

NetSpective Global Proxy Configuration Guide

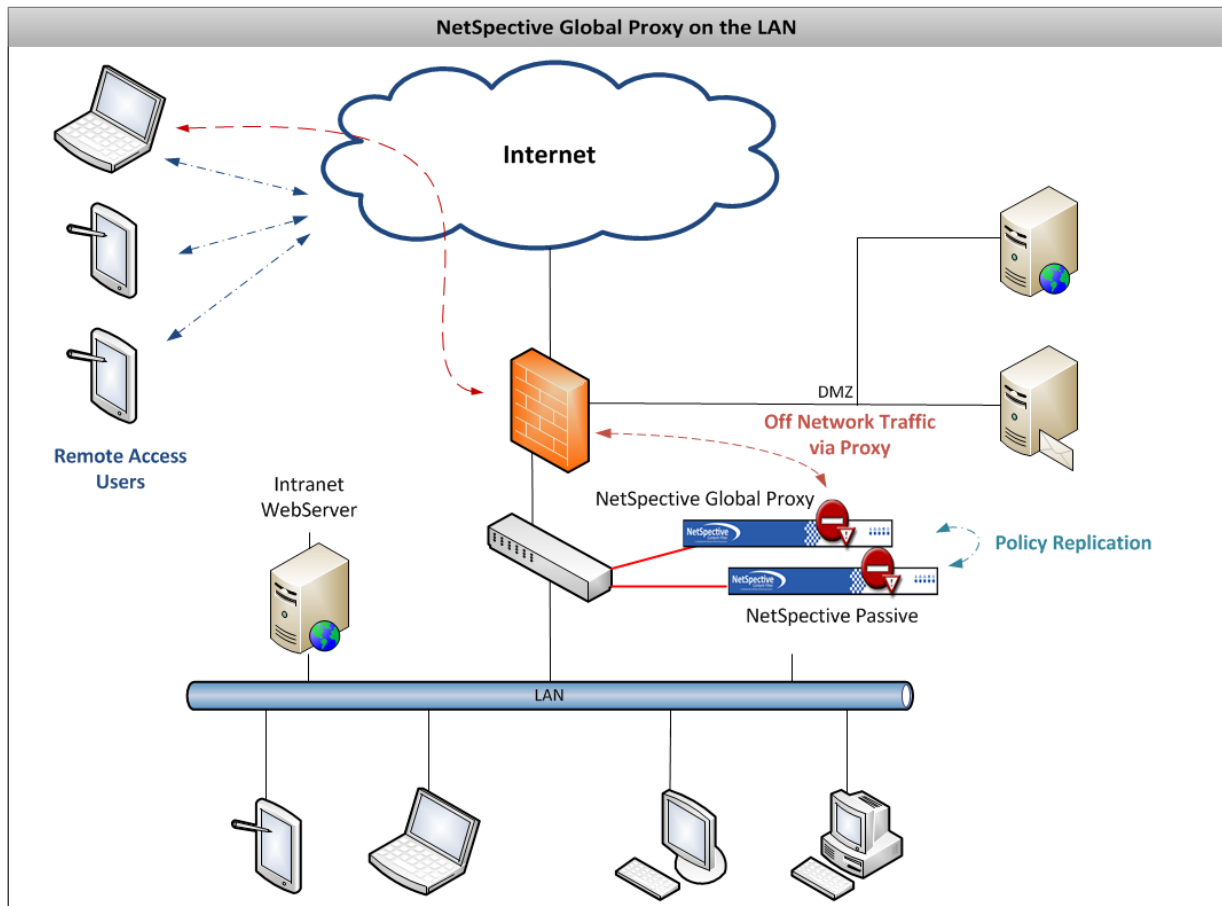


Table of Contents

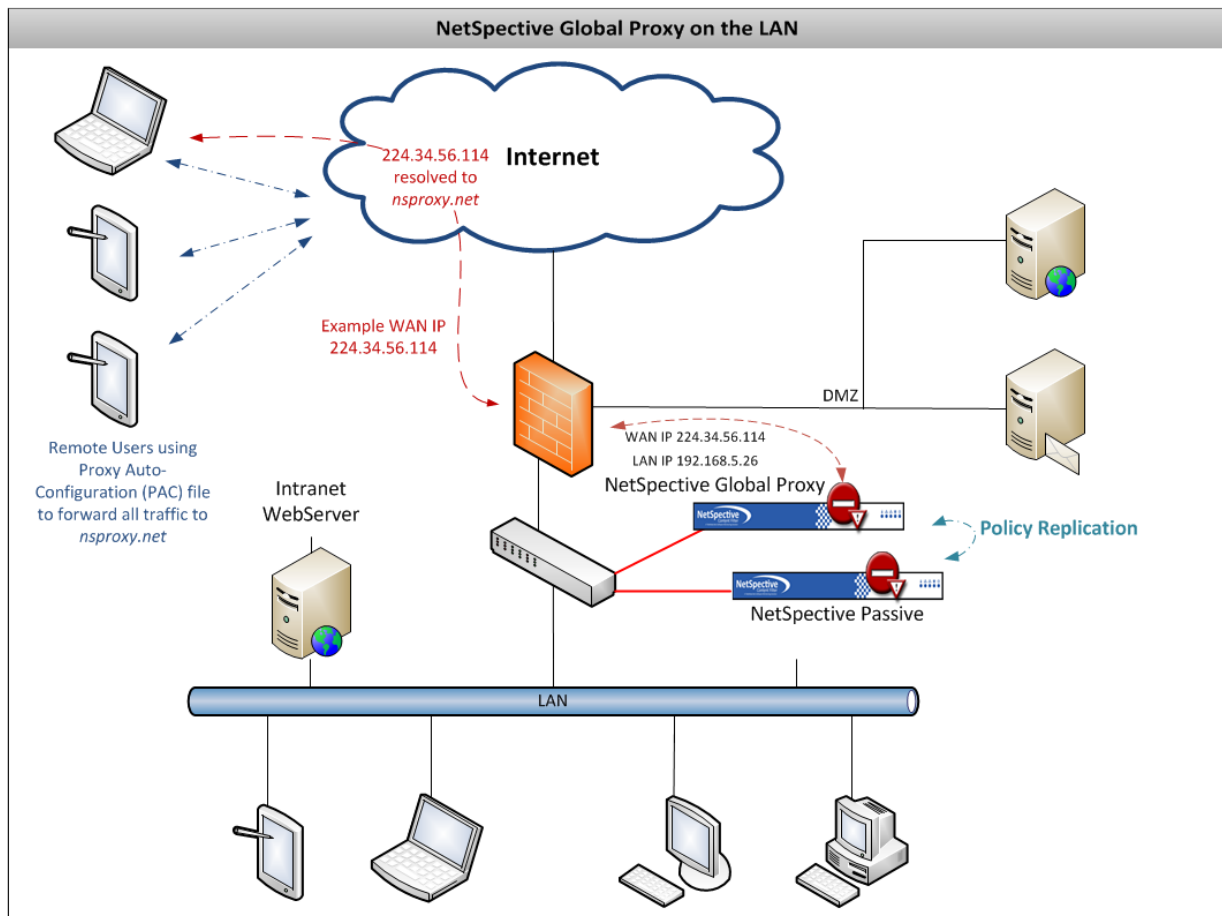
NetSpective Global Proxy.....	1
Table of Contents.....	2
NetSpective Global Proxy Deployment.....	3
Configuring NetSpective for Global Proxy	5
Networking.....	5
Apply a Certificate and Hostname	6
DNS settings on the Domain Controller.....	8
Public DNS and Firewall Configuration	9
Join the NetSpective to your Domain	9
Set Authentication Rules.....	10
Deployment	11
Proxy Configuration	11
Global Proxy Configuration with PAC file.....	13
Limitations with Global Proxies	14
iOS Web View, Apps that won't Authenticate, and iOS Updates	14
Beware of using Safe Search > Block HTTPS Web Search	14
Recent Activity delayed results with a Google SSL connection	14

NetSpective Global Proxy Deployment

The Global Proxy makes use of our existing proxy solution to filter devices on or off the network. The appliance sits inside the network, typically alongside our NetSpective Passive solution. We use policy replication to copy settings from one appliance to the other, so you only have to manage the parent device.



The Global Proxy will be given two IP addresses; one for your local area network, as well as an external IP address for the WAN. Your firewall will need to be configured to translate the WAN IP address into the LAN IP address. Remote users, such as iPads and Chromebooks, will send traffic to the DNS Hostname associated with the WAN address. Your firewall will need to allow this traffic and direct it to the appliance on the LAN.



