SIMPLIFIED DRIVE ENCRYPTION FOR DELL LATITUDE NOTEBOOKS

By Brian Berger

Dell™ Latitude™ D630 and Latitude D830 notebooks with Seagate® Momentus® hard drives and EMBASSY® management software from Wave Systems offer a comprehensive, simplified, hardware-based encryption solution to help protect critical data.

Related Categories:

Dell Latitude notebooks

Security

Wave Systems

Visit DELL.COM/PowerSolutions for the complete category index.

Deploying encryption in an enterprise environment can be critical to maintaining effective security, but can also be complicated to set up—requiring significant advance planning, coordination, and time. To help simplify this task, Dell Latitude D630 and Latitude D830 notebooks with Seagate Momentus FDE.2 hard drives and EMBASSY management software from Wave Systems allow administrators to rapidly set up and enable hardware-based drive encryption and bypass time-consuming procedures such as running the chkdsk utility—a process that can potentially take several hours on a typical 160 GB drive.

These data protection features are designed to be not only powerful, but also easy to use, comprehensively integrated, and scalable. The drive is designed to encrypt all files copied to it with a key stored in a secure area of the drive, without the performance overhead associated with software-based solutions for secure read and write operations. For end users, a provided password can be easily synchronized with an existing Microsoft® Windows® OS password, helping minimize the need for training and help-desk assistance and potentially making data protection as simple as closing the notebook after use. For administrators, robust reporting tools can provide detailed event logs indicating whether preboot authentication has been enabled, helping make supporting users at remote locations as easy as supporting those at an enterprise's headquarters, and helping prevent users or remote administrators from inadvertently compromising data security. And because the drive encryption is designed to be constantly enabled, these features also help simplify compliance with data protection laws and regulations.

ASSESSING THE NETWORK ENVIRONMENT

EMBASSY management software from Wave Systems works in tandem with Seagate Momentus FDE.2 drives in Dell Latitude D630 and Latitude D830 notebooks to help maximize security in environments based on Windows operating systems and the Microsoft Active Directory® directory service. EMBASSY Remote Administration Server (ERAS) is designed to integrate into existing Active Directory domains, essentially adding a second layer of protection to these Latitude notebooks by adding user-based authentication to the drive. A simple administration console allows administrators familiar with Microsoft Management Console (MMC) snap-ins for Active Directory to easily grant permissions to existing users and perform many other drive-related tasks.

Typically, a simple way to implement this technology in an existing infrastructure is to acquire Latitude

D630 and Latitude D830 notebooks from Dell and select the encrypted hard drive option during purchase, which includes a Seagate Momentus FDE.2 drive and preconfigured EMBASSY Trusted Drive Manager (TDM) client components in the system. ERAS is also available through Dell. After adding the client to the domain, administrators can remotely initialize the drive and manage it through ERAS. For existing Latitude D630 and Latitude D830 notebooks as well as Latitude models D530, D531, D620, D631, and D820, administrators can replicate the contents of a standard drive to a Seagate Momentus FDE.2 drive and install the TDM software, enabling the system to communicate with ERAS for further configuration.

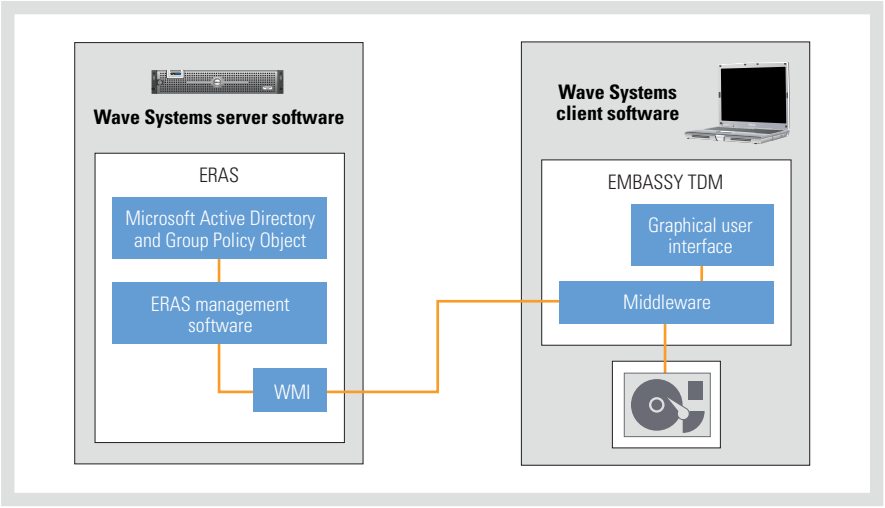

Figure 1. *EMBASSY software from Wave Systems for Dell Latitude D630 and Latitude D830 notebooks with encrypted Seagate Momentus hard drives*

