NetSpective Logon Agent Guide

NETSPECTIVE
WEBFILTER
A Grom Educational Services Monitoring Solution
15R
NETSPECTIVE
WEBFILTER
A Grom Educational Services Monitoring Solution
16Hi

GROM
EDUCATIONAL SERVICES

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, Georgia 30092

www.gromedu.com

Table of Contents

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.

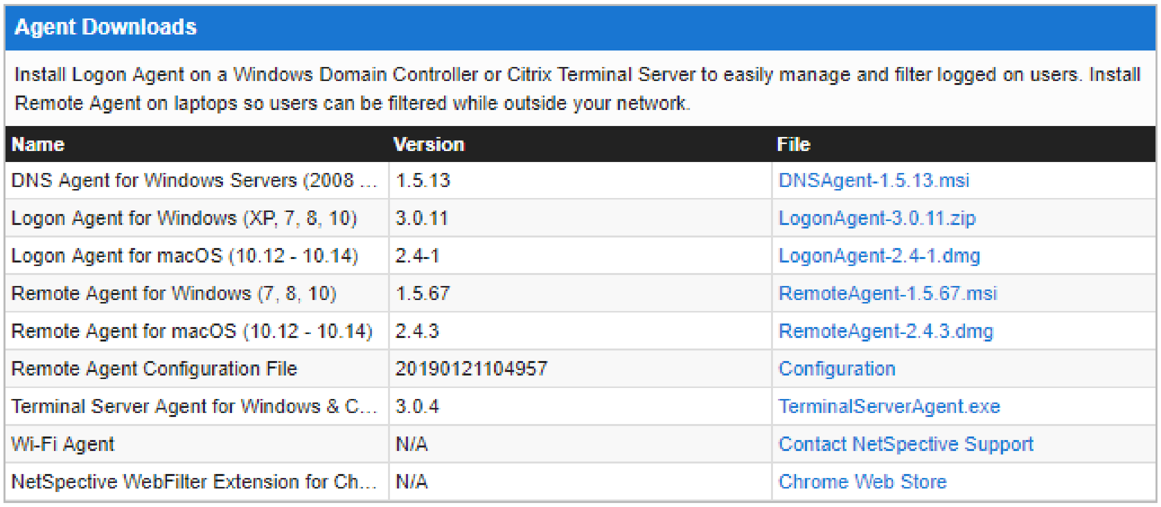
All Logon Agent and Remote Agents send packets over UDP to a corresponding NetSpective appliance. Since NetSpective processes the information with minimal overhead, the network will not be burdened with the traffic generated by the application.

Method 1 - Deploying the NetSpective Logon Agent 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.

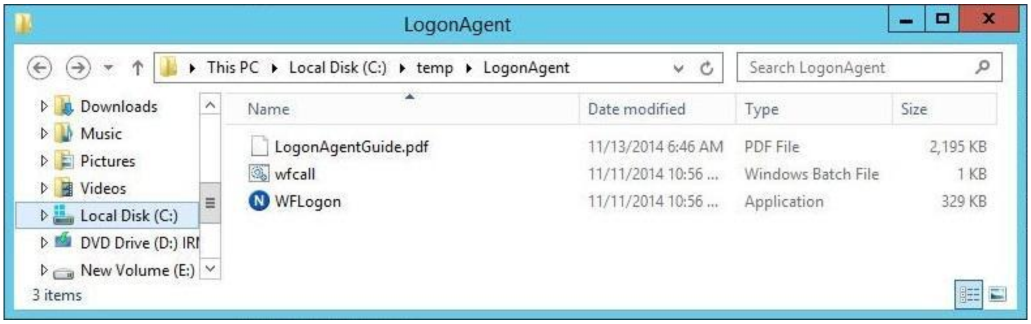


Agent Downloads

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.

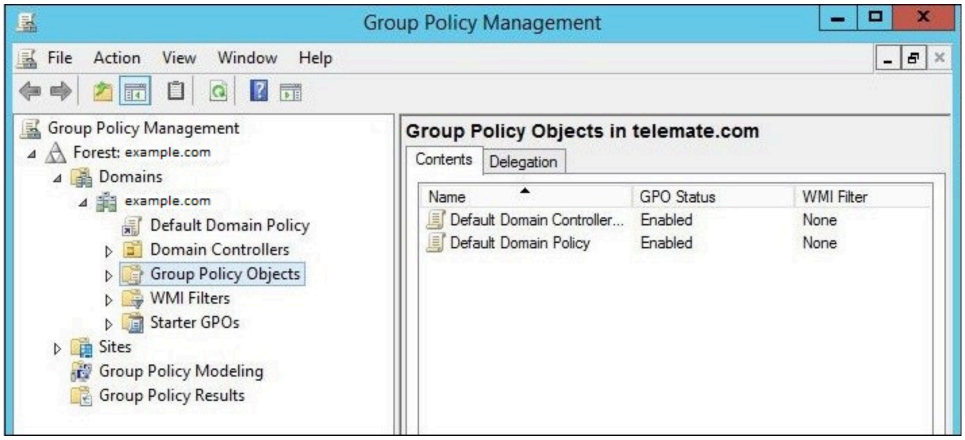
Name	Version	File
DNS Agent for Windows Servers (2008 ...	1.5.13	DNSAgent-1.5.13.msi
Logon Agent for Windows (XP, 7, 8, 10)	3.0.11	LogonAgent-3.0.11.zip
Logon Agent for macOS (10.12 - 10.14)	2.4-1	LogonAgent-2.4-1.dmg
Remote Agent for Windows (7, 8, 10)	1.5.67	RemoteAgent-1.5.67.msi
Remote Agent for macOS (10.12 - 10.14)	2.4.3	RemoteAgent-2.4.3.dmg
Remote Agent Configuration File	20190121104957	Configuration
Terminal Server Agent for Windows & C...	3.0.4	TerminalServerAgent.exe
Wi-Fi Agent	N/A	Contact NetSpective Support
NetSpective WebFilter Extension for Ch...	N/A	Chrome Web Store

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.



Name	Date modified	Type	Size
LogonAgentGuide.pdf	11/13/2014 6:46 AM	PDF File	2,195 KB
wfcall	11/11/2014 10:56 ...	Windows Batch File	1 KB
WFLogon	11/11/2014 10:56 ...	Application	329 KB

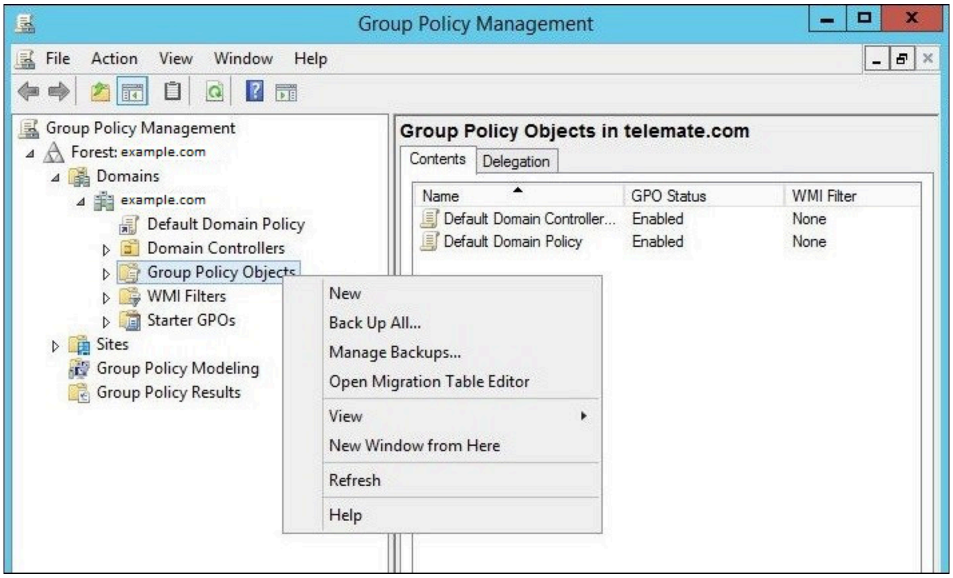
2. Next, access the Windows Server 2012 operating system and select Start, Programs, and Administration Tools, followed by Group Policy Management. Navigate down the domain listing. Select the domain where the users exist that you wish to bridge to the NetSpective Group(s).



Group Policy Objects in telemate.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None

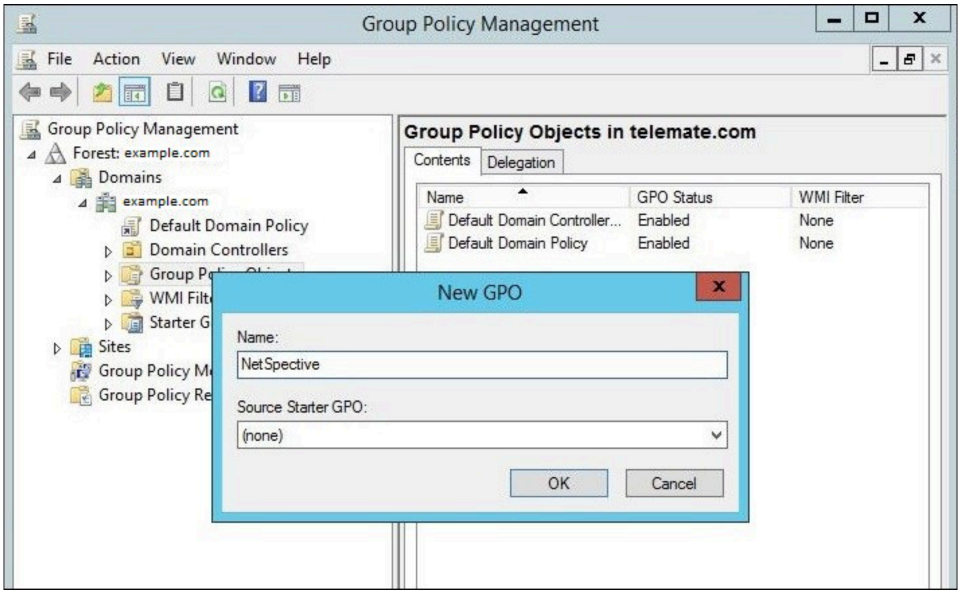
3. Right click on the 'Group Policy Objects' (GPO) and select 'New'.



Group Policy Objects in telemate.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None

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



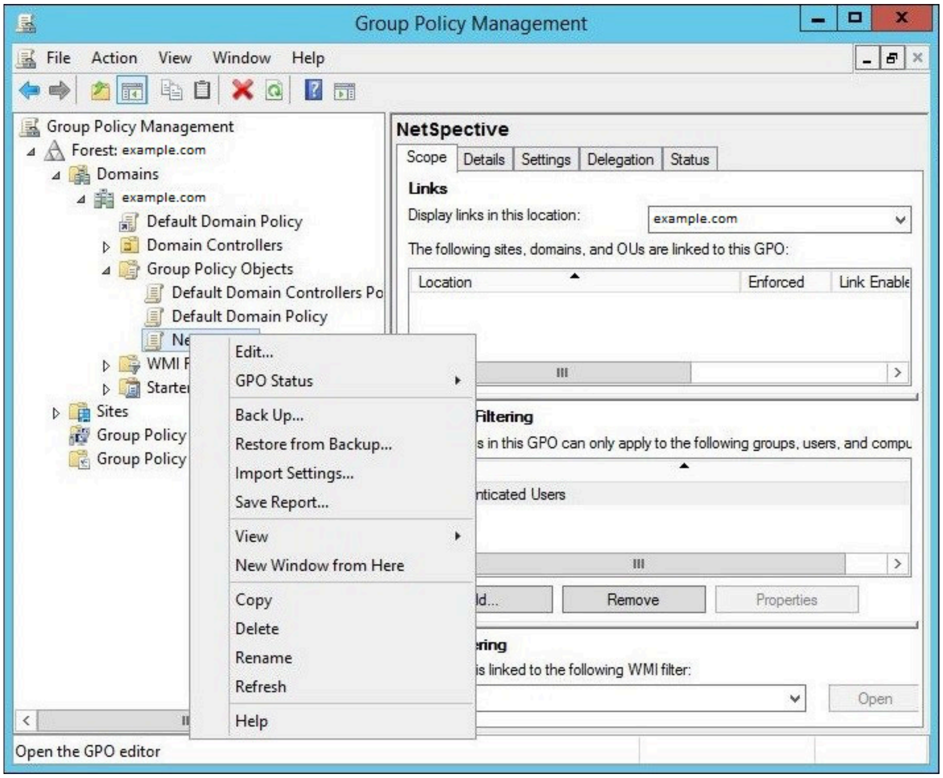
Group Policy Objects in telemate.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None

Name: NetSpective

Source Starter GPO: (none)

5. Select the Group Policy Object tree items and navigate to the ’NetSpective’ group policy object. Right click and select ‘Edit’.



NetSpective

Links

Display links in this location: example.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enable

Filtering

s in this GPO can only apply to the following groups, users, and compu

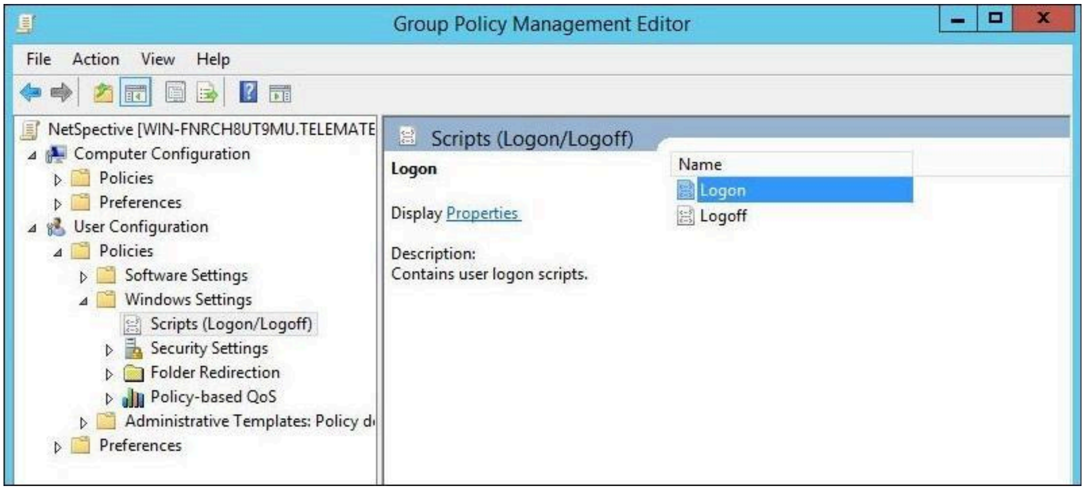
nticated Users

ring

is linked to the following WMI filter:

Open the GPO editor

6. 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 pain of the editor.

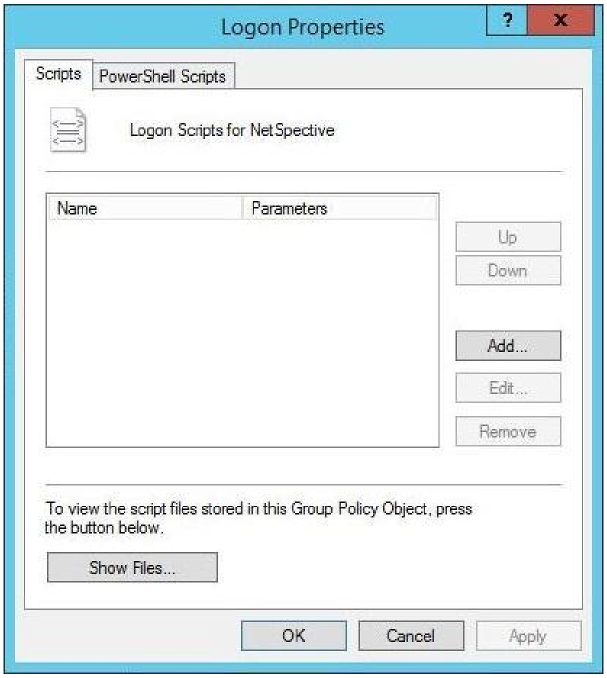


Logon

Display Properties

Description:
Contains user logon scripts.

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



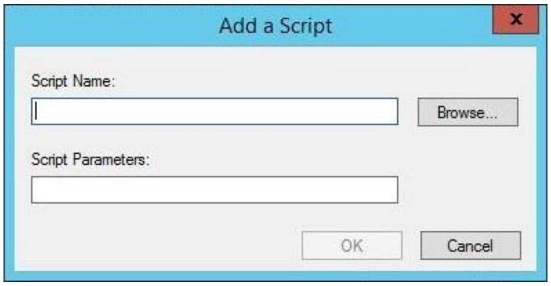
Logon Properties

Scripts | PowerShell Scripts

Logon Scripts for NetSpective

Name	Parameters

To view the script files stored in this Group Policy Object, press the button below.

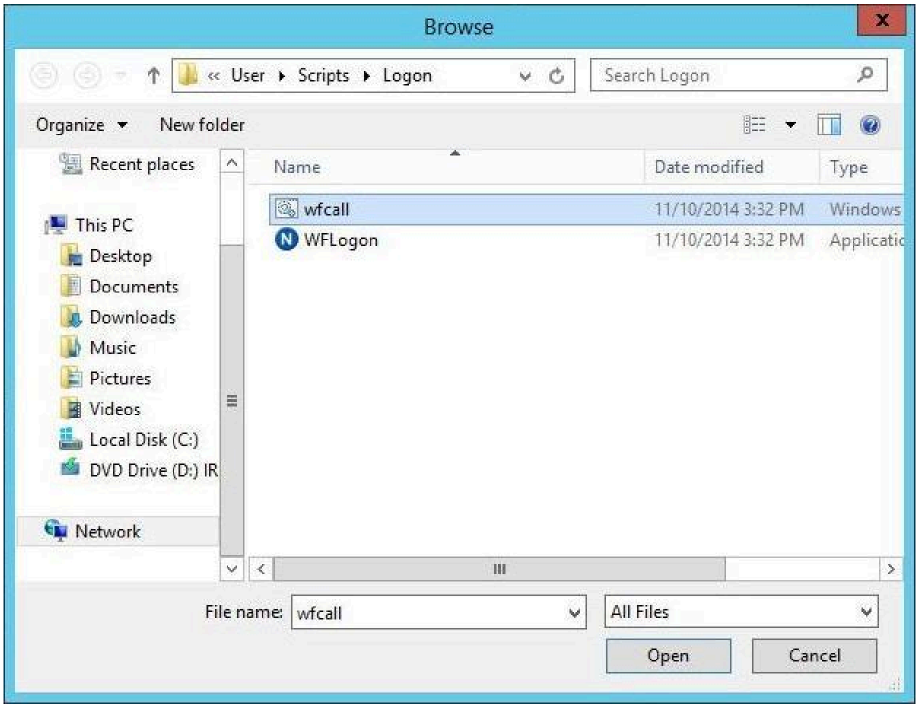


Add a Script

Script Name:

Script Parameters:

8. 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.

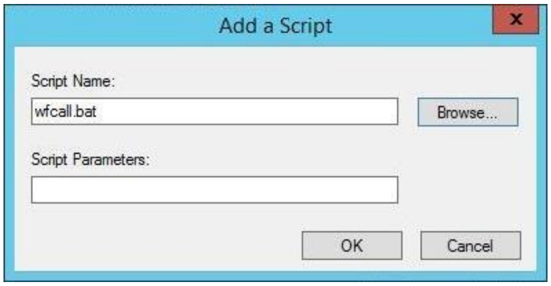


Name	Date modified	Type
wfcall	11/10/2014 3:32 PM	Windows
WFLogon	11/10/2014 3:32 PM	Applicatio

File name: wfcall

All Files

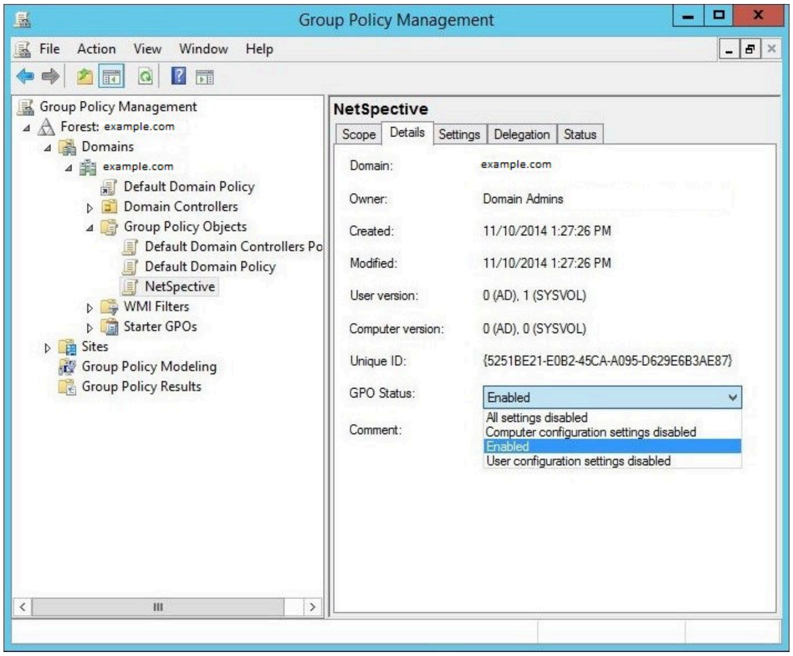
9. Select either the WFCall.bat or WFLogon.exe based on your requirements. Command line parameters are explained below under ‘WFLogon Command Line Parameters’. Once defined select OK to save. Continue the save process until you have returned to the NetSpective GPO in the Group Policy Management dialog.



Script Name: wfcall.bat

Script Parameters:

10. 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.



NetSpective

Domain: example.com

Owner: Domain Admins

Created: 11/10/2014 1:27:26 PM

Modified: 11/10/2014 1:27:26 PM

User version: 0 (AD), 1 (SYSVOL)

Computer version: 0 (AD), 0 (SYSVOL)

Unique ID: {5251BE21-E0B2-45CA-A095-D629E6B3AE87}

GPO Status: Enabled

Comment:

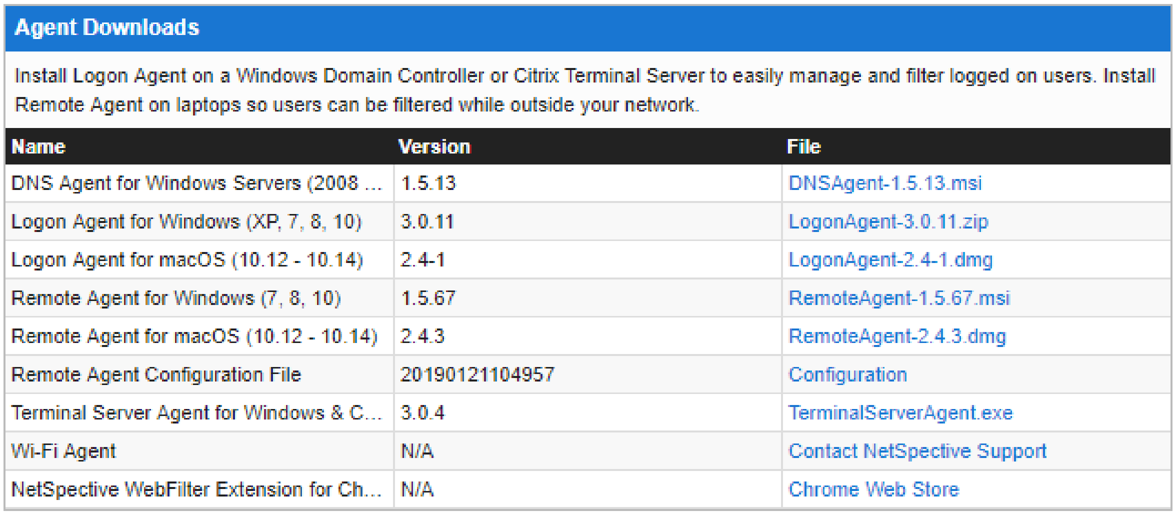
11. Now all users accessing the network will automatically execute the NetSpective logon Script executed based on the parameters provided.

Method 2 - 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.

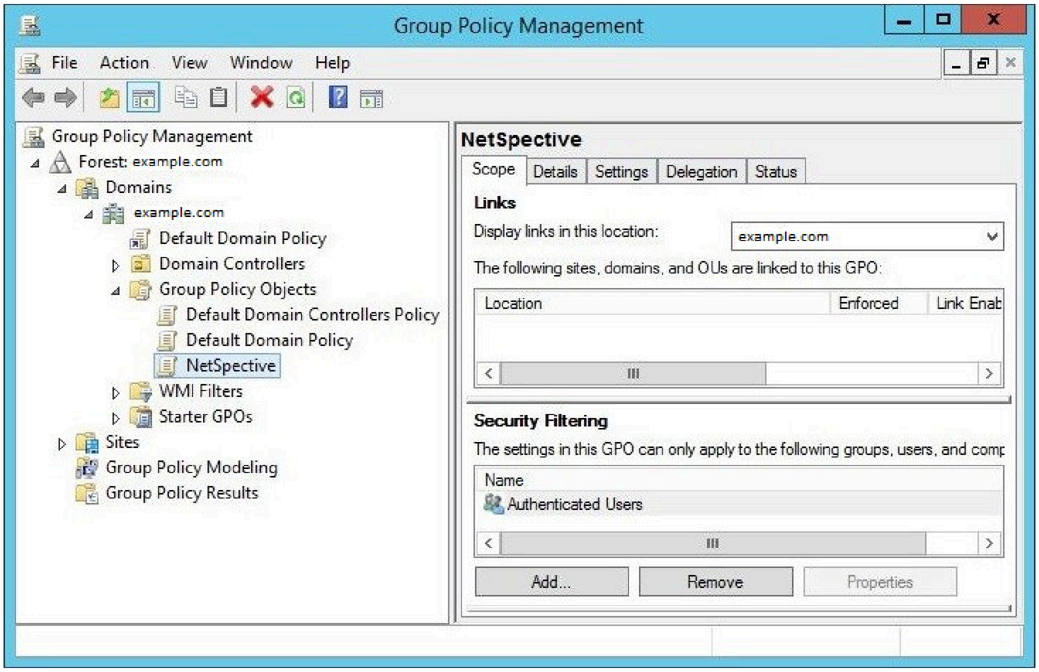


Agent Downloads

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
DNS Agent for Windows Servers (2008 ...	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 (10.12 - 10.14)	2.4-1	LogonAgent-2.4-1.dmg
Remote Agent for Windows (7, 8, 10)	1.5.67	RemoteAgent-1.5.67.msi
Remote Agent for macOS (10.12 - 10.14)	2.4.3	RemoteAgent-2.4.3.dmg
Remote Agent Configuration File	20190121104957	Configuration
Terminal Server Agent for Windows & C...	3.0.4	TerminalServerAgent.exe
Wi-Fi Agent	N/A	Contact NetSpective Support
NetSpective WebFilter Extension for Ch...	N/A	Chrome Web Store

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



NetSpective

Links

Display links in this location: example.com

The following sites, domains, and OUs are linked to this GPO:

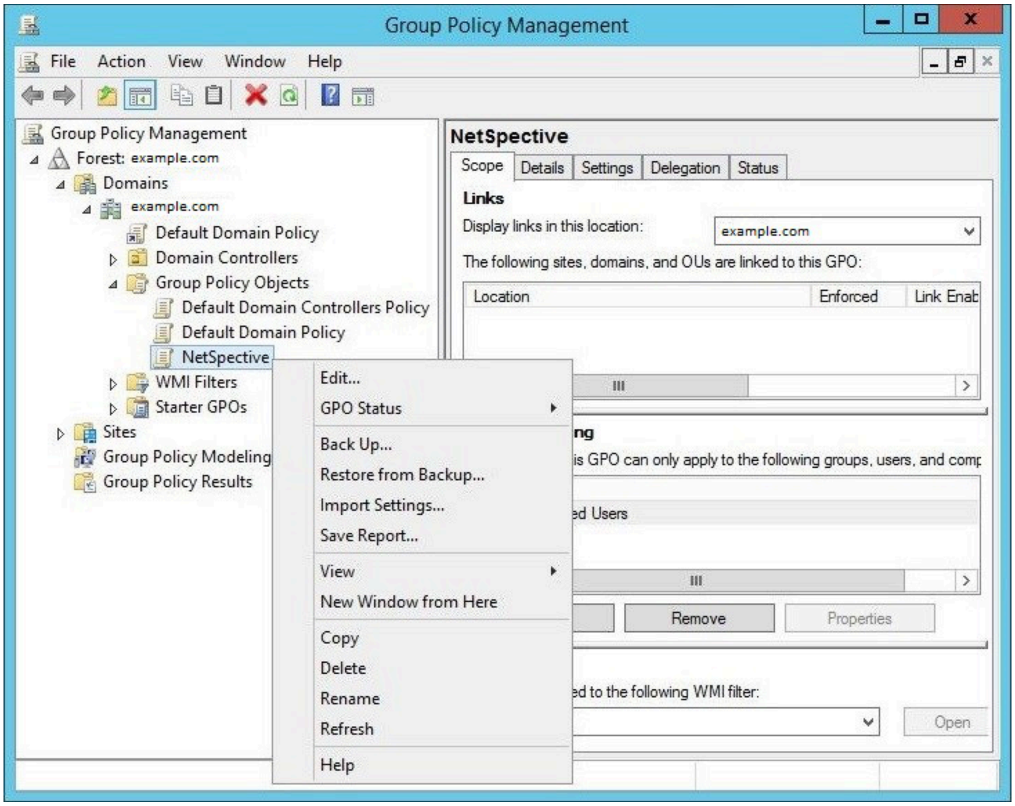
Location	Enforced	Link Enat

Security Filtering

The settings in this GPO can only apply to the following groups, users, and comp

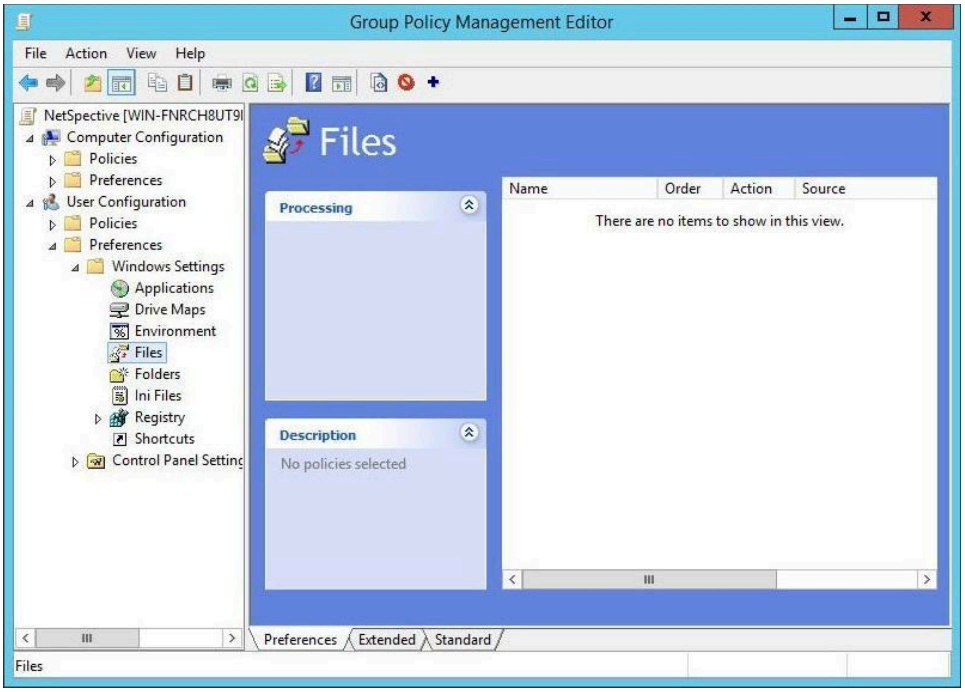
Name
Authenticated Users

3. Right click your Logon Agent GPO and click Edit



3. In the Group Policy Management Editor, navigate to:

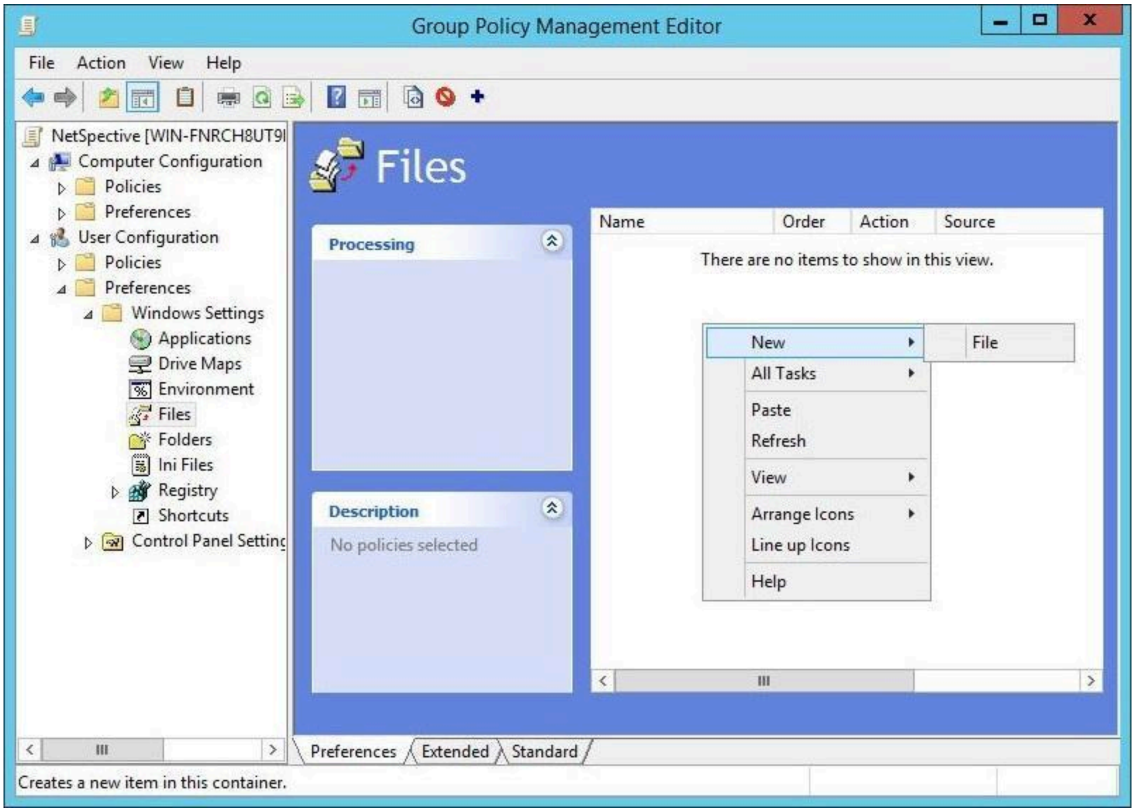
   User Configuration > Preferences > Windows Settings > Files



There are no items to show in this view.

No policies selected

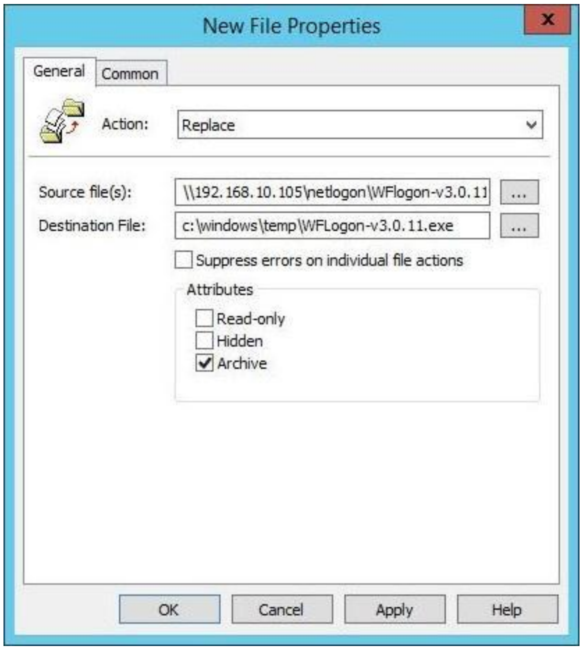
4. In the right pane entitled Files, right click and select New > File



5. 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.



Action: Replace

Source file(s): \\192.168.10.105\netlogon\WFlogon-v3.0.11

Destination File: c:\windows\temp\WFLogon-v3.0.11.exe

□ Suppress errors on individual file actions

Attributes

□ Read-only

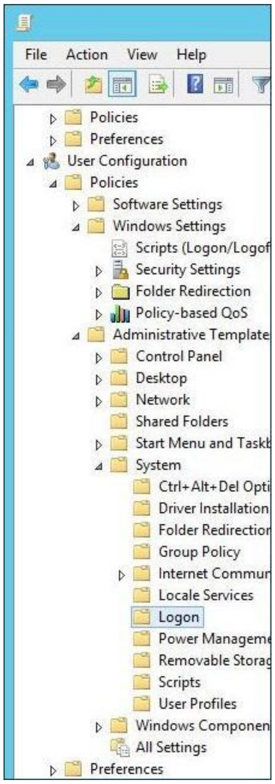
□ Hidden

☑ Archive

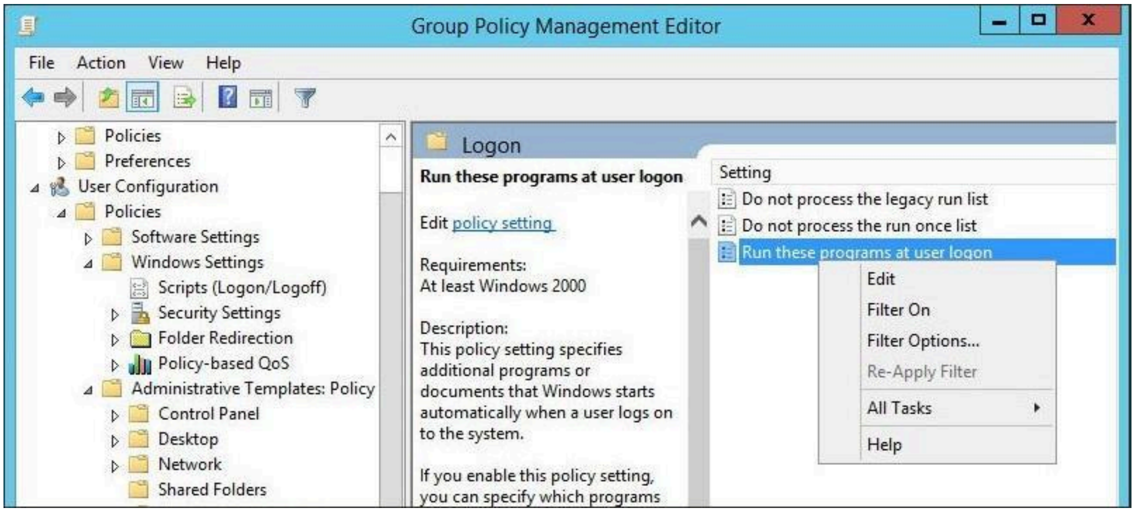
Example Logon Agent file name is WFLogon-v3.0.11.exe. Your Logon Agent file name may be different and must be specified in this field.

When you are finished, click the OK button.

6. Navigate to: User Configuration > Policies > Administrative Templates > System > Logon



7. In the right pane, right click "Run these programs at user logon" and select Edit.



Run these programs at user logon

Edit policy setting

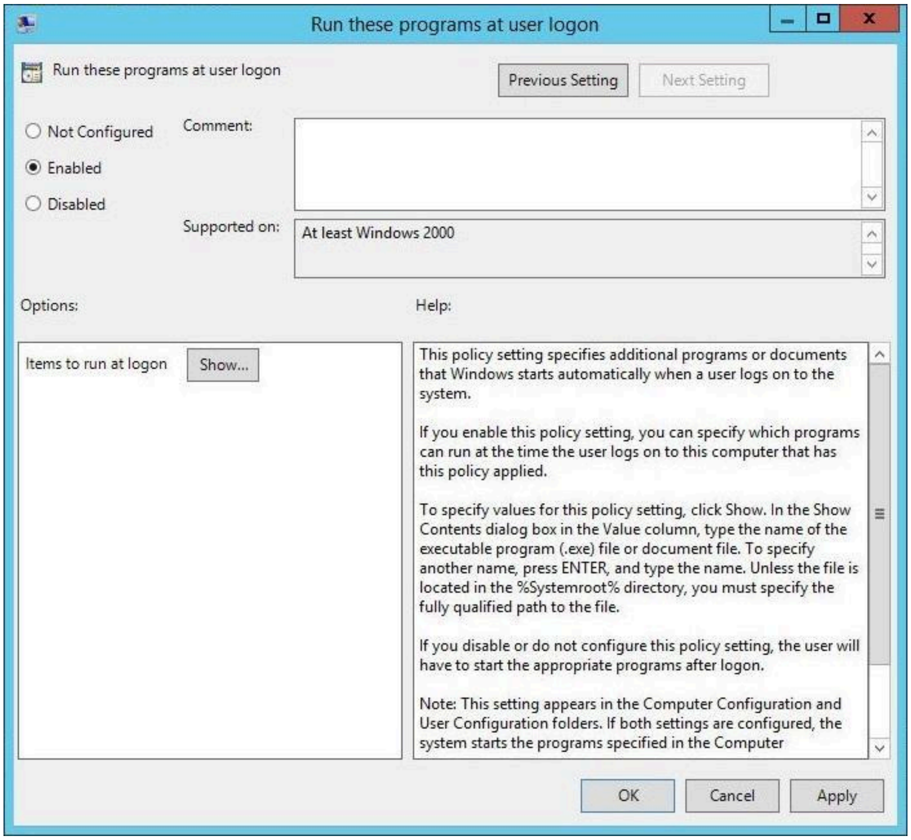
Requirements:
At least Windows 2000

Description:
This policy setting specifies additional programs or documents that Windows starts automatically when a user logs on to the system.

If you enable this policy setting, you can specify which programs

8. In the new windows, select Enable.

Under Options, click the Show button



Run these programs at user logon

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Items to run at logon

This policy setting specifies additional programs or documents that Windows starts automatically when a user logs on to the system.

If you enable this policy setting, you can specify which programs can run at the time the user logs on to this computer that has this policy applied.

To specify values for this policy setting, click Show. In the Show Contents dialog box in the Value column, type the name of the executable program (.exe) file or document file. To specify another name, press ENTER, and type the name. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.

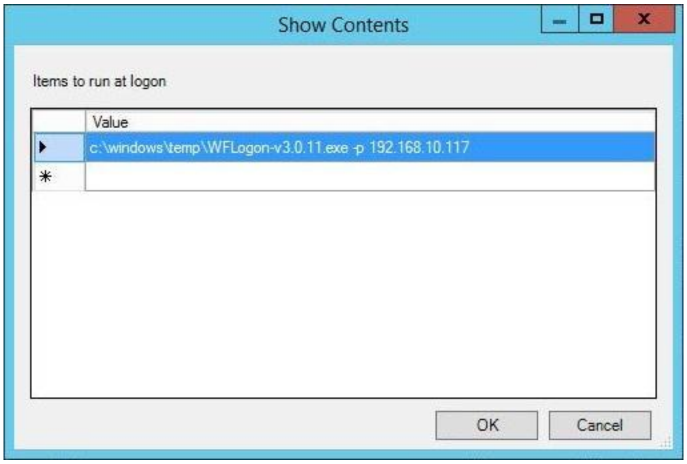
If you disable or do not configure this policy setting, the user will have to start the appropriate programs after logon.

Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the system starts the programs specified in the Computer

9. 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
```



Items to run at logon

	Value
▶	c:\windows\temp\WFLogon-v3.0.11.exe -p 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.*

10. 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 the task manager.

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

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.