



Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Microsoft Exchange Server Security Best Practices

Introduction

Many organizations rely on Microsoft Exchange to perform critical communications, necessitating paramount protection from malicious actors. Reported abuse and exploitation of vulnerabilities within Exchange further demonstrates the importance of implementing security best practices. [1], [2], [3], [4], [5], [6], [7], [8], [9] This paper—authored by the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), and Canadian Centre for Cyber Security (Cyber Centre)—provides security best practices for administrators on hardening on-premises (on-prem) Exchange. This document outlines several security best practices but is not an all-inclusive hardening guide. Active monitoring for compromises and planning for potential incidents and recovery, while not discussed in this guidance, are equally important areas for Exchange.

The threat to Exchange servers remains persistent. Exchange environments are continuously targeted for compromise and should be considered under imminent threat. As certain Exchange Server versions have recently become end-of-life (EOL), environments with these versions are at a heightened risk of compromise. The authoring agencies strongly encourage organizations to take proactive steps to mitigate risks and prevent malicious activity. The authoring agencies recommend the following prevention and hardening defenses as critical for Exchange servers to mitigate various compromise techniques and protect the sensitive information and communications they manage.

This guidance specifically provides recommendations for on-prem Exchange servers; for recommendations about on-prem Exchange Servers as part of hybrid Exchange instances, please see CISA's Emergency Directive 25-02: Mitigate Microsoft Exchange Vulnerability. [10]

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules

Enforce a prevention posture

Organizations should enforce a prevention posture to address cyber threats toward Exchange servers in on-prem network environments. This prevention posture incorporates cybersecurity guiding principles—such as deny-by-default, least privilege, timely updates, and minimizing the attack surface—to proactively protect these systems and their operating environments and reduce their exposure to cyber risks.

Maintain security updates and patching cadence

The most effective defense against exploitation is ensuring all Exchange servers are running the latest version and Cumulative Update (CU). [11] Administrators can leverage the Exchange Update Step-by-Step Guide, Health Checker, and SetupAssist tools to keep Exchange servers updated and in a ready state to adopt other defenses (e.g., Extended Protection as discussed later in the Configure Extended Protection section). [12], [13], [14] Delaying or failing to apply security patches compounds the risk over time of known vulnerability exploitation, putting the whole network at risk. [15]

The update cadence for Exchange Server is two CUs per year and monthly for security and hotfix updates. [16], [17] Malicious cyber actors can quickly develop exploits within days of patch releases, so updates should be applied as soon as practicable. When an update becomes available, Microsoft posts information about it on the Exchange Server build numbers and release dates page of the Exchange Server documentation. [18], [19] Microsoft may release interim mitigations and defensive tools for Exchange Server between discovery of a vulnerability and issuance of a patch. When that occurs, Microsoft posts information about the interim mitigations and tools on the Exchange Team Blog and, depending on the kind of mitigation, on the Exchange Emergency Mitigation (EM) service page. [20], [21] Applying these Microsoft developed and approved defenses minimizes exploitation risks to Exchange from known vulnerabilities and exploits.

Migrate end-of-life Exchange Servers

Microsoft Exchange Server Subscription Edition (SE) is the sole supported on-prem version of Exchange after Microsoft ended support for previous versions of Exchange on October 14, 2025. [22], [23] To avoid the cybersecurity risks associated with using an EOL product, organizations that are running an unsupported version of Exchange should migrate to Exchange Server SE or an alternative supported email server

software or service. When migrating, organizations should consider support for the organization's email clients (e.g., Outlook, Microsoft 365 Apps for Enterprise, Mozilla Thunderbird, Apple Mail, etc.) to ensure compatibility and maintain a strong overall email infrastructure cybersecurity posture. [24]

Running supported versions of software is critical to ensure timely mitigation of newly discovered vulnerabilities. If unsupported versions of Exchange Server must be used for a time (possibly due to extended migration timelines to Exchange Server SE or an alternative supported email server software or service), its attack surface should be limited as much as possible and not directly exposed to the Internet. Consider isolating the Exchange Server in a dedicated network segment and only using it for limited, internal communication. If needed for external communication, consider utilizing a separate and supported email security gateway service as an intermediary to protect the Exchange Server from direct Internet connections. For U.S. federal civilian executive branch (FCEB) agencies, follow the requirement in ED 25-02 to disconnect EOL Exchange servers (as applicable). [10]

