



## Executive Summary

As the leader in Wide Area Application Delivery, Blue Coat products accelerate and secure applications within your WAN and across the Internet. Blue Coat provides a robust and flexible solution that controls users and network resources, protects against Web-based threats, and accelerates the broadest range of WAN-based applications. Whether deployed on either end of a WAN, at Internet access points, or in front of business-critical services, Blue Coat ProxySG appliances provide control points that stop the bad and accelerate the good. To effectively meet the requirements of today's enterprise, an acceleration deployment that grows with the organization is required. A critical component of that evolution is a comprehensive management solution that allows administrators to effectively configure, manage, and monitor the solution.

## Why is Comprehensive Management necessary?

Network device management and monitoring are critical components in ensuring that service level agreements (SLAs) associated with fault tolerance and availability of key applications, systems, and network resources are met. With the expansion of enterprise networks, it is necessary to have some comprehensive and centralized method of configuring, managing, and monitoring network devices. Whether appliance deployment is due to the addition of a new remote office to the existing solution, or is an entirely new implementation global in scope, deployment and management of large numbers of network devices is a challenging task for administrators. For example, it is not uncommon for tens or even hundreds of appliances to be deployed worldwide, with administrators responsible for remotely configuring and managing them. Configuring and managing a few appliances, distributed or otherwise, can consume significant time and resources; imagine configuring fifty or even two hundred appliances individually. To effectively configure and manage large numbers of appliances centralized management is required. Centralized management enables administrators to easily perform appliance tasks that are typically time consuming and costly, regardless of appliance location.

After devices have been successfully deployed, part of the ongoing management of those devices is monitoring them. While an administrator with only a few appliances to monitor could easily verify device status by manually viewing health statistics, there is no substitute for tools that proactively provide critical status information. Even with only one appliance deployed, administrators will need to be notified when the appliance is utilizing resources outside of normal operation ranges and/or is approaching the resource capacity limits of the system so that appropriate corrective action can be taken. Today, network administrators can typically monitor the status of all devices in the network from one interface using software such as HP OpenView. For more detailed and comprehensive monitoring, however, appliance-specific solutions are desirable.

Another concern facing administrators who manage large numbers of appliances is how to interpret log information from numerous appliances. The importance of log analysis varies across different functional roles within the organization. For some, logs play a crucial role in the functioning of the business, such as being used to bill customers or for confirming regulatory compliance. For others, logs are used for troubleshooting and systems management purposes. Regardless of the business application of the log data, aggregating and obtaining meaningful information from a large set of log files can be impossible without tools designed specifically for that purpose.



## What Tools are Available to Provide Appliance Management?

### Blue Coat Director

#### Comprehensive Configuration/Monitoring/Health/Management

For configuration, day-to-day management, and monitoring of large numbers of appliances, Blue Coat offers Blue Coat Director, a management appliance designed to reduce management cost and complexity by providing centralized management of distributed and remote Blue Coat appliances. While having a central management device is clearly an advantage to individually configuring and managing a number of appliances, Blue Coat Director further simplifies appliance management by allowing administrators to take advantage of features such as configuration management, job scheduling, and automatic backups, while also providing advanced monitoring capabilities.

### Blue Coat ProxySG Appliances

#### Network Analysis

With Blue Coat ProxySG appliances typically deployed in the direct path of network traffic, analysis of network traffic can be done directly from the appliance. Originally designed to assist in making decisions about which traffic to accelerate, the ProxySG has become a popular tool for determining what exactly is on the wire without the need for external, third party tools. The optimized OS and network transparency deliver reliable, on-demand network assessment and enables the administrator to fine-tune configuration and policy management.

### Blue Coat Reporter

#### Reporting

Analysis of Blue Coat ProxySG logs can be easily achieved with Blue Coat Reporter, a software tool that provides comprehensive, identity-based reporting on Web communications, enabling enterprises to evaluate user compliance, validate Web policy enforcement, and manage network resources more effectively. Blue Coat Reporter provides breadth and visibility of Web-based user activities on your network, providing reports for all of Blue Coat's extensive logs to pinpoint and capture policy-defined activities by users.

## How does Blue Coat Director work?

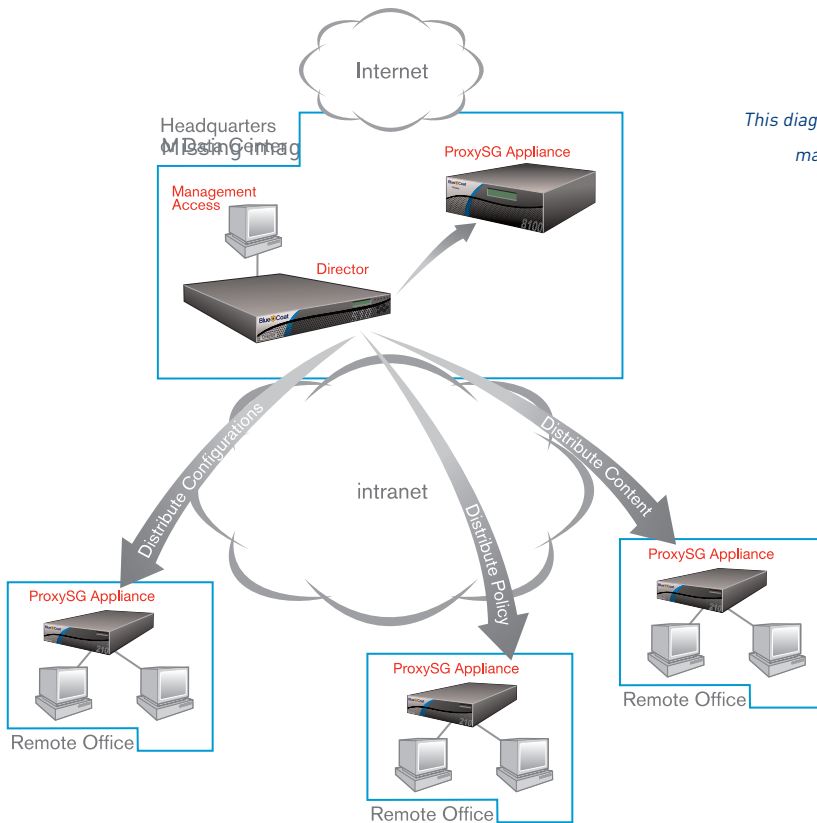
Blue Coat Director performs many functions crucial to comprehensive management which include an easy way to configure, manage, and monitor a large number of ProxySG appliances. Similar to ProxySG appliances, the administrator accesses the console of the Director appliance via an intuitive, user-friendly interface. Within the Director console, configuration management and monitoring functionality for all managed ProxySG appliances is available to the authorized administrator. A summary of some of these features is provided below.

### Comprehensive Configuration and Management

While multiple configuration features are available in Director, most configurations are accomplished using the Director features known as profiles and overlays. Profiles are modified configuration files used to configure ProxySG appliances. Instead of containing the entire appliance configuration, profiles do not include some appliance-specific information such as the IP address, DNS, and interface information. This allows the same profile to be used for multiple ProxySG appliances, reducing the time required to configure a number of appliances and also minimizing the chance for configuration error. For appliance-specific configuration options, overlays can be used. An overlay contains individual configuration options and are useful for configuring a particular appliance which may have a unique configuration setting, or to make a simple change that needs to be applied to a subset of appliances (such as modifying the HTTP freshness setting across all appliances in the network).



To push configuration changes to target ProxySG appliances, Director issues CLI commands to the target ProxySG over an SSH secured session.



*This diagram demonstrates how Blue Coat Director manages multiple ProxySG appliances.*

## Comprehensive Health Monitoring

Blue Coat Director provides a centralized system for monitoring appliances that is far superior to the standard SNMP monitoring typically employed in enterprise networks. From the monitoring pane in Director, administrators can view the health status of all ProxySG appliances managed by Director, individually or by group. Monitoring is accomplished by regular CLI-based polling of the ProxySG appliances managed by Director and problems are proactively reported by Director via the issuing of SNMP traps (or notifications) to the local SNMP management station. By performing regular CLI-based polling, Director is able to not only identify problems, but confirm that a device is active and healthy. If a problem is identified as a result of health status polling, Director sends a trap to the SNMP management station. This implementation is more desirable than individual appliances sending traps to the SNMP management station because traps coming from appliances across the WAN have a higher probability of becoming lost than those sent between the SNMP management station and Director (which typically reside in the same network). In addition, because Director determines appliance health via polling, even if there is a network failure between Director and the ProxySG, it will be identified by Director.

## How do ProxySG Appliances Provide Network Analysis?

ProxySG appliances have the advantage of often being deployed in the direct path of network traffic. By analyzing all of the traffic passing through the network, ProxySG appliances can display network traffic information in the appliance Management Console. This information can be used for purely informational purposes, or can be used to make management decisions regarding which protocols or applications can benefit from acceleration, and which should be blocked based on policy.



## How does Blue Coat Reporter work?

Blue Coat Reporter is a software tool designed to analyze logs from ProxySG appliances. After installing the Reporter software, the administrator can create custom reports based on ProxySG log files, or use any of the 150+ predefined reports, all from one user-friendly interface. For Reporter to process log files, it must have access to them. This is accomplished either by importing the logs or, for real-time reporting, logs can be continuously uploaded from the ProxySG appliance(s). Report generation can be initiated manually from the interface, or reports can be scheduled to run at specific intervals. To share reporting information, administrators can save and export reports, or Reporter can be configured to email reports to specific recipients as well.

## Blue Coat Difference

### Complete End-to-End Comprehensive Solution

Together with ProxySG appliances, Blue Coat Director and Reporter provide an end-to-end solution for complete network security and acceleration – flexible deployment, centralized management, proactive monitoring, and detailed reporting.

### CLI-Based Polling

While trap-based polling is a common appliance monitoring method, it only allows problems to be reported as they occur, and requires that traps reach the SNMP management station. Blue Coat Director monitors ProxySG appliances not only by issuing traps, but by proactively polling for health status at regular intervals. Relying solely on traps can be ineffective because it is during network problems (likely causing a problem with the functioning of the appliance and resulting in a trap) that traps are least likely to reach the management station. Because Director determines appliance health via polling, even if there is a network failure between Director and the ProxySG, it will be identified by Director.

### Differential Polling

Blue Coat Director implements a polling technique that prompts ProxySG appliances to indicate if their health status has not changed since the most recent poll. This allows Director to verify the health status of an appliance without requiring the current status of every possible health variable available. This method of polling provides the most efficient method of monitoring as it does not unnecessarily consume network resources and bandwidth, a possible concern when large numbers of appliances are deployed.

### Customized, Appliance-Specific Reports

Blue Coat Reporter has over 150+ customized, pre-defined reports. Because Blue Coat Reporter is designed specifically for Blue Coat ProxySG appliances, minimal configuration is required to deliver the specific reporting information that your organization requires.