Blue Coat® Systems

Common Policy: Providing Appropriate Security To Users Wherever They Go

Auto Policy Synchronization Guide

SGOS 6.7.x

BLUE COAT

Americas:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Rest of the World:

Symantec Limited
Ballycoolin Business Park
Blanchardstown, Dublin 15, Ireland

Document Revision: SGOS 6.7.x—01/2017

Contents

Chapter 1: Applying Appropriate Policy to Local and Remote Users

About this Document

This document describes how to integrate on-premises appliances (ProxySG appliance or Secure Web Gateway Virtual Appliance) with the Blue Coat Web Security Service to create filtering policies that you can apply globally to local and remote users. This capability is called *Auto Policy Synchronization* and is part of the larger Blue Coat Common Policy feature.

To use Auto Policy Synchronization, you create a cloud-based policy and subscribe your local ProxySG appliances to it. This is called *common policy* when it is shared between appliances and the Web Security Service.

Auto Policy Synchronization enables you to:

- Secure users with appropriate protection that best fits their environment as they travel in and out of the corporate network.
- Create a global policy that can be shared (wholly or partially) between remote and internal users.

Terminology

Refer to the following table for definitions of terms used in this document.

Table 1–1 Terms used in this document

Term	Description
Advanced Labs Network (ALN)	The Blue Coat test network. For details, refer to *Advanced Labs Network: Configuring Auto Policy Synchronization*.
auto policy synchronization	How policy between on-premises appliances and Web Security Service is synchronized. If the Web Security Service and registered appliances can communicate with each other, the policy is kept current because an automatic update occurs every 15 minutes.
Blue Coat WebFilter (BCWF)	Subscription service that delivers real-time protection for web content, categorization, and web application control.
BlueTouch Online (BTO)	Blue Coat support portal, which offers software downloads, documentation, and other information to help you with your Blue Coat appliances: https://bto.bluecoat.com You require a login to access some areas of BTO, such as downloads and release notes.
Command Line Interface (CLI)	One of two ways to access the ProxySG appliance; a command line tool where you can configure the appliance and execute administrative commands.
Common policy	A set of global rules created in WSS that can be applied to users in any location. It can also contain location-specific policy when necessary. In essence, common policy comprises rules that reflect your organization's acceptable use policy. The policy is shared by on-premises ProxySG appliances, ensuring that the same policy applies to both on-premises and remote users.
Content Policy Language (CPL)	The language in which ProxySG appliance policy is written. Policies can be customized to an organization's specific set of users and unique enforcement needs.
Web Security Service	Blue Coat's cloud-delivered security service. Web Security Service identifies and categorizes new web content in real time. Access the Web Security Service at the portal: https://www.threatpulse.com/login.jsp

Before You Begin

Blue Coat recommends that you familiarize yourself with Web Security Service documentation available at BTO:

https://bto.bluecoat.com/documentation/All-Documents/Web%20Security%20Service

When applicable, this document refers to other Blue Coat documents available on BTO; be sure to consult them as required.

Required Information

Before configuring common policy, gather the following information.

- Web Security Service user name and password
- BCWF username and password
- (For some configuration commands) ProxySG appliance `enable` password

Topics in this Chapter

This document has the following sections:

