Release Notes for Websense® Web Endpoint

Topic 55440 | Release Notes | Web Security Solutions | Updated 22-April-2015

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.2

Use these Release Notes to learn what's new and improved for Websense Web Endpoint in Web Security Gateway Anywhere version 7.8.2 and Cloud Web Security Gateway 2014 Release 2.

Please note that Websense Data Endpoint enhancements are described separately in the Data Security release notes linked here.

Websense endpoint solutions secure client workstations, laptops, and other endpoint devices from data loss and inbound web threats when the devices are outside the corporate network.

Endpoint solutions have a server component and include endpoint client software that runs on the endpoint devices to block, monitor, and log transactions (like Internet requests) according to your organization's security and acceptable use policies. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the device.

Websense Web Endpoint enforces the use of the hybrid service for Web Security Gateway Anywhere, and provides a seamless experience to end users for enforcing and directing traffic to Cloud Web Security. The endpoint software passes authentication information, enabling secure transparent authentication.

Contents

Operating system and browser requirements

This version adds support for the following operating system environments:

- Windows 8.1
- Mac OS X 10.9

New in Web Endpoint

Topic 55441 | Release Notes | Web Security Solutions | Updated 25-March-2014

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.2

New features in this release of Web Endpoint are described below.

Status and Diagnostic features for Windows endpoints

The installed Windows Web Endpoint now displays an icon in the end-user's task bar. The new icon serves as both a status indicator and an access point to additional diagnostic information.

- *Status indicators*
- *Diagnostic dialog*
- *Sample diagnostic screen shots and log files*
- *Diagnostic messages and related recovery steps*

Status indicators

Working as expected: When the Web Endpoint software is successfully configured, connectivity to the cloud service exists, and the hosted PAC file is correct and accessible, then all is well and the status icon is displayed as follows:

Temporary override: The system administrator can set a code in the Web Endpoint installation package that enables automatic, temporary **Override** when the end-user's machine encounters a network change event and then detects an absence of connectivity to the Websense cloud service. Network change events include the assignment of a new IP address to a laptop, for example.

This capability is useful for organizations whose traveling consultants or instructors 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 Internet access, the consultant may need to change the Internet access settings to complete required work.

- In these situations, whenever a network event occurs, the Web Endpoint checks to determine if connectivity to the Websense cloud service exists, and if the PAC file can be used.
- If the Websense cloud service cannot be reached, then the status icon shown below is displayed. The Web Endpoint is temporarily overridden.

Your consultant can then manually override the proxy settings on the laptop to ensure access to the Internet. Conditions that might necessitate a temporary override include:

- URL specifying the PAC file location is incorrect.
- Content type of the PAC file is incorrect.
- Endpoint cannot access the Websense cloud services.

A new **manual override** icon has also been introduced. If your site permits manual override, and your end user has enabled it, the following icon is displayed in the task bar:

Manual override for the Websense Web Endpoint can introduce a vulnerability that most sites do not wish to allow. Please contact your Websense Reseller or Websense Technical Support for more details about this feature.

Additional details about override options are provided in the section below titled *Override features for use with Internet Explorer*.

Diagnostic dialog

Another new feature in Web Endpoint at this release is a 3-part Diagnostic Dialog. This provides information that can assist you with troubleshooting if an endpoint machine is not behaving as expected.

