Release Notes for Websense® Web Endpoint

Topic 65058 | Release Notes | Web Security Solutions | Updated 29-May-2014

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.3

Use these Release Notes to learn what's new and improved for Websense Web Endpoint in Web Security Gateway Anywhere version 7.8.3 and Cloud Web Security Gateway 2014 Release 2 and later.

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

- *Browser requirements*
- *New in Web Endpoint*
  - *Cluster geo-location feature*
  - *Update to override features for use with Internet Explorer*
- *Endpoint installation overview*

Browser requirements

This version adds support for the following web browsers:

- Firefox 28
- Google Chrome 34

The following web browsers support the endpoint client on both 32-bit and 64-bit operating systems:

- Internet Explorer versions 7 to 11
- Firefox 3.x to 28 on Windows and Mac
- Safari 5.x on Windows
- Safari 5.x, 6.x, 7.x on Mac
- Google Chrome from 15 to 34 Windows and Mac
- Opera from 11 to 15 Windows and Mac

New in Web Endpoint

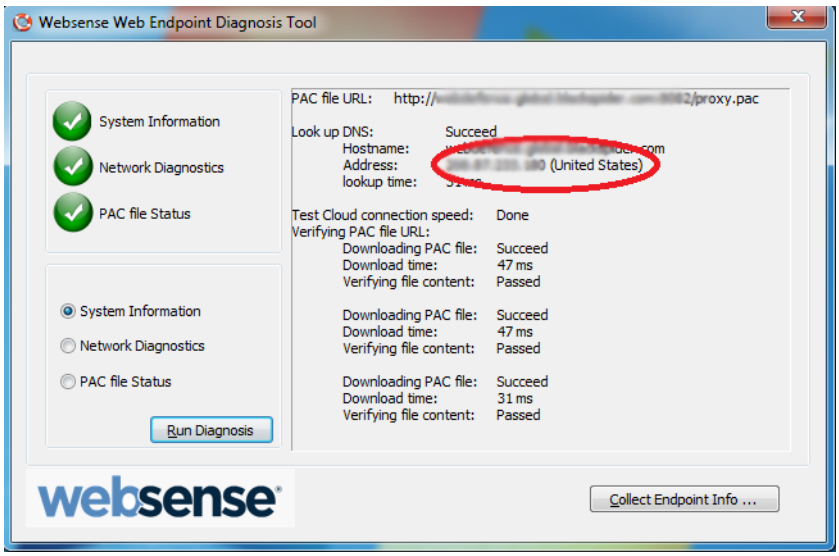
Topic 65059 | Release Notes | Web Security Solutions | Updated 29-May-2014

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.3

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

Cluster geo-location feature

Release 7.8.3 introduces a new feature that automatically shows the geo-location of the cloud service data center (cluster) that you are using. The new feature is available through the Web Endpoint Diagnosis Tool.



Update to override features for use with Internet Explorer

In this release, a disable feature now replaces the manual override feature described in an earlier release. The disable and override features 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 and disable features 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 disable option for the end user can also be made available. This option can introduce vulnerabilities, of course. If the disable option is enabled, it would permit end users to circumvent the protections offered by the endpoint software.

Important

If your organization desires to offer the disable 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 disabled the Web Endpoint service, a reboot will always enable it.

The temporary override and disable behaviors work as follows:

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 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.

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

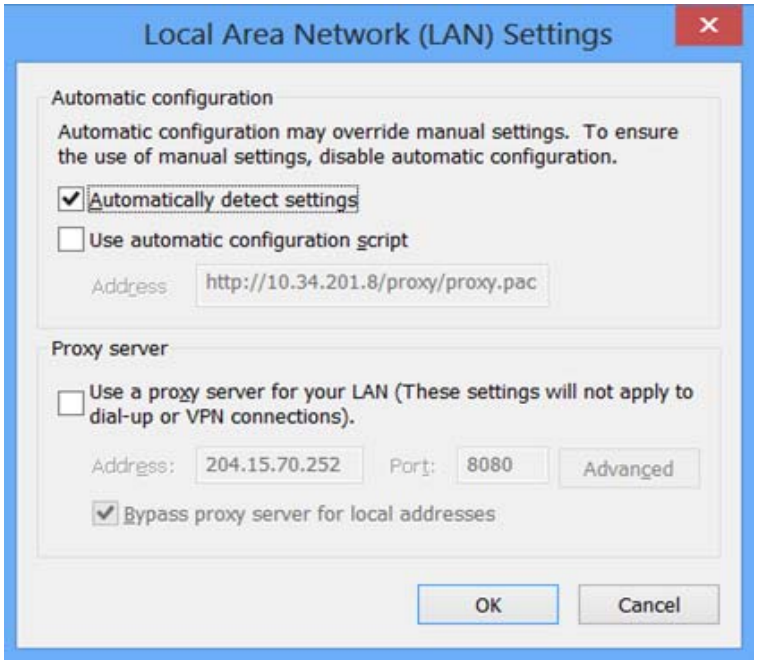
Websense Web Endpoint enforces use of the PAC file settings when the cloud service is reachable:

