



Ivanti Endpoint Security

Caching Proxy 3.5 Setup Guide

ivanti

Endpoint Security

powered by HEAT

Notices

Version Information

Caching Proxy 3.5 Setup Guide - Published: Jun 2020

Copyright Information

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

For the most current product information, please visit www.ivanti.com.

Copyright© 2020, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <https://www.ivanti.com/patents>.

Contents

Contents	4
Caching Proxy Requirements Checklist	5
Install Squid 3.5.x	7
Configure Squid	9
Test Caching Proxy Server Connectivity	16
Configure Endpoints to Use the Caching Proxy	18
Verify that Squid is Caching Content	26

Caching Proxy Requirements Checklist

Before you begin, make sure you have the following on hand:

Hardware

- ☐ A dedicated server that will function as your Caching Proxy.
- ☐ A hard disk with a low random seek time (3ms or less) and large disk cache.
- ☐ Large amount of RAM. We recommend 32 MB of RAM for every GB of disk space.

Third-party software

- ☐ Download Squid 3.5.x for Microsoft Windows from <http://squid.diladele.com/>. Currently only a 64-bit version is available.

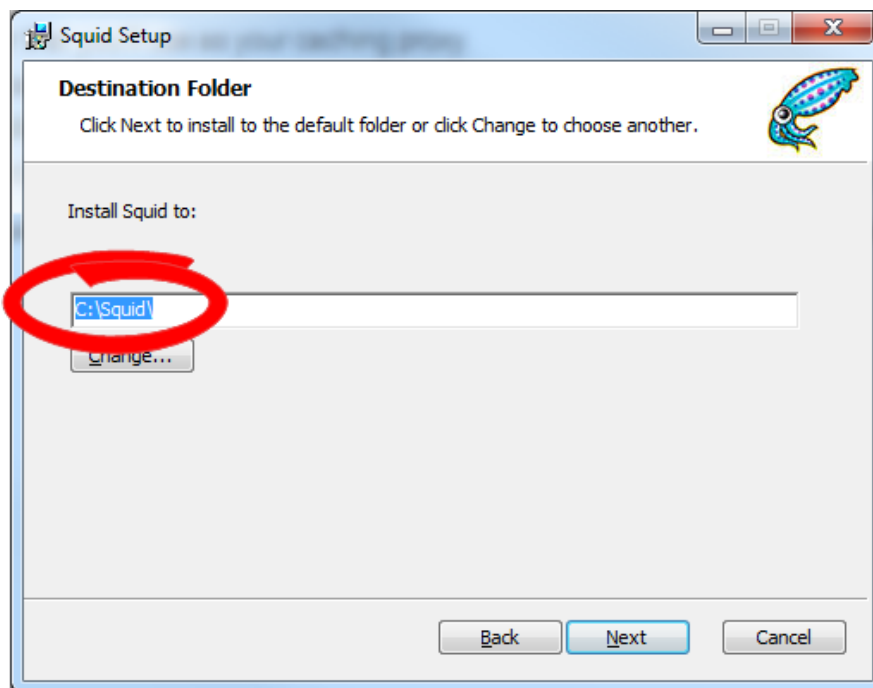
Diladele B.V. releases new versions of the Squid Caching Proxy MSI regularly. You can use any 3.5.x version but only versions 3.5.18 through 3.5.20 were officially tested to be compatible with Ivanti Endpoint Security.

- ☐ Notepad++ or similar text editor .
- ☐ An htpasswd generator to encrypt usernames and passwords.

Install Squid 3.5.x

Install Squid on the server you plan to use as your caching proxy.

1. Get the Squid MSI from <http://squid.diladele.com/>. Currently only a 64-bit version is available.
2. Log on to the server that you'll use as your caching proxy.
3. Copy the Squid 3.5.x MSI to the server.
4. Browse to the installer (`squid.msi`) and open it.
5. Complete the wizard. Take note of the installation path, as you'll be editing files within it during configuration. The default path is: `c:\squid\`



The install process can take up to 5 minutes. A **Squid for Windows** icon appears in the system tray when finished.



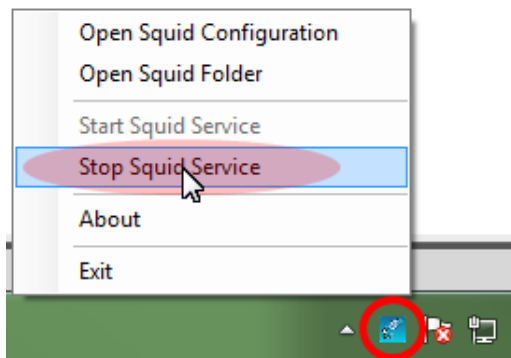
Configure Squid

Add and modify parameters using a text editor like Notepad++ to configure Squid for your environment. You'll need to stop and start Squid to activate the changes.

You cannot use a configuration file from an earlier Squid version as it is not compatible with 3.5.x.

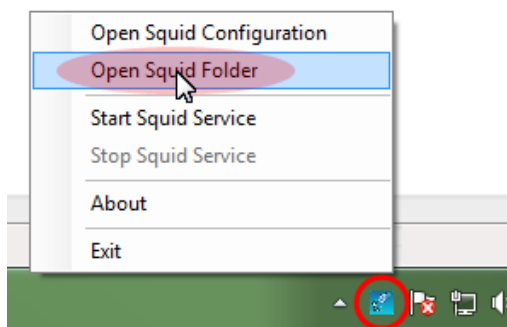
Step 1: Stop the Squid service

Stop the proxy server using the Squid system tray icon right-click menu.



Step 2: Open the **squid.conf** file in a text editor

1. Open the Squid Folder using the Squid system tray icon right-click menu.



2. Open `\etc\squid\squid.conf` in Notepad ++ or similar text editor.

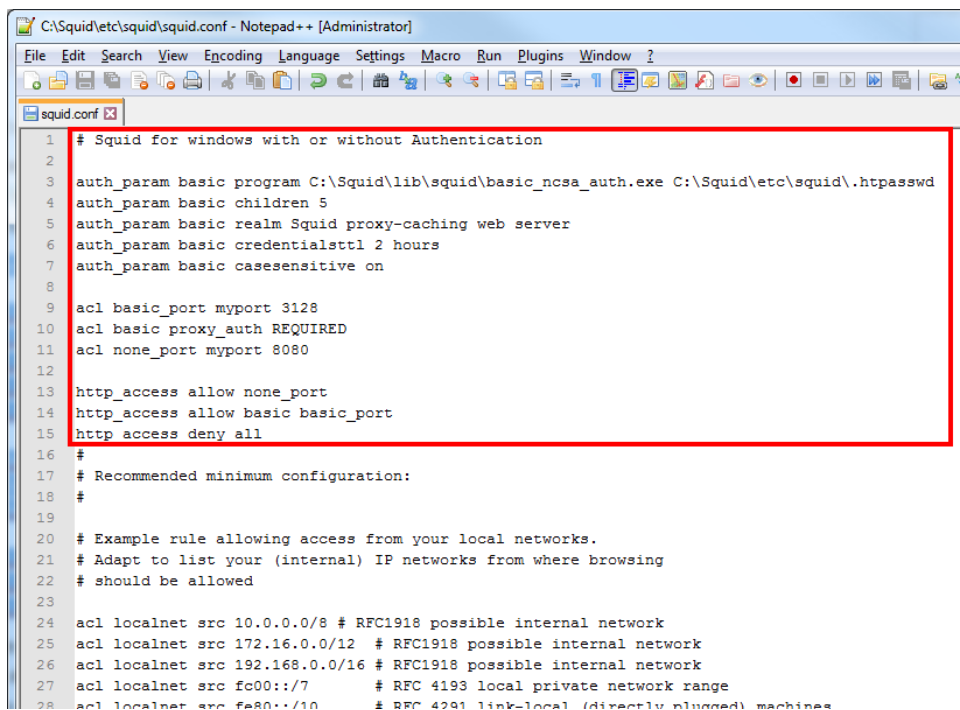
Step 3: Add and modify parameters

1. Add the lines below to the top of the file. They're parameters for setting up basic authentication in Squid.

```
# Squid for windows with or without Authentication
auth_param basic program C:\Squid\lib\squid\basic_ncsa_auth.exe C:\Squid\etc\squid\httpasswd
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive on

acl basic_port myport 3128
acl basic_proxy_auth REQUIRED
acl none_port myport 8080

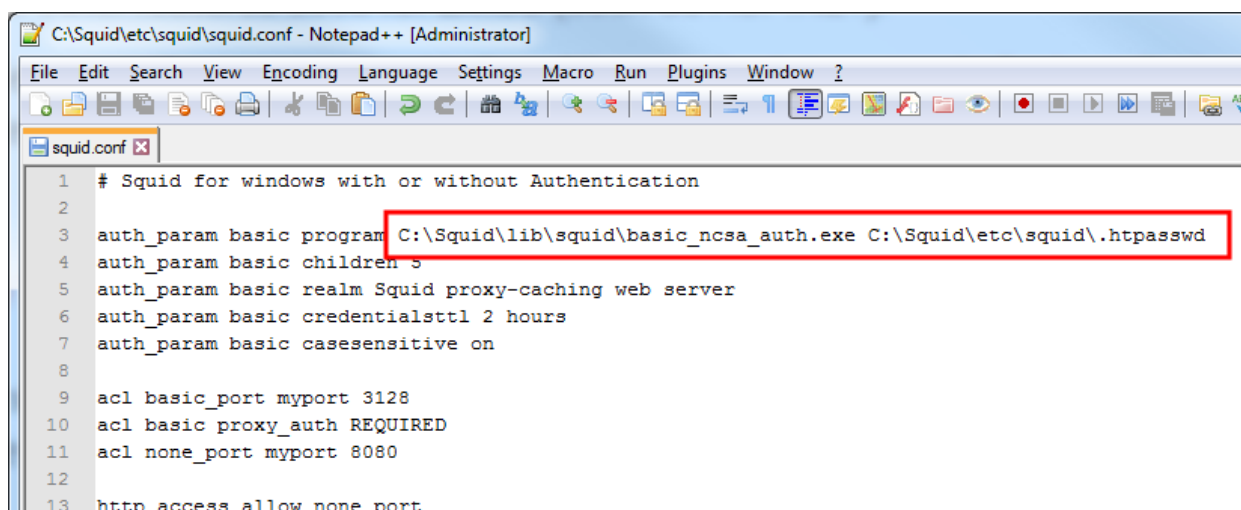
http_access allow none_port
http_access allow basic basic_port
http_access deny all
```



The screenshot shows a Notepad++ window titled "C:\Squid\etc\squid\squid.conf - Notepad++ [Administrator]". The window displays the contents of the squid.conf file. Lines 1 through 15 are enclosed in a red rectangular box, highlighting the configuration for basic authentication. The configuration includes setting the authentication program, children, realm, credentialsttl, and casesensitive options, as well as defining ACLs for basic_port and none_port, and setting http_access rules to allow access for the basic_port and deny access for all other requests.

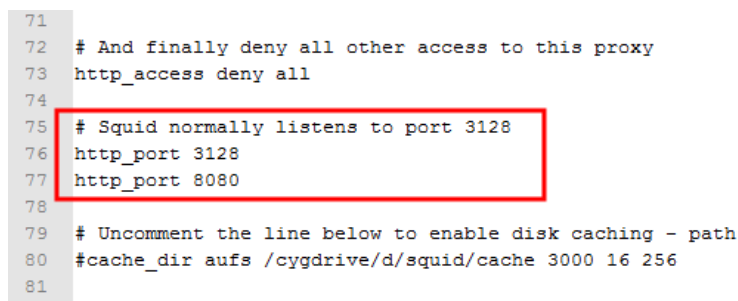
```
1 # Squid for windows with or without Authentication
2
3 auth_param basic program C:\Squid\lib\squid\basic_ncsa_auth.exe C:\Squid\etc\squid\httpasswd
4 auth_param basic children 5
5 auth_param basic realm Squid proxy-caching web server
6 auth_param basic credentialsttl 2 hours
7 auth_param basic casesensitive on
8
9 acl basic_port myport 3128
10 acl basic_proxy_auth REQUIRED
11 acl none_port myport 8080
12
13 http_access allow none_port
14 http_access allow basic basic_port
15 http_access deny all
16 #
17 # Recommended minimum configuration:
18 #
19
20 # Example rule allowing access from your local networks.
21 # Adapt to list your (internal) IP networks from where browsing
22 # should be allowed
23
24 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
25 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
26 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
27 acl localnet src fc00::/7 # RFC 4193 local private network range
28 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
```

2. Make sure the file paths in the **auth_param basic program** line match your install directory. They point to the authentication helper program and the .htpasswd file you'll create later.



```
C:\Squid\etc\squid\squid.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
squid.conf
1 # Squid for windows with or without Authentication
2
3 auth_param basic program C:\Squid\lib\squid\basic_ncsa_auth.exe C:\Squid\etc\squid\.htpasswd
4 auth_param basic children 5
5 auth_param basic realm Squid proxy-caching web server
6 auth_param basic credentialsttl 2 hours
7 auth_param basic casesensitive on
8
9 acl basic_port myport 3128
10 acl basic_proxy_auth REQUIRED
11 acl none_port myport 8080
12
13 http access allow none port
```

3. Under **# Squid normally listens to port 3128**, add **http_port 8080** directly below **http_port 3128**. 8080 is a listener port commonly used by proxy servers.



```
71
72 # And finally deny all other access to this proxy
73 http_access deny all
74
75 # Squid normally listens to port 3128
76 http_port 3128
77 http_port 8080
78
79 # Uncomment the line below to enable disk caching - path
80 #cache_dir aufs /cygdrive/d/squid/cache 3000 16 256
81
```

- Uncomment (remove the #) from the line **#cache_dir aufs** **/cygdrive/d/squid/cache 3000 16 256** and change the path to point to the cache folder **[c:/squid/var/cache**. This enables disk caching, reducing the network load for low-bandwidth remote locations.



You must create a Squid caching structure in the cache folder for this to work. We'll do that in Step 4.

```

75 # Squid normally listens to port 3128
76 http_port 3128
77
78 # Uncomment the line below to enable disk caching - path format is /cygdrive/<full path to cache folder>
79 cache_dir aufs c:/squid/var/cache 3000 16 256
80
81
82 # Leave coredumps in the first cache dir
83 coredump_dir /var/cache/squid

```

- At the very bottom of the file, add and set the **maximum_object_size** parameter. Without it, Squid, by default, will only cache files up to 4 MB in size.

```

75
76 dns_nameservers 8.8.8.8 208.67.222.222
77
78 max_filedescriptors 3200
79
80 maximum_object_size 200 MB
81

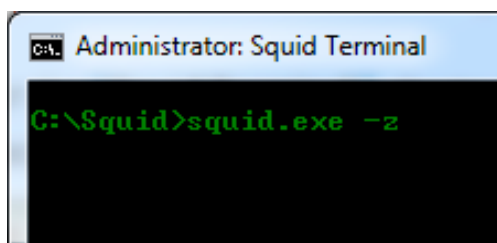
```

- Save the file.

- Your changes don't take effect until you restart the proxy server.
- Squid offers more configurable options than are visible in the `squid.conf` file provided by Diladele B.V. See the [Squid configuration file documentation](#) for more information.
- Option descriptions can also be found in `c:\Squid\etc\squid\squid.conf.documented` (open in Notepad ++ or similar text editor).

Step 4: Create the Squid caching folder structure

1. Make sure the cache folder **c:\squid\var\cache** exists.
2. Run the **Squid Terminal** shortcut on your desktop as an administrator.
3. Execute the command: `squid.exe -z`



Result: A folder structure is created for storing cached data in: **c:\squid\var\cache**

00	10/31/2016 6:45 PM	File folder
0A	10/31/2016 6:45 PM	File folder
0B	10/31/2016 6:45 PM	File folder
0C	10/31/2016 6:45 PM	File folder
0D	10/31/2016 6:45 PM	File folder
0E	10/31/2016 6:45 PM	File folder
0F	10/31/2016 6:45 PM	File folder
01	10/31/2016 6:45 PM	File folder

Step 5: Create a file to store encrypted usernames and passwords for authentication

1. Encrypt your username and password in the htpasswd format. Use a generator of your choice.

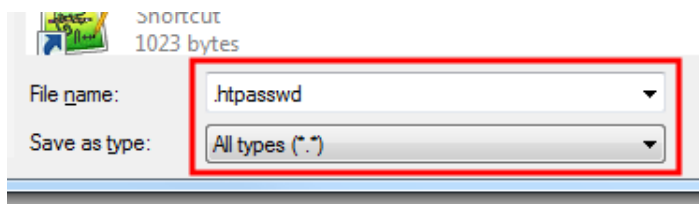
.htpasswd entry created

Copy the text below into your **.htpasswd** file.

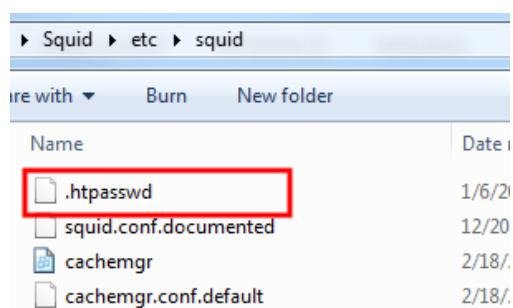
Remember: One entry per line.

admin:\$apr1\$5HqhbFow\$kI8BOCfLdzqw5H5Tpg5kq1

2. Paste the encrypted string into a text editor and create an **.htpasswd** file. Use the Save as type **All types (*.*)** when doing this in Notepad++.



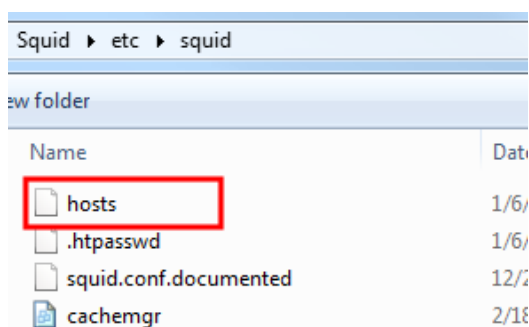
3. Copy the ready .htpasswd file into [c:\Squid\etc\squid].



Step 6: Copy your HOSTS file into Squid

1. Update your HOSTS file in **c:\Windows\System32\drivers\etc** as required. For example, with the proper Hostname and IP Address pair for the Global Subscription Service (GSS).

2. Copy it to `c:\Squid\etc\squid`.



If you don't want to use the HOSTS file method, you can change the default DNS name servers in the `squid.conf` file:

- a. Comment out (add a `#` before) `dns_nameservers 8.8.8.8 208.67.222.222`.
- b. Add the line `dns_nameservers [DNS name server IP address]`. If you have more than one, just separate them with a space.

```

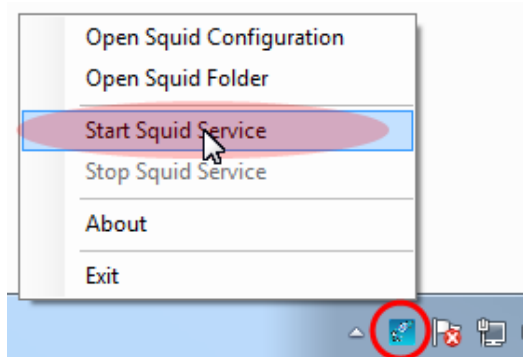
73 refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
74 refresh_pattern . 0 20% 4320
75
76 #dns_nameservers 8.8.8.8 208.67.222.222
77 dns_nameservers 10.120.129.158 165.21.83.88
78
79 max_filedescriptors 3200

```

- c. Save the `squid.conf` file.
- d. Restart the Squid service.

Step 7: Start the Squid service

Start the proxy server using the Squid system tray icon right-click menu.

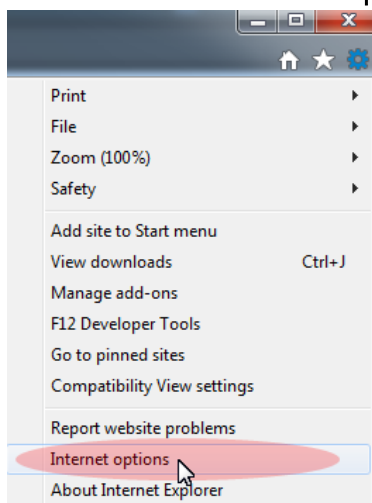


Test Caching Proxy Server Connectivity

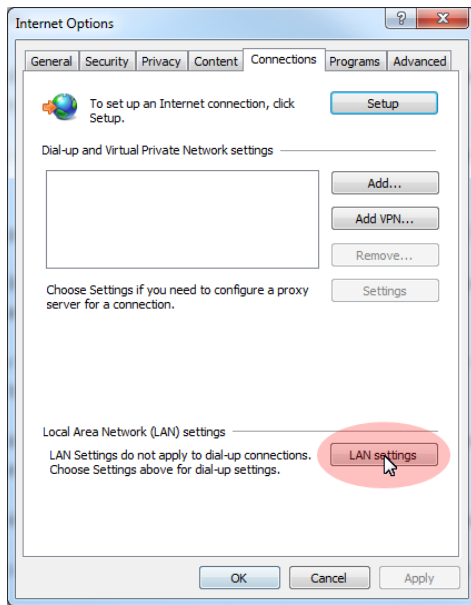
Check that the Server can connect to the Internet and Ivanti Endpoint Security

