

Balancing Act

This article first appeared in the February 2009 issue of *Novell Connection* magazine.

Striking the Right Balance So that All Your Endpoints Are Secure

USB storage devices have become as commonplace as car keys. In fact, many of you reading this article likely have a thumb drive hanging on your key ring. Of course, it doesn't stop there. MP3 players, PDAs, DVD/CD burners, mobile phones and digital cameras all provide digital storage that makes life easier and more enjoyable for the masses, while at the same time creating a security nightmare for organizations.

By tying security policies to identity, ZENworks Endpoint Security Management gives you the flexibility to make sure that users have the access they need with the proper controls in place, no matter what endpoint they are logged into.

Businesses lose billions of dollars a year as a result of data theft, data loss and the accompanying costs associated with clean up and recovery. A major contributor to this liability is inadequate endpoint protection, especially as it relates to mobile devices and intentional and unintentional misuse of mobile storage technologies. As an administrator, you face a difficult dilemma: how do you implement the appropriate levels of security and control without

impacting the productivity and agility your users need in regard to mobility and removable storage? Too often, endpoint security solutions sacrifice productivity for security, or vice versa.

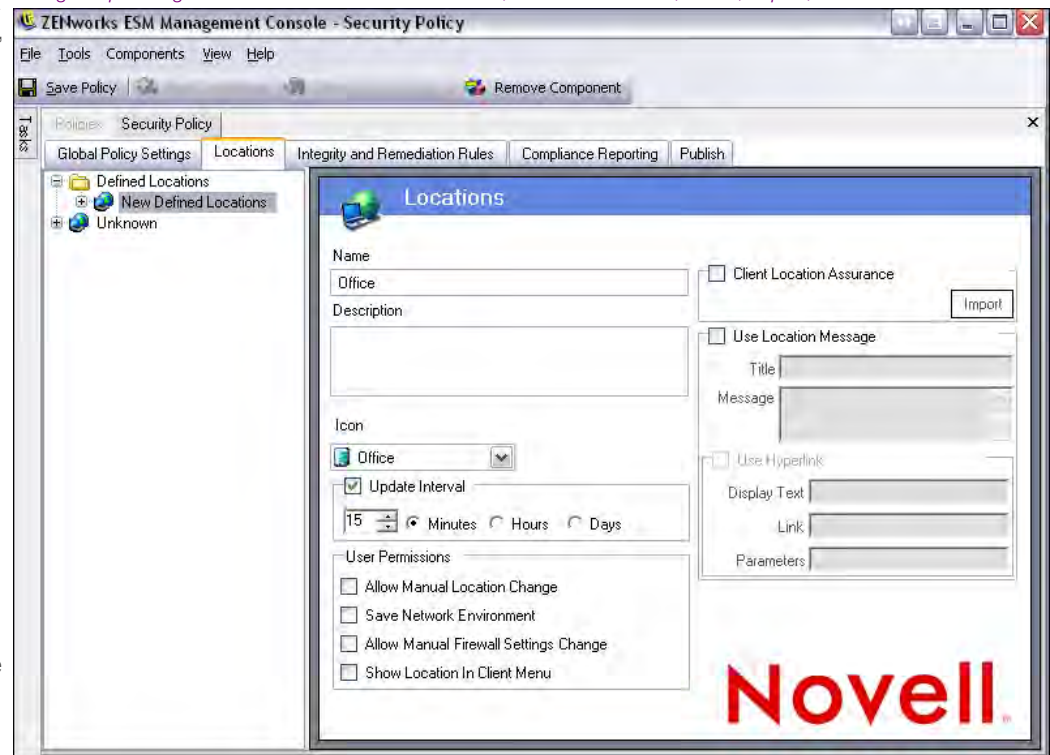
To help you strike the optimum balance in protecting your organization's digital assets, while enabling the agility and mobility of your users, Novell ZENworks Endpoint Security Management differentiates itself in two key areas: how it implements and manages protection, and the multiple levels of protection it provides.

