

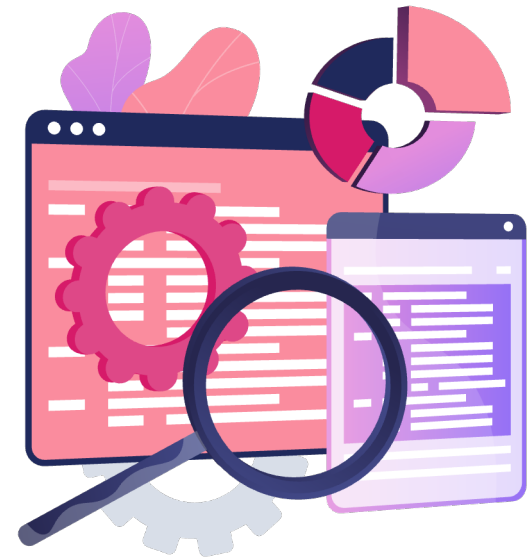
CHAPTER 10

MONITORING OPERATIONS

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Review the tools used to view logs and monitor devices.
- Configure log settings on the Management Server and Security Gateway.
- Use predefined and custom queries to filter log results.
- Monitor devices.

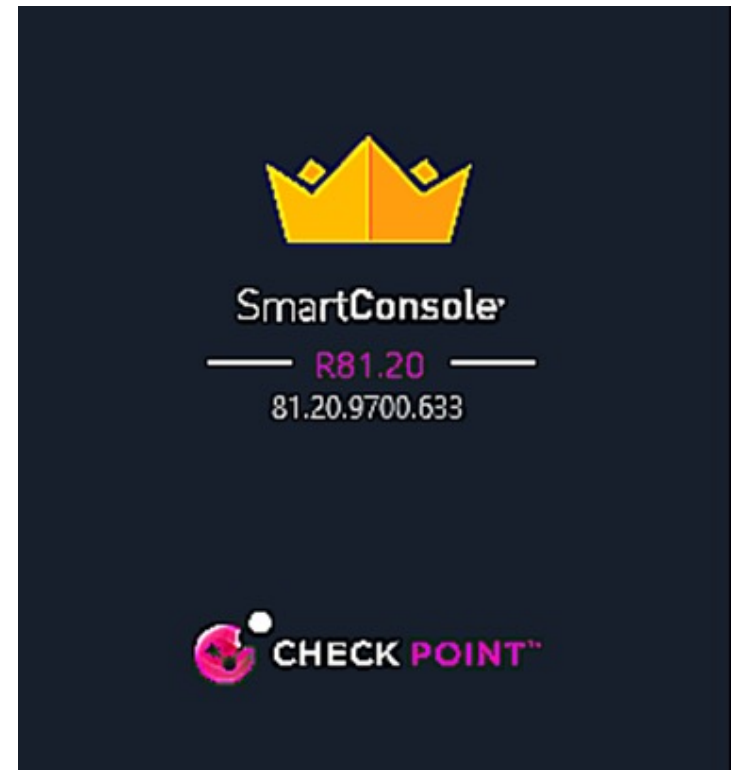


Tools Review

- SmartConsole
- SmartView Monitor
- SmartView

The SmartConsole Tool

- Traffic visibility tools help administrators:
 - Monitor traffic and connections.
 - Analyze log data.
 - Troubleshoot events.
 - Quickly respond to changes in traffic flow patterns or suspicious security activities.



SmartConsole - Logs View

The screenshot shows the SmartConsole interface with the 'Logs' view selected. The table displays security events with columns for Time, Severity, Source, Source Machine, Client Type, Source User, Server Type, Destination, and Attack Name. The interface includes a search bar at the top and a sidebar with navigation options like 'GATEWAYS & SERVERS', 'SECURITY POLICIES', 'LOGS & MONITOR', 'INFINITY SERVICES', and 'MANAGE & SETTINGS'.

Time	B...	A...	T...	Seve...	Con...	Su...	Perf...	Source	Source Machi...	Client Type	Source User...	Server Type	Destination	Attack Name
Today, 9:15:38 AM								192.168.5.7	Walter_Laptop	Chrome	Walter		192.168.72.15	
Today, 9:15:38 AM								192.168.5.7	Walter_Laptop	Chrome	Walter		192.168.61.14	
Today, 9:15:38 AM								192.168.5.18	Skyler_Laptop	Chrome	Skyler		192.168.72.15	
Today, 9:15:38 AM								192.168.5.18	Skyler_Laptop	Chrome	Skyler		192.168.61.14	
Today, 8:18:05 AM								192.168.5.10	Saul_Win	Chrome	Saul		192.168.72.15	
Today, 8:18:05 AM								192.168.5.10	Saul_Win	Chrome	Saul		192.168.61.14	
Today, 8:18:05 AM								192.168.5.18	Jesse_Laptop	Chrome	Jesse		192.168.72.15	
Today, 8:18:05 AM								192.168.5.18	Jesse_Laptop	Chrome	Jesse		192.168.61.14	
Today, 8:18:05 AM								10.1.0.50					10.2.0.27	Adobe Flash Protection Violation
Today, 8:18:05 AM								10.1.0.40					10.2.0.22	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.10					10.2.0.57	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.39					10.2.0.173	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.21					10.2.0.239	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.52					10.2.0.103	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.25					10.2.0.241	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.26					10.2.0.15	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.42					10.2.0.73	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.41					10.2.0.210	Adobe Shockwave Protection Violation
Today, 8:18:05 AM								10.1.0.44					10.2.0.124	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.37					10.2.0.149	Web Server Enforcement Violation
Today, 8:18:05 AM								10.1.0.50					10.2.0.102	Cisco Protection Violation
Today, 8:18:05 AM								10.1.0.36					10.2.0.45	Cisco Protection Violation
Today, 8:18:05 AM								10.1.0.7					10.2.0.189	Web Server Enforcement Violation
Today, 8:18:05 AM								10.1.0.20					10.2.0.112	Windows SMB Protection Violation
Today, 8:18:05 AM								10.1.0.49					10.2.0.155	Application Servers Protection Violation
Today, 8:18:05 AM								10.1.0.35					10.2.0.207	
Today, 8:18:05 AM								10.1.0.44					10.2.0.24	

- Monitor traffic and query for information.
- Custom queries can be easily created using predefined search filters. Search results are very quick.

SmartConsole - Monitor View

The screenshot displays the SmartConsole interface in Monitor View. The main window shows a table of devices with columns for Status, Name, IP, Version, Active Blades, Hardware, CPU Usage, and Recommended Updates. A context menu is open over the first row, with 'Monitor' selected. A secondary window titled 'Device & License Information - BranchOffice' is overlaid, showing detailed information for the selected device.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates
	Cluster	198.51.100.7	R81.20		3000 Appliances	99%	2
	te-Cluster-member-A	17.23.5.1	R81.20				
	te-Cluster-member-B	17.23.5.2	R81.20				
	GW	198.51.100.5	R81.20				
	chGw	192.0.2.100	R81.10				
	rGw	192.16.26.100	R81.20				
		192.0.2.200	R81				
		10.0.168.189	R81.20				
		192.16.26.7	R81.20				
		192.0.22.1	R80.40				
✓	Remote-2-gw	192.0.23.1	R80.40				
✓	Remote-3-gw	192.0.24.1	R80.40				
✓	Remote-4-gw	192.0.25.1	R80.40				
✓	Remote-5-gw	192.0.26.1	R81				
✓	RemoteBranchGw	198.51.100.120	R80.40				
✓	ThreatEmulationDevice	192.0.111.13	R81				

Device & License Information - BranchOffice

Device Status: ✓
License Status: ✓
System Counters: -
System: -
More: -
Traffic: -
Traffic: -

BranchOffice
IP Address: 198.51.100.7
State: Connection with 'BranchOffice' is lost

- Firewall
- Anti-Bot & Anti-Virus
- Zero Phishing
- Application Control
- Threat Emulation
Scanned Files in the Last 7 Days: 0
Malicious Files Detected in the Last 7 Days: 0
Remaining Quota on Cloud: "Wait"
Monthly Quota on Cloud Used: NaN%
- Threat Extraction
- URL Filtering
- IPS
- IPSec VPN

- Logs and events
- Performance
- Regulation compliance

The SmartView Monitor Tool: Monitor View

The screenshot shows the 'All Gateways' view in the SmartView Monitor tool. The table below lists the gateways and their status:

Gateway Name	IP Address	Average CPU	Active Virtual Memory	Disk Free %	Version
OfficeGw	192.16.26.7				
HeadquarterGw	192.16.26.100				
Corporate-GW	198.51.100.5				
HQgw	192.0.2.200				
EuropeBranchGw	192.0.2.100				
BranchOffice	198.51.100.7				
Corporate-Cluster-member-B	17.23.5.3				
Remote-5-gw	192.0.26.1				
mgmt	10.0.60.145	18%	6.63 GB	54	R81.20
Remote-3-gw	192.0.24.1				
Remote-2-gw	192.0.23.1				
ThreatEmulationDevice	192.0.111.13				
Remote-1-gw	192.0.22.1				
Remote-4-gw	192.0.25.1				
Corporate-Cluster-member-A	17.23.5.2				
RemoteBranchGw	198.51.100.120				

The detailed view for 'Corporate-GW' shows the following information:

- IP Address: 198.51.100.5
- State: Connection with 'Corporate-GW' is lost
- Firewall
- Zero Phishing
- Application Control
- Threat Extraction
- IPS
- IPSec VPN
- Anti-Bot & Anti-Virus
- URL Filtering

- Monitor Firewalls, Gateways, and VPNs.
- Not used to view logs.

The SmartView Tool: Log View

The screenshot displays the SmartView Log View interface. On the left, there are statistics for various security features: Blade (Firewall: 56.53%, Threat Emulation: 23.63%, HTTPS Inspection: 19.52%, System Monitor: 0.11%, SmartEvent Client: 0.07%, Threat Extraction: 0.07%, Application Control: 0.04%, URL Filtering: 0.04%), Action (Accept: 99.86%, Detect: 0.14%), Type (Log: 99.19%, Control: 0.81%), Severity (Informational: 100.0%), Confidence Level (N/A: 100.0%), and Protection Type. The main area shows a table of logs with columns for Time, B., A., T., Severity, Confidence Level, Protection Type, Protection Number, and File Name. The logs are filtered for the last 24 hours and show various HTTP Emulation events.

Time	B.	A.	T.	Severity	Confidence L...	Protection Type	Protection Na...	File Name
Feb 8, 2023 2:08:55 PM				Inf...	N/A	HTTP Emu...		seed
Feb 8, 2023 11:31:50 AM				Inf...	N/A	HTTP Emu...		am_delta_patch_1.381.3255.0_e6ae0556cb6b1dab21b8...
Feb 8, 2023 9:36:36 AM				Inf...	N/A	HTTP Emu...		38419047_0882aca7c6c28d9c0b0ee7317f49b6f7a74b1e...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419048_818baa7a7816dce1b1343ef0e1ff6a8cb68bc9...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419049_99bef314ca03271cb35eb06c6ada26475d953...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419050_6f55531a44445b22c0934d0a97d44d4d56a7...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419051_e770ad75a5dd999395784d4644116927533c...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419052_abd423b2a1fa42117aedeb07b6e48b6da121...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419053_9a72d86e3eaa273650f9a4bfd3273e538bb17...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419054_94ede20c50e79b05aa1d1732015479f790828...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419055_523066473c7f9b9f4fee5430918ef28f03a61...
Feb 8, 2023 9:36:30 AM				Inf...	N/A	HTTP Emu...		38419056_ba6f5333236c3417002a75605b2b8353c369...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419058_27c5b7e8ddaf4b1af8bc619c319f7fc91f30eaf...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419059_513b842ae1fc45a5bb140ee1d186e585e941f...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419060_425618d61aae7dd3bd402562e84210e5838a...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419061_05e533ce1525de3a6b14dfb7a30114261a7a3...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419062_001f2ae48360b8d5d54402c515237ebf42283...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38419063_3939fb5b61cb5a20110b6ed42dce09c2e1e1...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38418051_3a5b116c4930040711a209a079e14d676c...
Feb 8, 2023 9:36:29 AM				Inf...	N/A	HTTP Emu...		38418052_7e35e9007b5dce031e99801a11510da8a5...

- Browser-based tool used to access a Log Server to view logs.
- URL is case-sensitive.
- Not used to monitor devices.

