NetSpective WebFilter™

Setup Guide

Network Monitoring and Security Products by TeleMate.Net Software.

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
6.18.2013 Version 4.0

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

www.TeleMate.Net

CONTENTS

CONTACTING NETSPECTIVE SUPPORT

Thank you for choosing NetSpective as your Internet Content Filtering Solution. If you have any questions or need technical assistance with your NetSpective setup, please contact our helpdesk at 678-589-7120 or by email at netspectivesupport@telemate.net.

GETTING STARTED

In order to perform the initial configuration of NetSpective, you will need:

- A monitor and keyboard.
- Licensing data from TeleMate.Net Software (license key, licensing server, and licensing password). This information must be obtained by contacting registration services at 678-589-7140 or by email at registration@telemate.net.
- An Internet connection, allowing FTP downloads from public servers.

> NetSpective is a rack-mounted appliance. You will need to perform the initial steps of your configuration in a place where you will have easy access to the back of the device. Therefore, we suggest that you move the device to a rack only after performing the initial configuration steps. Once you successfully perform the steps listed in this manual, you are ready to access the Web-based administrative interface over your network.

NETWORK DEPLOYMENT STRATEGIES

There are two possible network deployment strategies: Passive (also referred to as side-scan) and Proxy configuration. Each deployment strategy is a licensable option.

Passive Configuration

The easiest method is to use a switch with mirroring or SPAN capabilities. This feature can be found in Cisco Catalyst series switches, as well as most economical and readily available switches. If you would like to use a switch along with your NetSpective, you must configure the switch so that traffic bound for your gateway/firewall or proxy can be monitored and intercepted by NetSpective.

Using a switch that automatically routes Internet traffic to the gateway/firewall or proxy server from the internal network, you will need to “mirror” the port that is being used for the internet traffic. The administrative network interface labeled “LAN A - Administrative NIC” should be connected to an available switch port and the mirrored port used for monitoring should be connected to the NetSpective interface labeled “LAN B - Monitoring NIC” as shown in Figure 1.

> Connecting the Monitoring NIC to the network is not required for licensing your NetSpective appliance. However, you will need to connect the Administrative NIC to your network for this purpose. You will not be able to access the Web-based administration interface without first licensing NetSpective.

Proxy Configuration

To properly control internet traffic in a proxy configuration both “LAN A - Administrative / Internal NIC” and “LAN B - External NIC” should be plugged into the upstream switch inside the firewall as shown in Figure 2.

