

# IRONKEY™ ENTERPRISE MANAGEMENT SERVER



## MANAGE WINDOWS TO GO AND SECURE STORAGE CENTRALLY

IronKey Enterprise Management Server is a reliable and highly scalable solution for managing IronKey Enterprise S1000, S250 and D250 hardware encrypted storage flash drives, IronKey Enterprise H350 and H300 hard drives and IronKey Workspace W700, W700SC and W500 drives for Windows To Go. This robust secure software server readily integrates with existing IT infrastructure, making it easy to deploy and administer end user drives and to remotely enforce policies. It also enhances the security of “always-on” IronKey hardware encryption by providing enterprise-class management capabilities that include the ability to implement two-factor authentication, deploy portable virtualized desktops, and disable or wipe clean rogue drives.

## CENTRAL MANAGEMENT AND REMOTE CONTROL

The IronKey Enterprise Management Server is a software virtual appliance that provides complete centralized remote management of devices. A single console gives your administrators an up-to-the-minute view of all applicable IronKey Enterprise S1000, S250 and D250 flash drives, Enterprise H350 and H300 hard drives and IronKey Workspace W700, W700SC and W500 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. This robust management environment— based on the proven IronKey hosted services architecture— scales to thousands of users.

## MANAGE WINDOWS TO GO DEVICES

Manage your IronKey Workspace W700, W700SC and W500 devices with the on-premises IronKey Enterprise Management Server. IronKey Workspace with Windows To Go is a PC on a Stick™ that equips employees and contractors with a portable Windows 8/8.1 or Windows 10 corporate image. This Microsoft-certified solution comes complete with your applications, security controls and access policies stored on a ruggedized, fully manageable USB flash drive – all at savings of up to 90% compared to the cost of laptops.

## ANTI-MALWARE PROTECTION

Many federal agencies have strict IT requirements for encrypting data at rest and for using USB drives on trusted networks. IronKey Enterprise Management Server enables options such as AutoRun malware defense, read-only mode, and IronKey Anti-Malware Service that meet and exceed these requirements.

## AN ADVANCED PLATFORM FOR THE SECURE ENTERPRISE

The IronKey Enterprise Management Server was designed to separate user and system to ensure maximum security and optimal flexibility — allowing organizations to use their preferred endpoint security software to securely deploy IronKey devices to end users. Advanced management features such as the exclusive IronKey Silver Bullet Service and Active Malware Defense can even protect against rogue users or similar insider threats by sending a remote self-destruct signal to the drive.

## BENEFITS

- Manage IronKey Workspace for Windows To Go and Secure Storage devices from a single console.
- Run on either your own dedicated hardware, or in a ESXi virtual environment.
- Monitor devices in the field with a powerful, flexible asset tracking system.
- Efficiently 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 monitoring data such as geographical access via a convenient dashboard.

# IRONKEY™ ENTERPRISE MANAGEMENT SERVER

## CENTRALLY ADMINISTER USAGE, PASSWORDS, & MORE

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

- Efficiently manage device inventory, lifecycle and maintenance—even for users in the field.
- Easily manage thousands of IronKey Enterprise S1000, S250 or D250 flash drives, IronKey Enterprise H350 and H300 hard drives and IronKey Workspace W700, W700SC and W500 devices and enforce device-specific policies for IronKey drives on and off the network.
- Remotely manage configurable policies, including password strength, password aging, password retry limits and onboard portable applications.
- Easily modify and update policies to permit and revoke user or administrative authorization.
- Remotely reset devices, reset passwords, update policies, force read only mode, disable or even detonate devices from anywhere in the world.
- Accurately manage user devices, user groups, and service licenses—adding or subtracting as needed when your requirements and users change.
- In conjunction with third-party device control solutions, establish whitelists to ensure that only secure IronKey devices can connect to an enterprise's computer.

## HOST SYSTEM REQUIREMENTS in ESXi ENVIRONMENT

- vSphere ESXi version 5.0 or higher (the ESXi version must support the Guest OS CentOS v6.6—the OS on which IronKey Enterprise Server is installed)
- 1GB or faster Ethernet physical network adapter
- 4GB physical RAM
- Physical data store must have 70GB available space

## HOST SYSTEM REQUIREMENTS in ACE PLAYER ENVIRONMENT

- Pentium Core 2 Duo or higher class system (quad-core recommended)
  - 2GHz or faster CPU minimum
- Windows Server 2003, Windows Server 2008 or Windows Server 2012
- 2GB minimum (4GB recommended)
- 5GB of free hard disk space required (12GB recommended)
- 16-bit display (32-bit display adapter is recommended)
- Microsoft SQL Server 2005, Microsoft SQL Server 2008 or Microsoft SQL Server 2012

## SALES CONTACTS

### WEBSITE

[www.ironkey.com](http://www.ironkey.com)

### US AND CANADA

[securitysales@imation.com](mailto:securitysales@imation.com)  
 +1 888 435 7682 or +1 408 879 4300

### EUROPE

[emeasecuritysales@imation.com](mailto:emeasecuritysales@imation.com)  
 +44 (0)1332 597 168

### ASIA PACIFIC

[apacsecuritysales@imation.com](mailto:apacsecuritysales@imation.com)  
 +65 6499 7199

## MANAGED DEVICES

### IronKey Enterprise Hardware Encrypted S1000, S250 & D250 Flash Drives

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

\*IronKey Enterprise S200 & D200 devices can also be managed.

### IronKey Enterprise H350 and H300 External Hard Drives

Next generation hard drive features USB 3.0 performance combined with extended storage capacity.

### IronKey Workspace W500, W700 & W700SC Windows To Go Drives

Microsoft-certified Windows To Go solutions that deliver a true Windows 8/8.1 or Windows 10 desktop protected by a trusted IronKey USB flash drive.

