



# Wave EMBASSY® Remote Administration Server (ERAS)

Directory-based security management for SEDs, TPMs, BitLocker® and Virtual Smart Cards

## Key Benefits:

- ✓ **Security:** Increases device security with centralized policy enforcement, secure user recovery and protected user and device credentials
- ✓ **Compliance:** Achieves compliance through active monitoring, logging and reporting of all user and device events, associated with Self-Encrypting Drives (SED), Trusted Platform Modules (TPM) and BitLocker client PCs
- ✓ **Cost:** Minimizes IT overhead and help desk costs associated with the setup, deployment and maintenance of device encryption and device ID solutions
- ✓ **Fit:** Transparent control that fits within your infrastructure, fits with your users and fits your security needs today and tomorrow

## Centralized Security Management

Organizations, both large and small, understand that centralized security management is a critical component to protecting their networks and, by association, the critical information that drives their businesses. Wave's software provides the policy-based access controls, comprehensive reporting, directory services integration, centralized control and end-user access recovery that companies require to cost effectively implement and administer endpoint encryption and authentication. Most importantly, Wave software gives IT the assurance that data is protected in the event that a computer (or its hard drive) is lost or stolen.

## Wave EMBASSY Remote Administration Server

Conventional security methodologies based on software alone fail to effectively authenticate users and machines on the network or secure data on lost or stolen laptops, or ensure compliance with laws that require disclosure of lost personal data. Fortunately, SEDs, TPMs and Microsoft® BitLocker, provide more secure, cost-effective and simpler ways to safeguard your critical business information. However, these technologies provide only half the answer. ERAS transforms SEDs, TPMs and BitLocker into enterprise-wide encryption and authentication solutions by adding essential centralized configuration and administration capabilities.

## Manageability and Control

ERAS provides a full set of capabilities to remotely search for, initialize, configure and administer a global fleet of computers with SEDs, TPMs and those using Microsoft BitLocker drive encryption. Through native integration with Microsoft Active Directory, ERAS delivers the means to centrally provision security policies to end-points across the enterprise, limit access of encrypted information to authorized individuals and remotely manage user and device credentials. Most importantly, ERAS adds an authority of proof, allowing organizations to demonstrate that they were, and are, compliant with regulations in the wake of a security breach. ERAS core features:

- Microsoft Management Console (MMC) snap-in provides both single user and group-level control
- Uses industry standard communication protocols to securely access remote endpoints
- Delegated, role-based administration
- Support for non-domain computers
- Provides group policy objects (GPO), scripting and command line operations
- Setup wizards for SED, TPM and BitLocker

## ERAS for Self-Encrypting Drives

SEDs are the most secure, best performing and most transparent encryption option for protecting data on laptops. ERAS is the only management solution that delivers drive initialization, user management, drive locking, user recovery and crypto erase for all Opal-based, proprietary and solid-state SEDs. In addition, ERAS provides:

- Common Access Card (CAC), smart card (Java and .NET)
- Secure user recovery using challenge/response
- Windows password synchronization and single-sign-on (SSO)
- User based SSO after recovery
- Reports and logs of device and user status and events
- Control for external SEDs
- Support for OPAL 1.0 and 2.0 SEDs
- User self-enrollment and user self-service password recovery

**wave**®

## ERAS for Virtual Smart Card

ERAS for Virtual Smart Cards provides full lifecycle management of Virtual Smart Cards on Windows 7 laptops and desktops, as well as Windows 8 and 8.1 laptops, desktops and tablets.

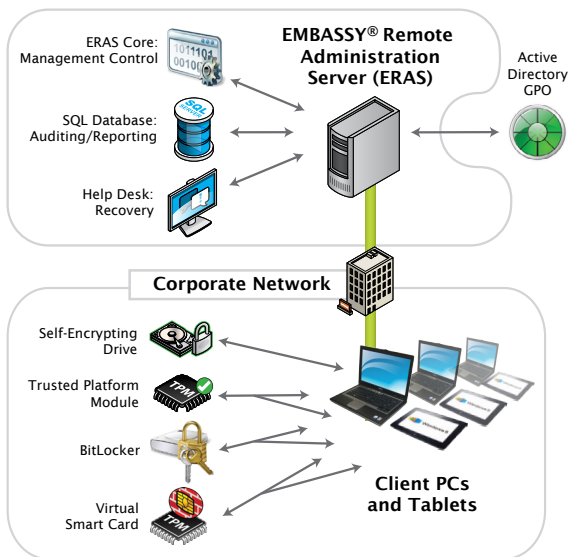
ERAS offers an intuitive user interface enabling I.T. to:

- Create and delete Virtual Smart Cards
- Recover Virtual Smart Cards
- List Virtual Smart Cards and content
- Configure PIN policies
- Generate reports

## ERAS for Trusted Platform Modules

TPMs are the most transparent and least expensive way to protect user IDs and to identify which PCs are yours and which ones aren't. Instead of enabling TPMs one machine at a time, ERAS provides activation, ownership and management of TPMs from a central location. Once TPMs are turned on, you can use ERAS to create hardware-based digital certificates for your VPN, wireless or other PKI-enabled applications – eliminating private key risks and ensuring device identity. In addition, ERAS:

- Puts TPM management under IT control
- Delivers TPM password reset for user recovery
- Reports on the TPM status (active/owned)
- Provides automated provisioning and deployment
- Enables use of TPM for Modern Access Control
- Creates and enables the use of certified keys and certificates for Device and User Identity services



## ERAS for Microsoft BitLocker

Microsoft BitLocker's tight platform integration and use of the TPM makes it a good starting point for drive encryption for organizations using Windows® 7, 8, or Vista. Wave ERAS provides a full set of capabilities to automate and secure the configuration and administration of Microsoft BitLocker. ERAS delivers a simple and intuitive administrative application for setting up, maintaining and reporting on BitLocker clients – eliminating the cost, complexity and uncertainty of designing your own solution through the use of "home-grown" scripts and directory modifications. In addition, ERAS:

- Enforces consistent policy settings across BitLocker clients
- Secures recovery passwords in an encrypted database
- Monitors, logs and reports on all BitLocker events associated with activation, policy management and user access and recovery
- Simplifies TPM activation for BitLocker and retains TPM for user and device authentication
- Provides a simple and transparent migration path from BitLocker to SEDs

## Technical Specifications

### ERAS Server Hardware Prerequisites (for managing up to 2000 accounts)

- System Processor: Minimum: 2 GHz, Recommended: 2.5 GHz, 4 Core or better
- System Memory: 8 GB RAM or more is recommended
- Free Disk Space: Minimum: 20GB Recommended: 40 GB
- 1 GB network interface

### ERAS Server and HelpDesk Prerequisites

- Windows Server 2008 (32/64 bits) and Windows Server 2008 R2 – standard edition (minimum)
- Windows Server 2012 and 2012 R2
- Domain functional level 2003, 2008 and 2012
- Microsoft Management Console (MMC) 3.0
- Microsoft Group Policy Console with SP1
- Microsoft SQL Server 2008, 2008 R2, 2012
- Microsoft Internet Information Service(IIS)
- Microsoft Windows Installer 4.5
- .NET Framework 3.5 SP1, 4.0

### ERAS Remote Console

- Windows 8.1, 8, 7, Vista
- Microsoft Management Console (MMC) 3.0
- .NET Framework 3.5 SP1, 4.0
- Microsoft Windows Installer 4.5

Microsoft, Windows, and BitLocker are either registered trademarks or trademark of the Microsoft group of companies.

## Wave Systems EMEA

### Northern Europe

50 Broadway  
St James Park  
London SW1H 0RG  
United Kingdom  
+44 1235 520956  
emea@wave.com

### Netherlands

Jan Pieterszoon  
Coenstraat 7  
2595 WP The Hague  
Netherlands  
+31 (0) 70 799 9326  
emea@wave.com

### Central/Eastern Europe

Tab's Office Center  
Niermannsweg 11 – 14  
40699 Erkrath (Düsseldorf)  
Germany  
+49 (0) 211 25030  
emea@wave.com

### Southern Europe, Africa & Middle East

La Grande Arche-Paroi Nord  
92044 Paris La Defense  
France  
+33 1 40 90 33 44  
emea@wave.com

### Israel

32 Habarzel Street  
Tel Aviv 69710  
Israel  
+972 3 6442662  
emea@wave.com