



# Mail Server Solution

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

Sales Info  
sales@sharetech.com.tw

Tech Support  
help@sharetech.com.tw



## Syslog Forwarding for Secure Storage and Easy Auditing

### Why Logs Matter

Beyond regular system backups, don't forget log files. Logs help detect issues and provide evidence for audits and incident investigations. Regulations on email retention periods vary across countries, ideally backed up on separate systems.

The screenshot shows the 'Use Log' tab in the management interface. It includes filters for start and end times (2025-08-27 00:00 to 24:00), account selection (All), and login IP/keyword search. A breadcrumb trail shows the navigation path: System > Device Setting > External Mail Archive > Architecture > Authentication & Permissions > Mail Audit & Firewall > Mail Encryption > Anti-Virus > Log. The log table below displays the following data:

Time	Account	Login IP	Menu	Event	Status
08-27 11:27:21	sharetech		Auth	Sign In	Normal
08-27 08:01:31	SYSTEM		Device Setting > Time Setting	NTP Update	Error
08-27 07:01:31	SYSTEM		Device Setting > Time Setting	NTP Update	Error
08-27 06:01:31	SYSTEM		Device Setting > Time Setting	NTP Update	Error
08-27 05:01:31	SYSTEM		Device Setting > Time Setting	NTP Update	Error
08-27 04:01:50	SYSTEM		Device Setting > Time Setting	NTP Update	Error

## Local Log Retention on Mail Server (MS Series) and Mail Archive (MA Series)

Servers generate a large amount of logs every day, including mail logs, SMTP logs, POP3 logs, audit logs, personal info logs, SMTP Auth. Fail Log, and more.

MS Series and MA Series have different default retention settings for each log type.

- Mail Log
- ▶ Mail Log
- ▶ SMTP Communication Log
- ▶ POP3 Communication Log
- ▶ Mail Full Text
- ▶ Notice Mail Log
- ▶ System Event Log
- ▶ Mail Audit Log
- ▶ Personal Info. Protection Log
- ▶ Advanced Audit Log
- ▶ In/Out Prohibit Log
- ▶ Mail Verification Signature Log
- ▶ Mail Encryption Log
- ▶ Blocked Message
- ▶ CloudHDD Service Log
- ▶ Account Apply Log
- ▶ Large File Download Log
- ▶ Recipient No. Limit Notice Log
- ▶ Encryption User Apply Log
- ▶ User Last Login Log
- ▶ System Log
- ▶ Log Period Setting

Date Keep In System HDD	Setup
Audit & Filter Log	<input type="text" value="7"/> Day(s)
Spam Mail In Quarantine	<input type="text" value="7"/> Day(s)
Virus Mail in Quarantine	<input type="text" value="7"/> Day(s)
Sandstorm Mail in Quarantine	<input type="text" value="7"/> Day(s)
Mail Log	<input type="text" value="12"/> Month
POP3 Log	<input type="text" value="2"/> Month
Hyper Link Download Log	<input type="text" value="3"/> Month
System Event Log	<input type="text" value="6"/> Month
Cloud-HDD Service Usage Log	<input type="text" value="12"/> Month
Apply Account Log	<input type="text" value="24"/> Month
Encryption User Apply Log	<input type="text" value="30"/> Month
System Status Log	<input type="text" value="36"/> Month
	<input type="text" value="42"/> Month
	<input type="text" value="48"/> Month
	<input type="text" value="54"/> Month
	<input type="text" value="60"/> Month

▲ MS Series Log Period Setting

Mail Log > Log Period Setting > Data Keep In System HDD

### Log Life Cycle

[Log > Mail Log]	<input type="text" value="60"/>	<input type="text" value="Month"/>
[Log > Use Log] Searcher / User - Logging	<input type="text" value="72"/>	Month
[Log > Block Log]	<input type="text" value="36"/>	Month
[Log > Auth. Fail Log]	<input type="text" value="36"/>	Month
[Device Setting > SMTP Server] Send Fail Log	<input type="text" value="36"/>	Month
SeparateEmail	<input type="text" value="7"/>	Day

▲ MA Series Log Life Cycle

Device Setting > Mail Handle > Log Life Cycle

## Support for Syslog Forwarding

ShareTech devices support the standard Syslog protocol, allowing logs to be forwarded to a central platform.

- Keep local logs for quick checks.
- Forward historical logs to [NAS](#) or [SIEM](#) for long-term storage, audits, and forensics.

If you need detailed CEF documentation, please contact us.

Remote Server Settings	Setup
Remote Server Settings	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server IP	<input type="text"/>
Server Port	<input checked="" type="radio"/> UDP <input type="radio"/> TCP Port: <input type="text" value="514"/>
Device Server Name	<input type="text"/> <input type="checkbox"/> Use local host name (mail.pin-x.xyz)

  

Log Settings	Setup
Log Format	<input checked="" type="radio"/> General <input type="radio"/> CEF (If you have detailed document requirements, please call your distributor or service vendor.)
Log Item	<input type="checkbox"/> All <input type="checkbox"/> Mail Log > System Event Log <input type="checkbox"/> Mail Log > Mail Log <input type="checkbox"/> Mail Log > Blocked Message <input type="checkbox"/> Mail Log > System Log > Pop3/Imap/WebMail Log
Log Collection	Every <input type="text" value="60"/> Minute(s)

▲ MS Series Remote Recording Server Setting  
System Management > Remote Recording Server

Remote Server Settings

Remote Server Settings  ON  OFF

Server IP

Server Port  UDP  TCP Port:

Device Server Name   
 Use local host name (ma.demo.sharetech.com.tw)

---

Log Settings

Log Format  General  CEF (If you have detailed document requirements, please call your distributor or service vendor.)

▲ MA Series Remote Recording Server Setting  
Device Setting > Remote Recording Server

Syslog Server

General Filter

Settings

Enable Syslog Server

Enable TCP  
Port: 514

Enable UDP  
Port: 514

Export  
Click the button below to export the SSL certificate.

▲ Syslog Server

## Enhancing Security

For enterprises that deploy a [SIEM system](#), logs can trigger alerts via event correlation, behavior analysis, and anomaly detection—boosting visibility and response efficiency.

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