As you can see in the second image, remote devices are configured to direct traffic to a hostname instead of an IP address. This is particularly useful if you wish to use a PAC (Proxy Auto-Configuration) file for configuring devices to use the global proxy. You will need to setup a public DNS so that the hostname resolves to an IP address in the cloud.

Configuring NetSpective for Global Proxy

Networking

Under **Device Settings > Network** we can see the IP address of the appliance, as well as the Default Gateway. If your appliance is in a single NIC configuration, then the single IP address on the Admin port is all you need. Only if your appliance is configured with dual NICs will you need to specify your Internal and External IP addresses. While we are here, you will also want to add in a DNS Server. This will be needed for Windows NTLM authentication as well as Global Proxy operation. Also, you should ensure that your AD Realm (example: "qatest.telemate.net") is a DNS search domain.

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	VLAN	Port	Status	Mac Address
Admin	192.168.10.120	255.255.255.0	N/A	Lan A	1000 Full	00:25:90:12:43:A8
Admin VLAN 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Lan A	1000 Full	00:25:90:12:43:A8
Admin VLAN 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Lan A	1000 Full	00:25:90:12:43:A8
Admin VLAN 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Lan A	1000 Full	00:25:90:12:43:A8
Admin VLAN 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Lan A	1000 Full	00:25:90:12:43:A8
Internal	<input type="text"/>	<input type="text"/>	N/A	Lan A	1000 Full	00:25:90:12:43:A8
External	<input type="text"/>	<input type="text"/>	N/A	Lan B	100 Half	00:25:90:12:43:A9

Default Gateway:

DNS Servers

Delete

Add

DNS Search Domains

Delete

Add

Networking 5

Apply a Certificate and Hostname

Proceed to **Device Settings > Certificate** where we will apply a certificate to the appliance. This is necessary for specifying the Hostname of the appliance. You may purchase a SSL Certificate from any certificate authority you wish. However, generating our self-signed certificate will work as well and is what we will focus on in this guide. As you can see in our example below, our test appliance will resolve to the hostname “netspective.qatest.telemate.net”.

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.qatest.telemate.net
Locality: Atlanta
State/Province: Georgia
Country: US

Issued By

Organization: TeleMate.Net Software, Inc.
Common Name: netspective.qatest.telemate.net
Locality: Atlanta
State/Province: Georgia
Country: US

SSL Information

Hostname: netspective.qatest.telemate.net

Validity

Issued On: Jan 28 22:44:27 2013 GMT
Expires On: Jan 26 22:44:27 2023 GMT

Generate Request

Add Certificate

To add a self-signed certificate, click on the Add Certificate button. Enter your desired hostname in the SSL Hostname field. When you are finished, click OK.

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

netspective.qatest.telemate.net

Intermediate CA Certificate (Optional)

OK Cancel

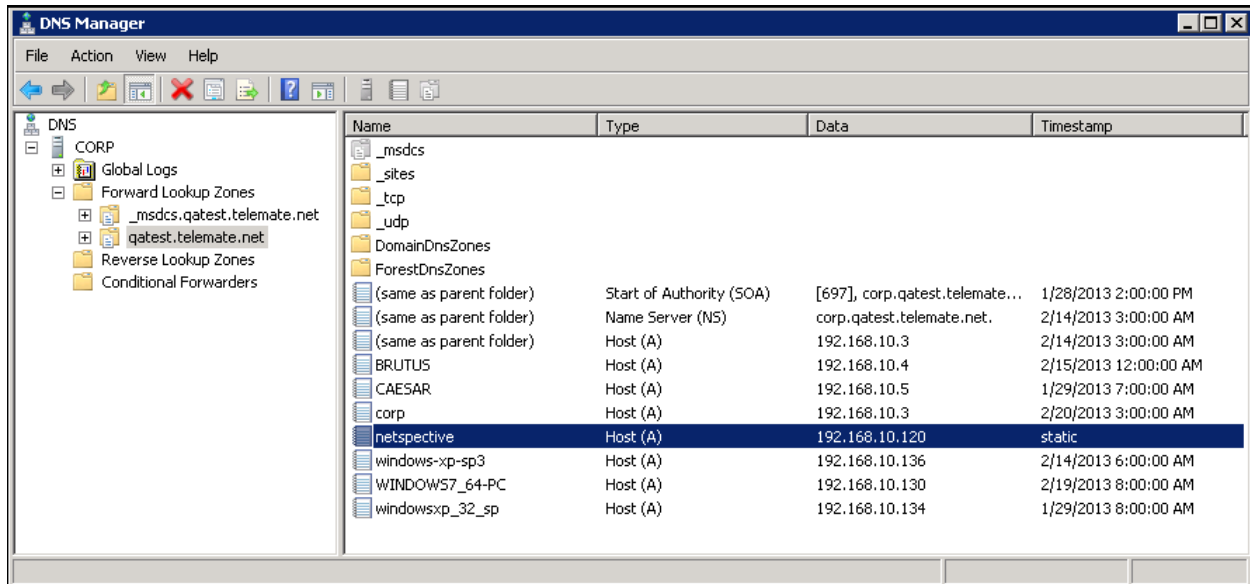
The hostname displayed is an example only.