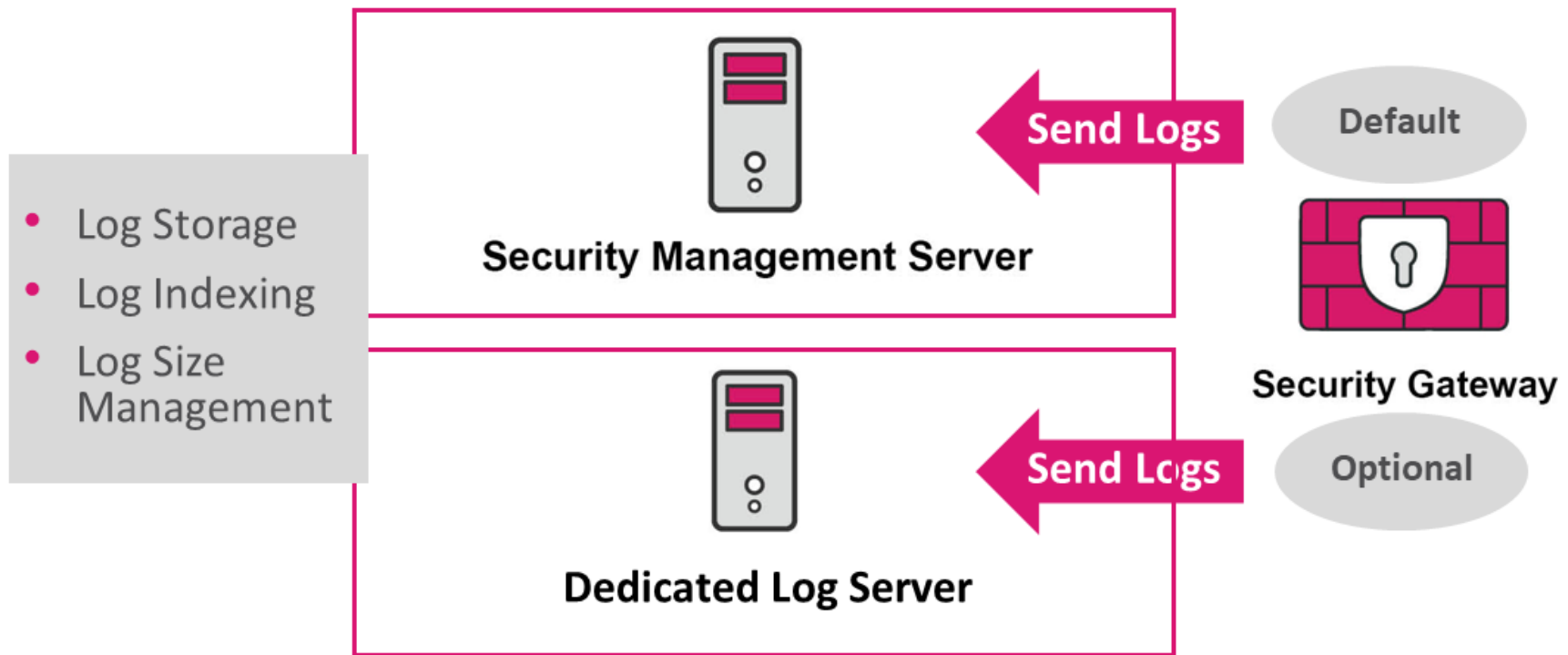
<https://log server IP address/smartview>

Tool Comparison

Tool	View Logs	Monitor Stats	How to Access
SmartConsole	Yes	Yes	Desktop client running on Windows host (SmartConsole Client and Portable SmartConsole) and Web SmartConsole
SmartView Monitor	No	Yes	SmartConsole Logs & Monitor → Tunnel & User Monitoring
SmartView	Yes	No	Web browser to access a Log Server

This chapter focuses on using SmartConsole to view logs and monitor statistics.

Understanding Logging





A dedicated Log Server can be used for organizations that generate a lot of logs.

Logs can be configured to be automatically forwarded to the Security Management Server or dedicated Log Server, according to a schedule.

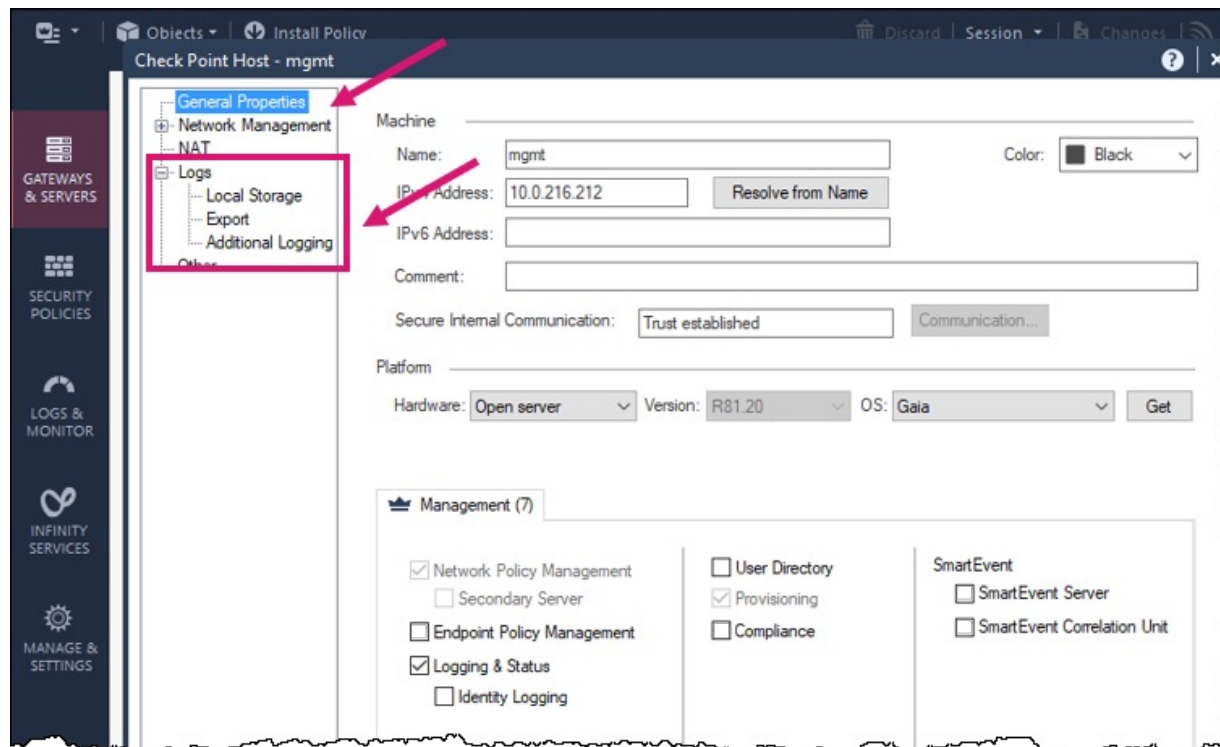
This is discussed in the CCSE course.

Why Collect Logs?



- Research alerts, rejected connections, and failed authentication attempts.
- Analyze traffic patterns.
- Meet compliance requirements.

Log Configuration on the Management Server



Gateways & Servers view:

- General Properties
- Logs

Log Configuration - General Properties

The screenshot shows the 'heck Point Host - mgmt' configuration window. The left sidebar contains a tree view with 'General Properties' selected. The main area is divided into sections: 'Machine' (Name: mgmt, IPv4 Address: 10.0.137.103, IPv6 Address: empty, Comment: empty, Secure Internal Communication: Trust established), 'Platform' (Hardware: Open server, Version: R81.20, OS: Gaia), and 'Management (7)'. The 'Management (7)' section contains several checkboxes: 'Network Policy Management' (checked), 'Secondary Server' (unchecked), 'Endpoint Policy Management' (unchecked), 'Logging & Status' (checked, highlighted with a red arrow), 'Identity Logging' (unchecked), 'User Directory' (unchecked), 'Provisioning' (checked), 'Compliance' (checked), 'SmartEvent' (unchecked), 'SmartEvent Server' (unchecked), and 'SmartEvent Correlation Unit' (unchecked).

- Ensure **Logging & Status** is enabled.
- Enabled by default on the Primary Management Server.
- Must be enabled on a Secondary Server.

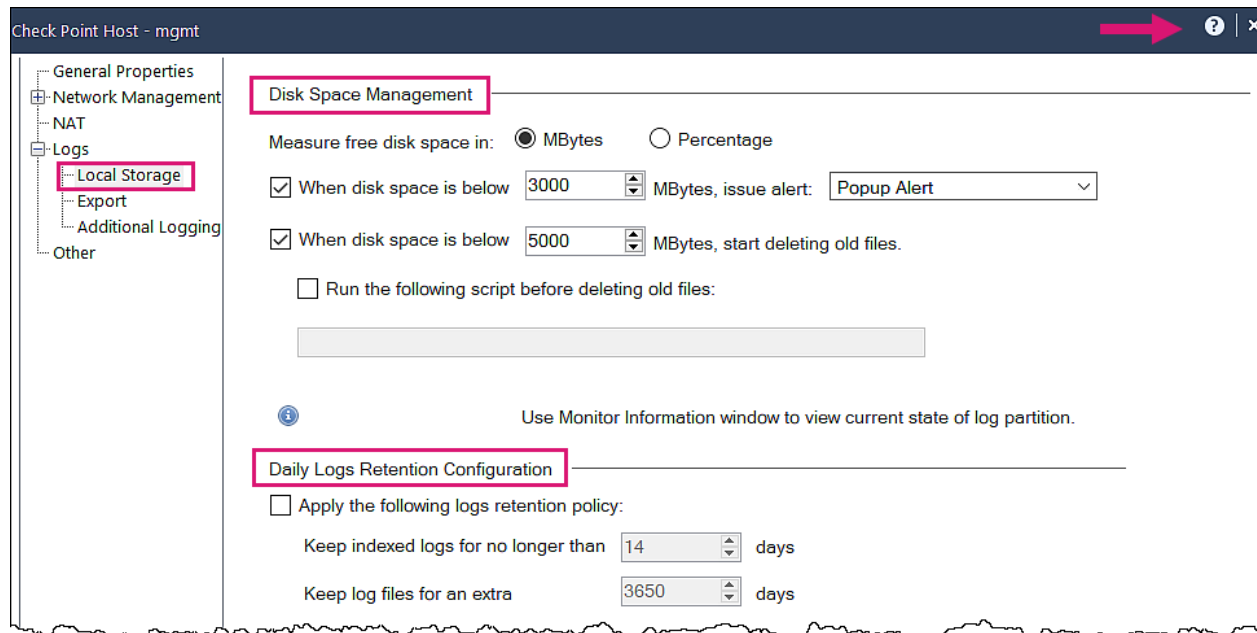
Log Configuration - Enable Log Indexing

The screenshot shows the Check Point management console interface. The left sidebar contains navigation options: GATEWAYS & SERVICES, SECURITY POLICIES, LOGS & MONITOR, INFINITY SERVICES, and MANAGE & SETTINGS. The main window displays the configuration for 'Check Point Host - mgmt'. Under 'General Properties', the 'Enable Log Indexing' checkbox is checked. Below this, an information icon indicates 'The Log Indexing uses more storage to provide fast log queries'. A section titled '14 gateways have configured this machine as their log server' contains a search bar and a 'View...' button. Below this is a table listing 14 gateways.

Gateway	IP Address	Comments	Type
ThreatEmulationDevice	192.0.111.13	Threat Emulation	Send Logs and Alerts
Remote-5-gw	192.0.26.1	ICAP server	Send Logs and Alerts
Remote-4-gw	192.0.25.1	Remote-4-gw	Send Logs and Alerts
Remote-3-gw	192.0.24.1	Remote-3-gw	Send Logs and Alerts
Remote-2-gw	192.0.23.1	Remote-2-gw	Send Logs and Alerts
Remote-1-gw	192.0.22.1	Remote-1-gw	Send Logs and Alerts
OfficeGw	192.16.26.7	OfficeGw	Send Logs and Alerts
HeadquarterGw	192.16.26.100	HeadquarterGw	Send Logs and Alerts
HQgw	192.0.2.200	Main Office gateway	Send Logs and Alerts
EuropeBranchGw	192.0.2.100	Europe Office gateway	Send Logs and Alerts
Corporate-GW	198.51.100.5	First Office gateway	Send Logs and Alerts
Corporate-Cluster	17.23.5.1		Send Logs and Alerts
BranchOffice	198.51.100.7	Second office gateway	Send Logs and Alerts
RemoteBranchGw	198.51.100.120	RemoteBranchGw	Send Logs and Alerts

- Enabled by default.
- Disabling increases the log query time.
- Click **View** to see the Gateways configured to send their logs to this Log Server.