CREATING A ROBUST MANAGEMENT INFRASTRUCTURE

ERAS enables administrators to manage Dell Latitude D630 and Latitude D830 notebooks with Seagate Momentus FDE.2 drives across a network within a domain (see Figure 1). Using ERAS requires the following:

- Any edition of the Microsoft Windows Server® 2003 OS with Service Pack 1 (SP1) or later
- A system running Windows Server 2003 or Windows XP with SP2 and the MMC snap-in (to utilize the remote console)
- MMC 3.0
- Microsoft Group Policy Management Console 3.0
- Microsoft SQL Server® 2005 Express Edition, Standard Edition, Workgroup Edition, or Enterprise Edition database platform
- Microsoft Internet Information Services (IIS) 6.0
- Microsoft .NET Framework 2.0
- Microsoft ASP.NET 2.0 Web Service extension enabled in the IIS Web services extension list
- Microsoft Windows Support Tools

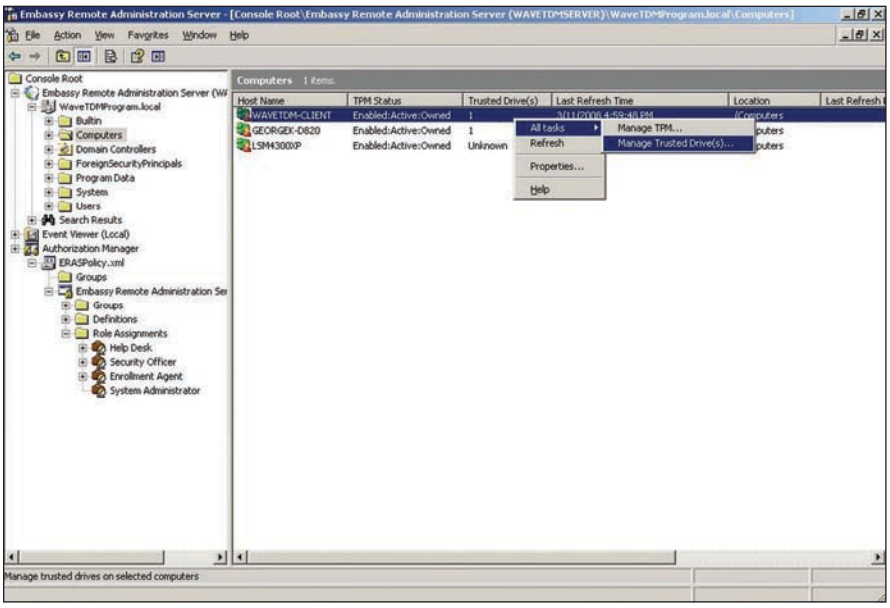

Figure 2. *Management console for EMBASSY Remote Administration Server from Wave Systems*

After ERAS has been installed on a Windows Server 2003 system, administrators should configure the server and client systems to belong to the same domain. Installing ERAS on the server requires a local administrator with administrative privileges in SQL Server and domain privileges to create the required accounts and user groups and make entries in Active Directory. Administrators can integrate ERAS with Active Directory or manage it through an XML ERAS policy file in conjunction with the SQL Server database. After the TDM software has been installed on the Latitude D630 or Latitude D830 notebook, administrators can use Group Policy to push a Windows Management Instrumentation (WMI) file down to these client systems, and then use the ERAS console to manage them (see Figure 2).

CONFIGURING AND MANAGING ENCRYPTED CLIENTS

ERAS is designed to support Dell Latitude D630 and Latitude D830 notebooks through their complete life cycle, from drive deployment to management to

disposal. The first step in activating the drive encryption is to set up preboot authentication, which administrators can do by initializing the drive. Users must then log in during the preboot process to gain access to the drive. Administrators can provide multiple users with access to a given client system, or use the drive properties window in ERAS to perform other management functions.