Ensure Emergency Mitigation Service remains enabled

Microsoft's interim mitigations are delivered through the Exchange Emergency Mitigation (EM) Service. EM is an automatically installed service on Exchange Mailbox servers and requires outbound connectivity to Microsoft's cloud-based Office Config Service (OCS).[1] The service actively applies mitigations to Exchange via the OCS. The deployed mitigations include Microsoft Internet Information Services (IIS) URL Rewrite rules—which blocks specific patterns of malicious HTTP requests—and the disabling of vulnerable Exchange services and App Pools. The Windows Event log and a separate Exchange log file[2] record the mitigation activities. Proactively ensuring the EM service remains enabled on an Exchange deployment is critical for mitigating cyber threats identified by Microsoft and maintaining the integrity and protection of sensitive information.[3] [21]

[1] Microsoft began automatic installation of EM with Exchange Server 2016 and 2019 with September 2021 CU.
[2] The Windows Application event log is in the \V15\Logging\MitigationService folder in the Exchange installation directory.
[3] Note that according to Microsoft's website, "the EM service isn't a replacement for Exchange Security Updates. However, it's the fastest and easiest way to mitigate the highest risks to internet-connected, on-premises Exchange servers before updating." [21]

Apply security baselines

Software and operating system security baselines help maintain a consistent security configuration across an organization's network infrastructure. Email communication on a network requires a mail server, mail clients, and an underlying operating system at a minimum; each component must have a security baseline applied to heighten the overall security posture of the email infrastructure.

As part of the configuration control process, administrators should apply and maintain the Exchange Server baseline, Windows security baselines, and applicable mail client security baselines. Maintaining a software baseline enables administrators to identify systems not conforming to the baseline and incorrect security configurations, as well as apply rapid remediations that reduce the attack surface available to an adversary. The Defense Information Systems Agency (DISA),[4] the Center for Internet Security (CIS), and Microsoft have released security baselines for Exchange Server and Windows.

Table 1: Security baselines for Exchange Server and Windows

Provider	Baseline
DISA	Exchange Server Security Technical Implementation Guide (STIG)
DISA	Microsoft Office System 2016 STIG
DISA	Microsoft Office 365 ProPlus STIG
CIS	Benchmark for Exchange
CIS	Microsoft Office Benchmark
Microsoft	Microsoft 365 Apps for Enterprise Security baseline

Enable built-in protections

Protecting Exchange servers requires a holistic approach to cover all components involved in handling and delivering email. When not using third-party antivirus, anti-malware, and Endpoint Detection and Response (EDR) capabilities, built-in or additional protection features from Microsoft or third parties should be enabled to contribute to a defense-in-depth approach:

- Antivirus, such as Microsoft Defender Antivirus (MDAV),
- Windows Antimalware Scan Interface (AMSI),
- Attack Surface Reduction (ASR),
- AppLocker and App Control for Business,

[4] Specific STIGs can be found using the search field on DISA's STIG web site at https://www.cyber.mil/stigs.

- Endpoint Detection and Response, and
- Exchange Server's anti-spam and anti-malware features.

MDAV, the built-in antivirus on Windows, detects and responds to malware and other cyber threats to Exchange servers. Exchange Server has integrated an AMSI capability to enable any anti-malware product that supports AMSI, including MDAV, to monitor content in HTTP requests received by the Exchange server. [25] Microsoft has a recommended antivirus exclusion list that can be configured to minimize incompatibilities and performance impacts from anti-malware products. [26] MDAV also includes a built-in ASR rule called "Block Webshell creation for Servers" to block webshell script creation by cyber threats on compromised servers with the Exchange Server role. [27]

Application Control for Windows (App Control for Business and AppLocker) is an important security feature that strengthens the security of Exchange servers by controlling the execution of executable content. [28], [29] Leveraging these application control features will proactively deny execution not otherwise approved, enhancing the cybersecurity posture of Exchange servers.

