safend
Securing Your Endpoints

SAFEND DATA PROTECTION SUITE
USER GUIDE
Version 3.6.1

Important Notice

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Safend. Such information is supplied solely for the purpose of assisting explicitly and properly authorized Safend Data Protection Suite users.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the expressed prior written permission of Safend.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this guide is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and with the expressed understanding that Safend shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

Copyright ©2005-2019

Safend. All rights reserved.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Table of Contents

1	**Introducing Safend Data Protection Suite**	**8**
1.1	Port and Device Control	8
1.1.1	*Port Control*	*8*
1.1.2	*Device Control*	*8*
1.1.3	*File Logging and Shadowing*	*10*
1.2	Data Control	11
1.2.1	*Data Control Policies*	*11*
1.2.2	*Discovery Policy*	*11*
1.3	Internal Hard Disk Encryption	12
1.3.1	*Safend Auditor*	*12*
1.4	Safend Data Protection Suite Components	13
1.5	Safend Data Protection Suite Management Console	15
1.5.1	*Safend Policy Definition*	*15*
1.6	Safend Policy Enforcement – Safend Data Protection Suite Client	16
1.7	Safend Data Protection Suite Implementation Workflow	17
2	**Getting Started**	**20**
2.1	Launching Safend Data Protection Suite Management Console	20
2.2	Application Overview	21
2.2.1	*Tabs*	*23*
2.3	Home Tab	26
2.3.1	*Home Tab Description*	*27*
3	**Policies Overview**	**29**
3.1	Defining a Policy	29
3.2	Quick Tour of the Policies Tab	29
3.3	Planning Policies	31
3.3.1	*User and Computer Policies*	*31*
3.4	Managing Policies	32
3.4.1	*Modifying a Policy*	*33*
3.4.2	*Deleting Policies*	*33*
3.4.3	*Exporting and Importing a Policy*	*33*

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3.5	Distributing Policies	33
3.5.1	*Architecture*	*34*
3.5.2	*Associating Policies with Organizational Objects*	*34*
3.5.3	*Associating a Policy with Organizational Objects*	*34*
3.5.4	*Restricting the policy to users/computers*	*41*
3.5.5	*Disassociating a policy from organizational objects*	*41*
3.6	Policy Merging	42
3.6.1	*Port and Device Control Policy Merging*	*42*
3.6.2	*Data Control Security Policy Merging*	*44*
3.6.3	*Discovery Policy Merging*	*46*
3.6.4	*Hard Disk Encryption Policy Merging*	*47*
3.6.5	*Settings Policies*	*47*
4	**Data Control**	**48**
4.1	Quick Tour of the Data Control Policy Window	48
4.2	About Data Classification	51
4.2.1	*End-user Based Data Classification*	*51*
4.3	Creating a New Data Classification	51
4.4	Creating Classification Rules	52
4.4.1	*Types of Classification Rules*	*53*
4.4.2	*Setting a Keyword Rule*	*54*
4.4.3	*About Total Minimum Weight*	*55*
4.4.4	*Setting a File Type Rule*	*55*
4.4.5	*Setting a File Properties (Name) Rule*	*56*
4.4.6	*Setting a File Properties (Size) Rule*	*56*
4.4.7	*Setting a File Properties (Title) Rule*	*57*
4.4.8	*Setting a File Properties (Subject) Rule*	*58*
4.4.9	*Setting a File Properties (Author) Rule*	*58*
4.4.10	*Setting a File Properties (Company) Rule*	*59*
4.4.11	*Setting a File Properties (Template) Rule*	*60*
4.4.12	*Setting a File Properties (Any) Rule*	*61*
4.4.13	*Setting a Pattern (Advanced) Rule*	*62*
4.4.14	*Setting a Data Fingerprints Rule*	*63*
4.4.15	*Adding Excluding Rules*	*64*

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.4.16 *Adding Rules from the Rules Repository* *65*
4.4.17 *Editing a Classification Rule* *66*
4.4.18 *Removing a Classification Rule* *66*
4.5 About a Data Control Security Policy 66
4.5.1 *Creating a Data Control Security Policy* *67*
4.5.2 *Channel Configuration* *72*
4.6 About Discovery Policies 99
4.7 Creating a Discovery Policy 100
4.7.1 *Configuring Discovery Settings* *100*

5 Port and Device Control Policies 103
5.1 About the Port and Device Control Policy Window 103
5.2 Port and Device Control Policy Window 106
5.3 Policy Properties Tab 106
5.3.2 *Approved WiFi Networks* *109*
5.3.3 *Anti-Hybrid Network Bridging* *109*
5.4 Approving Devices and WiFi Connections 119
5.4.1 *Adding Device Groups* *120*
5.4.2 *Adding a Device Using the Wizard* *121*

6 Hard Disk Encryption Policies 130
6.1 Hard Disk Encryption Process 130
6.2 Quick Tour of the Hard Disk Encryption Window 130
6.2.2 *Technician Mode Users* *134*

7 Additional Configuration Settings 136
7.1 Global Policy Settings 136

8 Managing Clients 157
8.1 Quick Tour of the Clients Tab 157
8.2 Hard Disk Encryption Utilities 170
8.3 Retrieving Latest Information from a Client 173

9 Viewing Logs 180
9.1 Quick Tour of the Logs Tab 180

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

9.2	Logs Table	182
9.2.1	*Viewing Additional Records*	*183*
9.3	Queries	190
9.3.1	*Collecting Logs*	*202*
10	**Running Reports**	**209**
10.1	Report Definitions	209
10.2	Quick Tour of the Reports Tab	209
11	**Administration**	**224**
11.1	Administering Data Protection Suite	224
11.1.1	*Administration Window*	*224*
11.1.2	*Deployment Settings*	*245*
12	**End-User Experience**	**259**
12.1	Safend Data Protection Suite Agents	259
12.1.1	*Safend Data Protection Suite Agent Messages*	*259*
12.1.2	*Data Control Messages*	*259*
13	**Appendix A – Safend Recovery Tool for Encrypted Hard Disk**	**286**
13.1	Bootable CD Recovery	286

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

About This Guide

- Chapter 1 **Introducing Safend Data Protection Suite**, introduces the Safend Data Protection Suite solution, the system's architecture and suggested workflow.
- Chapter 2 **Getting Started**, describes how to launch the Safend Data Protection Suite Management Console. It then provides a quick tour through the interface of the Safend Data Protection Suite Management Console and describes the Home Tab that provides access to the system's main functions.
- Chapter 3 **Policies Overview**, introduces and defines policies and describes how to manage and distribute policies to deploy Safend Data Protection Suite policies to the endpoints of your organization.
- Chapter 4 **Data Control**, describes how to build and manage Safend Data Protection Suite Data Classification, Security and Discovery policies in the Policies Tab.
- Chapter 5 **Port and Device Control Policies**, describes how to define Safend Data Protection Suite port and device control policies and how to manage them.
- Chapter 6 **Hard Disk Encryption Policies**, describes how to build and manage Safend Data Protection Suite Hard Disk Encryption Policies.
- Chapter 7 **Additional Configuration Settings**, describes global policy settings, and configuring Agent messages and the Configuration tab in the Policies tab.
- Chapter 8 **Managing Clients**, explains how to view the status of the Safend Data Protection Suite Clients protecting your organization's endpoints and how to perform actions on these Clients, such as updating Client policies, reviewing latest Client information and more.
- Chapter 9 **Viewing Logs**, describes how to monitor your organization by viewing logs derived from Safend Data Protection Suite Clients protecting your organization's endpoints, as well as logs derived from the Safend Data Protection Suite Server(s).
- Chapter 10 **Running Reports**, describes how to configure and run Safend Data Protection Suite reports.
- Chapter 11 **Administration**, describes how to define global Safend Data Protection Suite administration settings.
- Chapter 12 **End-User Experience**, describes the experience of being protected by Safend Protector Client, such as end-user messages, and the actions that can be performed in the Client, such as encrypting removable storage devices.
- **Appendix A – Safend Recovery Tool for Encrypted Hard Disk**, explains how to use the Safend Recovery Tool to recover the encrypted hard disk after a serious error occurs.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1 Introducing Safend Data Protection Suite

Safend Data Protection Suite provides a complete endpoint data protection solution. It includes port control, device control, removable storage encryption, internal hard disk encryption, content control, auditing and reporting in a single software product, with a single management server and a single, lightweight agent.

Note: The Safend Data Protection Suite consists of several license-activated modules. Organizations can purchase all modules, or select the specific modules required for their current security requirements. All functionality is provided by a single software product.

The following sections describe how the Safend Protection Suite works.

1.1 Port and Device Control

Safend Protector, a license-activated module of the Safend Data Protection Suite applies customized, highly-granular security policies over all physical and wireless ports and devices including the encryption of all data transferred to removable storage devices and CD/DVD media.

Further details about port control are provided in Port and Device Control Policies.

1.1.1 Port Control

The Safend Data Protection Suite can intelligently allow, block or restrict the usage of any or all computer ports in your organization according to the computer on which they are located, the user who is logged in and/or the type of port. Safend controls USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (e.g., dialup, 3G, etc.), WiFi, IrDA and Bluetooth ports.

A blocked port is unavailable. An indication that a port is blocked is given when the computer boots or when a policy is applied that disables a previously allowed port.

1.1.2 Device Control

The Safend Data Protection Suite enables defining which devices can access a port. The following device types, device models and/or devices can access a USB, PCMCIA or FireWire port:

- **Devices Types**: This option enables you to restrict access to a port according to the type of device that connect to it. Examples of device types are printers, network adapters, human interface devices (such as a mouse) or imaging devices. The device types that are available for selection are built into Safend Data Protection Suite. If you would like to allow a device that is not of one of the types listed here, you can use the Models or the Distinct Devices option, described below.
- **Models**: This option refers to the model of a specific device type, such as all HP printers or all M-Systems USB flash drives.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **Distinct Devices**: This option refers to a list of specific devices each with their own unique serial number. For example, the CEO's PDA may be allowed and all other PDAs may be blocked.

1.1.2.1 Protection Against Hardware Key Loggers

Hardware key loggers are devices that can be covertly connected by a hostile entity between a keyboard and its host computer to tap and record keyboard input and steal vital information, especially an identity or password. With Safend Data Protection Suite, you can safeguard your users against this threat: Safend Data Protection Suite can detect hardware key loggers connected to a USB or PS/2 port and policy can be set to block hardware key loggers upon detection.

1.1.2.2 WiFi Control

WiFi control ensures that users only connect to approved networks. You can specify which networks or ad hoc links can be accessed. You can specify the MAC address of the access points, SSID of the network, authentication method and encryption methods to define approved links.

1.1.2.3 Storage Control

Storage control provides an additional level to specify the security requirements of your organization. This can apply to all storage devices, internal or external, fixed or detachable. You can block storage devices completely or allow read-only access. You can also encrypt removable storage devices.

Similar to non-storage devices, storage devices can also be approved according to their type, model or unique ID.

1.1.2.4 U3 Smart Drive and Autorun Control

Certain USB flash drive devices, such as U3 devices, offer smart functionality in addition to their basic storage functionality. This functionality allows them to store and run applications once connected to a host computer. With Safend Data Protection Suite, end-users can use sophisticated storage devices while not exposing endpoints to possible exploitation by unsafe applications carried on these devices as part of their U3 and smart smart functionality.

1.1.2.5 Safend Storage Encryption

Safend Media Encryption allows administrators to manage encryption of all data transferred from organization endpoints to approved removable media devices such as USB flash drives, disk on keys, memory sticks, SD cards, CD/DVD and external hard disks. This provides organizations with comprehensive protection from both accidental data loss and deliberate leakage of corporate assets.

The Safend Data Protection Suite can restrict usage of encrypted devices and media on company computers. This extends the security borders of organizations and prevents employees from deliberately leaking data through these high-capacity devices.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Within the organization, media encryption is fully transparent. End-users can read and write to/from media, as they would normally do. However, when the same device or media is used on a computer that is not part of the organization, the data on it will not be accessible.

Safend media encryption is designed to work company-wide. Encrypted devices can be read and used interchangeably on any computer in the organization, while existing control based on device vendor/model and serial number still applies.

On removable storage devices, the Safend Data Protection Suite administrator can choose whether or not to allow specific users password-protected access to the data on unauthorized computers. If allowed, each user can set their own offline password and use the Offline Access Utility (on the encrypted device) on an unauthorized computer to enter their password and access the data securely.

1.1.2.6 File Control

File Control includes an additional layer of granularity and security by monitoring and controlling file transfers to/from external storage devices. Definitions are set on file type levels providing the ability to allow or block specific file transfers as well as generating logs and alerts.

1.1.2.7 File Type Control

With File Type Control a highly reliable classification of files is performed 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 protective layer that prevents data leakage.
- Preventing viruses/malware entering from external storage devices.
- Preventing inappropriate content entering via external storage devices, for example unlicensed software or content like music and movies or non work-related content like personal pictures.

Note: File Type Control, controls and monitors files transferred to/from removable storage devices only according to the file type, regardless of its content. To apply a more granular policy on files transferred to removable storage devices according to their data classification, based on the file content, use Data Control Security Policies.

1.1.3 File Logging and Shadowing

An additional level of monitoring the activity in your organization is provided in the File Logging feature, which enables you to log information written to or read from removable media devices or a CD/DVD. File logs as well are viewed in the Logs Tab. This option provides you with an audit trail of which data is transferred in and out of the organization and may be used to analyze

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

security incidents, as well as keep track of people's activity and notice potential abuse of portable storage devices. It will help you better comply with company security regulations and enhance the visibility of how your organizational data flows.

For highly sensitive departments in your organization, or for specific users who requires special attention, you can also use the File Shadowing feature. This feature allows you to collect copies of files moved to/from external storage devices. The files are stored in a central repository and can be viewed by authorized administrators.

Note: since using this ability will influence both network utilization and storage resources, use it with caution, preferably on small, well defined parts of your organization. Using file name monitoring and file shadowing allows administrators the freedom to create policies that do not restrict usage of devices, yet allow full visibility of the activity and content transferred to removable media.

1.2 Data Control

1.2.1 Data Control Policies

The Safend Inspector, a license-activated module of the Safend Data Protection Suite, defines how the Safend Data Protection Suite reacts when classified data is transferred through controlled channels. Each data control policy defines how the Safend Data Protection Suite reacts to a specific Data Classification. The user can define custom data classifications, or use built-in classifications provided by Safend. Safend Data Protection Suite inspects the following channels:

- Email
- Web
- External Storage
- Local Printers
- Network Shares
- Network Printers
- Portable Virtual Storage
- FTP
- Application Channels

1.2.2 Discovery Policy

The Safend Discoverer, a license-activated module of the Safend Data Protection Suite, allows security administrators to locate sensitive data stored on organizational endpoints. Discovery Policy helps identify gaps in data protection and compliance initiatives, and provides insight into which policies should be implemented using other modules of the Safend Data Protection Suite.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1.3 Internal Hard Disk Encryption

The Safend Encryptor is a license-activated module of the Safend Data Protection Suite. It enforces an enterprise wide policy to protect the data stored on PC and laptop hard drives, so that sensitive data cannot be read by unauthorized users in case of loss or theft.

The Safend Encryptor utilizes a Total Data Encryption technology that encrypts all data files, while avoiding unnecessary encryption of the operating system and program files. This innovative concept minimizes the risk of operating system failure, and poses negligible performance impact on user productivity.

Leveraging this unique encryption technology, Safend Encryptor provides a genuinely transparent hard disk encryption solution, by using the existing Windows login interface for user authentication.

Safend Encryptor utilizes industry standard AES-256 encryption, and is common criteria certified (evaluation assurance level 2 for sensitive data protection), and FIPS 140-2 certified. Encryption of data on internal hard drives is controlled by a policy and enforced by the Safend Data Protection Suite Client on the endpoint.

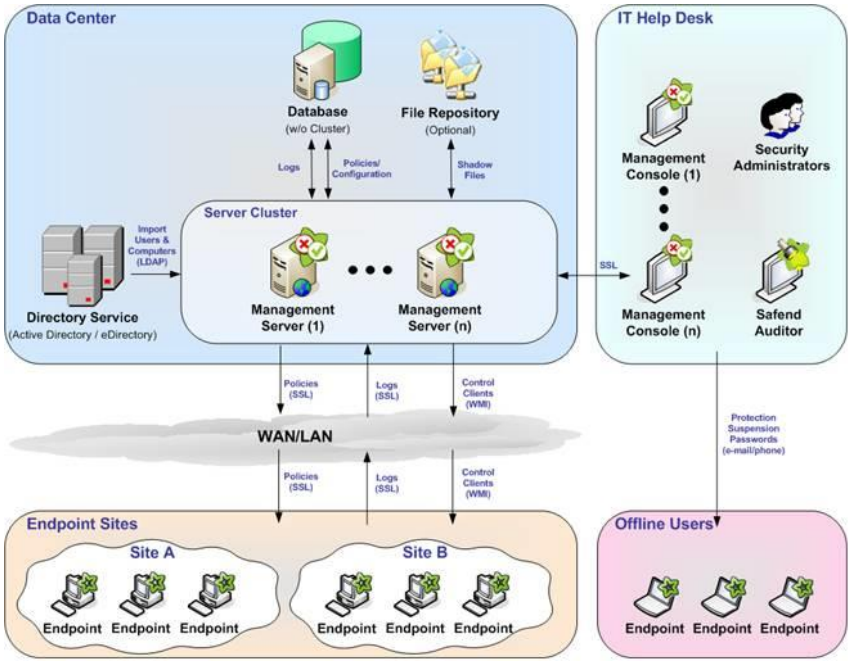
1.3.1 Safend Auditor

Although not an integral part of Safend Data Protection Suite, the Safend Auditor tool goes hand in hand with Safend Data Protection Suite, complementing it by providing a full view of which ports, devices and networks are (or were previously) in use by your organization's users. The output of a Safend Auditor scan can be used to select the devices and networks whose usage you want to approve.

For more details refer to the *Safend Auditor User Guide*.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1.4 Safend Data Protection Suite Components



The system comprises the following components:

Component	Description
Safend Data Protection Suite Management Server(s)	Safend Data Protection Suite Management Server(s) store policies and other definitions, collect logs from Clients, enable Client management and distribute policies to Clients. The Management Server(s) use either an internal/external database for its repository (see below). The Management Server(s) use IIS to communicate with Clients and Management Consoles (over SSL). Controlling Clients is performed via WMI. LDAP compliant protocols are used to synchronize with the existing organizational objects stored in Active Directory. The Management Server(s) distributes policies directly to Clients (via SSL).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Component	Description
Internal/External Database	Standard databases are used for storing system configuration, policies and log data. Administrators may opt to use an internal MySQL database supplied in the Management Server installation package or to connect to existing MSSQL database infrastructures. While using the internal database is simpler and maintenance free, connecting to an external database provides better performance and scalability. Note that server clustering is only possible using an external MSSQL database.
Safend Data Protection Suite Management Console	This enables you to manage Clients, view logs, define policies and administer the system. The Management Console can be installed and run from any computer on your network and uses SSL when communicating with the Management Server. The management console supports one-click deployment from the server website.
Safend Data Protection Suite Client	This protects and monitors the endpoints in your organization and alerts/reports about user activity. The Client communicates with a Safend Data Protection Suite Management Server using SSL.
Safend Auditor	Although not an integral part of Safend Data Protection Suite, Safend Auditor is a light-weight client-less tool that goes hand in hand with Safend Data Protection Suite and completes it by providing you with a full view of what ports, devices and networks are (or were previously) in use by your organization's users. You use the output of a Safend Auditor scan to select the devices and networks whose usage you want to approve.
Safend Data Protection Suite Management Server Cluster	A server cluster enables the installation of several Safend Data Protection Suite Management Servers connected to a single external database, so that they seamlessly share the load of traffic from the endpoints, as well as provide redundancy and high availability.

A server cluster can only be created on systems using an external MSSQL database (not an internal database), which can be accessible to all member servers of the cluster. These servers share a single MSSQL database or an MSSQL database cluster. The list of available servers is routinely transferred to clients. Clients randomly select the server with which to connect, in order to ensure an even distribution of the load between servers. In case of a failure to connect to a specific server, the client will immediately select another server and connect to it.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Note: Management Consoles will connect to the server from which they were originally installed.

1.5 Safend Data Protection Suite Management Console

Safend Data Protection Suite's Management Console is a unified management tool used by IT and/or security departments for defining permissions through policies, managing clients and monitorimg end user activity usage in an organization.

The Management Console integrates with Active Directory so that you can easily associate policies with your network computers and users. Distribution of policies is performed directly from the server(s) to the endpoints (via SSL).

The Safend Data Protection Suite Management Console is automatically installed on the same machine as the Safend Data Protection Suite Management Server during server installation and can be installed on additional computers as needed. After policies are distributed and applied to endpoints, you can view the log records in the Logs Tab, as described in Viewing Logs.

1.5.1 Safend Policy Definition

Administrators can create different policies using the Safend Data Protection Suite, where each policy configures different components of the Safend Data Protection Suite:

Policy Type	Description
Hard Disk Encryption Security Policy	These policies define whether or not the data on your internal Hard disks will be encrypted. See *Hard Disk Encryption Policies* for a detailed description.
Port & Device Control Security Policy	These policies specify an organization's policy regarding usage of physical ports, wireless ports, devices and WiFi networks. It also specifies whether the data on removable storage devices and CD/DVD media will be encrypted. See *Port and Device Control Policies* for a detailed description.
Data Control Security Policy	These policies specify an organization's policy regarding sensitive data transferred out of the protected machine using endpoint or network data transfer channels. See *Data* Control for a detailed description.
Data Control Discovery Policy	These policies define the parameters for the data discovery process, which locates and maps sensitive data stored on the organizational endpoints.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1.6 Safend Policy Enforcement – Safend Data Protection Suite Client

Safend Data Protection Suite Client constantly monitors real-time traffic on protected ports and applies customized, highly-granular security policies over all physical, wireless and removable storage interfaces. It blocks unauthorized activities, such as: plugging devices, writing to storage, connecting to WiFi networks or sending sensitive emails. It protects data written to storage devices, alerts administrators about unauthorized user actions attempts and logs events for future viewing and analysis.

If a relevant policy is applied, the Safend Data Protection Suite Client encrypts all data on the machine, making sure it is not compromised if the machine is lost or stolen.

Safend Data Protection Suite Client is a lightweight software package that transparently runs on endpoint computers at kernel level, and enforces protection policies on each machine on which it is applied. It has a minimal footprint (in terms of file size, CPU and memory resources) and includes redundant, multi-tiered anti-tampering features to guarantee permanent control over endpoints.

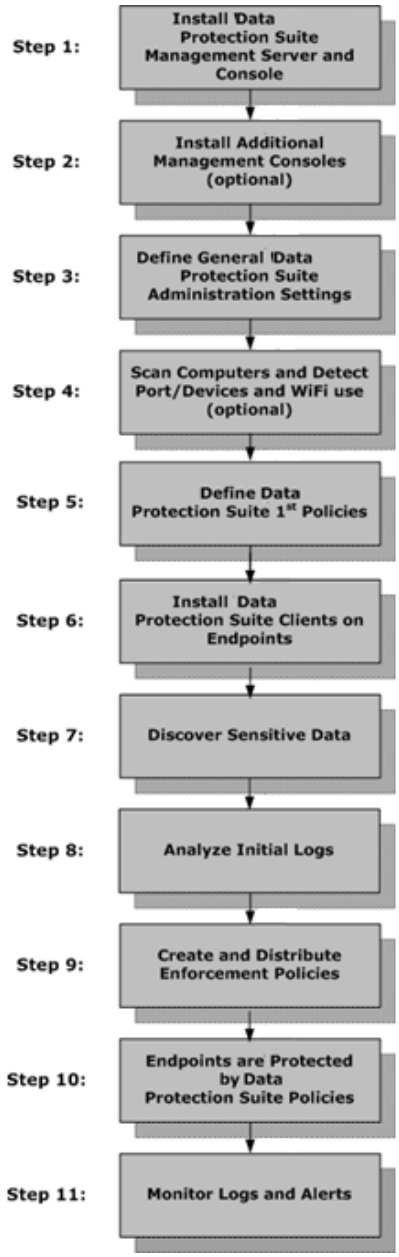
Safend Data Protection Suite Clients can be silently installed on all endpoints. Once policies have been distributed, the Client immediately starts protecting the computer.

