



Confidence in a connected world.

Understanding and Configuring Symantec Endpoint Protection Group Update Providers

*Martial Richard,
Technical Field Enablement Manager*

Table of Contents

Content

Introduction 3

What is a Group Update Provider? 4

How GUPs work..... 5

Configuring a GUP 9

Scalability..... 14

Troubleshooting a GUP 16

Introduction

Distributed Symantec Endpoint Protection environments across sites, cities, regions, countries require content updates on all systems across the organization with a minimum amount of time and bandwidth usage. The Group Update Provider (GUP), available with Symantec endpoint protection 11.0 RU5 and later, is Symantec's answer to this challenge.

This document provides an overview of the GUP feature, as well as information on how to configure and implement GUPs in a Symantec Endpoint Protection environment.

What is a Group Update Provider?

A GUP is a Symantec Endpoint Protection client designated to serve as a computer that will get content updates and publish them. The GUP is elected by a set of rules in the LiveUpdate policy based on the OS type, IP address or hostname and registry key. For each new required update package, the GUP will request a copy to the Symantec Endpoint Protection Manager (SEPM) and cache it for future requests. The computers in the client group will use the designated “Group Update Provider” as a local proxy for content updates. This configuration optimizes the bandwidth usage between the GUP and the SEPM.

You can configure a single GUP or multiple GUPS.

■ *Single Group Update Provider*

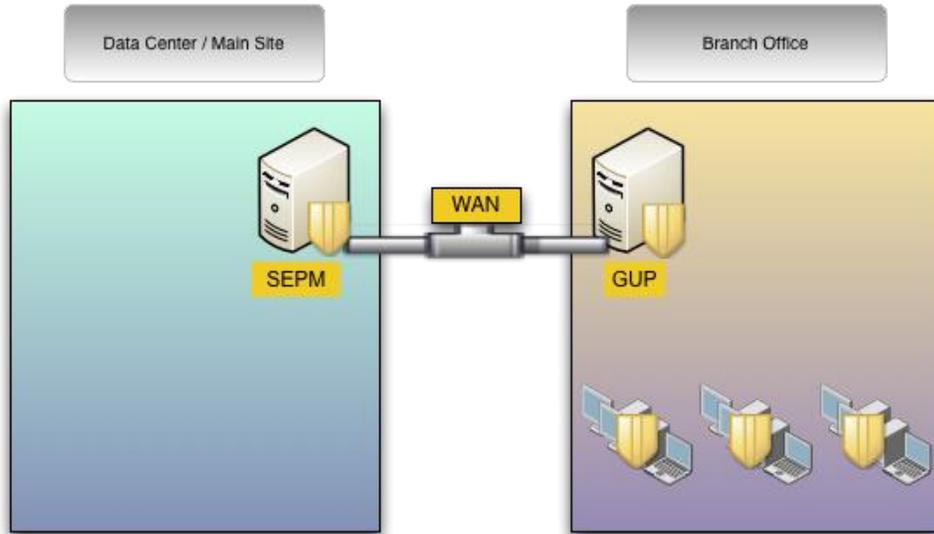
A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. A single Group Update Provider can be a client computer in any group. To configure a single Group Update Provider, you specify the IP address or host name of the client computer that you want to designate as the Group Update Provider.

■ *Multiple Group Update Provider*

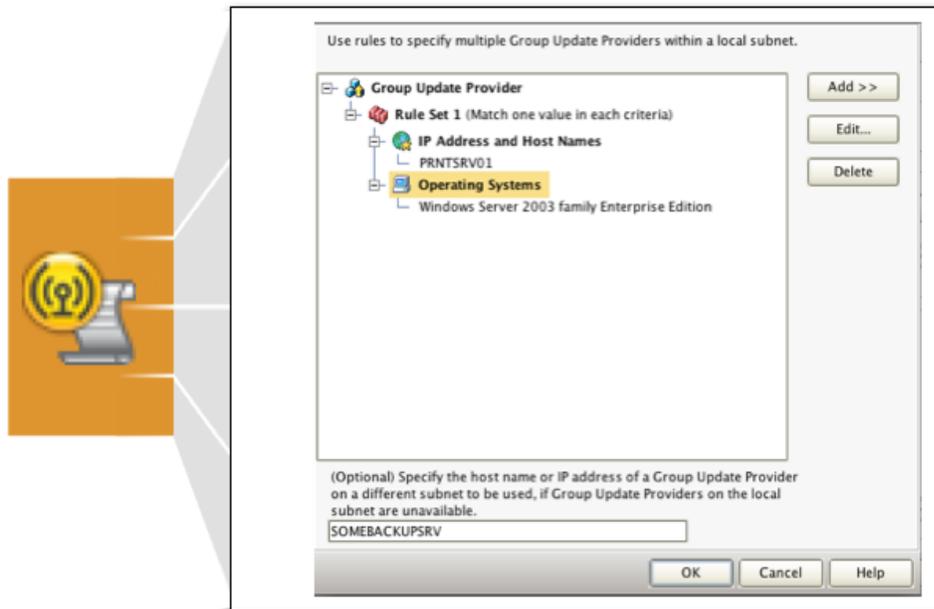
Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients across subnets. To configure multiple Group Update Providers, you specify the criteria that client computers must meet to qualify as a Group Update Provider. If a client computer meets the criteria, the Symantec Endpoint Protection Manager adds the client to its list of Group Update Providers. Symantec Endpoint Protection Manager then makes the list available to all the clients in your network. Clients check the list and choose the Group Update Provider that is located in their subnet. You can also configure a single, dedicated Group Update Provider to distribute content to clients when the local Group Update Provider is not available. You use a LiveUpdate Settings Policy to configure the type of Group Update Provider. The type you configure depends on how your network is set up and whether or not your network includes legacy clients.

