Important: Unified Agent 4.9.2 Local Enforcement is intended only for clients to connect to a ProxySG that has been designated as a Client Manager. Do not use the Unified Agent installer for clients that connect to the Web Security Service (ThreatPulse).

**Release Notes Contents**

Symantec Unified Agent Local Enforcement Release Notes contains the following sections:

- "Contents" on page 2
- "Installation and Deployment" on page 3
- "Known Issues" on page 4
- "Support" on page 5
Contents

These release notes provide feature descriptions, fixes, known issues, and compatibility notes. These release notes are organized as follows:

- "What’s New in This Release" and "Installation", below
- "Appearance" and "Features Not Available in This Release" on page 3

What’s New in This Release

Features

- Support for macOS High Sierra (10.13)

Fixes

- When service points are not successfully contacted, Unified Agent allows all traffic as long as the default action is allow.
- When the Unified Agent device moves to a network where the proxy requirement has changed (required-to-not required or vice-versa), Unified Agent would time out after an unusually long period.
  - The hostname must not be externally resolvable.
  - Ensure that your web browser specifies the DNS hostname for the PAC file to prevent long timeouts.
- Cloud-specific messages were removed from the diagnostics log.
- Unified Agent no longer wakes a sleeping device.
- Some status messages included an error number instead of describing the error.

Note: Go to www.symantec.com/security-center/network-protection-security-advisories to review the latest vulnerabilities and fixes for Unified Agent.
Appearance

- Unified Agent provides a Windows system tray icon to allow access to the agent console. The agent console displays three tabs:
  - **Status**—Displays web filtering statistics and current status.
  - **Advanced**—Lists the client manager IP and provides options for gathering traces, viewing diagnostics and updating the client configuration.
  - **About**—Displays Unified Agent software version details.

Features Not Available in This Release

The following feature is not available with this release of Unified Agent:

- Accelerating CIFS transfers and byte caching and compression through ADN tunnels

Installation and Deployment

Windows System Requirements

The following table summarizes Unified Agent system requirements:

<table>
<thead>
<tr>
<th>Version</th>
<th>Windows 7</th>
<th>Windows 8/8.1</th>
<th>Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>32/64 bit</td>
<td>32 and 64 bit versions, excluding Home editions</td>
<td>32 and 64 bit versions, excluding Home edition</td>
<td>32 and 64 bit versions, excluding Home edition</td>
</tr>
<tr>
<td></td>
<td>Professional Edition</td>
<td>Professional, Enterprise editions</td>
<td>Professional, Enterprise Editions</td>
</tr>
</tbody>
</table>

**Note:** Symantec recommends that you apply all available updates from Microsoft Windows Update.

OS X System Requirements

- OS X 10.9 and later

Browser Support

Unified Agent 4.9.2 supports all of the latest browser versions.
Upgrade Considerations

As a best practice, Symantec recommends that you upgrade the Client Manager to SGOS 6.5 or later before deploying Unified Agent 4.9.2 to ensure that Unified Agent can use all the latest Blue Coat Web Filtering (BCWF) features and improvements.

Before upgrading from ProxyClient to Unified Agent, you must manually uninstall ProxyClient.

As of ProxySG 6.6.3, Unified Agent can be deployed from a Client Manager. Consult Unified Agent 4.8.x Deployment and Administration Guide for Windows/OS X on support.symantec.com for instructions.

License Unified Agent

Your SGOS license enables you to designate a ProxySG appliance as the Client Manager for an unlimited number of Unified Agent connections. However, you must size your Unified Agent deployment based on Client Manager scalability.

**Important:** Unified Agent web filtering can be used only with the SGOS Proxy Edition. Web filtering *cannot* be used with the SGOS MACH5 Edition.

- To receive BCWF category updates, a valid BCWF database must be installed on the Client Manager with a valid username and password. All Unified Agent clients must connect to the licensed Client Manager at least once every 30 days.

For more information on SGOS licensing, refer to the *SGOS Administration Guide*.

Known Issues

- If ProxyClient is present on a system, it must be uninstalled; Unified Agent cannot be used as an upgrade for ProxyClient.

- When HTTPS filtering is enabled on the Client Manager, both **Block** and **Warn** actions trigger a notification but do not show the block page in the browser.

Compatibility Issues

- Unified Agent must be configured as a trusted application in **ZoneAlarm**.

- Unified Agent must be configured as a trusted application in **Kaspersky Internet Security**.
Support

- Contact Support & Services at support.symantec.com/en_US/contact-support.html

**Important:** On 21 May 2017 all BTO content and most of its functionality was migrated to support.symantec.com. All legacy bto.bluecoat.com links redirect to the new site.

Unified Agent Documentation

Use one of these methods to find the *Unified Agent Deployment and Administration* guides.

**Using the Product Menu**

1. Log in to support.symantec.com.
2. Click **Documentation**.
3. For **Enter a Product Name**, type **SGOS** and select **ProxySG Software - SGOS**.
4. For **Document Type** select **Administration Guide**.
5. Using your browser’s find function, search for **Unified Agent Agent**. Click **Load More** at the bottom of the page as needed.

**Using the Search Function**

1. Log in to support.symantec.com.
2. For **Search Products, Articles, or Forums**, search for **Unified Agent 4.8**.
3. Select the desired document from the results.