

AN OFFERING IN THE BLUE CYBER SERIES:

# NIST SP 800-171 Configuration Management & Configuration Management Primer

Presented by  
the DCMA DIBCAC ASSESSMENT TEAM

17 May 2022

#29 in the Blue Cyber Education Series



# Configuration Management: A Primer and NIST SP 800-171 CM Security Requirements

---

Presented By:

**Patrick Wicker & Robson Nyereyemhuka**

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

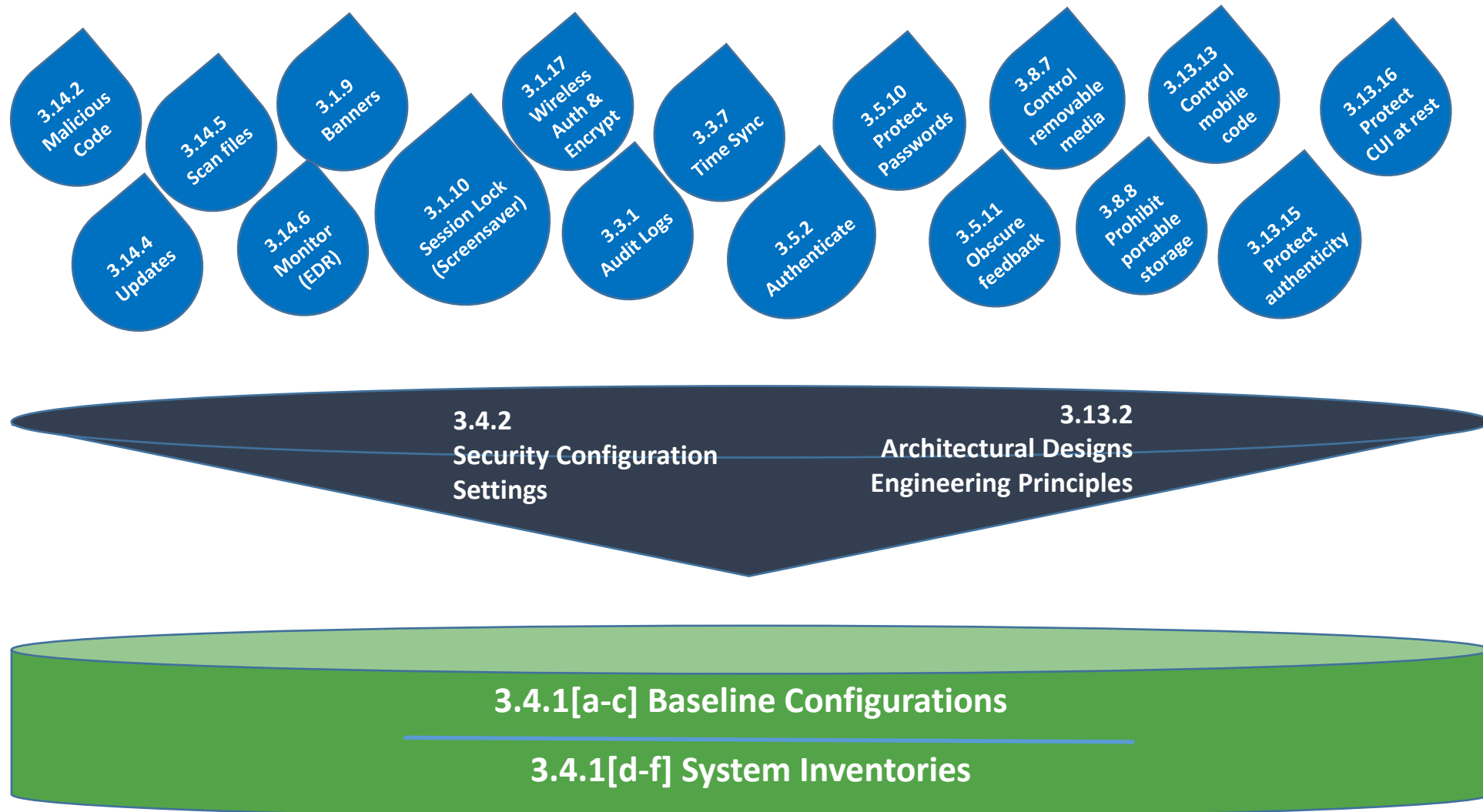
May 17, 2022

DISTRIBUTION STATEMENT A. Approved for public release DCMA PAO 17 May 2022: distribution unlimited.

*One team, one voice delivering global acquisition insight.*

Configuration management is the process of maintaining the **integrity of hardware, software, firmware, and documentation** related to the configuration and **change management** process. CM is a **continuous process of controlling and approving changes** to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

- Know what you have
- Configure it to be secure
- Know how it is configured
- Know when it changes



- Planning
- Identifying and Implementing Configurations
- Controlling Configuration Changes
- Monitoring

*NIST has a CM Plan and Change Request plans/outlines you could use at:  
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-128.pdf>*

## Policies

- Stated Purpose, Scope of Authority
- Expectations for compliance and performance
- Defined roles & responsibilities
- Link to procedures, standards, processes, etc..
- Align business and security objectives
- Built to last, resistant to change
- Endorsed by senior management

## Standards

- Mandatory rules that support policy
- May specify supported hardware/software
- Compulsory – must be enforced (same with policy)
- Ex. Encryption, Desktop, Laptop, Multifunction Printing

## Procedures

- Detailed, step-by-step instructions
- Reviewed and updated periodically (subject to change control)
- Meet the intent of policy
- Ex. Build instructions, Package applications, Software Request, Baseline Updates

## Guidelines

- Recommendations when standards do not apply
- More general vs specific
- Provide flexibility for unforeseen circumstances
- NOT the same as policy
- Ex. Mailbox management strategy, printing, resource usage

- Establish baselines - multiple baselines may exist
- Baselines represent the most secure state consistent with operational requirements and constraints
- Developed, reviewed, approved, and implemented
- May address:
  - Configuration settings
  - Software loads
  - Patch levels
  - Security controls
- Facilitated by automation



- Security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.
- Resources are plentiful:
  - Security Technical Implementation Guides (STIG)
  - Center for Internet Security (CIS) Benchmarks
  - Microsoft Security Compliance Toolkit
  - Security Content Automation Protocol (SCAP) Standards

*Security misconfigurations are one of the most common gaps that criminal hackers look to exploit. According to a recent report by Rapid 7, internal penetration tests encounter a network or service misconfiguration more than 96% of the time. (Standards can counter these)*

- Use formal procedures to maintain the baseline and control variations
- Track, review, analyze for security impact, approve and log changes
- Supported by existing security controls and concepts of least privilege, least functionality, separation of duties, auditing activities
- Facilitated by Configuration Control Boards, Change Advisory Boards, etc..
- Aided by process automation and tools:

Activities to validate that the system is adhering to organizational policies, procedures, standards, and the approved secure baseline configuration.

Identifies:

- Undiscovered/Undocumented system components
- Misconfigurations
- Vulnerabilities
- Unauthorized changes

## Assessment

- Rogue inventory scans
- Integrity scans/checks
- Endpoint detection/whitelisting
- Review change control records

## Reporting

- Vulnerability Scans
- Automated Inventory Scans
- SCAP
- Endpoint Detection/Response (EDR)
- Standards Compliance Metrics

- Use Common Secure Configurations for Settings
- Centralize Policy and Common Secure Configurations for Configuration Settings
- Tailor Secure Configurations According to System/Component Function and Role
- Eliminate Unnecessary Ports, Services and protocols (Least Functionality)
- Limit the use of Remote Connections
- Implement endpoint Protection Platforms
  - Anti-malware, Host-Based Firewalls, Host-Based IDS/IPS
  - Restrict mobile code use
- Use Cryptography
- Develop a Patch Management Process
- Control Software Installation

## 3.4.1 – SYSTEM BASELINING

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

### Objectives:

- a. A baseline configuration is established
- b. The baseline configuration includes hardware, software, firmware, and documentation
- c. The baseline is maintained (reviewed and updated) throughout the system development life cycle.
- d. A system inventory is established.
- e. The system inventory includes hardware, software, firmware, and documentation
- f. The inventory is maintained (reviewed and updated) throughout the system development lifecycle.

### What To Look For:

1. Policy/Procedure documentation on baseline configurations and system inventory
2. Standardized baseline configurations for servers, workstations, laptops, routers, switches, printers etc. Demonstration of baseline configurations to show hardware configurations, minimum OS and software versions and patch levels allowed, minimum firmware versions and network information.
3. Demonstration of system inventory tool(s) showing how inventory is managed maintained and that it consists of hardware, software, firmware, and documentation.
4. Change tickets, meeting minutes, emails etc. showing that baseline configurations and system inventory are reviewed and updated throughout SDLC.

### Resources:

1. Configuration Management Software
2. STIGS, GPOs, CIS Top 20 Benchmarks

## 3.4.2 – SECURITY CONFIGURATION ENFORCEMENT

Establish and enforce security configuration settings for information technology products employed in organizational systems.

### Objectives:

- a. Security Configuration settings for information technology products employed in the system are established and included in the baseline configuration.
- b. Security Configuration settings for information technology products employed in the system are enforced

### What To Look For:

1. Artifacts or documentation of what security settings are included as part of the baseline configurations (system hardening)
2. Demonstration of security settings are enforced

### Best Practices/Resources:

1. System hardening – removing all ports, protocols, programs, services, functions not required
2. Firewall rules, GPOs, CIS Top 20 Benchmarks, STIGs

*\* Impacts 3.13.2, 3.4.1*

## 3.4.3 – SYSTEM CHANGE MANAGEMENT

Track, review, approve or disapprove, and log changes to organizational systems.

### Objectives:

- a. Changes to the system are tracked
- b. Changes to the system are reviewed
- c. Changes to the system are approved or disapproved
- d. Changes to the system are logged

### What To Look For:

1. Documentation on Change Management Process
2. Demonstration of how changes are tracked (manual or tool used); how changes are reviewed, approved/disapproved and logged (Show sample change tickets)

### Best Practices/Tools Used:

1. Change Control Board (CCB)
2. Change tickets show requestor, approver, dates, severity, systems affected, who performed the work etc.
3. Configuration Management Software, Change Logs, Email, Spreadsheet



## 3.4.4 – SECURITY IMPACT ANALYSIS

Analyze the security impact of changes prior to implementation.

### **Objective:**

Determine if the security impact of changes to the system is analyzed prior to implementation.

### **What To Look For:**

Artifact (change ticket, meeting minutes, email, CCB report) showing that security impact of change requests are reviewed before implementation

### **Best Practices/Lessons Learned**

1. A Security POC as part of the CCB
2. Testing changes in non-production/sandbox environment before doing it in production.

\* *Impacts 3.11.1, 3.12.1, 3.14.1*

## 3.4.5 – ACCESS RESTRICTIONS FOR CHANGE

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

### Objectives:

[a],[b], [c],[d] Physical access restrictions associated with changes to the system are defined, documented, approved and enforced

[e],[f],[g],[h] Logical access restrictions associated with changes to the system are defined, documented, approved and enforced

### What to look for:

Policy/procedure documentation defining physical and logical access restrictions:

1. Ability to make changes is limited to authorized personnel
  1. Define, identify and document personnel that are allowed to make physical/logical changes to hardware, software, firmware etc.
  2. What tools/mechanisms are used to grant authorized access and prevent unauthorized access
2. Demonstrate physical access restrictions (onsite) – fencing, gates, guards, badges, proximity cards, physical/cypher lock keys and who has access. Demo proximity card software showing who has access to which doors and rooms
3. Demonstrate logical access restrictions (privileged access for authorized individuals) like Directory Service role-based access

### Best Practices/Tools Used

1. Physical Access: Proximity card readers, HID, key fobs, cypher locks, physical keys; security guards
2. Logical Access: Directory Services, VPN, privileged access to specific systems

## 3.4.6 – LEAST FUNCTIONALITY

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

### Objectives:

- a. Essential system capabilities are defined based on the principle of least functionality
- b. The system is configured to provide only the defined essential capabilities

### What To Look For:

1. Configuration management policy, plan or procedure defining least functionality (systems are configured to perform only the function it needs to, everything else is disabled).
2. Demonstrate configuration settings to show that systems only perform the required function

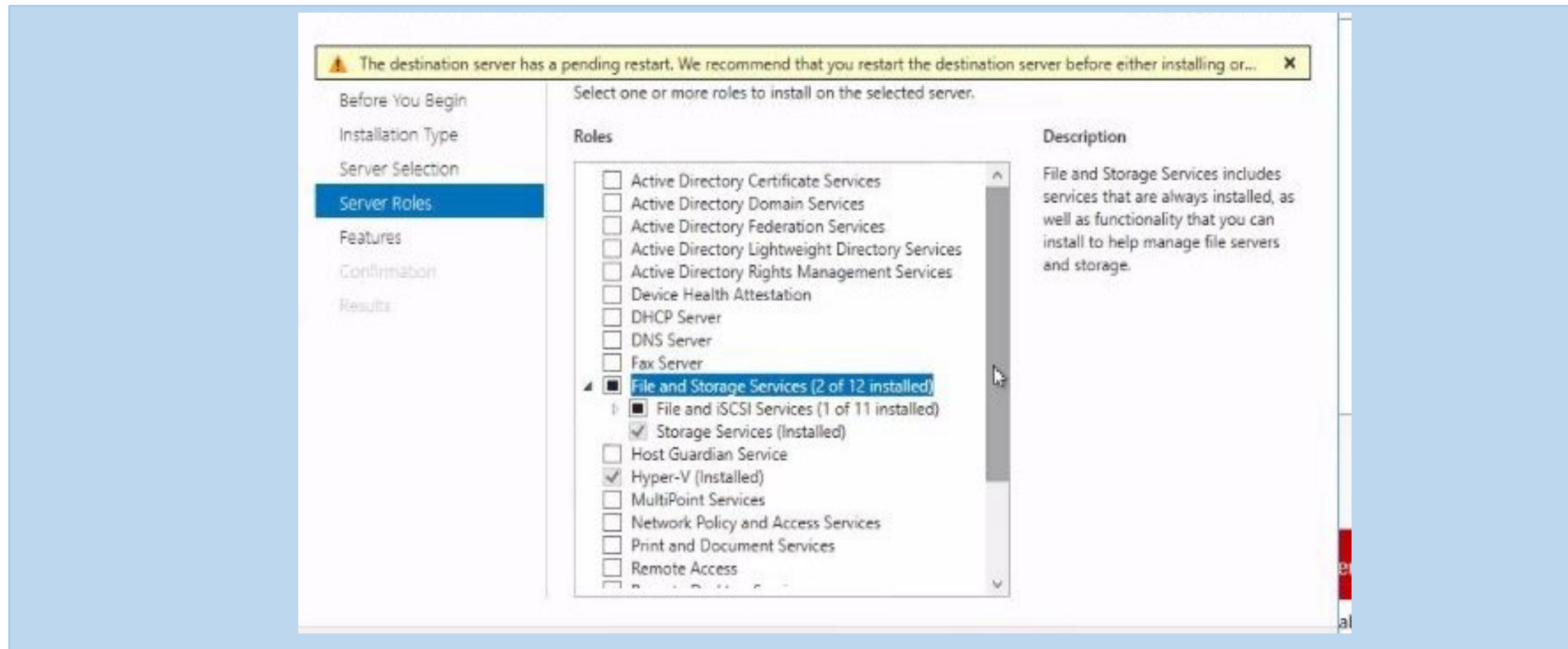
### Best Practices/Tools:

Tools: STIGs, CIS Benchmarks, GPOs, Server Role configurations in system settings

Best Practice: Servers must perform only one function. Example, a server designated as a domain controller, email server, file server etc. should have all other irrelevant services disabled

## 3.4.6 – LEAST FUNCTIONALITY

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.



The screenshot shows the Windows Server Roles and Features console. A yellow warning banner at the top states: "The destination server has a pending restart. We recommend that you restart the destination server before either installing or...". The left sidebar contains navigation options: "Before You Begin", "Installation Type", "Server Selection", "Server Roles" (selected), "Features", "Confirmation", and "Results". The main area is titled "Select one or more roles to install on the selected server." and contains a list of roles with checkboxes. The "File and Storage Services" role is expanded, showing sub-roles: "File and iSCSI Services (1 of 11 installed)" and "Storage Services (Installed)". The "Storage Services" sub-role is checked. The description for "File and Storage Services" is: "File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage."

| Roles   | Description   |
|---|---|
| <input type="checkbox"/> Active Directory Certificate Services                    | File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage. |
| <input type="checkbox"/> Active Directory Domain Services                         |   |
| <input type="checkbox"/> Active Directory Federation Services                     |   |
| <input type="checkbox"/> Active Directory Lightweight Directory Services          |   |
| <input type="checkbox"/> Active Directory Rights Management Services              |   |
| <input type="checkbox"/> Device Health Attestation                                |   |
| <input type="checkbox"/> DHCP Server  |   |
| <input type="checkbox"/> DNS Server   |   |
| <input type="checkbox"/> Fax Server   |   |
| <input checked="" type="checkbox"/> File and Storage Services (2 of 12 installed) |   |
| <input checked="" type="checkbox"/> File and iSCSI Services (1 of 11 installed)   |   |
| <input checked="" type="checkbox"/> Storage Services (Installed)                  |   |

## 3.4.7 – NONESSENTIAL FUNCTIONALITY

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

### Objectives:

[a],[d],[g],[j],[m] Define essential programs, functions, ports, protocols, and services

[b],[e],[h],[k],[n] Define nonessential programs, functions, ports, protocols, and services

[c],[f],[i],[l],[o] The use of nonessential programs, functions, ports, protocols, and services is restricted, disabled, or prevented as defined

### What To Look For:

1. Configuration Mgmt policy, plan, or procedure documentation that defines what an organization considers to be essential and non-essential programs, functions, ports, protocols and services.
2. Restricting roles allowed to perform program execution, prohibit program auto-execution, restricting program instances that can execute at the same time.

### Best Practices/Tools

1 Restrict programs/services like Bluetooth, peer-to-peer networking, internet connection sharing, SSDP Discovery, Routing and Remote Access and insecure ports/protocols like telnet, POP, FTP, SNMP, IMAP on a server

2 Tools include: GPOs, CIS Benchmarks, STIGs, router and firewall rules, host-based firewall, OS Configurations, MS InTune.

\* *Impacts 3.13.6, 3.14.6*

## 3.4.7 – NONESSENTIAL FUNCTIONALITY

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

### Examples of Non-Essential Protocols, Services and Programs

| Protocol          | Port            | Functions & Services          | Programs          |
|-------------------|-----------------|-------------------------------|-------------------|
| Telnet            | 23 (Telnet)     | App Store                     | Internet Explorer |
| POP               | 110 (POP)       | NetTcpPortSharing             | IIS               |
| FTP               | 20, 21 (FTP)    | Internet Sharing              | Freeware          |
| SNMP              | 161, 162 (SNMP) | USB Drive (Removable Storage) | Gaming / Xbox     |
| IMAP              | 143 (IMAP)      | Email (Client or Server)      |                   |
| ICMP (Echo Reply) |                 | File Downloads (Mobile)       |                   |
|                   |                 | HomeGroup                     |                   |
|                   |                 | Local Storage Capability      |                   |
|                   |                 | Peer-to-Peer Networking       |                   |
|                   |                 | SSDP Discovery                |                   |
|                   |                 | Routing                       |                   |
|                   |                 | Remote Access                 |                   |
|                   |                 | Printing                      |                   |
|                   |                 |                               |                   |

## 3.4.8 – APPLICATION EXECUTION POLICY

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

### Objectives:

- a. A policy specifying whether whitelisting or blacklisting is to be implemented is specified.
- b. The software allowed to execute under whitelisting or denied use under blacklisting is specified.
- c. Whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

### What To Look For:

1. Configuration management policy specifying whether an organization uses whitelisting or blacklisting.
2. An artifact or document listing all the whitelisted or blacklisted software based on which one is used.
3. Demonstrate technical control used to allow only whitelisted software and block everything else or block blacklisted software and allow installation and running of all other software.

### Resources:

Privilege Access Management, Application Packaging software, Proxy Server, Application whitelisting

## 3.4.9 – USER-INSTALLED SOFTWARE

Control and monitor user-installed software.

### Objectives:

- a. A policy for controlling the installation of software by users is established.
- b. Installation of software by users is controlled based on the established policy.
- c. Installation of software by users is monitored.

### What To Look For:

1. CM policy/procedure addressing user-installed software.
2. Administrative or technical controls that address user-installed software. Limiting software installation to privileged users. How are browser updates, browser scripts/add-ons and software updates managed.
3. Tool/mechanism used to monitor installation of software by users.

### Best Practices/Tools Used:

1. User Access Control (UAC), Restricting software installation to privileged users.
2. CM software, Asset Management software, Privilege Access Management, GPOs