the terms of the End User License Agreement and Warranty Certificate.

WITHOUT DEROGATING IN ANY WAY FROM THE AFORESAID, ALLOT WILL NOT BE LIABLE FOR ANY SPECIAL, EXEMPLARY, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR ANTICIPATED PROFITS, OR LOST BUSINESS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Copyright

Trademarks

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Allot and the Allot Communications logo are registered trademarks of Allot Communications Ltd.

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

Changes or modifications not expressly approved by Allot Communication Ltd. could void the user's authority to operate the equipment.

Version History

Each document has a version and a build number. You can tell the exact version and build of this document by checking the table below. Details of this document version are contained in the top row of the table below.

Document updates are released in electronic form from time to time and the most up to date version of this document will always be found on Allot's online Knowledge Base. To check for more recent versions, login to the support area www.allot.com/support.html and from the knowledgebase tab, enter the title of this document into the search field.

Doc Version	Product	Date	Summary of Changes
v2b	MSWE	21.07.2013	Updating Auto IP learning
v2a	MSWE	29.04.2013	Editorials
v2	MSWE	24.04.2012	First Release
v1b3	MSWE	14.01.2013	Updated screens - added HM config. screen and CMGM

Table of Contents

Important Notice iii
Table of Contents v
List of Figures vii

Chapter 1: Introduction 1-1

Purpose of this Document 1-1

Chapter 2: Getting Started 2-1

Logging on to MSWE 2-1
Navigating in MSWE 2-2
The MSWE Home Page 2-3

Chapter 3: User Management 3-1

Introduction to User Management 3-1
Managing MSWE Users 3-1
Adding New Users 3-1
Activating and Deactivating Users 3-2
Editing User Details 3-3
Changing Passwords 3-3

Chapter 4: Monitoring MediaSwift E 4-1

Domain Performance 4-1
Viewing Domain Traffic Graphs 4-2
Viewing Domain Statistics 4-3
Viewing MediaSwift E Servers in the Grid 4-5
Reviewing the Domain's Active Alarms 4-6
Server Performance 4-7
Detailed Server Statistics 4-9
Managing Services on MediaSwift E Servers 4-9
MediaSwift E Server Memory and Disk Resources 4-10
MediaSwift E Server Disks Management 4-11
MediaSwift E Server Alarms and Events 4-13
Video Statistics 4-16
Advanced Performance Monitoring Using Cacti 4-17

Chapter 5: System Configuration 5-1

System Configuration Overview 5-1
Using the Configuration Page 5-2
Configuring MediaSwift E Servers 5-3
Editing Zones 5-3
Managing Served IP Addresses 5-4
Defining Authorized IP Addresses 5-7
Content Provider IPs (CP IPs) 5-9
Network Management 5-15
Protocols Tab 5-16

Bandwidth Control 5-28
Configuring Event Notifications 5-34
Security Configurations....................5-38
Server Management....................5-40

Chapter 6: Diagnostic Tools....................6-1

HTTP Trace 6-1
CDR (Call Data Record) 6-3

Chapter 7: KPI Reporting Suite....................7-1

Introduction 7-1
Configuring the P2P-KPI 7-1
Changing the QoE Thresholds....................7-3
Changing the Rejected Sessions Thresholds 7-3
Changing the LRU Thresholds....................7-3
Changing the CPU Thresholds 7-4
Changing the MAX Throughput Thresholds....................7-4
Displaying the KPI Alerts 7-4

Chapter 8: Managing Multiple Domains 8-1

Introduction 8-1
GMS Home Page 8-1
Multi-Domain Configuration....................8-3
Global Parameters 8-3
Domain-Specific Parameters....................8-3

Chapter 9: Remote System Logging....................9-1

Available Logs....................9-1
Login Types....................9-1
Logging Examples 9-2
CLI Logging Example....................9-2
WM Logging Example....................9-2

List of Figures

Figure 1: MSWE Welcome Screen 2-1
Figure 2: MSWE Home Page 2-2
Figure 3: MSWE Navigation Links 2-2
Figure 4: MSWE Home Page Displaying all Servers 2-3
Figure 5: MSWE Users Management Window 3-1
Figure 6: Creating a New User 3-1
Figure 7: Update My Details Page 3-3
Figure 8: MSWE Home Page Displaying All Servers 4-1
Figure 9: MSWE Home Page with Zone Performance Data 4-2
Figure 10: MSWE Home Page with Performance Data for All Zones 4-2
Figure 11: Example of a Domain Traffic Graph 4-3
Figure 12: Example of the Throughput Tab in the Domain Statistics Area 4-4
Figure 13: Files Distribution Tab in the Domain Statistics Area 4-5
Figure 14: Example of the Domain Servers Area 4-5
Figure 15: Example of the System Notifications Area 4-6
Figure 16: Confirm Hiding of Acknowledged Alarm 4-7
Figure 17: Confirm Alarm Reactivation 4-7
Figure 18: Server Management Page for a Specific Server Unit 4-8
Figure 19: Server Management Page with Zone-specific Performance Data 4-9
Figure 20: Example of Server Services Area 4-9
Figure 21: Example of the Server Resources Area 4-11
Figure 22: Disk Status icon with Tooltip 4-11
Figure 23: Disks Management Window 4-12
Figure 24: Active Alarms Area 4-13
Figure 25: Confirm Hiding of Acknowledged Alarm 4-13
Figure 26: Confirm Alarm Reactivation 4-14
Figure 27: Events Log with Filters 4-14
Figure 28: CLI Log 4-15
Figure 29: Example of Video Statistics Page 4-16
Figure 30: Cacti Screen with Navigation Tree and Summary Graphs 4-17
Figure 31: MSWE Configuration Page Tabs 5-1
Figure 32: Yellow Highlighting Signifies Modified Configuration 5-2
Figure 33: Red Highlighting Signifies Invalid Configuration 5-2
Figure 34: Zones Main Window 5-3
Figure 35: Editing a Zone 5-3
Figure 36: Served Static IPs Window (without Zones) 5-5
Figure 37: Served Static IPs Window (without Zones) 5-5
Figure 38: Consolidated IPs Window 5-6
Figure 39: Filtered IPs Window 5-7
Figure 40: Authorized Managers IPs Window 5-8
Figure 41: CP IPs General Tab 5-9
Figure 43: CP Previous Configuration Reload 5-13
Figure 45: Content Providers Rules Management Settings Tab 5-14
Figure 46: Network Management Screen 5-15
Figure 47: Protocol Management BitTorrent Window 5-17

Figure 48: Protocol Management eDonkey 2000 Window 5-18
Figure 49: Protocol Management Internet Video/HTTP 5-19
Figure 50: Protocol Management Video/HTTP – Replace list... 5-20
Figure 51: Protocol Management Video/HTTP – YouTube Replace list........................... 5-21
Figure 52: Protocol Management Video/HTTP – Exclude list 5-23
Figure 53: Protocol Management Video/HTTP – YouTube Exclude list 5-24
Figure 54: Using Tracing Tool to Identify File IDs 5-25
Figure 55: HTTP/Video Sites Configuration 5-26
Figure 56: Peer-to-Peer Bandwidth Window 5-28
Figure 57: Bandwidth Limit Tooltip 5-29
Figure 58: Video/HTTP Bandwidth Window 5-30
Figure 59: Zones Session QoE Dialog Box.. 5-32
Figure 60: Session Rate Tooltip 5-33
Figure 61: Zones Session Rate Dialog Box.. 5-33
Figure 62: Events Notifications Window... 5-34
Figure 63: Severity: Major 5-36
Figure 64: Severity: Warning 5-36
Figure 65: Severity: Information.. 5-37
Figure 66: Security Window 5-38
Figure 67: Servers Management Main Window... 5-40
Figure 68: Changing Network Settings 5-41
Figure 69: Assigning OCM (HM/PM) Network Interfaces.. 5-42
Figure 70: Managing BitTorrent Trackers 5-43
Figure 71: BGP Sites Provisioning Check Box and Add icon 5-44
Figure 72: Add IP prefix to BGP Advertised List... 5-44
Figure 74: Upload New Version DIalog Box.. 5-45
Figure 75: Choose File Dialog Box... 5-45
Figure 76: Update New Version Dialog Box 5-45
Figure 77: Upgrading MSWE Server Software.. 5-47
Figure 79: Video/HTTP Subnet Monitor Window... 6-1
Figure 80: HTTP Trace Log with Activity Details.. 6-2
Figure 81: CDR Save Progress Details 6-3
Figure 82: Configure the KPI reporting indicators... 7-1
Figure 83: Configure the KPI reporting indicators... 7-2
Figure 84: Change the QoE thresholds.. 7-3
Figure 85: change the rejected sessions thresholds 7-3
Figure 86: The MSWE/G Home Page... 8-2
Figure 87: Global Multi-Domain Parameters.. 8-3
Figure 88: Domain Parameters.. 8-4
Figure 89: Example of CLI History Logs.. 9-2
Figure 90: Example of Events Log.. 9-2
Figure 91: Example of SSH Logs.. 9-3

Chapter 1: Introduction

Purpose of this Document

MediaSwift E (MSWE) is Allot's integrated caching and delivery system for Internet Service Providers (ISPs). MediaSwift E is designed to optimize network performance, while supporting bandwidth-intensive traffic, generated by peer-to-peer applications and Internet video.

The following cache servers are managed by MSWE:

- PCS – P2P Cache Server
- HCS – HTTP Cache Server

In addition, MSWE manages the following control servers:

- PDI – Monitor Controller (ex P2P Demand Identifier)
- HDI - HTTP Demand Identifiers
- PM – P2P Controller (ex Peer Manager)
- HM – HTTP Controller (ex HTTP Manager)

The MSWE is a complete element management facility that enables you to provision the MediaSwift E servers, and monitor their performance. Its user-friendly GUI enables you to perform all system management operations, including:

- Real-time monitoring of faults and alarms
- System configuration
- Compilation and reporting of statistics
- Event reporting
- User access and security management
- Diagnostic analysis of system malfunctions

Logging on to MSWE

Allot supplies you with a URL, user name, and password for logging on to MSWE.

➢ To log on to MSWE:

1. Browse to the MSWE login page according to the URL provided by Allot . The standard format is <http://server IP address>:8080/. The MediaSwift E MSWE login page is displayed, as shown in Figure 1.

Optionally is it possible to use HTTPS instead of HTTP.

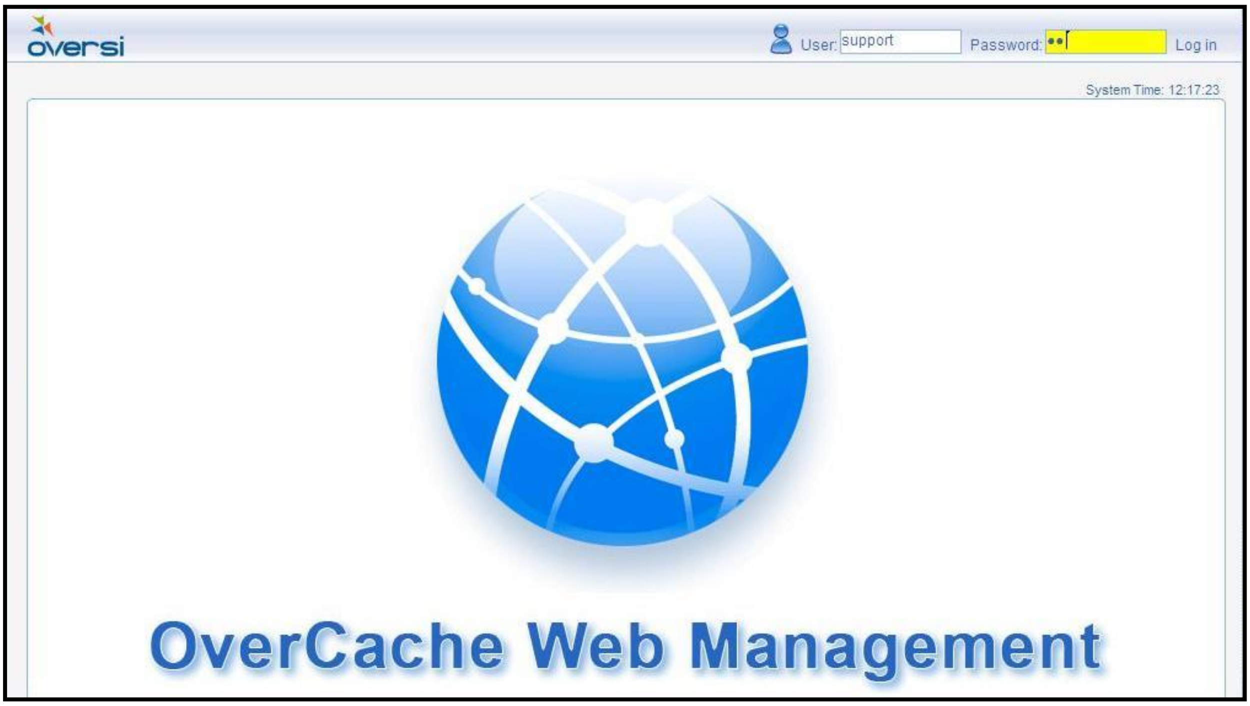
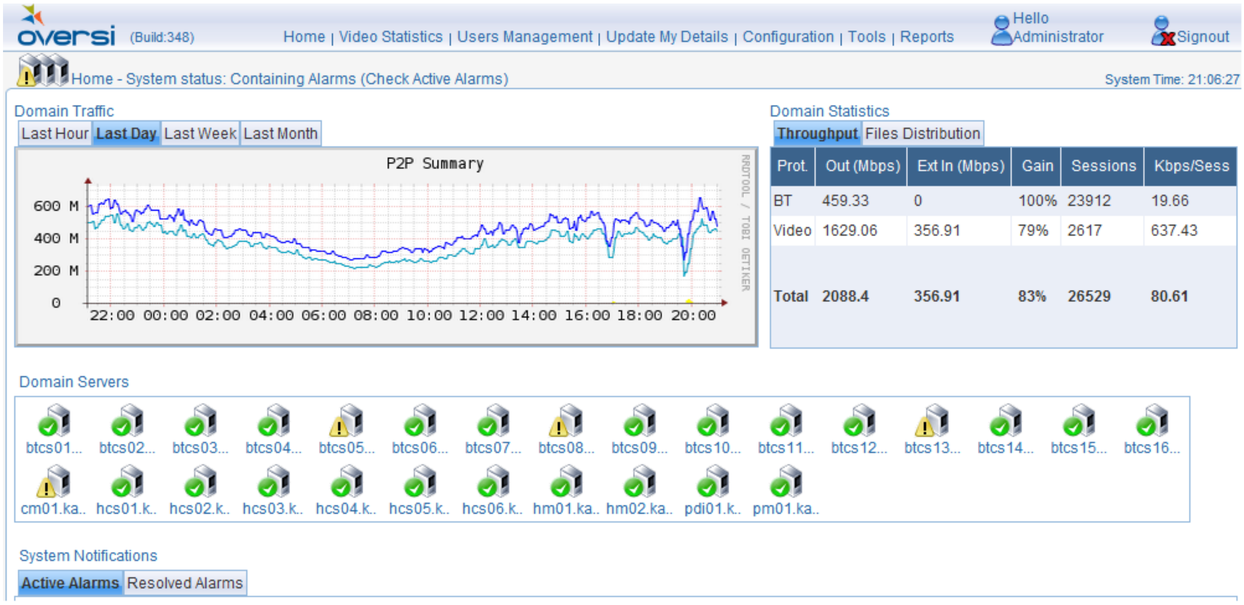


Figure 1: MSWE Welcome Screen

2. Enter your user name and password, as supplied by Allot. The MSWE Home page is displayed.



oversi (Build:348)
Home | Video Statistics | Users Management | Update My Details | Configuration | Tools | Reports
Hello Administrator
Signout
Home - System status: Containing Alarms (Check Active Alarms)
System Time: 21:06:27
Domain Traffic
Last Hour | Last Day | Last Week | Last Month
P2P Summary
600 M
400 M
200 M
0
22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00
RRDTOOL / TOBI OETIKER
Domain Statistics
Throughput | Files Distribution

Prot.	Out (Mbps)	Ext In (Mbps)	Gain	Sessions	Kbps/Sess
BT	459.33	0	100%	23912	19.66
Video	1629.06	356.91	79%	2617	637.43
Total	**2088.4**	**356.91**	**83%**	**26529**	**80.61**

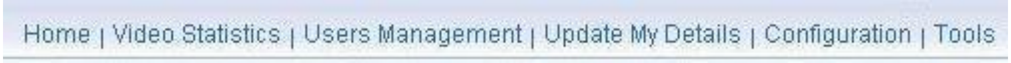
Domain Servers
btcs01... btcs02... btcs03... btcs04... btcs05... btcs06... btcs07... btcs08... btcs09... btcs10... btcs11... btcs12... btcs13... btcs14... btcs15... btcs16...
cm01.ka.. hcs01.k.. hcs02.k.. hcs03.k.. hcs04.k.. hcs05.k.. hcs06.k.. hm01.ka.. hm02.ka.. pdi01.k.. pm01.ka..
System Notifications
Active Alarms | Resolved Alarms

Figure 2: MSWE Home Page

NOTE **A user can only log on to one MSWE session at a time, you cannot operate multiple sessions simultaneously.**

Navigating in MSWE

You can navigate within MSWE by clicking the appropriate link located at the top of the MSWE screen.



Home | Video Statistics | Users Management | Update My Details | Configuration | Tools

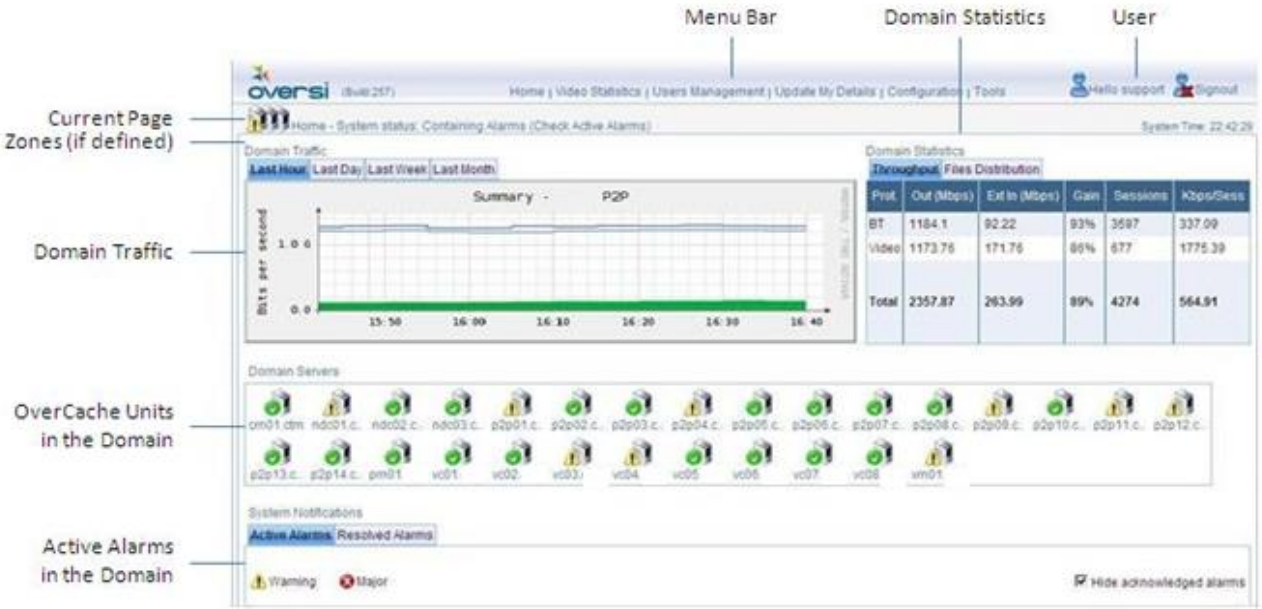
Figure 3: MSWE Navigation Links

The links navigate to the following pages within MSWE:

- **Home**: The Home page displays summary information for the entire array (or "grid") of MediaSwift E servers, as well as for individual servers. See Section 4.1 for an in-depth description.
- **Video Statistics**: The Video Statistics page contains information on bandwidth usage, and on the most popular videos requested by subscribers. Please refer to Section 4.2.
- **Managing MSWE Users**: The Users Management page enables you to perform administrative operations on the system. This page is described in Section 3.2.
- **Update My Details**: Enables the current user to change his password. Please refer to section 3.3.
- **Configuration**: This page, available to users authorized by the system administrator, is used to configure the MediaSwift E system. Configuration instructions are found in Chapter 5.
- **Tools**: The Tools page gives users access to diagnostic utilities intended to help service providers improve MediaSwift E system performance. The tools are described in Chapter 6.

The MSWE Home Page

The MSWE Home page displays an overview of all the MediaSwift E servers in a domain. An example of the Home page displaying all of the servers in a domain is shown in Figure 4.



Prot	Out (Mbps)	Ext In (Mbps)	Gain	Sessions	Kbps/Sess
BT	1184.1	92.22	93%	3597	337.09
Video	1173.76	171.76	86%	677	1775.39
Total	2357.87	263.99	89%	4274	564.91

Figure 4: MSWE Home Page Displaying all Servers

The Home page is divided into the following areas:

- **Status and Navigation:** Displays information on the page you are currently viewing, the current user, and a menu containing navigational links within MSWE.
- **Zones:** A zone is a group of IP address ranges, in which all its subscribers receive an identical class of-service from the service provider. If multiple zones are defined for the system, statistics and traffic information are displayed for specific zones configured in the system. The All tab displays statistics and traffic for all zones. The Default tab presents the same data for all subscribers whose IP addresses are not included in a zone. By selecting a specific Zone, you can display zone-specific data in the Domain Traffic and Statistics areas.

  NOTE **The Zones tab is displayed if the Zone feature is enabled on the system. Consult Allot Customer Support if you want to add support for zones – requires license.**

- **Domain Traffic:** Displays graphs representing the bandwidth usage of all the servers in the domain.
- **Domain Statistics:** Displays video statistics for MediaSwift E servers.
- **Domain Servers:** Contains an array of icons, each icon representing a MediaSwift E server in the grid.
- **System Notifications:** Displays a list of system faults that exist in the domain.

From the Home page, you can also view information regarding individual MediaSwift E servers.

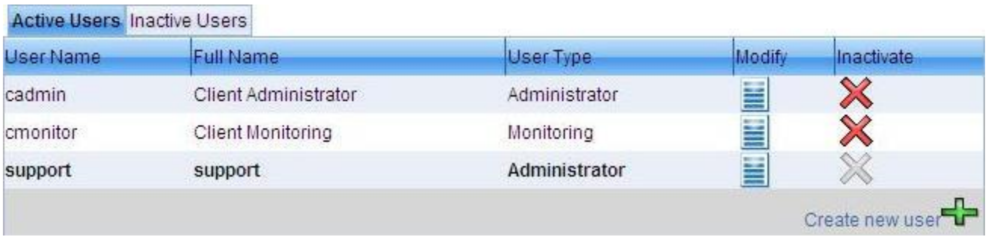
NOTE **All time-related information in MSWE is synchronized with the System Time, which is displayed in the top right corner of the screen.**

Chapter 3: User Management

Introduction to User Management

The MediaSwift E MSWE **Users Management** page enables administrators to manage each user's details and access privileges.

You can access the Users Management page by clicking the **Users Management** link at the top of the MSWE screen. The Users Management Window will appear as displayed in Figure 5.



Active Users | Inactive Users

User Name	Full Name	User Type	Modify	Inactivate
cadmin	Client Administrator	Administrator	▤	✗
cmonitor	Client Monitoring	Monitoring	▤	✗
support	support	Administrator	▤	✗

Figure 5: MSWE Users Management Window

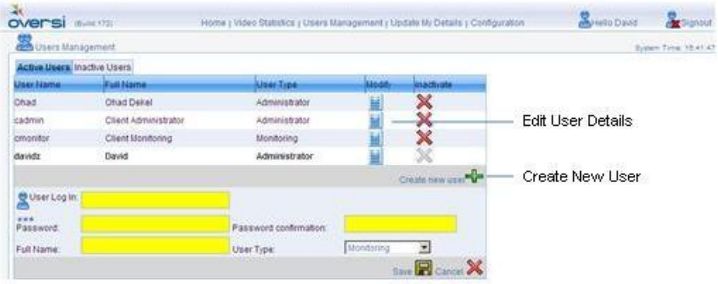
Managing MSWE Users

Adding New Users

When you add new users, you assign their user name, password and user type.

To add new users:

1. From the Users Management page, click on as seen in **Create New User**. The mandatory fields for creating a new user appear in yellow at the bottom of the screen, as depicted in Figure 6 below.



User Name	Full Name	User Type	Modify	Inactivate
Ohad	Ohad Dekel	Administrator	▤	✗
cadmin	Client Administrator	Administrator	▤	✗
cmonitor	Client Monitoring	Monitoring	▤	✗
davidz	David	Administrator	▤	✗

User Log In:

Password:

Password confirmation:

Full Name:

User Type: Monitoring

Figure 6: Creating a New User

2. Complete the fields as follows:
   - **User Log In:** The new user's MSWE user name.
   - **Password:** The new user's MSWE password.
   - **Password confirmation:** The new user's MSWE password entered a second time.

NOTE **Passwords must be at least 8 characters long. The password must contain a combination of alphabetic and numeric characters.**

- **Full Name**: The full name of the user.
- User type:
    - **Administrator**: Full permission to use system. This allows the administrator to configure the system, add new users, and to stop and start services.
    - **Configurator**: Same as the Administrator, except that the Configurator cannot perform user management tasks users (such as adding new users, or changing existing user properties).
    - **Monitoring**: User can perform monitoring only. The user can see system status and statistics, but cannot change configurations, cannot start and stop services, and cannot add/modify users.
    - **Video Monitoring**: Access to the video monitoring page only, in order to view "top video" statistics, and to export the statistics for use in the home page of the ISP's portal.

3. Click **Save** 💾.

   The user is added to the list of Active Users.

Activating and Deactivating Users

Instead of deleting users from the MSWE application, you can make their status **Inactive**. You can change their status back to **Active** at any time.

To deactivate users:

1. From the Users Management page (see the MSWE Users Management Window above in Figure 5), click **Inactivate** ✖ in the row containing the name of the user to be deactivated.

   You are prompted to confirm your action.

2. Click **OK**.

   The status of the user changes to **Inactive**.

➢ To activate users:

1. From the Users Management page (see the MSWE Users Management Window above in Figure 5), click **Activate** ✓ in the row containing the name of the user to be activated.

   You are prompted to confirm your action.

2. Click **OK**.

   The status of the user changes to **Active**.

Editing User Details

You can edit the details of existing MSWE users via the **Users Management** page.

➢ To edit user details:

1. From the Users Management page (see the MSWE Users Management Window above in Figure 5), click on **Modify** ☰ in the row containing the user whose details are to be modified.

   The fields containing the user's details appear at the bottom of the screen.

2. You may modify any of the user detail fields as described in Section 0 above.

3. Click **Save** 💾.

   The modified user's details are saved.

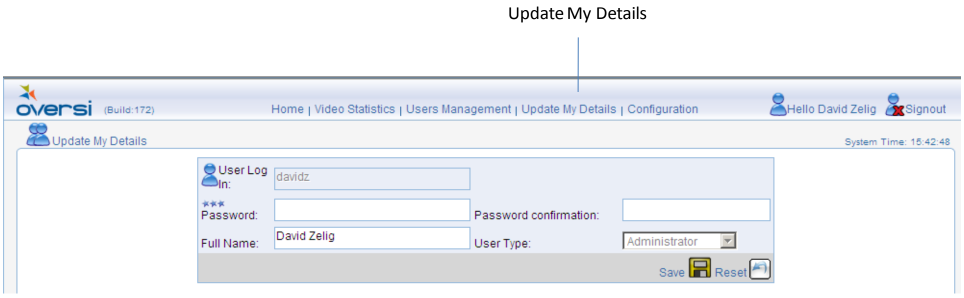
Changing Passwords

A user can change his or her own password at any time using the **Update My Details** page.

You can access this page by clicking the **Update My Details** link at the top of the MSWE screen.

➢ To change a password:

1. Click the **Update My Details** link at the top of the MSWE screen. The Update My Details page appears, as shown in Figure 7.



Update My Details

User Log In: davidz

Password:

Password confirmation:

Full Name: David Zelig

User Type: Administrator

Figure 7: Update My Details Page

2. In the **Password** field, enter your new password.

3. In the **Password confirmation** field, enter your password a second time.

NOTE **Passwords must be at least 8 characters long. The password must contain a combination of alphabetic and numeric characters.**

4. Click **Save** 💾.

   The user's new password is saved.

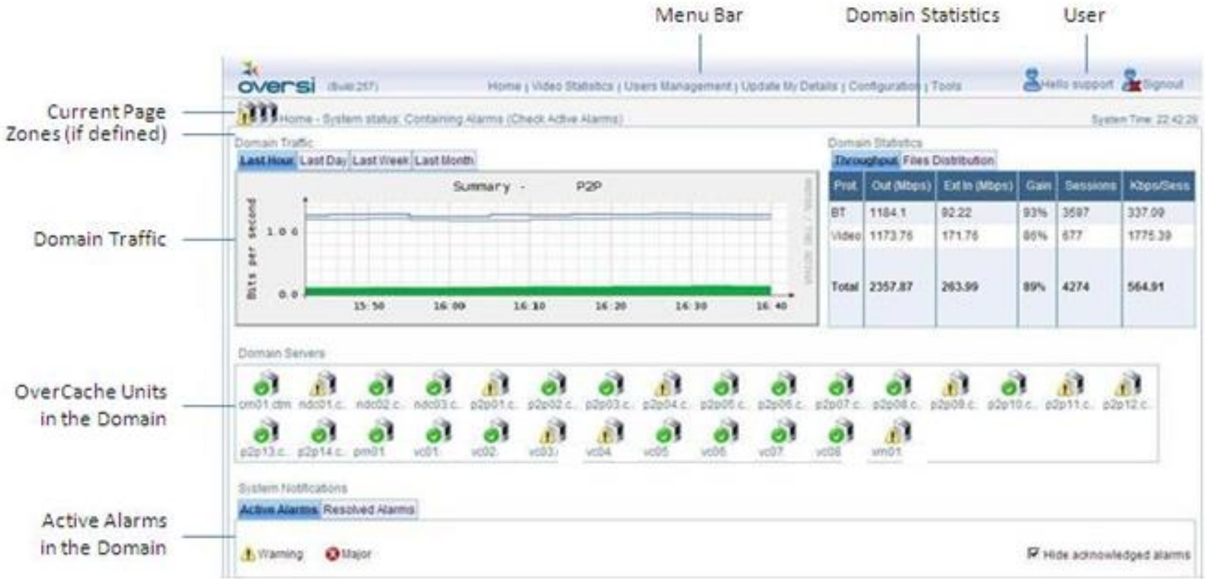
Chapter 4: Monitoring MediaSwift E

Domain Performance

The MSWE Home page enables network operators to monitor the performance of the MediaSwift E server grid in its domain, as well as the performance of individual servers.

The MSWE Home page displays an overview of all the MediaSwift E servers in a single domain.

An example of the Home page displaying all MediaSwift E servers in a domain is shown in Figure 8.



Home - System status: Containing Alarms (Check Active Alarms)

System Time: 22:42:29

Domain Statistics

Throughput | Files Distribution

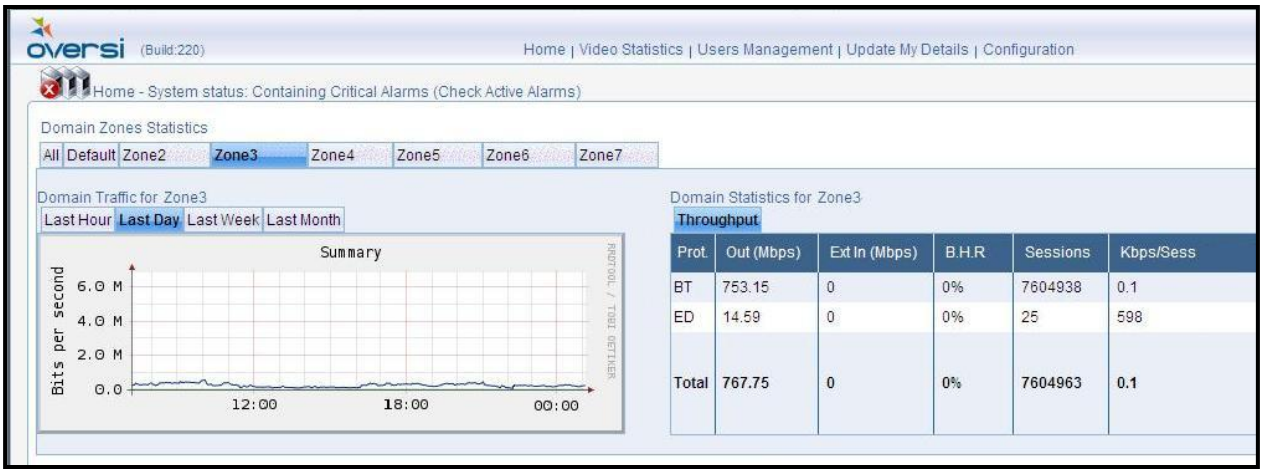
Prot.	Out (Mbps)	Ext In (Mbps)	Gain	Sessions	Kbps/Sess
BT	1184.1	92.22	93%	3597	337.09
Video	1173.76	171.76	86%	677	1775.39
Total	2357.87	263.99	89%	4274	564.91

Figure 8: MSWE Home Page Displaying All Servers

The MSWE Home page is divided into the following areas:

- **Status and Navigation**: The status and the navigation areas present the name of the page being viewed and the name of the current user, as well as navigational links within MSWE.
- **Zones**: A zone is a group of IP address ranges, in which all users in the group receive the same class of service from the caching system. You can display the traffic data and statistics for a specific zone by choosing the relevant zone tab. The **All** tab displays traffic data and statistics for all zones. The **Default** tab presents performance data for all subscribers whose IP addresses are not included in a specific zone. An example of the Home page displaying performance data for a specific zone is shown in Figure 9 below.

NOTE **The Zones tab is displayed if the Zone feature is enabled on the system. Consult Allot Customer Support if you want to add support for zones.**

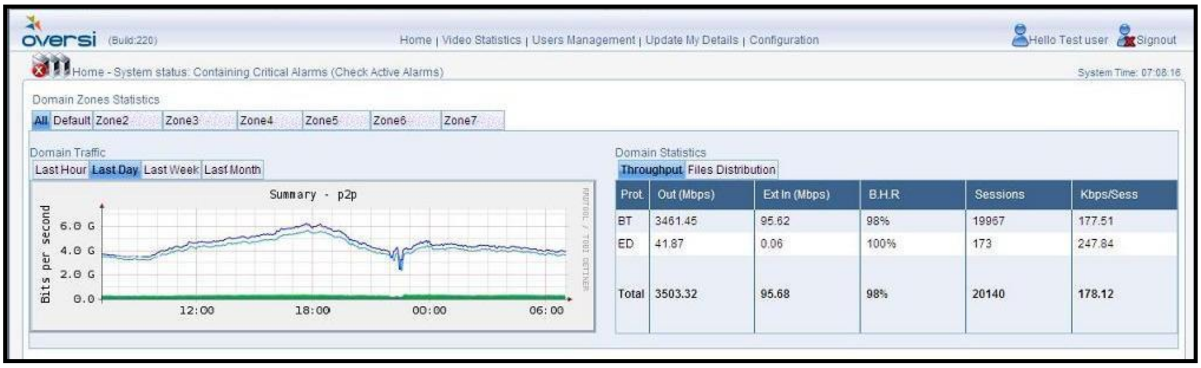


Prot.	Out (Mbps)	Ext In (Mbps)	B.H.R	Sessions	Kbps/Sess
BT	753.15	0	0%	7604938	0.1
ED	14.59	0	0%	25	598
Total	767.75	0	0%	7604963	0.1

Figure 9: MSWE Home Page with Zone Performance Data

- **Domain Traffic**: Displays graphs and traffic for all servers in the system.
- **Domain Statistics**: Displays statistics for all MediaSwift E servers.
- **Domain Servers**: Displays an icon for each MediaSwift E servers in the grid.
- **Domain Active Alarms**: Displays alerts for MediaSwift E servers.

NOTE **All time-related information in MSWE is sychronized with the System Time, which is displayed in the top right corner of the screen.**



Prot.	Out (Mbps)	Ext In (Mbps)	B.H.R	Sessions	Kbps/Sess
BT	3461.45	95.62	98%	19967	177.51
ED	41.87	0.06	100%	173	247.84
Total	3503.32	95.68	98%	20140	178.12

Figure 10: MSWE Home Page with Performance Data for All Zones

Viewing Domain Traffic Graphs

The **Domain Traffic** area in the Home page (see Figure 4) displays the bandwidth summary graph for peer-to-peer applications. The graph summarizes the peer-to-peer traffic for all servers in the domain.

If you select a specific zone from the **Zones** area, the graph displays traffic information for that zone. You can change the view of the graph to represent the last hour, day, week, or month.

➢ To view the domain graph:

1. If zones are configured, select a **Zone** in the Home page.
2. Select the time frame from one of the following tabs: **Last Hour**, **Last Day**, **Last Week**, or **Last Month**.

   The domain graph changes to reflect the data of the selected tab, as illustrated in Figure 11 below.

