

NetSpective Content Filter

User Guide



Copyright © 2002-2013 by TeleMate.Net Software, LLC. All rights reserved

Although the author and publisher have made every effort to ensure that the information in this document was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Printed in the United States of America
12.09.2013 Version 4.11

TeleMate.Net Software
5555 Triangle Parkway
Suite 150
Norcross, Georgia 30092

www.TeleMate.Net

Table of Contents

Introduction	1
Passive Configurations for the NetSpective Content Filter	1
Web Proxy Configurations for the NetSpective Content Filter.....	2
Addressing Proxy Avoidance with an Integrated Solution.....	3
Software as a Service Configurations for the NetSpective Content Filter	4
Passive Features.....	5
Proxy Features	6
Not Supported in Proxy.....	6
SaaS Features	7
Not Supported.....	7
List of Ports NetSpective Uses	7
NetSpective IPv6 Passive Deployment.....	7
NetSpective IPv6 Global Proxy Deployment	8
Device Information	9
System Information	9
License Information	11
Updates	13
Statistics	14
Activity Reports.....	14
Search Term Reports.....	20
Proxy Statistics Reports.....	20
Management Reports	22
Applying an Override from the Recent Activity Report	24
Registration.....	25
User Settings	25
Management.....	26
Managers	27
Users Tab (Group Manager Only)	32
IP Partitions.....	33
Groups Tab (Group Manager Only).....	34

Advanced Tab (Group Manager Only)	35
Groups.....	36
Properties Tab.....	37
Block Override Tab.....	39
Abuse Settings.....	40
Managers	41
Group Policy.....	42
Users	45
Mobile Pairing	49
Overrides.....	51
IP Address Override	51
System Control.....	56
Device Settings.....	56
Logging Settings	57
Network	60
LDAP Sources	62
Certificate.....	65
Advanced.....	68
Filter Settings	71
Customization	71
Proxy	79
Authentication	82
Mobile Compatible Portal	83
Mobile Compatible Portal	83
Proxy or Session Based Authentication	86
User Defined Categories	87
YouTube Schools	88
SIP Options (Passive Only)	89
Advanced.....	90
Remote Agent	91
Remote Agent Connection Settings	92
Remote Agent Connection Failure	93

Remote Agent Client Settings	94
NetSpective Mobile Browser	94
Replication	96
Utilities	98
Backup & Restore.....	99
Shutdown & Reboot.....	100

Introduction

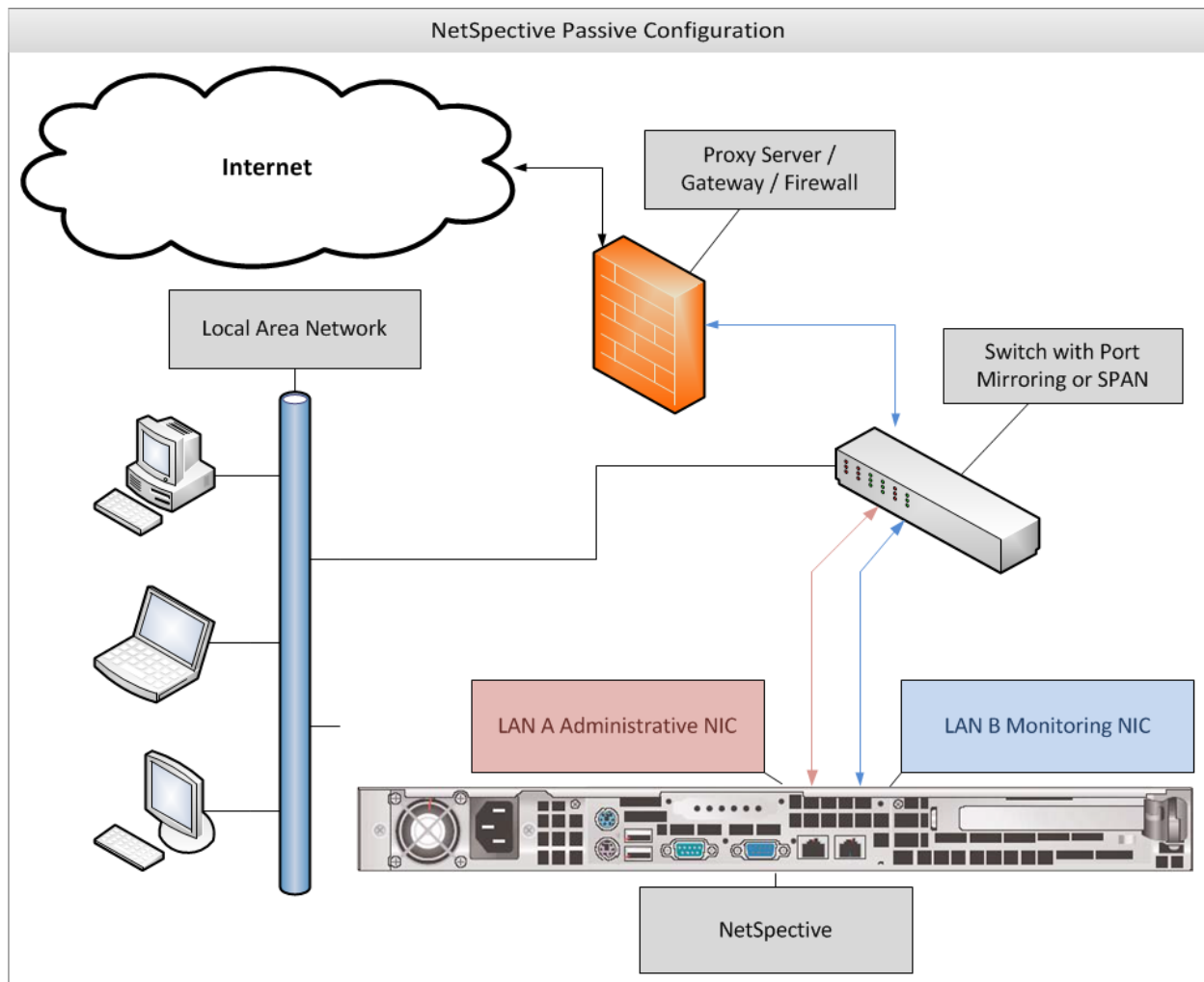
NetSpective is a sophisticated Internet content filtering appliance that maximizes the performance and security of your data network by eliminating undesirable web traffic. Its rack-mount configuration easily connects to your network, and its filtering and operational controls are simple and flexible. The web hosted interface provides real-time status updates and control, including compliance with federal filtering mandates and communications tracking requirements.

Passive Configurations for the NetSpective Content Filter

As a **Passive or Transparent** filter, NetSpective prevents network performance degradation. Side Scan™ is a firewall-independent filtering technology designed into NetSpective that reviews every packet of information going out to the web, including HTTP, HTTPS, FTP, NNTP, chat, peer-to-peer, Skype™, VoIP, and streaming media, and interrupts connections to websites or file sharing applications that have been blocked.

The signature based inspection incorporated into Side Scan enables a single NetSpective appliance to scale to support unlimited users in large networks as well as distributed networks leveraging NetSpective's ability to selectively replicate policy and device settings.

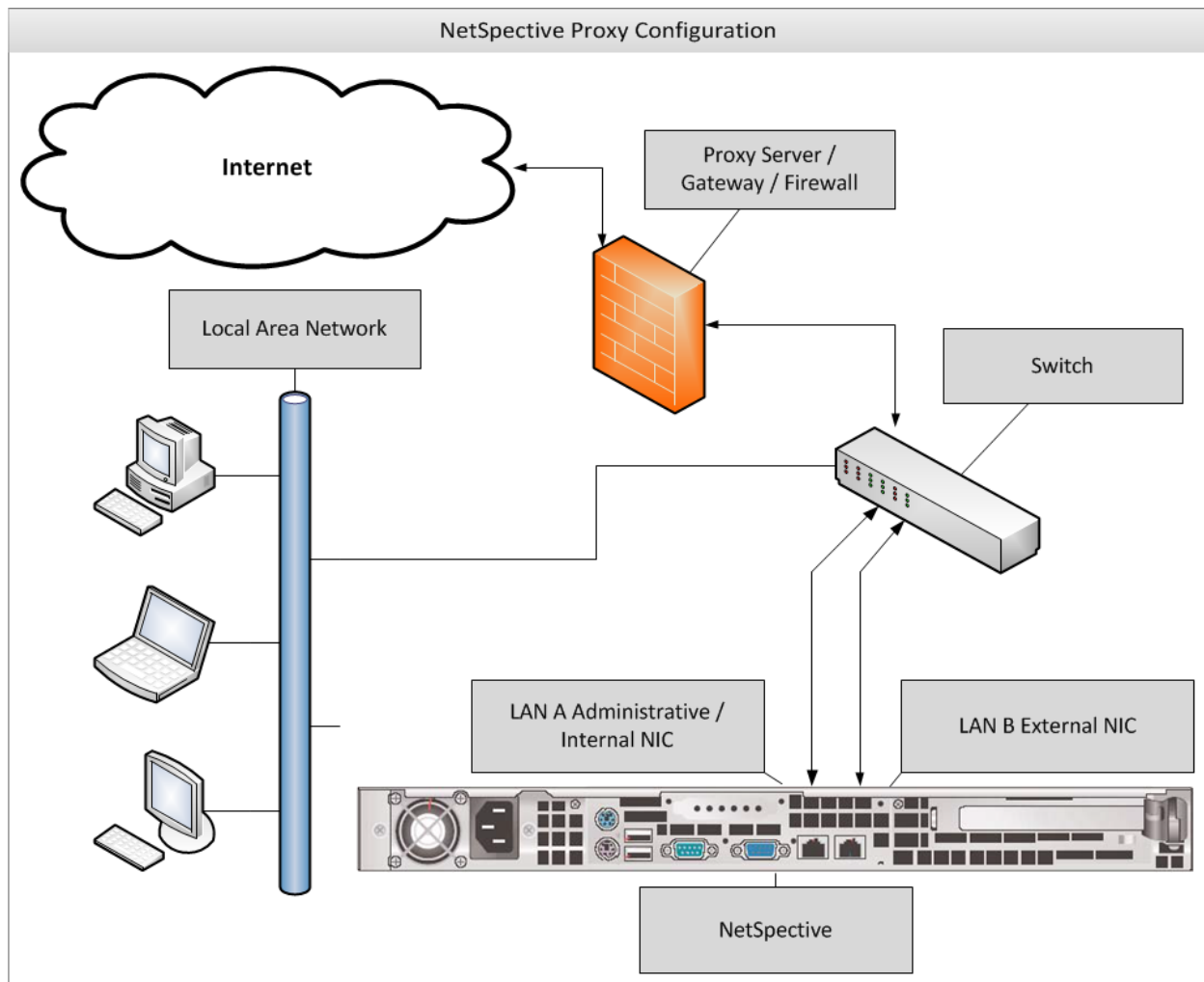
Flexible user-defined categories, URL and IP address white list or black list import functionality, file extension control, and robust search term restrictions tighten security enforcement in sensitive, closed network environments where data loss protection is critical.



LAN A sends blocking/redirection commands such as Block Pages and Portal redirects. LAN B monitors all network traffic as it passes by.

Web Proxy Configurations for the NetSpective Content Filter

As a **Web Proxy**, in addition to web filtering, NetSpective traffic shaping optimizes service for high priority applications while providing flexible control over nonessential, resource-intensive and undesirable traffic. Traffic shaping schedules communication streams into different classes of service with bandwidth limits and priorities. Control extended by group policy and Internet category allows the flexibility to block, log, or prioritize traffic.



Addressing Proxy Avoidance with an Integrated Solution

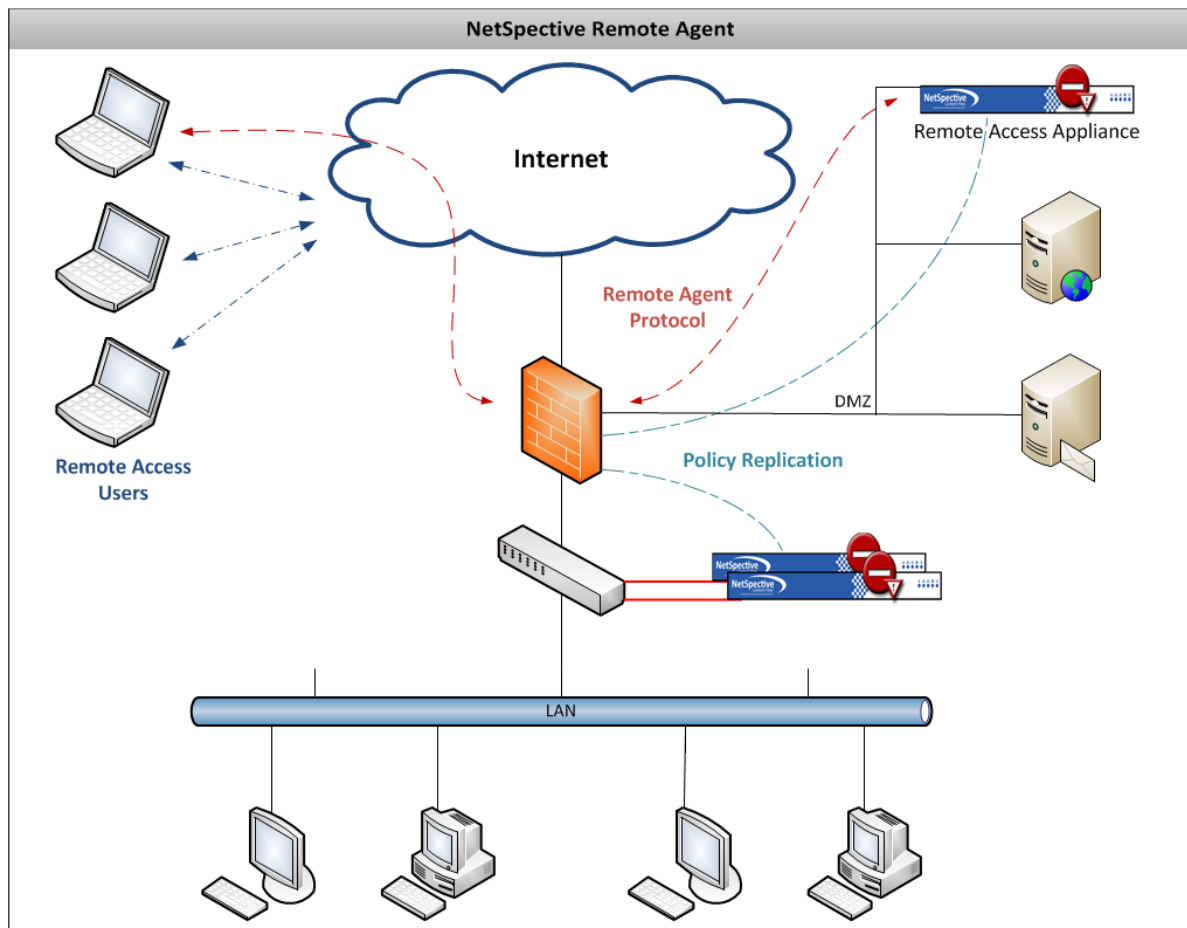
By combining both the **Passive** and **Web Proxy** solutions NetSpective expands protection by sealing security holes that often go undiscovered until the inevitable occurs. Proxy avoidance attempts can be caught without additional client-side configuration.

Software as a Service Configurations for the NetSpective Content Filter

As a **SaaS Offering**, NetSpective is capable of filtering and reporting on traffic both on and off the network, through the use of Remote Agents.

Security concerns and legal liability of threats caused by remote users increase sharply as computers leave your network's border security. Malware, spyware, phishing sites, closed P2P applications like Skype and proxy avoidance tools like Ultra Surf are the typical culprits. NetSpective's Remote Agent technology enforces internet policies regardless of physical location.

Installed at the socket level in Windows and Mac operating systems, agents protect and log all remote user Internet activity, are password protected, and provide a complete audit trail of all internet activity.



SaaS offering deploys Remote Agents to workstations, but hosts the appliance in the cloud.

Passive Features

- Configuration Options
 - Passive inspection using deep packet Side Scan technology
 - Remote Agent policy enforcement for mobile users with auditing
 - Mobile Portal with Pairing authentication for BYOD initiatives
 - IPv6 Support
- Filtering Control
 - Over 100 Categories including URL, P2P, Protocols, and Malware
 - HTTPS and SSL Deep Packet Inspection
 - Micro-updates classification of unknown content
 - Unlimited Group Policies by user, group, time of day, day of week
 - Flexible Override control with automatic expiration
 - Scalable to filter unlimited users in NAT, Non-NAT, & roaming DHCP
 - Load-balanced and failover cluster modes
 - Centralized Management with policy & configuration replication
 - Web Browser Single-Sign-On authentication for Windows domains
 - LDAP Integration for users, groups, and device managers
 - YouTube for Schools provides group association for [YouTube EDU](#) accounts
- Network Interoperability
 - Real-time Network Abuse Notification
 - Security profiles by group and category
 - Automatic system backups and One-Button product upgrades
 - On-Box drill down reports and a historical detail reporting suite

Proxy Features

- Traffic Shaping (Prioritization and limits)
- Divides bandwidth fairly between users
- SSL Validation detects categories of SSL-CERT (Server has a certificate), SSL-NOCERT, and RAW
 - Blocking RAW and SSL-NOCERT will shut down Skype, Bit Torrent, Gnutella, etc...
- Can block categories of Direct Connection - Unrated IP and Direct Connection - Unrated Hostname
 - Similar to HTTPS Unrated of passive product
- Very fast (1gbps, 5000 users, 15000 connections)
- Read only FTP->HTTP Gateway
 - You can browse to "ftp://microsoft.com" and the NetSpective will return a webpage with a directory list, or a file.
 - You can use a client like Filezilla, which supports a HTTP/1.1 proxy, to do full read/write FTP
- High Availability Clustering Support (2 NetSpectives, 1 is in standby mode if the other dies)
- Supports session based NTLM, Basic (LDAP), or Kerberos authentication
 - Works great in NAT or DHCP roaming scenarios
- Supports most pre-existing NetSpective features
 - Supports all current authentication options (Portal, LogonAgent, Remote Agent)
 - Safe Search, Abuse, Policy Reminder, Hot Updates, Overrides, Group Policy, Block Page Overrides, LDAP
- Supports IP based authentication methods like Logon Agent and Portal
- Supports the Proxy Auto Configuration protocol, used by Internet Explorer, Firefox, and other browsers / operating systems
- Supports IPv6 from proxy to internet

Not Supported in Proxy

- Terminal Server Agent is NOT supported by the proxy solution. Terminal Server users should just go through the proxy instead.
- Protocol Detection (Like Chat protocols, P2P protocols) is NOT supported. (See above about RAW and SSL-NOCERT, which can accomplish the same task).
- Protocols in the Group Policy screen only apply to Remote Agents communicating with NetSpective.
- See hover text for more exclusive features. Example: HTTPS Unrated says Passive / Remote Agent only.

SaaS Features

- Remote Agent policy enforcement for Windows and Mac users with auditing
- Hosted in the cloud and contains most features seen in Passive product
- LDAP Integration for users, groups, and device managers
 - Provided by request and requires professional services

Not Supported

- Load-balanced and failover cluster modes
- Mobile Portal with Pairing authentication for BYOD initiatives

List of Ports NetSpective Uses

Below is the list of ports used by NetSpective Passive and Proxy.

Service	Port	From Clients	To OLS	To NetAuditor
Administration Interface	TCP 80 / 443	X		
Portal	TCP 81	X		
Logon Agent	UDP 2020	X		
Terminal Server	UDP 2050	X		
Remote Agent	TCP/UDP 3001	X		
Proxy Port	TCP 3128	X		
Block Page	TCP 8080	X		
Software, Category Updates	TCP 21		X	
FTP Logging	TCP 21			X
NTP	UDP 123		X	
SSL Host Validator Service	TCP 443 / 4343		X	
Syslog	TCP or UDP 514			X

NetSpective IPv6 Passive Deployment

NetSpective Passive can be deployed in two ways:

We can deploy in an environment where the IPv4 stack is turned on.

We can deploy in an environment where the IPv4 and IPv6 stacks are turned on. This is referred to as a **Dual Stack** environment. This enables IPv6 passive filtering.

When working in a dual stack environment, we are making the assumption that every workstation can receive IPv4 traffic. While NetSpective will monitor all IPv4 and IPv6 traffic on the network, we will only send block pages and portal pages across IPv4. Traffic can still be intercepted and logged regardless of which stack the traffic appears on. However if you wish to receive a block page, the IPv4 stack will still need to be enabled.

NetSpective IPv6 Global Proxy Deployment

NetSpective Global Proxy should also be deployed in a dual stack environment only. The difference is, the proxy appliance will be configured with both an IPv4 and an IPv6 address.

Device Settings

admin | [help](#) | [logout](#)

Search:

Group: System

Network (IPv4)

Network (IPv6)

Certificate

Advanced

The NetSpective device allows you to configure some network settings, such as the network interfaces, DNS settings, and static routes. These settings will allow the device more flexibility and a greater range of control in more complicated networks. Note: Changing an interface's IP or netmask will require a restart of system services which may take a few minutes.

IPv6 Settings

☒ Enable IPv6 Network Interfaces and Static Routes

Interfaces

Interface	IP	Prefix	Port	Status	Mac Address
Admin	2001:480:e340:28::2:100	64	Lan A	1000 Full	00:0c:29:c3:f9:9e
External	2001:480:e340:a::ffff:10	64	Lan B	1000 Full	00:0c:29:c3:f9:a8

Default Gateway: 2001:480:e340:28::1

Additional Routes

<input type="checkbox"/>	Destination	Prefix	Gateway	Interface
<input type="checkbox"/>	::	0	2001:480:e340:a::1	External

Delete

Add

As the picture above shows, there are now two Network tabs. One for IPv4 and one for IPv6. The appliance can still be configured as a single port proxy, or a dual port proxy. Each interface will require an IPv4 and IPv6 IP address. The appliance still relies on the environment being dual stack for receiving block pages across IPv4. The minimum requirement for enabling proxy is to have an Admin IP address and an associated Default Gateway. If you are using a dual port proxy, then you will want to specify an additional route for the External interface.

Device Information

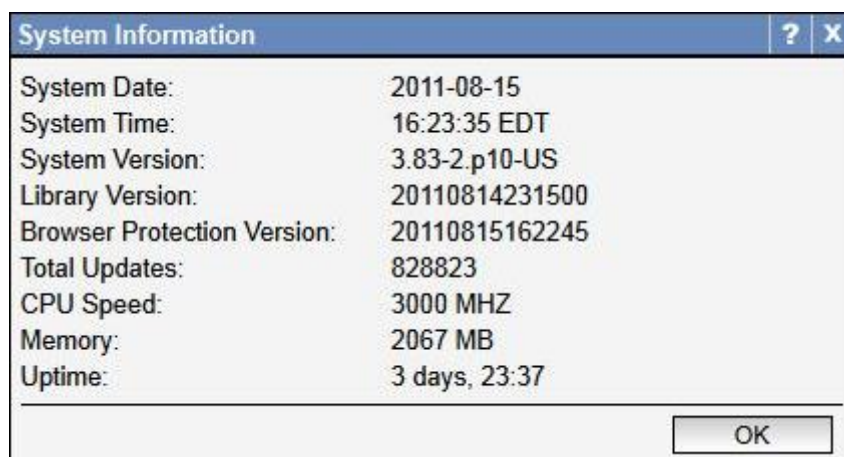
Under the Device Information heading, you will find links to various sections providing information on the version of NetSpective, licensing information, availability of updates, as well as network and CPU utilization. This section also provides links for easy access to your reporting tools.