STEP 1: Check that the server can connect to the Internet through the caching proxy port

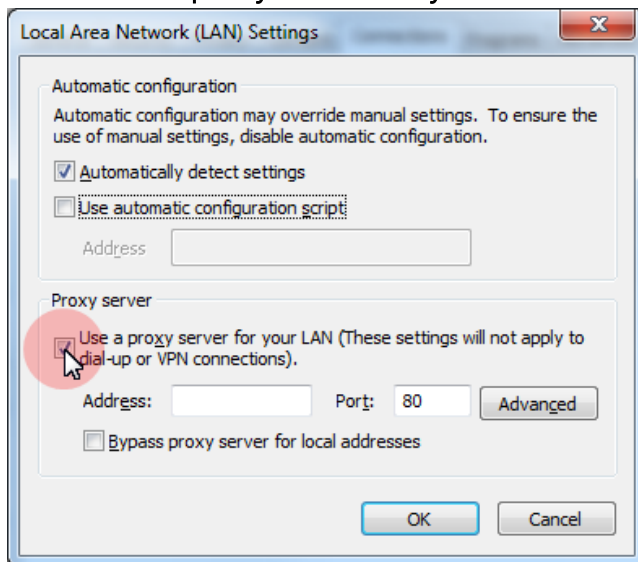
1. Launch **Internet Explorer**. In this example uses Internet Explorer 11.
2. Select **Tools > Internet Options**.



3. On the **Connections** tab, click **LAN Settings**.



4. Select **Use a proxy server for your LAN**.



5. In the **Address** field enter **127.0.0.1**.
6. In the **Port** field enter the Caching Proxy port number (3128 or 8080).
7. Click **OK**.
8. Browse to <http://www.ivanti.com> and verify that the pages loads successfully.

STEP 2: Check that the server can resolve the HEMSS DNS name

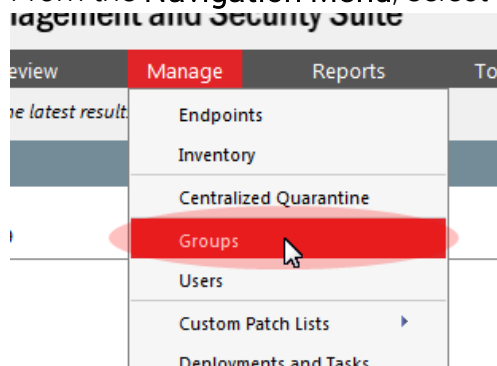
1. On the Caching Proxy server still configured to use the Caching Proxy port, launch Internet Explorer.
2. Browse to the Ivanti Endpoint Security Server using the DNS name, e.g. <http://IESS01>.
3. Verify that the Ivanti Endpoint Security login prompt appears. If you cannot get to this page, you may need to try to connect via the IP address

Configure Endpoints to Use the Caching Proxy

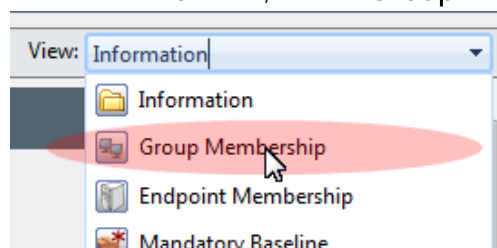
You must configure the agents on your endpoints to use the Caching Proxy server. We'll also deploy some content to a small number of endpoints to test it.

STEP 1: Create a custom endpoint group.

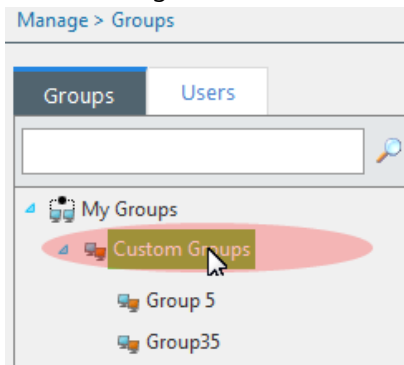
1. From the **Navigation Menu**, select **Manage > Groups**.



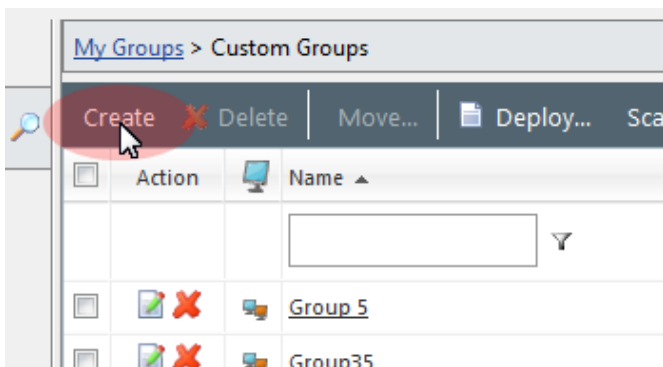
2. From the **View** list, select **Group Membership**.



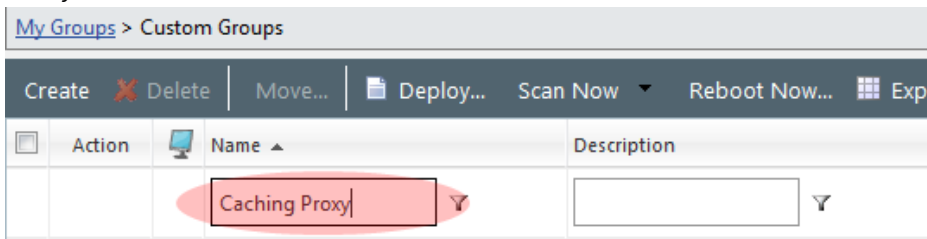
3. In the navigation tree, select **Custom Groups**.



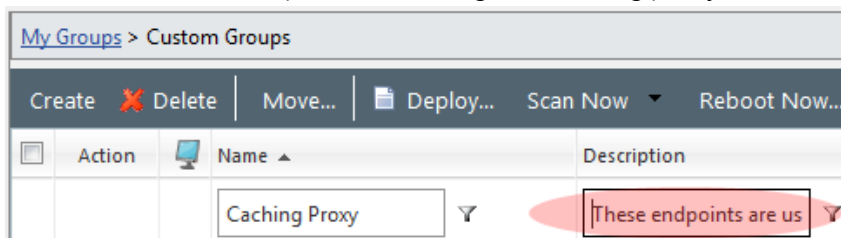
4. Click **Create**.



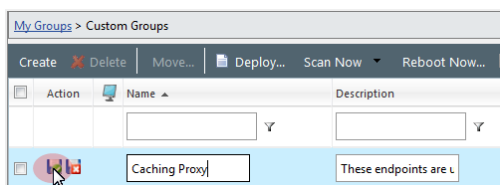
5. In the **Name** field, type a name for the group. In this example we'll use *Caching Proxy*.



6. Type a brief description about the group in the **Description** field. In this example we'll write *These endpoints are using the caching proxy server*.

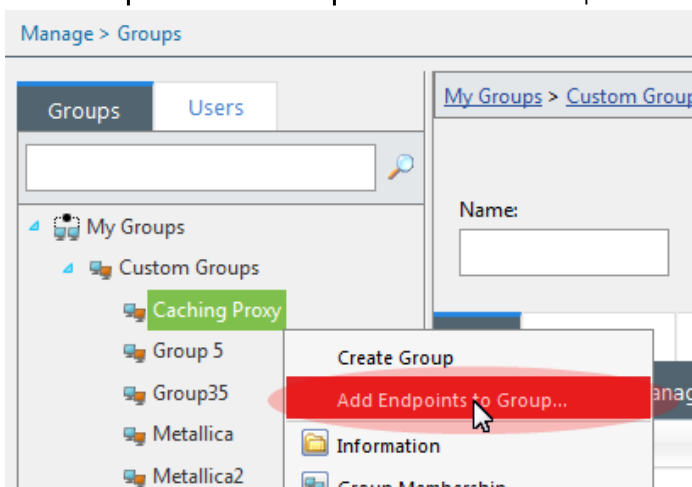


- Click the **Save** icon associated with the new group.

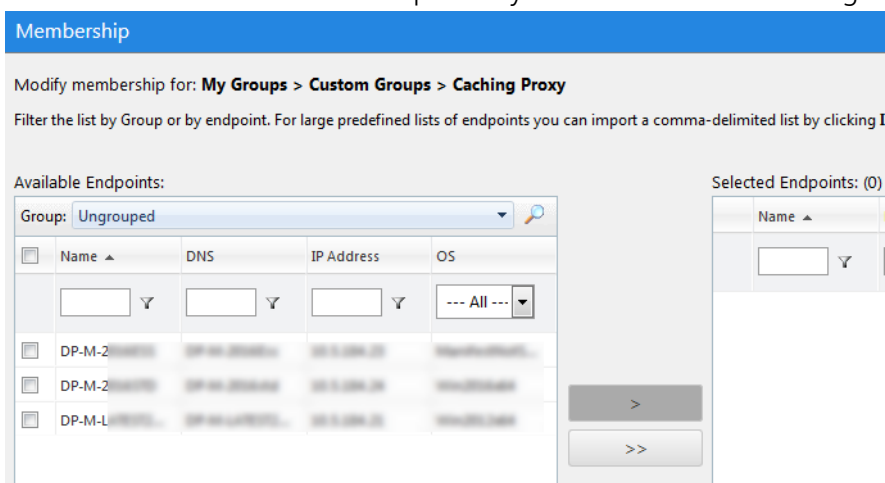


STEP 2: Assign the endpoints to the new Caching Proxy group.

- In the navigation tree, right-click on the Caching Proxy custom group and select **Add Endpoints to Group**. The Memberships dialog appears.



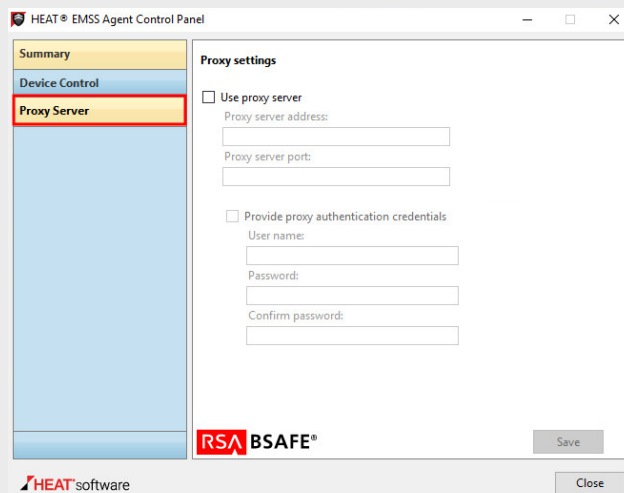
- Search for and select the endpoints you want to add to this group, then click **OK**.



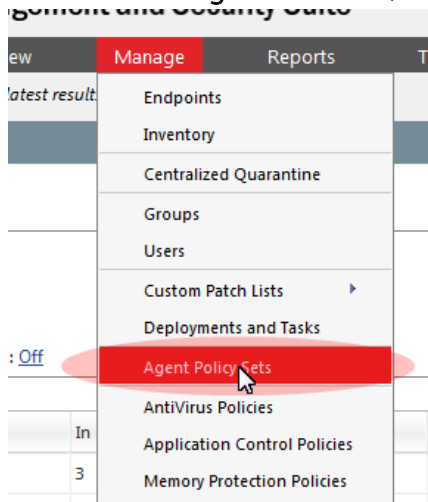
STEP 3: Create an Agent Policy Set for the group to use a FastPath server.

FastPath only works with endpoints with the Patch & Remediation module installed.

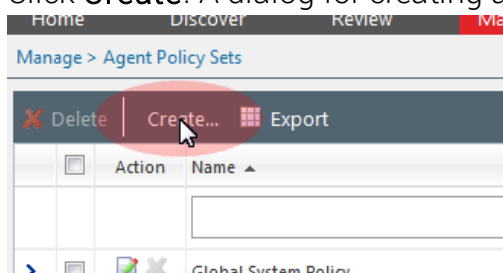
Those endpoints without it can be configured using their Agent Control Panel (Proxy Server section).



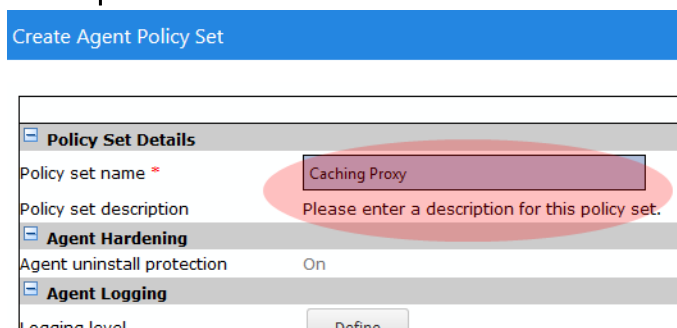
1. From the **Navigation Menu**, select **Manage > Agent Policy Sets**.



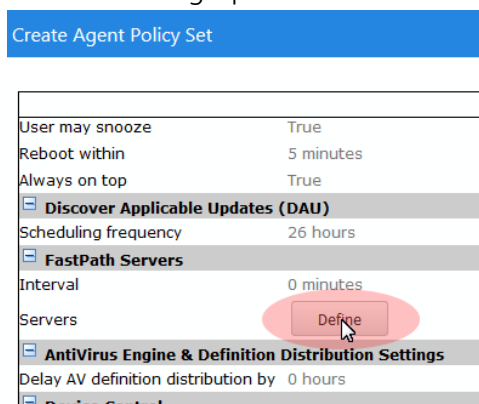
- Click **Create**. A dialog for creating an agent policy set opens.



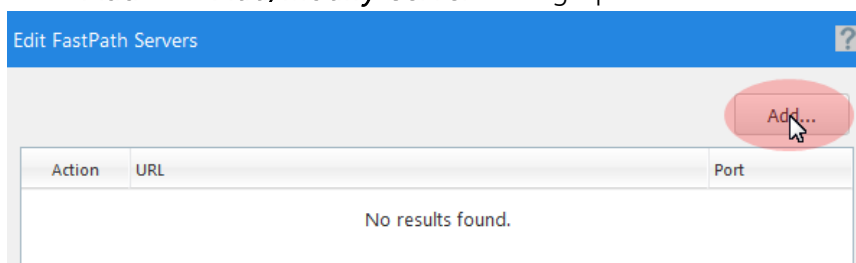
- In the **Policy Set Details** section, enter a **Policy set name** and **Policy set description**.



- Scroll down to the **FastPath Servers** section and click **Define**. The *Edit FastPath Servers* dialog opens.



- Click **Add**. The *Add/Modify Server* dialog opens.



6. Define the FastPath server information by entering the URL and Port number for the caching proxy server.

Add/Modify Server

URL:

Port: *

☐ Authenticated

7. Select **Authentication** and enter the proxy server user name and password.

☒ **Authenticated**

User Name: *

Password: *

Confirm Password: *

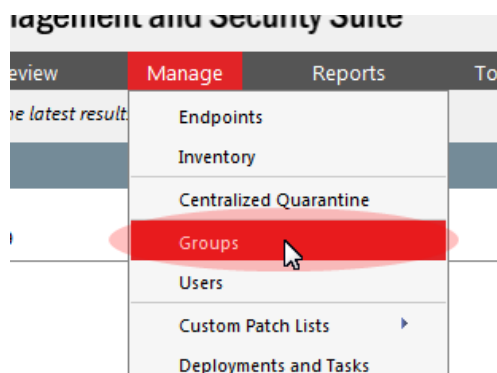
RSA BSAFE®

8. Click **OK**.

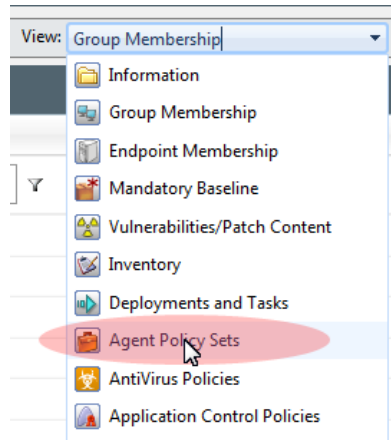
Endpoints will not begin connecting to the caching proxy server until the Agent on the endpoint has received the policy containing the FastPath server details. After establishing the policy containing Fast Path server details, wait until the communication interval between the Agent and the server has passed to ensure that the policy is downloaded and applied to the endpoint before executing the deployment in the next step.

STEP 4: Assign the newly created Agent Policy set to your custom group.

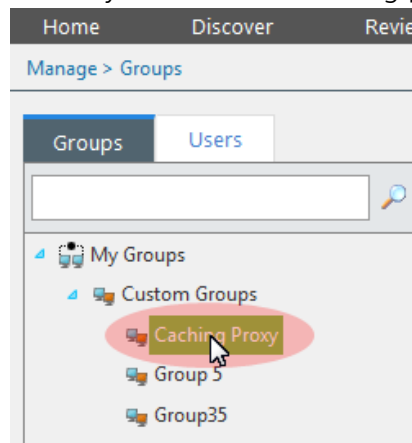
1. From the **Navigation Menu**, select **Manage > Groups**.



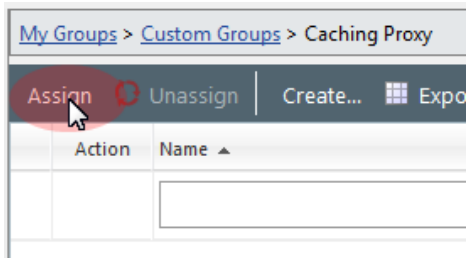
2. From the **View** list, select **Agent Policy Sets**.



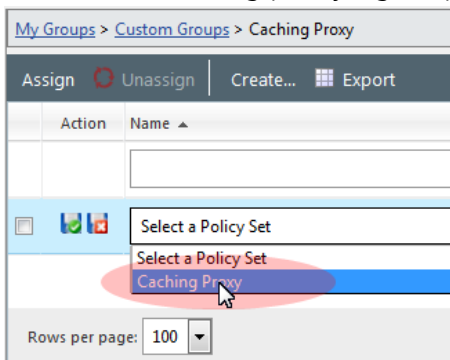
3. Select your custom caching proxy group from the directory tree.



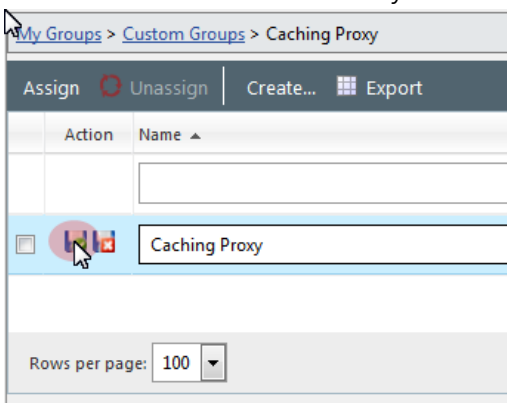
4. Click **Assign**. The **Select a Policy Set** list becomes active.



5. Select the caching proxy agent policy set you created.

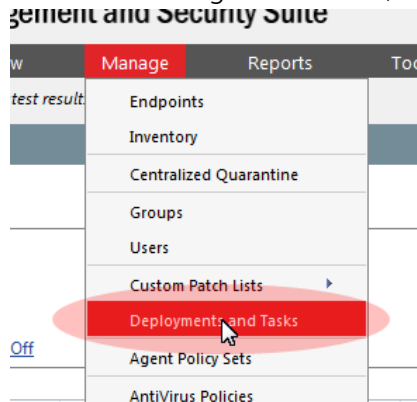


6. Click the **Save** icon to save your changes.

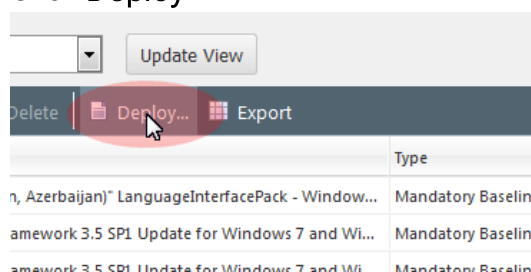


STEP 5: Deploy content to a small subset of the group. When the deployment is complete, the content is cached on the caching proxy server.

1. From the Navigation Menu, select **Manage > Deployments and Tasks**.



2. Click **Deploy**.



3. Complete the wizard. Make sure you select just a few endpoints from your custom group for this test deployment.

Verify that Squid is Caching Content

You can verify that content is flowing between Ivanti Endpoint Security, the Caching Proxy and your endpoints by monitoring specific logs and folders.

Check that the Caching Proxy is receiving content from Ivanti Endpoint Security by monitoring the contents of the cache folder.

1. Log in to the computer running the Caching Proxy.
2. Navigate to: **c:\squid\var**
3. Right-click on the **cache** folder.
4. Click **Properties**.

Result: The Properties dialog displays, showing the size of the cache folder. As endpoints receive new content through the Caching Proxy, the size of this folder increases.

Check that endpoints are connecting to the Caching Proxy by monitoring Squid logs.

The [Squid Log Files](#) topic on the Squid Wiki provides a complete explanation of how to read the Caching Proxy access logs.

1. Log in to the computer running the Caching Proxy.
2. Navigate to: `c:\squid\var\log\squid`
3. Open `access.log`.

Result: The log file displays, showing endpoint connectivity data.

