SPYRUS®

SPYRUS Enterprise Management System (SEMS)

Secure Control of Portable USB Devices

Secure Control of SPYRUS USB Devices

In today's environment of storing and communicating critical sensitive or classified data, there is continued awareness of the importance of protecting such data from compromise. Recent intentional cyberattacks by terrorists and nation-states against large and small entities provides unprecedented and unforeseen exposures of vulnerabilities to data theft and leakage. Nowhere is this gap more visible than in the endpoint management of user access to USB storage devices and their contents, and the ability to control access and use of these devices only to authorized users.

Worker and endpoint device mobility has brought an increase in productivity along with inherent risks associated with carrying confidential and proprietary enterprise data and intellectual property on a portable USB device that can easily fit in a briefcase, handbag or even in the palm of a hand. With such portable endpoints, it's no surprise that these devices can be temporarily misplaced or lost

And often they can be the target of cyberattacks by professionals—either by opportunity or because someone specifically wants that data and can exert coercion or threaten criminal harm. Organizational security policies to guide personal behavior are ineffective when data leakage attacks are malicious. Such policies do not protect against a rogue employee storing large amounts of valuable data on a device and walking out the door with it and the organization's information. Even loyal employees sometimes forget about security and carelessly leave their devices or device passwords exposed and unattended.

The strong encryption and password protection in all SPYRUS USB drives mitigates the threat from even professional and nation-supported sophisticated attacks on the data within the drives, but in scenarios with a rogue employee or some other type of criminal insider activity, encryption is no guarantee. If there is carelessness in hiding the password, or the hostile entity knows the encryption password or forces that knowledge, then your only security gate has been compromised.

The SPYRUS Enterprise Management System, SEMS, is the SPYRUS management system that remotely controls user access to, and the operational states of, enterprise-deployed USB devices and security tokens containing the embedded Rosetta Micro security controller, in order to mitigate threats of misuse and data loss by malicious or improper user operations.

SEMS offers global, national and organizational control over those important corporate and personal IT information assets which have previously been protected within the confined physical IT infrastructure of a facility, but now require more sophisticated and wide ranging protection as they travel the world within USB endpoint devices. Administrators using SEMS can remotely disable and re-enable a device, or remotely destroy keys and data to "kill" the operability of the device, issuing the appropriate command based on whether a device is misused, lost, or stolen. Regardless of where devices are located, devices can be managed and audit facilities will capture related user actions which can then be monitored centrally to observe profiles of use and trigger notifications for unusual activities.

Equally important for deployment is the ability to change policies for use of the device, often by groups or even by individuals. Rather than requiring the return of devices to organizational administrators for user registration, or modifying usage policies, e.g., off-line usage limits, or recovering forgotten passwords, SEMS supplies the facilities to execute such controls from a central location(s) to control devices globally. The SEMS hierarchical architecture facilitates national and organizational device policy definition, user audit and device control procedures such that help desk administrative consoles can be deployed based on respective enterprise needs. The device usage and protection polices most appropriate for each enterprise entity's criteria can be customized and enforced.

SPYRUS®

Remote Management

SEMS minimizes threats to an organization by providing secure device management and reporting capabilities. Devices can be managed and audited regardless of where they are located, and the organization's security policies are enforced whether or not a device is connected to a network.

Administrators using SEMS can remotely disable a device, or destroy the data and keys on a device, rendering it unusable.

Client / Server Model

The SEMS system comprises two components: the SEMS management server and the SEMS client component. SEMS administrators can set and enforce security policies for each registered device and define the actions performed by the SEMS client.

Each time a device is used, the SEMS client component creates a secure connection to the SEMS server to determine whether or not the action is permitted. If an administrator has disabled a device, the SEMS client blocks the device's operation, requiring subsequent administrator authorization to re-enable the device.

Offline Mode

A SEMS-managed device can be used even when the device cannot connect to the SEMS server.

An offline policy defines how many times a device can be used before having to re-establish a connection with SEMS or risk being disabled when offline logon thresholds are exceeded.

Security Infrastructure

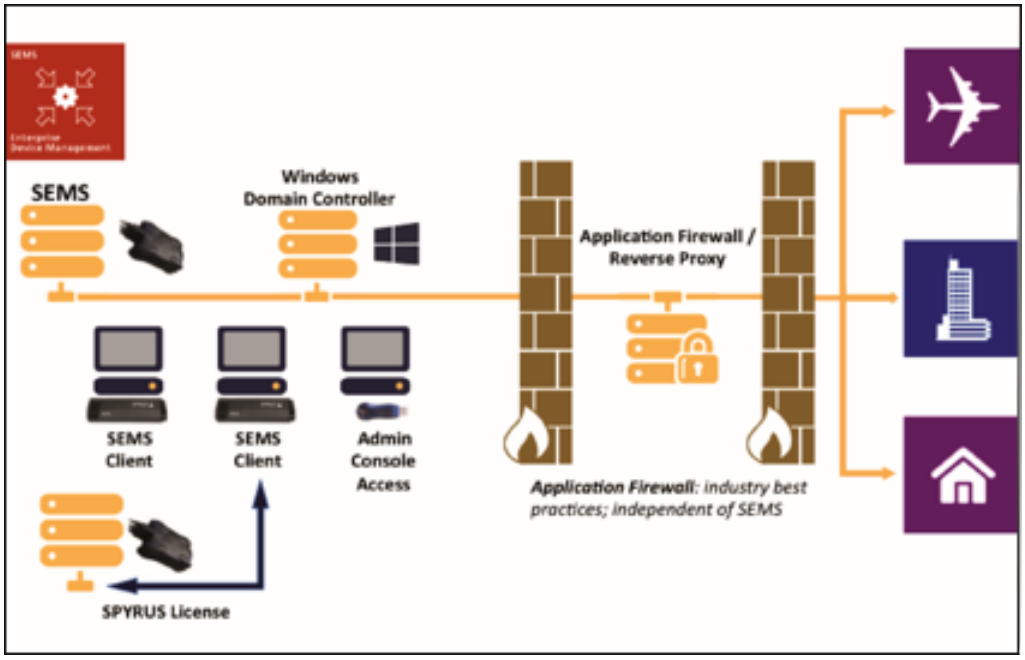
SEMS is designed using international government-approved next-generation cryptographic algorithms such as AES 256, ECDH P-384, and SHA-256 for digital signatures, key agreement, symmetric encryption, and hashing. SPYRUS "Defense-in-Depth" security modules offer cryptographic layers to secure client-server processes to combat both external and internal threats to networks and portable storage devices.

SPYRUS Rosetta USB readerless smart cards can be used at the SEMS Console for authentication to block unauthorized access to the SEMS Console, and also in the SEMS Security Module Service to generate and store cryptographic keys for use within the Microsoft CNG.

Device Control

Administrators can manage devices, monitor activity and usage and if necessary, due to misuse or theft, disable, or destroy a device. Devices can be managed regardless of where they are located. Management is performed based upon SEMS Groups, with policies that are downloaded and stored on the device. Meaning policy is enforced whether or not a device is in contact with SEMS. Administrators can reset lost passwords without destroying data and securely re-enable a user.

SPYRUS Enterprise Management System



Disable Device

Temporarily disable a device.

Destroy Device

When a device is known to be lost or stolen, a Destroy command remotely "kills" the device. If a logon attempt is made, the cryptographic keys are zeroized, rendering the device unusable. All data on the device is irretrievably lost.

Distributed Deployment

The SEMS enterprise hierarchical architecture facilitates national and organizational device Group policy definition and control procedures so that multiple help desk Console users can be deployed, for example, one for each country in which an organization operates, and the device usage and protection polices most appropriate for that country organization's criteria can be customized and enforced.

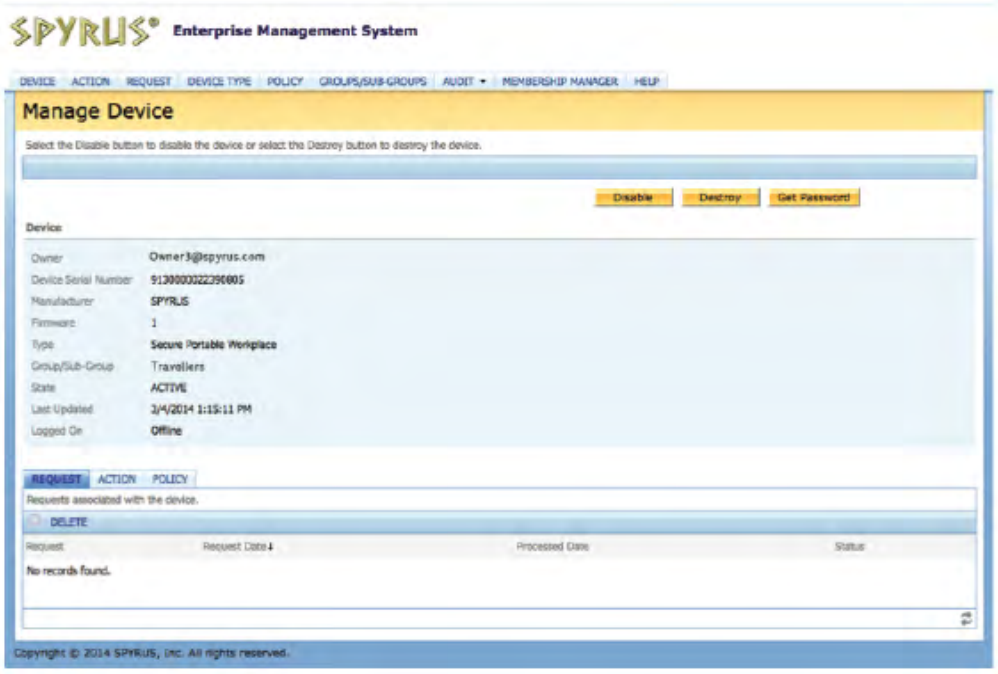
SEMS Groups allow for policies to be defined that represent geographic or organizational structures, allowing different security policies to be applied as appropriate to each SEMS Group. Administration is controlled at the Group level, whereby SEMS Console users are assigned to manage a specific group(s). Group separation is supported so that Console users assigned to manage one group cannot see or manage devices in another group. Roles and privileges can be assigned to each Console user to authorize different limitations over the device control for the users within their groups, e.g., device disablement or destruction decisions.

Transaction Auditing

All devices have on-line audit facilities that capture device registration, user session log-ons/log-offs password change, and group assignments. The PocketVault P-384 also captures all file transactions, as well as off-line user activity. Audited transactions are recorded in a database that can be searched using the SEMS Console. Console user transactions are also audited.

Ease and Economy of Use

Ease of use is an important consideration in deploying scalable device management systems. System Administrators primarily operate in a demand-based environment. SEMS allows them to take actions for control of devices based on user-driven operational help requests, threat circumstances, or organization-driven policy changes. The comprehensiveness of the SEMS Console controls provides real-time responsiveness to users, or to monitored alarm events without reliance on IT staff or vendor support.



SEMS Console Example

SPYRUS®

SEMS Features and Benefits

- Secure device management actively controls devices remotely to minimize threats to your enterprise domain.
- Complete device lifecycle management—register, audit, manage policies, enable/disable, and destroy devices.
- Remote disable and destroy (kill) capabilities protect against lost/stolen devices and employee misuse.
- SEMS device policies are enforced even when SEMS-managed devices are used on non-SEMS domain computers. Policy defines the number of times a device can be used offline before it must re-establish a connection with the SEMS server.
- SPYRUS Rosetta USB readerless smart cards can be used for multi-factor authentication.
- SEMS Security Module Service uses SPYRUS Rosetta to generate and store keys for use with the Microsoft CNG.
- Supports SPYRUS Windows To Go drives, namely: WorkSafe,
- WorkSafe Pro,
- Portable WorkPlace, and
- Secure Portable WorkPlace.
- Supports Pocket Vault P-384 hardware-encrypted USB drive.

Requirements

- Management Server
- 2.0 GHz 64-bit processor, 2 GB RAM, 100 GB hard drive
- Windows Server 2008 SP2 or Windows Server 2012 SP2 w/ all updates and current patches
- .Net Framework 4.0 or later
- Internet Information Services (IIS) 7.0 (2008) or 8.0 (2012)
- ASP .NET 3.5, ASP .NET 4.5, and IIS 6 Metabase Compatibility Options
- Microsoft Report Viewer 2010 SP1
- SQL Server 2008 or Server 2012 Enterprise Edition
- Certification Authority (CA) in the SEMS domain to create an SSL certificate
- Internet Explorer 7.0 or higher

Security Module Service Server

- 2.0 GHz 64-bit processor, 2 GB RAM, 100 GB hard drive
- Windows Server 2008 SP2 or Windows Server 2012 SP2 w/ all updates and current patches
- .Net Framework 4.0
- (optional) SPYRUS Rosetta USB readerless smart card (not required for software-only configuration)

Note: The security module service backup file storage device may be used in Microsoft high-availability cluster configurations to minimize downtime of the SEMS management system in case of server failures. For assistance in configuring the backup file storage device for such configurations, please contact SEMSsupport@spyrus.com.

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

For more information about SPYRUS products, visit www.SPYRUS.com or contact us by email or phone

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document number 400-420001-11