REDSHIELD ON-PREMISE

MANAGED APPLICATION SECURITY SERVICE

F5 BIG-IP ASM v11.6

INTEGRATION GUIDE

Purpose of this Document

This Integration Guide for RedShield On-Premise Managed Application Security Service describes the configuration procedure for integrating F5® BIG-IP® Application Security Manager™ (ASM) version 11.6 with RedShield cloud based management systems.

Document Control

Version	Date	Author	Comments
0.1	10/10/15	Sam Pickles	Draft
1.0	23/10/15	Sam Pickles	Release

Contact

For any queries regarding this document please contact:

Sam Pickles
Chief Technology Officer
RedShield
Level 12, Travel and Tourism House,
79 Boulcott St, Wellington
sam@aurainfosec.com
+64 27 253 4687

Contents

1 RedShield Overview 10
2 Basic Network Architecture 10
2.1 Management VLAN 11
2.2 Source Network Address Translation (SNAT) 12
2.3 X-Forwarded-For 12
2.4 SSL Requirements 12
2.5 Caching 12
3 Configuring IPSec VPN 12
3.1 VPN Tunnel Parameters 13
4 Configuring Authentication 14
5 Configuring Audit Logging 15
6 Configuring SNMP 16
7 Configuring Logging Profiles 17
8 RedShield Portal Access 19
8.1 Reporting Portal 19
8.2 RedEye Vulnerability Scanning Portal 19
8.3 Support and Knowledgebase Portal 19

1 RedShield Overview

RedShield Managed Web Application Firewall (WAF) and Distributed Denial of Service (DDoS) mitigation platform provides protection for high-value web applications. RedShield leverages the F5 BIG-IP Application Security Manager (ASM) module, custom F5® iRules®and our global high-availability cloud infrastructure, to provide comprehensive web vulnerability mitigation and a transparent and affordable DDoS solution.

RedShield is available both as a fully cloud based service, and a hybrid On-Premise service. This Integration Guide covers RedShield On-Premise Service.

2 Basic Network Architecture

The most common deployment architecture for F5 devices being installed into an existing network environment, is One-Armed, or SNAT mode (Source Network Address Translation). Please note that any common F5 deployment architecture is supported by RedShield, for delivery of service on existing F5 equipment or where specific design requirements exist (provided that traffic is fully proxied via the F5 in both inbound and outbound directions).

The advantage of the One-Armed SNAT architecture is that inbound user connections are simple to direct to the F5 from a firewall or upstream device, and then proxied traffic being forwarded to servers appears to originate from the F5's self IP address; which simplifies routing and has minimal impact on existing environments.

