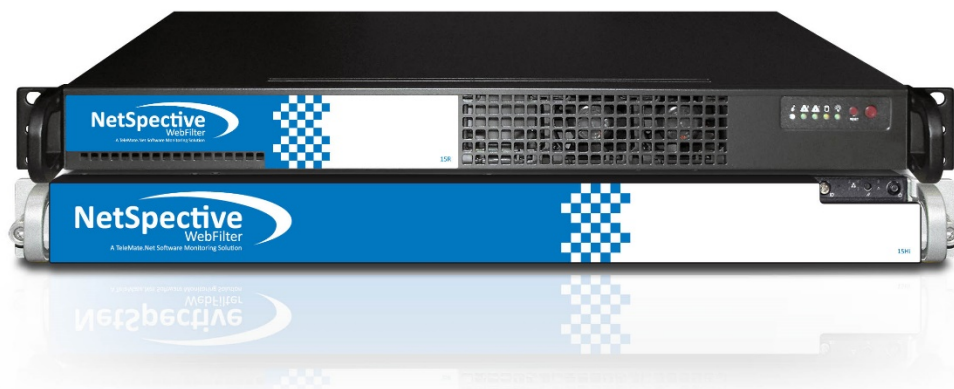


NetSpective User Guide



Copyright © 2002-2018 by Grom Educational Services, Inc. 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

Grom Educational Services, Inc.

3280 Pointe Parkway, Suite 2500

Peachtree Corners, GA 30092

www.GromEdu.com



Deployment Options

Hardware Scalability

NetSpective's 15R chassis is equipped with an octa-core Intel processor and can scale to 10,000 users. We can provide further scalability through our 15Hi chassis, which can scale to 10 Gbps and an unlimited number of users. The 15Hi is equipped with a hexa-core Intel processor and a redundant power supply.

Solutions	Number of Concurrent Users Supported	Bandwidth Capacity	Network Interface Types Supported
NetSpective 15RAppliance	250 users up to 10,000 concurrent users	1 Gbps Bandwidth	Ethernet
2 or More NetSpective 15RAppliances	10,000+ Users	2 Gbps+	Ethernet
NetSpective 15Hi 10 Gbps Appliance	Unlimited Users	10 Gbps Bandwidth	Ethernet or Fiber Optic Interface

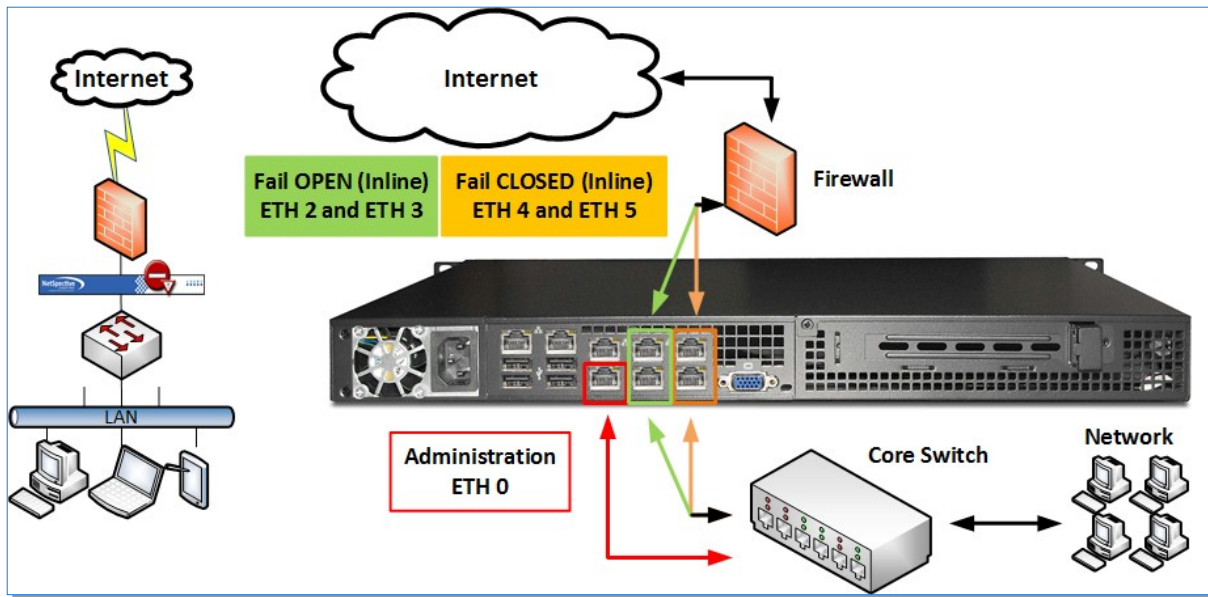
Model Options

Inline Deployment

As an Inline filter NetSpective prevents network performance degradation. SideScan 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 SideScan 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.

With our Inline approach, all packets flow through the appliance, monitoring all requests the internet. The appliance can be deployed as a fail open or fail closed system. SSL traffic is only inspected when the filtering policy permits it, allowing the majority of traffic to pass through unhindered. We do support multi-appliance load balancing and hot spare failover scenarios for redundancy.

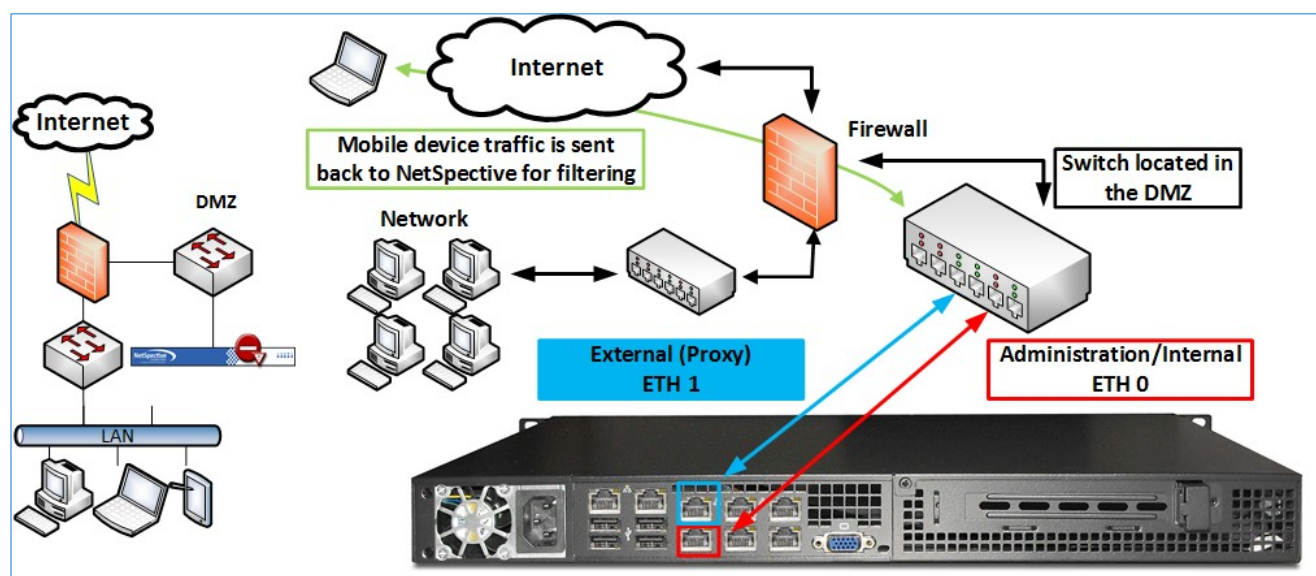


HTTPS Encrypted traffic is selectively decrypted by Group and Category. HTTP traffic is monitored and filtered passively by Group and Category.

Mobile Proxy Deployment

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.

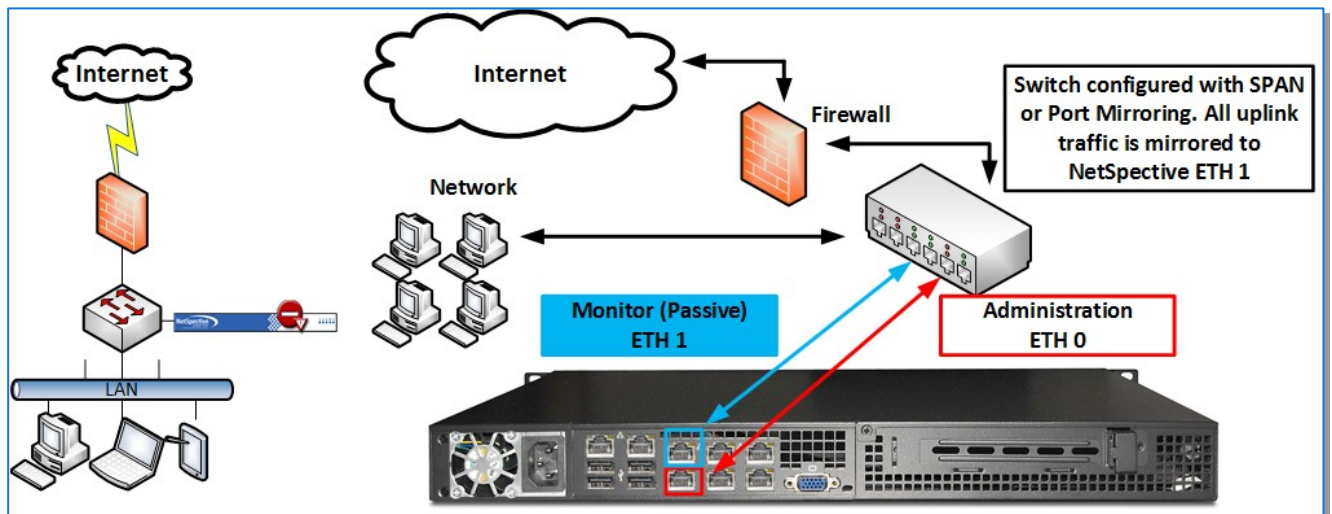
The Mobile Proxy solution can also be leveraged for filtering devices anywhere they are in the world. Configuration changes can be pushed through MDM solutions to force mobile devices such as iPads and Chromebooks to forward all traffic back to the NetSpective WebFilter. These devices can then be safely assigned to students to bring home.



Passive Deployment

NetSpective's Passive configuration allows for optimal filtering performance with zero traffic latency issues in even the highest of bandwidth environments. The primary advantage of passive filtering is wire-speed filtering. This is ideal for educational service providers.

With a Passive configuration, the appliance sits off the SPAN or Mirror port of a switch. This allows the NetSpective appliance to monitor all requests to the internet. Since the appliance is not inline, it is not a point of failure on the network and does not introduce any added latency. The passive configuration also supports multi-appliance load balancing and hot spare fail-over scenarios for redundancy.



ETH0 sends blocking/redirection commands such as Block Pages and Portal redirects.

ETH1 monitors all network traffic as it passes by.

Setup Checklist

This section outlines the steps to take for a basic installation and configuration of the NetSpective. These steps assume the appliance is already racked, given an IP address, and has a license file applied, as outlined in the Quick Start Guide.

Inline Configuration

1. [Build CA Certificate](#) - Before you can perform SSL Inspection, a CA Certificate needs to be created. You can learn more about SSL Inspection under "[Inspecting SSL Traffic with NetSpective Inline](#)". Once your CA Certificate is created, you can optionally use it to "[Build a Website Certificate](#)".
2. [Monitored Zones](#) – NetSpective will only filter IP ranges specified in the Monitored Zones section. Ensure your network zones are included here and any servers are excluded. This is also a good time to review your [Network Settings](#) and configure your [DNS Settings](#).
3. [Configure Directory Sources](#) – A typical deployment will identify users on the network through communicating with a Directory. Configure your Directory Source so NetSpective knows where to pull user information from.
4. [Add a Group](#) – Once we have our Directory synchronized, we can create a group of users in NetSpective and sync them to an Organizational Unit in your Directory. The group within NetSpective can then have a filtering policy linked to it.
5. [Edit Group Policy](#) – Now that a group has been created, you should see it listed in the left pane under the Management tab. You can now assign a filtering policy to those users. If you want to

get even more granular with their filtering policy, you can “[Override](#)” the categorization of specific sites to fit your needs.

6. [Authenticate Users](#) – Even though we have a group populated with users, the NetSpective is not aware of which IP address is assigned to each user. The physical appliance only sees packets associated with IP addresses and the directory does not tell us which IP addresses the users are assigned to. We need to use one of our “Authentication” methods to associate a user with the IP Address their workstation or device is using. There are many different ways to accomplish this. Our recommendation is to use [Remote Agents](#) for laptops and workstations, then any remaining iPads, Chromebooks, and BYOD (Bring Your Own Device) can be authenticated with the [Mobile Portal](#).
7. [Install and Configure NetAuditor](#) – While the NetSpective can provide general “Statistics” for user activity, logs are purged every night at Midnight. For archival reporting, we provide an application called NetAuditor.
8. [Install the DNS Agent for Windows Servers](#) – This should be installed on the primary Windows DNS server in your network. It is highly recommended for users who are decrypting and modifying Google traffic through the use of our various Google features.

Mobile Proxy Configuration

The Mobile Proxy was designed for filtering iPads and Chromebooks taken off network. The solution is intended to be paired with either the Inline solution or the Passive solution, which filter LAN traffic. Once the appliance is configured to act as a Mobile Proxy, you can easily “[Replicate](#)” your parent appliance’s settings and policy to the Mobile Proxy. If you are setting up a Mobile Proxy as a stand-alone device, most of the areas are similar to that of a Passive deployment. Below are the Mobile Proxy specific steps for setting up remote filtering.

1. [Configure Network Settings](#) and [DNS](#) – First decide if you are deploying a single NIC or Dual NIC proxy and define your IP addresses accordingly. You should take this time to fill in your DNS settings, since these will be required for authentication.
2. [Build a CA Certificate](#) and [Apply a Website Certificate](#) - Before you can perform SSL Inspection, a CA Certificate needs to be created. You can learn more about SSL Inspection under “[Inspecting SSL Traffic with NetSpective Inline](#)”. Once your CA Certificate is created, you can optionally use it to “[Build a Website Certificate](#)”. Building a Website Certificate is needed for “[Restricting Admin Access](#)” as well as to give the appliance a hostname.
3. [DNS Settings on the Domain Controller](#) – This allows the hostname to be used to direct traffic to the NetSpective Mobile Proxy.
4. [Public DNS and Firewall Configuration](#) – Workstations will need to be able to resolve the NetSpective hostname when outside of your network.


5. [Join the NetSpective to your Domain](#) – Similar to joining a workstation to the domain. NetSpective will need to be joined for Windows NTLM authentication.
6. [Set Authentication Rules](#) – This will allow the NetSpective Mobile Proxy to catch any IP address being directed to it and prompt for authentication. This is extremely important so rogue users cannot use the mobile proxy and slow down the appliance.
7. [Install the DNS Agent for Windows Servers](#) – This should be installed on the primary Windows DNS server in your network. It is highly recommended for users who are decrypting and modifying Google traffic through the use of our various Google features.


Passive Configuration

1. [Monitored Zones](#) – NetSpective will only filter IP ranges specified in the Monitored Zones section. Ensure your network zones are included here and any servers are excluded. This is also a good time to review your [Network Settings](#) and configure your [DNS Settings](#).
2. [Configure Directory Sources](#) – A typical deployment will identify users on the network through communicating with a Directory. Configure your Directory Source so NetSpective knows where to pull user information from.
3. [Add a Group](#) – Once we have our Directory synchronized, we can create a group of users in NetSpective and link them to an Organizational Unit in your Directory. The group within NetSpective can then have a filtering policy linked to it.
4. [Edit Group Policy](#) – Now that a group has been created, you should see it listed in the left pane under the Management tab. You can now assign a filtering policy to those users. If you want to get even more granular with their filtering policy, you can “[Override](#)” the categorization of specific sites to fit your needs.
5. [Authenticate Users](#) – Even though we have a group populated with users, the NetSpective is not aware of which IP address is assigned to each user. The physical appliance only sees packets associated with IP addresses and the directory does not tell us which IP addresses the users are assigned to. We need to use one of our “Authentication” methods to associate a user with the IP Address their workstation or device is using. There are many different ways to accomplish this. Our recommendation is to use [Remote Agents](#) for laptops and workstations, then any remaining iPads, Chromebooks, and BYOD (Bring Your Own Device) can be authenticated with the [Mobile Portal](#).
6. [Install and Configure NetAuditor](#) – While the NetSpective can provide general “Statistics” for user activity, logs are purged every night at Midnight. For archival reporting, we provide an application called NetAuditor.

The Public Group

The Public Group is the policy all unauthenticated users will receive. By default it only blocks Pornography. This group is intended to be a firewall for all users to hit before being placed in their proper authenticated group, associated by LDAP or IP range. The reason for this is closely tied to our authentication methods.

When using the Mobile Portal to authenticate mobile devices and BYOD, an unknown user's first access will be in the public policy. From here, they should be redirected to the Mobile Portal page, which is HTTPS (Assuming Mobile Portal is configured). If the user's first access to the web is HTTPS, then we can only inject ourselves into the SSL session and redirect to the portal page, if we are decrypting the traffic. Categories in the Public Policy that are not being decrypted will result in a block when attempting to redirect the user to the Mobile Portal. This is very important. Once SSL Inspection is properly configured, you'll want to ensure you are decrypting  most categories to ensure the end user gets the proper experience when using the internet. By decrypting on the Public Policy, we can ensure the end user gets properly redirected to the Mobile Portal with the first access to the web, without blocking them and causing confusion.

Keep in mind we do not recommend decrypting Certificate Authority and Technology. These categories are non-objectionable and contain sites used in authenticating to Google, as well as update services like Microsoft or iTunes updates, respectively. This is also why the Public group is the only group with the Allowed Unauthenticated Flag . Devices such as Chromebooks require packets to be sent to Google before the user ever sees a web browser for authentication. We place this flag on Certificate Authority by default to ensure devices like Chromebooks can contact their registration servers and can be provisioned without being authenticated. You can use the flag to tailor which categories will not prompt the user for portal authentication as well.

Authentication Overview

There are many different ways NetSpectre can associate a Username to an IP address. Authenticating users is common in deployments for not only providing granular filtering, but being able to report on user activity as well. Since there are so many different devices found in a network, we required different methods to authenticate each one. If you are having trouble figuring out how to pull user authentication from a specific device, or which method to use, this section will provide a simple overview on our recommended methods for each device type.

[Inline/Passive] Windows and Mac Desktops and Notebooks [On LAN/Off LAN] – The [Remote Agent](#) is your first line of authentication. The list of benefits to using the Remote Agents are long. Once installed, they cannot be uninstalled or tampered with by the user, authenticating and filtering the user both on LAN as well as off your network. They will download and install your CA Certificates and perform the SSL Inspection locally on the workstation, improving your appliance's performance. Since this agent is installed, the Remote Agent is aware of other programs running on the workstation and can be told to ignore those applications from SSL inspection.

[Passive] Windows, Mac, and Terminal Servers [On LAN] – The [Logon Agent](#) is a lightweight program that can pass username and IP address association over to NetSpective quickly. The Logon Agent is strictly a LAN technology and should not be used on notebooks being sent off network.

These two agents should cover the majority of devices your organization owns. The following methods were created for mobile devices. To ensure your NetSpective appliance remains optimized, we do not recommend using the following methods for your organization's workstations.

[Inline/Passive] iPads, iPhones, Android Phones and Tablets, Chromebooks [On LAN] – The [Wi-Fi Agent](#) is a transparent and automatic method of authenticating any device that is logging onto the wireless network using WPA2 authentication. There are no additional dialogues shown to the end user and authentication is instant even when a device travels from one access point to another. If your network has a RADIUS server providing 802.1x authentication, it is highly recommended for your organization to take advantage of the Wi-Fi Agent.

[Inline/Passive] iPads, iPhones, Android Phones and Tablets, Chromebooks [On LAN] – The [Mobile Portal](#) is a captive portal system. A webpage is displayed, asking the end user for their username and password. The Mobile Portal uses HTML5 and can be displayed on any browser or operating system.

[Mobile Proxy] iPads and Chromebooks [Off LAN] – For devices going home with students and staff, we use a combination of [Cached Session Based Authentication with Windows NTLM](#). Since users are bringing these devices home, we know the user is not likely to change. We can cache these credentials in NetSpective so users are not prompted for authentication repeatedly. We then authenticate against Windows NTLM to not only pass those credentials securely over the internet, but we can provide single sign-on by caching credentials within the device's web browser. The result is a seamless end user experience while still providing granular filtering.

NetSpective Public Communication and Ports

NetSpective contacts our online services to receive software and categorization updates frequently. The NetSpective also communicates to various services and agent through different ports. Consider creating firewall rules for these addresses and ports so the NetSpective may communicate properly.

The NetSpective On Line Service is currently at nsupdate.getnetspective.com, hvupdate.getnetspective.com, and ntp.getnetspective.com

Source	Destination	Protocol	Purpose
Appliance	NetSpective Online Service	Passive FTP	Software and List Update
Appliance	NetSpective Online Service	HTTPS TCP/443	List Update
Appliance	NetSpective Online Service	NTP	Time Synchronization
Appliance	Mail Server	SMTP	E-Mail Alert Messages
Appliance	Internet	HTTP, HTTPS, DNS	Google Authentication and Certificate Validation

Appliance (Proxy Mode)	Internet	All Web Protocols	User Internet Access
Proxy Workstations	Appliance (Proxy Mode)	TCP/3128	Proxy
Admin Workstations	Appliance	HTTP and HTTPS	Appliance Administration
Workstations	Appliance	TCP/81	Portal Authentication
Workstations	Appliance	TCP/8080	Block Page
Remote Agents	Appliance	TCP/3001 and UDP/3001	Remote Agent Protocol
Terminal Server	Appliance	UDP/2050	Terminal Server Agent Protocol

Inspecting SSL Traffic with NetSpectre Inline



There are two methods for inspecting SSL traffic with NetSpectre. The first and recommended method is with our Remote Agents with Transparent Endpoint Inspection. The second method is inline inspection through the use of a CA Certificate. Inline inspection should be reserved for mobile devices such as iPads and Chromebooks.

Remote Agent for Windows and macOS

The existing Remote Agent has been rebuilt to not only perform policy filtering but to inspect TLS protocol traffic at the workstation. The new Remote Agent with filters SSL traffic before it leaves the workstation. This provides two benefits. By moving this function to the workstation, the inline filtering appliance can move traffic to and from the destination uninterrupted, preventing network bottlenecks. In addition to maintaining performance, this method also reduces the risk of a man-in-the-middle attack as the traffic is never modified once it leaves the workstation.

Deploying the NetSpectre Remote Agent Client (Inline/Passive)

Before the Remote Agent can be used, it must know how to connect to your NetSpectre Appliances. You should specify all NetSpectre 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 NetSpectre appliance. You may have to set your firewall to forward UDP and TCP traffic to NetSpectre's listening port of 3001, as well as your firewall's address in the address list within NetSpectre. 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.

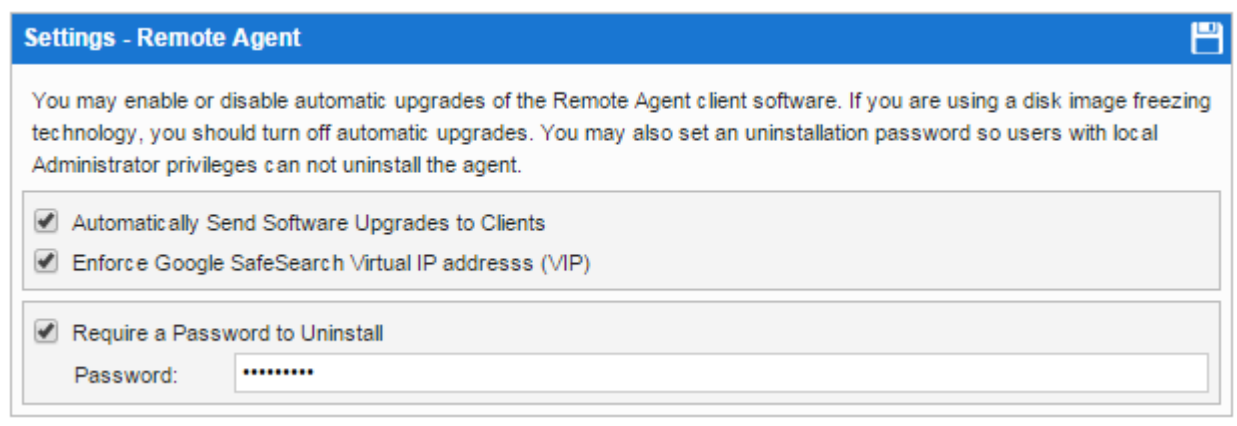
Internal and External Addresses - Remote Agent



To ensure that your remote clients behave correctly on all of your networks, enter the internal and external addresses for all of your NetSpectre devices. The default port is 3001, but it may be different for external addresses if you use port mapping.

<input type="checkbox"/> Address
<input type="checkbox"/> 10.2.40.154:3002
<input type="checkbox"/> 10.2.40.153:3001

The client install consists of two steps: installing an MSI (Microsoft Installer) package and applying the initial configuration file. After you apply the initial configuration file, each client will get configuration updates automatically from the appliance. If you have moved the NetSpective appliance to another IP address, the link may become broken and you may need to manually deploy the configuration update.

When you upgrade your NetSpective appliance to a new version, it may come with a new version of the client. You do not need to worry about deploying the remote client software, as the appliance will automatically update all clients when a new version becomes available.



Authentication > Agents > Client Settings

Installing and Uninstalling the MSI Package for Windows

The MSI package requires no parameters to install, which makes it easy to deploy automatically using software deployment services like SMS Server or Active Directory's Group Policy Objects. It also requires no parameters to uninstall (unless you decide to require an uninstall password).

To install the client silently from the command line:

```
msiexec.exe /i RoamingAgent.msi /quiet
```

To uninstall the client silently from the command line:

```
msiexec.exe /x RoamingAgent.msi /quiet
```

To uninstall the client silently with an uninstall password:

```
msiexec.exe /x RoamingAgent.msi /quiet PW=password
```

The install/uninstall requires administrator access to the client machine, and Windows will display a User Access Control (UAC) warning during the install (unless it is run as the local Administrator or SYSTEM account). When the install/uninstall is complete, you must reboot the client machine. The act of installing/uninstalling the driver may cause certain applications to become unstable if you do not reboot.

Applying the Configuration File

The easiest way to apply the configuration file is to open it in Windows Explorer. The install maps its filename extension (.nsconfig) to one of our program files (NSRemoteSetup.exe). Any user without administrative access can apply the configuration update. If needed, you could email an .nsconfig file to your users or instruct them to download it from a web site and apply it. Administrators can also apply the configuration the by placing the .nsconfig file in the '%ProgramFiles%\NetSpective Remote Agent\downloads' folder.

Deploying the Client Using Active Directory's Group Policy Objects

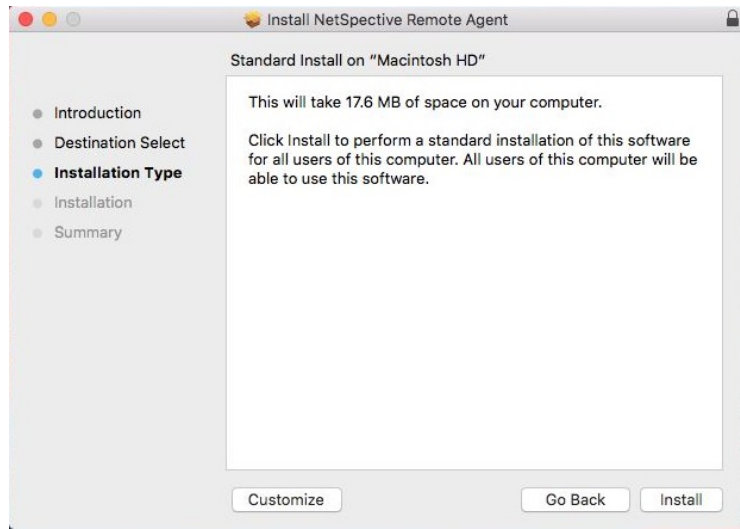
The client and its initial configuration can be deployed automatically to computers in a Windows domain using Group Policy Objects (GPO's). Microsoft has outlined the process of remotely installing software using a GPO in the following support article. <https://support.microsoft.com/en-us/kb/816102> Refer to support.microsoft.com for more information.

Installing and Uninstalling the PKG for macOS

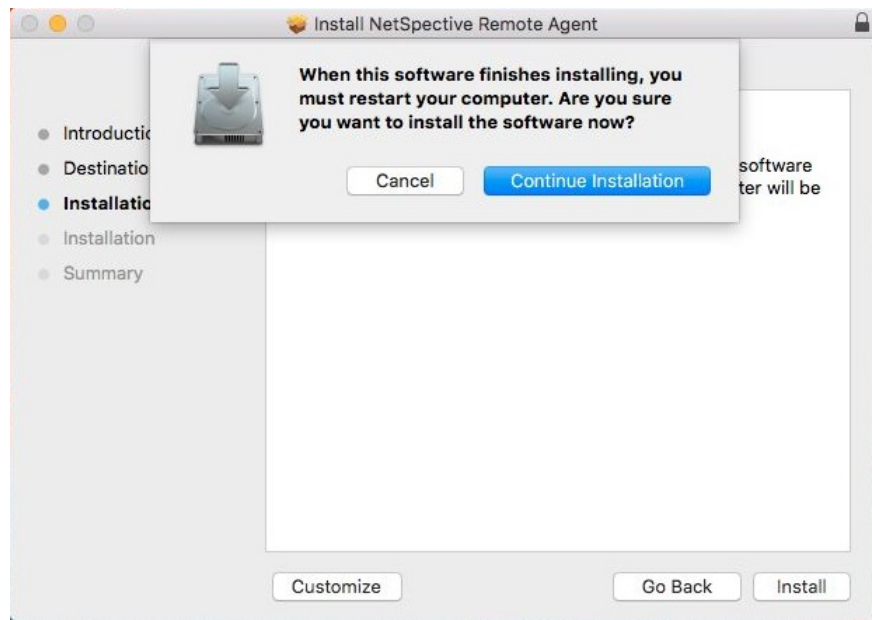
Much like the Windows Remote Agent, the client install consists of two steps: installing a PKG and applying the initial configuration file. After you apply the initial configuration file, each client will get configuration updates automatically from the appliance.

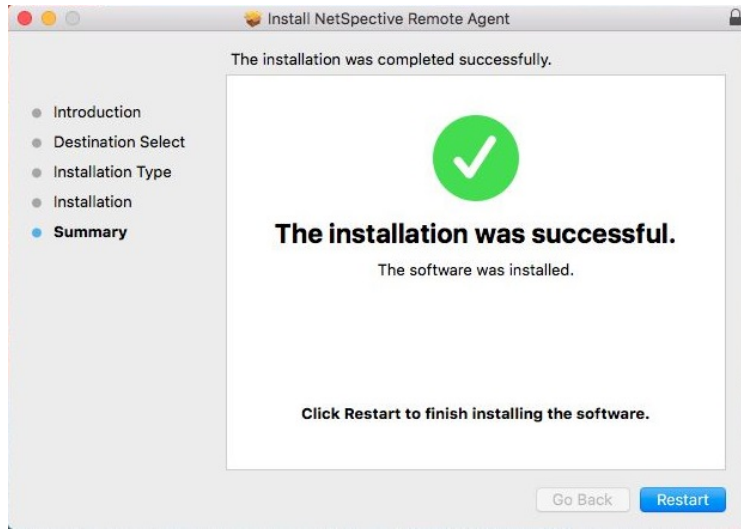
9. From the Downloads section of NetSpective, download the Remote Agent Client for macOS, as well as the Remote Agent Configuration File. Once both files have downloaded, open the RemoteAgent.dmg file and double click on the RemoteAgent.pkg. You will need Administrative access to proceed.

Agent Downloads		
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
Terminal Server Agent for Windows & Citrix	3.0.4	TerminalServerAgent.exe
Logon Agent for Windows (XP, 7, 8, 10)	3.0.11	LogonAgent-3.0.11.zip
Logon Agent for macOS (10.9 - 10.12)	2.3-14	LogonAgent-2.3-14.dmg
Remote Agent for Windows (7, 8, 10)	1.5.48	RemoteAgent-1.5.48.msi
Remote Agent for macOS (10.9 - 10.12)	2.3.3	RemoteAgent-2.3.3.dmg
Remote Agent Configuration File	20161106060858	Configuration
Wi-Fi Agent	N/A	Contact NetSpective Support

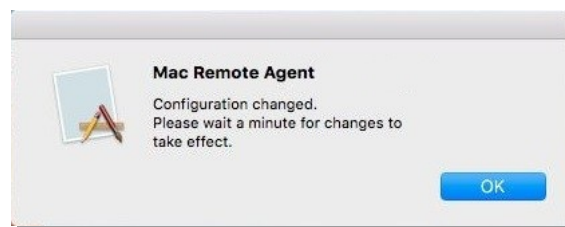


10. Proceed through the installation wizard. When you are finished, the wizard will ask you to reboot in order to complete the installation.





11. When your computer has finish rebooting, open the Remote Agent Configuration File. This will update the Remote Agent software.

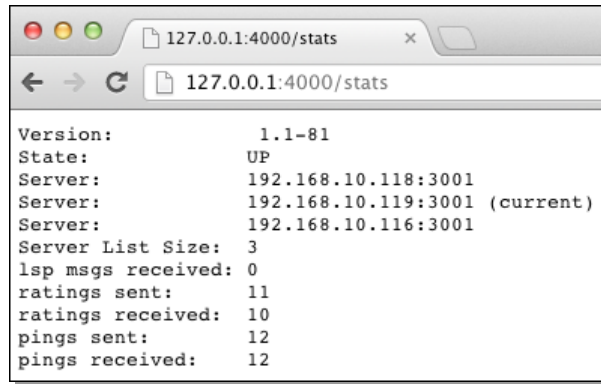


If you wish you uninstall the Mac Remote Agent, you can run the RemoteAgentUninstall.pkg. You will need Administrative privileges to proceed.



Verifying Remote Agent Connectivity

If you wish to verify that the Remote Agent has been installed correctly and has connectivity, there is an easy way to determine that information. Open a web browser on the machine you installed the Remote Agent on. Type the following command in the address bar: localhost:4000/stats



IP Addresses are examples only.

NetSpective Inline SSL Inspection

With the NetSpective Inline solution, SSL traffic can be inspected and manipulated on the appliance. NetSpective uses selective processing to inspect only encrypted traffic of interest. Categories that are being blocked do not need to be inspected and will traverse the network unhindered. The NetSpective Inline solution is capable of inspecting traffic on any device that trusts its CA Certificate, including mobile devices and BYOD.

