Office 365 Best Practices: Skype for Business/Lync

VERSION 9: 08/11/17

Symantec

Copyrights

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

About Skype For Business/Lync Interruptions

Enabling SSL Interception on the ProxySG appliance causes service issues with Skype for Business and Microsoft Lync clients.

What Conditions Cause Skype for Business/Lync to Fail?

Uninterrupted or problematic Skype for Business or Lync client connections depend on the SGOS configuration, what is intercepted, and in versus out of network requests. This does not apply to just overall availability, but individual functions within the service/client.

Symptoms

- Skype for Business clients unable to log in to either Office 365 or the on-premises Lync Server.
- Skype for Business clients unable to join meetings hosted on the on-premises Lync Server/Office 365 cloud/Lync Server behind NAT.
- Skype for Business clients are unable to join meeting audio bridge; they are still able to attend the audio bridge by calling in through the desk phone or opting to *not* be on the audio bridge.

The following conditions provide the symptoms based on specific configurations.

Condition 1

When:

- SGOS: SSL Interception: **On**.
- Client uses port `5061` but firewall blocks this port; the connection defaults to port `443`.

The following occurs:

- Skype for Business/Lync login fails.
- Joining an externally-hosted meeting fails.

Condition 2

When:

- SGOS: SSL Interception: **On**.
- SGOS: Tunnel on Error: **Off**.
- NAT exists between the clients and the Lync server.

The following might occur:

- Joining a meeting might fail.
- Media use within the meeting fails:
  - Skype for Business/Lync audio.
  - Skype for Business/Lync video.
  - Sharing desktop/application.

Technology Root Causes

- Various Microsoft clients, such as Skype for Business and Outlook, now strictly enforce the OCSP/CRL checks. SGOS did not include a CRL Distribution point extension or Authority Information Access (for OCSP) extension on the emulated certificates. This caused these Microsoft clients to abruptly conclude SSL/TLS handshakes and generate exceptions.
- The Skype for Business client uses Session Initiation Protocol (SIP) over SSL protocol during the login phase. If SGOS is configured to intercept SSL traffic on port 443, errors occur because SIP is not understood.
- Skype for Business clients use the Traversal Using Relay NAT (TURN) protocol (if UDP communication is blocked by firewall) to determine the audio functionality related servers. The ProxySG appliance does not understand the Pseudo-TLS handshake.

SGOS Fix

SGOS 6.5.9.15+ provides fixes (with some additional configuration) to allow Skype for Business and Lync clients to operate properly. See "Skype for Business/Lync Fix: SGOS Configuration" on page 6.

If you cannot install the recommended release (currently SGOS 6.5.10.x) at this time, Symantec provides a set of workaround instructions. See Skype for Business/Lync Best Practices.

Skype for Business/Lync Fix: SGOS Configuration

As described in "About Skype For Business/Lync Interruptions" on page 4, SGOS breaks some Skype for Business and Microsoft Lync application connections between clients. Most of these issues are caused after you enable SSL Interception on the ProxySG appliance.

Skype for Business uses the following protocols (in addition to HTTPS when SSL is enabled).

- The Session Initiation Protocol (SIP) is commonly used for voice and video calls and instant messages. Because this protocol defines the messages and traffic between client endpoints, the ProxySG appliance interception of this traffic can cause dropped connections.
- The (Microsoft) Traversal Using Relay NAT (TURN) protocol is used to allocate a public IP address and port on a globally reachable server and relay media from one endpoint to another endpoint.

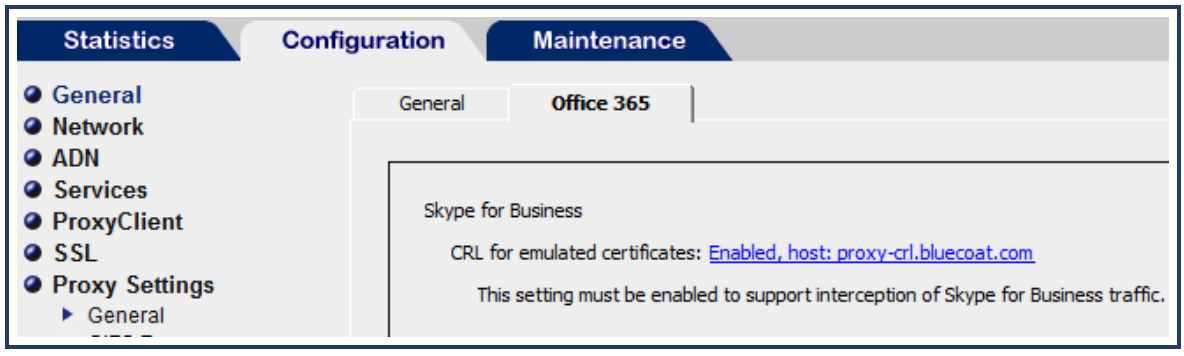
The following configuration and policies enable uninterrupted Skype for Business service.