When a violation of a Safend Data Protection Suite policy occurs or during specific usage activities, a message is displayed on the endpoint computer. A log entry may be created to record this event, according to the preferences defined in a policy.

The client can be installed in Stealth Mode, hiding both Safend tray icon and messages and making Safend Data Protection Suite Client invisible to the user at the endpoint.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1.7 Safend Data Protection Suite Implementation Workflow



Step		Description
1.	Install the Safend Data Protection Suite Management Server and Console	Described in the Safend Data Protection Suite Installation Guide.
2.	Install Additional Management Consoles (Optional)	Described in the Safend Data Protection Suite Installation Guide.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Step		Description
3.	Define General Safend Data Protection Suite Administration Settings	See Administration.
4.	Scan Computers and Detect Port/Device Usage (Optional)	Use Safend Auditor to detect the ports that have been used in your organization and the devices and WiFi networks that are or were connected to these ports, as described in the *Safend Auditor User Guide*.
5.	Define Safend Data Protection Suite 1st Policies	At this stage, is it recommended to create a permissive policy for the entire organization, which monitors end user activity. This policy will allow you to learn how devices and data are used in your organization for legitimate business processes, before enforcing a more restrictive policy. See *Policies Overview* for more information.
6.	Install Safend Data Protection Suite Client on Endpoints	Described in the Safend Data Protection Suite Installation Guide.
7.	Discover Sensitive Data	In this stage, you create and associate a Discovery policy for organizational endpoints to determine which endpoints store sensitive data. See *Data* Control for more information.
8.	Analyze Initial Logs	In this stage, you review the logs received from the endpoints and determine which user activity is an appropriate business process which should be allowed by policy and which is a potentially harmful action which should be blocked. See *Chapter 10, Viewing* Logs for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Step		Description
9.	Create and Distribute enforcement Policies	In this stage you define how data is protected in your organization: which machines and removable storage devices are encrypted; how ports, devices and WiFi networks are used and which data can be transferred out of protected endpoints.
10.	Endpoints are Protected by Safend Data Protection Suite Policies	In this stage, all security policies are enforced on the endpoints. Logs about attempts to violate these policies, as well as tampering attempts, are created and sent to the Management Server.
11.	Monitor Logs and Alerts	View and export the log entries generated by Safend Data Protection Suite Clients, as described in *Viewing* Logs. Analyze these logs and maintain ongoing visibility into the organization's security status, using Safend Reporter, as described in *Running Reports*.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

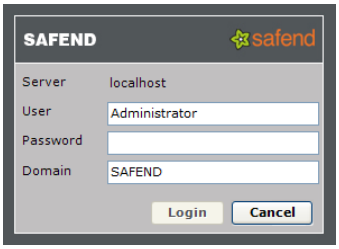
2 GETTING STARTED

This chapter first describes how to launch the Safend Data Protection Suite Management Console. It then provides a quick tour through the interface of the Safend Data Protection Suite Management Console by describing its main windows and menus, and the Home Tab.

2.1 Launching Safend Data Protection Suite Management Console

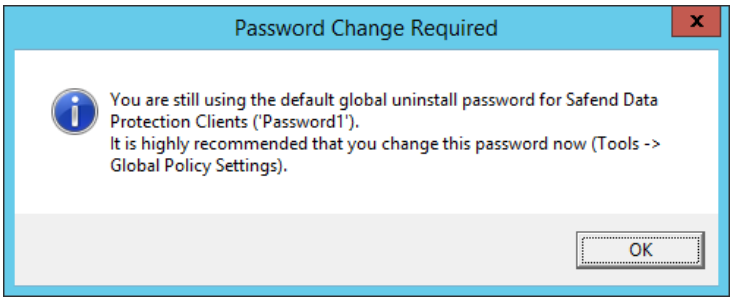
Logging in

1. Double click the icon on your desktop, or select **Start>Programs>Safend Data Protection Suite>Management Console**. The following window opens:



2. Type in your User name, Password and Domain.
3. Click **Login**.

   If you have acquired your permanent license and have not yet changed the default global uninstall password for Safend Data Protection Suite Clients, you will be prompted to do so in the following window.



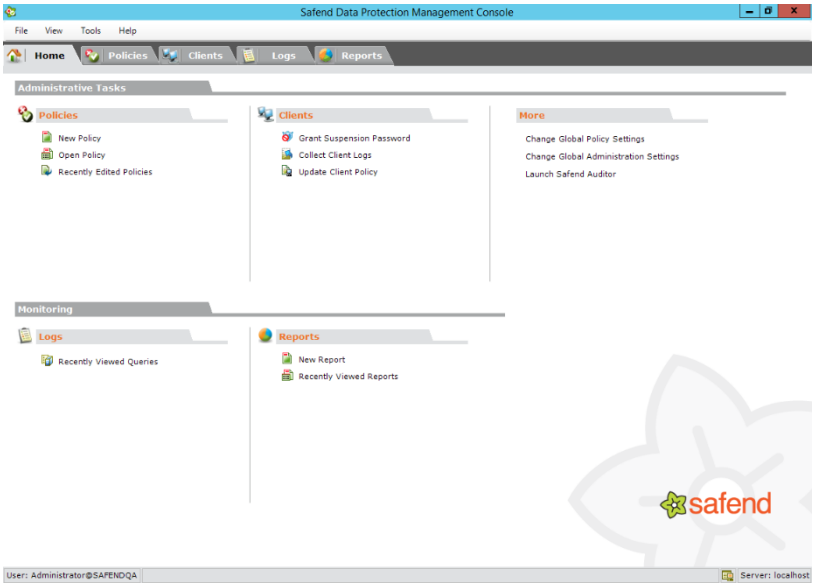
4. Click **OK**. The application opens, displaying the main window.

Note: A Safend Data Protection Suite administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work. A User Role defines the functions, OUs and domains of an organization to which a Safend Data Protection Suite administrator has access, as described in Defining Roles.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

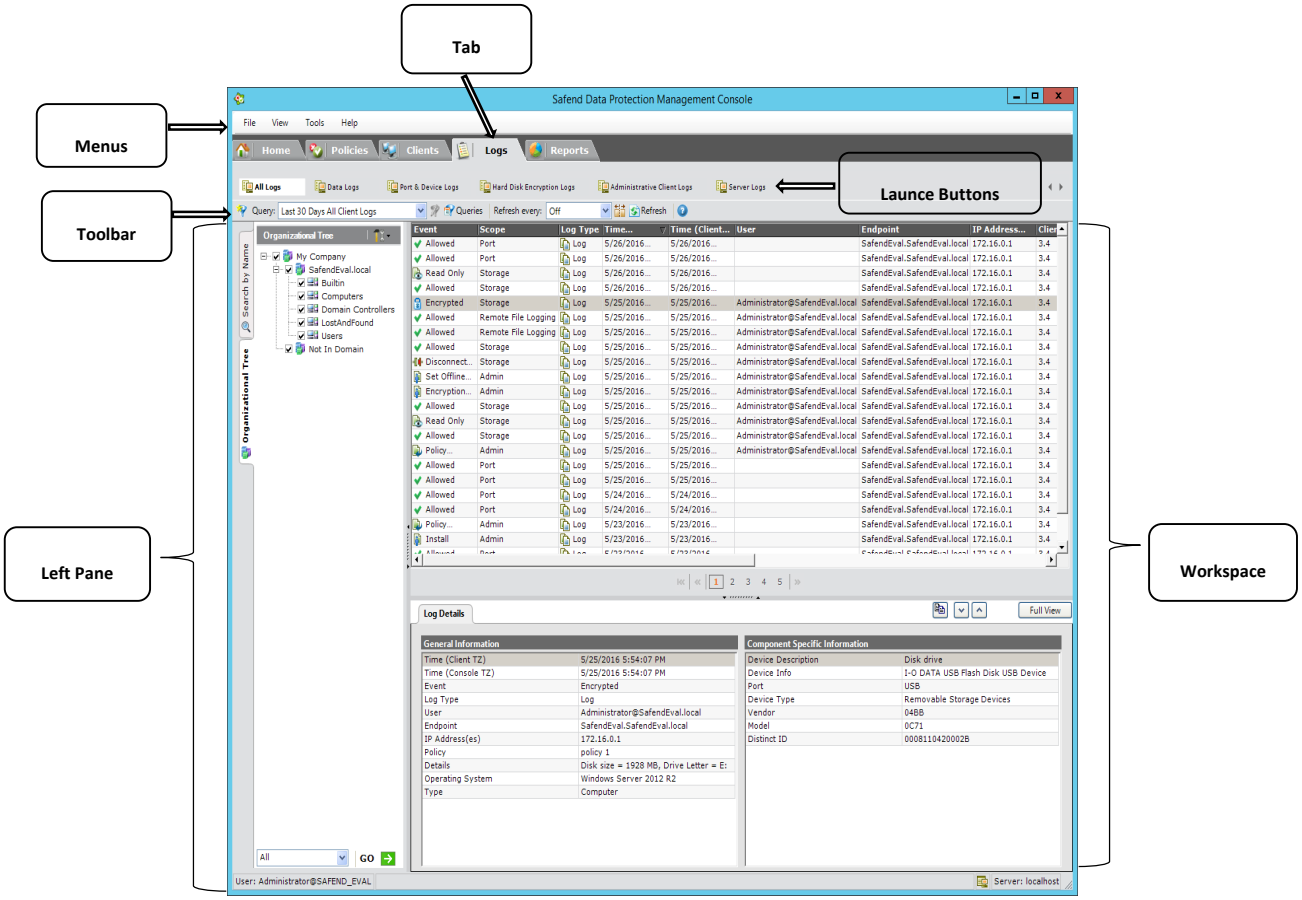
2.2 Application Overview

After logging into the Safend Data Protection Suite Management Console, the Home tab opens.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Click the **Logs** tab. The following window opens:



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

The window includes the following:

Area	Description
Menu Bar	Displays the available menus.
Tabs	Each tab deals with a different aspect of the application
Launch Buttons	Enables launching and handling windows.
Toolbar	Provides various functions which differ between the Policies, Logs and Clients Tabs.
Left pane	Area to make choices which will change what appears in the Workspace. This does not always appear and depends on the tab selected.
Workspace	The workspace provides different information and options, depending on the active Tab.

2.2.1 Tabs

Safend Data Protection Suite Management Console has five tabs. Each tab manages a different aspect of the application, as follows:

Tab	Description
Home	Provides an overview of the most common tasks and information available in the other Tabs. Activate tasks and accesses information.
Policies	Defines and manages policies.
Clients	Displays Client properties and status, updates Client policies, and generates a Client suspension password and more.
Logs	Queries, views and manages logs sent from protected Clients.
Reports	Generates and schedules different graphical reports based on the logs generated.

2.2.1.1 File Menu

The File menu in the Home Tab enables you to open new Policy windows, Log windows, Reports, to log out of the Management Console and to Exit the application.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
New	Opens a submenu that enables you to open a new policy or a new report. The policy options are: Protector, Encryptor, Inspector or Discovery policy.
Change User Role	See Change User Role for a description.
Import Policy	Imports a policy. (Policies Tab only.)
Import Classification	Imports a classification. (Policies Tab only.)
Logout	Logs the current user out of the Management Console.
Exit	Logs out the current user and closes the Safend Data Protection Suite Management Console.

2.2.1.2 Change User Role

A Safend Data Protection Suite administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work.

Note: A User Role defines the functions, OUs and domains of an organization to which a Safend Data Protection Suite administrator has access, as described in Defining Roles. The Change User Role option enables such an administrator to change this role at any time to another role that has been assigned to them.

View Menu

The View menu in the Home Tab enables you to view the progress of Client tasks and to view the different Tabs.

Option	Description
Refresh	Refreshes the current display.
Client Tasks	Displays the Client Tasks Progress window. Refer to Tracking Client Task Progress in Managing Clients to learn about Client tasks.
Policies	Displays the Policies Tab.
Logs	Displays the Logs Tab.
Clients	Displays the Clients Tab.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
Reports	Displays the Reports Tab.

Tools Menu

The Tools menu enables you to perform management and administration tasks.

Option	Description
Synchronize Virtual OU(s)	Imports files from a folder that contains all the Virtual OU machine lists. (This is only available in the Clients window.)
Update Policy	Updates policies on the Clients. For more information see Updating a Policy on a Client.
Collect Logs	Collects logs from the Clients specified (for details see Retrieving Latest Information from a Client in Managing Clients). This option can also be accessed by right-clicking on this client in the Clients Tab. Choose, Retrieve Latest Info (Collect logs).
Audit Devices	Accesses and launches Safend Auditor.
Grant Suspension Password	Creates a key that can be used to grant a suspension key for a user in order to temporarily suspend protection (for details see *Temporary Suspension of Safend Data Protection Suite* in *Managing Clients).* This option can also be accessed by right-clicking on this client in the Clients Tab.
Grant Device Access Key	This creates a password that can be used to access an encrypted device on a machine not running Safend Protector, when an end user forgets his/her password. Refer to *Granting a Device Access Key Offline* for more information.
Hard Disk Encryption Utilities	Provides the following utilities for granting an access key to an encrypted hard disk: • Grant One-Time Access Key: Creates a password that can be used to access a computer only once. This can be useful for enabling managers, for example, to access a computer only once without revealing the computer password. (For further information, see *Granting a one-time access* key.) • Grant Data Recovery Key: Creates a password that can be used to decrypt an encrypted hard disk after a major

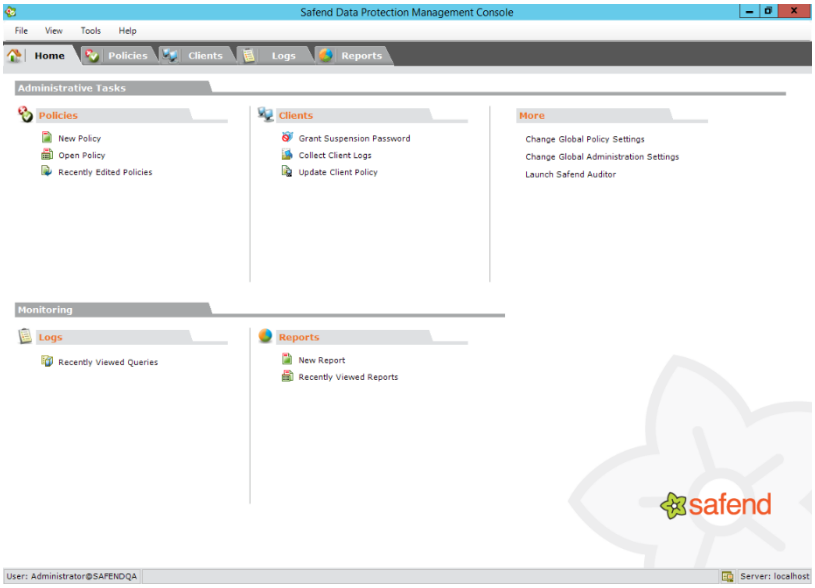
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
	technical failure. (For further information, see *Granting a data recovery* key.) These options can also be accessed by right-clicking on this client in the Clients Tab.
Global Policy Settings	Displays and modifies Global Policy Settings (for details see *Global Policy Settings*).
Global End User Messages	Edits various messages that are displayed in the Safend Data Protection Suite (for details see *Configuring Agent Messages*).
Data Label Templates	Data labels are added to emails increasing data awareness among the employees in an organization. This enables the administrator to define data labeling templates for the entire organization. See *Configuring Data Label Templates* for a description.
Administration	Enables administrator to perform administrative tasks (for details see Administration Window in Administration).

2.3 Home Tab

The Home Tab provides a central access point to the most common tasks and recent information from the other tabs.

Note: A general description of the tasks and information types which can be accessed from the Home Tab is provided here. To learn more about each task/information type, read the relevant chapter in this User Guide.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2.3.1 Home Tab Description

The workspace is divided into two areas: Administrative Tasks and Monitoring.

2.3.1.1 Administrative Tasks

Administrative Tasks is divided into 3 sections: Policies, Clients and More.

Option	Description
Policies Section	
New Policy	To define a new policy: Data Control, Port and Device Control, Hard-Disk Encryption or Data Discovery.
Open Policy	Opens an existing policy. Choose Data Control, Port and Device Control, Hard-Disk Encryption or Data Discovery. The relevant policy window opens.
Recently Edited Policies	A list of the last five policies that were edited is provided, along with the modification date. Click the required policy to open it.
Clients Section	
Grant Suspension Password	Allows you to grant a suspension password for a Client. This enables you to temporarily suspend Safend protection on the Client without having to uninstall the Safend Data Protection Suite Client.
Collect Client Logs	Allows you to select the clients from which you want to collect logs.
Update Client Policy	Updates policies on Clients immediately, without having to wait for the predefined update interval to complete.
More Section	
Change Global Policy Settings	Opens the Global Policy Settings window in order to view or change the Global Policy settings.
Change Administration	Opens the Administration window in order to view or change administration settings.
Launch Safend Auditor	Opens the path to the Safend Auditor window in order to launch Safend Auditor and scan your organizational network and detect currently and previously connected

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
	devices and WiFi links. Refer to the Safend Auditor User Guide for a detailed explanation.
Monitoring	
Logs	• View Last Day's Logs: displays the logs from the last days logs were sent. • Recently Viewed Queries: A list of the recently viewed queries (not including untitled queries) is provided.
Reports	
	New Report: Allows you to open a new Safend Data Protection Suite report. Recently Viewed Report: A list of the recently viewed reports is provided.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3 Policies Overview

This chapter provides an introduction to policies and describes how to manage and distribute Safend Data Protection Suite policies to protect the endpoints in your organization.

Using the Safend Data Protection Suite, the administrator can create different types of policies. Each type of policy configures a different component of the Safend Data Protection Suite:

- **Hard Disk Encryption Security Policy** defines whether or not the data on your internal Hard Disks will be encrypted.
- **Port & Device Control Security Policy** specifies your organization's policy regarding the usage of physical ports, wireless ports, devices and WiFi networks. It also specifies whether the data on removable storage devices and CD/DVD media will be encrypted.
- **Data Control Security Policy** specifies your organization's policy regarding sensitive data transferred out of the protected machine, using endpoint or network data transfer channels.
- **Data Control Discovery Policy** defines the parameters for the data discovery process, which locates and maps sensitive data stored on the organizational endpoints.

You can apply a policy to any of the organizational units that are defined in your Active Directory.

3.1 Defining a Policy

Safend Data Protection Suite Policies are defined in the Safend Data Protection Suite Management Console. You can define one policy for your entire organization, or define customized policies for different organizational objects defined in your Active Directory.

Policies are defined once and then updated on an as-needed basis when the need arises in your organization. Once you have defined and distributed a policy to Safend Data Protection Suite Clients you can view activity logs from each client through the Logs Tab in the Safend Data Protection Suite Management Console. After analyzing the logs, you may wish to adjust your policies.

Policies start protecting the endpoints in your organization after they have been distributed to the computers in your organization.

Note: It is recommended to first create a permissive policy for the entire organization, which monitors end user activities. This policy will allow you to learn how devices and data are used in your organization for legitimate business processes before enforcing a more restrictive policy.

3.2 Quick Tour of the Policies Tab

Click the Policies tab to open the Policies window.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

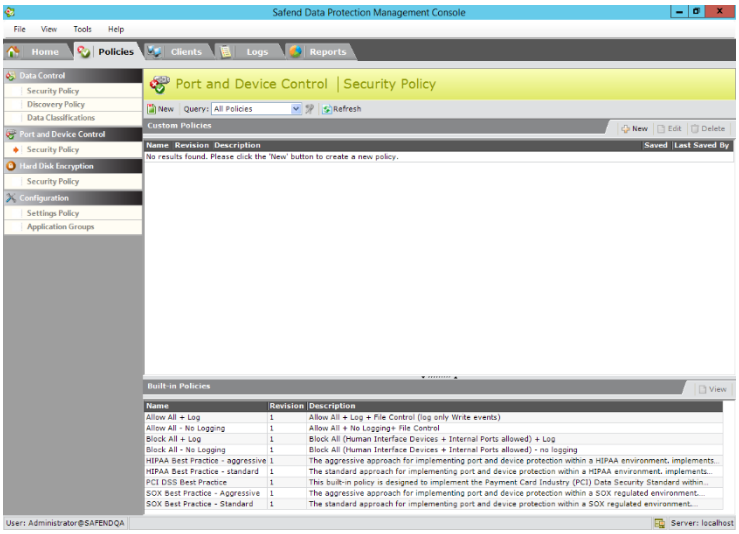
Toolbar

Option	Description
New	This opens a new policy.
Policies Order	This opens the *Policy Order* window which enables you to change the hierarchy order of the policies. This is used to determine which policy settings will take effect in cases where contradicting policies are applied to the same level in the organizational structure. This option is available only in the *Security Policy* window. For more information refer to *policy order*.
Query	*All Policies* is the default option, and all the policies will be displayed. Alternatively choose, *By Associated Object*, to view only the policies associated with a specific object.
Refresh	This updates the list of policies to provide you with an up-to-date view.

Note: The toolbar options will differ depending on what you choose in the left pane.

Workspace

The following screenshot displays the Policy tab Port and Device Control/Security Policy window.



The window is divided into the left pane and the main workspace to the right. The option you select in the left pane determines what will be displayed in the main workspace. The left pane includes the following options:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
Data Control	This consists of 3 options: • Security Policy: Provides a content aware protection layer for data transferred from the endpoint over network or physical channels. • Discovery Policy: Allow security administrators to scan organizational endpoints and discover sensitive data. • Data Classifications: Data classification is a set of definitions which are used by the system to automatically identify data, in order to be able to enforce the appropriate security action and/or monitoring level for the security incident. Data classifications are used by Data Control Security Policies and Data Control Discovery Policies.
Port and Device Control	This section contains definitions of the policy's security settings, which include: port control, device control, file control and media encryption.
Hard Disk Encryption	This section enables you to define which machines should be encrypted.
Configuration	This section enables you to define specific configuration settings for parts of the organization, different then the settings defined under Global Policy Settings.

The workspace displays various types of content, depending on the option you selected in the Data Control, Port and Device Control, Hard Disk Encryption and Configuration sections in the left pane of the window.

3.3 Planning Policies

Before defining policies, take the time to plan the policies best suited to your organization. The best Safend Data Protection Suite Policies for your organization are the ones that best meet your security needs, while still fulfilling the requirements of the people who need access through the ports of your organization's computers. The first thing to plan for is the types of objects to which the policies will apply.

3.3.1 User and Computer Policies

By default, Safend Data Protection Suite uses User Group and Computer Group definitions that are controlled by Active Directory. Each option has its own benefits, as described below.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **Per User Group**: Defining your policies per user group, enables you to be specific regarding the permissions for each user.
- **Per Computer Group**: Defining your policies by computers, enables protecting the endpoints of your organization's computers, regardless of which user is logged into the computer.

Policies that apply to users override policies that apply to computers:

- If you manage your organization by assigning policies to user groups, we recommend that you define one or more general policies for computers. This provides protection for each computer even when no user is logged in.
- Combining user policies and computer policies means that, for example, you can block USB storage devices on all the Customer Service department's computers, but you can allow the manager of the department a more permissive policy according to their username and password, regardless of the computer into which they are logged into.
- Safend Data Protection Suite enforces policies as follows: it first applies a user policy, if one exists for the user that is currently logged in. If not, Safend Data Protection Suite looks for a policy that applies to the computer, and uses it, if found. This means that when no user is logged in, the computer-based policy is used. It is therefore advisable to distribute user-based policies, so that a user is given the same policy regardless of the computer onto which he or she is logged, and to set computer-based policies that are more restrictive. These computer-based policies should still grant access to such devices such as a mouse and keyboard, to be used when no user, or a user outside of the domain, is logged in.