SSL Certificates

The NetSpective Webfilter supports two types of SSL Certificates. The CA Certificate is used for SSL Inspection. The other certificate is used to access the web administration via HTTPS. If you wish to use NetSpective Inline's SSL inspection, each device will need to accept your CA Certificate as a Trusted Root Certificate Authority. If a device does not trust your CA Certificate, they will not be able to visit any HTTPS webpages.

Building and Downloading the CA Certificate from NetSpective

Under Settings > Certificates > Certificate Authority, you must first build a CA Certificate. The requirements for a CA Certificate are as follows.

Field	Description
Organization	The Organization value cannot contain &, @, 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.
Organizational Unit	The Organizational Unit (OU) field is the name of the department or organization unit making the request.
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	An email address to be included in the certificate.
Common Name	The Common Name is the only required field. The common name is your name or your server's hostname (eg. Example Name or www.example.com).
Key Size	The key size to sign the Certificate with. Available selections are 1024-bit or 2048-bit.

Note: Rebuilding a CA Certificate will remove the previous CA Certificate and create a new one. You will have to add the new CA Certificate as a trusted certificate on your network again. Once you have built a CA Certificate, you can download it from the appliance from the same area. Choose the certificate format that best suits your devices and environment. All deployment methods below use the DER format.

CA Certificate Details

To manage SSL sessions, NetSpecive needs its own root Certificate Authority (CA) certificate that is trusted on your network. This is necessary so it can create its own copies of web site certificates and present them to users on your network without causing certificate trust errors or warnings in the web browser. By definition all root CA certificates are self-signed, so it is easier and more secure for NetSpecive to generate this certificate internally and export it to you to add to your domain's trusted list.

Issued

Organization: Example Company
Organization Unit: Development
Common Name:
Locality: Norcross
State/Province: GA
Country: US

Validity

Issued On: Sep 09 17:52:57 2015
Expires On: Sep 07 17:52:57 2025

CA Certificate - Downloadable Formats

Certificate (DER): [download](#)
Certificate (PEM): [download](#)
Certificate (PKCS12): [download](#)

Build CA Certificate

Build Website Certificate

A Note on Mozilla Firefox Support: There are few tools for deploying certificates to Firefox and the browser is generally not supported by most organizations because of this. There exists an Active Directory Administrative Template plugin to allow Firefox to be managed from Group Policies. However there has been no development on the project over the past several years and the only thing it allows you to do with certificates is completely replace the existing certificate store with a new one, so any user added certificates are wiped out.

You can also download the source code for an unsupported utility from Mozilla and then build the .exe and .dll's for the utility. Then you would need to distribute it to all the workstations on your network. Then you would have to create a batch file or script to find all the Firefox profile directories and then run the utility to install the certificate into each certificate store.

If you still wish to use Mozilla Firefox on your network, we can provide two options. The Remote Agent will copy the CA Certificate to each user profile on a workstation. The other option is to utilize the Policy Reminder page and have the end user install the certificate manually from Firefox

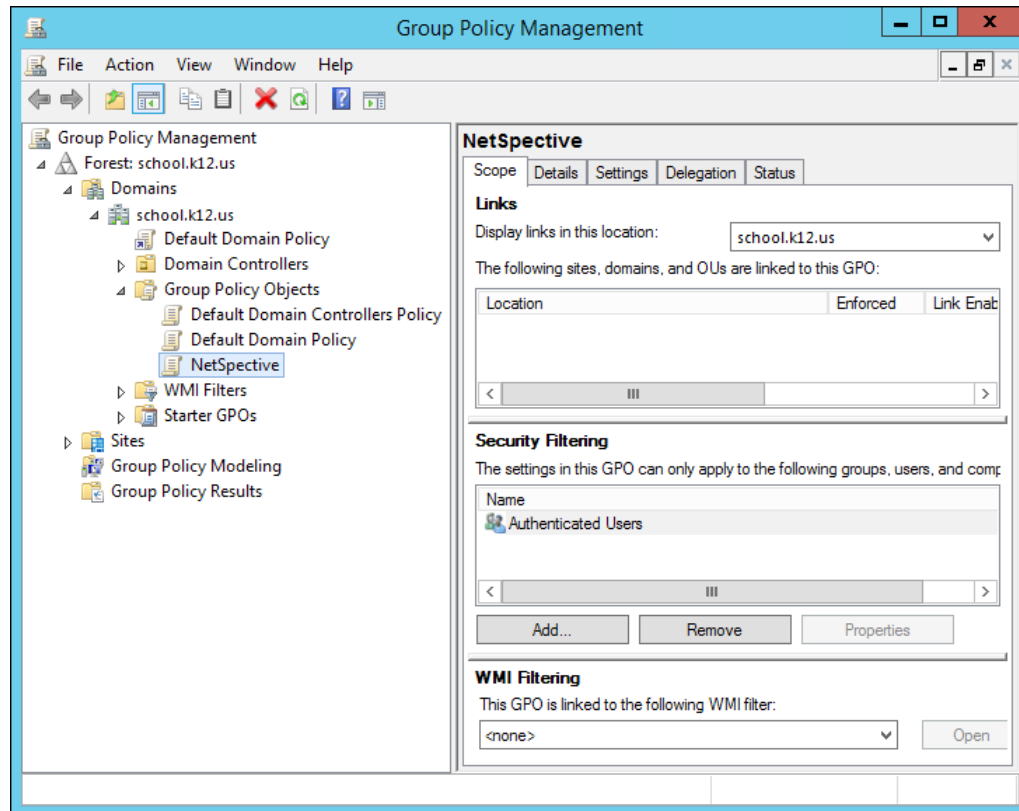
Deploying the CA Certificate Globally

Import CA Certificate through Active Directory

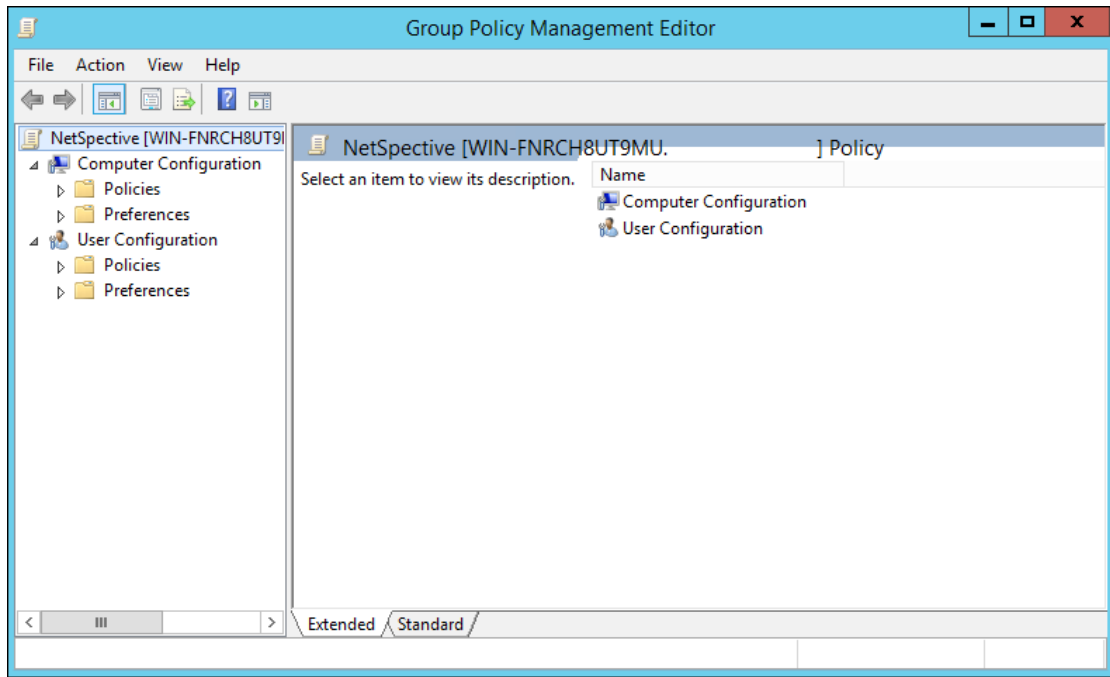
Microsoft's documentation for deploying certificates by using Group Policy can be found at the URL below.

<https://technet.microsoft.com/en-us/library/cc770315%28v=ws.10%29.aspx>

8. Begin by opening Group Policy Management and select GPO.
9. Right click on GPO select Edit.

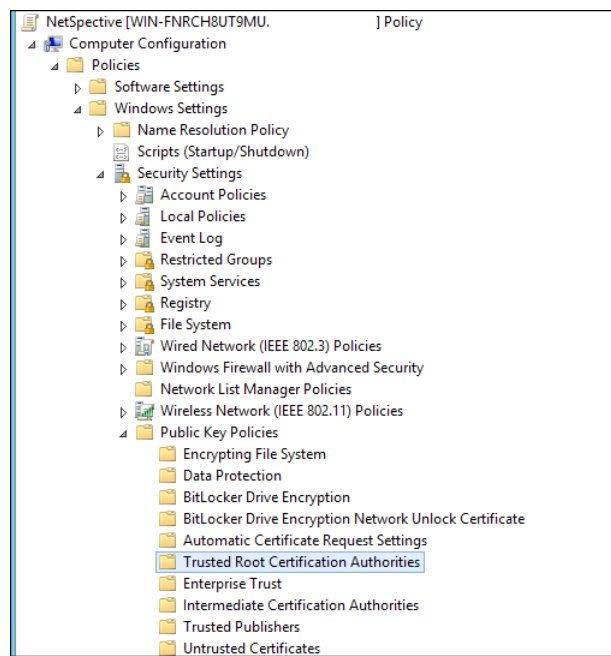


10. You will be presented with the Group Policy Editor.

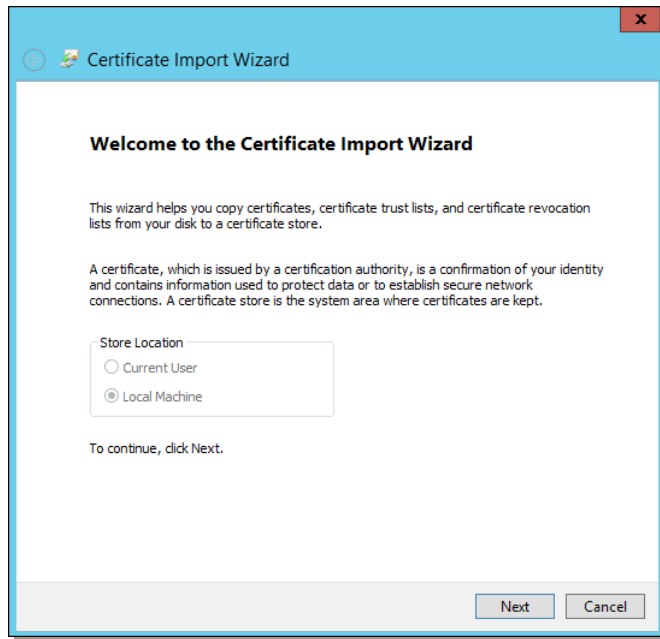


11. Go to Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trust Root Certification Authorities.

12. Right click and select Import to launch Certificate Import Wizard.



13. Select Local Machine and click Next.

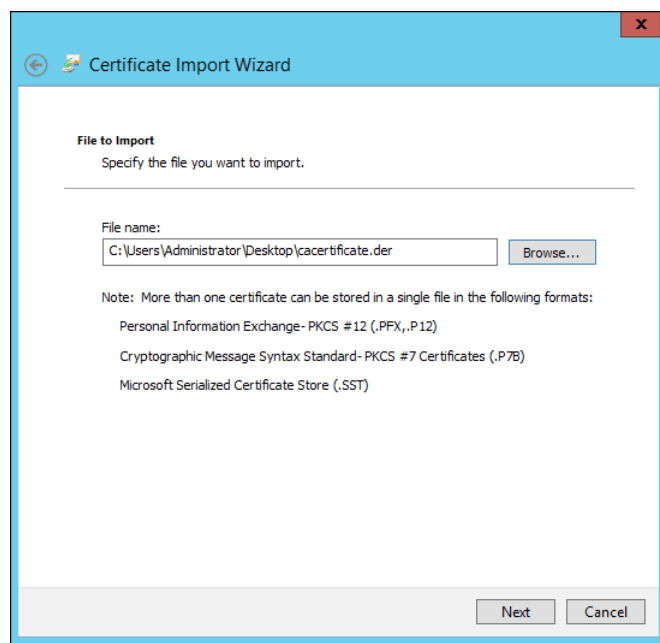


14. Select browse.

15. Select all files.

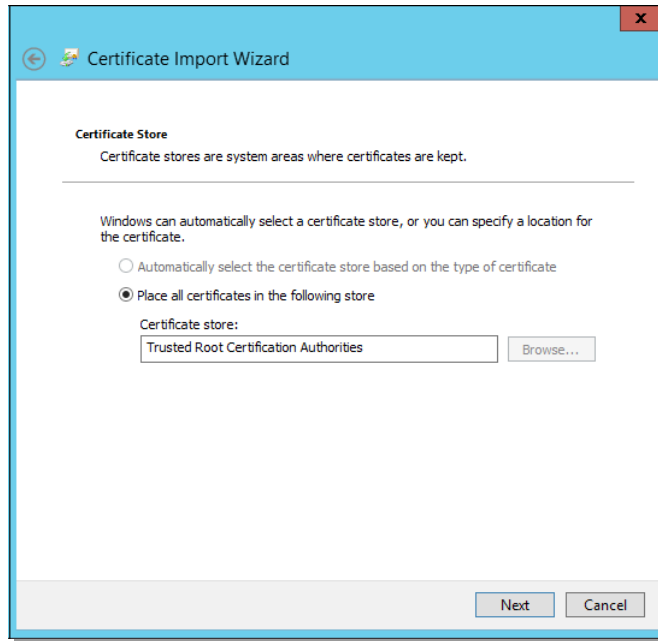
16. Select the downloaded CA Certificate file.

17. Once you are back to the Import screen click Open, then Next.

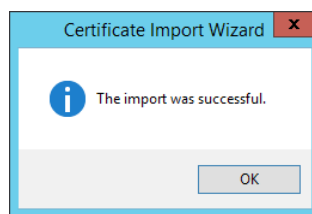
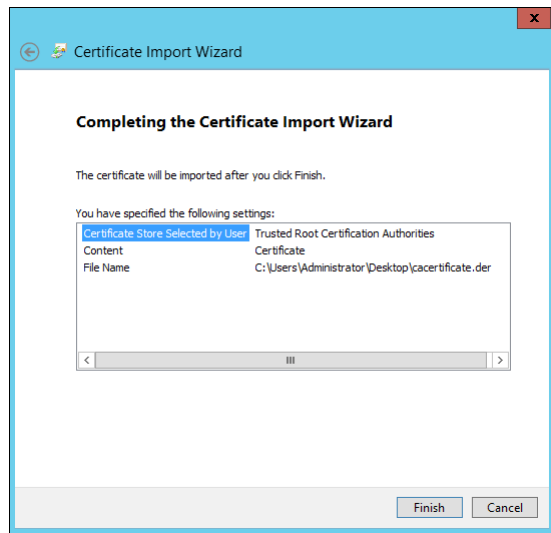


18. Certificate Store should be set to Trusted Root Certification Authorities.

19. Select Next.

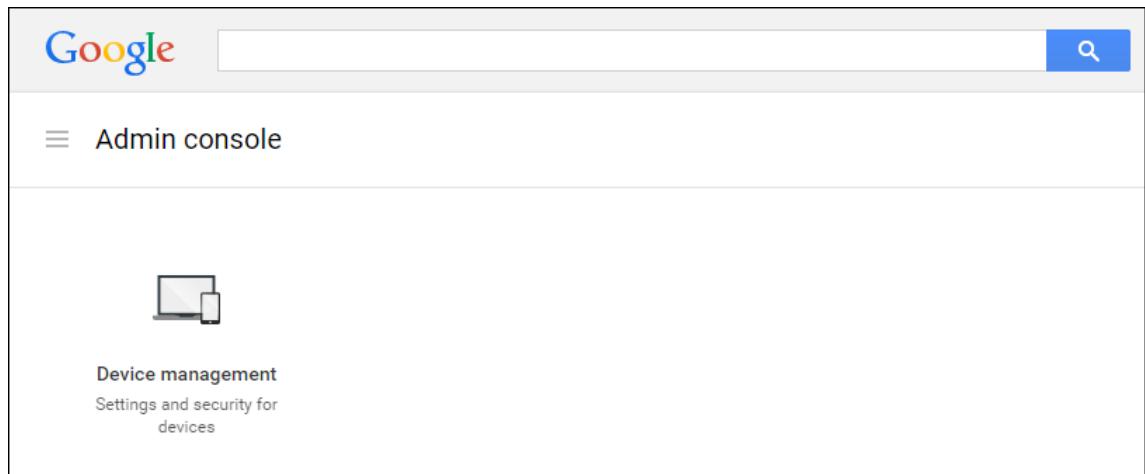


20. Summary screen will appear. Select Finish.

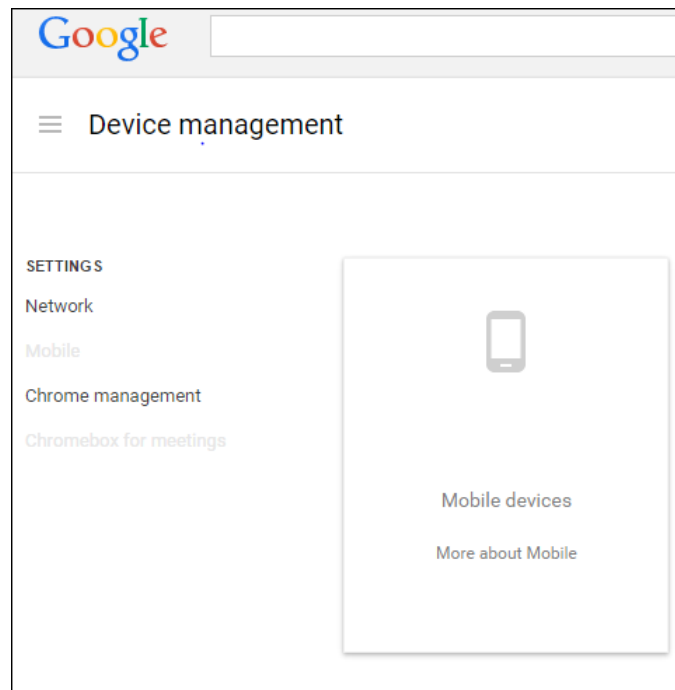


Import CA Certificate in Chrome Admin Console

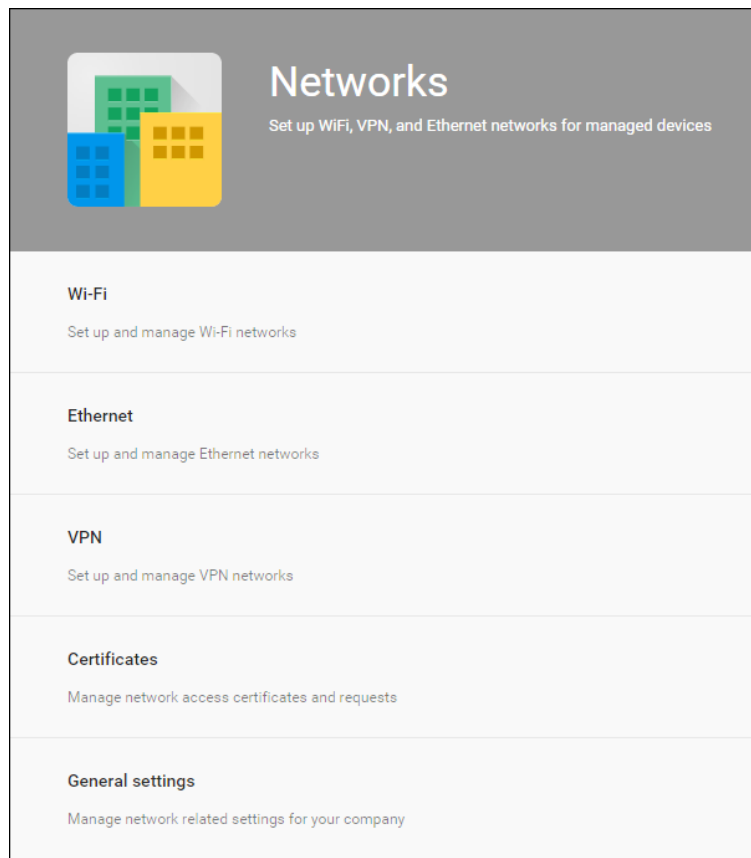
1. Sign into Google Admin Management Console.



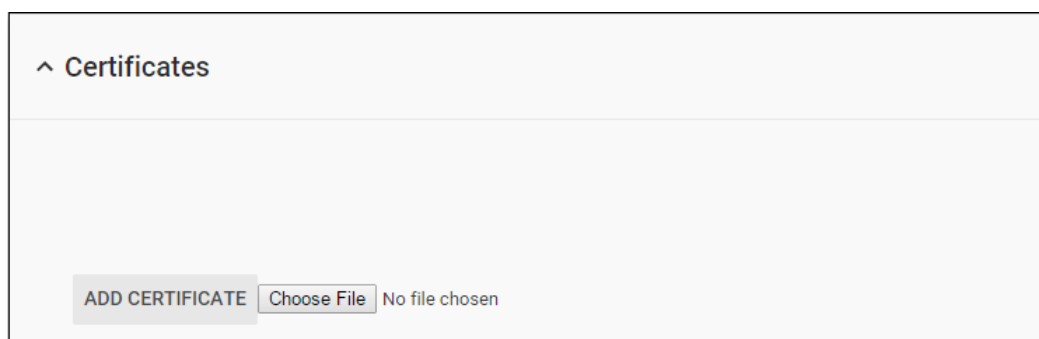
2. Select Device Management.



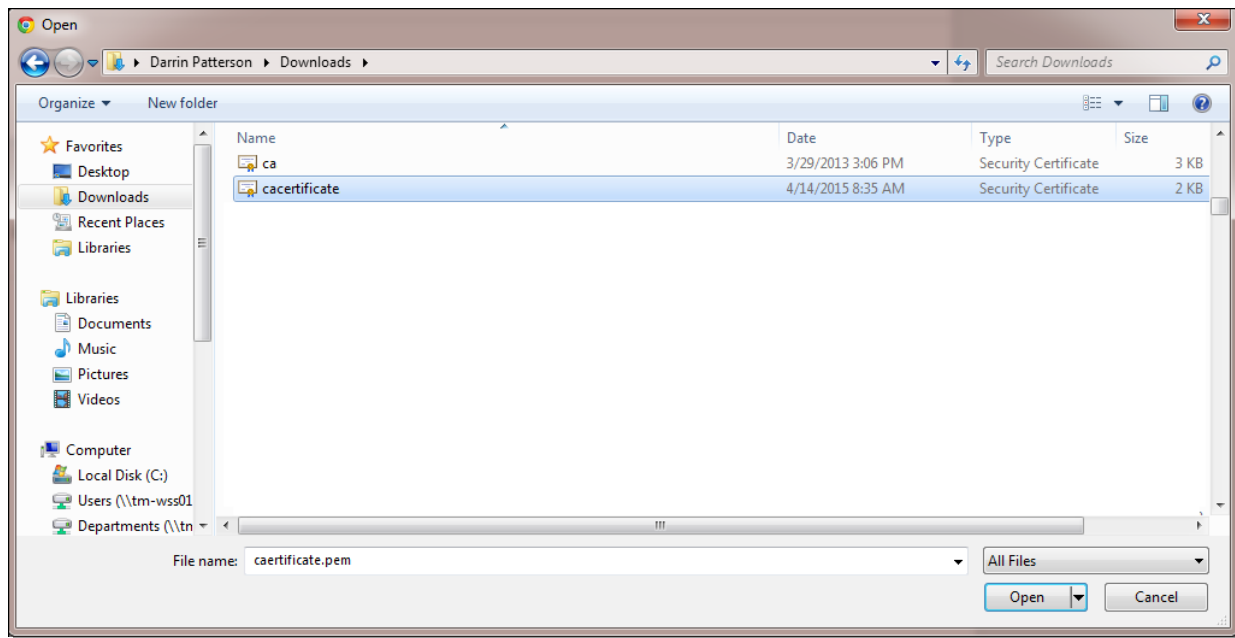
3. Select Network.



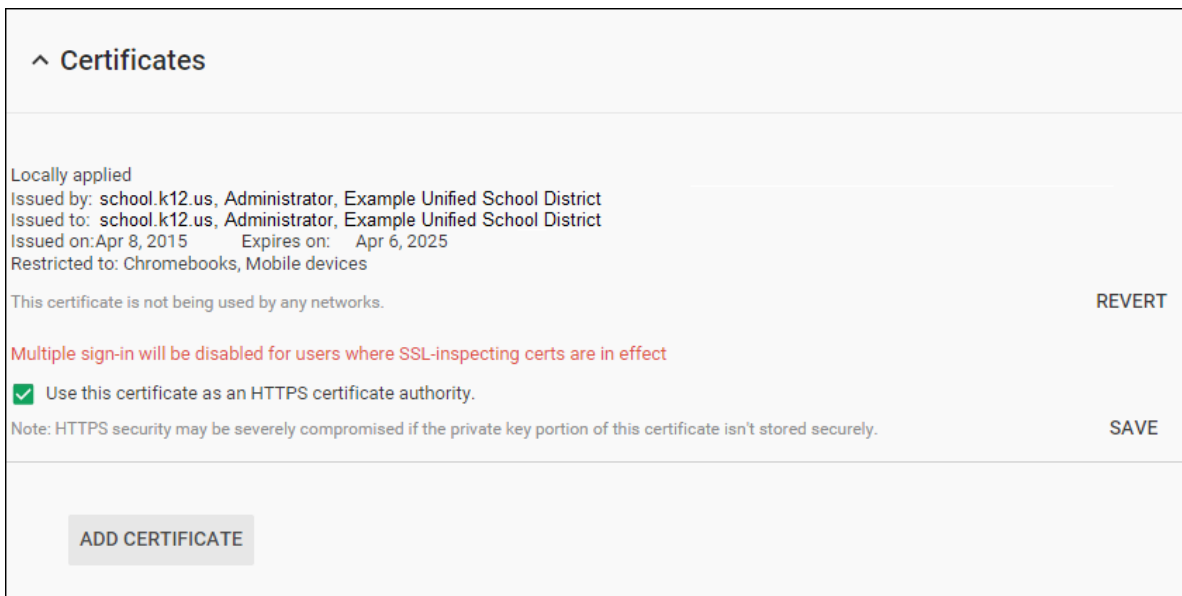
4. Select Certificates.



5. Select Add Certificate > Choose File.



6. We recommend the PEM file extension for Google Admin Console
7. Select the certificate file and click Open.
8. Check the box to Use this certificate as an HTTPS certificate authority.
9. Select Save.



10. Certificate will show as Certificate Authority.

^ Certificates

Certificate is marked as an HTTPS certificate authority

Locally applied

Issued by: school.k12.us, Administrator, Example Unified School District

Issued to: school.k12.us, Administrator, Example Unified School District

Issued on: Apr 8, 2015 Expires on: Apr 6, 2025

Restricted to: Chromebooks, Mobile devices

This certificate is not being used by any networks.

Multiple sign-in will be disabled for users where SSL-inspecting certs are in effect

☒ Use this certificate as an HTTPS certificate authority.

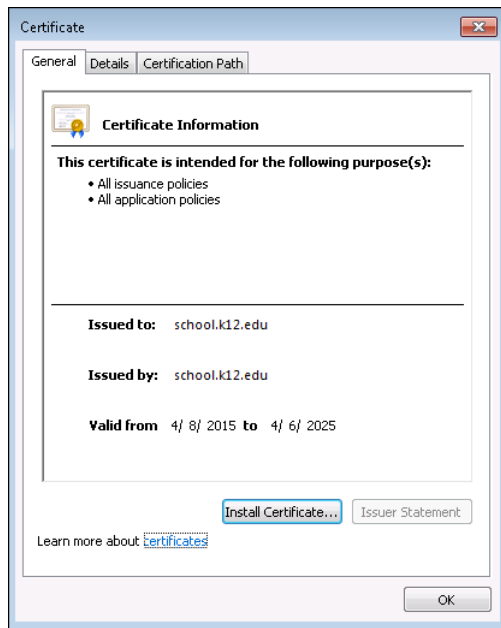
REVERT

ADD CERTIFICATE

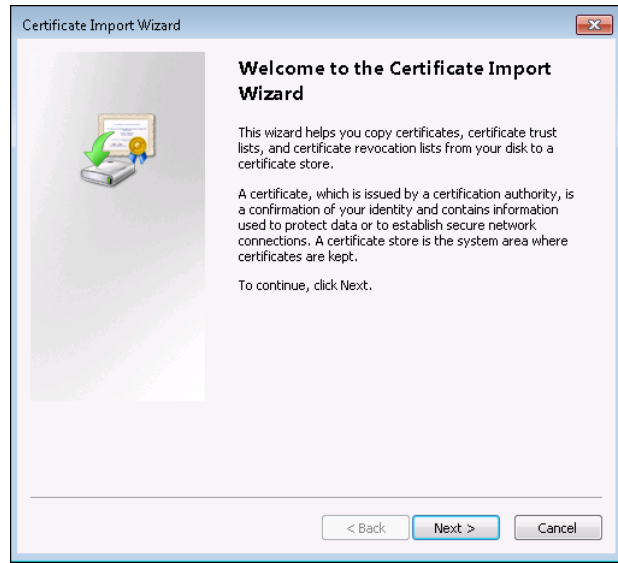
Deploying the CA Certificate Manually

Import CA Certificate in Windows 7 and 8

7. Ensure that you are logged in as an Administrator before proceeding.
8. Double click the downloaded certificate.
9. Select Install Certificate.

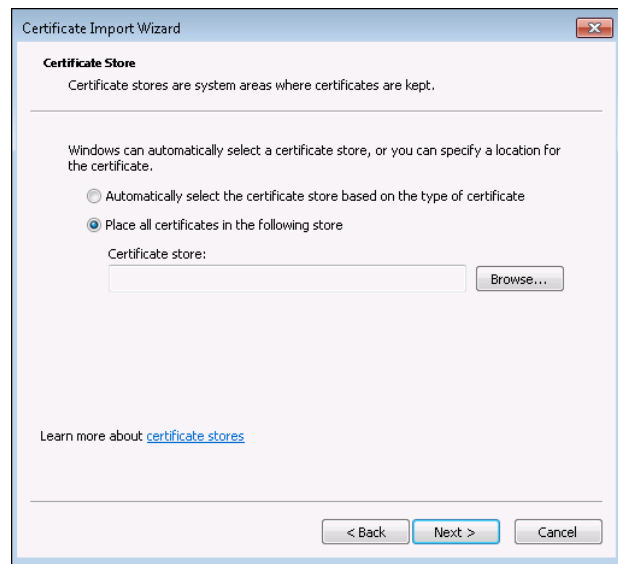


10. This brings up certificate import wizard. Select Next.

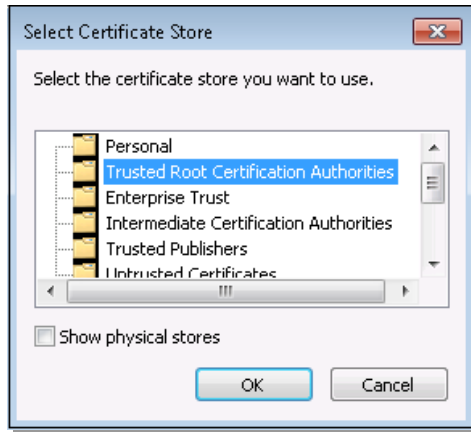


11. Select “Place all certificates in the following store”.

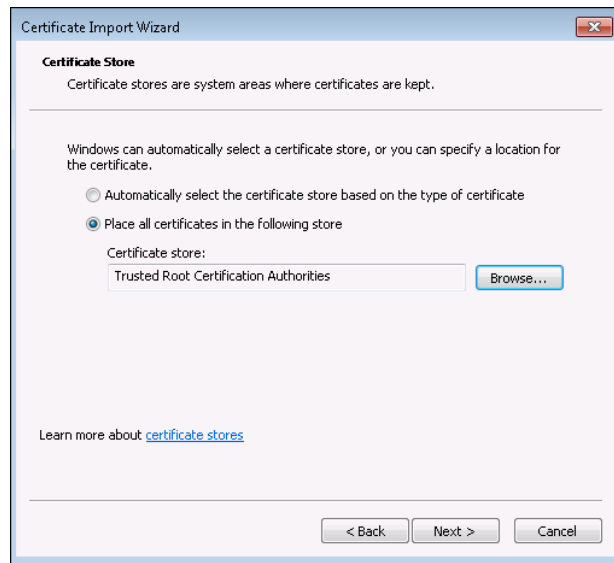
12. Select browse.



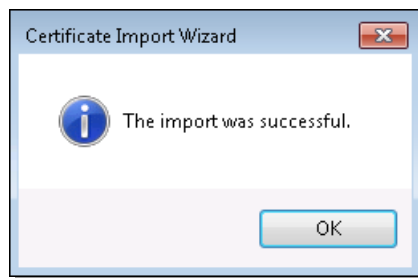
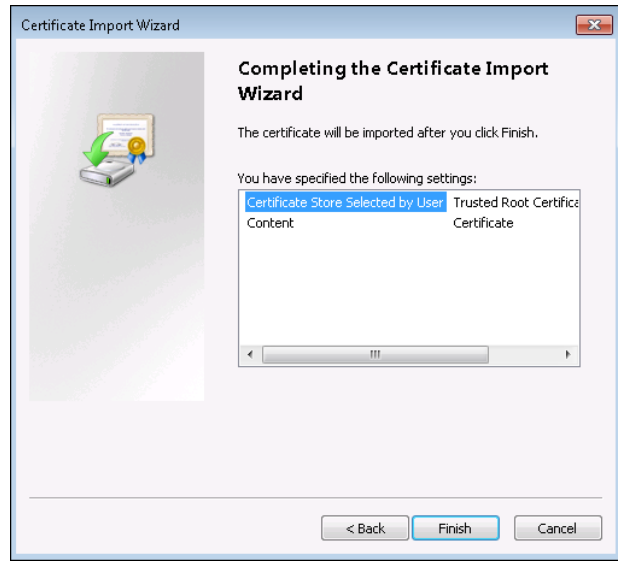
13. Select “Trusted Root Certification Authorities”.



