**GOVERNOR ERIC J. HOLCOMB'S**
**INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

---

**Author:** Smith, Travis

**Title:** "20 CIS Controls: Control 16 – Account Monitoring and Control"

**Website:** Tripwire

**Organization:** Tripwire

**Date:** 27 March 2018

**URL:** https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-16-account-monitoring/

**Accessed:** 12 July 2019

**Synopsis:** Today, I will be going over Control 16 from version 7 of the top 20 CIS Controls – Account Monitoring and Control. I will go through the thirteen requirements and offer my thoughts on what I've found.

Key Takeaways for Control 16

- **Don't forget the logs.** Enabling a lot of the later sections of this control will require gathering logging data from endpoints into a centralized location such as a SIEM. The security intelligence of the organization will be in your logs, so collect as much as you can without overburdening the tool and/or necessitating that analysts review the logs.
- **Missing password requirements.** The guidance on passwords has been removed from control 16. This is probably a good thing since it has been mostly duplicated by Control 4. If you're looking for guidance on password requirements, look at any major hardening guide or security framework.
- **Block common attacks.** Many common attacks that have been made public hit on a lot of the requirements in control 16. While a zero-day attack gets all of the press at security conferences, attackers are after valid credentials to make their attacks stealthier. Controlling authentication mechanisms and valid accounts is a cornerstone of building a proper security architecture.

# 20 CIS Controls: Control 16 - Account Monitoring and Control

Today, I will be going over Control 16 from version 7 of the top 20 CIS Controls – Account Monitoring and Control. I will go through the thirteen requirements and offer my thoughts on what I've found.

---

## Key Takeaways for Control 16

- **Don't forget the logs**. Enabling a lot of the later sections of this control will require gathering logging data from endpoints into a centralized location such as a SIEM. The security intelligence of the organization will be in your logs, so collect as much as you can without overburdening the tool and/or necessitating that analysts review the logs.
- **Missing password requirements**. The guidance on passwords has been removed from control 16. This is probably a good thing since it has been mostly duplicated by Control 4. If you're looking for guidance on password requirements, look at any major hardening guide or security framework.
- **Block common attacks**. Many common attacks that have been made public hit on a lot of the requirements in control 16. While a zero-day attack gets all of the press at security conferences, attackers are after valid credentials to make their attacks stealthier. Controlling authentication mechanisms and valid accounts is a cornerstone of building a proper security architecture.

---

## Requirement Listing for Control 16

### 1. Maintain an Inventory of Authentication Systems

**Description**: Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.

**Notes**: Relating back to the first two controls, you cannot protect that which you are unaware of. Authentication systems are the crown jewels of an attacker going after valid credentials, so be aware of where these systems live in your environment.

### 2. Configure Centralized Point of Authentication

**Description**: Configure access for all accounts through as few centralized points of authentication as possible, including network, security and cloud systems.

**Notes**: There are dedicated tools to pull credentials out of centralized authentication systems. Limiting how many you have allows you to more easily defend them. These should also be hardened as much as possible with authoritative sources such as the CIS Hardening Guides or the DISA STIGS.

### 3. Require Multi-factor Authentication

**Description**: Require multi-factor authentication for all user accounts on all systems, whether managed onsite or by a third-party provider.

**Notes**: This is probably one of the more impactful requirements in the entire set of controls. There are going to be varying levels of deploying MFA. Requiring it for any externally available service (VPN, web portals, etc.) will be a quick win rather than trying to scope the entire environment to MFA.

### 4. Encrypt or Hash all Authentication Credentials

**Description**: Encrypt or hash with a salt all authentication credentials when stored.

**Notes**: Attackers steal database passwords all the time. To make an attacker's job harder, each password needs to be encrypted (See section 18.5) or hashed with an algorithm. Since it is trivial to use a high-powered system to crack passwords, each user account should have a unique salt for the hash, as well.

### 5. Encrypt Transmittal of Username and Authentication Credentials

**Description**: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

**Notes**: Everything going across the network should be encrypted, especially credentials. Using a packet capturing tool, system administrators can quickly identify if credentials are being sent in the clear over the network.

### 6. Maintain an Inventory of Accounts

**Description**: Maintain an inventory of all accounts organized by authentication system.

**Notes**: Identity and access management is much harder to do than a single requirement in a set of controls. As with the first two Controls, getting insight into which users you have in your environment will unlock the potential to secure them.

### 7. Establish Process for Revoking Access

**Description**: Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts instead of deleting accounts allows preservation of audit trails.

**Notes**: Creating a process is as simple as documenting what needs to happen in order to revoke access. The technical details on how to follow through can be leveraged from existing frameworks like NIST or other regulatory bodies.

### 8. Disable Any Unassociated Accounts

**Description**: Disable any account that cannot be associated with a business process

or business owner.

**Notes**: The previous version of controls required that a list of accounts be reviewed periodically by business owners. While that is not called out in this version, it's still great advice. Many guidelines already state that each account should be a named owner such as a username. For the remaining accounts, generate a list and work towards associating them with a user, team, application, or business unit.

### 9. Disable Dormant Accounts

**Description**: Automatically disable dormant accounts after a set period of inactivity.

**Notes**: Unused accounts may not be monitored, so it's best to remove them if they are not needed. Don't forget that this also applies to third-party services such as Amazon Web Services as well.

### 10. Ensure All Accounts Have an Expiration Date

**Description:** Ensure that all accounts have an expiration date that is monitored and enforced.

**Notes:** Having an expiration date will make the previous requirement easier to manage. However, if a legitimate user is locked out because their account is expired, this may create additional overhead for the helpdesk team.

### 11. Lock Workstation Sessions After Inactivity

**Description:** Automatically lock workstation sessions after a standard period of inactivity.

**Notes:** To automatically do this, refer to whichever standards your organization are using. This is easily done with centrally managed group policies for Windows users. For another quick win, train users to lock their workstations when walking away as well. For Windows users, two keystrokes (Windows + L) is all it takes!

### 12. Monitor Attempts to Access Deactivated Accounts

**Description:** Monitor attempts to access deactivated accounts through audit logging.

**Notes:** This is facilitated by enabling and collecting audit logs on servers and endpoints. Your SIEM needs to be able to correlate login attempts to deactivated accounts, so an integration into your Active Directory or LDAP will be critical to making this easy for you.

### 13. Alert on Account Login Behavior Deviation

**Description:** Alert when users deviate from normal login behavior such as time-of-day, workstation location and duration.

**Notes:** As with the previous requirement, this is enabled by logging. Many SIEMs

will have this logic built into their correlation engine. If not, simple rules or reports for time of day, location and duration can be easily created and reported on during regular intervals.

See how simple and effective security controls can create a framework that helps you protect your organization and data from known cyber attack vectors by downloading this guide here.

**Read more about the 20 CIS Controls here:**

Control 20 – Penetration Tests and Red Team Exercises

Control 19 – Incident Response and Management

Control 18 – Application Software Security

Control 17 – Implement a Security Awareness and Training Program

Control 16 – Account Monitoring and Control

Control 15 – Wireless Access Control

Control 14 – Controlled Access Based on the Need to Know

Control 13 – Data Protection

Control 12 – Boundary Defense

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

Control 10 – Data Recovery Capabilities

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

Control 8 – Malware Defenses

Control 7 – Email and Web Browser Protections

Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs

Control 5 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Control 4 – Controlled Use of Administrative Privileges

Control 3 – Continuous Vulnerability Management

Control 2 – Inventory and Control of Software Assets

Control 1 – Inventory and Control of Hardware Assets



You can also learn more about the CIS controls here.