



## Safend Protector 3.3

# File Shadowing

## Feature Description

### 1. Overview

Granularity and visibility are of the essence in any security product, and even more in data leakage prevention products. Once installed, security policies are enforced on users and a security perimeter is established. At this stage security officers should be given the tools to pinpoint and identify security breaches, analyze the forensic evidence, assess its severity and take appropriate action. Safend Protector, with its wide granularity and comprehensive audit and logging features, excels in achieving these requirements.

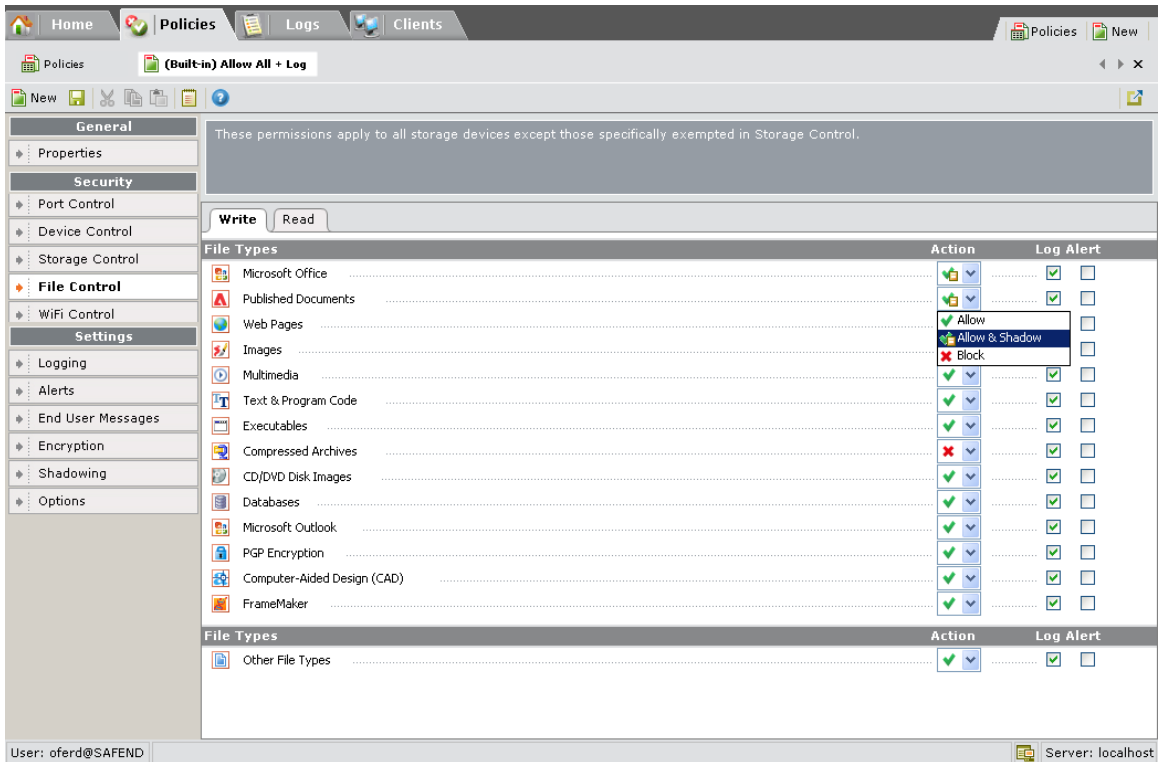
With version 3.3, Safend Protector now also provides File Shadowing – the ability to track and collect copies of files moved to/from external storage devices. It is now possible to set policies requiring shadowing of all data on each of the inbound and outbound channels separately as well as require shadowing only for specific file types. These policies can then be applied granularly on specific users or computers as well as on groups and OU's. Collected shadow files are stored securely in a central repository and available for review by authorized administrators.

Special emphasis was made on preserving the product's security and tamper resistance levels with the introduction of this new feature, while minimizing storage and network utilization requirements.

### 2. Granular Policies

Shadow policies are defined in the "File Control" tab of security policies. In this tab you may choose to shadow all files read/written from/to external storage devices or choose the specific file types to be shadowed.

An additional permission level was added on file types – "Allow & Shadow", as shown below:



In addition to the per-file type granularity, separate policies can be created for the inbound and outbound channels and administrators may also opt to exempt specific device types from shadowing definitions.

### 3. Minimal Impact on Endpoints

Interception of shadow files is made available through existing infrastructures of Safend Protector Client, which enable capturing file metadata as well as file contents on the inbound and outbound channels between the endpoint and external storage devices such as USB flash drives, memory cards, external hard drives and CD/DVD media. These capabilities provide features like File Type Control, Content Inspection and File Logging, and with this new version also File Shadowing.

Much like the existing logging mechanism, shadow files are cached on the machine when it is not possible to relay them to the server/s. This provides the means to overcome situations where mobile endpoints reside outside the organization as well as user attempts to bypass monitoring by disconnecting from the organizational network.

Administrators can set the size for this Local Cache, which is used to store the shadow files until they can be sent to the server. The size, as well as other related parameters, is set within the policy, enabling granular settings for different users and computers. For instance, administrators may see the need to allocate more storage space on laptops since, unlike desktops, they tend to function for considerable portions of the time outside the organizational network.

<b>General</b>	Use global Shadowing definitions in Global Policy Settings, or set policy specific Shadowing definitions.
Properties	<a href="#">Go to Global Policy Settings</a>
<b>Security</b>	
Port Control	
Device Control	
Storage Control	
File Control	
WiFi Control	
<b>Settings</b>	
Logging	
Alerts	
End User Messages	
Encryption	
<b>Shadowing</b>	
Options	

<b>Max Cache Size</b>	
<input type="radio"/> Use global settings:	1024 MB
<input checked="" type="radio"/> Set policy specific settings:	
Cache size will not exceed <input type="text" value="1024"/> MB	
<b>Action when Cache Exceeds Maximum Size</b>	
<input type="radio"/> Use global settings:	Allow users to write files to storage devices (no shadowing available)
<input checked="" type="radio"/> Set policy specific settings:	
<input checked="" type="radio"/> Allow users to write files to storage devices (no shadowing available)	
<input type="radio"/> Always block files written to a storage device	
<b>Max File Size</b>	
<input type="radio"/> Use global settings:	12 MB
<input checked="" type="radio"/> Set policy specific settings:	
Shadowed file will not exceed <input type="text" value="12"/> <input type="text" value="MB"/>	

Files stored in the Local Cache are both compressed and encrypted in order to maximize the use of the allocated cache size as well as to prevent users from tampering with evidence.

## 4. Minimal Network Utilization

Needless to say, network utilization is an issue that needs to be taken into account when applying file shadowing policies. The amounts of data that may result from these policies can be considerably large, and special attention should be given to minimizing the effects.

Multiple measures are available in the policy itself that may help in minimizing this effect. Measures like restricting policies to specific users/computers, focusing on relevant file types (for example, do not shadow images and multimedia files) and setting maximum file size.

Taking into account that these measures are not enough, in version 3.3, all the data sent over the net is compressed before it gets pushed up the SSL channel, thus dramatically reducing bandwidth usage.

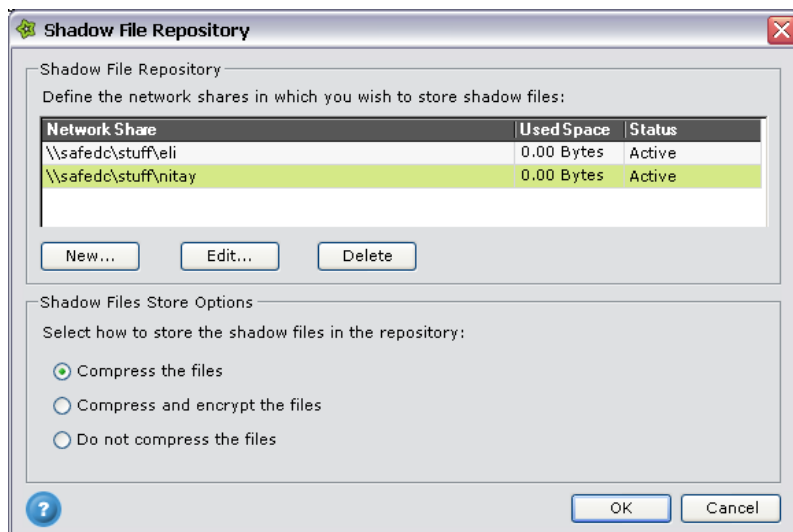
Additional enhancements will be provided in future versions, such as automatic or semi-automatic bandwidth throttling to minimize the effect when computers are connected via VPN, or at remote sites.

## 5. Central Repository for Shadow Files

Shadow files collected from endpoints are stored in a central repository. The files are stored under their original file names and format in a standard file system, providing an open interface for external systems to connect and index/search the information.

For the central repository, administrators define one or multiple network shares which will be used to store the shadow files. If multiple network shares are provided, a load balancing algorithm is used to verify that storage space is used evenly among all shares and seamless failover can occur in cases of failure in accessing one of the shares. The system also periodically purges old shadow files in the repository according to administrator defined depth requirements.

In order to optimize the usage of allocated storage space on the network shares, administrators may opt to store the files in a compressed mode as "\*.zip" files. This is expected to dramatically decrease storage requirements for up to 1:20 ratio. It should be noted, that this option can also be used when external index/search systems are applied on the repository, since most indexing engines in the market handle the zip format.



Typically, administrators should set the privileges for accessing these network shares in a way that will only allow access to the Management Server/s. This will prevent any users from accessing the files in the repository directly. The only exception to this is when connecting external systems to index/search the information. In which case, administrators should set the proper privileges to prevent unauthorized access.

As an additional security layer, it is also possible to store shadow files in encrypted mode, in order to minimize the chance that such files will be accessed by an unauthorized user (i.e. not via Safend Protector Management Console with the appropriate View Shadow Files permission).

## 6. View Shadow Files

Access to shadow files is provided from the File Logs window in Safend Protector Management Console.

File log events now also include shadowing related fields:

- **Shadow**– Yes/No
- **Shadow ID** – The name and path of the file in the central repository
- **Checksum** – A digital signature of the shadow file, for evidence purposes

Right-clicking file log events for file transfers that were shadowed, offers the user the option to open the shadow file, or alternatively to save it to a folder on his computer.

Since the information in shadow files may be highly sensitive, an additional permission (View Shadow Files) was added to the Role Based mechanism, in order to restrict access only to authorized administrators. In addition to that, every access to a shadow file is audited and stored in the database. These audit logs can be reviewed in the Server Logs window.

It is also possible to query for file log events that include a shadow file as well as query for a specific log event using the file name, as it appears in the central repository.

For evidence and non-repudiation purposes, a digital signature is calculated on the shadow file at the interception point (i.e. by Safend Protector Client). This signature is included in the file log event in the Management Console, and can be compared to the file that resides in the central repository, to validate that it is indeed the same file that was transferred by the user and rule-out any doubts as to its authenticity.

## 7. Focus on Security

Safend Protector is distinguished from other products in the market by its high security standard with regards to both architecture and tamper resistance. As mentioned above, a great deal of emphasis was given to the security aspects of this feature. These are covered below:

- **Local Cache Encryption** – Shadow files stored temporarily on the endpoint are encrypted, preventing users from gaining any knowledge about the shadowing process.
- **Tamper Resistance** – Users cannot access nor delete shadow files in the local cache. Any such attempt will instantly trigger an alert on the Management Console.
- **Secure Transport** – Shadow files are sent from endpoints to server/s over SSL secured communication channels.
- **Central Repository Encryption** – Shadow files stored in the central repository can be encrypted, thus preventing any access except by authorized administrators via the Management Console.
- **“View Shadow Files” Permission** – Access to shadow files is restricted only to administrators who are given a specific permission in the Role Based mechanism.
- **“View Shadow Files” Audit Log** – Every access to a shadow file is audited in the Server Logs.
- **Evidence Support** – A digital signature is computed at the interception point of each shadow file. This can be used as evidence to prove that the shadow file was indeed transferred by the user.

## 8. Miscellaneous

- **Server Scalability** – With the addition of this feature, the amounts of data transferred from the endpoints increases significantly. An additional new feature of version 3.3 is Server Cluster, allowing seamless cascading of servers as the traffic increases. See a description of this feature in a separate document.
- **Supported Storage Devices** – File Shadowing is provided for the following storage devices:
  - Removable Storage Devices
  - External Hard Disk Drives
  - CD/DVD Drives (limited to files read from CD/DVD)
- **Interaction with Content Inspection** – The File Shadowing feature is not available on systems configured with Content Inspection Integration.