> Endpoint Protection Implementation and Management

A key differentiator for ZENworks Endpoint Security Management is that it lets you implement and manage your endpoint security policies based on user identities. The device-based management implementations other solutions rely on lack the flexibility you need to strike the balance between data security and user agility. For example, you might want to allow certain executives or managers to copy data to thumb drives, while prohibiting rank and file users from doing so—regardless of what device they're on.

Extending this idea further, since you know your

Figure 1: *With the solution's location aware capabilities, a mobile endpoint's security policies can dynamically change depending on its current network environment, such as the office, home, airport, or a WiFi zone.*



executives deal with sensitive information, you might want to make sure that all data they copy to USB devices is always encrypted. By tying security policies to identity, ZENworks Endpoint Security Management gives you the flexibility to make sure that users have the access they need with the proper controls in place, no matter what endpoint they are logged into.

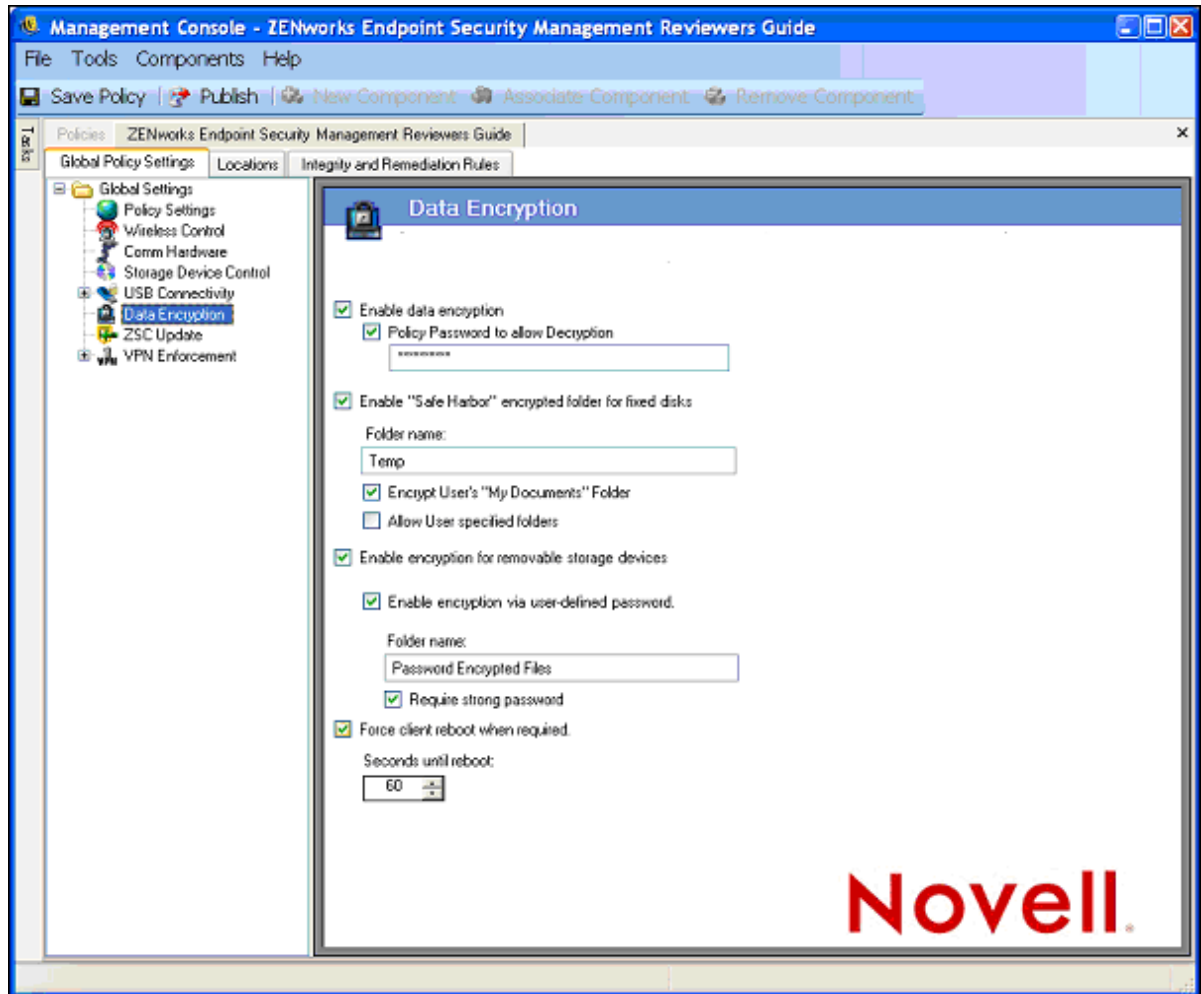
Also, instead of putting endpoint security decisions in the hands of end users—like some solutions do through pop-ups or local settings—ZENworks Endpoint Security Management gives you and your IT security specialists complete, centralized security management for all the endpoints in your enterprise. You govern security enforcement through the creation of identity-based security policies that get pushed out to every endpoint in your enterprise. Also, by using the solution's location awareness capabilities, you can have security policies dynamically change depending on what network environment an endpoint currently finds itself connected

to, such as the office, home, airport, a WiFi zone or some unknown location. (See Figure 1.)

Even though the solution is centrally managed, all policies are enforced locally, regardless of whether or not the endpoint is connected to the network. The agent has built-in self-defense that prevents users from turning off or circumventing security settings even if they have administrator privileges for their workstations. It also protects itself from being intentionally or unintentionally uninstalled, shut down, disabled or tampered with in any way that would expose sensitive data to unauthorized users.

The inherent flexibility in the solution's design enables you to implement it in the way that makes the most sense for your organization. If you have the immediate need to comply with strict regulatory requirements, you can roll out the level of enforcement you need on day one. You can also take a more phased approach, perhaps

Figure 2: ZENworks Endpoint Security Management has built in encryption key management to give you greater flexibility and control over mobile and removable storage security.



ZENworks Endpoint Security Management utilizes a storage device security driver that can, based on policy, enable, disable or configure as read-only any device that dynamically enumerates onto the system.

starting out with more lenient policies to ensure they don't impact your operations, and then leverage the solution's auditing and reporting capabilities to decide how, where and when you need to modify and tailor policy to meet your organization's endpoint security strategy.

The following represent the main components that you install when deploying a ZENworks Endpoint Security Management solution:

- Policy Distribution Service - Distributes security policies to the Endpoint Security Client (agent) and retrieves reporting data from the agent.
- Management Service - Manages user policy assignment and component authentication, reporting data retrieval, creation and dissemination of reports, and security policy creation and storage.
- Management Console - The graphic interface you use to both configure the Management Service and to create and manage user and group security policies.
- Client Location Assurance Service – Provides a real-time cryptographic guarantee of the current location of your endpoints by leveraging network environment parameters that you define.
- Endpoint Security Client (Agent) – Enforces the security on each endpoint where it is installed. A client agent for Windows XP and Windows 2000 enterprise computers is available, as well as one for computers running 32-bit versions of Microsoft Windows Vista with Support Pack 1 and Windows Server 2008.

> Multi-Level Protection

As a comprehensive endpoint security solution, ZENworks Endpoint Security Management provides a wide array of protections and controls. Specific to USB security, the solution focuses on four main areas of protection:

- Storage device enumeration
- USB bus enumeration
- White list device ID and serial number control
- Device encryption

Storage device enumeration determines if a storage device is even allowed to register with the endpoint's file system. To do this, ZENworks Endpoint Security Management utilizes a storage device security driver that can, based on policy, enable, disable or configure as read-only any device that dynamically enumerates onto the system. The storage device security driver sits in the kernel-level storage stack of all your endpoint devices, so it can control access to CD/DVD writers, thumb drives, floppy drives, flash memory cards, ZIP drives, PCMCIA cards and other types of removable media. The driver not only works to protect against data theft, but can stop harmful files—such as viruses, spyware and malware—from infecting your endpoints.

ZENworks Endpoint Security Management also gives you control at an access layer even closer to the USB bus. When a USB device tries to enumerate, it lets you configure policies that utilize device classes or device-friendly names to determine whether it will be enabled, disabled or configured as read-only.

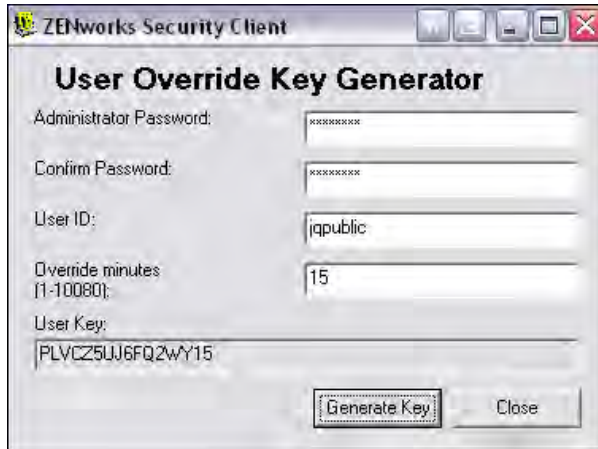
The white list device ID and serial number controls in the solution give you even more granular control over which devices are allowed, blocked or set to read only. By leveraging the device IDs and unique serial numbers of your approved USB devices, this control allows you to ensure that only the USB devices you know about can be used—and only in the manner you dictate.

But perhaps the most powerful and flexible control provided by ZENworks Endpoint Security Management is its encryption control. The solution utilizes AES 256-bit encryption to not only make sure that unauthorized copying of data to USB devices is unreadable, but to ensure that data on lost or stolen thumb drives can't be read by those outside your organization. (See Figure 2.)

In addition to protecting your valuable data, a primary goal of the solution's encryption capabilities is to facilitate the interaction of the users within your organization. If you hand one of your co-workers a thumb drive containing information they need to do their job, you want them to be able to read it. However, if they happen to lose that thumb drive on an airplane or a cab, you don't want whoever finds it to be able to read that data. The way ZENworks Endpoint Security Management implements data encryption on removable drives delivers this capability.

In addition to protecting your valuable data, a primary goal of the solution's encryption capabilities is to facilitate the interaction of the users within your organization.

Figure 3: *To provide a user a temporary emergency override to read encrypted data, you can generate a user-specific, time sensitive, one-time hash based on your encryption key.*



To give you greater flexibility and control, encryption key management is built into the solution. If you choose to encrypt all data copied to removable drives, when the solution pushes that policy out to your endpoints, it will place your organization's encryption key into the agents residing on your endpoints. This means that you and your coworkers can read the contents of that thumb drive from any of your organization's managed endpoints, regardless of whether they're connected to the network. It also means if the thumb drive gets lost, its data will be unreadable to anyone outside your organization. If for some reason you need to share a file on a thumb drive with someone outside your organization or policy group, the solution allows you to activate a sharing folder. Users beyond the scope of the policy would be able to access the sharing folder using a password, but they would not be able to read any encrypted files not residing within the sharing folder.

The encryption solution also allows you to give users one-time, temporary emergency override capabilities to read encrypted data on a removable drive that is inserted into a non-managed endpoint. This is extremely helpful in situations where your sales people or executives are on the road and need to use a thumb drive on a machine that doesn't have the agent. Perhaps, they're at a customer site giving a presentation on a customer computer. In these cases, you can generate a user-specific, time-sensitive, one-time hash based on your encryption key that enables them to temporarily read that encrypted data. (See Figure 3.)

> **Comprehensive Endpoint Security**

In addition to USB and removable storage security, ZENworks Endpoint Security Management is a comprehensive endpoint security solution that gives you centralized management and control over your endpoints' personal firewalls, wireless security, data encryption, VPN enforcement, antivirus management and remediation, application control, hardware communication control and integration with network access controls. (See Flipside of Mobile Security.) All of these capabilities combine to help you strike the ideal balance between complete endpoint security and user agility. **N**

Flip Side of Mobile Security

While ZENworks Endpoint Security Management helps you safeguard the security, health and productivity of your organization's endpoints, ZENworks Network Access Control delivers on the flipside of the mobile security equation: protecting your organization from mobile devices you do not own or manage that enter your environment. To learn more about ZENworks Network Access Control, visit www.novell.com/products/zenworks/networkaccesscontrol/.