14. Select Next to continue.

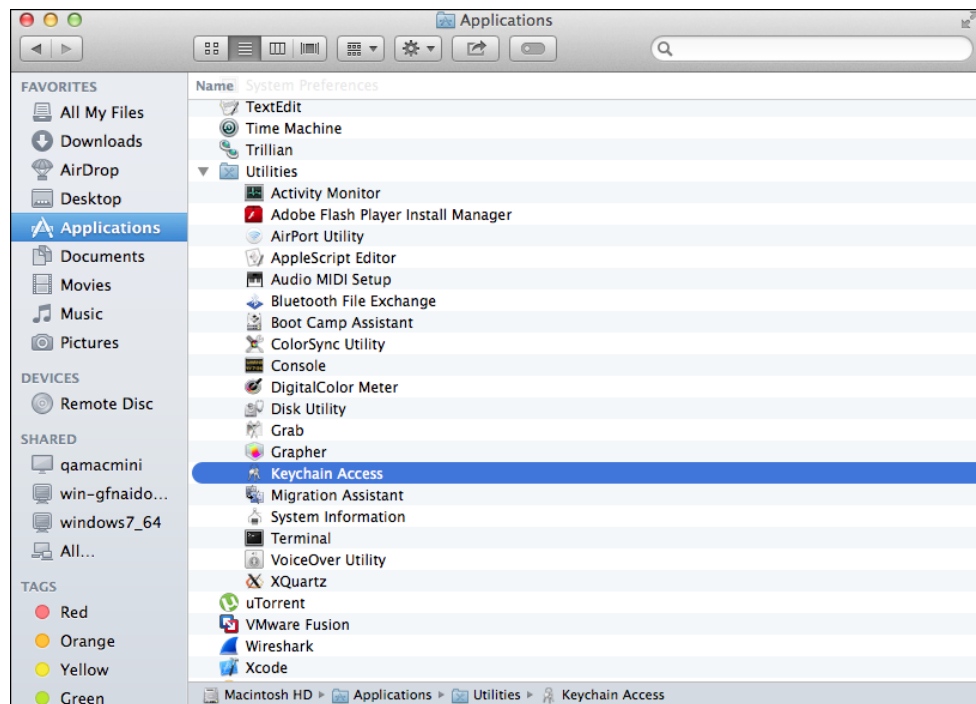


15. Select finish to run the import.

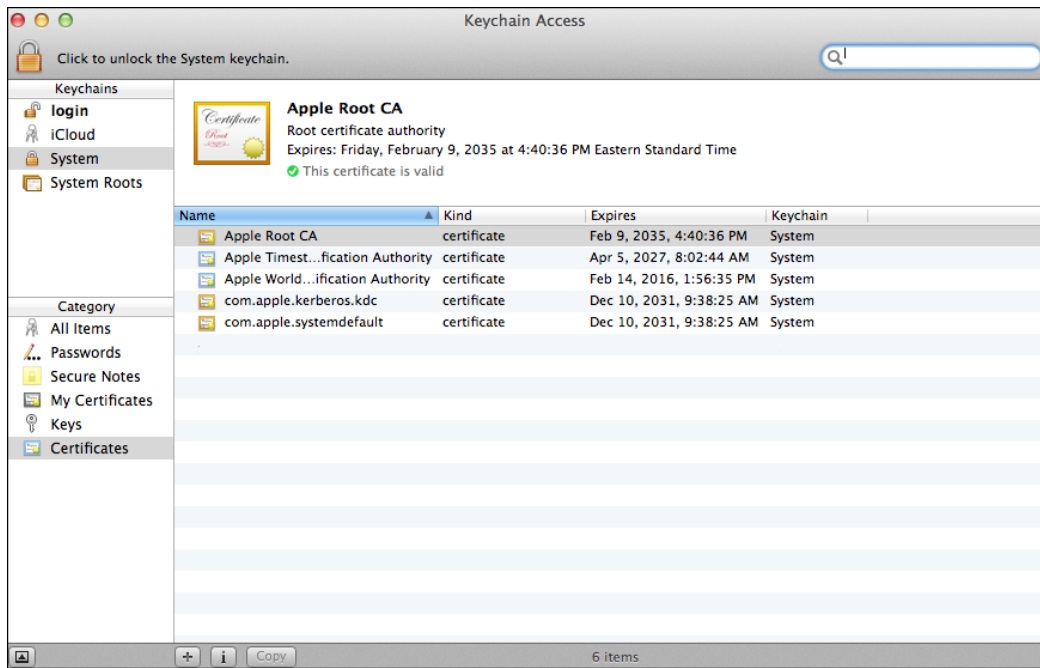


Import CA Certificate in macOS

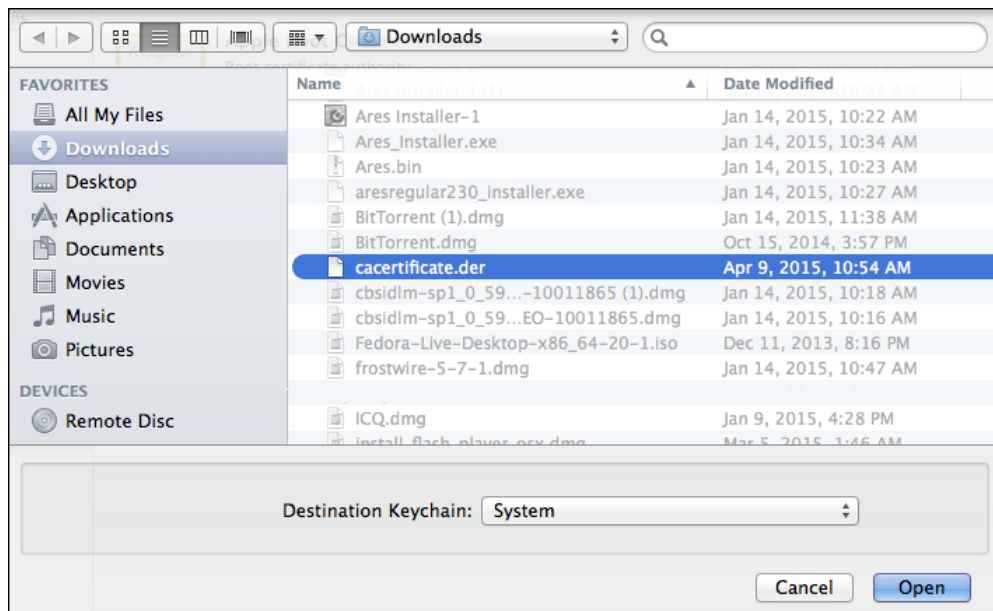
- From Applications > Utilities select Keychain Access.



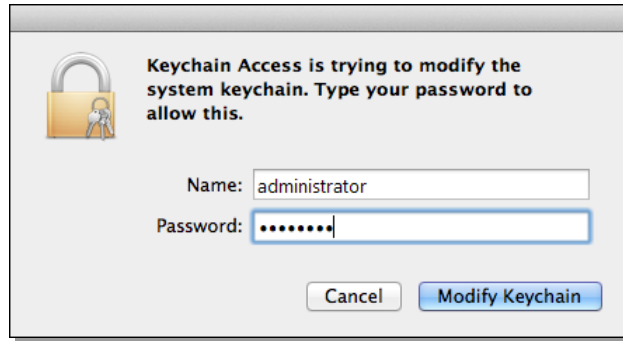
2. Select the Lock to unlock system keychain.
3. Enter the keychain password.



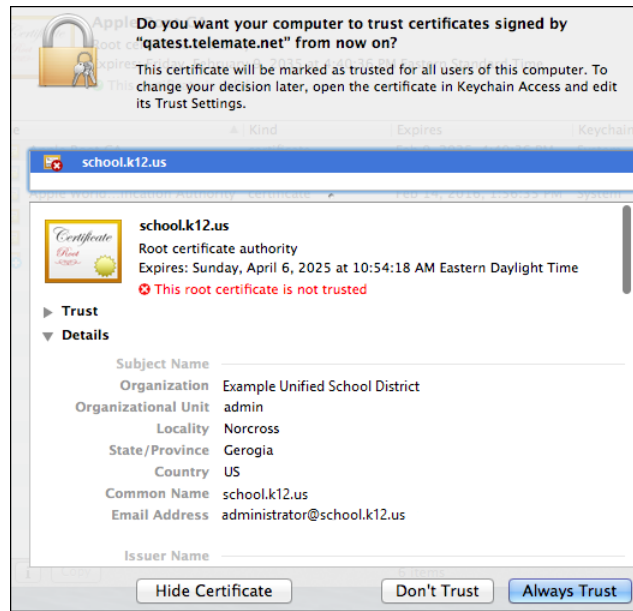
4. Go to File > import items.
5. Select the downloaded root CA with the destination System.



6. Enter the password to modify keychain access.



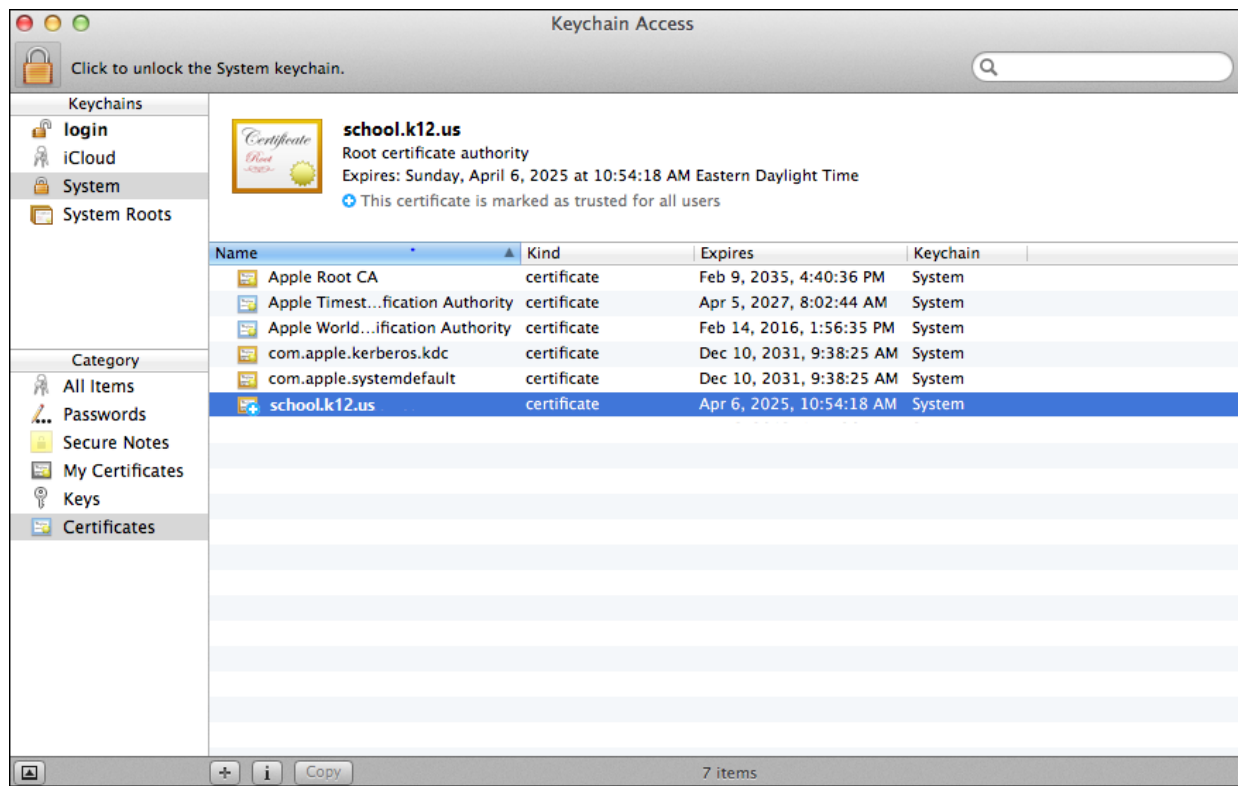
7. The certificate will be displayed. Select "Always Trust".



8. Enter the password once again.



9. Select the lock to close access to system keychain. You should see the newly added certificate.



Deploying the CA Certificate on Mobile Devices

Under Settings > Customization > Policy Reminder, you can customize the policy reminder page. You can now also enable a link to “Show CA Certificate Download and Install Instructions”. By enabling the Policy Reminder page in the Groups section, users will have to agree to your organization’s policy before surfing the internet. This page will now also show a link where users can download the certificate. If you wish to inspect SSL traffic on devices that log on your network, but are not owned by your organization, this page will be necessary for users to install the certificate.

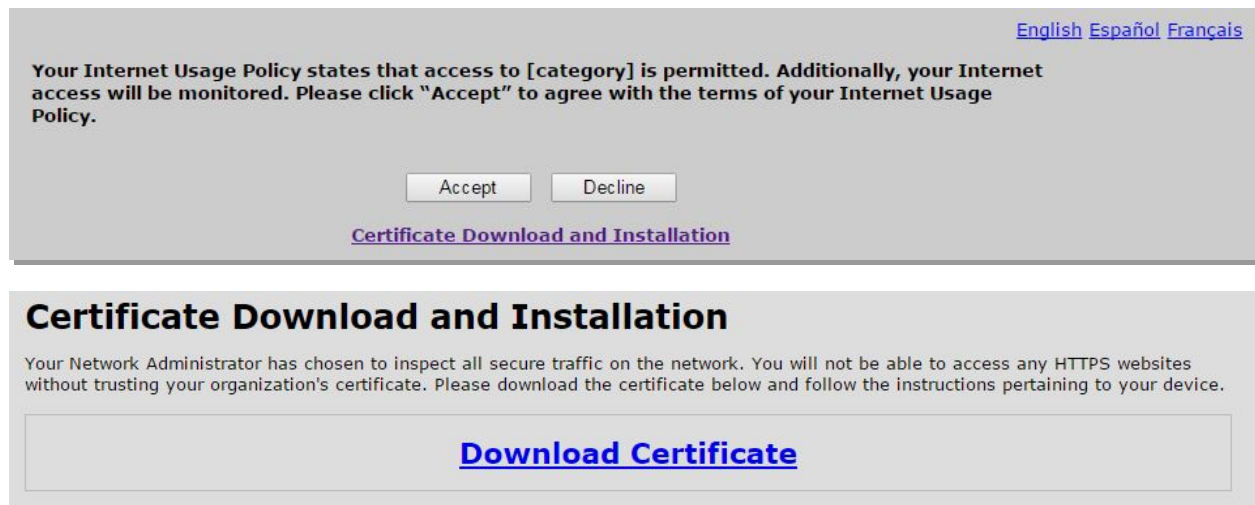
Policy Text

Group	Category	URL
Your Internet Usage Policy states that access to \${cat_name} is permitted. Additionally, your Internet access will be monitored. Please click “Accept” to agree with the terms of your Internet Usage Policy.		

Accept:
 Decline:

Certificate Download

☐ Show CA Certificate Download and Install Instructions



This Certificate Download and Installation page will also list simple instructions for Android, iOS, and Chromebook. The certificate on this page is in DER format with the .crt extension. This has been tested to be the preferred certificate for all three device types.

Import CA Certificate from Policy Reminder – Android

1. Click on **CA Certificate (DER)** and download the file.
2. You will be prompted to **Name the Certificate**. It is recommended to use the name of your school or organization. When you have entered a name, tap **OK**.
3. **IMPORTANT:** You may be prompted to set a lock screen PIN or Pattern set.
4. Tap **Done** to return to your web browser.

Import CA Certificate from Policy Reminder – iOS

- Click on **CA Certificate (DER)** and download the file.
- You will be prompted with the **Install Profile** screen. Click the **Install** button in the upper right corner.
- A warning message will appear. Click the **Install** button in the upper right corner.
- Click **Install Profile**
- Click **Done** in the upper right corner to return to Safari.

Import CA Certificate from Policy Reminder – Chromebook

- Click on **CA Certificate (DER)** and download the file.
- Open the Chrome browser and type **chrome://settings/certificates** into the address bar.

- Inside the **Certificate Manager** go to the **Authorities** tab and click on the "Import..." button at the bottom of the manager.
- Select **Google Drive** or **Downloads** to find the certificate file.
- **IMPORTANT:** If the file does not show up in either list change the file type filter at the bottom of the page to "All files" and search again.
- Select the certificate file and click on the **Open** button.
- Check the options to "**Trust this certificate for identifying websites**".
- Click the **OK** button.

Deploying the DNS Agent for Windows Servers

DNS Handling of Google Services

To improve the policy control of Google Services, updates have been made to the Remote Agents. These changes were made to dynamically pool DNS requests in order to prevent Google Services from tunneling over existing Google connections.

A simple example of Google's tunneling capabilities can be observed when Google uses the new HTTPS/2 protocol. A customer may want NetSpectre to force end users to only allowed domains for Google Apps such as mail.google.com, plus.google.com, and www.youtube.com that now use the same connection.

The DNS Agent would force these shared connections to decouple, allowing NetSpectre to manage each connection normally. Without the decoupling of these shared connections, we would not be able to properly manage connections going to these services and enforce related features.

Deploying the Agent

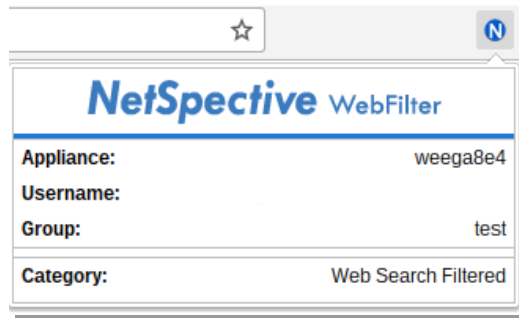
The agent download can be found under Authentication > [Agent Downloads](#)

The DNS Agent for Windows Servers is installed on the primary DNS server to add and maintain entries to the local DNS for Google services. This service can be used to segregate Google services for SSL decryption, enforce Safe Search, and restrict YouTube search settings. Once the service is installed, several new zones will appear in your DNS server to override the IP addresses for Google Services. The managed zones will be removed if you choose to uninstall the program.

Since this program runs as a service, there is no user interface. You can start and stop this service in the Control Panel --> Services. There is a self-explanatory configuration file available in C:\Program Files\DNS Agent\GlobalSettings.conf.

The NetSpective WebFilter Extension for Chrome

The NetSpective WebFilter Extension for Chrome was designed to filter Chromebooks both on or off campus. This suits the most common Chromebook deployments which are one-to-one initiatives, and on campus deployments where multiple users may use a single Chromebook.



NetSpective WebFilter Extension for Chrome filters browser traffic without the use of a proxy server.

Unlike the NetSpective Remote Agent for Windows and macOS, the Extension runs inside the Web Browser and will enforce policy on traffic before SSL encryption. However, it does not filter traffic from the ChromeOS Services and Chrome Apps such as locally installed games.

As of 5.3.0, the Chrome Extension fails OPEN in the event it cannot communicate with the NetSpective.

Prerequisites

There are several steps that should be performed before deploying Extension for Chrome. Please review the following:

1. The Chrome Extension requires a fully licensed and updated NetSpective appliance.
2. Assign a hostname to NetSpective in your DNS servers, e.g., webfilter.example.com. Google requires a valid Internet hostname so don't use .local domains.
3. If you are planning to filter your Chromebook off campus. It will be necessary to configure your Firewall Rules for inbound traffic to the NetSpective appliance on TCP port 8443. The DNS name for your appliance must be accessible from both inside and outside of your network.
4. Install an SSL Certificate on the appliance. The certificate cannot be a self-signed certificate. It must be signed by a public Certificate Authority (CA) or recognized as a valid CA by all of the devices in your network and Chromebooks.
5. Verify that NetSpective has the correct time. In the Device Settings > Advanced > System Time section, set the local time zone, and then press *Test NTP Server* to assure your appliance has

connectivity to a timeserver. A valid test will display "NTP Server Test OK." If you do not receive this message, consider changing the server IP address to a local NTP server or check your firewall rules.

6. You must have access to the Google Admin Console, <https://admin.google.com>, for your domain.
7. The Google's consoles work best with the Chrome web browser. You may download and install the Chrome web browser from <https://www.google.com/chrome/browser/desktop/index.html>.

Preparing for the Deployment

In the NetSpective Web Administration, navigate to Authentication > Extension for Chrome

Appliance Addresses - Extension for Chrome	
To ensure that your chrome agents behave correctly on all of your networks, enter the internal and external addresses for all of your NetSpective appliances. The default protocol is https and the default port is 8443, but it may be different for external addresses if you use port mapping.	
Address	
<input type="checkbox"/>	https://webfilter.yourdomain.org:8443

Settings - Extension for Chrome	
Cache Timeout:	3 Minute(s)
<input checked="" type="checkbox"/>	Block Notifications: Display when a blocked request does not result in a full page redirect, i.e., advertisements were blocked.
<input type="checkbox"/>	Image Replacement: Display the block image when an image request would result in a block redirect. i.e. image web search results.

Exemptions - Extension for Chrome	
Extension for Chrome has the option to ignore all accesses to the specified addresses.	
Hosts	
<input type="checkbox"/>	http://coolmath.com/
<input type="checkbox"/>	https://www.khanacademy.org/

Appliance Addresses – Extension for Chrome, select the Add button on the far right to add the Internal and External addresses of all your NetSpective appliances, one address at a time. Normally in the format of <https://webfilter.example.com:8443>. The hostname of the appliance(s) must match the SSL certificate installed on each appliance and have corresponding DNS entries.

Settings – Extension for Chrome, configure the behavior of the Chrome Extension. The Cache Timeout reduces communication between the Chrome Extension and the NetSpective by caching the last known policy for the user. The extension can then perform blocks and allows without asking the NetSpective for a policy check for each access. The default setting is 3 minutes, and we recommend opening a discussion with NetSpective Support before changing this value.

Notifications for Blocks – If you are surfing web content and parts of a webpage are being blocked, but the full page is not being blocked, the Chrome Extension can display a notification. This notification simply tells you a block occurred and the corresponding category.

Image Replacement – If images on a page are being blocked and filtered, checking this option will replace the blocked image with the NetSpective block icon.

Exceptions – Extension for Chrome, you can add URLs for websites that are allowed here. These exceptions will not be processed by the Chrome Extension and will go through the browser untouched.

When you are finished, click the download button at the top right and save the **appliances.json** file. This file will be used when Deploying the Chrome Agent.

Note: Each time you choose to add or edit these settings, you must download this file, and then update Google Admin Console.

Deploying the Extension for Chrome

The Chrome Extension like any other Chrome app can automatically installed (or force-install) on all of your Chromebooks through the Google Admin Console. Through this method, users will not be able to remove the extension from their account. If you would like additional information, please visit Google's support article for automatically installing apps.



<https://support.google.com/chrome/a/answer/6306504?hl=en>

Setup

Before you can force-install apps or extensions for your users, you need to turn on their **Chrome Web Store** service in your Admin console. You can find this service in your Admin console by going to **Apps > Additional Google Services**. For detailed steps, see [Turn Additional Google Services on or off](#).

Force-install the Extension for Chrome

1. Sign into the Google Admin console at <https://admin.google.com/>.
2. From the Admin console dashboard, click **Device Management**.
3. On the left, click **Chrome management**.
4. Click **App management**.
5. In the Find or Update Apps section, cut and paste the App ID shown below into the search field, and then press the Search button.
ID: plojahkfikogcannonlnbdajiljjhpid
6. Select the category of settings you want to configure:
User settings: Force-install the item for users who sign in with an account in your domain.
Public session settings: Force-install the item for users who sign in to a public session on your devices.

7. In the **Orgs** section on the left, click the organizational unit where you want to force-install the item. To install items for everyone your organization, select the top-level organizational unit.
8. Under **Force Installation**, click  to turn the setting on .
Note: If you're force-installing an item for a child organization, the force install setting might be inherited from the top-level organization. Click **Override** to change the setting from its parent. For more information, see [How the organizational structure works](#).
9. Under **Configure**, select **UPLOAD CONFIGURATION FILE**. Navigate to the appliances.json file you downloaded in the previous section.
10. Click **Save**.

Force-installing an app or extension gives it permission to access information on the device it's installed on.

Disable Incognito Mode and Developer Tools

To avoid user tampering with the operation of the Extension for Chrome, please disable Incognito Mode and Developer Tools options on the Chromebooks.

1. Sign in to the Google Admin console at <https://admin.google.com/>.
2. From the Admin console dashboard, click **Device Management**.
3. Under **DEVICE SETTINGS**, click **Chrome Management**.
4. Click **User Settings**.
5. Select the proper OU for your users.
6. Under the **Security** heading, locate the **Incognito Mode** option and then select **Disallow**.
7. Under the **User Experience**, locate **Developer Tools** option and then select **Never allow the use of built-in developer tools**.
8. Click **Save**.

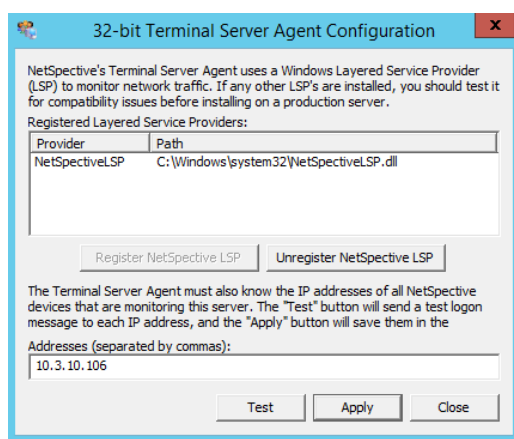
Deploying the NetSpective Terminal Server Agent (Inline/Passive)

The NetSpective Terminal Server Agent can be found on the NetSpective appliance under Utilities. The Terminal Server Agent consists of a configuration utility and a Winsock Layered Service Provider (LSP) module. LSPs are used by anti-virus, anti-spam, and anti-spyware vendors to scan and block harmful data in connections. The NetSpective LSP intercepts the initiation of TCP sessions to inform NetSpective about connection ownership. Please install NetSpective Logon Agent for Terminal Server on every Terminal Server in your network to provide personalized filtering policies for all of your users.

Note: If NetSpective is off-line or fails to respond, a terminal server user might experience a three second delay when starting a network application. If the NetSpective device fails to respond, the users will be subject to the group policy for the Terminal Server's IP address.

The Configuration Utility

This utility shows you what LSP's you currently have registered and allows you to register or unregister the NetSpective LSP. You must also enter the IP addresses of all NetSpective devices monitoring the current server's connection to the internet. If you add, remove, or change the IP address of a NetSpective device on your network, you need to run this utility to update the IP addresses. You are not required to reboot after making this change. However, if you choose to register or unregister the NetSpective LSP, it is necessary to reboot the server.



IP Addresses are examples only.

If you do encounter conflicts with another Layered Service Provider, we provide a command-line utility for trouble-shooting, installing, and removing LSP's. By default, it is installed here:

1. Utility: \Program Files\NetSpective Logon Agent\LSPInstall.exe
2. Documentation: \Program Files\NetSpective Logon Agent\README.TXT

Windows Server 2003 / 2008 (x86-64)

The current release of NetSpective LSP supports both 32-bit and 64-bit applications. If your server is 64 bit, you must still register the 32 bit LSP as well.

Logon Agent (Inline/Passive)

The NetSpective Logon Agent is an executable used to map an authenticated user name to one or many IP addresses assigned to the device accessing the network. The Logon Agent sends packets over UDP to a corresponding processing application on the NetSpective appliance. This creates a Username to IP Address association inside of the appliance. When NetSpective sees traffic on the wire, it is able to see the IP addresses of those users and associate it with their group and apply the content filtering policy. Different editions of the logon agent exist for Windows and macOS.

The logon Agent has multiple modes of operation, each of which can be tailored using simple command line arguments. Flexible options enable administrators to customize the behavior of the application including executing and terminating immediately where NetSpective processes the information with minimal overhead and no network burden generated by the application. Persistent modes of execution also exist for dynamic handling of mobile devices in DHCP environments.

All Logon Agent and Remote Agents send packets over UDP to a corresponding NetSpective appliance. Since NetSpective processes the information with minimal overhead, the network will not be burdened with the traffic generated by the application.

Method 1 - Deploying the NetSpective Logon Agent for Windows 7 Workstations and Later

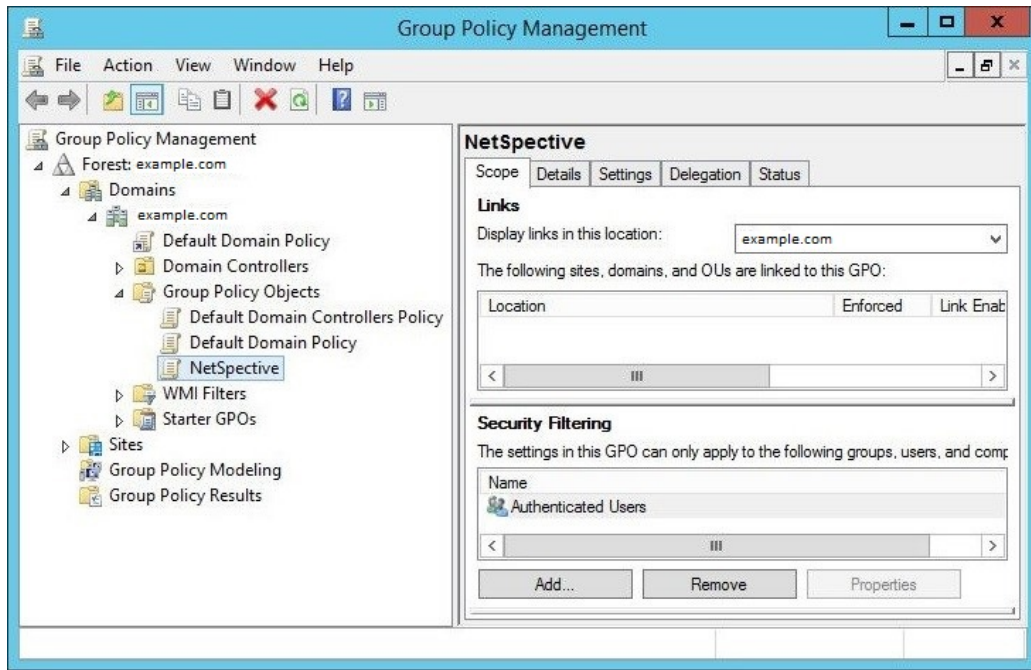
The steps below outline the process for configuring Microsoft Active Directory to store the Logon Agent on the user's local machine. The Logon Agent will then be run locally at startup instead of being downloaded from the domain controller.

The following steps are the same for Microsoft Active Directory 2008 and later

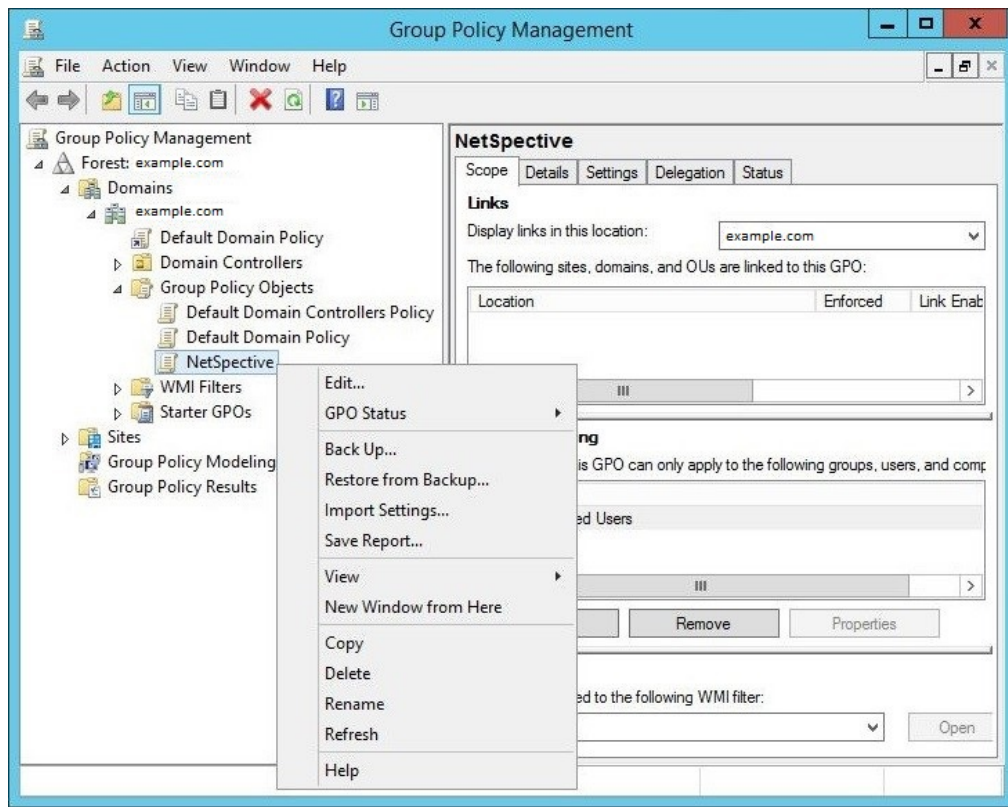
1. Begin by accessing the NetSpective Administrative Web Interface. Navigate to the Authentication > Downloads section and select to download the Logon Agent for Windows Domain Controllers (LogonAgent.zip). Once downloaded, unzip the contents of the zipped 'LogonAgent' folder to a location that is accessible from the Windows server.