The initial configuration of the Safend Data Protection Suite Client allows all port and device activity, meaning that nothing is blocked. A permissive configuration is necessary so that all port activity is not automatically blocked immediately following the installation of the Safend Data Protection Suite Client.

This means that until you actually define and distribute policies to your endpoints (per user or per computer), the computer that was only installed with the Safend Data Protection Suite Client will continue to operate as before (no blocking of ports and devices).

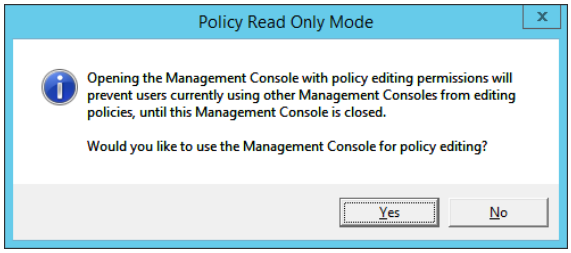
Note: If a policy on the endpoint is tampered with, the Safend Data Protection Suite immediately invokes a panic mode that blocks all access to ports and devices.

3.4 Managing Policies

The Policies window is a central focal point through which you can view a list of your policies and perform various actions such as edit policies, delete policies, export policies and more.

Note: Only one user can edit a policy at any one time. The first user to open a Management Console will have editing privileges. All other users will only have read-only privileges, unless another user specifically takes ownership. The following message is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



3.4.1 Modifying a Policy

After you have opened a policy, you can modify its definitions and save it.

In the various Policy windows, right-click the policy you wish to modify and select Edit or select the policy and click Edit.

3.4.2 Deleting Policies

You can delete policies that are no longer in use. Deleting policies removes them from Active Directory as well as from the Management Console. You may use the Ctrl key to perform a multiple selection of policies to be deleted.

In the various Policy windows, right-click the policy you wish to delete and select Delete or select the policy and click Delete.

3.4.3 Exporting and Importing a Policy

Policies can be exported from the policy database to a file on your computer for later use, for example, saving settings defined in the evaluation copy of the Management Console and using them with a licensed product. Once you have exported the policy, you can import it into the database at a later time.

Exporting a policy

1. In a Policy window, right-click the policy to export and select **Export**. *Save Export Result As* dialog box displays.
2. In the *Save Export Result As* dialog box select the file to export and click **Save**.

Importing a policy

1. In the File menu select **Import Policy**. The *Choose File to Import* dialog box displays.
2. In the *Choose File to Import* dialog box select the file to import and click **Save**.

3.5 Distributing Policies

A main strength of the Safend Data Protection Suite is its extensive integration with existing IT infrastructures. Once installed, the product automatically discovers the network, connects to Active Directory (AD) and synchronizes (read-only) with the existing organizational structure, including OU's, Groups, Users and Computers. This process allows administrators to use their

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

AD objects natively while performing tasks in the Safend Data Protection Suite Management Console.

3.5.1 Architecture

After installation, endpoints start to query the Management Server for the policies associated with them. This query is performed each time a computer starts, on user login and at a predefined interval. These communications are very similar to the way logs are sent from endpoints to the server(s), which is web-service based and utilizes SSL for authentication and encryption.

To ensure high performance, scalability and minimal network utilization, multiple optimizations have been added including compression of policies, server side caching and snapshots.

3.5.2 Associating Policies with Organizational Objects

The user interface for defining policies enables associating a policy to AD objects. This interface allows the association of a policy with multiple objects of various types. An additional functionality is provided for searching for objects either by name or by navigating the organizational tree. Policies can be associated to one or more of the following AD objects: domain, Organizational Unit (OU), group, user and computer

3.5.3 Associating a Policy with Organizational Objects

Associating a policy with organizational objects to apply the policy to the objects comprises the following steps:

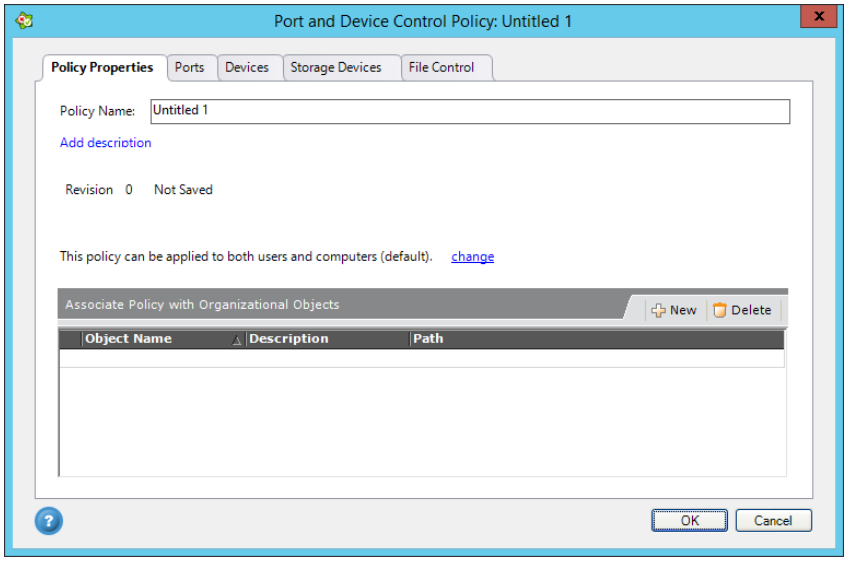
- Opening the Select Object window: described in Opening the Select Object Window.
- Filtering objects and selecting objects for policy association: described in *Filtering and Associating Objects*
- Restricting the policy to users/computers: described in Restricting the policy to users/computers.

Associating a policy with organizational objects is performed from the Select Object window which is accessed from the Policy Properties tab, after clicking the New button. The Select Object window displays organizational objects from which you select the required one(s). In this window you can filter the organizational units so that the list of objects from which you select the associated objects is focused and meets your needs (for example, if you want to associate a policy with users in a specific domain, there is no need to display other domains or computers in that domain).

3.5.3.1 Opening the Select Object Window

The Select Object window is opened from the Policy Properties tab. This tab is available in Data Control/Security Policy and Discovery Policy, Port and Device Control, Hard Disk Encryption and Configuration. When Port and Device Control/Security Policy is selected the following Policy Properties tab is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



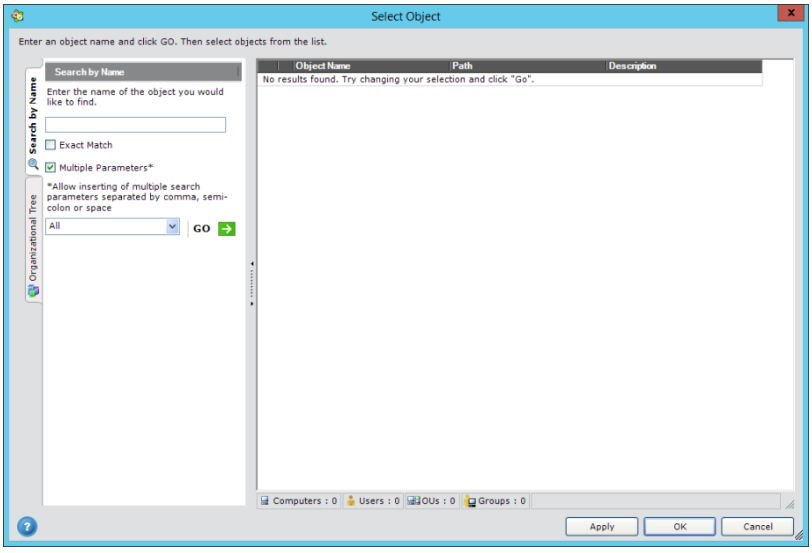
Policy Properties Window

This window enables you to enter the policy's name and a description. A new policy contains the default values, or the policy template values if defined.

The Policy Properties window displays the organizational objects with which this policy is associated. It displays the object name, its description if available and its path. Using the New and Delete buttons you can add objects to, and delete them from, the list of associated objects. Instructions for selecting objects for association, appear in *Selecting an Object for Association*.

Selecting an Object for Association

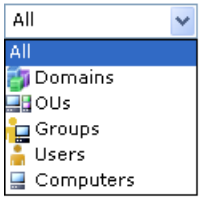
1. In the lower section of the Policy Properties tab, Associate Policy with Organizational Objects, click New. The Select Object window is displayed.



The Select Object window displays the Search by Name and Organizational Tree tabs in the left pane, and the Objects table on the right side. The tabs assist you in

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

selecting the required objects with which the policy should be associated. The tabs also contain a drop-down menu (the Object Type menu) that enables you to determine which object types should be displayed in the table.



2. The Objects table displays the results of your selection. From the displayed objects select objects to associate.

3.5.3.2 Filtering and Associating Objects

The left pane of the Select Object window includes two tabs to help you determine the organizational objects that will be displayed in the window and from which you will select the objects with which you want to associate the policy. These are the Search by Name tab and the Organizational Tree tab.

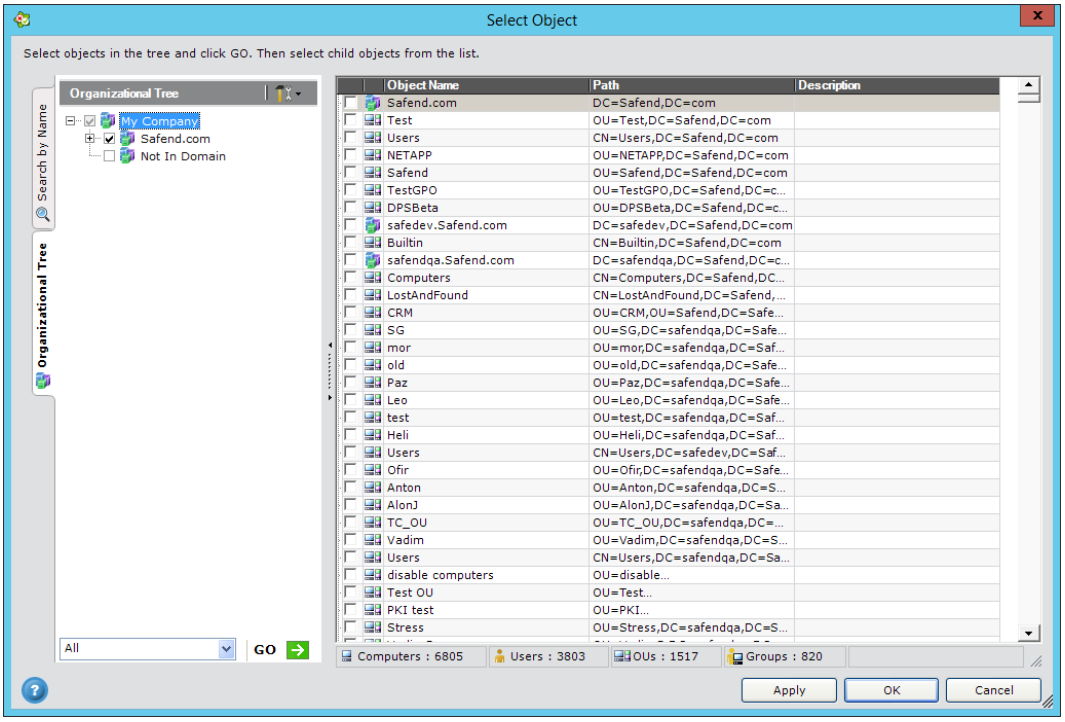
Note: If the Domain Partitioning feature is enabled, then only the organizational units assigned to this user's role are displayed.

Filtering Objects by Name

The Search by Name tab is a tool that you can use to determine the organizational objects (organizational units, groups, computers, users, etc.) to display. The search criteria you enter here determine the objects that will be displayed in the Objects table. Once you have selected and displayed those objects, you can then select which of the displayed objects should be associated with the policy.

Here is an example of the Search by Name tab:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Selecting and Associating Objects by Name

Note: The instructions in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the Policy Properties window.

This is where you select objects by their name and from the displayed list select objects for association.

Searching for a specific object

1. In the text box, enter the name of the computer or user you wish to display. You may enter multiple names separated by a comma, semicolon or space.
2. Check the **Exact Match** checkbox if you want to display an object with a name that exactly matches the string you entered in the text box. For computers you must enter the full computer name (including the domain suffix). If **Exact Match** is not selected, the Select Object window will display objects whose name contains the string that you entered.
3. From the Object Type drop-down menu in the lower left side, select the **object types** you wish to display or **All** if you want to display all types.

Note: When querying associated policies, the Object Type menu includes only Computers and Users.

4. Click GO. The window now displays a table of the objects (one or more) whose name matches your search criteria. If no computer or user is found whose name matches your search criteria, the table is empty and says **No Results Found**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

The Objects table contains a list of the objects that meet your filtering criteria. Each line contains the following columns:

a) Checkbox

b) Object Name

c) Path

d) Description.

Associating a policy with an organizational object

Note: Instructions 1-3 in this section also refer to querying associated policies by name. In that case, the result of your selection displays the policies associated with the selected objects in the Policy Properties window.

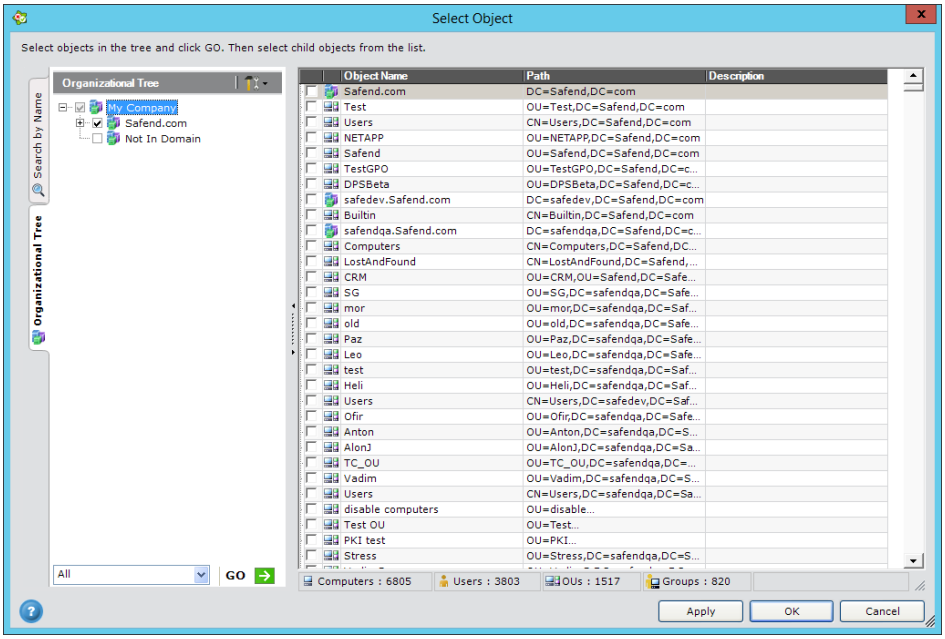
1. In the Objects table, select the objects (one or more) to which you wish to associate the policy, by checking the appropriate checkboxes.
2. To add the objects to the list of associated objects without closing the window, and to continue adding objects through an additional search, click **Apply**.
3. To add the objects to the list of associated objects and close the window, click **OK**. The objects are added to the list and the *Select Object* window closes. You can now view a list of the associated objects in the bottom part of the Policy Properties window.
4. Click **Save** to save the policy. The policy will be updated on Clients the next time Clients refresh their policy.

Filtering Objects using the Organizational Tree

The Organizational Tree is an additional tool you can use to determine which objects to display in the Objects table. Once you have selected and displayed those objects, you can then select which of the displayed objects should be associated with the policy.

The Organizational Tree tab displays the domain(s), organizational units, groups, users and computers in your organization, and the Not In Domain group (which includes all computers who do not currently belong to any domain). Here is an example of the Organizational Tree tab.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Note: The Organizational Tree is applicable only if you are using Active Directory, and if you have set the appropriate Directory definitions in the Administration window (refer to *Configuring General Tab Settings* in Chapter 12, Administration). If you are not using one of these Directory services, only one group is displayed in the Tree: Not In Domain. Selecting this group selects all computers.

Selecting and Associating Objects from the Organizational Tree

The instructions in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the Policy Properties window. This is where you select objects from the Organizational Tree and from the displayed list select objects for association.

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from the Safend Data Protection Suite Management Server, or synchronize it with Active Directory, depending on which Directory you have set Safend Data Protection Suite to use (the Directory may be more up-to-date, but also may take longer). Updating the Tree is done from the Organizational Tree Update menu (shown below) which is found at the top of the Organizational Tree tab.



Updating the organizational tree from the management server

> From the Organizational Tree Update menu, click **Refresh Tree**. The tree is updated.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Updating the organizational tree from the directory

From the Organizational Tree Update menu, click **Sync Tree with Directory**. The tree is updated. This may take several minutes.

1. If necessary, expand the Organizational Tree to view lower-level organizational units.
2. Select the required objects by checking the appropriate checkboxes.
3. From the Object Type menu 

below the Organizational tree, select the object types you wish to display for the selected objects or ***All*** if you want to display all types. This means that if, for example, you select a certain Organizational Unit in the Tree, you can then determine with this menu selection which of its members to display (only computers, only users, etc.).

   Note: When querying associated policies, the Object Type menu includes only Computers and Users.
4. At the bottom of the *Organizational Tree* tab, click 

. The window now displays a table including selected Tree objects and all objects that belong to them.

   The Objects table contains a list of the objects that meet your filtering criteria. Each line contains the following columns:

   e) Checkbox

   f) Object Name

   g) Path

   h) Description.

Associating a policy with an organizational object

Note: Instructions 1-3 in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the Policy Properties window.

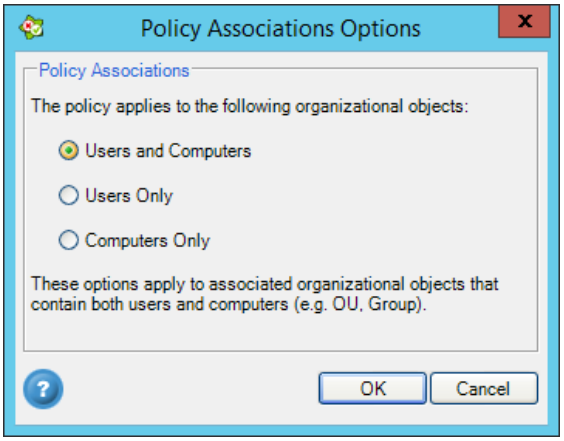
1. In the list of objects, select the objects (one or more) to which you wish to associate the policy by checking the appropriate checkboxes.
2. To add the objects to the list of associated objects without closing the window, and to continue adding objects through an additional search, click **Apply**.
3. To add the objects to the list of associated objects and close the window, click **OK**. The objects are added to the list and the *Select Object* window closes. You can now view a list of the associated objects in the bottom part of the *Policy Properties* window.
4. Optional - restrict the policy association to either computers or users within the selected objects, as described in *Restricting the policy to users/computers*.
5. Save the policy. The policy will be updated on Clients the next time Clients refresh their policy.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3.5.4 Restricting the Policy to Users/Computers

It is possible to associate policies with Groups, OUs and Domains, as well as to specific computers and users. When associating a policy with Groups, OUs and Domains that include both users and computers, you can restrict the association only to computers or users within this object. This is typically useful when creating a default machine policy for the entire organization. In such cases, the policy is associated with the entire domain and is restricted to be applied only to computers.

1. In the Policy Properties window, click the change link next to this policy can be applied to both users and computers (default)**.** The Policy Associations Options dialog box is displayed.



2. Select the relevant option and click **OK**. The text now indicates this restriction. For example, it may read: *This policy applies only to users*.

3.5.5 Disassociating a Policy from Organizational Objects

At times you may wish to disassociate a policy from an organizational object so that it no longer applies to this object.

Note: If the object from which a policy is disassociated needs to be protected, make sure a different policy is applied to it.

1. In the *Policy Properties* window, in the list of objects that appears in the *Associate Policy with Organizational Objects* section (bottom half of the window), select the object from which you want to disassociate the policy.
2. Click the **Delete** button or right-click the object and select **Delete** from the right-click menu.
3. In the *Delete Confirmation* window that opens, click **Yes** to confirm deletion. The object is removed from the list of associated organizational objects.
4. Save the policy.

Note: Until you save the policy, it continues to apply to the deleted associated object.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3.6 Policy Merging

When more than one policy is associated with an organizational object, the settings in all the associated policies can be merged to produce the settings that will be enforced on the endpoint. A typical example of using this capability is defining a general policy for a specific department, and another policy for a specific user in that department who requires additional permissions.

Policy merging occurs when there are two contradicting polices and one of them must take priority. The rules for policy merging differ between the different policy modules. The following sections describe how policy merging works in each of these modules.

3.6.1 Port and Device Control Policy Merging

Policy merging works as follows: for each port/device/storage device/file type/WiFi link, the most permissive definition of all merged policies is applied. However, there are a few exceptions to the most permissive apply rule that are specified below.

Here are a few examples:

Example 1:

Merged policies are Policy A and Policy B:

- Policy A permission for removable storage devices is Allow.
- Policy B permission for removable storage devices is Encrypt.
- Policy A and Policy B have different Settings.

If we merge Policy A and Policy B on an endpoint, the Allow permission will apply for removable storage devices, since Allow is more permissive than Encrypt.

Since Policy A and Policy B have different Settings, the Settings are taken from the definitions in Policy A since it is the first alphabetically.

Example 2:

Merged policies are Policy A and Policy B:

- Policy A permission for removable storage devices is Allow.
- Policy B permission for removable storage devices is Read Only.

If we merge Policy A and Policy B on an endpoint, the Allow permission will apply for removable storage devices, since Allow is more permissive than Read Only.

Example 3:

Merged policies are Policy A and Policy B:

- Policy A permission for disk on key Smart Functionality is Allow.
- Policy B permission for removable storage devices is Block.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

If we merge Policy A and Policy B on an endpoint, the Allow permission will apply for disk on key Smart Functionality, since Allow is more permissive than Block.

3.6.1.1 When Unclassified Devices are Allowed

When unclassified devices are defined as Allowed for the Security Action in the Devices tab, policy merging behaves differently with respect to Device Control.

This means that the security actions defined in the Devices tab of the policy are merged so that the most restrictive take effect, while the rest of the policy definitions (such as: Port Control, Storage Control and File Type Control) are still merged so that the most permissive security actions take effect, as described above.

This enables the administrator to gradually restrict the devices in different parts of the organization as Safend Data Protection Suite is assimilated in the organization.

Example:

The following example demonstrates how Devices Control and Storage Devices Control behave when unclassified devices are defined as Allowed in the Devices tab. The merged policies are Policy A and Policy B, as follows:

- In Policy A, Device Control specifies that printing devices are allowed.
- In Policy A, Storage Control specifies that removable storage devices are allowed.
- In Policy B, Device Control specifies that printing devices are blocked.
- In Policy B, Storage Control specifies that removable storage devices are blocked.

If we merge Policy A and Policy B for a specific endpoint, then printing devices will be blocked because the most restrictive Device Control security actions takes effect, and block is more restrictive than allow.

Removable storage devices will be allowed because the most permissive Storage Control security actions takes effect, and allow is more permissive than block (since the security actions of removable storage devices are a Storage Control definition and not a Device Control definition, they are still merged in the standard, most permissive manner).

3.6.1.2 When Other File Types are Allowed

When Other File Types are defined as Allowed in the File Control tab of the policy, policy merging behaves differently with regard to file control.

In this case, the most restrictive File Type Control definitions of all merged policies are enforced. This means that the Security Actions defined in the File Control tab of the policy are merged so that the most restrictive take effect, while the remainder of the policy definitions (such as: Ports, WiFi, Devices, Storage Devices Control) are still merged so that the most permissive security actions take effect, as described above.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Example 1:

> Policy A and Policy B are two merged policies.

> Policy A specifies that the permission for writing File Type Other is Blocked and that for writing File Type Published Documents is Blocked.

> Policy B specifies that the permission for writing File Type Other is Blocked and that for writing File Type Published Documents is Allowed.

If Policy A and Policy B are merged on an endpoint, then the Allowed permission for Published Documents will apply, since File Type Other is set to Blocked so that the most permissive definition for file groups applies, including Published Documents.

Example 2:

> Policy A and Policy B are two merged policies.

> Policy A specifies that the permission for writing File Type Other is Allowed and that for writing File Type Web Pages is Blocked.

> Policy B specifies that the permission for writing File Type Other is Allowed and that for writing File Type Web Pages is Allowed.

If Policy A and Policy B are merged on an endpoint, then the Blocked permission for Web Pages will apply, since File Type Other is set to Allowed so that the most restrictive definition for file groups applies, including Web Pages.

3.6.2 Data Control Security Policy Merging

Safend Data Control policies include several mechanisms to handle potential policy conflicts. Apart from potential policy setting conflicts, data classification associated with each policy can affect the merge result.

3.6.2.1 Unconfigured Settings

First, the administrator can set the security action and monitoring action of any of the protected channels to Not Configured. When applied alone, a Not Configured security action will be handled as an Allow policy, while a Not Configured monitoring action will be handled as No Record. When enforcing several data control policies simultaneously on the same machine/user, the settings will derive from the policy in which these settings are configured.

In other words, the Not Configured setting reduces the cases in which policies conflict, since they are ignored in the case of a conflict.

Example:

> Policy A has an email setting of Not Configured for Security Action and Log for Monitor Action.

> Policy B has an email setting of Block for Security Action and Log for Monitor Action.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

If we merge policy A and policy B on an endpoint, the applied email channel security action will be Block.

3.6.2.2 Data Labeling

When using data labeling for policies with different data classifications, the hierarchy is the following:

Data Label Settings

In the case when several different data classifications are matched, then the most "restrictive" approach will take precedence. This means that Label overrides Not Configured so the email will contain data labels, if at least one of the policies is set to Label.

Data Label Values

When merging 2 or more policies with different data classifications (different data names and data sensitivity), label values will be summed up so that the merged policy will contain data names from all data classifications (without re-occurrences) and the data sensitivity with the higher level.

3.6.2.3 Incident Matching Several Classifications

When a single data transfer action matches two different classifications, which are associated with contradicting data security policies, the more restrictive setting of each data channel from both policies will be applied. The restriction levels are as follows (the top is most restrictive):

Security Action	Monitoring Action	Monitoring Level
*Classify	Alert	Shadow & Incident
Block	Log	Text & Incident
Encrypt (ex. storage)	No Record	Incident
Ask User	Not configured	Not Configured
Allow		
Not Configured		

*The Classify security action overrides all other security actions to force selected end users to manually classify data.

Example:

> Policy A has an email setting of ask user for Security Action, Log for Monitor Action and Shadow & Incident Monitoring Level, and is associated with a credit card data classification.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

> Policy B has an email setting of Block for Security Action, Alert for Monitor Action and Incident for Monitoring Level, and is associated with a social security number data classification.

When an end user sends an email with attachment files that contain credit card data and social security numbers, the Block security action, Alert Monitoring Action and Shadow & Incident Monitoring Level will occur.

3.6.2.4 Policy Distance

In the case when a single data transfer action matches the same data classification which is associated with two or more contradicting data security policies, (meaning, in both policies the same channel is configured with different settings), the more specific policy applies. This means the policy that is applied to the user/machine in the most direct way will take priority over the more general policy. The following table describes the priority each object has over the other (the top has the highest priority):

Organizational Level Priority

> User/Machine:
  - Group
  - Child OU
  - Father OU
  - Domain

Example:

> Policy A has a web channel setting of Ask User for Security Action and is associated with credit card data classification on a group of customer service employees.

> Policy B has a web channel setting of Block for Security Action and is also associated with a credit card data classification on a specific end user. When the specific end user tries to post credit card data on the web he will be blocked, since Policy B is more specific than policy A and thus gets higher priority.

3.6.2.5 Policy Order

The Policy Order list is used to determine which policy settings will take effect in cases where conflicting policies, with similar data classifications, are applied to the same level in the organizational structure.

3.6.3 Discovery Policy Merging

It is recommended that only one Discovery policy is set at a time. But, if more than one policy is set, the more specific policy applies, as in Data Control Security Policy merging. In case two Discovery policies with similar data classifications are applied on the same level in the organizational structure, then the policy that has been recently created applies.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3.6.4 Hard Disk Encryption Policy Merging

If there is more than one policy and they conflict, decrypt takes priority over encrypt.

3.6.5 Settings Policies

In case there is a conflict between two or more settings policies, the more specific policy applies. If policies are applied on the same organizational object level, than the policy that has been most recently created applies.

Example:

> Policy A has the log transfer interval set to sending logs every 90 minutes and is applied on the entire domain organizational object.

> Policy B has the log transfer interval set to sending logs immediately and is applied on a group of marketing managers.

The policy merge for a marketing manager will ensure that logs from this laptop are sent immediately to the Management Server.

Note: It is recommended to use Global Policy Settings rather than specific Settings policies whenever possible, to limit the number of conflicts that may occur when using multiple specific Settings policies.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

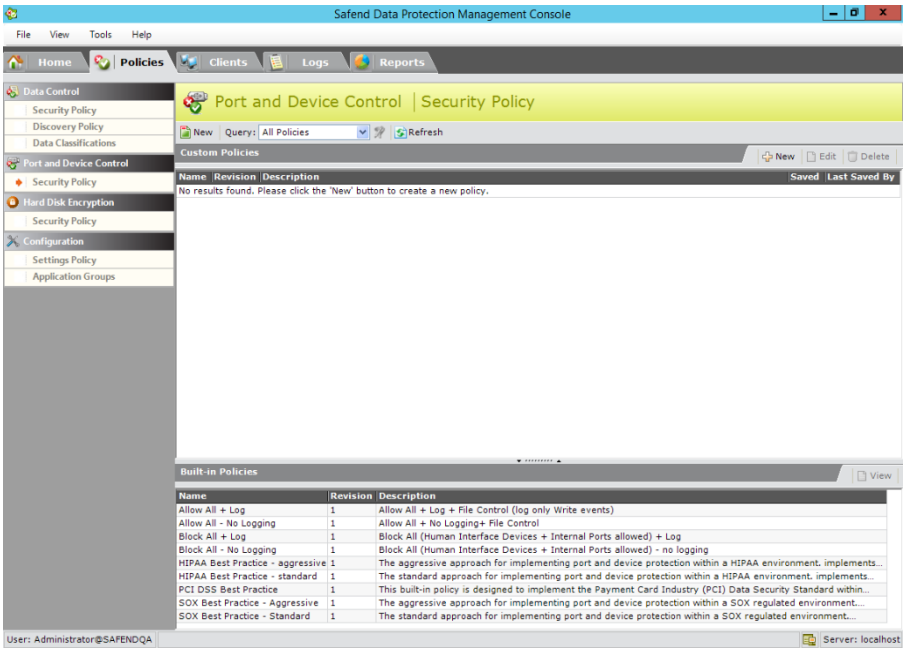
4 Data Control

Data policies control the data that exists in your organization, and maps sensitive data stored on organizational endpoints. Data Classification is the underlying set of definitions which are used by your system to automatically identify data, in order to be able to enforce the appropriate security action or monitoring level for the security incident.

Security Policies define how the Safend Data Protection Suite will respond when classified data is transferred through controlled channels. These policies provide an additional protection layer for data transferred over approved data transfer channels, such as a white-listed storage device, an approved WiFi connection, or even a machine's LAN connection. Security Policies enforce an accurate, data-centric security policy on data transferred via these endpoint channels, without disrupting normal business activity or end user productivity. Discovery Policies enable you to locate sensitive data stored on your organizational endpoints. Identifying where sensitive data is located in your organization is the foundation of any effective data protection policy.

4.1 Quick Tour of the Data Control Policy Window

Click the **Policies tab**. The *Port and Device Control* window is displayed:



Data control consists of three separate windows: Security Policy, Discovery Policy and Data Classification. The following describes the three windows in general, indicating where they differ.

4.1.1.1 Workspace

Each Data Control window contains a list of the different classifications/policies defined in the system. It is divided into two sections: the upper section is Custom Classification/Policies and the lower section is Built-in Classification/Policies.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- Custom Classifications/Policies are classifications/policies created by the user and may contain either built in or custom classification rules.
- Built-in Classifications/Policies are classifications/policies that are delivered with the system that can be used "as is". Each built-in classification contains built in classification rules. Built in classifications/ policies can also be used as a template for custom ones.

In this window you are able to add, edit and delete custom classifications/policies, and view details of both built in and custom classifications/policies.

4.1.1.2 MENUS

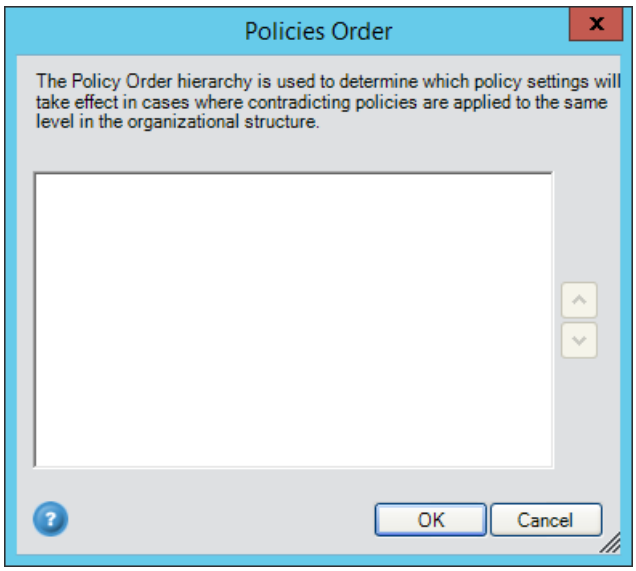
Button	Description
File	
Import Policy	This enables you to import an exported policy. It opens Choose File to Import to enable you to select a file.
Import Classification	This enables you to import an exported classification. It opens Choose File to Import to enable you to select a file.
Right-click	
Delete	This removes the Classification/Policy from the Custom Classification/Policy list.
Export	This enables you to export the Classification/Policy. It opens Save Export Result As.
Edit	This enables you to edit the Classification/Policy.
Duplicate	This enables you to duplicate the policy.
New	This enables you to create a new Classification/Policy.
View	This enables you to view the details of the Classification/Policy.
Customize	This enables you to customize the Classification/Policy according to your requirements.
Toolbar	
	This enables you to create a new classification/policy.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Button	Description
Policies Order	This opens the Policy Order window which enables you to change the hierarchy order of the policies. This is used to determine which policy settings will take effect in cases where contradicting policies are applied to the same level in the organizational structure. This option is available only in the Security Policy window.
Refresh	This refreshes the display.

Changing policy order

1. Click Policies Order in the toolbar. The Policies Order dialog box will be displayed.



2. Select one of the policies in the list.
3. Use the ^/v buttons on the right to re-order the policies according to the order you desire.

Button	Description
New	This enables you to create a new classification/policy.
Edit	This enables you to edit a classification/policy after selecting it.
Delete	This enables you to delete a classification/policy after selecting it.
View	This enables you to view a built-in classification/policy.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.2 About Data Classification

Data classification is a set of definitions which is used by the system to automatically identify data, in order to be able to enforce the appropriate security action and/or monitoring level of security incidents. Data classification consists of one or more classification rules and the Boolean relations between them (and, or, not).

These classifications are used by the Security and Discovery Policies.

4.2.1 End-user Based Data Classification

Often organizations struggle to define classification rules for sensitive information when using data discovery and content experts. The Safend Data Protection Suite takes an end-user driven approach to fine-tune data classification, by mandating designated users to manually classify data.

The IT/security administrator selects certain “key users” who act as content experts and asks them to start classifying the data they use as part of their everyday work. Every time they send files\data they are prompted to classify it according to a pre-defined data classification list. In this way the IT dept. can learn which data classifications need to be associated with the user’s group or department.

The main goal is to provide feedback to the IT\security dept. in order to ease the process of building accurate data classifications and maintaining them. This will enable your organization to achieve performance optimization, while at the same time increasing data leakage awareness.

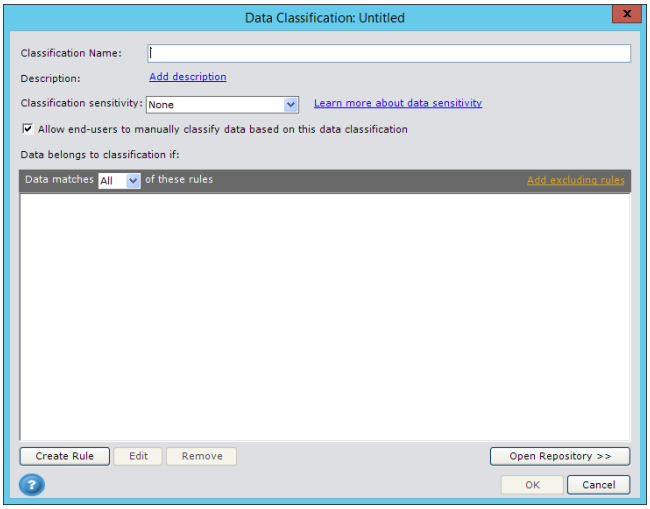
4.3 Creating a New Data Classification

Here is a description of how to create a new data classification. Multiple data classification techniques can be used.

1. Click 

above Custom Classification in the *Data Classification* window. The *Data Classification* window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



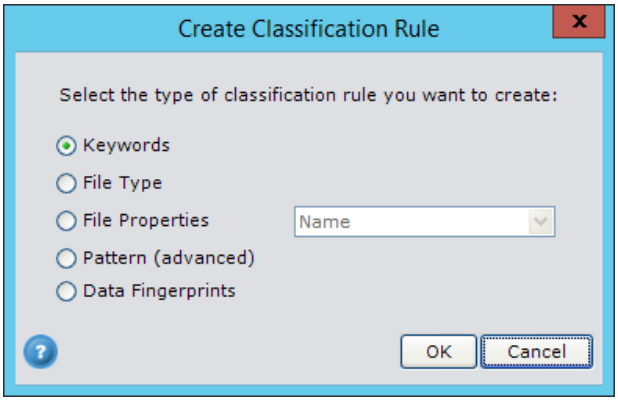
2. In the *Classification Name* field enter the name of the new classification.
3. Click Add description if you want to write a short description about the new classification.
4. Choose a Sensitivity Level from the drop-down list or leave it as None. For more information, see About Data Sensitivity
5. Choose whether to Allow end-users to manually classify data based on this data classification. For more information, see End-user Based Data Classification.
6. You can add a classification rule by clicking Open Repository >> and choosing a Built-in or Custom rule, or by clicking Create Rule.

Note: If you choose to allow end-users to manually classify data, it is recommended not to have more than 5 manual data classifications from which to choose, this is to simplify the end user manual data classification process.
The descriptions for the end-user based classifications should be short and clear. The user asked to manually classify data according to this data classification, can see a description of the classification by placing the mouse over the classification name (under Select Classifications) in the Email Classification message.

4.4 Creating Classification Rules

1. Click Create Rule in the *Data Classification* dialog box. The *Create Classification Rule* dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. Select the type of classification rule you want to create and click **OK**. For each type of classification rule a different window will open.

Each type of classification rule is configured differently, which is described in the following sections.

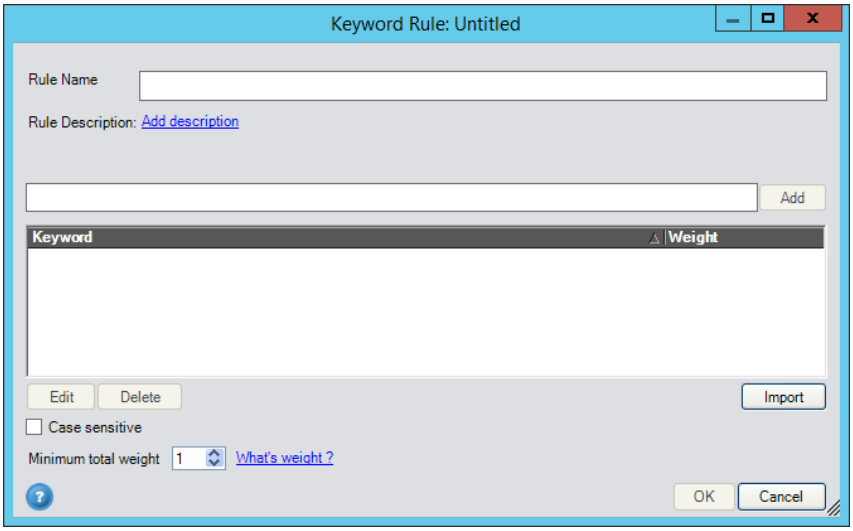
4.4.1 Types of Classification Rules

Rule Type	Description
Keywords	Keyword lists are used to identify data transfer incidents which contain specific keywords or keyword sequences. A "weight" mechanism facilitates the identification of logical content, by using dictionaries with different importance levels assigned to different phrases. See *Setting a Keyword Rule* for more information.
File type	Individual file types are recognized according to a full analysis of the file format. See *Setting a File Type Rule* for more information.
File Properties	Multiple meta-data parameters can be used to identify sensitive content, including full or partial file name, file size and more. See *Setting a File Properties (Name) Rule* for more information.
Pattern (advanced)	Textual pattern recognition is used to identify incidents which contain a pre-defined textual pattern, such as an email address, phone number, serial number or credit card number. See *Setting a Pattern (Advanced) Rule* for more information.
Data Fingerprints	Data fingerprinting is used to identify known content when it transferred off the endpoint, even if the data has been partially modified. See *Setting a Data Fingerprints Rule* for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.4.2 Setting a Keyword Rule

1. Select *Keywords* and click **OK** (alternatively, click **Edit** in the Data Classification dialog box for an existing keyword rule). The Keyword Rule window is displayed.



2. In the Rule Name field give the rule a name. If not, the rule name is automatically set to the first keyword from the list.
3. Click the Add description link beside Rule Description. A small window is opened where you can insert the rule description. After a description is entered, you can change it using the Edit link below the description.
4. Add a new keyword by entering the word or word sequence in the textbox above the Keyword list and clicking **Add** or pressing **ENTER**. The keyword will now be displayed in the Keyword list.
5. Check **Case sensitive** if you want to define the keywords in the dictionary as case sensitive.
6. Select the **Minimum total weight** from the drop-down list**.** This number defines the minimal total weight of the keywords found in the data, in order for it to match the classification rule. By default it is set to 1. You can adjust it in order to define that several different keywords should be included in the data for it to match the rule. The maximum number the user can enter is the total weight of all the keywords defined in the rule. This prevents the user from defining a rule which can never be matched.

Option	Description
Edit	This button enables you to edit an existing keyword.
Remove	This button enables you to delete keywords from the list.
Import	This button enables you to select a CSV file with words and weights. In the input file each keyword will be in a new line, and will be divided by a comma from its weight. For example, when importing the file:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

"Top, 1
Secret, 1
Confidential, 2
Top secret, 2".
The rule created will include 4 keywords: the first two each assigned with a weight of 1 and the last two each assigned with a weight of 2.

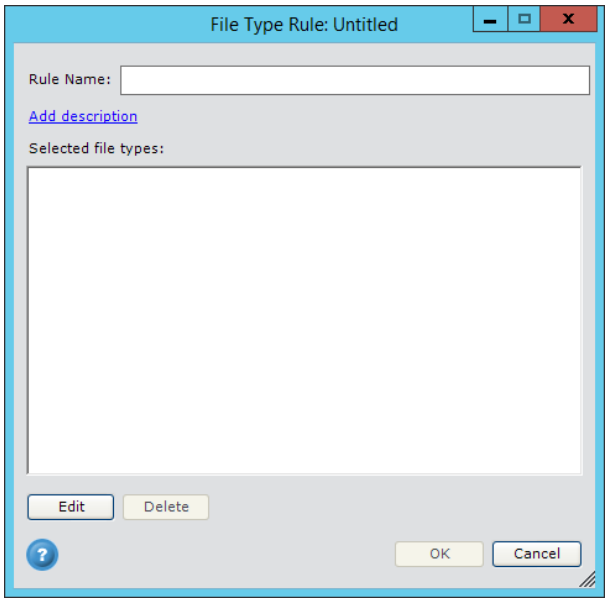
4.4.3 About Total Minimum Weight

This number defines the minimal total weight of the keywords found in the data in order for it to match the classification rule. By default it is set to 1. The user can adjust it in order to define that several keywords should be included in the data for it to match the rule. The maximum number the user can enter is the total weight of all keyword defined in the rule. This prevents the user from defining a rule which can never be matched.

4.4.4 Setting a File Type Rule

Individual file types are recognized according to a full analysis of the file format.

1. Select **File Type** in the *Create Classification Rule* dialog box and click **OK**. The *File Types Rule* dialog box is displayed.



2. Enter a name in the Rule Name field.
3. Click Add description to add a description of the rule, if you want.
4. Click the **Edit** button to select a File Type.
5. Choose a file type in the Select File Type dialog box and click **Apply**.
6. A new file type is added to the Selected file types list.
7. To remove a file type from the list, select it and click **Delete**.

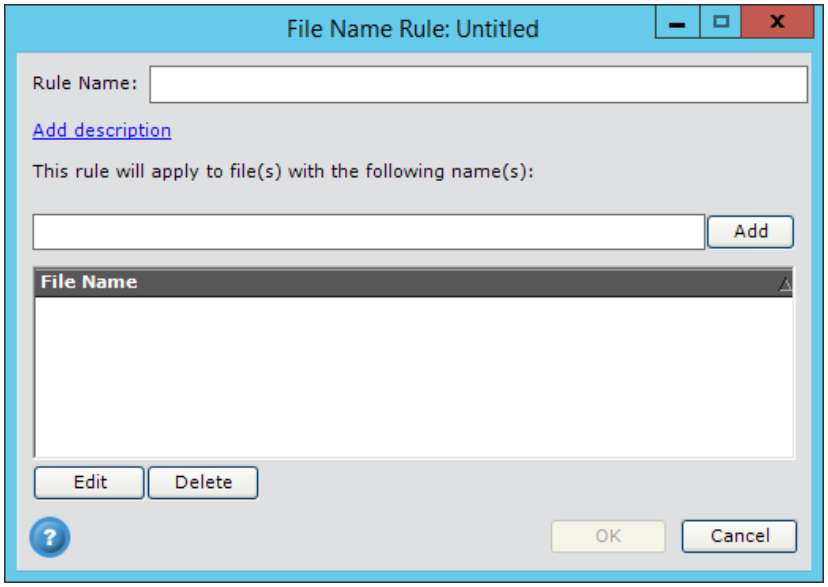
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

8. Click **OK** to save your changes and return to the Data Classification dialog box.

4.4.5 Setting a File Properties (Name) Rule

Multiple meta-data parameters can be used to identify sensitive content, including full or partial file name, file size, and more.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Name** from the drop-down list.
3. Click **OK** and the File Name Rule dialog box is displayed.



