CIS Controls v7
The Center for Internet Security
https://www.cisecurity.org/controls/

Partially Translated to Thai  by Songkrant Muneenaem CC.PSU. 1May2018
Cybersecurity Best Practices

CIS Controls and CIS Benchmarks are global industry best practices endorsed by leading IT security vendors and governing bodies.

Secure Your Organization

CIS Controls

IT security leaders use CIS Controls to quickly establish the protections providing the highest payoff in their organizations. They guide you through a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

Secure Your Systems & Platforms

CIS Benchmarks

Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks. They are continuously verified by a volunteer IT community to combat evolving cybersecurity challenges.
CIS Control v7
Launched on March 19, 2018
from
Critical Security Controls for Effective Cyber Defense (CSC)
Version 6.1 on August 31, 2016
First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises
7 Key Principles

When designing the latest version of the CIS Controls, our community relied on 7 key principles to guide the development process.

1. Improve the consistency and simplify the wording of each sub-control
2. Implement "one ask" per sub-control
3. Bring more focus on authentication, encryption, and application whitelisting
4. Account for improvements in security technology and emerging security problems
5. Better align with other frameworks (such as the NIST CSF)
6. Support the development of related products (e.g. measurements/metrics, implementation guides)
7. Identify types of CIS controls (basic, foundational, and organizational)
There are a number of authoritative information security standards that organizations can and do use to develop their programs. These standards are updated periodically and are aligned on the basic security process and the defensive controls to be implemented. Among the best known standards are those published by the National Institute of Standards and Technology (NIST), in particular Special Publication 800-53 and the Framework for Improving Critical Infrastructure Cybersecurity. The International Organization for Standardization’s ISO/IEC 27002:2013 is also foundational. In addition to the comprehensive technical standards, there are catalogs and lists of known security vulnerabilities.

While there is no dearth of information on the security risk management process and standards for security controls, synthesizing all of this information and prioritizing the actions to take can be a challenge. The Center for Internet Security’s Critical Security Controls for Effective Cyber Defense (the Controls) is designed to address this challenge.

### The Critical Security Controls Master Mapping (Excerpt)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CSC 1:</strong> Inventory of Authorized and Unauthorized Devices</td>
<td>CA-7: Continuous Monitoring&lt;br&gt;CM-8: Information System Component Inventory&lt;br&gt;IA-3: Device Identification and Authentication&lt;br&gt;SA-4: Acquisition Process&lt;br&gt;SC-17: Public Key Infrastructure Certificates&lt;br&gt;SI-4: Information System Monitoring&lt;br&gt;PM-5: Information System Inventory</td>
<td>ID.AM-1&lt;br&gt;ID.AM-3&lt;br&gt;PR.DS-3</td>
<td>A.8.1.1&lt;br&gt;A.9.1.2&lt;br&gt;A.13.1.1</td>
<td>164.310(b): Workstation Use - R&lt;br&gt;164.310(c): Workstation Security - R</td>
<td>Host Security User Equipment Security (Workstation, Laptop, Handheld)</td>
<td>2.4</td>
</tr>
</tbody>
</table>
6 Basic CIS Controls
Basic CIS Controls

1 Inventory and Control of Hardware Assets

(บันทึกรายการและความคุมทรัพย์สินที่เป็นฮาร์ดแวร์)
CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This CIS Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise’s network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise’s network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. But attackers have shown the ability, patience, and willingness to “inventory and control” our assets at very large scale in order to support their opportunities.

Managed control of all devices also plays a critical role in planning and executing system backup, incident response, and recovery.
<table>
<thead>
<tr>
<th>Sub-Control</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Control Title</th>
<th>Control Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Devices</td>
<td>Identify</td>
<td>Utilize an Active Discovery Tool</td>
<td>Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.</td>
</tr>
<tr>
<td>1.2</td>
<td>Devices</td>
<td>Identify</td>
<td>Use a Passive Asset Discovery Tool</td>
<td>Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Devices</td>
<td>Use DHCP Logging to Update Asset Inventory</td>
<td>Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Devices</td>
<td>Maintain Detailed Asset Inventory</td>
<td>Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Devices</td>
<td>Maintain Asset Inventory Information</td>
<td>Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Devices</td>
<td>Protect</td>
<td>Deploy Port Level Access Control</td>
<td>Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.</td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
<td>---------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.6</td>
<td>Devices</td>
<td>Respond</td>
<td>Address Unauthorized Assets</td>
<td>Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.</td>
</tr>
<tr>
<td>1.7</td>
<td>Devices</td>
<td>Protect</td>
<td>Utilize Client Certificates to Authenticate Hardware Assets</td>
<td>Use client certificates to authenticate hardware assets connecting to the organization's trusted network.</td>
</tr>
</tbody>
</table>
CIS Control 1: Procedures and Tools

This Control requires both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organizations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

Maintaining a current and accurate view of IT assets is an ongoing and dynamic process. Organizations can actively scan on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks.

In conducting inventory scans, scanning tools could send traditional ping packets (ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.
In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Many organizations also pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization’s asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems very dynamic. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization’s asset inventory.
Basic CIS Controls

2 Inventory and Control of Software Assets

(บันทึกรายการและควบคุมทรัพย์สินที่เป็นซอฟต์แวร์)
Inventory and Control of Software Assets
Basic CIS Controls

3 Continuous Vulnerability Management

(จัดการกับช่องโหว่ย่างต่อเนื่อง)
Continuous Vulnerability Management
Basic CIS Controls

4 Controlled Use of Administrative Privileges

(ควบคุมการใช้สิทธิพิเศษในการบริหารระบบ)
Controlled Use of Administrative Privileges
Basic CIS Controls

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

(กำหนดค่าที่ปลอดภัยให้กับฮาร์ดแวร์และซอฟท์แวร์ บนอุปกรณ์พกพา แล็ปท็อป เวิร์กสเตชัน และเซิร์ฟเวอร์)
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

CIS Control 5: System Entity Relationship Diagram
Basic CIS Controls

6 Maintenance, Monitoring and Analysis of Audit Logs

(บำรุงรักษา เฝ้าสังเกต และวิเคราะห์ ข้อมูลล็อกการใช้งานต่างๆ)
Maintenance, Monitoring and Analysis of Audit Logs
10 Foundational CIS Controls
Foundational CIS Controls

7 Email and Web Browser Protections

(ป้องกันอีเมลและเว็บเบราว์เซอร์)
Email and Web Browser Protections
8 Malware Defenses

Malicious software (Longdo Dictionary)
ออกแบบมาด้วยจุดประสงค์แอบแฝงบางอย่าง จุดประสงค์ดังกล่าวอาจจะเพื่อสร้างหน้าต่างโฆษณาที่เปิดขึ้นมาเองโดยอัตโนมัติ ด้วยความหวังที่ว่าจะให้คุณกดเข้าไปและสร้างรายได้ให้กับบุคคลเหล่านั้น หรือ รูปแบบของ spyware และ ไวรัสคอมพิวเตอร์ที่สามารถใช้เพื่อการขโมยตัวตนของคุณบนอินเตอร์เน็ต หรือ ติดตามกิจกรรมต่างของคุณ
Malware Defenses

CIS Control 8: System Entity Relationship Diagram
Foundational CIS Controls

9 Limitation and Control of Network Ports, Protocols, and Services

(จำกัดและควบคุม พอร์ต โปรโตคอล และบริการต่างๆ บนเครือข่าย)
Limitation and Control of Network Ports, Protocols, and Services
Foundational CIS Controls

10 Data Recovery Capabilities

(ต้องมีความสามารถคืนข้อมูลกลับมาได้)
CIS Control 10: System Entity Relationship Diagram

Data Recovery Capabilities
Foundational CIS Controls

11 Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

(กำหนดค่าที่ปลอดภัยให้กับอุปกรณ์เครือข่ายต่างๆ เช่น ไฟร์วอลล์ เราเตอร์ และสวิตช์)
Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
Foundational CIS Controls

12 Boundary Defense

(ป้องกันเขตเครือข่าย)
Foundational CIS Controls

13 Data Protection

(ปกป้องข้อมูล)
CIS Control 13: System Entity Relationship Diagram

Data Protection
Foundational CIS Controls

14 Controlled Access Based on the Need to Know

(ควบคุมให้เข้าถึงได้เฉพาะสิ่งจำเป็น)
CIS Control 14: System Entity Relationship Diagram

Controlled Access Based on the Need to Know
Foundational CIS Controls

15 Wireless Access Control

(ควบคุมการเข้าถึงผ่านทางระบบไร้สาย)
Wireless Access Control

CIS Control 15: System Entity Relationship Diagram
16 Account Monitoring and Control
(เฝ้าสังเกตและควบคุม บัญชีผู้ใช้)
Account Monitoring and Control

CIS Control 16: System Entity Relationship Diagram

- Identity & Access Management System
- Workforce Members
- Multi-Factor Authentication
- Configuration Enforcement System
- Computing Systems
- Alerting / Reporting Analytics System
<table>
<thead>
<tr>
<th>Basic</th>
<th>Foundational</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory and Control of Hardware Assets</td>
<td>7. Email and Web Browser Protections</td>
<td>17. Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
<td></td>
</tr>
</tbody>
</table>
4 Organizational CIS Controls
Organizational CIS Controls

17 Implement a Security Awareness and Training Program

(ดำเนินการฝึกอบรมสร้างความตระหนักรู้ด้านความปลอดภัย)
Implement a Security Awareness and Training Program
Organizational CIS Controls

18 Application Software Security

(จัดการความปลอดภัยของซอฟท์แวร์โปรแกรมประยุกต์)
CIS Control 18: System Entity Relationship Diagram

Application Software Security

Alerting / Reporting Analytics System

Secure Coding Standards

Education Plans / Training Programs

Code Analysis System

Web Application Firewall (WAF)

Computing Systems
Organizational CIS Controls

19 Incident Response and Management
(จัดการและตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย)
CIS Control 19: System Entity Relationship Diagram

Incident Response and Management

Alerting / Reporting Analytics System

Third Party Authorities

Incident Management Plans

Workforce Members
Organizational CIS Controls

20 Penetration Tests and Red Team Exercises

(ทดสอบเจาะส่วนต่างๆ และฝึกซ้อมบุกกรุกทั้งระบบ)
Penetration Tests and Red Team Exercises

CIS Control 20 System Entity Relationship Diagram
<table>
<thead>
<tr>
<th>Basic</th>
<th>Foundational</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory and Control of Hardware Assets</td>
<td>7. Email and Web Browser Protections</td>
<td>17. Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. Data Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14. Controlled Access Based on the Need to Know</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15. Wireless Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16. Account Monitoring and Control</td>
<td></td>
</tr>
</tbody>
</table>
Follow our prioritized set of actions to protect your organization and data from known cyber attack vectors.

Download all CIS Controls (PDF) →

New in CIS Controls Version 7: one “ask” per sub-control for easier implementation

CIS RAM is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls. Download CIS RAM
CIS RAM (Center for Internet Security® Risk Assessment Method) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls™ cybersecurity best practices. CIS RAM provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.
Cybersecurity Best Practices

CIS Controls and CIS Benchmarks are global industry best practices endorsed by leading IT security vendors and governing bodies.

Secure Your Organization

CIS Controls

IT security leaders use CIS Controls to quickly establish the protections providing the highest payoff in their organizations. They guide you through a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

Secure Your Systems & Platforms

CIS Benchmarks™

Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks. They are continuously verified by a volunteer IT community to combat evolving cybersecurity challenges.
With our global community of cybersecurity experts, we’ve developed CIS Benchmarks: 100+ configuration guidelines for various technology groups to safeguard systems against today’s evolving cyber threats.
CIS Benchmarks: Secure Your Systems & Platforms

Proven guidelines will enable you to safeguard operating systems, software and networks that are most vulnerable to cyber attacks.

They are continuously verified by a volunteer IT community to combat evolving cybersecurity challenges.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution Independent Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Desktop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debian Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SharePoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM DB2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIND</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CentOS Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple OS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Safari Browser</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
</tr>
<tr>
<td>Select Platform</td>
<td>Microsoft Azure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Print Devices</td>
<td></td>
</tr>
</tbody>
</table>
CIS Google Chrome Benchmark (for example)
## Benchmarks

The listing below displays all the benchmarks you currently have access to.

<table>
<thead>
<tr>
<th>Title</th>
<th>Version</th>
<th>Status</th>
<th>Community</th>
<th>Collections</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Google Chrome 46 Benchmark [imported]</td>
<td>v1.0.0</td>
<td>Published</td>
<td>CIS Google Chrome Benchmarks</td>
<td>CIS Google Chrome Benchmarks</td>
<td>jkrkoske</td>
</tr>
<tr>
<td>CIS Google Chrome Benchmark</td>
<td>v1.2.0</td>
<td>Published</td>
<td>CIS Google Chrome Benchmarks</td>
<td>CIS Google Chrome Benchmarks</td>
<td>jkrkoske</td>
</tr>
<tr>
<td>CIS Google Chrome Benchmark [imported]</td>
<td>v1.1.0</td>
<td>Published</td>
<td>CIS Google Chrome Benchmarks</td>
<td>CIS Google Chrome Benchmarks</td>
<td>jkrkoske</td>
</tr>
<tr>
<td>CIS Google Chrome Benchmark</td>
<td>v1.3.0</td>
<td>Draft</td>
<td>CIS Google Chrome Benchmarks</td>
<td>CIS Google Chrome Benchmarks</td>
<td>jkrkoske</td>
</tr>
<tr>
<td>CIS Google Chrome Benchmark [imported]</td>
<td>v0.0.1</td>
<td>Draft</td>
<td>CIS Google Chrome Benchmarks</td>
<td>CIS Google Chrome Benchmarks</td>
<td>bfrantz</td>
</tr>
</tbody>
</table>
Chrome 66

**Start**: Mar 27, 2018

**End**: Apr 26, 2018

**Tickets**: 1 / 4

**Description**

**Tickets**

- **Remove deprecated plugin sections**
- **1.3.2 (L1)** Ensure ‘Configure the required domain name for remote access hosts’ is set to ‘Enabled’ -- Unclear Guidance
- **1.1.2** Set ‘Enable alternate error pages’ to Disabled - Rationalie question
- RemoteAccessHostClientDomain deprecated

**Benchmarks**

- **CIS Google Chrome Benchmark v1.3.0**
Continuous Improvement for the latest Google Chrome 66.0.3359.117 as 27Apr2018

CIS Google Chrome 46 Benchmark [imported] v1.0.0 Published 2 years ago on Oct 30th 2015 : tested against Google Chrome v46.0.2490.80m

CIS Google Chrome Benchmark [imported] v1.1.0 Published 2 years ago on Mar 22nd 2016 : tested against Google Chrome v49.0.2623.87m

CIS Google Chrome Benchmark v1.2.0 Published 9 months ago on Jun 30th 2017 : tested against Google Chrome v59.0.3071.86

CIS Google Chrome Benchmark v1.3.0 Draft : tested against Google Chrome v62.0.3202.75
1 Computer Configuration

1.1 Google Chrome

1.1.1 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored)

1.1.2 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)

1.1.3 (L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled' (Scored)

1.1.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)

1.1.5 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)

1.1.6 (L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)

1.1.7 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)

1.1.8 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)

1.1.9 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)

1.1.10 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)
1.1.10 (L1) Ensure ‘import saved passwords from default browser on first run’ is set to ‘Disabled’ (Scored)

Profile Applicability:
- Level 1

Description:
This setting controls if saved passwords from the default browser can be imported.

Rationale:
In Chrome, passwords can be stored in plain-text and revealed by clicking the “show” button next to the password field by going to chrome://settings/passwords/.

Audit:
Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Google\Chrome\ImportSavedPasswords
```

Remediation:
To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative Template (ADM)\Google\Google Chrome\Import saved passwords from default browser on first run
```

Impact:
If this setting is disabled, saved passwords from other browsers are not imported.

Default Value:
Not Configured

CIS Controls:
16 Account Monitoring and Control
Account Monitoring and Control
### Appendix: Summary Table

<table>
<thead>
<tr>
<th>Control</th>
<th>Set Correctly</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.1.1</strong></td>
<td>(L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.2</strong></td>
<td>(L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.3</strong></td>
<td>(L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.4</strong></td>
<td>(L1) Ensure 'Block third party cookies' is set to 'Enabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.5</strong></td>
<td>(L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.6</strong></td>
<td>(L1) Ensure 'Enable AutoFill' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.7</strong></td>
<td>(L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.8</strong></td>
<td>(L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.9</strong></td>
<td>(L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.10</strong></td>
<td>(L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.1.11</strong></td>
<td>(L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.2.1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.2.2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.2.3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.2.4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.3.1</strong></td>
<td>(L2) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.3.2</strong></td>
<td>(L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.3.3</strong></td>
<td>(L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.3.4</strong></td>
<td>(L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Scored)</td>
</tr>
<tr>
<td><strong>1.4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1.4.1</strong></td>
<td>(L2) Ensure 'Default cookies setting is set to 'Enabled' (Keep cookies for the duration of the session)' (Scored)</td>
</tr>
<tr>
<td><strong>1.4.2</strong></td>
<td>(L1) Ensure 'Default Plugin Setting is set to 'Enabled' (Click to Play)' (Scored)</td>
</tr>
</tbody>
</table>
https://www.cisecurity.org/
CIS SecureSuite®
Membership

Start Secure, Stay Secure
A CIS SecureSuite Membership combines and automates the CIS Benchmarks, CIS Controls, and CIS-CAT Pro into one powerful, time-saving cybersecurity resource for businesses, nonprofits, and governmental entities.

- Leverage remediation content for rapid CIS Benchmark implementation
- Connect with CIS staff and developers for technical support

“It is the most important membership for the compliance review of information security available in the market today.”

— Senior Manager, Information Security & Compliance International Public Service & Communications Agency
Information Hub

What's New

⚠️ Advisory • 25 Apr 2018
A Vulnerability in Drupal Could Allow for Remote Code Execution

⚠️ Advisory • 25 Apr 2018
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

⚠️ Advisory • 18 Apr 2018
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

🔍 Blog post • 24 Apr 2018
Cloud Compliance – How to Stay Secure on an Intangible Infrastructure

🔍 Webinar • 17 Apr 2018
GDPR- How CIS can help!

Daily tip

Secure Wireless Networks
Follow these tips to better secure your wireless network:

- Change your network name and the default password.
- Encrypt the data on your network.
- Make sure your firewall is running.
- Disable guest networks.
- Turn off Wi-Fi Protected Setup.
Let's make Internet safe
For
Everyone