COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

macOS Enterprise Management and MDM Artefacts

The Managed Mac: Central Control, Central Records, and the Route Around a Locked Device

Most Macs in a workplace are not standalone machines; they are managed. Through Mobile Device Management (MDM) and related enterprise tools, an organisation enrols its Macs, applies policies, deploys software, and, crucially, keeps central records of them and often holds the means to unlock or reset them. For the lawyer, the managed Mac changes the picture in two ways. First, management leaves artefacts on the device, enrolment records, configuration profiles, policy state, that show how the machine was controlled and by whom, and that can themselves be evidence. Second, and more powerfully, the management system holds a central record and central control: the administrative console may hold logs, an inventory, an institutional recovery key, and the ability to access or reset the device, so the organisation, as owner and administrator, is often the lawful route around a locked machine. This guide sets out for UK lawyers how managed Macs work, what artefacts they leave, what the console holds, and how enterprise management is used lawfully as a source of evidence and access.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its enterprise-Mac work reads the management artefacts on the device, enrolment, profiles, policy state, and works with the organisation's MDM console as a central source of logs, inventory, recovery keys and lawful access. The analysis treats the managed Mac as one node in a controlled estate, uses the employer's lawful authority to reach evidence and access, and is reported under CPR Part 35 and CrimPR Part 19 with the scope of authority and data protection observed.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | MDM & ENTERPRISE ARTEFACTS | MANAGED-DEVICE ACCESS & LOGS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01 Executive summary

02 The problem in plain English: the managed Mac is not alone

03 How managed Macs and MDM work

04 Management artefacts on the device

05 What the MDM console holds

06 Lawful access, authority and honest limits

07 Deployment: evidence, access and the locked device

08 Source architecture: where else the evidence lives

09 Worked examples

10 Common mistakes and technical limitations

11 Questions to ask · Suggested wording

12 Checklist and red flags · When to involve a digital forensic expert

13 Frequently asked questions

14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

The headline point: most workplace Macs are managed through MDM, which leaves artefacts on the device showing how it was controlled and, more powerfully, gives the organisation a central console holding logs, inventory, recovery keys and the lawful ability to access or reset the machine, often the route around a locked device.

How it works (§3): organisations enrol Macs in MDM, applying configuration profiles and policies, deploying software, and managing the device centrally. **On-device artefacts (§4):** enrolment records, configuration profiles and policy state on the Mac show how it was managed and by whom, evidence in themselves. **The console (§5):** the MDM administrative system holds central logs, an inventory, device state, an institutional recovery key and often the ability to access, lock or reset the machine. **Lawful access and limits (§6):** the organisation, as owner and administrator, can lawfully provide access and records, within the scope of its authority and the UK GDPR. **Deployment (§7):** using management artefacts and the console as evidence, and as the lawful route to access a locked managed device.

- **The managed Mac is not alone:** it is enrolled, controlled and recorded by an organisation.
- **Management leaves artefacts:** enrolment, profiles and policy state are evidence on the device.
- **The console holds central records:** logs, inventory, recovery keys and device state.
- **Often the route around a lock:** the employer can lawfully access or reset a managed device.
- **Act within authority:** the organisation's lawful authority and the UK GDPR govern everything.

The managed Mac and the console behind it

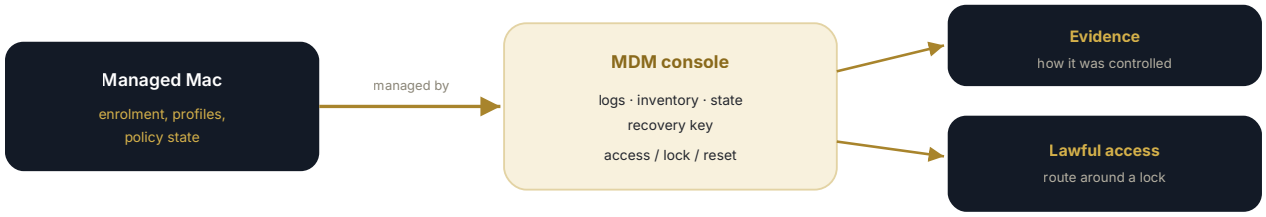

Figure 1 - the managed Mac carries management artefacts, and behind it the MDM console holds central records and the lawful means to access a locked device.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the managed Mac is not alone

A Mac on someone's desk at home is a standalone machine. A Mac issued by an employer usually is not. In most organisations, company Macs are managed: enrolled into a Mobile Device Management system that lets the organisation apply security policies, install and remove software, configure settings, and keep track of the machine centrally. The user works on the Mac, but the organisation controls it, and, importantly, records it. This changes the evidential picture in ways that are easy to miss if a managed Mac is treated as though it were a personal one.

