CIS Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile, network devices, non-computing/IoT devices, and servers) and software (operating systems and applications).

Why is this CIS Control Critical?

As delivered by manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease of deployment and ease of use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through the configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked” to allow the installation of new software or to support new operational requirements.

4.1: Establish and Maintain a Secure Configuration Process

Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV2`: Authorized software inventory
2. `GV1`: Enterprise asset inventory
3. `GV3`: Configuration Standard: This should include any enterprise-approved deviations from industry-standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
4. Date of last review and update of configuration standard

Operations

1. Identify whether Input 2 exists:
    1. If it exists, M1 = 1
    2. If it does not exist, M1 = 0
2. Identify and enumerate end-user devices, including portable and mobile, non-computing/IoT devices, and servers in `GV1` (M2)
3. Using the output of Operation 2 (M2), identify and enumerate the software installed on the assets using `GV2` (M3)
4. For each software identified in Operation 3 (M3):
    1. Enumerate software that is listed in the configuration standard `GV3` (M4)
    2. Enumerate software that is not listed in the configuration standard `GV3` (M5)
5. Compare the current date to the date provided in Input 4. Note the timeframe in months (M6)

Measures

- M1 = Output of Operation 1
- M2 = Count of applicable enterprise assets
- M3 = Count of software installed on applicable enterprise assets
- M4 = Count of software that is listed in the configuration standard
- M5 = Count of software that is not listed in the configuration standard
- M6 = Timeframe since last review and update in months

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M6 is greater than twelve, this Safeguard is measured at 0 and receives a failing score. The other metrics don't apply.

Standard Configuration Coverage

Metric	**The percentage of authorized software with secure configuration standards documented and maintained.**
Calculation	`M4 / M3`

4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Asset Type	Security Function	Implementation Groups
Documentation	Govern	1, 2, 3

Dependencies

- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV2`: Authorized software inventory
2. `GV1`: Enterprise asset inventory
3. `GV3`: Configuration Standard: This should include any enterprise approved deviations from industry standard baselines such as CIS benchmarks, DISA Security Technical Implementation Guides (STIGs), or U.S. government configuration baselines (USGCB).
4. Date of last review and update of the configuration standard

Operations

1. Identify whether Input 2 exists:
    1. If it exists, M1 = 1
    2. If it does not exist, M1 = 0
2. Identify and enumerate network infrastructure assets in `GV1` (M2)
3. Using the output of Operation 2 (M2), identify and enumerate the software installed on the assets using `GV2` (M3)
4. For each software identified in Operation 3 (M3):
    1. Enumerate software that is listed in the configuration standard `GV3` (M4)
    2. Enumerate software that is not listed in the configuration standard `GV3` (M5)
5. Compare the current date to the date provided in Input 4. Note the timeframe in months (M6)

Measures

- M1 = Output of Operation 1
- M2 = Count of applicable enterprise assets
- M3 = Count of software installed on applicable enterprise assets
- M4 = Count of software that is listed in the configuration standard
- M5 = Count of software that is not listed in the configuration standard

- M6 = Timeframe since last review and update in months

Metrics

- If M1 is 0, this Safeguard receives a failing score. The other metrics don't apply.
- If M6 is greater than twelve, this Safeguard is measured at 0 and receives a failing score. The other metrics don't apply.

Standard Configuration Coverage

Metric	**The percentage of authorized software with secure configuration standards documented and maintained.**
Calculation	`M4 / M3`

4.3: Configure Automatic Session Locking on Enterprise Assets

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized Software Inventory
3. `GV3`: Configuration standard

Operations

1. Identify and enumerate assets within `GV1` that support automatic locking due to inactivity (M1)

2. Use `GV5` to identify and enumerate assets from Operation 1 with authorized software installed (M2)

3. Check the configurations for the software using `GV3`:

1. For general computing assets, enumerate those assets with properly configured automatic locking (15 minutes or less) (M3)
2. For general computing assets, enumerate those assets with improperly configured automatic locking (greater than 15 minutes) (M4)
3. For mobile assets, enumerate those assets with properly configured automatic locking (2 minutes or less) (M5)
4. For mobile assets, enumerate those assets with improperly configured automatic locking (greater than 2 minutes) (M6)

Measures

- M1 = Count of assets capable of supporting automatic lockout
- M2 = Count of assets with authorized software installed to allow a lockout
- M3 = Count of general computing assets with properly configured lockout
- M4 = Count of general computing assets with improperly configured lockout
- M5 = Count of mobile assets with properly configured lockout
- M6 = Count of mobile assets with improperly configured lockout

Metrics

Properly Configured Assets

Metric	**The percentage of assets properly configured for automatic lockout.**
Calculation	`(M3 + M5) / M1`

4.4: Implement and Manage a Firewall on Servers

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, an operating system firewall, or a third-party firewall agent.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standard

Operations

1. Identify and enumerate servers capable of hosting a firewall using `GV1` (M1)
2. Identify and enumerate applications capable of hosting a firewall using `GV5` (M2)
3. Using configuration standards to check if firewalls are properly configured:
    1. Enumerate servers from Operation 1 with properly configured firewalls (M3)
    2. Enumerate servers from Operation 1 with improperly configured firewalls (M4)
    3. Enumerate applications from Operation 2 with properly configured firewalls (M3)
    4. Enumerate applications from Operation 2 with improperly configured firewalls (M4)

Measures

- M1 = Count of servers enterprise assets capable of hosting a firewall
- M2 = Count of applications software capable of hosting a firewall
- M3 = Count of servers with properly configured firewalls
- M4 = Count of servers with improperly configured firewalls
- M5 = Count of applications with properly configured firewalls
- M6 = Count of applications with improperly configured firewalls

Metrics

Implementation of Firewalls

Metric	**The percentage of properly configured firewalls within the enterprise**
Calculation	`(M3 + M5) / (M1 + M2)`

4.5: Implement and Manage a Firewall on End-User Devices

Implement and manage a host-based firewall or port-filtering tool on end-user devices with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Type	Security Function	Implementation Groups
Devices	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV1: Enterprise asset inventory
2. GV5: Authorized software inventory
3. GV3: Configuration standard

Operations

1. Identify and enumerate end-user devices capable of hosting a firewall or a deny rule using GV1 (M1)

2. Using configuration standards GV3 to check if firewalls or deny rules are properly configured on end-user devices:

    1. Enumerate assets from Operation 1 with properly configured firewalls or a configured default deny rule (M3)
    2. Enumerate assets from Operation 1 with improperly configured firewalls and lacking a configured default deny rule (M4)

Measures

- M1 = Count of end-user devices capable of hosting a firewall
- M2 = Count of end-user devices with a properly configured firewall or default deny rule
- M3 = Count of end-user devices with an improperly configured firewall and lacking a configured default deny rule

Metrics

Coverage

Metric	**The percentage of properly configured firewalls or deny rule on end-user devices**
Calculation	M2 / M1

4.6: Securely Manage Enterprise Assets and Software

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

Asset Type	**Security Function**	**Implementation Groups**
Devices	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standard

Operations

1. Using `GV5`, identify and enumerate authorized management software (M1)

2. Using `GV1`, identify and enumerate assets capable of supporting management software (M2)

3. Using the output of Operations 1 and 2, identify and enumerate assets with authorized management software installed (M3)

4. Using configuration standards `GV3` to check if management software is configured properly:

    1. Enumerate assets from Operation 3 with properly configured management software (M4)
    2. Enumerate assets from Operation 1 with improperly configured management software (M5)

Measures

- M1 = Count of authorized management software
- M2 = Count of enterprise assets capable of supporting management software
- M3 = Count of assets with authorized management software installed
- M4 = Count of assets with properly configured management software
- M5 = Count of assets with improperly configured management software

Metrics

Coverage

Metric	**The percentage of assets with properly configured authorized management software**
Calculation	`M4 / M2`

4.7: Manage Default Accounts on Enterprise Assets and Software

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

Asset Type	Security Function	Implementation Groups
Users	Protect	1, 2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 5.2: Use Unique Passwords

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV20`: Unique password policy

Operations

1. Use `GV5` to identify and enumerate authorized operating software, applications, and third-party software that contain default accounts (M1)

2. Use `GV1` to identify and enumerate assets with software from Operation 1, installed (M2)

3. For each asset identified in Operation 2, enumerate default accounts (M3)

4. Check if default accounts can be disabled:

    1. Enumerate accounts that are disabled (M4)
    2. Enumerate accounts that are enabled (M5)

5. If accounts cannot be disabled, ensure to change default passwords according to `GV20`: the enterprise's unique password policy:

    1. Enumerate accounts with changed passwords (M6)

Measures

- M1 = Count of software that uses default accounts
- M2 = Count of assets with software installed that uses default accounts
- M3 = Count of default accounts identified
- M4 = Count of default accounts that have been disabled
- M5 = Count of default accounts that are enabled
- M6 = Count of enabled default accounts with changed passwords

Metrics

Unusable Default Accounts

Metric	**The percentage of default accounts that have been rendered unusable**
Calculation	`M4 + M6 / M3`

4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standard

Operations

1. Use `GV5` to identify and enumerate authorized services (M1)

2. Use `GV1` to identify and enumerate services on enterprise assets (M2)

3. Compare outputs from Operations 1 and 2:

    1. Identify and enumerate authorized services on assets (M3)
    2. Identify and enumerate unauthorized services on assets (M4)

4. For authorized services in Operation 3.2, use `GV3` to check configurations:

    1. Identify and enumerate services that are configured correctly (disabled) (M5)
    2. Identify and enumerate services that are configured improperly (enabled) (M6)

Measures

- M1 = Count of authorized services
- M2 = Count of services on enterprise assets

- M3 = Count of authorized services on assets
- M4 = Count of unauthorized services on assets
- M5 = Count of unauthorized services that are disabled
- M6 = Count of unauthorized services that are enabled

Metrics

Compliant Services

Metric	**The percentage of services installed/running that are enterprise essential**
Calculation	`(M3 + M5) / M2`

Non-compliant Services

Metric	**The percentage of services installed/running that are enterprise essential**
Calculation	`M6 / M2`

4.9: Configure Trusted DNS Servers on Enterprise Assets

Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV1`: Enterprise asset inventory
2. `GV3`: Configuration standard

Operations

1. Use `GV1` to identify and enumerate authorized DNS servers (M1)

2. Use `GV1` to identify and enumerate assets configured for authorized DNS servers (M2)

3. Use GV3 to check the configuration of DNS servers identified on assets in Operation 2:

    1. Identify and enumerate assets with DNS servers that are properly configured (M3)
    2. Identify and enumerate assets with DNS servers that are improperly configured (M4)

Measures

- M1 = Count of authorized DNS servers
- M2 = Count of enterprise assets configured for DNS servers
- M3 = Count of assets with properly configured DNS servers
- M4 = Count of assets with improperly configured DNS servers

Metrics

Coverage

Metric	The percentage of assets with properly configured DNS servers
Calculation	M3 / M2

4.10: Enforce Automatic Device Lockout on Portable End-User Devices

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

Asset Type	Security Function	Implementation Groups
Devices	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV1: Enterprise asset inventory
2. GV3: Configuration standards

Operations

1. Use `GV1` to identify and enumerate all portable devices (M1)

2. Use `GV3` to check failed authentication configuration for all portable devices:

    1. Identify and enumerate failed authentication on laptops that are properly configured (20 failed attempts or less) (M2)
    2. Identify and enumerate failed authentication on laptops that are not properly configured (greater than 20 failed attempts) (M3)
    3. Identify and enumerate failed authentication on mobile devices that are properly configured (10 failed attempts or less) (M4)
    4. Identify and enumerate failed authentication on mobile devices that are not properly configured (greater than 10 failed attempts) (M5)

Measures

- M1 = Count of portable devices
- M2 = Count of properly configured laptops
- M3 = Count of improperly configured laptops
- M4 = Count of properly configured mobile devices
- M5 = Count of improperly configured mobile devices

Metrics

Compliance of Default Lockout

Metric	**The percentage of portable devices with properly configured failed authentication.**
Calculation	`(M2 + M4) / M1`

4.11: Enforce Remote Wipe Capability on Portable End-User Devices

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Asset Type	Security Function	Implementation Groups
Data	Protect	2, 3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. GV21: Portable end-user devices
2. GV3: Configuration standards

Operations

1. Use GV21 to identify and enumerate portable end-user devices that support remote wipe (M1)

2. Use GV3 to check configuration for remote wipe on portable devices capable of supporting as identified in Operation 1:

    1. Identify and enumerate portable devices with properly configured remote wipe (M2)
    2. Identify and enumerate portable devices with improperly configured remote wipe (M3)

Measures

- M1 = Count of portable devices capable of supporting remote wipe
- M2 = Count of properly configured portable devices
- M3 = Count of improperly configured portable devices

Metrics

Compliance of Remote Wipe

Metric	**The percentage of portable devices with properly configured remote wipe.**
Calculation	M2 / M1

4.12: Separate Enterprise Workspaces on Mobile End-User Devices

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

Asset Type	Security Function	Implementation Groups
Data	Protect	3

Dependencies

- Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
- Safeguard 2.1: Establish and Maintain a Software Inventory
- Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Inputs

1. `GV21`: Portable end-user devices
2. `GV5`: Authorized software inventory
3. `GV3`: Configuration standards

Operations

1. Use `GV5` to identify and enumerate authorized mobile device management software (M1)

2. Use `GV21` to identify mobile devices capable of supporting mobile device management software (M2)

3. Compare the output of Operations 1 and 2:

    1. Identify and enumerate mobile devices with authorized mobile device management software (M3)
    2. Identify and enumerate mobile devices without authorized mobile device management software (M4)

4. Use `GV3` to check configurations of mobile devices with mobile device management software:

    1. Identify and enumerate mobile devices with properly configured mobile device management software to separate enterprise workspace (M5)
    2. Identify and enumerate mobile devices with improperly configured mobile device management software (M6)

Measures

- M1 = Count of authorized mobile device management software
- M2 = Count of mobile devices capable of supporting mobile device management software
- M3 = Count of mobile devices with mobile device management software
- M4 = Count of mobile devices without mobile device management software
- M5 = Count of assets with properly configured mobile device management software
- M6 = Count of assets with improperly configured mobile device management software

Metrics

Compliance of Separation of Enterprise Workspace

Metric	**The percentage of mobile devices with properly separated enterprise workspace.**
Calculation	`M5 / M2`