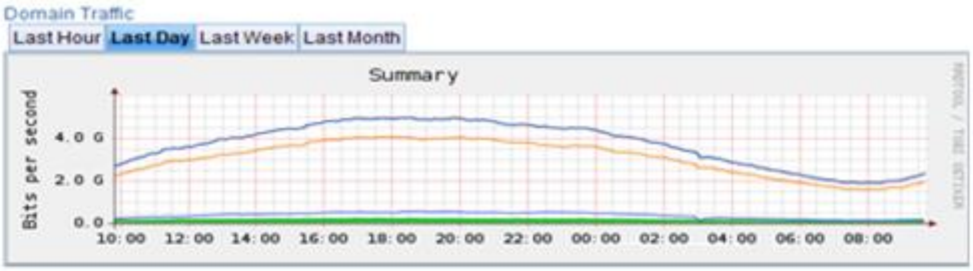


Figure 11: Example of a Domain Traffic Graph

The traffic levels displayed in the graph are represented by the following colors:

- **Dark blue line** – the total quantity of traffic (including overhead and payload) uploaded from all the servers in the domain.
- **Orange line** – eDonkey 2000 payload traffic uploaded from all the servers in the domain.
- **Light blue line** – BitTorrent payload traffic uploaded from all the servers in the domain.
- **Green area** – the total quantity of traffic (including overhead and payload) downloaded from peers to all the servers in the domain.

Video performance statistics are available through the Video Statistics page. See Section

Video Statistics for details.

Viewing Domain Statistics

The **Domain Statistics** area in the Home page (see Figure 4) displays statistics for all MediaSwift E servers.

NOTE **The statistics represent raw payload data, and do not account for the network overhead of the protocols. For this reason, there can be a discrepancy between the data displayed in this area and the data displayed in the graphs, which represent the actual bandwidth (including overhead) as indicated by the servers' NICs.**

The **Domain Statistics** area includes two tabs:

- **Throughput**: Displays the domain statistics according to the protocol used to upload or download files.
- **Files Distribution**: Displays the percentage of files according to size, by protocol and in total.

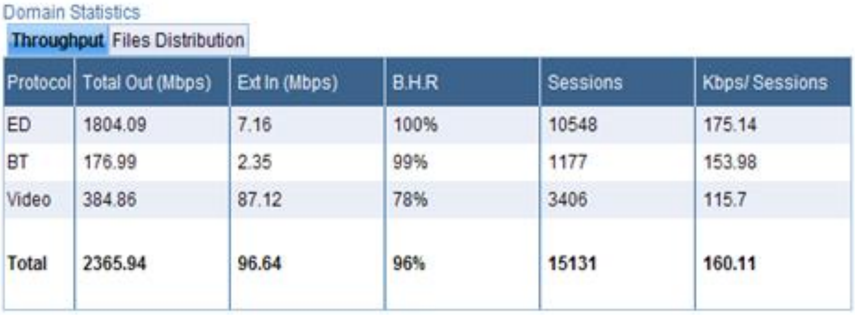
If a zone is selected in the **Zones** area, the **Domain Statistics** area view changes and does not display the **Files Distribution** tab or the **Ext In (Mbps)** and **Byte-Hit-Ratio** columns in the **Throughput** tab.

➢ **To display the information in the Domain Statistics area:**

- Select the **Throughput** tab or the **Files Distribution** tab.

Throughput Tab

The **Throughput** tabbed window displays domain statistics according to the protocol used to upload or download files. An example of the **Throughput** tab is displayed in Figure 12.



Protocol	Total Out (Mbps)	Ext In (Mbps)	B.H.R	Sessions	Kbps/ Sessions
ED	1804.09	7.16	100%	10548	175.14
BT	176.99	2.35	99%	1177	153.98
Video	384.86	87.12	78%	3406	115.7
Total	**2365.94**	**96.64**	**96%**	**15131**	**160.11**

Figure 12: Example of the Throughput Tab in the Domain Statistics Area

The **Throughput** tab displays the following columns:

- **Protocol**: The protocol used to upload or download the file. Statistics for the following protocols are collected:
  - BT: Bit Torrent
  - ED: eDonkey 2000 or eMule
  - Video: HTTP video and file download
  - Total: The summation of the domain statistics for all protocols.

- **Total Out (Mbps)**: The total bandwidth uploaded in Megabits per second for the specified protocol.
- **Ext In (Mbps)**: The total bandwidth downloaded from "external" sources outside the domain - in Megabits per second for the specified protocol. This data is not displayed in the Domain Traffic graph. (Note: This column is not displayed if a zone is selected in the **Zones** area.)

> **NOTE** **The green area in the Domain Traffic graph (like the one displayed in Figure 11) represents both the Ext In as well as the traffic entering the cache from local peers within the domain, therefore the value displayed in the graph is typically greater than the value of Ext In.**

- **B.H.R.**: Byte-Hit-Ratio. The B.H.R. represents the percentage of traffic found in the cache - that did not have to be downloaded from sources outside the domain. B.H.R is calculated according to the following formula:

  (Total Out – Ext In) ÷ Total Out

  (Note: This column is not displayed if a zone is selected in the **Zones** area.)

- **Sessions**: The number of concurrent active uploads from the domain, per protocol.
- **Kbps/Sessions**: The average upload speed of each session in Kilobits per second, per protocol.

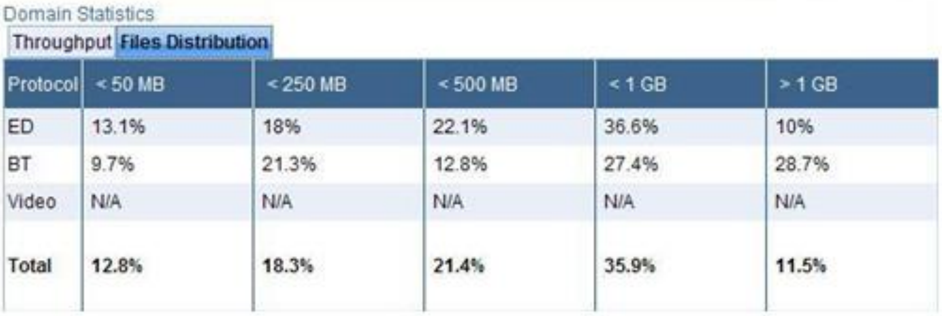
> **NOTES** **When analyzing the performance of the MediaSwift E system, please keep in mind the following definitions:**
>
> **"Uploading" refers to traffic forwarded by a MediaSwift E server to the clients.**
>
> **"Downloading" refers to traffic received by a MediaSwift E server.**

Files Distribution Tab

The **Files Distribution** tabbed window displays the percentage of files according to size, per protocol and in total.

> **NOTE** **The Files Distribution tab is not displayed when a specific zone is selected in the Zones area.**

An example of the **Files Distribution** tab of the Domain Statistics area is displayed in Figure 13.



Protocol	< 50 MB	< 250 MB	< 500 MB	< 1 GB	> 1 GB
ED	13.1%	18%	22.1%	36.6%	10%
BT	9.7%	21.3%	12.8%	27.4%	28.7%
Video	N/A	N/A	N/A	N/A	N/A
Total	12.8%	18.3%	21.4%	35.9%	11.5%

Figure 13: Files Distribution Tab in the Domain Statistics Area

The **Files Distribution** tab displays the following columns:

- **Protocol**: The protocol used to upload or download the file. Statistics for the following protocols are collected:

- **BT**: Bit Torrent
- **ED**: eDonkey 2000 or eMule
- **Video**: HTTP video
- **Total**: The percentage of distributed files, of the specified size, for all protocols

- Distribution of files by size, falling into the following categories
  - < 50 MB
  - < 250 MB
  - < 500 MB
  - < 1 GB
  - > 1 GB

Viewing MediaSwift E Servers in the Grid

The **Domain Servers** area in the Home page (Figure 4) displays an icon and name of each MediaSwift E unit in the *grid*. A grid is a group of logically-associated MediaSwift E servers that may be dispersed geographically over multiple points-of-presence.

An example of the **Domain Servers** area is displayed in Figure 14.

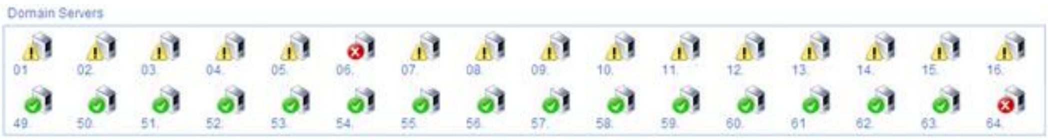


Figure 14: Example of the Domain Servers Area

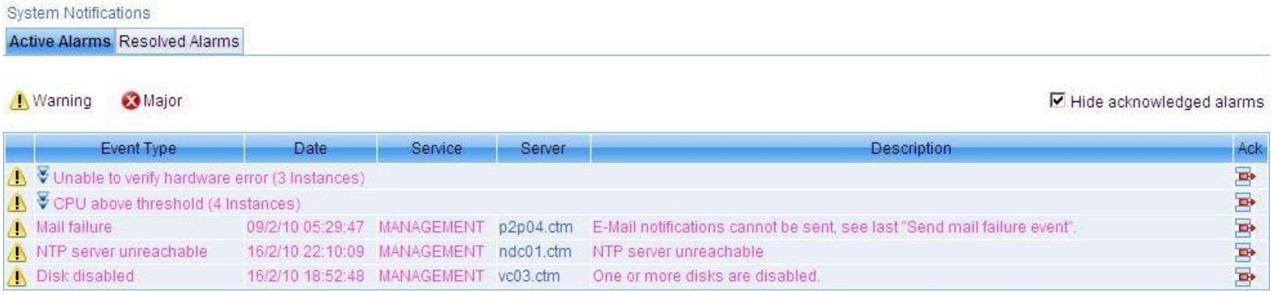
From the **Domain Servers** area, you can select an individual MediaSwift E unit and drill down to view more information. For more information, refer to

Server Performance, below.

Reviewing the Domain's Active Alarms

The **System Notifications** area in the Home page displays current alarms for the array of MediaSwift E servers in the provider's domain.

An example of the **System Notifications** area is displayed in Figure 15.



	Event Type	Date	Service	Server	Description	Ack
⚠	Unable to verify hardware error (3 Instances)					
⚠	CPU above threshold (4 Instances)					
⚠	Mail failure	09/2/10 05:29:47	MANAGEMENT	p2p04.ctm	E-Mail notifications cannot be sent, see last "Send mail failure event".	
⚠	NTP server unreachable	16/2/10 22:10:09	MANAGEMENT	ndc01.ctm	NTP server unreachable	
⚠	Disk disabled	16/2/10 18:52:48	MANAGEMENT	vc03.ctm	One or more disks are disabled.	

Figure 15: Example of the System Notifications Area

Each domain-level Active Alarm record includes the following information:

- **Alarm Level:** The level of the alert, as indicated by one of the following icons:
  - Major ☒ - followed by an orange-colored textual description

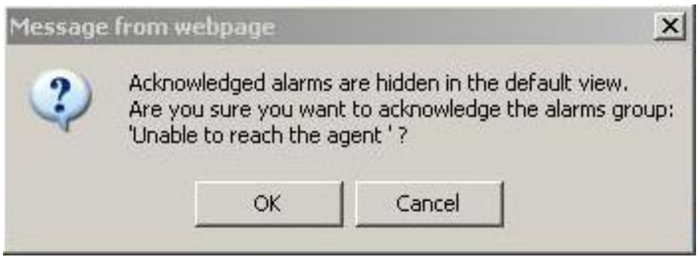
  - Warning ⚠ - followed by a pink-colored textual description

- **Event Type**: The type of event that caused the alarm. All alarms of the same type are typically grouped together. In the case that the event triggered a *group* of alarms, the event type is preceded by an icon that allows the technician to open and close the alarm group. Click on ▼ to open the alarm group, and on ▲ to close it.
- **Date:** The date and time of the event's occurrence.
- **Service**: The name of the software component ("service") that triggered the alert.
- **Server:** The name of the server that triggered the alert.
- **Description**: A short explanation of the problem.
- **Ack:** An icon specifying whether the alarm has been acknowledged or not. The red icon 🟥 signifies an un-acknowledged alarm, while a green 🟩 icon represents an acknowledged alarm. Click on the **Hide Acknowledged Alarms** check box ☑ to hide all acknowledged alarms.

➢ To acknowledge an alarm:

1. Identify the row containing the alarm or alarm group that is to be handled. Click on red icon 🟥 in order to acknowledge the alarm. The green "acknowledged alarm" icon 🟩 will appear instead.

   If the **Hide Acknowledged Alarms** check box is checked, the system displays a dialog box warning that the acknowledged alarm will be hidden from view, as displayed in Figure 16 below.



Message from webpage

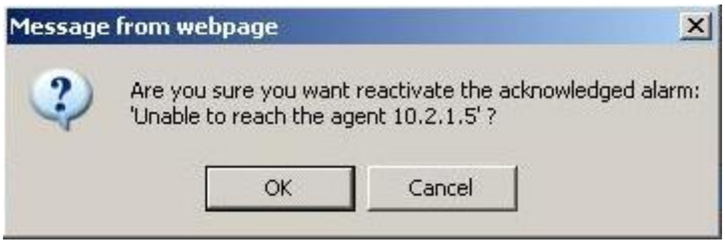
Acknowledged alarms are hidden in the default view.
Are you sure you want to acknowledge the alarms group:
'Unable to reach the agent ' ?

Figure 16: Confirm Hiding of Acknowledged Alarm

2. Click on **OK** if you wish to confirm the acknowledgement. The alarm will disappear from the Active Alarms area.

➢ To reactivate an acknowledged alarm:

1. Identify the row containing the acknowledged alarm or alarm group that is to be reactivated. Click on green icon 🟩 in order to reactivate the alarm. The system displays a dialog box warning that the acknowledged alarm will be reactivated, as displayed in Figure 17 below.



Message from webpage

Are you sure you want reactivate the acknowledged alarm: 'Unable to reach the agent 10.2.1.5' ?

Figure 17: Confirm Alarm Reactivation

2. Click on **OK** if you wish to confirm the reactivation. The red icon “unacknowledged alarm” will appear.

Server Performance

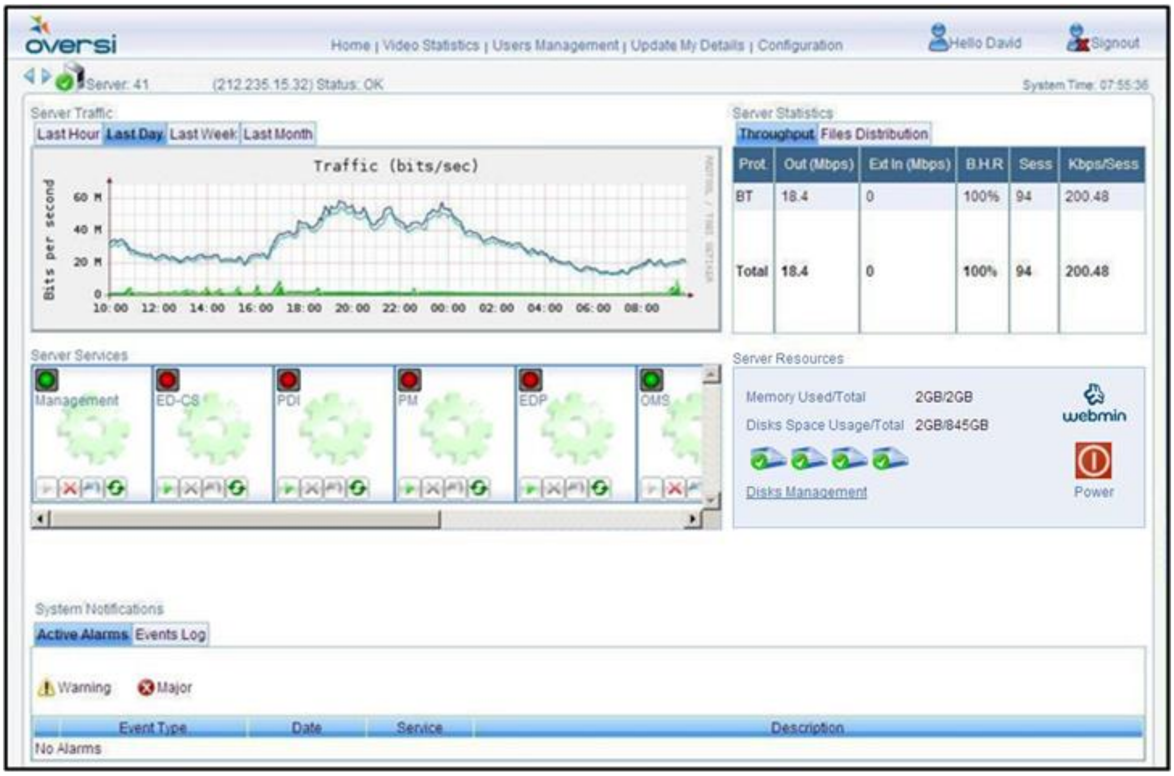
You can drill down to view information regarding a specific MediaSwift E server.

➢ To drill down to a specific server:

- Select the server unit from the Domain Servers area (see Figure 14 above) in the Home page.

The Home page changes to display information regarding the specific server you selected, and the page name changes to **Server Management.**

An example of the Server Management page for a selected server is displayed in Figure 18 below.



oversi
Home | Video Statistics | Users Management | Update My Details | Configuration
Hello David
Signout

Server: 41 (212.235.15.32) Status: OK

System Time: 07:55:36

Prot.	Out (Mbps)	Ext In (Mbps)	B.H.R	Sess	Kbps/Sess
BT	18.4	0	100%	94	200.48
Total	18.4	0	100%	94	200.48

Memory Used/Total 2GB/2GB

Disks Space Usage/Total 2GB/845GB

Event Type	Date	Service	Description
No Alarms			

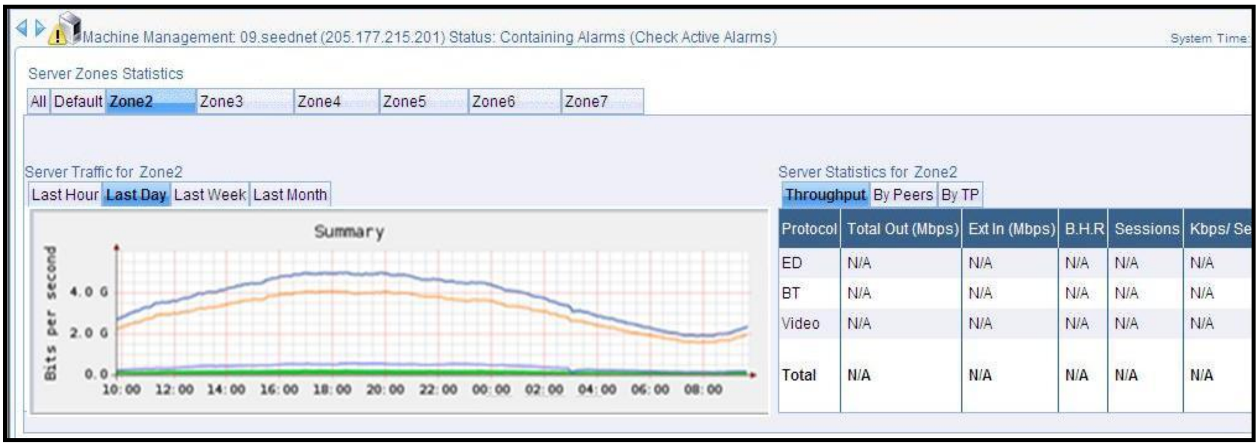
Figure 18: Server Management Page for a Specific Server Unit

The **Server Traffic**, **Server Statistics**, and **System Notifications** areas in the Server Management page operate identically to the relevant domain-based areas in the Home page. In these areas, the meaning of the information in the Server Management page is the same as that of the Home page, except that the information refers to the selected MediaSwift E server as opposed to the entire grid. For example, the Server Traffic graph on the Server Management page (see Figure 18) is essentially the same as the Domain Traffic graph on the Home page (see Figure 4), except that the first refers to a single server and the second summarizes the traffic of all the servers.

You can refer to the description of The MSWE Home Page, for more information regarding the following areas of the Server Management page:

- Server Traffic
- Server Statistics
- System Notifications

In addition, the Server Management Page enables you to access **Zone** related information for individual servers, as displayed in Figure 19 below.



Machine Management: 09.seednet (205.177.215.201) Status: Containing Alarms (Check Active Alarms)

Protocol	Total Out (Mbps)	Ext In (Mbps)	B.H.R	Sessions	Kbps/ Se
ED	N/A	N/A	N/A	N/A	N/A
BT	N/A	N/A	N/A	N/A	N/A
Video	N/A	N/A	N/A	N/A	N/A
Total	N/A	N/A	N/A	N/A	N/A

Figure 19: Server Management Page with Zone-specific Performance Data

The Server Management page also includes two areas that enable troubleshooting of the performance of specific MediaSwift E servers, as shown previously in Figure 18:

- **Server Services**: Enables you to manage the services on a specific server.
- **Server Resources:** Displays server resources, such as memory, disks, and also includes a server shutdown button.

➢ To navigate between servers in the grid:

- Click the next or previous server ◁ ▷ arrows in the top left corner of the screen.

Detailed Server Statistics

Detailed statistics on individual servers are available directly from the server page. By clicking on the performance graph, you will be directed to a new window containing detailed graphs on all aspects of server performance, such as CPU and memory utilization, disk space availability, number of files, hit ratio, and more. For more information, see Advanced Performance Monitoring Using Cacti.

NOTE **The availability of relevant graphs is dependent on the functionality of a specific server.**

Managing Services on MediaSwift E Servers

The **Server Services** area in the Servers Management page displays the services that are running or have been stopped on a specific server. A “green light” above the name of the service means that the service is running, while a “red light” is displayed when the service has stopped. An example of the **Server Services** area is displayed in Figure 20 below.

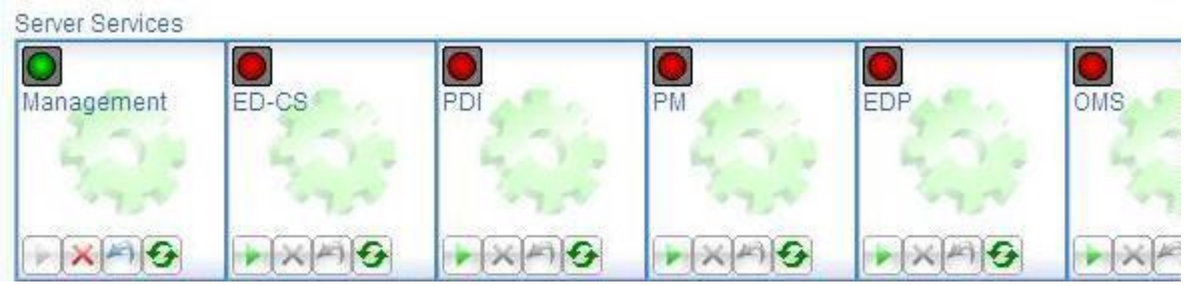


Figure 20: Example of Server Services Area

In the **Server Services** area you can start, stop, restart, or refresh a specific service on a server unit.

NOTE **It is not recommended to stop a service. If you need to do so, the service is stopped only until the unit or the management server restarts, or a new configuration is distributed through the Command Line Interface.**

The available services include:

- **Management**: Manages other MediaSwift E services
- **ED-CS:** ED2K Cache Server
- **BT-CS**: BitTorrent Cache Server
- **HTTP-CS**: HTTP Cache Server
- **EDP**: ED2K proxy that controls traffic for the ED2K protocol
- **PM**: Peer Manager controller
- **HM**: HTTP Manager controller
- **PDI**: P2P Demand Identifier
- **HDI:** HTTP Demand Identifier
- **PAgent:** Pathalizer Agent
- **CDR:** Connection Detail Record
- **BGP-S:** BGP Service
- **OMS**: The MSWE web management interface

➢ To manage the services of an individual server:

1. In the **Server Services** area (as seen in Figure 20), perform **one** of the following actions in the box of the appropriate MediaSwift E server:
   - Click the **Start** icon ▶ under the name of the service to start the service.
   - Click the **Stop icon** ☒ under to the name of the service to stop the service.
   - Click the **Restart icon** ↶ under to the name of the service to restart the service (that is, to stop it and automatically start it again).
   - Click the **Refresh** icon ⟳ under to the name of the service to refresh its status.
2. If you stopped or restarted a service, you are prompted to confirm.

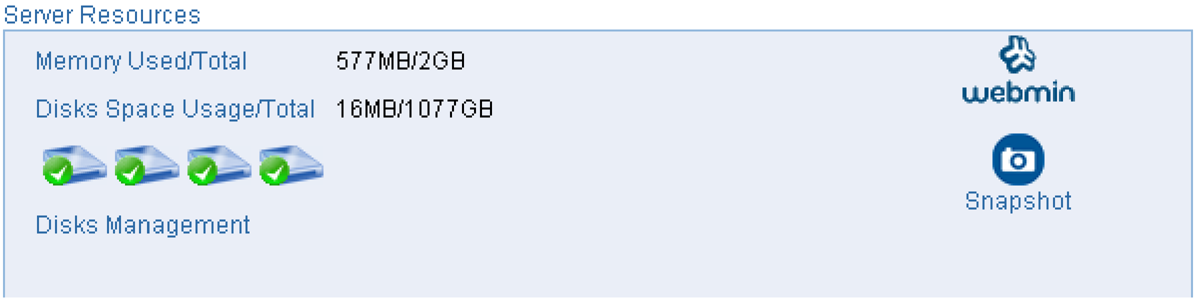
3. If you clicked **Stop** or **Restart**, click **OK**.

   The service stops or restarts, respectively.

MediaSwift E Server Memory and Disk Resources

The **Server Resources** area in the Server Management page (Figure 18) displays the memory and disk resources for a specific server, and features a **Snapshot** button used to generate log files and statistics about the current situation of the server on a zip file, that can be sent to Allot 's support team.

An example of the **Server Resources** area is displayed in Figure 21.



Server Resources

Memory Used/Total 577MB/2GB

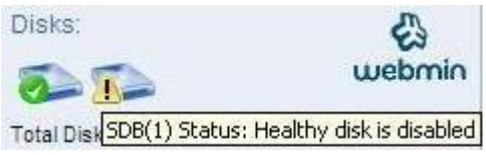
Disks Space Usage/Total 16MB/1077GB

Disks Management

Figure 21: Example of the Server Resources Area

The **Server Resources** area includes the following information:

- Memory resources
  - **Mem Used**: Server-based memory in use.
  - **Mem Total**: Total memory available in the system.
- Disk resources
  - **Total Disks Space**: The maximum storage on all disks.
  - **Total Disks Usage**: The total actual usage on all disks.
  - **Disk Status (OK or Fault)**: The status of the disk, as displayed on each disk icon. Hover over one of the icons to see a tooltip with a textual description of the disk's status.



Disks:

Total Disk SDB(1) Status: Healthy disk is disabled

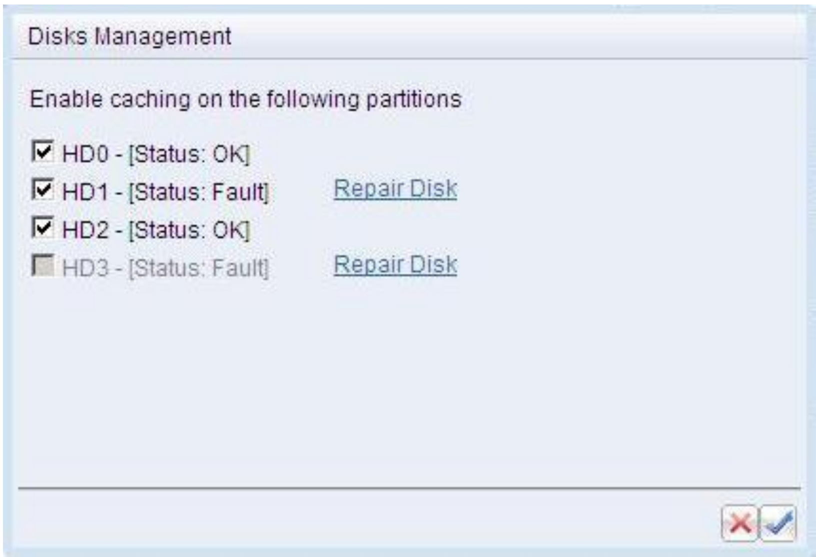
Figure 22: Disk Status icon with Tooltip

  - **Disks Management:** Allows the operator to enable or disable caching on any of the server's disks. See the section on Disk Management below
- **Snapshot button**: System status can be displayed and/or saved on a DOK and the file sent to Allot support

NOTE **To restart or power down the server, press the Reset button at the server itself.**

MediaSwift E Server Disks Management

The **Disks Management** window, shown in Figure 23, allows you to enable or disable caching on any of the disks in a MediaSwift E server. Disabling a faulty disk allows the operator to continue caching when the disk cannot be repaired immediately. Up to 2 disks can be disabled in any server.



Disks Management

Enable caching on the following partitions

☑ HD0 - [Status: OK]

☑ HD1 - [Status: Fault] Repair Disk

☑ HD2 - [Status: OK]

□ HD3 - [Status: Fault] Repair Disk

Figure 23: Disks Management Window

➢ To manage the disks of an individual server:

1. Click on the **Disks Management** link in the Server Resources area depicted in Figure 21. The Disks Management window will appear as shown in Figure 23

2. Use the check boxes to enable or disable each disk. Up to 2 disks can be disabled in a single server.

NOTES **For functional disks: Disabling a functional disk will result in an alarm. Enabling the disk clears the alarm.**

For malfunctioning disks: Enabling a malfunctioning disk will cause the system to generate an alarm. Disabling the disk will clear the alarm.

3. To repair an XFS file system error, click on the **Repair Disk** link next to the relevant partition. This action will stop the service running on the server, repair the XFS file system and return the service to operation. The service outage may last a few minutes.

4. Click on **Delete** ✕ to close the window without saving the modifications

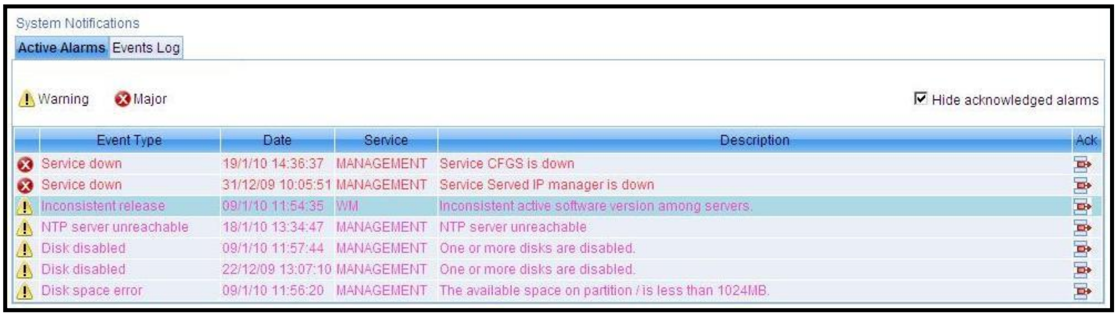
5. Click on **Apply** ✓ to submit the modifications and close the window.

MediaSwift E Server Alarms and Events

The **System Notifications** area in the System Management page (see Figure 18 above) displays lists of Active Alarms and Event Logs for a specific server.

Active Alarms

An example of the Active Alarms area is displayed in Figure 24 below.



System Notifications

⚠ Warning ✖ Major ☑ Hide acknowledged alarms

	Event Type	Date	Service	Description	Ack
✖	Service down	19/1/10 14:36:37	MANAGEMENT	Service CFGS is down	⇨
✖	Service down	31/12/09 10:05:51	MANAGEMENT	Service Served IP manager is down	⇨
⚠	Inconsistent release	09/1/10 11:54:35	WM	Inconsistent active software version among servers.	⇨
⚠	NTP server unreachable	18/1/10 13:34:47	MANAGEMENT	NTP server unreachable	⇨
⚠	Disk disabled	09/1/10 11:57:44	MANAGEMENT	One or more disks are disabled.	⇨
⚠	Disk disabled	22/12/09 13:07:10	MANAGEMENT	One or more disks are disabled.	⇨
⚠	Disk space error	09/1/10 11:56:20	MANAGEMENT	The available space on partition / is less than 1024MB.	⇨

Figure 24: Active Alarms Area

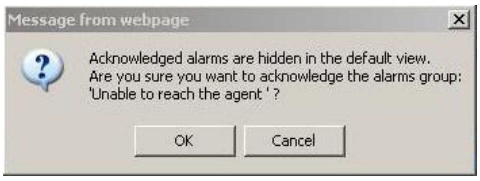
Each alarm record includes the following information:

- **Alarm Severity:** indicated by an icon next to the event:
    - Major ✖ - followed by an orange-colored textual description
    - Warning ⚠ - followed by a pink-colored textual description
- **Event Type**: The type of event that caused the alarm.
- **Date**: The date and time when the alarm was raised occurred.
- **Service**: The name of the component that triggered the alert.
- **Description:** An explanation of the alarm.
- **Ack:** An icon specifying whether the alarm has been acknowledged or not. The red ⇨ icon signifies an un-acknowledged alarm, while a green ⇦ icon represents an acknowledged alarm. Click on the **Hide Acknowledged Alarms** check box ☑ to hide all acknowledged alarms.

➢ To acknowledge an alarm:

1. Identify the row containing the alarm or alarm group that is to be handled. Click on red icon ⇨ in order to acknowledge the alarm. The green "acknowledged alarm" icon ⇦will appear instead.

   If the **Hide Acknowledged Alarms** check box is checked, the system displays a dialog box warning that the acknowledged alarm will be hidden from view, as displayed in Figure 25 below.



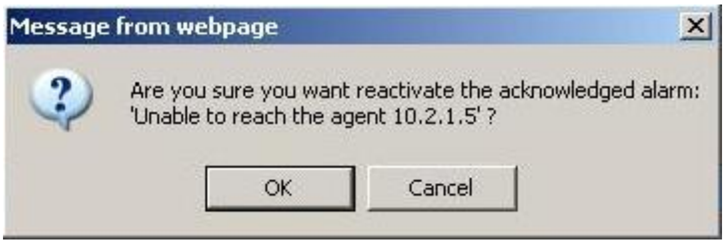
Acknowledged alarms are hidden in the default view.
Are you sure you want to acknowledge the alarms group:
'Unable to reach the agent ' ?

Figure 25: Confirm Hiding of Acknowledged Alarm

2. Click on **OK** if you wish to confirm the acknowledgement. The alarm will disappear from the Active Alarms area.

➢ To reactivate an acknowledged alarm:

1. Identify the row containing the acknowledged alarm or alarm group that is to be reactivated. Click on green icon in order to reactivate the alarm. The system displays a dialog box warning that the acknowledged alarm will be reactivated, as displayed in Figure 26 below.



Message from webpage

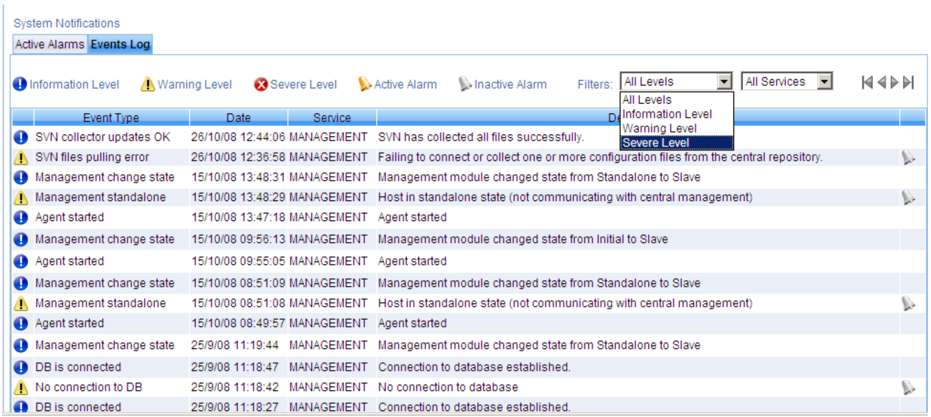
Are you sure you want reactivate the acknowledged alarm:
'Unable to reach the agent 10.2.1.5' ?

Figure 26: Confirm Alarm Reactivation

2. Click on OK if you wish to confirm the reactivation. The red icon “unacknowledged alarm” will appear.

Events Log

An example of the Events Log area is displayed below in Figure 27.



	Event Type	Date	Service	De	
❗	SVN collector updates OK	26/10/08 12:44:06	MANAGEMENT	SVN has collected all files successfully.	
⚠	SVN files pulling error	26/10/08 12:36:58	MANAGEMENT	Failing to connect or collect one or more configuration files from the central repository.	🔔
❗	Management change state	15/10/08 13:48:31	MANAGEMENT	Management module changed state from Standalone to Slave	
⚠	Management standalone	15/10/08 13:48:29	MANAGEMENT	Host in standalone state (not communicating with central management)	🔔
❗	Agent started	15/10/08 13:47:18	MANAGEMENT	Agent started	
❗	Management change state	15/10/08 09:56:13	MANAGEMENT	Management module changed state from Initial to Slave	
❗	Agent started	15/10/08 09:55:05	MANAGEMENT	Agent started	
❗	Management change state	15/10/08 08:51:09	MANAGEMENT	Management module changed state from Standalone to Slave	
⚠	Management standalone	15/10/08 08:51:08	MANAGEMENT	Host in standalone state (not communicating with central management)	🔔
❗	Agent started	15/10/08 08:49:57	MANAGEMENT	Agent started	
❗	Management change state	25/9/08 11:19:44	MANAGEMENT	Management module changed state from Standalone to Slave	
❗	DB is connected	25/9/08 11:18:47	MANAGEMENT	Connection to database established.	
⚠	No connection to DB	25/9/08 11:18:42	MANAGEMENT	No connection to database	🔔
❗	DB is connected	25/9/08 11:18:27	MANAGEMENT	Connection to database established.	