The change has two dimensions. The first is on the device itself: management leaves artefacts, records of enrolment, the configuration profiles that were applied, the policies in force, that show how the machine was controlled, by whom, and from when. These can be evidence in their own right, establishing that a device was a managed company asset, what restrictions applied, and what the organisation could do with it. The second, and more powerful, dimension is off the device, in the management system. The MDM console typically holds a central record of the managed estate: logs of the device's activity and compliance, an inventory of what is installed, the device's current state, and, very often, an institutional recovery key and the ability to access, lock, reset or wipe the machine remotely. This means the organisation, as owner and administrator, frequently holds both a body of central evidence and the lawful means to reach the device, including to unlock a machine that is otherwise locked (guide 133). For the lawyer, the managed Mac is therefore not one isolated device but a node in a controlled estate, and the organisation is often the key that opens it. All of this operates within the organisation's lawful authority and the data-protection framework. This guide sets out how managed Macs work, what artefacts they leave, what the console holds, and how enterprise management is used lawfully as a source of both evidence and access.

§ 0 3 · HOW IT WORKS

How managed Macs and MDM work

- **Enrolment:** a company Mac enrolled into the organisation's MDM system, so it comes under central management from that point, a fact recorded on the device and in the console (§4, §5): the moment control begins.
- **Configuration profiles and policies:** the organisation applying profiles and policies that set security, restrictions and configuration, so what the user could and could not do is defined and recorded (guide 134): the rules imposed.
- **Software deployment:** the organisation deploying and removing applications centrally, so what is installed reflects management decisions, and installations and removals are logged (§5): the managed software estate.
- **Central control:** the console able to query, lock, reset, wipe or access the device and to hold an institutional recovery key (guide 133), so the organisation retains real control over the machine (§6): the central authority over the device.
- **Artefacts on device and console:** the management leaving artefacts on the Mac and a fuller record in the console, both examined, so the managed relationship is evidenced from both ends (§4, §5): the two records.

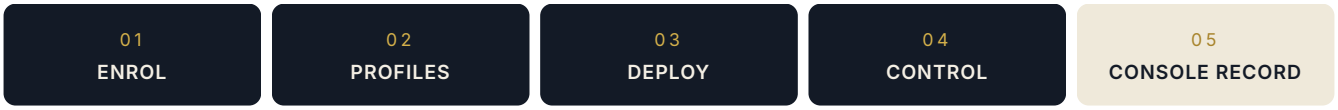

Figure 2 - the MDM lifecycle from enrolment through policy and deployment to central control, leaving artefacts on the device and a fuller record in the console.

§ 0 4 · ARTEFACTS ON THE DEVICE

Management artefacts on the device

- **Enrolment records:** artefacts showing that the Mac was enrolled in MDM, when, and by which organisation, so the device's status as a managed company asset, and the start of management, are established (§3): the enrolment evidence.
- **Configuration profiles:** the profiles applied to the device recording the security settings, restrictions and configuration in force, so what the user was permitted and prevented from doing is evidenced (guide 134): the applied-policy record.
- **Policy and compliance state:** the device's policy and compliance state showing whether it met the organisation's requirements, relevant to security and to what the machine could do (§5): the compliance evidence.
- **Managed accounts and settings:** managed accounts, certificates and settings on the device evidencing the organisational identities and access configured, tying the machine to the enterprise (guide 140): the enterprise identity on the device.
- **Read on the decrypted device:** these artefacts recovered from the acquired, decrypted Mac (guides 131, 133), with integrity preserved (guides 2, 3), and read alongside the system artefacts (guide 134): the sound recovery basis.

