



## Safend Protector 3.2

# What's New?

### New Security Features

#### File Type Control

Safend Protector 3.2 now includes an additional layer of granularity and security by inspecting files for their type as they are transferred to/from external storage devices. This technology allows for highly reliable classification of files by inspecting the file header contents rather than using file extensions, thus preventing users from easily bypassing the protection by renaming file extensions. With over 180 built-in file extensions covering all popular applications categorized into 14 file categories, policy definition has never been easier.

By inspecting both files downloaded to external storage devices and those uploaded to the protected endpoint, multiple benefits can be achieved:

- An additional protection layer for preventing data leakage
- Prevention of viruses/malware introduction via external storage devices
- Prevention of inappropriate content introduction via external storage devices.  
Examples of such content:
  - Unlicensed software
  - Unlicensed content (e.g. music and movies)
  - Non work-related content (e.g. personal pictures)

With this feature, administrators can define policies which approve/block specific file types on the inbound and outbound channels. This includes separate definitions for each channel as well as support for both white list and black list methodologies.

#### Content Inspection Integration

In version 3.2, Safend introduces a capability that leverages existing content monitoring and filtering solutions to enable ultra-granular data leakage prevention on endpoints. This feature adds an additional layer of security to the existing protection, so that capabilities extend beyond approving device types, specific devices and file types to monitoring the actual content of each file. With this capability, Safend aims at integrating with multiple vendors in order to maximize the value for its customers.

For its first go-to-market integration, Safend has chosen PortAuthority's (acquired by Websense) Information Leakage Prevention (ILP) solution. PortAuthority's content-aware solution addresses the issue of data leakage inside the network and at the network gateway (outgoing email, internal email, instant messaging, web communications, networked printing, etc.). This partnership combines the best-of-breed approaches from both providers to present a comprehensive, content-aware network and endpoint ILP solution.

With this new technology, each file that is downloaded from an endpoint to an external storage device can be inspected to determine whether it contains sensitive information of any kind (e.g. intellectual property, consumer data etc.). Once it is determined that the file contains sensitive information, the user is notified that this file should not be transferred to external devices, and a trace log is created for the administrator. With this log, available both from Safend Management Console and PortAuthority Console, the administrator is provided a fine-grained list of data breaches through external storage devices.

(\*) This feature is offered as an add-on to Safend Protector 3.2 requiring an additional license.

### **CD/DVD Media White Lists**

In version 3.2, Safend Protector includes the ability to white-list specific CD/DVD media, providing better control on the usage of CD/DVD drives. This mechanism computes a unique fingerprint identifying the data on each medium. Any change made to the data on the medium will revoke its fingerprint, and in turn remove the medium from the white list. This capability enhances the existing granularity of uniquely identifying devices down to the serial number level.

With this feature administrators can restrict users to use their CD/DVD drives only with approved media. The list of approved media is maintained by the administrator and may include software installation CDs, media with approved content and so on. Access to these authorized media will be limited to read-only mode so as to ensure they remain unchanged following authorization.

In order to facilitate the process of extracting fingerprints from CDs and DVDs, this version includes a new utility. The "Media Scanner" utility scans all the CD/DVD drives on a computer and generates a scan file with the media fingerprints. The utility may be used on any computer and does not require any network connection to the Management Server. This allows you to run the utility on a stand-alone machine in order to avoid the inherent risks of viruses and Trojans which can be introduced via CDs and DVDs.

### **Track Offline Usage of Removable Storage**

Encrypting data on removable storage devices allows organizations to enhance mobility and productivity without compromising security. Administrators can control which devices should be encrypted, as well as which users will be able to access encrypted devices outside the organization.

In version 3.2, Safend Protector provides administrators with improved visibility on the usage of such devices outside the organization. With this unique feature, every offline access to an encrypted device is tracked, providing a comprehensive log of each file transfer to/from this device. With this powerful log, administrators can audit users' actions even on non-company computers, in order to validate legitimate use of corporate data.

For example, a user may be granted with offline privileges for opening a presentation while visiting customer sites. In cases of legitimate use, only these files will be read from the device. On the other hand, a malicious user may abuse this privilege and

download all the data on the device to his home PC. With this new feature, all offline activity of the device is logged, stored securely on the device and uploaded to the Management Server as soon as the device connects to a company computer.

The method of storing offline usage logs on the device does not give the user any indication of the fact that his actions are being monitored. Users cannot access this log nor delete it (with the intention of destroying evidence).

## **Internal Ports**

Version 3.2 extends the reach of Safend Protector beyond external peripherals to include devices connected to the internal computer ports. Internal ports include storage busses such as IDE, SCSI, ATA and S-ATA, which are used to connect internal hard disk drives as well as PCI and PCI-X which cater to devices such as modems and network cards.

This is useful in scenarios such as the following: sophisticated malicious users may connect an additional hard disk drive to their internal IDE bus in order to extract corporate information to this device without leaving any trace. With this new feature, administrators can get immediate alerts on any connection or disconnection of devices to the internal ports of protected endpoints.

## **New Management Features**

### **Policy Server**

Previous versions of Safend Protector relied on Active Directory GPO (Group Policy Object) as the conduit for distributing policies to endpoints. The system leveraged this highly available and scalable architecture, but associating policy objects to users and computers required some user know-how.

Safend Protector 3.2 introduces an additional means of distributing policies to endpoints – the Policy Server. With this feature, policies are distributed directly from the Management Server to the endpoints using the existing SSL infrastructure. To facilitate this, policies are associated to the AD objects from within the Management Console, as part of the process of defining a policy.

With this new feature, Safend maintains and strengthens its highly granular policy management with the ability to set policies which are more general (to OUs or Groups) as well as policies which pinpoint the specific user or computer.

### **Integration with Novell eDirectory**

Similarly to its existing seamless integration with Active Directory, Safend Protector 3.2 now supports full integration with Novell's eDirectory. With this integration the Management Server can be configured to connect the eDirectory in order to import the organizational tree, including OUs, Groups, Users and Computers. This enables viewing of directory objects (computers/user groups) through the Management Console for policy association, log filtering and Client management purposes.

### **External Database Support**

Customers with existing database infrastructures may prefer to use these for storing Safend Protector configuration and log information instead of the built-in internal database provided with the Management Server installation package. This provides higher system scalability and leverages existing infrastructures and know-how.

When installing version 3.2, Safend Protector Management Server can connect to an existing Microsoft SQL (MSSQL) database instead of creating its internal database. Day-to-day maintenance of this database is still handled by Safend Protector including indexing, purging, and key/configuration backup. However, in this case it is the administrator's responsibility to backup log data.

## New Encryption Features

### Stronger Encryption

In previous versions, removable media encryption utilized the industry standard AES algorithm using 128 bit key length. In version 3.2, Safend Protector has been enhanced to also support AES of 256 bit key length.

### Portable, Agent-less Offline Access Utility

In previous versions, users were required to download the Offline Access Utility (from Safend website) in order to access encrypted devices. In version 3.2, encrypted devices now carry the Offline Access Utility on board, ensuring availability of the encrypted data to the authorized user at all times.

When plugging encrypted devices to non-company computers, this utility is the only accessible data on the device. Users can gain access to the encrypted data by running this utility and providing the access password.

### Enhanced Encryption End User Experience

Multiple enhancements have been made to the process in which users encrypt devices:

- **'Encryption required' indication** – A clear indication window has been added, instructing users to encrypt their device. Administrators can customize the notification text in this window.
- **Device Encryption Wizard** – A streamlined wizard guides the user while initializing new devices, setting offline access passwords and removing encryption from device. Access to these options is also available from the context menu of the device in Windows Explorer's "My Computer".
- **Backup/Restore Data** – When initializing new devices, users can maintain existing data on the device. All the data is automatically backed up on the computer before initializing the device. Upon completion, all the data is restored to the device.

## Additional Features

### Support for Windows Vista

Safend Protector Client version 3.2 can be now installed on Windows Vista endpoints. This includes all features of previous versions as well as the new features of version 3.2. The client installation package automatically detects the operating system and installs accordingly. All deployment modes are still available (i.e. MSI over GPO/3<sup>rd</sup> party system and manual installation).

### Additional CD/DVD Burning Formats

Safend Protector can monitor and block multiple CD/DVD burning formats. In this version the support for Universal Disk Format (UDF) has been added. This format is mainly used for DVD burning as well as in specific burning applications.

### Limit Log Sending to Time of Day

Logs are sent from Safend Protector Clients to the Management Server at a policy-defined frequency. In some environments it may be necessary to suppress log sending during specific hours, in order to minimize the effect on network capacity. This option has been added in version 3.2, and is available in the policy settings windows.

### Management Console Enhancements

Some usability enhancements and features have been added to the Management Console:

- **Reset/Delete Clients** – Within the Clients list, Administrators can now reset the status and/or delete clients in order to detect obsolete and non-communicating clients.
- **Block Hybrid Network Bridging** – The interface for configuring this feature has been added to the Port Control window. It allows you to activate the feature as well as define which of the 4 wireless ports (WiFi, Modem, IrDA and Bluetooth) should be blocked when endpoints connect to the corporate LAN.
- **Change Protected Domain** – Administrators can now choose the root domain when synchronizing with Active Directory and Novell eDirectory. This is useful in forest scenarios.
- **Status Bar** – A status bar has been added to the Management Console. This bar constantly shows the logged-in user and server name, and provides quick access to the Client Tasks window.
- **Built-In Queries** – Out-of-the-box sample queries are created upon installation. This provides insight on the types of queries that are possible as well as simplifying administrator actions.