In addition to the built-in Windows protections described above, implementing an EDR tool can provide additional visibility, detection, and protection capabilities to defend Exchange Server and Windows Server from advanced cyber threats. Most EDR tools can detect and prevent certain sophisticated cyber techniques that regular antivirus and anti-malware tools may not, and can aid in the investigation of and response to suspicious activities and incidents.

To help prevent recipients from receiving malicious emails, enable and configure other built-in protection features available within Exchange servers, such as the anti-spam and anti-malware features. [30], [31]

However, on-prem Exchange does not have built-in support for the Domain-based Message Authentication Reporting and Conformance (DMARC), Sender Policy Framework (SPF), or DomainKeys Identified Mail (DKIM) standards for email authentication to prevent certain types of spam and email masquerades. Add support for these standards when using Exchange by:

- manually setting DMARC and SPF records in DNS to match the Exchange servers' information for outbound email,

- using third-party Exchange add-ons to add DKIM signatures to outbound email, and/or
- routing email flows through external services for inbound and outbound email.

These protections add layered defenses and expand defensive coverage across Exchange Server and an organization's email.

Restrict administrative access

Only authorized, dedicated administrative workstations should be permitted to access Exchange administrative environments—i.e., the Exchange Admin Center (EAC) and remote PowerShell. Since EAC is web-based and hosted alongside Outlook on the Web (formerly called Outlook Web App or OWA), restricting access to EAC requires configuring Client Access Rules to disable access to EAC. [32] Then, access to the EAC website and remote PowerShell can be restricted by host firewall rules on the Exchange server, while still allowing the other ports and protocols required for mail flow and client access. [33]

Harden authentication and encryption

Authentication and encryption provide identity verification and confidentiality assurances. This section discusses the authentication and encryption security capabilities within Exchange. Hardening authentication and encryption is critical for ensuring confidentiality, integrity, and availability of communications on an Exchange server, while protecting sensitive data from unauthorized access or additional cyber threats.

Configure Transport Layer Security

Transport Layer Security (TLS) encryption protects data integrity and prevents techniques such as replay, data tampering, or impersonation. Exchange uses TLS for internal and external server communications. TLS encryption protects emails in transit, as well as user connections to the Exchange server (e.g., from Outlook or to Outlook on the Web). Refer to Microsoft's Exchange Server TLS configuration best practices and use the latest supported TLS configuration consistently across all Exchange servers. [34] Consider using Microsoft's Exchange Health Checker script for assistance checking the configurations. [13] Restart Exchange Server after any change in the TLS configuration to activate the new configuration. Consistent TLS settings will minimize

troubleshooting difficulties, unify the security posture of email communications, and avoid downgrading to weaker cryptographic protection.

Configure Extended Protection

Extended Protection (EP) provides additional authentication defenses against Adversary-in-the-Middle (AitM), relay, and forwarding techniques. [35], [36] EP enhances a TLS connection with a Channel Binding Token (CBT) and Service Binding to link the user's authentication information to a unique TLS session. [37], [38] If a malicious actor attempts to relay stolen credentials from a TLS session, the CBT of the actor's session is rejected due to a mismatch of the session information with the server.

Consistent TLS settings and New Technology LAN Manager (NTLM) configurations are required for EP to operate correctly across all existing Exchange servers. NTLM must be disabled or configured to only use NTLMv2 while refusing older NTLM versions. [35] Although Microsoft has deprecated NTLMv2 on Windows Server, the protocol will continue operating by default until its future removal. [39] EP is enabled by default beginning in newly installed versions of Exchange Server 2019 CU14. Consider using Microsoft's Exchange Health Checker to confirm EP's prerequisites are met prior to enabling EP on Exchange servers. [35], [40]

Configure Kerberos and SMB instead of NTLM

Exchange leverages the Kerberos, NTLM, and Server Message Block (SMB) protocols for secure authentication and communication purposes, such as in the context of Exchange Web Services and database availability groups. [41], [42] SMBv1 and NTLMv1 are disabled in the latest versions of the Windows (server and client) operating system and deprecated in earlier versions. [36], [39], [43], [44], [45] Organizations should audit for the prevalence of these legacy protocols within their enterprise networks and migrate towards modern secure protocols to ensure trusted mail flow. [33], [46], [47], [48], [49]