§ 0 5 · WHAT THE CONSOLE HOLDS

What the MDM console holds

- **Central logs and activity:** the console holding logs of the device's management activity, compliance and events, a central record independent of the device, obtainable from the organisation (guide 134): the off-device log.
- **Inventory and state:** an inventory of the device's hardware, software and configuration, and its current and historical state, so what was installed and how the machine was set up is recorded centrally (§4): the managed inventory.
- **Institutional recovery key:** very often an institutional FileVault recovery key held by the organisation, the lawful means to unlock the encrypted device (guide 133), of great value where the machine is locked (§6): the key to the lock.
- **Access and control actions:** the record of, and ability to perform, remote actions, access, lock, reset, wipe, so the organisation's control over the device, and its exercise, are evidenced and available (§7): the control record.
- **Obtained from the organisation:** the console records and capabilities obtained from the organisation as owner and administrator, by cooperation or lawful process, within its authority (§6): the lawful source.

§ 0 6 · LAWFUL ACCESS AND HONEST LIMITS

Lawful access, authority and honest limits

- **The organisation's lawful authority:** the employer, as owner and administrator of the managed device, able to provide access, records and an institutional recovery key lawfully, so the organisation is the proper source of both evidence and access (guides 111 to 114, 133): the authorised route.
- **Access a locked device lawfully:** the institutional recovery key or management access used to reach a locked managed Mac, the clean, lawful route around a lock that needs no attack on the encryption (guide 133): the lock lawfully opened.
- **Scope of authority:** the organisation's authority extending to the managed device and its business use, but bounded, so personal data and any personal use are handled with care and within the scope of that authority (guide 20): the boundary of control.
- **Data protection and proportionality:** the access and records handled proportionately under the UK GDPR, with employee-monitoring and privacy considerations respected, so the collection is lawful and minimised (guide 20): the proportionate, compliant reach.
- **State limits plainly:** what the organisation can and cannot lawfully access, and the scope of its authority, stated clearly, so the evidence and access are lawfully founded (guide 100): the honest, lawful account.

§ 0 7 · DEPLOYMENT

Deployment: evidence, access and the locked device

- **Management artefacts as evidence:** the enrolment, profiles and policy state establishing that a device was a managed company asset and what controls applied, evidence in employment and IP matters (§4): the managed status proved.
- **Console records as evidence:** the central logs, inventory and control record from the console evidencing the device's activity, configuration and the actions taken on it, independent of the device (§5): the central record deployed.
- **Lawful access to a locked device:** the institutional recovery key or management access used to reach a locked managed Mac, so a device that would otherwise be inaccessible is opened lawfully (guide 133): the lock opened via management.
- **Reaching the estate:** the managed relationship and console leading to the organisation's wider records and the associated accounts, so the managed device connects to the enterprise estate (guides 111, 140): the estate reached through management.
- **Honest, lawful presentation:** the artefacts, console records and access presented with the organisation's authority documented and the data-protection limits observed, under CPR Part 35 or CrimPR Part 19 (guides 100, 130): the enterprise evidence deployed defensibly.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a managed Mac is explicitly a node in a controlled estate, and the enterprise management system is itself a rich "where else the evidence lives" answer, holding centrally what the device holds locally and more. The device holds the enrolment records, configuration profiles, policy state and managed settings. But the MDM console holds central logs, an inventory, device state, and the institutional recovery key and control actions; the organisation's wider systems, its cloud services, mail, network and endpoint tools, hold the business records and activity the managed device connected to (guides 111 to 114); the directory and identity provider hold the managed accounts and access; and backups and snapshots (guides 132, 137) hold earlier device state. The discipline is to treat the console and the organisation as first-class sources alongside the device, so that management evidence and access are drawn from both ends, and so that a locked or wiped managed Mac is approached through the organisation's central records and its lawful control. When the device is locked, the institutional recovery key opens it; when the device is wiped or unavailable, the console's logs and inventory and the organisation's systems preserve much of the record; and the managed relationship ties the machine into the enterprise estate the organisation lawfully controls.

EVIDENCE	MANAGED MAC	MDM CONSOLE	ORG SYSTEMS (CLOUD/MAIL/ NET)	DIRECTORY / IDENTITY	BACKUPS / SNAPSHOTS	IF DEVICE LOCKED/ WIPED
Managed status	Y: enrolment	Y: enrolment record	Asset records	Device identity	Earlier state	Console holds it
Policy / config	Y: profiles	Y: policy record	n/a	n/a	Earlier profiles	Console holds it
Activity / compliance	System logs	Y: central logs	Service logs	Sign-ins	Earlier logs	Console + org systems
Recovery key / access	n/a (protected)	Y: institutional key	n/a	n/a	n/a	Console unlocks (guide 133)
Business records	Local copies	Pointers	Y: the records	Access records	Backups	Org systems hold them