General	
Host Name	Displays the host name of the current NetSpective device. Clicking the host name will open a dialog with additional system information.
License	Displays the current status of your NetSpective license. Possible status values are Inactive, Active, Grace, and Expired. Clicking the status will open a dialog with additional license information.
Updates	Displays the current status of device updates. Possible status values include Available, In Progress, and Current. Clicking the status will take you to the device updates page.
CPU Load	Displays the device's current CPU utilization as a percentage of the total.
Network	Displays the device's current network load in Mbps (1,000,000 bits per second). For passive devices, this is the total traffic seen by the Monitoring interface. For proxy devices, this is the total traffic being proxied for clients.
Statistics	The 'Statistics' link provides a quick look at the internet activity on your NetSpective device.
Reports	If enabled, the 'Reports' link will point to an install of NetAuditor somewhere on your network. NetAuditor can provide you with more detailed information about your Internet traffic using logs collected by your NetSpective device.

System Information


You can find the System Information dialog window by clicking on the hostname of your device. Here you can see information about your appliance including the time and date, the version of software the appliance is running, information about the appliance's CPU speed and memory, as well as the amount of time since the appliance was last rebooted.



System Information	
System Date	Displays the device's current date.
System Time	Displays the device's current time at the moment you opened the dialog. The time zone will also be displayed in abbreviated form. To change the time zone or NTP server visit the 'Advanced' tab on the Device Settings page.
System Version	Displays the device's software version. Go to the Updates section to check for new updates that may be installed manually or to enable automatic updates.
Library Version	Displays the device's library (categorization list) version. The version contains a date and time value indicating when it was created.
Total Updates	Displays the total number of categorization additions or changes contained in the last library update that the device downloaded and processed. A library update can be incremental (containing only the changes since the last update) so the number displayed here does not necessarily indicate the total number of entries in the categorization list.
CPU Speed & Memory	Displays the device's current hardware information.
Uptime	Displays the number of day(s), hour(s) and minute(s) that the device has been running since the last boot.

License Information

This section provides detailed information on the license of your NetSpective Appliance. If you wish to purchase additional licenses, or renew your subscription, please contact TeleMate.Net Software at (678)-589-7100.



The image shows a Windows-style dialog box titled "License Information". It contains two main sections: "License Information" and "License Status". The "License Information" section lists various parameters and their values. The "License Status" section provides a summary of the license's current state and what features are included. At the bottom, there is a copyright notice and an "OK" button.

License Information	
Product Level:	PURCHASED
Filtering Mode:	Proxy
Maximum Users:	1000
Maximum Connections:	2000
Maximum Mbps:	10
Remote Agent Users:	0/1000
Terminal Server Ports:	0/100000
Hostname:	wga0u6ou
Subscription Start:	2008-12-03
Subscription End:	2011-12-04
License Key:	2I70M-I0CHU-G1L0S-DGTPF

License Status	
License is up to date	
Adaptive Filtering Upload is Licensed	
Micro Updates are Licensed	
Browser Protection is Licensed	

Copyright © 2003-2011 TeleMate.Net Software, LLC. A global provider of Unified Call Management and Internet Security Solutions.

OK

License Information	
Product Level	Displays the device's license level, which may be PURCHASED, EVALUATION, or NFR (Not For Resale).
Filtering Mode	Displays the device's filtering mode, which may be Proxy or Passive.
Maximum Users	Displays the maximum number of users your NetSpective is currently licensed to support.
Maximum Connections (Proxy Only)	Displays the maximum number of connections the device will accept concurrently from clients.
Maximum Mbps (Proxy Only)	Displays the maximum bandwidth the proxy can receive or transmit. This value limits the total of receive and transmit bandwidth.
Remote Agent Users	Displays the number of currently logged on Remote Agent users and the maximum number of Remote Agent users for which the device is licensed.
Hostname	Displays the device's unique identifier. All log files generated by the device will have this hostname embedded in the file name.
Subscription Start	Displays the date that your subscription to the NetSpective Online Service began.
Subscription End	Displays the date your subscription to the NetSpective Online Service will end.
License Key	Displays the device's license key code. If you have enabled log file encryption, NetAuditor will need this key in order to decrypt the device's log files.
License Status	Displays the device's current license status and features.

Updates

The NetSpective device communicates with the NetSpective Online Service to receive updates and to send Adaptive Filtering, registration, and diagnostic information. The device may receive categorization changes, license renewals or changes, and system software updates. All communication is done via FTP and sensitive data is encrypted.

The screenshot shows the 'Updates' web interface. At the top, there are links for 'admin', 'register', 'help', and 'logout'. Below these are icons for a folder, a document, and a magnifying glass, followed by a 'Search:' text box. To the right is a 'Group:' dropdown menu set to 'System'. The main content area has a heading 'Updates' and a paragraph explaining that the device communicates with the NetSpective Online Service to receive category and software updates and send Adaptive Filtering data. It mentions that update status and/or communication errors are indicated below, and that if a system software update is available, the user can click 'Install Update' to install it. Below this is a section titled 'Update Status' with a black header. The status text reads: 'Jan 02 21:00:02 Downloaded 1 update'. At the bottom of the status section is a 'Server:' text box containing '38.81.65.41'. To the right of the server box are two buttons: 'Get Updates' and 'Install Update'. Below the status section is a section titled 'Automatic Update'. It contains a checked checkbox for 'Enable Automatic Update'. Below this are three dropdown menus: 'Update Time' set to '12:00 AM', 'Micro Updates' set to 'Every 10 Minutes', and 'Days' with checkboxes for 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are checked.

Automatic or Manual Updates

The default and recommended option is to enable Automatic Update, which ensures the device always has the latest categorization list. You may set the time of day and the day(s) of the week that you want the automatic update to occur. Alternatively, you can click the "Get Updates Now" button to immediately start an update operation.

Micro Updates

If you are licensed for this feature, you may set a higher frequency interval to check in with the Adaptive Filtering Service for updates. You may configure NetSpective to check for updates every 10 minutes, 1 hour, or 3 hours in addition to the regular daily update. Micro Updates are only enabled on days for which Automatic Update is enabled.

Installing System Updates

Certain system software updates may require a confirmation by the System Administrator before they are installed. If there is a system update ready to be installed, its name and version will be displayed in the status window and the "Install System Update" button will be enabled. Click the "Install System Update" button to install the update. The device may reboot itself as part of the install process.

Statistics

NetSpective provides several built in, real time, 'gas gauge' type reports as well as the ability to view or search a recent portion of the traffic activity log. For more detailed, flexible, and historical reporting, you may use NetAuditor to analyze your NetSpective traffic logs.

The real time reports are cleared every night at midnight. The Blocked Sites and Search Reports have a limited size data buffer that may be reset at various times during the day. These reports display a note at the bottom indicating from how far back data is available.

Recent Activity (Passive & Proxy), Recent Activity Summary (Proxy only), Blocked Sites and Block Page Overrides have the option to add overrides from the report. See Overrides in Reports for more information.

Activity Reports

Activity Reports are comprised of various access statistics illustrating the web traffic across your network. These include reports based on blocks, category accesses, protocols, groups and user summaries.

Recent Activity

This report shows recent internet activity blocked or monitored by NetSpective. Use the search field to find specific hostnames, users, IP addresses, or categories. Icons are shown if the request was blocked, an abusive category, or from a remote agent. You may use the search bar at the top of the report to search for specific activity. Recent Activity will also report on IPv6 traffic. Websites typically default to IPv4 if it is enabled, but you will find some that prefer IPv6. In the example below, Google is a good testing ground for IPv6 traffic. The IP address shown is that of the user workstation requesting the webpage from Google.


Statistics





TELEMATE|william.babji | register | help | logout

Search: eric.turner

Report: Recent Activity

Recent Activity				
Jul 08 11:21:13	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Admin Allow
HTTPS://atl01exs10.telemate.net:443				
Jul 08 11:20:28	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Internet Tools
HTTPS://www.google-analytics.com:443				
Jul 08 11:20:28	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Internet Tools
HTTPS://www.google-analytics.com:443				
Jul 08 11:20:27	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Internet Tools
HTTPS://www.google-analytics.com:443				
Jul 08 11:20:27	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Internet Tools
HTTPS://www.google-analytics.com:443				
Jul 08 11:20:10	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Internet Tools
HTTPS://clients6.google.com:443				
Jul 08 11:19:30	TELEMATE eric.turner	Development	[2001:470:e390:28::4:0]	Web E-Mail
HTTPS://mail.google.com:443				

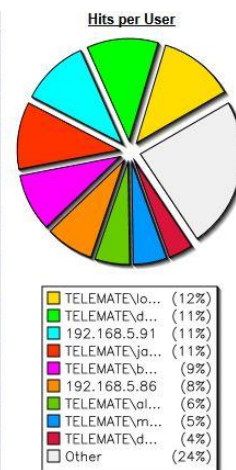
In proxy mode, you may click the  icon to view additional data such as the priority, duration, total bytes received and sent, and any error status.

Recent Activity				
	Aug 06 11:20:11	TELEMATE\reuben.richardson	Support	192.168.5.230:4236 Web E-Mail
HTTP://mail.google.com/mail/channel/bind?VER=6&it=2519751&at=xn3j35fbyfao6y68nwcfxgd6f6figi&RID=rpc&SID=57F45830F55F01CD&C=0&AID=291&TYPE=xmhttp&z=d3g9b4-81a3c7&t=1				
Priority:	Medium	Transmitted (KB):	1.662	
Duration:	00:03:17	Received (KB):	0.513	
Status:	200	Authentication:	Negotiate - Kerberos	
	Aug 06 11:20:10	TELEMATE\michael.hartley	Sales	192.168.5.185:3868 Travel
HTTP://68.142.229.15/521.mail.yahoo.com/ya/securedownload?clean=0&fid=Sent&mid=1_331464_AHMwvs4AAJeESnpKMwNpqyh8oKY&pid=2&tnf=&prefFile name=P1010598.JPG&cred=B_ANcP2IQxsK9iz5fpat5yEjxS1LTWwbkbNwnd6wZD0TckBATTvmYGnFkua0c_w_7_fj2XcwQqoSit2Kwvdq_8kNB6j1p2IIP9OQRQZKGN o&ts=1249572030&ner=yemail&sig=j5dlUgOcaZRsNd1eAt5OkA--				
	Aug 06 11:20:05	TELEMATE\michael.hartley	Sales	192.168.5.185:3673 Web E-Mail
HTTP://us.f521.mail.yahoo.com/ya/download?clean=0&fid=Sent&mid=1_331464_AHMwvs4AAJeESnpKMwNpqyh8oKY&pid=2&tnf=&prefFilename=P1010598.JPG				
Priority:	Medium	Transmitted (KB):	1.879	
Duration:	00:00:00	Received (KB):	0.714	
Status:	302	Authentication:	Negotiate - Kerberos	
	Aug 06 11:20:04	TELEMATE\michael.hartley	Sales	192.168.5.185:3744 Web E-Mail
HTTP://us.mc521.mail.yahoo.com/mc/showMessage?fid=Sent&filterBy=&midIndex=0&mid=1_331464_AHMwvs4AAJeESnpKMwNpqyh8oKY&f=1&m=1_331464_AHMwvs4AAJeESnpKMwNpqyh8oKY%2C1_331126_AGswvs4AArxeSnpJ%2BgD5A0voaXU%2C1_330789_AGswvs4AAwLSnpJbQJBVS0Bsdg%2C1_330452_AG4wvs4AAHTThSnpJAQCNPJCJ9nfc%2C1_330115_AG8wvs4AAFySnpImgF2XDnYBa4%2C1_329778_AG0wvs4AAVEzSnpINwweBfBMQWQw%2C&sort=date&order=down&startMid=0&pSize=25&hash=709e78335c8f2d6faaf796fe95cc20&jsrand=9639149&acrumb=uhY4W76AllZ&rand=1937009181&enc=auto&cmd=msg.sc an&pid=2&fn=P1010598.JPG&view=none				

Active Users (Top 20) (Passive Only)

This report shows the top Internet users. Since the counter queue is cleared daily at midnight, the most accurate report will be generated at the end of each workday.

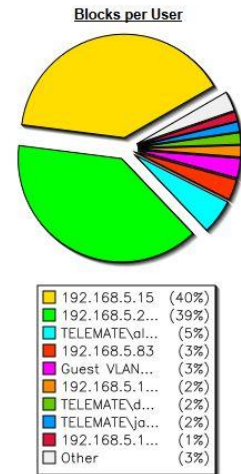
User	Hits	Blocks
TELEMATE\ola.orr	7530	26
TELEMATE\daniel.garcia	7101	37
192.168.5.91	6683	0
TELEMATE\james.wooden	6640	32
TELEMATE\brett.hujik	5699	0
192.168.5.86	4775	0
TELEMATE\alysha.mccree	3448	113
TELEMATE\miles.ethridge	3319	11
TELEMATE\darrin.patterson	2411	0
TELEMATE\sean.oneil	1885	0
mark	1793	0
TELEMATE\jeff.workman	1642	4
192.168.5.87	1149	0
192.168.5.15	909	828
TELEMATE\reuben.richardson	907	0
192.168.5.205	816	816
108.108.27.37	672	0
Guest VLAN-192.168.225.114	504	63
TELEMATE\eric.turner	426	0
66.87.110.35	290	0



Blocked Users (Top 20) (Passive Only)

This report shows the users with the most blocked traffic.

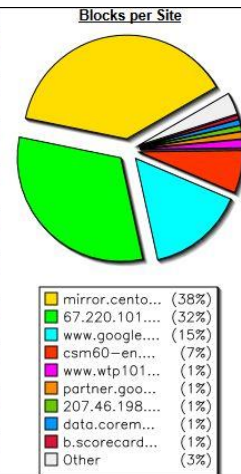
User	Hits	Blocks
192.168.5.15	909	828
192.168.5.205	817	817
TELEMATE\alysha.mccree	3448	113
192.168.5.83	74	67
Guest VLAN-192.168.225.114	504	63
TELEMATE\daniel.garcia	7103	37
192.168.5.169	39	37
TELEMATE\james.wooden	6645	32
192.168.5.170	31	30
TELEMATE\ola.orr	7533	26
192.168.5.177	14	14
TELEMATE\miles.ethridge	3321	11
192.168.5.178	11	6
TELEMATE\jeff.workman	1645	4
192.168.5.155	1	1
192.168.5.146	1	1
10.48.132.13	1	1



Blocked Sites (Top 20)

This report, in "leader-board" format, shows the top blocked sites by root URL, and how many times a user attempted to access each site.

Site	Category	Blocks
mirror.centos.org	Technology	180
67.220.101.134	Not Rated	148
www.google.com	Web Search	71
cs60-en.url.trendmicro.com	Software Update	31
www.wtp101.com	Anonymous Proxy & Hacking	6
partner.googleadservices.com	Web Search	5
207.46.198.112	Web E-Mail	4
data.coremetrics.com	Advertising	4
b.scorecardresearch.com	Advertising	3
mirrorlist.centos.org	Technology	3
www.googleadservices.com	Advertising	3
17.172.36.71	Not Rated	2
74.125.67.108	Not Rated	1
api.search.live.net	Web Search	1
googleads.g.doubleclick.net	Advertising	1
hiddenapp.com	Technology	1
imagec10.247realmedia.com	Advertising	1
iphone.playhaven.com	Gambling	1
oasc10010.247realmedia.com	Advertising	1
s.youtube.com	Web Search	1



Category Access Summary (Passive Only)

This summary report gives you a view of your NetSpective's daily activity. You can view how many hits have been allowed for specific categories.



Category Block Summary (Passive Only)

This summary report gives you a view of your NetSpective's daily activity. You can view how many blocks were made for a specific category.



Category Summary (Top 100) (Proxy Only)

This report gives you a view of your NetSpective's daily activity. You can view how much data was received and transmitted as well as how many blocks were made for a specific category.



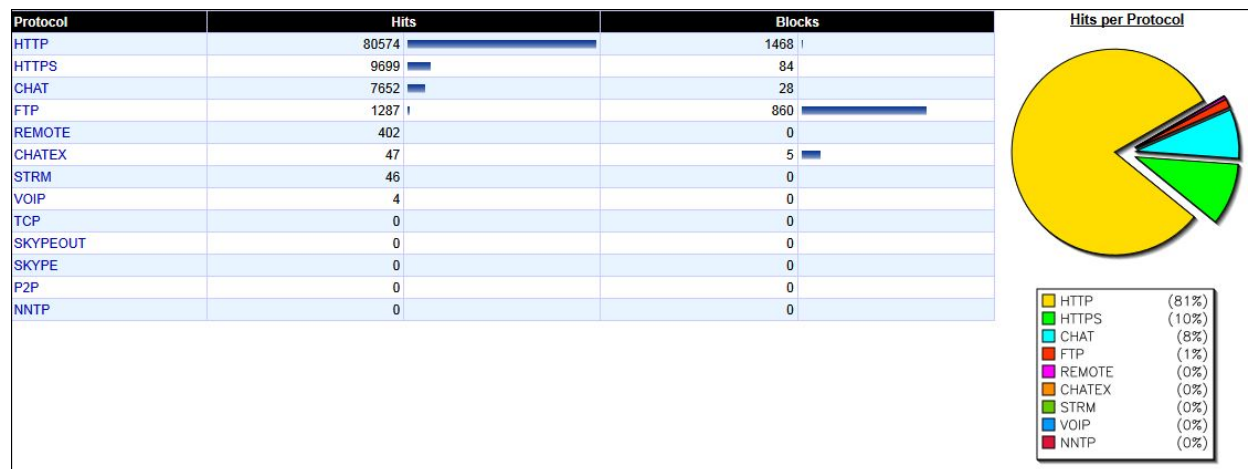
Group Summary (Top 100) (Proxy Only)

This report gives you a view of a group's daily activity. You can view how much data was received and transmitted for each priority class. Also, you can see how many blocks were made for that specific group.

Group ▼	Received (MB)			Transmitted (MB)			Blocks
	Low	Med	High	Low	Med	High	
Development	-	18.657	-	-	3.518	-	24
Public	0.696	0.600	-	1.374	0.032	-	-
Sales	-	165.210	-	-	14.609	-	-
Support	-	15.491	24.701	-	2.332	2.590	-

Protocol Summary (Passive Only)

This report lets you view the amount of traffic by protocol, and the ratio of hits to blocks for each protocol.



Protocol Summary (Proxy Only)

This report gives you a view of each protocol's daily activity. You can view how much data was received and transmitted for each priority class. Also, you can see how many blocks were made for that specific protocol.

Protocol ▼	Received (MB)			Transmitted (MB)			Blocks
	Low	Med	High	Low	Med	High	
FTP	-	0.001	-	-	0.001	-	-
HTTP	0.588	189.947	-	0.501	16.524	-	24
RAW	0.113	10.357	24.706	0.878	4.079	2.603	-

User Summary (Top 100) (Proxy Only)

This report gives you a view of each user's daily activity. You can see the number of connections, the data received and the data transmitted for each priority class. Also, you can see how many blocks were made for that specific user.

User ▼	Connections			Received (MB)			Transmitted (MB)			Blocks
	Low	Med	High	Low	Med	High	Low	Med	High	
TELEMATE\brandon.tabaska	-	-	-	-	0.176	-	-	0.010	-	-
TELEMATE\cindy.frederick	-	-	-	-	25.346	-	-	3.005	-	-
TELEMATE\craig.smilowitz	-	-	-	-	15.007	-	-	2.817	-	-
TELEMATE\david.jury	-	-	-	-	11.773	-	-	1.085	-	-
TELEMATE\domain.admin	-	-	-	-	0.423	-	-	0.018	-	-
TELEMATE\eric.turner	-	1	-	-	17.537	-	-	2.779	-	24
TELEMATE\jacob.kaseric	-	-	-	-	0.942	-	-	0.159	-	-
TELEMATE\james.wooden	-	1	-	-	13.565	-	-	3.042	-	-
TELEMATE\jeff.workman	-	1	-	-	17.952	-	-	1.550	-	-

Search Term Reports

These reports illustrate the phrases users have entered into popular search engines. You may choose between the top 100 popular searches, or the most recent 100 searches users have entered.

Popular Searches (Top 100)

This report shows the most frequently used search queries. If the search query matched an override the override's category will also be displayed.



Recent Searches (Last 100)

This report shows the most recent search queries entered into web search engines. If the search query matched an override the override's category will also be displayed.

Keyword	Category
secure ssl certificate	
secure ssl certificate	
john letchford	
yahoo	
list of major industries	
mapquest	
wadley ga news	

Proxy Statistics Reports

These reports show statistics related to the Proxy solution. These sections report on the various bandwidth and user statistics, multi-appliance cluster modes, as well as the top 100 DNS cached entries on the appliance.

Proxy Overview (Proxy Only)

This report shows NetSpective's current bandwidth and user load. Bandwidth, active user, and active connection counts are shown for each priority level and as a grand total. "Client Connections" shows the total number of active and idle client connections. "Concurrent Users" shows the number of unique authenticated and unauthenticated users.



Client Connections	Concurrent Users			
34	11			
	Low	Medium	High	Total
Receiving (Mbps)	0.00	0.01	0.00	0.01
Transmitting (Mbps)	0.00	0.01	0.00	0.01
Active Users	0	9	1	9
Active Connections	0	22	4	26

Cluster Status (Proxy Only)

This report shows all detected NetSpective devices on your network. Each report line shows the Admin IP, Internal IP (if one is configured), hostname, and cluster status of each device. You may use this report to view which device in a fail over cluster is active and if any devices are down.

Admin IP ▼	Internal IP	Host Name	Cluster Mode	Age (Seconds)
192.168.5.32	192.168.5.33	w634214p	None	2
192.168.5.41	192.168.5.42	wga0u6ou	Load Balanced	10

Connection Detail (Top 100) (Proxy Only)

This report shows all currently active or idle client connections. Idle connections show the user name or IP address, the time the connection has been idle, and the internal and external addresses and ports currently in use by NetSpective. Active connections additionally show the host and domain, path, total bytes received and sent, the priority, quota usage, group name, and category name. Click the  icon to view all information for a connection. Click the  icon to immediately close a connection.

The Quota column shows the percentage of a connection's fair and guaranteed bandwidth quota that is being currently used. If a connection's quota value is over 100%, it is using more than its fair share of bandwidth, which is allowed when other users have slower or idle connections. Sorting the connections by the Quota column lets you quickly find out which connections and users are currently using most of the available bandwidth.

User	Domain	Received (MB)	Transmitted (MB)	Quota (%) ▼	Duration	
TELEMATE\domain.admin		-	-	38.00	00:00:03	⊘
TELEMATE\reuben.richardson		-	-	33.00	00:00:02	⊘
Group: Client Address: 192.168.5.230:4575 Category: Local Address: 192.168.5.41:59705 Priority: Idle Server Address: 74.125.67.18:80 Authentication: Negotiate - Kerberos Path:						
TELEMATE\jeff.workman	mail.google.com	-	0.002	12.00	00:00:00	⊘
Group: Sales Client Address: 192.168.5.185:4765 Category: Web E-Mail Local Address: 192.168.5.41:57543 Priority: Medium Server Address: 74.125.67.18:80 Authentication: Negotiate - Kerberos Path: /mail/channel/bind?VER=6&it=2700019&at=xn3j33ykl3tuu4bjbkx70t1dk3x1m&SID=9FCE1E97D59F2210&RID=94340&zx=35zsmn-5cqst4&t=1						
TELEMATE\jennie.drake	scs.msg.yahoo.com	0.028	0.089	0.00	67:28:19	⊘

DNS Cache Entries (Top 100) (Proxy Only)

This report shows NetSpective's forward DNS cache. Domains and their corresponding IP addresses are shown in order of most recently accessed to least recently accessed. Also shown is each entries time until expiration.

