DATALOCKER®
SIMPLY SECURE

IRONKEY™ EMS CLOUD

ENTERPRISE MANAGEMENT SERVICE

MANAGE SECURE STORAGE CENTRALLY

Protecting your data, your mobile workforce and your organization is easy with the IronKey EMS Cloud. With this cloud-based secure command center, you can easily administer and police IronKey Enterprise S1000 or D300M encrypted storage flash drives, DataLocker H350 or H300 Enterprise hard drives, and DataLocker Sentry EMS encrypted flash drives through this advanced management console.

- Take control of encrypted mobile storage.
- Mitigate risks of data loss.
- Enhance productivity and collaboration.

FAST, FLEXIBLE DEPLOYMENT

With DataLocker's secure cloud-based service, you will be up and running within 15 minutes without the need for additional IT resources. Efficiently administrate the security of all EMS compatible encrypted flash drives and hard drives. Provision and initialize devices in ways that fit how your organization works – deploy by workgroups, activate devices by email, or distribute pre-initialized devices directly to employees.

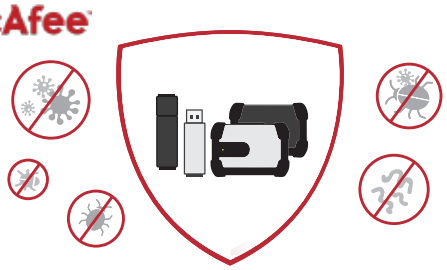
CREATE A VIRTUAL COMMAND CENTER

A single console gives your administrators an up-to-the-minute view of all applicable devices under their management, no matter where those devices are in the world. Your own dashboard presents easily scanned charts and graphs showing data about all devices under your management including user status, device status, device location and activity, device software version and more.

ANTI-MALWARE PROTECTION

Powered by McAfee

Many agencies have strict IT requirements for deploying USB drives within their environments. IronKey EMS Anti-Malware service, McAfee, allows administrators to enable AutoRun Malware Defense as just one of the key features to meet and exceed these requirements. With an on-board antivirus program that runs real-time monitoring of the files being stored on your secure mobile storage device, you can protect against viruses, worms, trojan horses and other malware threats when the device is being utilized on a Windows system.



BENEFITS

Manage IronKey Enterprise Secure Storage devices and DataLocker H300/ H350 Secure Storage devices from a single console.

Deploy and manage devices easily using this cloud-based service with minimal capital expenditure.

Monitor devices in the field with a powerful, flexible asset tracking system.

Efficiently and cost-effectively protect devices by administering usage and encryption policies, password restrictions, and more from a central console.

Role based administration provides flexibility and allows a single account to be leveraged by multiple groups within a single organization.

Strengthen authentication by enabling one-time passwords and simple but secure password recovery.

Administrators can remotely wipe or disable lost or stolen devices.

Extensive logging including visual tools for monitor data such as geographical access via a convenient dashboard.

Monitor devices in the field with this powerful, flexible asset management tool.

Administrators can force software updates to ensure all devices stay current.

DATALOCKER®
SIMPLY SECURE

IRONKEY™ EMS CLOUD

ENTERPRISE MANAGEMENT SERVICE

CENTRALLY ADMINISTER USAGE, PASSWORDS, AND MORE

Police device use and access by leveraging a broad range of flexible policy and password management controls.

- Enforce device-specific rules for password length and complexity, password change frequency, and more.
- Enable help desk admins to easily and remotely help users who have forgotten their passwords.
- Restrict the ability to use drives on certain computers by whitelisting specific IP addresses or address ranges.
- Remotely reset devices, reset passwords, update policies, force read-only mode, disable or even detonate devices from anywhere in the world.
- Activate and administer optional McAfee Anti-Virus protection software on some or all of the devices you manage.
- Enable users to generate One-Time Passwords for secure authentication from leading OTP platforms.
- Ensure devices stay current with the latest software by remotely forcing updates.

ENSURE COMPROMISED DRIVES DON'T COMPROMISE DATA

With IronKey EMS, administrators can remotely disable lost or stolen devices by locking out users and preventing password access. They can even destroy a device that a departing employee fails to return, erasing every block of data from the compromised device and destroying its on-board Crytopchip, rendering it unusable.

DEFINE AND CONTROL ADMINISTRATIVE ROLES

Help ensure that only the right people see and control device use across the enterprise by establishing and enforcing boundaries for device management.

MANAGED DEVICES

DataLocker H350/H300 Enterprise External Hard Drives and DataLocker Sentry EMS flash drives

Next generation hard drive features USB 3.0 performance combined with extended storage capacity. Sentry EMS flash drive is optionally managed by IronKey EMS.

IronKey Enterprise Hardware Encrypted S1000 & D300M Flash Drives

Mobile data security and regulatory compliance with military-grade encryption, strong authentication, and optional anti-malware defenses.

*Legacy IronKey EMS Supported Devices: S200, S250, D200, D250,IronKey Workspace W700 and W500 flash drives.

PART NUMBERS

To view IronKey EMS part numbers: datalocker.com/ems/#_emspartnumbers

SALES CONTACTS

datalocker.com
sales@datalocker.com
+1 855 897 8755 or +1 913 310 9088