Required SGOS Releases

- SGOS 6.5.10.4+
- SGOS 6.7.2+

SGOS Update

Symantec identified the causes and provided an SGOS update to restore proper chat client communications. The version is SGOS 6.5.9.15 is the first version to introduce this. Supported versions have a new tab that contains links to various Office 365-related configurations: **Configuration > Proxy Settings > General > Office 365**.



Following the update, additional SGOS configurations are required, as detailed in the following sections.

SGOS Configuration–Verify/Enable Protocol Detection on Services

You must enable Protocol Detection on all SGOS service listeners that intercept traffic generated by Skype for Business. The following services are relevant.

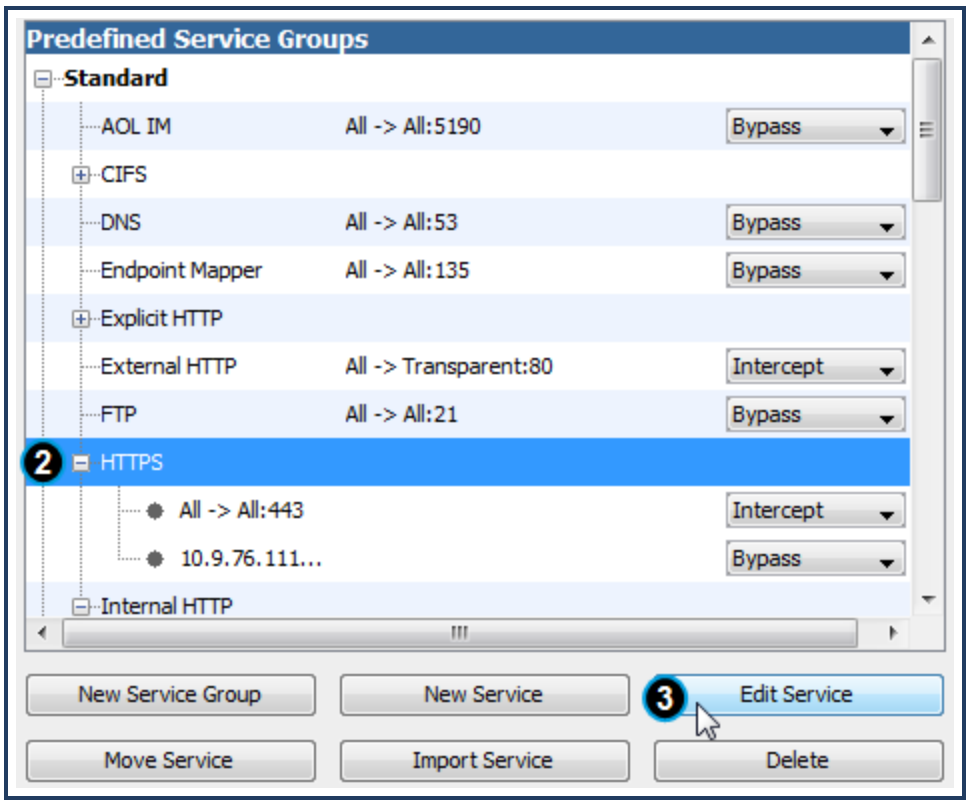
- HTTPS (SSL Proxy)
- Explicit HTTP

- Any custom TCP-Tunnel proxy
- Any SOCKS proxy if it intercepts traffic

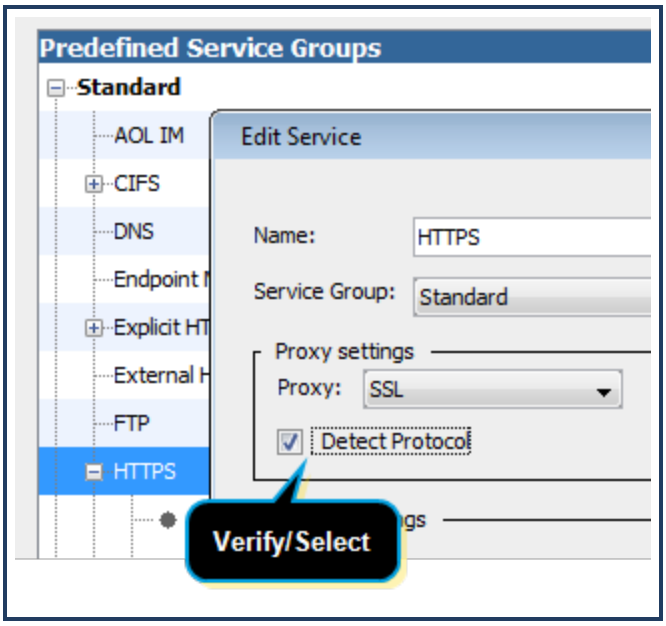
Verify/Enable Protocol Detection for a Service

The following task demonstrates verifying the HTTPS service.

1. In the ProxySG appliance Management Console, select the **Configuration > Services > Proxy Services > Proxy Services** tab.



