Windows Security Hardening

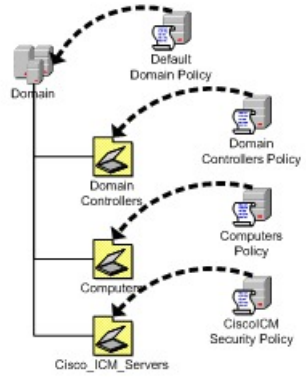
Windows Server Hardening

Unified CCE installer has a customized security policy in the form of Group Policy Object (GPO) backup. You can apply this policy into a separate Organization Unit (OU), that contains Unified CCE servers. The policy ensures the proper functioning of the Unified CCE application, and with improved security. Clearly identify the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and ensure that it is documented in accordance with your corporate policy.

Create this OU either at the same level as the **Computers** container or at the Cisco ICM Root OU. If you are unfamiliar with Active Directory, engage your Domain Administrator to assist you with Group Policy deployments.

Note You can only apply Unified CCE GPO backup to the member server OU that is created under Windows Server Domain Controller.

Figure 1: Group Policy Deployments



After the security policy is applied at the OU level, any differing policies must be blocked from being inherited at the Unified ICM/Unified CCE Servers OU. Keep in mind that you can override blocking inheritance, a configuration option at the OU object level, when you select the Enforced/No Override option at a higher hierarchy level. The application of group policies must follow a thought-out design that starts with the most common denominator, and those policies must be restrictive only at the appropriate level in the hierarchy.

Unified CCE Security Hardening for Windows Server

This topic contains the security baseline for hardening Windows Servers running Unified CCE.

This baseline is essentially a collection of Microsoft group policy settings

In addition to the GPO settings provided in the table, disable the following settings:

- NetBIOS
- SMBv1

Note For more details about these configurations, see the Microsoft Windows Server documentation.

The baseline includes only those settings whose severity qualifies as Critical and Important. The settings with Optional and None severity qualification are not included in the baseline.

Setting Name	Default Value	Compliance
Network security: LAN Manager authentication level	Send NTLMv2 response only	Send NTLMv2 response only. Refuse LM & NTLM
Network Security: Restrict NTLM: Audit NTLM authentication in this domain	Not defined	Not Defined
Network Security: Restrict NTLM: Incoming NTLM traffic	Not defined	Not Defined
Interactive logon: Require smart card	Not Defined	Not Defined
Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not defined	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not defined	Disabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled

Setting Name	Default Value	Compliance
Network security: Allow Local System to use computer identity for NTLM	Disabled	Enabled
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	Require NTLMv2 session security,Require 128-bit encryption
Microsoft network server: Server SPN target name validation level	Not Defined	Not Defined
Interactive logon: Smart card removal behavior	No Action	Lock Workstation
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	Require NTLMv2 session security,Require 128-bit encryption
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	4 logon(s)
Network Security: Restrict NTLM: NTLM authentication in this domain	Not defined	Not Defined
Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not defined	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled
Network Security: Restrict NTLM: Add server exceptions in this domain	Not defined	Not Defined

Setting Name	Default Value	Compliance
Network Security: Restrict NTLM: Audit Incoming NTLM Traffic	Not defined	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled
Shutdown: Clear virtual memory pagefile	Disabled	Disabled
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion	System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion
Network access: Shares that can be accessed anonymously	Not defined	Not Defined
Turn off the "Publish to Web" task for files and folders	Not configured	Not Configured
Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Enabled
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Classic - local users authenticate as themselves
Interactive logon: Do not require CTRL+ALT+DEL	Enabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Administrators
Turn off the Windows Messenger Customer Experience Improvement Program	Not configured	Not Configured

Setting Name	Default Value	Compliance
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	Disabled
Turn off Search Companion content file updates	Not configured	Not Configured
Network access: Allow anonymous SID/Name translation	Disabled	Disabled
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog
Recovery console: Allow automatic administrative logon	Disabled	Disabled
Turn off Autoplay	Disabled	Enabled
Turn off Windows Update device driver searching	Not configured	Not Configured
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled

Setting Name	Default Value	Compliance
Network access: Named Pipes that can be accessed anonymously	Not defined	Not Defined
Audit Policy: System: IPsec Driver	No auditing	Success and Failure
Audit Policy: System: Security System Extension	No auditing	Success and Failure
Audit Policy: Account Management: Security Group Management	Success	Success and Failure
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	None	Enabled
Audit Policy: Account Management: Other Account Management Events	No auditing	Success and Failure
Audit Policy: System: Security State Change	Success	Success and Failure
Audit Policy: Detailed Tracking: Process Creation	No auditing	Success
Audit Policy: System: Other System Events	Success and Failure	Success and Failure
Audit Policy: Logon-Logoff: Account Lockout	Success	Success
Audit Policy: Policy Change: Audit Policy Change	Success	Success and Failure
Audit: Audit the access of global system objects	Not defined	Not Defined
Audit Policy: Logon-Logoff: Special Logon	Success	Success
Audit Policy: Account Management: User Account Management	Success	Success and Failure
Audit Policy: Account Logon: Credential Validation	Success	Success and Failure

Setting Name	Default Value	Compliance
Audit Policy: Logon-Logoff: Logon	Success	Success and Failure
Audit Policy: Account Management: Computer Account Management	Success	Success
Audit Policy: Privilege Use: Sensitive Privilege Use	Success	Success and Failure
Audit Policy: Logon-Logoff: Logoff	Success	Success
Audit Policy: Policy Change: Authentication Policy Change	Success	Success
Audit: Audit the use of Backup and Restore privilege	Not defined	Not Defined
Audit Policy: System: System Integrity	Success and Failure	Success and Failure
Turn off toast notifications on the lock screen	Disabled	Enabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 minute(s)
Interactive logon: Message text for users attempting to log on	Not defined	Not Defined
Interactive logon: Machine inactivity limit	0 seconds	900 seconds
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled
Interactive logon: Message title for users attempting to log on	Not defined	Not Defined
Network security: Force logoff when logon hours expire	Enabled	Enabled
Sign-in last interactive user automatically after a system-initiated restart	Enabled	Disabled

Setting Name	Default Value	Compliance
Interactive logon: Display user information when the session is locked	Not defined	Not Defined
Interactive logon: Do not display last user name	Disabled	Enabled
Interactive logon: Machine account lockout threshold	Not defined	10 invalid logon attempts
Allow Remote Shell Access	Not configured	Not Configured
Devices: Prevent users from installing printer drivers	Enabled	Enabled
Create global objects	Administrators, Service, Local Service, Network Service	Administrators, Service, Local Service, Network Service
Access this computer from the network	Everyone, Administrators, Users, Backup Operators	Administrators, Authenticated Users
Domain controller: Allow server operators to schedule tasks	Not defined	Not Defined
Modify an object label	No one	No One
Generate security audits	Local Service, Network Service	Local Service, Network Service
Increase scheduling priority	Windows Server 2016: Administrators	Windows Server 2016: Administrators
Force shutdown from a remote system	Administrators	Administrators
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users	Administrators
Change the system time	Local Service, Administrators	Local Service, Administrators
Add workstations to domain	Not defined (Authenticated Users for domain controllers)	Not Defined
Create a pagefile	Administrators	Administrators
Profile single process	Administrators	Administrators
Deny log on as a batch job	No one	Guests
Act as part of the operating system	No one	No One
Change the time zone	Local Service, Administrators	Local Service, Administrators