Figure 27: Events Log with Filters

Each **Events Log** record includes the following information:

- **Event classification:** indicated by an icon next to the event:
  - Major ✖ - followed by an orange-colored textual description
  - Warning ⚠ - followed by a pink-colored textual description
  - Information ❗ - followed by a blue-colored textual description. (Information text is viewed only from the Server Management page.)
  - Active Alarm 🔔 - followed by a black-colored textual description
  - Inactive (Resolved) Alarm 🔔 followed by a gray-colored textual description

- **Event Type**: The type of event that caused the alarm.
- **Date**: The date and time when the event occurred.
- **Service**: The name of the component that triggered the alert.
- **Description**: A description of the event.

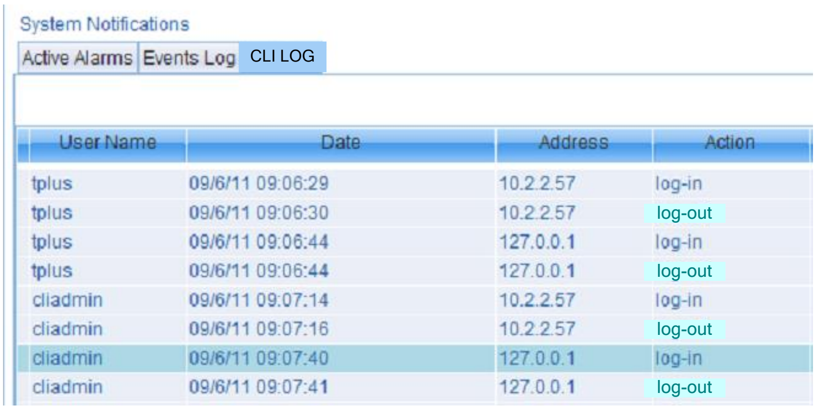
You can use a filter to display specific events based on the severity level and the service type.

➢ To filter events:

- In the Events Log **Filters** fields (shown in Figure 27), select a value from the Levels and Services drop-down lists.

WM CLI Logging

The CLI Log is used to track the entry of Allot service personnel into the caching system via SSH. An example of a CLI log is shown in Figure 28 below.



User Name	Date	Address	Action
tplus	09/6/11 09:06:29	10.2.2.57	log-in
tplus	09/6/11 09:06:30	10.2.2.57	log-out
tplus	09/6/11 09:06:44	127.0.0.1	log-in
tplus	09/6/11 09:06:44	127.0.0.1	log-out
cliadmin	09/6/11 09:07:14	10.2.2.57	log-in
cliadmin	09/6/11 09:07:16	10.2.2.57	log-out
cliadmin	09/6/11 09:07:40	127.0.0.1	log-in
cliadmin	09/6/11 09:07:41	127.0.0.1	log-out

Figure 28: CLI Log

The **CLI Log** produces log-in and log-out records including the following information:

- **User Name:** The user name of the technician operating the session.
- **Date**: The date and time when the action occurred.
- **Address**: The IP address of the server hosting the session.
- **Action**: A description of the action (log-in and log-out) taken by the operator.

Video Statistics

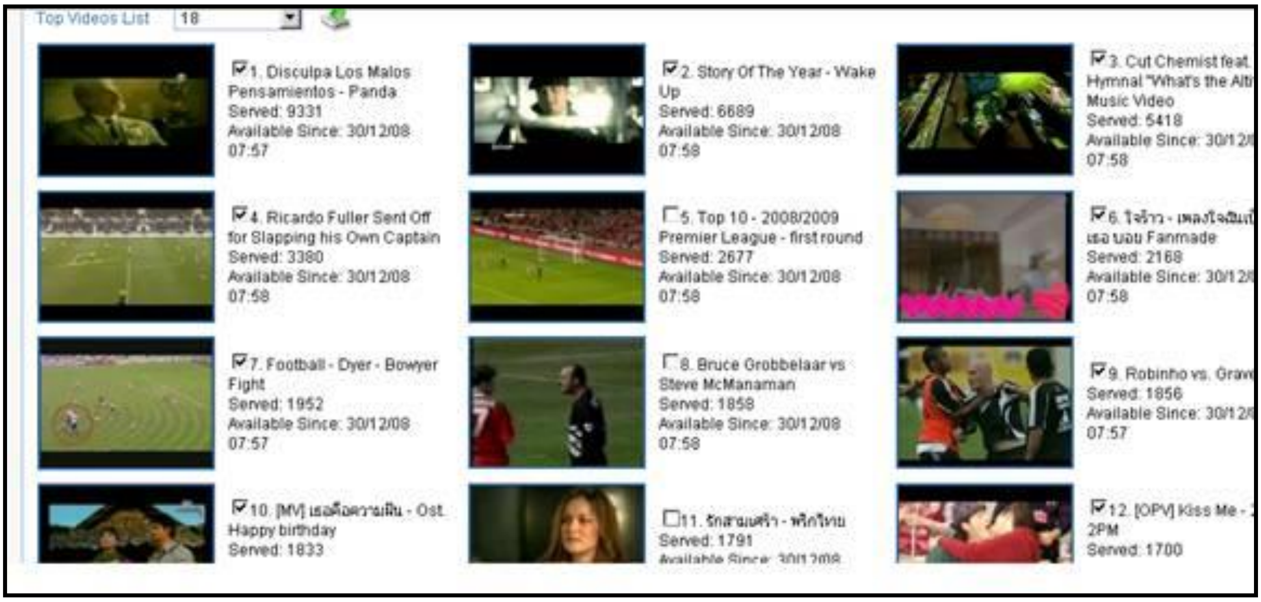
The **Video Statistics** page displays the quantity of bandwidth used by the service provider network for Internet video service, and displays the most popular video clips from the YouTube site.

➢ To view video traffic generated by the system:

1. Click the **Video Statistics** link at the top of the page.
2. Select the time frame from one of the following tabs: **Last Hour**, **Last Day**, **Last Week**, or **Last Month**.
3. The domain graph changes to display the data relevant to the selected tab.

➢ To view the most popular video clips on YouTube

1. Click the **Video Statistics** link at the top of the page.
2. Select the number of videos to be displayed in the list box (you can display as few as three, and as many as 100). The top selections appear on the page as shown in Figure 29.



Top Videos List 18

☑ 1. Disculpa Los Malos Pensamientos - Panda
Served: 9331
Available Since: 30/12/08 07:57

☑ 2. Story Of The Year - Wake Up
Served: 6689
Available Since: 30/12/08 07:58

☑ 3. Cut Chemist feat. Hymnal "What's the Alt
Music Video
Served: 5418
Available Since: 30/12/
07:58

☑ 4. Ricardo Fuller Sent Off for Slapping his Own Captain
Served: 3380
Available Since: 30/12/08 07:58

□ 5. Top 10 - 2008/2009 Premier League - first round
Served: 2677
Available Since: 30/12/08 07:58

☑ 6. ใจร้าว - เพลงใจฉันเ
เธอ นอน Fanmade
Served: 2168
Available Since: 30/12/
07:58

☑ 7. Football - Dyer - Bowyer Fight
Served: 1952
Available Since: 30/12/08 07:57

□ 8. Bruce Grobbelaar vs Steve McManaman
Served: 1858
Available Since: 30/12/08 07:58

☑ 9. Robinho vs. Grav
Served: 1856
Available Since: 30/12/
07:57

☑ 10. [MV] เธคือความฝัน - Ost Happy birthday
Served: 1833

□ 11. รักสามเศร้า - พริกไทย
Served: 1791
Available Since: 30/12/08

☑ 12. [OPV] Kiss Me -
2PM
Served: 1700

Figure 29: Example of Video Statistics Page

The system displays the following statistics for each video clip:

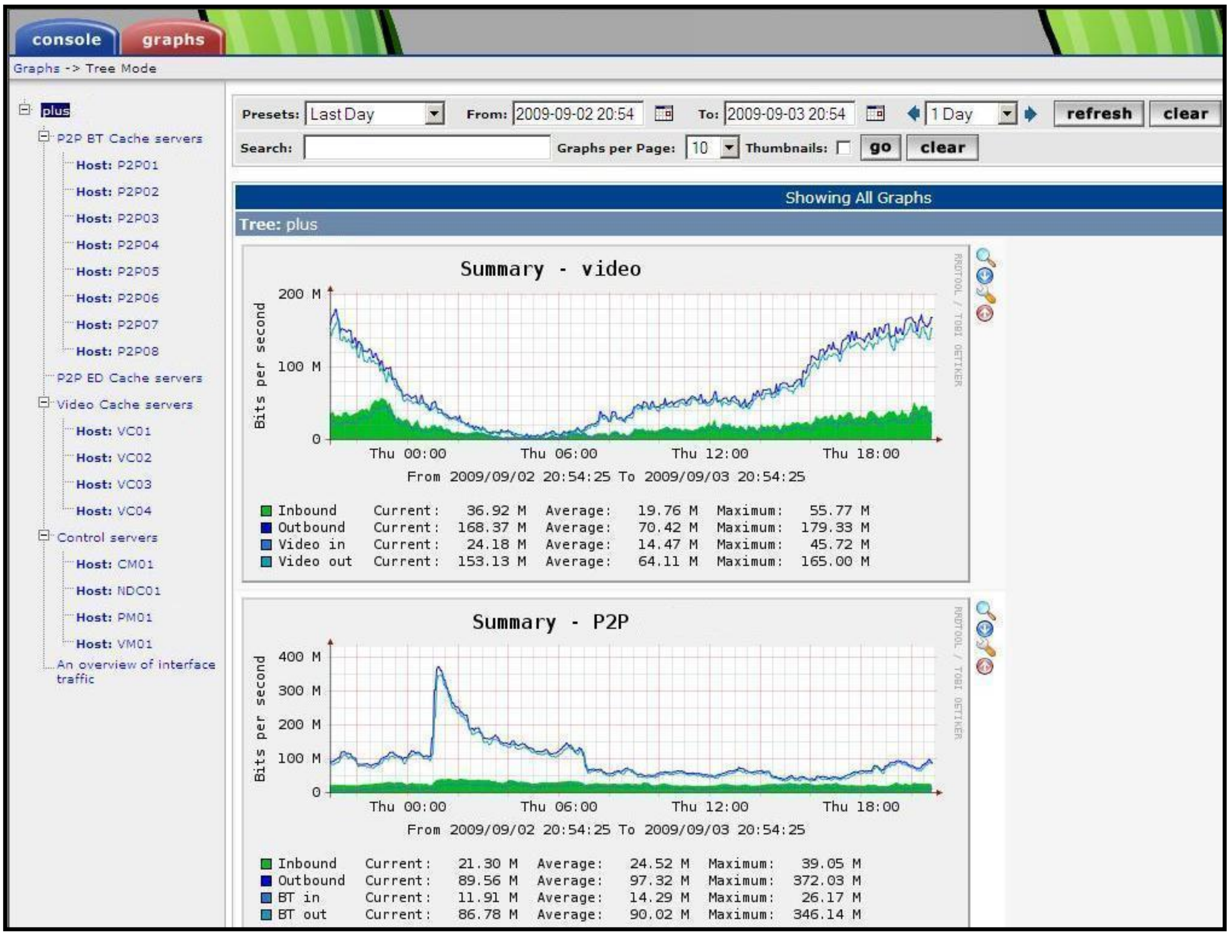
- **Video Name**: The name of the video as it appears in the original video site.
- **Served**: The number of times the video has been served from the video cache in the last 24 hours. This statistic is updated once every 15 minutes.
- **Available Since**: The date and time when the video was first served from the cache.

3. Click on the video picture or video name to open a new browser window that plays the video clip from the original video site.
4. You can select/unselect the video data that you want to export to an XML file by clicking the check box near each video name.
5. To create the XML file, click on the export button. The file contains the metadata of each video clip, and can be used to generate a "top video" video list on the service provider's portal.

Advanced Performance Monitoring Using Cacti

Allot's MediaSwift E uses a third-party software package, known as Cacti, in order to present advanced data on the performance of system servers. Cacti, an open source graphing tool, tracks the server's status and provides reports on traffic throughput, CPU utilization, memory utilization, available disk space, and other attributes.

Figure 30 below depicts a diagram showing the Navigation Tree and graphs with throughput data. System-wide summary data can be displayed by choosing the root element of the tree.



Graphs -> Tree Mode

- plus
  - P2P BT Cache servers
    - Host: P2P01
    - Host: P2P02
    - Host: P2P03
    - Host: P2P04
    - Host: P2P05
    - Host: P2P06
    - Host: P2P07
    - Host: P2P08
  - P2P ED Cache servers
  - Video Cache servers
    - Host: VC01
    - Host: VC02
    - Host: VC03
    - Host: VC04
  - Control servers
    - Host: CM01
    - Host: NDC01
    - Host: PM01
    - Host: VM01
  - An overview of interface traffic

Presets: Last Day From: 2009-09-02 20:54 To: 2009-09-03 20:54 1 Day

Search: Graphs per Page: 10 Thumbnails: □

Showing All Graphs

Tree: plus

Summary - video

From 2009/09/02 20:54:25 To 2009/09/03 20:54:25

```
🟩 Inbound    Current:   36.92 M  Average:   19.76 M  Maximum:   55.77 M
■ Outbound   Current:  168.37 M  Average:   70.42 M  Maximum:  179.33 M
■ Video in   Current:   24.18 M  Average:   14.47 M  Maximum:   45.72 M
■ Video out  Current:  153.13 M  Average:   64.11 M  Maximum:  165.00 M
```

Summary - P2P

From 2009/09/02 20:54:25 To 2009/09/03 20:54:25

```
🟩 Inbound   Current:  21.30 M  Average:  24.52 M  Maximum:  39.05 M
■ Outbound  Current:  89.56 M  Average:  97.32 M  Maximum: 372.03 M
■ BT in     Current:  11.91 M  Average:  14.29 M  Maximum:  26.17 M
■ BT out    Current:  86.78 M  Average:  90.02 M  Maximum: 346.14 M
```

Figure 30: Cacti Screen with Navigation Tree and Summary Graphs

For detailed descriptions on each of the available graphs and their interpretation, please refer to the latest version of the *MediaSwift E Performance Monitoring User Manual*.

Chapter 5: System Configuration

System Configuration Overview

This chapter describes how to configure the MediaSwift E platform using the MediaSwift E
MSWE system. MSWE's configuration capabilities are designed to give the service provider more control over internet bandwidth utilization, and over customer Quality of Experience.

All configuration activities are performed using the Configuration page. You can access the Configuration page by clicking on the **Configuration** link at the top of the MSWE home page.

The Configuration page consists of a series of tabbed windows, each tab having a unique function. The tabs are displayed in Figure 31 below:

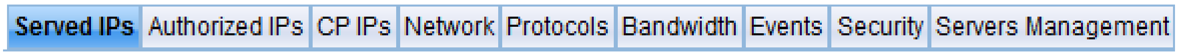


Figure 31: MSWE Configuration Page Tabs

In the event that a tabbed window is not applicable to the level of MSWE hierarchy, the tab is *grayed* and cannot be operated. See Chapter 2 for more details on the MSWE hierarchy.

The Configuration page includes the following tabbed windows – each of the windows is explained in depth in the course of this chapter:

- **Zones** (Optional): Enables you to assign a name and description for zones in the system.

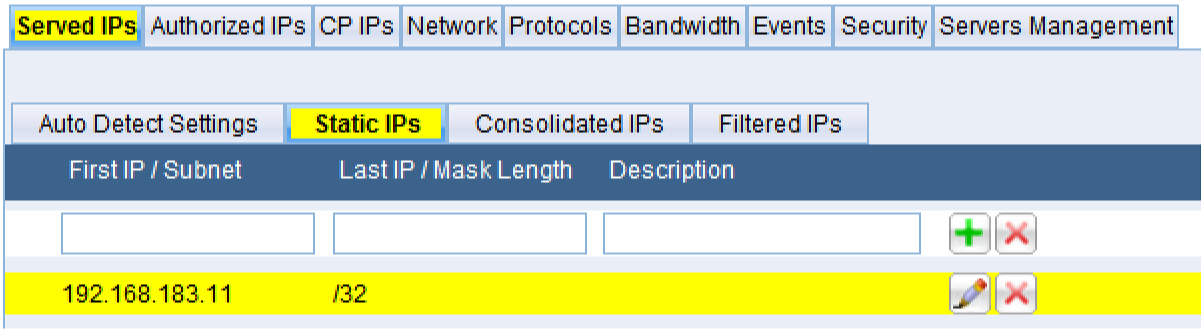
  NOTE **This option is available for customers where zones have been pre-defined.**

- **Served IPs**: Allows you to define and modify the IP addresses of MediaSwift E servers. If zones are enabled, you can define IP address ranges for each zone.
- **Authorized IPs**: Enables you to view and modify the list of the IP addresses of client workstations that are allowed to access the MSWE application, as well as the MediaSwift E system servers.
- **CP IPs:** Enables you to view and manage HM’s groups, HM groups policy, CP prefixes report thresholds and recommendation per site and BGP advertisement.
- **Network**: Enables you to define the identity of the stations authorized to manage the SNMP agent and MIB embedded in the MediaSwift E system servers, specify an NTP server that will be used to synchronize MediaSwift E system clocks and configure IP of local DNS servers.
- **Protocols**: Enables you to configure protocol-specific parameters for Bit Torrent, ED2K, and HTTP Video.
- **Bandwidth**: Allows you to limit the bandwidth allocated by the system on a time-of-day basis and control the QoE.
- **Events**: Enables you to receive notification of system events and malfunctions, either via a fault management system, or by Email.

- **Security**: Enables you to enable or disable an Access Control List (ACL) for the grid, configure TACACS servers and manage CLI password.
- **Servers Management**: This tab allows you to manage network configuration on the servers and service advance setting.

Using the Configuration Page

When a MediaSwift E configuration is modified, the tab of the updated window will be highlighted in yellow color, as illustrated by the diagram in Figure 32.



First IP / Subnet	Last IP / Mask Length	Description
192.168.183.11	/32	

Figure 32: Yellow Highlighting Signifies Modified Configuration

The yellow background is a sign that the modification has not been saved and implemented in the caching system. To deploy these changes, click the **Save** icon. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon. In both cases, the yellowed tab will revert back to its original color.

A red background, as illustrated in Figure 33 below, indicates that the modified configuration contains an invalid value. All modified parameters must fall within a range of valid values in order to be able to save the configuration.

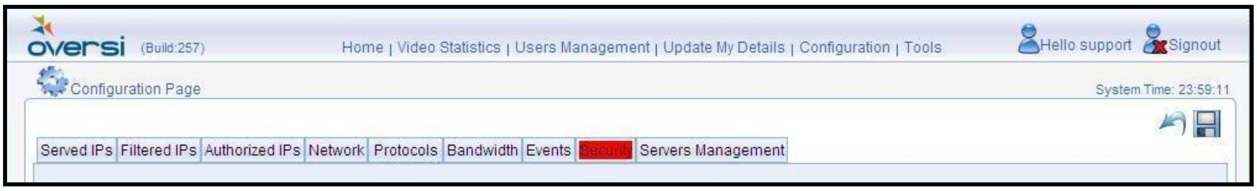


Figure 33: Red Highlighting Signifies Invalid Configuration

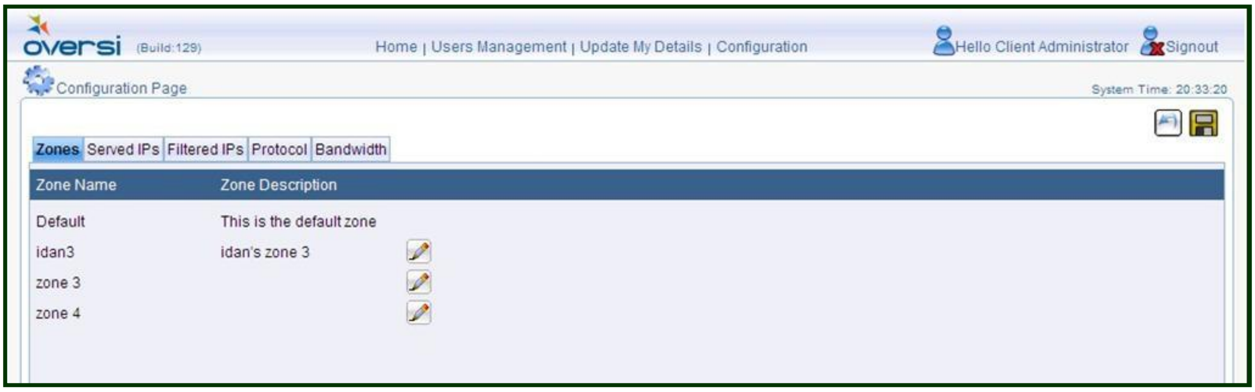
Configuring MediaSwift E Servers

Editing Zones

A zone is a logical group of IP address ranges. Subscribers within a zone receive a specific level of service that is defined by the service provider. Using zones, you can assign a session limit per user for peer-to-peer traffic, and view filtered information relevant to a specific range of IP addresses using the MSWE Home page and the Server Management page.

NOTE **This option is only available if it has been configured by Allot based on license.**

Only the name and description of a zone can be changed.

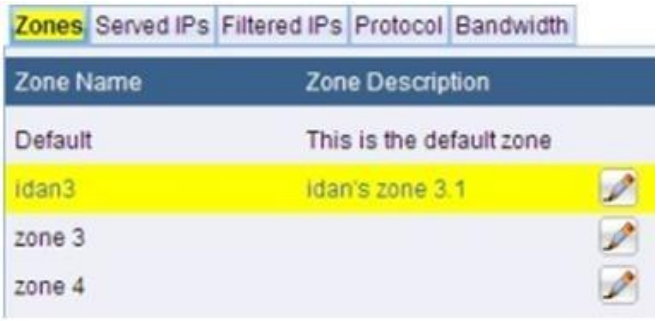


Zone Name	Zone Description
Default	This is the default zone
idan3	idan's zone 3
zone 3	
zone 4	

Figure 34: Zones Main Window

➢ To edit a zone:

1. In the **Zones** tab of the Configuration page, click the **Edit** icon next to the zone you want to edit.
2. (Optional) In the **Name** field, enter a new name for the zone.
3. (Optional) In the **Description** field, enter a new description for the zone.
4. Click **Apply** to update this zone, or **Cancel** to cancel this operation. If you click **Apply**, the new zone is modified and highlighted in yellow, as displayed in Figure 35:



Zone Name	Zone Description
Default	This is the default zone
idan3	idan's zone 3.1
zone 3	
zone 4	

Figure 35: Editing a Zone

5. If you wish to cancel the modifications and restore the original values to the updated windows, click the **Reload Configuration** icon.
6. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

Managing Served IP Addresses

The **Served IPs** tab in the Configuration page enables you to define and modify the IP addresses of clients served by the P2P Cache Server.

You can also assign an IP address range to a zone. If zones are enabled, you can select the zone for each IP address range.

There are four tabs:

- **Auto Detect Settings** – whereby the system automatically detects for new IPs at a pre-set interval (default value = 10 minutes)
- **Static IPs** – enables you to manually add networks or range of IPs
- **Consolidated IPs** – display the summarization of the Auto Detect learned IPs and Static IPs
- **Filtered IPs** – This tab allows you to define and modify the IP addresses of subscribers that will not be served from the P2P Cache (this configuration is not applicable for HTTP/Video).

Auto Detected Settings Tab

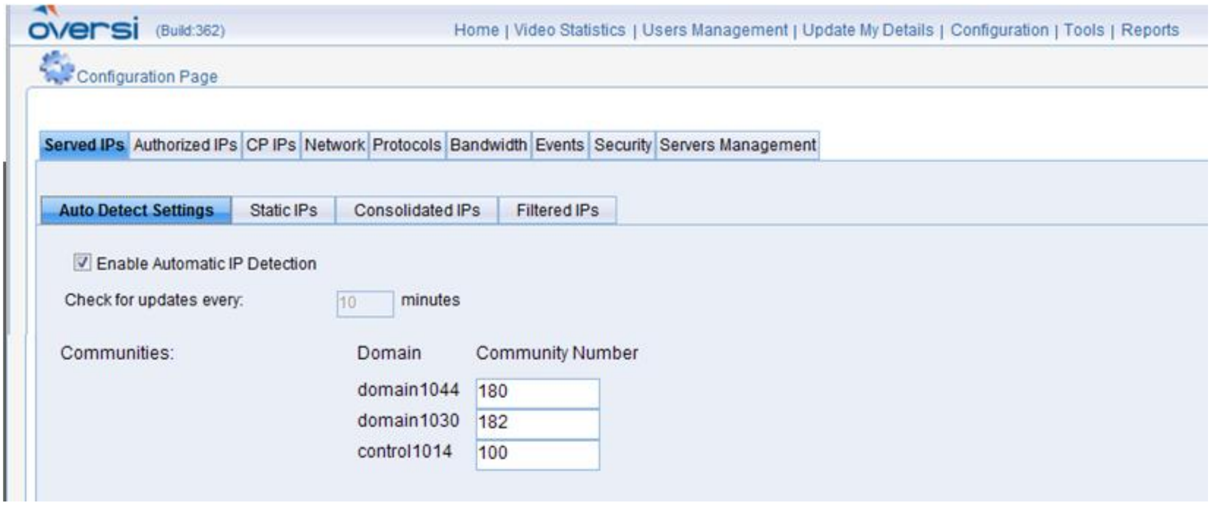
With the increase of operator's IP subnets and caching nodes area coverage (domains), it is important for service providers to use subscribers' dynamic IP address management. As oriented to service providers, the Auto Detect use BGP protocol advantages to learn internal subscribers' prefixes.

In this section you can enable the auto detect, configure the learning interval and in case of multi Domain deployment, configure the BGP communities per Domain.

On the dashboard select Configuration tab, select Servers Management tab. For the MediaSwift E Management server (i.e. AMS/CM) enable BGP-S service, to configure the BGP settings. The BGP-S service learn from Operator's BGP advertisement the subscribers prefixes and BGP communities per prefix.

In case of Out of band management and the AMS server cannot connect to the router, enable BGP-S service on any cache (or auxiliary) server which has connectivity to the router .

Only one server at each deployment can act as the BGP agent learning the subscribers' prefixes.



☑ Enable Automatic IP Detection

Check for updates every: 10 minutes

Communities:

Domain	Community Number
domain1044	180
domain1030	182
control1014	100

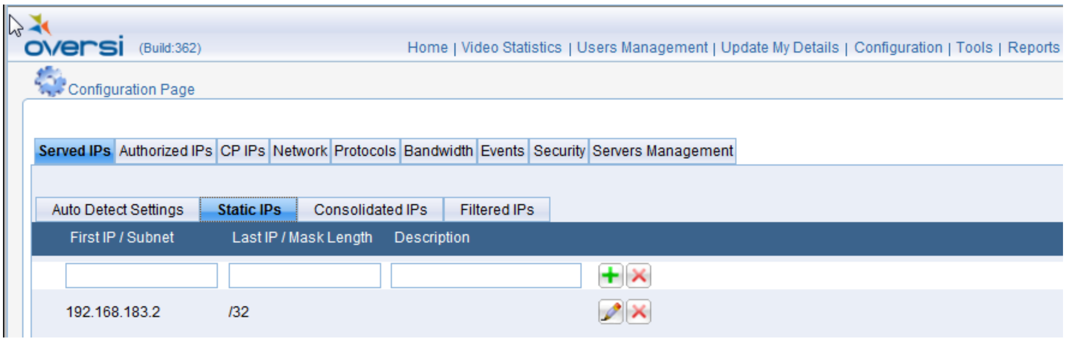
Figure 36: Auto Detect – Served/Domain Subscribers

After setting the BGP, select in the dashboard Configuration tab, select Served IPs tab, select Auto Detect Settings tab:

- **Enable Automatic IP Detection:** Selecting this check box enable the automatic detection of served IPs per system or per Domain if enabled.
- **Check for updates every:** Refresh duration interval.
- **Communities:** list the detected Domains (or communities)
  - Domain: Domain name as configured in the system.
  - Community Number: Community number as assigned by the Operator.

Static IPs Tab

In this section you can create a range of static IP addresses.



First IP / Subnet	Last IP / Mask Length	Description
192.168.183.2	/32	

Figure 37: Served Static IPs Window (without Zones)

➢ To define a Static IP address range:

1. In the **Served IPs** tab of the Configuration page, click the **Static IPs** tab.
2. Enter the IP address range in the **First IP** and **Last IP** fields, or enter the **Subnet** and **Netmask**, respectively.

NOTE: subnet mask format is not supported.

3. In the **Description** field, enter a description for the IP address range.
4. From the **Zones** drop-down list, select a zone. If zones are not enabled, the IP address range is assigned to the default zone.
5. Click **Add** to add the defined IP address range.
6. The new IP address range is highlighted in yellow, indicating that the **Served IPs** tab has been modified.
7. If you wish to cancel the modifications and restore the original values to the updated windows, click the **Reload Configuration** icon.
8. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

➢ To edit a served IP address range:

1. Select a row and click **Edit** .
2. Your selection appears in fields at the top of the Served IPs list, enabling you to modify its contents.
3. Edit the IP range fields accordingly and then click **Apply** to submit the changes, or **Cancel** to undo the modifications.
4. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
5. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

➢ To delete a served IP address range:

1. Select a row and click **Delete** .
2. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
3. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

Consolidated IPs Tab

The **Consolidated IP** display the summarization of the Auto Detect learned IPs and Static IPs.

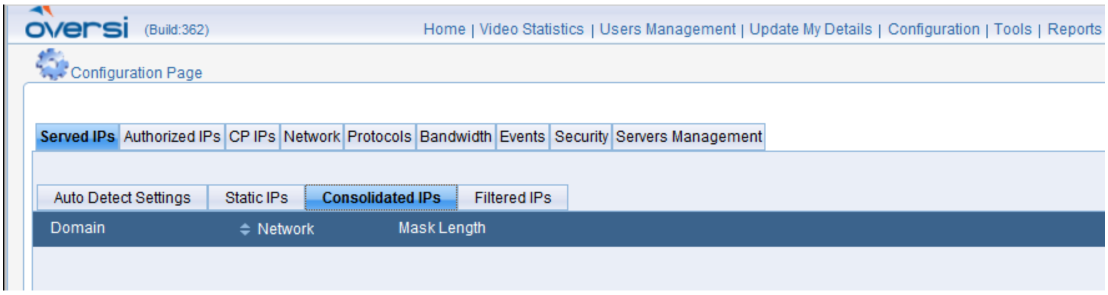


Figure 38: Consolidated IPs Window

Filtered IPs Tab

The **Filtered IPs** tab in the Configuration page enables you to define and modify the IP addresses of subscribers that will not receive P2P or HTTP caching service from the cache.

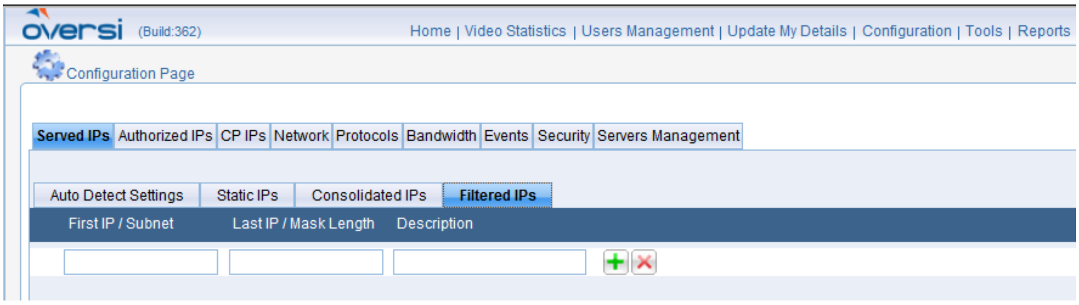


Figure 39: Filtered IPs Window

➢ To define filtered IP addresses:

1. In the **Filtered IPs** tab of the Configuration page, enter the IP address range in the **First IP** and **Last IP** fields, or enter the **Subnet** and **Netmask**, respectively.

2. In the **Description** field, enter a description for the filtered IP address range.

NOTE: subnet mask format is not supported.

3. Click **Add** to add the defined filtered IP address range.

4. The new filtered IP address range is highlighted in yellow, indicating that the **Filtered IPs** tab has been modified.

➢ To edit or delete a filtered IP range:

1. In the **Filtered IPs** tab of the Configuration page, select a row and click **Edit** or **Delete** next to the IP address range, respectively.

2. If you selected **Edit**, your selection appears in fields at the top of the Filtered IPs list, enabling you to modify its contents.

3. Edit the IP address range fields accordingly and then click **Apply** to submit the changes, or **Cancel** to cancel this operation.

4. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.

5. To deploy these changes on all servers in the grid, click **Save** .

Defining Authorized IP Addresses

The **Authorized IPs** tab enables you to view and modify the list of the IP addresses of ISP workstations that are allowed to access the MSWE application, and to access the MediaSwift E system servers for management purposes.

An example of the **Authorized IPs** tab is displayed in Figure 40.

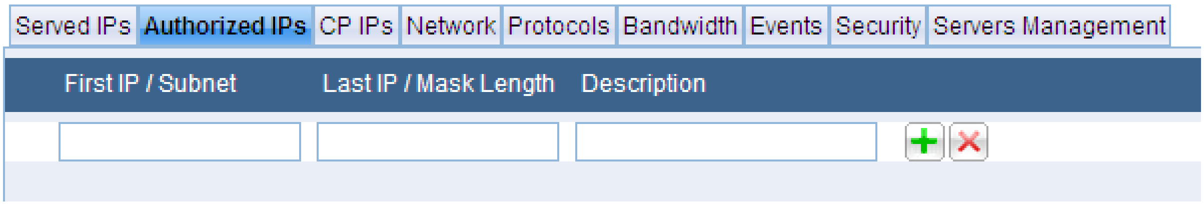


Figure 40: Authorized Managers IPs Window

➢ To define one or more authorized manager IP addresses:

1. In the **Authorized IPs** tab of the Configuration page, enter the IP address range in the **First IP** and **Last IP** fields, or enter the **Subnet** and **Netmask**, respectively.

NOTE: subnet mask format is not supported.

2. In the **Description** field, enter a description for the IP address range of the authorized managers.
3. Click **Add** ➕ to add the defined IP address range.
4. The new IP address range is highlighted in yellow, indicating that the **Authorized IPs** tab has been modified. You may continue in this fashion, adding multiple authorized managers.
5. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.
6. If you wish to save the modifications and deploy in the network, click **Save** 💾.

➢ To edit an authorized manager IP addresses:

1. To edit an authorized manager IP address: Select a row and click **Edit** ✎.
2. Your selection appears in fields at the top of the Served IPs list, enabling you to modify its contents. Click **Add** ➕ to save the redefined IP address range.
3. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.
4. If you wish to save the modifications and deploy in the network, click **Save** 💾.

➢ To delete an authorized manager IP addresses:

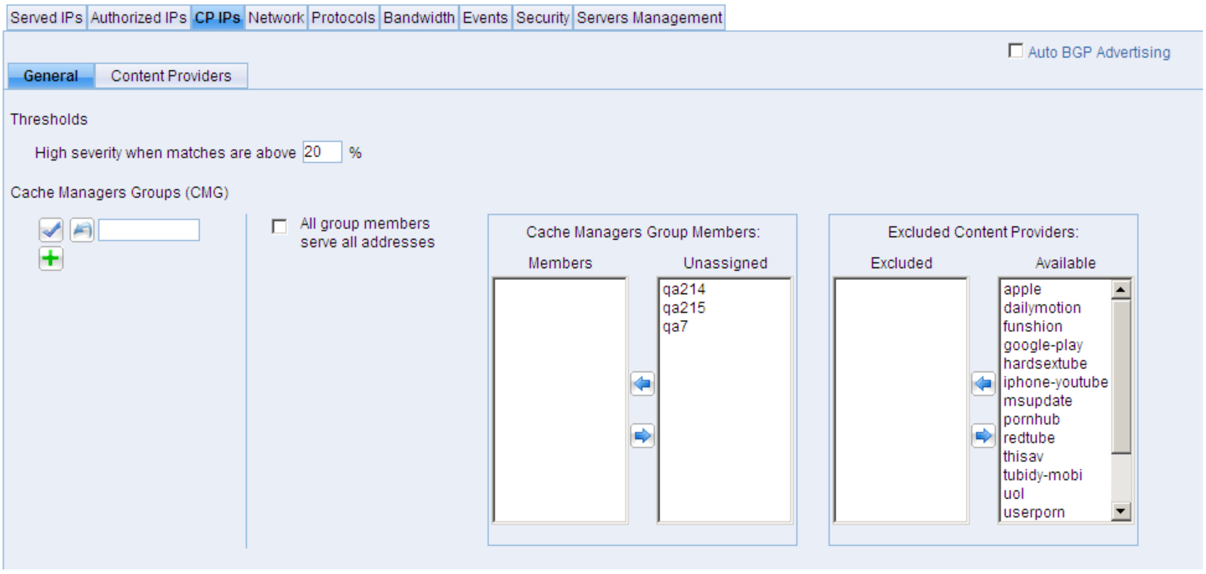
1. To delete an authorized manager IP address: Select a row and click **Delete** ✖.
2. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.
3. If you wish to save the modifications and deploy in the network, click **Save** 💾.