2. Locate and select the **HTTPS** service.
3. Click Edit. The interface displays the Edit Service dialog.



Verify that the **Detect Protocol** option is selected; if it not, select it and click **OK**.

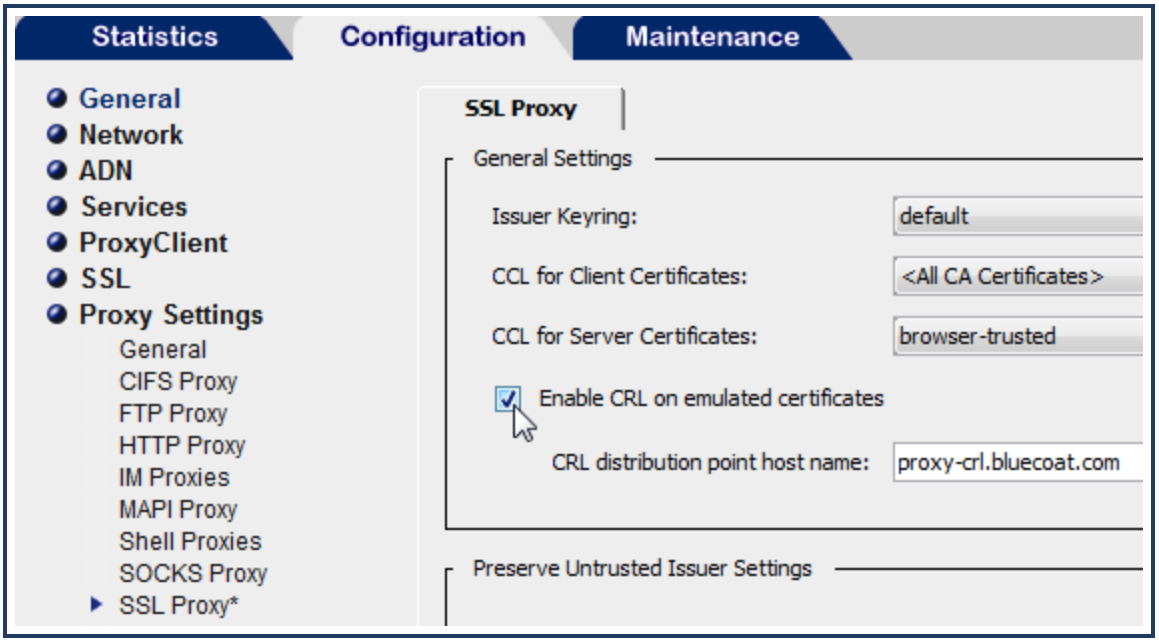
4. Repeat for the other applicable services described above.
5. Click **Apply**.

SGOS Configuration–Enable the CRL Distribution Point

Certificate Revocation Lists (CRLs) enable checking server and client certificates against lists provided and maintained by CAs that show certificates that are no longer valid.

Enable the CRL Distribution Point

1. In the ProxySG appliance Management Console, select the **Configuration > Proxy Settings > SSL Proxy** tab.



2. Select **Enable CRL on emulated certificates**.
3. Click **Apply**.

CLI equivalent command: `sgos#(conf ssl)` **`proxy crl-distribution-point enable`**

About the Default CRL Distribution Point

When the ProxySG appliance intercepts HTTPS (SSL) traffic and the issuer-keyring contains the *CRL Signing* purpose, SGOS adds a *CRL Distribution Point* URL in the forged certificate that is presented to the client.