The web server will restart and the Certificate screen will be updated with the new hostname information, as seen in the Common Name and Hostname Areas.

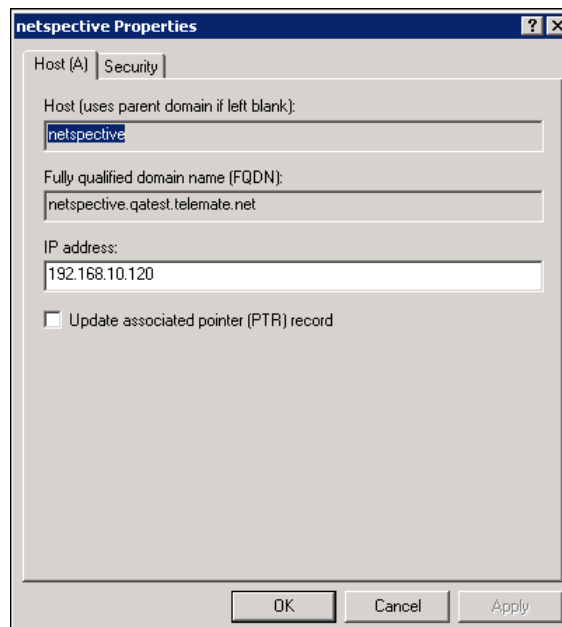
For more information on adding a certificate to NetSpective, refer to the [NetSpective Certificate Guide](#).

DNS settings on the Domain Controller

Setting up a DNS on your domain controller will vary depending on the server you are using. We simply need to set up a Forward Lookup Zone to match the hostname we gave the NetSpective. This will also look different depending on your organization's domain. With a DNS setting on the domain controller, proxy users can be directed to the appliance on network as well.



Our example Windows Server 2008 domain is qatest.telemate.net, so we configured our hostname to be netspective.qatest.telemate.net.



We then added the Forward Lookup Zone for 'netspective' and its IP address.

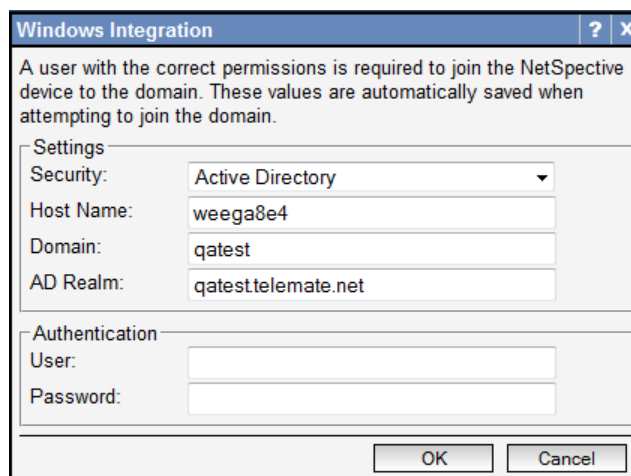
Public DNS and Firewall Configuration

This hostname will also need to be resolved outside of your network in the cloud. Your network administrator will need to configure this with your organization's public DNS service. The hostname will need to resolve to the WAN address configured for the NetSpective appliance on your firewall, which will allow communication into your network to the appliance.

Join the NetSpective to your Domain

Next we will join the NetSpective to your domain to enable Windows NTLM authentication. Windows integration sets up a trusted relationship between the NetSpective and your domain to allow users to be authenticated for the Global Proxy service. A domain user with sufficient privileges is required to add the NetSpective device to the domain.

Navigate to **Device Settings > Advanced** and find the **Windows Integration** heading. Click on the **Join** button and fill out the window that appears with the appropriate information. Since we are simply joining the appliance to the domain, the hostname of the appliance is used and not the hostname we created in the certificate. This can be found under the **Device Information** heading next to **Host Name**.