Figure 1: Passive Configuration

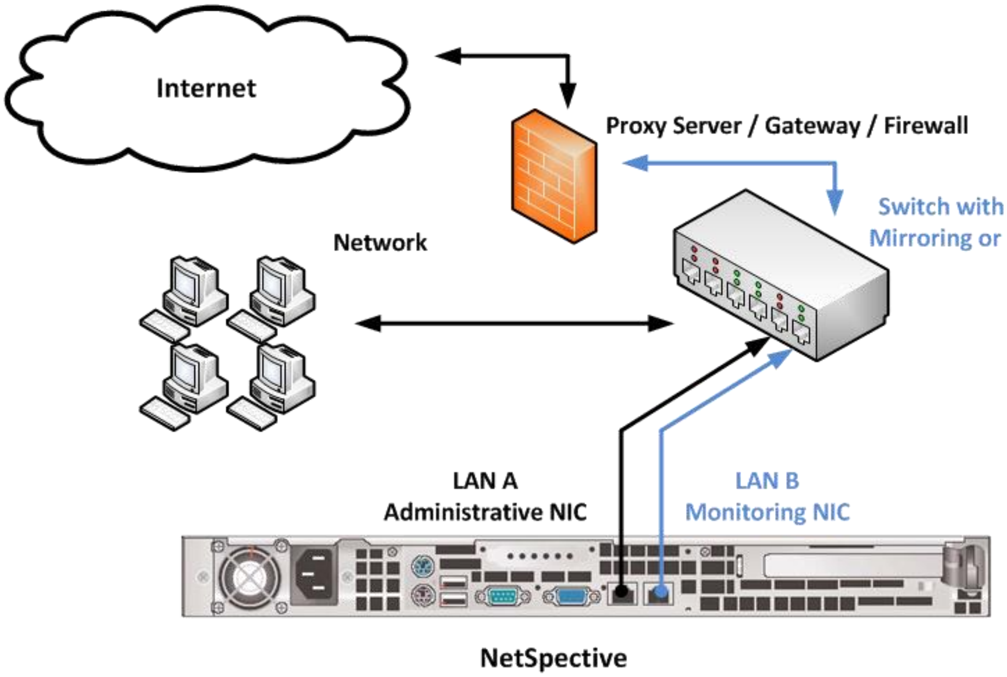


Figure 2: Proxy Configuration

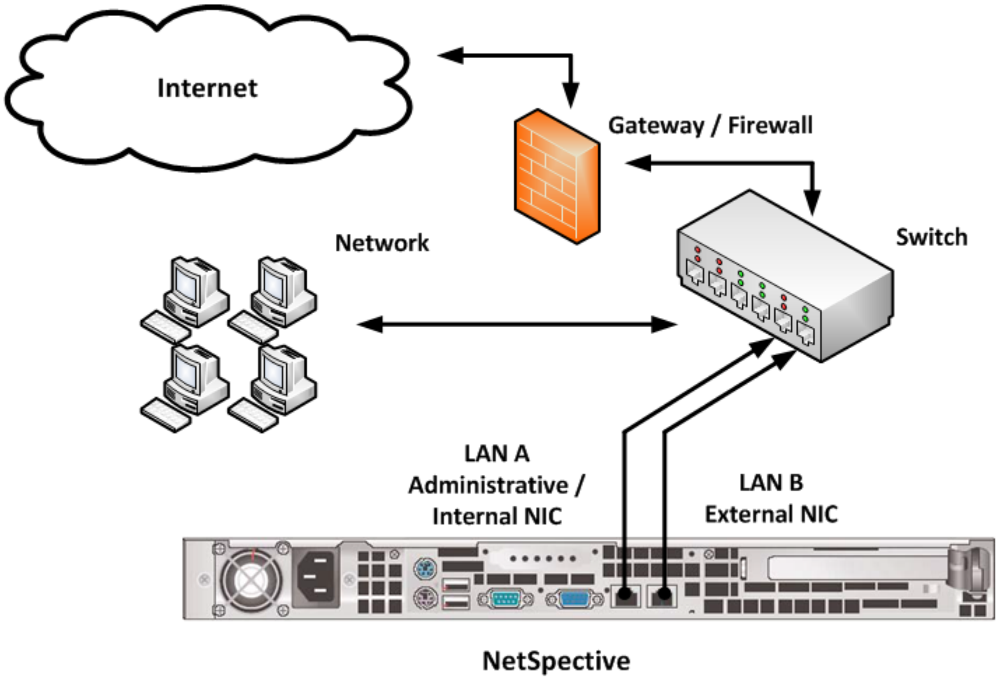
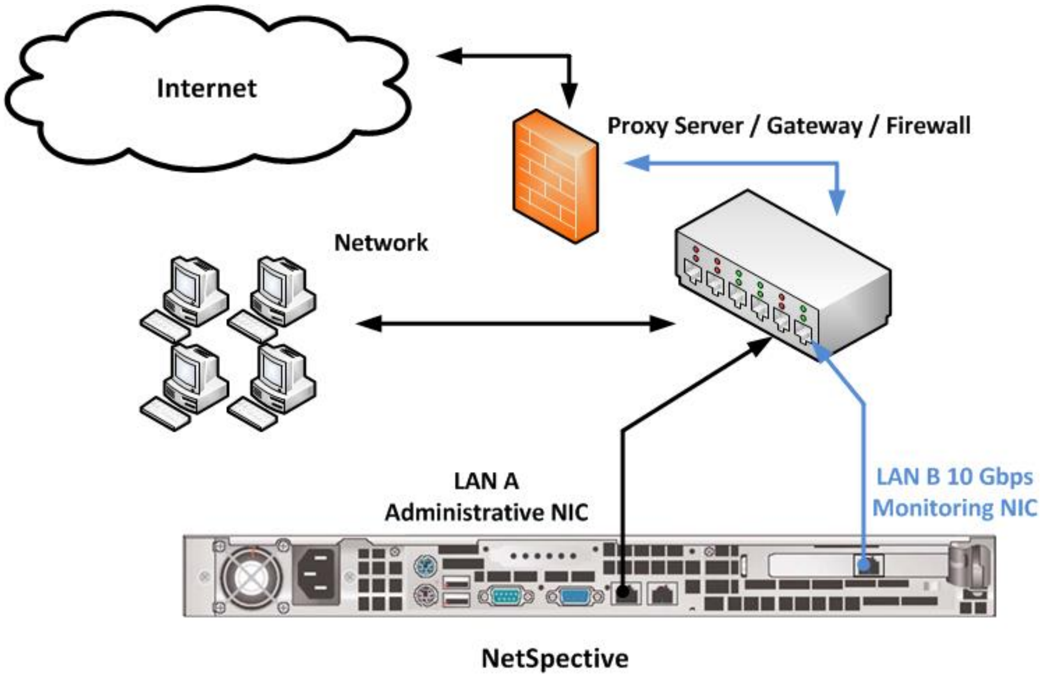