Organizations should start preparing for the removal of all NTLM support by enabling NTLM auditing and investigating continued use of NTLM. [50], [51], [52] Identify the third-party software (e.g., mail and Messaging Application Programming Interface [MAPI] clients), Exchange installations, or Windows instances that require upgrading or correcting configurations to be able to use Kerberos authentication (MAPI over HTTP)

instead of NTLM. [53] Kerberos improvements in Windows 11 remove NTLM dependencies. CU1 for Exchange Server SE will replace NTLMv2 with Kerberos, making Kerberos the default authentication protocol for communication among Exchange Servers. [54]

Configure Modern Authentication and multifactor authentication

Beginning with Exchange Server 2019 CU13, Exchange can use Modern Authentication (alternatively called Modern Auth), leveraging OAuth 2.0 and enabling multifactor authentication (MFA) with Active Directory Federation Services (ADFS) as a Security Token Service. [55] For organizations that use cloud-based Microsoft Entra ID identities, Hybrid Modern Authentication can be configured for access to on-prem Exchange mailboxes using Modern Authentication. [56] Modern Authentication replaces the deprecated Basic Authentication protocol and is included in supported Outlook clients to address the risk of clear text credentials used by Basic Authentication. Once Modern Authentication is configured, Basic Authentication should be disabled. [57] Modern Authentication only grants a client access to a user's mailbox after:

- ADFS authenticates the user with credentials or MFA,
- ADFS generates an access token, and
- Exchange validates access to the mailbox based on the token. [55]

Configure certificate-based signing of PowerShell serialization

The Exchange Management Shell (EMS) is an Exchange administrator PowerShell environment used to manage Exchange locally or remotely. PowerShell uses data serialization (i.e., converting .NET objects into a stream of bytes) when exchanging information remotely between sessions. Enabling certificate-based signing provides protection from unauthorized serialization payload manipulations. [58] Exchange allows administrators and users to have remote PowerShell access. Unless needed, remote PowerShell access by users should be disabled to reduce Exchange Server’s attack surface. [59] Beginning with the November 2023 Exchange Server Security Update (SU), certificate signing of serialized data has been enabled by default. All Exchange servers within a network must have this defense enabled and use the same active Exchange Server Auth Certificate.

Configure Strict Transport Security

Enable HTTP Strict Transport Security (HSTS) to force all browser connections to be encrypted with HTTPS. [60] HSTS works by sending a special HTTP response header from the server to the browser, called Strict-Transport-Security (STS). This header directs a browser to only connect to the server using encrypted HTTPS for a specified amount of time. Once a browser receives this header, it automatically changes any unencrypted HTTP requests for the site to HTTPS requests instead. Using HSTS to force HTTPS for web browser connections to Outlook on the Web or EAC mitigates certain AitM techniques. Administrators should enable and configure HSTS per Microsoft's recommendation to reduce risks from unencrypted HTTP connections. [60]

Similarly, all Simple Mail Transfer Protocol (SMTP) connections for sending and receiving emails between Exchange servers and external mail servers should be encrypted and authenticated. Some encryption and authentication requirements can be set in Exchange on the send and receive connectors using TLS configuration options. However, on-prem Exchange does not support the DNS-based Authentication of Named Entities (DANE) or Mail Transfer Agent Strict Transport Security (MTA-STS) standards for signaling authentication and encryption requirements with other mail servers. Instead, DANE and MTA-STS can be set up separately from Exchange to match Exchange's configuration and certificate information to secure inbound email received by Exchange from other servers. To secure outbound email using DANE or MTA-STS, it is necessary to route email from Exchange through a separate third-party service that supports these standards.

Configure Download Domains

Download Domains mitigates Cross-Site Request Forgery (CSRF) techniques via Outlook on the Web by ensuring attachments load from a different subdomain than the subdomain used for Outlook on the Web. With Download Domains configured, malicious cyber actors cannot steal the authentication cookies set by browsers because the new session does not have access to the authentication cookie for Outlook on the Web. [61]

Use role management and split permissions

Exchange Server has a Role Based Access Control (RBAC) model for managing the access and privileges of users and administrators, represented by management roles.