Section A: About the Auto Policy Synchronization Feature

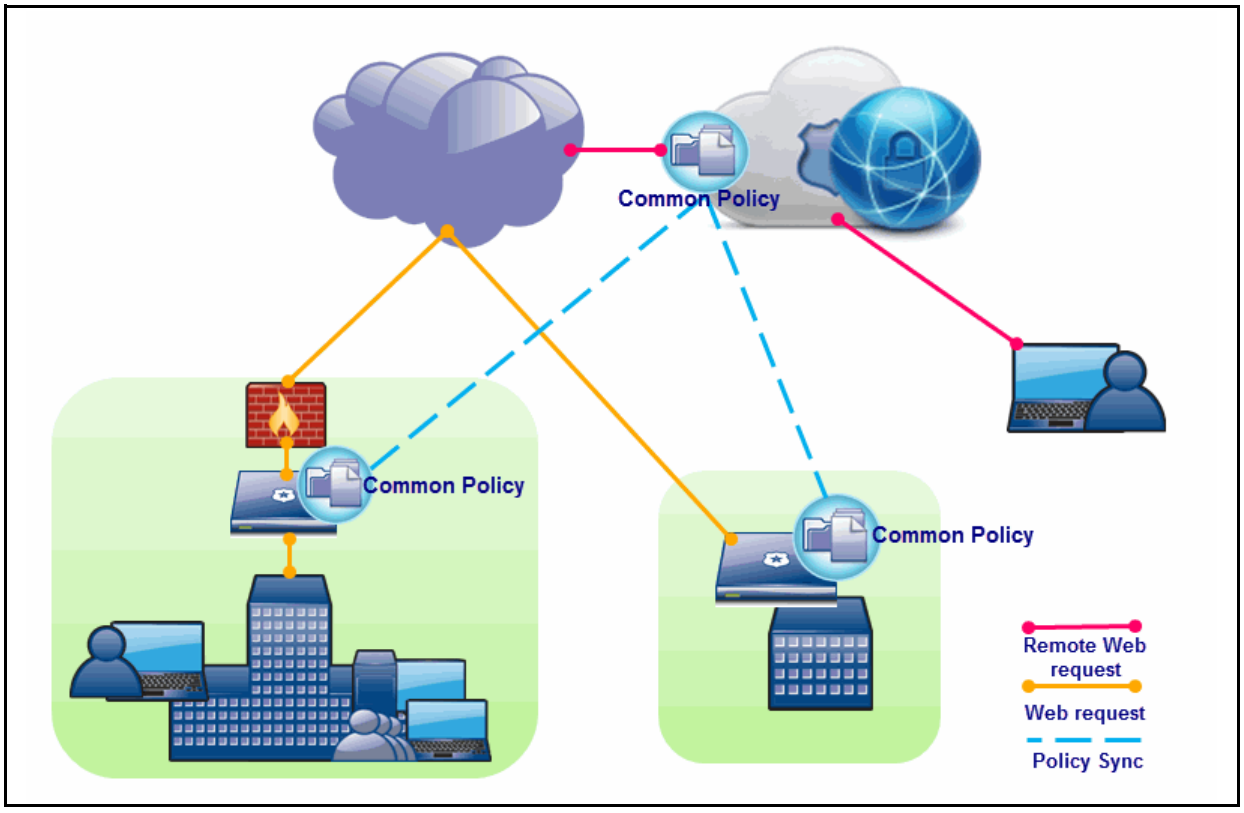
This section describes the Auto Policy Synchronization feature and its benefits, and provides operational details.

Protect Users and Devices Wherever They Are

With the proliferation of broadband and wireless networks, the traditional boundaries of the corporate network have changed. Corporate devices, which once sat safely behind the security of a well-defined network perimeter safeguarded by firewalls and a DMZ, now roam freely—often on unsecured networks. In essence, the corporate network is now anywhere the device is located.

To ensure that users and devices have the appropriate protection at all times and from all locations, administrators can create a single policy and enforce it on on-premises ProxySG appliances (those inside the corporate network) and in the Web Security Service. This policy can be applied on a global basis to all devices and users to ensure consistent protection and enforcement for individual employees around the world, no matter where they are.

Administrators can then configure a locally-defined policy (using the VPM or CPL) on the ProxySG appliances in each location to override the global policy as needed, providing the flexibility and granularity needed to conform to local requirements.



How Auto Policy Synchronization Works

To take advantage of the Auto Policy Synchronization feature, you must first create a cloud-based policy that reflects your organization's acceptable usage policy. This policy is called common policy on the ProxySG appliance.

After defining the common policy, you then register your on-premises ProxySG appliances with the Web Security Service. The registration process establishes a secure channel that authenticates and authorizes the appliance to the Web Security Service, associates it with a specific location, and enables subscription to cloud features such as common policy.

When you enable common policy on the ProxySG appliance, the appliance retrieves and installs the policy. Thereafter, all registered ProxySG appliances periodically synchronize their policy with that configured in the Web Security Service to ensure consistency. All of these transactions are completed in a secure channel with mutual authentication.

About Common Policy

Configured in the Web Security Service portal (**Solutions > Content Filtering > Policy**), common policy contains a set of global rules that can be applied to users in any location. It can also contain location-specific policy when necessary. In essence, common policy comprises rules that reflect your organization's acceptable use policy.

If the global policy does not conform to local conditions, you can either include location-specific policy in the common policy or modify the locally-defined policy on the ProxySG appliances in that location. The appliance evaluates the common policy rules *before* the local policy file so that local administrators can override any global rules that do not apply.

For example, a company might have to block specific URLs in a branch office to enforce compliance with local laws.

The common policy applies to all data accessed by users from outside the network. The common policy also applies to any data passing through ProxySG appliances inside the corporate network, if those appliances are registered and subscribed to the common policy feature. Once subscribed, all appliances periodically synchronize their policy with Web Security Service.

Note: Logistically, you cannot enable both common policy and universal policy, and the Web Security Service portal provides different features depending on which implementation you use.