Domain	IP	Timeout (Seconds)
mail.google.com	74.125.67.83	111
0.channel10.facebook.com	69.63.176.170	114
newsrss.bbc.co.uk	212.58.226.140	109
fxfeeds.mozilla.com	63.245.209.93	108
en-us.fxfeeds.mozilla.com	63.245.209.93	108
tap.rubiconproject.com	174.129.205.86	103
csm51.url.trendmicro.com	24.143.193.10	Expired
tap-cdn.rubiconproject.com	72.21.91.20	93
w.sharethis.com	8.17.64.63	86
www.google.com	74.125.67.147	Expired
botd.wordpress.com	76.74.255.125	100

Management Reports

These reports will offer managers and admins tools to assist them in managing users. They also help in managing locked users as well as other NetSpective managers.



Block Page Overrides (Last 100)

This report displays the most recent block page overrides for the current day. The time, group name, and the domain that was overridden are shown. If a manager authenticated the override, the manager name is also shown. You may use the search bar at the top of the report to search for a specific group, domain, or manager.

Time	Group	User	Manager	Domain
11:02 AM	Brett's Group	192.168.5.105	TELEMATE\brett.hujik	www.playboy.com

Currently Locked Users

This report shows users who are currently locked down by NetSpective's abuse detection. Each entry in the report displays the user's name or IP address, the expiration time of the lock down, and the user's total number of attempted accesses to abusive categories for the day. To unlock a user, click the unlock icon next to the user's name. To unlock all users in all groups you manage, click the 'unlock all users' icon at the top right of the report.

User	Abuse Hits	Lock Expires	
TELEMATE\brett.hujik	16	12:30	

Previously Locked Users

This report shows users who were previously, but no longer, locked down by NetSpective's abuse detection. Also shown is the users' total number of attempted accesses to abusive categories for the day.

User	Abuse Hits
TELEMATE\brett.hujik	16

LDAP Managers

This report displays each authorized LDAP manager. It also includes the manager's security level and the number of groups they are managing.


Managers - LDAP	
PRODMGMTVAARONOUTLAW	Group Manager (4 Groups)
PRODMGMTABBHEYHAGER	Group Manager (0 Groups)
PRODMGMTABBIEBACON	Group Manager (0 Groups)
PRODMGMTABBYMERCADO	Group Manager (0 Groups)

Local Managers

This report displays each authorized local manager. It also includes the manager's security level and the number of groups they are managing.

Managers - Local	
admin	Administrator
brett	Group Manager (4 Groups)
District 1 Admin	Group Manager (1 Group)

Applying an Override from the Recent Activity Report

Overrides from reports are only available in Recent Activity (Passive & Proxy), Recent Activity Summary (Proxy only), Blocked Sites, and Block Page Overrides. To add an override, hover over the URL or domain and an icon  should appear. Click the icon, and select *Add Override* from the menu.

Recent Activity				
Aug 15 16:21:19	TELEMATE\ola.orr	Support	192.168.5.160	Portal
HTTP://rdir.att.net/s/editorial.dtl?ep=23&eeld=7817645&nocache=73				
Aug 15 16:21:18	USRRHANSCOM03	Exempt but Monitored	192.168.5.91	Government
HTTP://www.nsa.gov/_root/images/footer_print.jpg				
Aug 15 16:21:18	USRRHANSCOM03	Exempt but Monitored	192.168.5.91	Internet Tools
HTTP://www.google-analytics.com/_utm.gif?utmwv=5.1.4&utms=1&utmn=935578982&utmhn=www.nsa.gov&utms=ISO-8859-1&utmsr=1280x1024&utmsc=24-bit&utmul=en-us&utmje=0&utmfl=10.1%20r53&utmdl=Career%20Opportunities%20at%20the%20National%20Security%20Agency%20(NSA)&utmhid=990650193&utmr=http%3A%2F%2Fwww.google.com%2Furl%3Fsa%3D%26source%3Dweb%26cd%3D1%26ved%3D0CDcQwMoADAA%26url%3Dhttp%253A%252F%252Fwww.nsa.gov%252Fcareers%252F%26rct%3Dj%26q%3Dnsa%26ei%3Dtn9JTyKBL8PagQIE94zCDA%26usg%3DAFQJCNHUXtobQYTwSh2l9zReIWBZJ5QM2w&utmip=%2Fcareers%2F&utmcc=UA-20753548-1&utmcc=...utma%3D176212410.2127950088.1313439687.1313439687.1%3B%2B__utmz%3D176212410.1313439687.1.1.utmcsr%3Dgoogle%7Cutmccn%3D(organic)%7Cutmcmd%3Dorganic%7Cutmctr%3Dnsa%3B&utmu=q~				

Override

Overrides may be created to allow, block, or recategorize specific web sites, news groups, IP addresses, web search terms, or file types. Overrides are assigned per group with the System group taking precedence over all other groups.

Group:

System

Type:

Domain

Override:

rdir.att.net

Comment:

Category:

Admin Block

Referrer Depth:

None

OK

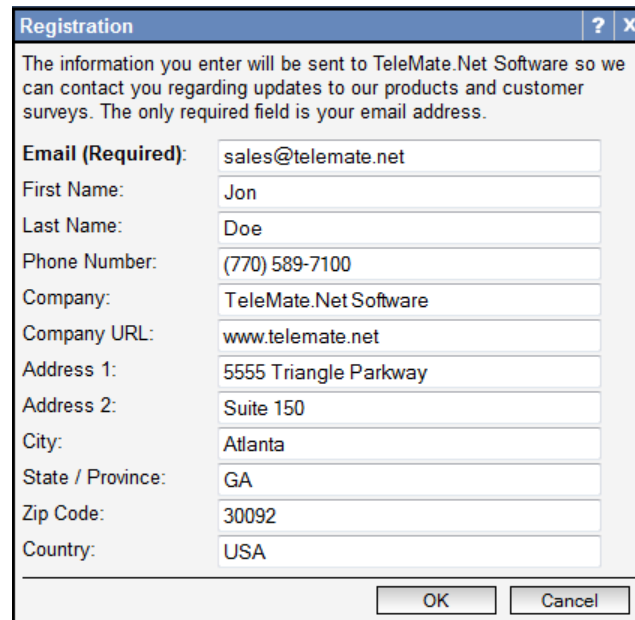
Cancel

Once the dialog has opened, select the System group to create system-wide overrides or select a group for group overrides. You can modify the type and override to fit your needs. Comments are optional and are there only for your own reference. Finally, select the category you wish to assign from the Category drop down box. Select 'Admin Allow' or 'Admin Block' to always allow or block the activity, or select a user defined or standard category. Click the 'OK' button when finished.

The override is now active and will be listed in the Overrides section. For more information on managing overrides visit the help on Overrides.

Registration

The information you enter in the registration page will be sent to TeleMate.Net Software so we can contact you regarding updates to our products and customer surveys. The only required field is your email address.



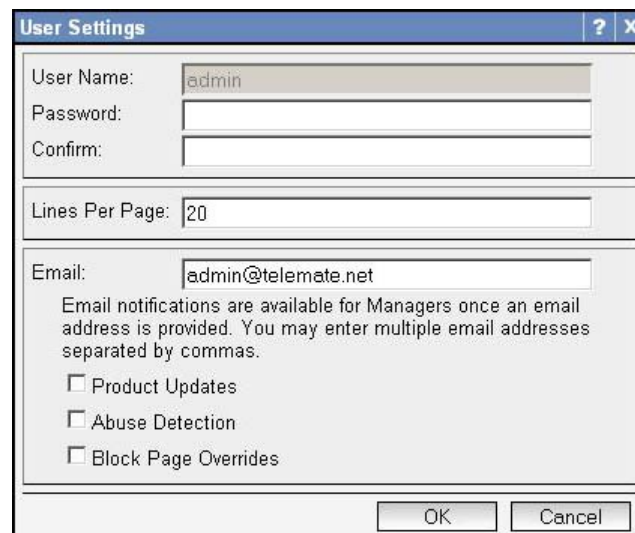
A screenshot of a 'Registration' dialog box. The title bar says 'Registration' with a question mark and a close button. The main text reads: 'The information you enter will be sent to TeleMate.Net Software so we can contact you regarding updates to our products and customer surveys. The only required field is your email address.' Below this is a list of fields: 'Email (Required):' with the value 'sales@telemate.net', 'First Name:' with 'Jon', 'Last Name:' with 'Doe', 'Phone Number:' with '(770) 589-7100', 'Company:' with 'TeleMate.Net Software', 'Company URL:' with 'www.telemate.net', 'Address 1:' with '5555 Triangle Parkway', 'Address 2:' with 'Suite 150', 'City:' with 'Atlanta', 'State / Province:' with 'GA', 'Zip Code:' with '30092', and 'Country:' with 'USA'. At the bottom are 'OK' and 'Cancel' buttons.

Registration	?	X
The information you enter will be sent to TeleMate.Net Software so we can contact you regarding updates to our products and customer surveys. The only required field is your email address.		
Email (Required):	sales@telemate.net	
First Name:	Jon	
Last Name:	Doe	
Phone Number:	(770) 589-7100	
Company:	TeleMate.Net Software	
Company URL:	www.telemate.net	
Address 1:	5555 Triangle Parkway	
Address 2:	Suite 150	
City:	Atlanta	
State / Province:	GA	
Zip Code:	30092	
Country:	USA	
OK		Cancel

If you are in a replicated environment, enter your information in the parent node. The parent node will replicate the information to all of their child nodes.

Your registration information will be sent to the NetSpective Online Service during an automatic or manual update.

User Settings



A screenshot of a 'User Settings' dialog box. The title bar says 'User Settings' with a question mark and a close button. The fields are: 'User Name:' with 'admin', 'Password:' (empty), 'Confirm:' (empty), 'Lines Per Page:' with '20', and 'Email:' with 'admin@telemate.net'. Below the email field is a note: 'Email notifications are available for Managers once an email address is provided. You may enter multiple email addresses separated by commas.' There are three checkboxes: 'Product Updates' (unchecked), 'Abuse Detection' (unchecked), and 'Block Page Overrides' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.

User Settings	?	X
User Name:	admin	
Password:		
Confirm:		
Lines Per Page:	20	
Email:	admin@telemate.net	
Email notifications are available for Managers once an email address is provided. You may enter multiple email addresses separated by commas.		
<input type="checkbox"/> Product Updates		
<input type="checkbox"/> Abuse Detection		
<input type="checkbox"/> Block Page Overrides		
OK		Cancel

Administrators or managers may wish to change their password or update their notification settings. They do this from the User Settings dialog. This dialog is accessed by clicking on their user name in the upper left part of the page. The options available to change are:

Properties

The general properties required to set up a NetSpective administrator or manager.

User Setting Properties	
User Name	A name to identify the user. This name is also their login name to the NetSpective Administration site. It can only be changed by an administrator from the Managers section.
Password	The login password for the NetSpective Administration site.
Confirm	Confirm the password given above.

Options

This refers to additional user specific options. These options will affect the usability of the NetSpective Administration website.

Lines Per Page

The 'lines per page' option shown on the listing page defaults to 20 rows. Additional lines are displayed on subsequent pages. The new lines per page value will be saved in a cookie and will affect all pages with paging. If you clear your browser cookies the lines per page value will revert to the default value of 20.

Notification Settings

In order to receive email notifications, an Email is required. Available notification types include product updates and abuse detection.

Notification Settings	
Email	An email address associated with the administrator or manager.
Product Updates	If checked the administrator or manager will receive notification about product updates.
Abuse Detection	If checked the administrator or manager will receive notification about abuse detection.
Block Page Overrides	If checked the administrator or manager will receive notification about block page overrides.

Management

In this section you will find all the tools for managing Users, Groups, Managers, and their filtering policies. Any managers classified as a 'Group Manager' will specifically have access to only this section.

Managers

In addition to the built-in admin manager, you may create other managers to delegate authority of your NetSpective. You may create manager accounts manually or you may use an LDAP source (such as Active Directory) to authenticate users and passwords. Managers may have different levels of authority, which are summarized by the table below.

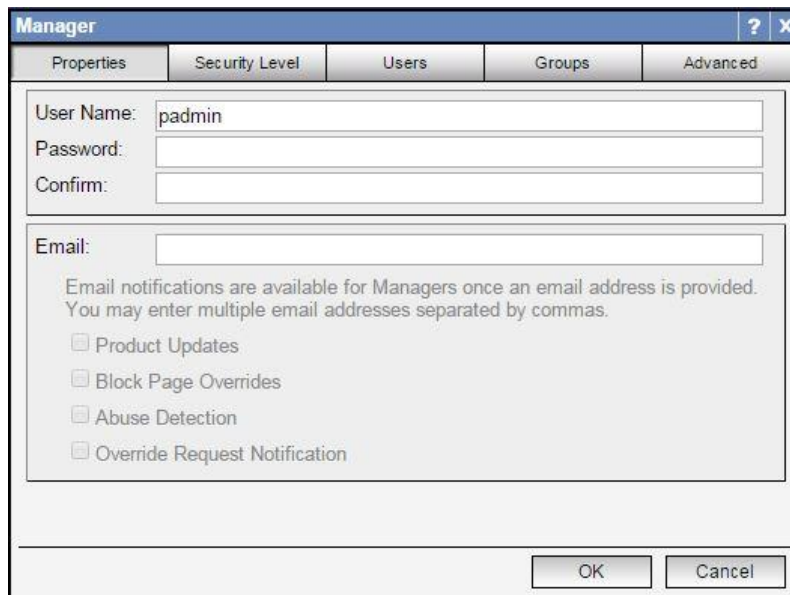
Managers		admin register help logout
  	Search: <input type="text"/>	 Group: <input type="text" value="System"/>
Local	LDAP Groups	LDAP Users
Manager		Security Level
<input checked="" type="checkbox"/> admin		Administrator
<input type="checkbox"/> brett		Group Manager
<input type="checkbox"/> District 1 Admin		Group Manager
<input type="checkbox"/> HQ Admin		Group Manager
<input type="checkbox"/> NOC Admin		Group Manager
<input type="checkbox"/> Sales Manager		Group Manager
<input type="button" value="Delete"/> <input type="button" value="Configure LDAP Sources"/>		

Security Level	Permissions
System Administrator	Create/edit/delete other managers (except admin). Create/edit/delete Groups and Users. Edit all of NetSpective's configuration options. Authorize a temporary override of the block page for any group.
Policy Administrator	Create/edit/delete other managers (except admin). Create/edit/delete Groups and Users. Authorize a temporary override of the block page for any group. Edit all of NetSpective's filtering options.
Group Manager	Edit the group policy for assigned groups and categories allowed by security options. Edit the group options for assigned groups. Edit site overrides for assigned groups, if allowed by security options. Move users between managed groups, but cannot add or remove users or groups. Authorize a temporary override of the block page for assigned groups.
Mobile Device Manager	Edit mobile pairings for assigned groups.
Block Page Override Manager	Authorize a temporary override of the block page for assigned groups.

Group Managers have additional configurable security options. The options include the ability to change the available permissions for managing Users and Groups. Group Managers also have security options to block access to the Overrides section, specific categories on the Group Policy page, and can be limited to managing only specific IP ranges. These options are only available for Group managers configured to authenticate manually (Local) or authenticate individual users using an LDAP source (LDAP Users).

Creating or Updating Managers

There are two basic ways you can create managers that are recognized by NetSpective. You may create a manager via the 'Local' tab and set a password manually, or you may create a manager via the 'LDAP Groups' or 'LDAP Users' tabs and have LDAP handle password authentication. To create a manager click the 'Add' button from the control bar near the top of the page. To update a manager, click on the manager's name.



The screenshot shows a dialog box titled "Manager" with a standard Windows-style title bar (minimize, maximize, close buttons). Below the title bar is a tabbed interface with five tabs: "Properties", "Security Level", "Users", "Groups", and "Advanced". The "Properties" tab is currently selected. Inside the "Properties" tab, there are three text input fields: "User Name:" (containing "padmin"), "Password:", and "Confirm:". Below these is an "Email:" label followed by a text input field. Under the email field, there is a block of text: "Email notifications are available for Managers once an email address is provided. You may enter multiple email addresses separated by commas." Below this text are four checkboxes, all of which are unchecked: "Product Updates", "Block Page Overrides", "Abuse Detection", and "Override Request Notification". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Figure 1: Local User

The screenshot shows the 'Manager' dialog box with the 'Security' tab selected. The 'LDAP Source' dropdown is set to 'QALab'. The 'LDAP Object' dropdown is set to 'Group: PRODMGMT\Administrators'. The 'OK' and 'Cancel' buttons are at the bottom right.

Manager	
Properties	Security
LDAP Source: QALab LDAP Object: Group: PRODMGMT\Administrators	
<div>OK Cancel</div>	

Figure 2: LDAP Group

The screenshot shows the 'Manager' dialog box with the 'Security' tab selected. The 'LDAP Source' dropdown is set to 'QALab'. The 'LDAP User' dropdown is set to 'PRODMGMT\Administrator'. The 'Email' field contains the text 'The email address will be supplied by LDAP'. Below this, there is a section for email notifications with three unchecked checkboxes: 'Product Updates', 'Abuse Detection', and 'Block Page Overrides'. The 'OK' and 'Cancel' buttons are at the bottom right.

Manager	
Properties	Security
LDAP Source: QALab LDAP User: PRODMGMT\Administrator	
Email: The email address will be supplied by LDAP Email notifications are available for Managers once an email address is provided. You may enter multiple email addresses separated by commas. <input type="checkbox"/> Product Updates <input type="checkbox"/> Abuse Detection <input type="checkbox"/> Block Page Overrides	
<div>OK Cancel</div>	

Figure 3: LDAP User

Manager Properties

The general properties required to set up a NetSpective manager.

User Name - A name to identify the manager. This name will also be their login name for the NetSpective Administration interface and/or the block page override form.

Password - The manager's password. (Not applicable for LDAP Users)

Confirm - Confirm the password given above.

Notification Settings

In order to receive email notifications, an email address is required. Available notification types include product updates and abuse detection. Note: The email address for LDAP managers is queried automatically from the LDAP server.

Notification Settings	
Email	An email address associated with the manager. You may enter multiple email addresses separated by commas (',').
Product Updates	If checked the manager will receive notification about product updates.
Abuse Detection	If checked the manager will receive notification about abuse detection.
Block Page Overrides	If checked the manager will receive notification about block page overrides.

Security Tab

You may choose which security level a manager or group of managers has. Click the 'Security Level' drop down to pick Administrator, Group Manager, or Block Page Override Manager. For Group and Block Page Override managers, select which groups they are assigned to by selecting the check boxes next to the group names in the group listing.



The security level of an individual LDAP manager will override the security level of any LDAP groups he or she is a member of, and all managed groups must be explicitly set. For example, even if the LDAP group "Sales" is set to the security level of Group Manager, you may set LDAP user "Michael", who is a member of the "Sales" LDAP group, to be a higher or lower security level, such as Administrator or Block Page Override Manager.

LDAP managers who have not been assigned a specific individual security level will have a security level set to the highest of any LDAP groups they are a member of. For example, user "Tim" who is a member of both the "Sales" and "NetSpective Admins" LDAP groups will be an Administrator if the "NetSpective Admins" LDAP group is set to be Administrator level. As a different example, if user "Sally" is a member of both the "Sales" LDAP group and the "Corporate" LDAP group, and both "Sales" and "Corporate" are set to Group Manager level, "Sally" will be a Group Manager of all groups assigned to either "Sales" or "Corporate" to manage.

Users Tab (Group Manager Only)

The Users tab provides the ability to grant or take away additional privileges for Group Managers. Managers can be granted access to create users, edit users, delete users, or import/export users.

You will also have the ability to manage access to specific IP address ranges, also referred to as IP Partitions.

The screenshot shows a window titled "Manager" with a tabbed interface. The "Users" tab is selected. The window contains two sections for granting access:

- Grant access to the following sections:**
 - ☐ Create User
 - ☒ Edit User
 - ☒ Delete User
 - ☐ Import/Export Users
- Grant access to Create/Edit options:**
 - ☒ Set Dynamic IP
 - ☒ Set Static IP/Range: All IPs and IP Ranges (with a dropdown arrow and a small icon)
 - ☒ Change Group Assignment

At the bottom right, there are "OK" and "Cancel" buttons.

IP Partitions

IP Partitions are used to limit access to specific IP Ranges. The partitions are assigned to Group Managers. The managers will only be able to add and/or modify Users within the configured IP Ranges. This is a licensable feature in our service provider level license. Please contact our support team if interested in using IP Partitions.

IP Partitions

Partitions

- ☐ District - XYZ
- ☒ Range A - Zone 1
- ☐ Range A - Zone 2
- ☐ Range B - Zone 1

IP Partitions are used to limit access to specific IP Ranges. The partitions are assigned to Group Managers. The managers will only be able to add and/or modify Users within the configured IP Ranges.

Name: Range A - Zone 1

IP Ranges

IP Range: - VLAN ID:

- ☒ 10.13.1.100 - 10.13.1.255

Save Cancel Close

Creating or Updating IP Partitions

To create a partition click the Add button at the top left of the dialog. To update a partition click the partition's link from the Partition list. Once the partition's data has been loaded in the right side of the dialog, update the necessary information:

Partition Name

The partition name is a required field and must be unique. The name is used to identify the IP ranges that are assigned to the partition.

IP Ranges

IP Ranges are unique to the partition. The range cannot include or overlap another range. A VLAN ID can also be assigned as part of an IP range. To add a range, input the start IP and end IP in the area at the top of the listing of IP Ranges. Once done, click the Add button. To edit an existing IP Range, select the range from the list. The range will be loaded into the area at the top of the listing. Once you have finished editing the IP Range make sure you click the Save button. Check or select the IP Ranges and click the Delete button in the area at the top of the listing to delete the ranges.

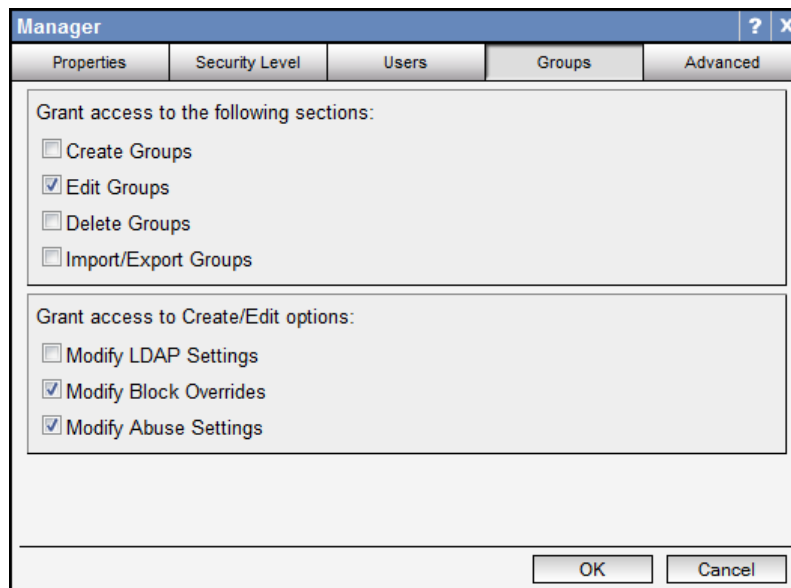
Deleting IP Partitions

To delete an IP Partition, select the check box next to each partition's name. Once the partitions are selected, click the Delete button to delete the partitions.

Groups Tab (Group Manager Only)

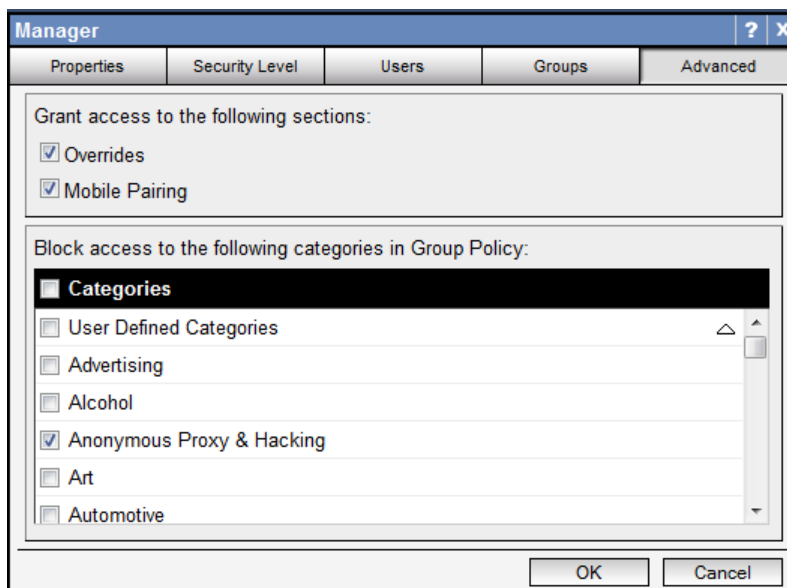
The Groups tab provides the ability to grant or take away additional privileges for Group Managers. Managers can be granted access to create groups, edit groups, delete groups, or import/export groups.

You will also find an additional section for additional create and edit options. Here managers can be granted access to modify LDAP settings, modify block overrides, and modify abuse settings.



Advanced Tab (Group Manager Only)

You may choose to disable access of certain options for managers. Managers can be blocked from accessing the Overrides section, preventing them from adding or modifying overrides. They can also be blocked from accessing the Mobile Pairing section. In Group Policy, managers can be blocked from seeing and accessing specific categories. This prevents them from being able to change a categories block or abuse settings.



Deleting Managers

To delete managers, select the check box next to each manager's name. To delete all managers displayed on the current page, select the check box in the upper left-hand portion of the table. Once the managers are selected, click the Delete button to delete the managers. If all managers on a page are selected, the option to select the managers on every page will become available.

Assigning Groups to Managers

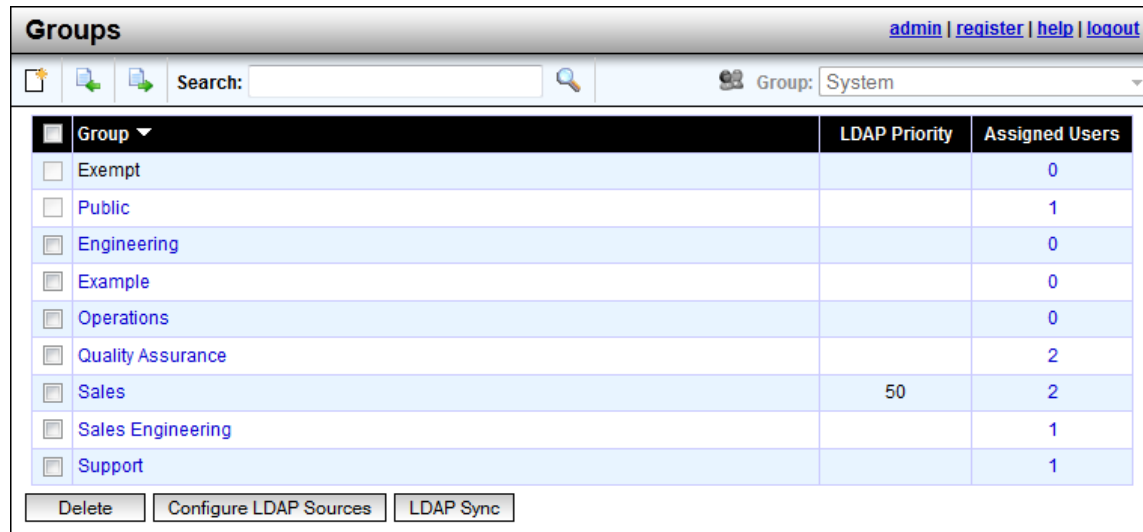
You may assign a manager to multiple groups by using the security tab, as described above in the "Security" section, or you may assign multiple managers to a group from the Groups page.

Viewing All Assigned Managers

You may view all managers and their security levels, including those only included by an LDAP group, by going to the All Assigned Managers report, under the 'Statistics' screen.

Groups

The Groups page provides a listing of all user defined and built-in groups which hold users. The built-in groups are the Public and Exempt groups. By creating and using additional groups, you have flexibility in creating filtering policies and more detailed information in reports.



Group ▼	LDAP Priority	Assigned Users
<input type="checkbox"/> Exempt		0
<input type="checkbox"/> Public		1
<input type="checkbox"/> Engineering		0
<input type="checkbox"/> Example		0
<input type="checkbox"/> Operations		0
<input type="checkbox"/> Quality Assurance		2
<input type="checkbox"/> Sales	50	2
<input type="checkbox"/> Sales Engineering		1
<input type="checkbox"/> Support		1

Delete Configure LDAP Sources LDAP Sync

Users are assigned to a group either manually or by LDAP and each group has its own filtering policy. Each group's filtering policy can be customized to ignore, monitor, or block specific content categories at specific times of day. All unknown or unassigned users are assumed to be members of the Public Group and use its filtering policy. Therefore, it is recommended that the Public Group should have the most restrictive filtering policy. The Exempt Group's policy, which cannot be changed, always ignores all traffic.

Creating or Updating Groups

To create a group, click the Add button from the control bar near the top of the page. To update a group click the group's link. Once the dialog has opened, update the necessary information:

Properties Tab

This tab contains the general properties of a NetSpective group. A unique group name is the only required field.

The screenshot shows a dialog box titled "Group" with a standard Windows-style title bar (minimize, maximize, close buttons). Below the title bar are four tabs: "Properties" (selected), "Block Override", "Abuse Settings", and "Managers".

The "Properties" tab contains the following fields and sections:

- Group:** A text input field containing the value "Sales".
- LDAP Source:** A dropdown menu showing "TMDC".
- LDAP Object:** A dropdown menu showing "OrgUnit: Sales.Telemate.Net Software.tele".
- LDAP Priority:** A text input field containing the value "50".
- Alternate Days Policy:** A section with the text "A policy for alternate days is a group policy that will be used on the designated days of the week instead of the default group policy." Below this is a checkbox labeled "Enable Policy for Alternate Days". If checked, there are seven checkboxes for the days of the week: Sunday (checked), Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday (checked).
- YouTube Access:** A section with the text "Limit YouTube access to only educational videos on YouTube EDU using a YouTube For Schools code. **Warning:** Flash must be allowed in the group policy." Below this is a dropdown menu showing "None".
- Safe Search:** A section with the text "When enforcing Safe Search" and a checkbox labeled "Enable YouTube Safety Mode and Block YouTube Login".
- Activity Log Redaction:** A section with the text "Permanently redact certain activity log attributes." and three checkboxes: "Source IP Address", "Username", and "Group Name".

At the bottom of the dialog box are two buttons: "OK" and "Cancel".

LDAP

A NetSpective group can be configured to mirror the user list of a specific Group or Organizational Unit in a LDAP Directory. NetSpective will automatically synchronize itself periodically with the LDAP server to make sure its list of users is kept up to date.

Select a LDAP Source from the "Source" drop down. If you have not created a LDAP source, see LDAP Sources for details on creating one. After selecting a source, select a Group or OU from the "Object" drop down.

LDAP Priority

When NetSpective synchronizes with your LDAP Server it evaluates all NetSpective Groups by priority level then alphabetical order. A user that exists in more than one LDAP Group or OU will be assigned to the first NetSpective Group evaluated with one of the user's LDAP Groups or OUs. LDAP priority level will order groups with the lowest number first.

Alternate Days Policy

A Group may have an additional policy, referred to as an Alternate Day Policy, which applies only to certain days of the week. A Group's default policy will continue to apply to all other days of the week.

YouTube | Schools

NetSpective can limit YouTube access to only educational videos on [YouTube EDU](#) by assigning a YouTube For Schools code to a NetSpective group. Members of the group will only be able to view videos YouTube has flagged as educational or videos found in the assigned account's playlist. If you take advantage of this feature, ensure that the Flash protocol is not blocked in the Group Policy section for the group you are using this feature with.

YouTube enforcing Safe Search

Clicking the checkbox will enforce Safe Search for YouTube. This feature will also block SSL YouTube logins.

Redact Log Attributes

Traffic associated with a group may be logged, but certain attributes may be redacted including the source IP address, username and group name. This will only redact attributes on log data created after the settings are saved. The redacted data cannot be recovered.

Block Override Tab

The block page override feature enables blocked web sites to be temporarily allowed for a certain period of time by entering a password or by providing credentials of an authorized manager. The override can affect the entire NetSpective group or just the user from which the override originated.

Group

Properties

Block Override

Abuse Settings

Managers

Mode:

Individual Override

Duration:

30 minutes

Authentication:

☒ Manager Credentials

☐ Password:

☒ Enable Notification

Send email notifications after a manager has issued block page overrides for the day.

☒ Enable Request Category Change

Allow users to request a category change from the NetSpective block page.

OK

Cancel

Block Overrides	
Mode	Either disabled, Group Override, or Individual Override.
Duration	The number of minutes to override the block.
Authentication	Enter a password that will be used to authorize override requests 'Manager Credentials' requires a manager's login and password for authentication. See the 'Managers' section for details on creating managers who can use this feature.
Notification	After a specified number of block page overrides have been completed an email notification will be sent to administrators and managers when the option is enabled. In order to receive the email, the administrator and managers must enable notification of Block Page Overrides in User Settings or Manager Properties.
Request Category Change	Enables users within the group to request a category change right from the block page.

Abuse Settings

Different groupings of Abuse Settings, called Levels, can be configured and assigned to Categories. The assignment is done on the Group Policy page. Each Level has its own options for Notifications and Abuse Detection.

The screenshot shows a 'Group' dialog box with four tabs: 'Properties', 'Block Override', 'Abuse Settings' (selected), and 'Managers'. The 'Settings' dropdown is set to 'Level 1'. The 'Abuse Settings' tab contains three sections, each with a checked checkbox and configurable values:

- Policy Reminder:** Display every 1320 minutes for all levels.
- Email Notification:** If there are 50 hits to "Level 1" Categories in 10 minutes, resend every 30 minutes for repeated hits.
- Abuse Detection:** If there are 100 hits to "Level 1" Categories in 15 minutes, lock down all Level 1 Categories for 180 minutes.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

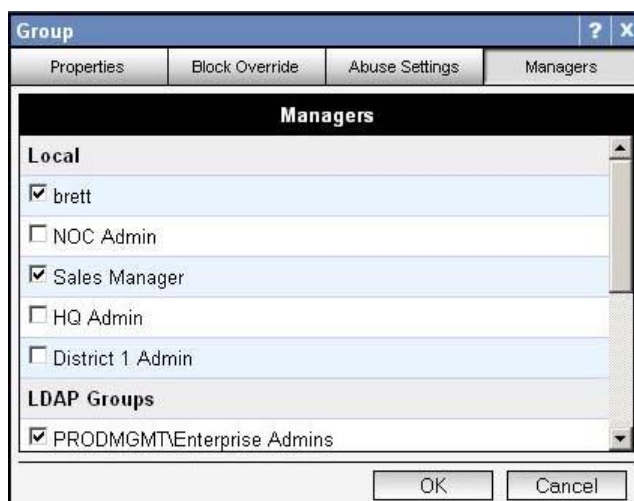
If Policy Reminder is enabled, users will be prompted with a page containing information on your company's Internet usage policy with the choice to accept or decline that policy. The page will only be displayed for categories marked as abusive and will prompt the policy after a specified number of hours. The page displayed can be configured in Filter Settings. For more information check the Policy Reminder documentation.

If Notification is enabled, the administrators and managers assigned to the group will receive an email notice once the notification limits have been met. If the administrator or manager does not wish to receive an email, they can turn off Abuse Settings emails in their User Settings.

If Abuse Detection is enabled, the users assigned to the group will be monitored for activity to categories marked as abusive. Once a user's abuse limit has been reached, either all other Categories marked with this abuse level, all of the user's Internet Activity, or just the user's Web Activity will be shut down (locked) for a certain period of time. To unlock a user that is currently locked, go to the Currently Locked Users page under the Statistics section.

Managers

This tab shows the Group and Block Page Override managers who are assigned to the selected group. You may change manager assignments by checking or unchecking the check box next to each manager or manager group name. If a group of managers is checked, its members are also shown with gray check marks next to their names indicating that they are all assigned to the group.



Assigning Users to Groups

Users are assigned to groups in the Users section. See the help on Users for more information on assigning users to groups.

Deleting Groups


To delete groups select the check box next to each group's name. To delete all groups displayed on the current page, select the check box in the upper left-hand portion of the table. Once the groups are selected, click the Delete button to delete the groups. If all groups on a page are selected, the option to select the groups on every page will become available.

Importing Groups

Groups can be imported from a simple text file. The first row can be an optional header row. The following is an example of the file format:

```
"Groups"  
"Group #1"  
"Group #2"  
"Group #3"
```

To import, select the 'Import' button from the control bar. Once the dialog is open, click the 'Browse...' button and select the file you wish to import. Click 'OK' and the import will begin.









In addition, categories you choose to block or monitor can also be marked as abusive (). If a user is blocked a certain number of times, that user will have his or her internet access locked down (disabled) for a specified duration of time. Alternatively, if the category is set to monitor, the user will be presented with your company's Internet usage policy and must accept or decline the terms of the policy. The user will be prompted again after a specified time out. You may configure the abuse options on the Group Properties page after you have flagged certain categories as abusive.

Note: Chat Protocols, Streaming Media Protocols, Remote Login Protocols, and Voice Over IP Protocols may not be marked as abusive.


Alternate Days

A Group may have an additional policy, referred to as an Alternate Day Policy that applies only to certain days of the week. A Group's default policy will continue to apply to all other days of the week. You can enable an Alternate Day Policy in the Group Properties page.

Policy Action Colors	
Red	Block and log traffic
Yellow	Monitor (Log) traffic
Green	Ignore traffic, don't log
Orange	(Only for subcategory group headers) Indicates that the subcategories in a grouping have different policies. Expand the subcategory group to view the policy for each subcategory.

Special Icons	
	This flag indicates the category is Abusive. The number in the icon signifies which Abuse Detection Level will be used for the abuse. If Policy Reminder is enabled for the level and the category is set Log/Monitor, the first attempted accesses to this category will trigger the Policy Reminder page and the Policy Reminder must be accepted by the user. If Abuse Detection is enabled, attempted access to this category will trigger the Abuse Detection feature. When Notification is enabled, emails will be sent to the managers and administrators of the group when the feature is triggered.
	Click on this icon to change a category's policy rule (Block, Monitor, or Ignore) for all 24 hours.
	This icon indicates that Block Page Overrides are not allowed for the category.
	This icon indicates the category is set to allow unauthenticated traffic, bypassing the normal rules on the Authentication tab. This option is only available in the Public group. This is useful for software update programs and other devices which cannot authenticate as a user.
	(Proxy Only) Each category can be set to one of three priority classes for shaping traffic – High (), Medium () and Low (). By default, all categories are Medium priority.

Modifying Policy

To modify a group policy, first select the correct group from the selector at the upper right of the page. Click on a box in the grid to change the action for a specific hour. Click on the  icon to change the action for all hours. By default, each click will cycle the action through Ignore, Monitor, and Block. You can change this click action by using the selector below the policy grid. When finished modifying the policy, click the 'Save' icon in the control bar at the top of the page.

Save To

Save To lets you save all or part of the currently selected policy to another group's policy. Click the 'Save To...' icon in the control bar at the top left of the page. Once the dialog is open, select the categories you wish to copy and the destination group(s) to receive the copy.

Copy Public

If you are modifying a group other than the Public group, you may click the 'Copy Public' icon to copy the Public Group's policy into the current group. The changes are not finalized until you click the 'Save' icon.

Safe Search

NetSpective's Safe Search feature transparently converts all Google, Yahoo, Bing, MSN, Hotbot, Lycos, Ask, and Dogpile searches into "Safe Mode" searches. To enable Safe Search, block the "Web Search" category and allow the "Web Search Filtered" category. The current state of Safe Search is also displayed at the bottom of the page. Also by clicking on the Safe Search icon the "Web Search" and "Web Search Filtered" categories will be set to the proper state.

Note: Additionally, you can prohibit certain search terms in the Overrides page.

HTTPS / SSL Blocking

In Passive mode, NetSpective monitors the network for particular signatures much like an intrusion detection product. Since HTTPS tunnels HTTP sessions over SSL, NetSpective detects the SSL connection and takes actions based on the categorization of the HTTPS/SSL server. In Proxy mode, NetSpective treats direct (non-HTTP) connections as potential SSL traffic.

If the IP address of an HTTPS/SSL server is categorized and the policy is set to block, then all HTTPS and other SSL connections to it are blocked. Therefore, an objectionable site cannot be accessed via HTTPS (port 443 or otherwise), SSH, or any other protocol based on SSL.

NetSpective also utilizes the adaptive filtering process for public SSL sites. When the appliance detects uncategorized SSL accesses on port 443, the site is temporarily categorized as "HTTPS Unrated" and then uploaded to the Adaptive Filtering Lab for categorization.

The NetSpective Adaptive Filtering Lab will categorize the site based on the following criteria:

If the site's SSL certificate is invalid, self-signed, or signed by an untrusted certificate authority, then the site will be categorized as "HTTPS Untrusted".

If the site's SSL certificate is valid, signed by a trusted certificate authority, and the site cannot be categorized, then the site will be categorized as "HTTPS Trusted".

If the site's SSL certificate is valid, signed by a trusted certificate authority, and the site can be categorized, then the site will be categorized as a specific category (for example, "Mature Content"). Thus, blocking "Mature Content" would block HTTP and HTTPS traffic to the site.

Users

The Users page provides a listing of users by group membership. You can manually add users, assign users into groups, delete users, and search for users. Users have all of their IP addresses grouped together, both IPv4 and IPv6. Each user with multiple addresses has a drop down toggle, so you can view each address.

Users				TELEMATE\william.babji register help logout	
Search: <input type="text"/>		Group: [All Assigned Users]			
User		Addresses		Group	
TELEMATE\domain.backup	LDAP	10.2.40.144 - 10.2.40.159, 2001:470:e390:28::4:0 - 2001:470:e390:28::4:fff		Domain Admins	
TELEMATE\eric.turner	LDAP	10.2.40.144 - 10.2.40.159, 2001:470:e390:28::4:0 - 2001:470:e390:28::4:fff		Development	
		VLAN	IP Address or Range		
			10.2.40.144-10.2.40.159		
			2001:470:e390:28::4:0-2001:470:e390:28::4:fff		

Currently Logged On Users

NetSpective's Logon Agent, Remote Agent, Mobile Portal, Terminal Server Client and Authentication Portal automatically report user information to NetSpective when users log on. These users can be viewed and assigned to a group other than Public by selecting the special [Current Logged On] group in the Users screen. From the Current Logged On list, users that have an IP can be manually logged out. User's that have logged in via NetSpective's Logon Agent or Authentication Portal will have an IP.

Creating or Updating Users

To create a user click the 'Add' button from the control bar near the top of the page. To update a user click the user's link. When creating a static IP user or an IP range user, the IP address field will accept either an IPv4 or an IPv6 address. Addresses associated with the user you are creating are now listed in the pane below.

The screenshot shows a 'User' dialog box. At the top, there's a title bar with a question mark and a close button. Below the title bar, there are two input fields: 'Group' with a dropdown menu showing 'Development' and 'User' with a text box containing 'TELEMATE\eric.turner'. Below these fields is a checkbox labeled 'Use as a location (An IP Address or Range is required)'. Underneath the checkbox is a section titled 'IP Addresses and Ranges' which contains a table with three columns: 'IP Address', 'VLAN', and 'IP Address'. There is an 'Add' button to the right of the table. Below the table is a section titled 'Dynamic IP Associations (Requires NetSpective Logon Agent)' which contains a list of two entries: 'VLAN 10.2.40.144 - 10.2.40.159' and 'VLAN 2001:470:e390:28::4:0 - 2001:470:e390:28::4:fff'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Once the dialog has opened, complete the necessary information.

Requirements	
Group	A group to assign the user to.
User	A name to identify the user.
IP Address	A user can be assigned an IP Address or IP Address range, if that user is running the NetSpective Logon Agent they can by assigned a dynamic IP.

The Users section is the only area of NetSpective that requires ranges of IP addresses to be typed out with the starting IP and the ending IP.

Use as Location

If "Use as location" is checked, the user will be treated as a location. A location must have a single IP or a range of IPs. Locations have a higher precedence than a regular user when evaluating which group policy to enforce. For example, a NetSpective user, john.smith, is configured using dynamic IP and a location, Media Center, is configured with a range of IPs. When John Smith logs into a computer that is in the Media Center IP range, he will use the group policy for the group that contains the Media Center location. If John Smith logs into a computer outside that IP range he will use the group policy for group containing the NetSpective user john.smith.

Use with VLAN ID

If "Use with VLAN ID" is checked, the user will be also be associated with the specified VLAN ID.

User Specific Overrides

User Specific Overrides allow overrides to be created for individual users. Creating a user override simplifies cases when an override is needed for a single user and not the entire group. These overrides can also be configured to expire, making them easier to manage. In the user list, there are icons designating whether a user has any active User Specific Overrides configured. Overrides that have expired are not considered active.

User Specific Overrides - TELEMATEEric.turner

User Specific Overrides affect only the user and not the entire group. The priority determines when the override will be evaluated, either before the System's or the Group's overrides. Only Administrators can create and edit System overrides. These overrides can also be configured to start and end on certain days.

Override:

Start Date:

2011-08-16

Comment:

End Date:

Never

Category:

Admin Block

Referrer Depth:

None

Priority:

System

Save



Clear

Overrides

<input type="checkbox"/>	ggpht.com	Admin Allow	2010-12-16	Never	
<input type="checkbox"/>	googleusercontent.com	Admin Allow	2010-12-20	Never	
<input type="checkbox"/>	paperbackswap.com	Admin Allow	2010-10-21	Never	

Delete

Close

User Specific Override Icons	
	The user has no active overrides assigned to him. An expired override is not considered active.
	The user has active overrides.

To manage User Specific Overrides click on the icon in the user list. Once the dialog has opened, overrides can be added by entering the information in the proper fields and clicking 'Save'. To edit an existing override click on the override in the list and it will be loaded in the management area. To delete user overrides, select the checkbox next to each override. To delete all overrides, select the checkbox in the upper left-hand portion of the table. Once the overrides are selected, click the 'Delete' button to delete the overrides.

User Specific Override Fields	
Override	An override can be a domain, IP or URL.
Expiration	The Expiration is the day that the override will expire. If left blank, the override will never expire. Expiration dates will show up red in the override list if they have passed the expiration date.
Category	The category can be any NetSpective category. The Category respects the settings in the Group Policy the user is assigned to.
Priority	The Priority determines when and how the override is evaluated. If a user override is set to System priority it will take precedence over a normal System override. A Group priority will take precedence over a normal Group override. The Group priority will be ignored if a normal System override exists for the same override value.

Assigning Users to Groups

To assign users select the checkbox next to each user's name. To assign all users displayed on the current page (to the same group), select the checkbox in the upper left-hand portion of the table. Once the users are selected, click the 'Assign' button. When the dialog opens, select the group where you want the users to be assigned. Click 'OK' when you are finished.

Deleting Users

To delete users select the checkbox next to each user's name. To delete all users displayed on the current page, select the checkbox in the upper left-hand portion of the table. Once the users are selected, click the 'Delete' button to delete the users. If all users on a page are selected, the option to select the users on every page will become available.

Importing Users

Users can be imported from a simple text file. The first row can be an optional header row. The following is an example of the file format:

```
"User", "Address"
"192.168.5.240", "192.168.5.240"
"bill.jackson", "1.1.134.157"
"mary.baker", "1.1.134.158"
"jill.jones", "1.1.134.159"
"john.smith", ""
```

To import, select the 'Import' button from the control bar. Once the dialog is open, choose the group that all the imported users will be assigned to. Next click the 'Browse...' button and select the file you wish to import. Click 'OK' and the import will begin.

Exporting Users

To export, select the 'Export' button from the control bar. When your browser's download dialog appears, select where you would like to save the export file.

The users exported will reflect what is currently being displayed. Only users in the group shown will be exported. The search field will also affect the results of the export.

Mobile Pairing

Mobile Pairings are associations between users and mobile devices, such as smartphones and tablets. They are ideal for devices that do not typically lend themselves to easy identification and association with a user. When a mobile device is paired, a token is stored on the device that allows NetSpective to identify the device and associate it with a user. Pairings will allow you to filter HTTP traffic for devices with policies specific to a user. Another advantage of mobile pairings is the ability to limit the time a user has access to the Internet. See the Authentication section on how to configure your NetSpective to allow mobile device pairing.

Managing Mobile Pairings

To manage Mobile Pairings click on the mobile device in the list. Once the dialog has opened, update the necessary information:

Managing Mobile Pairings	
Name	The name is a description assigned to the mobile device. On creation the name defaults to a name containing information about the mobile device if it can be determined.
Comment	The comment is only used to store additional information. During the request to pair the end-user has the option to include a comment that will be shown here.
Timeout	Timeout either displays when the user's pairing expires or if reset, shows an option to set the amount of time until it expires.
User	The user the mobile device is assigned to. Clicking Unpair will remove the user association with the device.

Pairing

Select a user from the list and click Pair to associate the user with the mobile device. Use the Group drop down or the Start With field to narrow down the list of available users.

Note: A change to the paired user will not be saved until you click the OK button and save all the changes.

History

The history shows the most recent changes to the mobile device's properties. It lists when the change occurred, who made the changes, the user assigned and what action was taken. Actions can include Changed Properties, Reset Timeout, Changed Pairing, Removed Pairing, Forced Expire, Requested Pairing, and Pairing Canceled.

Unpair Mobile Devices

Unpairing a mobile device removes the user association. To unpair mobile devices select the check box next to each device's name. To unpair all devices displayed on the current page, select the check box in the upper left-hand portion of the table. Once the devices are selected, click the Unpair button to unpair the mobile devices.

Expire Mobile Pairings

Expiring a mobile pairing forces the pairing to the expired state. To expire mobile pairings select the check box next to each device's name. To expire all pairings displayed on the current page, select the check box in the upper left-hand portion of the table. Once the devices are selected, click the Expire button to expire the mobile device pairings.

Delete Mobile Devices

To delete mobile devices and their pairings select the check box next to each device's name. To delete all devices displayed on the current page, select the check box in the upper left-hand portion of the table. Once the devices are selected, click the Delete button to delete the mobile devices. If a mobile device is deleted the user will need to request to be paired again.

Overrides

Overrides may be created to allow, block, or categorize specific web sites, news groups, IP addresses, web search terms, or file types. The different types of overrides are grouped together on different pages.

Overrides

Search: All

Group: System

Domains

IP Addresses

URLs

Search Terms

File Extensions

Requests

<div></div> Domain	Start Date	End Date	Category	Override
<div></div> cnn.com	2013-01-03	Never	News	News
<div></div> drudgereport.com	2013-01-03	Never	News	Admin Block
<div></div> fark.com	2013-01-03	Never	News	Web Log
<div></div> images.google.com	2013-01-03	Never	Web Search	Admin Block
<div></div> ipcop.com	2013-01-03	Never	Technology	Technology
<div></div> klout.com	2013-01-03	Never	Society	Reference
<div></div> netflix.com	2013-01-03	Never	Streaming Media	Entertainment

Delete

Clean Up

The Exempt group is never blocked and is exempt from all overrides. All other groups, including the Public group, have their own override lists. Additionally, system-wide overrides may be created. System level overrides are processed first and affect all groups except the Exempt group.

IP Address Override

The Overrides section supports overriding both IPv4 and IPv6 addresses. This section will accept slash notation for designating IP ranges.

Overrides

[TELEMATE\william.babji](#) | [register](#) | [help](#) | [logout](#)

Search: All

Group: Sales Engineering

Domains

IP Addresses

URLs

Search Terms

File Extensions

News Groups

Requests

<input type="checkbox"/>	IP Address	Start Date	End Date	Category	Override
<input type="checkbox"/>	10.0.0.0/8	2014-07-10	Never	Internal	Admin Block
<input type="checkbox"/>	2001:470:e398:28::/64	2014-07-10	Never		Admin Allow

Delete

Clean Up

Web Search Term Override

The web search term override feature is used to assign terms or combinations of terms used at search engines to a specific category. This feature in itself is a method of preventing a user from finding objectionable content. In addition, when a term is assigned to an abusive category that is blocked, it also triggers the abuse detection feature. Thus, a user searching for abusive content can also be given an abuse lockout.

Overrides admin register help logout						
		Search: All <input type="text"/>	Group: System			
Domains	IP Addresses	URLs	Search Terms	File Extensions	Requests	
<input type="checkbox"/>	Search Term ▼	Start Date	End Date	Category	Override	
<input type="checkbox"/>	mp3	2013-01-03	Never		Admin Block	
<input type="checkbox"/>	proxy	2013-01-03	Never		Anonymous Proxy & Hacking	
<input type="checkbox"/>	smut	2013-01-03	Never		Pornography	
<input type="checkbox"/>	xxx	2013-01-03	Never		Pornography	
Delete		Clean Up				

The search term override feature requires whole word matching; you will need to enter search terms exactly as they appear in the search. Plurals and common misspellings will not automatically be matched. If you override "porn" and "pornography", and someone searches for "porno" or "pron", it will be missed. If you enter multiple terms together, like "anonymous proxy", each of the terms specified must be in the search for it to be matched. Extra terms in the search will not cause a problem, so someone searching for "World of Warcraft cheats" would be picked up by the "warcraft" search term. Search terms are supported for Google, Yahoo, and Microsoft search engines.

NetSpective adds two internal reports used to tune your term assignments. The "Popular Searches" report shows you the most popular web searches made by users since midnight. The "Recent Searches" report shows the last 100 searches, which is useful to review traffic during the day. In both of these reports, the terms are matched to their corresponding category if an override exists. You can use to determine the effectiveness of your search term overrides and to find new terms.

Searching Overrides

There is an additional search option when searching overrides. You have the ability to filter the list by whether the overrides are from an import or a manual override.

Override Processing Order






The data below shows the processing rule order. If an override exists in both the System group and a regular group, the override in the regular group will be colored Gray indicating that it will never be processed.

1. Exempt Group (Never blocked)
2. System Overrides (URL, IP Address, File Extension)
3. Group Overrides (URL, IP Address, File Extension)
4. System and Group Search Term Overrides

Override Rule Examples

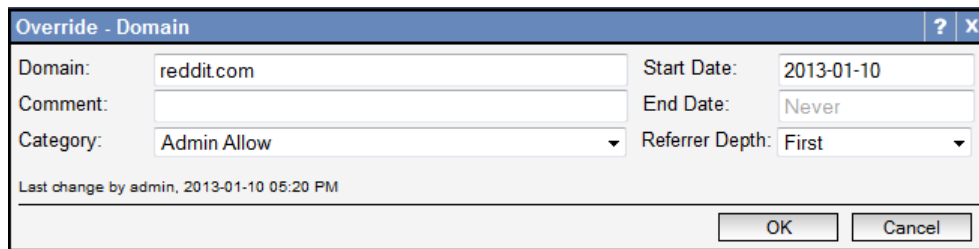
Example	Type	Description
mysite.com	Domain	Matches activity to mysite.com and its subdomains (www.mysite.com, images.mysite.com, etc.)
jenny.mysite.com	Domain	Matches activity to jenny.mysite.com and its subdomains. Since this rule is more specific than the previous rule (mysite.com), it will have higher precedence.
mysite.com/news/	URL	Matches activity to the /news/ directory and its subdirectories (/news/images/, etc.) on mysite.com
mysite.com/watch?v=qg1ckCkm8YI	URL	Matches activity to the specific page including the query string on the mysite.com
proxy	Search Term	Matches a web search containing "proxy" as a keyword
legal proxy	Search Term	Matches a web search containing both "legal" and "proxy" as keywords
.swf	File Extension	Matches Shockwave Flash™ files
.mpeg	File Extension	Matches MPEG Audio/Visual files
edu	Domain	Matches all domains ending in the top level domain "edu" (www.berkeley.edu, etc.).
alt.binaries.sounds	News Group	Matches the alt.binaries.sounds news group and all news groups below it (alt.binaries.sounds.mp3, etc.).
168.100.5.201	IP Address	Matches the IP address 168.100.5.201
168.100.5.0/24	IP Address	Matches the IP addresses 168.100.5.0 - 168.100.5.255. Since this rule is less specific than the previous rule (192.168.5.201), it will have lower precedence.

Special Override Icons

Icon	Description
	The Override is marked as a referrer, first or second depth.
	A System Override already exists for this override. The System Override will have an higher priority.
	NetSpective's category is the same as the override category currently selected.
	NetSpective's category is the same as the override category currently selected. However, NetSpective's category is not exclusive. There are subdomains or sites that may have a different NetSpective category.
	NetSpective's category has changed since this override was first created.

Creating or Updating Overrides

When adding an override, make sure you are on the correct page for that override type. Also, make sure you are in the correct group that you wish the override to be placed. Select the System group to create system-wide overrides. For adding an override, select the "Add" button in the upper left corner in the control bar. For an update click the link for the override you wish to edit.



Override - Domain	
Domain: reddit.com	Start Date: 2013-01-10
Comment:	End Date: Never
Category: Admin Allow	Referrer Depth: First
Last change by admin, 2013-01-10 05:20 PM	
OK Cancel	

Once the dialog has opened, enter the override in the proper field. Comments are optional and are there only for your own reference. If the override is marked as a referrer, then content that was referred from the page will also have the override category. A first depth referrer setting will allow content referenced by the override, dependent upon the complexity of the page or site. A second depth referrer will allow a page referenced by the override to fully render, dependent upon the complexity of the second page. The start date will default to today, but can be set for any time in the future. The end date can be left to 'Never' expire or an expiration date can be specified. Last, select the category you wish to assign from the Category drop down box. Select 'Admin Allow' or 'Admin Block' to always allow or block the activity, or select a user defined or standard category. Click the 'OK' button when finished.

The override is now active and will be displayed in the list. Also shown is the date the override was added; the assigned category, and the default NetSpective categorization (if applicable). The override list may be sorted by clicking on the header of the column by which you wish to sort.

Note: Currently, to override an FTP site it must be entered as an IP address in the IP overrides.

Deleting Overrides

To delete overrides select the checkbox next to each override's name. To delete all overrides displayed on the current page, select the checkbox in the upper left-hand portion of the table. Once the overrides are selected, click the Delete button to delete the overrides. If all overrides on a page are selected, the option to select the overrides on every page will become available.

Importing Overrides

Overrides can be imported from a simple text file. The first row can be an optional header row. The following is an example of the file format:

```
"Domain"  
"cnn.com"  
"edu"  
"finance.yahoo.com"  
"mysite.com/news"
```

Putting addresses in quotations is optional.

To import, select the 'Import' button from the control bar. Once the dialog is open, choose the group and category that all the imported overrides will be assigned to. Next click the 'Browse...' button and select the file you wish to import. Click 'OK' and the import will begin.





Exporting Overrides

To export, select the 'Export' button from the control bar. When your browser's download dialog appears, select where you would like to save the export file.

The overrides exported will reflect what is currently being displayed. Only overrides in the group and type being shown will be exported. The search field will also affect the results of the export.

Requests

Requests are submitted via the block page. Groups that have request category change enabled will be able to suggest a new category for a blocked site. See the Groups section for information on enabling this feature per group. The request listing will include the site, user (if available), group, time of request, the suggested category and the current category of the site. Adding a request to the override list will remove it from the request list. A request cannot be added if an override already exists for the selected group.

Overrides admin register help logout						
			Search: <input type="text" value="All"/>		Group: <input type="text" value="Sales Engineering"/>	
Domains	IP Addresses	URLs	Search Terms	File Extensions	News Groups	Requests
<input type="checkbox"/>	Override	User	Group	Date ▼	Category	Request
<input type="checkbox"/>	reddit.com	Mr. Bill	Sales Engineering	2013-01-04	Pornography	Society
<input type="button" value="Delete"/>						

System Control

In this section you will find several areas for authenticating users, modifying those authentication settings, as well as various settings for the appliance itself. Customization for NetSpective's redirect pages are also found in this section.

Device Settings

This section includes areas for configuring logging settings, managing the devices network settings, setting up your LDAP sources, and adding a signed certificate.

NetSpective can generate log files which may be processed by NetAuditor to create reports. Log files are transferred via FTP to a server of your choice. You may configure automatic log transfers that occur daily, hourly or every few minutes.

Configure Logging Settings

NetSpective can generate activity logs when logging is enabled. With logging enabled more detailed information can be retrieved about activity on your network.

Log Settings	
Disable Logging	This option disables the generation of activity logs.
Syslog Settings	This option enables logging with syslog as the method of log transfer.
FTP Settings	This option enables logging with ftp as the method of log transfer.

Configure NetAuditor

The NetAuditor settings allow you to configure a hyperlink to the NetAuditor's web portal. If the port number is also required, include it after the IP or hostname separated by a colon (ex. 192.168.5.100:8080). The link will be displayed in the side navigation in the Device Information section. You also have the option to automatically transfer the NetSpective log files when NetAuditor is launched by the hyperlink. If you do not currently have NetAuditor it can be downloaded from the Utilities page.

Configure Syslog Settings

When Syslog is selected, logging is enabled and will be transferred to the designated syslog server. The transfer of logs will happen at least every minute. Log messages will retain the internal and actual timestamp of the particular activity, unless removal is selected. Transfer over reliable TCP or unreliable UDP may be selected.

Syslog Settings	
Server	IP address or host name of the Syslog server.
Port	The port of the syslog server, default is 514.
Transfer Mode	The method of transfer. Available selections are TCP and UDP. TCP is the preferred setting.
Add Timestamp	If checked, the internal timestamp will be added from the activity logs.
Facility	The facility that activity log messages should be given. Selections are limited to the eight Log Local facilities that syslog supports.

Configure FTP Settings

When Logging is enabled, NetSpective will store the log file data until the data is transferred to a specified FTP server. The device can only store up to five (5) gigabytes of log file data, when the limit is reached older log files will be overwritten or discarded. The settings for configuring NetSpective for FTP transfers are:

FTP Settings	
IP or Hostname	IP address or host name of the FTP server.
User Name	User name required to access the FTP server.
Password	Password required for accessing the FTP server.
Directory	Directory on the FTP server you wish to use. Example: "/public/logs" (Do not enter the quotation marks). If you leave this field empty, logs will be transferred to the users default directory.

Choosing a Transfer Schedule

When you set up the log transfer schedule, you will need to have some idea of how much traffic your device generates in a given period. The device will store the logs on disk before they are transferred, and then will erase them once they have been successfully transferred to your specified FTP server.

However, since the device can only store up to five (5) gigabytes of log file data, log transfers must occur often enough that this limit is not reached otherwise older log files must be overwritten and discarded. For most companies, one day's amount of data will not come close to this limit, but a week's worth of data may exceed it.

We recommend transferring one day's worth of log file data to your FTP server and examining the total size of the logs. For example, if the device generates 800 megabytes of data in a typical day, you should set the transfer schedule to be at most every couple of days to avoid exceeding the device's 5 gigabyte limit.

Transfer Logs (Manual)

To force an immediate log transfer, click the "Transfer Logs" button. The device will then attempt to upload all of its log files to the specified FTP server. Diagnostic output will be displayed in a dialog.

Purging Logs

You may erase all log files on the device that have not yet been transferred by clicking the "Purge Logs" button. This will not erase any logs already transferred to your FTP server.

Network

The NetSpective device allows you to configure some network settings, such as the network interfaces, DNS settings, and static routes. These settings will allow the device more flexibility and a greater range of control in more complicated networks.

Device Settings

[admin](#) | [register](#) | [help](#) | [logout](#)

Search:

Group: System

Logging

Network

LDAP Sources

Certificate

Advanced

The NetSpective device allows you to configure some network settings, such as the network interfaces, DNS settings, and static routes. These settings will allow the device more flexibility and a greater range of control in more complicated networks. Note: Changing an interface's IP or netmask will require a restart of system services which may take a few minutes.

Interfaces

Interface	IP	Netmask	Device	Status	Mac Address
Admin	192.168.5.26	255.255.255.0	eth0	100 Full	00:03:47:6C:50:18
Monitor	N/A	N/A	eth1	down	00:01:02:EB:9B:A3

Default Gateway:

DNS Servers

DNS Search Domains

Additional Routes

<input type="checkbox"/> Destination	Netmask	Gateway
No Routes Found		

Interfaces

You may view and change the IP address and Netmask of the device's Ethernet and virtual interfaces. You may also view the link status and MAC Hardware addresses of your Ethernet devices.

Admin Interface

This interface was initially configured during the text mode installation. Use this interface to access the NetSpective web-based administration page.

You may secure the administration page to only accept connections from certain IP addresses. You may do this via the "Restrict Admin Access" menu option in the console setup interface.

Internal Interface (Proxy Only)

If this interface is configured with an IP address, NetSpective's proxy service will listen for client connections on it. Otherwise, NetSpective's proxy service will listen on the Admin interface. On appliances with 2 Ethernet ports, the internal interface is a virtual device that shares the Admin Ethernet port. The proxy service listens on port 3128.

To enable failover or certain types of load balancing, you must configure the internal interface with an IP address.

External Interface (Proxy Only)

NetSpective can function without this interface being configured. However, to obtain maximum performance and to utilize all available Ethernet ports, you may configure this interface with an IP address. When this interface is configured, NetSpective will use it to send and receive all external (upstream) traffic.

Monitoring Interface (Passive Only)

NetSpective captures traffic with this interface. Typically, this interface is plugged into a mirrored port of a switch. Block packets, however, are sent through the Admin interface.

Default Gateway

Enter the default gateway that the device will use for traffic not on its local subnet.

DNS

You may enter a list of DNS servers to use and a list of DNS Search Domains. For example, a search domain of "telemate.net" will allow a short hostname of "intranet" to resolve to "intranet.telemate.net". Providing a DNS server will allow NetSpective to use host names in addition to IP addresses for other settings, such as the Logging FTP server.

Additional Routes

Network Routing is used to provide the NetSpective device with information that helps it direct data to different subnets. This allows the NetSpective device to support complex networks.

Add a Network Route

To create a network route, click the Add button at the bottom of the routes section. To edit a route, click the network route's link. Once the dialog has opened, update the necessary information:

Network Route	
Destination	Specifies the destination of the route. The destination can be an address of a network or an individual host.
Netmask	The netmask associated with the destination. The netmask can be 255.255.255.255 for an individual host or it may be the netmask of a subnet, for example 255.255.254.0.
Gateway	The host that traffic matching this destination and netmask should be forwarded to. The gateway must be able to route traffic to another network.

Deleting a Network Route

To delete network routes, select the check box next to each route's name. To delete all network routes displayed, select the check box in the upper left-hand portion of the table. Once the network routes are selected, click the Delete button to delete the network routes.

LDAP Sources

NetSpective connects to LDAP directories to collect User Name, User Group Assignments, and Organizational Units. This information is used to map LDAP Containers or Groups to NetSpective Groups where Content Filtering policies are assigned. LDAP sources support bridging to Active Directory, eDirectory, or Open Directory as well as a combination of each as an environment requires.

The screenshot shows the 'Device Settings' interface with the 'LDAP Sources' tab selected. A search bar and a 'Group' dropdown (set to 'System') are at the top. Below a descriptive paragraph, a table lists three LDAP sources: Apple, Novell, and Windows. Each row has a checkbox, a name, a host, an LDAP type, and a status. The Novell row is highlighted in orange and has a 'Processing' status. At the bottom are 'Delete', 'Add', and 'Sync' buttons.

<input type="checkbox"/>	LDAP Source	Host	LDAP Type	Status
<input type="checkbox"/>	Apple	192.168.10.200	Open Directory	OK
<input type="checkbox"/>	Novell	192.168.10.201	eDirectory	Processing
<input type="checkbox"/>	Windows	192.168.10.202	ActiveDirectory	OK

Managers can also be assigned to NetSpective and may use their LDAP password to log on. In the same manor Users can be synchronized to groups, management privileges can be delegated to Managers using an LDAP OU, Group, or individual user accounts.

Creating or Updating LDAP Sources

To add a new LDAP Source, click the Add button. To change a source, click on the name of the source you would like to edit. Once the dialog has opened, enter the appropriate information.

The screenshot shows the 'LDAP Source' configuration dialog box. It contains fields for Name, LDAP Type (a dropdown menu), NetBIOS Domain, IP or Hostname, Port, Login DN, Password, and Search Base. The fields are populated with example data: Name: 'Prodmgmt qa domain', LDAP Type: 'Active Directory', NetBIOS Domain: 'prodmgmt', IP or Hostname: '192.168.10.202', Port: '389', Login DN: 'prodmgmt\administrator', Password: masked with dots, and Search Base: 'dc=prodmgmt, dc=local'. 'OK' and 'Cancel' buttons are at the bottom.

Name – A name to identify the LDAP Source.

LDAP Type – The LDAP Type can either be Active Directory or eDirectory. The Disabled option removes the LDAP Source as an option from group configuration.

IP or Hostname – The IP or Hostname of the LDAP server. A hostname requires NetSpective to be configured to use a valid DNS Server.

Port – The port number specifies which TCP port is used to connect to the server. If the LDAP server is not using its default port you should set it here. If port 636 is selected, the LDAP connection will be made using LDAPS (secure LDAP over SSL); however, the remote certificate will not be verified.

Login DN – The LDAP Distinguished Name of the user who will login and view the users and groups defined in the LDAP tree. This user should have read-only access to the users and groups in the tree and the users' group memberships. Using an Administrative account is not recommended.

Example Login DN's

Type	Login DN
Active Directory	telemate\joe.smith
Active Directory	cn=NetSpective LDAP,cn=Users,dc=example,dc=com
Active Directory	cn=Joe Smith,ou=Development,ou=Telemate.Net Software,dc=telemate,dc=net
eDirectory	cn=admin,o=test
Open Directory	uid=netspective,cn=users,dc=qa,dc=xserve,dc=com

Failure to select a proper hostname, user name and password will result in a verification failure. This is most likely due to an incorrect Login DN or that the Login DN/password was typed in the in the wrong case. If necessary, consider exporting the LDAP tree to an LDIF file and confirming the distinguished name of the user.

Password – The password to authenticate the Login DN.

Search Base - A LDAP Distinguished Name that will be used as the root (base) for LDAP searches. In most cases, you will want to set the search base to be the root of your LDAP Tree. However, if you are in a large organization you may choose to improve synchronization performance by setting a more selective search base that omits unneeded user or group objects. Make sure that the user defined by the 'Login DN' has read-only access to all objects under the search base.

Example Search Base

Type	Search Base
Active Directory	dc=telemate,dc=net
eDirectory	o=test
Open Directory	dc=xserve,dc=com

Integration with an Active Directory Forest

If your environment contains an Active Directory forest with multiple Windows domains, there are two options for associating NetSpective groups with Active Directory groups containing users with mixed domain membership. Both methods involve the use of a Global Catalog Server (GCS).

Option 1: Using Universal Groups

This method only needs one configured LDAP Source. This source must be a Global Catalog Server that listens on port 3268. Configure this source with an empty search base or a search base that is above all domains in the forest, for example, 'dc=com'. You may associate a NetSpective group to any Universal Group in this source.

Option 2: Using Non-Universal Groups

This method requires one LDAP source which is a Global Catalog Server, as described above in Option 1. In addition, you must configure a regular Active Directory source (port 389) for each domain in the forest. A source for each individual domain is required because a Global Catalog server does not contain enough membership information for non-universal groups. You may associate a NetSpective group to any group returned by the GCS source, universal or not.

LDAP Lookup Precedence Order

If multiple LDAP Sources are required, a precedence order can be established by the order they exist in the LDAP Source list. The precedence order for associating users to groups is done alphabetically by the LDAP Source name defined for each source.

Deleting LDAP Sources




To delete LDAP sources select the check box next to each source's name. To delete all LDAP sources displayed on the current page, select the check box in the upper left-hand portion of the table. Once the sources are selected, click the Delete button to delete the sources. If all LDAP Sources on a page are selected, the option to select the LDAP Sources on every page will become available.

If you wish you force a resynchronization of an LDAP source, simply check the box next to a source and click the Sync button.

Certificate

The NetSpective device allows you to add a certificate from a Certificate Authority. When you connect to the NetSpective Administration site via SSL (https), the server authenticates itself by presenting a digital certificate. The certificate is proof that a third party has verified that the website belongs to who it claims to belong to.

Device Settings[admin](#) | [register](#) | [help](#) | [logout](#)

 Search:

Group: System

Logging

Network

LDAP Sources

Certificate

Advanced

The certificate is used by the NetSpective device when connecting to the administration website by SSL.

Certificate Details (Self Signed)

Issued To

Organization: TeleMate.Net Software, Inc.

Organization Unit: N/A

Common Name: netspective

Locality: Atlanta

State/Province: Georgia

Country: US

Issued By

Organization: TeleMate.Net Software, Inc.

Common Name: netspective

Locality: Atlanta

State/Province: Georgia

Country: US

Validity

Issued On: May 22 18:35:42 2008 GMT

Expires On: May 20 18:35:42 2018 GMT

Generate Request

Add Certificate

Certificate Details

The Certificate details show the information for the current certificate. By default, the NetSpective device will use a Self-signed certificate. Self-signed certificates are not certified by a Certificate Authority so you may still receive warnings or certificate exceptions when browsing the NetSpective Administration site by SSL (https).

Generate a Certificate Request

Before you add a SSL Certificate, you need to generate a Certificate Signing Request (CSR) for the authority generating your certificate. To do this click the Generate Request button at the bottom right of the screen.



Once the dialog has opened, update the necessary information:

SSL Certificate Request Requirements	
Name	The Name field is optional. It could represent the individual making the request or a name to identify the request.
Unit	The Unit field is optional. It is used to identify certificates registered to an organization. The Unit or Organizational Unit (OU) field is the name of the department or organization unit making the request.
Organization	The Organization value cannot contain an &, @, or any other symbol in its name, you must spell out the symbol or omit it. For example: AB & C Corporation would be ABC Corporation or AB and C Corporation.
City/Locality	The City or Locality field is the city or town name. Do not abbreviate the name. For example: Saint Louis, not St. Louis
State	The State field is the state or province name. Do not abbreviate the name, spell it out completely. For example: Georgia
Country	The Country where the Organization exists. Use the two-letter code without punctuation for country, for example: US or CA.
Email	The Email field is optional.
Host+Domain	The Host+Domain refers to the Common Name. The common name is a combination of the host name and domain name. It looks like "host.domain.com".

Certificate Request Result

After clicking the OK button in the Generate Request dialog, a new dialog will open with the Certificate Request data. This will be required to create a certificate. A Certificate Authority will ask for this information when you go to apply for a certificate. Make sure to include the entire text of the Certificate Signing Request including the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----.

Add a Certificate

After you have applied for a Certificate from a Certificate Authority, you will receive from them a SSL Certificate and, optionally, an Intermediate CA Certificate, in a similar format as the Certificate Request. Copy and paste the certificate(s) into the form areas provided. Make sure to include the header line, -----BEGIN CERTIFICATE-----, and the footer line, -----END CERTIFICATE-----.

Add Certificate

NetSpective will use the certificate's common name (CN) as its SSL hostname. If this behavior is unintended, as is the case with a wild card SSL certificate, you may specify NetSpective's SSL hostname by entering it in the SSL Hostname field. When entering the certificate in the area provided make sure to include the header line (BEGIN CERTIFICATE) and the footer line (END CERTIFICATE).

SSL Certificate

SSL Hostname (Optional)

Intermediate CA Certificate (Optional)

OK Cancel

Restore the Default Certificate

If you have changed the certificate and wish to restore the default certificate, click the Restore Default button from the control bar near the top of the page. This option is not available if the default certificate is already loaded.

Advanced

The Advanced options section includes system date and time, SNMP configuration, and SMTP settings.

System Time Test NTP Server	SMTP Settings Test Email
NTP enables automatic time synchronization. Please ensure that the NTP server and timezone are valid and that your firewall allows UDP port 123. Enter "none" to disable NTP.	
NTP Server: <input type="text" value="10.2.2.48"/>	Server: <input type="text" value="10.2.2.64"/>
Time Zone: <input type="text" value="America/New_York"/>	Return Address: <input type="text" value="helpdesk@telemate.net"/>
	User: <input type="text"/>
	Password: <input type="password"/>
	<input type="checkbox"/> Use SSL/TLS
SNMP Configuration	Windows Integration
<input checked="" type="checkbox"/> Enable SNMP Download MIB	Windows Integration will allow you to set up a trust relationship between the NetSpective device and your domain. This will allow users to be authenticated.
Allowed Network/Mask: <input type="text" value="10.2.0.0/16"/>	Host Name: WFPASSIVE
Community: <input type="text" value="thecolbert"/>	Domain: TELEMATE
LDAP Settings	Status: Active
Synchronization Interval: <input type="text" value="6 hours"/>	<input type="button" value="Join"/>
Override Requests	
Notification Interval: <input type="text" value="5 minutes"/>	
Custom Redirect	
<input type="checkbox"/> Enable Redirect	
IP Address: <input type="text"/>	

System Time

NetSpective can use an NTP server to automatically keep its internal clock synchronized. By default, it will synchronize to TeleMate.Net Software's NTP server at approximately 1:00 AM every day. It is important to make sure you have selected the correct time zone for your location. If you are having trouble communicating with the NTP server, make sure your firewall allows outbound UDP traffic on port 123.

SNMP Configuration

NetSpective may be monitored via SNMP so that you may keep track of its health and filtering activity. NetSpective exports industry-standard MIBS and a custom MIB that may be downloaded from the Utilities section. Please see your SNMP client's documentation for information on how to load custom MIBS. If you do not load NETSPECTIVE-MIB you may still access that dataset by using numeric OIDs but you will not see descriptions of any values.

Configuration

The SNMP service is disabled by default so that you may optionally configure any security settings before starting it. All SNMP information is read-only but access may be further restricted to a specific Network/Mask and/or a custom Community string.

Network/Mask Examples	
0.0.0.0/0	Allows access from any IP address (Default)
192.168.5.0/24	Allows access only from the 192.168.5 network
192.168.10.201	Allows access only from 192.168.10.201

Community Examples	
public	Allows access from most out-of-the-box SNMP clients (Default)
secret123	Allows access only from SNMP clients configured to use 'secret123' as the Community string

LDAP Settings

LDAP Synchronization lets you configure how often the NetSpective device will poll its LDAP sources for changes to users, groups, and organizational units. By default, the polling interval is every 30 minutes.

Override Requests

Admins and NetSpective managers can enable Override Requests emails to be sent to them periodically. These emails will notify managers when there are override requests waiting to be assessed. In this section, the interval can be changed between 5 minutes and daily. The default is set to send emails daily

SMTP Settings

If you want to be able to send email for abuse notification, you must specify an email server to use.

Server

This is the host name or IP address of your mail server. Most popular mail servers support the SMTP protocol, which is the standard protocol for Internet email. Keep in mind that your IT staff may have disabled it, or they may have configured security so that it may only be used with some email addresses. The default port is 25, and you should almost never have to change this. If you need to use a different port, enter the server and port separated with a colon, like 192.168.5.22:25.

Return Address

This is an optional return address field for sending email. Some SMTP servers require a valid email address for the return address.

User

This is an optional user name field for accessing the SMTP server. The user name can be an email address.

Password

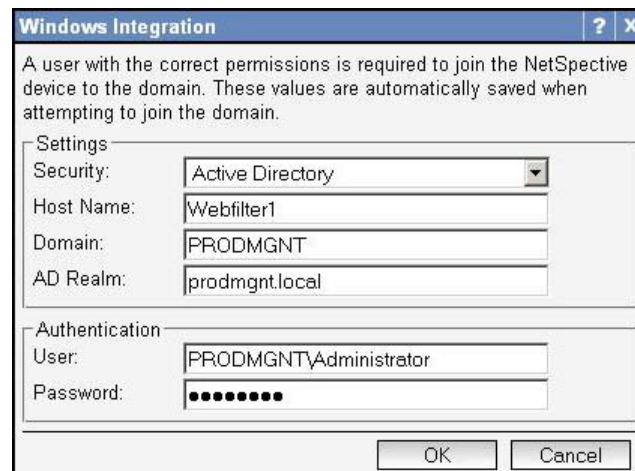
This is an optional password field for accessing the SMTP server.

Use SSL/TLS

Check this option to use Transport Layer Security (TLS) for secure communications.

Windows Integration

Windows Integration allows you to set up a trust relationship between the NetSpective device and your domain. This will allow users to be authenticated for the Portal page and the Proxy service. A domain user with sufficient privileges is required to add the NetSpective device to the domain.



Security

This may be set to either "Windows NT" or "Active Directory". Networks with older domain controllers may only accept "Windows NT", and newer domain controllers may only accept "Active Directory".

If you want to use "Active Directory" security, you must first create a DNS Host Record ("A" Record) for NetSpective. For example, if your AD Realm is "telemate.net", and NetSpective's host name in your network is 'mynetspective', you must create a DNS Host Record for "mynetspective.telemate.net". Also, you must ensure that your AD Realm (example: "telemate.net") is a DNS search domain in the Device Settings -> Network tab.

Host Name

The host name is the short name of the NetSpective device. You can choose any name to represent the NetSpective device on your domain. (Example: mynetspective)

Domain

The Windows NT compatible (Short) domain of your network. (Example: telemate)

AD Realm (Active Directory Only)

The Active Directory Realm of your network. (Example: telemate.net)

Status

If the NetSpective device has been successfully joined to the domain, the status will be *Active*. Otherwise, the status will be *Inactive*.

Filter Settings

Here you will find options to customize redirect pages, proxy settings, links to our various authentication agents as well as NetAuditor, define custom categories, add YouTube for Schools codes, and SIP options.


Customization

The customization section allows you to edit the content on each redirect page. These pages include the block page, policy reminder page, standard portal, mobile compatible portal, and the mobile pairing pages. Each page can be customized with different color, text, images, even HTML code. Edited pages can be viewed with the preview button.

Block Page

Your NetSpective will display a block page when a URL is blocked. The text of the block page can be customized for each language. To load the block page configuration for a specific language, select the desired language from the list located at the top of the configuration screen. Once loaded, the text and options can be configured.

Filter Settings[admin](#) | [register](#) | [help](#) | [logout](#)

 Search:

Group: System

Customization

Authentication

Define Categories

YouTube | Schools

SIP Options


Advanced

[Block Page](#) | [Policy Reminder](#) | [Standard Portal](#) | [Mobile Compatible Portal](#) | [Mobile Pairing](#)

You may customize NetSpective's block page using the text entries below. Click a toolbar icon to insert a predefined macro (for example, the URL that was blocked). You may also customize the colors shown for an abuse warning or abuse lockout. Click Preview to view a sample block page.

Language: English [Select Group] [Select Mode]

Blocked Text



[blockedurl] has been categorized as [category]. It has been blocked per your organization's [policy]Internet Usage Policy[/policy] for group [group].

Policy URL:

Override Text

If you would like to override the block of this site for [duration] minutes, please enter the override password below:

Label (User):

User Name:

Label (Password):

Password:

Button:

Override

Display Options

☒ Foreground Graphic

☒ Background Graphic

Abuse Options

Warning Color: [None]

Lockdown Color: Red

Request Text

If you would like to request a different category for this site, please select a new one below:

Label (Back):

Back

Label (Request):

Request Change

Label (Category):

Category:

Label (Comment):

Comment

Button:







Request Change

System Control

72

Editing Block Text


The text is displayed on the block page when a user visits a blocked URL. There are special tags available that will provide information specific to the user or blocked URL. The tag information is listed below:

Tag Name	Button	Text	Description
Blocked URL		[blockedurl]	Inserts the blocked URL.
Blocked Category		[category]	Inserts the blocked category.
Internet Usage Policy		[policy]Usage Policy[/policy]	Inserts the enclosed text as a link to the Internet usage policy.
Group		[group]	Inserts the group the blocked user belongs to.
User IP		[userip]	Inserts the IP Address of the blocked user.
User Name		[username]	Inserts the user name of the blocked user.

The **Policy URL** is the value of the hyperlink used on the block page for the Internet usage policy.

Editing Override Text

The override text is only displayed if the user or group has the override mode enabled. The text is displayed at the bottom of the block page below the block text. There are special tags available for use with the override text, the tags are listed below:

Tag Name	Button	Text	Description
Override Duration		[duration]	Inserts the duration, in minutes, the override will last.

Underneath the override text on the block page are fields to rename the user name label, password label and override button text. The text for the user name label can be set in the **Label (User)** field. The text for the password label can be set in the **Label (Password)** field. The submit button text can be set in the **Button** field.

Display Options

The foreground and background images on the normal, abuse and warning block pages can be disabled by unchecking the box associated with each type.

Abuse Options

The Abuse Options allow you to configure the warning and abuse block pages to have a different color background. This allows for easier identification of block type when a user has been sent to a block page.

Preview

The preview option is located in the top right of the block settings page. When a block page type is selected, the block page settings will automatically be saved. A new browser window will then open with a sample of the block page for the selected type.

Policy Reminder

NetSpective will display a Policy Reminder page when a category is flagged as abusive and its action is set to 'Monitor'. This is done on the Group Policy page. The text of the policy page can be customized for each language. To load the policy page configuration for a specific language, select the desired language from the list located at the top of the configuration screen. Once loaded, the text and options can be configured.

The screenshot shows the 'Filter Settings' interface. At the top, there are links for 'admin', 'register', 'help', and 'logout'. Below these are icons for file operations and a search bar. A 'Group' dropdown menu is set to 'System'. A navigation bar contains tabs: 'Customization', 'Authentication', 'Define Categories', 'YouTube | Schools', 'SIP Options', and 'Advanced'. Below the navigation bar, a breadcrumb trail shows 'Block Page | Policy Reminder | Standard Portal | Mobile Compatible Portal | Mobile Pairing |'. The main content area has a text block explaining that the Policy Reminder page can be customized using text entries and toolbar icons. Below this, there is a 'Language' dropdown set to 'English' and a 'Preview' button. The 'Policy Text' section contains a text area with a sample policy reminder message. The 'Policy Buttons' section has two input fields for 'Accept' and 'Decline' button labels.

Editing Policy Text

The policy text will accept HTML and CSS to allow for further customization of policy text. There are also special tags available that will provide information specific to the user or URL. The tag information is listed below:

Tag Name	Button	Text	Description
Blocked URL		[blockedurl]	Inserts the blocked URL.
Blocked Category		[category]	Inserts the blocked category.
Group		[group]	Inserts the group the blocked user belongs to.

Editing Policy Buttons

There are fields to rename the Accept button and Decline button text. The text for the Accept button can be set in the **Accept** field. The text for the Decline button can be set in the **Decline** field.

Standard Portal

NetSpective can use the Standard Authentication Portal to authenticate users from unknown IP addresses. You may configure certain IP address ranges to use the Standard Portal by using the Authentication tab. The standard portal's appearance can be customized by using the provided options and by using HTML and CSS.

Filter Settings [admin](#) | [register](#) | [help](#) | [logout](#)

Search: Group:

Customization | **Authentication** | Define Categories | YouTube | Schools | SIP Options | Advanced

[Block Page](#) | [Policy Reminder](#) | **[Standard Portal](#)** | [Mobile Compatible Portal](#) | [Mobile Pairing](#)

You may customize NetSpective's Authentication Portal login page using the text entries below. The Authentication Portal may be activated via the Filter Settings -> Authentication tab.

Language:

Label Text	
Label (Title):	<input type="text" value="Login"/>
Label (User):	<input type="text" value="User:"/>
Label (Password):	<input type="text" value="Password:"/>
Button:	<input type="text" value="Submit"/>

Additional Text
<pre><style type="text/css"> form#frm { position: static; margin: 20px auto; } h1 { text-align: center; } p { text-align: center; } </style> <h1>Network Authentication Portal</h1> <p>NetSpective requires that you log in with your user name and password to enable internet access.</p></pre>

Editing Portal Text

The text of the portal page can be customized for each language. To load the portal page configuration for a specific language, select the desired language from the list located at the top of the configuration screen. Once loaded, the text and options can be configured.

Label Text

There are fields to rename the login title label, user name label, password label and submit button text. The text for the login title label can be set in the **Label (Title)** field. The text for the user name label can be set in the **Label (User)** field. The text for the password label can be set in the **Label (Password)** field. The submit button text can be set in the **Button** field.

Additional Text

The additional text is displayed on the page when a user is redirected to the Authentication Portal. The additional text will accept HTML and CSS to allow for further customization of the portal page.

Mobile Portal

NetSpective can use the Mobile Portal to authenticate users from unknown IP addresses. You may configure certain IP address ranges to use the portal by using the Authentication tab. The mobile portal's appearance is designed using HTML5 standards in order to optimize appearance on mobile devices such as smart phones and tablets. Text on the portal page can be customized by using the provided options.

The screenshot shows the 'Filter Settings' interface. At the top, there are links for 'admin', 'register', 'help', and 'logout'. Below these are icons for a folder, a document, and a magnifying glass, followed by a 'Search:' field. To the right is a 'Group:' dropdown menu set to 'System'. A row of tabs includes 'Customization', 'Authentication', 'Define Categories', 'YouTube | Schools', 'SIP Options', and 'Advanced'. Below the tabs is a row of links: 'Block Page', 'Policy Reminder', 'Standard Portal', 'Mobile Compatible Portal' (which is highlighted), and 'Mobile Pairing'. The main content area has a heading 'You may customize NetSpective's Mobile Compatible Portal logon page using the text entries below. The Portal may be activated via the Filter Settings -> Authentication tab.' Below this is a 'Language:' dropdown set to 'English' and a 'Preview' button. The 'Label Text' section on the left contains five fields: 'Page Title' (NetSpective), 'Label (Link)' (Login), 'Label (User)' (User), 'Label (Password)' (Password), and 'Button' (Submit). The 'Additional Text' section on the right contains a text area with the text: 'NetSpective requires that you log in with your user name and password to enable Internet access.'

Editing Portal Text

The text for the portal page can be customized for each language. To load the portal page configuration for a specific language, select the desired language from the list located at the top of the configuration screen. Once loaded, the text and options can be configured.

Label Text

There are fields to rename the page title, link label, user name label, password label and submit button text. The page title is displayed in the upper left corner of the page. The text can be set in the Page Title field. The link label is for the link that will be displayed when Mobile Portal is used in conjunction with Mobile Pairing. The link will be displayed in the upper right corner of the Mobile Pairing page. The text can be set in the Label (Link) field. The user name, password and submit button are found in the center of the page below the Additional Text. The text for the user name label can be set in the Label (User) field. The text for the password label can be set in the Label (Password) field. The submit button text can be set in the Button field.

Additional Text

The additional text is displayed in the center of the page when a user is redirected to the Mobile Portal.

Mobile Pairing

NetSpective can use the Mobile Pairing page to authenticate unknown IP addresses by associating devices with users. You may configure certain IP address ranges to use mobile pairing by using the Authentication tab. The page's appearance is designed using HTML5 standards in order to optimize appearance on mobile devices such as smart phones and tablets. Text on the mobile pairing page can be customized by using the provided options.

The screenshot shows the 'Filter Settings' interface with the 'Mobile Pairing' tab selected. At the top, there are links for 'admin', 'register', 'help', and 'logout'. Below this is a search bar and a 'Group' dropdown set to 'System'. A navigation bar contains tabs: 'Customization', 'Authentication', 'Define Categories', 'YouTube | Schools', 'SIP Options', and 'Advanced'. The 'Mobile Pairing' tab is active, showing a breadcrumb trail: 'Block Page | Policy Reminder | Standard Portal | Mobile Compatible Portal | Mobile Pairing |'. The main content area explains that users can customize the Mobile Pairing page and provides a 'Language' dropdown set to 'English' and a 'Preview' button. The configuration is divided into two sections: 'Label Text' and 'Text (Pair)'. The 'Label Text' section includes fields for 'Page Title' (NetSpective), 'Label (Link)' (Pair), 'Button (Pair)' (Pair), and 'Button (Cancel)' (Cancel). It also has a checked 'Allow Comments' checkbox with a 'Comment' field and an unchecked 'Make Required' checkbox. The 'Text (Pair)' section contains a text area with the message: 'NetSpective requires that you pair your device to enable Internet access.' Below this is the 'Text (Waiting)' section with a text area containing 'Waiting to be paired...'.

Editing Portal Text

The text for the pairing page can be customized for each language. To load the pairing page configuration for a specific language, select the desired language from the list located at the top of the configuration screen. Once loaded, the text and options can be configured.

Label Text

There are fields to rename the page title, link label, pair button text, cancel button text and set comment options. The page title is displayed in the upper left corner of the page. The text can be set in the Page Title field. The link label is for the link that will be displayed when Mobile Pairing is used in conjunction with Mobile Portal. The link will be displayed in the upper right corner of the Mobile Portal. The text can be set in the Label (Link) field. The pair button is located on the initial pairing page. The text can be set in the Button (Pair) field. The cancel button is on the "waiting to pair" page. The text can be set in the Button (Cancel) field.

When pairing, you have the option to allow or require users to provide a comment before requesting their device be paired. If Allow Comment is checked then the Mobile Pairing page will display an area for adding a comment. The placeholder text in the comment area is customizable and can be set in the field below the Allow Comment check box. To require a comment before accepting a pairing, check the Make required checkbox.

Text (Pair)

The pairing text is displayed in the center of the page when a user is redirected to the Mobile Pairing page.

Text (Waiting)




Depending on the pairing configuration, a user may be presented with a "waiting page" once they click the Pair button. The waiting text is displayed on the "waiting page".

Proxy


NetSpective can use traffic shaping to give higher or lower priority to certain traffic and to limit traffic. NetSpective may also operate in a load balanced or fail over cluster. Finally, NetSpective may host a Proxy Auto Configuration (PAC) file to support easy configuration of client computers.

It should be noted that there is limited IPv6 support for Proxy Auto Configuration. You will find settings for this under Filter Settings > Proxy. When adding rules the WPAD file, it will not accept IPv6 special rules.

Filter Settingsadmin | [help](#) | [logout](#)



Search:



Group: System

Proxy

NetSpective can use traffic shaping to give higher or lower priority to certain traffic and to limit traffic. NetSpective may also operate in a load balanced or fail over cluster. Certain destination sites or IP addresses, such as your local intranet, can be configured to bypass NetSpective or use an alternate proxy.

Proxy Settings

Cluster Mode: None/Standalone

Max Mbps: 100

☐ Enable X-Forwarded-For Header

☐ Enable Google NoSSLSearch Option

Priority Settings

	Low	Medium	High
Target (%)	1	9	90
Limit (%)	no limit	no limit	no limit





Proxy Automatic Configuration

Last Updated On: 2014-07-16 09:06 AM - [Download](#)

NetSpective Proxies: 10.2.40.117 - [Edit List](#)

Rules

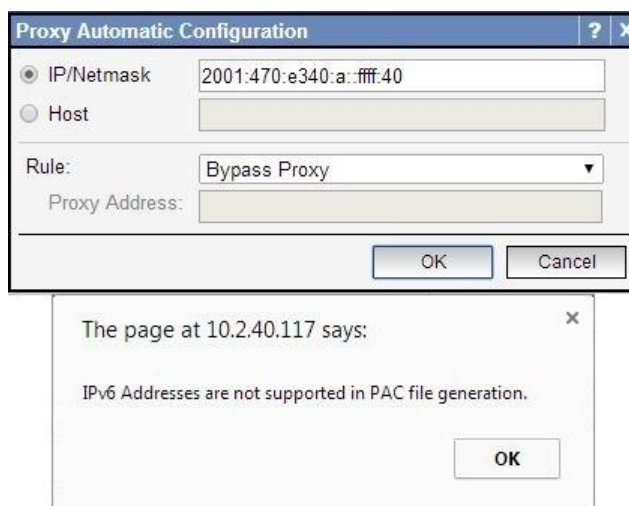
☐ Exclude Simple Hostnames

<input type="checkbox"/> Destination IP/Netmask	Rule		
<input type="checkbox"/> 192.168.0.0/16	Bypass Proxy		
<input type="checkbox"/> Destination Host Name	Rule		
<input type="checkbox"/> *.telemate.net	Bypass Proxy		

Delete

Add

The Rules section will give an error message when attempting to add an IPv6 rule.



Max Mbps

The maximum total receive and transmit bandwidth that the NetSpective device will allow. This should be set no higher than your maximum internet bandwidth to avoid congestion and maximize fairness.

Note: In a load balanced cluster, this represents the maximum bandwidth allowed by the entire cluster. Each device will be limited to a constant fraction of this bandwidth.

Cluster Mode

NetSpective devices may run as a standalone device or as part of a cluster. There are two types of clusters, fail over and load balanced. You may view the current cluster status via the Cluster statistics report.

Fail Over

Multiple NetSpective appliances are configured with the same Internal IP address. The appliances coordinate so that only one of them is active and will reply to ARP requests for the shared Internal IP. If the active appliance goes down for more than 60 seconds, one of the backup appliances will automatically take over. The running appliance with the lowest Admin IP address (192.168.5.1 is lower than 192.168.5.3) will always be the active node in the cluster.

Load Balanced

In this mode, multiple NetSpective appliances simultaneously service client connections. There are 3 primary ways to configure load balancing.

Separate load balancer device - Direct Routed: All appliances should have the same Internal IP address and ARP disabled.

Separate load balancer device NAT - All appliances should have a unique IP address and ARP enabled.

Proxy Auto Configuration (PAC) balancing - All appliances should have a unique IP address and ARP enabled. You may use the NetSpective PAC generator to automatically balance the load among all appliances.

Priority Settings

NetSpective supports 3 priority classes of traffic - High, Medium, and Low. Each priority class has a configurable target percentage of maximum bandwidth, for example High priority traffic may use 75% of the maximum allowed bandwidth even when there is demand for Medium and Low traffic. The target percentages must add up to 100%. A priority class may use more than its target percentage only if the other priorities are not currently using their entire target.

Each priority class can also have an optional limit of maximum bandwidth, for example Low priority traffic may be limited to using no more than 20% of maximum bandwidth, even when there is no demand for High or Medium traffic.

Traffic is assigned to one of the priority classes via the Group Policy page. By default, all traffic is Medium priority.

Proxy Automatic Configuration

Proxy Automatic Configuration is an open, multi-vendor standard for easy configuration of client browsers and devices. On startup, web browsers and devices will issue a DNS request for a special hostname and download a configuration file. This configuration file defines what proxies to use based on the client's IP and the destination of their traffic. NetSpective can generate and host the PAC file. However, you must configure your DNS server to map the hostname "wpad.[YOUR DOMAIN]" to the Admin or Internal IP of the NetSpective appliance. For example, if your domain was "telemate.net", you would map "wpad.telemate.net" to the NetSpective device.

Last Updated On / Download

Displays the last date and time that the PAC file was updated by an Administrator. If you would like to host the PAC file on a different web server, you may download the file by clicking on the 'Download' link.

NetSpective Proxies

This setting is required. Click 'Edit' to bring up a dialog that displays all currently detected NetSpective devices and the list of assigned proxy IP addresses or hostnames. Make sure the device's IP or DNS hostname, as well as any other devices in a load balanced cluster, are in the 'Assigned' list. You may add an IP or DNS hostname of a NetSpective proxy device by clicking the 'Add' button. Click "OK" when you are finished.

Note: To use Kerberos authentication, the Proxy Automatic Configuration file must contain DNS hostname(s) and not IP Addresses of the NetSpective devices. Kerberos requires a DNS hostname for operation.

Rules

You may wish to exempt certain sites, such as your intranet sites, to bypass the proxy to ensure maximum performance or to not interfere with internet shaping rules. You can also force certain sites to use a different proxy, which may be useful for complicated scenarios. Click 'Add' to add a destination rule. Rules are evaluated in order from top to bottom and the first matching rule is used. Click the up or down arrows to the right of a rule to move it up or down in the order.

Authentication

NetSpective can require authentication from users with unknown IP addresses (IPs not statically assigned to a user or dynamically assigned by Logon Agent). Authentication methods are the Portal web page and, if in Proxy mode, session based authentication. The Authentication section allows you to enable each authentication method for a range of IPv4 or IPv6 addresses on your Wi-Fi network. This area will also accept slash notation to designate a range of IP addresses.

Authentication Portal

Users can be redirected to the Portal logon page, which may require a user name and password to be entered manually (LDAP mode) or use automatic integrated Windows authentication (Windows mode). You must join NetSpective to a Windows domain to use Windows authentication. To use LDAP authentication, you must configure an LDAP source. If for some reason a Windows integrated login fails, the user will be directed to the Portal web page and will be able to use his or her LDAP login.

When a user authenticates via the Portal, NetSpective will remember that IP address to user association for a specified time. You may configure the timeout to be based on traffic inactivity or based on time from last log on. You may also enter the number of minutes or hours that Portal logons will be kept before timing out.

When Windows Integrated Logon is selected, some users' browsers may require additional configuration or the user may still be prompted for authentication. In Internet Explorer, the NetSpective device will need to be added to the 'Local Intranet Sites'. In IE 7, to add a local intranet site go to Tools -> Internet Options, then select the Security tab, select Local Intranet, click Sites and then select Advanced. In Firefox, navigate to about:config. Then add the IP of the NetSpective device to *network.automatic-ntlm-auth.trusted-uris*. For a detailed configuration guide for configuring Internet Explorer for single sign-on authentication using group policies please refer to the NetSpective Authentication Guide.

Mobile Compatible Portal

Mobile Compatible Portal is used to authenticate users from unknown IP addresses. You may configure certain IP address ranges to use the portal by using the Authentication tab. The mobile compatible portal's appearance is designed using HTML5 standards in order to optimize appearance on mobile devices such as smart phones and tablets.

Customization	Authentication	Define Categories	YouTube Schools	SIP Options	Advanced
<p>NetSpective can require authentication from users with unknown IP addresses (IPs not statically assigned to a user or dynamically assigned by Logon Agent). Users can be redirected to the Portal logon page, which may require a user name and password to be entered manually (LDAP mode) or use automatic integrated Windows authentication (Windows mode). NetSpective devices in proxy mode may also use session based authentication using LDAP, Windows NTLM, or Kerberos providers. Note: IP/Netmask rules are evaluated in order from top to bottom and the first matching rule is used.</p>					
Logon Agent Settings					
<input type="checkbox"/> Log out inactive Logon Agent Users at midnight					
Inactivity Duration: <input type="text" value="12"/> Hour(s) <input type="button" value="v"/>					
Authentication Rules					
<input type="checkbox"/>	Name	IP	Netmask	Mode	
<input type="checkbox"/>	range1	10.0.0.0	255.0.0.0	No Authentication	<input type="button" value="up"/> <input type="button" value="down"/>
<input type="checkbox"/>	range2	172.16.0.0	255.240.0.0	No Authentication	<input type="button" value="up"/> <input type="button" value="down"/>
<input type="checkbox"/>	range3	192.168.0.0	255.255.0.0	No Authentication	<input type="button" value="up"/> <input type="button" value="down"/>
<input type="button" value="Delete"/>		<input type="button" value="Add"/>			

Filter Settings > Authentication

Mobile Compatible Portal with Pairing

Mobile Compatible Portal with Pairing is the same as the Mobile Compatible Portal, except that the credentials supplied will be used to pair the mobile device to a user. Pairing is the association of a mobile device with a NetSpective User for a specified amount of time. A token is generated by the NetSpective and stored on the mobile device. The token is then used to identify the association between the mobile device and the assigned user until the timeout period is reached, or to permanently pair as configured.

The screenshot shows the 'Authentication Rule' configuration window. The 'Name' field is set to 'internal' and the 'Zones' field is set to '2001:470:e390:28::/64'. The 'Mode' is set to 'Mobile Portal - Passive'. Under the 'Authentication' section, 'Authentication' is checked, 'Method' is set to 'LDAP', 'Option' is set to 'Pairing by Authentication', and the 'Timeout' is set to 'Logon' with a value of '30' minutes. The 'Pairing by Request' section is unchecked. The 'Pairing Revalidation Period' is set to '20' minutes. The 'OK' and 'Cancel' buttons are at the bottom.

Filter Settings > Authentication: Click on a Rule

Portal Authentication Methods

Portal based authentication can be leveraged as a 'stop gap' measure to ensure all users are authenticated before accessing the Internet through a browser. The portal is design to force users to authenticate in networks where unauthenticated access is available.

LDAP Authentication

LDAP Authentication provides simple, encrypted HTTPS based authentication that should be compatible with any modern browser. Users' passwords will be checked against any LDAP sources you have configured. In addition, local NetSpective managers can authenticate using their NetSpective login name and password.

Windows NTLM Authentication

Windows NTLM Authentication provides single sign on capabilities for Windows users. In addition, some browsers, like Firefox, also support this method on other operating systems like Linux and Mac OS X. In order to use Windows NTLM authentication, NetSpective must be joined to a Windows domain. If for some reason a Windows integrated login fails, the user will be directed to the portal web page and will be able to use his or her LDAP login if enabled.

When Windows Integrated Logon is selected, some users' browsers may require additional configuration or the user may still be prompted for authentication. In Internet Explorer, the NetSpective device will need to be added to the 'Local Intranet Sites'. In IE 7, to add a local intranet site go to Tools -> Internet Options, then select the Security tab, select Local Intranet, click Sites and then select Advanced. In Firefox, navigate to about:config. Then add the IP of the NetSpective device to network.automatic-ntlm-auth.trusted-uris. If you require a detailed configuration guide for configuring Internet Explorer for single sign-on authentication using group policies, you may reference the 'Configuring Internet Explorer for Single Sign-On Authentication using Group Policies' section of the Authentication Guide.

Pairing Authentication

Enabling pairing will redirect end-users to a web page where they can request to be paired. Pairing is the association of a mobile device with a NetSpective User for a specified amount of time. A token is generated by the NetSpective and stored on the mobile device. The token is then used to identify the association between the mobile device and the assigned user.

If Authentication is enabled, the authentication type must be one of the Mobile Compatible options in order for Pairing to also be enabled. The option of a silent automatic pairing is also available for devices where administrators do not wish to have users prompted when authentication is required. The option can also be leveraged to create IP zone based pooling to a group policy.

Portal Timeout

When a user authenticates via the Portal, NetSpective will remember that IP address to user association for a specified time. You may configure the timeout to be based on traffic inactivity or based on time from last log on. You may also enter the number of minutes or hours that Portal logons will be kept before timing out. Mobile Compatible Portal with Pairing timeout is limited to time from last log on.

Pairing Allow Temporary Access

Instead of having the end-user waiting for a manager to assign the device, temporary access can be given. Granting temporary access will assign the device to a specified Group policy. Temporary Access shall timeout after the configured time.

Temporary Access can be configured to not prompt the end-user but pair automatically. However, if Pair is used in conjunction with Authenticate the end-user must be prompted since they will have a choice to either login or pair.

Pairing Revalidation Period

Paired devices that have been inactive for the configured time will be revalidated via the portal to assure they have a proper pairing. This setting applies to authentication ranges that are configured for either 'Pairing by Authentication' or 'Pairing by Request.'

Example – Let's say you are permanently paired with your iPad and the Pairing Revalidation Period is set to 60 minutes. When you first come onto the network in the morning and open your web browser, the browser will validate the pairing with NetSpective. You may see the pairing page for a brief moment, but it will disappear almost instantly and take you to your destination. This is a 'Pairing Revalidation'.

Throughout the day, even if you aren't surfing the web, your iPad will be accessing the internet through various services such as email, software updates, etc. These keep a constant flow of communication active between your device and the NetSpective. Since we have a constant flow of communication between your iPad and the NetSpective, there is no need to validate your device's pairing.

When you go home in the evening and your iPad leaves the network, your flow of communication with the NetSpective stops. This is when the Pairing Revalidation Period of 60 minutes comes into play. The NetSpective wants to be absolutely sure that you are who you are, so that someone else isn't taking advantage of your filtering policy and seeing unwanted content. If NetSpective does not communicate with your device for the 60 minutes that the Pairing Revalidation Period is set to, then the next time your device comes back onto the network, NetSpective will require your iPad to be revalidated. Once again, this can be done by opening your web browser where you will see the pairing page for a brief moment before it vanishes. Once that happens, your iPad is again validated. Your surfing and background services will continue to communicate with NetSpective and keep your device validated.

Proxy or Session Based Authentication

Proxy or Session based authentication is only available in NetSpective devices in proxy mode.

NetSpective devices in proxy mode may also use session based authentication. You may configure NetSpective to advertise multiple methods of session based authentication, and clients can choose to use any method they support.

Cached Session Based Proxy Authentication

This setting will cache the user's credentials and login on the appliance for the specified period of time. This can be set to inactivity or since login. Users will not be prompted to authenticate after the initial authentication.

Basic / LDAP

This option provides simple, encrypted HTTPS based authentication that should be compatible with any HTTP client. Users' passwords will be checked against any LDAP sources you have configured. In addition, local NetSpective managers can authenticate using their NetSpective login name and password.

NTLM (Windows Integrated)

This option provides single sign on capabilities for Windows users. In addition, some browsers such as Firefox also support this method on other operating systems such as Linux and Mac OS X. You must join NetSpective to a Windows domain to use NTLM Windows authentication.

NetSpective Wi-Fi Agent

Alternate methods of binding User ID to IP Addresses have been developed and are available based on customer requirements. For environments that utilize authentication at the wireless access point, NetSpective deployments can be customized to dynamically bind DHCP log and Access Control Server logs (RADIUS logs).


Entering Rules

To add an Authentication rule, click 'Add' at the bottom of the screen. Enter the IP and netmask of the users and select the method of Authentication. When finished, click OK. To delete an Authentication rule, click the checkbox next to it and click the "Delete" button. To move a rule up or down, click the Up or Down arrow at the right of the table. Note: Rules are evaluated in order from top to bottom and the first matching rule is used.

User Defined Categories

User defined categories are categories that can be named by the user. The only overrides associated with a defined category are those that are set up by the user on the Overrides page. Blocking a defined category is handled on the Group Policy page along with the other categories. When naming a defined category, a name can be set for each of the available languages.

Filter Settings[admin](#) | [register](#) | [help](#) | [logout](#)

 Search:

Group:

Customization

Authentication

Define Categories

YouTube | Schools

SIP Options

Advanced

You may create overrides that map to custom categories. Set the names of the custom categories below. If the category name for a language is blank the block page will default to the English name. Click the Trash icon to remove all overrides that are currently assigned to that category.

Language:

Categories

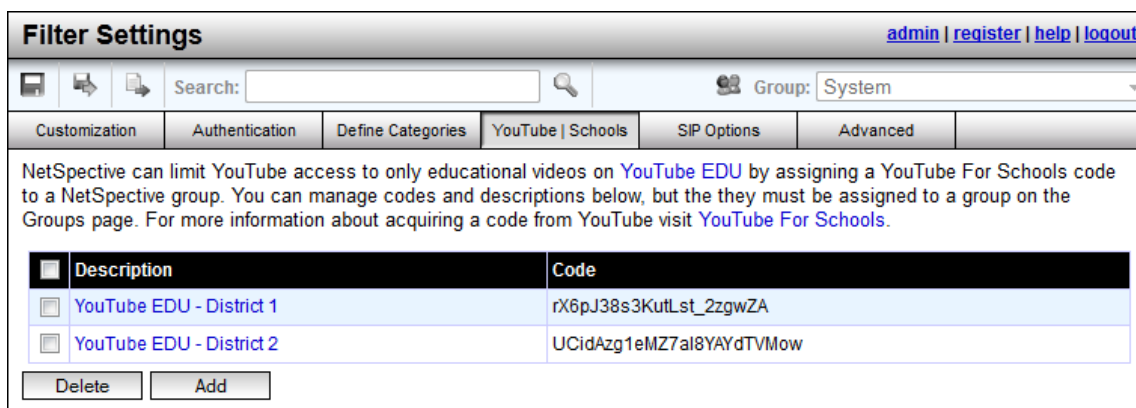
<input checked="" type="checkbox"/> User Defined #1:	<input type="text" value="Anonymous Proxy Testing"/>	<input type="checkbox"/> User Defined #11:	<input type="text" value="User Defined 11"/>
<input checked="" type="checkbox"/> User Defined #2:	<input type="text" value="Black List"/>	<input type="checkbox"/> User Defined #12:	<input type="text" value="User Defined 12"/>
<input checked="" type="checkbox"/> User Defined #3:	<input type="text" value="Software Update"/>	<input type="checkbox"/> User Defined #13:	<input type="text" value="User Defined 13"/>
<input checked="" type="checkbox"/> User Defined #4:	<input type="text" value="VoIP"/>	<input type="checkbox"/> User Defined #14:	<input type="text" value="User Defined 14"/>
<input checked="" type="checkbox"/> User Defined #5:	<input type="text" value="Image Searches"/>	<input type="checkbox"/> User Defined #15:	<input type="text" value="User Defined 15"/>
<input checked="" type="checkbox"/> User Defined #6:	<input type="text" value="User Defined 6"/>	<input type="checkbox"/> User Defined #16:	<input type="text" value="User Defined 16"/>
<input checked="" type="checkbox"/> User Defined #7:	<input type="text" value="User Defined 7"/>	<input type="checkbox"/> User Defined #17:	<input type="text" value="User Defined 17"/>
<input checked="" type="checkbox"/> User Defined #8:	<input type="text" value="User Defined 8"/>	<input type="checkbox"/> User Defined #18:	<input type="text" value="User Defined 18"/>
<input checked="" type="checkbox"/> User Defined #9:	<input type="text" value="User Defined 9"/>	<input type="checkbox"/> User Defined #19:	<input type="text" value="User Defined 19"/>
<input checked="" type="checkbox"/> User Defined #10:	<input type="text" value="User Defined 10"/>	<input type="checkbox"/> User Defined #20:	<input type="text" value="User Defined 20"/>

Enabling or Disabling User Defined Categories

Only an enabled User Defined Category can be seen in the Group Policy page and used in an override. When a User Defined Category is disabled all associated overrides will be deleted. The overrides will not be deleted until the changes are saved.

YouTube | Schools

NetSpective can limit YouTube access to only educational videos on [YouTube EDU](#) by assigning a YouTube For Schools code to a NetSpective group. See the Groups help for details on configuring a group with a code. For more information about acquiring a code from YouTube visit [YouTube For Schools](#).



Filter Settings [admin](#) | [register](#) | [help](#) | [logout](#)

Search: Group:

Customization Authentication Define Categories **YouTube | Schools** SIP Options Advanced

NetSpective can limit YouTube access to only educational videos on [YouTube EDU](#) by assigning a YouTube For Schools code to a NetSpective group. You can manage codes and descriptions below, but they must be assigned to a group on the Groups page. For more information about acquiring a code from YouTube visit [YouTube For Schools](#).

<input type="checkbox"/>	Description	Code
<input type="checkbox"/>	YouTube EDU - District 1	rX6pJ38s3KutLst_2zgwZA
<input type="checkbox"/>	YouTube EDU - District 2	UCidAzg1eMZ7aI8YAYdTVMow

Delete Add

To add a new code, click the 'Add' button. To change a code, click on the description of the code you would like to edit. Once the dialog has opened, enter the appropriate information:

Description – A description to easily identify the YouTube For Schools code.

Code – The code or school ID provided by YouTube for use with YouTube For Schools.

To delete YouTube For Schools codes select the check box next to each code's description. To delete all codes displayed, select the check box in the upper left-hand portion of the table. Once the codes are selected, click the Delete button to delete the codes.

SIP Options (Passive Only)

The Session Initiation Protocol (**SIP**) is a signaling protocol. It is commonly used in multimedia communication such as voice and video over the Internet.

The screenshot shows the 'Filter Settings' web interface. At the top, there are links for 'admin', 'register', 'help', and 'logout'. Below these are icons for a folder, a document, and a magnifying glass, followed by a 'Search:' text box. To the right is a 'Group:' dropdown menu set to 'System'. A navigation bar contains tabs for 'Customization', 'Authentication', 'Define Categories', 'YouTube | Schools', 'SIP Options' (which is active), and 'Advanced'. The main content area has a heading 'The Session Initiation Protocol (SIP) is a signalling protocol. It is commonly used in multimedia communication such as voice and video over the Internet. You can block all SIP registrations, block SIP audio and/or video sessions or choose to permit or block certain SIP Providers.' Below this, there are two sections: 'Media' and 'Service Providers'. The 'Media' section has the text 'Block SIP when the media type contains:' followed by four radio buttons: 'Audio Only', 'Video Only', 'Audio and Video', and 'All Media' (which is selected). The 'Service Providers' section has a dropdown menu set to 'Only allow Service Providers in this list' and a list box containing 'All Service Providers'. At the bottom of the 'Service Providers' section, there is a link 'Active Providers' and two buttons, 'Delete' and 'Add'.

Once you have chosen to block SIP in the Group Policy screen, you can use this screen to control the criteria of the SIP sessions you choose to block. You can block all SIP registrations, block SIP audio and/or video sessions or choose to permit or block certain SIP Providers.

A SIP Provider is the hostname of for the SIP server used by a provider and may be different than the provider's actual website. Additionally, many SIP providers may use different hostnames for SIP client registration, outbound calls and inbound calls. Please use the "Display Active SIP Providers" option (option appears when logging is enabled) to see which SIP Providers were previously permitted by the appliance. Use the content of the report to determine the name of the SIP hosts you wish to block.

To block a SIP provider you do not need to enter every SIP host seen in the report, it is possible to add the top level domain of a Provider to block all SIP hosts. For example, if your SIP Provider had servers "sip1.mysip.com", "sip2.mysip.com", "sip3.mysip.com" then you only need to block "mysip.com".

Advanced

This section contains advanced options that include Remote Logins, VLAN Traffic, and other options.

The screenshot shows the 'Filter Settings' interface with the 'Advanced' tab selected. The top navigation bar includes links for 'admin', 'register', 'help', and 'logout'. Below the navigation bar is a search bar and a 'Group' dropdown menu set to 'System'. The main content area is divided into two sections: 'Options' and 'Browser Protection'. In the 'Options' section, there are four checkboxes: 'Block URLs with Cross-Site Scripting (XSS)' (unchecked), 'Block Remote Logins Between Private IP Addresses' (unchecked), 'Monitor and Process VLAN Traffic' (checked), and 'Copy Original VLAN Tag When Blocking' (unchecked). The 'Browser Protection' section includes a description of the feature and a single checkbox 'Enable Browser Protection' which is checked.

Customization	Authentication	Define Categories	YouTube Schools	SIP Options	Advanced
Options <input type="checkbox"/> Block URLs with Cross-Site Scripting (XSS) <input type="checkbox"/> Block Remote Logins Between Private IP Addresses <input checked="" type="checkbox"/> Monitor and Process VLAN Traffic <input type="checkbox"/> Copy Original VLAN Tag When Blocking					
Browser Protection NetSpective Browser Protection checks for web sites attempting to interfere with normal computer functions or mislead users into providing personal information to unauthorized parties. <input checked="" type="checkbox"/> Enable Browser Protection					

Block URLs with Cross Site Scripting (XSS)

Enable this option to block accesses to URLs containing JavaScript meta-characters.

Block Remote Logins between Private IP addresses (Passive Only)

By default, this is unchecked and Remote Logins between IANA Private Network Ranges (such as 192.168.*.*) will not be blocked when the Group Policy is set to block. Enable this check box to make a Group Policy block applies to IANA Private Network Ranges.

Filter VLAN Traffic (Passive Only)

Check this option to make NetSpective filter traffic encapsulated inside Ethernet VLAN packets.

Copy Original VLAN Tag When Blocking (Passive Only)

By default, this is unchecked and NetSpective will not put VLAN tags on its block packets when blocking VLAN traffic. If your switch won't route untagged packets, check this option. This option only applies when "Filter VLAN Traffic" is enabled. The NetSpective admin interface must be on VLAN0. The default/native VLAN on Cisco switches is VLAN 1.

Browser Protection

NetSpective Browser Protection checks for web sites attempting to interfere with normal computer functions or mislead users into providing personal information to unauthorized parties. If you enable this option, NetSpective will enable the 'Malware' and 'Phishing' categories and configure all group policies to block these categories by default. The Browser Protection feature indicates that a site has a high probability of being an attack site. The absence of a warning does not guarantee that a site is trustworthy.

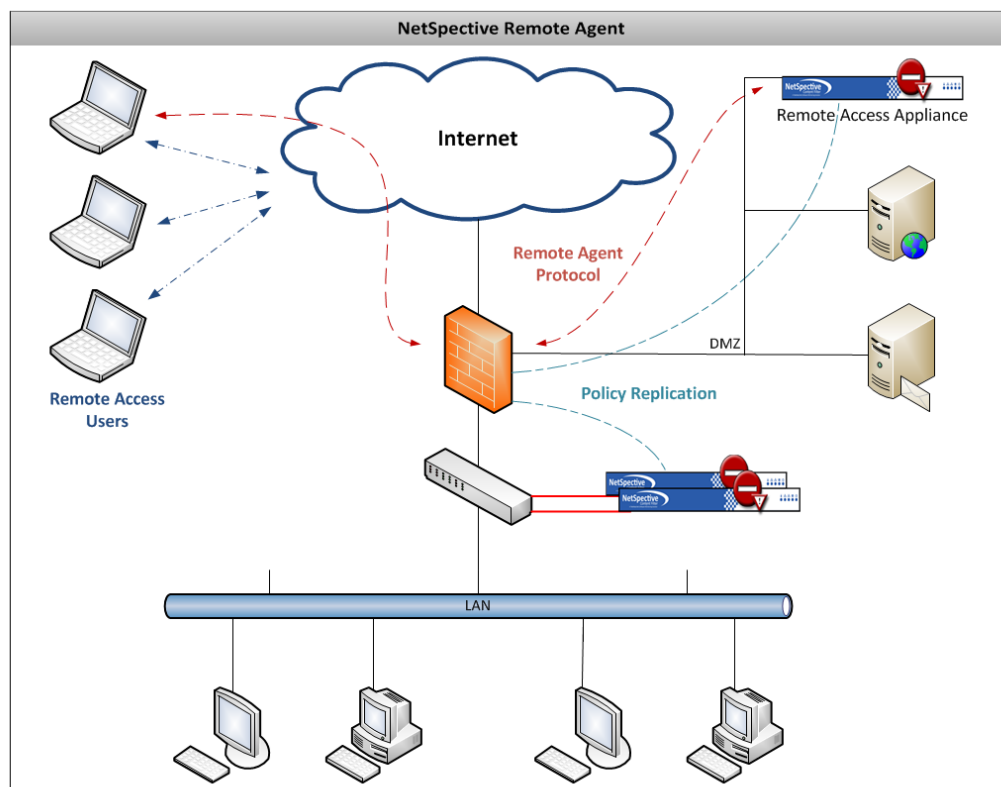
Skype Blocking Behavior (Passive Only)

If your NetSpective device is licensed for SkypeOut, you may block all of Skype, which includes Peer-to-Peer (PC-to-PC) and SkypeOut (PC to telephone). Or, you may choose to block only SkypeOut. When choosing to block only SkypeOut, you may set a percentage of the SkypeOut traffic that will be blocked.

Remote Agent

The Remote Agent is an enhancement of the NetSpective logon agent technology to extend your Internet Usage Policy to remote users that can be either on the network or off. This is the technology used in our SaaS offering, but is also offered in our Passive model. The agent installs as a service and driver on remote workstations where it monitors or blocks internet usage. It also maintains an active communication link with the NetSpective remote access appliance via the Remote Agent Protocol. The Remote Agent Protocol is used for policy decisions, logging, and configuration and software updates. The NetSpective Remote Agent is currently supported on Windows 7 and 8 operating systems and latest versions of Mac OS.

Based on security practices and the volume of remote computers being filtered, consideration should be given to placing a NetSpective appliance in the DMZ.



Remote Agent Connection Settings

Before the Remote Agent can be used, it must know how to connect to your NetSpective Appliances. You should specify all NetSpective appliances on your network with both public and private addresses. Depending on the location of the remote access user, the network, and the load on the appliances, the Remote Agent client will choose to communicate with the appropriate NetSpective appliance. You may have to set your firewall to forward UDP and TCP traffic to NetSpective's listening port of 3001, as well as your firewall's address in the address list within NetSpective. The order of the servers in the list makes no difference. When the Remote Agent client tries to connect, it broadcasts to all servers at once and connects to the first one that responds.

Connection Settings	Connection Failures	Client Settings	Mobile Browser						
<p>To ensure that your remote clients behave correctly on all of your networks, enter the internal and external addresses for all of your NetSpective devices. The default port is 3001, but it may be different for external addresses if you use port mapping.</p> <p>Address List</p> <table border="1"><thead><tr><th><input type="checkbox"/></th><th>Address</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>192.168.5.80:3001</td></tr><tr><td><input type="checkbox"/></td><td>50.76.227.243:3001</td></tr></tbody></table> <p><input type="button" value="Delete"/> <input type="button" value="Add"/></p>				<input type="checkbox"/>	Address	<input type="checkbox"/>	192.168.5.80:3001	<input type="checkbox"/>	50.76.227.243:3001
<input type="checkbox"/>	Address								
<input type="checkbox"/>	192.168.5.80:3001								
<input type="checkbox"/>	50.76.227.243:3001								

Remote Agent > Connection Settings

Remote Agent Connection Failure

Occasionally the Remote Agent client might not have access to the NetSpective appliance and will act in an offline mode. This could happen when initially accessing the internet from a hotel or wireless hotspot. You will need to set the behavior of the client when it is offline. You have the option to permit all access to the internet or deny all accesses with the exception of notable websites that you specify. You also have the option to enable a user initiated grace period when you choose to deny all, for access situations where the user must hit an initial web page to activate their internet connection. When offline, the Remote Agent will log the user's activity and will report this activity to the NetSpective appliance when it returns online.

Connection Settings	Connection Failures	Client Settings	Mobile Browser										
<p>These settings affect the behavior of your remote clients when they fail to connect to a NetSpective server. You may choose to allow the clients to access the Internet without restrictions, or you may choose to block all access except for a specific set of hosts.</p> <p>Block or Allow?</p> <p><input type="checkbox"/> When the connection fails, block everything but whitelisted hosts.</p> <p><input type="checkbox"/> Allow user initiated grace period of <input type="text" value="1"/> minute(s) every <input type="text" value="5"/> minutes.</p> <p>Whitelist</p> <table border="1"><thead><tr><th><input type="checkbox"/></th><th>Host or IP</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>tm-mail.telemate.net</td></tr><tr><td><input type="checkbox"/></td><td>google.com</td></tr><tr><td><input type="checkbox"/></td><td>test.com</td></tr><tr><td><input type="checkbox"/></td><td>zzz.com</td></tr></tbody></table> <p><input type="button" value="Delete"/> <input type="button" value="Add"/></p>				<input type="checkbox"/>	Host or IP	<input type="checkbox"/>	tm-mail.telemate.net	<input type="checkbox"/>	google.com	<input type="checkbox"/>	test.com	<input type="checkbox"/>	zzz.com
<input type="checkbox"/>	Host or IP												
<input type="checkbox"/>	tm-mail.telemate.net												
<input type="checkbox"/>	google.com												
<input type="checkbox"/>	test.com												
<input type="checkbox"/>	zzz.com												

Remote Agent > Connection Failure

Remote Agent Client Settings

After configuring the connection options, you are ready to install the client and apply the initial configuration file. You can download the Remote Agent utility that will be installed on remote workstations or laptops from the Utility section of the NetSpective interface. All configuration changes are pushed to the clients via the Remote Access Protocol. Once the Remote Agent is installed, you must download the encrypted configuration file from the appliance and install it on the remote workstations.

If any of your users have administrative access to their workstations, you may also want to require an uninstall password to make it harder to remove the Remote Agent software.

Connection Settings	Connection Failures	Client Settings	Mobile Browser
<p>You may enable or disable automatic upgrades of the Remote Agent client software. If you are using a disk image freezing technology, you should turn off automatic upgrades. You may also set an uninstallation password so users with local Administrator privileges can not uninstall the agent.</p>			
Settings			
<input type="checkbox"/> Automatically Send Software Upgrades to Clients			
<input checked="" type="checkbox"/> Require Uninstallation Password			
Password: <input type="password"/>			
Downloads			
To download the Remote Agent installation package and configuration file, go to the Utilities download page.			

Remote Agent > Client Settings

NetSpective Mobile Browser

The NetSpective Mobile Browser app for iPads is available for free in the [Apple App Store](#). The Mobile Browser app allows you to monitor and filter internet content on an iPad device no matter where the user takes it. We recommend that you use the Apple Configurator to install and configure the Mobile Browser, as well as to lock down your iPad devices so that your users cannot run Safari, remove the Mobile Browser app, or bypass it by installing another web browser.

Mobile Browser Settings

NetSpective allows you to choose an authentication method for the Mobile Browser to use for identifying the user. You may choose to either use the device name (which can be specified in the Apple Configurator) or to require the user to enter an LDAP login and password. If you choose LDAP authentication, the login name and password entered by the user will be forwarded to your NetSpective device via secure HTTP, which NetSpective will then validate using the LDAP sources you have configured. If you choose LDAP authentication, we recommend that you change the 'LDAP Logon Prompt', which is what users will see when they are asked to log on.

It is important to set the 'Logon Agent Inactivity' timeout appropriately. When the Mobile Browser app is not active on an iPad, the operating system will not allow the mobile browser to keep a link open to NetSpective due to the impact on battery life. When a filtered iPad is brought into school (or the office) in the morning and grabs a new IP address on your wireless network, NetSpective will not know which user has logged on until the Mobile Browser is opened. The inactivity timeout helps keep users from having to re-open the Mobile Browser multiple times per day to re-establish the link. If your iPads are configured to check email every 15 minutes, we recommend that you set this value higher, such as 20 minutes.

Some organizations need the Mobile Browser to treat certain file types as attachments (e.g. pdf, epub, doc). In the Attachment File Types section, you can specify filename extensions or MIME types that you want the mobile browser to open as attachments. By default, the Mobile Browser has its own settings to allow your users to add up to 5 of their own file types (which your users can find in the iPad Settings app). If you do not wish to allow users to specify their own, you can disable this feature in the browser by unchecking the 'Allow' checkbox in that section.





Connection Settings	Connection Failures	Client Settings	Mobile Browser			
<p>These settings only affect the iPad Mobile Browser app. We recommend that you test these settings in conjunction with the Apple Configurator to install and configure the Mobile Browser, and to lock down your iPad devices so that it can not be uninstalled or circumvented.</p>						
Authentication Settings						
User ID scheme: LDAP Authentication						
LDAP Logon Prompt: TeleMate Authentication						
Logon Agent Inactivity: 20 Minute(s)						
Attachment File Types						
Specify filename extensions (e.g. pdf, doc, rtf) or MIME types (e.g. application/pdf, video/avi) for the file types you want the mobile browser to open as attachments.						
<input checked="" type="checkbox"/> Allow each iPad to define their own additional attachment file types						
<table border="1"><thead><tr><th>Attachment File Type</th></tr></thead><tbody><tr><td><input type="checkbox"/> .pdf</td></tr><tr><td><input type="checkbox"/> .doc</td></tr></tbody></table>				Attachment File Type	<input type="checkbox"/> .pdf	<input type="checkbox"/> .doc
Attachment File Type						
<input type="checkbox"/> .pdf						
<input type="checkbox"/> .doc						
Delete Add						

Remote Agent > Mobile Browser

Replication

Replication makes it easier to manage multiple NetSpective appliances. It provides a method to automatically synchronize settings between a parent device and other devices configured as child nodes. You may choose to replicate almost all settings, in the case of a fail over or load balanced cluster, or you may allow certain groups of settings to be overridden by a child node, in the case of branch offices. Settings that are always synchronized by replication include users, groups, managers, overrides, and policies.

Replication [admin](#) | [register](#) | [help](#) | [logout](#)

   Search: 

Group: System

Replication automatically pushes user, group, and policy settings from one parent NetSpective to many child devices.

Replication Role: Parent

<input type="checkbox"/>	Node Name	Appliance ID	Filtering Mode	Status
<input type="checkbox"/>	HotSpare	N/A	Passive	Sync Pending


Delete

Replication Roles

There are three replication roles NetSpective can have. They are Stand-Alone, Parent and Child. Devices that are not part of a replication group should have a role of "Stand-Alone" and are managed individually. Otherwise, devices that are part of a replication group should have a role of "Parent" or "Child". Users, groups, policies, and other configuration settings are managed centrally on a parent device and are automatically pushed to all of its child devices. A child device should have only one parent device. A NetSpective device in Child mode does not let you edit any settings that are replicated to it by its parent. These replicated settings are hidden from the administration web interface.

To change a device's replication role, select a role from the drop down list. This will immediately change the role for the device. The replication role can only be changed if there are no child nodes defined.

Creating or Updating Replication Nodes

The Replication page shows a listing of all child nodes if the NetSpective is set to the Parent role. A red status indicates an error occurred while synchronizing that node. Hover the mouse pointer over the warning icon () to see a detailed error message.

Replication Node

☒ Enable

Node Name:

Filtering Mode:

Passive

IP or Hostname:

Password:

Public Policy:

Public

Replication Options

☐ Optional Replication

☒ Authentication

☒ Automatic Backup

☒ Logging

☒ NetAuditor

☒ NTP

OK

Cancel

To add a replication node, click the 'Add' button in the upper left corner of the control bar. To view or change properties of a node, click the name of the node you would like to edit.

Replication Settings	
Node Name	A name to identify the child node.
Filtering Mode	The mode for which the child device is licensed. This may be "Proxy" or "Passive".
IP or Hostname	The IP or hostname of the child node. A hostname requires NetSpective to be configured to use a valid DNS server.
Password	The "admin" account password for the child node.
Public Policy	The policy that will be used as the Public policy on the child node.
Options	A list of settings that will be replicated with the child node. Some settings are required for all nodes, some are never replicated, and some may be individually enabled or disabled. By default, all settings are selected for replication.

When a node is added, it will be set to Enabled by default. If you do not want the node to receive updates, click the node and uncheck the Enabled checkbox. After a node has been added, a status message will be available to help troubleshoot an error if one should occur. A parent device needs to open a connection to its child nodes on TCP port 80 to synchronize settings. Please ensure that your firewalls allow this if your devices are located in different networks.

Deleting Replication Nodes

To delete replication nodes, select the checkbox next to each node's name. To delete all nodes displayed on the current page, select the checkbox in the upper left-hand portion of the table. Click the Delete button to delete the selected nodes. If all nodes on a page are selected, the option to select the nodes on every page will become available.

Utilities

NetSpectre comes with certain utilities you may download to assist in network integration and monitoring. Depending on your license, available utilities and settings include Logon Agent, Remote Agent, SNMP MIB and NetAuditor.

The version numbers you see below are that of the initial IPv6 build's release. Always make sure to update Logon Agents and Remote Agents to their newest version.

Agents

Install Logon Agent on a Windows Domain Controller or Citrix Terminal Server to easily manage and filter logged on users. Install Remote Agent on laptops so users can be filtered while outside your network.

Name	Version	File
Windows / Citrix Terminal Server Agent	3.0.4	TerminalServerAgent.exe
Logon Agent for Windows Domain Controllers	3.0.8	LogonAgent.zip
Logon Agent (Mac OS 10.5 - 10.6)	2.1-11	LogonAgent-2.1-11.dmg
Logon Agent (Mac OS 10.7 - 10.9)	2.3-9	LogonAgent-2.3-9.dmg
Remote Agent Client (Windows)	1.4.6	RemoteAgent.msi
Remote Agent Client (Mac OS 10.5 - 10.6)	1.1-95	RemoteAgent-1.1-95.dmg
Remote Agent Client (Mac OS 10.7 - 10.9)	2.1-6	RemoteAgent-2.1-6.dmg
Remote Agent Configuration File	N/A	Configuration

SNMP MIB

Download and install the NetSpectre SNMP MIB on to a computer you use for SNMP monitoring. This MIB provides NetSpectre specific OIDs.

Name	Version	File
SNMP MIB	2.0	NETSPECTIVE-MIB.txt

NetAuditor

NetAuditor delivers in-depth information on Web traffic patterns, content classification, non-essential bandwidth usage and more. It provides a comprehensive summary as well as a detailed audit of Web, FTP, peer-to-peer, instant messaging, and other types of Internet traffic on your network.

Name	File
NetAuditor 3	NetAuditor3Setup-RC.exe

Agents

The Logon Agent is installed on a Windows Domain Controller or Citrix Terminal Server to easily manage and filter logged on users. The Remote Agent is installed on laptops so users can be filtered while outside your network.

SNMP MIB

NetSpectre may be monitored via SNMP so that you may keep track of its health and filtering activity. This MIB provides NetSpectre specific OIDs.




NetAuditor

NetAuditor is an application that delivers in-depth information on Web traffic patterns, content classification, non-essential bandwidth usage and more. It provides a comprehensive summary as well as a detailed audit of Web, FTP, peer-to-peer, instant messaging, and other types of Internet traffic on your network. The link provided will download the NetAuditor setup executable from the www.telemate.net website. NetAuditor 3 also supports IPv6. This new version is required for IPv6 archival reporting. If you are unsure of what version you should be running, install the latest version downloaded from the NetSpective appliance or contact our support department.

Backup & Restore

The backup and restore page provides the ability to backup or restore the settings for your NetSpective. With a backup, all settings will be saved except the system administrator password and networking configuration.

Backup & Restore

 Search:

Backup and Restore saves all settings except the system administrator password and networking configuration. Automatic backups can be transferred via FTP to a server of your choice. When enabled, automatic backups occur daily at 10:00 pm.

Automatic Daily Backups

☒ Enable Automatic Daily Backups

Automatic Backup Status

2009-05-18 10:00:01 PM Backing up settings...
2009-05-18 10:00:01 PM Transferring autobackup.weega8e4.3.5-82.p7.2009-05-18-220001.fc to 19
2009-05-18 10:00:03 PM Could not read reply from control connection: Connection reset by pee
2009-05-18 10:00:03 PM Operation Failed: FTP transfer failed

FTP Settings

IP or Hostname:

User Name:

Password:

Directory:

Automatic Daily Backups

When automatic backups are enabled, NetSpective transfers the backup file to a specified FTP server. Files are transferred daily at 10:00 pm. The settings for configuring NetSpective for FTP transfers are:

Automatic Daily Backup to FTP Requirements	
IP or Hostname	IP address or host name of the FTP server.
User Name	User name required to access the FTP server.
Password	Password required for accessing the FTP server.
Directory	Directory on the FTP server you wish to use. Example: <code>"/public/backups"</code> (Do not enter the quotation marks). If you leave this field empty, logs will be transferred to the users default directory.

Backup Settings (Download)

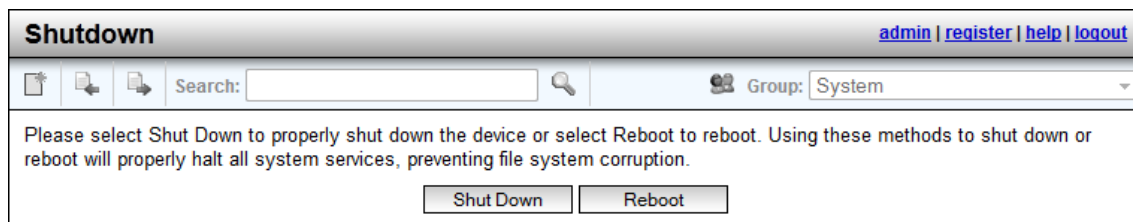
To download a backup of the current device settings, click the "Backup Settings" icon on the toolbar near the top of the page. When your browser's download dialog appears, select where you would like to save the backup file.

Restore Settings

To restore settings from a backup file, click the "Restore Settings" icon on the toolbar near the top of the page. Select the backup file you wish to use. Then click the "OK" button.

Shutdown & Reboot

From the System Control menu, you can properly shut down or reboot your NetSpective. We recommend that you shut down before physically moving the device. Using these methods to shut down or reboot will properly halt all system services, preventing file system corruption.



Shutdown [admin](#) | [register](#) | [help](#) | [logout](#)

Search:

Group:

Please select Shut Down to properly shut down the device or select Reboot to reboot. Using these methods to shut down or reboot will properly halt all system services, preventing file system corruption.

Click Shut Down or Reboot, to shut down or reboot the system. To deactivate and reactivate your system, please press the power switch on the NetSpective chassis. After a shutdown, please wait 1 minute before pressing the power switch.