

SOC Use Case Report

UC-017: Disable User Account Control (UAC)

Author	Abishek V
Date	1 feb 2026
Environment	Home SOC Lab (VirtualBox)
Primary Logs	Windows Security Logs / Registry Events
Target OS	Windows 10

1. Use Case Summary

Use Case ID	UC-017
Use Case Name	Disable User Account Control (UAC)
Category	Privilege Escalation / Defense Evasion
SOC Tier	L1 (Triage + Investigation + Escalation)
Severity Guideline	High → Critical

User Account Control (UAC) is a core Windows security feature that limits the impact of malicious activity. Disabling UAC reduces system protection and is commonly abused by attackers to enable silent privilege escalation.

2. Scenario

- Endpoint: Windows 10 (192.168.56.110)
- User account: `clair`
- Security feature: User Account Control (UAC)
- Action observed: UAC disabled via registry modification

SOC risk point: UAC is rarely disabled on endpoints outside of controlled testing or troubleshooting. Unauthorized changes indicate elevated risk.

3. Telemetry and Evidence

Primary logs

- Windows Security Event Logs
- Registry modification telemetry

Key Event Sources

- **4688** Process creation (cmd / PowerShell)
- **4657** Registry value modification
- **4624** Associated logon session

4. Detection Logic

Trigger when:

- registry keys controlling UAC are modified
- UAC-related values are set to disable enforcement

Common registry paths:

- `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System`
- `EnableLUA = 0`

5. SOC L1 Playbook

Phase A: Triage

1. Confirm registry modification affecting UAC
2. Identify actor account and endpoint
3. Determine timing relative to other alerts

Phase B: Investigation

1. Identify method used to disable UAC
2. Review activity before and after UAC change
3. Check for privilege escalation or malware execution
4. Scope for similar registry changes on other systems

6. Evidence Timeline

Time	Event ID	Entity / Source	Observation
01:18:44	4688	powershell.exe	Registry modification command executed
01:18:47	4657	EnableLUA	UAC registry value set to 0
01:18:55	4624	clair	Active user session confirmed

Outcome: User Account Control disabled without authorization. Escalation required.

7. False Positive Checks

- approved troubleshooting or testing
- controlled lab or training environment
- IT-admin sanctioned configuration change

8. Verdict Criteria

True Positive if:

- UAC disabled without approval
- change followed by suspicious execution
- actor account is unexpected

Unauthorized disabling of UAC should be escalated immediately.

9. SOC Response Actions

- re-enable UAC and restore baseline settings
- isolate endpoint if compromise suspected
- review recent privileged activity
- reset credentials if required

10. Ticket Notes

Ticket: UC-017 Disable UAC Detected

Severity: Critical

Verdict: Escalation required

Analyst Notes

- Detected registry modification disabling User Account Control.
- Change occurred during active user session without authorization context.
- Classified as defense evasion and escalated for incident response.