How GUPs work

To better understand how GUPs work, consider a scenario in which a SEPM is installed in the Main Office / Datacenter of ACME Corp. The Branch Office, which has a slow WAN, requires a GUP to improve the performance of content distribution.

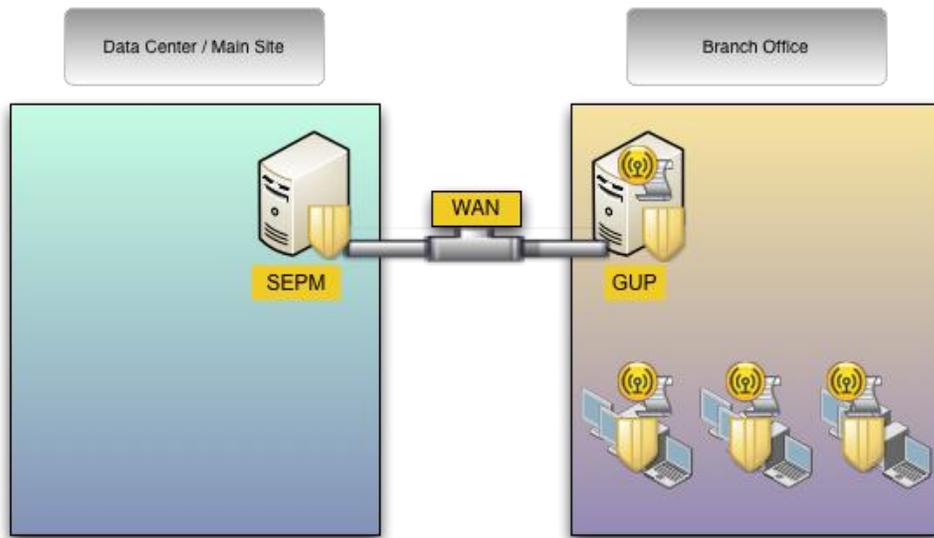


Step 1: LiveUpdate policy is created to designate the GUP, based on the server's name and operating system. For this example, the GUP is designated by the name `PRNTRSRV01` running Windows Server 2003 Enterprise Edition.

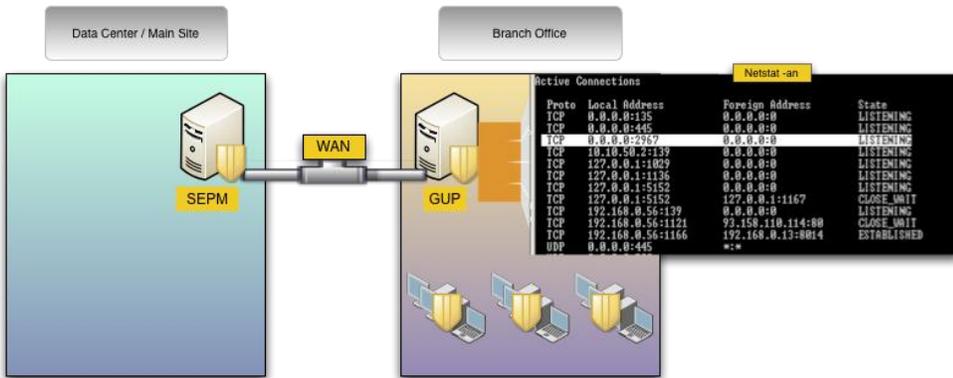


Step 2: The policy is retrieved on a configured heartbeat to all Symantec Endpoint Protection Clients at the site.