- 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

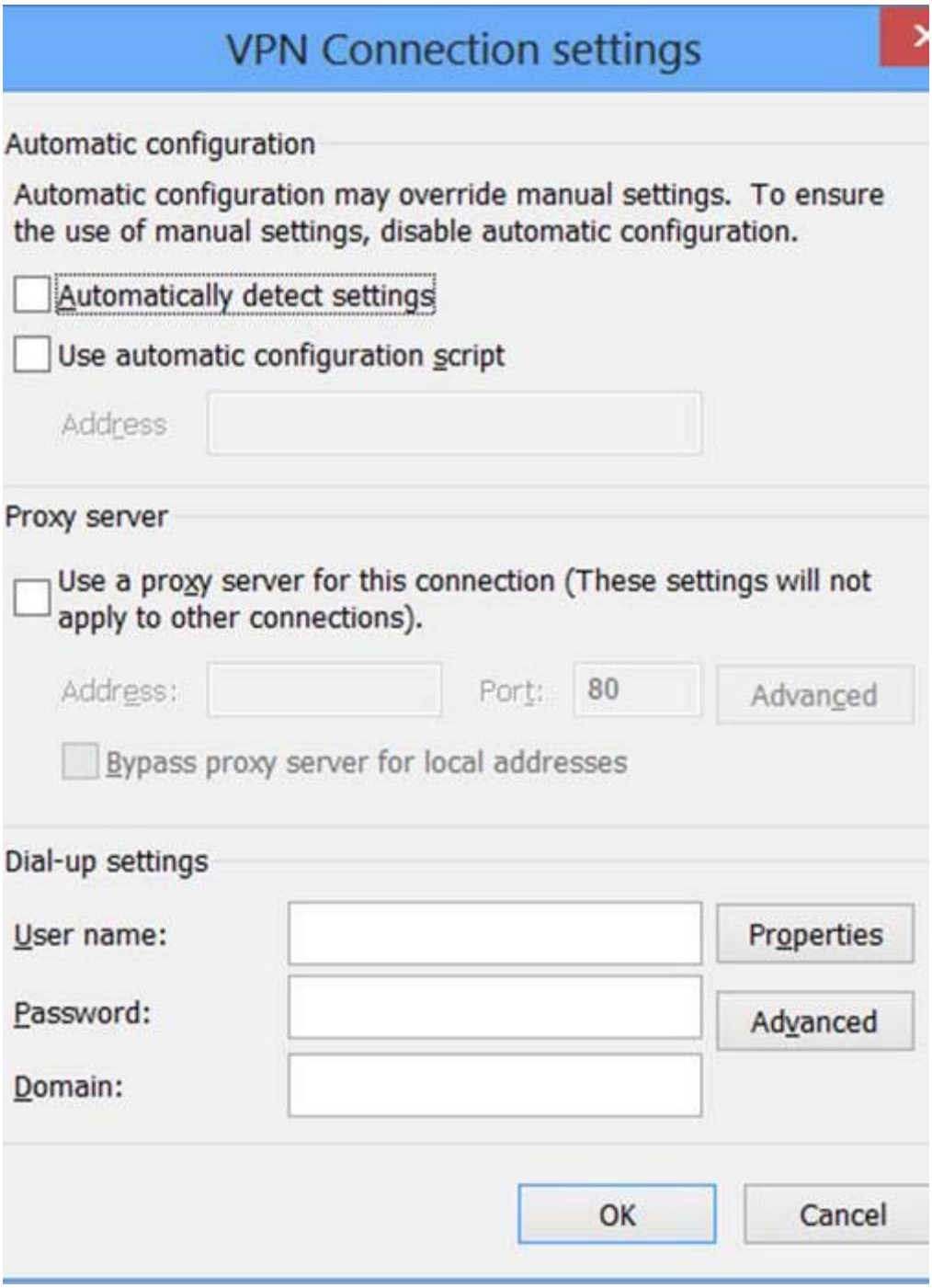
Web Endpoint allows users to change Internet Explorer (IE) proxy settings when the cloud service is not reachable.

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 Application section of the Windows system event log when your system administrator enables the disable option to build an installation package and the following occurs:

- Endpoint detects the cloud service is not reachable or Endpoint is disabled. (Event ID 256: “Websense SaaS Service has entered local user defined mode.”)
- Endpoint detects the cloud service is reachable again or Endpoint is enabled. (Event ID 257: “Websense SaaS Service has entered cloud enforce mode.”)

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 65060 | Release Notes | Web Security Solutions | Updated 29-May-2014

Applies to:	Cloud Web Security Gateway 2014 Release 2 and later Web Security Gateway Anywhere, v7.8.3

For details on installing and deploying Web Endpoint, see Installing and Deploying Web Endpoint.