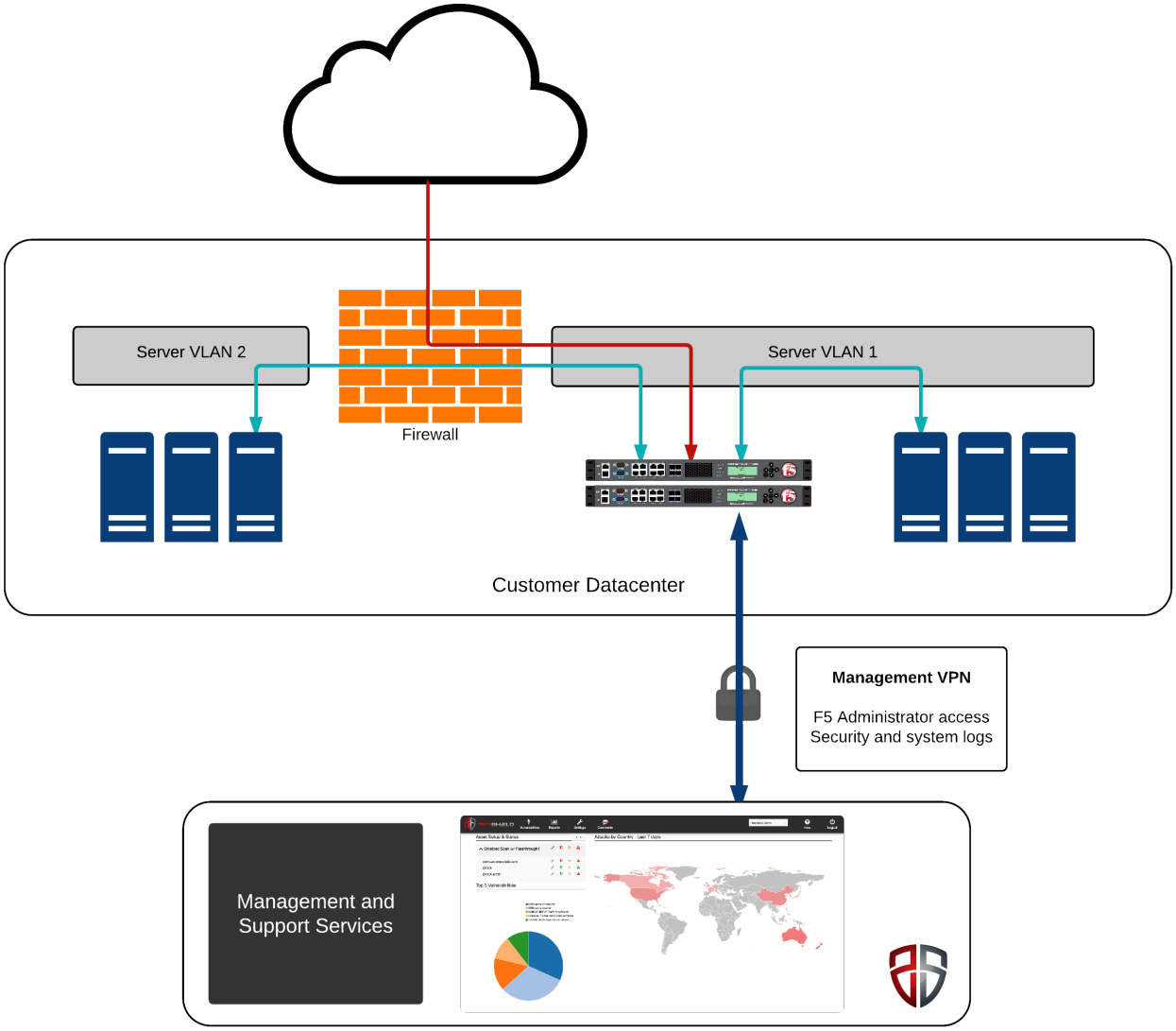


Fig 1: Basic Service Architecture (One-Armed SNAT)

2.1 Management VLAN

F5 Big IP ASM requires a separate VLAN/subnet for its management interface. A VPN is required in order to facilitate RedShield management traffic to and from the ASM. Security attack logs on this VLAN are forwarded from the ASM via the VPN to reach RedShield log servers for analysis and incident detection. RedShield administrators may use the VPN to log in to the management interface of the ASM during change windows to perform updates.

2.2 Source Network Address Translation (SNAT)

SNAT allows traffic to be fully proxied via the ASM, retrofitted into an existing network environment without requiring routing changes to networks or servers.
Incoming traffic has a destination IP address of the ASM's Virtual Server; which then proxies traffic to the application server and translates both the source and destination IP of the traffic.

2.3 X-Forwarded-For

Due to the requirements to proxy traffic and translate both source and destination IP addresses, the application server is unable to detect the client's true IP address in the arriving packets; however the ASM is configured to insert an X-Forwarded-For header (or custom format header) which contains this information.

2.4 SSL Requirements

SSL is decrypted by the ASM, and re-encrypted for user traffic being forwarded to the application server.

An updated certificate and keys are required on the ASM. These may be submitted to RedShield consultants during deployment if not already configured on the ASM.

2.5 Caching

Caching may be configured on the F5 to provide acceleration and server offload benefits for web applications. Cache clearance is performed via the RedShield portal or directly on the ASMs.

3 Configuring IPSec VPN

IPSec site-to-site VPN should be configured between your datacentre, and RedShield's management network; to allow RedShield consultants and management systems to communicate with BIG-IP ASM on your site.

The VPN should be configured on a network device such as a firewall, separate to the BIG-IP ASM, which is capable of routing to the F5 management interfaces and able to maintain an IPSec tunnel to RedShield's network via the internet.

RedShield's VPN settings do not have any specialised IP addressing requirements. Customers will only see public IP addresses from RedShield, both as tunnel end-points and sources of traffic within the tunnel. At the customer end, any IPv4 addressing scheme may be supported from public or private ranges as required.

3.1 VPN Tunnel Parameters

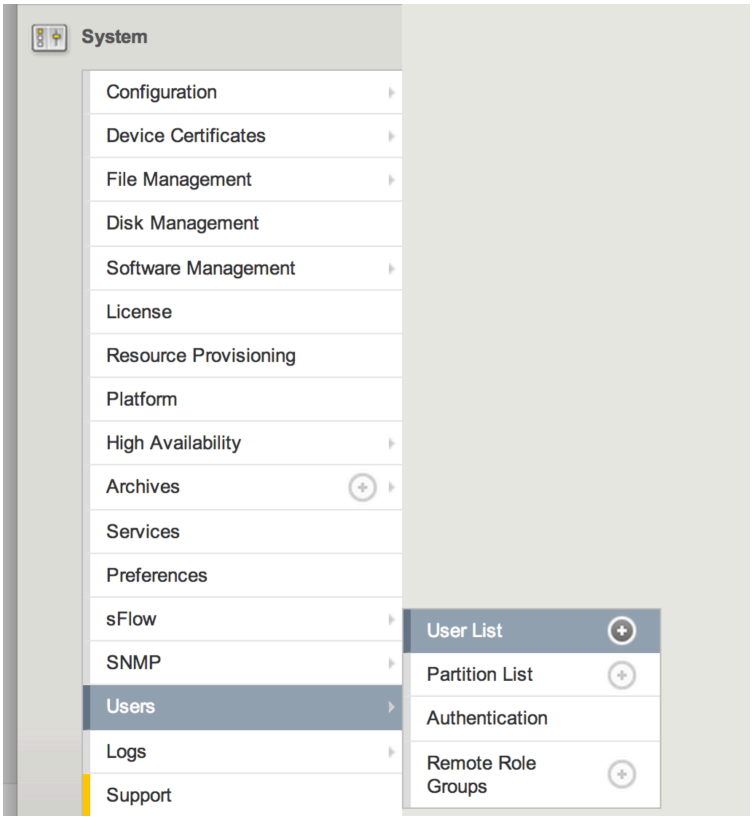
IP addresses and other details will be exchanged with RedShield during service setup. Security parameters for configuring VPN include the following:

IKE Phase One	
Passphrase	Pre Shared – Minimum 16 characters, mixed case letters, numbers and special characters. RedShield will generate and send during setup.
Diffie-Hellman Group	Group 5
Encryption Algorithm	AES-256
Hash Algorithm	SHA-256
Lifetime	86400

IKE Phase Two	
Diffie-Hellman Group	Group 5
Encryption Algorithm	AES-256
Authentication Algorithm	SHA-256
Lifetime	3600
Perfect Forward Secrecy (PFS)	Enabled
Compression and Vendor ID	Disabled
Dead Peer Detection	Disabled
XAUTH & Aggressive Mode	Disabled
IKE Version	V1

