Web Endpoint Features (icons, override, disable, diagnostics)

Topic 65061 | Web Endpoint | Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

Websense® Web endpoint secures client machines such as laptops from inbound web threats when the devices are outside the corporate network. For Web Security Gateway Anywhere and Cloud Web Security end users, it is designed to provide a seamless experience for authenticating and directing traffic to the cloud service. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the device.

This article covers the following topics related to the Web Endpoint in both hybrid and cloud-only configurations:

- *Icon status indicators*
- *Normal operations*
- *Automatic temporary endpoint override*
- *Disabling the endpoint*
- *Diagnostics*

Additional resources

The following articles and guides are available to assist you with downloading and preparing the Web endpoint for deployment in your network.

- Web Endpoint Deployment Overview (Web Security Help)
- Installing and Deploying Web Endpoint
- How do I install the hybrid Web Endpoint client?
- Combining Web and Data Endpoint Clients

For information about the Web Endpoint in Cloud Web Security, see Setting up Web Endpoint in the Cloud Security Help.

Icon status indicators

Topic 65062 | Web Endpoint| Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

Websense Web Endpoint on the Windows operating system displays one of three possible status icons in your task bar. The icon serves as both a status indicator and an access point to additional diagnostic information.

Icon	Hover Text	Description
	Websense: Enabled	The Web Endpoint software is successfully configured, connectivity to the cloud service exists, and the cloud PAC file is correct and accessible.
	Websense: Override	The Websense cloud service cannot be reached. The Web Endpoint is automatically temporarily overridden. Your consultant can then manually override the proxy settings on the laptop to ensure access to the Internet. See *Normal operations*.
	Websense: Disabled	This icon displays if you've allowed your end users to disable the endpoint and they then disable it. See *Disabling the endpoint*.

Important

Note that if an end user has disabled the Web Endpoint service, a reboot will always enable it.

See *Diagnostics*, page 10, for information on endpoint diagnostics.

Normal operations

Topic 65075 | Web Endpoint| Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

When Websense Web Endpoint is successfully configured, connectivity to the cloud service exists, and the cloud PAC file is correct and accessible, the endpoint enforces use of PAC file settings and does the following:

- Sends out direct HTTP requests to download a PAC file.
- Makes sure users cannot change IE proxy settings when the endpoint detects:
  - A Websense PAC file is available.
  - The endpoint is downloading a real PAC file.
- Overrides proxy settings that users may have set while the cloud service was not reachable, after detecting that the service status has changed from unreachable to reachable.

Automatic temporary endpoint override

Topic 65063 | Web Endpoint| Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

When a network change occurs, the endpoint checks to determine if it can still reach the Websense cloud service. If it cannot, an automatic override takes effect. You don't need to enable the automatic override feature. It is on by default. Here are examples of conditions under which an automatic override occurs:

Network change, such as:

- Switch from Wi-Fi to Ethernet
- Establishment of a VPN connection.
- Assignment of a new IP address to a laptop.

And the endpoint is then unable to access the Websense cloud service for reasons such as:

- An upstream proxy
- A captive portal
- No Internet access
- Content type of the PAC file is incorrect

Note that override can also occur without a network change, if the following occurs:

- URL specifying the PAC file is incorrect

Endpoint override allows users to continue using the Internet even during technical difficulties (provided Internet access is available), although there will be no security during this time. Override also allows users to change their Internet access (PAC file) settings.

Automatic override is useful if you have traveling consultants or instructors who often work in client networks behind devices over which you have no control. If a consultant or other traveler from your company is using a client network and is positioned behind a proxy server or other network device that prevents direct access to Internet resources, the consultant may need to change the Internet access settings to complete required work.

During an override, the endpoint continues to send authentication information. Once connectivity to the cloud service resumes, the endpoint is automatically re-enabled.

Note that you have an option that allows end users to manually disable the endpoint. This option can introduce vulnerabilities. See *Disabling the endpoint*, page 9, for details.

Override with Internet Explorer

The override behaviors described in this section apply only to Web Endpoint clients using the Internet Explorer (IE) browser. You can manage proxy settings only via the IE browser.