White Paper: Understanding and Configuring Group Update Providers

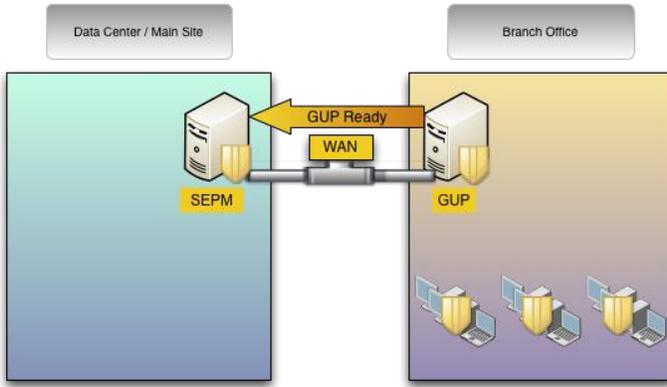


Step 3: The Server PRNTRSV01 is a match to the GUP rule. The GUP feature is enabled the server listening on TCP port 2967. The other clients in the Branch Office do not a match the GUP rule. They will instead contact the GUP to get content updates.

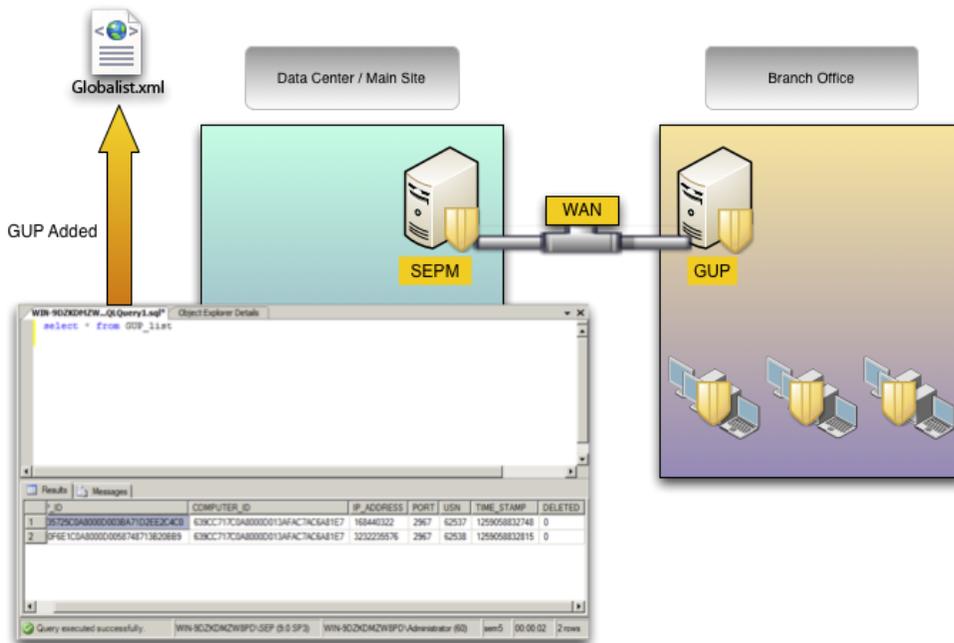


White Paper: Understanding and Configuring Group Update Providers

Step 4: The Server PRNTSRV01 contacts and notifies the SEPM that the GUP feature is enabled and ready.

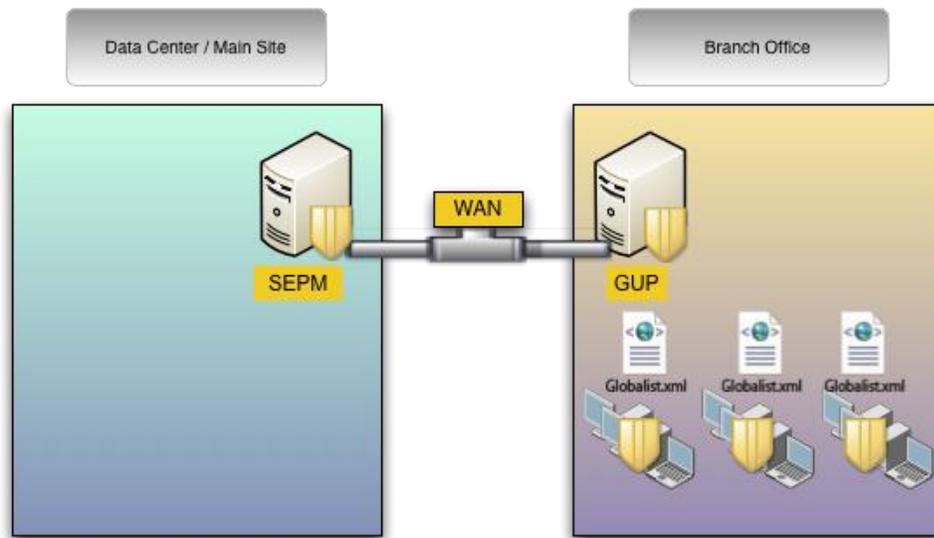


Step 5: The SEPM adds PRNTSRV01 to the GUP_list table in the database. Once the database table updates, the SEPM updates the Globalist.xml file, located at C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup



White Paper: Understanding and Configuring Group Update Providers

Step 6: The Symantec Endpoint Protection client contact the SEPM to get the list of known GUPs and download the `globalist.xml` file.



Step 7: The client sort numerically the list of GUPs available for their subnet and then individually contact each of these until they receive a reply. If there is no reply for any of the listed GUPs in the subnet, then an attempt is made to contact the backup GUP on a remote subnet. If there again is no reply, the client will attempt to connect to the SEPM to download the content update.

Configuring a GUP

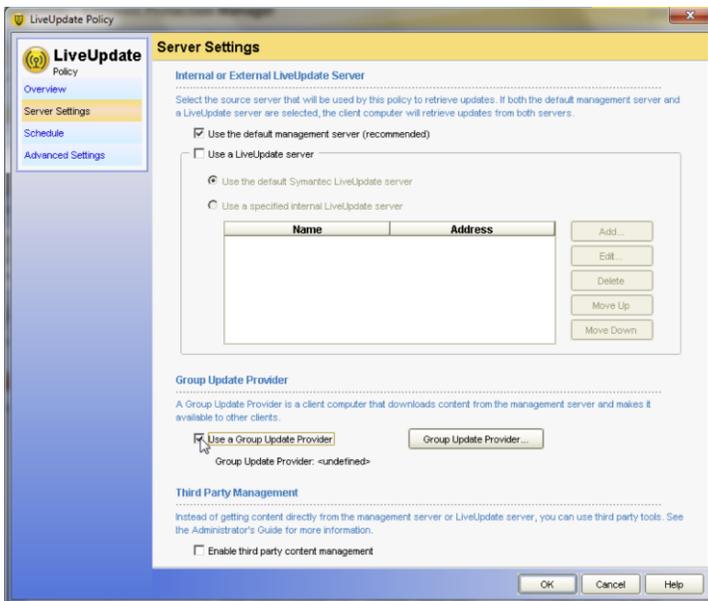
1. Create a new LiveUpdate policy.



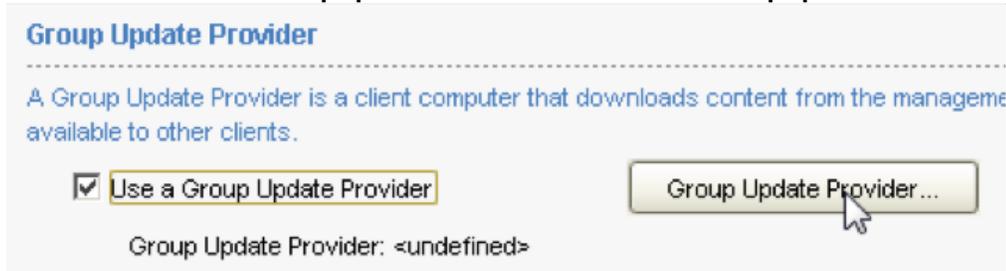
2. Name that policy accordingly and in production environment add a meaningful description of the rules used to designate the GUPs.



3. On the Server Settings tab, ensure the **Use default management server box** is checked, as the GUP feature cannot be activated without this setting.



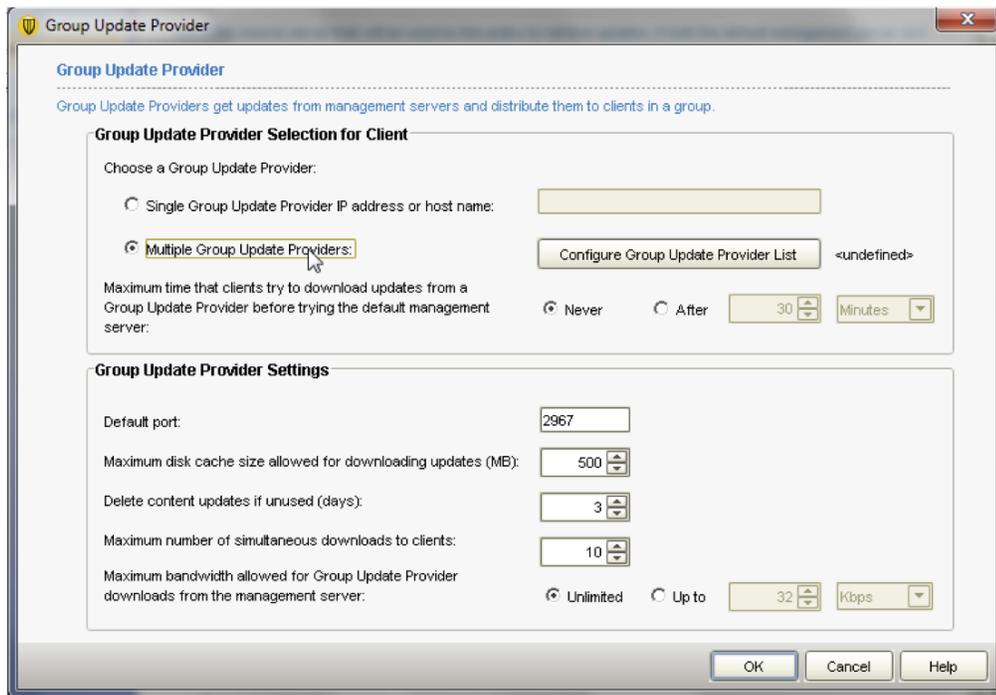
- 4 Check the **Use a Group Update Provider** box and then click **Group Update Provider**.