Windows Integration

A user with the correct permissions is required to join the NetSpective device to the domain. These values are automatically saved when attempting to join the domain.

Settings

Security: Active Directory

Host Name: weega8e4

Domain: qatest

AD Realm: qatest.telemate.net

Authentication

User:

Password:

OK Cancel

Image depicts examples only.

Set Authentication Rules

For NetSpective to filter users globally, we will need to configure Authentication Rules for the entire internet. We can accomplish this in two rules. Navigate to the **Filter Settings > Authentication** page. Note the arrows on the far right for changing the priority of the rules. If you configure your NetSpective to use a more specific rule, for example with our Standard Portal for workstations on your network, you will want those specific rules to be at the top of your list. You can easily use these arrows to move our Global Proxy rules to the bottom.

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

Search: Group: System

Customization Proxy **Authentication** Define Categories YouTube | Schools Advanced

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.

Logon Agent Settings

☐ Log out inactive Logon Agent Users at midnight
Inactivity Duration: Hour(s)

Authentication Rules

	Name	IP	Netmask	Mode		
<input type="checkbox"/>	https test	192.168.10.136	255.255.255.255	Standard Portal; Authentication (LDAP)	↑	↓
<input type="checkbox"/>	Proxy Internet Zone 1	0.0.0.0	128.0.0.0	Proxy; Authentication (Windows NTLM)	↑	↓
<input type="checkbox"/>	Proxy Internet Zone 2	128.0.0.0	0.0.0.0	Proxy; Authentication (Windows NTLM)	↑	↓

Example: Standard Portal rule is at the top of the list, where Proxy Internet Zones are located at the bottom.

To create these Authentication Rules, click the **Add** button below. We will create a single rule; the rule will have the **Address 0.0.0.0** and **Netmask 0.0.0.0** to encompass the entire internet range. This rule will have the Portal set to **Proxy (Session Based)** and have **Windows NTLM** checked. The Timeout section is greyed out since our portal is session based.

Authentication Rule ? X

Zone Name:

Address:

Netmask:

Portal: Proxy (Session Based)

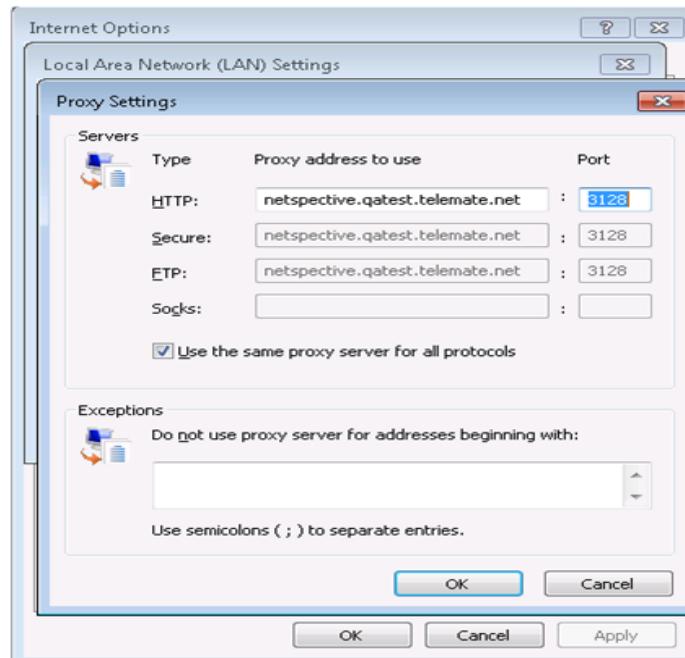
Method: ☐ LDAP ☒ Windows NTLM

Timeout: Logon Minute(s)

Deployment

Proxy Configuration

Devices can be configured in the traditional proxy way by pointing your device to the hostname we configured. As you can see in the examples below, devices show the full hostname as well as **Port 3128**. This is the port NetSpective Global Proxy listens on for user traffic.



Example: Windows Proxy Settings



Example: iPad manual proxy settings.