When the endpoint goes into override, the following behavior occurs:

1. The end user is allowed to change the IE proxy settings as necessary.
2. The “automatic” proxy setting is enabled.
3. The proxy settings are set to the most recently saved proxy settings that the user previously entered, but are left unchecked (**not** enabled). If the end user is behind an upstream proxy, then the user will need to manually enable that proxy setting.

If the cloud service becomes reachable (and the client is **not** set to disable), then the following behavior occurs:

1. Existing proxy settings are saved for later use.
2. Proxy settings are then set to use the Websense PAC file.
3. The end user is no longer able to change or save the proxy settings.

If the client machine is set to disable Web Endpoint, the following behavior occurs:

1. The end user is allowed to change the IE proxy settings as necessary.

If the cloud service becomes reachable, because the user manually re-enables Web Endpoint or reboots, the following behavior occurs:

1. Existing settings are not saved.
2. Proxy settings are set to use the Websense PAC file.

The browser will need to be closed and reopened for the new settings to take effect.

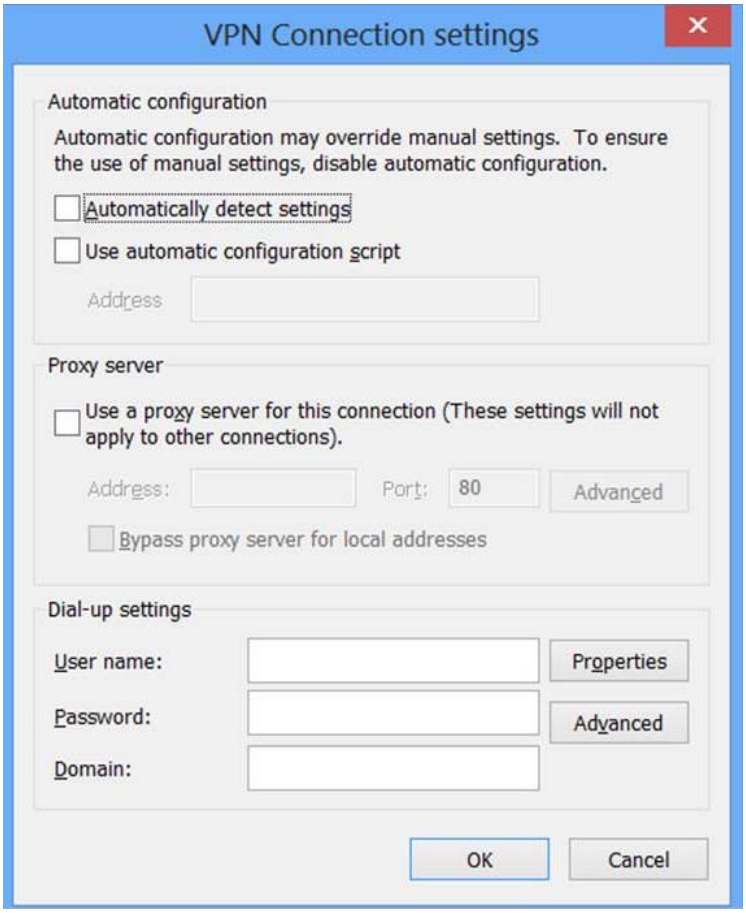
Allowing user changes to IE settings if the cloud service is not reachable

Web Endpoint allows users to change Internet Explorer (IE) proxy settings when the cloud service is not reachable.

Users can change anything in the IE proxy settings dialog box, when the endpoint detects that the service is not reachable.

Note that even the PAC file URL can be changed.

Users can also change IE proxy settings for a specific Remote Access Service connection when the endpoint detects that the cloud service is not reachable.



Saving end user proxy setting changes

When the cloud service is not reachable, the endpoint software saves end-user proxy settings in an encrypted file.

The endpoint then loads the settings from the encrypted file when the cloud service is resumed, and saves additional changes to the same encrypted file when users make them.

Limitations

- End users need to restart their previously opened IE browsers after making changes, in order to apply new settings. Note that changes made through the control panel or other browsers may not be retained.
- If the cloud proxy automatically re-engages due to network changes (for example, the user plugs in a 3G card), the end user needs to restart the browser. Until that restart, existing user sessions that were created before the endpoint re-enforces a Websense PAC file may still use old proxy settings.
- End users' browsers and browser add-ons retain Microsoft limitations after the endpoint stops enforcing Websense PAC settings. The Websense Web Endpoint does not modify the behavior of browsers and browser add-ons when it stops enforcing proxy settings.