Setting Name	Default Value	Compliance
Synchronize directory service data	Not defined	Not Defined
Lock pages in memory	No one	No One
Access Credential Manager as a trusted caller	No one	No One
Create a token object	No one	No One
Debug programs	Administrators	Administrators
Deny log on as a service	No one	Guests
Deny access to this computer from the network	Guests	Guests, NT AUTHORITY\Local account and member of Administrators group
Back up files and directories	Administrators, Backup Operators	Administrators
Shut down the system	Administrators, Backup Operators, Users	Administrators
Deny log on locally	Guests	Guests
Replace a process level token	Local Service, Network Service	Local Service, Network Service
Modify firmware environment values	Administrators	Administrators
Allow log on locally	Guest, Administrators, Power Users, Users, Backup Operators	Administrators, Users
Restore files and directories	Administrators, Backup Operators	Administrators
Profile system performance	Administrators,NT Service\WdiServiceHost	Administrators,NT Service\WdiServiceHost
Log on as a batch job	Not defined	Not Defined
Perform volume maintenance tasks	Administrators	Administrators
Manage auditing and security log	Administrators	Administrators
Enable computer and user accounts to be trusted for delegation	No one	No One
Impersonate a client after authentication	Administrators, Service, Local Service, Network Service	Administrators, Service, Local Service, Network Service

Setting Name	Default Value	Compliance
Load and unload device drivers	Administrators	Administrators
Take ownership of files or other objects	Administrators	Administrators
Adjust memory quotas for a process	Local Service, Network Service, Administrators	Administrators, Local Service, Network Service
Log on as a service	Not defined	Not Defined
Create symbolic links	Administrators	Administrators
Create permanent shared objects	No one	No One
System cryptography: Force strong key protection for user keys stored on the computer	Not defined	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabled
Windows Firewall: Domain: Allow unicast response	Yes	No
Windows Firewall: Domain: Apply local firewall rules	Yes	Yes (default)
Windows Firewall: Domain: Inbound connections	Block	Enabled
Windows Firewall: Private: Firewall state	On	On
Windows Firewall: Private: Apply local connection security rules	Yes	Yes (default)
Windows Firewall: Private: Allow unicast response	Yes	No
Windows Firewall: Public: Apply local firewall rules	Yes	Yes (default)
Windows Firewall: Public: Apply local connection security rules	Yes	Yes
Windows Firewall: Public: Firewall state	On	On

Setting Name	Default Value	Compliance
Windows Firewall: Private: Outbound connections	Allow	Allow (default)
Windows Firewall: Domain: Outbound connections	Allow	Allow (default)
Windows Firewall: Domain: Firewall state	On	On
Windows Firewall: Public: Allow unicast response	No	No
Windows Firewall: Public: Inbound connections	Block	Enabled
Windows Firewall: Domain: Apply local connection security rules	Yes	Yes (default)
Windows Firewall: Private: Display a notification	Yes	Yes (default)
Windows Firewall: Domain: Display a notification	Yes	Yes (default)
Windows Firewall: Public: Display a notification	Yes	Yes
Windows Firewall: Public: Outbound connections	Allow	Allow (default)
Windows Firewall: Private: Inbound connections	Block	Enabled
Windows Firewall: Private: Apply local firewall rules	Not defined	Yes (default)
Default Protections for Internet Explorer	Enabled	Enabled
Password protect the screen saver	Not Configured	Enabled
Local Poilcy `User Account Control: Admin Approval Mode for the Built-in Administrator account`	Disabled	Disabled

Setting Name	Default Value	Compliance
Default Protections for Software	None	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	Enabled
Apply UAC restrictions to local accounts on network logons	None	Enabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	Prompt for consent on the secure desktop
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	Disabled
Local Policy `User Account Control: Virtualize file and registry write failures to per-user locations`	None	Disabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled	Enabled
WDigest Authentication	Disabled	Disabled
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	Automatically deny elevation requests
System ASLR	None	Enabled
System DEP	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled

Setting Name	Default Value	Compliance
Enable screen saver	Enabling/disabling the screen saver is managed locally by the user.	Enabled
Force specific screen saver	Disabled	Enabled
Increase a process working set	Not Defined	Not Defined
User Account Control: Detect application installations and prompt for elevation	Disabled	Enabled
System SEHOP	Enabled: Application Opt-Out	Enabled
Network Security: Configure encryption types allowed for Kerberos	Not defined	Not Defined
Set client connection encryption level	Not configured	Not Configured
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled
Domain controller: LDAP server signing requirements	Not defined	Not Defined
Network security: LDAP client signing requirements	Negotiate signing	Negotiate signing
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled
Microsoft network server: Digitally sign communications (always)	Disabled	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Enabled

Setting Name	Default Value	Compliance
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Application: Specify the maximum log file size (KB)	20480 KB	Enabled
Security: Specify the maximum log file size (KB)	20480 KB	Enabled
Setup: Specify the maximum log file size (KB)	20480 KB	Enabled
Audit: Shut down system immediately if unable to log security audits	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled
Domain controller: Refuse machine account password changes	Not defined	Not Defined
Domain member: Disable machine account password changes	Disabled	Disabled
Domain member: Maximum machine account password age	30 days	30 day(s)
Network access: Do not allow storage of passwords and credentials for network authentication	Not Defined	Not Defined
Interactive logon: Prompt user to change password before expiration	5 days	14 day(s)
Allow indexing of encrypted files	Disabled	Disabled
Accounts: Rename administrator account	Not Defined	Not Defined
Do not display network selection UI	Disabled	Enabled

Setting Name	Default Value	Compliance
Allow Microsoft accounts to be optional	Disabled	Enabled
Accounts: Administrator account status	Disabled	Not Defined
Accounts: Guest account status	Disabled	Disabled
Accounts: Rename guest account	Guest	Not Defined
Prevent enabling lock screen slide show	Disabled	Enabled
Prevent enabling lock screen camera	Disabled	Enabled
IRC Ports	Disabled	Disabled
Outgoing Email Port 25	Disabled	Disabled
Advanced Audit Policy Configuration - Account Logon: Audit Credential Validation	Success	Success and Failure
Administrative Templates (Computer): `Always install with elevated privileges`	Disabled	Disabled
Advanced Audit Policy Configuration - Object Access: `Audit Other Object Access Events`	No Auditing	Success and Failure
Administrative Templates (User) - Cloud Content: `Do not suggest third-party content in Windows spotlight`	Disabled	Enabled
Administrative Templates (User) Cloud Content: `Do not use diagnostic data for tailored experiences`	Disabled	Enabled

Setting Name	Default Value	Compliance
Administrative Templates (User) Cloud Content: `Turn off all Windows spotlight features`	Disabled	Enabled
Administrative Templates (Computer): `Allow input personalization`	Enabled	Disabled
Administrative Templates (Computer): `Allow Online Tips`	Enabled	Disabled
Administrative Templates (Computer): `Enable Structured Exception Handling Overwrite Protection (SEHOP)`	Disabled for 32-bit processes	Enabled
Administrative Templates (Computer): `Turn off multicast name resolution`	Disabled	Enabled
Administrative Templates (Computer): `Enable Font Providers`	Enabled **Note** You can download the fonts that are included in Windows but not stored on your local, on demand, from an online font provider.	Disabled
Administrative Templates (Computer): `Enable insecure guest logons`	Enabled **Note** The SMB client allows insecure guest logons.	Disabled
Administrative Templates (Computer): `Prohibit use of Internet Connection Sharing on your DNS domain network`	Disabled **Note** All users can access the Mobile Hotspot.	Enabled
Administrative Templates (Computer): `Remote host allows delegation of non-exportable credentials`	Disabled	Enabled