Order of Policy Evaluation

When Auto Policy Synchronization is configured, the policy installed on the ProxySG appliance is a combination of the common policy and all locally-defined policies. As stated earlier, common policy is evaluated first. The default order of evaluation is as follows:

1. Common Policy

2. Visual Policy Manager (VPM)
3. Local Policy
4. Central Policy
5. Forward Policy

Note: If multi-tenant policy is installed on the ProxySG appliance, you must disable multi-tenancy before enabling common policy. Issue the following CLI command:

```
#(config general)multi-tenant disable
```

For details on multi-tenant policy, refer to the *Multi-Tenant Policy Deployment Guide* on BTO.

Prerequisites

The following are prerequisites to using the Auto Policy Synchronization feature:

- (For Management Console configuration; recommended) Install SGOS 6.7.x or later on your on-premises ProxySG appliances.

  (For CLI-only configuration) Install SGOS 6.4.x or later on your on-premises ProxySG appliances.
- Obtain a Blue Coat Web Security Service account. (Contact your Blue Coat Sales representative.)
- Obtain a Cloud Services: Common Policy subscription. (Contact your Blue Coat sales representative.) The subscription is referred to as an *entitlement*.

Section B: Configure Auto Policy Synchronization

To use the Auto Policy Synchronization feature, you must complete tasks in the Web Security Service portal as well as on the on-premises ProxySG appliances that you want to subscribe to common policy. The following is a high-level list of these tasks:

1. Ensure that you have satisfied all prerequisites listed in "Prerequisites" on page 6.
2. Install the Client Connector and Auth Connector.

   See "Task One: Initial Configuration" on page 7.
3. Create the common policy in the Web Security Service portal.

   See "Task Two: Common Policy Configuration" on page 7.
4. Configure the ProxySG appliance:
   a. Enable Blue Coat WebFilter on the appliance.
   b. Register the appliance with Web Security Service.
   c. Enable common policy on the appliance.

   See "Task Three: Appliance Configuration" on page 8.

Task One: Initial Configuration

This section describes the installation tasks you must complete before enabling common policy.

1. Install the Client Connector software on all devices that travel outside corporate networks. This is required only if you plan to enforce common policy on these devices.

   For more information about configuring the Client Connector, refer to the *Web Security Service Access Methods WebGuide* on BTO.
2. Download and install the Auth Connector to at least one domain controller (or member server), depending on the access method. The Auth Connector connects to the Web Security Service and provides the user/group information from the Active Directory (AD).

   For more information about installing the Auth Connector, refer to the *Web Security Service Access Methods WebGuide* on BTO.

Task Two: Common Policy Configuration

This section describes how to create common policy in the Web Security Service to prepare for on-premises appliance registration.

Log in to the Web Security Service Portal

Log in to the Web Security Service portal:

1. In a browser, enter the following URL:
   `https://portal.threatpulse.com`
2. Enter your access credentials. The browser displays the **Overview** dashboard.

Create Common Policy Rules

Create common policy rules:

1. Access the Web Security Service portal.
2. If you are not already in Solutions mode, select **Solutions**.
3. Select **Content Filtering > Policy**.
4. Select **Blocked Categories**. All available categories display, grouped by category genres.
5. To block a category, select it. To allow a category, clear it. Making a change to an option displays a yellow triangle with an exclamation mark. This symbol indicates that the change is not yet committed.

6. Click **Activate** to commit the changes.

Note: Blocking the Security Threats categories helps prevent malware from entering your network; thus, these categories are always included and cannot be cleared. They are displayed only for your information.

Task Three: Appliance Configuration

After configuring common policy in the Web Security Service, you must register your on-premises appliances and enable common policy.

Verify Blue Coat WebFilter is Enabled

Before registering your appliance, verify that the Blue Coat WebFilter service is enabled on the appliance and that the subscription is valid.

Verify that Blue Coat WebFilter is enabled and valid:

1. Log into the Management Console:
   `https://`*`proxysg_ip`*`:8082`
2. Select **Configuration > Content Filtering > General**.
3. Under **Providers**, verify that **Blue Coat WebFilter** is enabled. If it is disabled, select it to enable it.

4. Select **Configuration > Content Filtering > Blue Coat**.
5. Click **Apply** to save your changes.

   To download the current WebFilter database, click **Download Now**. (You might need your BCWF credentials.)

Register the Appliance with Your Web Security Service Account

Registration is used to authenticate and authorize the appliance and its traffic to the Web Security Service. The registration process also associates the ProxySG appliance with a user-specified location. The location is automatically added to the Web Security Service when you register the appliance.

Register the appliance with the Web Security Service account:

1. In the Management Console, select **Configuration > Cloud Configuration > Cloud Registration**.

   The browser displays the Cloud Registration tab.
2. Click **Register This Device**.
3. On the registration dialog, enter the following details:
   - **Username**: The Web Security Service account username
   - **Password**: The Web Security Service account username
   - **Location**: The location with which to associate the appliance, such as *Chicago4* or *DC2*.

     If the appliance was registered previously, the location associated with it appears in the Device Information section; however, you can enter a different location in this dialog.
4. Click **Register**. If registration is successful, the console displays the message, "This device has been registered with portal.threatpulse.com".

Deregister the Appliance

To deregister the appliance and revert to local policy only, see "How do I deregister the appliance?" on page 27.

Manage Locations

Each appliance must be registered with a specific location. Registering the ProxySG appliance with the Web Security Service (see "Register the Appliance with Your Web Security Service Account" on page 9) automatically adds the specified location.

Alternatively, you can add locations before registration in the Web Security Service portal. You can also merge existing locations in the portal.

Manage locations in the Web Security Service portal:

1. Log in to the Web Security Service portal.

2. If you are not already in Service mode, select **Service**.
3. Select **Network > Locations.**
4. To add a location:
   a. Click **Add Location**. The browser displays the Add Location dialog.
   b. Complete the Location dialog:
      - Provide the **Name** of the location. For example, enter the name of the city where the appliance is located.
      - Select **Blue Coat Device** as the Access Method.
      - Select the **Estimated User** range that will be sending Web requests through this gateway interface. Blue Coat uses estimated user counts to help to determine resource allocation.
      - Select a **Time Zone** and fill out location information.
   c. Click **Save**.

Move Locations

To move an appliance to another location, see "How do I move a registered appliance to another location?" on page 28.

Enable Common Policy Synchronization

After registering your appliance, you must subscribe to common policy.

Enable common policy:

1. In the Management Console, select **Configuration > Cloud Configuration > Cloud Registration > Cloud Services**.
2. In the list of Services, select **Common Policy** and click **Apply**.

   After the appliance notifies you that a change was made, dismiss the message and look in the Status column look for details such as "Enabled. expires on *YYYY-MM-DD*".
3. To verify that common policy is enabled, click the **Cloud Registration** tab. and review the status details in the Device Information section, including entitlement, the last common policy update, and subscribed services.

Force an Update

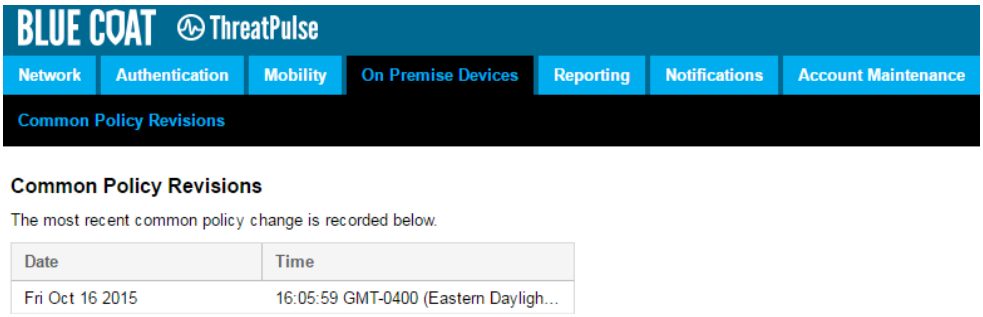
After common policy is enabled, appliance policy synchronizes with the Web Security Service at 15-minute intervals. This interval cannot be changed, but to force a common policy update, click **Update Now** (**Configuration > Cloud Configuration > Cloud Registration > Cloud Services**). The console displays an "Update in progress" message. To cancel the download in progress, click **Cancel**.

Verify Policy Installation

To verify that the most recent common policy rules have been downloaded and installed, compare the timestamp in the ProxySG Management Console with that in the Web Security Service portal.

Verify policy installation:

1. In the Management Console, select **Configuration > Cloud Configuration > Cloud Registration**.
2. In the Device Information section, look for the date and time of the last policy update.
3. Log i n to the Web Security Service portal.
4. Select **Service > On Premise Devices > Common Policy Revisions**.



5. Note the timestamp. If it differs from that on the ProxySG appliance, the policies are not synchronized.
6. (If necessary) Update the policy on the appliance; see "Force an Update" on page 10.

Disable Common Policy

You can disable common policy to revert policy to local policy rules only.

Disable common policy:

1. In the Management Console, select **Configuration > Cloud Configuration > Cloud Registration > Cloud Services**.
2. In the list of Services, clear the **Common Policy** selection and click **Apply**.

   After the appliance notifies you that a change was made, dismiss the message and look in the Status column look for details such as "Disabled. expires on *YYYY-MM-DD*".

   On the Cloud Registration tab, under Device Information, the Common Policy entitlement should display the same status. In addition, Cloud Services statistics should not appear on the **Licensing** and **Subscription** tabs (**Statistics > Health Monitoring**).

Section C: Troubleshoot Issues with Auto Policy Synchronization

If you receive common policy update errors or policy compilation warnings, do the following:

Troubleshooting Task	Reference
Verify all prerequisites have been met.	"Prerequisites" on page 6
Verify that the Blue Coat WebFilter service is enabled.	"Verify Blue Coat WebFilter is Enabled" on page 8
Review the entitlement status.	Step 3 in "Enable Common Policy Synchronization" on page 10
Log in to the Web Security Service portal to check for error messages.	"Review Web Security Service Portal Error Messages" on page 12
Troubleshoot policy warnings and errors.	"Check Installed Policy" on page 13
Review the Event log for warnings or errors.	"Check the Event Log" on page 15

Review Web Security Service Portal Error Messages

To review errors and warnings in the Web Security Service, click **Messages** in the upper right corner of the portal.

Check Installed Policy

The following policy commands can help you troubleshoot policy compilation warnings and errors:

- "View Installed Policy" on page 13
- "View Policy Deprecations, Errors, and Warnings" on page 13
- "Display the Policy Source" on page 14
- "Perform a Policy Trace" on page 15

For more information on CLI commands and CPL, refer to the *Command Line Interface Reference* and the *Content Policy Language Reference*, respectively, on BTO.

View Installed Policy

Use the `show policy` command to view installed policy. The output of this command lists both the common policy and the local policy that are currently installed. You can also use the `show policy` command to verify your changes to common policy.

Issue the following command:

```
#(config) show policy
```

The following is an example of the output:

```
#(config) show policy
   ;Policy - Current
   ; Installed Policy -- compiled at: Wed, 01 Aug 2012 20:24:16 UTC
   ;     Default proxy policy is DENY
   ; Customer Configuration
   define config.customer
     string:company.name("Blue Coat Systems") ; default
     string:visuals.css("0204") ; default
     string:coach.duration("session") ; default
     string:password_override.duration("session") ; default
   --More--
```

Note: When a locally-defined policy is installed on the appliance and common policy is enabled, the installed policy is always a combination of local and common policy. See "Order of Policy Evaluation" on page 5 for more information.

View Policy Deprecations, Errors, and Warnings

Use the `show policy listing` command to display deprecated CPL and compilation errors and warnings.

Issue the following command:

```
#(config cloud-service) show policy listing
```

The following is an example of the output:

```
#(config cloud-service) show policy listing
```

```
Policy installation
Compiling new configuration file: Inline configuration
Wed, 01 Aug 2012 22:18:00 UTC
Warning: Access logging has been disabled in configuration; all
access_log properties will be ignored

There were 0 errors and 1 warning
```

Display the Policy Source

Use the `show sources policy` command to view elements of the specified policy. This can be useful for comparing common policy with local policy.

Issue the following command:

```
#(config cloud-service) show sources policy
```

The following is an example of the output:

```
#(config cloud-service) show sources policy ?
   central              Show source file for central policy
   common               Show source file for common policy from the cloud
   forward              Show source file for forward policy
   local                Show source file for local policy
   threat-protection    Show source file for threat-protection policy
   vpm-cpl              Show source file for VPM CPL policy
   vpm-xml              Show source file for VPM XML policy
   #(config cloud-service) show sources policy common
   ;Policy Version: 35
   <Proxy BC_Appropriate_Use> condition=BC_appropriate_use_layer_guard
   [Rule] ; Blocked Categories
      condition=BC_CF_blocked_categories
   variable.BC_AU_Decision("DENIED_CATEGORY_GLOBAL")
   [Rule] ; default
      variable.BC_AU_Decision("ALLOWED_DEFAULT")

   define condition BC_CF_blocked_categories
     category=('Child Pornography','Gambling','Illegal Drugs','Malicious
   Outbound Data/Botnets','Malicious Sources','Phishing','Proxy
   Avoidance','Scam/Questionable/Illegal','Spam','Violence/Hate/
   Racism','Weapons')
   end

   define condition BC_Cloud_AU_HTTPS_Restricted_categories
      server.certificate.hostname.category=('Child
   Pornography','Gambling','Illegal Drugs','Malicious Outbound Data/
   Botnets','Malicious Sources','Phishing','Proxy Avoidance','Scam/
   Questionable/Illegal','Spam','Violence/Hate/Racism','Weapons')
   end
```

Perform a Policy Trace

Use the Policy Trace function to debug web access issues. When something is allowed and it should not be (or vice versa), use a policy trace to diagnose the issue.

Refer to the following Blue Coat Knowledge Base article for more information:

http://bluecoat.force.com/knowledgebase/articles/Solution/Howtousepolicytracetodebugaccessissues

Check the Event Log

The Event log includes messages relating to Web Security Service status, configuration, and warnings/errors.

- Web Security Service status and configuration changes:
  - Registration/Deregistration
  - Configuration changes (for example, switching from production to ALN
- Web Security Service errors and warnings:
  - Registration/Deregistration
  - State (for example, update errors or entitlement warnings)
  - Feature-related errors and warnings
  - Web Security Service network change-related errors and warnings

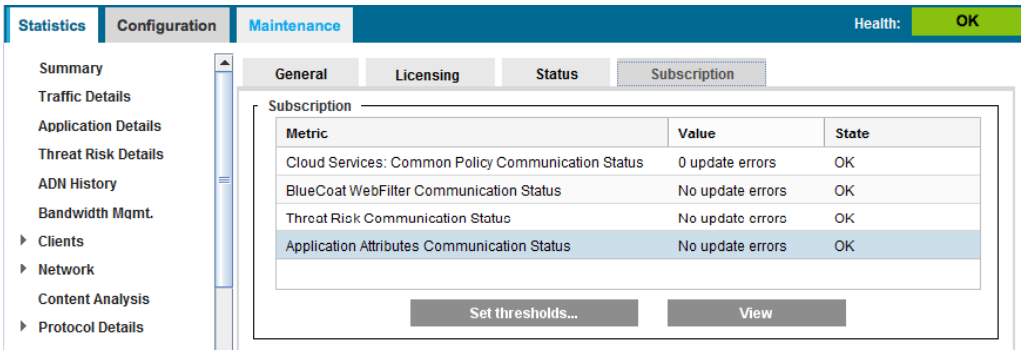
Section D: Monitor the Auto Policy Synchronization Feature

The appliance monitors synchronization errors and the Web Security Service entitlement status. You can accept the default thresholds and notification settings or modify the; see "Change Threshold and Notification Settings" on page 17.

Note: If you do not see Web Security Service health monitoring metrics, refresh your browser. The Management Console might not display them if it was running before you registered the appliance. Similarly, the metrics might be visible after deregistration until you refresh the browser.

Monitoring Auto Policy Synchronization Error Status

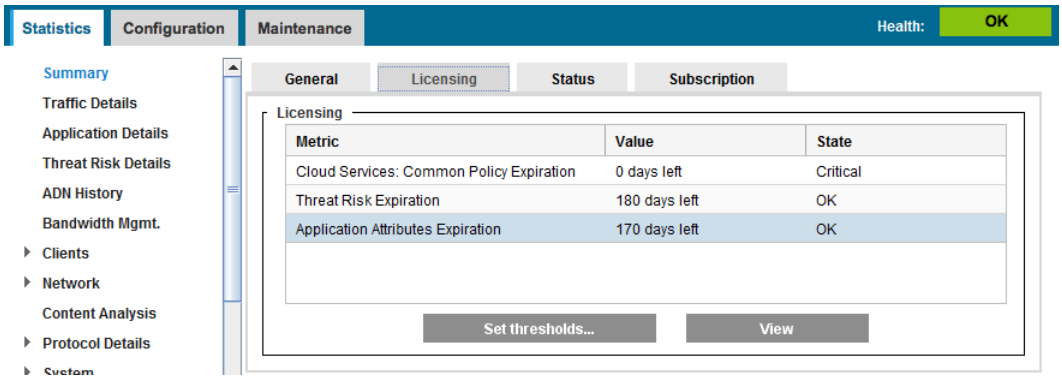
The appliance automatically synchronizes its global policy with the master policy in the Web Security Service. The **Cloud Services: Common Policy Communication Status** metric in the **Statistics > Health Monitoring > Subscription** page displays the status of the update.



By default, if communication with the server fails for more than 24 hours, the appliance health changes to **Warning**. If communication fails for more than 48 hours, the appliance health changes to **Critical**.

Monitor Web Security Service Entitlement

The Web Security Service license is referred to as an *entitlement*. Look for the **Cloud Services: Common Policy Expiration** metric on the **Statistics > Health Monitoring > Licensing** page; it reports the days remaining until the entitlement expires.



By default, a **Warning** is issued (and the appliance health state changes) when there are 30 days or fewer before the entitlement expires. The state changes to **Critical** when the entitlement expires (0 days).

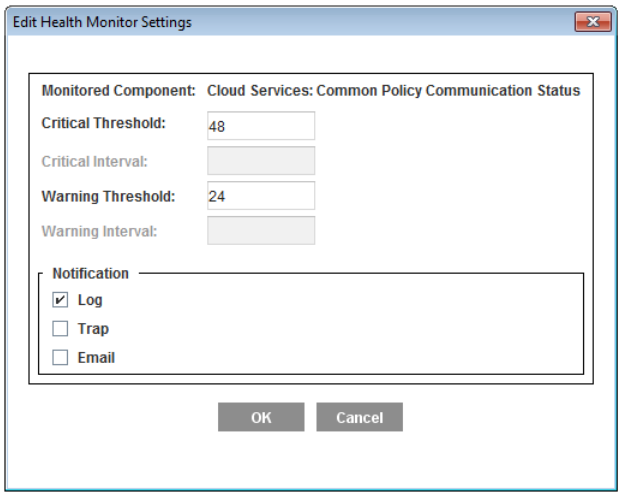
Note: See also "What happens if my common policy entitlement expires?" on page 29.

Change Threshold and Notification Settings

You can modify the default settings for the Web Security Service health monitoring metrics.

Change threshold and notification settings:

1. Select **Maintenance > Health Monitoring.**
2. Click one of the following tabs:
   - **General** for **Cloud Services: Common Policy Communication Status**
   - **Licensing** for **Cloud Services: Common Policy Expiration**
3. Select the metric whose default you want to change.
4. Click **Edit**. The console displays the Edit Health Monitor Settings dialog.



5. Change the **Critical** and **Warning** thresholds as desired.
6. Change the notification properties.
   - **Log** reports state changes in the event log.
   - **Trap** sends an SNMP trap to all configured management stations.
   - **Email** sends an e-mail message to recipients specified in the `event-log mail` command.
7. Click **OK**.
8. Click **Apply**.

Section E: Limitations and Upgrade/Downgrade Considerations

Limitations

Windows and Mac laptop client location awareness is not yet able to put the client into bypass mode when behind a ProxySG appliance with common policy enabled. Such clients continue to connect to Web Security Service and execute policy in the Web Security Service.

Upgrade/Downgrade Considerations

Before downgrading/upgrading SGOS, consider the following:

- SGOS versions prior to 6.4.x do not support the Auto Policy Synchronization feature; however, the following Web Security Service settings are restored if you subsequently upgrade to SGOS 6.4 or later (and have not restored the factory defaults):
  - Registration state (registered/unregistered)
  - Common policy subscription state (enabled/disabled)
  - Web Security Service network (production/ALN)
- SGOS versions 6.4.x through 6.6.x support Auto Policy Synchronization, but the **Configuration > Cloud Configuration** tabs do not exist in those versions; thus, you configure the feature in the CLI only. Refer to Appendix A: "Auto Policy Synchronization Command Reference" on page 23 for an overview of the CLI commands.

Appendix A: Auto Policy Synchronization Command Reference

Use the following commands to configure and manage auto policy synchronization as well as health monitoring alerts and notifications for the feature:

- "#(config) cloud-service"
- "#(config) alert threshold cloud-common-policy"
- "#(config) alert notification cloud-common-policy"

These commands are described in the following sections.

#(config) cloud-service

Use the `cloud-service` commands to configure options relating to the Web Security Service and Advanced Lab Network (ALN). The Web Security Service enables all subscribed devices to share the same common policy, whether on-premises and off-premises. The policy can also be modified on the appliance to conform to local conditions. In this way, you can create general policies that apply to all locations while overriding rules that conflict with local requirements. To use this service, you must first obtain a Web Security Service account (contact your Blue Coat sales representative).

The ALN provides a Web Security Service testing environment. It includes all current functionality plus yet-to-be released new features. Use the ALN to preview and test these new features and provide feedback to Blue Coat. To use the ALN, contact your Blue Coat sales representative.

Syntax

`#(config) cloud-service`

This changes the prompt to:

`#(config cloud-service)`

To display the ALN CLI options, you must use the `reveal-advanced all` command at the `enable` or `config` prompt:

`#(config) reveal-advanced all`

Subcommands

`#(config cloud-service) common-policy {disable | enable}`

Enables or disables subscription to the policy installed on Web Security Service. To use this service, BCWF must be enabled and the appliance must be registered with the Web Security Service. Enabling common policy enables all subscribed devices to share the same policy configuration, whether on-premises and off-premises. The policy synchronizes with the master file every 15 minutes from last boot time. This interval cannot be changed but you can force an immediate update.

`#(config cloud-service)` **`deregister`** [**`force`**]

Removes the appliance from Web Security Service. The `force` option forces deregistration even if there are errors (the appliance removes all cloud-provisioned policy and returns the system to the pre-registration state).

`#(config cloud-service)` **`exit`**

Returns to the (config) submode.

`#(config cloud-service)` **`register location-name`** *`cloud-service-username`* [*`password`*]

Registers the appliance with Web Security Service. Before registering the appliance, you must have obtained a Web Security Service account.

`#(config cloud-service)` **`update-now`** [**`force`**]

Synchronizes the installed common policy with the master file in the cloud. You can use this command to re-download the common policy even if the ProxySG appliance appliance has the latest copy of policy as this may be useful when troubleshooting.

`#(config cloud-service)` **`cloud-network`** {**`advanced-labs`** | **`production`**}

Selects the Web Security Service to use, the ALN or production. By default the appliance will always use the production portal. To display this subcommand, you must enter the `reveal-advanced all` command from the config or enable prompt.

Note: You must have an ALN account to use the Advanced Labs Network. To obtain an account, contact your Blue Coat sales representative.

`#(config cloud-service)` **`view`**

View Web Security Service status for the appliance.

Example

```
#(config) register chicago2 admin@example.com Admin
  ok
#(config) common-policy enable
  ok
#(config) view
Location:                           chicago2
Last successful update time:        2012-07-11 14:42:04-07:00PDT
Last attempted update time:         2012-07-12 08:03:38-07:00PDT
Failed update attempts:             0
Entitlements:
  Common Policy:                    enabled, expires on 2014-02-28
```

#(config) alert threshold cloud-common-policy

Sets alert threshold properties for Web Security Service common policy entitlement and update errors. All settings revert to defaults if the appliance is deregistered from Web Security Service.

Syntax

```
#(config) alert threshold cloud-common-policy {subcommands}
```

Subcommands

```
#(config) alert threshold cloud-common-policy {entitlement {warn-threshold | crit-threshold} update-errors {warn-threshold | warn-interval | crit-threshold}}
```

#(config) alert notification cloud-common-policy

Sets the alert notification properties for Web Security Service common policy and related synchronization update errors. Set the e-mail properties using the `event-log mail` command. All settings revert to defaults if the appliance is deregistered from Web Security Service.

Syntax

```
#(config) alert notification cloud-common-policy {subcommands}
```

Subcommands

```
#(config) alert notification cloud-common-policy {entitlement {email | log | trap | none} | update-errors {email | log | trap | none}}
```

Appendix B: Auto Policy Synchronization FAQ

Topics in this section:

How do I deregister the appliance?

Method 1 - To deregister the appliance from Web Security Service:

1. In the Management Console, select **Configuration > Cloud Configuration > Cloud Registration**.

   The browser displays the Cloud Registration tab.

2. Click **De-register This Device**.

   If deregistration is successful, the console displays the message, "This device is not registered with portal.threatpulse.com".

   If you encounter connection errors while trying to deregister, try the CLI command:

   ```
   #(config cloud-service) deregister force
   ```

Method 2 - To deregister the appliance from within the Web Security Service portal:

1. Log in to the Web Security Service portal.
2. If you are not already in Service mode, select **Service**.
3. Select **Service > Network > Locations**.
4. Select the location and click **Edit**. The browser displays the Location dialog.
5. Select the appliance, right click, and select **Deregister**.

How do I move a registered appliance to another location?

Do one of the following:

- In the Management Console, deregister the appliance (see "How do I deregister the appliance?") and register it again (see "Register the Appliance with Your Web Security Service Account" on page 9). The previous location is automatically populated; when you register the appliance again, specify the new location.
- Issue the `#(config cloud-service) register` command again, specifying the new location. See the following example:

```
#(config cloud-service) view
Cloud Service status:
Location:                              sunnyvale1
Last successful update time:           2012-08-01 13:38:29-07:00PDT
Last attempted update time:            2012-08-01 13:38:29-07:00PDT
Failed update attempts:                0

Entitlements:
Common Policy:                       enabled, expires on 2014-02-28
Last modified time:                2012-07-13 12:37:57-07:00PDT

#(config cloud-service) register santa_clara top_admin@example.com
admin
   ok
```

This operation deregisters the appliance from the `sunnyvale` location and registers in the `santa clara` location.

How do I switch from the ALN to the production network?

Issue the following CLI commands:

```
# en
   Enable Password: password
# reveal-advanced all
# conf t
#(config)cloud-service
#(config cloud-service) cloud-network production
```

Why can't I see all of the cloud-service commands?

Issue the `reveal-advanced all` command from the `enable` or `config` prompt:

```
# en
   Enable Password: password
# reveal-advanced all
# conf t
#(config)cloud-service
#(config cloud-service)
```

What happens if my common policy entitlement expires?

If the common policy entitlement expires:

- The appliance health state changes to **Critical**.
- The common policy no longer synchronizes with Web Security Service.
- The last version of common policy downloaded before the entitlement expired is still in effect on the ProxySG appliance.

If you subsequently renew the license by purchasing a new subscription, the ProxySG appliance automatically updates the license. The appliance downloads the latest common policy at the next 15-minute update interval or if you click **Update Now** (**Configuration > Cloud Configuration > Cloud Registration**) to force an immediate update. When the license status is valid again, the appliance's health monitoring state changes to **OK**.

Can I use the VPM to create local policy?

You can use either VPM or CPL to create local policy.

Why are some Web Security Service portal options missing?

If the current account is provisioned for Universal Policy, the following screens are hidden when the portal is in **Solutions** mode:

- **Overview > Object Library**
- **Content Filtering > Policy**
- **Threat Protection > Policy**
- **Search Controls > Policy**