[62] Administrators traditionally used highly privileged Active Directory (AD) Domain Administrator accounts to manage both AD and Exchange. With this configuration, an Exchange compromise often leads to domain compromise. Instead, the management responsibilities should be separated to achieve the least privilege principles described in NSA's Defend Privileges and Accounts. [63] Exchange Server enables separation of duties and least privilege through Exchange's RBAC model for split permissions. [64] Organizations should implement split permissions to leverage RBAC security benefits and reduce over-privileged users and administrators.

Use P2 FROM header manipulation detection

The P2 FROM header within the email exchange process was susceptible to spoofing by permitting forged senders to be displayed as legitimate senders by email clients. Starting with the November 2024 SU, Exchange can detect this malicious technique and counter it by adding a phishing notification and an X-MS-Exchange-P2FromRegexMatch header within emails by default. [65] This default security setting should not be disabled. Additional transport rule actions can be configured to build upon this detection to automate prevention actions. [65]

Conclusion

These Exchange Server best practices incorporate principles for Embracing a Zero Trust Security Model. [66], [67], [68] Zero Trust is based on an acknowledgement that threats exist and will inevitably occur within and outside of traditional network boundaries. To address these threats using Zero Trust concepts, the best practices described above focus on hardening user authentication and access, ensuring strong network encryption, and minimizing application attack surfaces.

Securing Exchange servers is essential for maintaining the integrity and confidentiality of enterprise communications and functions. By adhering to the best practices outlined in this document, organizations can significantly reduce their risk from cyber threats. Continuously evaluating and hardening the cybersecurity posture of these communication servers is critical to staying ahead of evolving cyber threats and ensuring robust protection of Exchange as part of the operational core of many organizations.

Works cited

[1] Federal Bureau of Investigation (FBI), et al. Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations. 2022. https://www.ic3.gov/CSA/2022/220914.pdf

[2] Cybersecurity and Infrastructure Security Agency (CISA), FBI, and National Security Agency (NSA). Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization. 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-277a

[3] Microsoft Corporation. Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server. 2022. https://msrc.microsoft.com/blog/2022/09/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

[4] CISA. CISA adds Four Known Exploited Vulnerabilities to Catalog. 2024. https://www.cisa.gov/news-events/alerts/2024/08/21/cisa-adds-four-known-exploited-vulnerabilities-catalog

[5] FBI, CISA, and Department of Health and Human Services (HHS). #StopRansomware: ALPHV Blackcat. 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a

[6] Microsoft Corporation. Released: March 2024 Exchange Server Security Updates. 2024. https://techcommunity.microsoft.com/blog/exchange/released-march-2024-exchange-server-security-updates/4075348

[7] Microsoft Corporation. Guidance for investigating attacks using CVE-2023-23397. 2023. https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/

[8] Microsoft Corporation. Stopping attacks against on-premises Exchange Server and SharePoint Server with AMSI. 2025. https://www.microsoft.com/en-us/security/blog/2025/04/09/stopping-attacks-against-on-premises-exchange-server-and-sharepoint-server-with-amsi/

[9] Microsoft Corporation. HAFNIUM targeting Exchange Servers with 0-day exploits. 2021. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[10] Cybersecurity and Infrastructure Security Agency. ED 25-02: Mitigate Microsoft Exchange Vulnerability. 2025. https://www.cisa.gov/news-events/directives/ed-25-02-mitigate-microsoft-exchange-vulnerability

[11] NSA. NSA's Top Ten Cybersecurity Mitigation Strategies. 2018. https://media.defense.gov/2019/Jul/16/2002158046/-1/-1/0/DDD-190716-666-071.PDF

[12] Microsoft Corporation. Exchange Updates Step-by-Step Guide. 2025. https://m365accelerator.microsoft.com/exchange/exchange-update

[13] Microsoft Corporation. Health Checker. 2025. https://aka.ms/ExchangeHealthChecker