Figure 3: 10 Gbps Passive Configuration



INSTALLING THE APPLIANCE HARDWARE IN YOUR NETWORK

1. Unpack NetSpective and connect the monitor to the video graphics adapter on the back plate of NetSpective.
2. Connect the keyboard to the interface on the back plate.
3. Connect the power cables of both NetSpective and the monitor, then power them up. The power switch is located on the front of the device. Additional information can be found in the **NetSpective Hardware Installation Guide**.

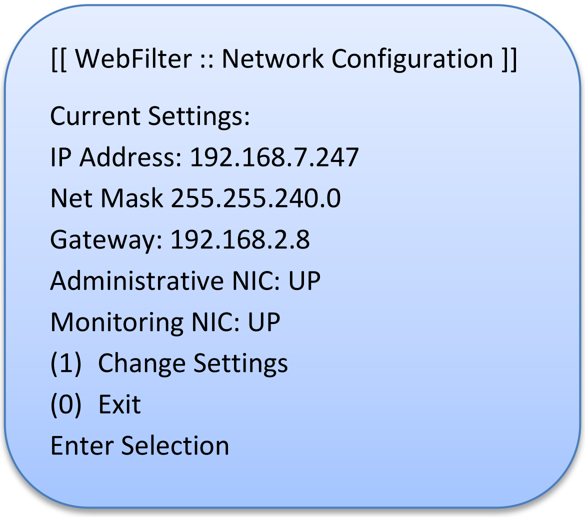
After NetSpective boots up, a login prompt will appear. Type '**admin**' and press enter. When the device prompts you for a password, enter '**webfilter**'. You will be able to change the password later from the Web-based administrative interface. When the login process is complete, you will see a text-based administrative console menu:

```
[[ WebFilter :: Main Menu ]]

    (1)  Configure Networking
    (2)  License Device
    (3)  Network Diagnostics
    (4)  Reset to Factory Default Settings
    (5)  Reboot / Shutdown
    (0)  Exit
```

Network Configuration Settings

From the Main menu, type '**1**' and press enter to access the **Configure Networking** menu. Your current (default) network settings are displayed (see figure). Note that your network card link status is displayed for both the Monitoring NIC and the Administrative NIC.



```
[[ WebFilter :: Network Configuration ]]

Current Settings:
IP Address: 192.168.7.247
Net Mask 255.255.240.0
Gateway: 192.168.2.8
Administrative NIC: UP
Monitoring NIC: UP
(1)  Change Settings
(0)  Exit
Enter Selection
```

Type '**1**' and press enter to change the settings:

1. Type in a new IP address for NetSpective; press enter to continue.
2. Type in the appropriate netmask of NetSpective; press enter to continue.
3. Type in the IP address of the network gateway; press enter to continue.
4. Finally, type 'Y' and press enter to accept the changes. Press enter to return to the menu. Review your settings and reconfigure if necessary. If the settings are acceptable, type '0' and press enter to return to the Main menu.
5. **Installing 10 Gbps Network Configuration:** The network configuration page will list two monitoring NICs, one for the onboard gigabit NIC and one for the 10 Gbps NIC. Simply select option 4 'Swap Monitoring NIC' to swap the active NIC to the 10 Gbps NIC.

After configuring your network settings, please be sure to use the Shutdown option before you move the device or power off (option #5 from the Main Menu, described in this document)

> Please confirm that the Administrative NIC is connected to your network and is in the "up" link status mode.

Licensing the Device

To complete the licensing process you should have received the following licensing data from TeleMate.Net. If you do not have this information, please contact us at 678-589-7140 or by email at registration@telemate.net for assistance.

- NetSpective Licensing key and password
- IP address of a NetSpective Licensing Server

1. From the Main menu type ‘**2**’ and press enter to access the **Licensing** Menu. Once there, type 1 and press enter to license your NetSpective.
2. Type in the name or IP address of the licensing server. Press enter to continue.
3. Type in the license key (20 characters plus dashes) and press enter. Please be sure to type all characters exactly as provided.
4. Type in the licensing password and press enter to continue.

NetSpective will now connect to the licensing server to activate your license. This will be followed by the startup of additional services on the system. Once this process is complete, press enter to return to the Licensing menu. Review your licensing information (licensing key, number of users, license level, and subscription start and end dates). Type ‘0’ and press enter to return to the Main menu.

Network Diagnostics

If NetSpective licensing fails, please check your network settings (Main menu, 2), or test the connection to the licensing server using the Network Diagnostic menu. If the problem persists, please contact NetSpective Support at 678-589-7120.

From the Main menu, type ‘**3**’ and press enter to access the Network Diagnostics menu. This option should be used to diagnose any network connectivity issues. For further assistance, contact your system administrator. You may type ‘0’ and press enter to return to the Main menu at any time.

1. To ping a host, type ‘1’ and press enter. Type in the IP address of the host to ping and press enter. You should see at least 3 packets being sent. If ping fails, check your connections, firewall rules, or any NetSpective setting, which could prevent a successful ping. Once ping finishes, you will be taken to the Main menu.

2. To display the route to a host via traceroute, type ‘2’ and press enter. Type in the IP address of the host to trace. If traceroute fails, check your connections, firewall rules, or any NetSpective setting, which could prevent a successful connection. If traceroute succeeds and you are still having problems, make sure to check your firewall to ensure you have FTP access to public servers. Once traceroute finishes, you will return to the Main menu.

Reset to Factory Defaults

On the Main menu, type ‘**4**’ and press enter to access the Reset to Factory Default Settings menu. Type ‘1’ and press enter to reset NetSpective to its original configuration. A prompt will ask for your confirmation before proceeding. To continue with the reset, type ‘Y’ and press enter.

> Important Note: If you reset the device, you will lose all of your configuration settings, including the blocking policies configured via the web browser interface.

Reboot/Shutdown

From the Main menu, type ‘**5**’ and press enter to access the Reboot/Shutdown option.

1. To reboot, type ‘1’ and press enter. At the confirmation prompt, type ‘Y’ and press enter to reboot.
2. To shutdown, type ‘2’ and press enter. At the confirmation prompt, type ‘Y’ and press enter to shut down your NetSpective.

WEB-BASED ADMINISTRATION

Now that you’ve successfully configured and licensed your NetSpective appliance, you can access the Web-based Administration interface. From any Web browser on your network, type in the IP address you assigned from the Network Configuration step in your Web browser’s Address bar. For example, if you assigned 192.168.2.247 as the IP address for NetSpective, you would type http://192.168.2.247 in your Web browser’s address bar. A dialog box will appear prompting you to enter your user name and password. The default user name is ‘**admin**’ and the default password is ‘**webfilter**’. You can change the default administrative password from the ‘Managers’ tab in the NetSpective Web interface.

From any of the areas you see in the product, clicking on the ‘**Help**’ or ‘**?**’ icon will take you to the help section. When a new tab opens, you will see the help section that refers to the area of the product you are in. The help section will give you a description of each section of the product. At the top of every help page you will see links to our Authentication Guide and User Guide.

- The **Authentication Guide** outlines all our methods of determining username and IP address association. This includes ways to authenticate BYOD, 1 to 1, and off network users. Once you have your LDAP sources, Groups, and Group Policies configured, this will be the most helpful guide for deploying your Logon Agents and configuring our Mobile Portals.
- The **User Guide** contains an overview of all the sections of our product. If you are looking for more information on a particular section, or want to see some examples of how things are set up, or are just interested in a description on what a particular area of the product is for, refer to this guide.

> Note: Our **Public Policy** is a catch-all policy. Any unauthenticated users will fall under this policy and be filtered. You may want to jump to the **Group Policy** section of this guide if you have placed the appliance in your network and do not want users surfing unwanted content.

Update the NetSpective Software Version

The first thing we want to do is make sure the appliance is up to date and can communicate with our online service.

1. Navigate to the **Device Information** heading on the left side and click on the link next to **Updates**. This link may read **Current** , **Available** , or **Error**.