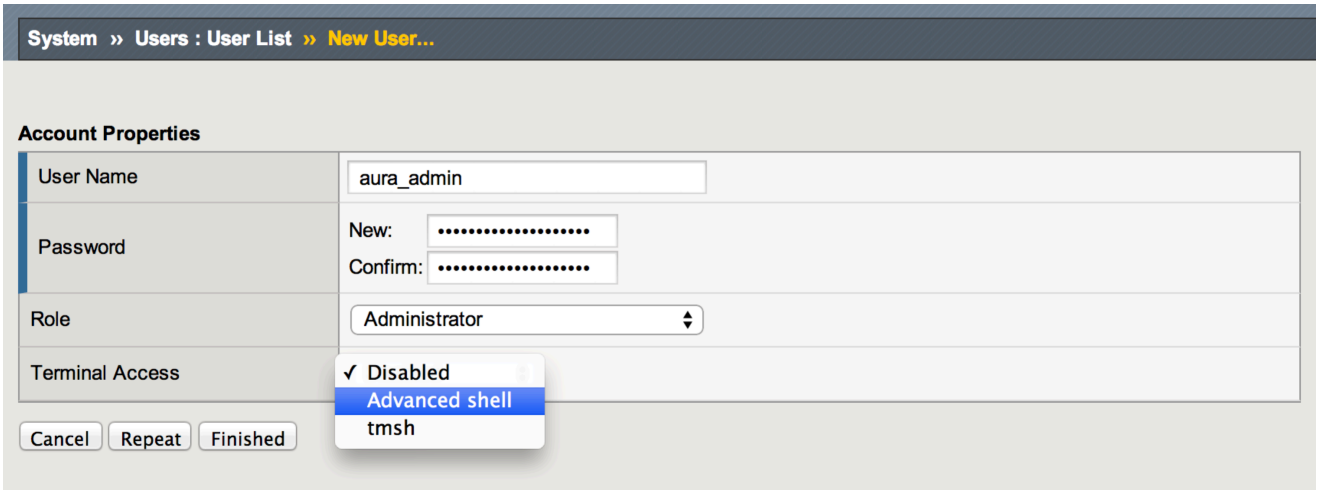
4 Configuring Authentication

RedShield requires access to the BIG-IP ASM management web interface and command line, to enable access to BIG-IP ASM policies, general system diagnostics and management, and iRules. A user should be configured to allow access to the system; using either a system-wide account such as rs_admin, or using accounts for each RedShield consultant individually by request.



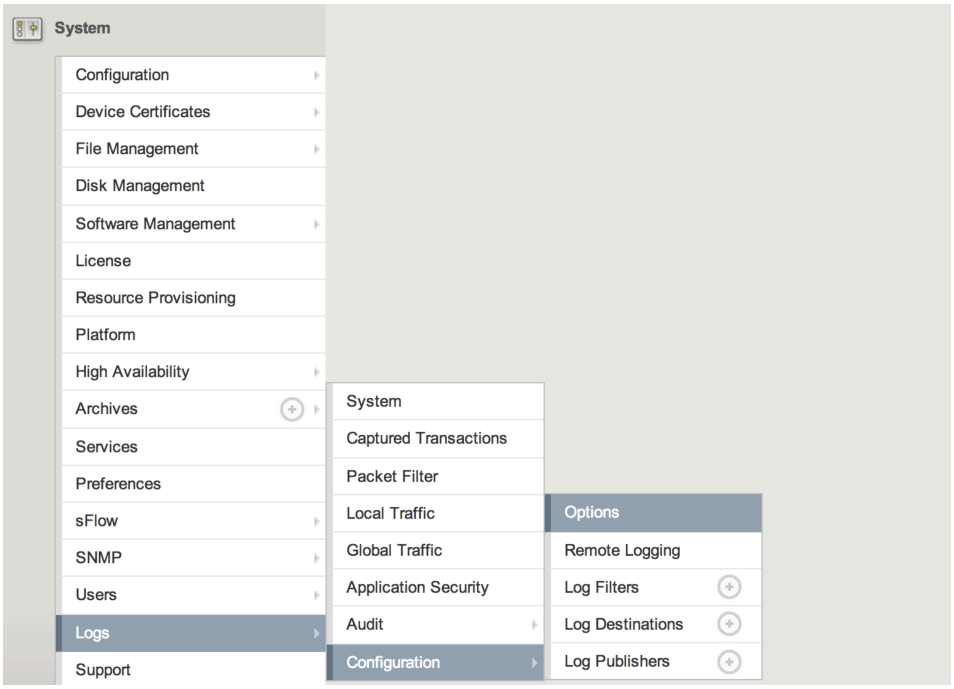
Configure a strong password (12 characters or more, mixed case letters, numbers and special characters), and send this to RedShield using a secure method such as those outlined in the following article:

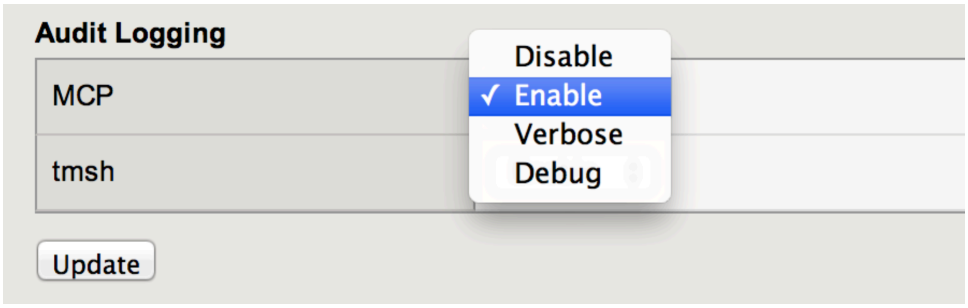
https://auraredeye.zendesk.com/entries/25101763-Securely-Exchanging-Files-and-Data-with-Aura