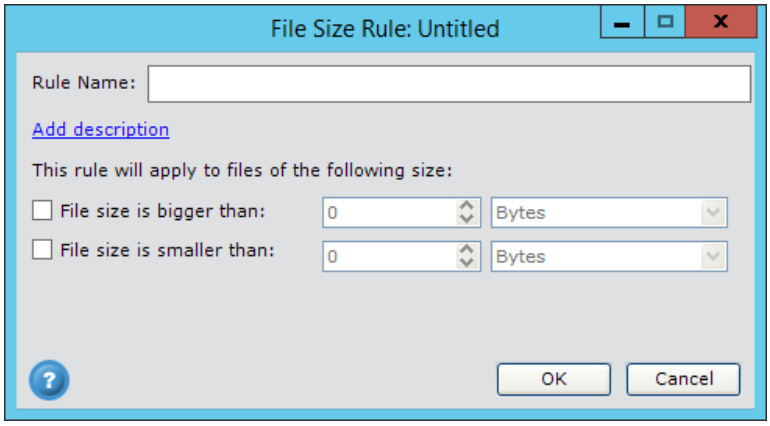
4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following name(s) field.
7. Click **Add** and the new name will be displayed in the File Name list.
8. Select a file name from the *File Name* list and click **Edit** to change it or **Delete** to remove it from the list.

4.4.6 Setting a File Properties (Size) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file size.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Size** from the drop-down list.
3. Click **OK** and the File Size Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

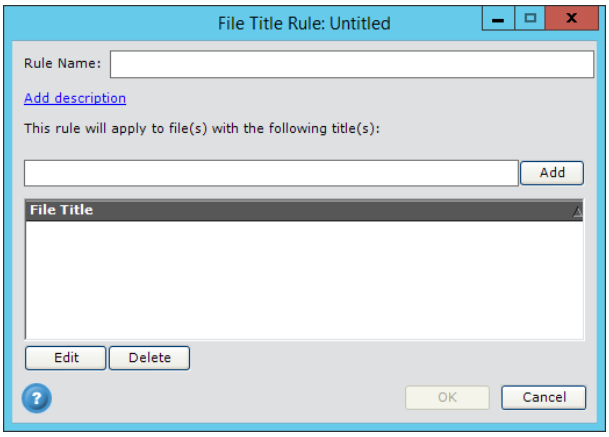


4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Select either **File size is bigger than** or **File size is smaller than**. Choose the value and the unit from the relevant drop-down lists.
7. Click **OK** to return to the Data Classification dialog box.

4.4.7 Setting a File Properties (Title) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file title.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Title** from the drop-down list.
3. Click **OK** and the File Title Rule dialog box is displayed.



4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following title(s) field.
7. Click Add and the new name will be displayed in the File Title list.
8. Select a file name from the File Title list and click Edit to change it or **Delete** to remove it from the list.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.4.8 Setting a File Properties (Subject) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file subject.

1. Select File Properties in the Create Classification Rule dialog box.
2. Choose Subject from the drop-down list.
3. Click OK and the File Subject Rule dialog box is displayed.



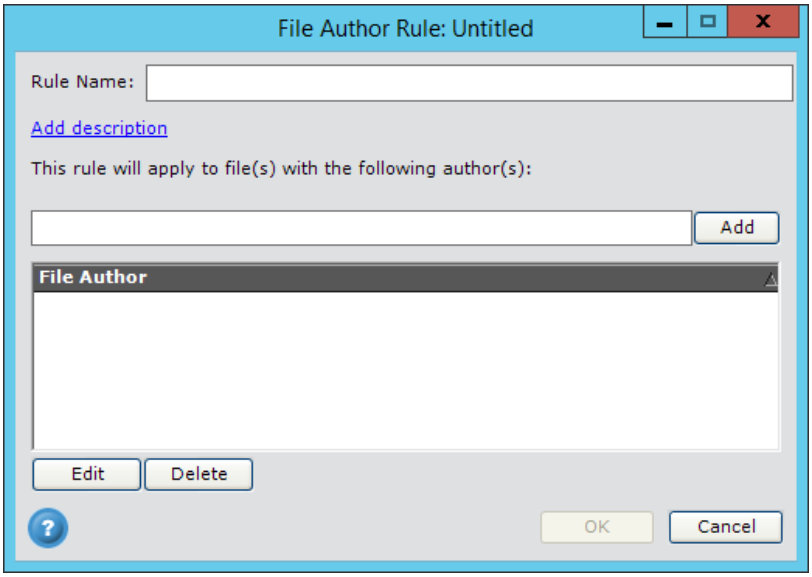
4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following subject(s) field.
7. Click Add and the new name will be displayed in the File Subject list.
8. Select a file name from the File Subject list and click Edit to change it or Delete to remove it from the list.

4.4.9 Setting a File Properties (Author) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file author.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Author** from the drop-down list.
3. Click **OK** and the File Author Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following author(s) field.
7. Click **Add** and the new name will be displayed in the File Author list.
8. Select a file name from the File Author list and click **Edit** to change it or **Delete** to remove it from the list.

4.4.10 Setting a File Properties (Company) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file company name.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Company** from the drop-down list.
3. Click **OK** and the File Company Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



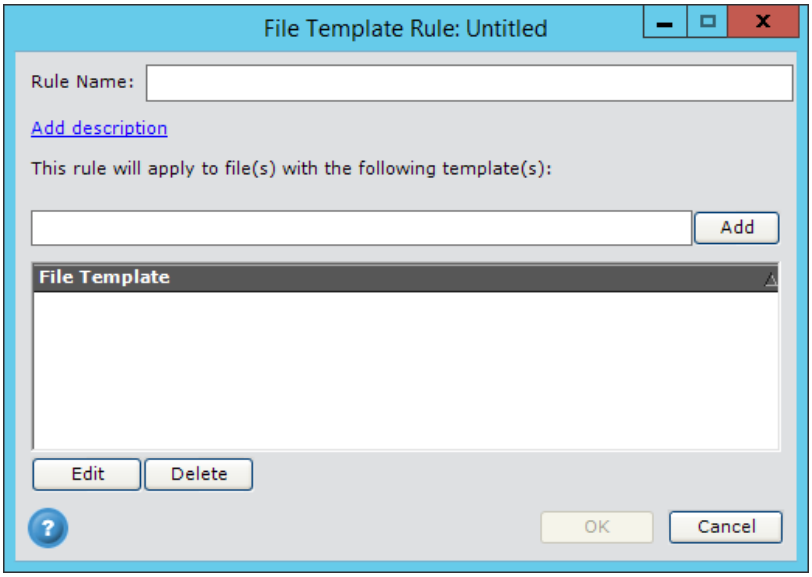
4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following company name(s) field.
7. Click **Add** and the new name will be displayed in the File Company list.
8. Select a file name from the File Company list and click **Edit** to change it or **Delete** to remove it from the list.

4.4.11 Setting a File Properties (Template) Rule

Multiple meta-data parameters can be used to identify sensitive content, including the file template.

1. Select File Properties in the Create Classification Rule dialog box.
2. Choose **Template** from the drop-down list.
3. Click **OK** and the File Template Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



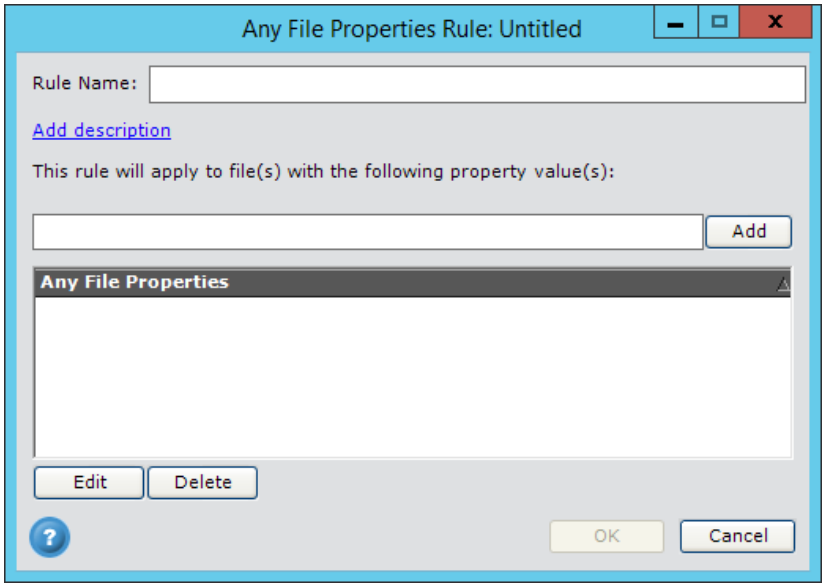
4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following template(s) field.
7. Click Add and the new name will be displayed in the File Template list.
8. Select a file name from the File Template list and click Edit to change it or Delete to remove it from the list.

4.4.12 Setting a File Properties (Any) Rule

This rule enables the Safend administrator to define an additional file property classification that will be matched against "any" file property within a file, including custom properties the file contains. This rule can contain file property values similar to a 3rd party tagging solution: for example the file is given a “Classified” tag. The Safend agent will be able to match files in which their metadata contains these exact pre-defined values and block\allow transfer operations according to the policy security action.

1. Select **File Properties** in the Create Classification Rule dialog box.
2. Choose **Any** from the drop-down list.
3. Click **OK** and the Any File Properties Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



4. Enter a name in the Rule Name field.
5. Click Add description to add a description of the rule, if you want.
6. Enter a File name in the This rule will apply to file(s) with the following property value(s) field.
7. Click **Add** and the new name will be displayed in the Any File Properties list.
8. Select a file name from the Any File Properties list and click **Edit** to change it or **Delete** to remove it from the list.

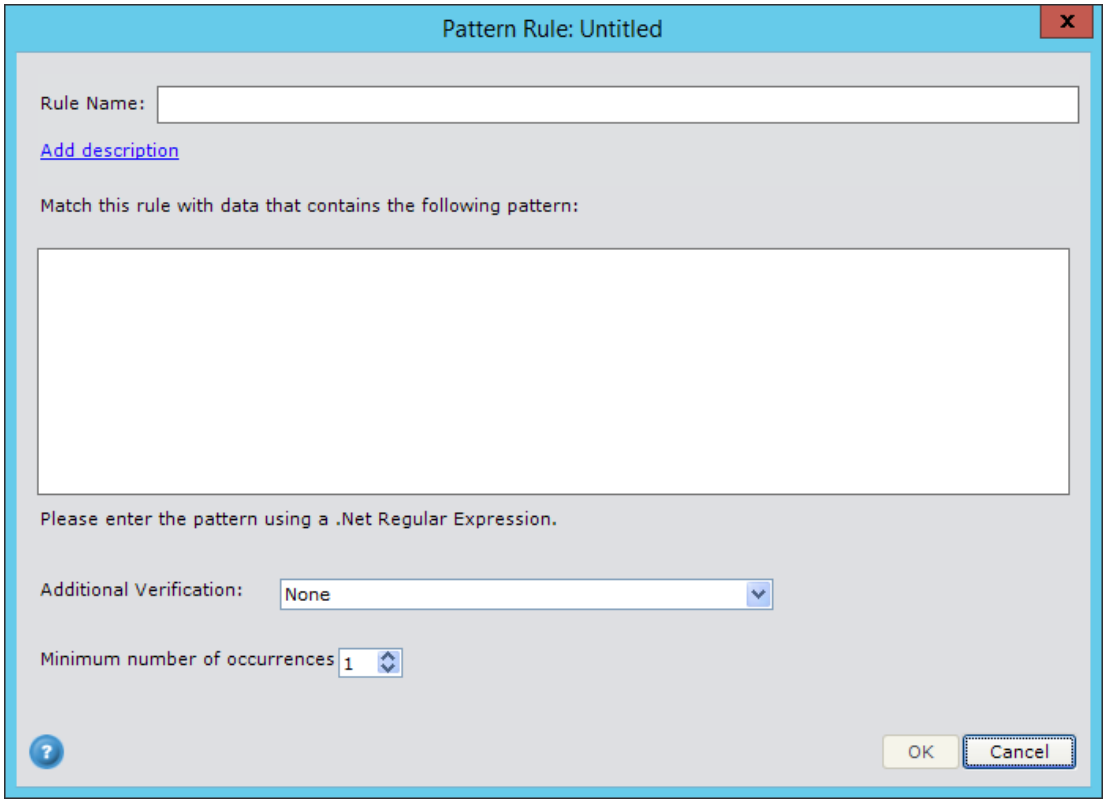
4.4.13 Setting a Pattern (Advanced) Rule

Textual pattern recognition is used to identify incidents which contain a pre-defined textual pattern, such as an email address, phone number, serial number or credit card number.

Note: Before creating a custom pattern rule, it is recommended that you check the rule repository to see if an appropriate rule already exists in the system.

1. Select **Pattern (Advanced)** in the Create Classification Rule dialog box and click **OK**. The Pattern Rule dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. Enter a name in the Rule Name field.
3. Click Add description to add a description of the rule, if you want.
4. In the Match this rule with data that contains the following pattern field, add the textual pattern of interest using a .net Regular Expression.
5. Select an additional mathematical verification method in the Additional Verification field, if it is relevant (for example a credit card or ID number). If no mathematical verification of the detected pattern is required, select **None**.
6. Choose the Minimum number of occurrences value from the drop-down list to define how many times the pattern must be included in the incidents, in order for the classification rule to match.
7. Click **OK** to return to the *Data Classification* dialog box.

4.4.14 Setting a Data Fingerprints Rule

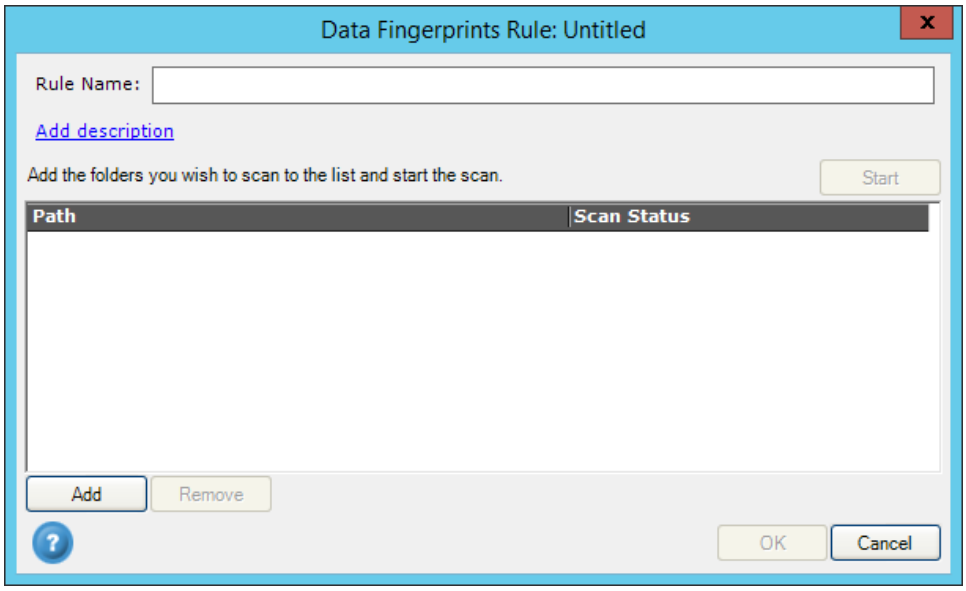
Note: In order for data fingerprinting to work a file must contain at least three sentences, each containing at least 3 words (excluding words such as, a, the, in, at, by, to, about, and, or, etc.). Also the text must be in a text file format, for example .txt, Word document format (.doc\.docx) and other texts formats (not including, .xls or .ppt).

Data fingerprinting is used to identify known content when it transferred off, or stored on the endpoint, even if the data has been partially modified. The data fingerprinting process is designed to identify partial copies of textual documents, such as Word files, PDF documents etc.

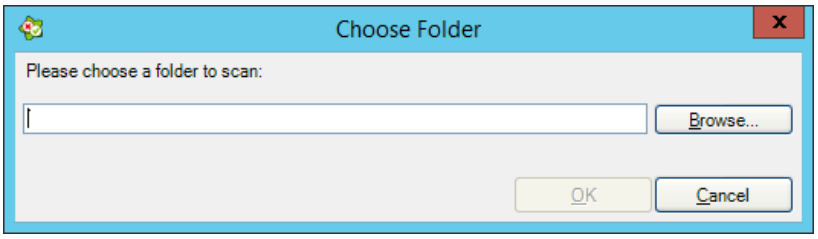
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Data on the endpoint will match such a classification rule, if it contains a large enough portion of the original fingerprinted documents.

1. Select **Data Fingerprints** in the *Create Classification Rule* dialog box and click **OK**. The Data Fingerprints Rule dialog box is displayed.



2. Enter a name in the Rule Name field.
3. Click Add description to add a description of the rule, if you want.
4. Add the folders to the list you want to scan, by clicking **Add**. The Choose Folder to Scan dialog box is displayed.



5. In *Path to folder*, enter or Browse... to a folder path.
6. After selecting a folder you can press **Start** and scan the folder.
7. Click **OK** to return to the Data Classification dialog box.
8.

4.4.15 Adding Excluding Rules

Excluding rules are used to identify data which will not match the data classification. This is how you add excluding rules.

1. Click Add excluding rules. The Data belongs to Classification if list is now divided into an upper half (included rules) and lower half (excluding rules).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

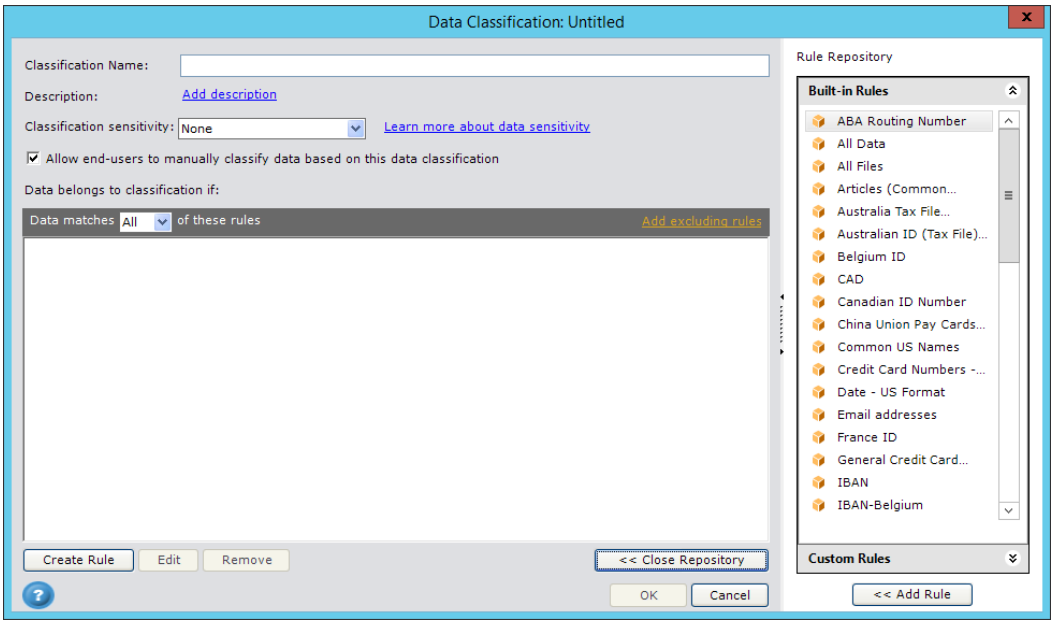
2. Click Create Rule and choose Exclude Rule (not Include Rule).

3. Create an Exclude Rule as described for the various types of classification rules. The excluding rules can be inactivated by clicking Remove excluding rules.

4.4.16 Adding Rules from the Rules Repository

Rules can be added from the Rules Repository. The Rules Repository consists of Built-in Rules and Custom Rules. They can be added to both the included rules and excluded rules list.

1. Click Open Repository >> at the bottom of the Classification window. The Rules Repository is displayed on the right of the Data Classification dialog box.



2. Choose a rule from the Built-in Rule list.

3. Alternatively choose a Custom Rule after clicking ».

4. Click << Add Rule to add a rule to the Data belongs to classification if list. The rule can be added either as an included or excluded rule.

4.4.16.1 Defining Rule Relations

> Choose All for a list of rules that must be matched in order for the classification to apply (the default option).

> Choose Any for a list of rules that at least one of them must be matched for the classification to apply.

> Choose excluding rules for a list of rules that must not be matched in order for the classification to apply. The same All or Any options are available also for the exclusion rules.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.4.17 Editing a Classification Rule

1. Select a rule in the Data belongs to classification if list that you wish to change.
2. Click Edit... . The Rule window will be displayed.
3. Depending on the type of rule, follow the procedures for setting the different types of Classification rules.

4.4.18 Removing a Classification Rule

1. Select a rule in the Data belongs to classification if list that you wish to remove.
2. Click Remove. The rule will be removed from the list.

4.5 About a Data Control Security Policy

A Data Control Security Policy defines how the Safend Data Protection Suite reacts when classified data is transferred through controlled channels. Each data control policy defines how the Safend Data Protection Suite reacts to a specific Data Classification. You can define custom data classifications, or use a built-in classification provided by Safend (see About Data Classification for more information).

A security incident represents a single user data transfer event within a protected channel. The security settings set for each channel influence security incidents which take place in this channel, and the record is set according to the defined record level on the entire incident (and not on any specific parts of it).

The following is a per channel definition for security incidents:

Channel	Security Incident Definition
Email	Single email sent (including email body, meta data and all attachments). See *Email Configuration*.
Web	Single data posting action (example – user clicks "submit", "upload", etc.). This includes all posted data and all web-related meta data. See *Web Configuration*.
External Storage	A single file transferred. If the user transfers more than one file at the same time they are still considered separate incidents. A file which includes other files (such as a compressed folder) is considered one incident. See *External Storage Configuration*.
Cloud Storage	A single file transferred. See Cloud Storage Configuration.
Network/Local Printers	Single printing action (user clicks "print"). See Network Printers Configuration and Local Printers Configuration.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Network Shares	A single file transferred. See Network Shares Configuration.
Portable Virtual Storage	A single file transferred. See Portable Virtual Storage Configuration.
FTP	A single file transferred. See FTP Configuration
Application categories	Application access to the data, either file access or access through copy/paste.

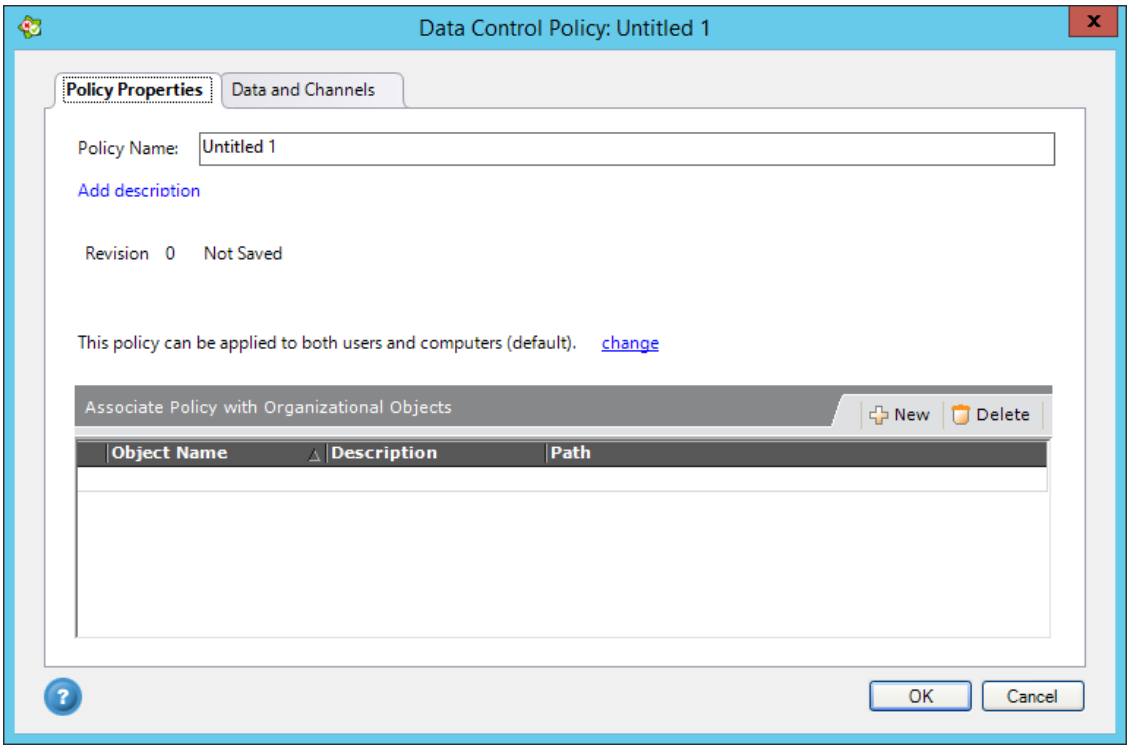
4.5.1 Creating a Data Control Security Policy

1. Click the New button on the right in Custom Policies.
2. The new policy window will be displayed which enables you to create a new Data Control Security Policy.