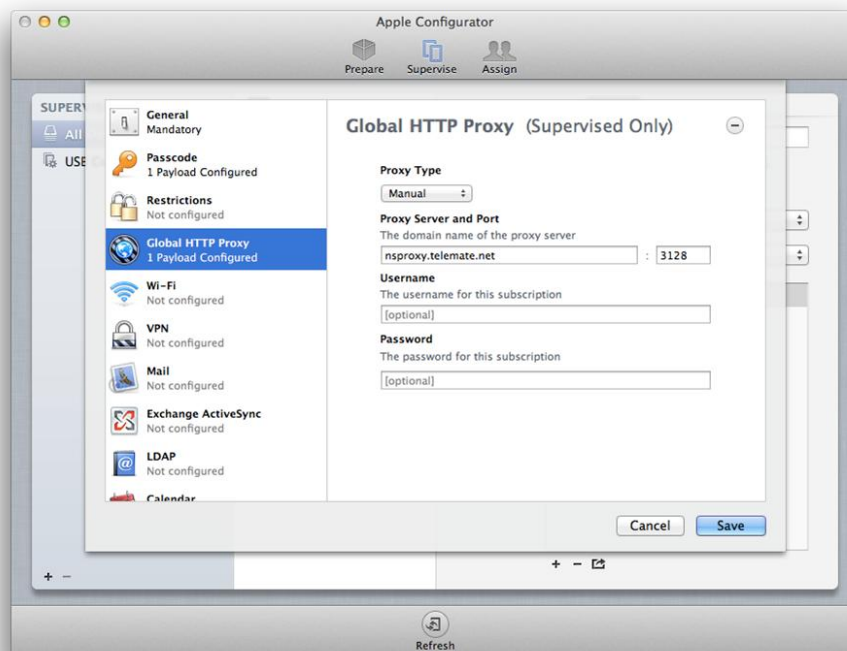
Global Proxy Configuration with PAC file

The preferred method to configure devices would be with a Proxy Auto-Configuration (PAC) file. This can be used to configure multiple devices at the same time with Global Proxy settings.

Navigate to **Filter Settings > Proxy** on the appliance. Under the **Proxy Automatic Configuration** heading, click the download link to obtain a PAC file.

Proxy Automatic Configuration	
Last Updated On:	2013-02-08 04:29 PM - Download
NetSpective Proxies:	netspective.qatest.telemate.net - Edit List

This file can then be used with MDM solutions such as the Apple Configurator to easily provision multiple devices to use the Global Proxy.



Example: Apple Configurator using PAC file.

Limitations with Global Proxies

iOS Web View, Apps that won't Authenticate, and iOS Updates

Upon using the Global Proxy, you may notice that some apps will fail to work. Some examples of this are Netflix and Google Earth. The issue lies within the iOS Web View code, where it contains a defect on how an app authenticates with a Global Proxy. An app developer would need to code around this defect in order to make the app work with any Global Proxy solution. The app is basically trying to authenticate with the Global Proxy, but this defect will not allow the app to complete the authentication. Users will likely notice their keyboard has frozen and the app will have to be terminated. A number of apps have already been created with workarounds in place, but some have not.

This is related to iOS updates as well. On a device using the Global Proxy, if the user is authenticating against the Global Proxy then the iOS Update will fail. Users will likely encounter the message: "Software Update Unavailable – Software update not available at this time, try again later". The Apple Configurator however, can still be used to update a device to the latest software release.

Beware of using Safe Search > Block HTTPS Web Search

Safe Search is an excellent tool for keeping users safe from unwanted search results on the internet. When enabled, we included the option to also block HTTPS Web Search. This feature however should be used with extreme caution as it can disable many services your mobile devices may be using.

For example, the majority of Google's features and educational services require an SSL connection. If we block that SSL connection, we are essentially disabling most of the functionality that Google provides. This is especially important for devices such as Chromebooks where the device relies on authentication with Google's services to perform the majority of its tasks.

Recent Activity delayed results with a Google SSL connection

You may experience some delays with traffic appearing in the **Statistics > Recent Activity** section. This section is generally used as a troubleshooting means for administrators and TeleMate.Net's support team. These delays should only be experienced with an SSL connection with Google. When a user opens an SSL tunnel to Google, Google does not timeout that user right away. This usually takes between 3 and 5 minutes for Google to take action.

This is expected by the design of NetSpective and isn't quite a limitation. NetSpective tracks session bandwidth and log records are not written to disk until the session is closed. As a result, it may take those 3 to 5 minutes before the user's accesses appear in the Recent Activity page. A workaround for this would be to force that session timeout by closing the user's web browser.

Note: This traffic will appear as RAW since the NetSpective doesn't know what it is. This is simply because we cannot see inside that SSL tunnel.