5 Configuring Audit Logging

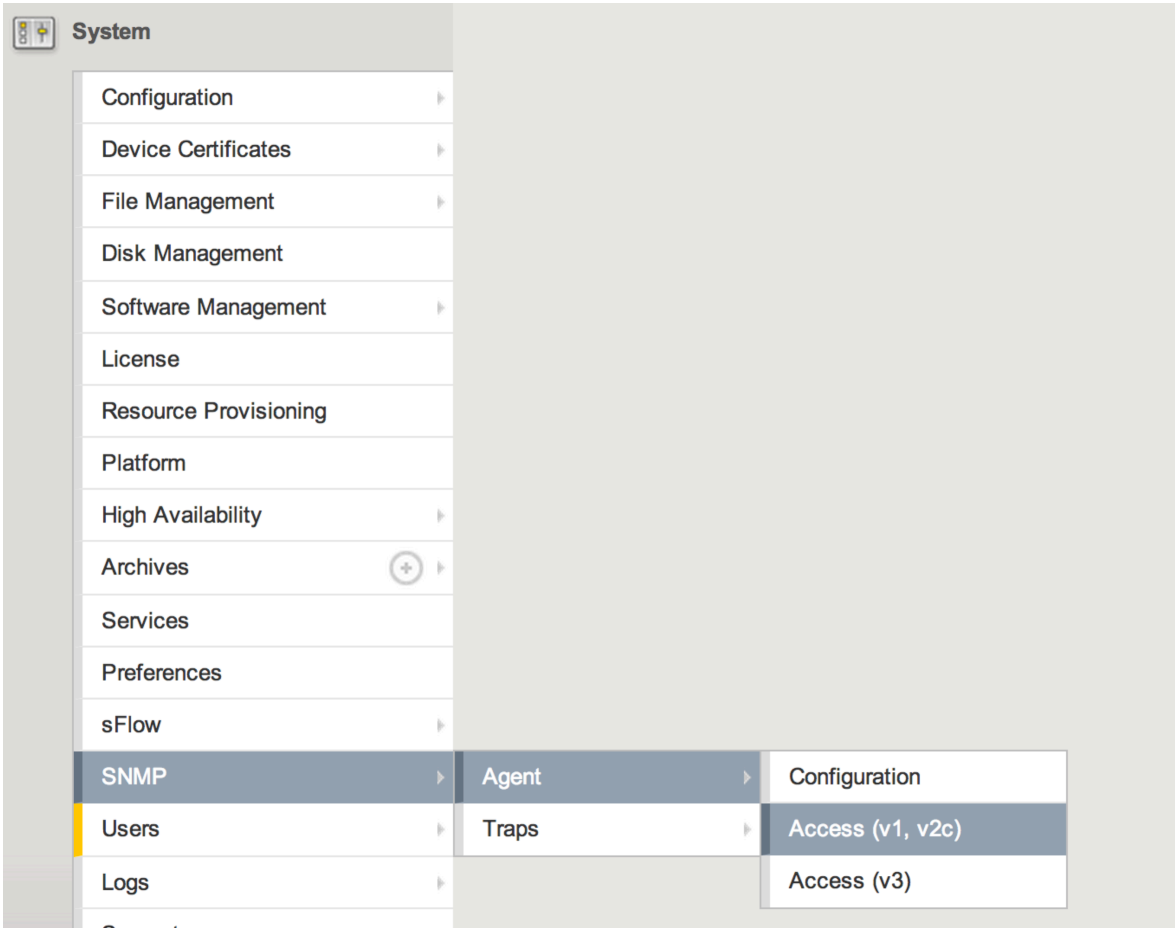
Audit logging should be enabled to track changes on the BIG-IP ASM platform made by any administrator as follows:





6 Configuring SNMP

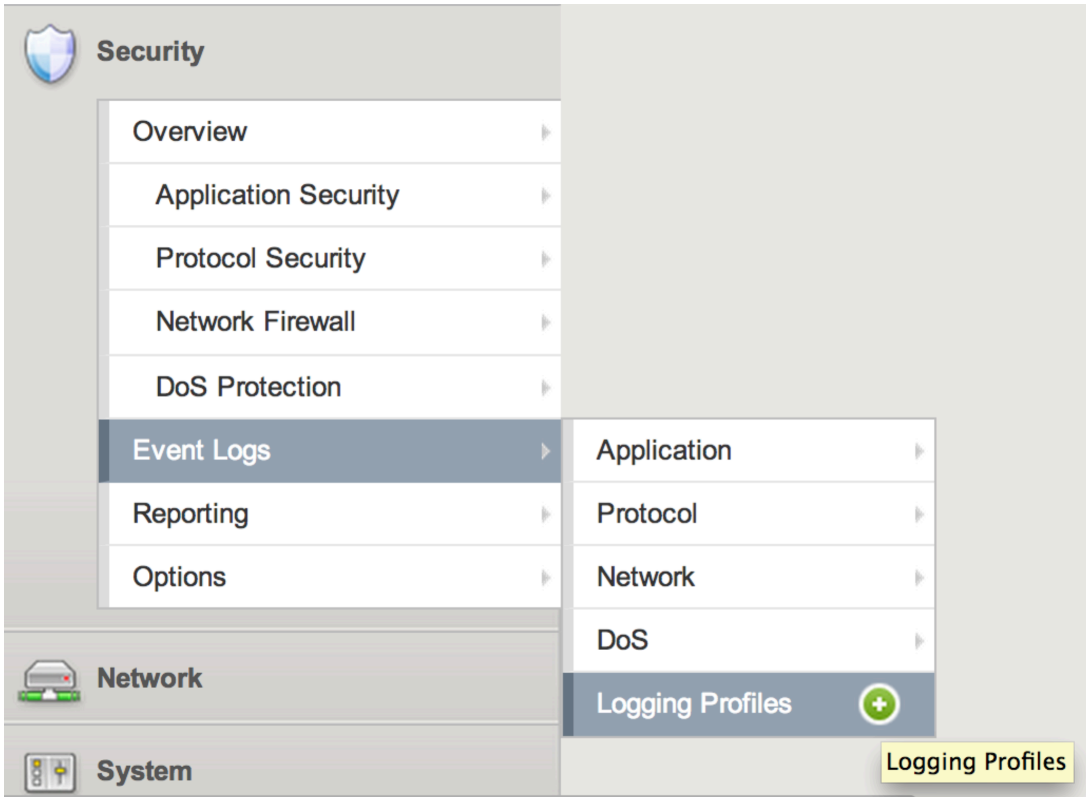
Remote monitoring of the BIG-IP ASM is performed using SNMP. RedShield will provide the source IP address of the monitoring server when the VPN tunnel is established. Once you have the IP address for the RedShield monitoring server, configure access to SNMP as follows (SNMPv3 will be supported in a future release):



Configuration parameters will be provided by RedShield at time of setup.

7 Configuring Logging Profiles

Logging is configured by RedShield consultants during setup. If an On-Premise SIEM or log server is available which requires a copy of ASM attack event logs, this may be added as a destination to the logging profile by standard change request. Logging profiles are configured as follows:



The following settings (defaults are used unless values specified here):

Logging Profile Settings	
Application Security	Enabled
Local Storage	Enabled
Guarantee Local Logging	Disabled
Response Logging	Off
Remote Storage	Enabled

Remote Storage Type	TCP
IP Address	<RedShield will supply>
Port	<RedShield will supply>
Storage Format (User Defined)	SUPPORT_ID=%support_id%;TYPE=%attack_type%;DATE=%date_time%;DEST_IP=%dest_ip%;DEST_PORT=%dest_port%;GEO=%geo_location%;HEADERS=%headers%;HTTP_CLASS=%http_class_name%;IP_ADDR_INT=%ip_address_intelligence%;IP_CLIENT=%ip_client%;METHOD=%method%;POLICY=%policy_name%;PROTO=%protocol%;REQ_STATUS=%request_status%;RESP_CODE=%response_code%;SESS_ID=%session_id%;SEV=%severity%;SIG_IDS=%sig_ids%;SIG_NAMES=%sig_names%;SRC_PORT=%src_port%;SUB_VIOLATIONS=%sub_violations%;HOST=%unit_hostname%;URI=%uri%;USERNAME=%username%;VIOLATION_DETAILS=%violation_details%;VIOLATIONS=%violations%;XFF=%x_forwarded_for_header_value%;QUERY_STR=%query_string%;REQ=%request%;
Maximum Query Size	Any
Maximum Entry Length	64K
Report Detected Anomalies	Enabled
Request Type	Illegal Requests Only

8 RedShield Portal Access

8.1 Reporting Portal

Details will be supplied during setup by RedShield for the Reporting Portal.

8.2 RedEye Vulnerability Scanning Portal

Details will be supplied during setup by RedShield for the Vulnerability Scanning Portal.

8.3 Support and Knowledgebase Portal

Details will be supplied during setup by RedShield for the Support Portal.