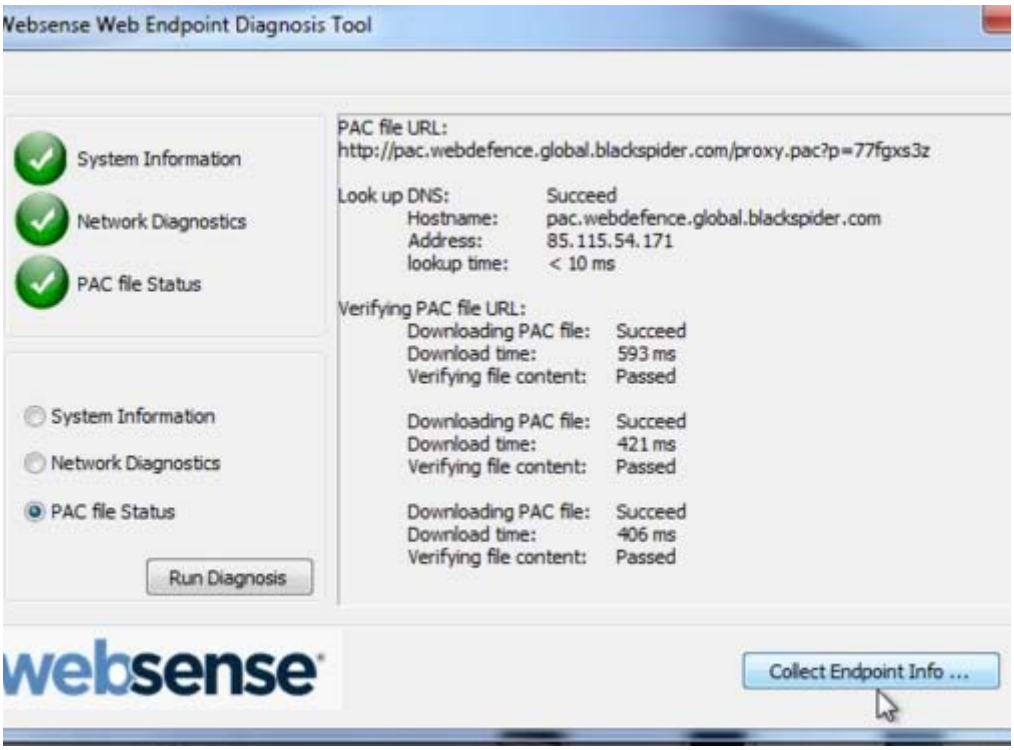
To access the new Diagnostic Dialog, simply double-click on the new endpoint status icon in the task bar.

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

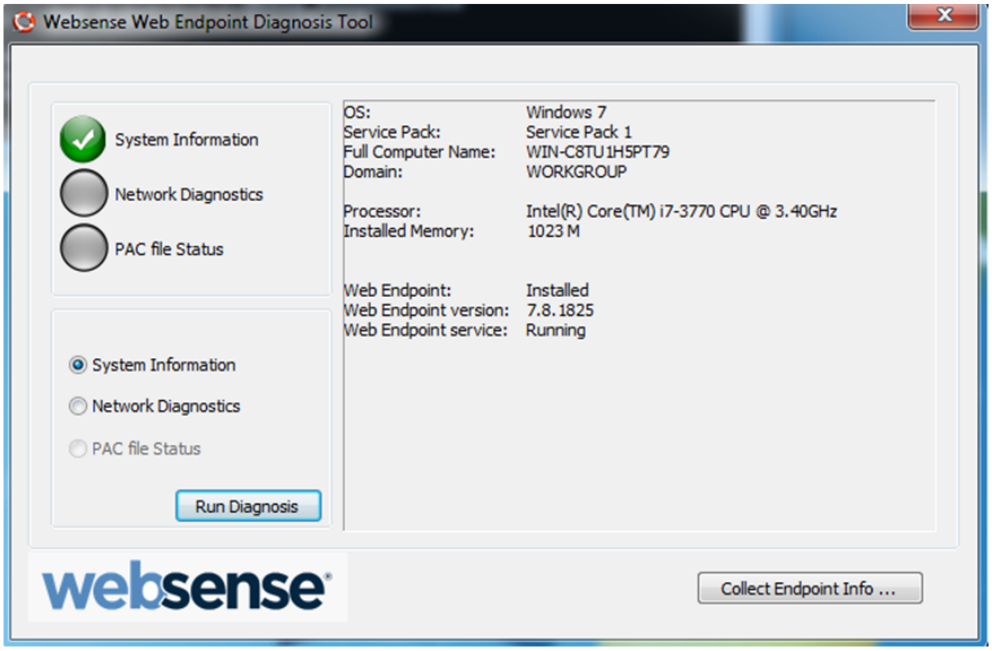
NOTE: Corresponding log files generated from these new diagnostics can easily be collected with the existing **CLIENTINFO.EXE** tool. To run this tool, click the **Collect Endpoint Info...** button on the diagnostics screen, as shown below.