The Updates section is where we will apply system updates, manage category update intervals, and configure Micro Update intervals. From here the Update Status window will show you the most recently downloaded and applied updates, as well as any system updates that have been downloaded and are awaiting installation.

2. Click the **Get Updates** button to check for system updates. This will also download any License, Browser Protection, or Category Updates that are waiting for your appliance. This section also shows the IP address of the online service that sends out updates. If you are having trouble connecting to the updates server, make sure your firewall is allowing the NetSpective to connect to that IP address. For a list of all the port numbers and IP addresses that NetSpective uses, see the User Guide.

3. If the Update Status window shows a new version of NetSpective is ready to be installed, click the **Install Update** button. The appliance will restart during this process.

Backup and Restore from a previous NetSpective installation

These settings can be found under the **System Control** heading by clicking on **Backup & Restore**. If you are upgrading from a previous NetSpective deployment, you may already be utilizing the Automatic Daily Backups feature.

In the upper left corner you can find the **Backup Settings (Download)** and **Restore Settings (Upload)** buttons. Simply use the Backup Settings to download the configuration on your previous appliance. Make certain your new appliance has all available updates applied to it before using the Restore Settings.

Replication Roles

NetSpective can be configured with multiple appliances as hot spares for fail-over redundancy. You can replicate your configuration settings from the **System Control** heading under **Replication.** Here you can define the current appliance as a 'Stand-Alone', 'Parent', or 'Child'. From your Parent appliance, you can then add child devices from the 'New' button in the upper left corner.

When adding a Child appliance to your replication, specify the Filtering Mode (Passive or Proxy), the IP address of the child appliance, the password of the child appliance's Admin account, and the Public Policy on the parent you wish to use as the child's public policy. You can optionally specify which settings you wish to replicate to the child appliance.

A word on how NetSpective applies filtering policy to users

NetSpective filtering policy is configured in the **Group Policy** section. These Group Policies are then tied to **Groups**, allowing you to set different policies for each group of users. Groups are then populated with users, typically through LDAP integration or manually through the **User** section. The easiest and quickest way to bring in all of your users is through your **LDAP Sources**.

Configure LDAP Integration

NetSpective supports integration with Active Directory, eDirectory, and Open Directory. You may have any number of domain controllers configured in NetSpective as well as any combination you wish. NetSpective does not require Administrator privileges, only the ability to read your Group/OU trees.

1. Navigate to the **System Control** heading and click on **Device Settings > LDAP Sources**.

2. Click the **Add** button to add a new LDAP source. Be sure to fill out all the fields properly to ensure NetSpective can read your entire directory tree structure. Specifying the NetBIOS Domain will ensure that all your users will be pulled in with the same domain name. If you are unsure of the format that a field requires, hover over the ❓ icon or click on the help '**?**' section for more information. If you wish to use a hostname instead of the IP address of your domain controller, you will need to specify a DNS server in the **Device Settings > Network** section.

   NetSpective will require an LDAP Source for each of your domain controllers to stay up to date and accurate. This includes any Global Catalog Servers you may have.

3. When you are finished, click the **OK** button. NetSpective will begin to pool information from your domain controller. When NetSpective is done with the synchronization, the Status field should read OK. If you refresh the page and do not see OK, or if the Status reads an error, check to make sure all of your settings are correct.

   NetSpective automatically syncs with all your LDAP sources periodically. This setting can be changed in the **Device Settings > Advanced** section, or you can manually sync your sources with the **Sync** button.

For more information on setting up your LDAP sources, refer to the Authentication Guide.

Create and Populate Groups with LDAP Users

Here we will be creating groups to apply policy settings to, and populate them with users. Groups are read in alphabetical order, so users in multiple groups will have policy settings applied to the first group they are seen in.

There are two groups in the system by default. The **Exempt** group is exempt from all filtering policies and NetSpective will ignore all traffic from this group. The **Public** group is for all unknown or unassigned users. By default, all users fall into this group until they authenticate into the appliance. Since this group contains unauthenticated users, we recommend configuring the public group to be the most restrictive policy.

1. Navigate to the **Management** heading and click on **Groups**. Click the **Add** button in the upper left corner. This will open the Group Properties window. Here we can begin configuring a group by giving it a name in the first field called Group.