[14] Microsoft Corporation. SetupAssist. 2021. https://microsoft.github.io/CSS-Exchange/Setup/SetupAssist/

[15] CISA. Reducing the Significant Risk of Known Exploited Vulnerabilities. 2025. https://www.cisa.gov/known-exploited-vulnerabilities

[16] Microsoft Corporation. Updates on Servicing Exchange Server 2019. 2024. https://techcommunity.microsoft.com/blog/exchange/updates-on-servicing-exchange-server-2019/4355545

[17] Microsoft Corporation. Exchange Server update FAQ. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-server-update-faq#exchange-server-update-types-and-release-schedule

[18] Microsoft Corporation. Exchange Server build numbers and release dates. 2025. https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates

[19] Microsoft Corporation. Updates for Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/new-features/updates
[20] Microsoft Corporation. Exchange Team Blog: You Had Me at EHLO. 2025. https://techcommunity.microsoft.com/t5/exchange-team-blog/bg-p/Exchange
[21] Microsoft Corporation. Exchange Emergency Mitigation (EM) service. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-emergency-mitigation-service
[22] Microsoft Corporation. Exchange Server Subscription Edition (SE) is now available. 2025. https://techcommunity.microsoft.com/blog/exchange/exchange-server-subscription-edition-se-is-now-available/4424924
[23] Microsoft Corporation. End of Support for Exchange Server 2016 and Exchange Server 2019: T-12 Months. 2024. https://techcommunity.microsoft.com/blog/exchange/end-of-support-for-exchange-server-2016-and-exchange-server-2019-t-12-months/4268516
[24] Microsoft Corporation. Exchange Server supportability matrix. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix#supported-email-clients
[25] Microsoft Corporation. Exchange Server AMSI integration. 2025. https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/amsi-integration-with-exchange
[26] Microsoft Corporation. Running Windows antivirus software on Exchange servers. 2025. https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/windows-antivirus-software
[27] Microsoft Corporation. Attack surface reduction rules reference. 2025. https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference
[28] Microsoft Corporation. Application Control for Windows. 2025. https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol
[29] Microsoft Corporation. App Control for Business and AppLocker Overview. 2025. https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol-and-applocker-overview
[30] Microsoft Corporation. Antispam protection in Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/antispam-protection
[31] Microsoft Corporation. Antimalware protection in Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antimalware-protection/antimalware-protection
[32] Microsoft Corporation. Client Access Rules in Exchange 2019. 2025. https://learn.microsoft.com/en-us/exchange/clients/client-access-rules/client-access-rules
[33] Microsoft Corporation. Network ports for clients and mail flow in Exchange. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/deployment-ref/network-ports
[34] Microsoft Corporation. Exchange Server TLS configuration best practices. 2024. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-tls-configuration?view=exchserver-2019
[35] Microsoft Corporation. Configure Windows Extended Protection in Exchange Server. 2024. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-extended-protection?view=exchserver-2019
[36] Microsoft Corporation. Mitigating NTLM Relay Attacks by Default. 2024. https://msrc.microsoft.com/blog/2024/12/mitigating-ntlm-relay-attacks-by-default/