The following section describes all the features of the new policy window, in order to create a new policy.

4.5.1.1 Policy Properties Tab

In this window, the user can name the policy, change its description and associate it with organizational objects.

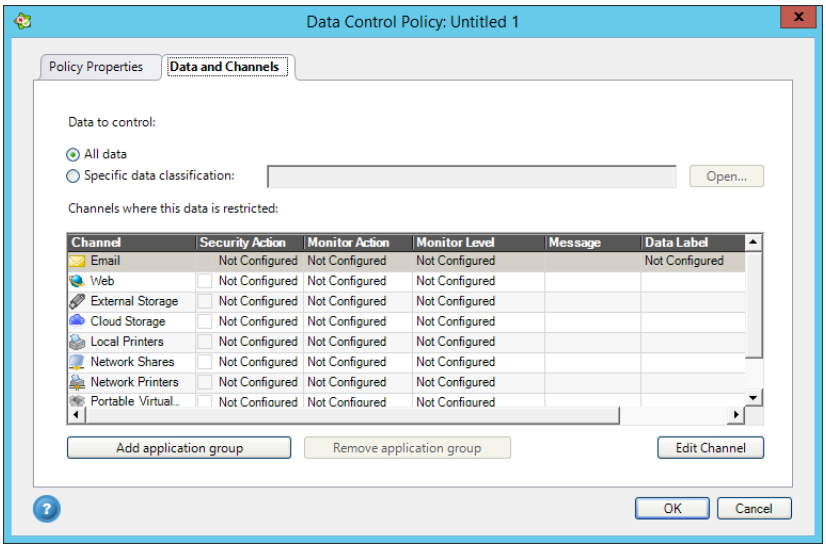


See Associating a Policy with Organizational Objects for a detailed description of this tab.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.5.1.2 Data and Channels Tab

When you click the Data and Channels tab the following window is displayed.

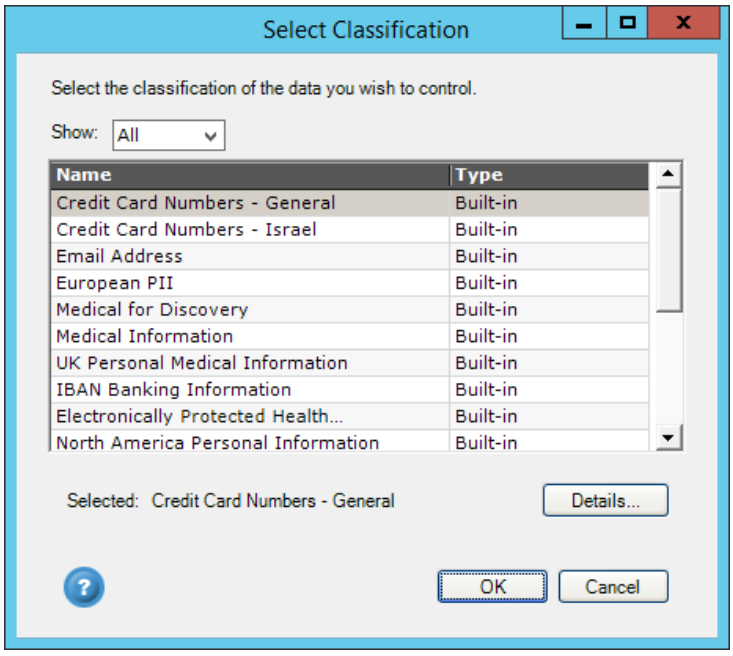


This window is divided into two sections. The first section, Data to Control, allows you to select the classification to which the policy will refer.

The bottom part of the window, Channels Where this Data is Restricted, displays a table showing all the channels which are built-in to the system. All channel settings are displayed as "not configured".

4.5.1.3 Data to Control

You have the option to select either All data or Specific data classification. If you select Specific data classification and click Open, the following window is displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Here you select a Built-in or Custom classification. In Show you can select which classifications will be displayed (All, Built-in, Custom). Click Details to view information about the classification you have chosen. The Data Classification dialog box will be displayed.

Note: It is risky to use “all data” instead of a specific classification, and it is preferable to create a wide classification, looking for most file types rather than using the “all data” option.

Data Restricted Channels

Option	Description
Channel	
Email	This controls outgoing email using Microsoft Outlook or Lotus Notes.
Web	This controls web posts using a plug-in to Windows Internet Explorer.
External Storage	This controls data transfer to external storage devices (DOK, external HD, SD cards, etc.).
Cloud Storage	This controls data uploaded via popular cloud storage client applications: Dropbox, Box.net, Google Drive and Microsoft SkyDrive.
Local Printers	This controls data printed to local printers.
Network Shares	This channel inspects files that are being uploaded to Network Path servers.
Network Printers	This controls printing data using a network printer.
Portable Virtual Storage	This channel inspects files that are being copied to Smart Devices that are not recognized as external storage devices in Windows Explorer but as Smart Devices that have their own file transferring protocol. An example of such devices can be a Nokia Smart Phone, Media Players, etc.
FTP	This channel inspects files that are being uploaded to FTP servers.
Application Data Access Control	This controls pre-defined application access to confidential data, via direct file access or the clipboard. Applications are divided into application groups, and each application group can be added to any policy and controlled as a data transfer channel.
Security Action	
Allow	Allows the action to be performed.

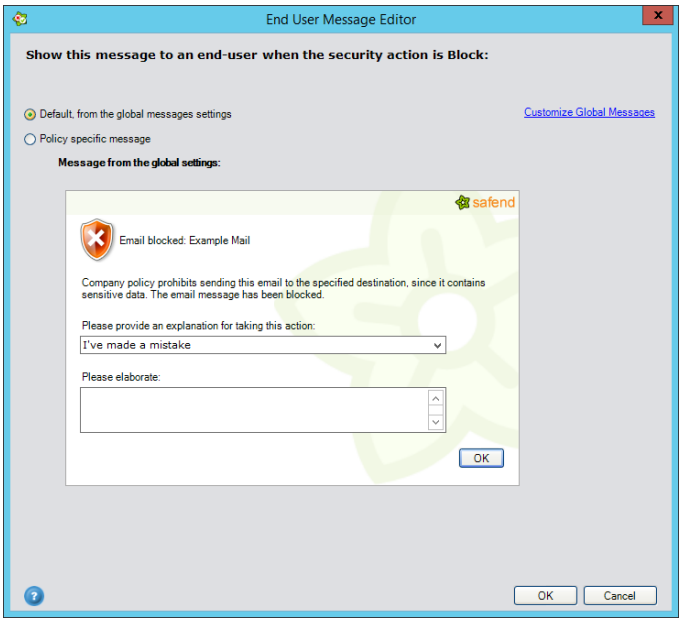
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
Block	Stops the action the user is trying to perform.
Encrypt	In External Storage data channel: Allows the data transfer action, only if the storage device is encrypted.
Ask User	Prompts the user with an "are you sure?" question. Allows the action to be performed only if the user selected "yes". It is an additional indication that sensitive data is involved.
Not Configured	The default option. This means this security policy does not define a security action for the channel. If this is the only action applied for a specific incident the result will be the same as "allow". The difference between the two is when policy merging is required. Refer to *Data Control Security Policy Merging* for more information.
Classify	This enables the end user to classify data for this channel. See End-user Based Data Classification for more information.
	If a plus sign (+) appears in one of the Security Actions (for example ) this means that this data channel has one or more destination groups assigned to it. Therefore, the additional security settings for channels destination groups may override this Security Action. See Destination Groups for more information.
Monitor Action	
Log	Logs the incident according to the monitoring level. Sends the log in the predefined intervals.
Alert	Sends the record immediately as an alert.
No Record	Does not send any information about the incident.
Not Configured	This is the default option. It yields the same result as *No Record*.
Monitor Level	
Incident	Sends only incident details, without the content of the file.
Text & Incident	Sends the textual content of the file and file general information, together with the incident details.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

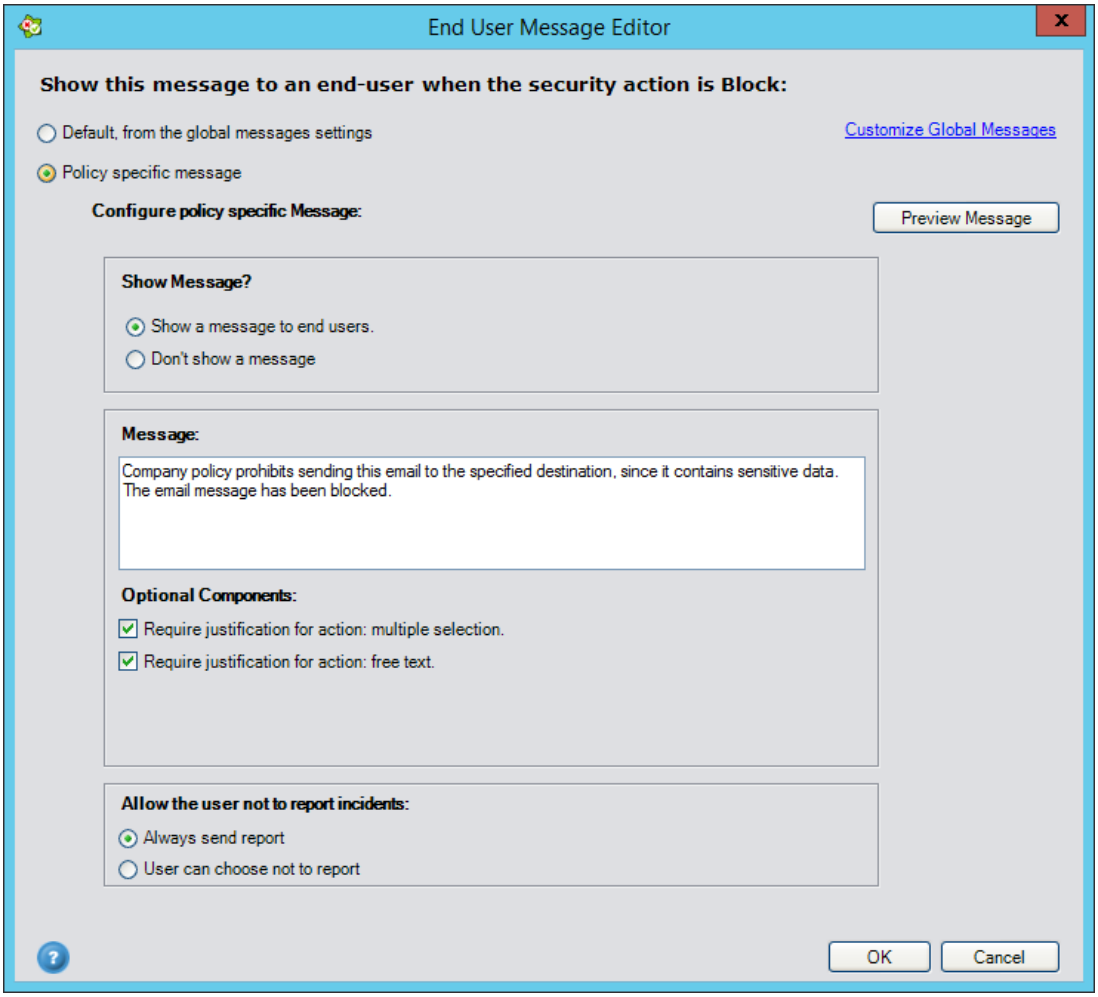
Option	Description
Shadow & Incident	Sends the complete copy of the file (file shadow) to the server, together with incident details.
Message Column	
Global	This option is available when the Security Action chosen is other than Not Configured.

When you click Global in the Message column or double click, here is an example of a default message that will be displayed in the End User Message Editor.



If you select Policy specific message, the following will be displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



See Configuring Agent Messages for further information.

Data Label Column

Here you choose whether to set a data label (Data Label) or not (Not Configured). If you choose Data Label, double click on it and the Email Settings window opens. Here you create a data label after choosing Data Label and clicking Edit Labels. See Email Data Channel Settings and Configuring Data Label Templates for more information about setting a data label.

4.5.2 Channel Configuration

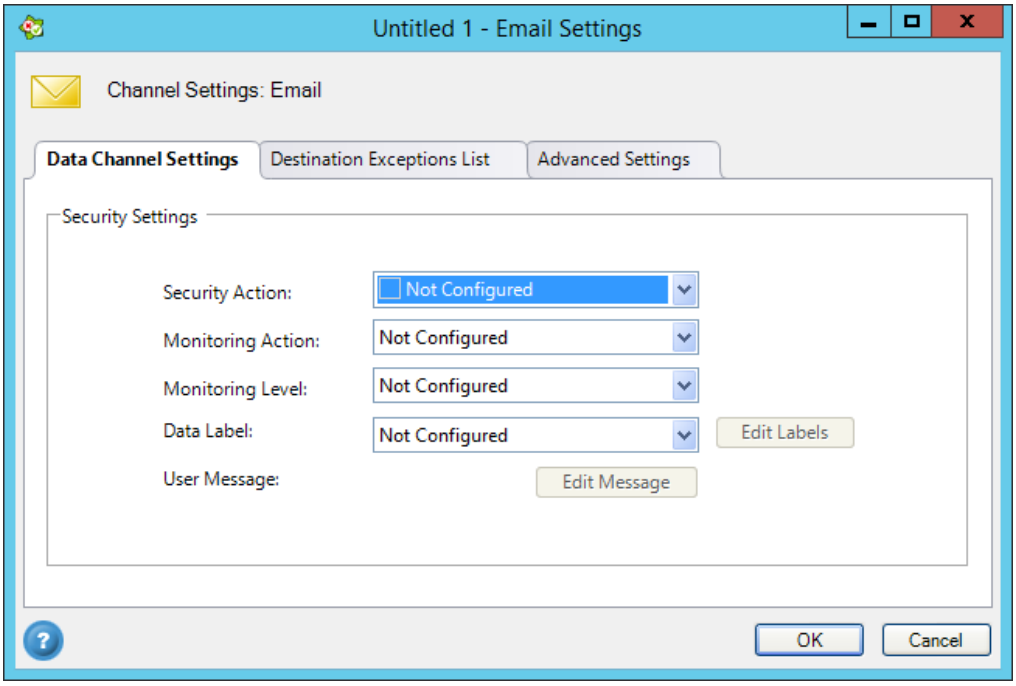
To configure or edit existing channel settings, select the channel of interest and click Edit Channel or double click the selected channel. The appropriate Channel Settings window will be displayed.

The following is a description of how to configure each channel.

4.5.2.1 Email Configuration

When you select Email as the Channel in the Data and Channels tab and click Edit Channel, the Email Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This window consists of 3 tabs. The Data Channel Settings tab displays the current settings and allows you to change these settings. The Destination Exceptions List tab enables you to add, edit or delete Destination Groups. In the Advanced Settings tab are various additional settings.

Email Data Channel Settings

This displays the current Data Channel Settings and allows you to change these settings.

Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *No Record*, *Log* or *Alert*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
Data Label	Choose whether you want to add a Data Label or leave it Not Configured. Click Edit Labels to open the Data Label Templates window. See Configuring Data Label Templates for more information. Data Labels allow you to add labels to email messages based on a classification name or sensitivity. Note: Email data labeling is supported only on Outlook email clients.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Setting	Description
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

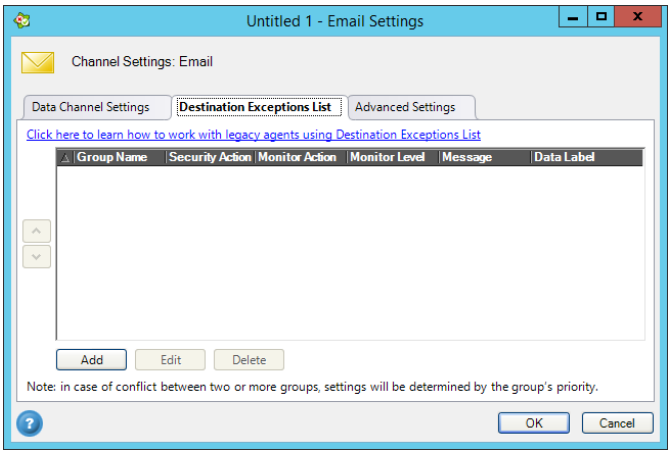
Destination Groups

Destination groups ("Blacklist\Whitelist" groups) allow you to easily define data control policies according to data destinations and economize the number of policies required for different security actions per different destinations. This enables you to fine-tune each channel in a data control policy according to data destinations (email recipient, domain, URL, network path, etc.). The Destination Exceptions list contains Destination groups. Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the Group Name, Security Action, Monitor Action, Monitor Level, Message and Data Label are displayed.

Note: email aliases are not reliable for email blacklist\whitelist entries because Outlook 2013 automatically expands aliases to their final email addresses before DPS interrogates the destination addresses.

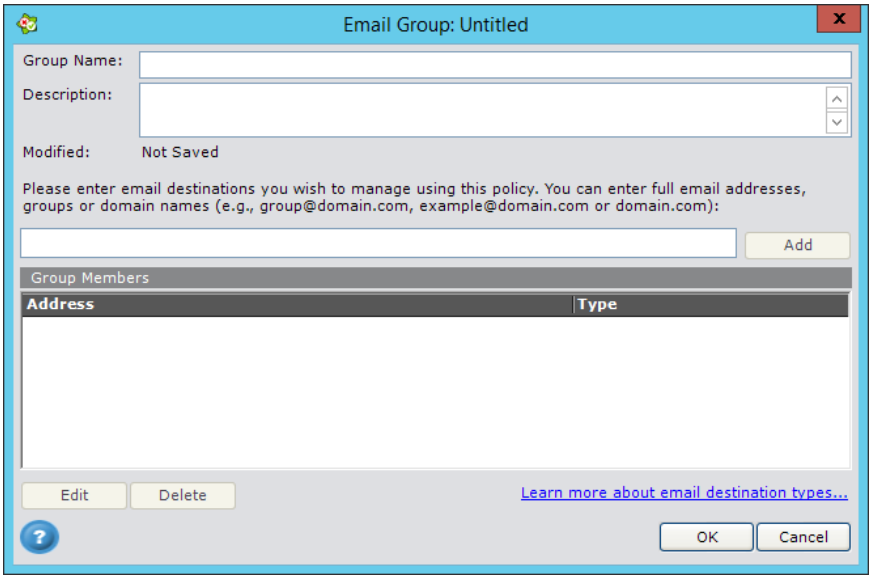
Email Destination Exceptions List

In this tab are listed Destination Groups and you can add groups, edit groups or delete groups from this list.



When you click Add, the Email Group dialog box is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Here you create a new email group.

Adding an email group

1. Enter a Group Name.
2. In the Description field, you can add a description about this new group.
3. In the text box enter email address groups or domain names. For example, see the following section, Email Destination Examples.
4. Click **Add**. The address will be entered in the Group Members list and the type will be determined automatically.
5. Click **OK** to add the group to the Destination Exceptions List.
6. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level Message and Data Labels.
7. The \ buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
8. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking Delete.

Email Destination Examples

The Destination Exception is case sensitive. The following table presents examples of recommended email destinations (left column) and the email addresses that will be matched (right column) when using these email destinations:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Address Example	Type	Effectively Matches
“Domain.com”	Domain or non-SMTP address	Matches emails sent to addresses that contain the domain name. for example: **user@domain.com** or **user@subdomain.domain.com**.
“Domain”	Domain or non SMTP address	Matches emails sent to addresses that contain the domain name. For example: **user@domain.com**. It can also match emails sent to Lotus Notes canonical addresses and domains like: Domain/user.
“User@domain.com” Or **“Group@domain.com”**	SMTP Address	Matches emails sent to specific email addresses like: **user@domain.com.** Or, email to email groups whose SMTP address is **group@domain.com.**
“Domain/user” Or “Domain/group”	Domain or non-SMTP address	Matches emails sent to addresses or groups according to their Lotus Notes canonical name like: domain\user or domain/group.
“REGEX: regular expression”	Regular Expression	Matches emails sent to recipients that match the custom regular expression.

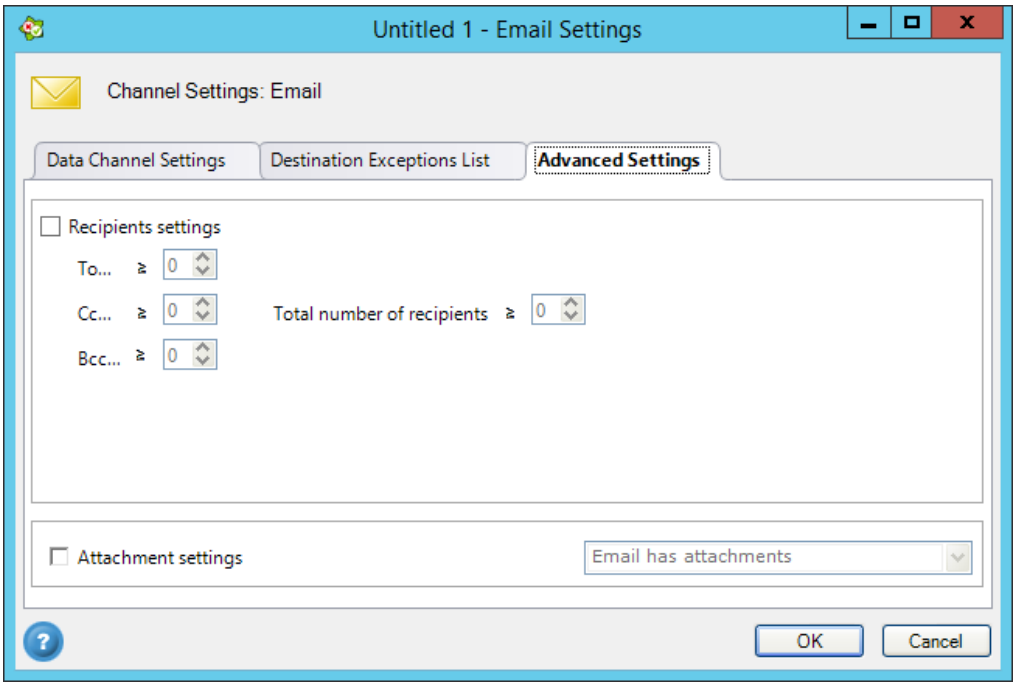
Notes:

> To whitelist emails that are sent to internal recipients, simply add your organization’s domain names to a destination group and select a permissive security action for the group (“Allow” or “Not configured”). This allows you to effectively differentiate between email messages sent to external and internal recipients.

