



ShareTech UTM Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw



Logs are the key to prevention and recovery

Logs are the core of cybersecurity regulations worldwide. They not only support incident tracking and audits but also serve as the foundation of defense.

Real-time Anomaly and Intrusion Detection

Logs can reveal abnormal login activities, changes in access patterns, and traffic fluctuations, helping to identify potential attacks.

Time	Account	IP Address	Management IP	Menu Path	Action	Events Content
2025-08-25 11:07:56	s	61	59	System Login	Login	Success
2025-08-25 10:26:34	st	192.	192	Policy > Security Policy > Incoming	Edit	Rule ID
2025-08-25 10:25:58	st	192.	192	Policy > Security Policy > Incoming	Change	Rule ID
2025-08-25 09:56:38	st	192.	192	Network > PPPoE > PPPoE	Reconnect	Name
2025-08-25 09:56:27	st	192.	192	System Login	Login	Success
2025-08-22 16:46:28		192.	59.	System Login	Login	Success
2025-08-22 09:29:26		192.	59.	System Login	Login	Success
2025 08 21 11:23:13		192.	59.	System Login	Login	Success
2025 08 20 14:53:03		192.	59.	System Login	Login	Success
2025-08-20 11:06:06		192.	59.	System Login	Login	Success
2025-08-20 10:49:46		192.	59.	Configuration > Administrator > USB Backup Log	Save	Export log data to USB stick
				Configuration > Administrator > USB Backup Log	Save	Export log data to USB stick

▲ Figure 1

Log records in HDD

Servers generate a large amount of logs every day, including flow analysis logs, firewall protection logs, intranet protection logs, VPN logs, system logs, and more. Most devices can store logs locally for over 12 months.

Data Storing Time When System capacity usage reaches % (Range : 80 ~ 99) * the data storage time will be reduced automatically

Notification Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
URL Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
Software Blocking Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
Firewall Protection Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
IPS Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
WAF Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
Mail Log and Record	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/> ?
Audit Mail	<input type="text" value="12"/> Day(s) (Range : 1 ~ 999)	<input type="button" value="Change"/> ?
Spam Mail	<input type="text" value="12"/> Day(s) (Range : 1 ~ 999)	<input type="button" value="Change"/> ?
Deleted Mail	<input type="text" value="15"/> Day(s) (Range : 1 ~ 999)	<input type="button" value="Change"/> ?
WEB Record	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
FTP Record	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/> ?
Deleted F I P Files	<input type="text" value="12"/> Day(s) (Range : 1 ~ 999)	<input type="button" value="Change"/> ?
System Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
Flow Analysis Log	<input type="text" value="90"/> Day(s) (Range : 1 ~ 99)	<input type="button" value="Change"/>
DNS Query Log	<input type="text" value="30"/> Day(s) (Range : 1 ~ 99)	<input type="button" value="Change"/>
Sandstorm Record	<input type="text" value="30"/> Day(s) (Range : 1 ~ 99)	<input type="button" value="Change"/>
Dashboard Log	<input type="text" value="90"/> Day(s) (Range : 1 ~ 99)	<input type="button" value="Change"/>
Anomaly Log	<input type="text" value="12"/> Month(s)	<input type="button" value="Change"/>
Intranet Protection Log	<input type="text" value="30"/> Day(s) (Range : 1 ~ 99)	<input type="button" value="Change"/>

▲ Figure 2- UTM Data storing Time

HiGuard diskless models

HiGuard diskless models can store logs locally for over 3 months, and allow log backup to USB for later search. Besides, the system exports logs that **are about to be deleted** and saves them to a USB. The logs on the USB can then be mounted for extended retention, with a maximum retention period of up to 36 months. Therefore, it is important to regularly check the USB status (Figure 3).

These USB backups can also be mounted on other ShareTech UTM devices, but please note that if the firmware versions differ, the mounting process may fail.

Administrator Account Security Setting IP Address Clear Data **USB Backup Log**

Export log data to USB stick(Exported data can still be retained after a specified period of time.)

Log Retention Period Month(s)

Enable

Export Option

- Select All
- Notify Log
- Authentication Log
- Mail Log
- ZTA VPN Log
- DNS Query Log
- Intranet Protection Log
- URL Log
- DNS Filter Log
- WEB Virus Record
- L2TP Log
- Sandstorm Log
- Software Blocking Log
- IPS Log
- PPTP Server Log
- System Log
- Dashboard Log
- Firewall Protection Log
- WAF Log
- SSL/VPN Log
- Flow Analysis Log
- Anomaly Log

Mount USB Drives

Enable

USB Used Status 12% (1.7G / 15G)

Import Option

- [IPS Log](#) (2025-06-03 16:13:24 ~ 2025-07-25 18:49:30)
- [Mail Log](#) (2025-05-15 11:00:15 ~ 2025-05-27 23:00:14)
- [ZTA VPN Log](#) (2025-05-22 00:16:35 ~ 2025-05-22 00:52:21)
- [System Log](#) (2025-05-12 11:38:36 ~ 2025-07-28 18:37:21)
- [Flow Analysis Log](#) (2025-05-14 00:00:00 ~ 2025-08-27 23:59:57)
- [Sandstorm Log](#) (2025-07-13 00:00:00 ~ 2025-08-27 23:59:59)
- [Dashboard Log](#) (2025-05-14 00:00:00 ~ 2025-08-27 00:00:00)
- [Anomaly Log](#) (2025-07-14 07:33:49 ~ 2025-07-28 17:34:55)
- [Intranet Protection Log](#) (2025-07-15 15:39:23 ~ 2025-08-25 17:57:09)

▲ Figure 3 Configuration > Administration > USB Backup log

Exported USB data can still be retained after a specified period. (Figure 3)

For example, the system logs are retained on the device for 1 month and ZTA VPN logs are retained for 3 months. And then USB backup logs retention period is 36 months, then the system log can be retained on the USB for up to 35 months, while the ZTA VPN log can be retained on the USB for 33 months. (Figure 4)

PPTP Server Log	3 ▼ Month(s)	Change
SSL VPN Log	3 ▼ Month(s)	Change
L2TP Log	3 ▼ Month(s)	Change
ZTA VPN Log	3 ▼ Month(s)	Change
System Log	1 ▼ Month(s)	Change
Flow Analysis Log	1 Day(s) (Range : 1 ~ 99)	Change
DNS Query Log	1 Day(s) (Range : 1 ~ 99)	Change
Sandstorm Log	1 Day(s) (Range : 1 ~ 99)	Change

▲ Figure 4 Configuration > Administration > Clear Data > Data Retention Period

Supports Syslog Forwarding

Logs can be centralized to enterprise platforms. In cases of malware intrusion or unauthorized access, logs provide the critical basis for reconstructing attack paths. Forward logs to NAS or SIEM for long-term storage, audits, and forensics.

If you need detailed CEF documentation, please contact us.

Remote Connect Setup

Remote Connect Setup

Enable

Server IP

Server Port (UDP 514)

Device HostName

Log Setting

Log Format General CEF

Log Item

Select All

Object Application Control Log IPS Log Firewall Protection Log URI Filter Log Authentication Log DNS Filter Block Log

Advanced Protection Anomaly IP Analysis Log Intranet Protection Log

WAF WAF Log

Mail Security Mail Log

Content Record WEB Virus Record

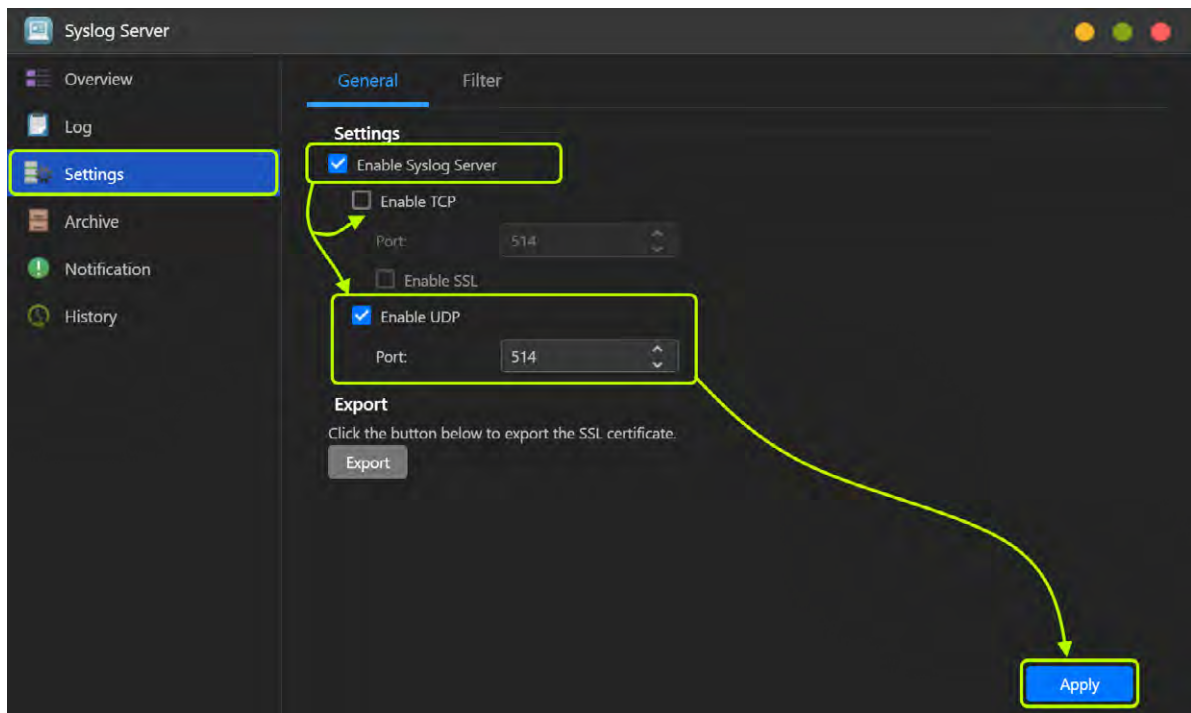
VPN PPTP Log L2TP Log SSLVPN Log IPsec Tunnel

ZTA VPN ZTA VPN Log

Log System Operation

Status Flow Analysis

▲ Figure 5

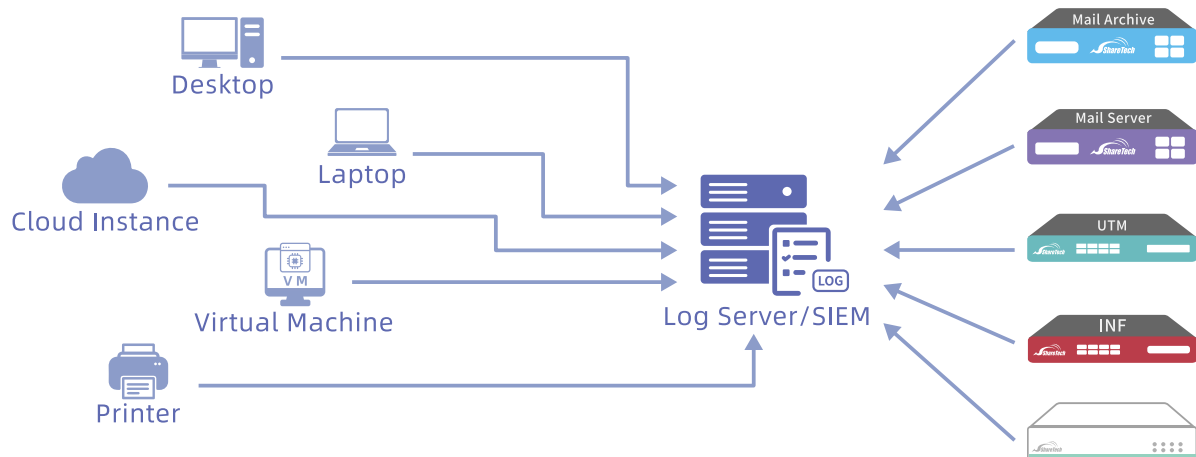


▲ Figure 6

Enhancing Security

Through log aggregation and analysis, enterprise can build user behavior models, integrate with SIEM, and transform defense from passive to proactive.

Alternatively, open-source tools like [Wazuh](#), [Graylog](#), or [LibreNMS](#) can be used to build enterprise monitoring platforms.



▲ Figure 7