Setting Name	Default Value	Compliance
Administrative Templates (Computer): `Continue experiences on this device`	The default behavior depends on the Windows edition.	Disabled
Administrative Templates (Computer): `Block user from showing account details on signin`	Disabled **Note** You can choose to show the account details on the sign-in screen.	Enabled
Administrative Templates (Computer): `Turn off picture password sign-in`	Disabled **Note** You can set up and use a picture password.	Enabled
Administrative Templates (Computer): `Untrusted Font Blocking`	Windows Server 2016: Off **Note** No fonts are blocked.	Windows Server 2016: Enabled **Note** Untrusted fonts and log events are blocked.
Administrative Templates (Computer): `Allow network connectivity during connected standby (plugged in)`	Enabled **Note** When plugged in, the network connectivity will be in standby mode.	Disabled
Administrative Templates (Computer): `Turn off the advertising ID`	Disabled **Note** You can choose whether the applications can use the advertising ID for experiences across all the applications.	Enabled
Administrative Templates (Computer): `Allow a Windows app to share application data between users`	Disabled	Disabled
Administrative Templates (Computer): `Configure enhanced anti-spoofing`	You can enable or disable enhanced anti-spoofing on supported devices.	Enabled
Administrative Templates (Computer): `Allow Use of Camera`	Enabled **Note** Camera devices are enabled.	Disabled

Setting Name	Default Value	Compliance
Administrative Templates (Computer): `Turn off Microsoft consumer experiences`	Disabled **Note** You will see suggestions from Microsoft, and notifications about your Microsoft account.	Enabled
Administrative Templates (Computer): `Require pin for pairing`	Disabled **Note** Personal Identification Number (PIN) is not required to pair with a wireless display device.	Enabled
Administrative Templates (Computer): `Allow Telemetry`	Disabled **Note** You can configure the Telemetry level in settings.	Enabled: 0 - Security [Enterprise Only]
Administrative Templates (Computer): `Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service`	Disabled **Note** The Connected User Experience and Telemetry service sends data back to Microsoft, automatically, using an authenticated proxy.	Enabled **Note** Authenticated proxy is disabled.
Administrative Templates (Computer): `Disable pre-release features or settings`	You can configure the **Let Microsoft try features on this build** option in Settings.	Disabled
Administrative Templates (Computer): `Do not show feedback notifications`	Disabled **Note** In the Windows Feedback application, you will see notifications for feedback. You can configure the time duration to receive feedback questions.	Enabled
Administrative Templates (Computer): `Toggle user control over Insider builds`	Enabled **Note** You can download and install Windows Preview software on your devices.	Disabled

Setting Name	Default Value	Compliance
Administrative Templates (Computer): `System: Specify the maximum log file size (KB)`	Disabled **Note** The default log size is 20,480 KB, the local administrator can change this value using the **Log Properties** dialog.	Enabled - 32,768 or greater
Administrative Templates (Computer): `Allow Message Service Cloud Sync`	Enabled	Disabled
Administrative Templates (Computer): `Block all consumer Microsoft account user authentication`	Disabled	Enabled
Administrative Templates (Computer): `Prevent the usage of OneDrive for file storage`	Disabled	Enabled
Administrative Templates (Computer): `Allow Cloud Search`	Enabled **Note** Cloud Search is enabled - it allows search and Cortana to search cloud sources like OneDrive and SharePoint.	Enabled **Note** Cloud Search is disabled.
Administrative Templates (Computer): `Configure Watson events`	Enabled **Note** When a program or service crashes or fails, Watson events are sent to Microsoft, automatically.	Disabled
Administrative Templates (Computer): `Scan removable drives`	Disabled **Note** Removable drives are not scanned during a full scan, but they can be scanned during the quick or custom scan.	Enabled

Setting Name	Default Value	Compliance
Administrative Templates (Computer): `Turn on e-mail scanning`	Disabled **Note** E-mail scanning by Windows Defender Antivirus is disabled.	Enabled
Administrative Templates (Computer): `Configure Attack Surface Reduction rules`	Disabled **Note** ASR rules are not configured.	Enabled
Administrative Templates (Computer): `Configure Attack Surface Reduction rules: Set the state for each ASR rule`	Disabled **Note** ASR rules are not configured.	Blocked
Administrative Templates (Computer) `Prevent users and apps from accessing dangerous websites`	Disabled **Important** Users and applications are not blocked from connecting to dangerous domains.	Enabled: Block
Administrative Templates (Computer): `Allow suggested apps in Windows Ink Workspace`	Enabled **Note** The suggested applicationss in the Windows Ink Workspace are allowed.	Disabled
Administrative Templates (Computer): `Allow Windows Ink Workspace`	Enabled **Note** The Windows Ink Workspace is permitted above the lock screen.	Enabled **Note** The access above lock is disabled.
Administrative Templates (Computer): `Allow remote server management through WinRM`	Disabled **Note** The WinRM service does not respond to requests from a remote computer, regardless of the WinRM listeners configuration.	Disabled

Setting Name	Default Value	Compliance
Administrative Templates (Computer): `Manage preview builds`	Disabled **Note** Preview builds are not installed on the device, until you configure it in: **Settings** > **Update and Security**.	Enabled **Note** Preview builds are disabled.
Administrative Templates (Computer): `Select when Preview Builds and Feature Updates are received`	Disabled **Note** Feature Updates will not be delayed when released by Microsoft.	Enabled - Semi-Annual Channel, 180 or more days. :
Advanced Audit Policy Configuration `Audit Directory Service Access`	Success	Success and Failure
Administrative Templates (User) `Turn off Help Experience Improvement Program`	Disabled	Enabled
Administrative Templates (User) `Prevent users from sharing files within their profile`	Disabled	Enabled
Local Policy - Accounts: `Block Microsoft accounts`	You can use Microsoft accounts with Windows.	You cannot add or login with Microsoft accounts.
Local Policy `Network access: Do not allow storage of passwords and credentials for network authentication`	Disabled	Enabled
Local Policy `Network access: Shares that can be accessed anonymously`	None	Blank

Setting Name	Default Value	Compliance
Local Policy `Network security: Configure encryption types allowed for Kerberos`	• RC4_HMAC_MD5 • AES128_HMAC_SHA1 • AES256_HMAC_SHA1 • Future encryption types References: 1	• AES128_HMAC_SHA1 • AES256_HMAC_SHA1 • Future encryption types
Local Policy `User Account Control: Admin Approval Mode for the Built-in Administrator account`	Disabled	Enabled
Local Policy `User Account Control: Behavior of the elevation prompt for standard users`	Prompt for credentials. **Note** When a functionality requires an elevation to higher level privilege, the system prompts you to enter the administrator credentials. The higher level privilege is permitted if the credentials are valid.	The system denies the elevation to higher level privilege, automatically.
Local Policy `User Account Control: Detect application installations and prompt for elevation`	Disabled	Enabled
Local Policy `User Account Control: Only elevate UIAccess applications that are installed in secure locations`	Enabled	Enabled
Local Policy `User Account Control: Virtualize file and registry write failures to per-user locations`	Enabled. **Note** The system redirects the application write failures at run time to defined user locations, for both the file system and registry.	Enabled

Other Windows Hardening Considerations

The following table lists the IIS settings with their corresponding default and possible values.

Setting Name	Default Value	Supported Values
ASP.NET Application Custom Error	RemoteOnly	• **On**: The system displays custom errors to both remote systems and the local host. • **Off**: The system displays ASP.NET errors to both remote systems and the local host. • **RemoteOnly**: The system displays custom errors to the remote systems and ASP.NET errors to the local host. **Note** You can use any of these options available without impacting the system functionality.
HTTPOnlyCookie	Off	Off
WMI - Namespace level security	Everyone	Administrators
Disable NetBIOS	Default	Disabled
Configure SMB v1 server is set to Disabled	Disabled	Disabled

Note Certain extensions, such as .exe, .htm and .dll, cannot be filtered in IIS.

Windows Security Hardening