Disable or Remove Feature or Program, Mitigation M1042 - Enterprise

Archived: 2026-04-05 13:04:18 UTC

Enterprise T1098 Account Manipulation

Remove unnecessary and potentially abusable authentication and authorization mechanisms where possible.

.001 Additional Cloud Credentials

Remove unnecessary and potentially abusable authentication mechanisms where possible. For example, in Entra ID environments, disable the app password feature unless explicitly required.

.002 Additional Email Delegate Permissions

If email delegation is not required, disable it. In Google Workspace this can be accomplished through the Google Admin console.[1]

.004 SSH Authorized Keys

Disable SSH if it is not necessary on a host or restrict SSH access for specific users/groups using `/etc/ssh/sshd_config`. Setting the `PermitRootLogin` directive to `no` will prevent the root user from logging in via SSH.[2]

Enterprise T1595 .003 Active Scanning: Wordlist Scanning

Remove or disable access to any systems, resources, and infrastructure that are not explicitly required to be available externally.

Enterprise T1557 Adversary-in-the-Middle

Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.

.001 LLMNR/NBT-NS Poisoning and SMB Relay

Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. [3]

.002 ARP Cache Poisoning

Consider disabling updating the ARP cache on gratuitous ARP replies.

Enterprise T1547 .007 Boot or Logon Autostart Execution: Re-opened Applications

This feature can be disabled entirely with the following terminal command: `defaults write -g ApplePersistence -bool no`.

Enterprise T1671 Cloud Application Integration

Do not allow users to add new application integrations into a SaaS environment. In Entra ID environments, consider enforcing the "Do not allow user consent" option.[4]

Enterprise T1059 Command and Scripting Interpreter

Disable or remove any unnecessary or unused shells or interpreters.

.001 PowerShell

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions.

Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

.005 Visual Basic

Turn off or restrict access to unneeded VB components.

.007 JavaScript

Turn off or restrict access to unneeded scripting components.

Enterprise T1092 Communication Through Removable Media

Disable Autoruns if it is unnecessary.[5]

Enterprise T1609 Container Administration Command

Remove unnecessary tools and software from containers.

Enterprise T1555 .004 Credentials from Password Stores: Windows Credential Manager

Consider enabling the "Network access: Do not allow storage of passwords and credentials for network authentication" setting that will prevent network credentials from being stored by the Credential Manager.[6]

Enterprise T1114 .003 Email Collection: Email Forwarding Rule

Consider disabling external email forwarding.[7]

Enterprise T1611 Escape to Host

Remove unnecessary tools and software from containers.

Enterprise T1546 .002 Event Triggered Execution: Screensaver

Use Group Policy to disable screensavers if they are unnecessary.[8]

.014 Event Triggered Execution: Emond

Consider disabling emond by removing the Launch Daemon plist file.

Enterprise T1011 Exfiltration Over Other Network Medium

Disable WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel in local computer security settings or by group policy if it is not needed within an environment.

.001 Exfiltration Over Bluetooth

Disable Bluetooth in local computer security settings or by group policy if it is not needed within an environment.

Enterprise T1052 Exfiltration Over Physical Medium

Disable Autorun if it is unnecessary. [5] Disallow or restrict removable media at an organizational policy level if they are not required for business operations. [9]

.001 Exfiltration over USB

Disable Autorun if it is unnecessary. [5] Disallow or restrict removable media at an organizational policy level if they are not required for business operations. [9]

Enterprise T1210 Exploitation of Remote Services

Minimize available services to only those that are necessary.

Enterprise T1133 External Remote Services

Disable or block remotely available services that may be unnecessary.

Enterprise T1564 .006 Hide Artifacts: Run Virtual Instance

Disable native virtualization technologies such as Hyper-V if not necessary within a given environment. Consider also disabling Windows Sandbox if it is not needed to test or debug applications.

.007 Hide Artifacts: VBA Stomping

Turn off or restrict access to unneeded VB components.[10]

Enterprise T1562 Impair Defenses

Consider removing previous versions of tools that are unnecessary to the environment when possible.

.010 Downgrade Attack

Consider removing previous versions of tools that are unnecessary to the environment when possible.

Enterprise T1559 Inter-Process Communication

Registry keys specific to Microsoft Office feature control security can be set to disable automatic DDE/OLE execution. [11][12][13] Microsoft also created, and enabled by default, Registry keys to completely disable DDE execution in Word and Excel.[14]

.002 Dynamic Data Exchange

Registry keys specific to Microsoft Office feature control security can be set to disable automatic DDE/OLE execution. [11][12][13] Microsoft also created, and enabled by default, Registry keys to completely disable DDE execution in Word and Excel.[14]

Enterprise T1046 Network Service Discovery

Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

Enterprise T1137 Office Application Startup

Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing.

Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins. For some add-ins types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code from executing. [15]

.001 Office Template Macros

Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing.

Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins. For some add-ins types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code from executing. [15]

Enterprise T1219 Remote Access Tools

Consider disabling unnecessary remote connection functionality, including both unapproved software installations and specific features built into supported applications.

.002 Remote Desktop Software

Consider disabling unnecessary remote connection functionality, including both unapproved software installations and specific features built into supported applications.

Enterprise T1563 Remote Service Session Hijacking

Disable the remote service (ex: SSH, RDP, etc.) if it is unnecessary.

.001 SSH Hijacking

Ensure that agent forwarding is disabled on systems that do not explicitly require this feature to prevent misuse. [16]

.002 RDP Hijacking

Disable the RDP service if it is unnecessary.

Enterprise T1021 Remote Services

If remote services, such as the ability to make direct connections to cloud virtual machines, are not required, disable these connection types where feasible. On ESXi servers, consider enabling lockdown mode, which disables direct access to an ESXi host and requires that the host be managed remotely using vCenter.[17][18]

.001 Remote Desktop Protocol

Disable the RDP service if it is unnecessary.

.003 Distributed Component Object Model

Consider disabling DCOM through Dcomcnfg.exe.[19]

.004 SSH

Disable the SSH daemon on systems that do not require it, especially ESXi servers. For macOS, ensure Remote Login is disabled under Sharing Preferences.[20]

.005 VNC

Uninstall any VNC server software where not required.

.006 Windows Remote Management

Disable the WinRM service.

.008 Direct Cloud VM Connections

If direct virtual machine connections are not required for administrative use, disable these connection types where feasible.

Enterprise T1091 Replication Through Removable Media

Disable Autorun if it is unnecessary. [5] Disallow or restrict removable media at an organizational policy level if it is not required for business operations. [9]

Enterprise T1505 Server Software Component

Consider disabling software components from servers when possible to prevent abuse by adversaries.[21]

.003 Web Shell

Consider disabling functions from web technologies such as PHP's `evaI()` that may be abused for web shells. [21]

Enterprise T1649 Steal or Forge Authentication Certificates

Consider disabling old/dangerous authentication protocols (e.g. NTLM), as well as unnecessary certificate features, such as potentially vulnerable AD CS web and other enrollment server roles.[22]

Enterprise T1553 .005 Subvert Trust Controls: Mark-of-the-Web Bypass

Consider disabling auto-mounting of disk image files (i.e., .iso, .img, .vhd, and .vhdx). This can be achieved by modifying the Registry values related to the Windows Explorer file associations in order to disable the automatic Explorer "Mount and Burn" dialog for these file extensions. Note: this will not deactivate the mount functionality itself.[23]

Enterprise T1218 System Binary Proxy Execution

Many native binaries may not be necessary within a given environment.

.003 CMSTP

CMSTP.exe may not be necessary within a given environment (unless using it for VPN connection installation).

.004 InstallUtil

InstallUtil may not be necessary within a given environment.

.005 Mshta

Mshta.exe may not be necessary within a given environment since its functionality is tied to older versions of Internet Explorer that have reached end of life.

.007 Msiexec

Consider disabling the `AlwaysInstallElevated` policy to prevent elevated execution of Windows Installer packages.[24]

.008 Odbcconf

Odbcconf.exe may not be necessary within a given environment.

.009 Regsvcs/Regasm

Regsvcs and Regasm may not be necessary within a given environment.

.012 Verclsid

Consider removing verclsid.exe if it is not necessary within a given environment.

.013 Mavinject

Consider removing mavinject.exe if Microsoft App-V is not used within a given environment.

.014 MMC

MMC may not be necessary within a given environment since it is primarily used by system administrators, not regular users or clients.

.015 Electron Applications

Remove or deny access to unnecessary and potentially vulnerable software and features to prevent abuse by adversaries. Many native binaries may not be necessary within a given environment: for example, consider disabling the Node.js integration in all renderers that display remote content to protect users by limiting adversaries' power to plant malicious JavaScript within Electron applications.[25]

Enterprise T1221 Template Injection

Consider disabling Microsoft Office macros/active content to prevent the execution of malicious payloads in documents [26], though this setting may not mitigate the Forced Authentication use for this technique.

Enterprise T1205 Traffic Signaling

Disable Wake-on-LAN if it is not needed within an environment.

Enterprise T1127 Trusted Developer Utilities Proxy Execution

Specific developer utilities may not be necessary within a given environment and should be removed if not used.

.001 MSBuild

MSBuild.exe may not be necessary within an environment and should be removed if not being used.

.002 ClickOnce

Disable ClickOnce installations from the internet using the following registry key: `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\TrustManager\PromptingLevel - Internet:Disabled` [27][28]

ClickOnce may not be necessary within an environment and should be disabled if not being used.

.003 JamPlus

JamPlus may not be necessary within a given environment and should be removed if not used.

Enterprise T1552 .005 Unsecured Credentials: Cloud Instance Metadata API

Disable unnecessary metadata services and restrict or disable insecure versions of metadata services that are in use to prevent adversary access.[29]