Agent Downloads		
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
Terminal Server Agent for Windows & Citrix	3.0.4	TerminalServerAgent.exe
Logon Agent for Windows (XP, 7, 8, 10)	3.0.11	LogonAgent-3.0.11.zip
Logon Agent for macOS (10.9 - 10.12)	2.3-14	LogonAgent-2.3-14.dmg
Remote Agent for Windows (7, 8, 10)	1.5.48	RemoteAgent-1.5.48.msi
Remote Agent for macOS (10.9 - 10.12)	2.3.3	RemoteAgent-2.3.3.dmg
Remote Agent Configuration File	20161106060858	Configuration
Wi-Fi Agent	N/A	Contact NetSpective Support

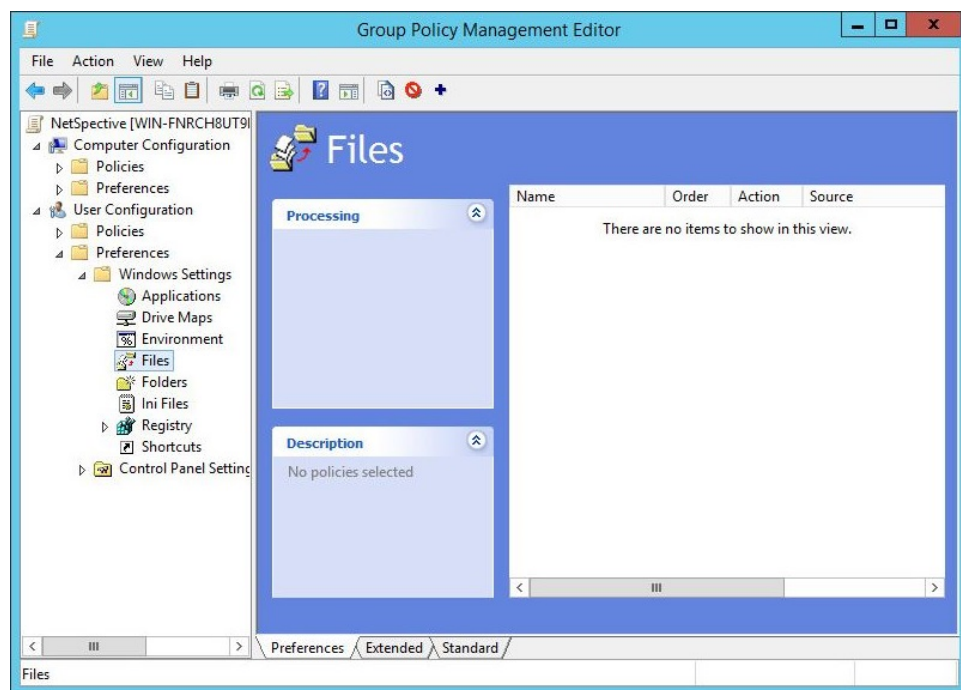
2. Open Group Policy Management and click on your Logon Agent GPO. In this example, the GPO is named 'NetSpective'



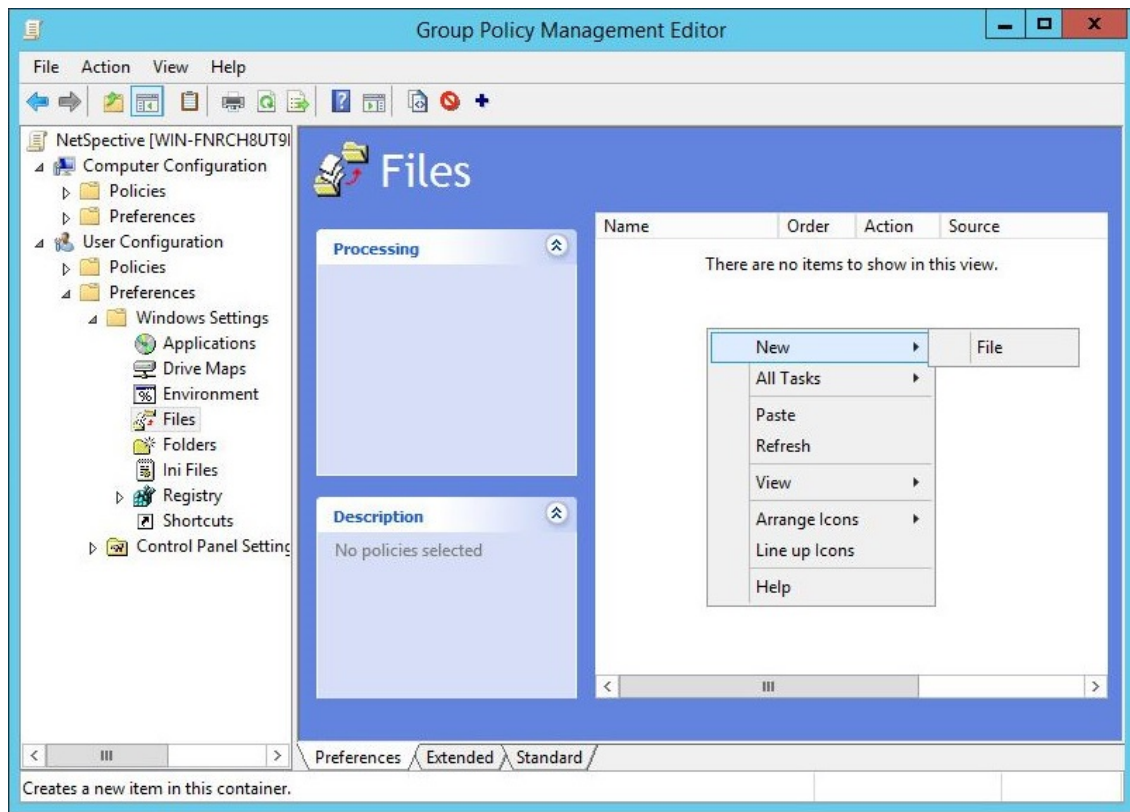
3. Right click your Logon Agent GPO and click Edit



- In the Group Policy Management Editor, navigate to:
User Configuration > Preferences > Windows Settings > Files



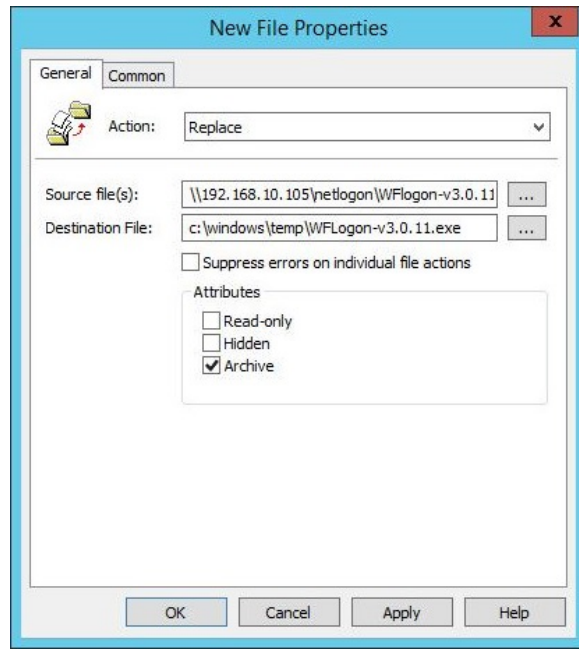
- In the right pane entitled Files, right click and select New > File



1. From the Action menu, select Replace

In the field for Source Files, select the full path of the Logon Agent on your server.

In the field for Destination File, select the path you want the Logon Agent to run from on the Local Machine. This replaces the need for the '-c' parameter seen in the logon script. This step forces the Logon Agent to be copied to the local machine's temp folder and we will execute the logon agent from that folder. In our example we are copying the logon agent to 'c:\windows\temp\' with the full file name of the logon agent.

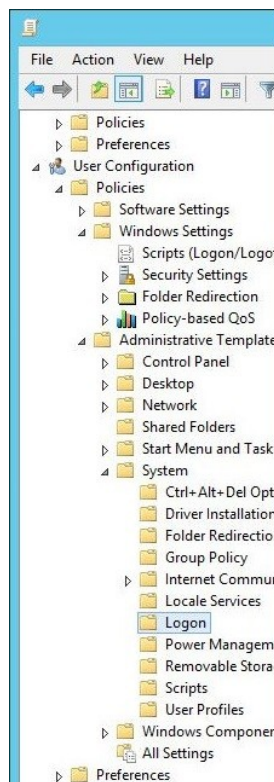


Example Logon Agent file name is WFLogon-v3.0.11.exe. Your Logon Agent file name may be different and must be specified in this field.

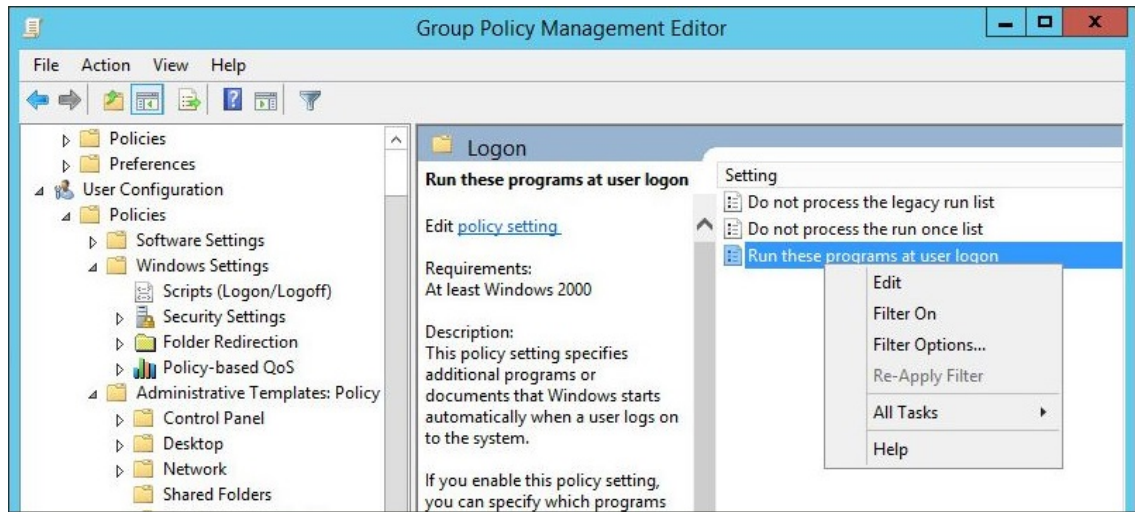
When you are finished, click the OK button.

2. Navigate to:

User Configuration > Policies > Administrative Templates > System > Logon

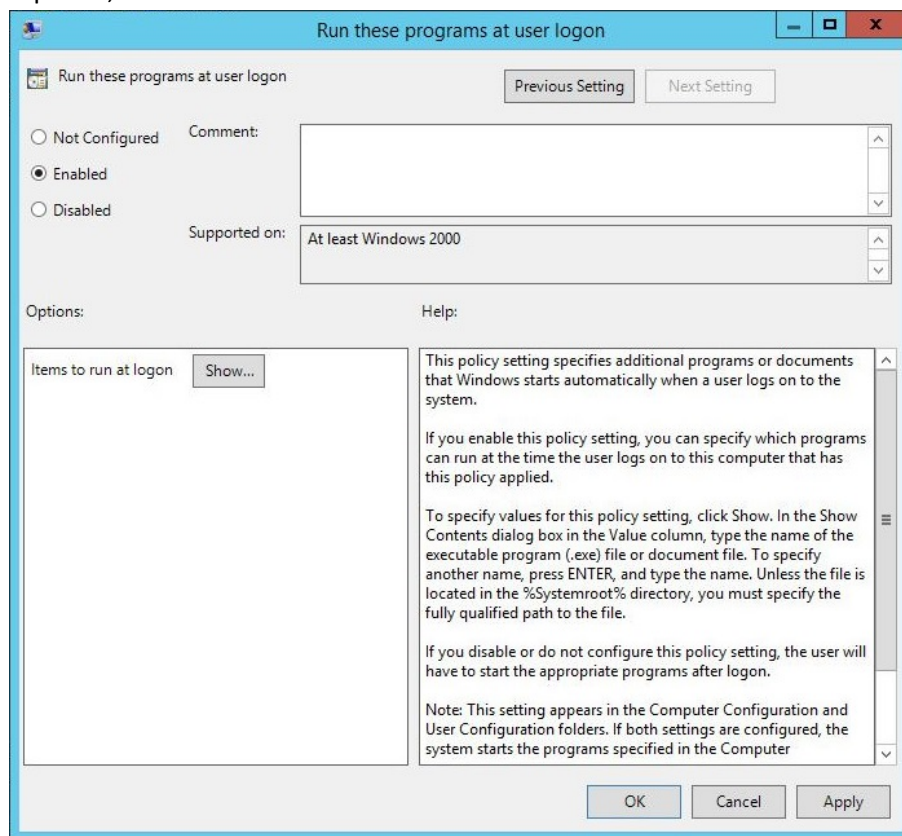


1. In the right pane, right click “Run these programs at user login” and select Edit.



3. In the new windows, select Enable.

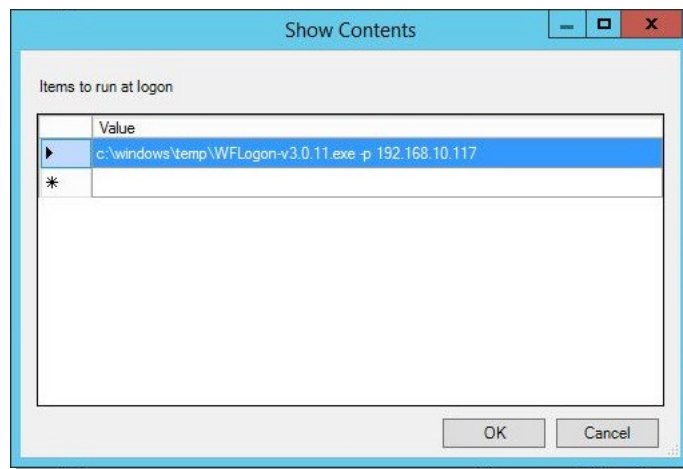
Under Options, click the Show button



4. Enter the value for the full Logon Agent path on the Local Machine. This is the same path you selected in step 5. This value should also include any Logon Agent parameters you wish to use, as well as the IP addresses of your NetSpective appliances.

The '-s' Silent flag hides the persistent application from the Windows systray icon.

Example: `C:\windows\temp\WFLogon-v3.0.11.exe -s 192.168.10.117`



When you are finished, select OK.

Note: If you are running multiple appliances in replication mode, the addresses of both appliances should appear in the logon script, separated by a space.

5. This completes the setup process for the Windows Logon Agent. Once the policies have replicated, the Logon Agent should be running on domain machines. You can typically see WFLogon.exe running in task manager.

If the Logon Agent is not running on some machines, see the Troubleshooting section of this guide.

Method 2 - Deploying the NetSpective Logon Agent using WFCall.bat

Active Directory relies on the Domain Name Service (DNS) to provide Group Policy access. This may require installing DNS on the domain controller and configuring the client systems so that they use the controller as their DNS server. Consult the appropriate documentation on Active Directory from Microsoft for more details.

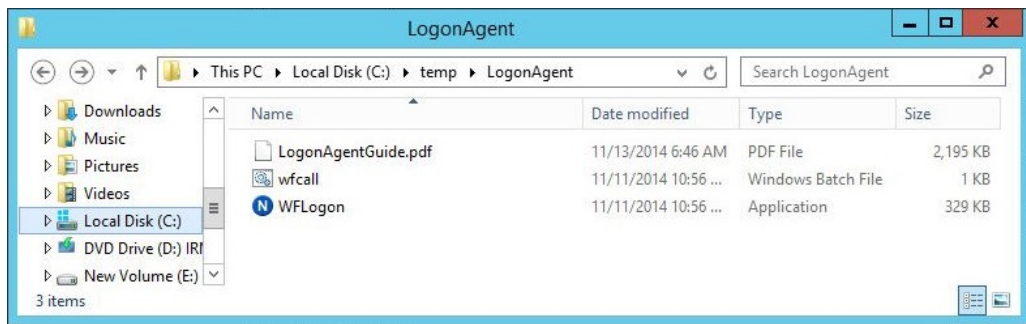
The following steps are the same if you are using Microsoft Active Directory 2008 and 2008 r2

1. Begin by accessing the NetSpective Administrative Web Interface. Navigate to the Authentication > Downloads section and select to download the Logon Agent for Windows

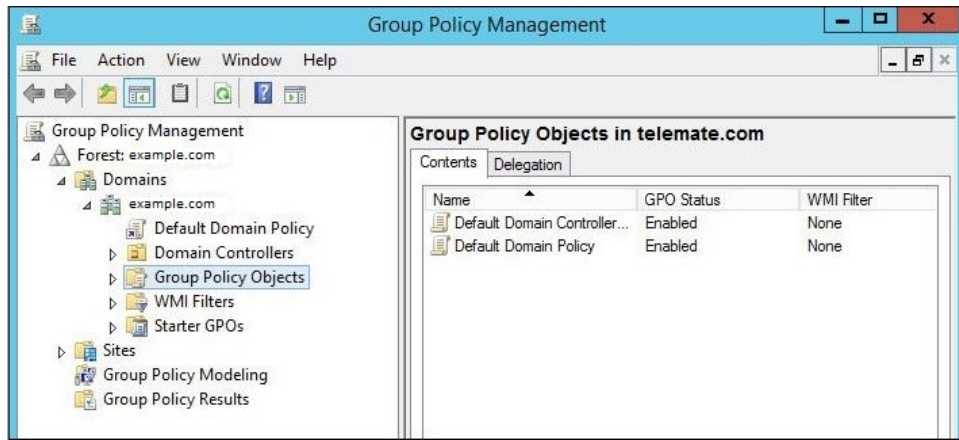
Domain Controllers (LogonAgent.zip). Once downloaded, unzip the contents of the zipped 'LogonAgent' folder to a location that is accessible from the Windows server.

Agent Downloads		
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	3.0.11	LogonAgent.zip
Logon Agent (Mac OS 10.6 - 10.7)	2.1-11	LogonAgent-2.1-11.dmg
Logon Agent (Mac OS 10.8 - 10.10)	2.3-13	LogonAgent-2.3-13.dmg
Remote Agent Client (Windows)	1.4.11	RemoteAgent.msi
Remote Agent Client (Mac OS 10.6 - 10.7)	1.1-96	RemoteAgent-1.1-96.dmg
Remote Agent Client (Mac OS 10.8 - 10.10)	2.1-15	RemoteAgent-2.1-15.dmg
Remote Agent Configuration File	N/A	Configuration
Wi-Fi Agent	N/A	Contact NetSpective Support

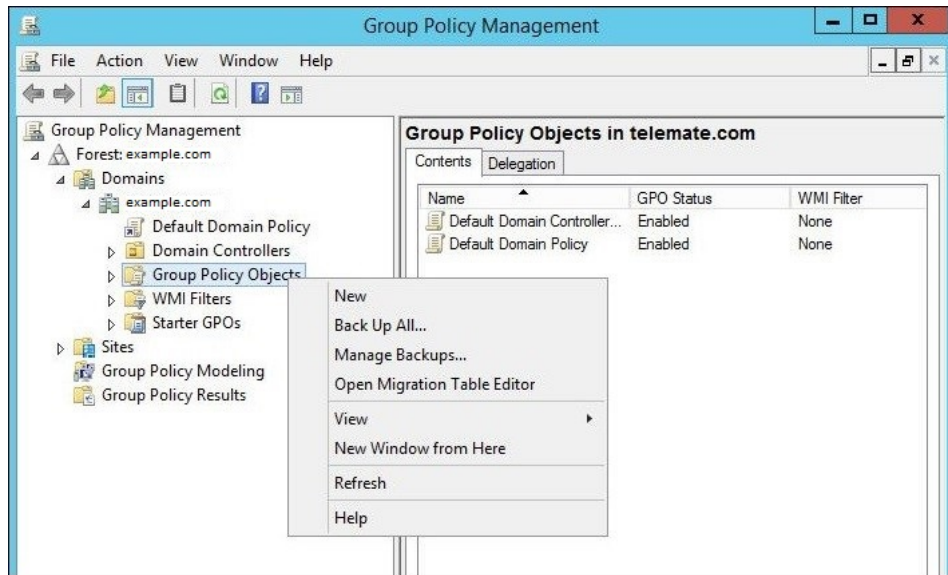
The LogonAgent folder contains several files. WFLogon.exe is the NetSpective application used to associates domain user names to machine IP addresses. WFLogon.exe has several command line parameters that may be used to tailor how the application executes and selectively define default values. WFCall.bat is a batch file that enables administrators to enhance the execution of the WFLogon.exe if required.



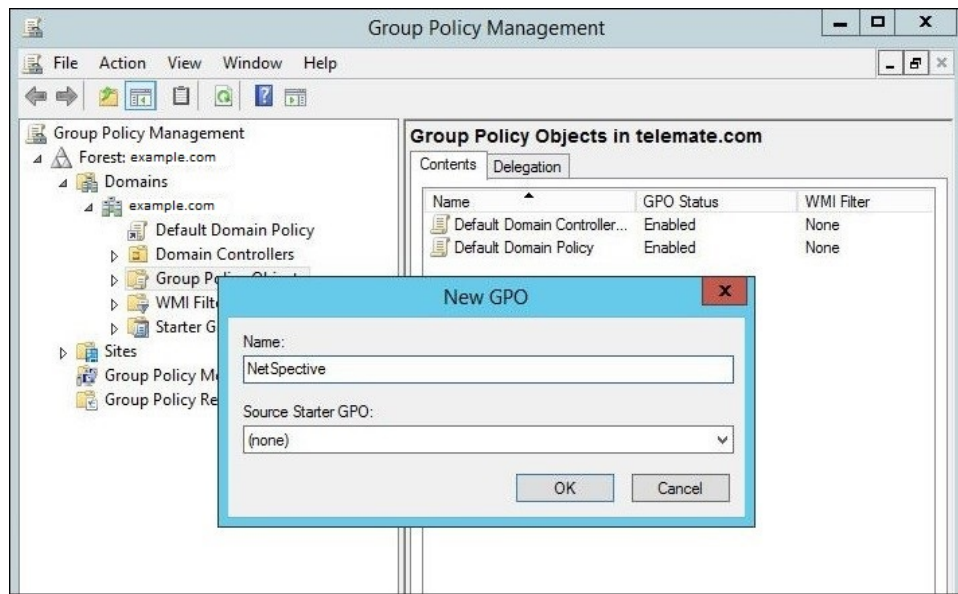
2. Next, access the Windows Server 2012 operating system and select Start, Programs, and Administration Tools, followed by Group Policy Management. Navigate down the domain listing. Select the domain where the users exist that you wish to bridge to the NetSpective Group(s).



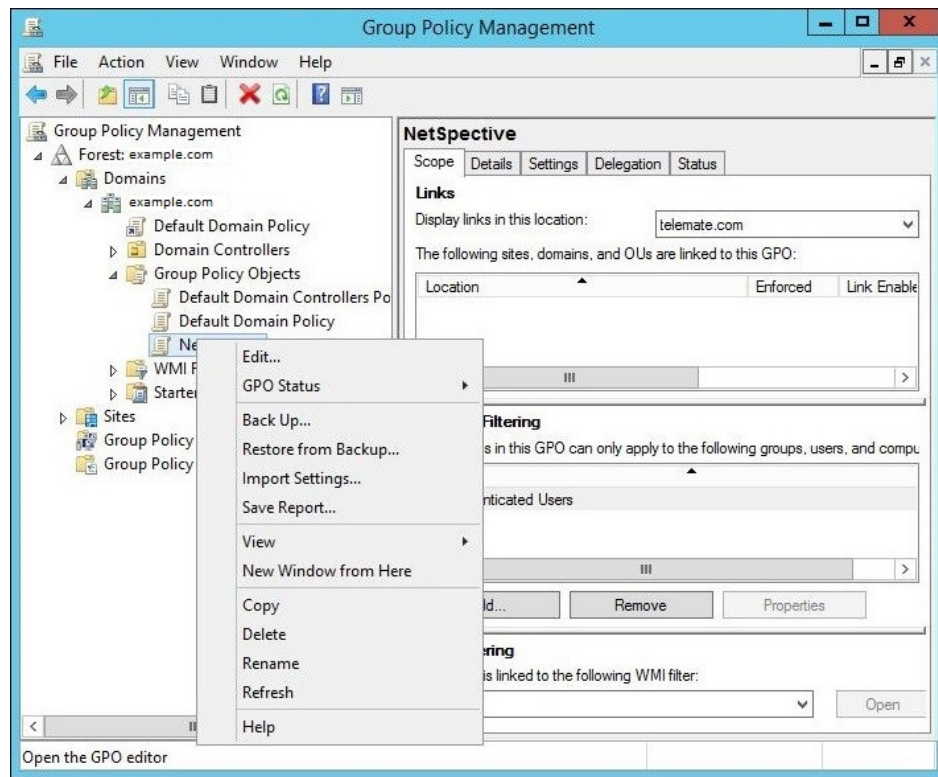
1. Right click on the 'Group Policy Objects' (GPO) and select 'New'.



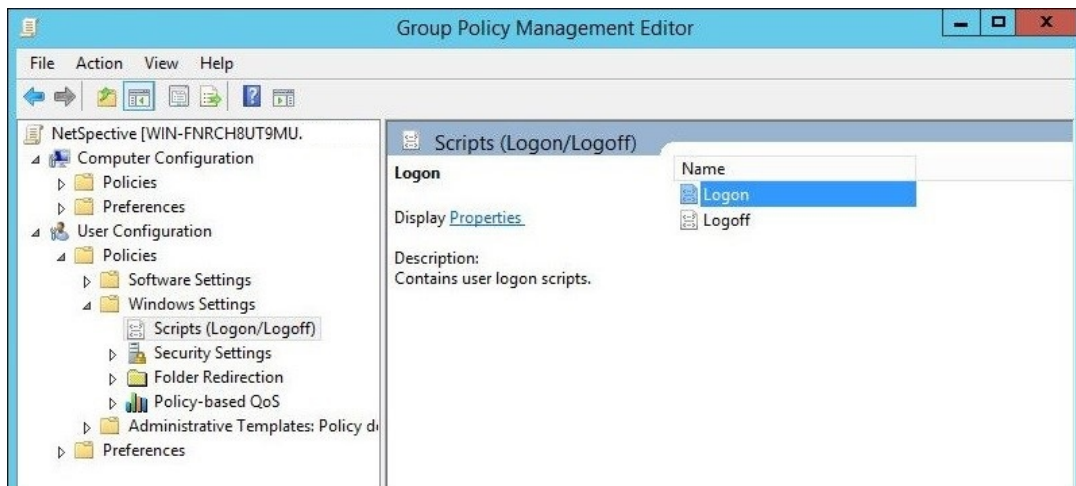
1. On the New GPO dialog enter 'NetSpective' or a descriptive name representing your internal naming conventions. 'Source Starter GPO' should remain as (none).



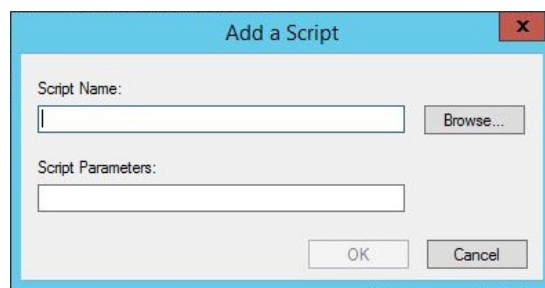
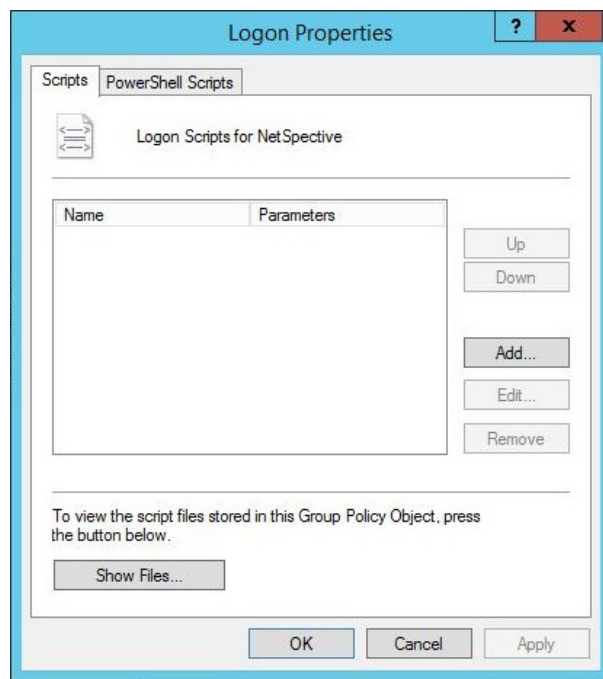
- Select the Group Policy Object tree items and navigate to the 'NetSpective' group policy object. Right click and select 'Edit'.



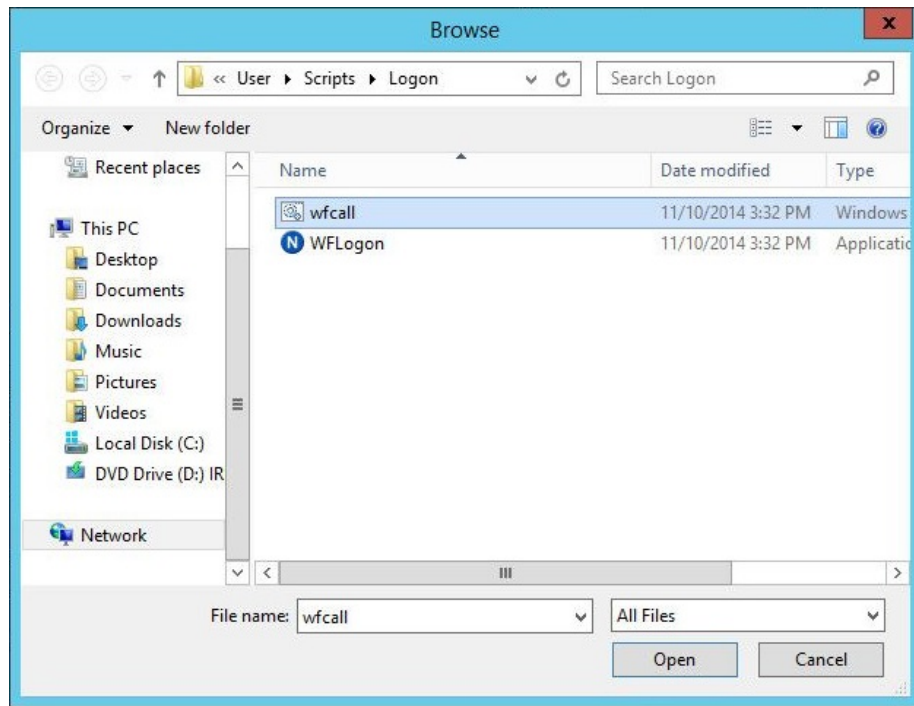
- Upon selecting Edit, the Group Policy Management Editor will open for the NetSpective GPO. Navigate to 'User Configuration', 'Windows Settings', 'Scripts (Logon/Logoff)'. Select 'Logon' script in the right pane of the editor.



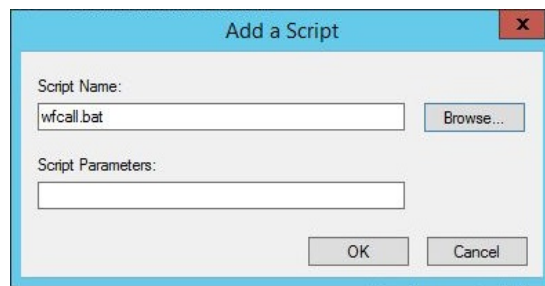
- Select the Logon script. Right click or double click to display the logon script properties and select the Add button.



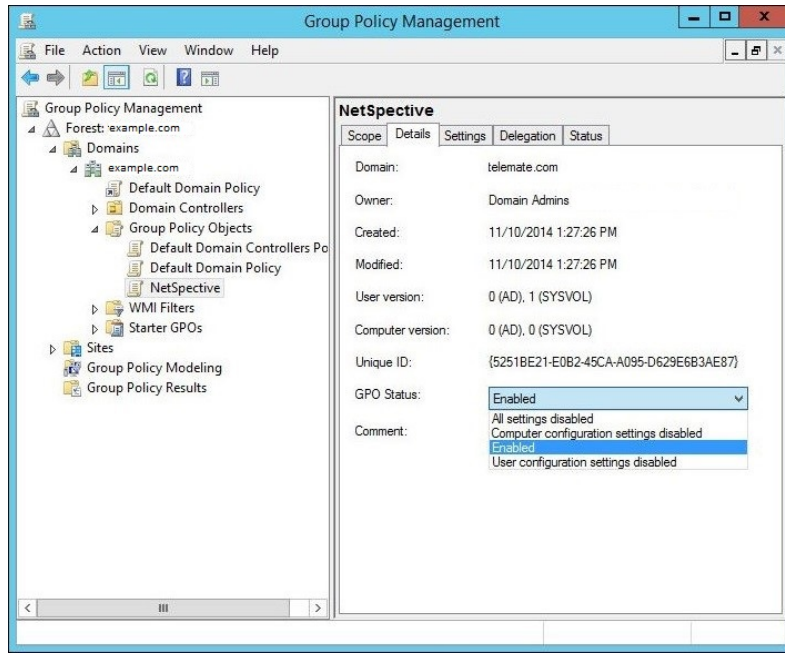
- From the 'Add a Script' Dialog, select Browse. Next access the folder you unzipped the LogonAgent.zip into from Step 1. Select and Copy both the WFLogon.exe and WFCall.bat into the default folder the Browse opens to. This folder is the folder for the NetSpective GPO.



- Select either the WFCall.bat or WFLogon.exe based on your requirements. Command line parameters are explained below under 'WFLogon Command Line Parameters'. Once defined select OK to save. Continue the save process until you have returned to the NetSpective GPO in the Group Policy Management dialog.



- Once you have returned to the NetSpective GPO, select the Detail tab to confirm (or set) the GPO status to 'Enabled'. Upon completion, exit the Group Policy Management.



- Now all users accessing the network will automatically execute the NetSpective logon Script executed based on the parameters provided.

Troubleshooting

1. Verify that the EXE is being copied to the correct local folder.
 - a. If not, attempt to verify that the current GPO settings have been applied to that machine, that the GPO is actually being applied to the test account, that it can read from the source folder, that it can write to the destination folder, etc.
 - b. Verify that the EXE is being launched automatically from the local folder.
2. If not, check the %TEMP% folder for a wflogon.log file. If it's not there, attempt to launch it manually from the Windows "Run" dialog (using the same command-line parameters), see if any errors/warnings pop up, etc.
 - a. Verify that the EXE reliably stays running through various scenarios and with anti-virus installed. Log out and back in, reboot and log back in, put it to sleep and wake it up, disconnect from the network, reboot, log back in, then reconnect to the network.
 - b. Hover the mouse icon over the blue icon and verify the IP addresses. Perhaps change the IP and make sure it gets updated properly.
 - c. Surf the web and make sure the traffic is attributed to the correct group and user in NetSpective Recent Activity.