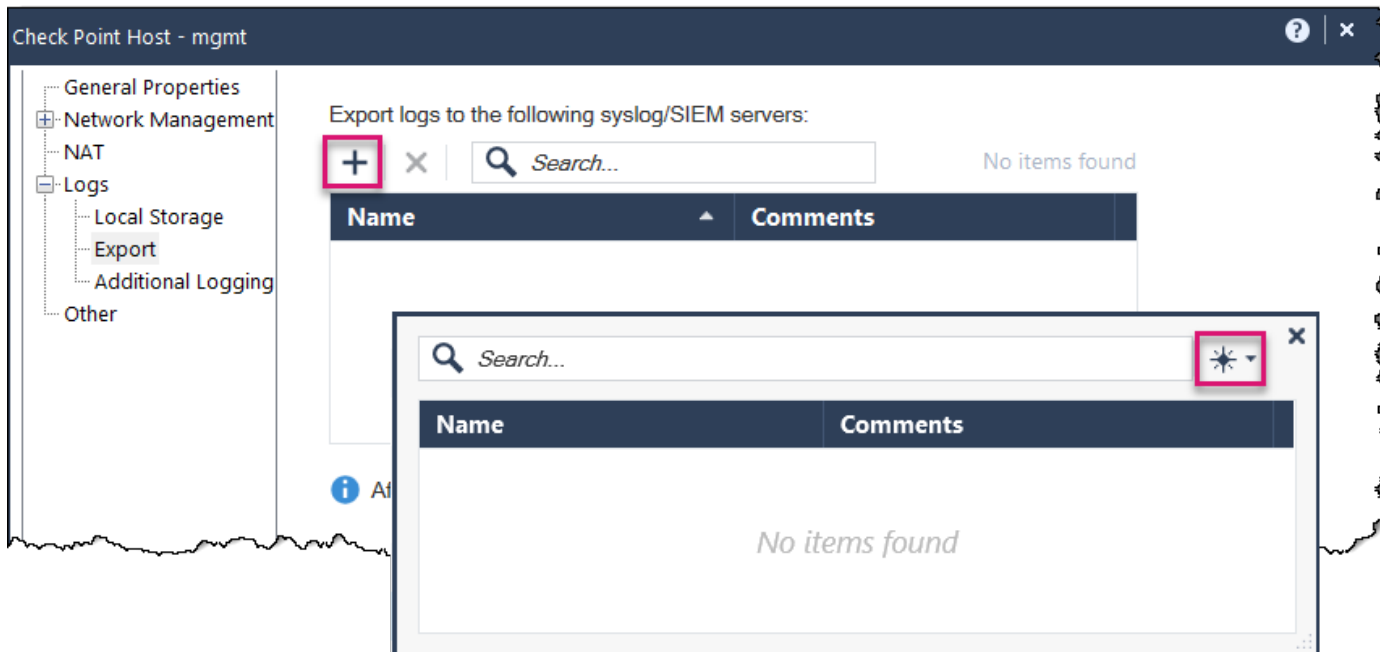
Log Configuration - Local Storage



- Disk Space Management
- Daily Log Retention Configuration

See student guide for explanation of settings.

Log Configuration - Export



- Settings related to the export of logs to a Security Information and Event Management (SIEM) server:
- General, Data Manipulation, and Attachment settings.

After you configure a Log Exporter, you must run Install Database.

Log Configuration - Additional Logging

Check Point Host - mgmt

General Properties
Network Management
NAT
Logs
Local Storage
Export
Additional Logging
Other

Log Forwarding Settings

Forward log files to Log Server: [dropdown]
Log forwarding schedule: [dropdown] [Manage...]

Log Files

Create a new log file when the current file is larger than [1000] MBytes
 Create a new log file on scheduled times [dropdown] [Manage...]

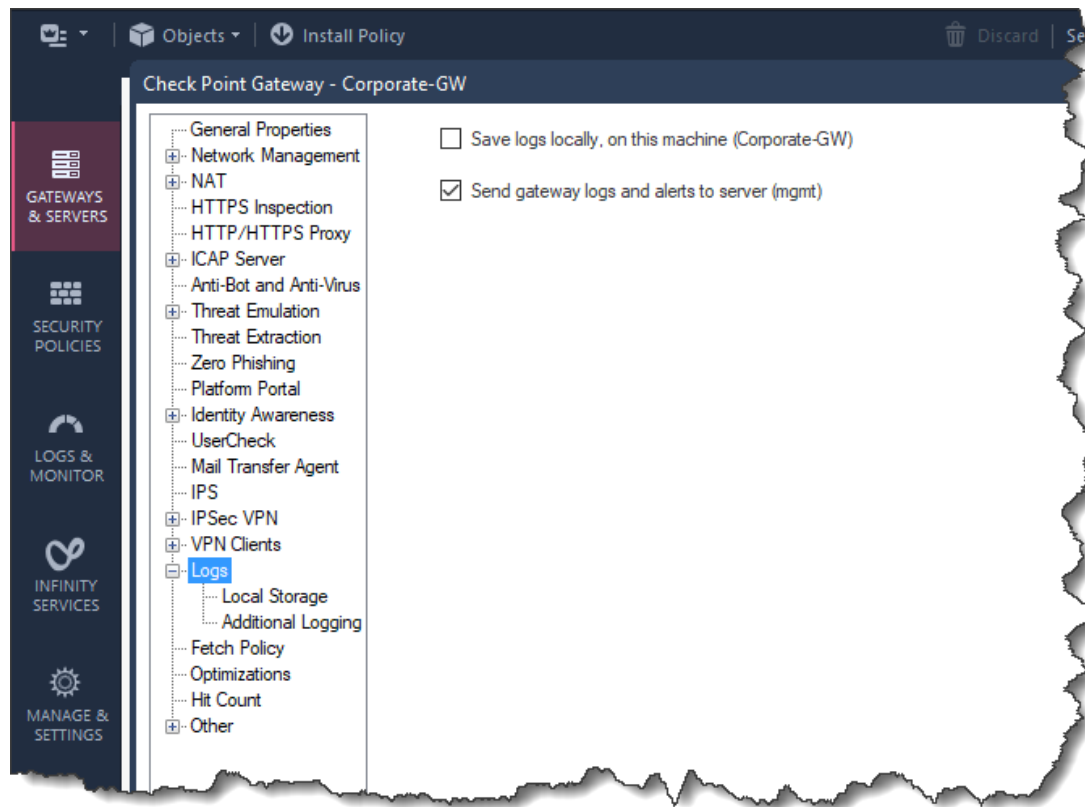
Advanced Settings

When disk space is below [100] MBytes, stop logging.
Update Account Log every [3600] Seconds
 Turn on QoS Logging
 Detect new Citrix ICA application names
 Accept Syslog messages
 SmartEvent Intro Correlation Unit

- Log Forwarding Settings
- Log Files
- Advanced Settings

See student guide for explanation of settings.

Log Configuration on the Security Gateway

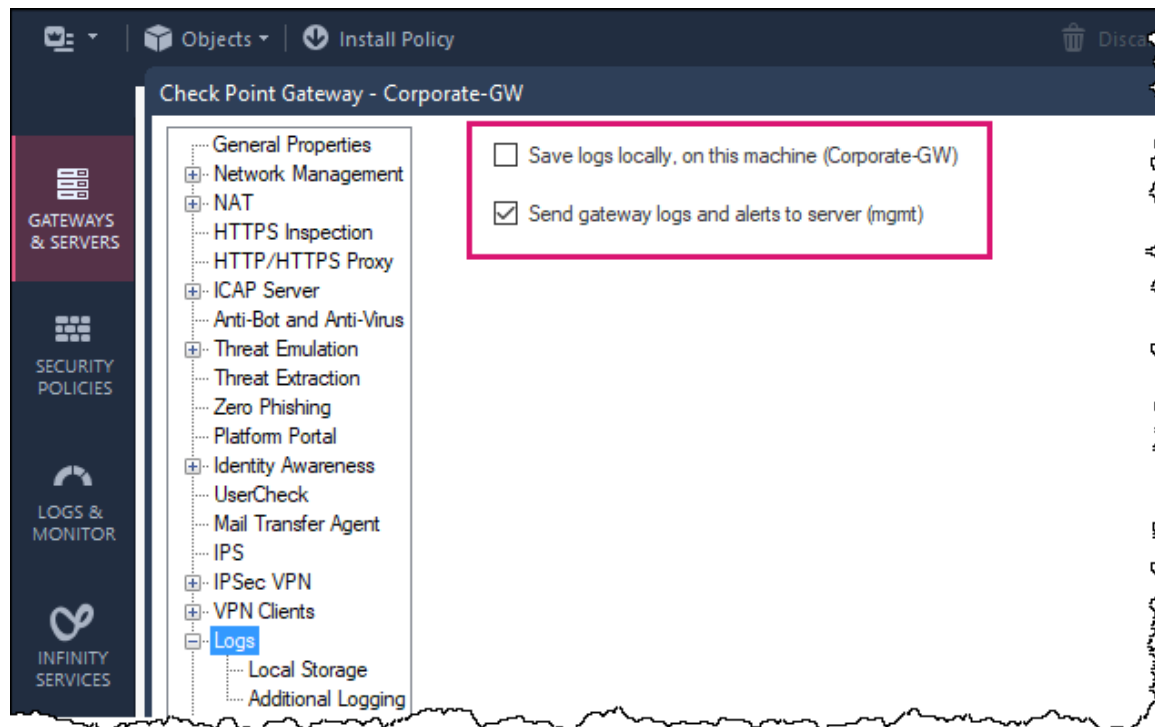


- Similar process as configuring logging on the Security Management Server.

Gateways & Servers view:

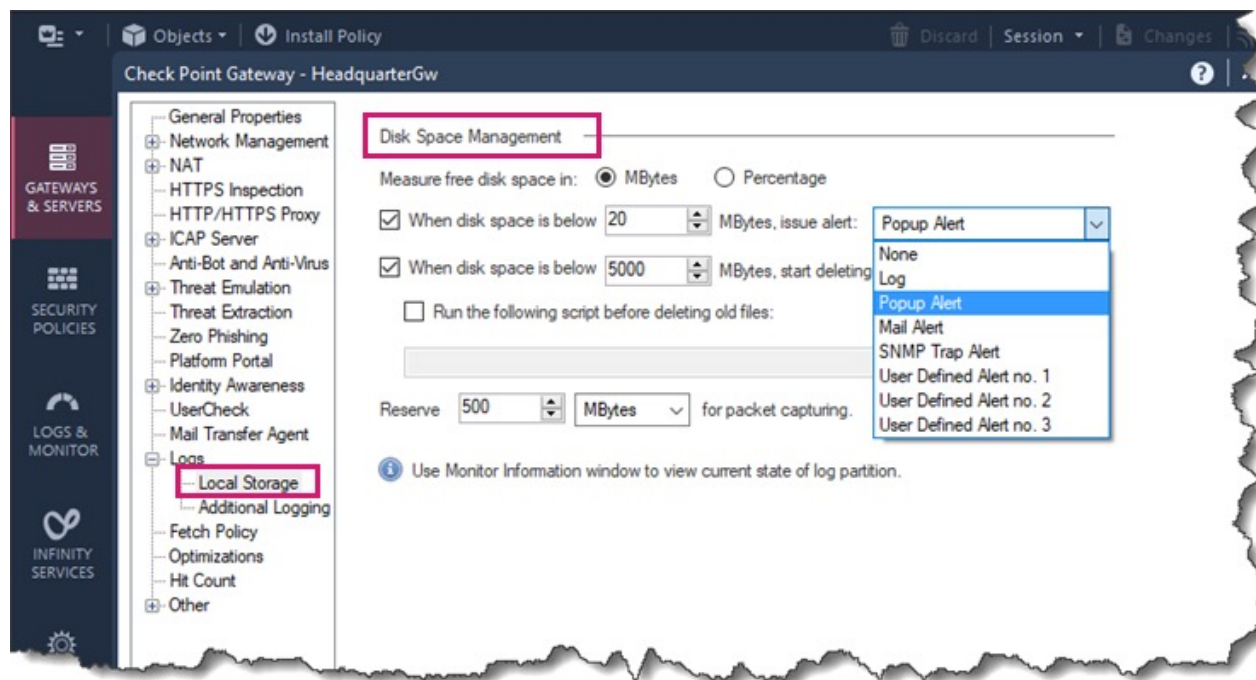
- Logs

Gateway Log Configuration - Logs



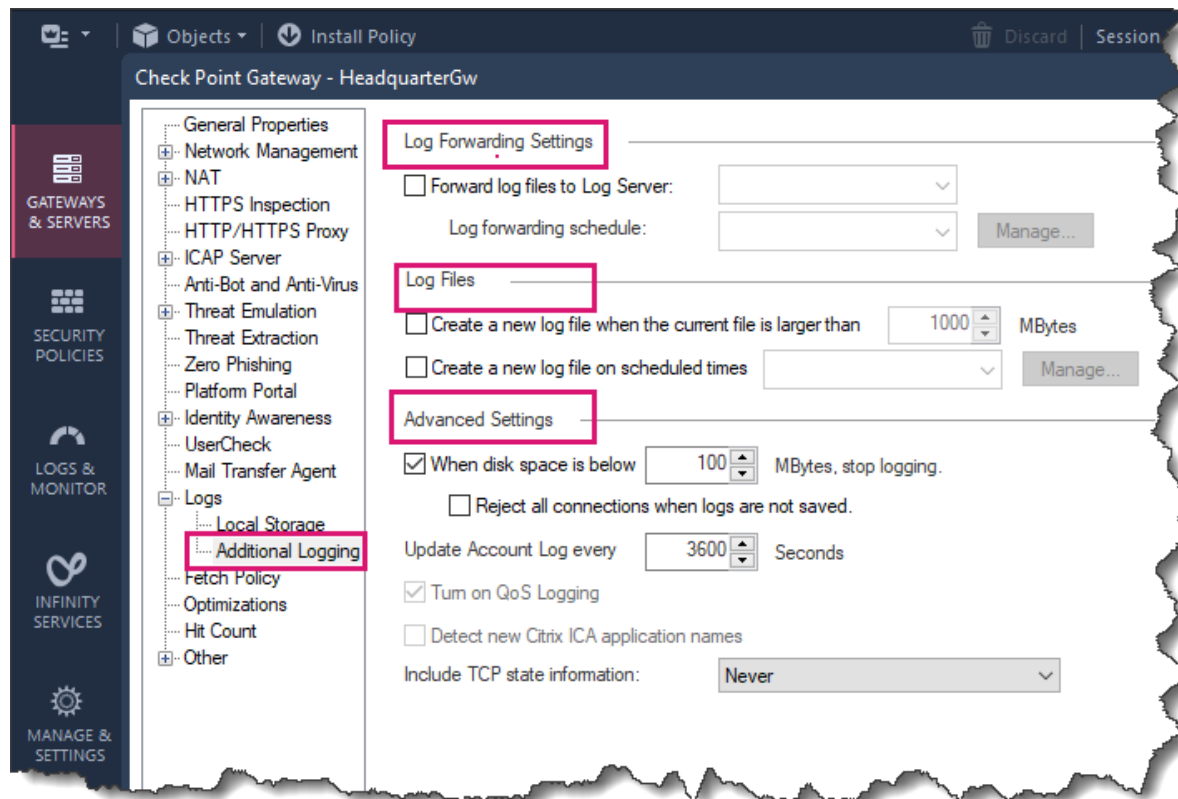
- Save logs locally, on the machine [Gateway]
- Send Gateway logs and alerts to the server [Management Server]

Gateway Log Configuration - Local Storage



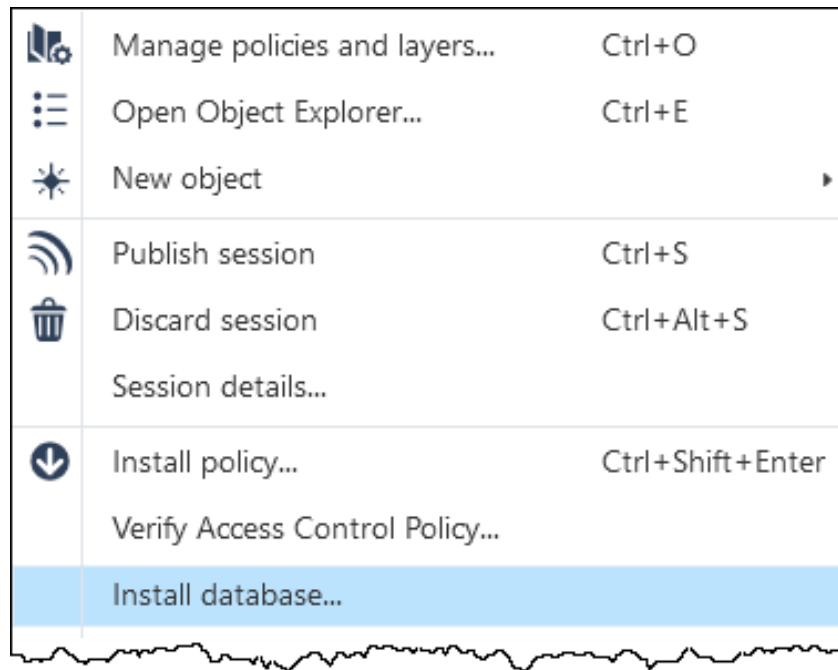
Disk Space Management

Gateway Log Configuration - Additional Logging



- Log Forwarding
- Log Files
- Advanced Settings

Installing the Database



After the log configuration is complete, the next step is to install the database.

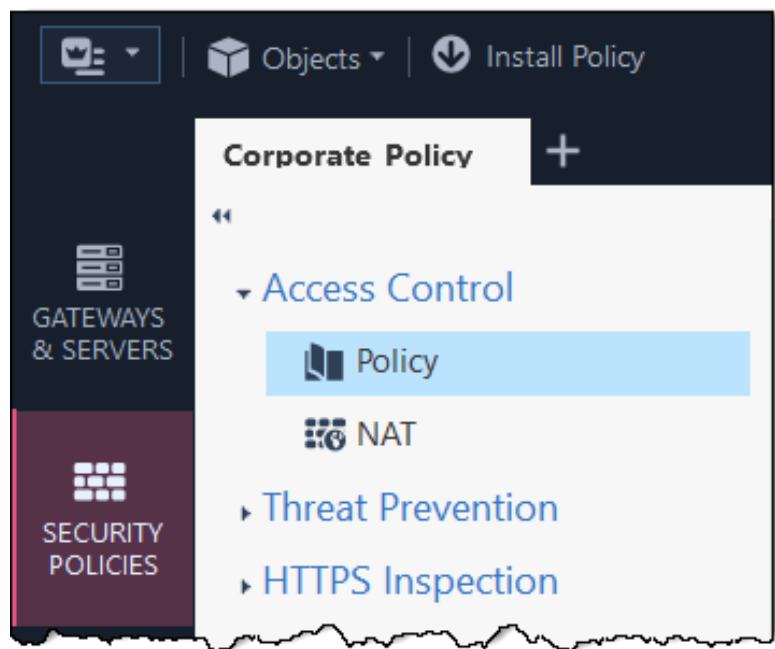
Track Options for Rules (Logs Tab)

- Show the most relevant traffic patterns in the logs.
- Provide an understanding of user behavior.
- Provide data for reports.

For training purposes, most examples use an Access Control Policy.

Logs are useful if they show the traffic patterns in which you are interested.

Configuring Track Options in a Rule

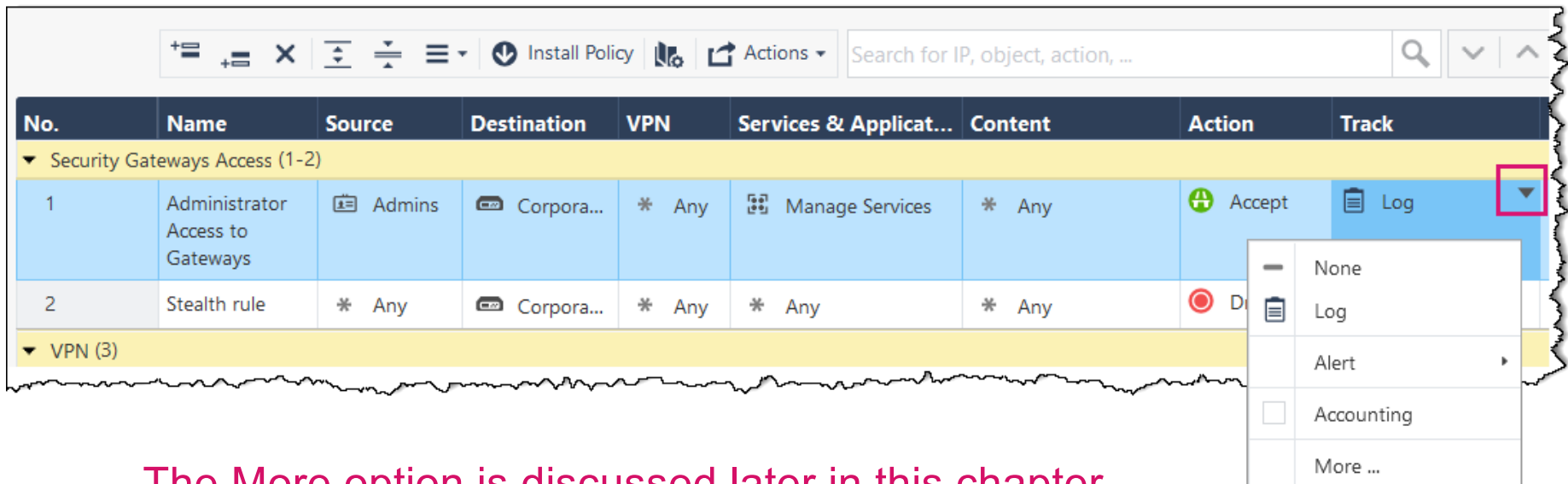


SmartConsole Security Policies view:

- Access Control → Policy

Track Options

- In the Track column, click the down arrow to view tracking options.

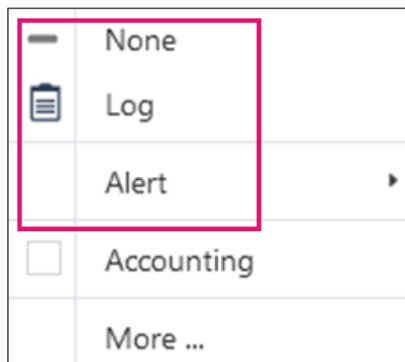


The screenshot shows a configuration interface with a table of rules. The table has columns: No., Name, Source, Destination, VPN, Services & Applicat..., Content, Action, and Track. The first rule is 'Administrator Access to Gateways' with Action 'Accept' and Track 'Log'. A dropdown menu is open in the Track column, showing options: None, Log, Alert, Accounting, and More ... The 'More ...' option is highlighted with a red box.

No.	Name	Source	Destination	VPN	Services & Applicat...	Content	Action	Track
▼ Security Gateways Access (1-2)								
1	Administrator Access to Gateways	Admins	Corpora...	* Any	Manage Services	* Any	Accept	Log
2	Stealth rule	* Any	Corpora...	* Any	* Any	* Any	D	
▼ VPN (3)								

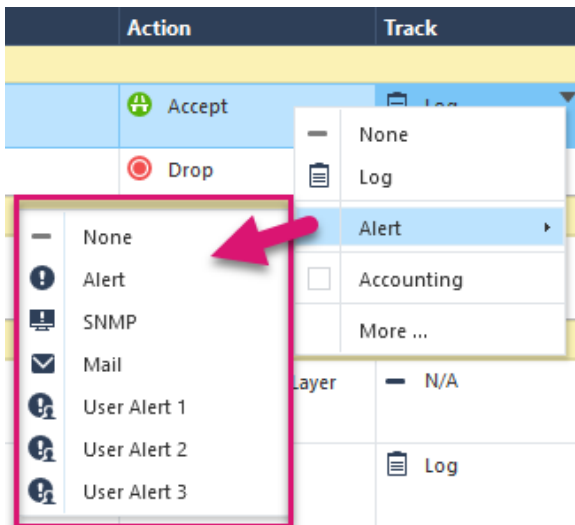
The More option is discussed later in this chapter.

Track Options - None, Log, and Account



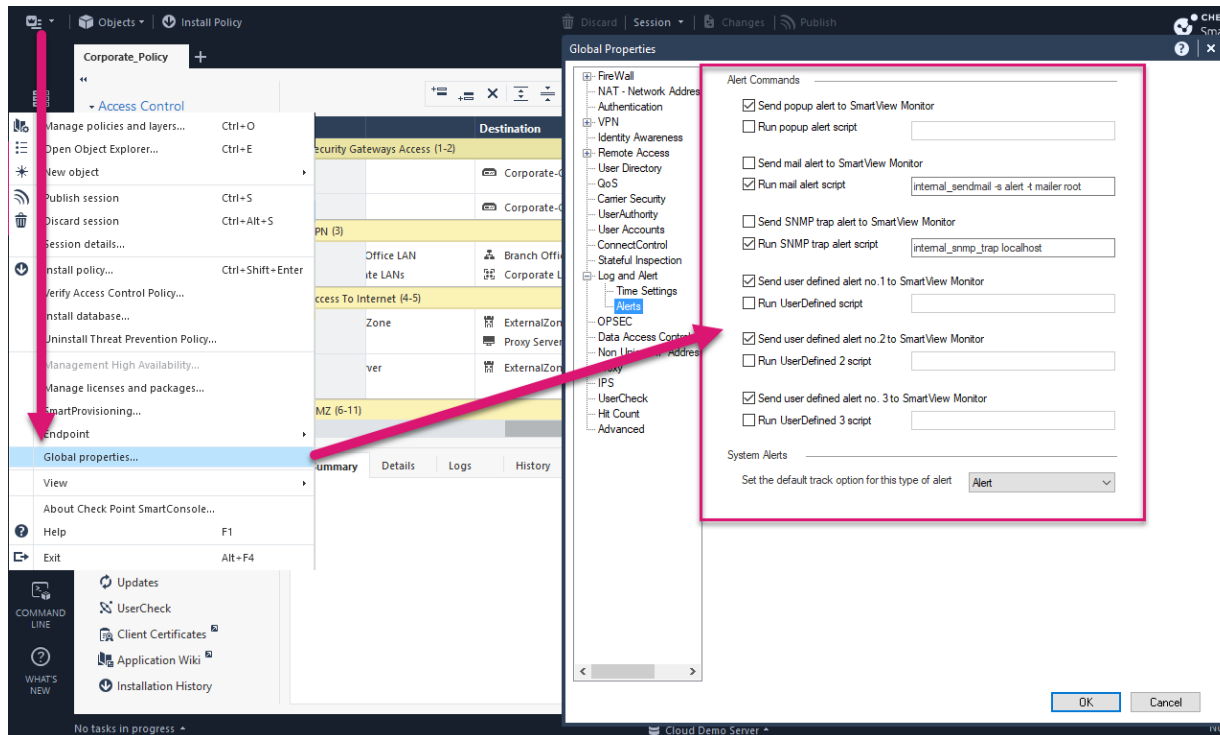
Option	Description
None	Do not generate a log for this rule.
Log (Default Option)	Enables log tracking for the rule. Information includes: <ul style="list-style-type: none">• Source• Destination• Source Port• Destination Port
Accounting	Updates the log at 10-minute intervals. Information includes: <ul style="list-style-type: none">• Upload bytes• Download bytes• Browse time

Track Options - Alert



Alert	Description
None	Do not generate a log for this rule.
Alert*	Generate a log and run a script.
SNMP*	Send SNMP alert or run a script.
Mail*	Send an email or run a script.
User Alert 1-3*	Send one to three customized alerts defined by a script.

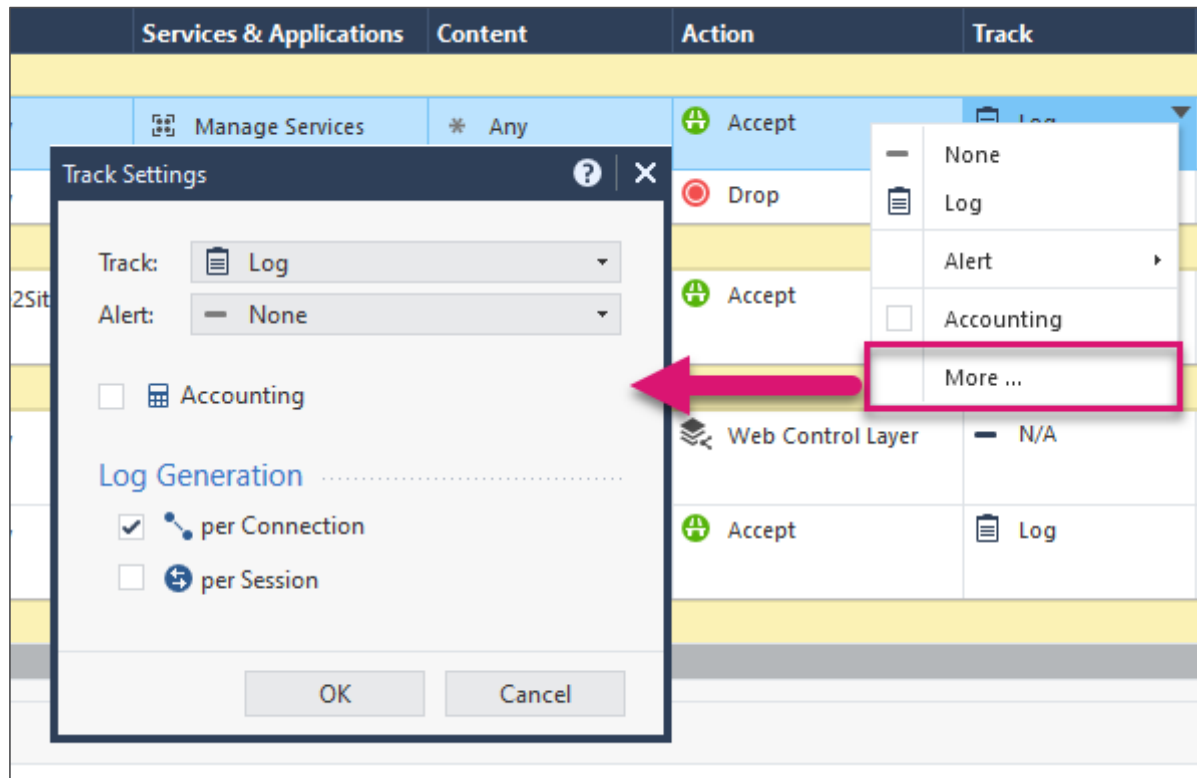
Alert Scripts



Alerts can be configured to send a popup alert to SmartView Monitor and/or run a script.

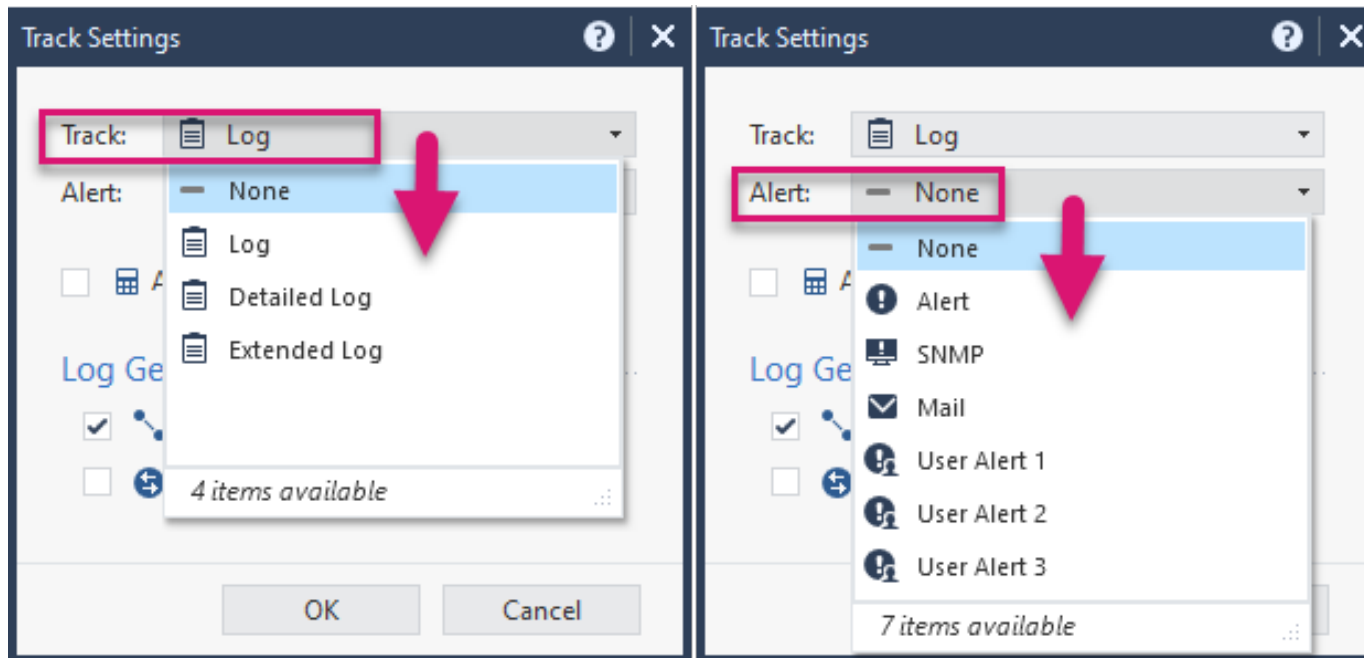
Menu → Global Properties → Log and Alert → Alerts

Track Settings - More



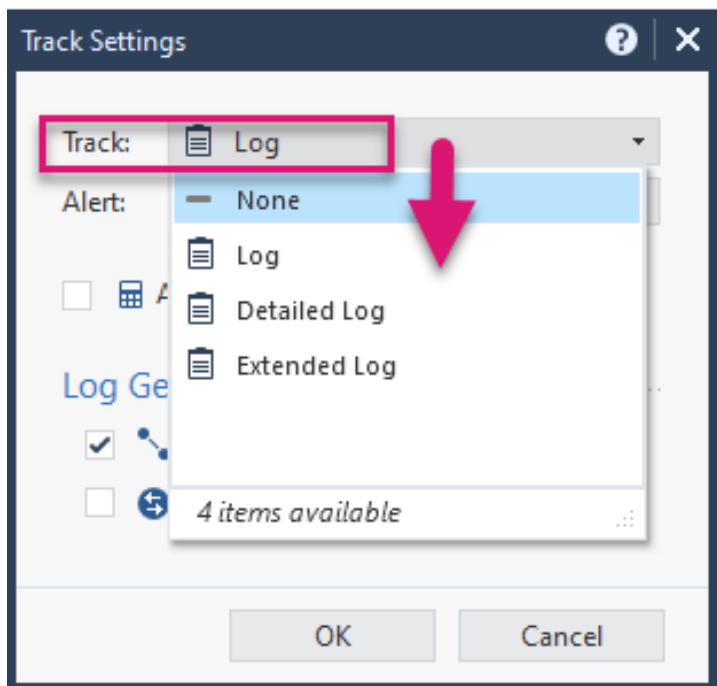
Provide additional track options for log detail that is tracked and log generation per connection, session, or both.

Track Settings – More (Continued)



- None
- Log
- Detailed Log
- Extended Log

Track Settings – More (Continued)



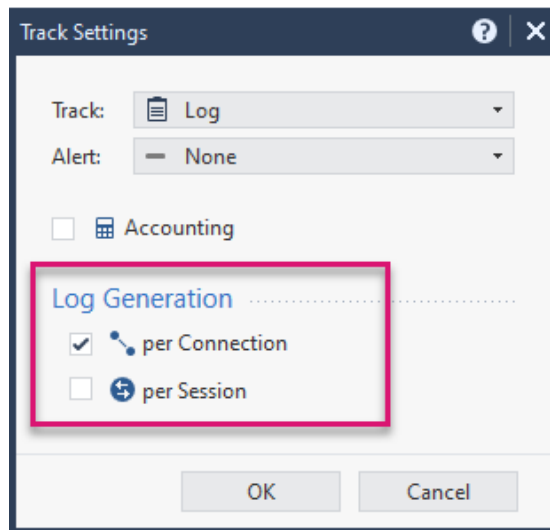
Use **Detailed Log** for a cleanup rule (Any/Internet/Accept) of an Applications and URL Filtering Policy Layer that was upgraded from an R77 Application Control Rule Base.

IMPORTANT

Detailed Log and **Extended Log** are only available if one or more of these Software Blades (features) are enabled on the Layer:

- Applications & URL Filtering
- Content Awareness
- Mobile Access

Log Generation Option



Log Generation	Description
per connection	Enable to show a different log for each connection in the session. <ul style="list-style-type: none">• Default for rules in a layer with only firewall enabled.
per session	Enable to generate one log for all the connections in the same session. <ul style="list-style-type: none">• Default for rules in a Layer with Applications and URL Filtering or Content Awareness enabled.

Accounting option is the same as covered previously.

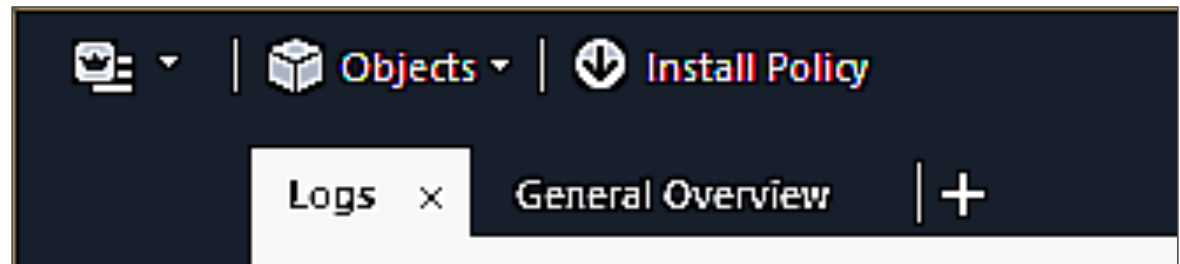
Log Queries

- Can return thousands of results.
- Network performance is not impacted because the log view typically only displays the first 50 results.
- Results can be exported to a comma separated value (CSV) file.



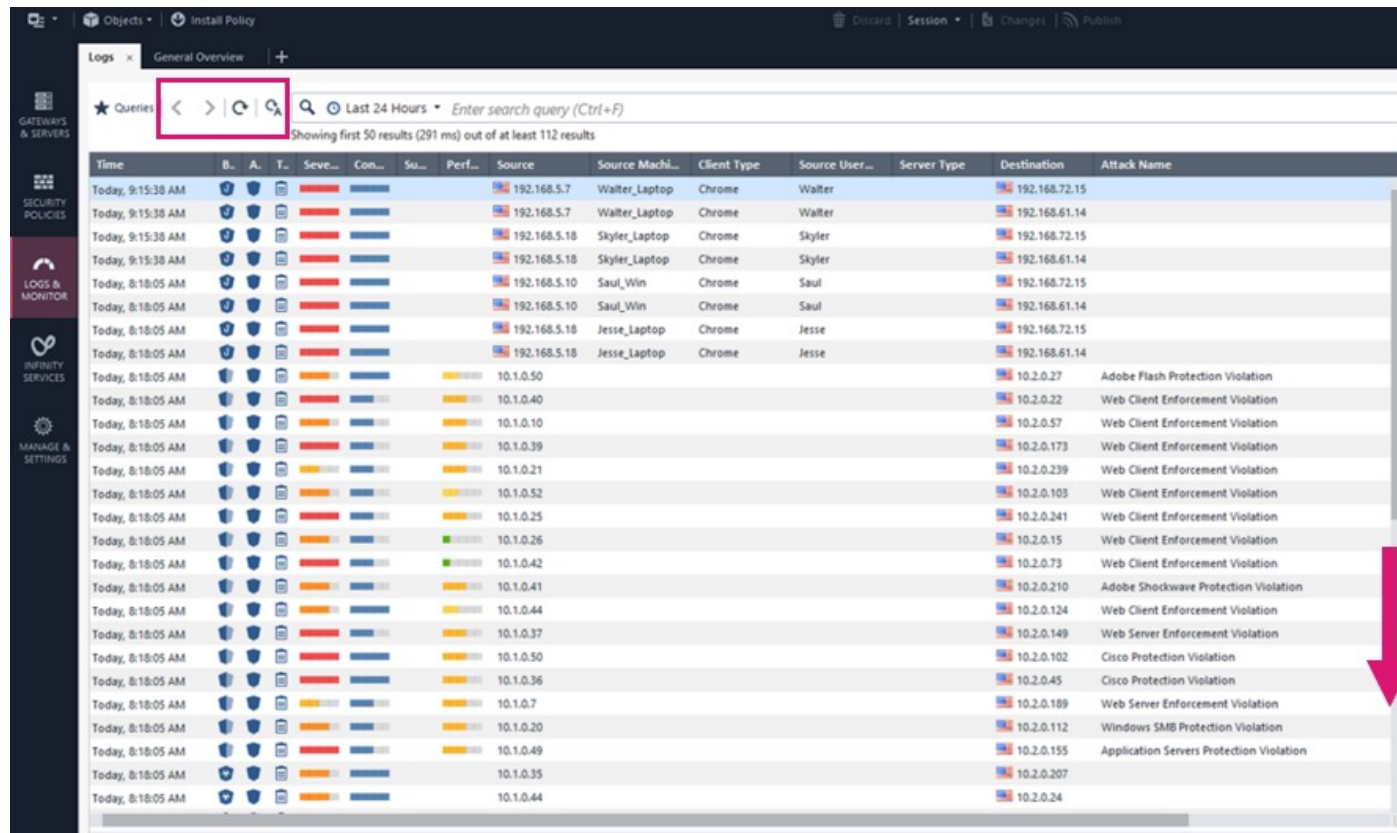
SmartConsole Log Options

- View the first 50 results.
- Use predefined queries to collect specific logs.
- Create custom queries to collect specific logs.



SmartConsole Logs & Monitor view → Logs tab

Navigating SmartConsole Log Queries



Showing first 50 results (291 ms) out of at least 112 results

Time	B.	A.	T.	Seve...	Con...	Su...	Perf...	Source	Source Machi...	Client Type	Source User...	Server Type	Destination	Attack Name
Today, 9:15:38 AM								192.168.5.7	Walter_Laptop	Chrome	Walter		192.168.72.15	
Today, 9:15:38 AM								192.168.5.7	Walter_Laptop	Chrome	Walter		192.168.61.14	
Today, 9:15:38 AM								192.168.5.18	Skyler_Laptop	Chrome	Skyler		192.168.72.15	
Today, 9:15:38 AM								192.168.5.18	Skyler_Laptop	Chrome	Skyler		192.168.61.14	
Today, 8:18:05 AM								192.168.5.10	Saul_Win	Chrome	Saul		192.168.72.15	
Today, 8:18:05 AM								192.168.5.10	Saul_Win	Chrome	Saul		192.168.61.14	
Today, 8:18:05 AM								192.168.5.18	Jesse_Laptop	Chrome	Jesse		192.168.72.15	
Today, 8:18:05 AM								192.168.5.18	Jesse_Laptop	Chrome	Jesse		192.168.61.14	
Today, 8:18:05 AM								10.1.0.50					10.2.0.27	Adobe Flash Protection Violation
Today, 8:18:05 AM								10.1.0.40					10.2.0.22	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.10					10.2.0.57	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.39					10.2.0.173	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.21					10.2.0.239	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.52					10.2.0.103	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.25					10.2.0.241	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.26					10.2.0.15	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.42					10.2.0.73	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.41					10.2.0.210	Adobe Shockwave Protection Violation
Today, 8:18:05 AM								10.1.0.44					10.2.0.124	Web Client Enforcement Violation
Today, 8:18:05 AM								10.1.0.37					10.2.0.149	Web Server Enforcement Violation
Today, 8:18:05 AM								10.1.0.50					10.2.0.102	Cisco Protection Violation
Today, 8:18:05 AM								10.1.0.36					10.2.0.45	Cisco Protection Violation
Today, 8:18:05 AM								10.1.0.7					10.2.0.189	Web Server Enforcement Violation
Today, 8:18:05 AM								10.1.0.20					10.2.0.112	Windows SMB Protection Violation
Today, 8:18:05 AM								10.1.0.49					10.2.0.155	Application Servers Protection Violation
Today, 8:18:05 AM								10.1.0.35					10.2.0.207	
Today, 8:18:05 AM								10.1.0.44					10.2.0.24	

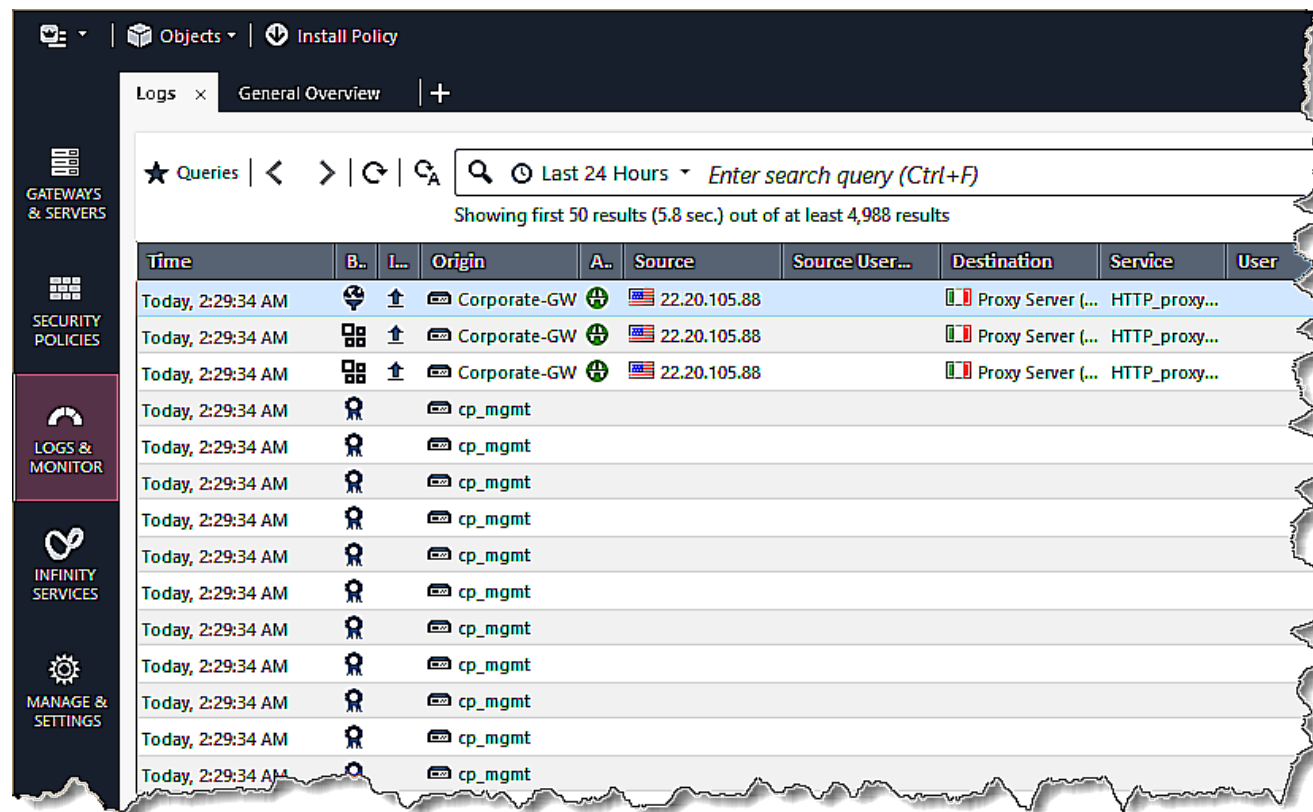
SmartConsole typically displays the first 50 results.

Predefined Log Queries

- Used to filter logs based on specific criteria.
- You can use as is or modify them to include/exclude existing criteria.
- You can also save predefined queries to a My Favorites list (discussed later).



Viewing Predefined Log Queries



The screenshot shows the Check Point management console interface. The left sidebar contains navigation options: GATEWAYS & SERVERS, SECURITY POLICIES, LOGS & MONITOR (highlighted), INFINITY SERVICES, and MANAGE & SETTINGS. The main area displays the 'Logs' tab with a search bar and a table of log entries. The search bar is set to 'Last 24 Hours' and shows 'Showing first 50 results (5.8 sec.) out of at least 4,988 results'. The table has columns for Time, B., I., Origin, A., Source, Source User..., Destination, Service, and User. The first three rows show traffic from 'Corporate-GW' to 'Proxy Server (... HTTP_proxy...)' with source IP '22.20.105.88'. The remaining rows show traffic from 'cp_mgmt'.

Time	B.	I.	Origin	A.	Source	Source User...	Destination	Service	User
Today, 2:29:34 AM		↑	Corporate-GW		22.20.105.88		Proxy Server (... HTTP_proxy...	HTTP_proxy...	
Today, 2:29:34 AM		↑	Corporate-GW		22.20.105.88		Proxy Server (... HTTP_proxy...	HTTP_proxy...	
Today, 2:29:34 AM		↑	Corporate-GW		22.20.105.88		Proxy Server (... HTTP_proxy...	HTTP_proxy...	
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						
Today, 2:29:34 AM			cp_mgmt						

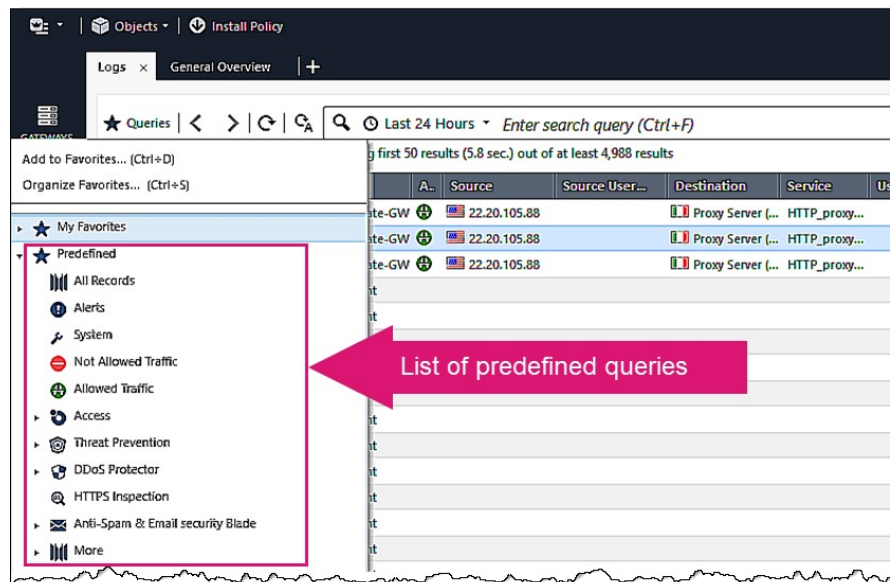
- Click the **Logs** tab.
- Click **Queries**.

Default Time Query – Last 24 Hours

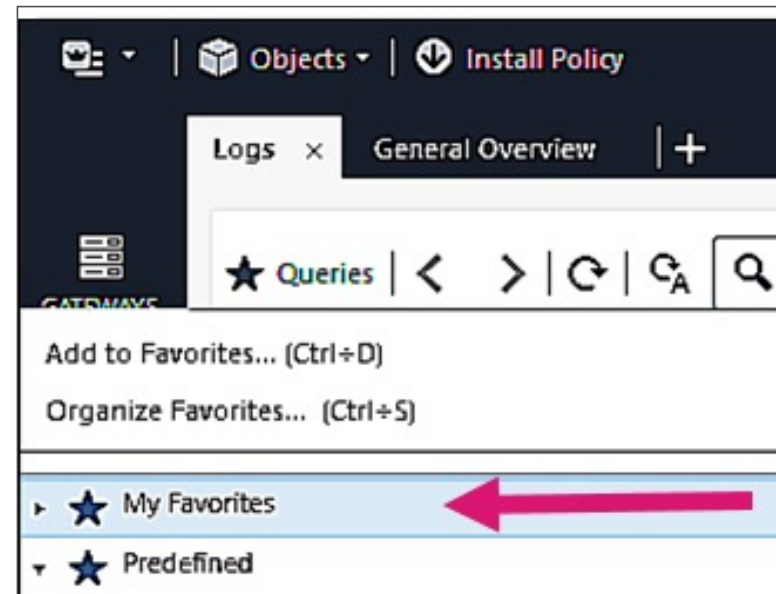
The screenshot shows the Check Point management console interface. The top navigation bar includes 'Objects' and 'Install Policy'. The main area is titled 'Logs' and 'General Overview'. A search bar contains the text 'action(drop OR reject OR block)'. A dropdown menu is open, showing various time query options. The 'Last 24 Hours' option is highlighted in blue, and a red arrow points to it. The background shows a table of log entries with columns for 'Time', 'Source User...', 'Destination', and 'Service'.

Time	Source User...	Destination	Service	
Today, 2:29:34 AM	.100.1	198.51.100.255	nbname (UDP/137)	
Today, 2:29:34 AM	.100.1	198.51.100.255	nbname (UDP/137)	
Today, 2:29:34 AM	xy Server (...)	192.168.88.9	FW1_log (TCP/257)	
Today, 2:29:34 AM	xy Server (...)	192.168.88.9	FW1_log (TCP/257)	
Today, 2:29:34 AM	xy Server (...)	172.24.250.10	domain-udp (UDP/53)	
Today, 2:16:12 AM	Office (1...	fra15s28-in-f10...	dest-unreach (ICMP)	
Today, 2:16:12 AM	Office (1...	fra15s28-in-f10...	dest-unreach (ICMP)	
Today, 2:16:12 AM	Office (1...	68.232.35.182	dest-unreach (ICMP)	
Today, 2:16:12 AM	BranchOffice	BranchOffice (1...	68.232.35.182	dest-unreach (ICMP)
Today, 2:16:12 AM	BranchOffice	BranchOffice (1...	172.103.211.130...	dest-unreach (ICMP)

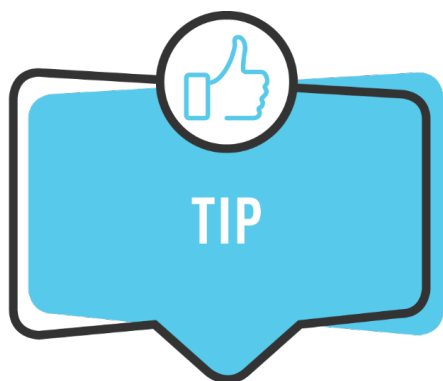
Query Organization



Predefined



My Favorites



You can save existing queries or add custom queries to this list for future use.

You can also create additional folders to organize the queries in a way meaningful to you.

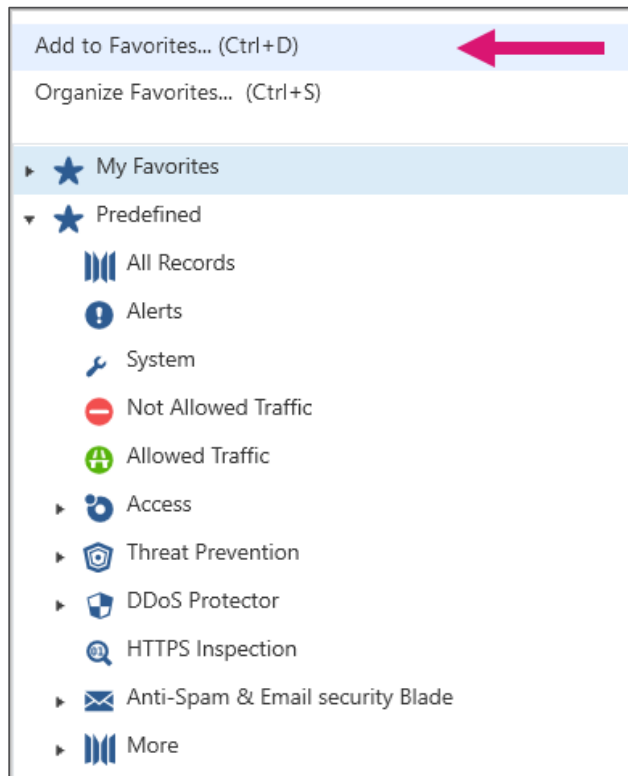
Selecting a Query

The screenshot shows the Check Point logs interface. A search bar at the top contains the query 'action:(drop OR reject OR block)'. A dropdown menu is open, showing a list of predefined queries. The 'Not Allowed Traffic' query is selected, and a tooltip displays its details: 'Name: Not Allowed Traffic' and 'Query: action:(drop OR reject OR block)'. A table of log results is visible in the background, showing columns for Source, Source User, Destination, and Service.

Source	Source User	Destination	Service
10.55.248.217		10.5.245.152	http
10.55.250.106		10.111.166.9	http
10.55.248.145		10.111.166.9	http
10.30.150.8	Joe Roberts	10.37.212.170	http
10.30.150.8	Joe Roberts	10.37.212.170	http
10.55.251.133		10.111.165.253	http
10.30.146.38		172.29.40.222	http
10.55.248.71		10.103.133.47	http
10.55.250.106		10.111.165.8	http
10.55.248.248	Joe Roberts	10.111.165.211	http
10.0.43.6		10.31.86.173	http
10.55.251.133		10.111.165.253	http
10.0.34.182	Paul Harris4	10.109.145.162	http
10.30.146.38		172.29.40.222	http
10.55.248.217		10.5.245.152	http
10.55.250.106		10.111.166.9	http

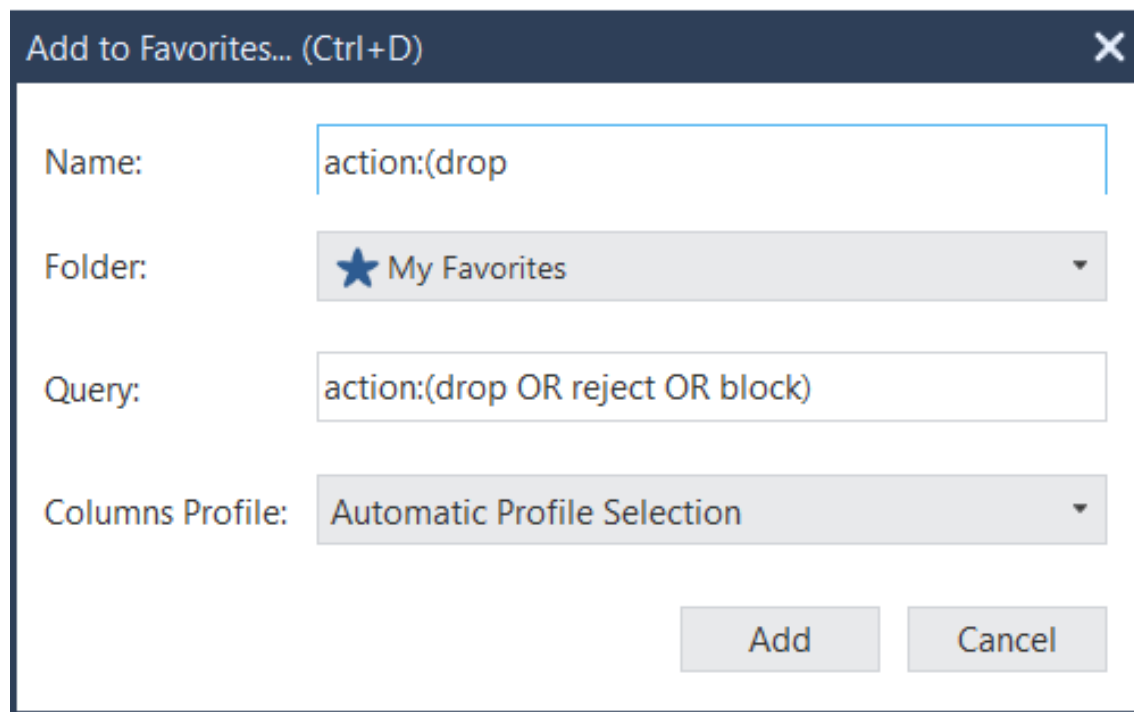
- Select a query to run from the list.
- The new query action appears in the search bar.

Adding a Query to My Favorites



- On the Logs tab, click **Queries**.
- Select a query; for example, **Not Allowed Traffic**.
- Click **Add to Favorites**.

Adding a Query to My Favorites (Continued)



Add to Favorites... (Ctrl+D)

Name:

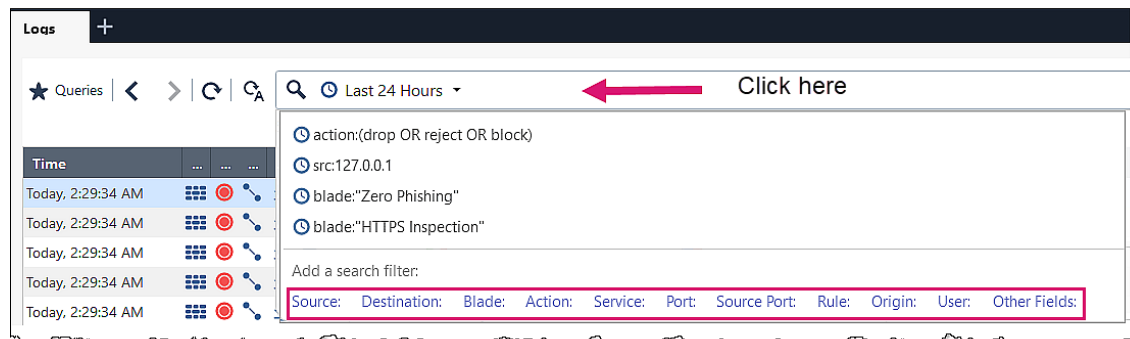
Folder:

Query:

Columns Profile:

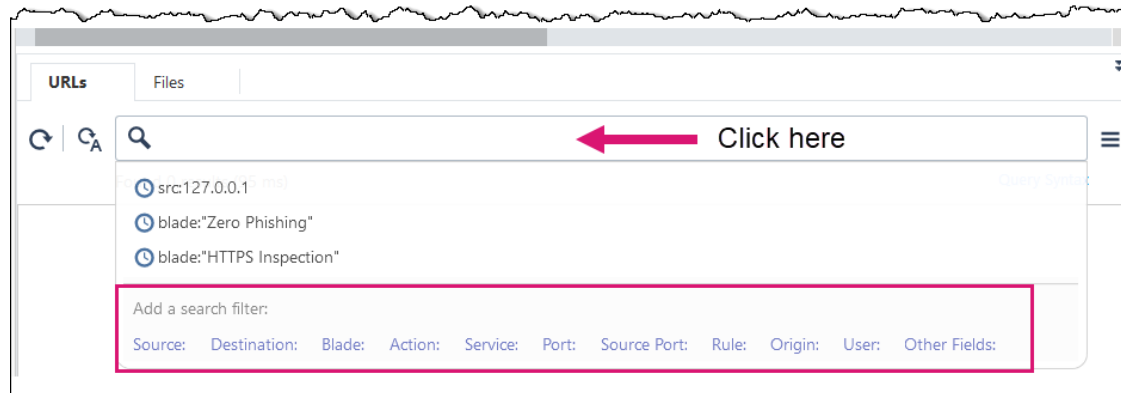
Customize the query details, as appropriate.

Adding a Search Filter



To or bottom of page:

Click in the search bar, then click link to add search criteria.



Creating Complex Queries

- When a query is created, the criteria is displayed in the Query Definition field at the top of the window.
- The basic query syntax is:

[:]

- Boolean operators
- Wildcards
- Fields
- Ranges

Using SmartConsole Query Language References

The screenshot displays the SmartConsole interface with a log table and a 'Tops' sidebar. The table shows log entries with columns for Time, B., A., T., Seve..., Con..., Su..., Perf..., Source, Source Machi..., and Client Type. The 'Tops' sidebar lists various categories like Top Sources, Top Destinations, etc. Two red arrows point to 'Query Syntax' links in the top and bottom search bars.