Fallback strategy in one line: treat the MDM console and the organisation as first-class sources; when the managed Mac is locked or wiped, the institutional recovery key opens it and the console and org systems preserve much of the record.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE LOCKED MANAGED MAC THE CONSOLE OPENED

An employee under investigation returned a locked company MacBook and would not give the password. Because the device was managed, the §5 and §6 console route resolved it cleanly: the organisation, as owner and administrator, held an institutional FileVault recovery key in its MDM console, and used it to unlock the encrypted device lawfully (guide 133), with no attempt to break the encryption and no need to compel the individual. The §4 on-device artefacts confirmed the enrolment and the policies in force, and the machine was then acquired (guide 131). The employer's lawful control had provided the route around the lock. The lesson is §6's: a managed Mac is owned and administered by the organisation, which often holds an institutional recovery key and the means to access the device, so on a company machine the console is frequently the clean, lawful route around a lock, and establishing that a device is managed is one of the first and most valuable questions.

EXAMPLE 2 · THE CONSOLE RECORD THAT TOLD THE FULLER STORY

A dispute needed to know what had been done on and to a company Mac over time. The §5 MDM console held a fuller, independent record than the device alone: central logs of the device's management activity and compliance, an inventory of software installed and removed, and a record of the remote actions taken on the machine, all held centrally and obtained from the organisation (guide 134). This §8 central record corroborated and extended the §4 on-device artefacts, and survived independently of anything done to the device. The picture was built from both ends, the managed Mac and the console behind it. The lesson is §5's: the MDM console holds a central record of the managed device, logs, inventory, state and control actions, that is independent of the device and often fuller than it, so a managed Mac is examined from both ends, and the console frequently supplies evidence the device alone cannot.

EXAMPLE 3 · THE AUTHORITY THAT HAD TO BE RESPECTED

An employer wished to use its management control to reach everything on an employee's company Mac, including plainly personal material. The §6 scope-of-authority discipline shaped the approach: the organisation's lawful authority extended to the managed device and its business use, but personal data and any personal use had to be handled with care, proportionately and within the UK GDPR, with employee-monitoring and privacy considerations respected (guide 20). Access was scoped to what the matter required, the authority for each step documented, and the limits stated plainly. The management control was powerful, but it was exercised within its lawful bounds. The lesson is §6's: enterprise management gives real control and lawful access, but that authority is not unlimited, it extends to the managed device and business use, and personal data must be handled proportionately and within the data-protection framework, so the reach is scoped, documented and kept within the organisation's actual authority.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Treating a managed Mac as standalone:** the fundamental error, missing that the organisation holds central records and lawful access (Example 1, §2).
- **Not establishing management status:** failing to check whether the device is managed, and so missing the console route (§4).
- **Ignoring the console:** examining the device while overlooking the fuller central record and the recovery key (Example 2, §5).
- **Attempting to break encryption:** trying to crack a locked managed Mac instead of using the institutional recovery key (Example 1, §6).
- **Overreaching the authority:** using management control to access personal material beyond the organisation's lawful authority (Example 3, §6).
- **Ignoring data protection:** reaching managed-device data without proportionality or regard to employee monitoring and privacy (§6, guide 20).
- **Not documenting authority:** failing to record the basis and scope of each access (§7).
- **Overlooking a wiped device's central record:** assuming a reset managed Mac holds nothing, when the console and org systems do (§8).

Technical limitations

- **Authority is bounded:** the organisation's control extends to the managed device and business use, not without limit: the core limit (§6).
- **Data protection applies:** personal data on a managed device must be handled proportionately and lawfully (§6, guide 20).
- **Console depends on configuration:** what the console holds and can do varies by MDM setup, so it is established, not assumed (§5).
- **A wiped device loses local data:** a remotely reset Mac loses its local content, though the console and org systems may retain records (§8).
- **MDM evolves:** Apple's management framework and MDM tools change across versions, checked per configuration (§3).

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Is the Mac a managed company device, and does the organisation hold the MDM console, an institutional recovery key and central records?
- Is there lawful authority, and appropriate policies, to reach the device and its data, including any personal use?
- If the device is locked or has been reset, can the console provide access or records?

Ask your opponent (or the organisation)

- Please confirm whether the device at Schedule 1 is managed, and preserve and disclose the MDM enrolment, configuration and central records, and any institutional recovery key.
- Please disclose the console logs, inventory and record of remote actions for the device.
- Please confirm the scope of management authority and the applicable device-use and monitoring policies.

Ask your eDiscovery / forensic provider

- Is the device managed, and what do the on-device management artefacts show?
- What does the MDM console hold, including logs, inventory and any recovery key, and can it provide lawful access?
- How is the access scoped within the organisation's authority and the UK GDPR, and documented?

SUGGESTED WORDING · INSTRUCTION FOR AN ENTERPRISE-MANAGEMENT ANALYSIS

> "We instruct you to examine the enterprise-management position of the device at Schedule 1 in relation to Schedule 2. Please: (1) establish whether the device is managed (enrolled in MDM), and recover the on-device management artefacts, enrolment records, configuration profiles, policy and compliance state, and managed accounts and settings, from the acquired, decrypted device; (2) obtain from the organisation, as owner and administrator and within its lawful authority, the MDM console records, central logs, inventory, device state, the record of remote actions, and any institutional recovery key; (3) where the device is locked, use the institutional recovery key or management access to reach it lawfully, without attempting to break the encryption, and where it has been reset, recover the record from the console and the organisation's systems; (4) treat the console and the organisation as first-class sources alongside the device, and connect the managed device to the wider enterprise estate; and (5) scope the access to the organisation's actual authority and the matter, handle personal data proportionately under the UK GDPR with monitoring and privacy considerations respected, document the authority for each step, and state the limits plainly."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The enterprise-management checklist

- ☐ Management status established (is the device MDM-enrolled?)
- ☐ On-device artefacts recovered: enrolment, profiles, policy state
- ☐ MDM console records obtained: logs, inventory, state, actions
- ☐ Institutional recovery key identified where held
- ☐ Locked managed device opened lawfully via the console
- ☐ A reset device's record recovered from console and org systems
- ☐ Console and organisation treated as first-class sources
- ☐ Access scoped to the organisation's lawful authority
- ☐ Personal data handled proportionately under the UK GDPR
- ☐ Authority for each step documented; limits stated

Red flags

- A managed Mac treated as a standalone device: Example 1.
- Management status not established.
- The console and its records overlooked: Example 2.
- An attempt to break a locked managed Mac instead of using the key: Example 1.
- Management authority overreached into personal material: Example 3.
- Data protection and monitoring limits ignored.
- The authority for access not documented.

When to involve a digital forensic expert

Whenever a workplace Mac is in issue, because the odds are it is managed, and management changes both what evidence exists and how the device can lawfully be reached: the expert establishes whether the device is enrolled and recovers the on-device management artefacts, enrolment, profiles, policy state, that show how it was controlled (§4), and, crucially, works with the organisation to obtain the MDM console's central records, logs, inventory, device state and control actions, that are independent of and often fuller than the device (Example 2, §5). Where the managed Mac is locked, the institutional recovery key held in the console provides the clean, lawful route around the lock, with no attack on the encryption (Example 1, guide 133), and where it has been reset, the console and the organisation's systems preserve much of the record (§8). Throughout, the access is scoped to the organisation's lawful authority, personal data is handled proportionately under the UK GDPR, and each step's authority is documented and reported under CPR Part 35 or CrimPR Part 19 (Example 3, §6). This guide closes the macOS block. Through **cflab.uk** and **e-discovery.uk**, enterprise-management work treats the

managed Mac for what it is: not a lone device, but a node in a controlled estate whose owner often holds both the central record and the lawful key.

§ 1 3 · COMMON QUESTIONS

Frequently asked questions

Why does it matter whether a Mac is managed?

Because it changes everything about evidence and access (§2). A managed Mac is enrolled in the organisation's MDM system, so the organisation controls and records it centrally. That means there are management artefacts on the device showing how it was controlled, and, more powerfully, a central console holding logs, inventory, device state, often an institutional recovery key, and the ability to access or reset the machine. So the organisation frequently holds both a body of evidence and the lawful means to reach the device, which a standalone-device approach would entirely miss.

The company Mac is locked. Can we still get in?

Very often yes, through the console (§6, Example 1, guide 133). A managed Mac is owned and administered by the organisation, which typically holds an institutional FileVault recovery key in its MDM console. As owner and administrator, the organisation can use that key to unlock the encrypted device lawfully, with no attempt to break the encryption and no need to compel the individual user. So on a company machine, the console is frequently the clean, lawful route around a lock, which is why establishing that a device is managed is an early, valuable step.

What does the MDM console actually hold?

A central, independent record of the device (§5, Example 2). Typically it holds logs of the device's management activity and compliance, an inventory of the hardware and software, the device's current and historical state, a record of remote actions taken, and often an institutional recovery key. Because this is held centrally, it survives independently of the device and is frequently fuller than the device's own artefacts, so a managed Mac is examined from both ends, the device and the console, with the console obtained from the organisation.

Can the employer just access everything on the Mac?

No, the authority is bounded (§6, Example 3). The organisation's lawful authority extends to the managed device and its business use, and it does have real control, but that authority is not unlimited. Personal data and any personal use of the device must be handled proportionately and lawfully, within the UK GDPR, with employee-monitoring and privacy considerations respected. So access is scoped to what the matter requires and to the organisation's actual authority, the basis for each step is documented, and the limits are stated plainly.

The device was remotely wiped. Is everything gone?

The local data may be, but the record often is not (§8). A remotely reset managed Mac loses its local content, but the MDM console retains its central logs, inventory and state, and the organisation's wider systems, cloud, mail, network, hold much of the business record the device connected to, along with backups (guide 137). So a wiped managed device does not necessarily end the enquiry: the central and organisational records frequently preserve a great deal, which is another reason the console and the organisation are treated as first-class sources.

How does a managed Mac connect to the wider case?

Through the enterprise estate it belongs to (§8). The managed relationship ties the device to the organisation's systems, its cloud services, mail, network and identity provider, and the account map (guide 140), so the managed Mac is a node in a controlled estate rather than an isolated machine. Following the management artefacts and the console leads to the organisation's wider records and the associated accounts, all reachable lawfully through the organisation's authority, so the device becomes an entry point to the broader evidence the enterprise holds.

§ 14 · REFERENCE

Glossary

MDM
Mobile Device Management; central management of devices.

Managed device
A device enrolled in and controlled by MDM.

Enrolment
Bringing a device under MDM management.

Configuration profile
A set of settings and restrictions applied by MDM.

Policy / compliance
The rules a managed device must meet.

MDM console
The admin system holding central records and control.

Inventory
The central record of a device's hardware and software.

Institutional recovery key
An org-held key to unlock a managed device.

Remote action
Access, lock, reset or wipe from the console.

Scope of authority
The lawful bounds of the organisation's control.

Sources and authoritative references

The enterprise-management disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (MDM and enterprise artefacts, managed-device access and logs, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Identification and Phase 04 · Collection (managed-device identification and collection as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Apple Platform Deployment and Platform Security guides (MDM, enrolment, configuration profiles and institutional recovery keys): support.apple.com, Deployment · support.apple.com, Platform Security
- ICO, employee-monitoring and UK GDPR guidance (proportionate handling of managed-device and personal data): ico.org.uk · Forensic Science Regulator, Code of Practice v2: gov.uk, FSR Code
- PD 57AD and CPR Part 31 · CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Enterprise-management work at the laboratory treats the workplace Mac for what it usually is: not a lone device, but a node in a controlled estate whose owner often holds both the central record and the lawful key. The first step is to establish whether the device is managed and to recover the on-device management artefacts, enrolment, configuration profiles, policy and compliance state, and managed settings, that show how the machine was controlled and by whom (§4). The organisation is then engaged, as owner and administrator and within its lawful authority, to obtain the MDM console's central records, the logs, inventory, device state and record of remote actions that are independent of, and often fuller than, the device (Example 2, §5). Where the managed Mac is locked, the institutional FileVault recovery key held in the console provides the clean, lawful route around the lock, with no attack on the encryption (Example 1, guide 133); where it has been reset, the console and the organisation's wider systems preserve much of the record (§8). Throughout, the access is scoped to the organisation's actual authority, personal data is handled proportionately under the UK GDPR with monitoring and privacy considerations respected, and each step's authority is documented and reported under CPR Part 35 or CrimPR Part 19 (Example 3). This guide closes the macOS and Apple-silicon block. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and the governing insight is that on a managed Mac, the organisation behind the device frequently holds the evidence, and the key, that the device alone would not give up.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace