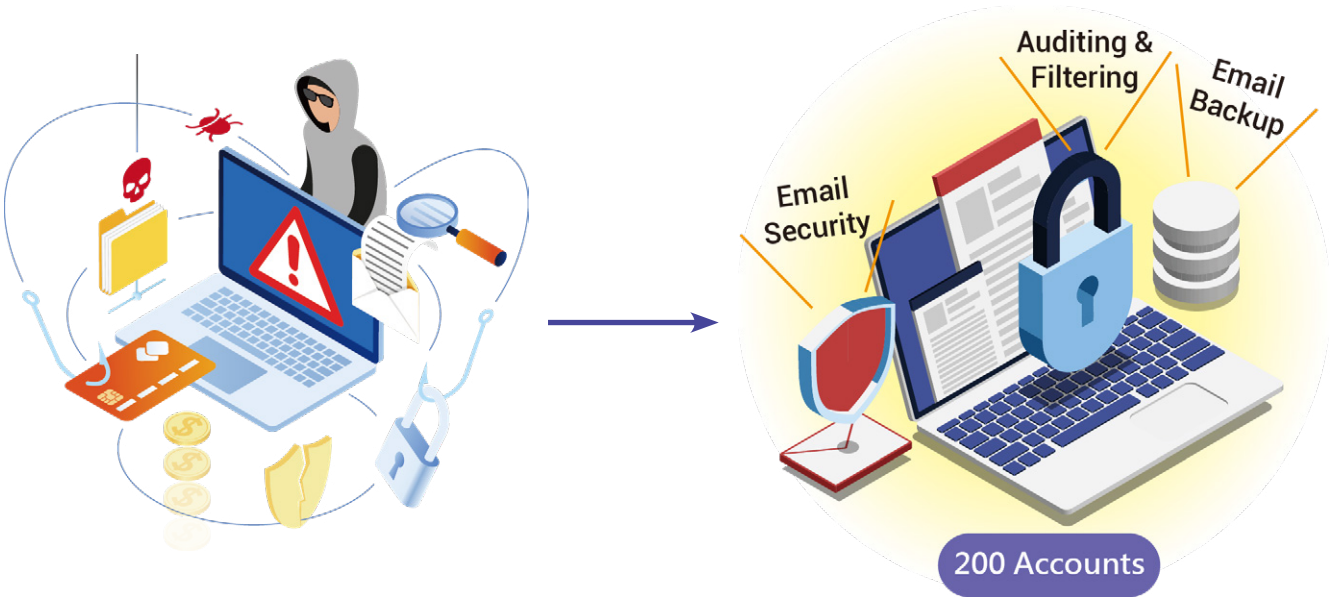
Hardware-Based Mail Server

MS-6410X

Email is essential to business communication. As email traffic and security threats continue to grow, SMBs need a stable, high-performance, and secure email service.

ShareTech's hardware-based mail server, MS-6410X, is designed for environments with fewer than 200 users. It integrates email security, mail logging & backup, email auditing & filtering, and mobile email access, making it ideal for SMBs, government agencies, and schools.

Trusted by tens of thousands of enterprise users in Taiwan, ShareTech continues to deliver efficient and reliable email solutions for evolving market needs.



2026.06

ShareTech sales@sharetech.com.tw | www.sharetech.com.tw | help@sharetech.com.tw

Features

Email Security

Email Firewall

The email firewall provides in-depth email inspection through abnormal traffic detection, authentication detection, and SMTP SASL. It filters email threats that traditional firewalls may not be able to block.

With multi-layer filtering, it effectively helps protect businesses against spam, mass mailing attacks, Trojans, dictionary attacks, and hacker intrusions, ensuring secure and reliable enterprise email operations.

Mail Gateway

ShareTech Mail Gateway can be securely deployed in front of an existing mail server to deliver high-performance spam filtering. Powered by OS64 3.0 and multi-layer email scanning, it helps block spam, viruses, malicious emails, phishing, relay abuse, and spyware-generated messages, strengthening email security and service quality.

Multi-Layered Spam Filtering

MS-6410X provides multiple spam filtering mechanisms, including greylisting, fingerprint detection, blacklist/whitelist settings, reverse IP lookup, SPF, DKIM, DMARC, and sender anomaly.

It also supports URL filtering, abnormal sending detection, and compressed attachment scanning for ZIP/RAR files. Emails that violate security rules will be filtered or blocked, reducing email-based threats.

Spam Mail Auto-Learning System

ShareTech's R&D team uses advanced intelligent learning technologies to analyze inbound and outbound email data and identify hidden threats. By automatically learning the characteristics of SPAM and HAM emails through a spam classification engine, the system helps detect thousands of potential malware and virus patterns.

Through cloud-based intelligent learning, data sharing, and connected threat analysis, ShareTech helps organizations block attacks and trace malicious sources more effectively.

Protection Against Ransomware

MS-6410X allows administrators to set rules to inspect email subjects, attachments, and file extensions, helping quarantine or block suspicious emails before they cause ransomware infections.

In addition to attachment-based threats, MS-6410X analyzes URL, IP, domains to block ransomware attacks and strengthen email security.

Dual Antivirus Engines

MS-6410X includes the **ClamAV engine** to detect over 4 million viruses, worms, and Trojans across email, web, and FTP traffic. Virus signatures are updated automatically every day to keep protection current with minimal cost.

Organizations can also add **ShareTech engine** for enhanced email security, along with complete virus filtering reports, logs, and abnormal alert notifications.

SPF/DKIM/DMARC Authentication

Sender Policy Framework (SPF) defines a process to validate an email message sent from an authorized mail server to detect forgery and prevent spam.

DomainKeys Identified Mail (DKIM) allows an organization to claim responsibility for a message in a way that the recipient can validate.

Moreover, **Domain-based Message Authentication, Reporting and Conformance (DMARC)** is added to allow a sender's domain to indicate that their emails are authenticated by either SPF or DKIM and tell the receiving mail server what to do if neither of those authentication methods passes.

AI Spam (Subscription)

AI Spam uses ShareTech's proprietary Chinese word segmentation database to analyze email content and sender behavior, helping distinguish legitimate emails from malicious messages and reduce the risk of phishing attacks. With continuous automatic learning, the system can identify zero-day phishing emails and deliver up to 99.5% detection accuracy.

"Digital Signature" Email Verification

MS-6410X helps prevent email fraud and message tampering by adding a digital signature and original email verification link to outgoing messages. Recipients can use the link to connect back to the sender's mail server, verify the original email content, and confirm that the sender and message details match.

Shared Email Signature (Disclaimer)

MS-6410X can automatically add a shared company signature and email disclaimer to outgoing emails. Administrators can customize signature content by domain and define specific accounts or IP addresses that are excluded from the shared signature policy.

Email Auditing, Recording, and Backup

Email Content Auditing & Filtering

MS-6410X automatically scans and filters emails based on corporate policies to detect inappropriate email behavior. It supports full email content scanning, keyword filtering by inbound or outbound domains, and flexible actions such as quarantine, deletion, sender IP blocking, notifications, and copy forwarding. This helps administrators enforce internal policies and comply with corporate and regulatory requirements.

Personal Info. Filtering (Optional)

MS-6410X provides optional personal info. filtering to help organizations manage sensitive information in emails. Administrators can configure audit rules for personal data such as ID numbers, credit card numbers, phone numbers, mobile numbers, and dates of birth.

Complete Email Recording & Backup

MS-6410X records all inbound and outbound emails, including attachments, and can automatically back up data to a network share or FTP server. Administrators can search emails, review blocking reasons, and access externally backed-up email records for tracking and management.

ShareTech sales@sharetech.com.tw | www.sharetech.com.tw | help@sharetech.com.tw

System Backup and Recovery

MS-6410X supports scheduled system backups and USB backup and recovery. In the event of a local hard drive failure, administrators can restore the system from a USB backup, helping reduce downtime and simplify system maintenance.

Various Management Tools

Seamless Email Migration

MS-6410X supports seamless email migration via POP3 and IMAP, automatically transferring accounts and emails from the existing mail server without requiring users to re-enter their credentials. Administrators can also create user accounts manually or integrate with AD/LDAP accounts for more flexible account management.

Decentralized Management

MS-6410X allows organizations to define administrator permissions based on departmental roles and responsibilities. Access rights can be assigned for email logs, user management, system management, log search, spam management, traffic statistics, POP3 proxy, and more.

Email Encryption with TLS

MS-6410X supports TLS encryption for SMTP, POP3, and IMAP connections. This helps protect email data during transmission between user devices and the mail server, reducing the risk of interception.

Central/Branch Architecture (Branch)

MS-6410X supports central-branch mail architecture for organizations with multiple locations or high-volume email traffic. It helps accelerate email delivery while synchronizing databases, accounts, and mail communication logs between the central and branch servers through encrypted channels.

All email records, including outbound, inbound, and inter-branch emails, are consolidated into the central server database, providing reliable records for tracking and auditing when needed.

High Availability and Remote Backup (Optional)

MS-6410X supports active/standby high availability to help maintain continuous email service. If the Master server experiences a hardware failure, the Slave server automatically takes over email processing and becomes the primary server.

For remote backup, mail servers can be deployed at headquarters and the branch office. If the headquarters one fails, the system can automatically switch to the branch one to keep email services running without interruption.

Comprehensive Logs

MS-6410X records user mailbox login activity and administrator operations. Administrators can search various logs, including mail, SMTP, POP3, email auditing, blocking, system events, and more. Log retention periods can be configured, and full-text search is supported for faster tracking and troubleshooting.

Diverse Statistical Reports

MS-6410X provides clear and easy-to-read reports, including top N mail usage, account usage, top N login usage, mail type, top N of quarantine, top N dangerous password, top N of spam mail, and other visual statistics to support efficient system management.

POP3 Proxy

MS-6410X provides POP3 proxy support, allowing users to collect emails from multiple accounts through a single local mailbox. This helps users manage important messages more efficiently without switching between different platforms.

Threat Intelligence Dashboard (Optional)

The Dashboard transforms complex data into clear visual charts. It provides real-time monitoring, audit statistics, user behavior analysis, blocking records, account authentication data, and various security reports.

Easy Management

MS-6410X supports web-based configuration and firmware updates. Administrators can use built-in network tools including Ping, Traceroute, DNS lookup, port lookup, and test email delivery.

Personal Webmail

Personal Webmail

MS-6410X includes 10GB Webmail with an Outlook Express-style interface, allowing users to get started quickly. Users can use it through a browser from anywhere, with different tools and encrypted transmission to ensure secure email communication.

Cloud HDD

Cloud HDD uses the storage space of MS-6410X to provide users with a shared file space. Files can be uploaded or downloaded through Webmail, with permission controls such as read-only, read/write, or forbid access.

Download records, including time, username, and IP address, are retained to help ensure file-sharing security. When email attachments exceed the size limit, large files can be converted into download links for recipients.

Calendar

Webmail includes a calendar tool to help users manage daily activities and schedules. It also supports group calendars, allowing teams to keep track of departmental events. The Webmail calendar is available through both the web interface and mobile apps for iOS and Android, with schedule synchronization across devices.

Outlook Contact & Google Calendar Sync (Optional)

ShareTech provides Outlook Connector, allowing contacts (including groups) to synchronize between Webmail and Outlook. Updates made in either interface can be synchronized quickly and regularly for a smoother email experience.

ShareTech Calendar can also integrate with Google Calendar (optional), allowing users to view meetings, tasks, and personal schedules on a single page for easier planning.

Delayed Sending & Email Recall

Webmail supports delayed sending, allowing users to set a delay time such as 30 seconds, 1 minute, or longer. During this period, users can cancel the email, make changes, and send it again.

Email recall is available when both the sender and recipient use the same mail server. If not, the system will send a notification email to the recipient instead.

ShareTech sales@sharetech.com.tw | www.sharetech.com.tw | help@sharetech.com.tw

Authentication: Two-Step OTP & Passwordless Biometrics

MS-6410X supports multi-factor authentication to help prevent unauthorized access.

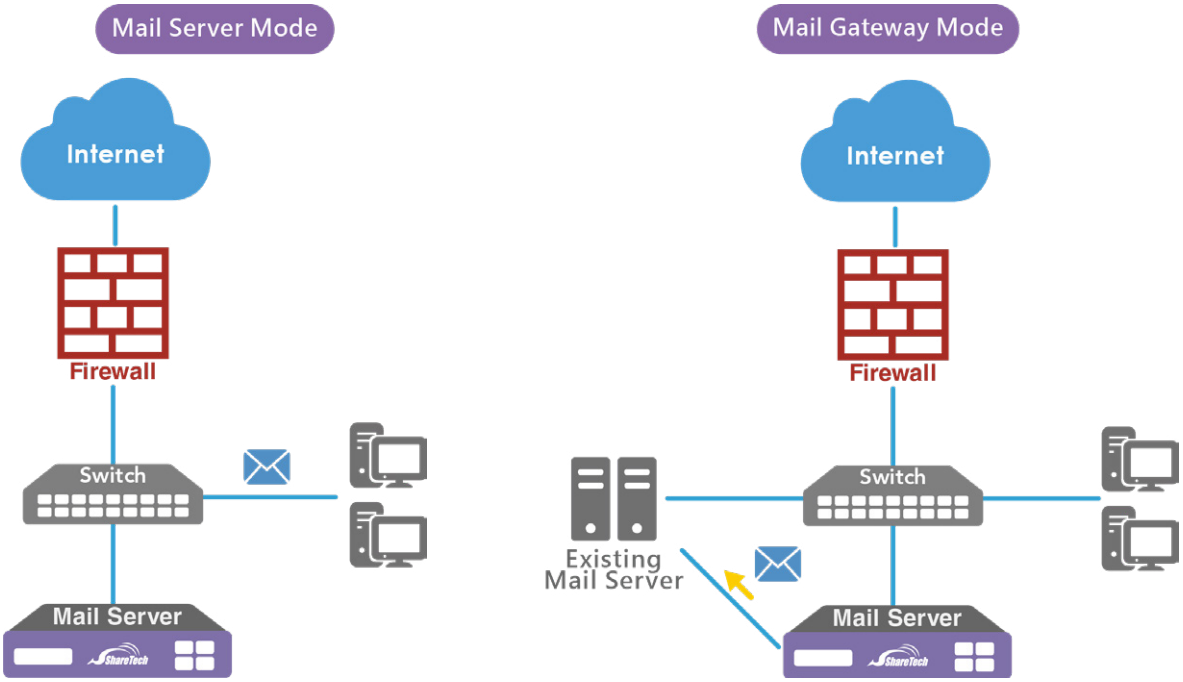
Two-step authentication: it provides real-time OTP codes via email or third-party authenticators such as Google Authenticator or Microsoft Authenticator.

Passwordless authentication (Biometrics): ShareTech Authenticator supports passwordless biometric login, delivering a faster and more secure authentication experience.

Architecture

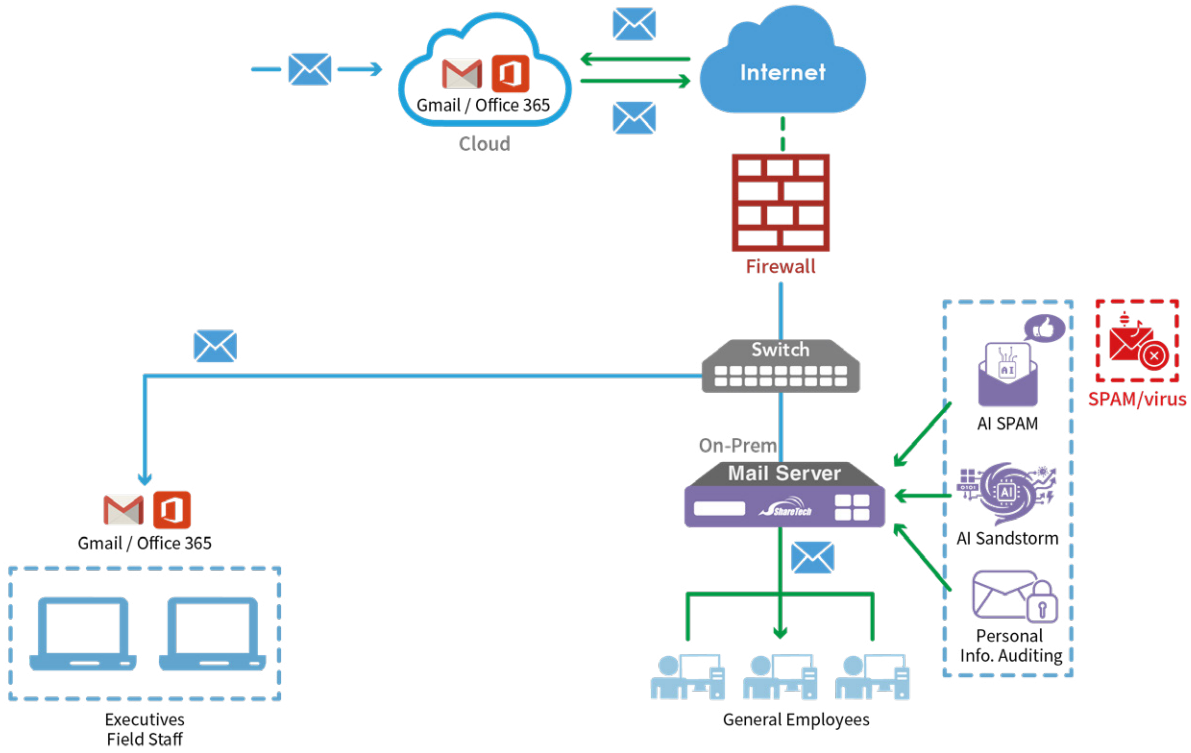
Flexible Deployment with Mail Server and Gateway Modes

- In standard **mail server mode**, MS-6410X can operate as a complete mail server and provide users with Webmail access.
- In **gateway mode**, ShareTech Mail Server can be deployed in front of an existing mail server to provide antivirus, anti-spam, and email auditing services.



Hybrid Cloud Email Architecture

- ShareTech Mail Server can work with Google Workspace or Microsoft 365 in a hybrid cloud setup.
- Organizations can host general employee email accounts on premises while using cloud accounts for executives or field staff for convenient mobile access, reducing licensing costs and overall email system expenses.



ShareTech sales@sharetech.com.tw | www.sharetech.com.tw | help@sharetech.com.tw

Model		MS-30X	MS-6400X	MS-6410X	MS-6420X	MS-6430X	MS-6440L
Hardware							
Memory		4G	4G	4G	4G	8G	16G
Storage		500G	500G	1TB	1TB	2TB	2TB x 3
Disk Array		X	X	X	X	X	RAID 0 / 1 / 5
Form Factor		Desktop	1U	1U	1U	1U	1U
LCM		X	X	•	•	•	X
Port Configuration		LAN	LAN / HA	LAN / HA	LAN / HA / iSCSI	LAN / HA / iSCSI	LAN / HA
Network Interfaces		1 x GE	2 x GE	2 x GE	3 x GE 2 x 10G SFP+	3 x GE	1 x GE
Capacity							
Accounts		30	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Suggested Users		Under 30	Under 100	Under 200	Under 200	Under 400	600 - 1,000
Software Features							
Basic Setup	Multiple Domains	5	5	•	•	•	•
	Email Migration	•	•	•	•	•	•
	POP3 Proxy (Admin / User)	• / X	• / X	• / X	• / 5	• / 10	• / Unrestricted
	SMTP Proxy	X	X	X	•	•	•
	Email Encryption	X	X	X	•	•	•
	Mail Gateway	X	X	•	•	•	•
	Mail Content Authentication	X	X	•	•	•	•
	Queue Management	•	•	•	•	•	•
Antivirus & Spam Filtering	ClamAV	•	•	•	•	•	•
	ShareTech Engine	Subscription	Subscription	Subscription	Subscription	Subscription	1-Year Support
	Rspamd	•	•	•	•	•	•
	Blacklist and Whitelist / Greylist	• / •	• / •	• / •	• / •	• / •	• / •
	IP Reputation	•	•	•	•	•	•
	URL Filtering	•	•	•	•	•	•
	Bayesian Filtering	•	•	•	•	•	•
	Spam Auto-Learning	•	•	•	•	•	•
	Spam Learning and Sharing	•	•	•	•	•	•
	SPF, DKIM, DMARC	•	•	•	•	•	•
	AI Sandstorm	X	X	X	Subscription	Subscription	Subscription
	*AI Spam	X	X	Subscription	Subscription	Subscription	Subscription
Auditing & Recording	Policy	•	•	•	•	•	•
	Mail In / Out Auditing	•	•	•	•	•	•
	Content Filtering	•	•	•	•	•	•
	Personal Info Filtering	Optional	Optional	Optional	•	•	•
	Mail Record	•	•	•	•	•	•
Mail Firewall	SMTP SASL	•	•	•	•	•	•
	DNS Defense	•	•	•	•	•	•
	Abnormal Mail Delivery Detection	•	•	•	•	•	•
	Trusted IP List	•	•	•	•	•	•
Account	Account Registration and Group Management	•	•	•	•	•	•
	Decentralized Management	•	•	•	•	•	•
	Account Creating Methods (Local / AD / LDAP)	•	•	•	•	•	•
Backup	FTP / Samba / USB	•	•	•	•	•	•
	iSCSI	X	X	X	•	•	X
	Personal Mail Recovery	•	•	•	•	•	•
	USB Backup Drive Data Recovery	•	•	•	•	•	•
Management	SSL Certificate	•	•	•	•	•	•
	UPS	•	•	•	•	•	•
	HA / Off-Site Backup	X / X	• / X	• / Optional	• / •	• / •	• / •
	Central / Branch Architecture	X	Branch	Branch	Central / Branch	Central / Branch	Central / Branch
	Hard Disk Checking	•	•	•	•	•	•
	DNS Server	•	•	•	•	•	•
	Web Server	X	X	•	•	•	•
	Log	•	•	•	•	•	•
	Report	Optional	Optional	•	•	•	•
	E-paper	Optional	Optional	•	•	•	•
	Dashboard	X	X	Optional	Optional	Optional	Optional
Webmail	Capacity (MAX. 100G)	10GB	10GB	10GB	30GB	30GB	100GB
	Identity Authentication (2FA / Passwordless)	•	•	•	•	•	•
	Auto-Reply / Forward	•	•	•	•	•	•
	Mail Retrieving / Delayed Sending	•	•	•	•	•	•
	Cloud HDD / Bulletin / Calender	• / • / •	• / • / •	• / • / •	• / • / •	• / • / •	• / • / •
	Google Calendar Sync	Optional	Optional	Optional	•	•	•
	Mail Rule	•	•	•	•	•	•
	Mail APP (iOS & Android)	•	•	•	•	•	•

Note*: Memory must be at least 8 GB.