Advanced Options: WFLogon Command Line Parameters

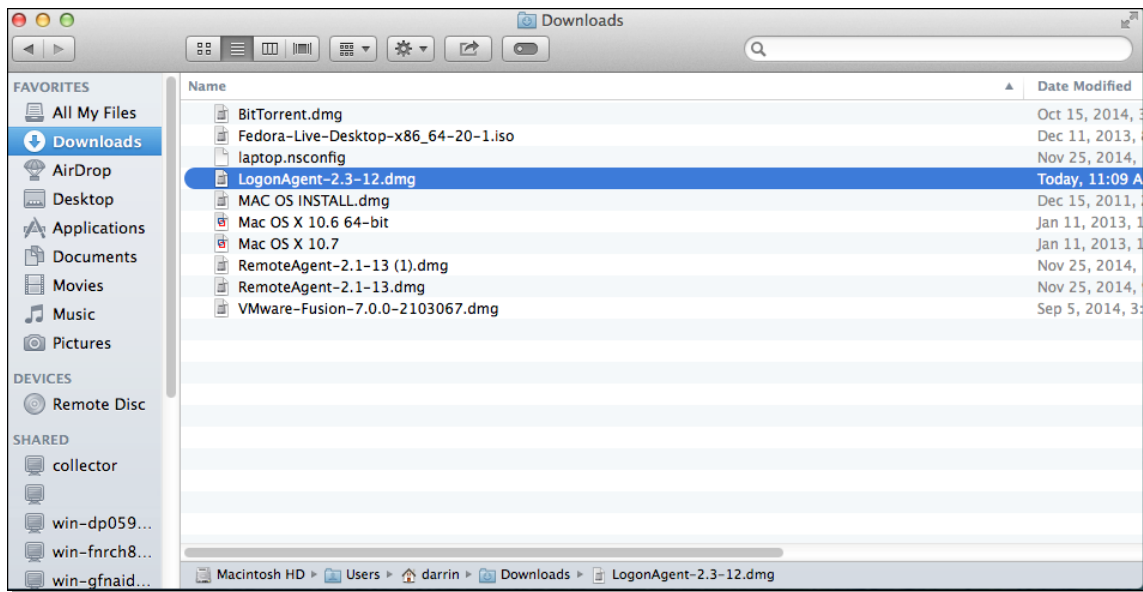
All flags that can be used with the WFLogon.exe:

- o Disables persistent mode and is not recommended.
- c Copy netlogon.exe to %TEMP% and launch from there. If the copy fails, it will launch from \\<domain>\NETLOGON
- s The Silent flag hides the persistent (-p parameter) application in the Windows systray icon.
- v The Verbose flag logs execution and exceptions to the Windows Event Log.
- q The Quit flag, often referred to as the logoff flag, is used to perform a forced logoff or disassociation of the LDAP User ID to an IP address. This flag should not be used in conjunction with the persistent flag.
- u The Username flag is an optional setting used as a mechanism to ask the OS for the user name.
- d The Domain flag is an optional setting used as a mechanism to ask the OS for the domain name.

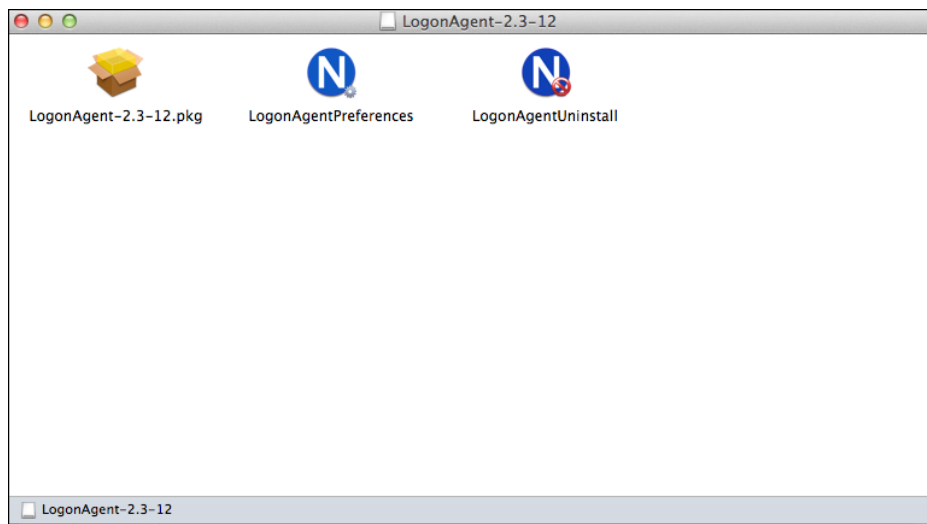
Deploying the NetSpective Logon Agent for macOS

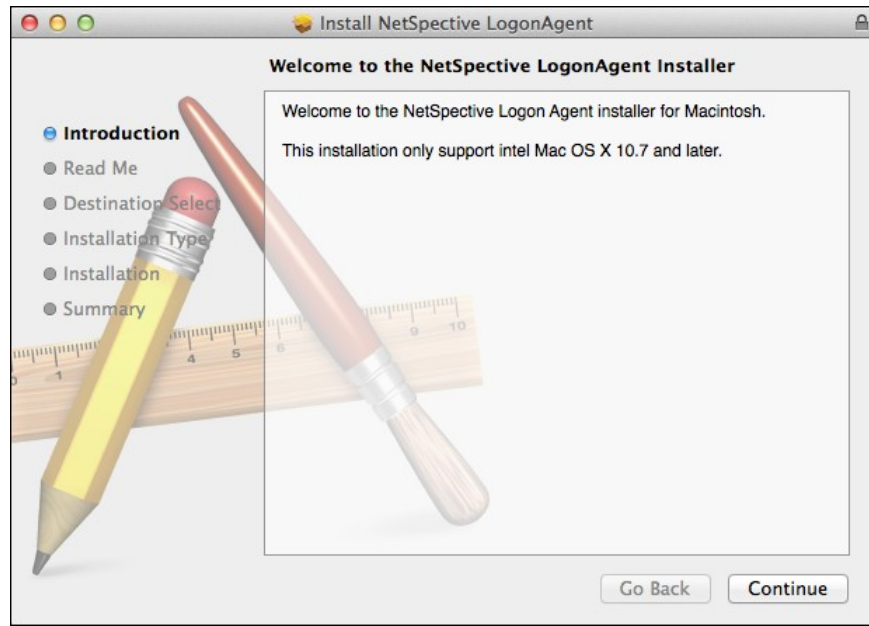
5. From the Downloads page on your NetSpective appliance, download the latest NetSpective Logon Agent disk image LogonAgent.dmg to your local Macintosh operating system.

Agent Downloads		
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
Terminal Server Agent for Windows & Citrix	3.0.4	TerminalServerAgent.exe
Logon Agent for Windows (XP, 7, 8, 10)	3.0.11	LogonAgent-3.0.11.zip
Logon Agent for macOS (10.9 - 10.12)	2.3-14	LogonAgent-2.3-14.dmg
Remote Agent for Windows (7, 8, 10)	1.5.48	RemoteAgent-1.5.48.msi
Remote Agent for macOS (10.9 - 10.12)	2.3.3	RemoteAgent-2.3.3.dmg
Remote Agent Configuration File	20161106060858	Configuration
Wi-Fi Agent	N/A	Contact NetSpective Support



6. Mount and open the downloaded disk image file. Within LogonAgent.dmg is the Install Package, LogonAgentPreferences, and LogonAgentUninstall. Select the Install Package to execute the installation process. Please note installation requires administrative credentials.





7. The installation contains a Read Me section. Below is the full text from the Read Me. This outlines the format you will see usernames in NetSpective. You will be able to tailor the agent's settings after the installation using the LogonAgentPreferences.

If this is a new installation, make sure to set the address of your NetSpective appliance using the supplied LogonAgentPreferences application.

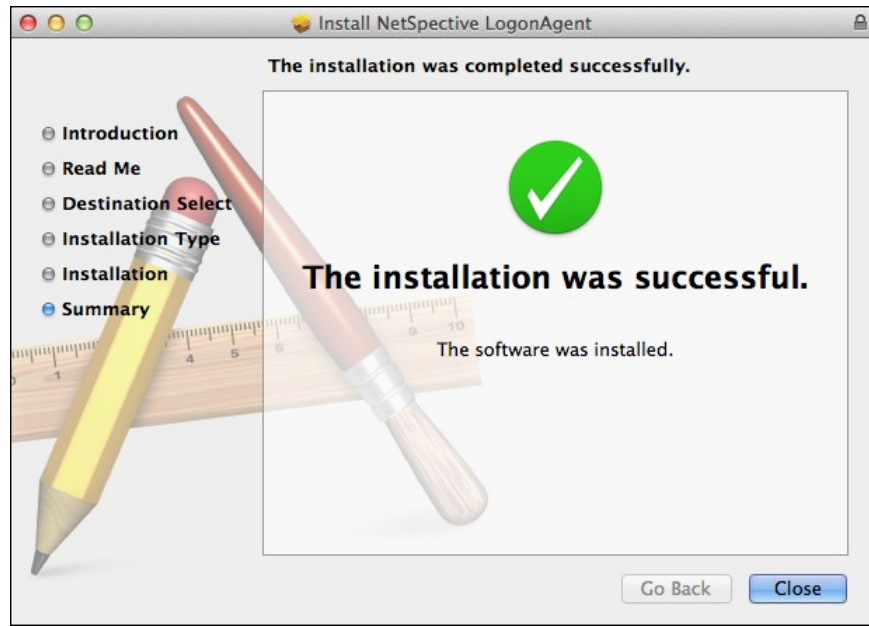
By default LogonAgent does not append the hostname to the beginning of usernames for nondomain users. This setting can also be changed with the LogonAgentPreferences application.

LogonAgent will report the short name of the currently active user to the specified list of NetSpective appliances. A local user will be reported as 'username' or 'hostname\username' depending on whether the "prepend hostname" option is enabled. A user from OpenDirectory will be reported as 'username'. A user from ActiveDirectory will be reported as 'domain\username'.

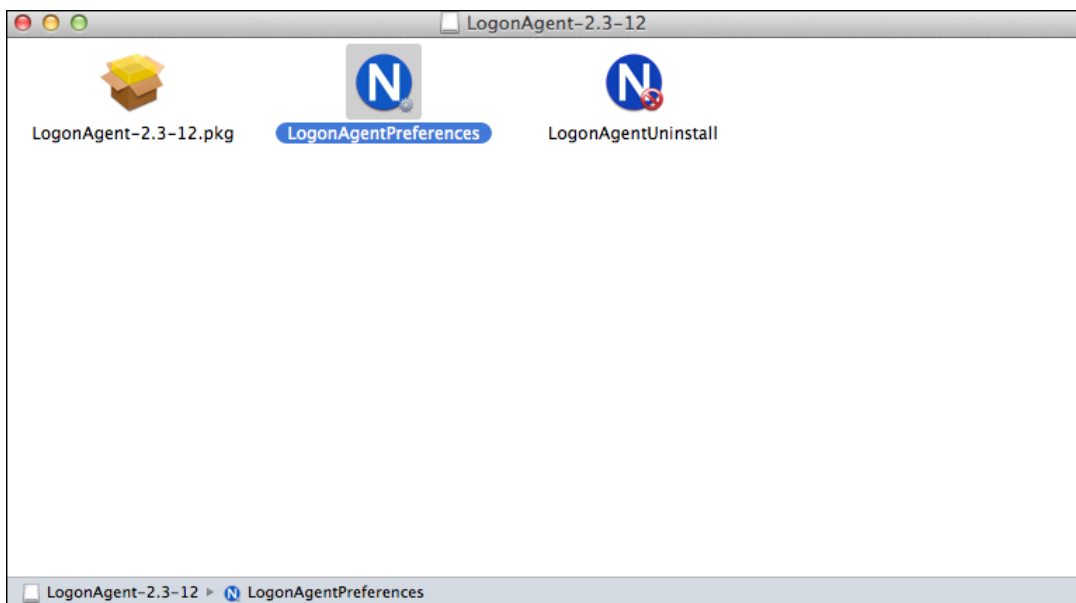
LogonAgent for Mac will respond to user login events or network change events.

It is not necessary to reload the LogonAgent launch daemon after changing preferences.

8. Click continue through the windows and install the agent. The agent will take up 627 KB of space on the workstation. When you are finished, close the installer.



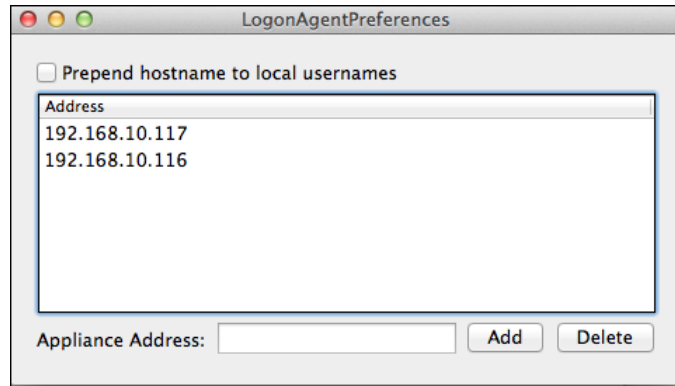
9. To configure the Logon Agent, run the LogonAgentPreferences file.



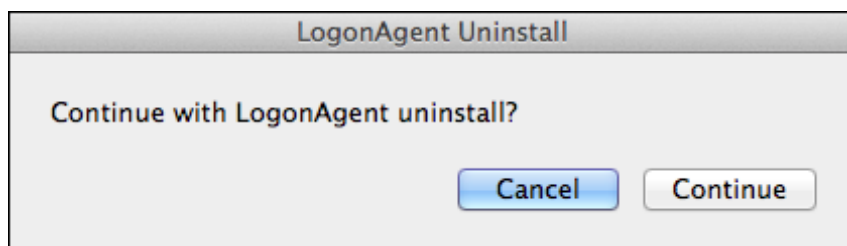
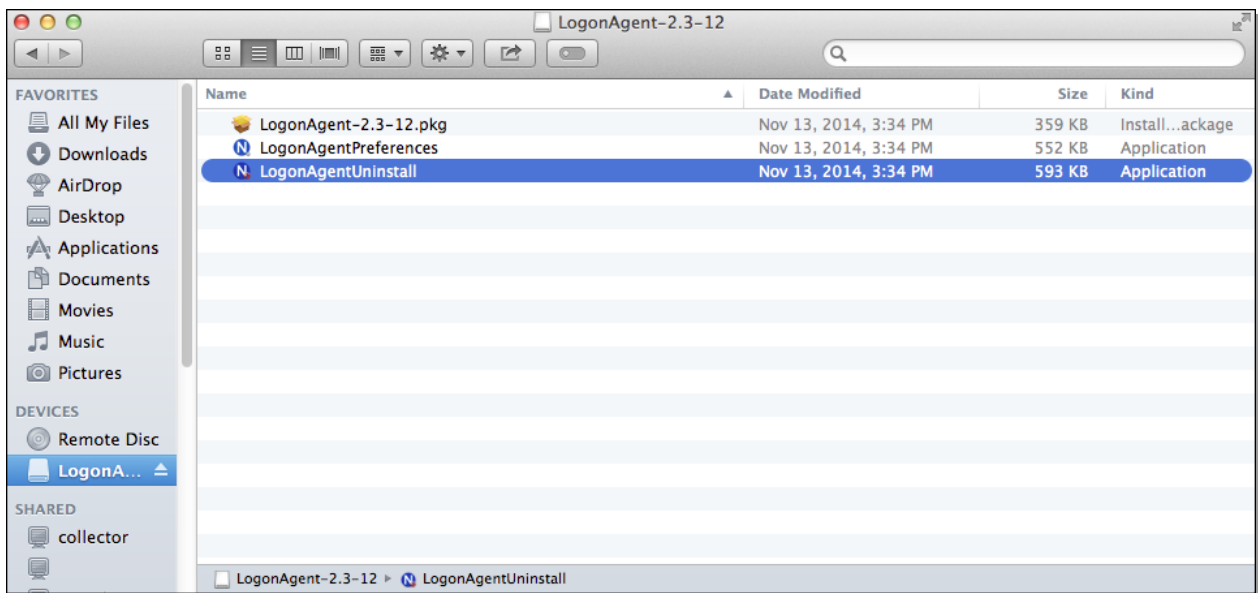
10. The LogonAgentPreferences program is used to configure the LogonAgent for sending logon events to the NetSpective. In our example, we have added the admin IP addresses of our two NetSpective appliances to the configuration. IP addresses of each of your NetSpective devices must be included in the configuration and may be added one at a time.

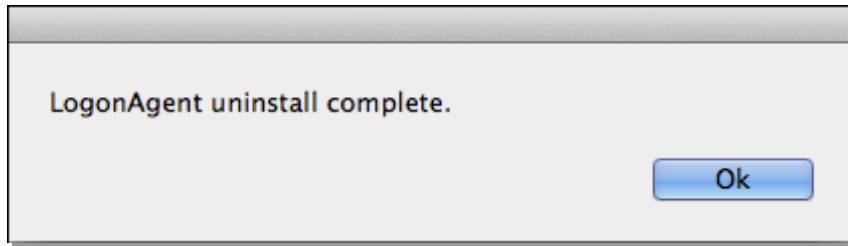
As noted in the Read Me in section 3, the option to prepend hostnames to local usernames is found in this configuration tool. This should only be used if you require users to appear in

NetSpective as 'hostname\username'. When you are finished, simply close the utility to save the configuration.



11. The package also contains the LogonAgentUninstall file. This is used to remove the LogonAgent from the workstation. This process also requires administrative privileges.





NetSpective Wi-Fi Agent Overview

The Wi-Fi Agent is intended to solve the needs of ISDs and school districts using multiple wireless zones with a need for transparent authentication. If users already are authenticating through RADIUS, and are receiving an IP address through the DHCP server, then the Wi-Fi Agent can be implemented. We can use these sources to authenticate users in NetSpective for a transparent and secure login.

How the Wi-Fi agent works

Our goal is to gather the information we need so that we can properly authenticate a user.

NetSpective requires a Username and IP Address for authentication. Here is how we'll obtain it.

6. RADIUS Logs – Containing a MAC Address and Username.
7. DHCP Server Logs – Containing the IP Address and MAC Address.

Collector Pro is a flexible, Windows based application used to relay logs from one server to another in real time. Collector Pro is used to relay these logs to the Wi-Fi Agent. The Wi-Fi Agent will then correlate the MAC Addresses from each log, to determine the Username and IP Address of each user. This will then be sent to NetSpective so these users can be given a filtering policy.

Use Case Scenario Examples

An organization may have various Wi-Fi zones:

7. Guest Wireless
8. Devices incompatible with WPA2 Enterprise – Authenticated with NetSpective Mobile Portal.
9. Open Wi-Fi - Devices authenticating with a common password or a Captive Portal System.
10. Devices compatible with WPA2 Enterprise – Username and IP Address authentication data is provided in the secure RADIUS logs.
11. Internal Wireless o Devices compatible with WPA2 Enterprise – Username and MAC Address is gathered from RADIUS logs.

End User Experience

The Wi-Fi Agent reduces the need for the NetSpective Mobile Portal. Users already authenticating through RADIUS can be brought in with the Wi-Fi Agent. With the Wi-Fi Agent deployment, the end user will never be prompted for NetSpective authentication and no software needs to be put on their device, giving them a completely transparent experience. Investment Cost

The Wi-Fi agent is a small, Windows based program. It can run on any type of Server or VM environment. Log collection is done through the Collector Pro program, also lightweight and Windows based. We simply require a non-dedicated Windows server or VM to run the process of gathering this data and relaying it to NetSpective. Since both programs are lightweight and flexible, this can be used with any existing servers or VMs in your environment.

Deployment of the Wi-Fi Agent

Since most customers have various Wi-Fi solutions, we require at minimum, a day of professional services for this deployment. This service is provided for free to a customer with an unlimited license. Once deployed, the agent runs quietly in the environment with no necessary customer interaction.

Deploying the NetSpective Mobile Portal for BYOD Initiatives (Inline/Passive)

The NetSpective Mobile Portal was designed with HTML5 to be web browser and operating system independent, making it effective at filtering mobile devices. The Mobile Portal is configured by applying a set of rules to an IP address range. This IP address range can typically be the range of your wireless zone, where mobile devices are most likely going to try and connect to. The rules applied to this address range are what will determine the behavior of the Mobile Portal and how users will interact with it.

Note: NetSpective will prioritize authentication methods starting with the most specific method first. Your Logon Agent users, Remote Agent users, and Static IP addresses will not be affected by the Mobile Portal settings and will not be asked to authenticate twice.

Configuring the Mobile Portal for LDAP Authentication

12. The Authentication Rules section has a number of rules already set up. These rules are prioritized from most specific to least specific. To create a new rule, click the Add button.

Authentication Rules		
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 NTLM). NetSpective devices in proxy mode may also use session based authentication using LDAP or Windows NTLM.		
<input type="checkbox"/> Name	Mode	Method
<input type="checkbox"/> Cached Mobile Proxy - Chromebooks	Proxy Cached Session	Authentication (Google)
<input type="checkbox"/> Mobile Portal - Inactivity Timeout 9 Hrs	Mobile Portal	Authentication (LDAP)
<input type="checkbox"/> Mobile Portal - Logon Timeout 30	Mobile Portal	Authentication (LDAP)

Filter Settings > Authentication | IP Addresses are examples only.

13. From the Authentication Rule window, you will see fields for Name, Mode, and Method. Each field is required for portal authentication. When you have created a rule, click the save icon.
 - a. The Name is just the name to identify the Rule.
 - b. The Mode refers to the type of portal you wish to use
 - c. The Method is the type of authentication that will be used to associate the user's IP with a Username, such as LDAP.
 - d. The Timeout determines how often the user will be prompted for authentication. Consider the timeout carefully depending on the types of users and devices associated with this rule.

Users can be redirected to a portal logon page, which may require a request to pair, a user name and password to be entered manually, or use an automatic integrated Windows authentication.

Name:

Mode:

Authentication

Method:

Timeout:

Option: ☐ Use the authentication credentials to automatically pair to the authenticated user.

Pairing

Pairing by Request: ☐ Associate a device with a user for a specified amount of time.

These settings are recommended for basic Mobile Portal authentication.

14. Next, create an Authentication Range. This is a range of IP addresses, typically mirroring your Wi-Fi network, which will have a Rule applied to it. To create a new rule, click the Add button.




Assign authentication rules to ranges, where ranges are network addresses or zones entered in CIDR format, i.e. '192.168.0.0/16'.

Rule:

Range:




IP Addresses are examples only.

15. Enter your IP address range in the Range field. Select the Rule you created in the previous step. When you are finished, click the save icon.

Authentication Rules   

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 NTLM). NetSpective devices in proxy mode may also use session based authentication using LDAP or Windows NTLM.

<input type="checkbox"/>	Name	Mode	Method
<input type="checkbox"/>	Cached Mobile Proxy - Chromebooks	Proxy Cached Session	Authentication (Google)
<input type="checkbox"/>	Mobile Portal - Inactivity Timeout 9 Hrs	Mobile Portal	Authentication (LDAP)
<input type="checkbox"/>	Mobile Portal - Logon Timeout 30	Mobile Portal	Authentication (LDAP)

Authentication Ranges   




Specify a range of IP addresses that will use one of the Authentication Rules created above.

<input type="checkbox"/>	Network	Rule
<input type="checkbox"/>	::/128	Mobile Portal - Logon Timeout 30
<input type="checkbox"/>	192.168.10.0/24	Mobile Portal - Logon Timeout 30
<input type="checkbox"/>	172.16.0.0/16	Mobile Portal - Logon Timeout 30
<input type="checkbox"/>	10.0.0.0/8	Mobile Portal - Inactivity Timeout 9 Hrs
<input type="checkbox"/>	0.0.0.0/0	Cached Mobile Proxy - Chromebooks

Configuring the Mobile Portal for Windows NTLM Authentication




Configuring the Mobile Portal for Windows NTLM Authentication requires all of the same steps as LDAP Authentication did. However there are a few extra steps that need to take place in order to enable Windows NTLM.

8. In the Settings > Network > DNS section, add a valid entry to the DNS Servers section. When you are finished, click the save icon.

DNS Servers   

DNS Servers will allow you to use hostnames in addition to IP addresses for other settings, such as the Logging FTP server.

<input type="checkbox"/>	Server
<input type="checkbox"/>	10.2.2.49
<input type="checkbox"/>	10.2.2.48
<input type="checkbox"/>	8.8.8.8

DNS Search Domains   

DNS Search Domains will allow you to use a short hostname of "intranet" to resolve to "intranet.example.com" if a search domain of example.com is provided.

<input type="checkbox"/>	Search Domain
<input type="checkbox"/>	example.com

IP Addresses are examples only.

- Under Authentication > Windows Integration, fill out the fields relative to your network's domain, then click the Join button. This will set up a trusted relationship between the NetSpective device and your domain. When you are finished, click the save icon in the upper left hand corner.

Windows Integration

Settings

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. These values are automatically saved when attempting to join the domain.

Security: Active Directory ▼

Host Name: netspective.test.example.com

Domain: EXAMPLE

AD Realm: test.example.com

Status: Inactive

Authentication

A user with the correct permissions is required to join the NetSpective device to the domain.

User: admin

Password:

Join

- You may now proceed with creating a rule in the Authentication Rules section. Following the same steps as in the previous section for LDAP Authentication, selecting Windows NTLM this time instead of LDAP. When you are finished, click the save icon.

Users can be redirected to a portal logon page, which may require a request to pair, a user name and password to be entered manually, or use an automatic integrated Windows authentication.

Name: Mobile Portal - Inactivity Timeout 9 Hrs

Mode: Mobile Portal - Passive ▼

Authentication

Method: x Windows NTLM

Timeout: Inactivity ▼ 9 Hour(s) ▼

IP Addresses are examples only.

When Windows NTLM 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 more information see the Configuring Internet Explorer for Single Sign-On Authentication using Group Policies section of this guide.

Configuring the Mobile Portal with Pairing

Once again, we are going to create an Authentication Rule to specify what IP address range is going to be authenticated by the portal. However this time we will enable the option for Pairing by Authentication and optionally, Pairing by Request. If Authentication is enabled, the authentication type must be one of the Mobile Portal options in order for Pairing to also be enabled.

In the Authentication Rules window, click on the one of the rules you have created. Check the option "Use the authentication credentials to automatically pair to the authenticated user". This will permanently pair the authenticated user with their device. When Pairing by Authentication is enabled, the Pairing Revalidation Period will also be enabled. Click the save icon when you are finished.

Users can be redirected to a portal logon page, which may require a request to pair, a user name and password to be entered manually, or use an automatic integrated Windows authentication.

Name:	Mobile Portal - Logon Timeout 30		
Mode:	Mobile Portal - Passive ▼		
Authentication			
Method:	x LDAP		
Timeout:	Logon ▼	30	Minute(s) ▼
Option:	<input checked="" type="checkbox"/> Use the authentication credentials to automatically pair to the authenticated user.		
Pairing			
Pairing by Request:	<input type="checkbox"/> Associate a device with a user for a specified amount of time.		
Pairing Revalidation:	20	Minute(s)	▼

Pair 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.

Pairing by Request and Temporary Access




10. In the Authentication Rule window, you have the option of selecting Pairing by Request. By checking this box, users in the address range specified in this rule will be allowed to pair by

request. The portal page will display a dialog box where the user can enter in any text they want to identify who they are.

11. Once you have selected 'Pairing by Request', you will also be able to select Temporary Access as well. This will enable you to place users that have requested pairing to be given temporary internet access. You can place them under the policy of your choice, 'Timeout' specifies how long the user will be given access for, and 'Reset' will prevent logins for the amount of time specified.

Pairing	
Pairing by Request:	<input checked="" type="checkbox"/> Associate a device with a user for a specified amount of time.
Temporary Access:	<input checked="" type="checkbox"/> Grant temporary access and assign the device to a policy for a specified amount of time.
Prompt:	Yes (Show Pairing page) ▼
Policy:	CIPA Compliant ▼
Timeout:	30 Minute(s) ▼
Reset:	5 minutes after timeout ▼
Pairing Revalidation:	20 Minute(s) ▼

12. All users authenticating with the Pair by Request option will appear in the Management > Paired Mobile Devices section of NetSpective. From here we can see a list of devices and other information such as which authentication range the user is on, the user logged into each device, the group that device is in, and when the pairing will expire.

Paired Mobile Devices						  
<input type="checkbox"/>	Mobile Device	Comment	Authentication Rule	User	Group	Status
<input type="checkbox"/>	Windows-Steve T...		test			Waiting (713 days,...
<input type="checkbox"/>	Droid 3 - William B...		test			Waiting (850 days,...
<input type="checkbox"/>	iPhone-NSK8a421...		test			Waiting (877 days,...
<input type="checkbox"/>	Nexus 7 (2013) - ...		test		Corporate	Never Expires
<input type="checkbox"/>	iPhone - Miles	Miles	test		Corporate	Never Expires

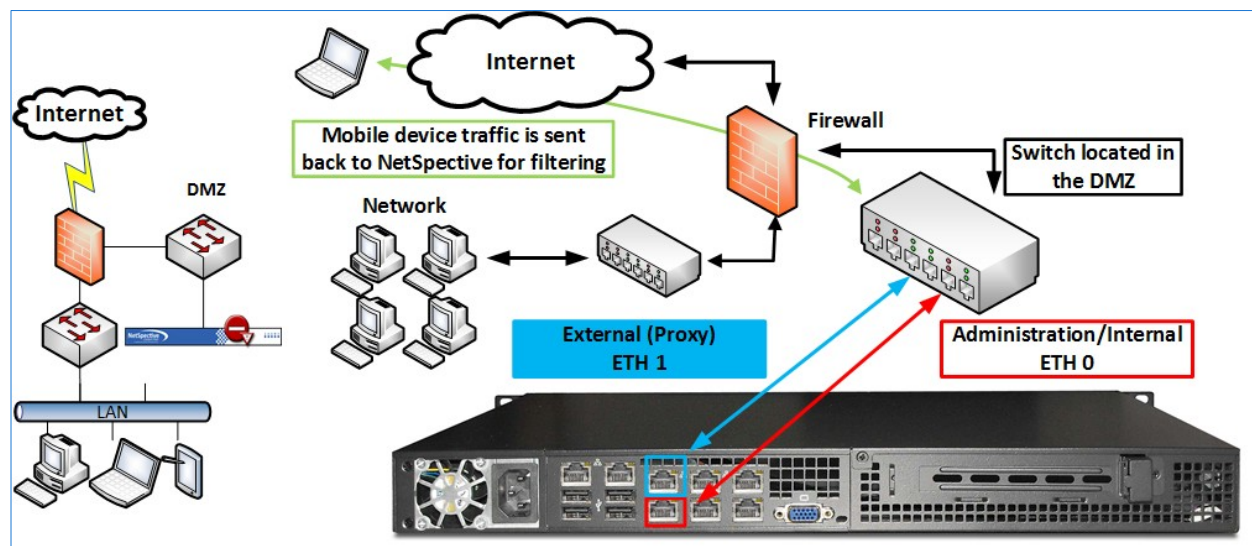
13. Clicking on a device will open the Mobile Device window's Properties. Here you can alter the visible name of the device, add comments, change the period of time the user will be paired for, and change who is paired with the selected device.

Mobile Devices, such as smartphones and tablets, can be associated with users. The name below 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.

Name:	iPhone-NSK8a421c40782	Timeout:	Waiting (877 days, 3 hours, 27 minutes)	Set
Comment:		User:		Unpair

NetSpective Mobile Proxy Deployment

The Mobile 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 Mobile 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 mobile proxy. You will need to setup a public DNS so that the hostname resolves to an IP address in the cloud.

Configuring NetSpective for Mobile Proxy

Restrict Admin Access

You may want to consider restricting admin access to your Mobile Proxy appliances, since they can be accessed from outside your network. Connect a keyboard and monitor to your appliance and enter the console interface.

Choose option 5 for Restrict Admin Access. Here you can add the IP addresses that are allowed to access the NetSpective Web Administration.

Networking

Under 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 Mobile Proxy operation. Also, you should ensure that your AD Realm (example: "test.example.com") is a DNS search domain.

Settings

☐ Allow IPv6 Network Interfaces and Static Routes

Interfaces

Changing an interface's IP or netmask will require a restart of system services which may take a few minutes.

Interface	Description	Status	Mac Address
eth0	Admin	1000 Full	00:50:56:26:1b:8f
Admin: 10.2.40.152 255.255.255.0			
Admin VLAN 1:	VLAN	IP Address, eg. 192.168.1.10	255.255.255.0
Admin VLAN 2:	VLAN	IP Address, eg. 192.168.1.10	255.255.255.0
Internal:		IP Address, eg. 192.168.1.10	255.255.255.255
eth1	External	down	00:50:56:2b:a7:53
External:		IP Address, eg. 192.168.1.10	Netmask, eg. 255.255.255.0


Default Gateway

Default Gateway: 10.2.40.1

Apply a Certificate and Hostname

Proceed to Settings > Certificates 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 "test.example.com".

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.

Certificate Details (Self Signed)

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

Issued To

Organization:	Example Organization
Organization Unit:	N/A
Common Name:	test.example.com
Locality:	Atlanta
State/Province:	Georgia
Country:	US

Issued By

Organization:	Example Organization
Common Name:	test.example.com
Locality:	Atlanta
State/Province:	Georgia
Country:	US

SSL Information

Hostname:	test.example.com
-----------	------------------

Validity

Issued On:	Oct 2 14:11:12 2015 GMT
Expires On:	Sep 29 14:11:12 2025 GMT

Generate Request

Add 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: netspective.test.example.com

Intermediate CA Certificate: (Optional)

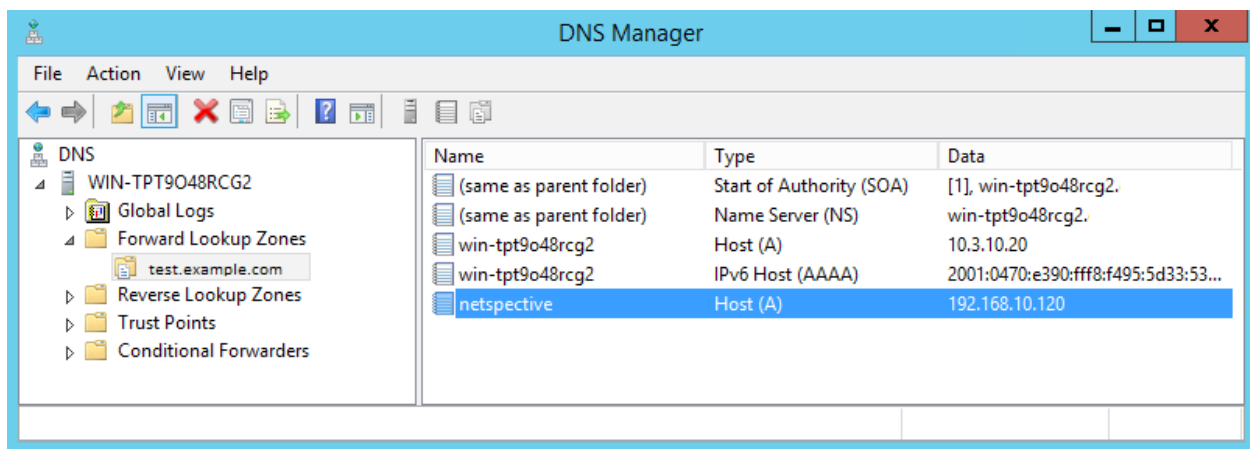
Add Cancel

The hostname displayed is an example only.

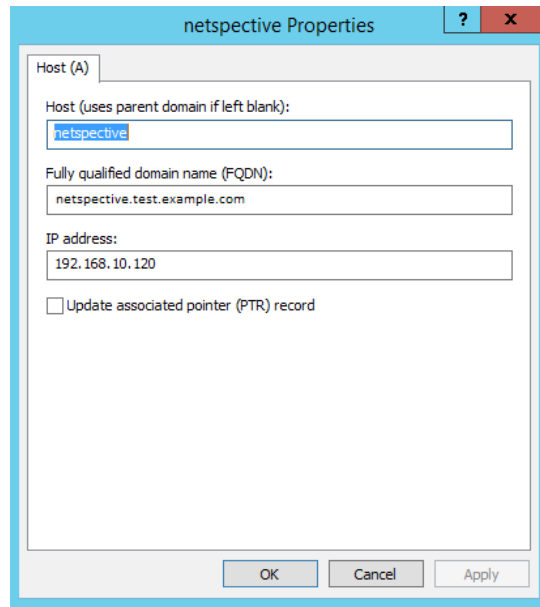
The web server will restart and the Certificate screen will be updated with the new hostname information, as seen in the Common Name and Hostname Areas.

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 test.example.com, so we configured our hostname to be netspective.test.example.com.



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 Mobile Proxy service. A domain user with sufficient privileges is required to add the NetSpective device to the domain.

Navigate to Authentication > Windows Integration. Fill out the window that appears with the appropriate information and click on the Join button. 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 Updates section of NetSpective.

Windows Integration

Settings

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. These values are automatically saved when attempting to join the domain.

Security: Active Directory

Host Name: netspective.test.example.com

Domain: EXAMPLE

AD Realm: test.example.com

Status: Inactive

Authentication

A user with the correct permissions is required to join the NetSpective device to the domain.

User: admin

Password:

Join

Image depicts examples only.

Set Authentication Rules

For NetSpective to filter users globally, we will need to configure Authentication Rules for the entire internet. Navigate to the Authentication > Authentication Rules. First we will create an Authentication Rule for mobile users. A typical deployment will utilize Cached Session Based Authentication and Windows NTLM.

Users can be redirected to a portal logon page, which may require a request to pair, a user name and password to be entered manually, or use an automatic integrated Windows authentication.

Name: Cached Mobile Proxy - Chromebooks & iPads

Mode: Cached Session Based

Authentication

Method: Windows NTLM

Timeout: Logon 30 Hour(s)

Next create an Authentication Range to encompass all IP addresses. We do this so the Mobile Proxy will catch any IP address directing traffic to the appliance. Make sure you associate this range with the Authentication Rule you just created.

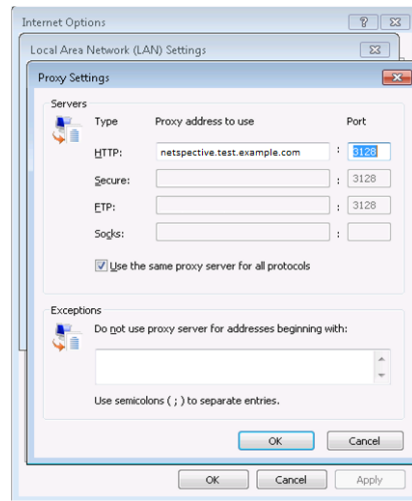
Assign authentication rules to ranges, where ranges are network addresses or zones entered in CIDR format, i.e. '192.168.0.0/16'.

Rule: Cached Mobile Proxy - Chromebooks

Range: 0.0.0.0/0

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 Mobile Proxy listens on for user traffic.



Example: Windows Proxy Settings



Example: iPad manual proxy settings.

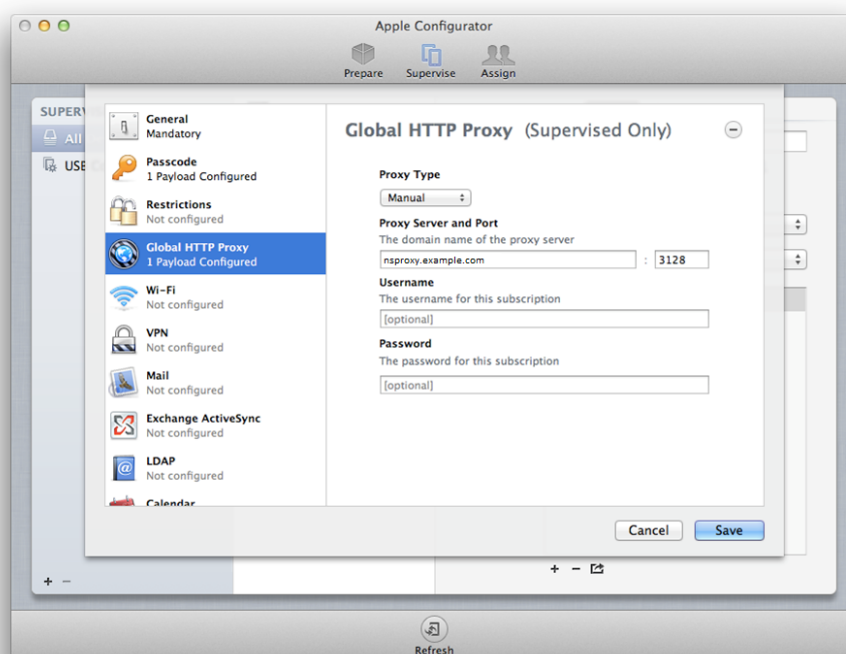
Mobile Proxy Configuration with PAC file

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 Mobile Proxy settings.

Navigate to Authentication > Proxy on the appliance. Under the Auto-Config (PAC) heading, click the download button to obtain a PAC file.



This file can then be used with MDM solutions such as the Apple Configurator and Google Admin Console to easily provision multiple devices to use the Mobile Proxy.



Example: Apple Configurator using PAC file.

Multiple Appliances Configuration

Replication Settings

Replication settings can be found under the Settings tab in the NetSpective Web Administration. Depending on the type of NetSpective appliances you are deploying, your settings will be different.

If you have a mix of Inline and Proxy appliances, you should generally make the Inline appliance the parent in the replication tree. When replicating in this scenario, you may replicate all settings except for Authentication. The goal is for the Inline appliance to handle BYOD authentication, while the Proxy's authentication is set for Mobile Proxy authentication.

Ensure DNS is configured on each appliance

If you haven't configured a DNS server from the previous parts of the guide, then this should be done first. Ensure each appliance is configured with a valid DNS server.

Under Settings > Network, you will find the section for DNS Servers. Click the Add button, enter an IP address, and click the OK button.

Configure IP addresses on each appliance

Depending on the type of proxy configuration you choose, the IP address configuration will be a little different each time. These settings can be configured in the Settings > Network section of the Web Administration.

Single NIC Configuration

Admin – Administration, Incoming & Outgoing Traffic Flow

Internal – Virtual Shared IP between appliances

Dual NIC Configuration

Admin – Administration & Incoming Traffic Flow




External – Outgoing Traffic Flow

Internal – Virtual Shared IP between appliances

The Virtual Shared IP is the same across all proxies. This is the address that your hostname will resolve to. Depending on the Proxy Mode, the appliance will then route traffic to the appropriate appliance.

In a Dual NIC Configuration, an additional route must be configured. This route tells the appliance, any traffic received should be sent out the external interface, and this is how to get out the target website. Under Settings > Network > Routes, you can configure an additional route.

In the example below, our external interface is on the 10.3.11.0 network. The Address says and Netmask tells the appliance, any traffic that needs to be sent out, should go out the External interface to this Gateway. Please use this as an example only, as your network configuration may vary.

Additional Routes




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

<input type="checkbox"/>	Destination	Netmask	Gateway	Interface
<input type="checkbox"/>	0.0.0.0	0.0.0.0	10.3.11.1	External

Enter a valid route, for example a destination of "192.168.10.0", a netmask of "255.255.255.0", and a gateway of "192.168.5.1". The gateway must be reachable through a configured interface.

Address:

0.0.0.0

Netmask:

0.0.0.0

Gateway:

10.3.11.1

Interface:

External

Configure the Proxy Mode Type (Fail Over or Load Balanced)

Load Balance

In this mode, multiple NetSpective proxy appliances are configured with the same Internal IP address (Virtual Shared IP). 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. Configure these settings under Settings > Proxy:

Cluster Mode: Load Balance

Check – Use Address Resolution Protocol (ARP)

Under Proxy Automatic Configuration > NetSpective Proxies, click the Edit List link. Edit the list to have each Admin IP of your proxy appliances under the Assigned column. When you are finished, click OK and then click the Save button in the upper left corner.

Failover

In this mode, multiple NetSpective proxy appliances simultaneously service client connections. The traffic will be distributed evenly across all proxy appliances. Configure these settings under Settings > Proxy:

Cluster Mode: Failover

Under Auto-Config (PAC) > NetSpective Proxies, Select the Internal (Shared Virtual IP) of your proxy appliances under the Detected Proxies menu, then click the Add Detected Proxy button. When you are finished, click the Save button in the upper right corner.

Create DNS A Record for the Parent Hostname

This is the hostname we created earlier in this document. On your domain controller, create a DNS A record for this hostname.

As you can see the IP Address we are using for this hostname is the Internal (Virtual Shared IP) of our proxy appliances.

Create a CNAME Record associated with the DNS A Record

Next create a CNAM record called “wpad” without quotes. Browse and select the DNS A record you just created in the previous step.

2008/2012 Update Block List to allow WPAD

WPAD is what your on-network devices will be using to obtain proxy settings. However on Windows Server 2008 and 2012, WPAD is blocked by default on these versions of Windows Server. The following excerpt is taken from Microsoft’s support site found [here](#).

Updating the block list

Use the dnscmd command-line tool to manage the global query block list. Open a command line prompt, and then do the following:

1. To check whether the global query block is enabled, type the following: `dnscmd /info /enableglobalqueryblocklist`
2. To display the host names in the current block list, type the following: `dnscmd /info /globalqueryblocklist`
3. To disable the block list and ensure that the DNS Server service does not ignore queries for names in the block list, type the following: `dnscmd /config /enableglobalqueryblocklist 0`
4. To enable the block list and ensure that the DNS Server service ignores queries for names in the block list, type the following: `dnscmd /config /enableglobalqueryblocklist 0`
5. To remove all names from the block list, type the following: `dnscmd /config /globalqueryblocklist`
6. To replace the current block list with a list of the names that you specify, type the following: `dnscmd /config /globalqueryblocklist name [name]...`

Limitations with Global Proxies

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

Upon using the Mobile 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 Mobile Proxy. An app developer would need to code around this defect in order to make the app work with any Mobile Proxy solution. The app is basically trying to authenticate

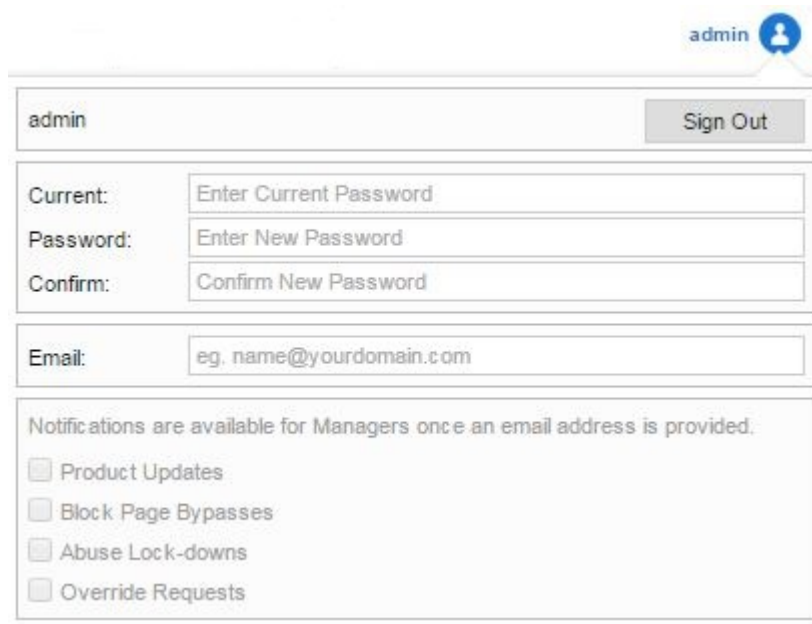
with the Mobile Proxy, but this defect will not allow the app to complete the authentication. Users will likely notice their keyboard has frozen and the app will have to be terminated. A number of apps have already been created with workarounds in place, but some have not.

This is related to iOS updates as well. On a device using the Mobile Proxy, if the user is authenticating against the Mobile 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.

NetSpective Web Interface Help

Admin Manager Settings

Here you can change the password for the main Administrator manager account. You should also consider adding an email address and enabling the notifications at the bottom of the window. Product updates and release notes are sent from NetSpective Online Service to customers with the “Product Updates” notification enabled. Without setting this section up, you will not receive information regarding product updates.



The screenshot shows the 'Admin Manager Settings' web interface. At the top right, there is a user profile icon labeled 'admin'. Below this, the username 'admin' is displayed next to a 'Sign Out' button. The main form contains three password fields: 'Current:' with placeholder text 'Enter Current Password', 'Password:' with 'Enter New Password', and 'Confirm:' with 'Confirm New Password'. Below these is an 'Email:' field with placeholder text 'eg. name@yourdomain.com'. At the bottom, a section titled 'Notifications are available for Managers once an email address is provided.' contains four unchecked checkboxes: 'Product Updates', 'Block Page Bypasses', 'Abuse Lock-downs', and 'Override Requests'.

Category Lookup

The Category Lookup was designed to allow users to see the categorization of websites in our internal database. With the Group field set to none, any Domain, URL, or IP address entered in the address bar

will return the default categorization in the NetSpective filtering database. This should help in determining how you should configure Group Policies.

Category Lookup can also be used to determine how a group is being filtered. You can select a group of users and determine how a website is being categorized for them. This will take into account any overrides made for the System as well as Group Overrides. This will NOT account for user specific overrides.



Look up the Category assigned to any URL, Domain, or IP. If a group is selected, category displayed will be relevant to the group and may be a group override.

Address:







Group:

Category:

Updates

The Updates area can be accessed by clicking the Updates icon in the far upper right corner of the web interface. This icon will dynamically change when there are no updates, updates ready to install, or if your license is about to expire.



Icon	Status	Description
	Default	Appliance is updated and there are no errors.
	Info	There is information about a product update waiting to be read in the Updates section.
	Warning	Your subscription is about to expire.
	Error	You NetSpective license has expired. You will no longer receive updates.
	In Progress	The update service is currently contacting the online service in search of updates, or is in the progress of downloading updates.
	Available	A software package has been downloaded and is available for installation.

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. You can click the Get Updates button to immediately start an update operation.

System software and license updates 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 Update button will be enabled. Click the Install Update button to install the update. The device may reboot itself as part of the install process.

Updates

Update status and/or communication errors are indicated below. If there is a system software update available you may click "Install Update" to install it.

Status

Oct 02 11:32:54 Browser Protection updates are current
Oct 01 13:55:30 Downloaded 1 update

Updates Server: 38.81.65.41

Get Updates Install Updates

Automatic 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.

You may also set a higher frequency interval to check in with the Adaptive Filtering Service for Micro 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.

Automatic Updates

NetSpective communicates with the NetSpective Online Service to receive category and software updates and send Adaptive Filtering data on day(s) and time(s) of your choice.

☒ Enable Automatic Updates

Update Time: 12:00 AM

Micro Updates: Every 10 Minutes

Days:
☒ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☒ Saturday

Version Information

Field	Version Information
Filtering Mode	Displays the device's licensed mode of filtering. Options are Inline, Passive, Proxy.
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.
Browser Protection Version	Displays the device's browser protection (categorization list) version for Malware and Phishing sites. 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.

Active User Information

Active User Information is present in the Updates area to keep you aware of your current license status. If additional User Licenses are needed contact your NetSpective Sales Representative for assistance.

Field	User Information
Total Active Users	The sum of all active dynamic and static IP address users, static range users, and IP addresses having a policy being enforced.
Active Dynamic or Static IP Users	Dynamic users are authenticated users via an LDAP source; Static IP users are authenticated users tracked by IP Address.
Active Static Range Users	Static IP address range users are authenticated or assigned ranges.
Active IP Addresses	IP addresses that are unauthenticated but having a policy being enforced.

Subscription Information

Field	Subscription Information
Subscription Name	Displays the device's unique identifier. All log files generated by the device will have this hostname embedded in the file name. Your hostname is unique to your appliance and is often required when contacting customer support.
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.

System Information

Field	System Information
System Date/Time	Displays the device's current date and 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.
CPU Speed	Displays the clock rate of the CPU.
Memory	Displays the amount of Random-access memory in the device.
Uptime	Displays the number of day(s), hour(s) and minute(s) that the device has been running since the last boot.

Contact Information

The information you enter will be used contact you regarding updates to our products and customer surveys. Some values maybe be populated based on licensed information. This provides customer support with a point of contact for support calls. In the event a support request is made but no contact information is given, support can contact the customer using the information provided here.

Statistics

Activity

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 (Proxy)

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								
Date/Time	User	Group	IP	Category	Received	Transmitted	Priority	Status
Oct 02 12:55:31		Develop...	10.2.40....	User Def...	151 B	1.75 KB	Medium	
http://data.cnn.com/jsonp/breaking_news/domestic.json?callback=jQuery111204619607159582275_1443121804261								
Oct 02 12:53:31		Develop...	10.2.40....	User Def...	151 B	1.75 KB	Medium	
http://data.cnn.com/jsonp/breaking_news/domestic.json?callback=jQuery111204619607159582275_1443121804261								

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.

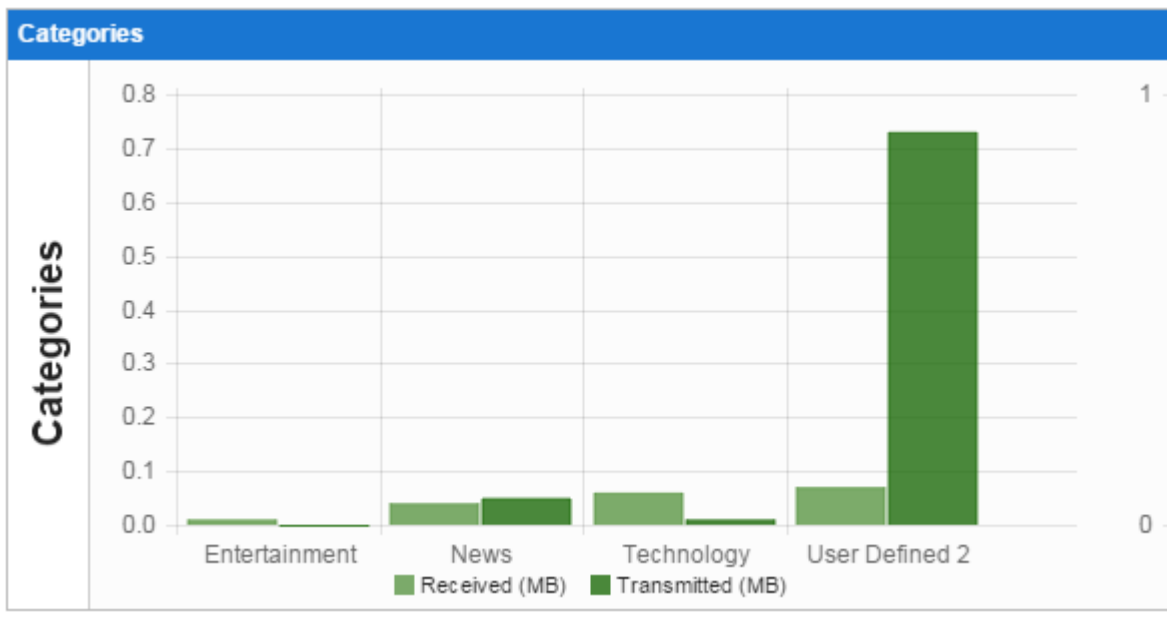
Activity Summary (Proxy)

This report shows the top Internet sites that have been accessed. This report will show amount of bandwidth sent and received from each site, as well as the number of blocks and accesses for each site. Since the counter queue is cleared daily at midnight, the most accurate report will be generated at the end of each workday.

Recent Activity Summary						
Domain	Received	Transmitted	Blocks	Accesses	Start	End
data.cnn.com	139.06 KB	1.18 MB	-	690	2015-10-01 01:55 PM	2015-10-02 12:55 PM
www.cnn.com	66.36 KB	83.76 KB	-	46	2015-10-01 02:09 PM	2015-10-02 12:39 PM

Summary Volume (Proxy)

This section will highlight the Top Categories accessed, Top Protocols Accessed, Top Users, and Top Groups accessing the internet, and the associated bandwidth sent and received. Clicking the buttons on the right of the header will allow you to see more or less data on each graph.

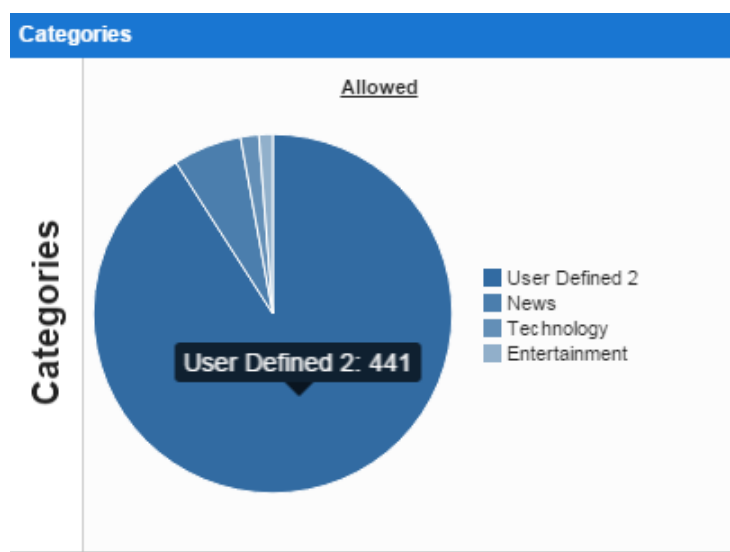


Activity (Inline/Remote)

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.

Summary (Access)

This section will highlight the Top Categories accessed, Top Users, and Top Groups accessing the internet, as well as the associated number of hits and blocks. Clicking the buttons on the right of the header will allow you to see more or less data on each graph.



Proxy Statistics

Proxy Overview

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.



Proxy Overview				
	Low	Medium	High	Total
Receiving	0	0	0	0
Transmitting	0	0	0	0
Active Users	0	0	0	0
Active Connections	0	0	0	0
Concurrent Users	-	-	-	0
Client Connections	-	-	-	0



User Summary Statistics

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 Summary Statistics										
User	Connections			Received			Transmitted			Blocks
	Low	Medium	High	Low	Medium	High	Low	Medium	High	
_UNK...	-	-	-	-	0	-	-	1.75 KB	-	-
	-	-	-	-	0	-	-	926.62 KB	-	-

Connection Detail

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  to immediately close a connection.

Connection Detail							
User	Domain	Received	Transmitted	Priority	Quota (%)	Duration	
Tel...		0	0	Idle	0.00	00:00:26	 
Group:		Category:		Authentication: N/A			
Client Address: 10.2.40.144:57469		Local Address: 10.2.40.152:45848		Server Address: 157.166.249.67:80			

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.

DNS Cache Entries

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.

DNS Cache Entries		
Domain	IP	Timeout (Seconds)
a-fst1.apartmenttherapy.com	23.235.46.249	Expired
a-fst2.apartmenttherapy.com	23.235.46.249	Expired

Searches

Recent Searches

These reports illustrate the phrases users have entered into popular search engines. You may click the buttons on the right of the header to show more or less results.

Popular Searches

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

Miscellaneous

Appliance Statistics

This report shows the CPU usage in real time, both utilization and idle. The right side shows network utilization in Mbps.

Abuse Lock-downs

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.

Block Page Bypasses

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.

Managed Sessions (Inline/Proxy Only)

This report displays the SSL Sessions the NetSpective is currently managing or inspecting. The report lists domains with their associated client IP, the destination server IP, transmitted and received packets, and the duration the session has been open.

Active Ethernet (Inline Only)

This report shows the NetSpective NICs that are monitoring traffic and any MAC addresses the appliance is connecting to. The Age column shows how long these sessions have been active.

Cluster Status

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.

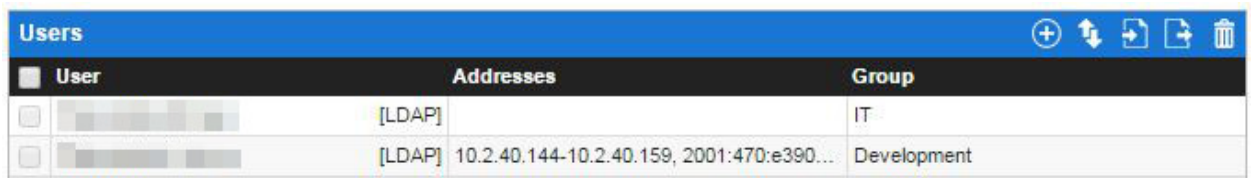
Management

All Assigned Users

The All Assigned 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. You may also import or export a list of users.

Currently Logged On Users

NetSpective's Logon Agent, Remote Agent, Terminal Server Client, Authentication Portal, Mobile Portal, and Wi-Fi Agent 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 [Assign Users to a Group] button in the header. 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.



Users		
User	Addresses	Group
[LDAP]		IT
[LDAP]	10.2.40.144-10.2.40.159, 2001:470:e390...	Development

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 name. Once the dialog has opened, complete the necessary information.

Field	Requirements
User	A name to assign the user to.
Group	A group 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 be assigned a dynamic IP. Both IPv4 and IPv6 addresses may be entered. Each user can support up to 5 addresses.

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.

Paired Mobile Devices

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.

Paired Mobile Devices						
<input type="checkbox"/>	Mobile Device	Comment	Authentication Rule	User	Group	Status
<input type="checkbox"/>	iPhone-NSK8a421...		test			Waiting (881 days,...
<input type="checkbox"/>	Nexus 7 (2013) - ...		test		Corporate	Never Expires
<input type="checkbox"/>	iPhone - Miles	Miles	test		Corporate	Never Expires

Managing Mobile Pairings

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

Field	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.

Mobile Devices, such as smartphones and tablets, can be associated with users. The name below 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.

Name:	<input type="text" value="iPhone-NSK8a421c40782"/>	Timeout:	<input type="text" value="Waiting (881 days, 1 hour, 43 minutes)"/>	<input type="button" value="Set"/>
Comment:	<input type="text"/>	User:	<input type="text"/>	<input type="button" value="Unpair"/>

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.

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 Mobile Device button to unpair the devices.

Force Mobile Device to Expire

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 Force Mobile Device to 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 Mobile Device button to delete the mobile devices. If a mobile device is deleted the user will need to request to be paired again.

Digital Citizenship License

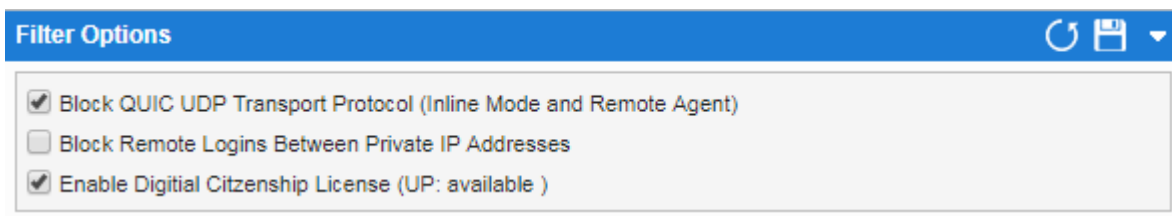
The Grom Digital Citizenship License or DCL for short, is a joint collaboration between NetSpective and Grom Educational Services. The feature, once deployed, will redirect users to a website where they must watch a series of videos and answer questions based on the video content. These videos are designed to educate students on the dangers of the internet and inform them on how to be good digital citizens. Over time, the videos will change and have new content, so that students are not seeing the same videos each year. The test is broken into three different grade levels with different sets of questions for the three groups. Once the test is completed, the student, as well as NetSpective, will be notified if the test was passed or failed. If the student passes the test, they may download their Grom Digital Citizenship License, a .pdf that they can print out. Once the user has passed the test, or the timeframe for the test has expired, they may surf the internet normally under their group policy.

The only requirements for the feature to function is for the user to be authenticated to a group. The DCL will not function in the Public group. NetSpective must also be able to see and modify the user's traffic in order to redirect the user to the DCL Test. If a user is accessing SSL traffic, then category associated with that traffic must also be decrypted.

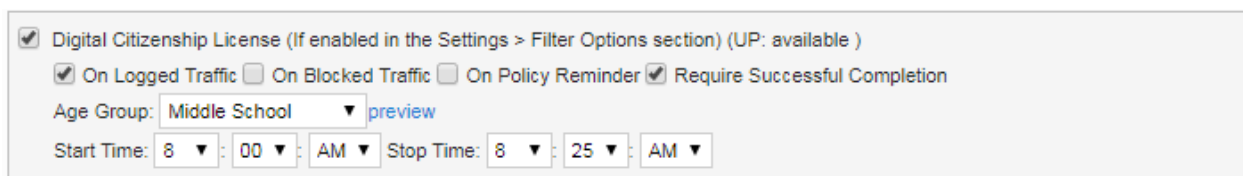
The DCL Test Site requires a user ID to be sent from NetSpective in order to function. If multiple users are using the same domain\username, they will be treated as the same user. Once that user has passed

or failed, all subsequent attempts to take the test will be treated as that same user and they will also already have passed or failed.

Under Settings > General, ensure that the Digital Citizenship License feature is enabled by checking the box next to it. After you are finished, click the Save icon in the upper right corner.



The Digital Citizenship License is a group based feature and will only function for the groups you enable it for. Under Management > Groups, select the group of users you want using the DCL, then click on the Policy tab.



Click on the Properties button in the upper right corner to view the DCL Configuration. The feature must also be enabled here with the first check box in order to redirect users to the test website. You have four options for presenting the test.

On Logged Traffic – This will cause any categories that are marked in Yellow (Logged) to redirect users to the DCL Test. Users must not have taken the test, and must access the internet through a web browser during between the Start Time and Stop Time.

On Blocked Traffic – This will cause any categories that are marked in Red (Blocked) to redirect users to the DCL Test. Users must not have taken the test, and must access the internet through a web browser during between the Start Time and Stop Time.

On Policy Reminder – This will cause any categories that are marked with an abuse flag, and also has the Policy Reminder enabled, to redirect users to the DCL Test. Users must not have taken the test, and must access the internet through a web browser during between the Start Time and Stop Time.

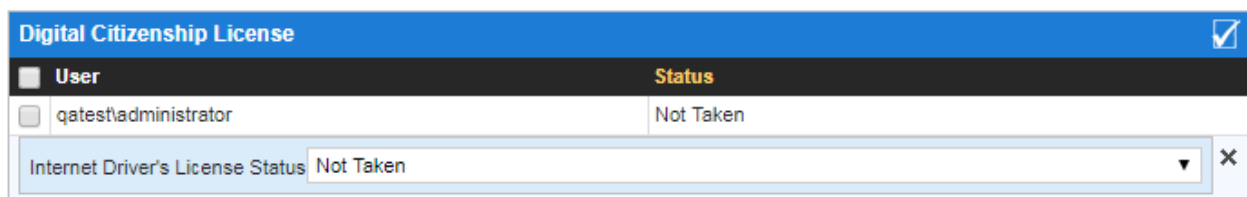
Require Successful Completion – This must be used alongside one of the previous three options. With this enabled, users who fail the DCL Test will continue to be redirected back to the test until they have passed.

Next, select the age group that is most appropriate for your group of users. The test website will show the simplest and fewest set of questions for Elementary School users, and the most complex questions for High School users. You may use the Preview link to view a sample of the DCL Test website.

Finally, select the Start Time for when users will begin to be redirected to the DCL Test website, and the Stop Time for when the feature will automatically disable redirecting users. We recommend discussing this time with Teachers and Staff beforehand, so that your school is not taken by surprise when students cannot access the internet as they expect. Times of the day when all students in the group are not in a lesson are best, such as home room or the first period of the day, when time can be blocked out to perform the test.

Managing the Digital Citizenship License Users

There are several ways of accessing the same listing of users. If you are currently managing a group of users, selecting the DCL tab on the right pane will give you a listing of just that group's users. There is also a folder on the left column for Digital Citizenship License, where you can see a listing of All Users, or only the Currently Logged On Users.



When you select one of these three areas, you will see a list of your users, as well as their Status, (Passed, Failed, or Not Taken). Clicking on a user's name will provide a drop down menu where you can manually change their status. Alternatively, you can select multiple users with the check box, then use the Set User Digital Citizenship License button in the upper right corner to change the status of many users at once. You may also click on the heading of each column to sort that column, if you wanted all Failed users to appear at the top of example.

Group 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 shown in the Type column.

Group Overrides							
Override	Type	Referrer	Group	Start Date	End Date	Current Category	Override Category
<input type="checkbox"/> cnn.com	Domain		Group A	2015-08-27	Never	News	User Defined 1
<input type="checkbox"/> data.cnn.com	Domain		Public,CIPA Compliant	2015-08-27	Never	News	User Defined 1

Search Term

The 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.

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
	A System Override already exists for this override. The System Override will have a 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

For adding an override, select the "Add" button in the upper right corner in the header. For an update click the override you wish to edit.

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 Save and Close 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.

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.

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. Putting addresses in quotations is optional:

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

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.

User Overrides

User 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.

Override 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 [Group Settings](#) section for information on enabling this feature per group. The request listing will include the domain, user (if available), group, time of request, the current category and the requested 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.

Requests

Override

Type

User

Group

Request Date

Current Category

Requested Category

iprrromotech...

Domain

Group B

2014-07-24

Not Rated

Reference

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. 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.

Domain:

ipromotechchange.com

Comment:

www.ipromotechchange.com

Category:

Reference

Start Date:

2014-07-24

End Date:

Never

Referrer Depth:

None

Assign Groups:

x

Group B



Confirm

Delete

Policy Templates

Policy Templates allow you to create a ruleset of policy settings and link them to multiple groups at the same time. Any changes to the policy template will change the policy for the associated groups instantly. Multiple templates can then be created for different situations such as for online testing. Click the Add button to be taken to a blank policy where you can then give the template a name before saving.

Templates can then be associated with a group of users by clicking on that Group's name and going to the [Group Settings](#) page.

Policy Templates		 
<input type="checkbox"/> Policy		Assigned
<input type="checkbox"/> COE Template		1
<input type="checkbox"/> Common Core Template		1

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.

Groups			   
<input type="checkbox"/> Group	Source Priority		Assigned Users
<input type="checkbox"/> Exempt			0
<input type="checkbox"/> Public			0
<input type="checkbox"/> CIPA Compliant			0

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.

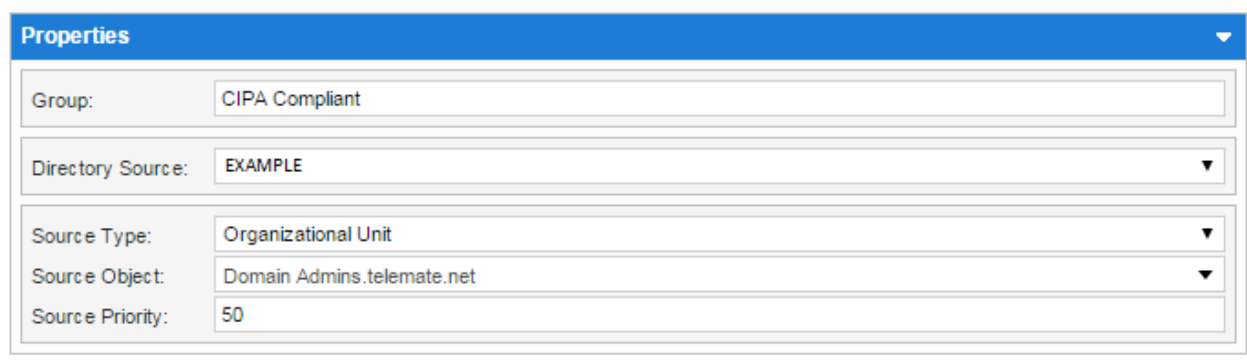
Settings

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

Directory Source

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 Directory 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 Source Object drop down.



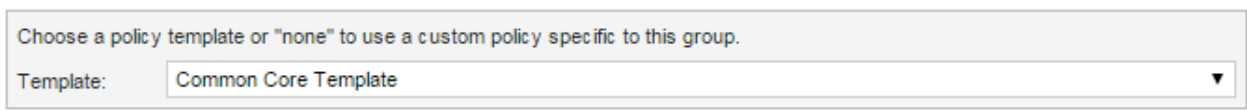
Properties	
Group:	CIPA Compliant
Directory Source:	EXAMPLE
Source Type:	Organizational Unit
Source Object:	Domain Admins.telemate.net
Source Priority:	50

Source 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. Source priority level will order groups with the lowest number first.

Policy Template

You can link this group to a preconfigured Policy Template. Policy Templates can be shared across multiple groups. If you wish to use a custom policy for this group only, select None.



Choose a policy template or "none" to use a custom policy specific to this group.	
Template:	Common Core Template

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.

Alternate Days Policy is a group policy that will be used on designated days of the week instead of the default group policy.

☒ Enable Policy for Alternate Days

Template:

Days Active: ☒ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☒ Saturday

Block Page Management

The Block Page Bypass 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 bypass can affect the entire NetSpective group or just the user from which the override originated.

Type	Block Bypasses
Mode	Either disabled, Group, or Individual.
Bypass Duration	The number of minutes to bypass the block.
Bypass Authentication	Enter a password that will be used to authorize block page bypasses. Manager Credentials requires a manager's login and password for authentication.
Bypass Notification	After a specified number of block page bypasses 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 Bypass Notifications in the Security section.
Override Requests	Enables users within the group to request a category change right from the block page.

Block Page Bypass:

Bypass Duration:

Bypass Authentication: ☒ Manager Credentials ☐ Password:

Bypass Notification: ☒ Send email notifications after block page bypasses have been issued for the day.

Override Requests: ☐ Allow users to request a category change from the block page.

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.

Permanently redact certain activity log attributes.

☐ Source IP Address ☐ Username ☐ Group Name

Policy

Properties – Safe Search

NetSpective's Safe Search feature transparently converts all Google, Bing, Yahoo, Ask, Baidu, Dogpile, DuckDuckGo, Hotbot, InfoSpace, and Lycos searches into "Safe Mode" searches. To enable Safe Search, check the box next to Safe Search. Search engines that are not allowed and are unchecked can also be redirected to the search engine of your choice from the Redirect drop down menu. You must decrypt the Web Search category to enable this feature.

☒ Safe Search

If a search engine is blocked, users can be redirected to an approved search engine. Also, specific search engines can be allowed that support safe search.

Redirect:

Allowed: ☒ Google ☒ Bing ☒ Yahoo ☒ Ask ☒ Baidu ☒ Dogpile ☒ DuckDuckGo ☒ HotBot ☒ InfoSpace ☒ Lycos

Properties – Policy Reminder

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 [Settings > Customization](#).

☒ Policy Reminder: Display every minutes for all levels.

Properties – Restrict YouTube Content

With these settings, you may restrict the content displayed on YouTube. By enforcing Strict or Moderate modes, NetSpective will perform a header injection on each request sent to YouTube, enforcing these modes when viewing or searching for content from within YouTube. Videos on YouTube that are flagged as Mature Content will not be played. This is a group based setting that can be enabled or disabled for each group. You must decrypt and allow the Streaming Media category to enable this feature. For a detailed description on what YouTube considers Moderate or Restrict, please see the associated Google support article.

<https://support.google.com/youtube/answer/174084>

Restrict YouTube Content: ☒ Disabled ☐ Strict ☐ Moderate

Properties – Restrict Facebook Content

By enabling the check box for Restrict Facebook Content, the WebFilter will allow traffic to Facebook regardless of your policy setting for the Society category. Once this feature is enabled, you can disable functionality of Facebook features and actions by checking the associated checkboxes. You can disable as many Facebook features as you would like. Restrict Facebook Content is a group feature that can be enabled or disabled for each of your groups. You must decrypt the Society category to enable this feature.



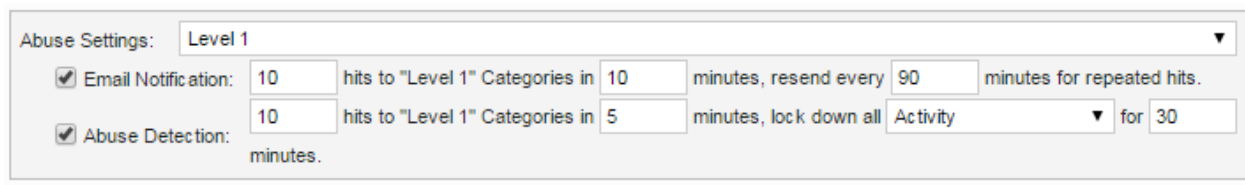
The screenshot shows a settings panel titled "Restrict Facebook Content:". It features a checked checkbox for the main title and a row of ten unchecked checkboxes for specific features: Postings, Photo Uploads, Video Uploads, Friending, Messaging, Events, Notifications, Groups, Video, and Games & Apps.

Properties - 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.

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.

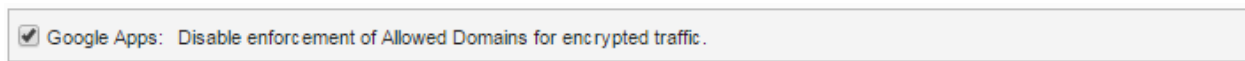
If Abuse Detection is enabled, the users assigned to the group will be monitored for activity to categories marked as abusive. Once a user's abuse limit has been reached, either all other Categories marked with this abuse level, all of the user's Internet Activity, or just the user's Web Activity will 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.



The screenshot shows the "Abuse Settings:" panel for "Level 1". It includes two main sections: "Email Notification:" and "Abuse Detection:". The "Email Notification:" section has a checked checkbox and fields for "10 hits to 'Level 1' Categories in 10 minutes, resend every 90 minutes for repeated hits." The "Abuse Detection:" section has a checked checkbox and fields for "10 hits to 'Level 1' Categories in 5 minutes, lock down all Activity for 30 minutes."

Properties - Google Apps

You may find that certain privileged users do not wish to have their Google Apps forced to the school's domain. If these users wish to still sign in with their personal Gmail account, you may check this option to disable the enforcement of the Allowed Domains feature. If you wish to configure NetSpective to force users into using a specific Google Apps domain, see the [Google Integration](#) section.



The screenshot shows a settings panel titled "Google Apps:". It contains a checked checkbox followed by the text "Disable enforcement of Allowed Domains for encrypted traffic."

Group Policy

Every group has its own policy that can Block, Monitor, or Ignore internet activity based upon category and time of day. The policy is displayed as a grid with categories as the vertical axis and time of day as the horizontal axis. Each box in the grid is a color which represents the action to take.










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.

Color		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.	

Flag	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 that NetSpective will perform SSL Decryption on all HTTPS traffic in this category.
	<i>(Proxy Only)</i> 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.
	<i>(Proxy Only)</i> 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.

When performing SSL Inspection, there are certain categories that are required to be decrypted in order to maintain functionality of NetSpective Features.

Safe Search requires that Web Search and Web Search Filtered are being decrypted.

NetSpective recommends a set of categories to decrypt and can be found under the CIPA Compliant group policy. A general rule would be to only decrypt traffic you are blocking, so that block pages can be sent to SSL sessions, as well as categories such as Education, Society, Streaming Media, Web Search, and Web Search Filtered.

There are also some websites that should not be decrypted due to the target website not accepting third party certificates, such as Apple updates, Microsoft updates, etc. We suggest NOT decrypting the Technology category for this reason.

Overrides (View Only)

This section is a read only view of the group's overrides. To add or edit any overrides, you must go to the [Group Overrides](#) section pertaining to the type of override you wish to make.

Users

The Groups – Users Tab displays the current list of users who are members of the group you have selected in the left pane. Members can be viewed, searched for, added and deleted in this section. For more information on navigating the Users tab, see the All Assigned Users section.

Managers

The Managers tab is a view only list of managers that have control over the group you have selected in the left pane. To add, remove, or change manager settings, please see the Security tab.

Authentication

Authentication Rules

Authentication Rules are IP ranges that can be set to display one of the various Captive Portals the NetSpective can use for Mobile Device authentication. Captive Portals are used to authenticate users from unknown IP addresses. The Rules define which portal will be displayed, as well as the method of authentication that will be asked from the end user. The Standard Portal is a legacy HTML portal used to authenticate workstations that are not able to run the Logon Agent. The Mobile Portal's is designed using HTML5 standards in order to optimize appearance on mobile devices such as smart phones and tablets.

To set up an Authentication Rule, see the [Deploying the NetSpective Mobile Portal for BYOD Initiatives](#) section.

Authentication Ranges

Authentication Rules are IP ranges that can be set one of the Rules you define in the Authentication Rules section. This IP range will then display the associated captive portal and authentication method the rule defines. Ranges are ordered from most specific to least specific and will take precedence from top to bottom.

To set up an Authentication Range, see the [Deploying the NetSpective Mobile Portal for BYOD Initiatives](#) section.

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.

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 designed to force users to authenticate when no other means of authentication is compatible with the device.

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.

Google Authentication

Google Authentication leverages OAuth2 to pull a user's Google username (Gmail Address) from your Google directory. The Mobile Portal will display a Login with Google button to securely authenticate the user.

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 macOS. 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.

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.

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.

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)

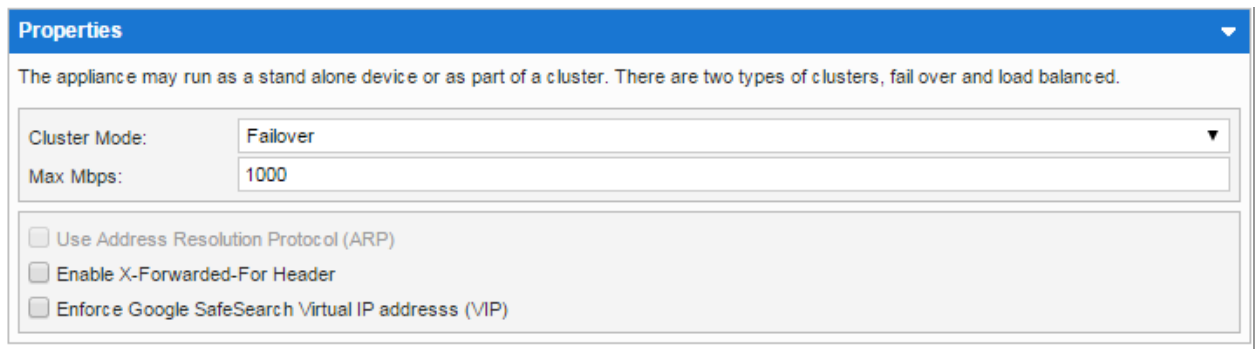
This option provides single sign on capabilities for Windows users. In addition, some browsers such as Firefox also support this method on other operating systems such as Linux and macOS.

Note: You must join NetSpective to a Windows domain to use NTLM Windows authentication.

Proxy

Settings

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.



The screenshot shows a 'Properties' dialog box with a blue header. Below the header, a text box states: 'The appliance may run as a stand alone device or as part of a cluster. There are two types of clusters, fail over and load balanced.' Below this, there are two input fields: 'Cluster Mode:' with a dropdown menu set to 'Failover', and 'Max Mbps:' with a text box containing '1000'. At the bottom, there are three unchecked checkboxes: 'Use Address Resolution Protocol (ARP)', 'Enable X-Forwarded-For Header', and 'Enforce Google SafeSearch Virtual IP addresss (VIP)'.

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.

1. **Separate load balancer device** - Direct Routed: All appliances should have the same Internal IP address and ARP disabled.
2. **Separate load balancer device NAT** - All appliances should have a unique IP address and ARP enabled.
3. **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.

IPv6 for External Hostnames

When IPv6 for External Hostnames is enabled, the proxy can utilize the IPv6 protocol to communicate with compatible external servers. To be eligible for IPv6 communication with the proxy, a server needs to have a valid domain name (ex: www.google.com) and an IPv6 address registered with DNS.

X-Forwarded-For Header

When the X-Forwarded-For Header is enabled, an additional header will be added or modified to show the origination of the HTTP traffic passing through the proxy.

Enforce Google SafeSearch Virtual IP address (VIP) Option

When enforcing the Google Virtual IP Address (VIP) option, proxy connections to www.google.com and other Google owned top level domains are replaced with forcesafesearch.google.com.

Restrict YouTube Content

Restrict YouTube Content is similar to the option found in the group policy properties. With these settings, you may restrict the content displayed on YouTube. By enforcing Strict or Moderate modes, the Proxy will rewrite DNS entries for YouTube, enforcing these modes when viewing or searching for content from within YouTube. Videos on YouTube that are flagged as Mature Content will not be played. This is a Proxy based setting and will affect all Mobile Proxy users regardless of Group and Policy settings, so long as you are allowing the Streaming Media category. For a detailed description on restrict YouTube DNS rewrites, see the associated Google support article.

<https://support.google.com/youtube/answer/6214622>

For a detailed description on what YouTube considers Moderate or Restrict, please see the associated Google support article.

<https://support.google.com/youtube/answer/174084>

Priority Settings

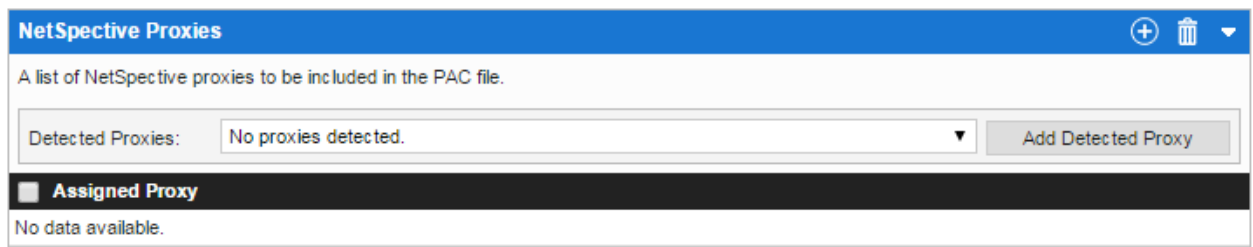
NetSpective supports 3 priority classes of traffic - High, Medium, and Low. Each priority class has a configurable target percentage of maximum bandwidth, for example High priority traffic may use 75% of the maximum allowed bandwidth even when there is demand for Medium and Low traffic. The target percentages 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.

Auto-Config (PAC)

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 "example.com", you would map "wpad.example.com" to the NetSpective device. For setting up Proxy Auto-Configuration, see the [Mobile Proxy Configuration with PAC file section](#).



Last Updated On / Download Button

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' button.

NetSpective Proxies

This setting is required. Click the drop down menu to display a list of 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.

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.

Rules - Settings

To exempt certain sites, such as your local intranet, 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. Rules are evaluated in order from top to bottom.

☒ Exclude Simple Hostnames

Rules - Network

	Destination	Rule
<div></div>	<input type="checkbox"/> 192.168.5.2/32	NetSpective Proxy
<div></div>	<input type="checkbox"/> 192.168.5.1/32	NetSpective Proxy

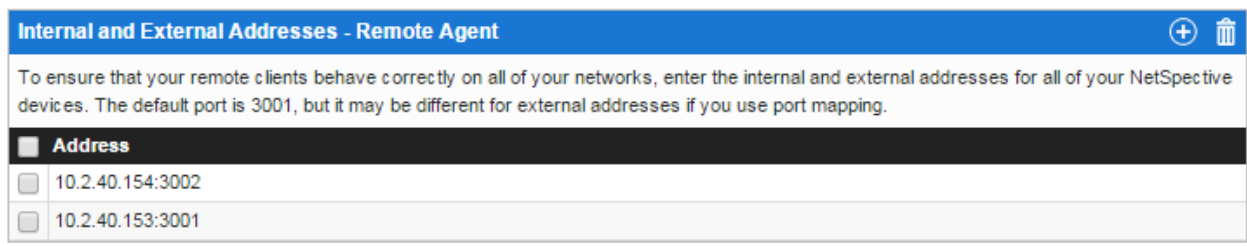
Rules - Host Names

	Destination	Rule
No data available.		

Agents

Connection Settings

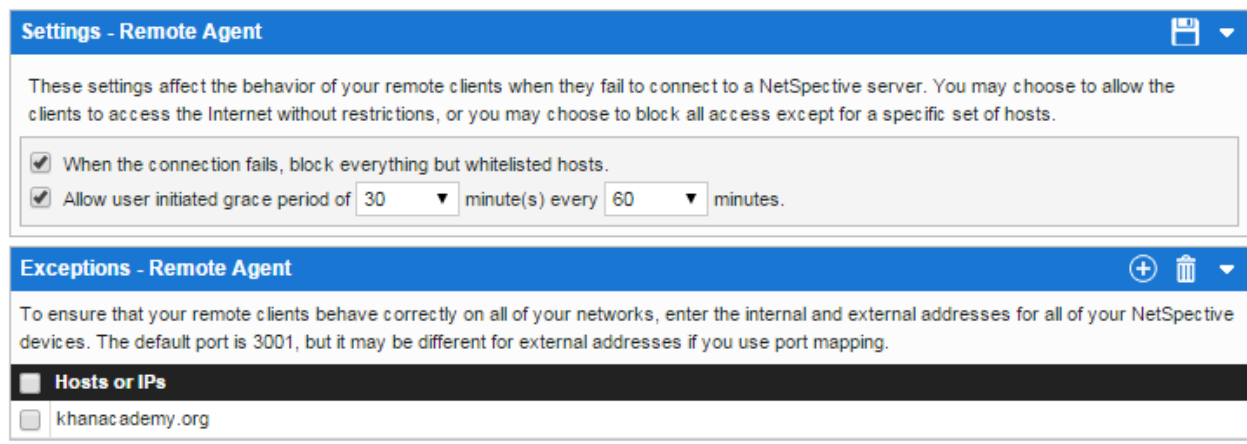
Before the Remote Agent can be used, it must know how to connect to your NetSpective Appliances. You should specify all NetSpective appliances on your network with both public and private addresses. Depending on the location of the remote access user, the network, and the load on the appliances, the 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.



Internal and External Addresses - Remote Agent	
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.	
Address	
<input type="checkbox"/> 10.2.40.154:3002	
<input type="checkbox"/> 10.2.40.153:3001	

Connection Failures

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.



Settings - Remote Agent	
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.	
<input checked="" type="checkbox"/> When the connection fails, block everything but whitelisted hosts.	
<input checked="" type="checkbox"/> Allow user initiated grace period of 30 minute(s) every 60 minutes.	

Exceptions - Remote Agent	
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.	
Hosts or IPs	
<input type="checkbox"/> khanacademy.org	

Client Settings

The Remote Agent can be configured to Automatically Send Software Upgrades to Clients. This can potentially be disruptive to end users. Remote Agent upgrades may require a reboot upon upgrading. Also, most imaging software, such as a Deep Freeze, can force a workstation in an endless reboot if the agent continually attempts to upgrade.

Enforcing Google Safe Search VIP will force all Google domains to redirect to Google's Safe Search IP address. This is not necessary for enforcing safe search and is purely optional. This will give you the same results on off network devices as the Google Safe Search VIP script would give to on network workstations. For more information on Google Safe Search VIP, see the Google Integration – Apps section.

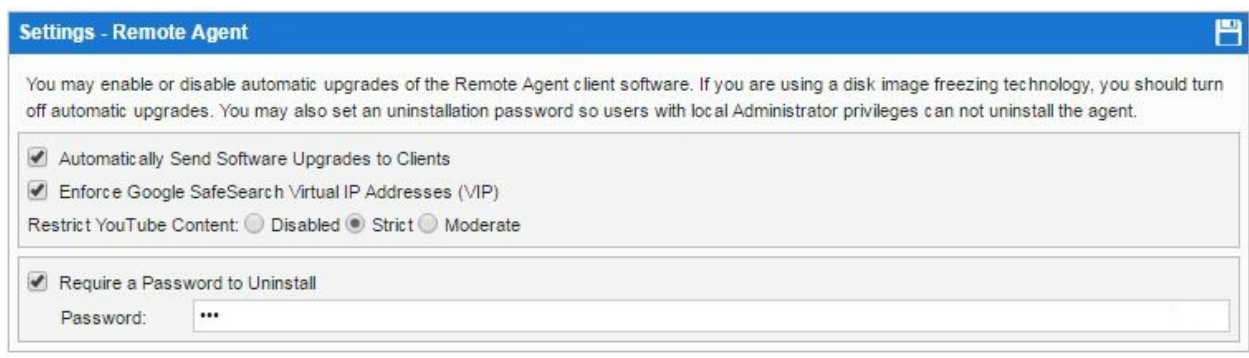
Restrict YouTube Content is similar to the option found in the group policy properties. With these settings, you may restrict the content displayed on YouTube. By enforcing Strict or Moderate modes, the Remote Agent will rewrite DNS entries for YouTube, enforcing these modes when viewing or searching for content from within YouTube. Videos on YouTube that are flagged as Mature Content will not be played. This is a Remote Agent based setting and will affect all Remote Agent users regardless of Group and Policy settings, so long as you are allowing the Streaming Media category. For a detailed description on restrict YouTube DNS rewrites, see the associated Google support article.

<https://support.google.com/youtube/answer/6214622>

For a detailed description on what YouTube considers Moderate or Restrict, please see the associated Google support article.

<https://support.google.com/youtube/answer/174084>

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.



SSL Inspection

Here you can enable SSL Inspection for all of your Remote Agents. SSL Inspection will be performed on the end user's workstation instead of inline at the appliance. The Remote Agent will download and install the NetSpective CA Certificate as well.

After enabling SSL Inspection for Remote Agents, there are two more areas you can optionally configure. You may exclude IP ranges from being inspected as well as exclude Application from being inspected. Some applications or servers refuse to respect a third party's certificate and will only use their own. The Google Drive application and Dropbox app are good examples of programs that should be exempt from SSL Inspection. Simply use the Add button and enter the exact file name of the application or IP address range you do not wish to perform SSL Inspection on.

Settings - Remote Agent

These settings affect how your Remote Agents decide whether to inspect (e.g. decrypt and re-encrypt) SSL traffic. These setting will be combined with each user's policy selections regarding which categories to inspect.

☒ Enable SSL Inspection for Remote Agents

Address Range Exceptions - Remote Agent

Address Ranges

<input type="checkbox"/>	10.0.0.0/8	10.0.0.0 - 10.255.255.255
<input type="checkbox"/>	10.5.0.0/16	10.5.0.0 - 10.5.255.255
<input type="checkbox"/>	10.5.1.0/24	10.5.1.0 - 10.5.1.255
<input type="checkbox"/>	10.5.1.1/32	10.5.1.1 - 10.5.1.1

Application Exceptions - Remote Agent

Applications

<input type="checkbox"/>	googledrivesync.exe
--------------------------	---------------------

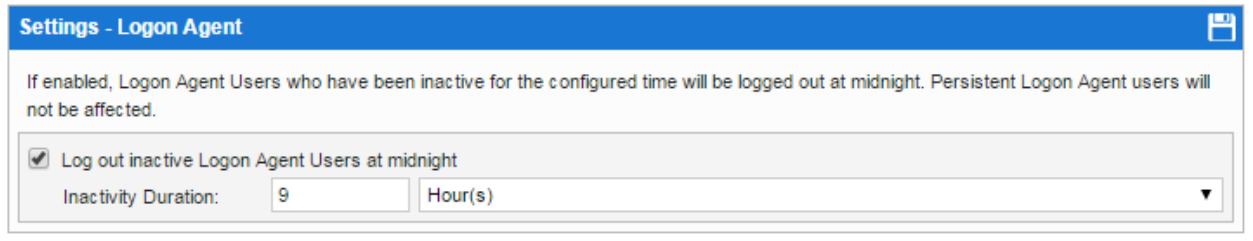
Logon Agent

The NetSpective Logon Agent is an executable used to map an authenticated user name to one or many IP addresses assigned to the device accessing the network. The Logon Agent sends packets over UDP to a corresponding processing application on the NetSpective appliance. This creates a Username to IP Address association inside of the appliance. When NetSpective sees traffic on the wire, it is able to see the IP addresses of those users and associate it with their group and apply the content filtering policy. Different editions of the logon agent exist for Windows, Macintosh, and remote computers. Ideally the Logon Agent should be placed in specific shared folders on the domain controller. The application can then be called from a default logon script (.bat or .cmd) file or from the directory service group policy object.

The logon Agent has multiple modes of operation, each of which can be tailored using simple command line arguments. Flexible options enable administrators to customize the behavior of the application including executing and terminating immediately where NetSpective processes the information with minimal overhead and no network burden generated by the application. Persistent modes of execution also exist for dynamic handling of mobile devices in DHCP environments.

All Logon Agent and Remote Agents send packets over UDP to a corresponding NetSpective appliance. Since NetSpective processes the information with minimal overhead, the network will not be burdened with the traffic generated by the application. The Logon Agent will NOT download and install any CA Certificates. Certificates will need to be deployed manually or through GPOs if you are using the Logon Agent and wish to perform SSL Inspection.

The Logon Agent Settings area allows you to log out users at midnight if they have been inactive for the specified duration.



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.

Settings - Mobile Browser

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.

User ID Scheme:

Device Name

LDAP Logon Prompt:

Mobile Filter Authentication

Logon Agent Inactivity:

20

Minute(s)

☒ Allow each iPad to define their own additional attachment file types

Attachment File Types - Mobile Browser

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.

Attachment File Types

☐ pdf

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.

Agent Downloads

NetSpective comes with certain utilities you may download to assist in network integration and monitoring. Available utilities and settings include DNS Agent for Windows Servers, Windows, and macOS, Remote Agent for Windows and macOS, the Remote Agent Configuration File, and the Terminal Server Agent.

Agent Downloads		
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
DNS Agent for Windows Servers (2008 - 2016)	1.5.13	DNSAgent-1.5.13.msi
Logon Agent for Windows (XP, 7, 8, 10)	3.0.11	LogonAgent-3.0.11.zip
Logon Agent for macOS (10.9 - 10.12)	2.3-15	LogonAgent-2.3-15.dmg
Remote Agent for Windows (7, 8, 10)	1.5.63	RemoteAgent-1.5.63.msi
Remote Agent for macOS (10.9 - 10.12)	2.3.9	RemoteAgent-2.3.9.dmg
Remote Agent Configuration File	20170110113153	Configuration
Terminal Server Agent for Windows & Citrix	3.0.4	TerminalServerAgent.exe
Wi-Fi Agent	N/A	Contact NetSpective Support

NetSpective User Guide 113

Google Sign-In

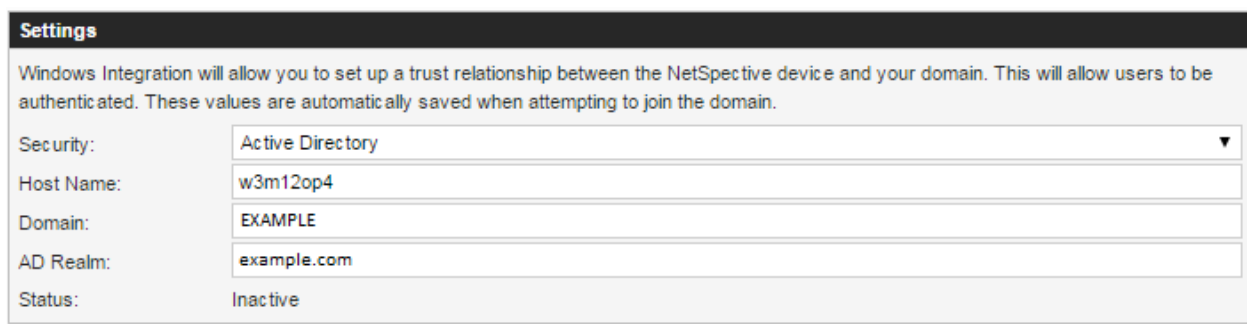
The Google Integration section allows NetSpective to communicate to a Google Apps for Education domain. By doing this, we can provide features specific to Google domains and Google devices.

The Client Settings are used to leverage Google Sign-In with our Mobile Portal. By doing this, the portal will display a Google Sign-In icon that users are familiar with. The portal can then authenticate this user against the Google domain to associate their Gmail address with their IP address. This is a single sign-on method of authentication and the user can be re-validated transparently. Allowed Domains can then be used to limit the domains your users are authenticating with.

Due to the rapid changes to the Google Admin and Google Developer consoles, a separate documentation is kept for deploying Google Authentication, so that it may be updated more frequently. Please see our [NetSpective Sign-In with Google and Google Apps Directory Synchronization](#) document for more information.

Windows Integration

Windows Integration allows you to set up a trust relationship between the NetSpective device and your domain. This is required for Windows NTLM authentication for both the captive portals as well as session based authentication on the proxy solution. These are typically desired as they allow credentials to be cached within a web browser for Single Sign On Authentication. When setting up Windows Integration, a domain user with sufficient privileges is required to add the NetSpective device to the domain.



The screenshot shows a 'Settings' window for Windows Integration. It contains a descriptive text at the top and several input fields. The 'Security' field is a dropdown menu set to 'Active Directory'. The 'Host Name' field contains 'w3m12op4'. The 'Domain' field contains 'EXAMPLE'. The 'AD Realm' field contains 'example.com'. The 'Status' field is labeled 'Inactive'.

Settings	
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. These values are automatically saved when attempting to join the domain.	
Security:	Active Directory ▼
Host Name:	w3m12op4
Domain:	EXAMPLE
AD Realm:	example.com
Status:	Inactive

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 "example.com", and NetSpective's host name in your network is 'mynetspective', you must create a DNS Host Record for "mynetspective.example.com". Also, you must ensure that your AD Realm (example: "example.com") 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: example)

AD Realm (Active Directory Only)

The Active Directory Realm of your network. (Example: example.com)

Status

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

Directory Sources

Directory sources are used to easily populate NetSpective with users or managers. Directory sources support bridging to Active Directory, eDirectory, Open Directory, or Google Directory as well as a combination of each as an environment requires. After configuring a source, NetSpective groups can be configured to mirror an Organizational Unit or Group available in that source.

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

Due to the rapid changes to the Google Admin and Google Developer consoles, a separate documentation is kept for configuring a Google Directory, so that it may be updated more frequently. Please see our [NetSpective Sign-In with Google and Google Apps Directory Synchronization](#) document for more information.

Directory Sources			
Directory sources may be used to easily populate users and/or managers. After configuring a LDAP directory source, groups can be configured to mirror an Organizational Unit or Group available in that source. Also, managers can be assigned and may use their source password to log on.			
<input type="checkbox"/> Source	Server	Type	Status
<input type="checkbox"/> Google	admin@telemate.net	Google	Initializing
<input type="checkbox"/> EXAMPLE	atl01dc1	Disabled	N/A
<input type="checkbox"/> EXAMPLE	10.2.2.48	Active Directory	OK

Creating or Updating Sources

To add a new 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.

11. **Name** – A name to identify the LDAP Source.
12. **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.
13. **IP or Hostname** – The IP or Hostname of the LDAP server. A hostname requires NetSpective to be configured to use a valid DNS Server.
14. **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.
15. **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 DNs

Type	Login DN
Active Directory	example\joe.smith
Active Directory	cn=NetSpective LDAP,cn=Users,dc=example,dc=com
Active Directory	cn=Joe Smith,ou=Development,ou=Example.Com,dc=example,dc=com
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.

3. **Password** – The password to authenticate the Login DN.
4. **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=example,dc=com
eDirectory	o=test
Open Directory	dc=xserve,dc=com
Google OAuth2	

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

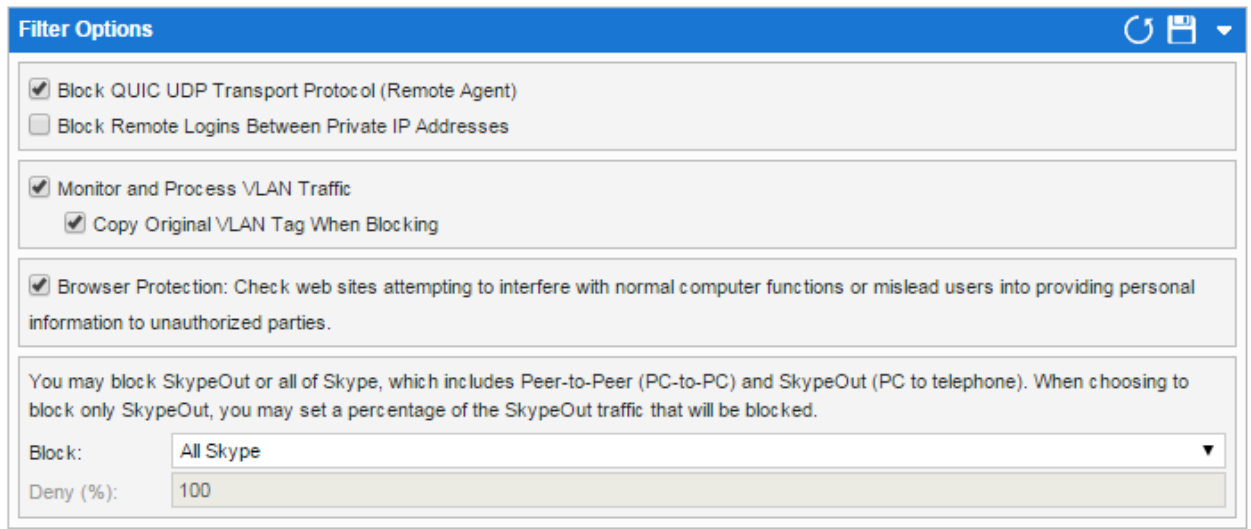
To delete LDAP sources select the check box next to each source's name. To delete all LDAP sources displayed on the current page, select the check box in the upper left-hand portion of the table. Once the sources are selected, click the Delete button to delete the sources. If all LDAP Sources on a page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

Settings

Filter Options

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



The screenshot shows the 'Filter Options' dialog box with a blue header bar containing a refresh icon, a save icon, and a dropdown arrow. The dialog is divided into several sections. The first section contains two checkboxes: 'Block QUIC UDP Transport Protocol (Remote Agent)' which is checked, and 'Block Remote Logins Between Private IP Addresses' which is unchecked. The second section contains 'Monitor and Process VLAN Traffic' (checked) and a sub-option 'Copy Original VLAN Tag When Blocking' (checked). The third section contains 'Browser Protection: Check web sites attempting to interfere with normal computer functions or mislead users into providing personal information to unauthorized parties.' (checked). The fourth section contains explanatory text about blocking SkypeOut or all of Skype, followed by a 'Block:' dropdown menu set to 'All Skype' and a 'Deny (%)' text box set to '100'.

Block QUIC UDP Transport Protocol

By default this option is checked. By blocking the QUIC protocol, Chrome will downgrade its connection to the target website from using QUIC to SSL/TLS, which can be decrypted with the Inline solution and Remote Agents. If this option is unchecked, surfing to any of Google's properties will likely result in an error.

QUIC (Quick UDP Internet Connections, pronounced quick) is an experimental transport layer network protocol designed by Google. QUIC was designed to provide security protection equivalent to TLS/SSL, along with reduced connection and transport latency, and bandwidth estimation in each direction to avoid congestion. QUIC's main goal is to improve perceived performance of connection-oriented web applications that are currently using TCP.

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

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

Copy Original VLAN Tag When Blocking

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.

Note: The NetSpective admin interface must be on VLAN0. The default/native VLAN on Cisco switches is VLAN 1.

Browser Protection

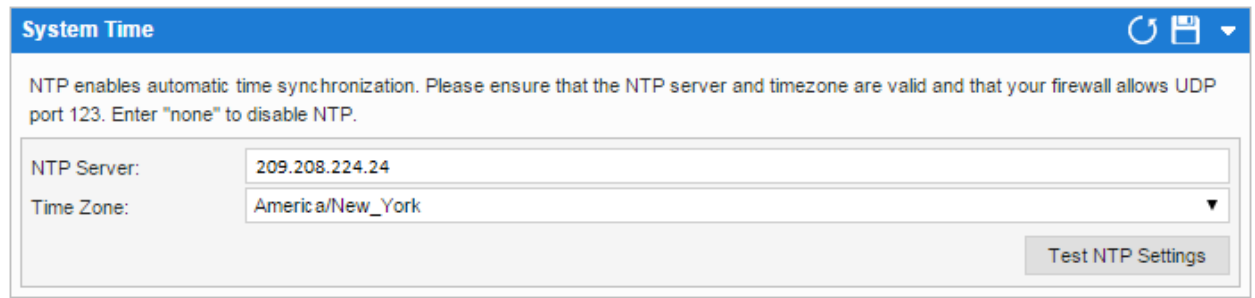
NetSpective Browser Protection checks for web sites attempting to interfere with normal computer functions or mislead users into providing personal information to unauthorized parties. If you enable this option, NetSpective will enable the 'Malware' and 'Phishing' categories and configure all group policies 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

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.

System Time

NetSpective can use an NTP server to automatically keep its internal clock synchronized. By default, it will synchronize to NetSpective Online Service'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.



The screenshot shows the 'System Time' configuration window. At the top, there is a blue header with the title 'System Time' and icons for refresh, save, and a dropdown arrow. Below the header, a text box contains the instruction: '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.' Below this, there are two input fields: 'NTP Server:' with the value '209.208.224.24' and 'Time Zone:' with a dropdown menu showing 'America/New_York'. A 'Test NTP Settings' button is located at the bottom right of the form.

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.

The image shows a 'SNMP Configuration' window. It has a blue title bar with the text 'SNMP Configuration' and three icons on the right: a refresh icon, a download icon, and a save icon. Below the title bar is a form with a checkbox labeled 'Enable SNMP' which is checked. Below the checkbox are two text input fields. The first is labeled 'Allowed Network/Mask:' and contains the text '10.2.0.0/16'. The second is labeled 'Community:' and contains the text 'public'.

Configuration

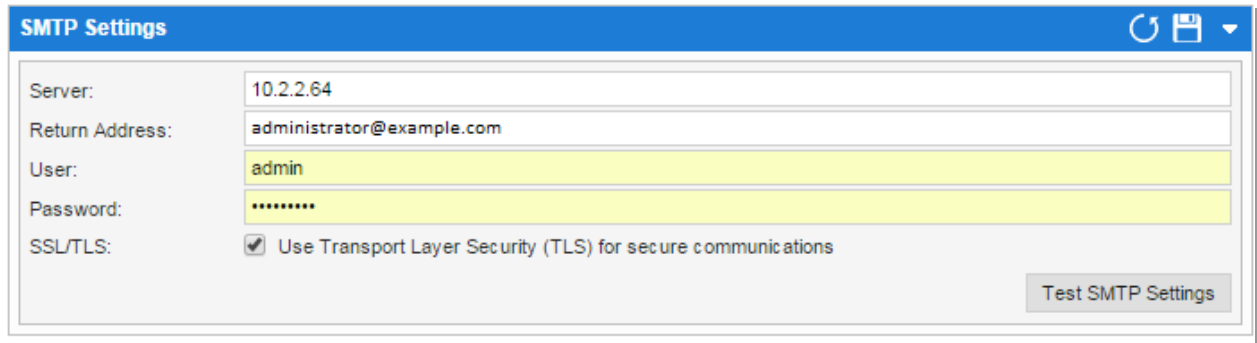
The SNMP service is disabled by default so that you may optionally configure any security settings before starting it. All SNMP information is read-only but access may be further restricted to a specific Network/Mask and/or a custom Community string.

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

SMTP Settings

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



The screenshot shows a window titled "SMTP Settings" with a blue header bar containing a refresh icon, a save icon, and a dropdown arrow. The main area contains several input fields: "Server:" with the value "10.2.2.64", "Return Address:" with "administrator@example.com", "User:" with "admin", and "Password:" with masked characters "*****". Below these is a checkbox labeled "SSL/TLS:" which is checked, with the text "Use Transport Layer Security (TLS) for secure communications" to its right. A "Test SMTP Settings" button is located in the bottom right corner.

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. This is, however, required in some situations, such as using Gmail as your SMTP server. If you need to use a different port, enter the server and port separated with a colon, like smtp.gmail.com: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.

SIP Options

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

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".

Google Apps

The Google Apps Allowed Domains allows you to specify the domain a user can use a Google application with. Users will only be able to log into apps such as Drive and Gmail, with an account that uses the domain specified here. This is helpful in Google Apps for Education classrooms to prevent students from logging with their personal Google account to Gmail or Drive, where they may be hosting objectionable material.

Due to the rapid changes to the Google Admin and Google Developer consoles, a separate documentation is kept for deploying Google Authentication, so that it may be updated more frequently. Please see our [NetSpective Sign-In with Google and Google Apps Directory Synchronization](#) document for more information.

Network

Settings

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.

Traffic

The appliance by default will only filter traffic. SSL inspection is disabled until it is properly set up and enabled in this section. We have provided the ability to disable each of these functions from within the web interface.

Monitored is any traffic that the appliance can perform filtering upon. This includes filtering for HTTP, HTTPS, any protocols we support, and across all ports. Do not confuse this with “Managing” HTTPS traffic. With Monitored, we can identify and block HTTPS traffic, but we will not be decrypting the SSL session to see traffic within the tunnel.

Managed is strictly the function of performing inspection upon SSL traffic. Without this, we will not see traffic inside of an SSL tunnel. Managed is disabled by default due to a number of settings that must be created by the Administrator, such as DNS and Certificate Authority. Once these are configured, the Managed toggle can be switched from Off to On.

Traffic		
Monitored	Inspected traffic that can be filtered. Note: Turning Monitored off will cause traffic to not be inspected and filtering policy will not be enforced.	ON
Managed	SSL traffic that is being diverted and inspected for filtering policy enforcement. Note: Turning Managed off will prevent future sessions from being inspected and handled.	ON

Settings

☐ Allow IPv6 Network Interfaces and Static Routes

Interfaces

Changing an interface's IP or netmask will require a restart of system services which may take a few minutes.

Interface	Description	Status	Mac Address
eth0	Admin	1000 Full	00:50:56:26:1b:8f
Admin:	10.2.40.152	255.255.255.0	
Admin VLAN 1:	10 192.168.126.3	255.255.255.0	
Admin VLAN 2:	11 192.168.126.0	255.255.255.0	
Internal:	IP Address, eg. 192.168.1.10	255.255.255.255	
eth1	External	down	00:50:56:2b:a7:53
External:	IP Address, eg. 192.168.1.10	Netmask, eg. 255.255.255.0	

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. For more information on clustering, see the clustering help page.

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.

Uplink \ Downlink Interfaces (Inline Only)

NetSpective Inline takes advantage of two interfaces. ETH2 and ETH3 are bypass ports which will fail open in the event of hardware failure. Alternatively, ETH4 and ETH5 can be utilized to fail closed in the event of hardware failure. Each Ethernet port in the pair can send traffic upstream to your firewall, or downstream to your local area network, and are interchangeable.

Default Gateway

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

Default Gateway

Default Gateway: 10.2.40.1

DNS

You may enter a list of DNS servers to use and a list of DNS Search Domains. For example, a search domain of "example.com" will allow a short hostname of "intranet" to resolve to "intranet.example.com". 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.

DNS Servers

DNS Servers will allow you to use hostnames in addition to IP addresses for other settings, such as the Logging FTP server.

Server
<input type="checkbox"/> 10.2.2.49
<input type="checkbox"/> 10.2.2.48
<input type="checkbox"/> 8.8.8.8

DNS Search Domains

DNS Search Domains will allow you to use a short hostname of "intranet" to resolve to "intranet.example.com" a search domain of "example.com" is provided.

Search Domain
<input type="checkbox"/> example.com

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.

Additional Routes

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

Destination	Netmask	Gateway	Interface
<input type="checkbox"/> [New Network Route]			

Enter a valid route, for example a destination of "192.168.10.0", a netmask of "255.255.255.0", and a gateway of "192.168.5.1". The gateway must be reachable through a configured interface.

Address: 10.2.40.10

Netmask: 255.255.255.0

Gateway: 10.2.40.1

Interface: Admin

Add a Network Route

To create a network route, click the Add button. To edit a route, click the network route. Once the dialog has opened, update the necessary information:

Address: 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.

Interface: Specify the network interface that should use this additional route.

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.

Monitored Zones

The NetSpective must identify which zones on your network it should provide filtering for. You will see three examples of private IP zones to be filtered. You may delete these examples and enter ones specific to your network, excluding any zones you do not wish to filter. Please ensure you add both IPv4 and IPv6 zones in this area.

Monitored Zones			
Monitored Network Zones are IP ranges that are filtered and/or monitored. IP Addresses not included in the specified zones will not be monitored and not have a policy enforced.			
<input type="checkbox"/>	VLAN	Network	Range
<input type="checkbox"/>		::/128	:: - ::
<input type="checkbox"/>		192.168.0.0/16	192.168.0.0 - 192.168.255.255
<input type="checkbox"/>		172.16.0.0/12	172.16.0.0 - 172.31.255.255
<input type="checkbox"/>		10.0.0.0/8	10.0.0.0 - 10.255.255.255

You may also create network zones that should be excluded from filtering. These ranges can overlap with included ranges and will take higher precedence so that they will be applied first. This is helpful for excluding servers and internal websites from being filtered and managed.

Logging

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.

Field	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 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.

Field	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

URL:

ftp-example.telemate.net

User Name:

anonymous

Password:

Directory:

/uploads/webfilter-logs

Encrypt:

☒ Encrypt the log files before transfer.

Schedule:

☒ Once a day at

11:00 pm

☐ Every

1

Hour(s)

☐ Every

5

Minutes

Transfer Logs

Purge Logs

Field	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.

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.

Editing Block Text

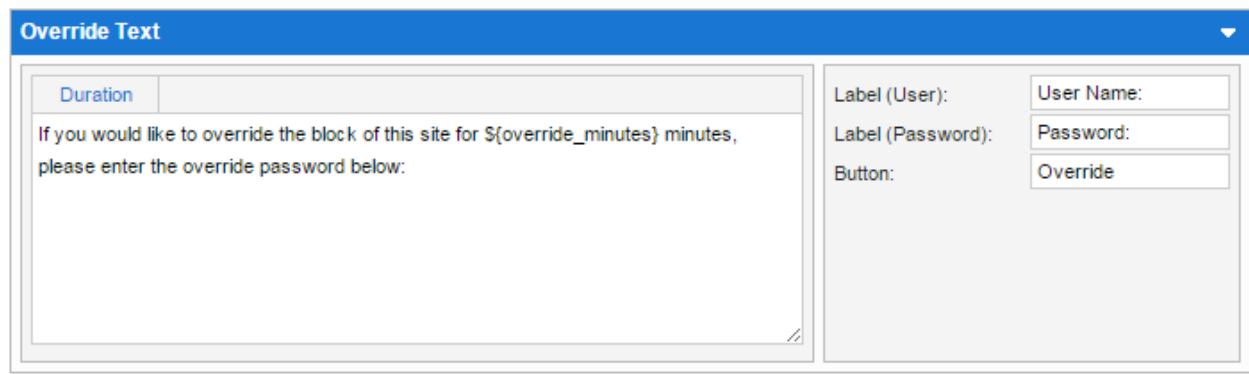
The text is displayed on the block page when a user visits a blocked URL. There are special tags available that will provide information specific to the user or blocked URL. The tag information is listed below:

Tag Name	Text	Description
URL	[blockedurl]	Inserts the blocked URL.
Blocked	[category]	Inserts the blocked category.
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	Text	Description
Override Duration	[duration]	Inserts the duration, in minutes, the override will last.

Next to 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.

Editing Request Text

The request text is only displayed if the user's group has the request category change enabled. The text is displayed on a separate page accessed from a link in the upper left corner of the block page.

On the request category change pane the text can be customized in the Label (Back) field. On the block page the text can be customized in the Label (Request) field.

Next to the request text on the request category change pane are fields to rename the category label, comment label and the button text. The text for the Category label can be set in the Label (Category) field. The text for the comment label can be set in the Label (Comment) field. The submit button text can be set in the Button field.

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.

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	Text	Description
URL	[blockedurl]	Inserts the blocked URL.
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.

Certificate Download

You can now also enable a link to “Show CA Certificate Download and Install Instructions”. This page will now also show a link where users can download the certificate, as well as a set of instruction for installing the certificate on various mobile devices. If you wish to inspect SSL traffic on devices that log on your network, but are not owned by your organization, this page will be necessary for users to install the certificate. You can learn more about these certificate deployment options under [Deploying the CA Certificate on Mobile Devices](#).

Certificate Download

☐ Show CA Certificate Download and Install Instructions

Standard Portal

NetSpectre 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.

Authentication Text

```

<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>

```

Label (Title):
 Label (User):
 Label (Password):
 Button:

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

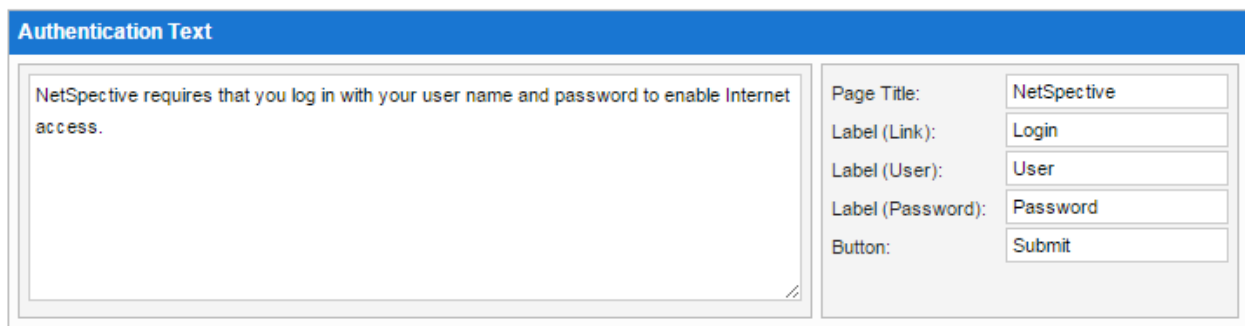
There are fields to rename the login title label, user name label, password label and submit button text. The text for the login title label can be set in the **Label (Title)** field. The text for the user name label can be set in the **Label (User)** field. The text for the password label can be set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



Authentication Text	
NetSpective requires that you log in with your user name and password to enable Internet access.	Page Title: NetSpective
	Label (Link): Login
	Label (User): User
	Label (Password): Password
	Button: Submit

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

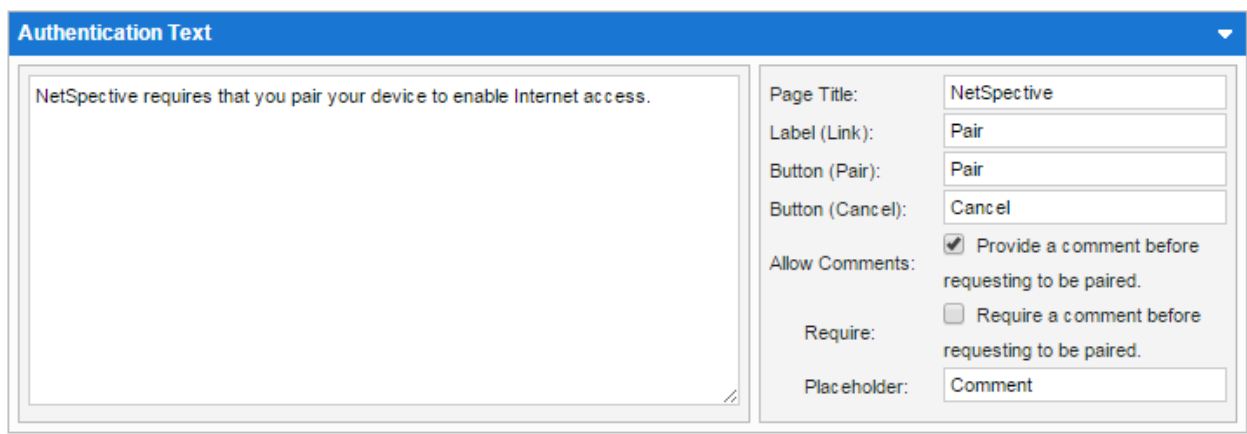
of the page below the Additional Text. The text for the user name label can be set in the Label (User) field. The text for the password label can be set in the Label (Password) field. The submit button text can be set in the Button field.

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 a configuration window titled "Authentication Text". On the left is a large text area containing the text "NetSpective requires that you pair your device to enable Internet access." On the right is a form with the following fields and options:

- Page Title: NetSpective
- Label (Link): Pair
- Button (Pair): Pair
- Button (Cancel): Cancel
- Allow Comments: ☒ Provide a comment before requesting to be paired.
- Require: ☐ Require a comment before requesting to be paired.
- Placeholder: Comment

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".

Certificates

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.

Certificate Details (Self Signed)

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

Issued To

Organization:

Example Company

Organization Unit:

N/A

Common Name:

netspective.test.example.com

Locality:

Atlanta

State/Province:

Georgia

Country:

US

Issued By

Organization:

Example Company

Common Name:

netspective.test.example.com

Locality:

Atlanta

State/Province:

Georgia

Country:

US

SSL Information

Hostname:

netspective.test.example.com

Validity

Issued On:

Oct 2 14:11:12 2015 GMT

Expires On:

Sep 29 14:11:12 2025 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:

Field	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 Create CSR 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-----.

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.

Certificate Authority

To manage SSL sessions, NetSpective needs its own root Certificate Authority (CA) certificate that is trusted on your network. This is necessary so it can create its own copies of web site certificates and present them to users on your network without causing certificate trust errors or warnings in the web browser. By definition all root CA certificates are self-signed, so it is easier and more secure for NetSpective to generate this certificate internally and export it to you to add to your domain's trusted list.

CA Certificate Details

To manage SSL sessions, NetSpective needs its own root Certificate Authority (CA) certificate that is trusted on your network. This is necessary so it can create its own copies of web site certificates and present them to users on your network without causing certificate trust errors or warnings in the web browser. By definition all root CA certificates are self-signed, so it is easier and more secure for NetSpective to generate this certificate internally and export it to you to add to your domain's trusted list.

Issued

Organization:	Example Company
Organization Unit:	Development
Common Name:	
Locality:	Norcross
State/Province:	GA
Country:	US

Validity

Issued On:	Sep 09 17:52:57 2015
Expires On:	Sep 07 17:52:57 2025

CA Certificate - Downloadable Formats

Certificate (DER):	download
Certificate (PEM):	download
Certificate (PKCS12):	download

Build CA Certificate

Build Website Certificate

CA Certificate Details

The CA Certificate details shows the information for the current certificate authority. If a certificate has been built, you will have the ability to download the public key from a link in the upper right hand corner. For more information on building a CA Certificate, as well as deploying it across your network, see the [Building and Downloading the CA Certificate from NetSpective](#) section.

Build CA Certificate

Build a root Certificate Authority (CA) certificate for NetSpective, so it can create its own copies of web site certificates and present them to users on your network without causing certificate trust errors or warnings in the web browser. To create the CA Certificate, you will need to provide information that you want included in the certificate. To do this click the Build CA Certificate button at the bottom right of the screen. Once the dialog has opened, update the necessary information. The common name is the only required field:

Field	Description
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.
Organizational Unit	The Organizational Unit (OU) field is the name of the department or organization unit making the request.
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	An email address to be included in the certificate.
Common Name	The Common Name is the only required field. The common name is your name or your server's hostname (eg. Example.Com or www.example.com).
Key Size	The key size to sign the Certificate with. Available selections are 1024-bit or 2048-bit

Rebuilding a CA Certificate will remove the previous CA Certificate and create a new one. You will have to add the new CA Certificate as a trusted certificate on your network again.

Build SSL Website Certificate

Once you have created a CA Certificate, you will have the ability to build a new certificate for NetSpective's administration web site signed by the current CA certificate. If you add this CA certificate to your network's trusted list, this will keep you from having to pay a third party like VeriSign to sign the certificate for you. To create the SSL Website Certificate, you will need to provide information similar to that used by the CA Certificate. By default the information is populated from the information in the CA Certificate with the exception of the SSL Hostname. The SSL Hostname is required and is typically contains Host + Domain Name (eg. server.example.com).

Restore the Default CA Certificate Settings

If you have built a CA certificate and wish to restore the default settings, click the Restore Default button from the control bar near the top of the page. Restoring the default settings will delete the current CA certificate and its private key. If you restore the default setting we recommend that you also remove it from your network's trusted root CA list.

If you used this CA certificate to sign NetSpective's admin website certificate, you will need to generate and sign a new one.

Trusted Certificates

When NetSpective manages an SSL session, it must validate web site certificates the same way the web browser does for non-managed sessions. This allows NetSpective to determine whether it should provide a valid trusted certificate for sites like facebook.com versus an untrusted certificate for sites like face-book.com. To properly validate certificates, NetSpective needs to know which Certificate Authority (CA) certificates to trust. The default CA certificates included with NetSpective match the list supported by Microsoft Internet Explorer, but you can disable them and import your own CA certificates if you wish.

Trusted Certificates

Select a certificate file to import. NetSpective supports the PEM (base64 encoded X.509) format, the DER (binary encoded X.509) format, and the PFX (PKCS #12) format. The password is optional, and would only be needed to open PFX files that are password-protected.

NOTE: You may combine several PEM files into one if you wish to import many certificates with one upload. Each certificate in the file needs to start with the "----- BEGIN CERTIFICATE ----" line and end with the "----- END CERTIFICATE ----" line that is used in that format.

Password (Optional):

Import File:

When NetSpective manages an SSL session, it must validate web site certificates the same way the web browser does for non-managed sessions. This allows NetSpective to determine whether it should provide a valid trusted certificate for sites like facebook.com versus an untrusted certificate for sites like face-book.com. To properly validate certificates, NetSpective needs to know which Certificate Authority (CA) certificates to trust. The default CA certificates included with NetSpective match the list supported by Microsoft Internet Explorer, but you can disable them and import your own CA certificates if you wish.

Import a Trusted Certificate

You can import your own trusted certificates. NetSpective supports the PEM (base64 encoded X.509) format, the DER (binary encoded X.509) format, and the PFX (PKCS #12) format. To import a trusted certificate click the Import button at the bottom left of the page. Choose a file to import. The password is optional, and would only be needed to open PFX files that are password-protected.

You may combine several PEM files into one if you wish to import many certificates with one upload. Each certificate in the file needs to start with the "----- BEGIN CERTIFICATE ----" line and end with the "----- END CERTIFICATE ----" line that is used in that format.

Delete or Disable a Trusted Certificate

Only Trusted Certificates that were imported can be deleted. Trusted Certificates provided with NetSpective cannot be deleted only disabled. Disabling a trusted certificate will prevent it from being used as a Certificate Authority to validate certificates.

Enable a Trusted Certificate

If a trusted certificate provided by NetSpective has been disabled, it can be easily re-enabled by selecting the certificates and clicking the Enable button at the bottom of the page. Enabling the certificate will allow NetSpective to start using the Certificate Authority to properly validate certificates.

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.

User Defined Categories	
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.	
<input checked="" type="checkbox"/> User Defined #1	User Defined 1
<input checked="" type="checkbox"/> User Defined #2	User Defined 2
<input type="checkbox"/> User Defined #11	User Defined 11
<input type="checkbox"/> User Defined #12	User Defined 12

Enabling or Disabling User Defined Categories

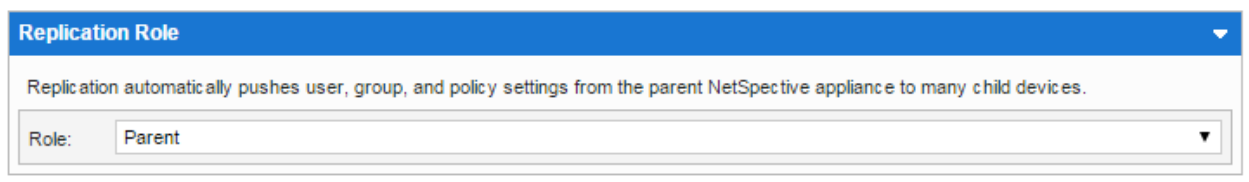
Only an enabled User Defined Category can be seen in the Group Policy page and used in an override. When a User Defined Category is disabled all associated overrides will be deleted. The overrides will not be deleted until the changes are saved.

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 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.

A screenshot of a web interface for configuring a device's replication role. At the top is a blue header bar with the text "Replication Role" and a small downward arrow. Below the header is a light gray box containing the text "Replication automatically pushes user, group, and policy settings from the parent NetSpective appliance to many child devices." Below this text is a form field with the label "Role:" and a dropdown menu. The dropdown menu is currently set to "Parent" and has a small downward arrow on its right side.

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.

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.

Field	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.

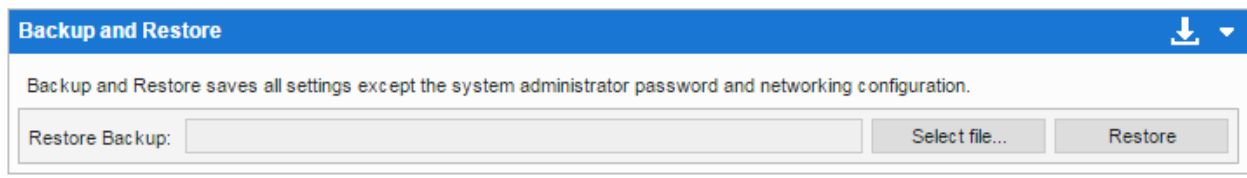
When a node is added, it will be set to Enabled by default. If you do not want the node to receive updates, click the node and uncheck the Enabled checkbox. After a node has been added, a status message will be available to help troubleshoot an error if one should occur. A parent device needs to open 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.

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.



The screenshot shows a web interface titled "Backup and Restore" with a blue header bar. Below the header, a message states: "Backup and Restore saves all settings except the system administrator password and networking configuration." At the bottom, there is a section labeled "Restore Backup:" followed by a text input field, a "Select file..." button, and a "Restore" button.

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.

Automatic Daily Backups

Automatic backups can be transferred via FTP to a server of your choice. When enabled, automatic backups occur daily at 10:00 pm.

☒ Enable Automatic Daily Backups

Status

(No Status)

FTP Settings

IP or Hostname:

38.81.65.36

User Name:

tmpublic

Password:

tmpublic

Directory:

/

Transfer Now

Backup Settings (Download)

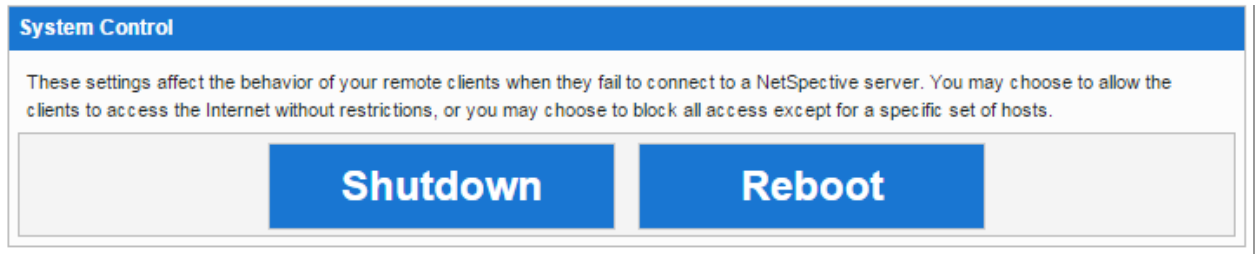
To download a backup of the current device settings, click the "Backup Settings" icon on the toolbar near the top of the page. When your browser's download dialog appears, select where you would like to save the backup file.

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.

System Control

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.



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.

Security

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.

Security Level	Permissions
System Administrator	<ol style="list-style-type: none"> 1. Can create/edit/delete other managers (except admin). 2. Can create/edit/delete Groups and Users. 3. Can edit all of NetSpective's configuration options. 4. Can authorize a temporary override of the block page for any group.
Policy Administrator	<ol style="list-style-type: none"> 5. Can create/edit/delete other managers (except admin). 6. Can create/edit/delete Groups and Users. 7. Can authorize a temporary override of the block page for any group. 8. Can edit all of NetSpective's filtering options.
Group Manager	<ol style="list-style-type: none"> 1. Can edit the group policy for assigned groups and categories allowed by security options. 2. Can edit the group options for assigned groups. 3. Can edit site overrides for assigned groups, if allowed by security options. 4. Can move users between managed groups, but cannot add or remove users or groups. 5. Can authorize a temporary override of the block page for assigned groups.
Mobile Device Manager	<ol style="list-style-type: none"> 6. Can edit mobile pairings for assigned groups.
Block Page Override Manager	<ol style="list-style-type: none"> 1. Can 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.

Manager Properties

The general properties required to set up a NetSpective manager.

1. **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.
2. **Password:** The manager's password. (Not applicable for LDAP Users)
3. **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.

Field	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

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.

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.

Manager Type:	Local
Manager Name:	Local Admin
Password:	*****
Confirm:	*****
Email notifications are available for Managers once an email address is provided. If the manager type is set to Local, you may enter multiple email addresses separated by commas. Otherwise, the email address will be supplied by LDAP.	
Email:	helpdesk@telemate.net
Notifications:	<input checked="" type="checkbox"/> Block Page Bypasses <input checked="" type="checkbox"/> Abuse Lock-downs <input checked="" type="checkbox"/> Override Requests
Security Level:	Group Manager
Groups Managed:	<input checked="" type="checkbox"/> Group A <input checked="" type="checkbox"/> Group B
Grant access to the following sections:	
Grant Access:	<input checked="" type="checkbox"/> Edit User <input checked="" type="checkbox"/> Delete User <input checked="" type="checkbox"/> Set Dynamic IP for Users <input checked="" type="checkbox"/> Set Static IP/Range for Users <input checked="" type="checkbox"/> Change Group Assignment for Users <input checked="" type="checkbox"/> Edit Groups

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.

Manager Type

You can select from Local, Directory Source Group, and Directory Source User. Local managers can be assigned a name and password. Directory Source Group managers are an entire group or OU of users pulled from LDAP and will all be configured with the same manager settings. If you wish for more granular settings, the Directory Source User will assign single LDAP users to become managers.

Email Notifications

Managers can be configured to receive email notifications from the appliance. These include Block Page Bypasses, Abuse Lock-downs, and Override Request notifications. Local managers can be configured with an email address while Directory Source Group and User managers will have their email address pulled from LDAP.

Field	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 Level

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 from the Groups Managed field below.

Grant Access (Group Manager Only)

The Grant Access field 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.

NetAuditor

Your NetSpective is preconfigured with some basic settings to enable the built in Statistics, however, logs are not being archived and will be deleted at midnight without setting up a logging server. 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. Logs are purged from NetSpective every day around Midnight.

For more archival reporting, you will want to install NetAuditor to offload logs and report on them. You can download NetAuditor from the [Settings > Logging](#) section.

NetAuditor 3.x Server Requirements

5. Server or VM OS – Any 64 bit Windows Server OS from 2008 to 2012 r2
6. Desktop or VM OS – Any 64 bit Windows Desktop OS
7. CPU – 2GHz minimum
8. Memory – 4GB minimum
9. Disk Space – Varies depending on the number of devices in a network and the amount of bandwidth being used, as well as how long the logs are to be kept for.
4. Navigate to the Settings heading and click on Logging. Here you can configure Syslog Settings or FTP Settings. Change the Server IP address to the IP of the server you plan on installing NetAuditor on. For Syslog, the recommended settings are Transport Mode - TCP and Timestamp enabled.
5. At the top of the Logging page is a hyperlink to download NetAuditor. Save this executable and install it on a server with sufficient storage space.
6. Once the installation of NetAuditor has finished, a window will pop up asking you how to license the product.
 - a. If you have been licensed for NetSpective reporting only, click Yes.
 - b. 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.
7. Licensing NetAuditor can be done in the right column under Collection Service Settings > Licensing Settings. Simply enter in the information sent to you by NetSpective.
8. Updates for NetAuditor will be downloaded automatically. To install these updates, navigate to the Help menu and click on Install Update.
9. 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.

10. 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. You can also force the creation of your 'NetSpective' process by right clicking on 'NetSpective' under Syslog Server and choosing Create Device.

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