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

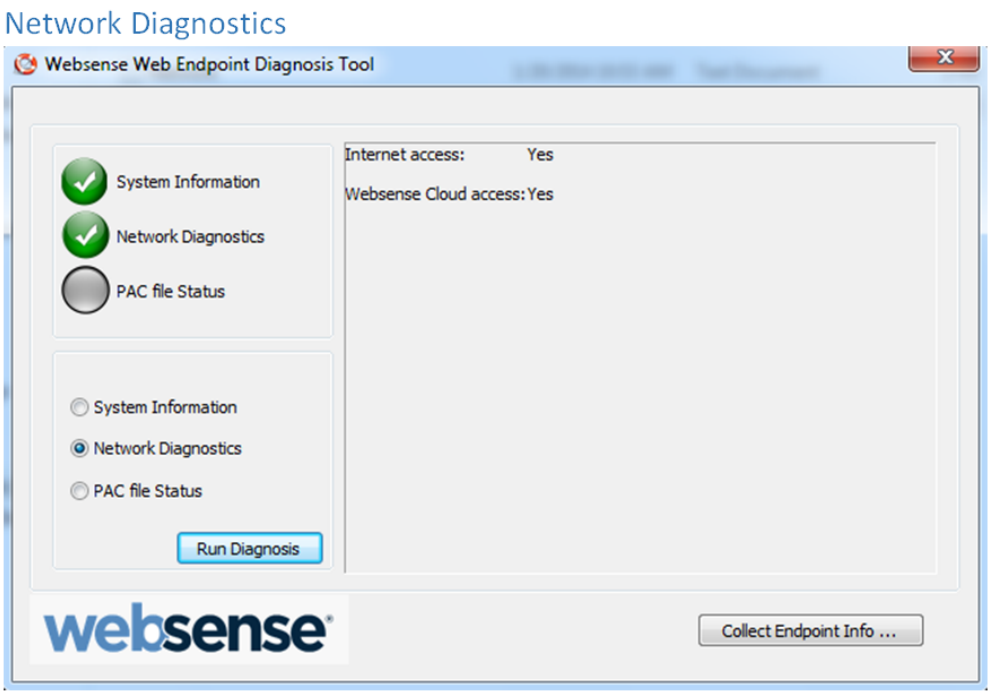
[01/20/2014 10:49:44] PAC file URL: http://pac-lg-qa.odd.blackspider.com:8082/proxy.pac?p=22xx4zbf

[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

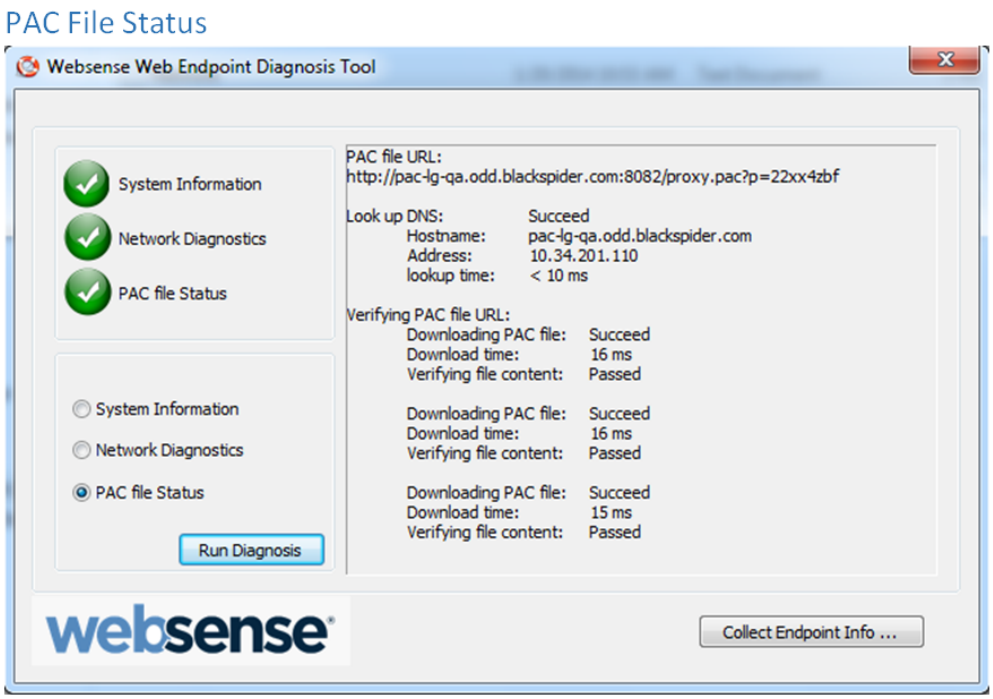
[01/20/2014 10:53:30] DNS Result: 85.115.54.181,