> When using Lotus Notes, it is recommended to verify that your Lotus Notes objects (email addresses and groups) have SMTP addresses or contain the organizational domain in the “Mail Domain” field. This facilitates the bulk exclusion of addresses or groups by domain.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Email Advanced Settings



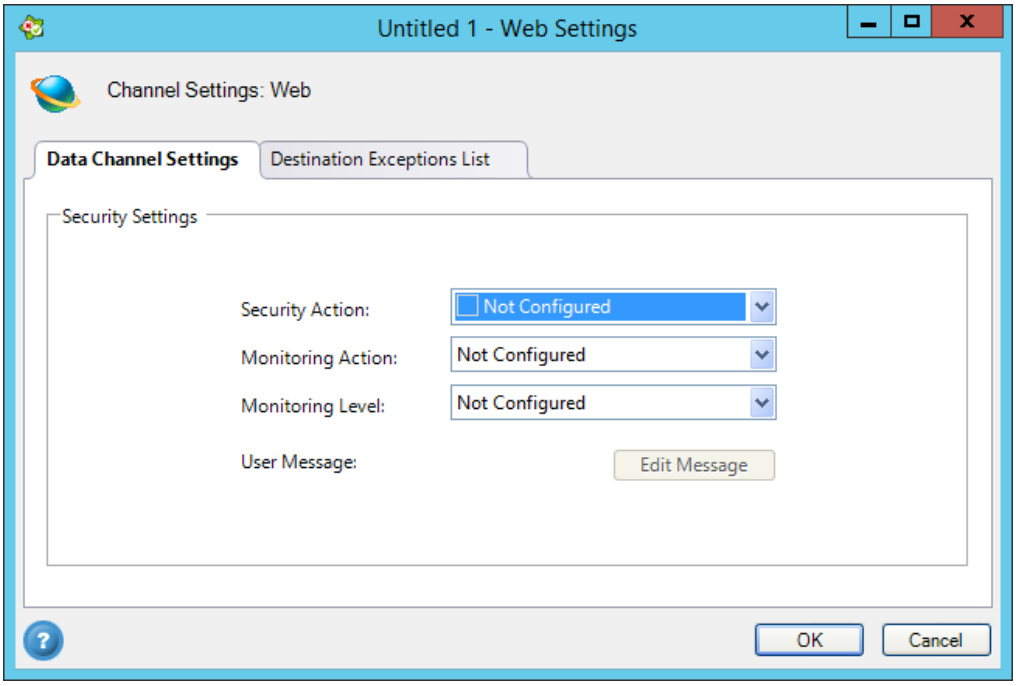
In the Advanced Settings tab you can choose the following settings.

Setting	Description
Recipients settings	When you select this you can determine the *Total number of recipients* of this email. Also you can select the number of *To*, *Cc* and *Bcc* recipients.
Attachment settings	When you select this you can choose whether the *Email has attachments* or *Email doesn't have attachments*.

4.5.2.2 Web Configuration

When you select Web as the Channel in the Data and Channels tab and click Edit Channel, the Web Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This displays the current *Data Channel Settings* and allows you to change these settings, and add, edit or delete groups in the *Destination Exceptions List tab*.

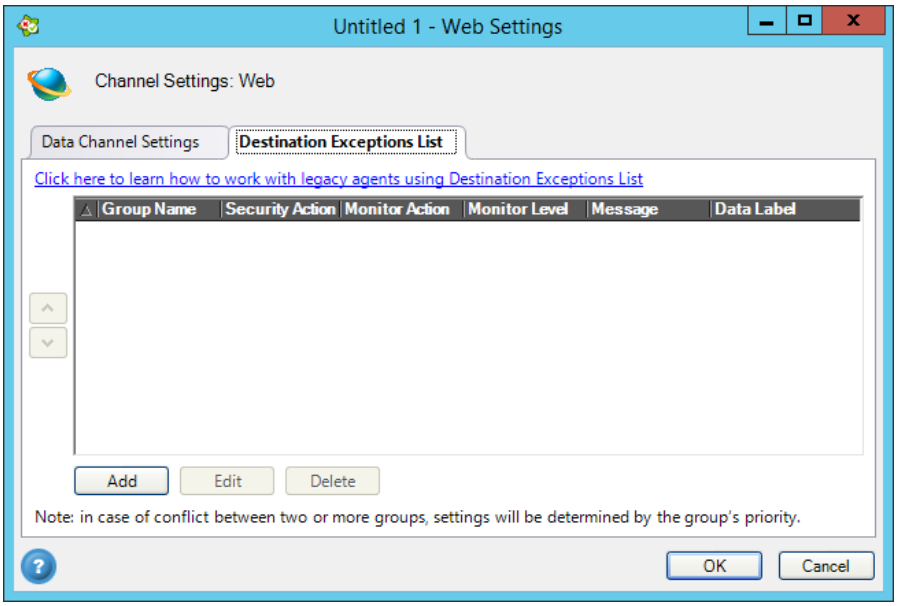
Web Data Channel Settings

Here you configure/edit the Web settings. Here is a description of the settings.

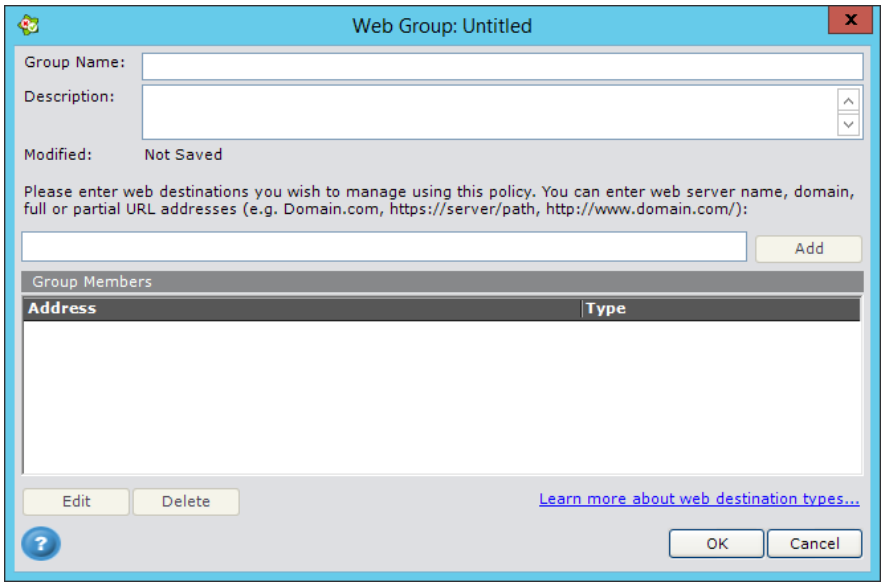
Setting	Description
Security Action	Choose the security action. The default is Not Configured, or choose: Allow, Block, Ask User or Classify.
Monitoring Action	Choose the monitoring action. The default is Not Configured, or choose: No Record, Log or Alert.
Monitoring Level	Choose the monitoring level. The default is Not Configured, or choose: Incident, Text & Incident, or Shadow & Incident.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Web Destination Exceptions List



In the Destination Exceptions List you can configure Destination groups (Blacklist\Whitelist groups). Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the Group Name, Security Action, Monitor Action, Monitor Level and Message are displayed. See *Destination Groups* for more information. When you click Add, the Web Group dialog box is displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Adding a web group

1. Enter a Group Name.
2. In the Description field, you can add a description about this new group. In the text box enter web destinations you want to manage using this policy. You can enter full or partial URL addresses. For examples see the following section, Web Destination Examples.
3. Click **Add**. The address will be entered in the Group Members list and the Type will be determined automatically.
4. Click **OK** to add the group to the Destination Exceptions List.
5. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level and Message.
6. The  buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
7. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking Delete.

Web Destination Examples

The Destination Exception is case sensitive. The following table presents examples of recommended web destinations (left column) and the URL addresses that will be matched (right column) when using these web destinations:

Address Example	Type	Effectively Matches
"Domain.com"	Web destination	Matches data posted to web sites with addresses that contain the domain name (regardless of protocol). For example: **http://www.domain.com**, **http://domain.com**, **www.domain.com/** and **https://domain.com**.
"Server"	Web destination	Matches data posted to sites whose addresses contain the web server name. For example **https://server/page/.**
"**http://www.domain.com:port**"	Web destination	Matches data posted to a website via the HTTP protocol and specific port. For example, addresses that start with: **http://www.domain.com:port/.**

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Address Example	Type	Effectively Matches
www.domain.com	Web destination	Matches data posted to sites whose addresses contain **www.domain.com. For example: http://www.domain.com/.**
"REGEX: regular expression"	Regular Expression	Matches data posted to websites whose address matches the custom regular expression.

Notes:

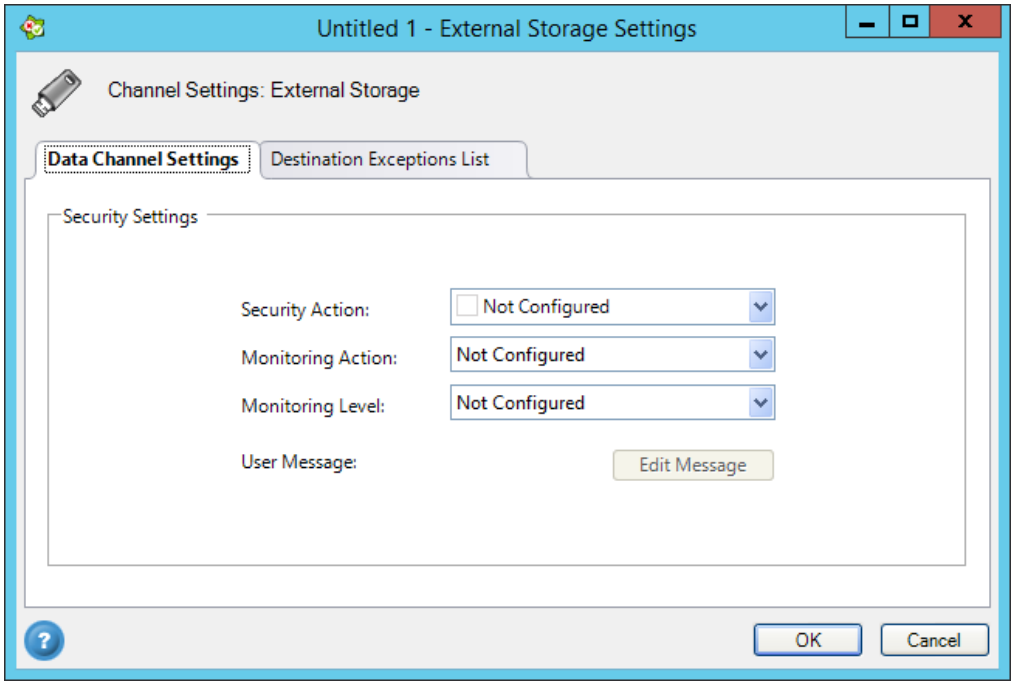
- You can also enter domains without a top-level domain, for example: "domain" that will match http://domain/page/.
- It is recommended to enter general web destination objects, preferably domains or web server names. These will have more chance to match addresses and websites that use various protocols (http, https) than more exact objects like http://domain.com/ or www.domain.com/ that only match specific protocols.
- It is recommended to use DNS names of web servers instead of IP addresses whenever possible, unless you are certain that your end users access a web server by its IP address instead of DNS name. If you are not sure, enter two separate records, one for the IP address and another one for the DNS name of the web server.

4.5.2.3 External Storage Configuration

When you select External Storage as the Channel in the Data and Channels tab and click 

, the External Storage Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This displays the current Data Channel Settings and allows you to change these settings, and add edit or delete groups in the Destination Exceptions list.

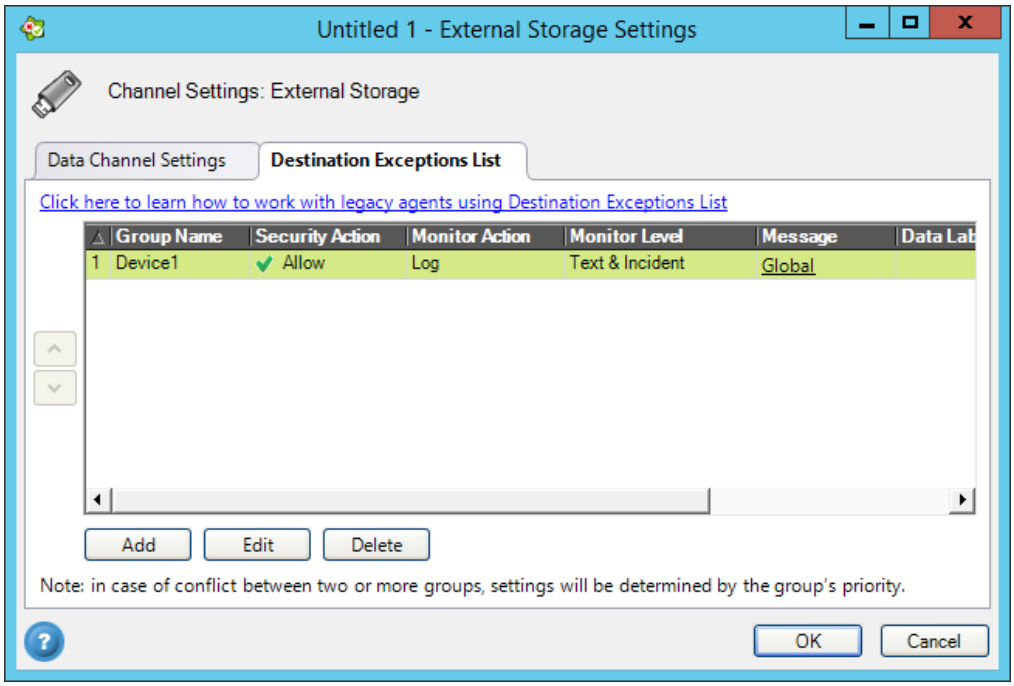
External Storage Data Channel Settings

Here you configure/edit the External Storage settings. Here is a description of the settings.

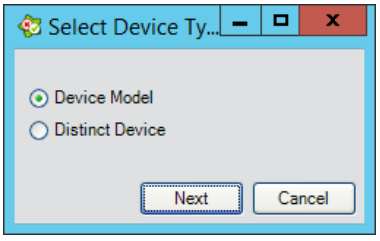
Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *No Record*, *Log* or *Alert*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

External Storage Destination Exceptions List



1. In the Destination Exceptions List you can configure Destination groups (Blacklist\Whitelist groups). Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the *Group Name*, *Security Action*, *Monitor Action*, *Monitor Level* and *Message* are displayed.
2. When you click Add, the Select Device Type dialog box is displayed.



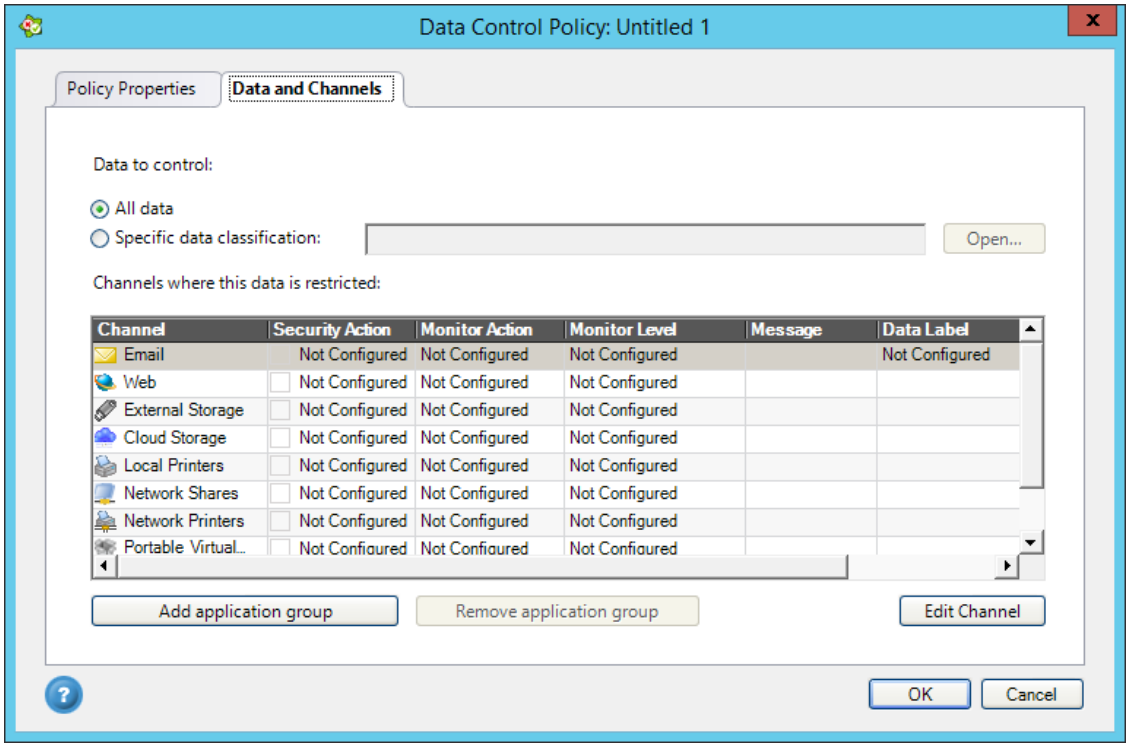
3. You can select either Device Model or Distinct Device. For an in-depth discussion of the steps required to add a new external device, refer to Approving Devices.
4. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level and Message.
5. The \ buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
6. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking Delete.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.5.2.4 Cloud Storage Configuration

This data channel controls file uploads by the following popular cloud storage client applications: Dropbox, Box.net, Google Drive, and Microsoft SkyDrive.

When you want to select Cloud Storage settings you configure/edit the Cloud Storage settings directly from the Data and Channels tab.

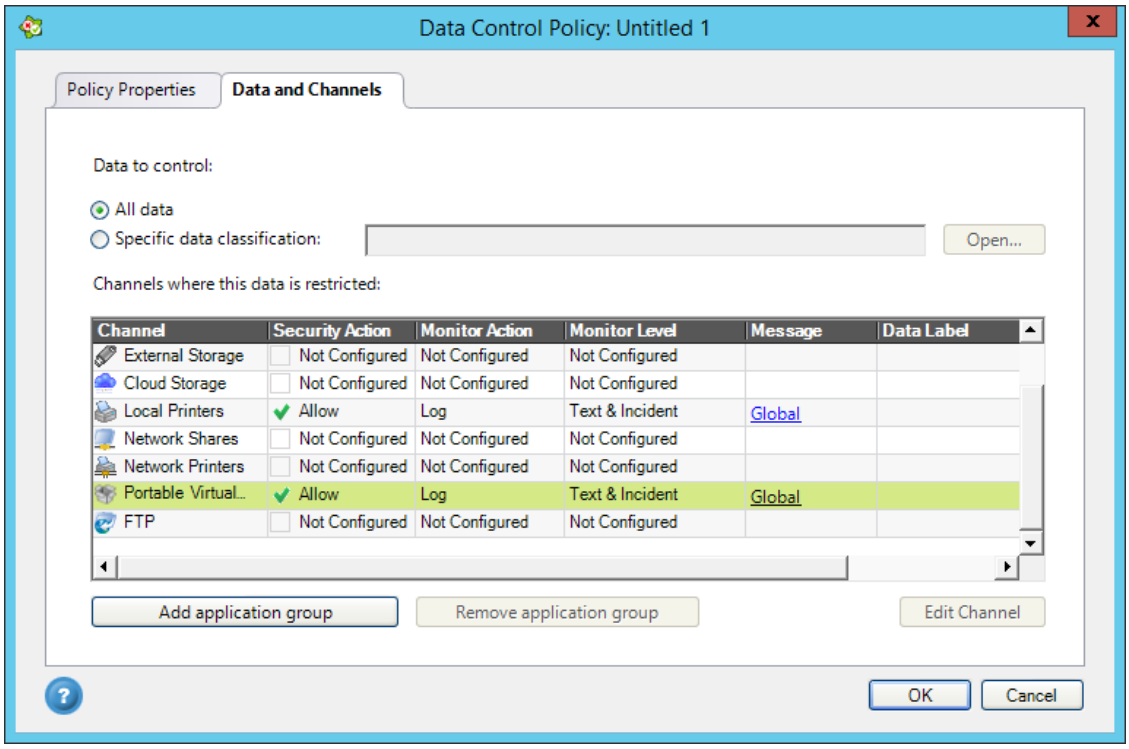


Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *Log*, *Alert* or *No Record*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
User Message	Edit the end-user message by clicking Global. This will appear when a Security Action other than *Not Configured* is choosen. See *Editing an End User* Message for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4.5.2.5 Local Printers Configuration

When you want to select Local Printers settings you configure/edit the Local Printers settings directly from the Data and Channels tab.

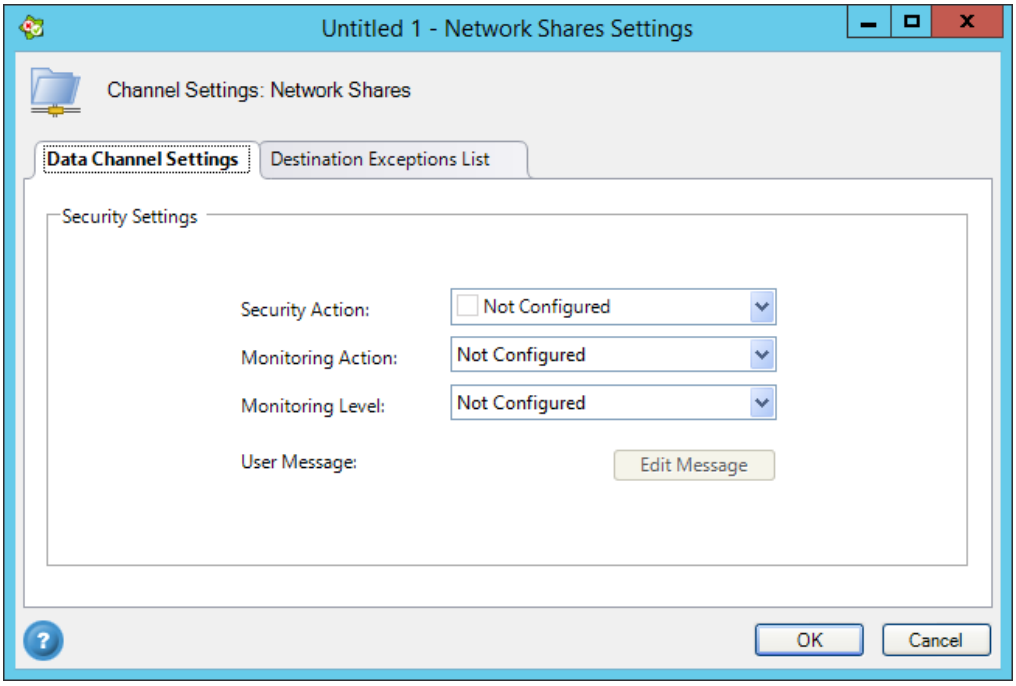


Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *No Record*, *Log* or *Alert*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

4.5.2.6 Network Shares Configuration

When you select Network Shares as the Channel in the Data and Channels tab and click Edit Channel, the Network Shares Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This displays the current *Data Channel Settings* and allows you to change these settings, and add edit or delete groups in the *Destination Exceptions list*.

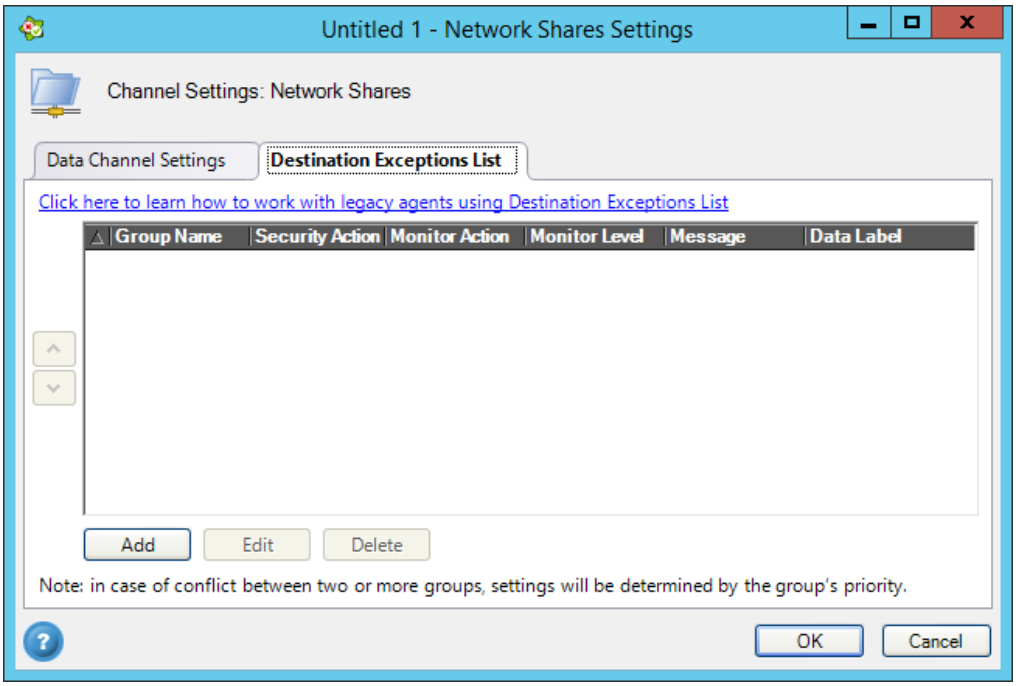
Network Shares Data Channel Settings

Here you configure/edit the Network Shares settings.