[37] Microsoft Corporation. Windows Extended Protection <extendedProtection>. 2022. https://learn.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/windowsauthentication/extendedprotection/
[38] Microsoft Corporation. Supporting Extended Protection for Authentication (EPA) in a service. 2023. https://learn.microsoft.com/en-us/windows/win32/secauthn/epa-support-in-service
[39] Microsoft Corporation. Features removed or no longer developed in Windows Server. 2025. https://learn.microsoft.com/en-us/windows-server/get-started/removed-deprecated-features-windows-server
[40] Microsoft Corporation. Released: 2024 H1 Cumulative Update for Exchange Server. 2024. https://techcommunity.microsoft.com/blog/exchange/released-2024-h1-cumulative-update-for-exchange-server/4047506
[41] Microsoft Corporation. Authentication and EWS in Exchange. 2024. https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/authentication-and-ews-in-exchange
[42] Microsoft Corporation. Manage database availability groups in Exchange groups in Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/high-availability/manage-ha/manage-dags
[43] Microsoft Corporation. SMBv1 is not installed by default in Windows version 1709, Windows Server version 1709 and later version. 2023. https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows
[44] Microsoft Corporation. Deprecated features for Windows client. 2024. https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features
[45] Microsoft Corporation. The evolution of Windows authentication. 2023. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848
[46] Microsoft Corporation. NTLM Blocking and You: Application Analysis and Auditing Methodologies in Windows 7. 2019. https://techcommunity.microsoft.com/blog/askds/ntlm-blocking-and-you-application-analysis-and-auditing-methodologies-in-windows/397191
[47] Microsoft Corporation. Audit use of NTLMv1 on a Windows Server-based domain controller. 2025. https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/audit-domain-controller-ntlmv1
[48] Microsoft Corporation. Detect, enable, and SMBv1, SMBv2, and SMBv3 in Windows. 2025. https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3
[49] Microsoft Corporation. Disabling Legacy Authentication in Exchange Server 2019. 2019. https://techcommunity.microsoft.com/blog/exchange/disabling-legacy-authentication-in-exchange-server-2019/712048
[50] Microsoft Corporation. Configure Kerberos authentication for load-balanced Client Access services. 2023. https://learn.microsoft.com/en-us/exchange/architecture/client-access/kerberos-auth-for-load-balanced-client-access?view=exchserver-2019
[51] Microsoft Corporation. Enable or disable MAPI access to mailboxes in Exchange Server. 2023. https://learn.microsoft.com/en-us/exchange/clients/mapi-mailbox-access?view=exchserver-2019
[52] Microsoft Corporation. Configure MAPI over HTTP in Exchange Server. 2023. https://learn.microsoft.com/en-us/exchange/clients/mapi-over-http/configure-mapi-over-http?view=exchserver-2019

[53] Microsoft Corporation. MAPI over HTTP in Exchange Server. 2023. https://learn.microsoft.com/en-us/exchange/clients/mapi-over-http/mapi-over-http?view=exchserver-2019
[54] Microsoft Corporation. Exchange Server Roadmap Update. 2025. https://techcommunity.microsoft.com/blog/exchange/exchange-server-roadmap-update/4132742
[55] Microsoft Corporation. Enabling Modern Auth in Exchange on-premises. 2024. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/enable-modern-auth-in-exchange-server-on-premises?view=exchserver-2019
[56] Microsoft Corporation. How to configure Exchange Server on-premises to use Hybrid Modern Authentication. 2024. https://learn.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication
[57] Microsoft Corporation. Disable Basic authentication on Exchange Server virtual directories. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/disable-basic-authentication-on-exchange-server-virtual-directories
[58] Microsoft Corporation. Configure certificate signing of PowerShell serialization payloads in Exchange Server. 2024. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-serialization-payload-sign?view=exchserver-2019
[59] Microsoft Corporation. Control remote PowerShell access to Exchange servers. 2023. https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers?view=exchange-ps#use-the-exchange-management-shell-to-enable-or-disable-remote-powershell-access-for-a-user
[60] Microsoft Corporation. Configure HTTP Strict Transport Security (HSTS) in Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/configure-http-strict-transport-security-in-exchange-server
[61] Microsoft Corporation. Configure Download Domains in Exchange Server. 2025. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-download-domains
[62] Microsoft Corporation. Understanding management role assignments. 2023. https://learn.microsoft.com/en-us/exchange/understanding-management-role-assignments-exchange-2013-help
[63] NSA. Defend Privileges and Accounts. 2019. https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf
[64] Microsoft Corporation. Configure Exchange Server for split permissions. 2023. https://learn.microsoft.com/en-us/exchange/permissions/split-permissions/configure-exchange-for-split-permissions?view=exchserver-2019
[65] Microsoft Corporation. Exchange Server non-RFC compliant P2 FROM header detection. 2024. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-non-compliant-p2from-detection?view=exchserver-2019.
[66] NSA. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[67] CISA. Mitigate Microsoft Exchange Server Vulnerabilities. 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

[68] Microsoft Corporation. Security best practices for Exchange Server. 2023. https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/security-best-practices?view=exchserver-2019

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the authoring agencies, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov