Enable Log Forwarding

After you create the Server Profiles that define where to send your logs (see Define Remote Logging Destinations), you must enable log forwarding. For each log type, you can specify whether to forward it to Syslog, email, SNMP trap receiver, and/or Panorama.

Before you can forward log files to a Panorama Manager or a Panorama Log Collector, the firewall must be configured as a managed device. You can then enable log forwarding to Panorama for each type of log. For logs forwarded to Panorama, support for centralized log forwarding to an external syslog server is available.

The way you enable forwarding depends on the log type:

- **Traffic Logs**—You enable forwarding of Traffic logs by creating a Log Forwarding Profile (**Objects > Log Forwarding**) and adding it to the security policies you want to trigger the log forwarding. Only traffic that matches a specific rule within the security policy will be logged and forwarded. For details on setting up a log forwarding profile, see Log Forwarding Profiles.
- **Threat Logs**—You enable forwarding of Threat logs by creating a Log Forwarding Profile (**Objects > Log Forwarding**) that specifies which severity levels you want to forward and then adding it to the security policies for which you want to trigger the log forwarding. A Threat log entry will only be created (and therefore forwarded) if the associated traffic matches a Security Profile (Antivirus, Anti-spyware, Vulnerability, URL Filtering, File Blocking, Data Filtering, or DoS Protection). For details on setting up a log forwarding profile, see Log Forwarding Profiles. The following table summarizes the threat severity levels:

Severity	Description
Critical	Serious threats, such as those that affect default installations of widely deployed software, result in root compromise of servers, and the exploit code is widely available to attackers. The attacker usually does not need any special authentication credentials or knowledge about the individual victims and the target does not need to be manipulated into performing any special functions.
High	Threats that have the ability to become critical but have mitigating factors; for example, they may be difficult to exploit, do not result in elevated privileges, or do not have a large victim pool.
Medium	Minor threats in which impact is minimized, such as DoS attacks that do not compromise the target or exploits that require an attacker to reside on the same LAN as the victim, affect only non-standard configurations or obscure applications, or provide very limited access. In addition, WildFire Submissions log entries with a malware verdict are logged as Medium.
Low	Warning-level threats that have very little impact on an organization's infrastructure. They usually require local or physical system access and may often result in victim privacy or DoS issues and information leakage. Data Filtering profile matches are logged as Low.
Informational	Suspicious events that do not pose an immediate threat, but that are reported to call attention to deeper problems that could possibly exist. URL Filtering log entries and WildFire Submissions log entries with a benign verdict are logged as Informational.

- **Config Logs**—You enable forwarding of Config logs by specifying a Server Profile in the log settings configuration. (**Device > Log Settings > Config Logs**).
- **System Logs**—You enable forwarding of System logs by specifying a Server Profile in the log settings configuration. (**Device > Log Settings > System Logs**). You must select a Server Profile for each severity level you want to forward. For a partial list of system log messages and their corresponding severity levels, refer to the System Log Reference. The following table summarizes the system log severity levels:

Severity	Description
Critical	Hardware failures, including HA failover and link failures.
High	Serious issues, including dropped connections with external devices, such as LDAP and RADIUS servers.
Medium	Mid-level notifications, such as antivirus package upgrades.
Low	Minor severity notifications, such as user password changes.
Informational	Log in/log off, administrator name or password change, any configuration change, and all other events not covered by the other severity levels.

Log Forwarding Profiles

Log forwarding profiles allow you to forward traffic and threat logs to Panorama or an external system. A log forwarding profile can be added to a security zone to forward zone protection logs or to a security policy to forward logs for traffic that matches that policy. You can also configure a default log forwarding profile—the settings in the default profile will be used as the default log forwarding settings for new security zones and new security policies. This allows you to consistently include your organization's preferred log forwarding settings in new policies and zones automatically, without administrators having to manually add them each time.

The following sections show how to create a log forwarding profile and how to enable a profile to be used as the default log forwarding settings for new security policies or security zones:

▲ Create a Log Forwarding Profile

▲ Set Up or Override a Default Log Forwarding Profile

Create a Log Forwarding Profile

Create a log forwarding profile that can be added to security policies and security zones, in order to forward traffic and threat logs to Panorama or an external system. Forwarded logs can be sent as SNMP traps, syslog messages, or email notifications.