Content Provider IPs (CP IPs)

General Tab

This section enables you to view and manage alert threshold, HM’s (HTTP Controllers) groups and HM groups policy.

Please note: HTTP Controller is new Allot name for HTTP Manager. There are some screens that still include Cache Manager labels.



□ Auto BGP Advertising

Thresholds

High severity when matches are above 20 %

Cache Managers Groups (CMG)

□ All group members serve all addresses

Cache Managers Group Members:

Members	Unassigned
	qa214 qa215 qa7

Excluded Content Providers:

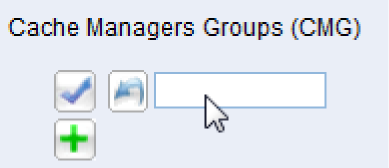
Excluded	Available
	apple dailymotion funshion google-play hardsextube iphone-youtube msupdate pornhub redtube thisav tubidy-mobi uol userporn

Figure 41: CP IPs General Tab

➢ To create a Cached Manager Group (CMGs):

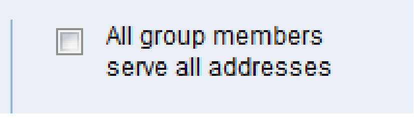
1. With the **Configuration** tabs displayed, click the **CP IPs** tab. See Figure 41 above.

2. Click the **General** sub-tab



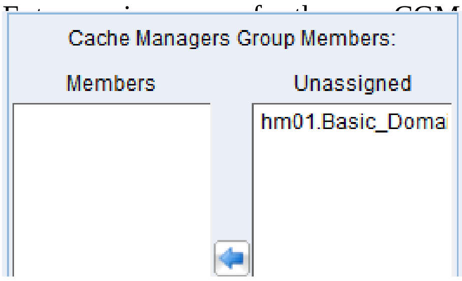
Cache Managers Groups (CMG)

3. If you want to advertise in the BGP the same prefixes on all the HM’s in the new group, check the box for “All group members serve all addresses. Not checking this box, the prefixes advertisement will be load balanced between the HM’s in this group based on weight of number of requests.



□ All group members serve all addresses

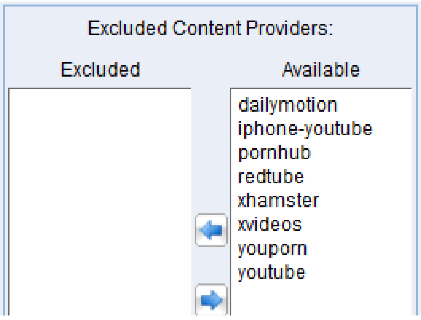
4. Enter a unique name for the new CGM.



Cache Managers Group Members:

Members	Unassigned
	hm01.Basic_Domai

5. In the CMGM pane select an assigned HM server that is displayed in the **Members** column.
6. If the HM server you want to select is unassigned, in the **Un-assigned** (right-hand) column, click the required server and then click the ⬅ button to transfer it to the left-hand box. See the section below.



Excluded Content Providers:

Excluded	Available
	dailymotion iphone-youtube pornhub redtube xhamster xvideos youporn youtube

7. In the **Excluded Content Providers** pane ensure that ONLY the required content providers are displayed in the **Available** column.

   Use the ⬅ and ➡ buttons to move the entries into the correct columns (see the section below for a detailed description).

8. Click the ➕ button to add another CMG.
9. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.
10. If you wish to save the modifications and deploy in the network, click **Save**.💾

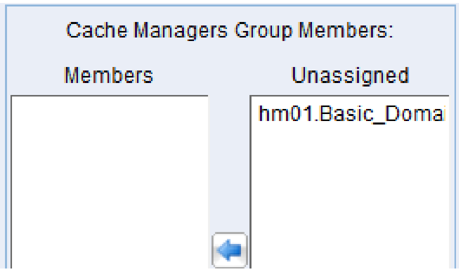
➢ To delete a CMG entry:

- Click **Delete** ☒ next to any row you wish to delete.

➢ To assign or exclude an HM Server:

1. With the **Configuration** tabs displayed, click the **CP IPs** tab. See Figure 41 above.

2. Click the **General** sub-tab



3. Select an unassigned server and then click the ⬅ button.

   OR

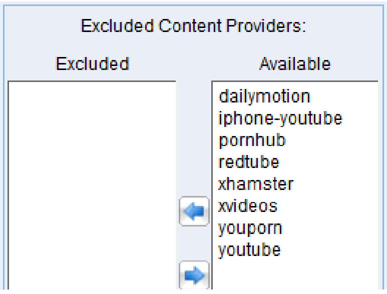
   Select the server you want un-assigned and then click the ➡ button.

4. Click **Save** 💾.

➢ To exclude a CP in the Excluded Content Provider pane:

1. With the **Configuration** tabs displayed, click the **CP IPs** tab. See Figure 41 above.

2. Click the **General** sub-tab



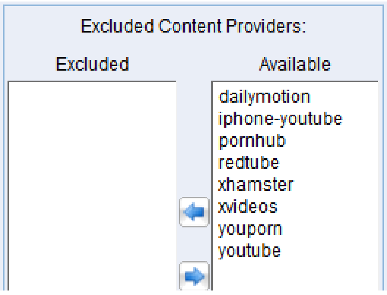
3. Select one or more entries in the **Available** column.

4. Click the ⬅ button to transfer them to the **Excluded** column.

➢ To transfer an excluded CP to the Available pane:

1. With the **Configuration** tabs displayed, click the **CP IPs** tab. See Figure 41 above.

2. Click the **General** sub-tab

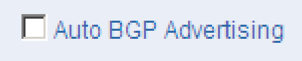


3. Select one or more entries in the **Excluded** column.

4. Click the ➡ button to transfer them to the **Available** column.

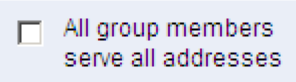
➢ Auto BGP Advertising without operator acknowledge

Select


□ Auto BGP Advertising

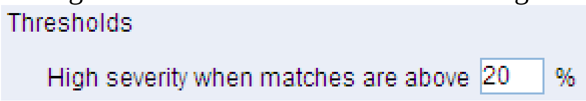
➢ BGP load balancing between HTTP Controllers in same group

Select


□ All group members serve all addresses

➢ Content Providers IP subnets change Alarm

Configure Content Provider IP Subnet change alarm threshold (default 20% change)


Thresholds

High severity when matches are above 20 %

Content Providers Tab

This screen displays the active cached content providers. The content providers that have changes are marked. You can click an entry and drill down.

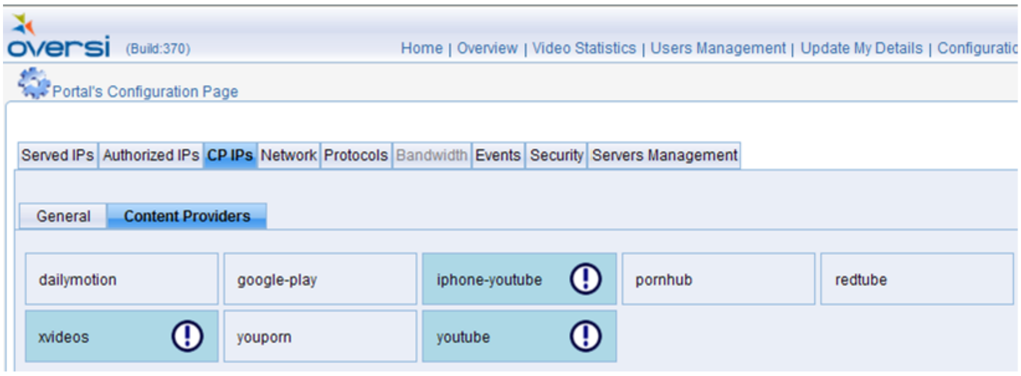
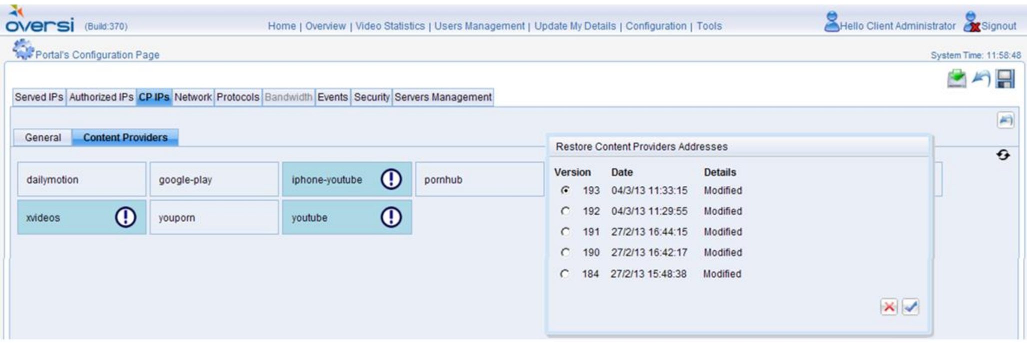


Figure 42: CP IPs Content Providers Tab

You can click an entry and drill down.

➢ Revert to Previous Content Providers Configuration

Revert to previous content providers configuration is possible by clicking on icon. Select the required configuration and approve by clicking



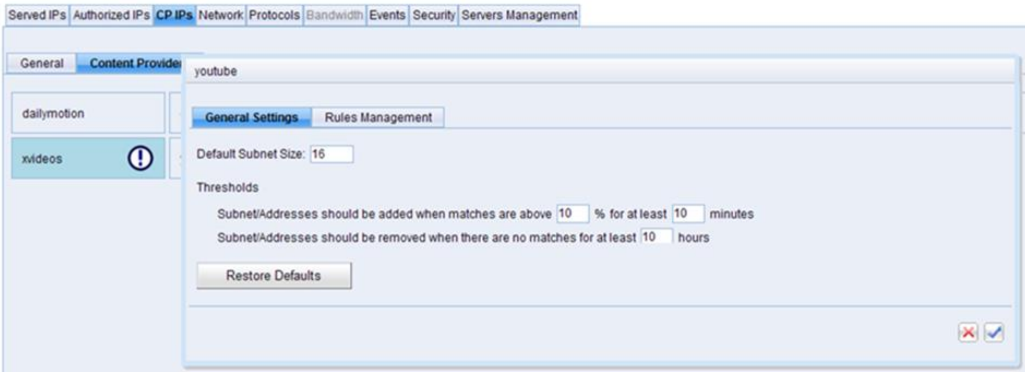
Restore Content Providers Addresses

Version	Date	Details
● 193	04/3/13 11:33:15	Modified
○ 192	04/3/13 11:29:55	Modified
○ 191	27/2/13 16:44:15	Modified
○ 190	27/2/13 16:42:17	Modified
○ 184	27/2/13 15:48:38	Modified

Figure 43: CP Previous Configuration Reload

Specific Content Provider General Tab

After clicking a content provider entry, a drill down allows per Content Provider configuration.



youtube

Default Subnet Size: 16

Thresholds

Subnet/Addresses should be added when matches are above 10 % for at least 10 minutes

Subnet/Addresses should be removed when there are no matches for at least 10 hours

Figure 44: Content Providers General Settings Tab

The General Settings tab allows configuration of content providers IP subnets thresholds:

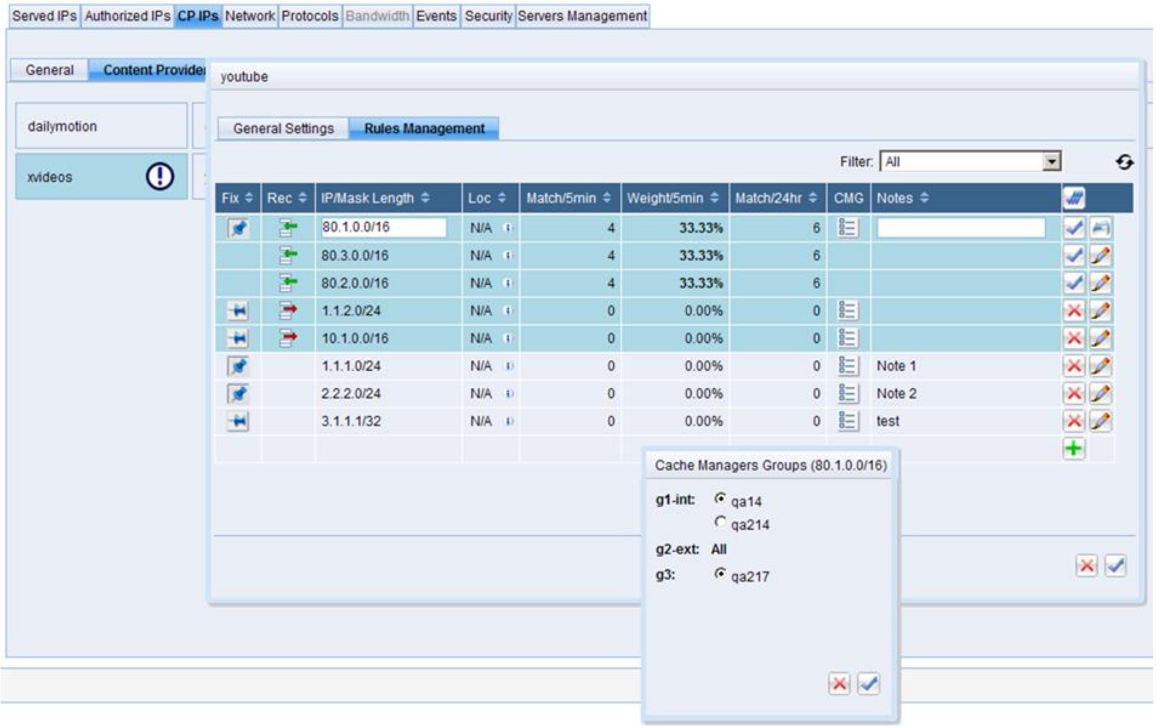
Match: set the **Percentage** of IP subnets matches during a Time window

Time: set the **Time** window for IP subnets match

History Match: set the IP subnets **Persistence Time Window** before removal

Specific Content Provider Rules Management Tab

Content provider IP subnets configuration updates.



youtube

Filter: All

Fix	Rec	IP/Mask Length	Loc	Match/5min	Weight/5min	Match/24hr	CMG	Notes
		80.1.0.0/16	N/A	4	33.33%	6		
		80.3.0.0/16	N/A	4	33.33%	6		
		80.2.0.0/16	N/A	4	33.33%	6		
		1.1.2.0/24	N/A	0	0.00%	0		
		10.1.0.0/16	N/A	0	0.00%	0		
		1.1.1.0/24	N/A	0	0.00%	0		Note 1
		2.2.2.0/24	N/A	0	0.00%	0		Note 2
		3.1.1.1/32	N/A	0	0.00%	0		test

Cache Managers Groups (80.1.0.0/16)

g1-int: ● qa14 ○ qa214

g2-ext: All

g3: ● qa217

Figure 45: Content Providers Rules Management Settings Tab

The Content Provider Rules Management Tab provides the following information:

IP Subnet and Mask: content provider IP subnet

Match/5min: Hits on this subnet during the last 5 min

Weight/5min: Hits weight **%** out of total content provider subnets hits

Match/24h: Total hits in last 24 hours

CMG: assigned HTTP Controller Group

Notes: operator notes for this subnet. When notes are added to subnet it is considered as static and will not be changed automatically.

The following are reports and actions per IP subnets (detected or added manually):

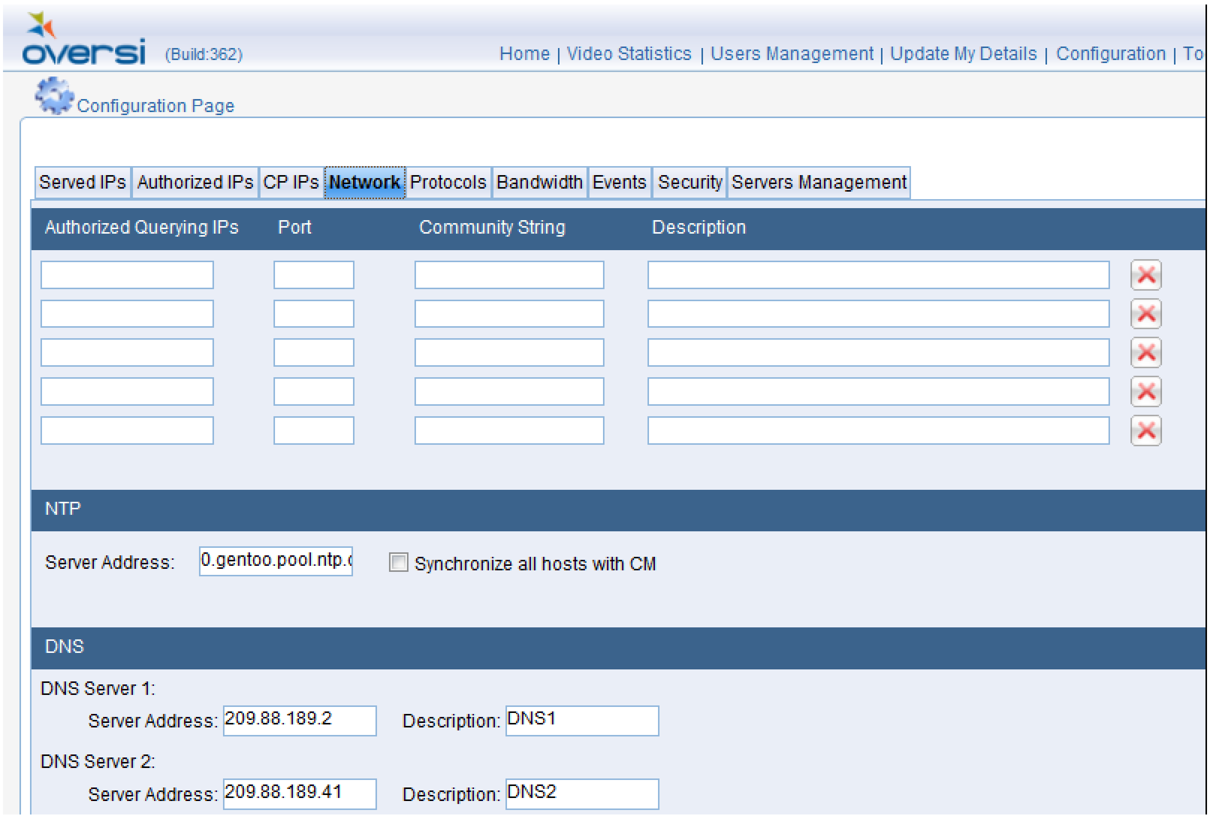
- IP Subnet recommended for **removal**. Click on red icon .
- IP Subnet recommended for **addition**. Click on green icon .
- Setting IP Subnet to **static**. Click the button. It will be changed to .

- **Add** static IP Subnet. Click the ➕ button.
- Click **Delete** ✕ on IP Subnet you wish to delete.
- IP Subnet assigned to **CMG** HTTP Controllers Group. Click the ☰ button.
- Add note to IP subnet click **Edit** ✎. Please note it will be set as static.
- **Accept** all updates and configuration by click on ✓ button.

Network Management

The **Network** tab in the Configuration page enables you to define:

- The identity of the stations that will be authorized to monitor the SNMP agent and MIB embedded in the MediaSwift E system servers.
- A Network Time Protocol (NTP) server that allows MediaSwift E servers to periodically synchronize their system clocks.



oversi (Build:362)
Home | Video Statistics | Users Management | Update My Details | Configuration | To
Configuration Page
Served IPs | Authorized IPs | CP IPs | Network | Protocols | Bandwidth | Events | Security | Servers Management

Authorized Querying IPs	Port	Community String	Description	
				✕
				✕
				✕
				✕
				✕

NTP

Server Address: 0.gentoo.pool.ntp.(□ Synchronize all hosts with CM

DNS

DNS Server 1:

Server Address: 209.88.189.2 Description: DNS1

DNS Server 2:

Server Address: 209.88.189.41 Description: DNS2

Figure 46: Network Management Screen

➢ To authorize an SNMP monitoring station:

1. In the Network tab of the Configuration page, select a row, and enter the **Authorized Querying IP** Address of the station, the **Listening Port** number, the **SNMP Community String,** and a **Description** of the management station.

2. Click **Delete** ✖ next to any row you wish to delete.

3. To save your configuration, click **Save** 💾.

➢ To specify a Network Time Protocol (NTP) server:

1. In the Network tab of the Configuration page, enter the IP Address of your Network Time Protocol server in the NTP section of the window.

2. If you want all servers to synchronize themselves with the MSWE's Central Management (CM) Server, enable the **Synchronize all hosts with CM** check box. The CM server will act as an NTP proxy for the system servers. If the check box is disabled, all servers will synchronize their clocks directly with the NTP server that you specify.

3. To save your configuration, click **Save** 💾.

➢ To specify a DNS Server:

1. Ensure the Network tab of the Configuration page is displayed.

2. In the DNS pane, enter the IP Address of your DNS server.

3. To save your configuration, click **Save** 💾.

Protocols Tab

The **Protocols** tab in the Configuration page enables you to configure protocol-specific parameters for BitTorrent, ED2K and Video:

- For both BitTorrent and ED2K, you can configure the system to prevent single sourcing (that is, you can prevent caching for P2P files that do not have multiple sources).
- Hash blocking can be configured for BitTorrent and ED2K.

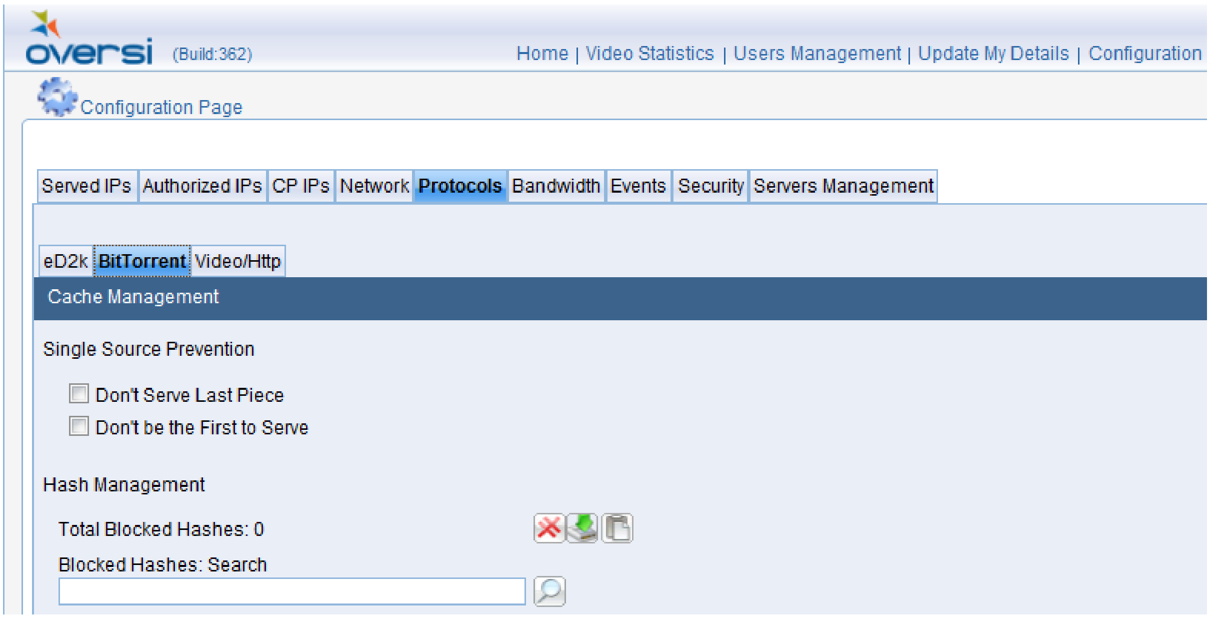
> **NOTE** **The hash block should be used to implement the "Notice and Take Down" procedure required by law. The hash block option is applied based on the ED2K file hash or BitTorrent hash. If you have received a notice of copyright infringement or illegal content, you should receive the correct hash from the notification entity, and use the hash blocking procedure as defined below for the respective protocol, in order to properly invoke the block operation.**

- For Video, you can configure video replacements and videos that will not be served from the cache.

The **Protocols** tab is divided into secondary tabs, by protocol type.

BitTorrent Tab

The **BitTorrent** secondary tab is dedicated to setting parameters for traffic being distributed using the BitTorrent protocol.



Cache Management

Single Source Prevention

□ Don't Serve Last Piece

□ Don't be the First to Serve

Hash Management

Total Blocked Hashes: 0

Blocked Hashes: Search

Figure 47: Protocol Management BitTorrent Window

➢ To configure BitTorrent:

1. In the **Single Source Prevention** area, select one of the following:
   - **Don’t Serve Last Part:** Ensures that the last part of all files is not served.
   - **Don't be the First to Serve:** Ensures that clients without any part of the file are not served by the cache. Only clients that receive at least one piece from other sources will continue to be served from the cache.
2. In the **Hash Management** area, enter a hash to block or search for, and then click **Add** or **Search**, respectively. Using the **Export** icon, you may export a list of blocked hashes.

NOTE **Bit Torrent hashes must be 40 hexadecimal characters in length.**

3. To delete all the blocked hashes, click **Delete All**. The system asks you to confirm this action, displaying a dialog box with the question: "Are you sure you want to delete all blocked hashes?"
4. Click **OK** to proceed or click **Cancel** to abort this operation.
5. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.
6. To deploy these changes on all servers in the grid, click **Save**.

The **Top Seen Trackers** area displays a list of top trackers compiled by Allot P2P Demand Identifiers (PDIs). The following data are supplied for each tracker in the list:

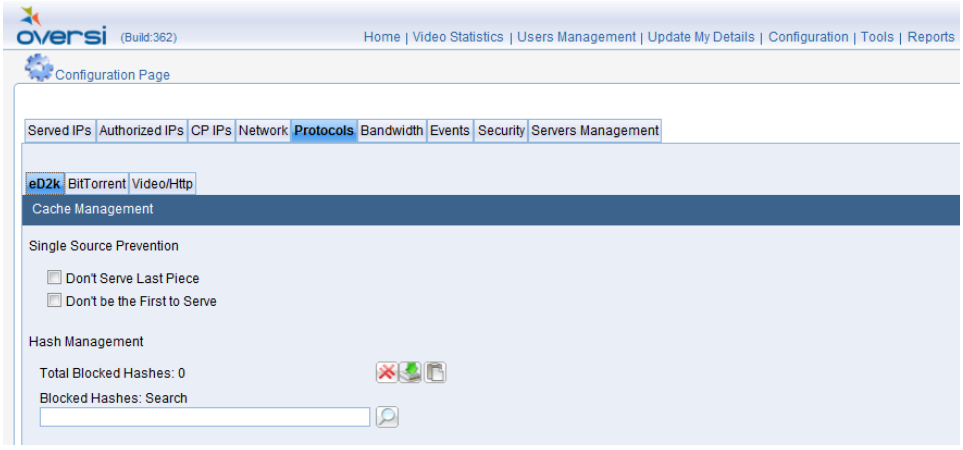
- **Tracker IP:** The IP Address of the BitTorrent tracker.

- **24H Requests:** The number of client requests handled by the tracker during the last 24 hour period.
- **Total Requests:** The number of client requests handled since the last tracker reset.
- **Current Clients:** The number of clients served during the last 30 minutes.
- **Last Request Clients:** The date and time of the last request handled by the tracker.

This information should be verified from time to time, and the traffic of the top trackers should be redirected to the Peer Manager (PM) Server.

eD2K Tab

The **eD2K** secondary tab is dedicated to setting parameters for traffic being distributed using the eDonkey 2000 file sharing protocol.



Single Source Prevention

☐ Don't Serve Last Piece

☐ Don't be the First to Serve

Hash Management

Total Blocked Hashes: 0

Blocked Hashes: Search

Figure 48: Protocol Management eDonkey 2000 Window

➢ To configure eD2k:

1. In the **Single Source Prevention** area, select one of the following:
   - **Don’t Serve Last Part:** Ensures that the last part of all files is not served.
   - **Don't be the First to Serve:** Ensures that clients without any part of the file are not served.
2. In the **Hash Management** area, enter a hash to block or search for, and then click **Add** ✚ or **Search** 🔍, respectively. Using the **Export** ⬇ icon, you may export a list of blocked hashes.

NOTE **ED2K hashes must be 32 hexadecimal characters in length.**

3. To delete all the blocked hashes, click **Delete All** ✖. The system asks you to confirm this action, displaying a dialog box with the question: "Are you sure you want to delete all blocked hashes?"
4. Click **OK** to proceed or click **Cancel** to abort this operation.

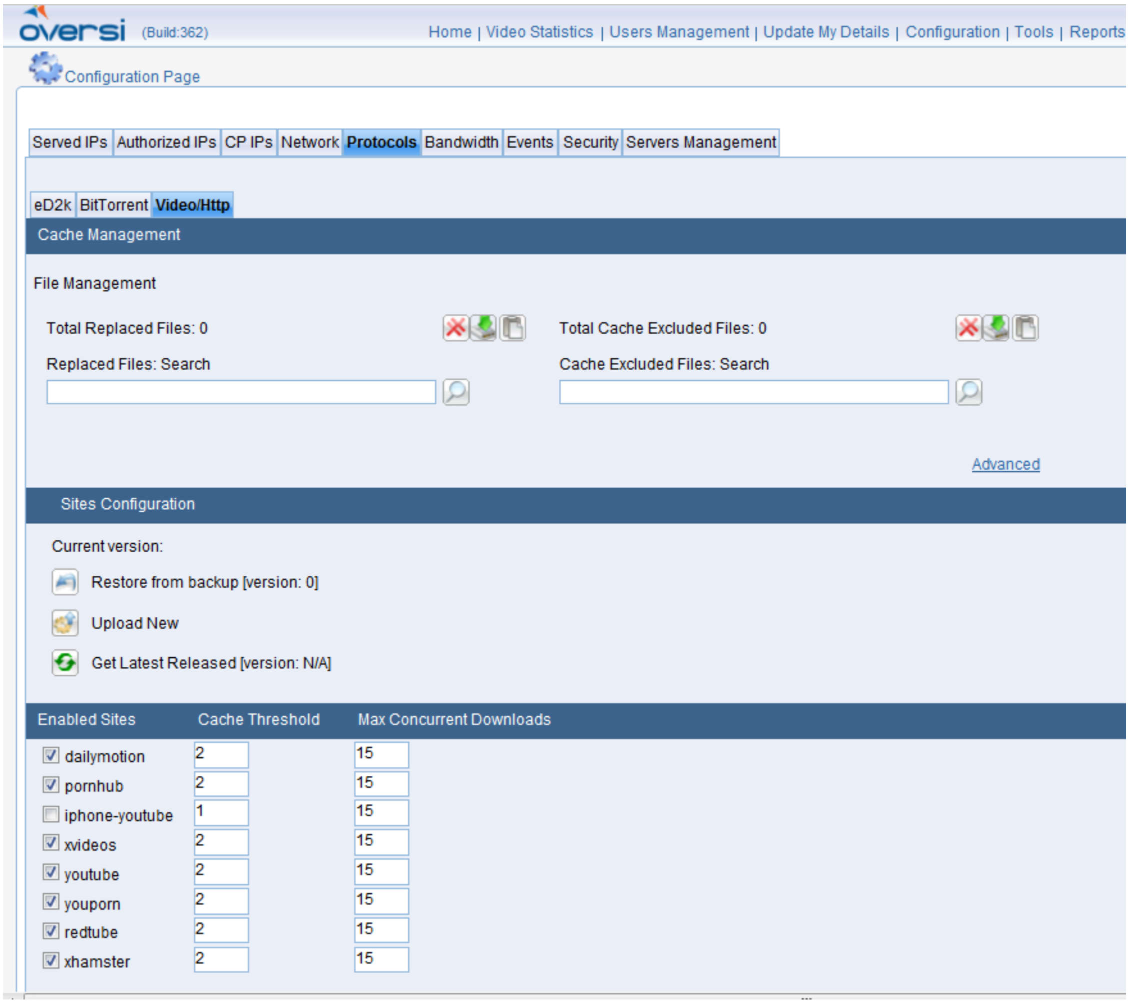
5. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.

6. To deploy these changes on all servers in the grid, click **Save** .

Video/HTTP Tab

The **Video/Http** secondary tab is dedicated to setting parameters for traffic being distributed using the HTTP protocol for video, file downloading and SW update/download applications. The tabbed window, as displayed in Figure 49 below, is divided into three operational areas:

- Cache Management
- Sites Configuration
- Enabled Sites


oversi (Build:362)
Home | Video Statistics | Users Management | Update My Details | Configuration | Tools | Reports
Configuration Page
Served IPs | Authorized IPs | CP IPs | Network | Protocols | Bandwidth | Events | Security | Servers Management
eD2k | BitTorrent | Video/Http
Cache Management
File Management
Replaced Files: Search
Cache Excluded Files: Search
Advanced
Sites Configuration
Current version:
Restore from backup [version: 0]
Upload New
Get Latest Released [version: N/A]

Total Replaced Files: 0

Total Cache Excluded Files: 0

Enabled Sites	Cache Threshold	Max Concurrent Downloads
☑ dailymotion	2	15
☑ pornhub	2	15
□ iphone-youtube	1	15
☑ xvideos	2	15
☑ youtube	2	15
☑ youporn	2	15
☑ redtube	2	15
☑ xhamster	2	15

Figure 49: Protocol Management Internet Video/HTTP

Cache Management

The **Cache Management** area of the **Video/Http** tabbed window is dedicated to controlling access to videos and other HTTP-based content.

You can control the access to specific files from the cache in two ways:

- **Replaced Files.** Files that are not allowed to be displayed in your territory due to government regulations or for other legal reasons, can be replaced with a default file, typically displaying a short message.
- **Cache Excluded.** Alternatively, you can select specific files that will not be served by the cache and will be always served by the original site.

NOTE **Consult Allot Customer Support for recommendations regarding a default replacement file (typically a video file). This feature is available for all sites.**

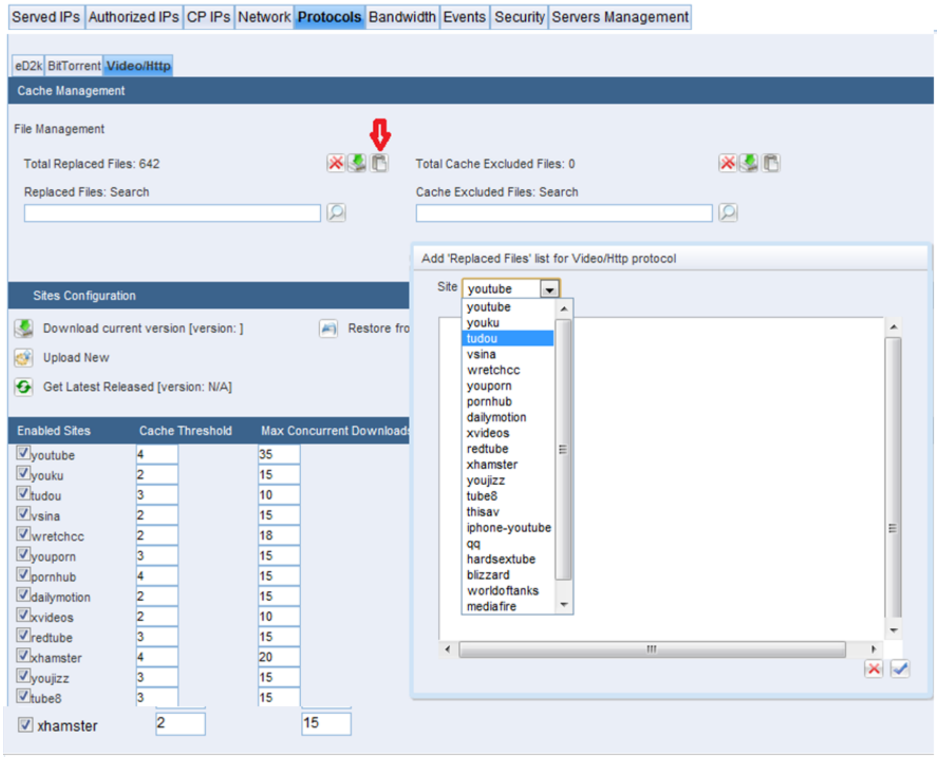
➢ To replace a file:

1. In the **Replace Files** field, enter the File ID of the file to be replaced. This is the string that identifies the file in the original site. Then click **Add** ➕. You may continue in this fashion, adding multiple replaced files. To find out the File ID, use the procedure below.
2. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
3. If you wish to save the modifications and deploy them in the network, click **Save**

➢ To replace a list of files:

The system includes optional replace files from a list per site.