Administrators can use the Security Control window in ERAS (accessed through the drive properties window) to access the cryptographic erase feature, which allows them to quickly erase drives remotely from the server to help prevent dissemination of confidential information on an encrypted Latitude D630 or Latitude D830 notebook. They can then rapidly re-image and redeploy the drive—a task that may take several hours with typical software-based disk encryption.

When end users forget their password, administrators can also use the ERAS Security Control window for password recovery to help regain drive access, a feature that does not require a connection to the network. The ERAS Help Desk feature also offers a way for end users to retrieve passwords by providing direct physical access to the server through a standard Web browser, a feature that can typically be used on any system connected to the domain (see Figure 3). For example, administrators might provide this designated access to an office manager when the normal IT staff members are not available.

> **"The drive is designed to encrypt all files copied to it with a key stored in a secure area of the drive, without the performance overhead associated with software-based solutions for secure read and write operations."**

Administrators can also use ERAS to manage embedded security technology for Trusted Platform Modules (TPMs). TPMs are chips integrated into select Dell systems that function like embedded smart cards, and can be used to generate encryption or authentication keys and help securely store certificates and other critical information. ERAS offers similar initialization and management features for TPMs as it does for the encrypted drives in Latitude D630 and Latitude D830 notebooks. By combining both technologies, ERAS helps provide a comprehensive solution for securing enterprise systems.

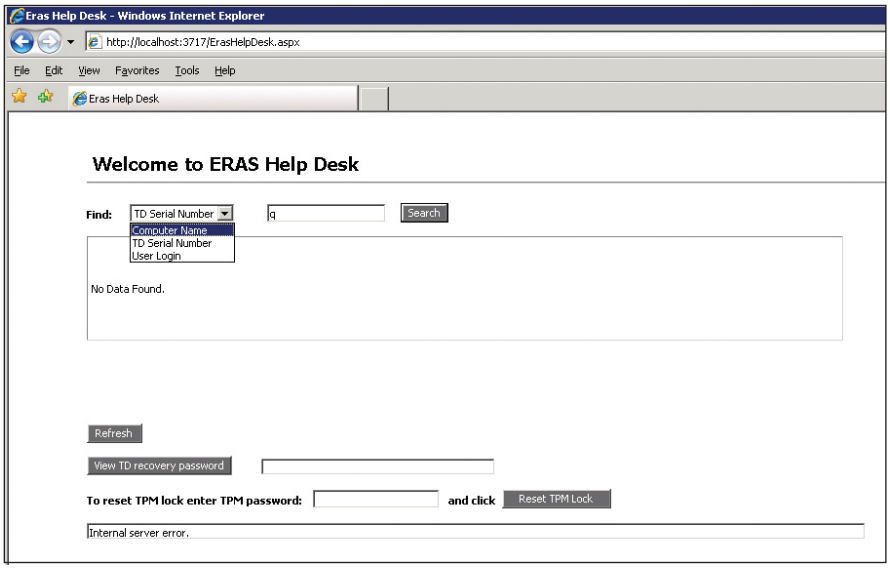

Figure 3. *Help Desk Web browser–based interface for EMBASSY Remote Administration Server from Wave Systems*

PROTECTING CRITICAL ENTERPRISE DATA

Deploying drive encryption has typically been a time-consuming task for enterprise IT administrators. Dell Latitude D630 and Latitude D830 notebooks with Seagate Momentus FDE.2 hard drives and EMBASSY management software from Wave Systems offer a comprehensive, simplified solution for securing client systems, enabling administrators to rapidly deploy and manage encrypted drives to help protect critical enterprise data.

Brian Berger is the executive vice president of marketing and sales for Wave Systems, where he is responsible for developing and implementing the company's trusted computing strategy. Brian is a director for the Trusted Computing Group and serves as chair of the organization's Marketing Working Group. He holds several patents, has a B.A. degree, and attended the Harvard Business School Executive Education program.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINK

Dell Latitude notebooks:
DELL.COM/Latitude