Enterprise IT - Mobile Devices

# Enterprise IT - Mobile Devices

We have developed a series of logging requirements for Mobile Devices (also known as End-user Devices), such as thin-clients, desktops, laptops, tablets and mobile smart phones at different maturity tiers in order to support defenisve cyber security, such as detecting breaches.

## Baseline Maturity Tier

### 1. Device power events

Log Collection Principle(s): 1

Devices must create and forward local power events.

* a: power on (including good or bad state)
* b: power off (including if restart)
* c: disk encryption state

### 2. User identification activity

Log Collection Principle(s): 1, 2

Devices must create and forward local Authentication and Authorisation events.

These event types must be logged and forward:

* a: account creation
* b: account lockout
* c: account unlock
* d: account authentication failures
* e: account authentication successes after 3 or more failures
* f: account password changes
* g, group membership addition / deletion (in particular, any group that gives admin access)
* h: group creation
* i: privilege modification for users (changes to ACL's, granting of new roles in RBAC models)
* j: privilege escalation events (use of sudo, UAC)
* k: multi-factor authentication state, such as:
  + 1: enabled
  + 2: disabled
  + 3: reset/rotation
  + 4: recovery method used

### 3. Domain name service query logs

Log Collection Principle(s): 4

DNS query logs must be created and forwarded, even where they are captively routed through central enterprise IT DNS services that forward comparable log data.

* a: device IP addresses (local and public, if known/applicable)
* b: VLAN tag for associated network interface (if known)
* d: query
* e: query response content including
  + 1: returned record(s) or NXDOMAIN
  + 2: authoritative nameserver
* e: query response code

### 4. Security-related operating system event data

Log Collection Principle(s): 6

Any additional security-related logs, as defined by [NCSC's Logging Made Easy template](https://github.com/ukncsc/), from all end-user devices operating a Microsoft Windows operating system must be created and forwarded.

Comparable events from other operating systems (for example, Apple macOS or QubesOS) to that described by NCSC's Logging Made Easy template must also be created and forwarded.

### 5. Security-related software event logs

Log Collection Principle(s): 6

Security-related logs from any local endpoint protection software (for example, anti-virus) should be forwarded.

* a: detection information
  + 1: process/binaries
  + 2: detection criteria (for example, malware type)
* b: reaction information (for example, quarantine)
* c: 'last scan' information
* d: signature information

### 6. Network information

Log Collection Principle(s): 5

Devices must create and forward sufficient data to record the network posture around the device.

* a: IP address of DHCP server
* b: IP address leased
* c: IP address subnet leased
* d: IP address lease duration
* e: Network interface identifier
* f: DHCP response instructions, for example:
  + 1: DNS servers
  + 2: Proxy servers

### 7. VPN dial-up activity

Log Collection Principle(s): 5

Where dial-up VPN is in use, connection-related log data must be created and forwarded.

* a: success or unsuccess status
* b: VPN concentrator domain name and IP address
* c: user/certificate identifier(s) used
* d: network interface identifier

## Enhanced Maturity Tier

### 1. Firewall log data for denied network traffic

Log Collection Principle(s): 5

All firewall DENY log data must be forwarded.

* a: client IP address
* b: network interface identifier(s)
* c: request response code
* d: request content, including:
  + 1: IP protocol (for example, ICMP)
  + 2: destination/target port
  + 3: destination/target IP address
  + 4: destination/target hostname address (if reverse lookup performed)

### 2. Command/executable runtime information

Log Collection Principle(s): 6

Log data to reflect the launching and subsequent processing activity stemming from user, or user profile, triggered commands/executables.

* a: user identifier(s)
* b: device identifier(s)
* c: command executed
* d: executable launched

### 3. Configuration information

Log Collection Principle(s): 6

Devices must create and forward sufficient data to record the changing state of device configurations.

* a: profile or GPO changes
* b: conflict detection