On this page, you can either use the legacy mode (single GUP) or the multiple Group update provider option.

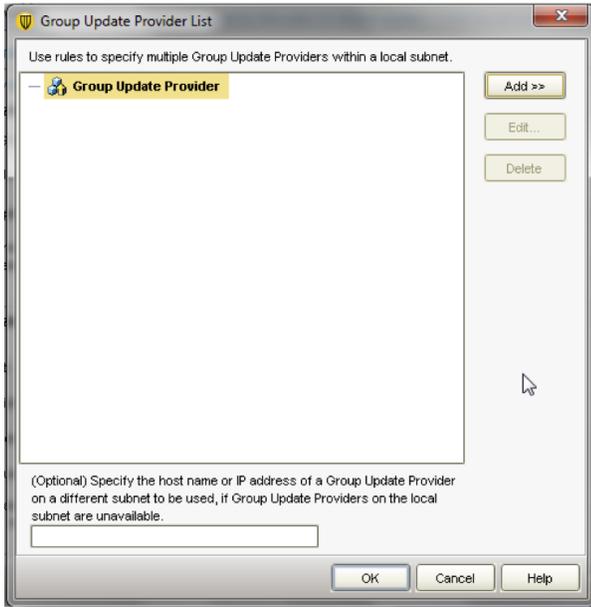
Important: At the time of publication, the RU5 client has a bug listed with the legacy GUP feature, where it is not possible to enter a fully qualified domain name for a GUP name (etrack 1854618). This will be fixed in RU6. In the meantime, the workaround consists on creating the required policy on a SEPM with MR4 MP2 or earlier and import the policy to the RU5 SEPM.

To use the Multiple GUP feature with rules to elect the clients, select **Multiple Group Update Provider** and click **Configure Group Update Provider List**.



To designate (additional?) clients as GUPs click on **Add** to add rules.

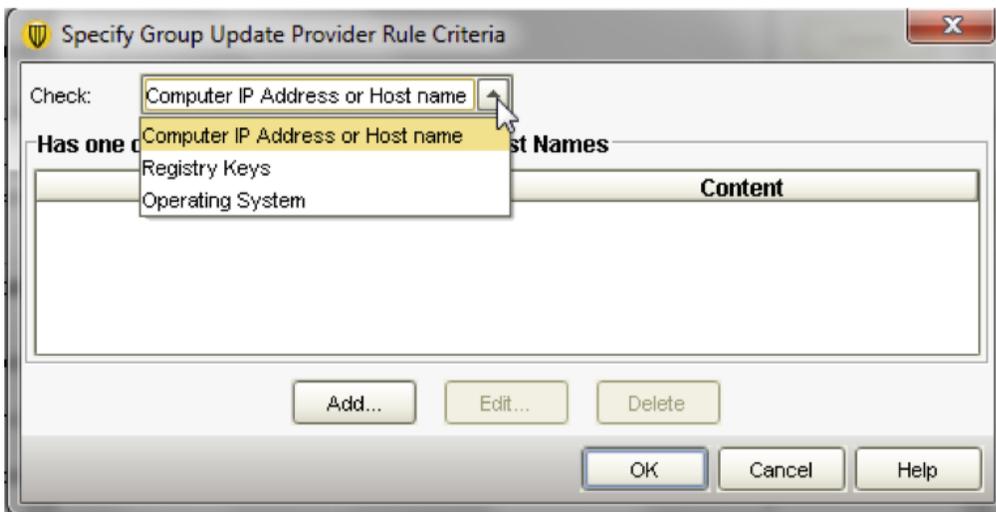
White Paper: Understanding and Configuring Group Update Providers



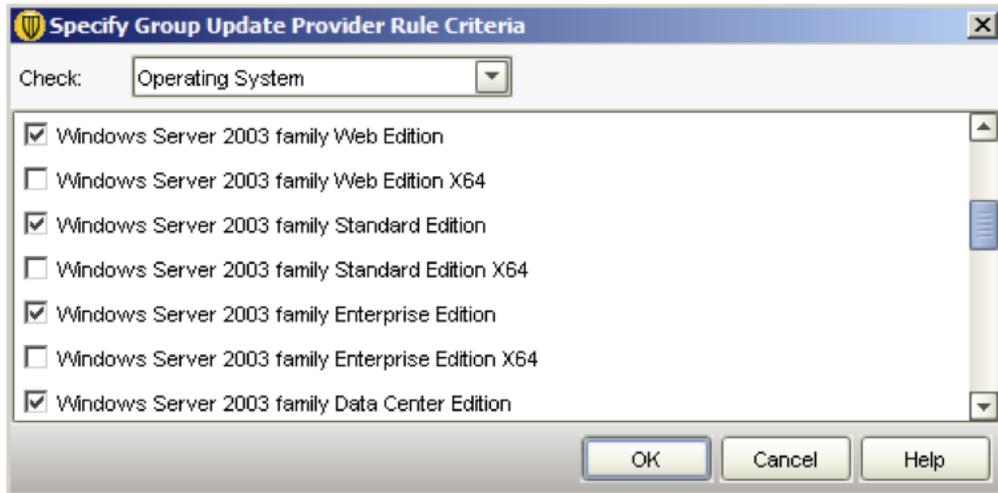
The rule is a combination of criteria:

- Computer IP or Name
- Registry Key
- Operating System

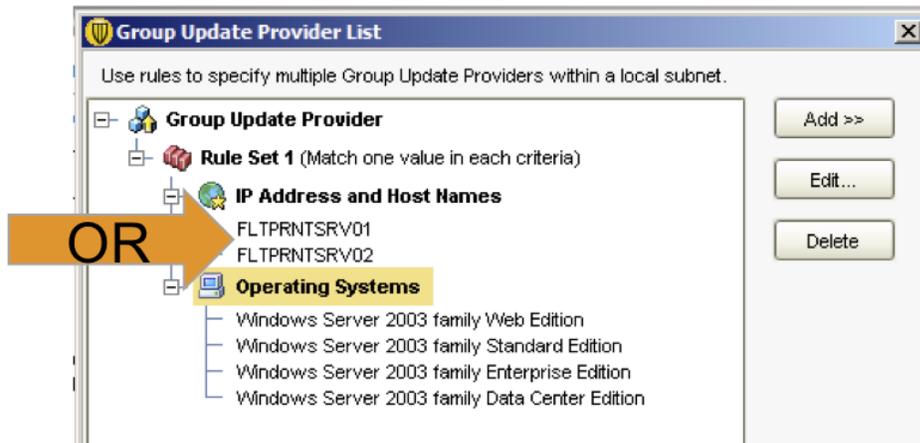
Note that you can use wildcards for the computer name, allowing you to, for example, designate all file and print servers as GUPs by setting a `FLPRNT*` as computer name. This allows you to simplify the rule sets used throughout your organization.



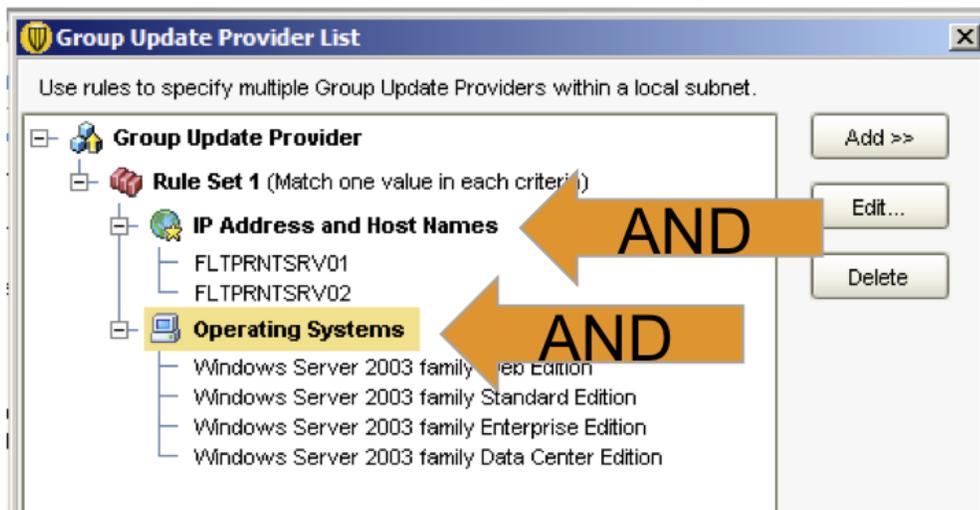
If you choose **Operating system**, you can see all editions of a given version. Ensure to select all that apply (Version and 32 or 64 bit).



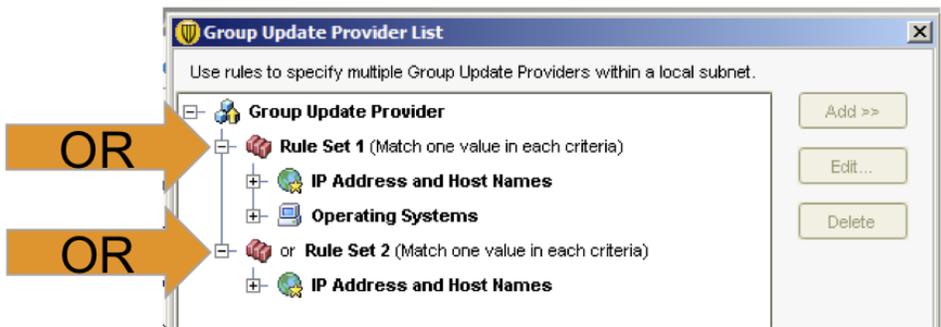
Once the rules have been created, the conditions for a given criteria are displayed using a logic operator OR.



When a rule set has two or more criteria, a logical operator AND is used between criteria. The example below designates "One of these Hosts running on one of these versions of windows 2003".



Finally, if you add several rules set then a logical operator OR is used.



Scalability

While the limitation of GUPs due to complexity fell with RU5, the main challenge was the lack of known scalability. A recent performance test found that a GUP on a dedicated system on a Gigabit LAN can serve up to 10, 000 clients. A more conservative figure of 5,000 should be kept in mind to ensure that the GUP as designed does not need a dedicated system but can run on a multipurpose server.

The following table shows the results of the performance test, the values for %, MB and Mbit/s have been rounded up so are they are evenly presented:

Environment & Configuration				GUP Server Performance			
Content Filesize	# of Clients	# of GUP threads	Client Heartbeat	100% clients updated after 1st heartbeat	Avg Windows CPU usage (%)	Avg Windows Memory usage (MB)	Avg Network usage (Mbit/s)
1mb	100	10	1 hour	Yes	5	100	1
5mb	100	10	1 hour	Yes	5	110	2
50mb	100	10	1 hour	Yes	5	140	15
1mb	1000	10	1 hour	Yes	5	110	3
5mb	1000	10	1 hour	Yes	5	120	15
50mb	1000	10	1 hour	Yes	25	165	120
1mb	1000	100	1 hour	Yes	5	105	5
5mb	1000	100	1 hour	Yes	5	110	15
50mb	1000	100	1 hour	Yes	25	160	120
1mb	5000	100	1 hour	Yes	5	110	15
5mb	5000	100	1 hour	Yes	10	120	60
50mb	5000	100	1 hour	Yes	90	165	570
1mb	10000	100	1 hour	Yes	10	110	25
5mb	10000	100	1 hour	Yes	25	120	120
50mb	10000	100	1 hour	No (took > 12 hours)	90	150	570
1mb	10000	1000	1 hour	Yes	10	110	25
5mb	10000	1000	1 hour	Yes	25	120	120
50mb	10000	1000	1 hour	No (took > 12 hours)	95	180	570
1mb	10000	1000	2 hours	Yes	10	115	15
5mb	10000	1000	2 hours	Yes	25	115	60
50mb	10000	1000	2 hours	No (took > 24 hours)	95	180	570
1mb	10000	1000	30 mins	Yes	15	115	50
5mb	10000	1000	30 mins	Yes	50	140	240
50mb	10000	1000	30 mins	No (took > 12 hours)	95	180	570

Testing conditions:

For these tests, the GUP server had a dedicated machine specification of Win2k3 SP1 running on a P4 2ghz with 1GB RAM and 1gbit/s NIC

For these tests, the GUP is running a SEP client version RU5, with AV/AS and Proactive Threat Protection enabled (no Network Threat Protection)

The tests showed the disk I/O impact on the GUP Server is always minimal, since most of the file I/O utilizes memory

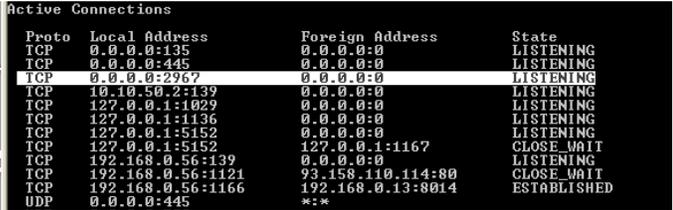
Note the following configurations that can impact performance:

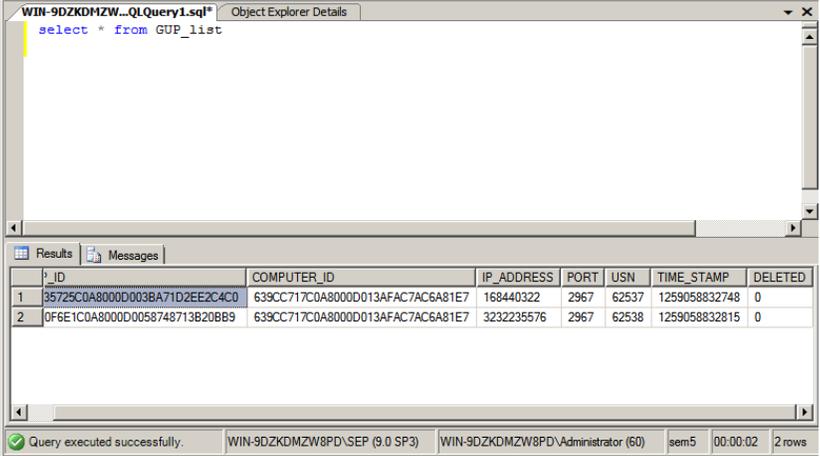
Running Network Threat Protection (Firewall and IPS) on the GUP Server can as much as double the CPU utilization. This performance impact is most noticeable with larger content files

Although the GUP Servers can be run in Virtual Machines, but there will be some performance degradation similar to any other application.

Troubleshooting a GUP

The GUP feature depends of a chain of events involving the SEPM, the database, the network and the clients in order to work properly. Errors occur during these steps. This section provides some guidelines of where to look when the GUP feature is not working as expected.

Step in the process	Symptoms	Tools and Troubleshooting Steps
Policy is created	The policy cannot be applied to a specific group in the console.	<p>The policy creation depends on the health of the SEPM and the database.</p> <ul style="list-style-type: none"> - Check the <code>/Tomcat/Log/scm0.log</code> file for any error - Check the Event viewer on the SQL server for errors
Policy is applied to a group	Policy is not received by the Clients	<p>The policy is published on the IIS part of SEPM under <code>DATA/Outbox/Agent/GROUP UID</code> Check the time stamps on the files on these folders to ensure the policy has been published by the SEPM.</p> <p>On the client side check connectivity with the SEPM with the usual network tools:</p> <ul style="list-style-type: none"> - <code>Ping -a <SEPM FQDN></code> - <code>Tracert <SEPM IP></code> - <code>Nslookup <SEPM>FQDN></code>
GUP feature is enabled	The designated GUP is not active	<p>Check the policy to ensure that the Name / IP matches the real name of the GUP you wish to activate.</p> <p>Check the Policy serial Number on the client under Help and Support >troubleshooting to see if it matches the one published in the console under Client> Group where the GUP should be >Details >policy serial number.</p> <p>On the GUP Server, check that the feature is enabled by running a <code>netstat -an</code> and see if the port TCP 2967 is listening.</p>  <pre> Active Connections Proto Local Address Foreign address State TCP 0.0.0.0:135 0.0.0.0:0 LISTENING TCP 0.0.0.0:445 0.0.0.0:0 LISTENING TCP 0.0.0.0:2967 0.0.0.0:0 LISTENING TCP 10.10.50.2:139 0.0.0.0:0 LISTENING TCP 127.0.0.1:1029 0.0.0.0:0 LISTENING TCP 127.0.0.1:1136 0.0.0.0:0 LISTENING TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING TCP 127.0.0.1:5152 127.0.0.1:1167 CLOSE_WAIT TCP 192.168.0.56:139 0.0.0.0:0 LISTENING TCP 192.168.0.56:1121 93.158.110.114:80 CLOSE_WAIT TCP 192.168.0.56:1166 192.168.0.13:8014 ESTABLISHED UDP 0.0.0.0:445 *:*</pre> <p>Check on the database on the GUP-List table if the GUP has been added.</p> <ul style="list-style-type: none"> - <u>On the console</u> retrieve the unique ID for the GUP under Client>Group>client Property.

		<p>- On the SQL server, connect to the <code>sem5</code> database and run the following query:</p> <pre>SELECT * FROM GUP_LIST</pre>  <p>The computer ID for your GUP should appear in this table.</p>
<p>The clients are contacting GUPs to retrieve content update</p>	<p>The clients are not up to date with content.</p>	<p>Check that the clients have the latest policy by verifying the Policy serial number.</p> <p>Check for any pending connection to the GUP's IP address. By using the <code>Use the netstat -an</code> command</p> <p>If it is the case, you can investigate further with a sniffing utility to capture the traffic when you start the SEP client service.</p>

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