If you do not wish to populate a group with LDAP users, then a name is all that is required and you can click the OK button to finish. You can then create static IP address users and place them into this group from the **Users** section.

2. Select the **LDAP Source** you wish to pull groups of users from. The drop down menu will list all of the sources you have created in the previous section. This will populate the **LDAP Object** section, where you can then select the group or organizational unit you wish to associate this group with.

   Optionally you can specify the LDAP Priority. With this feature you can force a group tied to your LDAP to appear higher or lower on the list instead of alphabetically. If you have a user in multiple groups, this can be used to force their policy to be tied to a specific group.

3. When you are finished, click the OK button at the bottom. If your LDAP group contains users, you should see the number of Assigned Users populate on the right.

This is all that is needed to create groups. However, because we apply many settings on a group by group basis, further configuration can be done when clicking on a group name. Here you can also enable features such as; Alternate Days Policy, YouTube for Schools, Block Page Overrides, Request Category Change, Policy Reminder, and Abuse Detection. Refer to the Help section or User Guide for more information on each feature.

Configure Group Policy

This section is where you can set which categories will be blocked and logged for a group. You can see which group you are configuring in the upper right corner. We recommend configuring the **Public** group first to lock down sensitive material for all unauthenticated users. If you have multiple groups to configure, it can become time consuming to edit each one manually. In the upper left hand corner you can find the **Save-To** feature. Note the group you are currently configuring before clicking the save-to button. A window will appear with a list of your categories on the left and your groups on the right. You can use this to copy the category settings of your current group to other groups, saving you from having to configure each group manually or make changes to each group individually.

The **Group Policy** page lists categories and protocols on the left, with a time based grid on the right. Categories can be set to **Block** (Content will be blocked and logged), **Log** (Content will be allowed, but logged), or **Ignore** (Content will be allowed through and will not be logged). These settings can be applied hourly in the grid, indicated by the time at the top heading, or for the entire day by clicking on the ◷ clock icons. Italicized categories contain sub categories, which can be viewed by clicking on the italicized category name. A category may have sub categories where some may be set to block and others may be set to log. In this case, the main category will appear as orange in the grid on the right.

The **Safe Search** feature can be found on the bottom left corner of the screen. Clicking the padlock icon will set the Web Search category to **Block** and the Web Search Filtered category to **Log**. This will force users in this group to use only safe search engines, or force the safe search function to be enabled on many popular search engines such as Google and Bing.

When you are finished making changes, be sure to click the **Save** button to save your settings.

Managing Overrides

Further category customization can be done in the **Overrides** section where you may create a whitelist or blacklist of individual website domains, IP addresses, specific URLs, search terms, or newsgroups. The **System** group will apply an override for all groups in the system. Websites can be set to block, allow, or changed to any of the categories found in the Group Policy section. Further customization can be done by placing categories in "User Defined" custom categories. These User Defined categories can be renamed in the Filter Settings > Define Categories section.

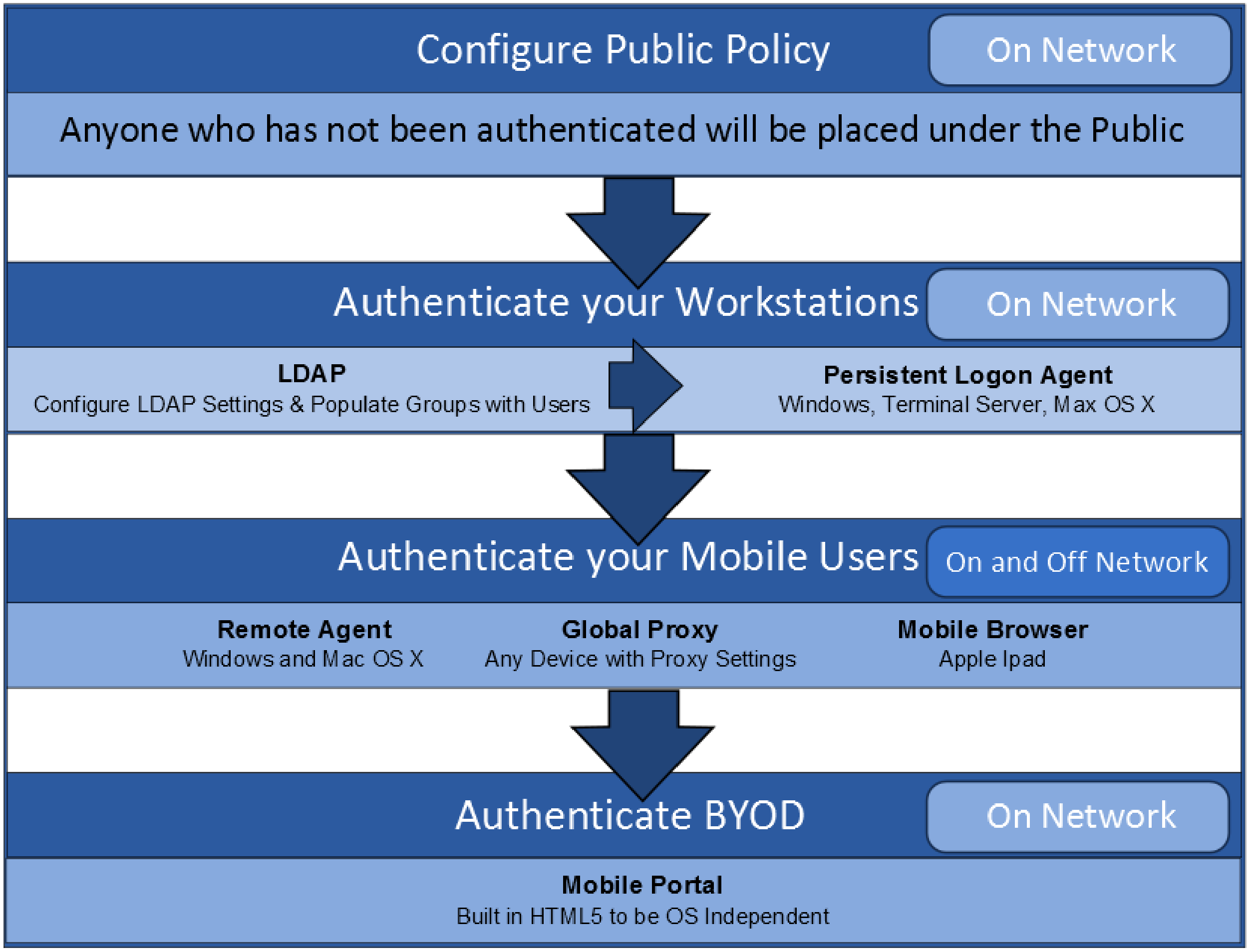
Options for overrides include the start and end date to specify when an override becomes active and deactivates. The referrer depth feature will apply the same category override for any content referenced on the overridden website. For example, if you override yahoo.com to Admin Allow, and yahoo's webpage contains logo images linked from Microsoft.com, then those logo images will also be allowed. This feature can be used in a number of ways, such as creating a repository of YouTube video links on a hosted web page that can be viewed, while blocking the rest of the content from YouTube.

Authenticating Users

Although we have created groups of users and have applied policy to them, we still don't know which users are using which IP address. For this we need to implement a means of authenticating users onto the appliance, to associate the usernames we already have with the IP address they are using. NetSpective has multiple ways of handling this for on-network workstations, off-network notebooks, BYOD initiatives, and the various operating systems those devices use. Since we have so many choices, we created the **Authentication Guide** found in the Help section. This guide details all of our authentication methods as well as the steps to implement each of them.

The flowchart below illustrates which method to use for each device as well as the order in which you should implement them.

Steps to Setup Authentication for Users



Configure Public Policy — On Network

Anyone who has not been authenticated will be placed under the Public

Authenticate your Workstations — On Network

LDAP
Configure LDAP Settings & Populate Groups with Users

Persistent Logon Agent
Windows, Terminal Server, Max OS X

Authenticate your Mobile Users — On and Off Network

Remote Agent
Windows and Mac OS X

Global Proxy
Any Device with Proxy Settings

Mobile Browser
Apple Ipad

Authenticate BYOD — On Network

Mobile Portal
Built in HTML5 to be OS Independent

If you have been following this guide, then we recommend you begin with our Persistent Logon Agent, as shown in the flowchart. This will authenticate the majority of your workstations and be the least cumbersome to your users. Logon Agents live on the Domain Controller and are simply pushed out through a Group Policy Object or Network Logon Script.

Once you have the Logon Agent deployed, you can proceed to authenticate mobile users. Our Remote Agents and Mobile Browser are perfect for users taking devices home.

Lastly, the Mobile Portal was designed with HTML5 to filter any on network device. This should be used only for BYOD initiatives and any device not already filtered by the previous methods listed.

Configure Logging and Install NetAuditor

Your NetSpective is preconfigured with some basic logging settings to enable the **Statistics** link under the **Device Information** heading. Under Statistics you can see several reports giving you an overview of recent traffic. The **Recent Activity** is an important tool for seeing the hits users made to the internet and why they were blocked. Use the **Search** bar at the top to narrow down results for Users, IP addresses, Groups, or URLs.

For more granular reporting, you will want to install NetAuditor to offload logs and report on them.

NetAuditor 3.x Server Requirements

- **Server or VM OS –** Any Windows Server OS from 2003 SP2 to 2008 R2
- **Desktop or VM OS –** Any Windows Desktop OS from XP SP2 to Windows 8
- **CPU –** 1GHz minimum, 2GHz Recommended
- **Memory –** 2GB minimum, 4GB recommended
- **Disk Space and Virtualization Requirements –** Refer to the NetAuditor First Steps Guide. From the client interface, click the heading **Help** and select **First Steps Guide**.

1. Navigate to the **System Control** heading on the left and click on **Device Settings > Logging**. Here you can see Syslog Settings have been enabled and preconfigured. Change the Server IP address to the IP of the server you plan on installing NetAuditor on. The other settings should remain set to TCP and Timestamp enabled.

   Enable NetAuditor Link has also been given an example. This feature provides a **Reports** link under the **Device Information** heading, next to **Statistics.** This gives the administrator easy access to the NetAuditor Web Interface.

2. Navigate to the **System Control** heading and click on **Utilities**. Below you will find the NetAuditor heading. Download and install **NetAuditor 3**.

3. Once the installation of NetAuditor 3 has finished, a window will pop up asking you how to license the product.

   If you have been licensed for NetSpective reporting only, click **Yes**.

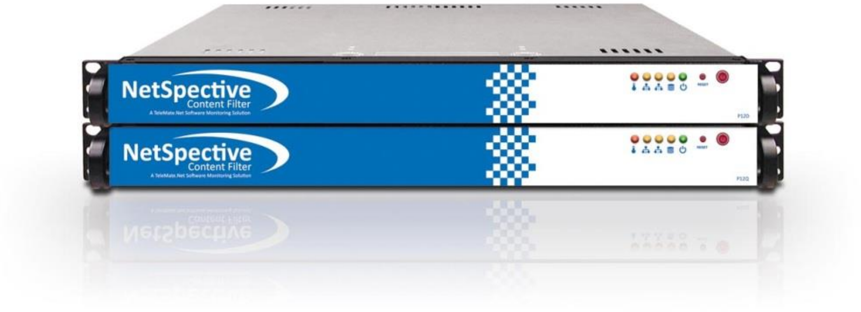
   If you have been licensed for NetSpective as well as reporting on Firewall logs, click **No**. The window indicates you will be given a 30 day evaluation license; however the license you purchased can be applied within the application's interface.

   Licensing NetAuditor can be done in the right column under
   Collection Service Settings > Licensing Settings. Simply enter in the information sent to you by TeleMate.Net Software.

4. Updates for NetAuditor will be downloaded automatically. To install these updates, navigate to the **Help** menu and click on **Install Update**.

5. In order to start collecting the logs that NetSpective is trying to send, you will need to create a Syslog Server. In the left column, right-click on **Syslog Server** and **Add New Instance**. You can name this anything you want, such as 'NetSpective'. Once the server has been created, right-click on it and select **Enable**. A moment later you should see the **Processing & Web Service** create a tree for NetSpective with the Hostname of the appliance under that service. This indicates that NetAuditor is receiving logs from NetSpective and is processing them.

If NetAuditor is not seeing logs from NetSpective, you may have to disable Windows Firewall, ensure communication is allowed in your Firewall, ensure that the Syslog Server is set to TCP, or that NetSpective is seeing any amount of traffic to log.


NetSpective
Content Filter
A TeleMate.Net Software Monitoring Solution
NetSpective
Content Filter
A TeleMate.Net Software Monitoring Solution

TeleMate.Net®
SOFTWARE

5555 Triangle Parkway Suite 150

Norcross, GA 30092
(Tel) 678-589-7100
(Fax) 678-589-7110
www.telemate.net

P/N: 509-1145-00 REV: 0A