Disabling the endpoint

Topic 65064 | Web Endpoint| Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

You have an option that allows end users to manually disable the endpoint; however, be aware that if the disable option is enabled, it would permit end users to circumvent the protections offered by the endpoint software.

Important

Note that if an end user has disabled the Web Endpoint service, a reboot will always enable it.

In the Websense Endpoint package builder, on the Web Endpoint Proxy Settings dialog box, select “Enable local user defined Proxy Setting.”

If you are not using the Package Builder (this applies if you have Web Endpoint only), set the code for the disable function by adding the following to the HWSconfig.xml file before building the endpoint:

```
<LocalProxySetting EnableLocalProxySetting=”1”/>
```

Once set, end users can right click the endpoint icon and select **Disable** to manually disable the endpoint, and click **Enable** to re-enable the endpoint.

If the endpoint is manually disabled, end users can still use the Internet, although there will be no endpoint protection. When disabled, the endpoint:

- No longer intercepts traffic.
- No longer provides transparent user identification to the cloud and hybrid services.
- No longer prevents users from changing their proxy settings.

Unlike override mode, proxy setting changes in the disable mode are not stored for subsequent use, nor is the browser automatically set to use the auto proxy. And, unlike the automatic temporary override, manually disabling the endpoint does stop the endpoint from sending authentication information. Again, note that if an end user has disabled the endpoint, a reboot always enables it.

Diagnostics

Topic 65065 | Web Endpoint| Updated 25-Aug-2014

Applies To:	Websense Web Endpoint, v7.8.x Websense Web Security Gateway Anywhere, v7.8.x Websense Cloud Web Security Gateway, 2014 Release 4 and later

Windows Web Endpoint offers a three-part Diagnostic Dialog that you or your end users can access by double-clicking any of the three possible endpoint status icons that display in the task bar. The Diagnostic Dialog provides information that can assist you with troubleshooting if an endpoint machine is not behaving as expected.

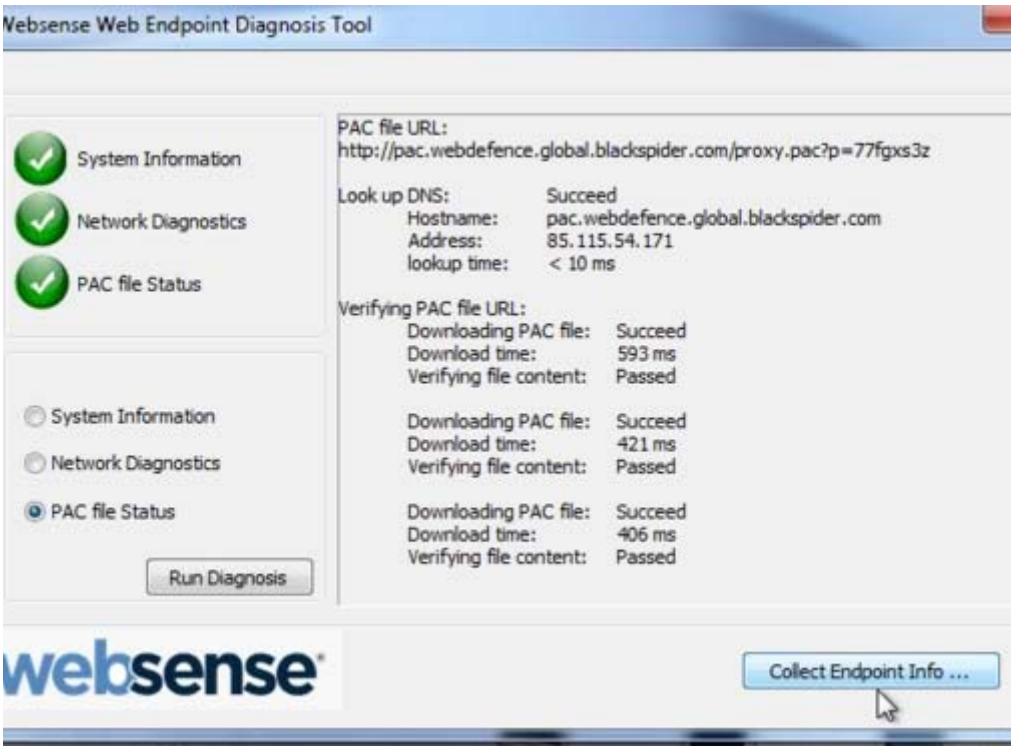
To access the new Diagnostic Dialog, simply double-click on the endpoint status icon in the task bar.

When the dialog is launched, each of the diagnostic tests is executed in sequence. If one of the tests results in a failure, the subsequent tests are not automatically run.

Three diagnostic tests are accessed from this dialog. They run in this sequence:

1. **System Information** - collects basic information related to the specific system on which the endpoint software is installed
2. **Network Diagnostics** - collects information related to basic network connectivity
3. **PAC File Status** - collects information to determine if the PAC file is accessible

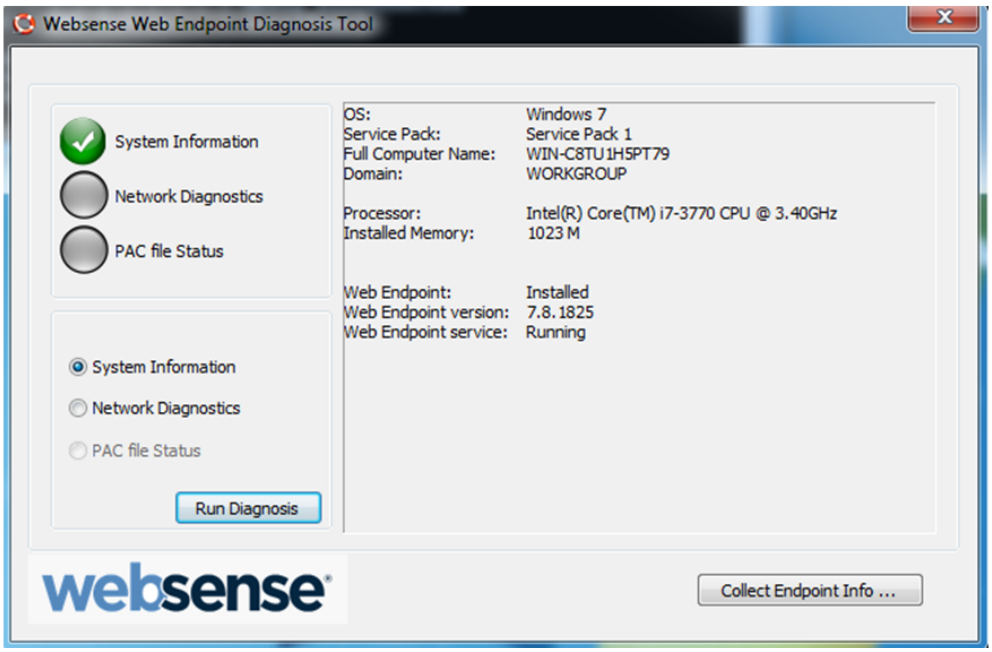
NOTE: Corresponding log files generated from these new diagnostics can easily be collected with the existing **CLIENTINFO.EXE** tool. To run this tool, click the **Collect Endpoint Info...** button on the diagnostics screen, as shown below.



The resulting file is placed onto the desktop. Attach the file to an email to Websense Technical Support or your authorized Websense Reseller.

Sample diagnostic screen shots and log files

System Info



[01/20/2014 10:49:44] ==========Running System Check==========

[01/20/2014 10:49:44] OS: Windows 7

[01/20/2014 10:49:44] Service Pack: Service Pack 1

[01/20/2014 10:49:44] Computer Name: WIN-C8TU1H5PT79

[01/20/2014 10:49:44] Full Computer Name: WIN-C8TU1H5PT79

[01/20/2014 10:49:44] Login User Name: Herbert

[01/20/2014 10:49:44] Domain: WORKGROUP

[01/20/2014 10:49:44] Processor: Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz

[01/20/2014 10:49:44] Installed Memory:1023 M

[01/20/2014 10:49:44] Free system Memory: 446836736 bytes

[01/20/2014 10:49:44] Free Disk space: 51574292480 bytes

[01/20/2014 10:49:44] Web Endpoint: Installed

[01/20/2014 10:49:44] Web Endpoint version: 7.8.1825

[01/20/2014 10:49:44] Web Endpoint service: Running

[01/20/2014 10:49:44] Install Path:C:\Program Files\Websense\Websense Endpoint\

[01/20/2014 10:49:44] Whitelist: OUTLOOK\.EXE|WORDPAD\.EXE|CURL\.EXE

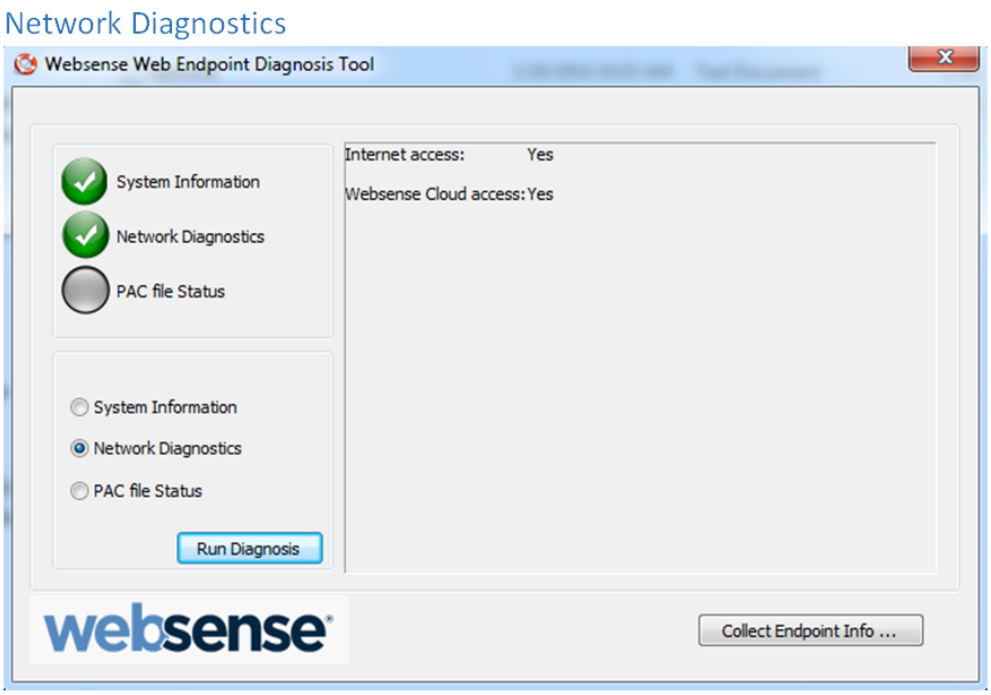
[01/20/2014 10:49:44] PAC file URL: http://pac-lg-qa.odd.blackspider.com:8082/proxy.pac?p=22xx4zbf

[01/20/2014 10:49:44] PAC URL:pac-lg-qa.odd.blackspider.com Port: 8082

[01/20/2014 10:49:44] Check PAC URL Passed.

[01/20/2014 10:49:44] ==========End of System Diagnosis==========

Network Diagnostics



[01/20/2014 10:53:29] ==========Running Network Check==========

[01/20/2014 10:53:29] Internet access:

[01/20/2014 10:53:29] Yes time = 827 ms

[01/20/2014 10:53:29] Websense Cloud access:

[01/20/2014 10:53:29] Resolving URL http://query.webdefence.global.blackspider.com

[01/20/2014 10:53:30] Succeed time = 265 ms

[01/20/2014 10:53:30] Done time < 10 ms

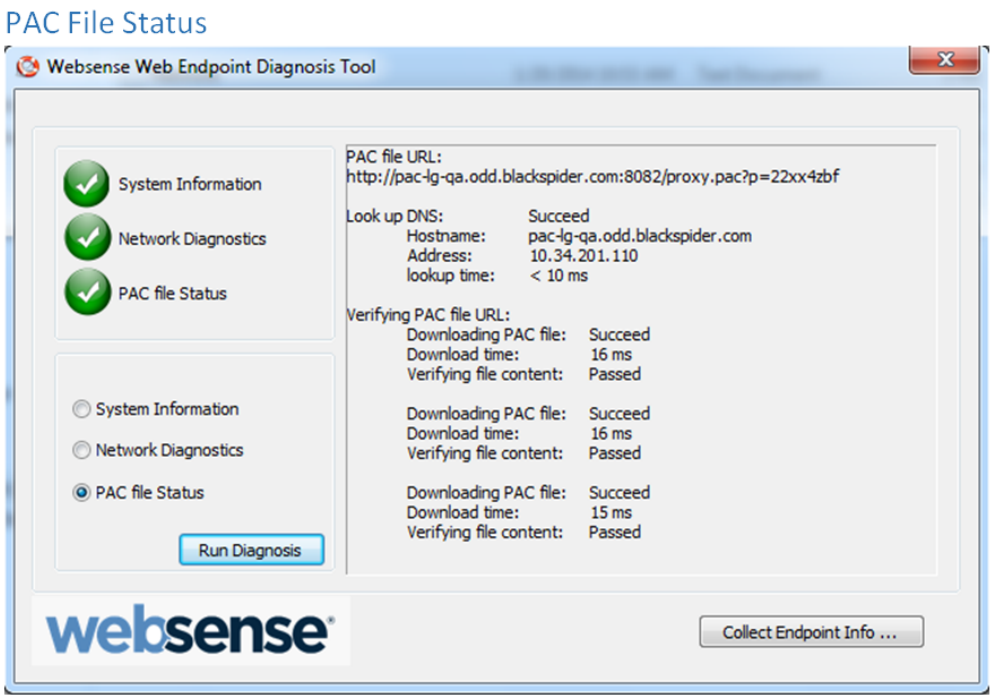
[01/20/2014 10:53:30] DNS Result: 85.115.54.181,

[01/20/2014 10:53:30] Yes

[01/20/2014 10:53:30] Websense Proxy Server:webdefence-lg-qa.odd.blackspider.com:8081

[01/20/2014 10:53:30] ==========End of Network Diagnosis==========

PAC File Status



[01/20/2014 10:56:21] ==========Running PAC file Check==========

[01/20/2014 10:56:21] PAC file URL:

[01/20/2014 10:56:21] http://pac-lg-qa.odd.blackspider.com:8082/proxy.pac?p=22xx4zbf

[01/20/2014 10:56:21] Look up DNS:

[01/20/2014 10:56:21] Succeed

[01/20/2014 10:56:21] Hostname:

[01/20/2014 10:56:21] pac-lg-qa.odd.blackspider.com

[01/20/2014 10:56:21] Address:

[01/20/2014 10:56:21] 10.34.201.110

[01/20/2014 10:56:21] lookup time:

[01/20/2014 10:56:21] < 10 ms

[01/20/2014 10:56:21] Verifying PAC file URL:

[01/20/2014 10:56:21] Downloading PAC file:

[01/20/2014 10:56:21] Succeed

[01/20/2014 10:56:21] Download time:

[01/20/2014 10:56:21] 16 ms

[01/20/2014 10:56:21] Verifying file content:

[01/20/2014 10:56:21] Passed

[01/20/2014 10:56:21] PAC file size is 3810

[01/20/2014 10:56:21] Downloading PAC file:

[01/20/2014 10:56:21] Succeed

[01/20/2014 10:56:21] Download time:

[01/20/2014 10:56:21] 16 ms

[01/20/2014 10:56:21] Verifying file content:

[01/20/2014 10:56:21] Passed

[01/20/2014 10:56:21] PAC file size is 3810

[01/20/2014 10:56:21] Downloading PAC file:

[01/20/2014 10:56:21] Succeed

[01/20/2014 10:56:21] Download time:

[01/20/2014 10:56:21] 15 ms

[01/20/2014 10:56:21] Verifying file content:

[01/20/2014 10:56:21] Passed

[01/20/2014 10:56:21] PAC file size is 3810

[01/20/2014 10:56:21] The average downloading time is 15 ms

[01/20/2014 10:56:21] ==========End of PAC file Diagnosis==========