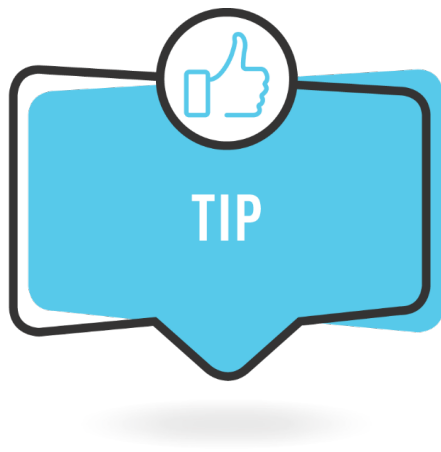
Time	B..	A.	T..	Seve...	Con...	Su...	Perf...	Source	Source Machi...	Client Type
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	192.168.5.10	Saul_Win	Chrome
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	192.168.5.10	Saul_Win	Chrome
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	192.168.5.18	Jesse_Laptop	Chrome
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	192.168.5.18	Jesse_Laptop	Chrome
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	10.1.0.50		
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	10.1.0.40		
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	10.1.0.10		
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	10.1.0.39		
Today, 8:18:05 AM	✓	✓	✓	✓	✓	✓	✓	10.1.0.21		

Click either Query Syntax link.

Query Language Online Help

The screenshot shows the Check Point SmartConsole R81.20 Help page for Query Language. The page features a navigation bar with the Check Point logo and tagline 'YOU DESERVE THE BEST SECURITY'. Below the logo, there are links for 'SUGGESTED TRAINING' (CCSE), 'Knowledge Base' (MIND (TRAINING), HACKING POINT, CYBER RANGE, CERTIFICATIONS), 'Feedback', 'Security Awareness', and 'Join the Community' (JUMP START). The main content area is titled 'SmartConsole and SmartView Query Language' and includes a search bar, a breadcrumb trail, and a 'FEEDBACK' button. The text explains that a powerful query language allows users to filter log files based on criteria, and provides the basic query syntax: `[<Field>:] <Filter Criterion>`. It also mentions that Boolean operators can be used to combine multiple criteria: `[<Field>:] <Filter Criterion> {AND|OR|NOT} [<Field>:] <Filter Criterion> ...`. The page footer includes the date '18 January 2023', a 'Was this helpful?' feedback prompt, and the copyright notice '© 2022 Check Point Software Technologies Ltd.'

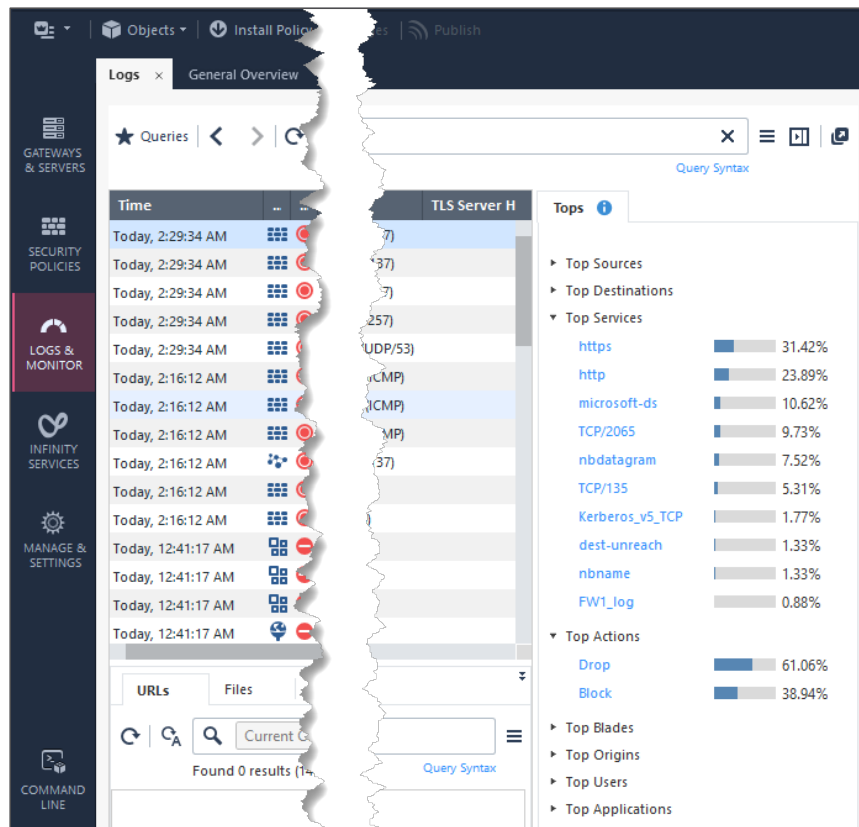
Always use the online documentation as your reference source when creating custom queries.



There are many methods to access online Help and documentation:

- Quantum R81.20 Home Page (sk173903)
- Check Point Support Center
- SmartConsole application menu → Help
- Question mark icon on SmartConsole window (when present)

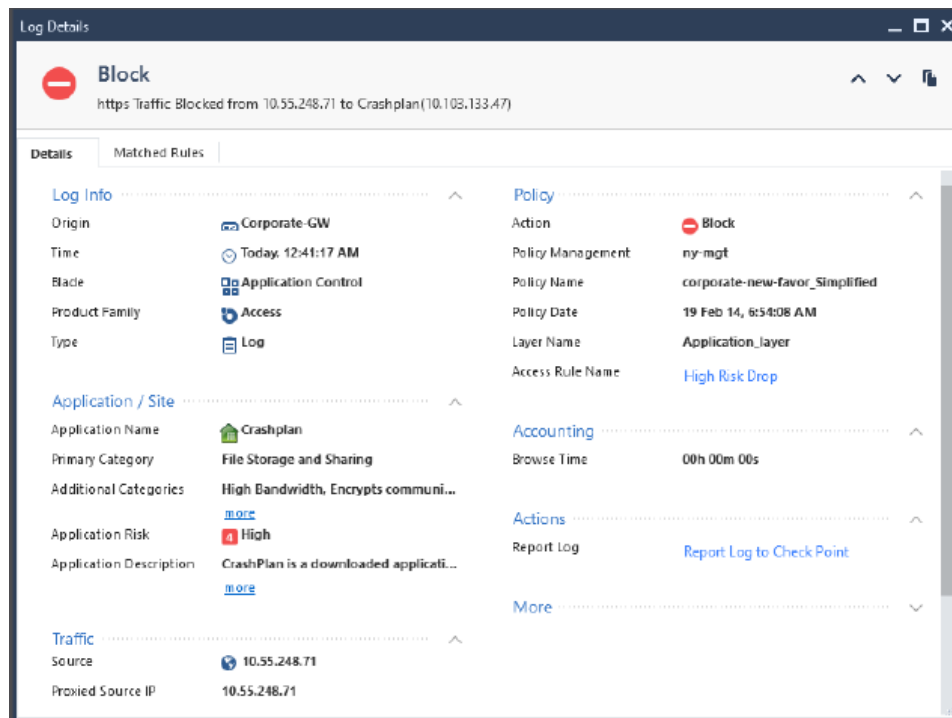
Tops Tab



Category	Item	Percentage
Top Services	https	31.42%
	http	23.89%
	microsoft-ds	10.62%
	TCP/2065	9.73%
	nbdatagram	7.52%
	TCP/135	5.31%
	Kerberos_v5_TCP	1.77%
	dest-unreach	1.33%
Top Actions	Drop	61.06%
	Block	38.94%

- Provides a way to filter logs in top categories.
- Expand any heading on the Tops tab to see the top items in that category.
- Click any link to see only the logs associated with that selected item.

Log Details



- Double-click to view log details.
- Details include log information and policy and traffic flow details.
- Click any link to view more information.

Monitoring Traffic and Connections

- SmartConsole and SmartView Monitor provide similar monitoring features with some viewing features unique to SmartView Monitor.

View	SmartConsole	SmartView Monitor
Gateway Status	Yes	Yes
System Counters	Yes	Yes
Traffic	Yes	Yes
VPN Tunnel Monitoring	No	Yes
Remote Users	No	Yes

This course focuses on monitoring with SmartConsole.

Gateways & Servers - Status Column

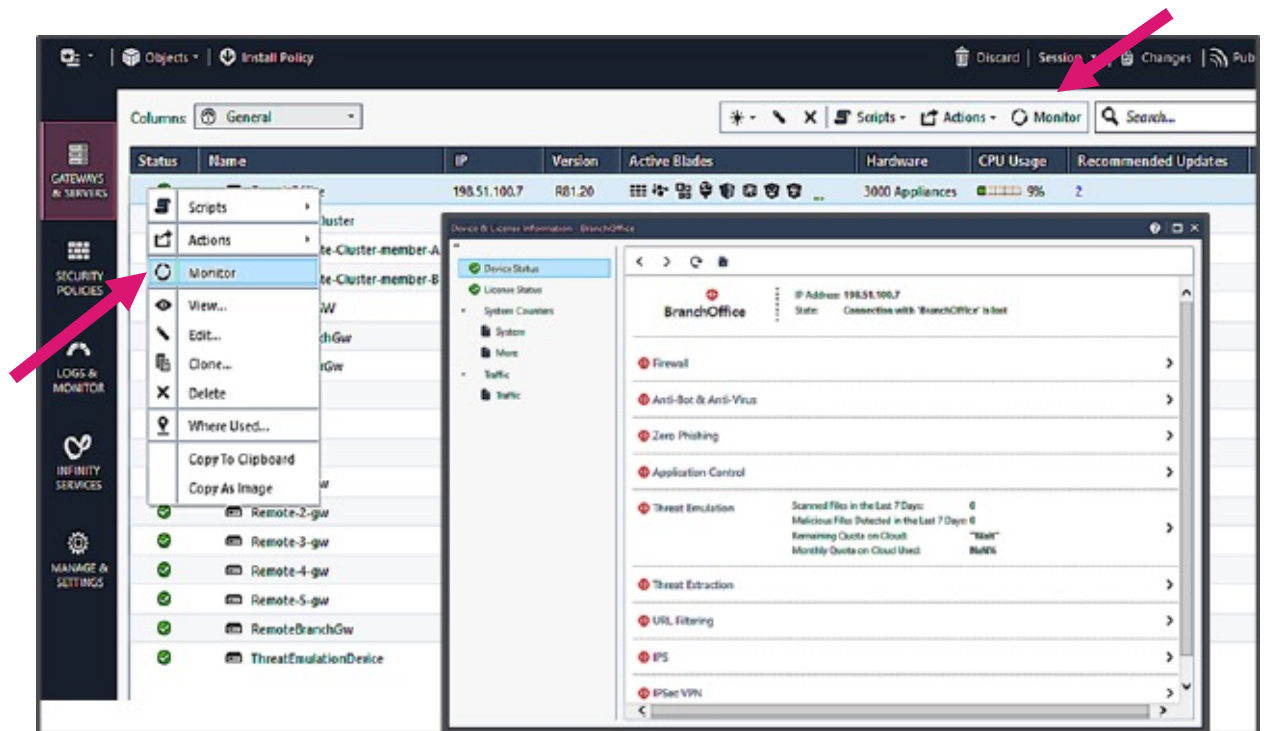
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Re...
OK	BranchOffice	198.51.100.7	R81.20	[Icons]	3000 Appliances	9%	2
OK	Corporate-Cluster	17.23.5.1	R81.20	[Icons]	26000 Appliances	11%	3
Problem	Corporate-Cluster-member-A	17.23.5.2	R81.20	[Icons]	26000 Appliances		
Problem	Corporate-Cluster-member-B	17.23.5.3	R81.20	[Icons]	26000 Appliances		
OK	Corporate-GW	198.51.100.5	R81.20	[Icons]	23000 Appliances	24%	2
OK	EuropeBranchGw	192.0.2.100	R81.10	[Icons]	5000 Appliances	17%	1
OK	HeadquarterGw	192.16.26.100	R81.20	[Icons]	23000 Appliances	9%	2
OK	HQgw	192.0.2.200	R81	[Icons]	15000 Appliances	18%	3
OK	mgmt	10.0.73.236	R81.20	[Icons]	Open server	7%	2
OK	OfficeGw	192.16.26.7	R81.20	[Icons]	23000 Appliances	14%	2
OK	Remote-1-gw	192.0.22.1	R80.40	[Icons]	1590 Appliances	11%	2
OK	Remote-2-gw	192.0.23.1	R80.40	[Icons]	1550 Appliances	4%	3
OK	Remote-3-gw	192.0.24.1	R80.40	[Icons]	5000 Appliances	6%	1
OK	Remote-4-gw	192.0.25.1	R80.40	[Icons]	5000 Appliances	24%	2
OK	Remote-5-gw	192.0.26.1	R81	[Icons]	5000 Appliances	16%	2
OK	RemoteBranchGw	198.51.100.120	R80.40	[Icons]	Open server	9%	2
OK	ThreatEmulationDevice	192.0.111.13	R81	[Icons]	TE Appliances	4%	2

- OK
- Attention
- Problem
- Waiting
- Disconnected
- Untrusted

SmartConsole: Monitor View

Two ways to monitor devices. From the Gateways & Servers view:

- Right-click a device and select **Monitor**.
- Select a device and click the **Monitor** icon.



Review Questions

1. Which tool can be used to collect and view logs and monitor devices?
2. How many logs are typically displayed in the default view?
3. What information is available in the Gateway & Servers Monitor view?

Lab 10A

Elevating Traffic View



Lab 10B

Monitor System States