[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==========

Diagnostic messages and related recovery steps

Code	Message	Recovery steps
IDP_SOCKETS_INIT_FAILED	Windows sockets initialization failed.	Restart Windows and check again. If the error still occurs, try reinstalling the TCP/IP protocol
IDS_INITDEBUGLOGFAIL	Debug log initialization failed	Manually clean up the contents in the "Diag" folder under the Web Endpoint installation folder. Make sure guest has read and write privileges for the "Diag" folder
IDS_INITINFOLOGFAIL	Information log initialization failed	Manually clean up the contents in the "Diag" folder under the Web Endpoint installation folder. Make sure guest has read and write privileges for the "Diag" folder
IDS_STRINGDLGSTCSTRING	Welcome to Websense Endpoint Proxy Diagnosis Tool	Information only
IDS_STRINGSYSPROXYAGENT	Web Endpoint: Not Installed	Check if Websense Web Endpoint is installed properly. Reinstall if needed.
IDS_STRINGSYSAGENTSERVICE	Web Endpoint service: Stopped	Information only
IDS_STRINGSYSPACURL	PAC file URL:	Information only
IDS_STRINGSYSAGENTVERSION	Web Endpoint Version:	Information only
IDS_STRINGSYSDETECTFAIL	Web Endpoint information initialization failed	Restart Windows and check again. If the error still occurs, reinstall Web Endpoint.
IDS_STRINGSYSGETINFOFAIL	Failed to get Web Endpoint Client information	Restart Windows and check again. If the error still occurs, reinstall Web Endpoint.
IDS_STRINGNETINTERNET	Internet access: Failed	Check local Internet connection
IDS_STRINGNETCLOUDACCESS	Socket initialization failed	Check local proxy setting. Check content of PAC file.
IDS_STRINGSYSINVALIDPACURL	Invalid PAC URL.	Check Web Endpoint PACFile URL setting
IDS_STRINGSYSERRWINSOCK	Socket initialization failed	Restart Windows and check again
IDS_STRINGNETACCESSFAIL	Resolving PAC file server address failed	Check Web Endpoint PACFile URL Server setting

Code	Message	Recovery steps
IDS_STRINGPACDNSERROR	Resolving DNS record of PAC file host failed	Check Web Endpoint PACFile URL Server setting. Check local DNS setting.
IDS_STRINGPACDOWNLOADFAIL	Download PAC file from server failed	Check Web Endpoint PACFile URL setting.
IDS_STRINGPACFILEVERIFYERROR	The downloaded PAC file has invalid format	Check PAC file at server
IDS_STRINGPACDOWNLOADTIME	The average downloading time is	Information only

Override features for use with Internet Explorer

The override behaviors described in this section apply only to Web Endpoint clients using the Internet Explorer (IE) browser.

- *Enforcing PAC file settings when the cloud service is reachable*
- *Allowing user changes to IE settings if the cloud service is not reachable*
- *Limitations*

Specifics about override triggers and how to re-enable enforcement are detailed here.

- If permitted by your system administrator when the Web Endpoint package was built, an automatic, temporary override of the Web Endpoint occurs when a network event occurs (such as the assignment of a new IP address) and connectivity to the Websense cloud service is unavailable (or the PAC file cannot be used).
- A manual override option for the end user can also be made available. This option can introduce vulnerabilities, of course. If enabled, it would permit end users to circumvent the protections offered by the endpoint software.

Important

If your organization desires to offer the manual override option to end users, please contact your Websense Reseller of Websense Technical Support for more details.

Re-enable endpoint functionality by right-clicking the icon and selecting **Enable**. Note that if an end user has enabled an override for the Web Endpoint service, a reboot will always enable it.

The override behavior works as follows:

If the client machine is manually set to override**,** or if a network event occurs and the client cannot reach the Websense cloud service (because of an upstream proxy, lack of Internet access, or a captive portal), then 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 manual override), 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.

This behavior applies for Internet Explorer only. The browser will need to be closed and reopened for the new settings to take effect.

Enforcing PAC file settings when the cloud service is reachable

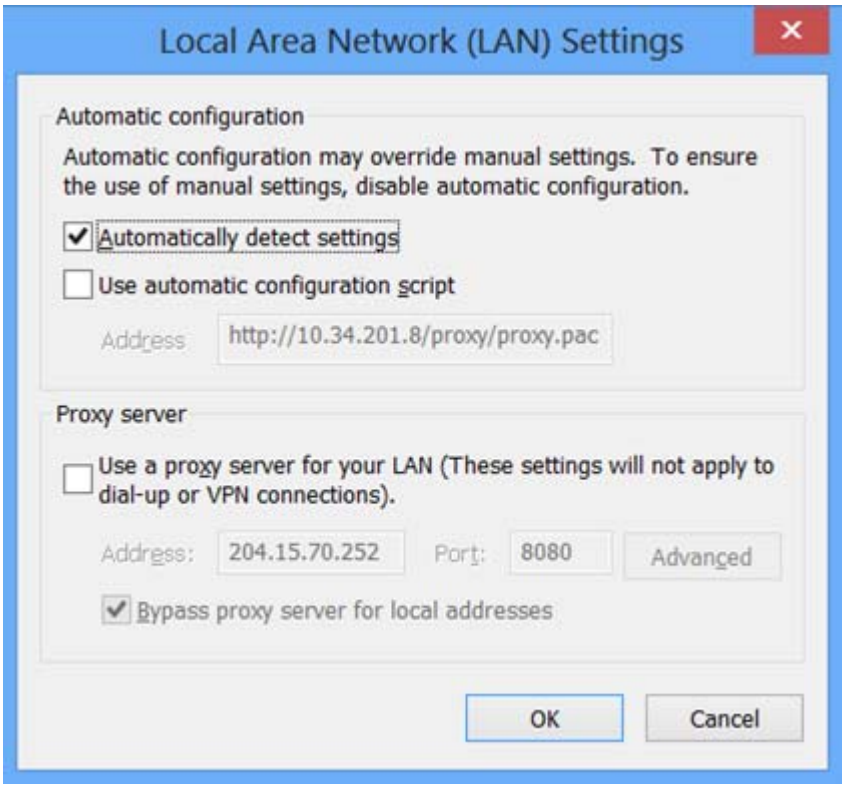
Websense Web Endpoint enforces use of the PAC file settings when the cloud service is reachable:

- 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.

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

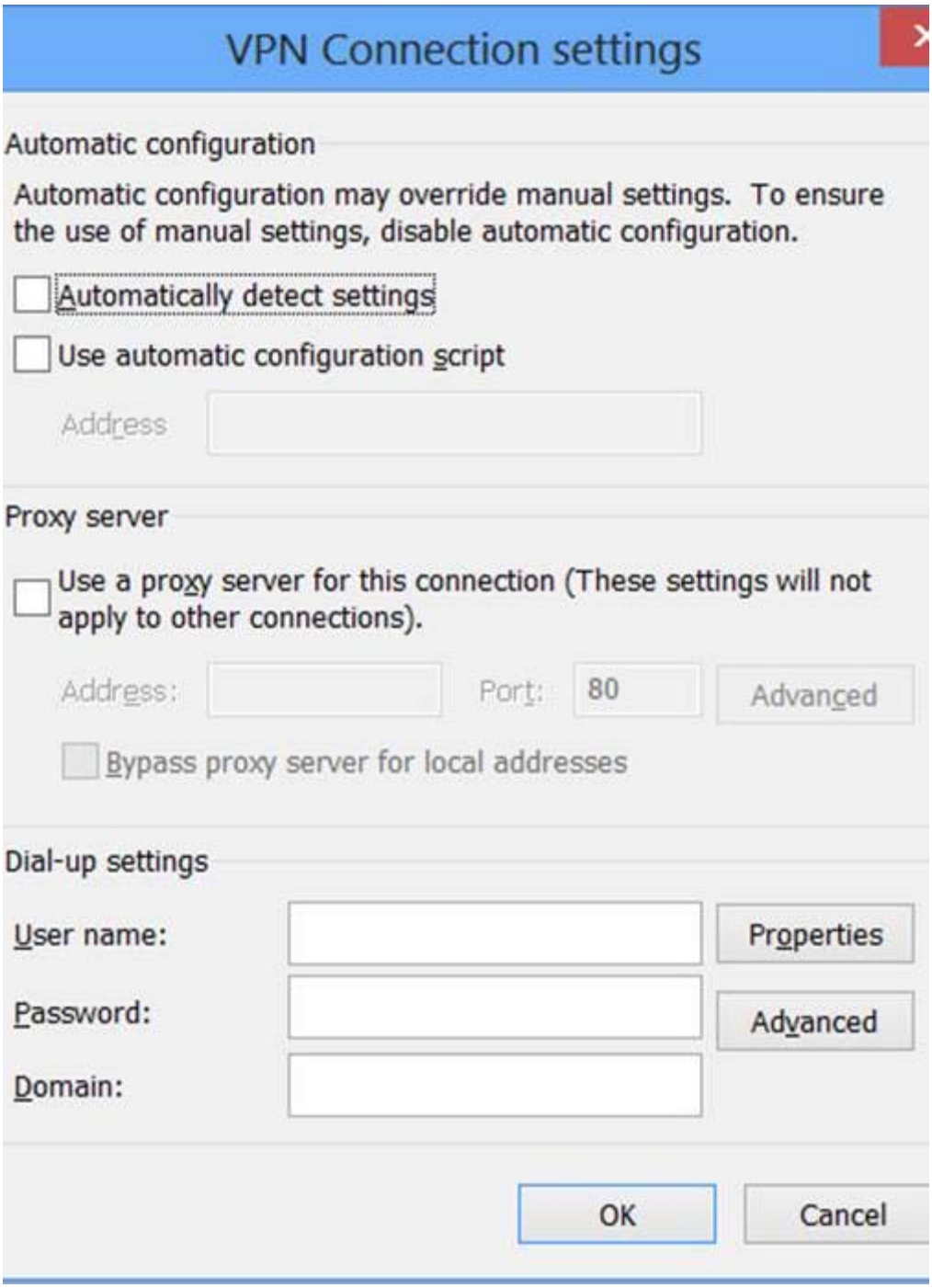
Web Endpoint allows users to change Internet Explorer (IE) proxy settings when the cloud service is not reachable.

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.

Logging

The endpoint software sends logs to the Windows system event log when:

- End users make changes to proxy settings.
- The endpoint detects that the status of the cloud service changes from unreachable to reachable.

All logs are in English.

Limitations

- End users need to restart their previously opened browsers after making changes, in order to apply new settings.
- 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.

Additional resources

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

- How do I install the hybrid Web Endpoint client?
- Combining Web and Data Endpoint clients

Endpoint installation overview

Topic 55443 | Release Notes | Web Security Solutions | Updated 25-March-2014

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.2

Two manual Windows deployment methods are detailed below.

Manually deploying Web Endpoint for Windows

Deploy via GPO

To deploy Web Endpoint via Group Policy Object (GPO):

1. Create a shared folder on the domain controller and set its permissions to read-only.
2. Use a text editor to create a batch file (.bat) in the shared folder (for example **installwebep.bat**).
3. Type the following **msiexec** command into the batch file:

   ```
   msiexec /package "\\<path>\Websense Endpoint.msi" /quiet
   /norestart WSCONTEXT=<value>
   ```

   In your file, replace:

   - <path> with the actual path to the Websense Endpoint.msi file
   - <value> with the WSCONTEXT string shown on the **Settings > Hybrid Configuration > Hybrid User Identification** page (in the Web Security manager) or the **Web Security > Endpoint** page (in the Cloud Web Security portal).
4. Save and close the file.
5. Open the Group Policy Management Console (GPMC) and create a new (or open an existing) GPO for the OU in which your computer accounts reside. To create a new GPO:
   a. In the console tree, right-click Group Policy Objects in the forest and domain in which you want to create a Group Policy object (GPO).
   b. Click **New**.
   c. In the New GPO dialog box, specify a name for the new GPO, then click **OK**.
6. Navigate to **Computer Configuration > Windows Settings > Scripts**, then double-click **Startup** in the right pane.
7. Click **Add**.
8. In the Script Name field, type the full network path and file name of the batch file you created in step 2, then click **OK** and close the GPMC.
9. Run the **gpupdate /force** command from a command prompt to refresh the group policy.

The application is installed on startup. The client may not be fully functional until a reboot occurs.

Deploy to a single machine

1. Copy the endpoint client installation file to a temporary folder on the client machine, then unzip the file.
2. Open a command prompt, then navigate to the location of the unzipped endpoint client files.
3. Enter the following command:

   ```
   msiexec /package "Websense Endpoint.msi" /norestart
   WSCONTEXT=xxxx
   ```

   Replace “xxxx” with the unique configuration code shown on the **Settings > Hybrid Configuration > Hybrid User Identification** page (in the Web Security manager) or the **Web Security > Endpoint** page (in the Cloud Web Security portal). The code is shown as part of the **GPO command** string.

Please see the Web Endpoint documents in the Websense Solution Center and Websense Technical Library for additional setup details.