The default CRL Distribution Point URL is `proxy-crl.bluecoat.com/ssl/crl/issuer_CA.crl`, which resolves to a valid IP address from any Internet source. When the client connects through this URL, the same intercepting ProxySG appliance serves the CRL to the client. The CRL is valid for 30 days after which the SGOS generates a new one.

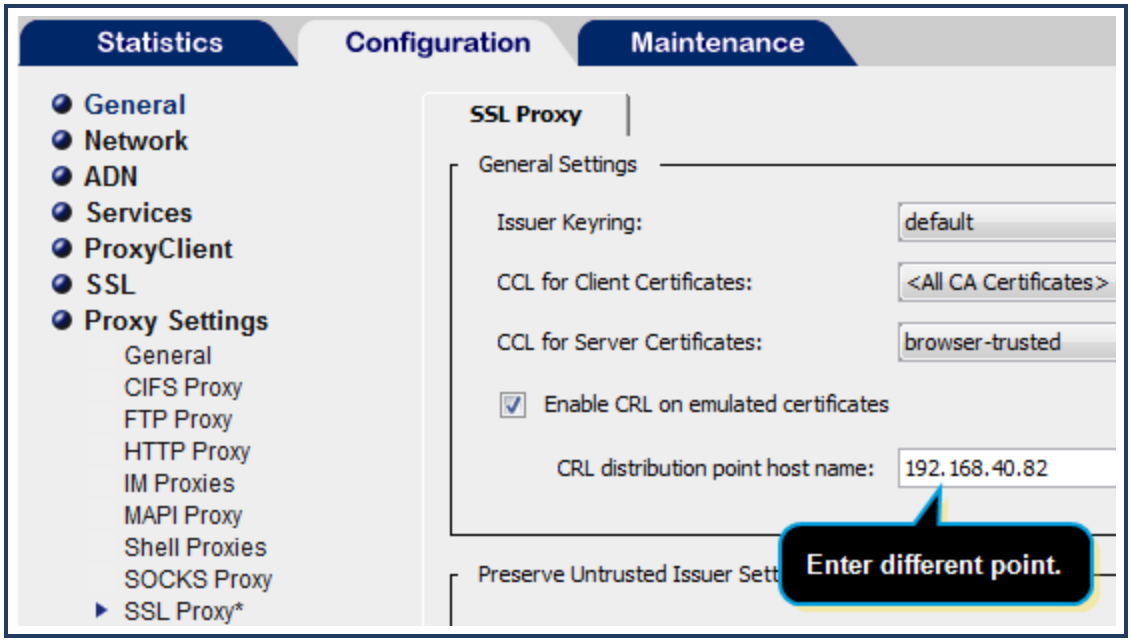
Change Scenarios

Scenario 1–In your deployment, the traffic might route to two different ProxySG appliances–based on HTTP (port `80`/`8080`) or HTTPS (`443`). Because the distribution point is URL-based, the request for CRL might go to the incorrect appliance.

Scenario 2–Multiple ProxySG appliances reside behind a load balancer. Each appliance has its own issuer_CA.

If all ProxySG appliances use the same issuer keyring, you are not required to change the CRL Distribution Point URL.

To accommodate these scenarios, SGOS 6.5.9.14+ provides an option to change the CRL distribution point to the ProxySG appliance IP address or FQDN . Perform this change on each appliance.



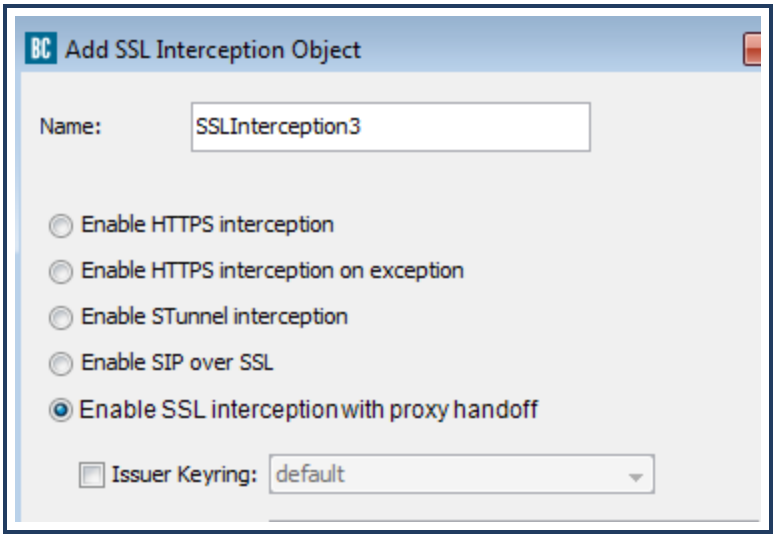
1. Remaining on the **Configuration > Proxy Settings > SSL Proxy** tab, enter the FQDN or the IP address of the ProxySG in the CRL distribution point host name field. Do *not* use the URL scheme (`http`/`https`) or the path to the CRL. For example: `mycompany.com`.
2. Click **Apply**.

```
sgos#(conf ssl) proxy crl-distribution-point hostname <fqdn | ip_address>
```

Policy 1–Enable SSL Interception with Proxy Handoff

This policy allows for the detection of MS-TURN and SIPS. If you have a policy for HTTPS Interception, this policy replaces that.

1. Access the VPM (**Configuration > Policy > Visual Policy Manager**).
2. Modify the **Policy > SSL Intercept Layer** (do *not* create a new one unless one does not exist). Right-click the **Action** column and select **Set**.
3. In the Set Action dialog, click **New** and select **Enable SSL Interception**. The VPM displays the Add Object.



   a. Select **Enable SSL interception with with proxy handoff**.

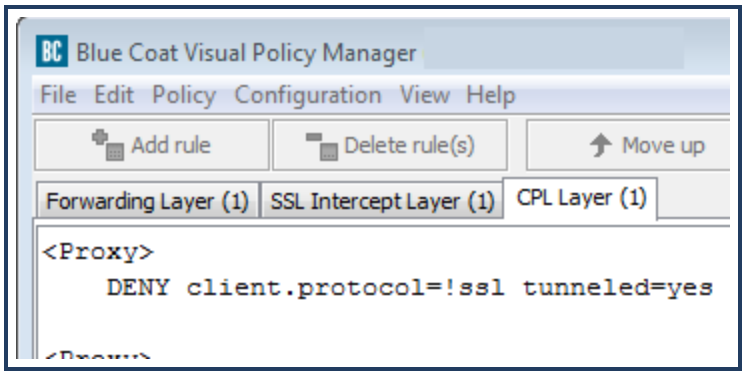
      This performs SSL interception on the traffic and then hands traffic off to a proxy capable of handling it, if such a proxy is available and protocol detection is enabled for that proxy. In cases where protocol detection is disabled or the protocol is not recognized, this option behaves the same as **Enable STunnel interception**.

   b. Click **OK**.
4. With the new object selected, click **OK** to add the object to the layer.
5. Do not install the policy at this time.

Policy 2–Deny Unknown, Undetected Protocols

Because of the Policy 1–Enable SSL Interception with Proxy Handoff step, SGOS detects HTTPS, SIPS, and MS-TURN over SSL; however, SGOS then allows other undetected protocols over SSL (the STunnel route), which might present a potential security risk. Because of this, Symantec/Symantec recommends that you instruct the ProxySG appliance to deny all unknown protocols that are not detected.

Add the following policy. You cannot create a VPM object to accomplish this, but you can add this to an existing **CPL Layer** in the VPM (or add it to the Local or other policy file).



The known protocols are HTTPS, SIPS, and MS-TURN. The proxy denies all traffic that is traversing over an *intercepted* SSL connection that is not one of these three protocols.

Click **Install Policy**.

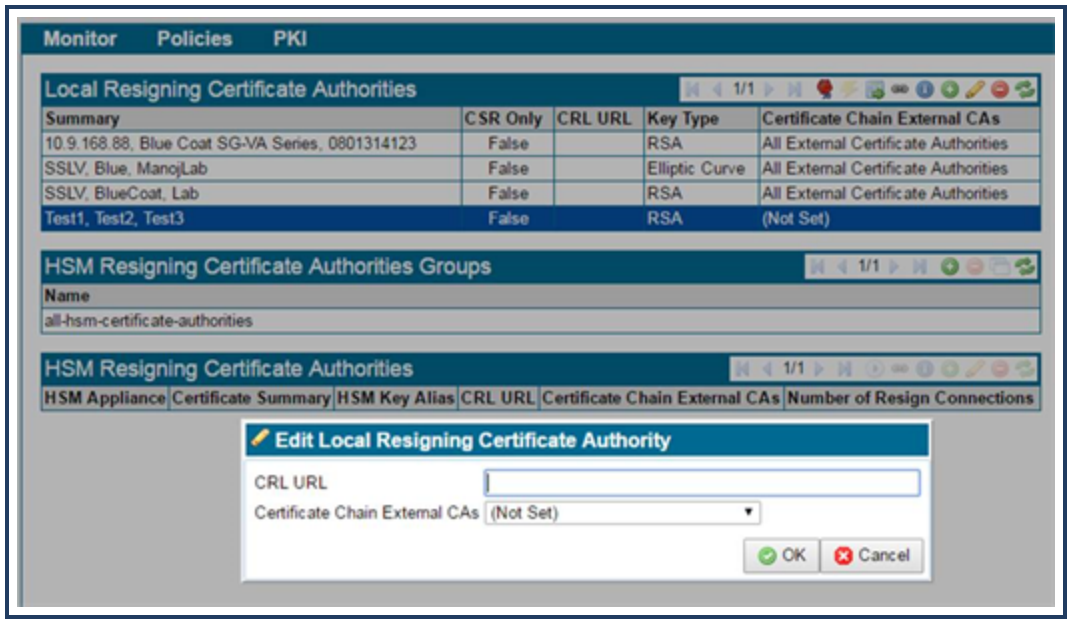
Notes

- For non-intercepted SSL traffic, the proxy cannot apply the Detection Protocol policy. Such traffic is not affected by the rule if other policy allows it; which means it tunnels through the proxy.
- For cases where Protocol Detection is disabled, this policy:
  - Denies CONNECT requests through the HTTP Proxy;
  - Denies requests through the SOCKS Proxy;
  - Denies all traffic through the TCP-Tunnel Proxy service.

  If you have such a deployment, you must adjust your CPL to allow those specific services/requests in this layer *before* the **DENY** rule applies for undetected protocols over intercepted SSL.

SSL Visibility Deployed?

If you have a Symantec SSL Visibility appliance deployed between the clients and the ProxySG appliances, the Skype for Business connection might fail (for example, cannot join a meeting) because the SSL Visibility appliance sends the client certificate without the CRL Distribution Point and is not configured to cut through the traffic. The SSL Visibility appliance provides an option to associate a CRL with a re-signing CA, which allows for multiple CRL points.



Known Issues

Symantec is aware of the following issues, which are currently under investigation.

- B#241685–Although the Management Console **> Statistics > Active Sessions** data displays SIP over SSL and MS-Turn data, you cannot filter by the SIP, SIP over SSL, or MS-Turn client protocols.
- B#243233–Error messages have not been updated to reflect the MS-Turn, SIP, or SIPS values.
- B#242276–Windows phones might not be able to join Skype for Business meetings.
- B#243071–Applies to SGOS 6.5.9.14. Disable SSL Detection policy prevents access to specific HTTPS URLs. See Resolved Issues below.

  See High-Level Topic in WebGuide

Resolved Issues

- B#243333–REVISED

  Authentication *might* have failed for HTTPS traffic when using the policy that was recommended for Skype for Business in SGOS 6.5.9.14. This is resolved in SGOS 6.5.9.15+.

- B#243527–SGOS 6.5.9.15+ changes an option in the VPM SSL Interception object. The **Enable SSL interception with automatic protocol detection** option is now **Enable SSL interception with proxy handoff**. The actual `SSL-Intercept` layer policy installed when this option is selected changed from `ssl.forward_proxy(yes) detect_protocol(yes)` to `ssl.forward_proxy(yes)`.

  The new option does not enable protocol detection in policy. If you enabled the previous policy, Symantec/Symantec recommends that after upgrading, enable **Protocol Detection** on the traffic Service (or in a separate layer if you cannot enable it on the service) and click **Install Policy**, which updates the post-upgrade policy.

- B#243071–Disable SSL Detection policy prevented access to specific HTTPS URLs. SGOS 6.5.9.15+ provides a fix.

  Post upgrade tasks:

- If you previously used the Disable SSL Detection VPM object: After upgrading to a build with the fix (6.5.9.15+), you must open the VPM and click **Install Policy** again to get the correct policy.
- For SGOS 6.5.9.14 through 6.5.10.3 and you have manually installed CPL policy similar to `detect_protocol[ssl,https](no)`, edit that policy to `detect_protocol[ssl,https,sips,sip](no)'`. This allows the policy to maintain the same behavior as in 6.5.9.14.

  See https://support.symantec.com/en_US/article.TECH246796.html for details.