1. In the **Replace Files** field, select the list bottom (marked by red arrow on the figure below).



Total Replaced Files: 642

Replaced Files: Search

Total Cache Excluded Files: 0

Cache Excluded Files: Search

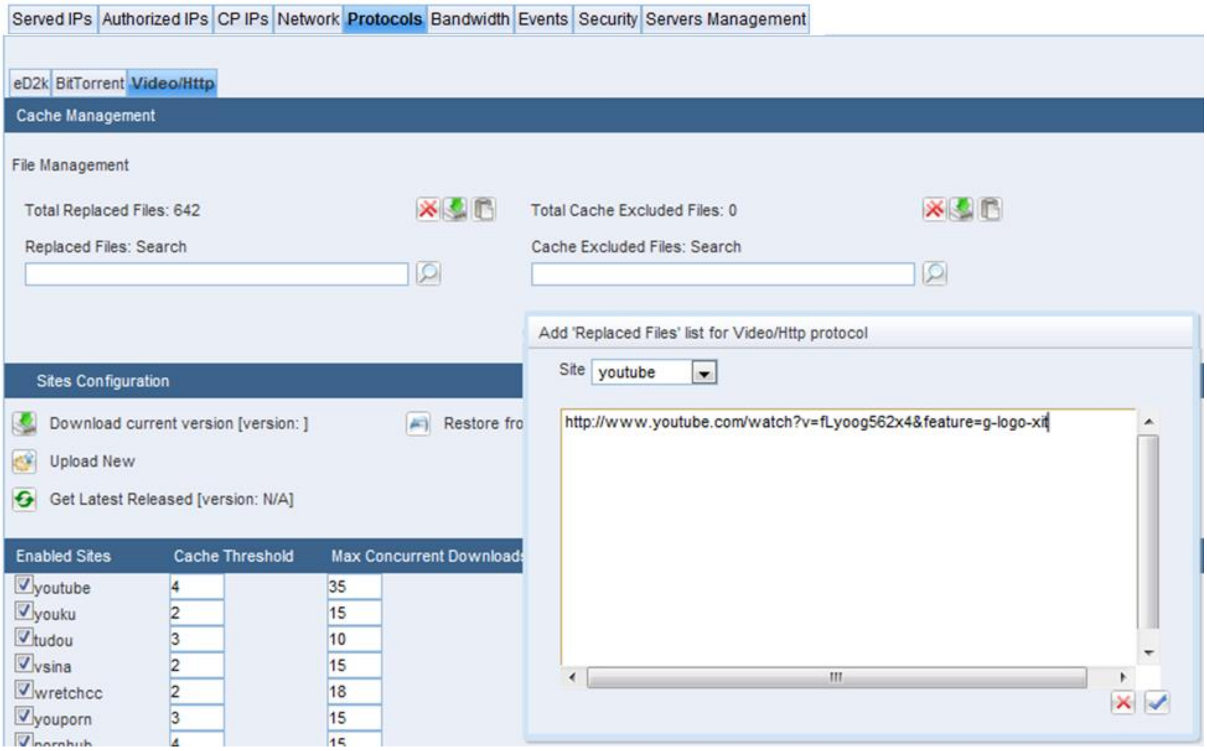
Add 'Replaced Files' list for Video/Http protocol

Site: youtube

Enabled Sites	Cache Threshold	Max Concurrent Download
☑ youtube	4	35
☑ youku	2	15
☑ tudou	3	10
☑ vsina	2	15
☑ wretchcc	2	18
☑ youporn	3	15
☑ pornhub	4	15
☑ dailymotion	2	15
☑ xvideos	2	10
☑ redtube	3	15
☑ xhamster	4	20
☑ youjizz	3	15
☑ tube8	3	15
☑ xhamster	2	15

Figure 50: Protocol Management Video/HTTP – Replace list

2. Select the site you wish to replace with a list
3. Enter list of urls (see figure below) – apply only for YouTube


Served IPs | Authorized IPs | CP IPs | Network | Protocols | Bandwidth | Events | Security | Servers Management
eD2k | BitTorrent | Video/Http
Cache Management
File Management
Sites Configuration
Download current version [version:]
Restore fro
Upload New
Get Latest Released [version: N/A]

Total Replaced Files: 642

Replaced Files: Search

Total Cache Excluded Files: 0

Cache Excluded Files: Search

Add 'Replaced Files' list for Video/Http protocol

Site: youtube

http://www.youtube.com/watch?v=fLyoog562x4&feature=g-logo-xit

Enabled Sites	Cache Threshold	Max Concurrent Download
☑ youtube	4	35
☑ youku	2	15
☑ tudou	3	10
☑ vsina	2	15
☑ wretchcc	2	18
☑ youporn	3	15
☑ pornhub	4	15

Figure 51: Protocol Management Video/HTTP – YouTube Replace list

4. Click on the **OK** ✓ icon to exit the dialog box. The selected urls will be added to the Replaced Files list or the Cache Excluded list as selected.
5. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** 💾.

➢ To delete a replaced file ID from the list:

1. In order to specify the replaced file to be deleted, you must search for the file ID. In the **Replaced Files** field, enter the ID of the file to be replaced.
2. Then click **Search** 🔍. If the file ID is found in the replaced files list, it will appear in a line below the search field, together with a **Delete** ☒ icon.
3. Click on **Delete** ☒ to remove the file ID to the list.
4. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.
5. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** 💾.

➢ To delete all replaced files:

1. To delete all the replaced files, click **Delete All** . The system asks you to confirm this action, displaying a dialog box with the question: "Are you sure you want to delete all replaced files?"
2. Click **OK** to proceed or click **Cancel** to abort this operation.
3. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
4. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

➢ To export a list of all replaced files:

- Click the **Export** icon in order to export a text file containing a list of the files IDs.

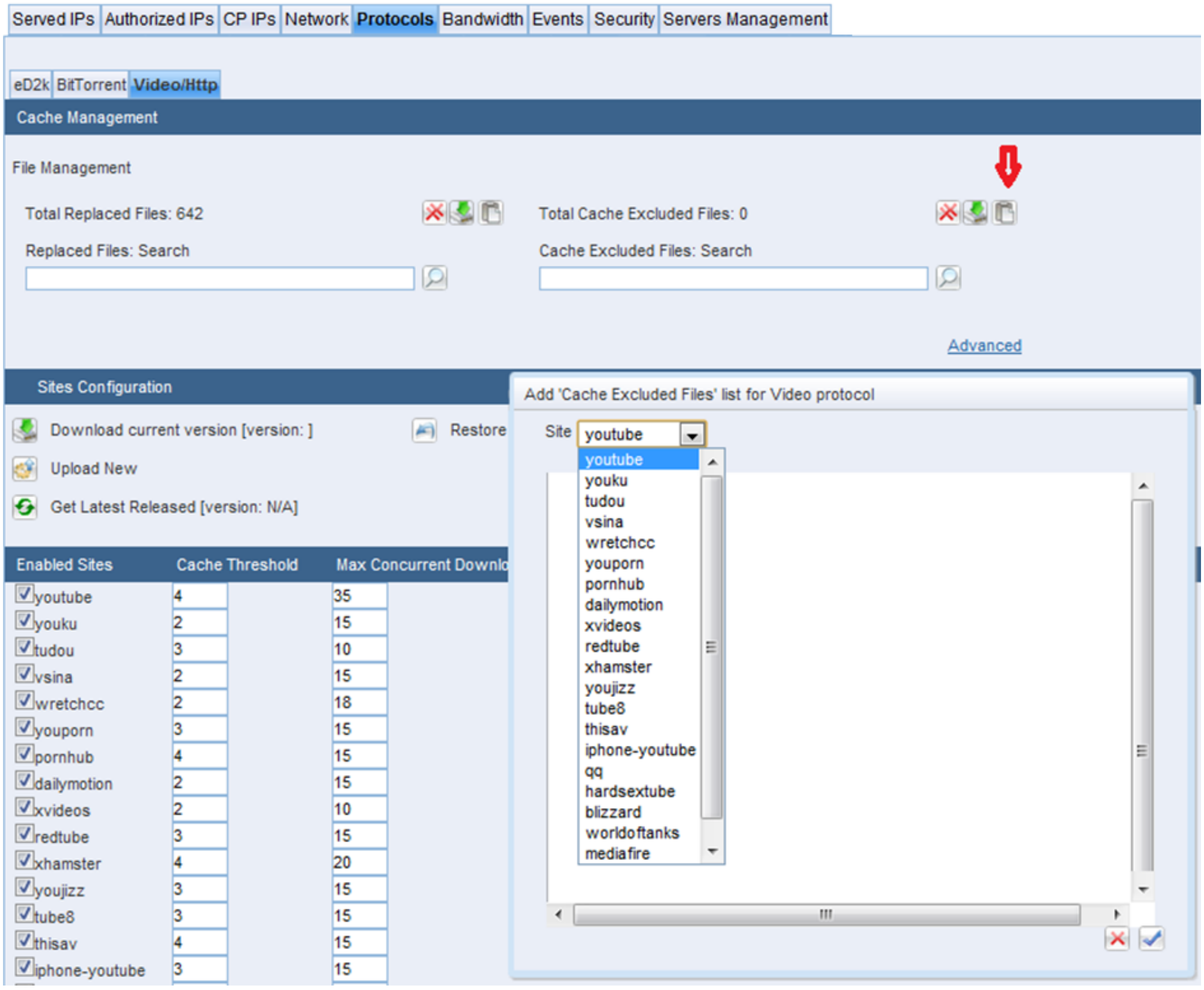
➢ To exclude a file from caching:

1. In the **Cache Excluded Files** field, enter the ID of the file to be excluded from caching. This is the string that identifies the file in the original site. Then click **Add** . You may continue in this fashion, adding multiple files to the exclusion list.
2. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
3. If you wish to save the modifications and deploy in the network, click **Save** .

➢ To exclude a list of files:

The system includes optional exclude files from a list per site.

1. In the **Exclude Files** field, select the list bottom (marked by red arrow on the figure below).



Cache Management

File Management

Total Replaced Files: 642

Total Cache Excluded Files: 0

Replaced Files: Search

Cache Excluded Files: Search

Sites Configuration

Download current version [version:]

Restore

Upload New

Get Latest Released [version: N/A]

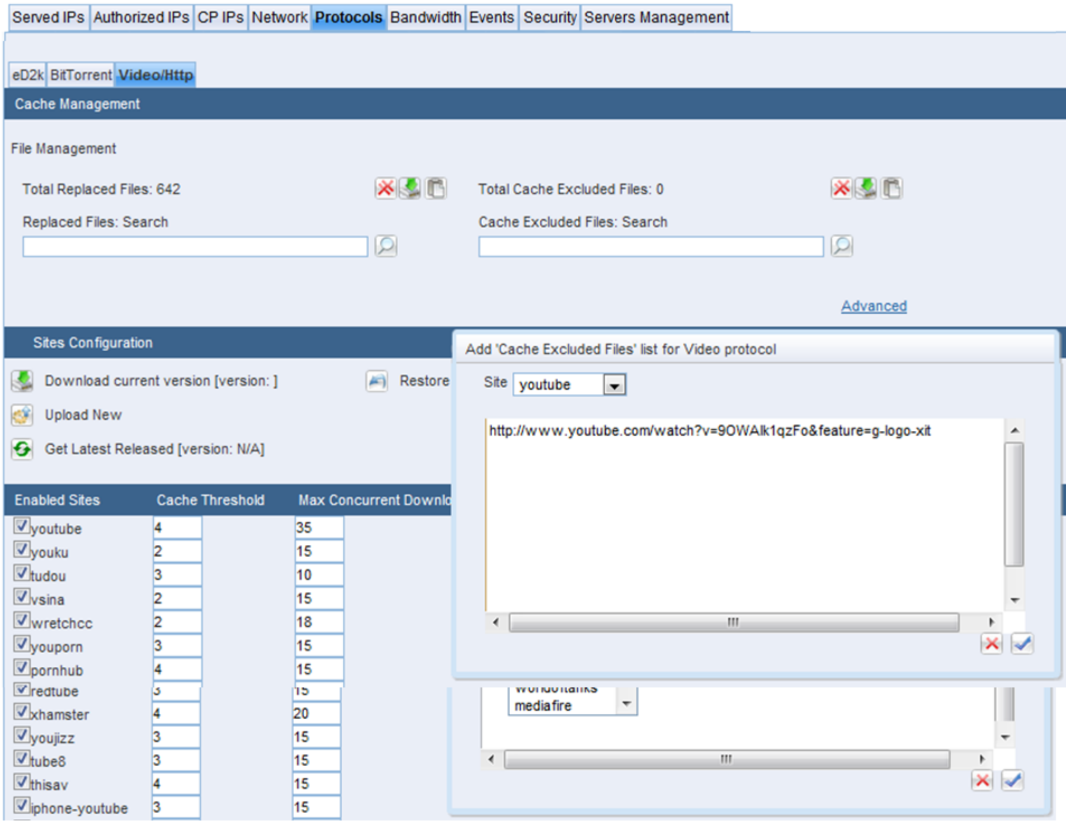
Add 'Cache Excluded Files' list for Video protocol

Site: youtube

Enabled Sites	Cache Threshold	Max Concurrent Downlo
☑ youtube	4	35
☑ youku	2	15
☑ tudou	3	10
☑ vsina	2	15
☑ wretchcc	2	18
☑ youporn	3	15
☑ pornhub	4	15
☑ dailymotion	2	15
☑ xvideos	2	10
☑ redtube	3	15
☑ xhamster	4	20
☑ youjizz	3	15
☑ tube8	3	15
☑ thisav	4	15
☑ iphone-youtube	3	15

Figure 52: Protocol Management Video/HTTP – Exclude list

2. Select the site you wish to exclude with a list.
3. Enter list of URLs (see figure below).



Cache Management

File Management

Total Replaced Files: 642

Replaced Files: Search

Total Cache Excluded Files: 0

Cache Excluded Files: Search

Sites Configuration

Download current version [version:]
Restore
Upload New
Get Latest Released [version: N/A]

Enabled Sites	Cache Threshold	Max Concurrent Downlo
☑ youtube	4	35
☑ youku	2	15
☑ tudou	3	10
☑ vsina	2	15
☑ wretchcc	2	18
☑ youporn	3	15
☑ pornhub	4	15
☑ redtube	3	15
☑ xhamster	4	20
☑ youjizz	3	15
☑ tube8	3	15
☑ thisav	4	15
☑ iphone-youtube	3	15

Add 'Cache Excluded Files' list for Video protocol

Site: youtube

http://www.youtube.com/watch?v=9OWAlk1qzFo&feature=g-logo-xit

Figure 53: Protocol Management Video/HTTP – YouTube Exclude list

4. Click on the **OK** ✓ icon to exit the dialog box. The selected urls will be added to the Exclude Files list or the Cache Excluded list as selected.

5. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** 💾.

➢ To delete a file from the cache exclusion list:

1. In order to specify the file to be deleted from the cache exclusion list, you must search for the file ID. In the **Cache Excluded Files**, enter the ID of the file to be deleted from the cache exclusion list.

2. Then click **Search** 🔍. If the file ID is found in the cache exclusion list, it will appear in a line below the search field, together with a **Delete** ✗ icon.

3. Click on **Delete** ✗ to remove the file ID to the list.

4. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** ↶ icon.

5. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** 💾.

➢ To delete all files from the cache exclusion list:

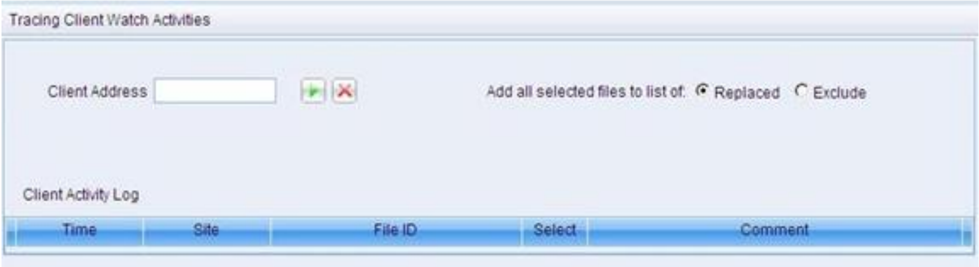
1. To delete all the files from the cache exclusion list, click **Delete All** . The system asks you to confirm this action, displaying a dialog box with the question: "Are you sure you want to delete all excluded files?"
2. Click **OK** to proceed or click **Cancel** to abort this operation.
3. If you wish to cancel the modifications and restore the original values to the updated windows, click on the **Reload Configuration** icon.
4. If you wish to save the modifications and deploy these changes on all servers in the grid, click **Save** .

➢ To export a list of all the files on the cache exclusion list:

- Click the **Export** icon in order to export a text file containing a list of the file IDs.

➢ To identify the file ID of a specific file or video:

1. The file ID is typically a string generated by the video or HTTP site at which the file can be accessed. To identify this file ID (in order to replace or exclude the file in the cache), use a regular internet-connected PC to view or download the file – a “Client PC.”.
2. Record the IP address of the Client PC for further use.
3. Click on the **Advanced** link in the Cache Management section. A dialog box, shown in Figure 54 below, will appear.



Tracing Client Watch Activities

Client Address

Add all selected files to list of: ● Replaced ○ Exclude

Client Activity Log

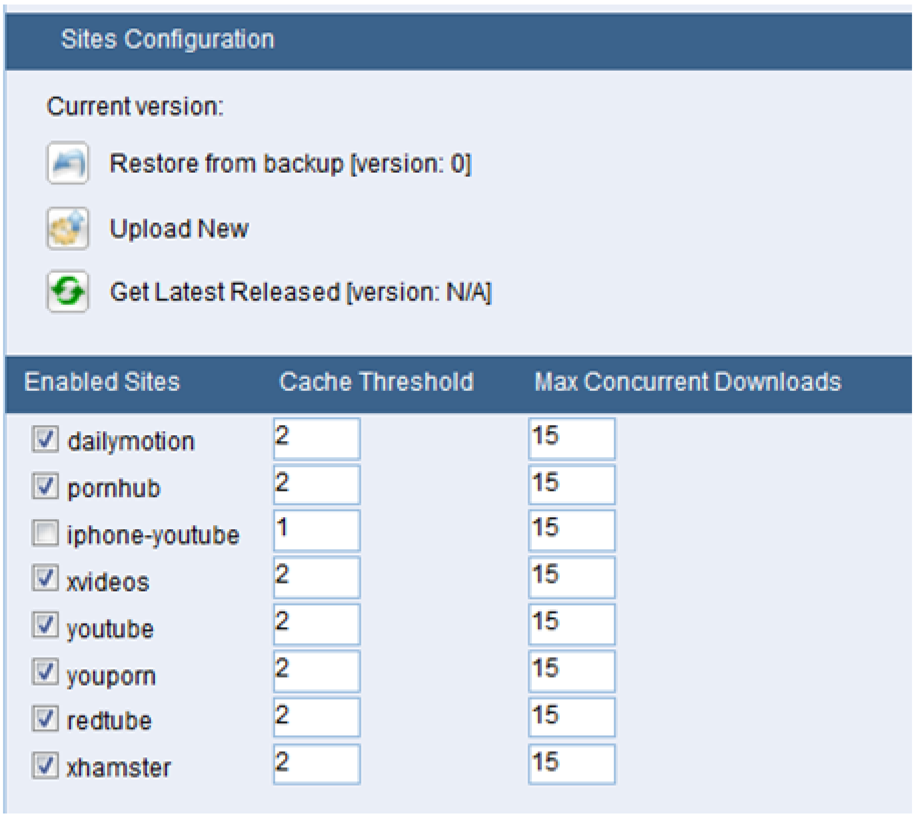
Time	Site	File ID	Select	Comment

Figure 54: Using Tracing Tool to Identify File IDs

4. Enter the IP address of the Client PC in the **Client Address** field, and click on the **Start** . Icon to begin a trace.
5. Using the PC, play the videos or download the files to be identified. The file IDs of each file accessed will appear in the Client Activity Log.
6. Select the file IDs to be replaced or excluded, and then select whether the file is to be **Replaced** or **Excluded** using the radio button.
7. To end the trace, click on the **Stop** icon.
8. Click on the **OK** icon to exit the dialog box. The selected file IDs will be added to the Replaced Files list or the Cache Excluded list as selected.

Sites Configuration

The **Sites Configuration** area of the **Video/Http** tabbed window is used to update the MSWE's site configuration file. The site configuration file is an Allot -supplied file containing per-site information on:



Sites Configuration

Current version:

Restore from backup [version: 0]

Upload New

Get Latest Released [version: N/A]

Enabled Sites	Cache Threshold	Max Concurrent Downloads
☑ dailymotion	2	15
☑ pornhub	2	15
□ iphone-youtube	1	15
☑ xvideos	2	15
☑ youtube	2	15
☑ youporn	2	15
☑ redtube	2	15
☑ xhamster	2	15

Figure 55: HTTP/Video Sites Configuration

The Sites Configuration section displays the version number of the currently installed site configuration file, and allows the operator to replace the currently installed file in three ways:

- Restoring a back-up of the previously installed file.
- Uploading a new site configuration file sent to the provider by Allot.
- Downloading a new site configuration file available on Allot 's servers. This feature will be available in a future version.

➢ To restore a backup of the previously installed configuration file:

- Click on the **Restore from Backup** icon. The system restores the configuration file whose version is displayed in the window.

➢ To upload a new version of the configuration file that has been shipped by Allot:

1. Click on the **Upload New** icon. The system displays a dialog box containing a file browser.

2. Select the new configuration file, and upload the file into the system. Following the upload, the version number of the new file should appear in the “Current version” field.

Enabled Sites

The **Enabled Sites** area of the **Video/Http** tabbed window allows the operator to select the internet sites that will receive caching support. For each enabled site, you can control the following parameters:

- **Cache Threshold**: The number of requests for a specific file that will trigger a download of the file to the caching system.
- **Max Concurrent Downloads**: The maximum number of files that the caching system can download concurrently from the enabled site.

➢ To enable a web site for caching and configure the downloading activity from the site:

1. Click the check box adjacent to the name of the desired web site to enable the site for caching.
2. Enter the number of requests for a single file that will trigger a download of the file to the cache in the **Cache Threshold** field.
3. In the **Max Concurrent Downloads** field, enter a number representing the maximum number of downloads the caching system can perform simultaneously.
4. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.
5. To deploy these changes on all servers in the grid, click **Save** .

Bandwidth Control

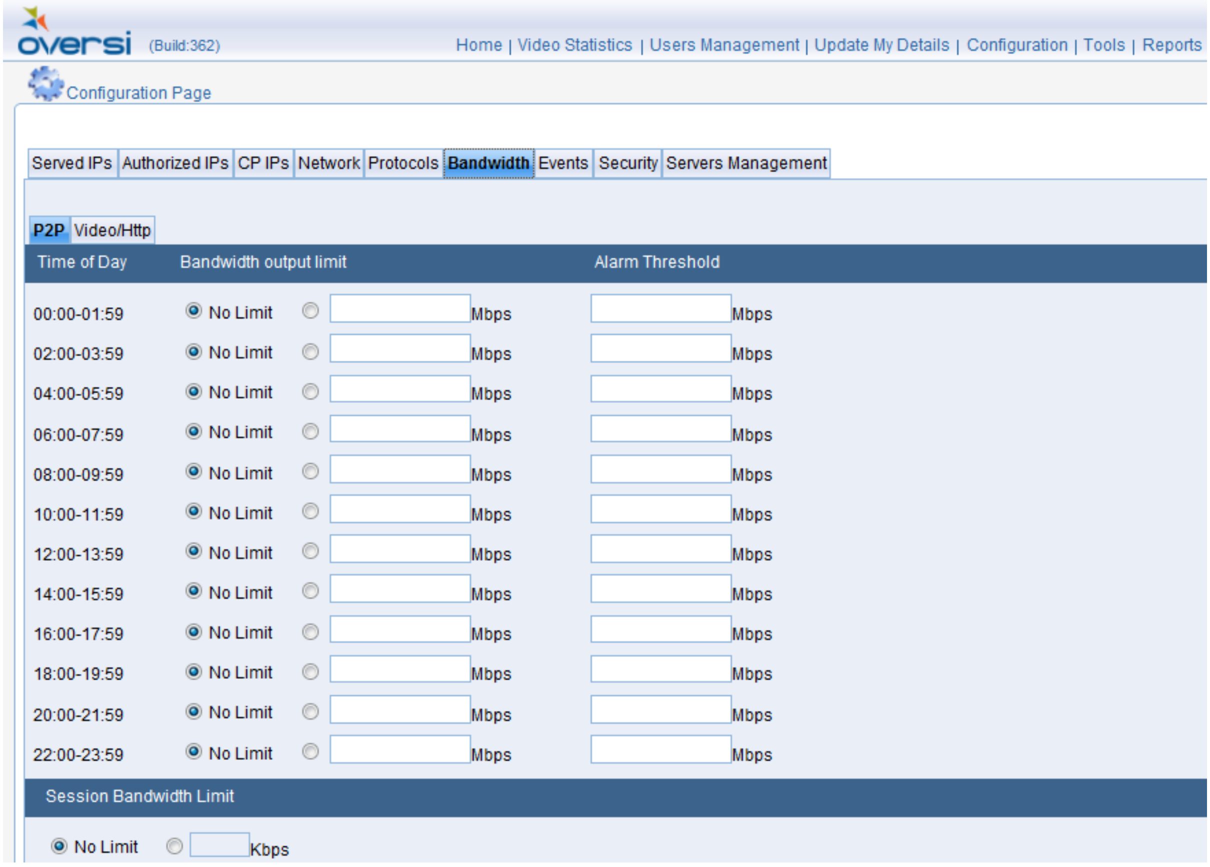
The **Bandwidth** tab in the Configuration page enables you to limit the bandwidth allocated by the system on a time-of-day basis. For example, the system can be configured to relieve congestion in access networks during business hours by limiting access to multimedia content.

The tab allows you to define throughput thresholds that will raise an alarm when crossed.

The **Bandwidth** tab offers separate controls for peer-to-peer applications and for video applications, using secondary tabs. This allows for optimized handling of server performance for each application type.

Peer-to-Peer Bandwidth Control

The **P2P** secondary tab is dedicated to controlling the bandwidth of peer-to-peer applications. An example of the P2P tabbed window appears in Figure 56 below:



Time of Day	Bandwidth output limit	Alarm Threshold
00:00-01:59	● No Limit ○ Mbps	Mbps
02:00-03:59	● No Limit ○ Mbps	Mbps
04:00-05:59	● No Limit ○ Mbps	Mbps
06:00-07:59	● No Limit ○ Mbps	Mbps
08:00-09:59	● No Limit ○ Mbps	Mbps
10:00-11:59	● No Limit ○ Mbps	Mbps
12:00-13:59	● No Limit ○ Mbps	Mbps
14:00-15:59	● No Limit ○ Mbps	Mbps
16:00-17:59	● No Limit ○ Mbps	Mbps
18:00-19:59	● No Limit ○ Mbps	Mbps
20:00-21:59	● No Limit ○ Mbps	Mbps
22:00-23:59	● No Limit ○ Mbps	Mbps

Session Bandwidth Limit

● No Limit ○ Kbps

Figure 56: Peer-to-Peer Bandwidth Window

The **Peer-to-Peer Bandwidth** tab has the following areas:

- **Time of day table**: Enables you to limit system throughput at two hour time intervals throughout the day, and configure a threshold that generates an alarm when a specified percentage of the allocated bandwidth is reached.
- **Session Bandwidth Limit**: Used to configure the maximum bandwidth that can be allocated to a client in the course of a caching session.

NOTE **All time-related information in MSWE is sychronized with the System Time of the centralized management server, which is displayed in the top right corner of the screen.**

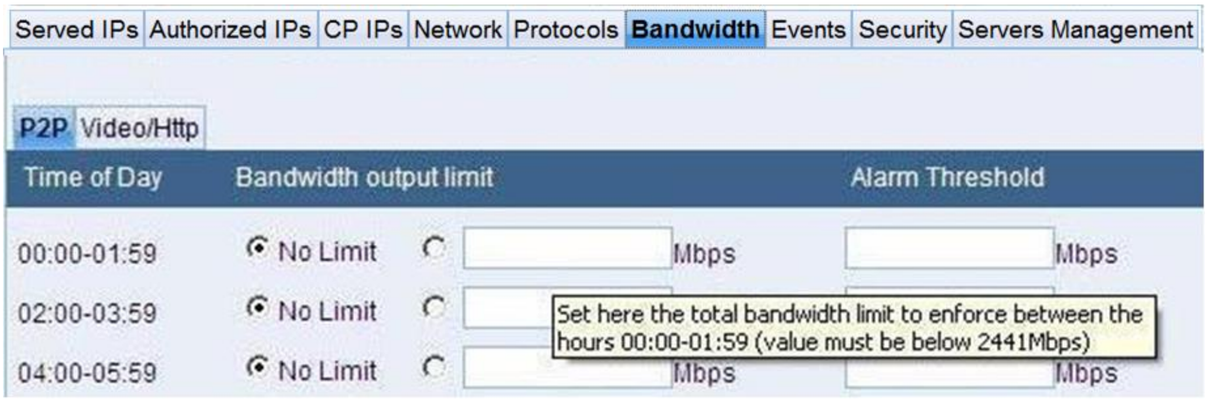
➢ To limit the bandwidth output:

1. In the **Bandwidth** tab of the Configuration page, select the time of day interval for which you want to limit bandwidth.

2. If you wish to limit bandwidth output during this time period, select the radio button next to the **Bandwidth Output Limit** Text Box, and enter a value in Megabits per second. Otherwise, select the **No Limit** Radio Button.

3. In order to receive an alarm message when the bandwidth output approaches the defined limit, enter a bandwidth threshold in Megabits per second in the **Alarm Threshold** Text Box.

NOTE **Be careful not to enter Bandwidth Output Limit and Alarm Threshold values that are above the limit specified in the license provided by Allot. For advice on the maximum possible allocation, hover over one of the fields, and review the information on the tooltip that appears, as per the example shown in Figure 57 below:**



Time of Day	Bandwidth output limit			Alarm Threshold
00:00-01:59	● No Limit	○	Mbps	Mbps
02:00-03:59	● No Limit	○		
04:00-05:59	● No Limit	○	Mbps	Mbps

Set here the total bandwidth limit to enforce between the hours 00:00-01:59 (value must be below 2441Mbps)

Figure 57: Bandwidth Limit Tooltip

4. In the **Session Bandwidth** area, select the **No Limit** option to allow unlimited bandwidth to be served to each client during a session, or to specify a rate in Kbps (if no rate is selected, this field is highlighted in red). If zones are configured, select the rate of bandwidth to be served for each zone.

NOTES **The modified fields in the Bandwidth tab are highlighted in yellow. The values must be saved in order to implement them in the system.**

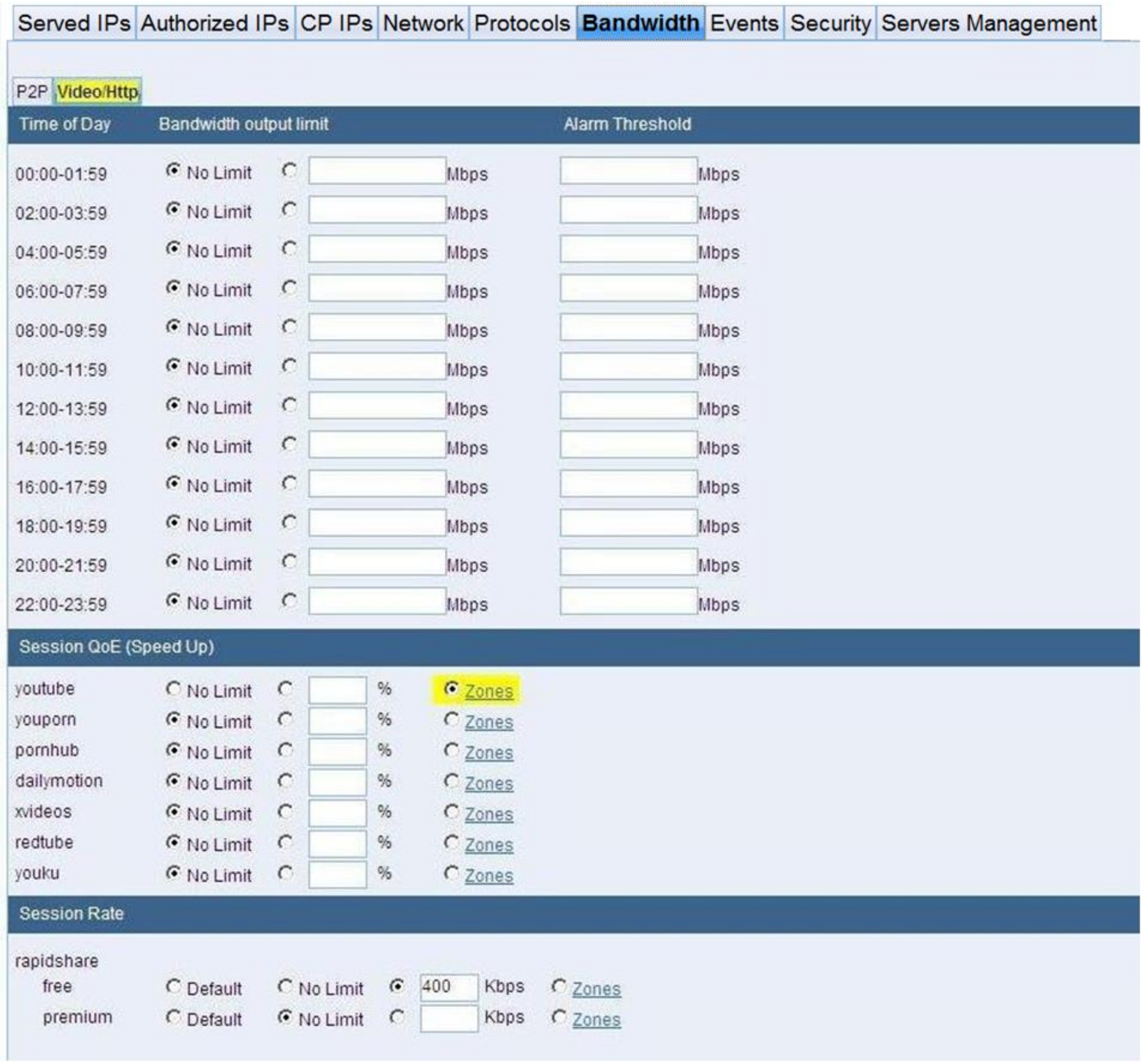
Illegal entries (such as bandwidth output limits that are above the maximum licensed bandwidth) are displayed in red.

5. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.

6. To deploy these changes on all servers in the grid, click **Save**.

Video/HTTP Bandwidth Control

The **Video/Http** secondary tab is dedicated to controlling the bandwidth of HTTP applications. An example of the Video/Http tabbed window appears in Figure 58 below:



Time of Day	Bandwidth output limit			Alarm Threshold
00:00-01:59	● No Limit	○	Mbps	Mbps
02:00-03:59	● No Limit	○	Mbps	Mbps
04:00-05:59	● No Limit	○	Mbps	Mbps
06:00-07:59	● No Limit	○	Mbps	Mbps
08:00-09:59	● No Limit	○	Mbps	Mbps
10:00-11:59	● No Limit	○	Mbps	Mbps
12:00-13:59	● No Limit	○	Mbps	Mbps
14:00-15:59	● No Limit	○	Mbps	Mbps
16:00-17:59	● No Limit	○	Mbps	Mbps
18:00-19:59	● No Limit	○	Mbps	Mbps
20:00-21:59	● No Limit	○	Mbps	Mbps
22:00-23:59	● No Limit	○	Mbps	Mbps

Session QoE (Speed Up)				
youtube	○ No Limit	○	%	● Zones
youporn	● No Limit	○	%	○ Zones
pornhub	● No Limit	○	%	○ Zones
dailymotion	● No Limit	○	%	○ Zones
xvideos	● No Limit	○	%	○ Zones
redtube	● No Limit	○	%	○ Zones
youku	● No Limit	○	%	○ Zones

Session Rate				
rapidshare				
free	○ Default	○ No Limit	● 400 Kbps	○ Zones
premium	○ Default	● No Limit	○ Kbps	○ Zones

Figure 58: Video/HTTP Bandwidth Window

The **Video/Http Bandwidth** tab has the following areas:

- **Time of day table**: Enables you to limit system throughput at two hour time intervals throughout the day, and configure a threshold that generates an alarm when a specified percentage of the allocated bandwidth is reached.
- **Session QoE:** Enables you to control the session bandwidth limit per video site, effectively allowing you to configure a specified Quality of Experience (QoE) on a per-site basis.

Every video file has a specified CODEC rate which represents the minimum bit rate necessary to ensure that the video is displayed smoothly and without interruption. MediaSwift E identifies this rate in both the FLV and MP4 file formats.

For scenarios in which bandwidth is being limited, or when traffic rate is approaching the server's physical limitations, the cache server does not accept new requests if they will cause existing connections to be served below the minimum CODEC + 20% rate.

- **Session Rate:** Enables you to control the rate in Kbps for sites that serve files and *not* videos (such as file sharing and software download/update sites). Some of these sites include user categories, and the session rate can be controlled per user category.

NOTE **All time-related information in MSWE is sychronized with the System Time of the centralized management server, which is displayed in the top-right corner of the screen.**

➢ To limit the bandwidth output:

1. In the **Bandwidth** tab of the Configuration page, select the **Http/Video** secondary tab. The Bandwidth page for Http/Video services is displayed.

2. If you wish to limit bandwidth output during a specific time period, select the radio button next to the **Bandwidth Output Limit** Text Box, and enter a value in Megabits per second. Otherwise, select the **No Limit** radio button.

3. In order to receive an alarm message when the bandwidth output approaches the defined limit, enter a bandwidth threshold in Megabits per second in the **Alarm Threshold** Text Box.

   Important: Be careful not to enter **Bandwidth Output Limit** and **Alarm Threshold** values that are above the limit specified in the license provided by Allot . For advice on the maximum possible allocation, hover over one of the fields, and review the information on the tooltip that appears, as per the example shown in Figure 57 above.

NOTE **The modified fields in the Bandwidth tab are highlighted in yellow. The values must be saved in order to implement them in the system.**

4. Illegal entries (such as bandwidth output limits that are above the maximum licensed bandwidth) are displayed in red. Click **Reload Configuration** to reset all of the tabs with the changes made to the configuration.

5. To deploy these changes on all servers in the grid, click **Save** .

NOTE **Consult Allot Customer Support for the recommended setting for your network.**

➢ To control the bandwidth per session (Session QoE):

1. In the **Bandwidth** tab of the Configuration page, select the **Http/Video** secondary tab. The Bandwidth page for Http/Video services is displayed.

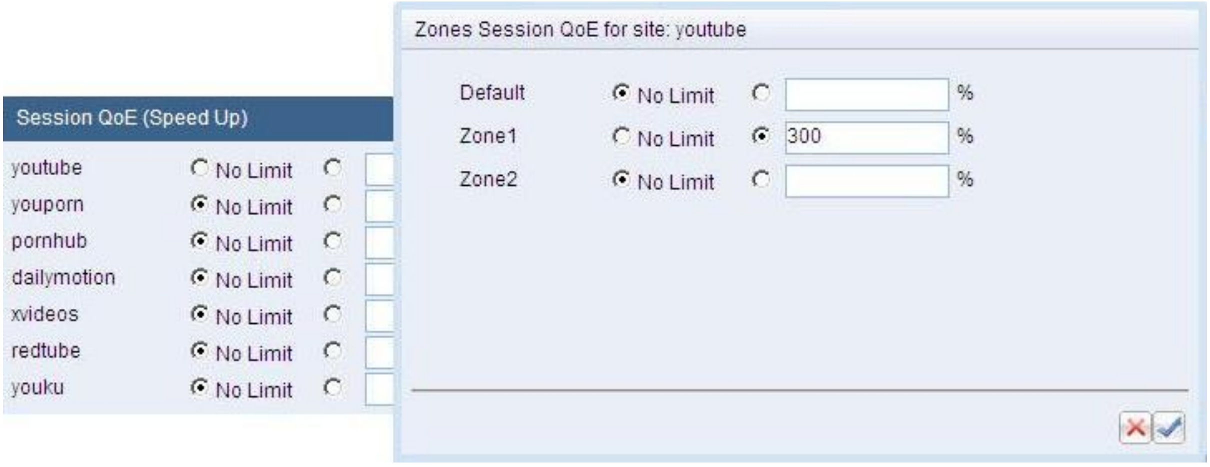
2. Look at the list of video sites in the **Session QoE (Speed Up)** area. For each video site, determine whether you want to control the session rate or leave it unlimited.

3. To allow unlimited bandwidth, choose the **No Limit** radio button.

4. If you choose to control the session rate, sel**ect the** right-hand radio button, and enter the improved bit rate as a percentage over the CODEC rate.

➢ To control the bandwidth per session (Session QoE) for zones:

1. In the **Bandwidth** tab of the Configuration page, select the **Http/Video** secondary tab. The Bandwidth page for Http/Video services is displayed, as shown below in Figure 59.



Session QoE (Speed Up)

youtube	○ No Limit	○
youporn	● No Limit	○
pornhub	● No Limit	○
dailymotion	● No Limit	○
xvideos	● No Limit	○
redtube	● No Limit	○
youku	● No Limit	○

Zones Session QoE for site: youtube

Default	● No Limit	○	%
Zone1	○ No Limit	● 300	%
Zone2	● No Limit	○	%

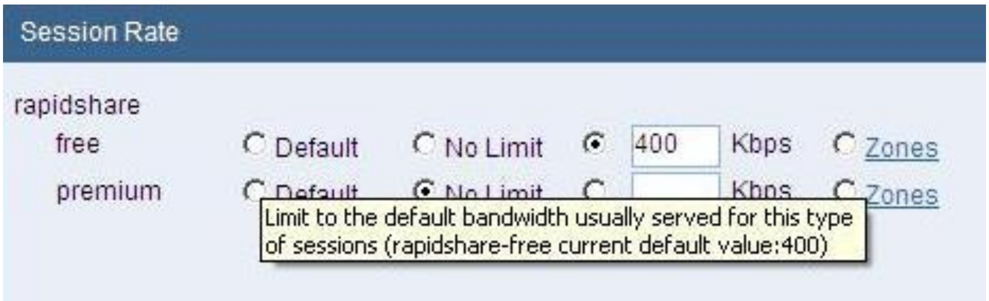
Figure 59: Zones Session QoE Dialog Box

2. Select the **Zones** radio button located on the row of the relevant Http/Video site, and click on the **Zones** link. A dialog box appears with a list of zones and bandwidth configuration options for each zone:
   - **No Limit.** Choose this option in order to provide unlimited bandwidth.
   - **Defined Limit.** This option a**ll**ows you to enter an improved bit rate as a percentage over the CODEC rate.

3. Select the **Save** ✓ icon to save the settings, or the **Cancel** ✗ icon to cancel the modific**ations.**

➢ To control the session rate for non-video sites:

- Choose a session rate per user category, by selecting the appropriate radio button.
  - **Default.** If selected, the cache will use the same rate as the original site for this user category. To view the default rate, hover over the default button to display a tooltip containing the session rate in Kbps, as shown below in Figure 60.
  - **No Limit.** Choose this option in order to provide unlimited bandwidth.
  - **Defined Limit.** This option allows you to enter a non-default rate limit, in Kbps.
  - **Per-Zone Definition.** The **Zones** option allows you to select the session rate on a per-zone basis.



Session Rate

rapidshare

free ○ Default ○ No Limit ● 400 Kbps ○ Zones

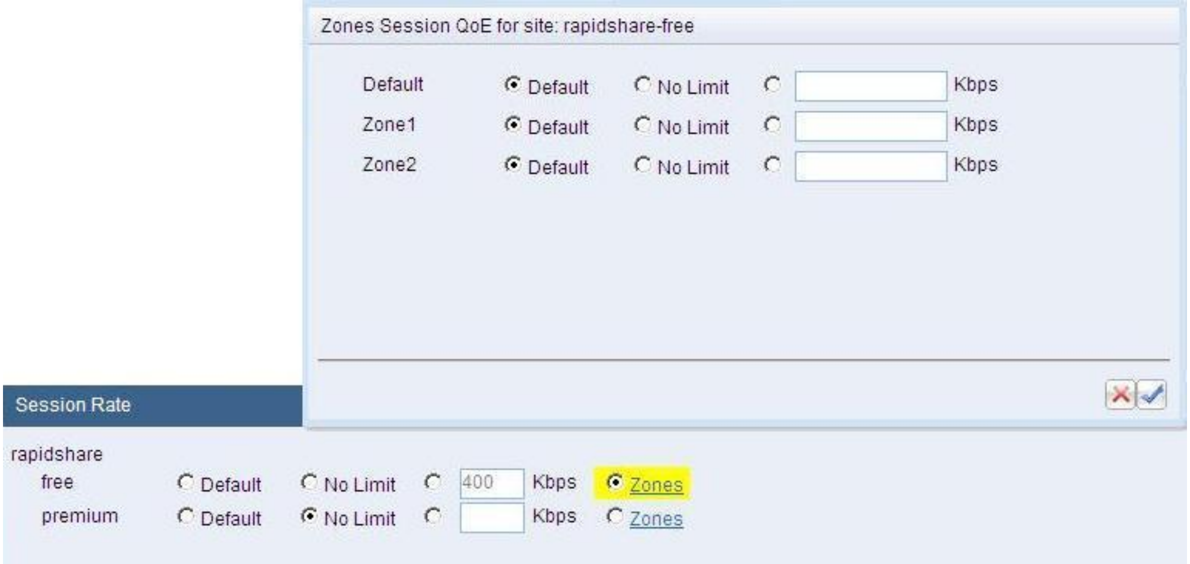
premium ○ Default ● No Limit ○ Kbps ○ Zones

Limit to the default bandwidth usually served for this type of sessions (rapidshare-free current default value:400)

Figure 60: Session Rate Tooltip

➢ To control the session rate for non-video sites for zones:

1. In the **Bandwidth** tab of the Configuration page, select the **Http/Video** secondary tab. The Bandwidth page for Http/Video services is displayed, as shown below in Figure 61.



Zones Session QoE for site: rapidshare-free

Default ● Default ○ No Limit ○ Kbps

Zone1 ● Default ○ No Limit ○ Kbps

Zone2 ● Default ○ No Limit ○ Kbps

Session Rate

rapidshare

free ○ Default ○ No Limit ○ 400 Kbps ● Zones

premium ○ Default ● No Limit ○ Kbps ○ Zones

Figure 61: Zones Session Rate Dialog Box

2. Select the **Zones** radio button located on the row of the relevant Http/Video site, and click on the **Zones** link. A dialog box appears with a list of zones and bandwidth configuration options for each zone:
   - **Default.** If selected, the cache will use the same rate as the original site for this user category. To view the default rate, hover over the default button to display a tooltip containing the session rate in Kbps, as shown below in Figure 60.
   - **No Limit.** Choose this option in order to provide unlimited bandwidth.
   - **Defined Limit.** This option allows you to enter a non-default rate limit in Kbps.

3. Select the **Save** ✓ icon to save the settings, or the **Cancel** ✗ icon to cancel the modific**ations.**

Configuring Event Notifications

The **Events** tab in the Configuration page enables you to receive notification of system events and malfunctions, either via a fault management system, by Syslog or by Email.

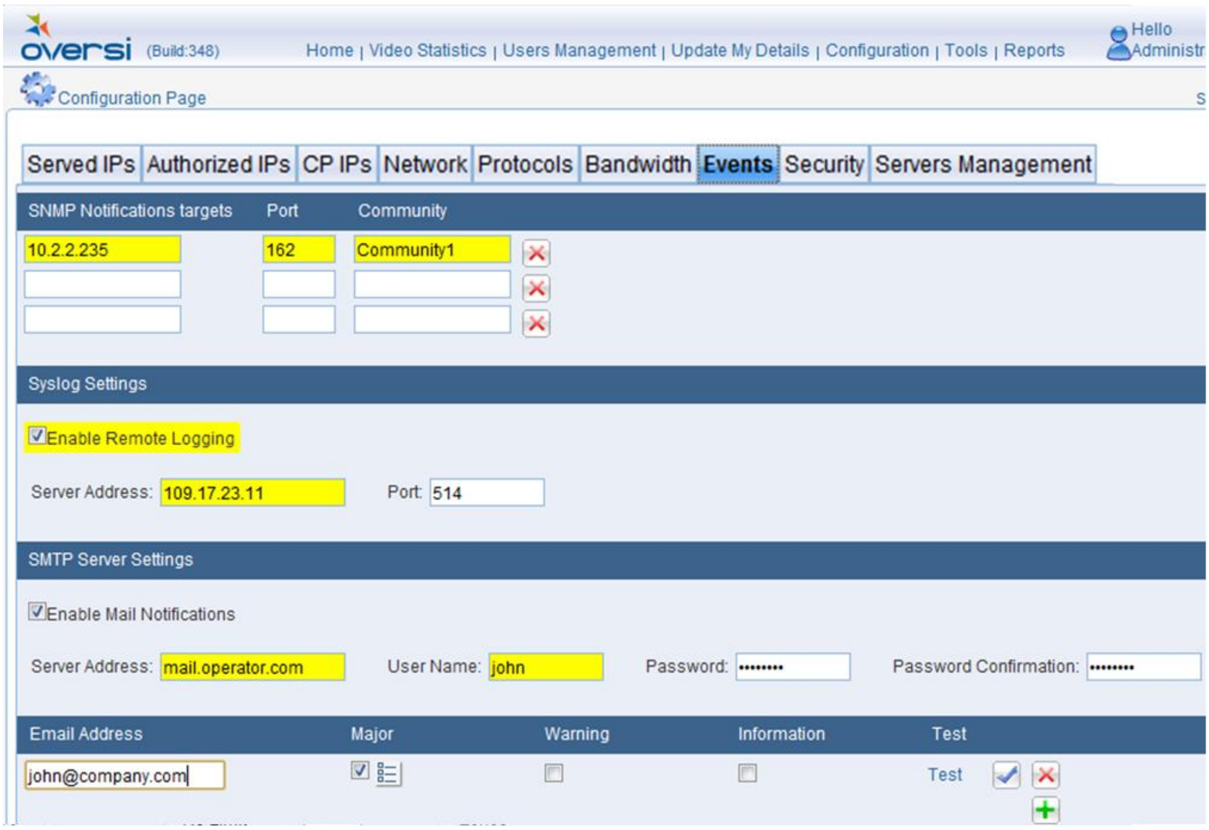
Event Notifications to Fault Management Systems

Network Management Systems (NMSs) or Operations Support Systems (OSSs) can receive information about system events and alarms using the SNMP protocol.

MSWE can be configured to send SNMP-based trap messages to up to three different management systems.

➢ To process the event notifications via a fault management system:

1. Select the **Events** tab of the Configuration page. The Events tabbed window appears as shown below:



SNMP Notifications targets	Port	Community
10.2.2.235	162	Community1

Syslog Settings

☑ Enable Remote Logging

Server Address: 109.17.23.11 Port: 514

SMTP Server Settings

☑ Enable Mail Notifications

Server Address: mail.operator.com User Name: john Password: •••••••• Password Confirmation: ••••••••

Email Address	Major	Warning	Information	Test
john@company.com	☑	□	□	Test

Figure 62: Events Notifications Window

Event Notifications by SNMP TRAPs

MSWE can be configured to send notifications of system-critical events to remote server by SNMP trap:

- **SNMP Notifications Targets**: The remote SNMP server IP Address
- **Port**: The port number which the remote SNMP server listen
- **Community:** The SNMP Community String

1. Select the Events tab of the Configuration page.

2. To remove an existi management station from the notification list, click on the **Delete** ✖ icon.

3. To save your configuration, click **Save** 💾.

NOTE **If you need more targets than are available on the default screen, please consult Allot support. Allot can extend the number of targets as needed.**

Event Notifications by Syslog (Remote Logging)

MSWE can be configured to send notifications of system-critical events to remote server by Syslog.

➢ To receive Event Notifications by Syslog:

1. Select the **Events** tab of the Configuration page.
2. Select the **Enable Remote logging** checkbox in the "Syslog Settings" pane.
3. Enter the IP address and port of the Remote Logging server.

   To save your configuration, click **Save** 💾.

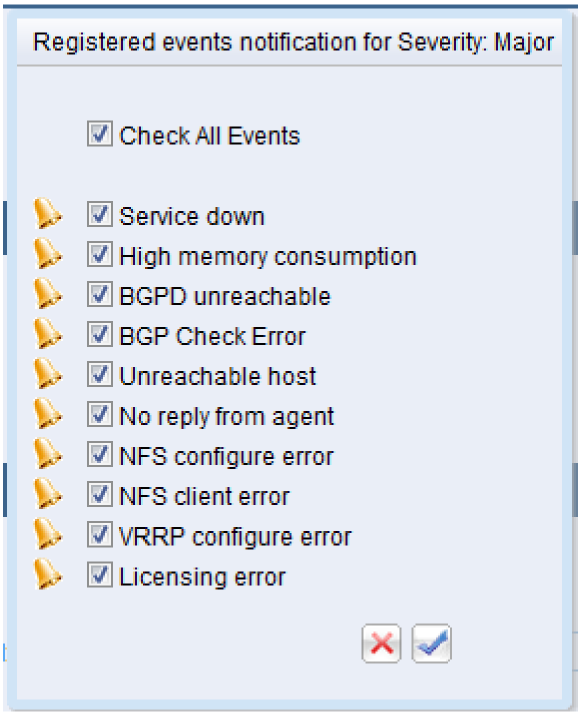
Event Notifications by Email

MSWE can be configured to send Email notifications of system-critical events to one or more network operators.

➢ To receive the events notifications by Email:

1. Select the **Events** tab of the Configuration page.
2. Select the **Enable Mail Notification** check box in the SMTP Server Settings area.
3. Enter the **Server Address**, **User Name**, and **Password**. In the **Password Confirmation** field, enter the password again.
4. In the **Email Address** area, enter the Email address to which the event notification will be sent.
5. Select the warning levels (major, warning, information) to be reported by clicking on the associated check box ☑.
6. Lists of events are shown in Figure 63 (major), Figure 64 (warning), and Figure 65 (information). System faults are designated by a bell icon. Check the events to be registered for notification.
7. Click Save 💾.

NOTE **You can send a test Email by clicking Test.**



Registered events notification for Severity: Major

☑ Check All Events

☑ Service down

☑ High memory consumption

☑ BGPD unreachable

☑ BGP Check Error

☑ Unreachable host

☑ No reply from agent

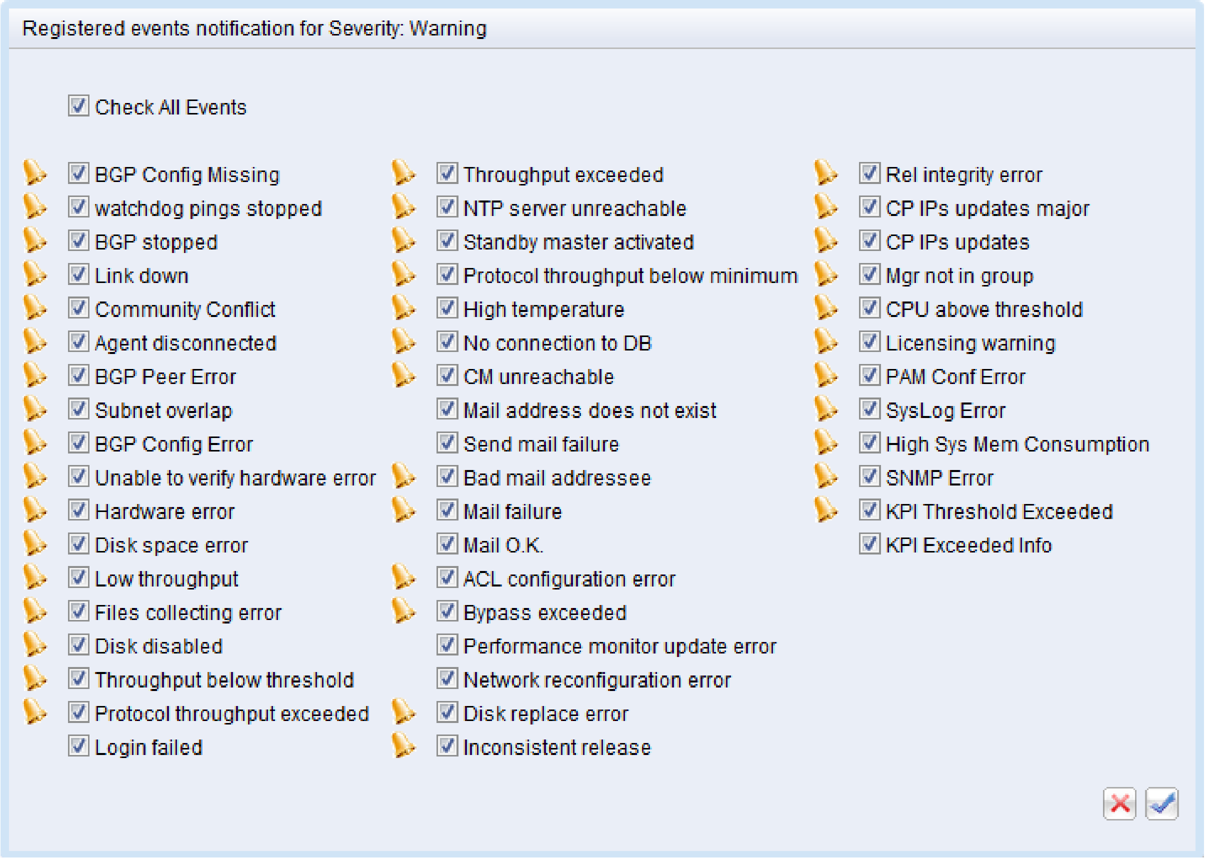
☑ NFS configure error

☑ NFS client error

☑ VRRP configure error

☑ Licensing error

Figure 63: Severity: Major



Registered events notification for Severity: Warning

☑ Check All Events

☑ BGP Config Missing

☑ watchdog pings stopped

☑ BGP stopped

☑ Link down

☑ Community Conflict

☑ Agent disconnected

☑ BGP Peer Error

☑ Subnet overlap

☑ BGP Config Error

☑ Unable to verify hardware error

☑ Hardware error

☑ Disk space error

☑ Low throughput

☑ Files collecting error

☑ Disk disabled

☑ Throughput below threshold

☑ Protocol throughput exceeded

☑ Login failed

☑ Throughput exceeded

☑ NTP server unreachable

☑ Standby master activated

☑ Protocol throughput below minimum

☑ High temperature

☑ No connection to DB

☑ CM unreachable

☑ Mail address does not exist

☑ Send mail failure

☑ Bad mail addressee

☑ Mail failure

☑ Mail O.K.

☑ ACL configuration error

☑ Bypass exceeded

☑ Performance monitor update error

☑ Network reconfiguration error

☑ Disk replace error

☑ Inconsistent release

☑ Rel integrity error

☑ CP IPs updates major

☑ CP IPs updates

☑ Mgr not in group

☑ CPU above threshold

☑ Licensing warning

☑ PAM Conf Error

☑ SysLog Error

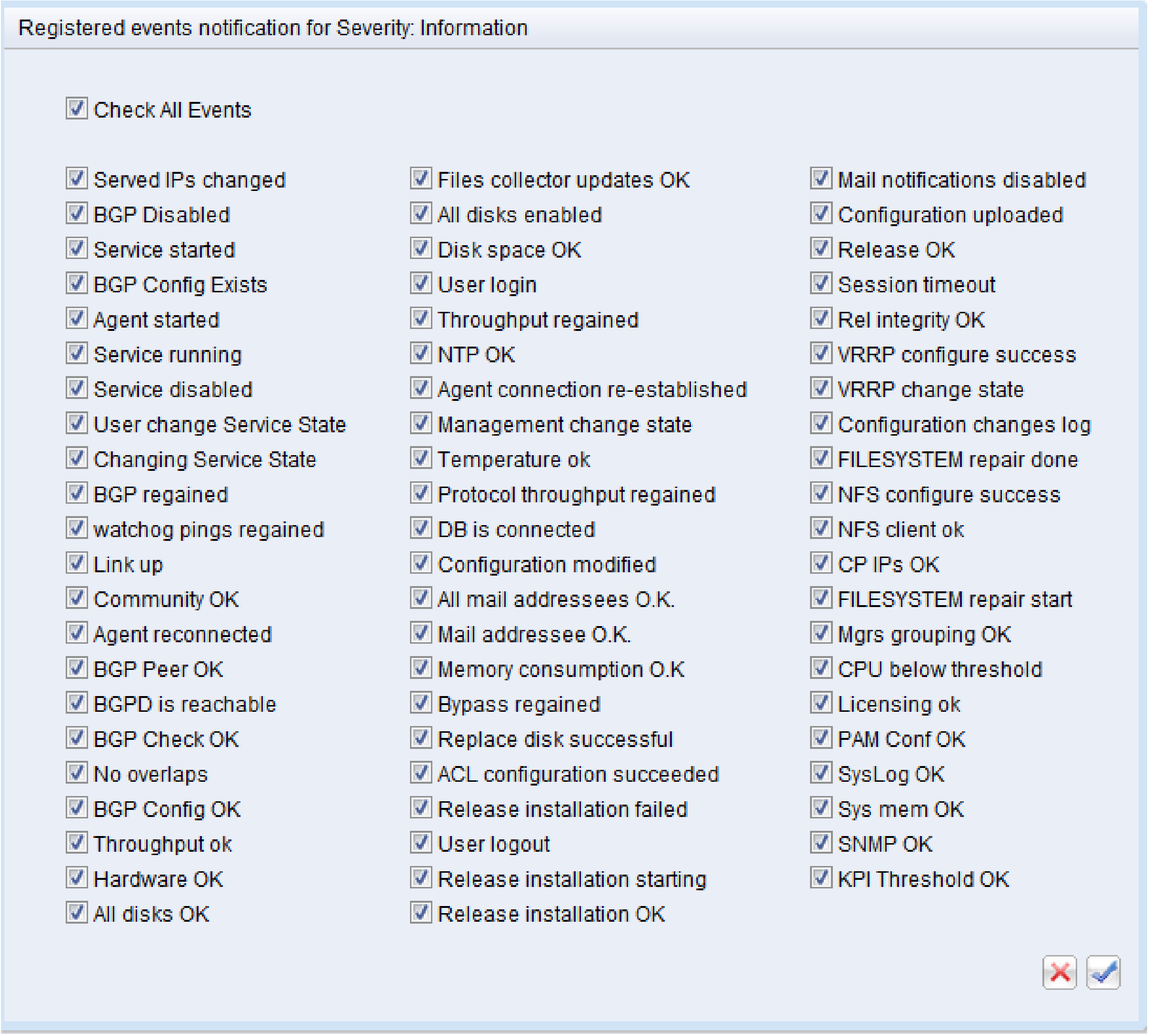
☑ High Sys Mem Consumption

☑ SNMP Error

☑ KPI Threshold Exceeded

☑ KPI Exceeded Info

Figure 64: Severity: Warning



Registered events notification for Severity: Information

☑ Check All Events

☑ Served IPs changed
☑ BGP Disabled
☑ Service started
☑ BGP Config Exists
☑ Agent started
☑ Service running
☑ Service disabled
☑ User change Service State
☑ Changing Service State
☑ BGP regained
☑ watchog pings regained
☑ Link up
☑ Community OK
☑ Agent reconnected
☑ BGP Peer OK
☑ BGPD is reachable
☑ BGP Check OK
☑ No overlaps
☑ BGP Config OK
☑ Throughput ok
☑ Hardware OK
☑ All disks OK

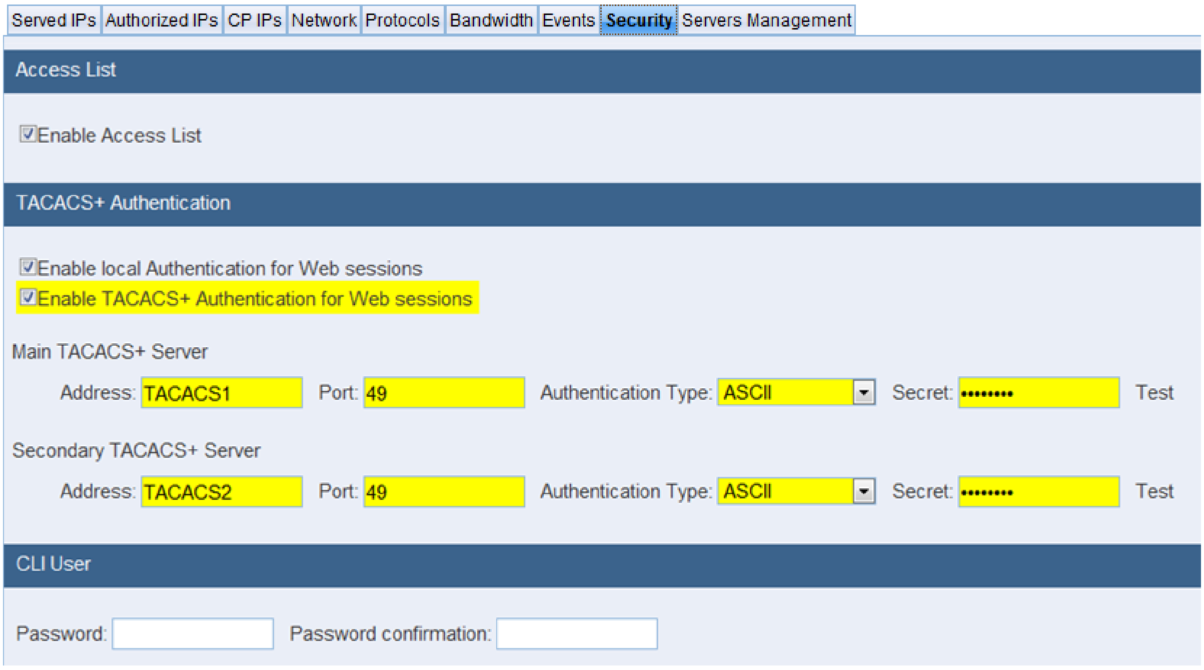
☑ Files collector updates OK
☑ All disks enabled
☑ Disk space OK
☑ User login
☑ Throughput regained
☑ NTP OK
☑ Agent connection re-established
☑ Management change state
☑ Temperature ok
☑ Protocol throughput regained
☑ DB is connected
☑ Configuration modified
☑ All mail addressees O.K.
☑ Mail addressee O.K.
☑ Memory consumption O.K
☑ Bypass regained
☑ Replace disk successful
☑ ACL configuration succeeded
☑ Release installation failed
☑ User logout
☑ Release installation starting
☑ Release installation OK

☑ Mail notifications disabled
☑ Configuration uploaded
☑ Release OK
☑ Session timeout
☑ Rel integrity OK
☑ VRRP configure success
☑ VRRP change state
☑ Configuration changes log
☑ FILESYSTEM repair done
☑ NFS configure success
☑ NFS client ok
☑ CP IPs OK
☑ FILESYSTEM repair start
☑ Mgrs grouping OK
☑ CPU below threshold
☑ Licensing ok
☑ PAM Conf OK
☑ SysLog OK
☑ Sys mem OK
☑ SNMP OK
☑ KPI Threshold OK

Figure 65: Severity: Information

Security Configurations

The **Security** tabbed window in the Configuration page enables you to control grid and management system security. An illustration of the window appears below in Figure 66.



Access List

☑Enable Access List

TACACS+ Authentication

☑Enable local Authentication for Web sessions

☑Enable TACACS+ Authentication for Web sessions

Main TACACS+ Server

Address: TACACS1 Port: 49 Authentication Type: ASCII Secret: •••••••• Test

Secondary TACACS+ Server

Address: TACACS2 Port: 49 Authentication Type: ASCII Secret: •••••••• Test

CLI User

Password: Password confirmation:

Figure 66: Security Window

Access Control List

The Access Control List (ACL) allows only stations whose addresses are set at the **Authorized Managers IPs** screen to access the MSWE application and to access the servers using management applications.

➢ To set security for the grid:

1. In the **Security** tab of the Configuration page, select **Enable Access List**.
2. Click **Save** .

NOTE **MSWE alerts you if your IP address is not found in the list of Authorized Managers. You may be locked out of MSWE if this occurs.**

User and TACACS+ Authentication

MSWE contains a client-side implementation of the TACACS+ Authentication Service. If desired, MSWE user authentication can be performed by the service provider’s TACACS+ servers TACACS+ support enables the CSP to use its own centralized authentication server (TACACS+ server/s) to manage the access to MediaSwift E management interfaces (MSWE and CLI) and manage the privileges levels. The system supports connectivity with up to two TACACS+ servers (redundancy). MSWE allows you to enable MSWE-specific user authentication if the TACACS+ servers are unavailable.

➢ User authentication method:

1. Check one or both of the following check boxes
   - Enable local Authentication
   - Enable TACACS+ Authentication
2. The following logic applied to the checkboxes combinations:
   - If only “**Enable local authentication**” is selected: the authentication of the user will be with the MediaSwift E local database, so user’s access privileges will apply as configured in the Users Management page of MSWE.
   - If only “**Enable TACACS+ Authentication**” is selected: then the user name and password are authenticated with the TACACS+ server, which return authorization and user privilege level to the system.
   - If both options selected, “**Enable local authentication**” and “**Enable TACACS+ Authentication**”: in this case, the system will attempt first to authenticate with the TACACS+ servers. If it fails, it will use the MediaSwift E local database to verify the user’s name password, and identify the user’s privileges.
3. Configure the Main TACACS+ Server.
   - **Address.** The IP Address or DNS Name of the server.
   - **Port.** The TCP/IP port of the server application.
   - **Authentication Type.** Choose either ASCII, PAP, or CHAP from the list box.
   - **Secret.** The secret key of the TACACS+ server.
   - **Test.** Click on the **Test** link to check the connection with the server and verify the validity of the configuration.
4. Configure the Main TACACS+ Server.
   - **Address.** The IP Address or DNS Name of the server.
   - **Port.** The TCP/IP port of the server application.
   - **Authentication Type.** Choose either ASCII, PAP, or CHAP from the list box.
   - **Secret.** The secret key of the TACACS+ server.
   - **Test.** Click on the **Test** link to check the connection with the server and verify the validity of the configuration.
5. Click **Save** 💾.

NOTE **For the examples of users configuration on TACACS+ Server and for the additional details about TACACS+ integration and support by MediaSwift E please refer to the document “*MediaSwift E MSP TACACS+ support Technical Note*”**

CLI User

This enables the provider to set the cliadmin password for ALL the servers connected on the system (see Figure 66 above).

➢ To set the global cliadmin password:

- Enter a password and then enter it again in the confirmation box.

Server Management

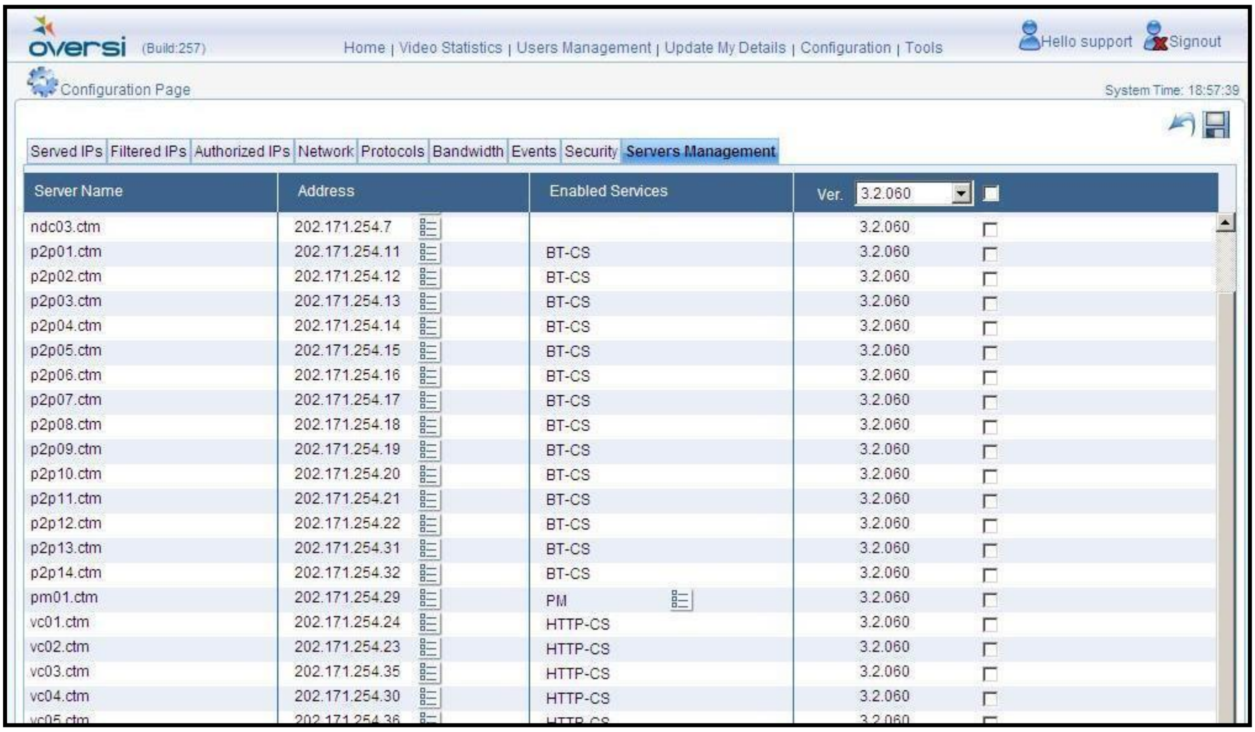
The **Servers Management** tabbed window in the Configuration page enables you to perform the following activities:

- Monitor the services enabled at each server.
- Change the IP addresses of the servers.
- Perform maintenance activities (BGP configuration, interface type selection) on any server which run BGP-S service.
- Configure service advance settings for services (PM and PAgent).
- Download new software versions to the servers.

Monitoring Enabled Services

You can view the screen depicted in Figure 67 below by selecting the **Servers Management** tab. It displays a list of servers, their IP Addresses, and the services currently enabled on them.

All servers can be configured with up to two (for cache servers) or three (for PMs and HMs) network interfaces. It is possible to enhance network security by defining an out-of-band management interface in addition to the interface or interfaces used by the application. If out-of-band management is set, all management traffic will be forwarded over this interface, fully separating user and internet application traffic from the MSWE management network..



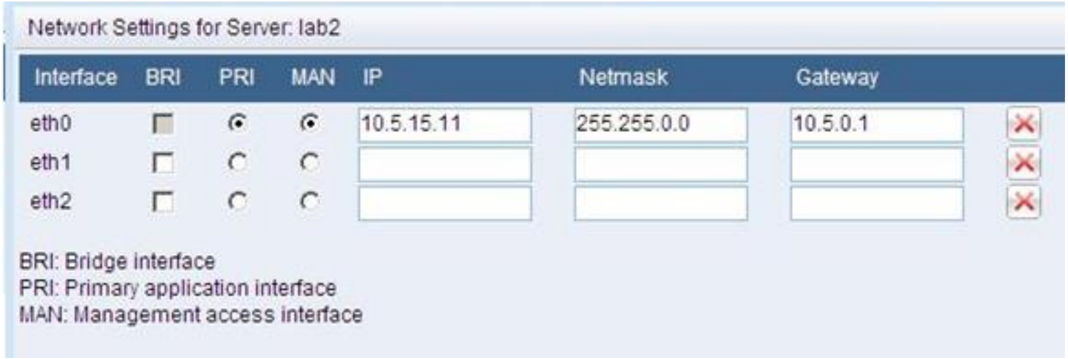
Server Name	Address	Enabled Services	Ver. 3.2.060 ▾	☐
ndc03.ctm	202.171.254.7		3.2.060	☐
p2p01.ctm	202.171.254.11	BT-CS	3.2.060	☐
p2p02.ctm	202.171.254.12	BT-CS	3.2.060	☐
p2p03.ctm	202.171.254.13	BT-CS	3.2.060	☐
p2p04.ctm	202.171.254.14	BT-CS	3.2.060	☐
p2p05.ctm	202.171.254.15	BT-CS	3.2.060	☐
p2p06.ctm	202.171.254.16	BT-CS	3.2.060	☐
p2p07.ctm	202.171.254.17	BT-CS	3.2.060	☐
p2p08.ctm	202.171.254.18	BT-CS	3.2.060	☐
p2p09.ctm	202.171.254.19	BT-CS	3.2.060	☐
p2p10.ctm	202.171.254.20	BT-CS	3.2.060	☐
p2p11.ctm	202.171.254.21	BT-CS	3.2.060	☐
p2p12.ctm	202.171.254.22	BT-CS	3.2.060	☐
p2p13.ctm	202.171.254.31	BT-CS	3.2.060	☐
p2p14.ctm	202.171.254.32	BT-CS	3.2.060	☐
pm01.ctm	202.171.254.29	PM	3.2.060	☐
vc01.ctm	202.171.254.24	HTTP-CS	3.2.060	☐
vc02.ctm	202.171.254.23	HTTP-CS	3.2.060	☐
vc03.ctm	202.171.254.35	HTTP-CS	3.2.060	☐
vc04.ctm	202.171.254.30	HTTP-CS	3.2.060	☐
vc05.ctm	202.171.254.36	HTTP-CS	3.2.060	☐

Figure 67: Servers Management Main Window

Changing the IP Addresses of Network Interfaces

The **Network Settings** icon in the Addresses column enables you to define and modify the IP addresses of the various cache servers and managers.

Click on the icon to display the **Network Settings** window, which is depicted in Figure 68.



Network Settings for Server: lab2

Interface	BRI	PRI	MAN	IP	Netmask	Gateway	
eth0	□	●	●	10.5.15.11	255.255.0.0	10.5.0.1	☒
eth1	□	○	○				☒
eth2	□	○	○				☒

BRI: Bridge interface
PRI: Primary application interface
MAN: Management access interface

Figure 68: Changing Network Settings

➢ To modify the network settings of a server's Ethernet interface:

6. Choose the interface to be modified (eth0, eth1, etc.)
7. Select BRI column for HDI server, to designate the monitoring interface or interfaces. You can select one or more monitoring interfaces. Interfaces selected as BRI do not have IP address configuration and cannot be set to PRI or MAN interfaces.
8. If the selected interface is to be considered the primary application interface, click on the radio button in the PRI column.
9. If the selected interface is to be used to forward and receive management traffic, click on the radio button in the **MAN** column. The IP Address associated with this interface will appear in the Address column of the Servers Management window.

NOTES At least one interface in the server must be defined as the PRI interface – the primary interface for forwarding of service traffic. At least one interface in the server must be defined as the MAN interface – this can be set to the same interface as the PRI interface (in case of in-band management), or to a different interface (in the case of dedicated out-of-band interface).

Please note that if a dedicated out-of-band interface is defined, all management communications between the server and the authorized management addresses, SNMP monitoring addresses and SNMP notification targets will always use this interface. It is the ISPs responsibility to configure the routing parameters in the DCN network to support this configuration.

10. Enter the IP address that is to be associated with it in the IP field.
11. Enter the subnet mask of the interface in the **Netmask** field.
12. Enter the address of the gateway for traffic being forwarded through this interface in the **Gateway** field.

In order to achieve optimal network performance, the PM servers should monitor the activity of BitTorrent trackers, respectively. The Servers Management Main Window, depicted in Figure 67, displays a list of enabled services.

The **Advanced Settings** icon adjacent to the name of the enabled HM or PM service enables the operator to:

- Manage access interface and internet interface

- Monitor the activity of tracker or site IPs, and determine which IP addresses should be redirected to the managers
- Configure the IP addresses to be redirected in the case that the PM use BGP for redirection of these addresses to the managers

If the above servers are BGP peers that advertise IP addresses to the network, it is necessary to perform the following activities in order to properly maintain the ISP's network:

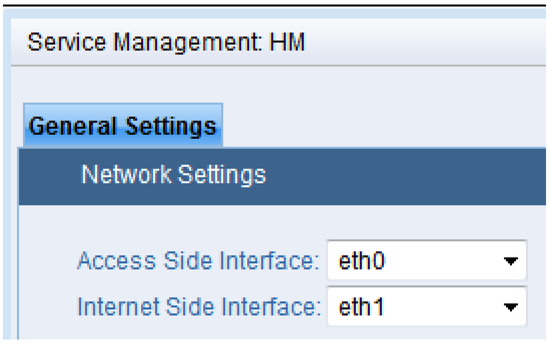
- Display the currently redirected IP addresses
- Monitor the activity level at the various sites
- Provide additional addresses to be advertised via BGP

Monitoring and maintenance can be performed on PM or HM servers by clicking on the adjacent **Advanced Settings** ☰ icon.

Maintaining the Peer Manager and HTTP Manager Servers

➢ To modify the role of PM or HM Interfaces:

13. Click the **General Settings** tab, displaying the screen that appears in **Error! Reference source not found.**.



Service Management: HM

General Settings

Network Settings

Access Side Interface: eth0

Internet Side Interface: eth1

Figure 69: Assigning OCM (HM/PM) Network Interfaces

14. Modify the ID of the Ethernet interface to be used to forward traffic to and from subscribers in the field labeled **Access Side Interface**.

15. Modify the ID of the Ethernet interface to be used to forward traffic to and from the Internet in the field labeled **Internet Side Interface**.

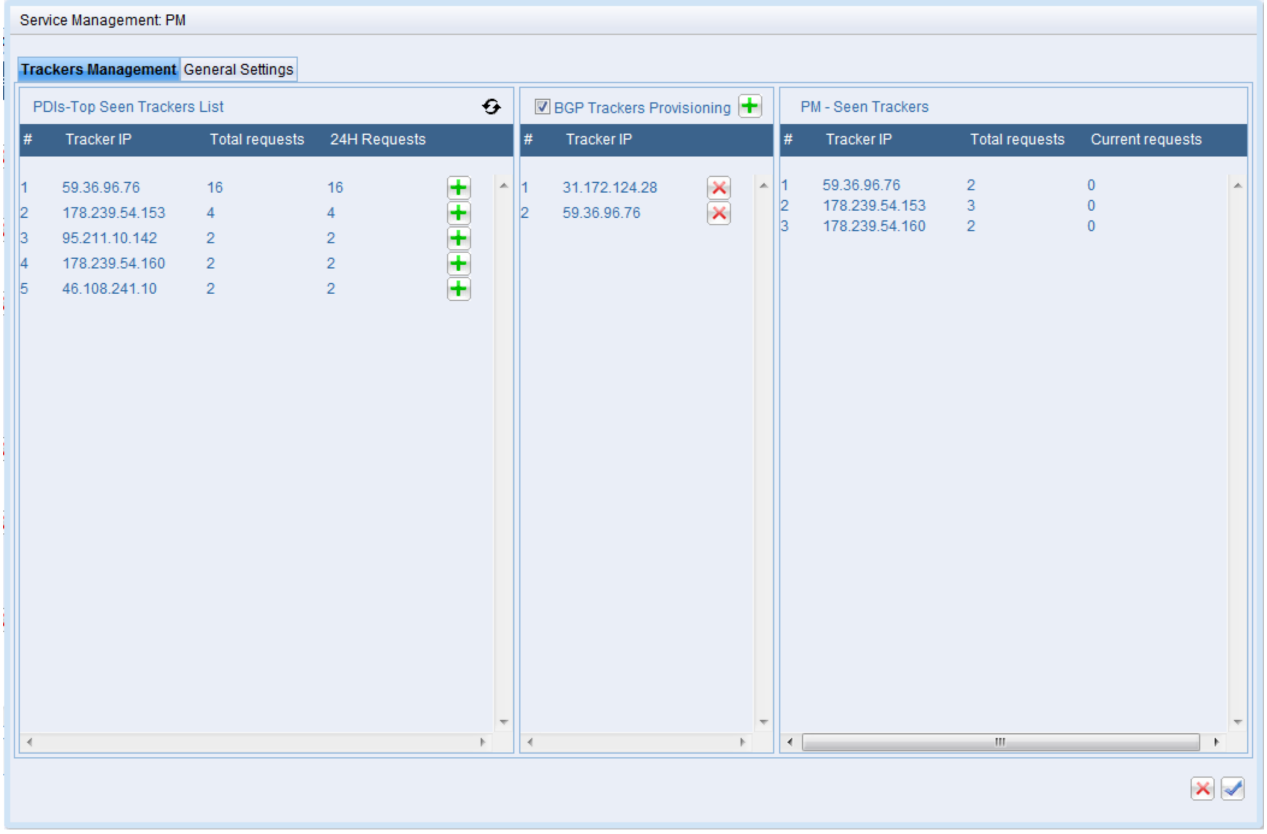
16. Click on **Delete** ✕ to close the window without saving the modifications

17. Click on **Apply** ✓ to submit the modifications and close the window.

➢ To maintain the PM Tracker List:

1. Click on the **Advanced Settings** ☰ icon adjacent to the PM-BT service as it appears in Figure 67. The **Service Management PM-BT** window will appear.

2. To manage the tracker list advertisement in the BGP, click on the **Trackers Management** tab, displaying the screen that appears in Figure 70.



Service Management: PM

Trackers Management | General Settings

PDIs-Top Seen Trackers List

#	Tracker IP	Total requests	24H Requests	
1	59.36.96.76	16	16	+
2	178.239.54.153	4	4	+
3	95.211.10.142	2	2	+
4	178.239.54.160	2	2	+
5	46.108.241.10	2	2	+

☑ BGP Trackers Provisioning +

#	Tracker IP	
1	31.172.124.28	☒
2	59.36.96.76	☒

PM - Seen Trackers

#	Tracker IP	Total requests	Current requests
1	59.36.96.76	2	0
2	178.239.54.153	3	0
3	178.239.54.160	2	0

Figure 70: Managing BitTorrent Trackers

3. You can sort each column by clicking on the column heading. The first click sorts all entries in ascending order, and the second click will sort them in descending order.

   In order to view missing addresses, sort **PDIs - Top Seen Tracker List** with **24H window** in descending order, and sort the **Peer Manager - Seen Trackers** list by the values in the **Tracker IP** column.

NOTE **In some network configurations, advertising the tracker addresses through the PM will re-route the traffic out of the PDI monitoring port. This can be identified if the tracker list on the left side does not appear on the PM Seen trackers (right side) after the BGP configuration, while the trackers on the right side are still active.**

1. Select the **BGP Sites Provisioning** check box in order to manage BGP advertisement on PM.

2. To add IP addresses of BitTorrent trackers to be advertised by BGP, click on the **Add** + icon appearing next to the desired Tracker IP. The Tracker IP address is added to the BGP Sites Provisioning column.

3. In order to add an IP address **not on the HM mapped sites** list, click on the **Add** + icon next to the BGP Sites Provisioning check box, as shown here in Figure 72:

Figure 71: BGP Sites Provisioning Check Box and Add icon

4. A dialog box is displayed, allowing you to enter the IP address or range manually, as shown in Figure 72 below. Enter the address or range to be added to the sites list.

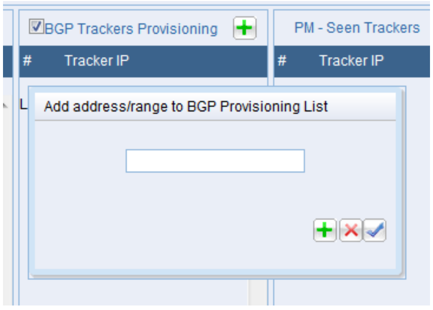

☑BGP Trackers Provisioning
PM - Seen Trackers
#
Tracker IP
#
Tracker IP
Add address/range to BGP Provisioning List

Figure 72: Add IP prefix to BGP Advertised List

5. Click on **Add** ✚ to add the IP prefix to the tracker IP list.

6. Click on **Delete** ✖ to close the window without saving modifications.

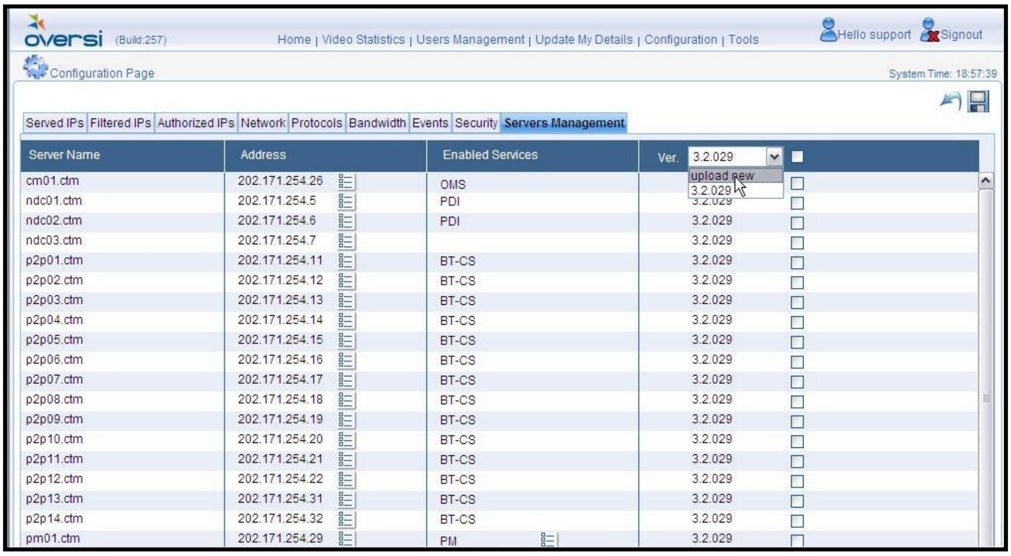
7. Click on **Apply** ✔ to add the IP prefix to the Tracker IP list and close the window.

Uploading a New Software Version to the System

MSWE can be used to upload a new version of the MediaSwift E system software to the main repository, in preparation for a software upgrade. A file containing a new software version is periodically supplied by Allot to its customers.

➢ To upload a new software version from a file supplied by Allot

1. Select the option “upload new” from the **Ver.** list box, as seen in Figure 73 below. A dialog box, **Upload New Version**, will appear, as shown in Figure 74 below.



Server Name	Address	Enabled Services	Ver. 3.2.029	■
cm01.ctm	202.171.254.26	OMS		□
ndc01.ctm	202.171.254.5	PDI	3.2.029	□
ndc02.ctm	202.171.254.6	PDI	3.2.029	□
ndc03.ctm	202.171.254.7		3.2.029	□
p2p01.ctm	202.171.254.11	BT-CS	3.2.029	□
p2p02.ctm	202.171.254.12	BT-CS	3.2.029	□
p2p03.ctm	202.171.254.13	BT-CS	3.2.029	□
p2p04.ctm	202.171.254.14	BT-CS	3.2.029	□
p2p05.ctm	202.171.254.15	BT-CS	3.2.029	□
p2p06.ctm	202.171.254.16	BT-CS	3.2.029	□
p2p07.ctm	202.171.254.17	BT-CS	3.2.029	□
p2p08.ctm	202.171.254.18	BT-CS	3.2.029	□
p2p09.ctm	202.171.254.19	BT-CS	3.2.029	□
p2p10.ctm	202.171.254.20	BT-CS	3.2.029	□
p2p11.ctm	202.171.254.21	BT-CS	3.2.029	□
p2p12.ctm	202.171.254.22	BT-CS	3.2.029	□
p2p13.ctm	202.171.254.31	BT-CS	3.2.029	□
p2p14.ctm	202.171.254.32	BT-CS	3.2.029	□
pm01.ctm	202.171.254.29	PM	3.2.029	□

Figure 73: Uploading MediaSwift E Server Software

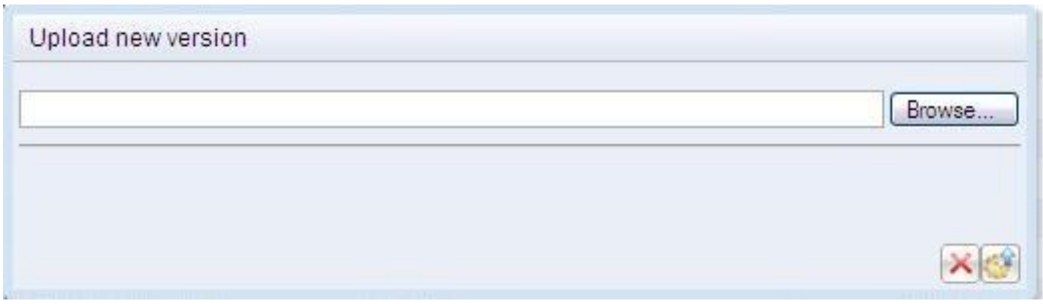


Figure 74: Upload New Version DIalog Box

2. Enter the file name (including the complete path) or click **Browse** to use the **Choose** File dialog box, as illustrated in Figure 75 below.

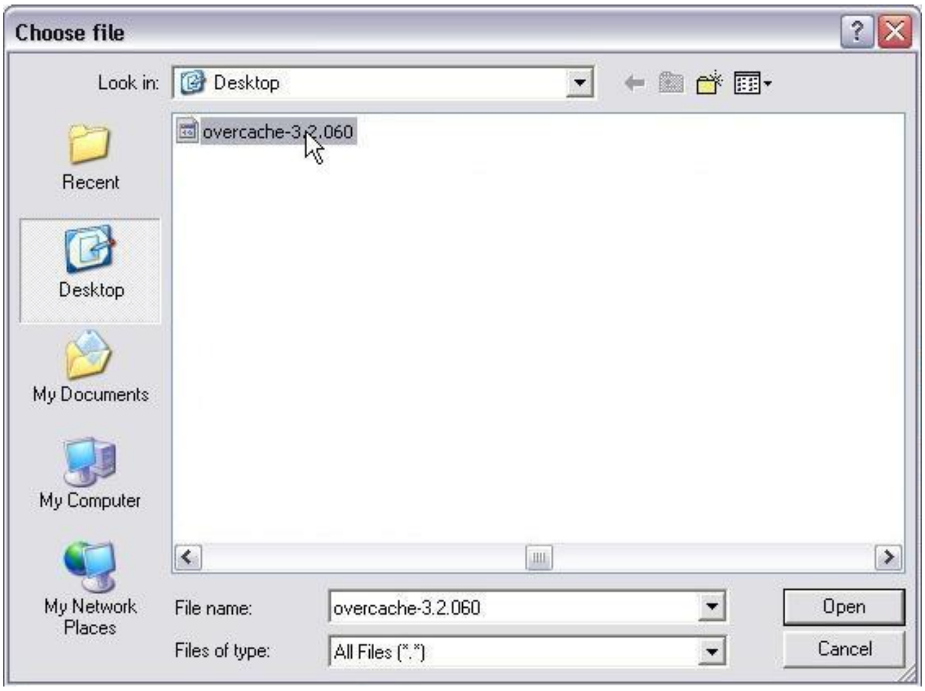
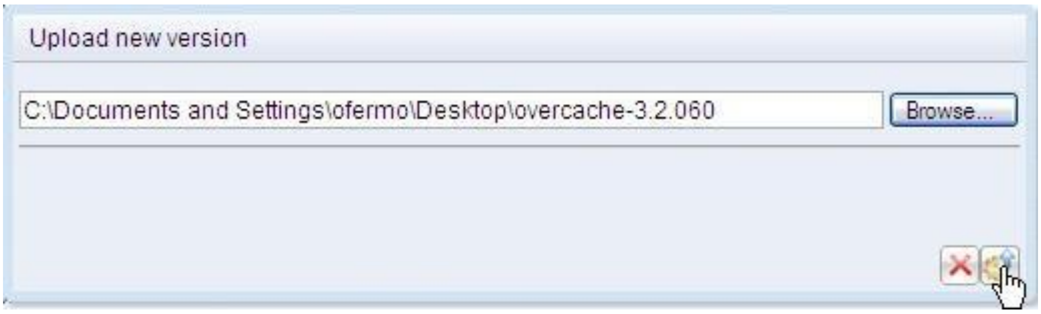


Figure 75: Choose File Dialog Box

3. Select the file, and click **Open.** Windows copies the entire file path/name to the **Upload New Version** dialog box, as shown in Figure 76 below.



C:\Documents and Settings\ofermo\Desktop\overcache-3.2.060

Figure 76: Update New Version Dialog Box

4. Click on the **Start Upload** icon. The dialog box displays the message, “Please wait while uploading file.” When the upload of the new version is complete, the message, “Finished Synchronizing all Servers,” is displayed.

If the upload to the MSWE server fails, the process will be marked as failed, and an error message is displayed. If the upload process fails for a specific, non-MSWE server, a notification message is displayed, but the upload continues with the other servers in the system. The system will complete the upload to the failed server once the server is reactivated.

NOTE **Following the upgrade, it is recommended to monitor the system's operation for a few hours. In case of a system failure that may be caused or suspected to be caused by the software update, you can easily rollback to the previous version by selecting the version from the Ver. list box, and repeating the steps described above.**

Upgrading Server Software

MSWE can be used to download new software versions to MediaSwift E servers (including the Central Management Server that contains the MSWE service). The new software is activated automatically. Using MSWE, you can upgrade (or downgrade) the software of a single server, or simultaneously perform upgrades / downgrades to multiple servers. The Servers Management window reports on the progress of the current downloads, and provides an alert if errors occur.

NOTE **When upgrading the MediaSwift E server network, you must upgrade the MSWE Server server(s) before upgrading the rest of the servers in the grid. If you are using the Global MSWE system, the first upgrade must be performed on the MSWE/G server.**

If upgrading from an Allot -supplied disk, make sure that all servers have the same software version before beginning the upgrade. This will enable you to perform a version rollback later on, if necessary.

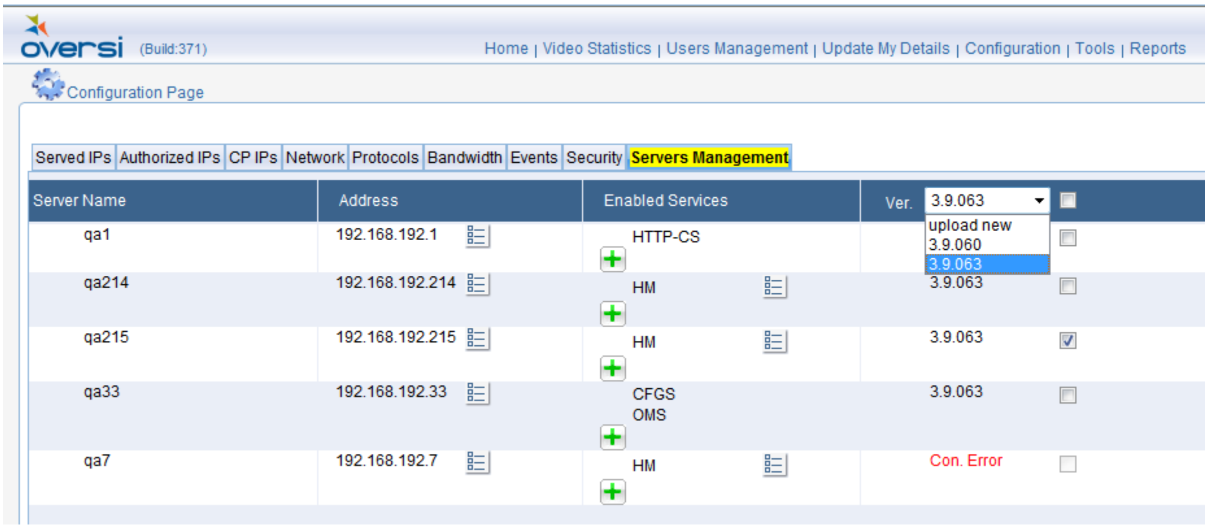
➢ To upgrade the MSWE server software:

1. Click on the **Servers Management** tab, displaying a screen similar to the screen depicted in Figure 77 below.
2. Upgrade the MSWE software in the MSWE server before upgrading the rest of the MediaSwift E servers, as shown in Figure 77 below. Click on the check box opposite the MSWE server, and select the required software version from the **Ver.** list box. Following the selection, the version number and the **Servers Management** tab will be highlighted in yellow.

NOTE **If a new version is to be installed from an update file provided by Allot , please select "upload new" from the Ver. list box, and follow the instructions for installing a new version.**

3. Click **Save** 💾 to begin the download process. The **Ver.** field will display status messages regarding the state of the download. If the download fails, an error message will appear.

NOTE **Once the new MSWE version has been successfully downloaded, the MSWE server resets itself, disconnecting MSWE clients from the server. The client must log in again in order to re-establish the connection to the MSWE server.**



Server Name	Address	Enabled Services	Ver. 3.9.063	□
qa1	192.168.192.1	HTTP-CS		□
qa214	192.168.192.214	HM	3.9.063	□
qa215	192.168.192.215	HM	3.9.063	☑
qa33	192.168.192.33	CFGS OMS	3.9.063	□
qa7	192.168.192.7	HM	Con. Error	□

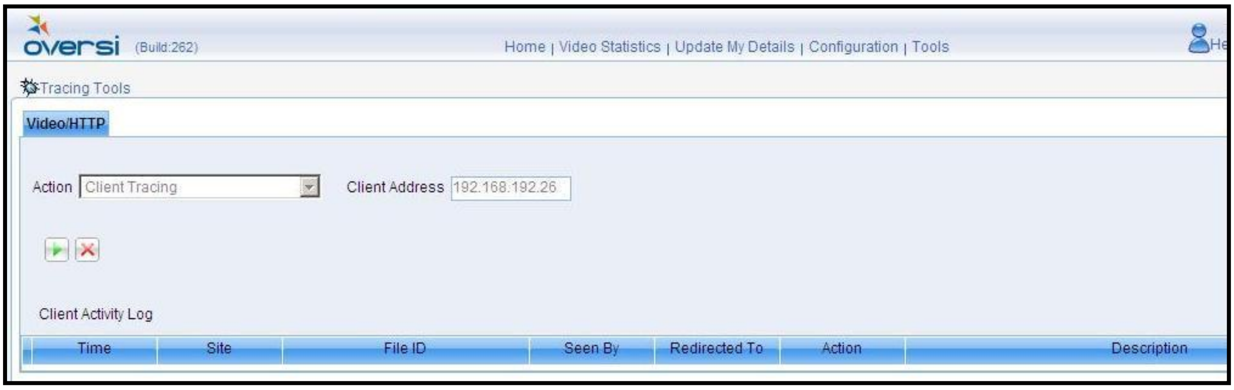
Figure 77: Upgrading MSWE Server Software

Chapter 6: Diagnostic Tools

HTTP Trace

The HTTP Trace function allows the operator to follow the flow of a specific subscriber's HTTP requests, and to track the cache system's handling of these requests. This function is useful in the event that a subscriber reports that he is experiencing low quality or denial-of-service phenomena when accessing certain HTTP or video sites.

It is also possible to trace an entire subnet of HTTP/Video sites. This option is available under **"Subnet Monitor"** option.

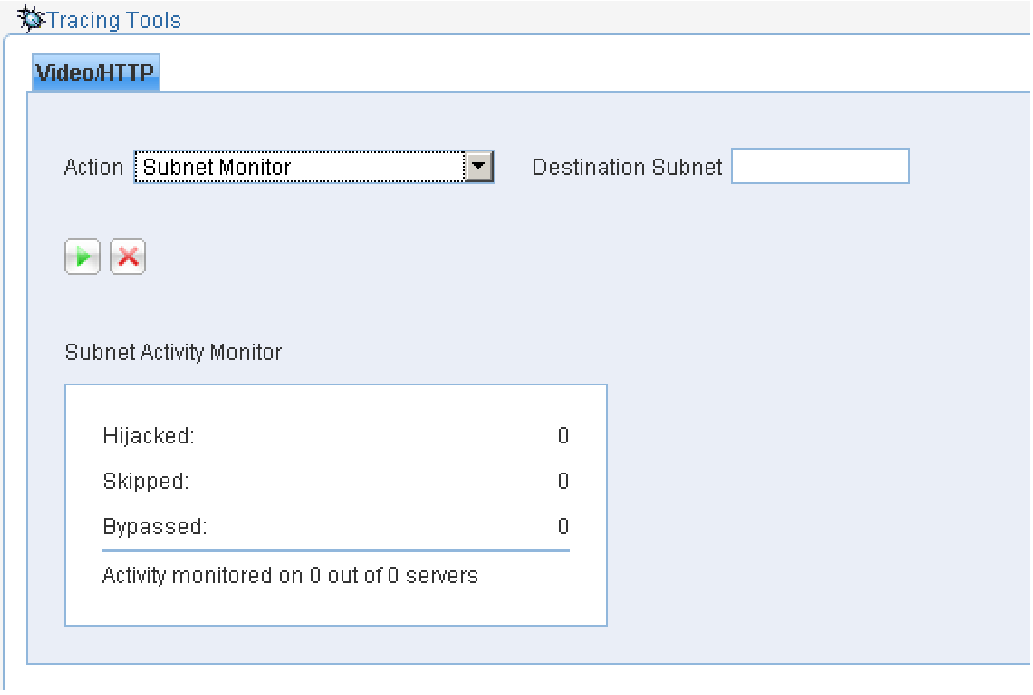

oversi
(Build:262)
Home | Video Statistics | Update My Details | Configuration | Tools
He
Tracing Tools
Video/HTTP
Client Activity Log

Action: Client Tracing

Client Address: 192.168.192.26

Time	Site	File ID	Seen By	Redirected To	Action	Description

Figure 78: Video/HTTP Client Tracing Window



Action: Subnet Monitor

Destination Subnet:

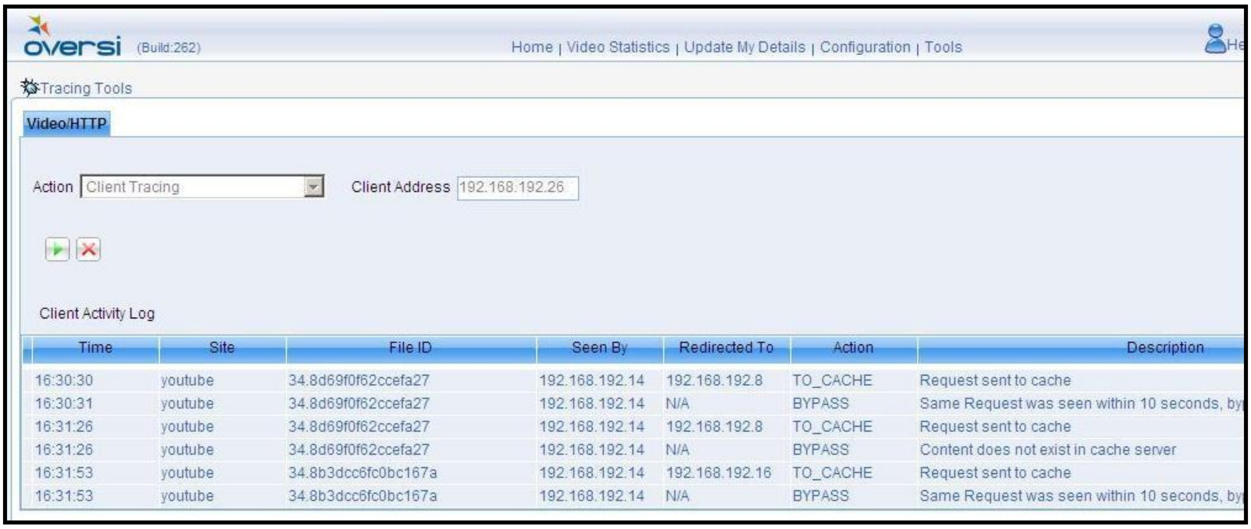
Hijacked:	0
Skipped:	0
Bypassed:	0

Activity monitored on 0 out of 0 servers

Figure 79: Video/HTTP Subnet Monitor Window

➢ To operate the HTTP Trace function:

1. On the **Tools** page, click on the **Video/HTTP** tab, displaying a screen similar to the screen depicted in Figure 78 above.
2. Choose the “Client Tracing” option in the **Action** list box.
3. In the **Client Address** field, enter the IP address of the subscriber whose requests are to be traced.
4. Press on the **Start** ▶ icon to begin the trace. MSWE begins to trace requests, and displays them in the **Client Activity Log**, as seen in Figure 80 below, with the following details:
    - **Time** – the time at which the request was received
    - **Site** – The IP address of the video site
    - **File ID** – the ID of the video file requested
    - **Seen By** – the HTTP Manager that handled the request
    - **Redirected To** – the IP address of the HTTP Cache Server that handled the request
    - **Action** – the action taken by the HTTP Manager
    - **Description** – a further explanation of the action taken by the HM


oversi
(Build:262)
Home | Video Statistics | Update My Details | Configuration | Tools
He
Tracing Tools
Video/HTTP

Action: Client Tracing

Client Address: 192.168.192.26

Client Activity Log

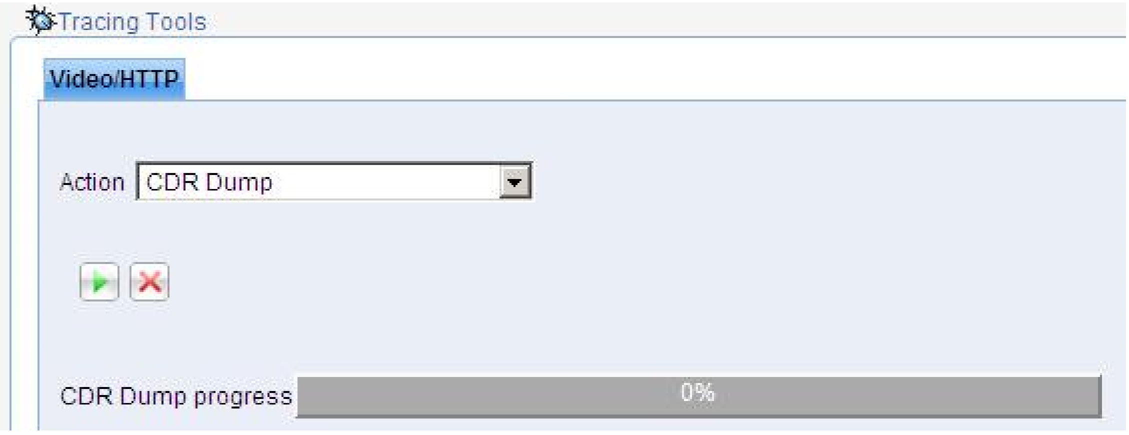
Time	Site	File ID	Seen By	Redirected To	Action	Description
16:30:30	youtube	34.8d69f0f62ccefa27	192.168.192.14	192.168.192.8	TO_CACHE	Request sent to cache
16:30:31	youtube	34.8d69f0f62ccefa27	192.168.192.14	N/A	BYPASS	Same Request was seen within 10 seconds, by
16:31:26	youtube	34.8d69f0f62ccefa27	192.168.192.14	192.168.192.8	TO_CACHE	Request sent to cache
16:31:26	youtube	34.8d69f0f62ccefa27	192.168.192.14	N/A	BYPASS	Content does not exist in cache server
16:31:53	youtube	34.8b3dcc6fc0bc167a	192.168.192.14	192.168.192.16	TO_CACHE	Request sent to cache
16:31:53	youtube	34.8b3dcc6fc0bc167a	192.168.192.14	N/A	BYPASS	Same Request was seen within 10 seconds, by

Figure 80: HTTP Trace Log with Activity Details

5. Press on the **Stop** ✖ icon to end the trace.

CDR (Call Data Record)

CDR (Call Data Record) record each user request from the cache server for HTTP video or P2P files. The records are saved on regular periods in csv format and are available for retrieval through the tools tab.



Action CDR Dump

Figure 81: CDR Save Progress Details

NOTE **The CDR feature availability depends on appropriate license from Allot . This option will not be available for configuration or monitoring without appropriate license.**

The use of CDR may be subject to local privacy protection laws and the use of the information is under the sole responsibility of the operator.

➢ **To view information gathered by the CDR function:**

1. From the Tools tab select **CDR Dump**.
2. From the open window browse to and select the files you want to copy to your local server for further processing.
3. When completed you can download the dump file for scrutiny and evaluation.
4. If you wish to retrieve the up-to-date CDR records (from the last download period to the present) select ▶.

   A progress bar indicates the system processing.
5. Once finished, you can download the dump file for further evaluation.

Chapter 7: KPI Reporting Suite

Introduction

Because of the rapid growth of the P2P industry it has become imperative that management have the proper tools enabling them enough time to plan expanding their infrastructure well before the situation becomes critical. The KPI (Key Performance Indicator) Reporting tool suite consists of a set of configurable system watchdogs that open an alarm when the system becomes slow and unresponsive due to an insufficient infrastructure.

Configuring the P2P-KPI

You can configure all the KPI (Key Performance Indicator) tools as required. When these settings are changed you must save the changes for each tool individually. If you wish to return to the default factory settings please use the values shown in the table below.

QoE – Quality of Experience

LRU – Last Recently Used (files)

There are five configurable dual watchdogs' used as performance indicators in each group. Each report indicator unit can only create an alert when BOTH their thresholds are reached together.

Table 1: KPI Reporting Tools Field Descriptions

KPI Tool	Default	Description
Sessions QoE	200Kbps 60%	Alert - when session speed is below this value **AND** servers cross this threshold.
Rejected Sessions	5 (sessions) 60%	Alert - when more than the selected sessions are rejected **AND** servers cross this threshold.
Disks LRU	14 days 60%	Alert – when there is less than the number of selected days for the deletion of the least used files **AND** the servers cross this threshold.
CPU	70% 60%	Alert – when CPU is above threshold **AND** servers cross this threshold.
MAX Throughput	160 Mbps 60%	Alert – when max throughput is above threshold **AND** servers cross this threshold.

NOTE **The values shown in the examples below are the actual factory defaults.**

➢ To configure the KPI reporting indicators:

1. Click the **Reports** tab.

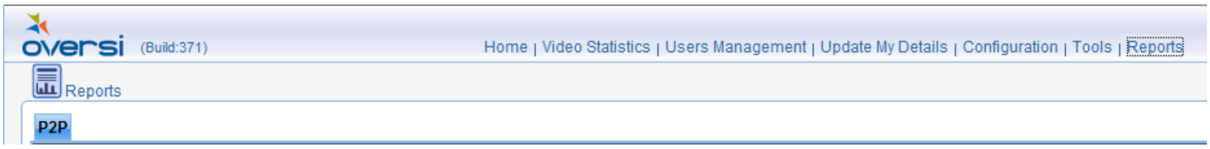
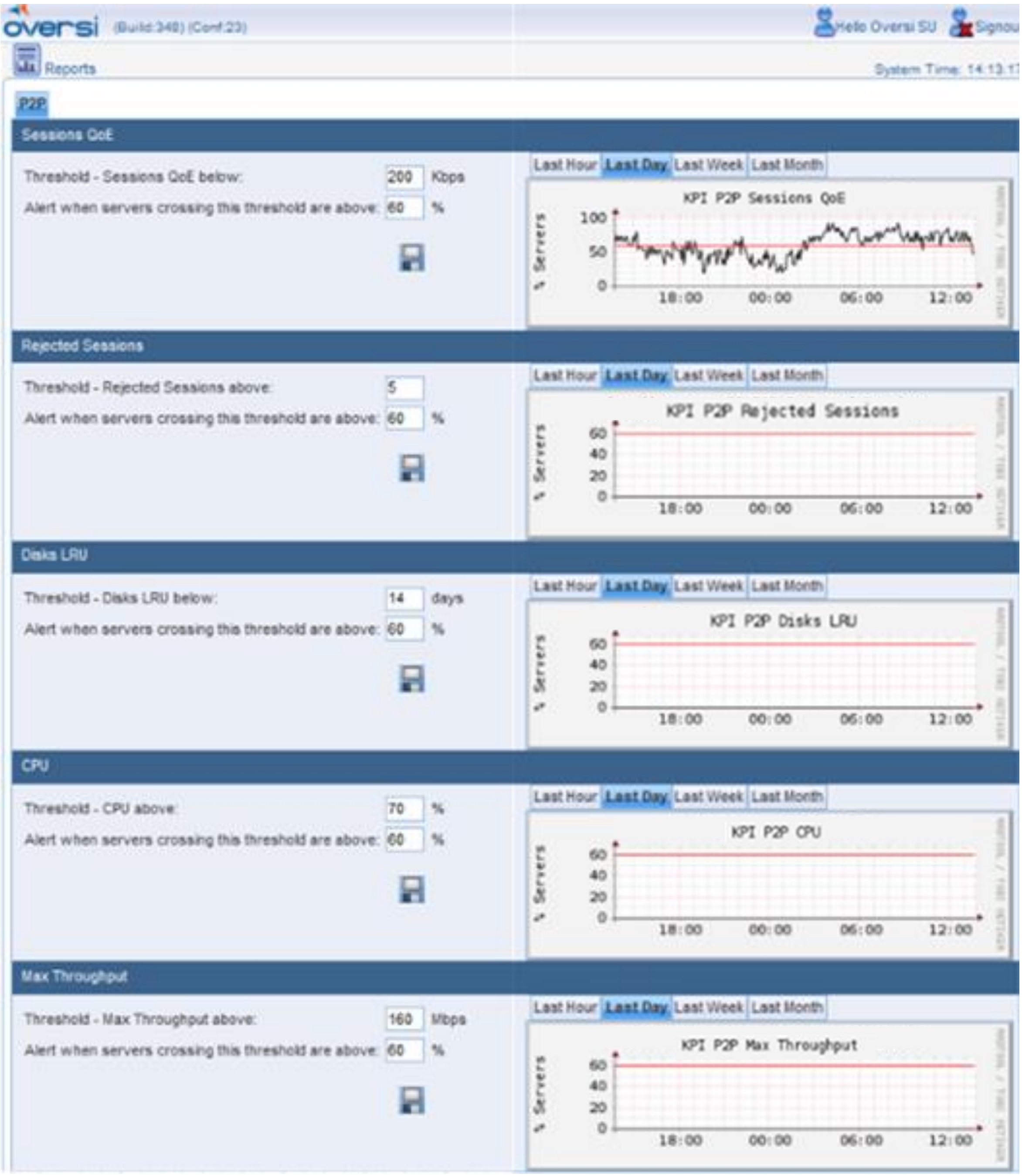

oversi
(Build:371)
Home | Video Statistics | Users Management | Update My Details | Configuration | Tools | Reports
Reports
P2P

Figure 82: Configure the KPI reporting indicators



oversi (Build:348) (Conf:23)

Hello Oversi SU Signou

Reports

System Time: 14:13:17

P2P

Sessions QoE

Threshold - Sessions QoE below: 200 Kbps

Alert when servers crossing this threshold are above: 60 %

Rejected Sessions

Threshold - Rejected Sessions above: 5

Alert when servers crossing this threshold are above: 60 %

Disks LRU

Threshold - Disks LRU below: 14 days

Alert when servers crossing this threshold are above: 60 %

CPU

Threshold - CPU above: 70 %

Alert when servers crossing this threshold are above: 60 %

Max Throughput

Threshold - Max Throughput above: 160 Mbps

Alert when servers crossing this threshold are above: 60 %

Figure 83: Configure the KPI reporting indicators

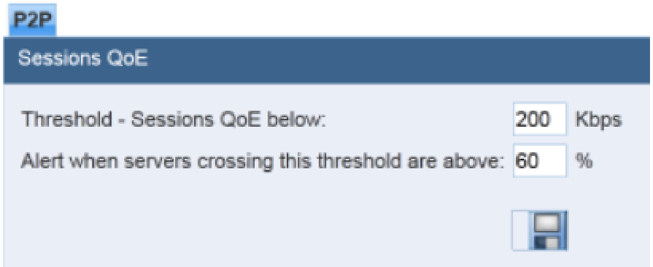
2. Use the table above as a guide change the configurations as required.
3. When you change values in any report indicator unit you must click the 💾 button to save the changes.
4. Click a tab on the graph display to change the reported time period.

Changing the QoE Thresholds

These values correspond to the Quality of Experience of the viewer relative to the loading of the server.

➢ To change the QoE thresholds:

1. Click the **Reports** tab.



Sessions QoE

Threshold - Sessions QoE below: 200 Kbps

Alert when servers crossing this threshold are above: 60 %

Figure 84: Change the QoE thresholds

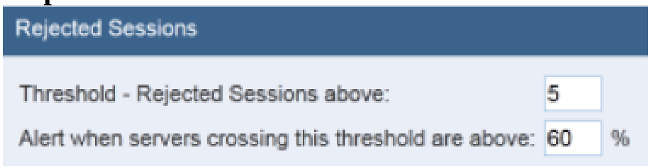
2. Change the threshold values as required.
3. Click the 💾 button to save the changes.

Changing the Rejected Sessions Thresholds

These values correspond to the number of rejected sessions and the loading of the server.

➢ To change the rejected sessions thresholds:

1. Click the **Reports** tab.



Rejected Sessions

Threshold - Rejected Sessions above: 5

Alert when servers crossing this threshold are above: 60 %

Figure 85: change the rejected sessions thresholds

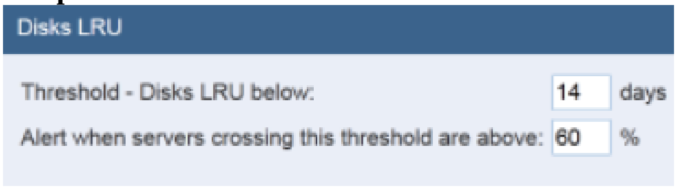
2. Change the threshold values as required.
3. Click the 💾 button to save the changes.

Changing the LRU Thresholds

These values correspond to which last recently used files to delete when the server becomes too loaded.

➢ To change the last recently used file thresholds:

1. Click the **Reports** tab.



Disks LRU

Threshold - Disks LRU below: 14 days

Alert when servers crossing this threshold are above: 60 %

Figure 70: change the rejected sessions thresholds

2. Change the threshold values as required.

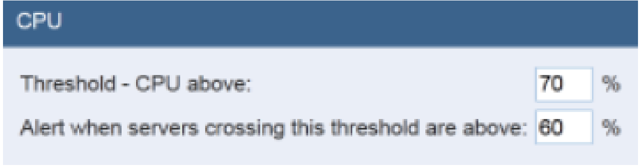
3. Click the 💾 button to save the changes.

Changing the CPU Thresholds

These values correspond to CPU usage when the server becomes too loaded.

➢ To change the CPU usage thresholds:

1. Click the **Reports** tab.



CPU

Threshold - CPU above: 70 %

Alert when servers crossing this threshold are above: 60 %

Figure 70: change the CPU usage thresholds

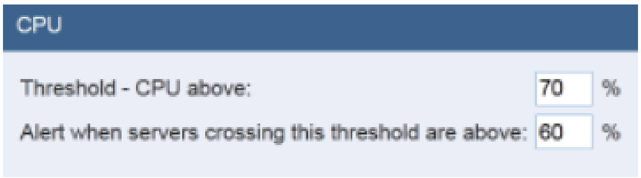
2. Change the threshold values as required.
3. Click the 💾 button to save the changes.

Changing the MAX Throughput Thresholds

These values correspond to maximum throughput when the server becomes too loaded.

➢ To change the maximum throughput thresholds:

1. Click the **Reports** tab.



CPU

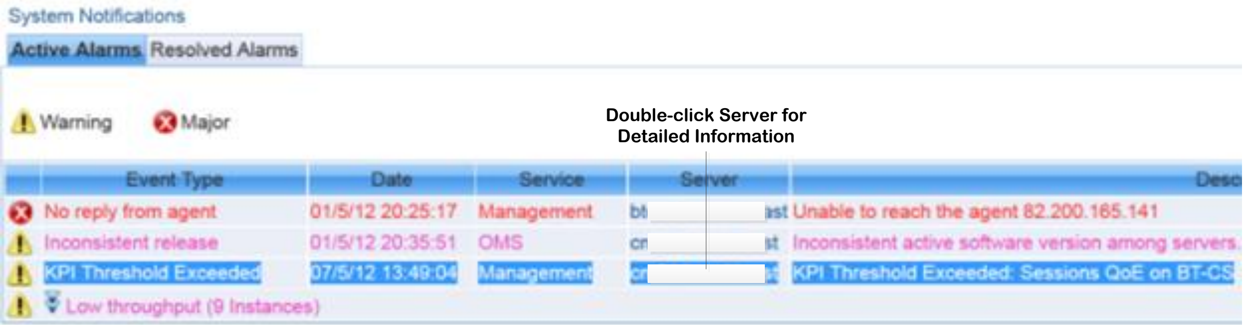
Threshold - CPU above: 70 %

Alert when servers crossing this threshold are above: 60 %

Figure 70: change the CPU usage thresholds

2. Change the threshold values as required.
3. Click the 💾 button to save the changes.

Displaying the KPI Alerts



System Notifications

Active Alarms | Resolved Alarms

⚠ Warning ⊗ Major

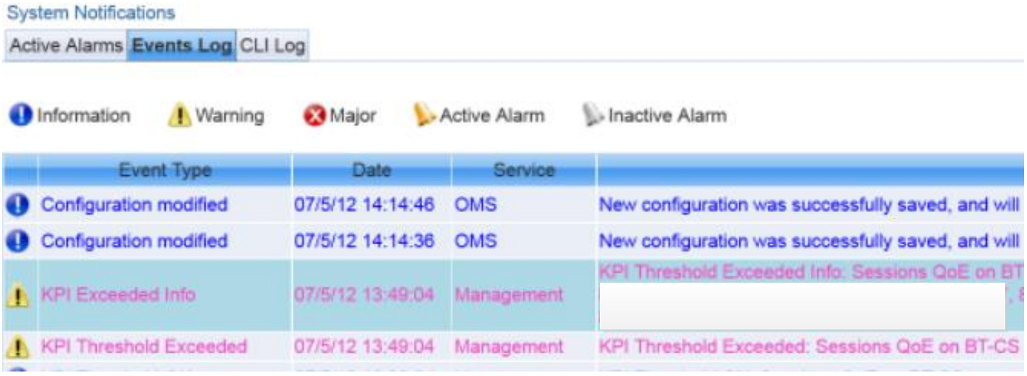
Double-click Server for Detailed Information

	Event Type	Date	Service	Server	Desc
⊗	No reply from agent	01/5/12 20:25:17	Management	bt[redacted]ast	Unable to reach the agent 82.200.165.141
⚠	Inconsistent release	01/5/12 20:35:51	OMS	cr[redacted]st	Inconsistent active software version among servers.
⚠	KPI Threshold Exceeded	07/5/12 13:49:04	Management	cr[redacted]st	KPI Threshold Exceeded: Sessions QoE on BT-CS
⚠	Low throughput (9 Instances)				

Figure 70: Displaying the Active Alarms

➢ To display the KPI alerts:

1. Click the **Active Alarms** tab, if it is not already displayed.
2. If there is a KPI alert, double-click the server as shown above.



	Event Type	Date	Service	
●	Configuration modified	07/5/12 14:14:46	OMS	New configuration was successfully saved, and will
●	Configuration modified	07/5/12 14:14:36	OMS	New configuration was successfully saved, and will
⚠	KPI Exceeded Info	07/5/12 13:49:04	Management	KPI Threshold Exceeded Info: Sessions QoE on BT
⚠	KPI Threshold Exceeded	07/5/12 13:49:04	Management	KPI Threshold Exceeded: Sessions QoE on BT-CS

Figure 70: Displaying the KPI alert in Event Log

1. Using the displayed IP addresses you can verify if the server in question is overloaded.
2. Use the **Reports** tab to see the graphic display and click the different tabs to get an idea of the problem if any.

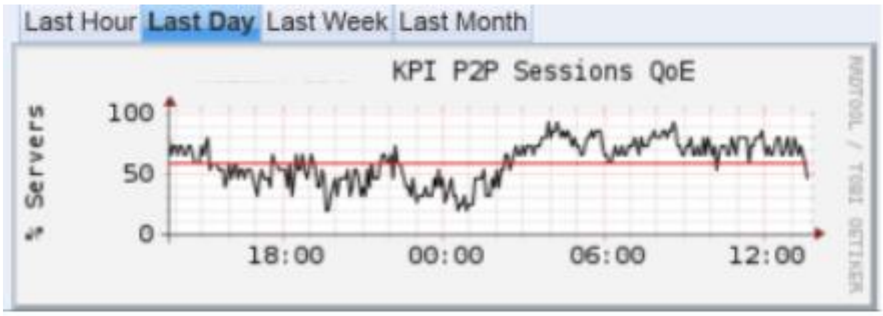


Figure 70: Example of KPI P2P session QoE

Your graphs will look different as this example was made during the testing phase.

Chapter 8: Managing Multiple Domains

Introduction

Allot’s MSWE is composed of two-tiered management levels that enhance the scalability of the MediaSwift E network by allowing the MSWE to serve as a multi-domain portal, providing centralized control over multiple cache sites. A GMS (Global management System) server is a portal managing multiple DMS (Domain Management Systems) servers, where each domain is a single logical cache (cache grid) managing a group of users.

This architecture is designed for ISPs with multiple points-of-presence (POPs), in which each POP is served by its own cache grid. The system associates each end user to the appropriate cache grid by mapping the user’s IP address to one of the POPs.

NOTE **The control elements of the cache system are managed together from a logical point of view, independently of their physical location within the POPs.**

From the GMS main screen, the operator can perform the following scalability-enhancing activities:

- Drilling-down in order to configure and monitor individual domain sites
- Aggregation and presentation of alarm and performance statistics from all domain
- Efficient, one-step configuration of global parameters across all domains

Each multi-domain system includes the following:

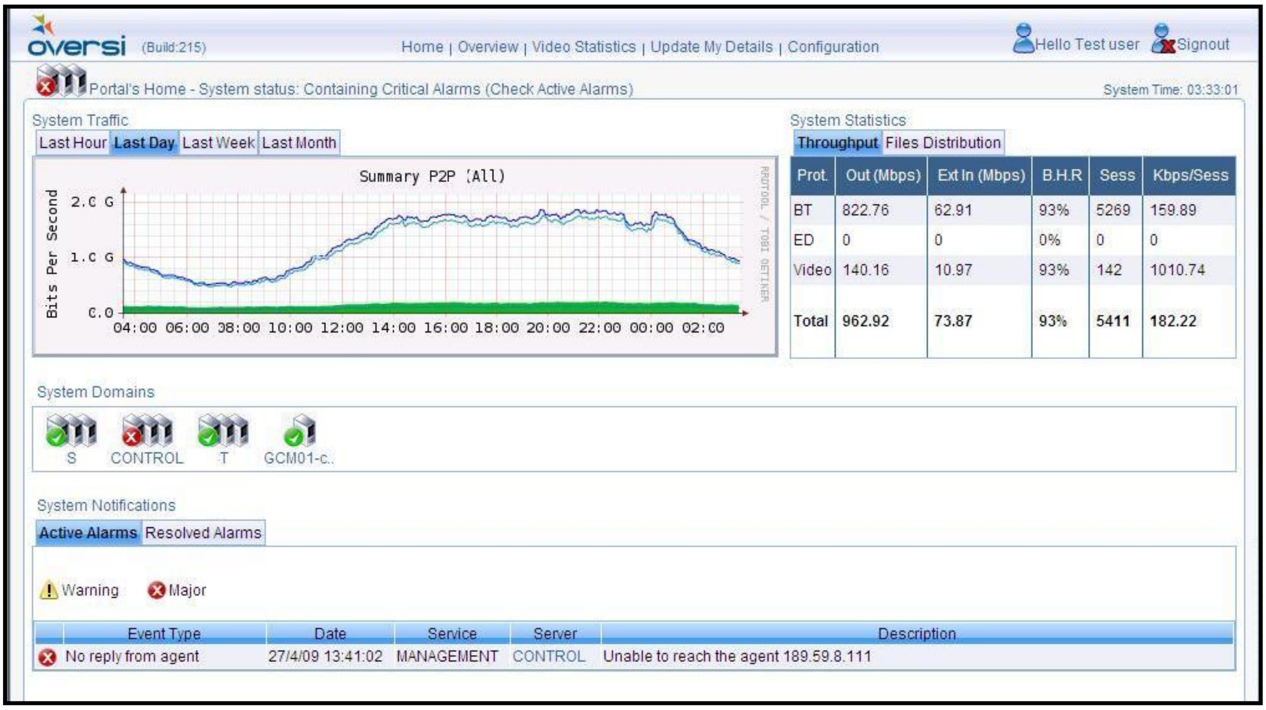
- A single GMS server
- A DMS server for the control plane elements (HM, pm, PDI, HDI etc.).
- A DMS server for each cache grid (each cache grid is composed of HTTP grid and P2P grid)

GMS Home Page

The Global Management System’s Home Page offers the following functionalities:

- **Global System Status:** The top line of the Home Page displays the Global System Status – reporting on the most severe alarm that exists in the network.
- **Per-Domain Traffic Measurements**: The System Traffic graph provides a log of per-domain traffic measurements. Each domain is represented by a colored line in the graph. Graphs are available with the following granularities:
    - Last Hour
    - Last Day
    - Last Week
    - Last Month
- **System Statistics**: The Global Statistics Table presents aggregated statistics. For a complete explanation of the table and its use, please see section 4.1.2, Viewing Domain Statistics.
- **System Domains.** This section contains links to the following domain pages:

  - **MSWE/G -** The page of the Global Management System server that provides global access to the domains.
  - **Domains** – A unique domain is defined for each POP. The domain is represented by an icon that serves as a link to a domain-level MSWE page used to manage all the control elements (PMs, HMs, PDIs, HDIs) across the ISP’s network.
- **Global Active Alarms.** This tabbed window contains a list of currently active alarms aggregated from all of the domains.
- **Global Resolved Alarms.** This tabbed window contains a list of resolved alarms aggregated from all the domains.



Portal's Home - System status: Containing Critical Alarms (Check Active Alarms)

System Time: 03:33:01

Prot.	Out (Mbps)	Ext In (Mbps)	B.H.R	Sess	Kbps/Sess
BT	822.76	62.91	93%	5269	159.89
ED	0	0	0%	0	0
Video	140.16	10.97	93%	142	1010.74
Total	**962.92**	**73.87**	**93%**	**5411**	**182.22**

Event Type	Date	Service	Server	Description
No reply from agent	27/4/09 13:41:02	MANAGEMENT	CONTROL	Unable to reach the agent 189.59.8.111

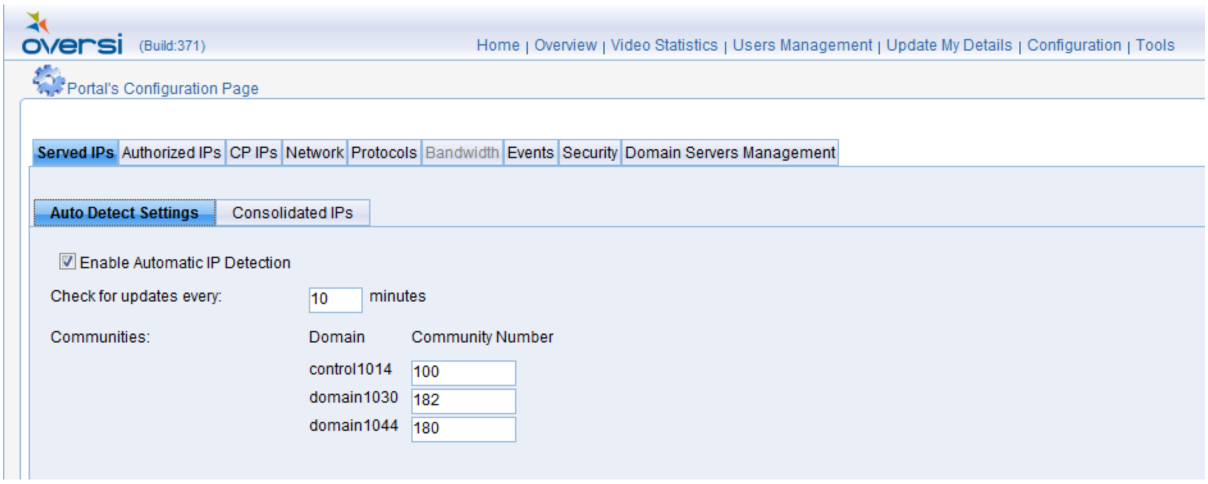
Figure 86: The MSWE/G Home Page

Multi-Domain Configuration

The MSWE/G multi-domain configuration facility uses the same screens as those described in previous chapters of this manual. Parameters applicable across the whole ISP network are configured at the global level, and parameters which are applicable only at the domain level are managed using a domain-specific server.

Global Parameters

Some MediaSwift E system parameters are configurable at the global level. These parameters are propagated automatically to the relevant servers across the domains. The parameters that are globally configurable, as displayed in the tabbed windows in Figure 87 below, are as follows:


oversi (Build:371)
Home | Overview | Video Statistics | Users Management | Update My Details | Configuration | Tools
Portal's Configuration Page
Served IPs
Authorized IPs
CP IPs
Network
Protocols
Bandwidth
Events
Security
Domain Servers Management
Auto Detect Settings
Consolidated IPs

☑ Enable Automatic IP Detection

Check for updates every: 10 minutes

Communities:

Domain	Community Number
control1014	100
domain1030	182
domain1044	180

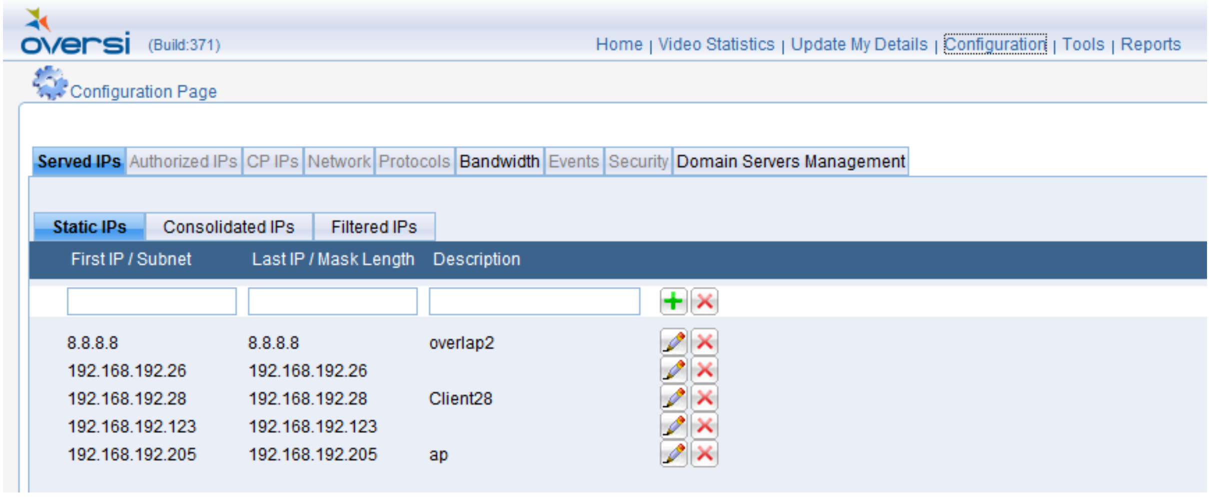
Figure 87: Global Multi-Domain Parameters

- **Authorized IPs**: Enables you to view and modify the list of the IP addresses of client workstations that are allowed to access the MSWE application, as well as the MediaSwift E system servers.
- **Network**: Enables you to define the identity of the stations authorized to manage the SNMP agent and MIB embedded in the MediaSwift E system servers, and to specify an NTP server that will be used to synchronize MediaSwift E system clocks.
- **Protocols**: Enables you to configure protocol-specific parameters for Bit Torrent, ED2K, and HTTP Video.
- **Events**: Enables you to receive notification of system events and malfunctions, either via a fault management system, or by Email.
- **Security**: Enables you to enable or disable an Access Control List (ACL) for the grid.
- **Domains Servers Management**: This tab allows you to perform monitoring and maintenance activities on Peer-to-Peer Manager (PM) Servers and HTTP Manager (HM) Servers.

Tabbed windows that can be operated only on the domain level have grayed tabs and cannot be selected.

Domain-Specific Parameters

The following parameters are configurable for domain-specific servers at the domain level only:



First IP / Subnet	Last IP / Mask Length	Description
8.8.8.8	8.8.8.8	overlap2
192.168.192.26	192.168.192.26	
192.168.192.28	192.168.192.28	Client28
192.168.192.123	192.168.192.123	
192.168.192.205	192.168.192.205	ap

Figure 88: Domain Parameters

- **Served IPs:** Defining the IP addresses of MediaSwift E servers.
- **Filtered IPs:** Selecting subscribers that will not receive caching service from the P2P Cache Server.
- **Consolidated IPs:** Automatic learning and Static configurations.

- **Bandwidth:** Limiting the bandwidth allocated by the system on a time-of-day basis.

- **Servers Management:** Configuration of Peer Manager (PM) and HTTP Manager (HM) Servers.

Chapter 9: Remote System Logging

IMPORTANT NOTE **It is good practice to use a Remote System Logging server for when multiple people can make changes to the system. Also, keeping a remote copy of the Allot system logs on a secure log server, not only gives you greater visibility from a systems management perspective, but can prove invaluable if there is ever a security incident, when the local copies of the log files on the target system have been compromised or destroyed.**

The Allot system has a comprehensive built-in logging mechanism that can be configured to channel logging information over the network to a Remote System Logging server. All events such as logging in and out together with any changes detected in the system. Event logs can be collected from all the servers as well as the logging in and out information from the central management server.

Using the logging information displayed on the Remote System Logging server you can see when someone has logged in, logged out, what changes have been made and more importantly what changes were uploaded and exactly when.

Filters can be added to the software running the Remote System Logging server and configured for local requirements. This would give you instant visibility of ONLY what is important for you to display.

Available Logs

The available log information sent to the Remote System Logging server are divided into two:

1. Web Management sessions.
   a. Logging in and out.
   b. Configuration changes.
   c. Configuration Uploading.
2. CLI sessions history for all servers.
   a. Logging in and out.
   b. CLI user actions.
3. SNMP traps sent by all servers (Sends message when trap is sent).

Login Types

There are two types of logging in to the system:

1. CLI via SSH (remote) or a local console.
   SSH uses the network cable and the local console is via the RS-232 interface.
2. Web Management login.

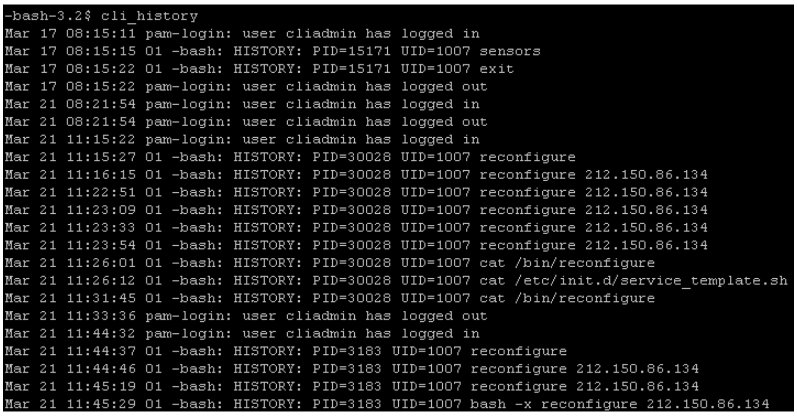
Logging Examples

We have four locations for logging:

- CLI history
- WebManagement event log (see page 4-14)
- WebManagement CLI log (see page 4-15)
- Remote syslog

CLI Logging Example

This is an example of the CLI history logs.



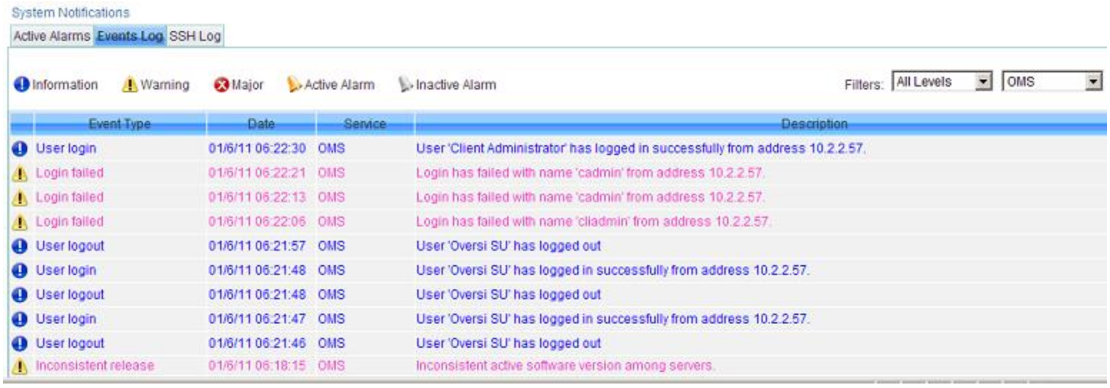
```
-bash-3.2$ cli_history
Mar 17 08:15:11 pam-login: user cliadmin has logged in
Mar 17 08:15:15 01 -bash: HISTORY: PID=15171 UID=1007 sensors
Mar 17 08:15:22 01 -bash: HISTORY: PID=15171 UID=1007 exit
Mar 17 08:15:22 pam-login: user cliadmin has logged out
Mar 21 08:21:54 pam-login: user cliadmin has logged in
Mar 21 08:21:54 pam-login: user cliadmin has logged out
Mar 21 11:15:22 pam-login: user cliadmin has logged in
Mar 21 11:15:27 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure
Mar 21 11:16:15 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure 212.150.86.134
Mar 21 11:22:51 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure 212.150.86.134
Mar 21 11:23:09 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure 212.150.86.134
Mar 21 11:23:33 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure 212.150.86.134
Mar 21 11:23:54 01 -bash: HISTORY: PID=30028 UID=1007 reconfigure 212.150.86.134
Mar 21 11:26:01 01 -bash: HISTORY: PID=30028 UID=1007 cat /bin/reconfigure
Mar 21 11:26:12 01 -bash: HISTORY: PID=30028 UID=1007 cat /etc/init.d/service_template.sh
Mar 21 11:31:45 01 -bash: HISTORY: PID=30028 UID=1007 cat /bin/reconfigure
Mar 21 11:33:36 pam-login: user cliadmin has logged out
Mar 21 11:44:32 pam-login: user cliadmin has logged in
Mar 21 11:44:37 01 -bash: HISTORY: PID=3183 UID=1007 reconfigure
Mar 21 11:44:46 01 -bash: HISTORY: PID=3183 UID=1007 reconfigure 212.150.86.134
Mar 21 11:45:19 01 -bash: HISTORY: PID=3183 UID=1007 reconfigure 212.150.86.134
Mar 21 11:45:29 01 -bash: HISTORY: PID=3183 UID=1007 bash -x reconfigure 212.150.86.134
```

Figure 89: Example of CLI History Logs

WM Logging Example

WebManagement Events Log

See page 4-14 for more details.

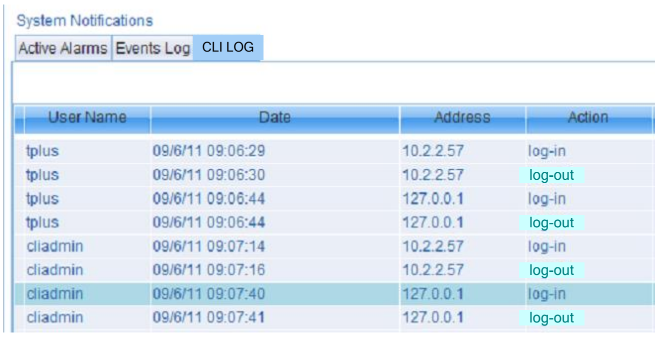


Event Type	Date	Service	Description
User login	01/6/11 06:22:30	OMS	User 'Client Administrator' has logged in successfully from address 10.2.2.57.
Login failed	01/6/11 06:22:21	OMS	Login has failed with name 'cadmin' from address 10.2.2.57.
Login failed	01/6/11 06:22:13	OMS	Login has failed with name 'cadmin' from address 10.2.2.57.
Login failed	01/6/11 06:22:06	OMS	Login has failed with name 'cliadmin' from address 10.2.2.57.
User logout	01/6/11 06:21:57	OMS	User 'Oversi SU' has logged out
User login	01/6/11 06:21:48	OMS	User 'Oversi SU' has logged in successfully from address 10.2.2.57.
User logout	01/6/11 06:21:48	OMS	User 'Oversi SU' has logged out
User login	01/6/11 06:21:47	OMS	User 'Oversi SU' has logged in successfully from address 10.2.2.57.
User logout	01/6/11 06:21:46	OMS	User 'Oversi SU' has logged out
Inconsistent release	01/6/11 06:18:15	OMS	Inconsistent active software version among servers.

Figure 90: Example of Events Log

WebManagement CLI Log

See page 4-15 for more details.



User Name	Date	Address	Action
tplus	09/6/11 09:06:29	10.2.2.57	log-in
tplus	09/6/11 09:06:30	10.2.2.57	log-out
tplus	09/6/11 09:06:44	127.0.0.1	log-in
tplus	09/6/11 09:06:44	127.0.0.1	log-out
cliadmin	09/6/11 09:07:14	10.2.2.57	log-in
cliadmin	09/6/11 09:07:16	10.2.2.57	log-out
cliadmin	09/6/11 09:07:40	127.0.0.1	log-in
cliadmin	09/6/11 09:07:41	127.0.0.1	log-out

Figure 91: Example of SSH Logs

End of Document