Setting	Description
Security Action	Choose the security action. The default is Not Configured, or choose: Allow, Block, Ask User or Classify.
Monitoring Action	Choose the monitoring action. The default is Not Configured, or choose: No Record, Log or Alert.
Monitoring Level	Choose the monitoring level. The default is Not Configured, or choose: Incident, Text & Incident, or Shadow & Incident.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

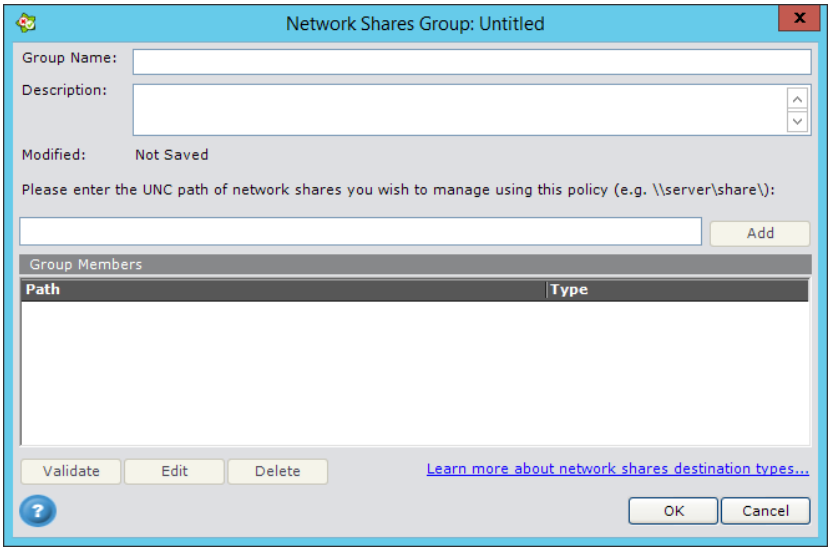
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Network Shares Destination Exceptions List



1. In the Destination Exceptions List you can configure Destination groups (Blacklist\Whitelist groups). Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the *Group Name*, *Security Action*, *Monitor Action*, *Monitor Level* and *Message* are displayed. See *Destination Groups* for more information.

2. When you click Add, the Network Shares Group dialog box is displayed.



3. Here you create a new Network Shares group.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Adding a Network Shares group

1. Enter a Group Name.
2. In the Description field, you can add a description about this new group.
3. In the text box enter the UNC path for network shares you want to manage using this policy. For example: \\server\share\.
4. Click **Add**. The path will be entered in the Group Members list and the Type will be determined automatically.
5. Click **OK** to add the group to the Destination Exceptions List.
6. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level and Message.
7. The  buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
8. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking Delete.

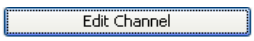
Network Shares Examples

The Destination Exception UNC is case sensitive. The following table presents examples of recommended network share destinations (left column) and the network shares that will be matched (right column) when using these destinations:

Network Share Example	Type	Effectively Matches
"\\server1\share1"	UNC path	Matches network shares by UNC path. In this case it will match data transfers to a network share named "Share1" on the file server "Server1".
"REGEX: regular expression"	Regular Expression	Matches data transfers to a network share whose UNC path matches the custom regular expression.

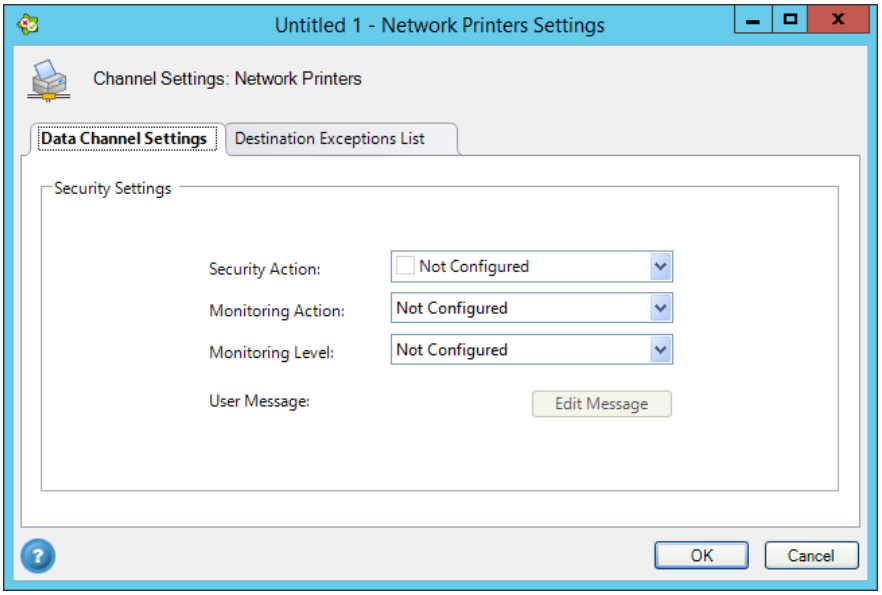
If you have mapped drive letters for network shares in your organization, enter the original full UNC path of the mapped drives.

4.5.2.7 Network Printers Configuration

When you select Network Printers as the Channel in the Data and Channels tab and click 

, the Network Printers Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



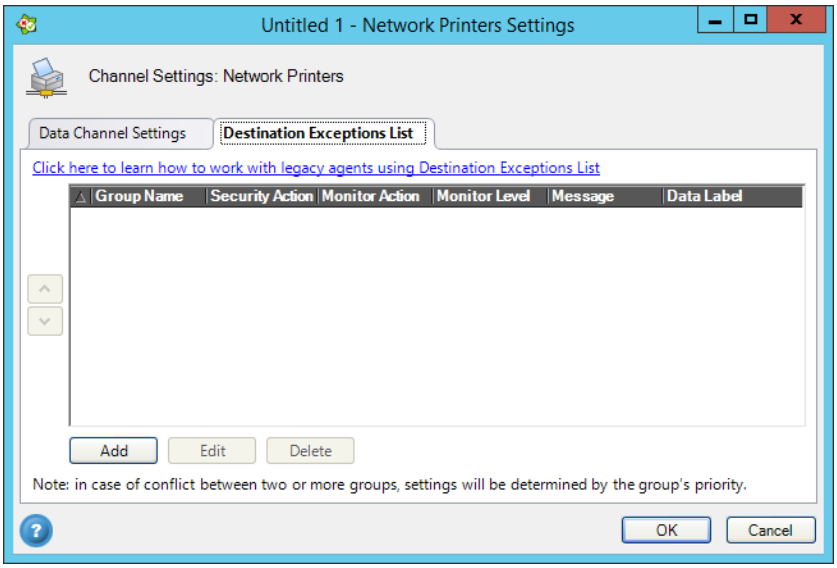
This displays the current Data Channel Settings and allows you to change these settings, and add edit or delete groups in the Destination Exceptions list.

Network Printers Data Channel Settings

Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *No Record*, *Log* or *Alert*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

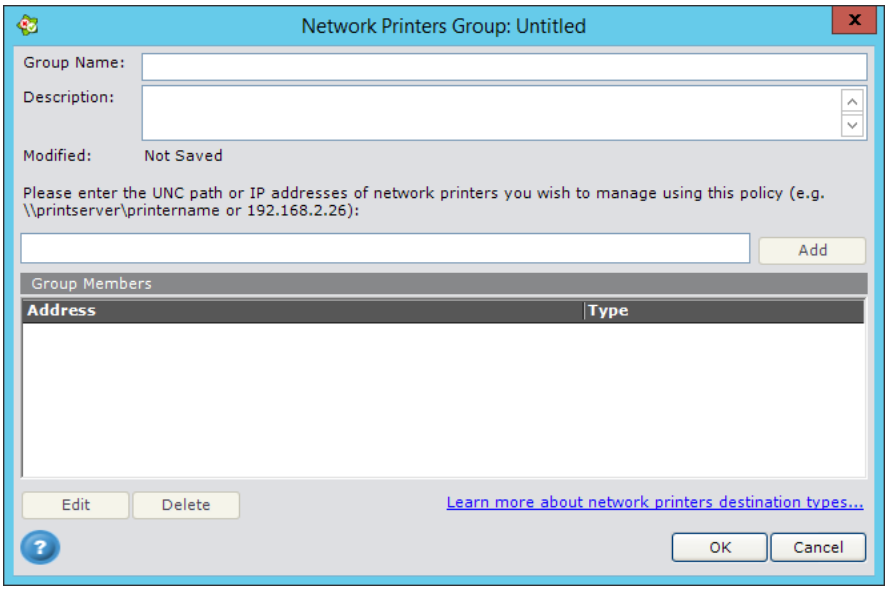
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Network Printers Destination Exceptions List



In the Destination Exceptions List you can configure Destination groups (Blacklist\Whitelist groups). Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the Group Name, Security Action, Monitor Action, Monitor Level and Message are displayed. See Destination Groups for more information.

When you click Add, the Network Printers Group dialog box is displayed.



Here you create a new Network Printers group.

Adding a Network Printers group

1. Enter a Group Name.
2. In the Description field, you can add a description about this new group.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3. In the text box enter the UNC path of the printers you wish to manage using this policy. For examples see the following section, Network Printer Examples.
4. Click **Add**. The address will be entered in the Group Members list and the Type will be determined automatically.
5. Click **OK** to add the group to the Destination Exceptions List.
6. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level and Message.
7. The  buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
8. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking Delete.

Network Printer Examples

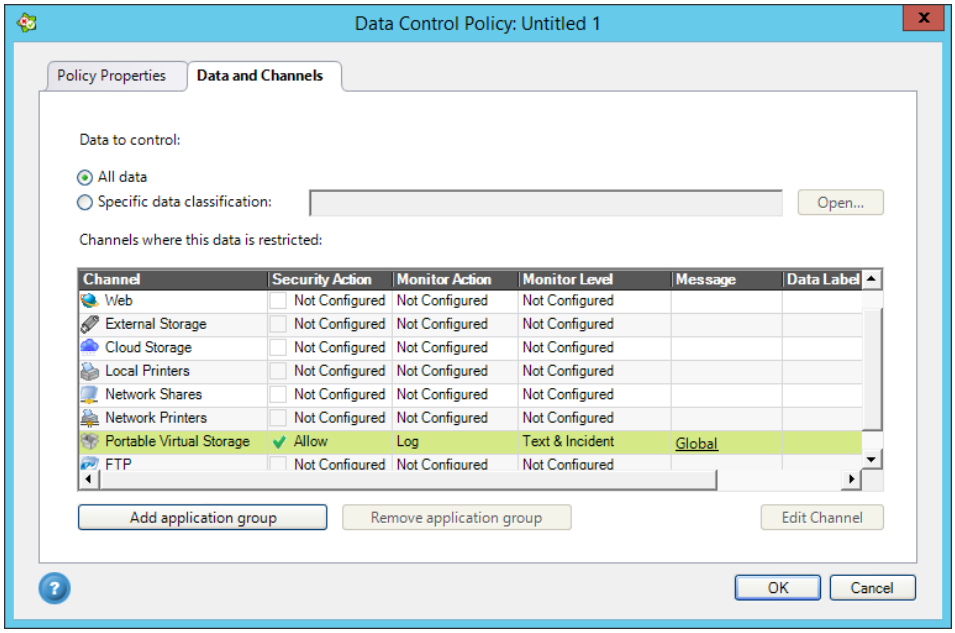
The Destination Exception is case sensitive. The following table presents examples of recommended printer destinations (left column) and the printers that will be matched (right column) when using these printer destinations:

Printer Example	Type	Effectively Matches
"\\server1\printer1"	UNC path	Matches printers by the printer's UNC path. In this case it will match data sent to "Printer1" located in the print server named "Server1".
"REGEX: regular expression"	Regular Expression	Matches data sent to a printer whose UNC path or IP matches the custom regular expression.

4.5.2.8 Portable Virtual Storage Configuration

When you want to select Portable Virtual Storage settings you configure/edit the Portable Virtual Storage settings directly from the Data and Channels tab.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



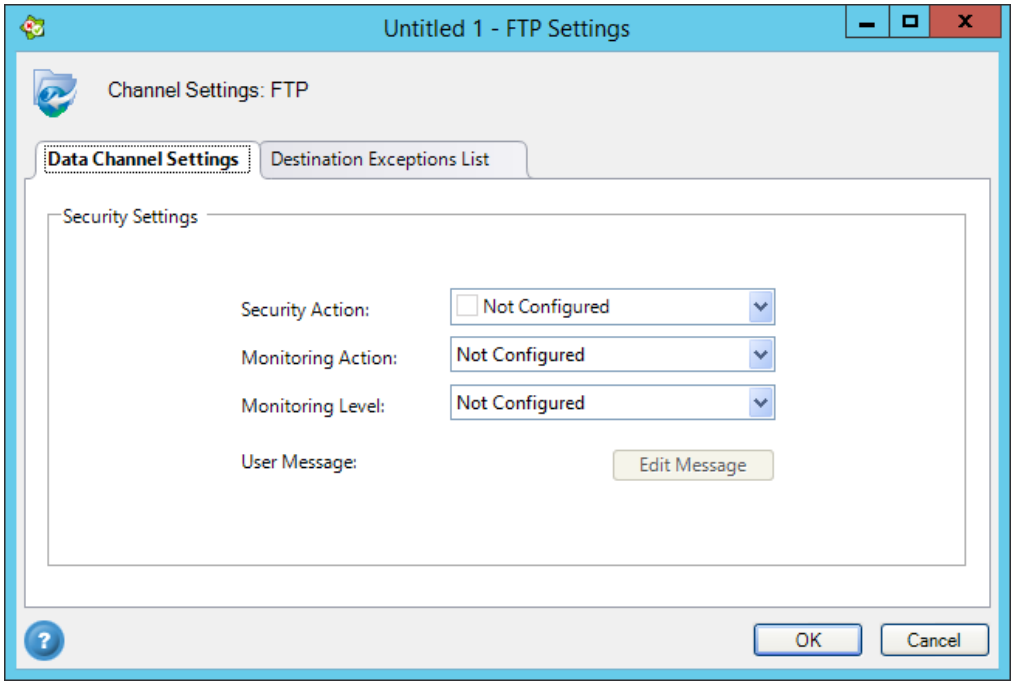
Setting	Description
Security Action	Choose the security action. The default is Not Configured, or choose: Allow, Block, Ask User or Classify.
Monitoring Action	Choose the monitoring action. The default is Not Configured, or choose: No Record, Log or Alert.
Monitoring Level	Choose the monitoring level. The default is Not Configured, or choose: Incident, Text & Incident, Shadow & Incident.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

4.5.2.9 FTP Configuration

When you select FTP as the Channel in the Data and Channels tab and click 

, the FTP Settings window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



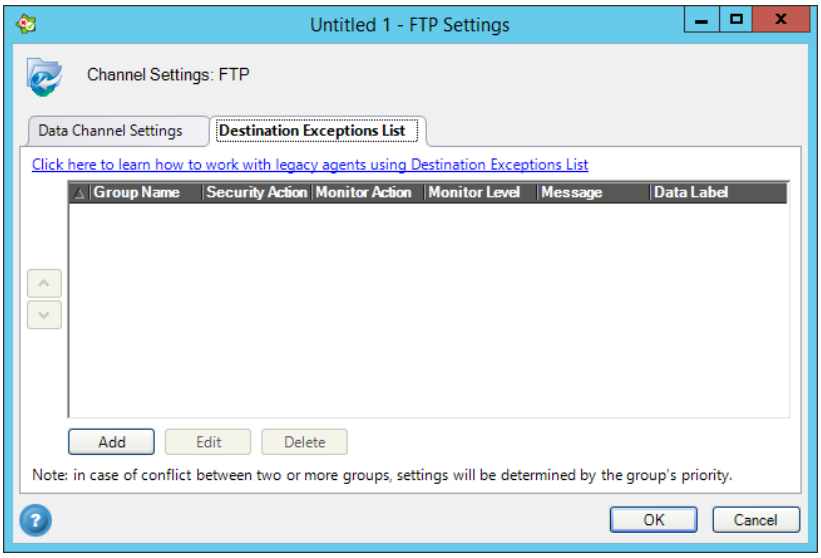
This displays the current Data Channel Settings and allows you to change these settings, and add edit or delete groups in the Destination Exceptions list.

FTP Data Channel Settings

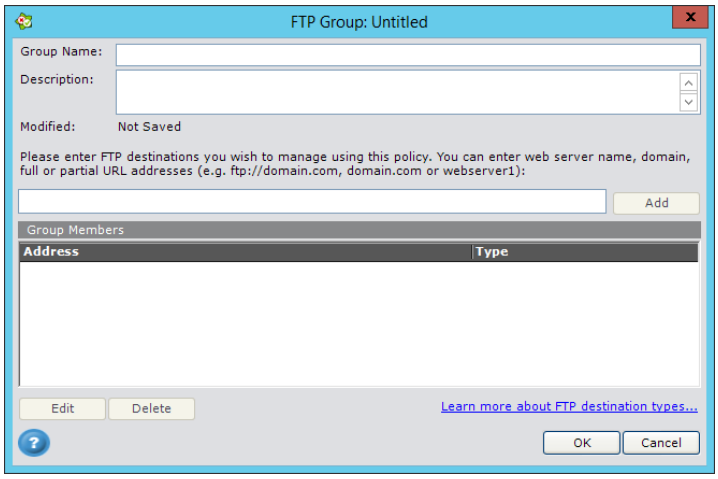
Setting	Description
Security Action	Choose the security action. The default is *Not Configured*, or choose: *Allow*, *Block*, *Ask User* or *Classify*.
Monitoring Action	Choose the monitoring action. The default is *Not Configured*, or choose: *No Record*, *Log* or *Alert*.
Monitoring Level	Choose the monitoring level. The default is *Not Configured*, or choose: *Incident*, *Text & Incident*, or *Shadow & Incident*.
User Message	Edit the end-user message by clicking Edit. See Editing an End User Message for more information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

FTP Destination Exceptions List



1. In the Destination Exceptions List you can configure Destination groups (Blacklist\Whitelist groups). Each group can become a Whitelist or Blacklist by changing the groups' security actions. For each group in the list, the *Group Name*, *Security Action*, *Monitor Action*, *Monitor Level* and *Message* are displayed. See *Destination Groups* for more information.
2. If you click Add, the FTP Group dialog box is displayed.



Adding an FTP group

1. Enter a Group Name.
2. In the Description field, you can add a description about this new group.
3. In the text box, enter FTP destinations that you wish to manage using this policy. You can enter full or partial URL addresses. For examples, see the following section, FTP Destination Examples.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4. Click **Add**. The address will be entered in the Group Members list and the Type will be determined automatically.
5. Click **OK** to add the group to the Destination Exceptions List.
6. Once the group is added to the Destination Exceptions list you are able to set the different security settings for each group: Security Action, Monitoring Action, Monitoring Level and Message.
7. The  buttons to the left of the Destination Exceptions List are enabled after selecting a group from the list. These buttons move the selected group up or down a row and change the order and priority of the groups. In cases of conflict between the Security Actions of two or more groups, priority will be given to the higher group in the list.
8. You can change an address in the list by selecting it and clicking Edit. You can also remove an address from the list by selecting it and clicking **Delete**.

FTP Destination Examples

The Destination Exception is case sensitive. The following table presents examples of recommended FTP destinations (left column) and the FTP addresses that will be matched (right column) when using these FTP destinations:

Address Example	Type	Effectively matches
"Domain.com"	Web destination	Matches data uploaded to FTP servers whose address contains the domain name. for example: **ftp://server.domain.com/** or **ftps://server.domain.com/.**
"Server"	Web destination	Matches data uploaded to an FTP server whose address starts with: **ftp://server.domain.com/**.
"**ftp://server.domain.com/**"	Web destination	Matches data uploaded to an FTP server whose address starts with: **ftp://server.domain.com/**.
"**ftp://Server.domain.com/folder1/folder2**"	Web destination	Matches data uploaded to a specific folder (folder 2) in a specific FTP server (server.domain.com).
"REGEX: regular expression"	Regular Expression	Matches data uploaded to FTP sites whose address matches the custom regular expression.

- You can also enter domains without a top-level domain, for example: "domain" that will match ftp://domain/folder/.
- You can enter specific FTP folders that will be matched by entering the folder's FTP address. For example: ftp://server.domain.com/folder1/.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- It is recommended to use DNS names of FTP servers instead of IP addresses whenever possible, unless you are certain that your end users access FTP servers by their IP address, instead of DNS name. If you are not sure, enter two separate records, one for the IP address and another one for the DNS name of the FTP server.

4.5.2.10 Destination Exceptions List: Support for Legacy Agents

Safend Data Protection suite version 3.4.6 and above provides the ability to configure various security settings of data control policies according to the destination to which the data is transferred. For example, a policy can be set to block sensitive emails from being sent to external email recipients while allowing users to send sensitive emails to internal email addresses (based on the organization's domain name).

Previous versions of Safend Data Protection agents (3.4.5 SP1 and below) provided limited means to control data, based on its destination. Policy settings could only be configured to apply when sending data to specific destinations ("Blacklist" mode) or to ignore the policy's security settings for specific destinations ("Everywhere, except for whitelist" mode).

The following capabilities have been added to the 3.4.6 Data control policy:

- The ability to define multiple destination groups in a single data control policy.
- The ability to configure different security settings to multiple destination groups.
- The ability to resolve group conflicts by assigning a priority to each destination group.

Policies that involve these new capabilities will be ignored by legacy agents. Organizations that still have legacy Safend Data Protection agents (version 3.4.5 SP1 and below) and wish to configure additional security settings based on destination groups, need to carefully follow the security settings conversion table below, to ensure that the legacy agents can properly handle the new data control policy settings.

Security Settings Conversion Table Supported by Legacy Agents

The following table presents the security settings that are supported by legacy agents (version 3.4.5 SP1 and below). The 1st and 2nd columns to the left show the legacy data control policy security settings while the 3rd and 4th columns present the recommended configuration that should be set in order to apply these settings using the new 3.4.6 data control policy.

Data Control Policy Settings	
Data Channel Security Action	Security Action of Destination Group
Allow	
Block	
Ask user	

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Data Control Policy Settings	
Encrypt	
Not configured	
Allow	Not configured*
Block	Not configured*
Ask user	Not configured*
Encrypt	Not configured*
Not configured	Not configured*
Not configured	Allow*
Not configured	Block*
Not configured	Ask user*
Not configured	Encrypt*
Not configured	Not configured*

* Legacy agents only support a single destination group in each data channel. Configuring a data channel with more than one destination group will cause the legacy agent to ignore the data control policy entirely.

Other configurations, which do not appear in the 3rd and 4th columns, will not be supported by legacy agents.

4.5.2.11 Application Data Access Control

Application data access control allows you to protect additional data transfer channels. Safend Data Protection Suite controls access of pre-defined applications to classified data on your hard drive, through direct access to files on the local file system or through user copy/paste actions.

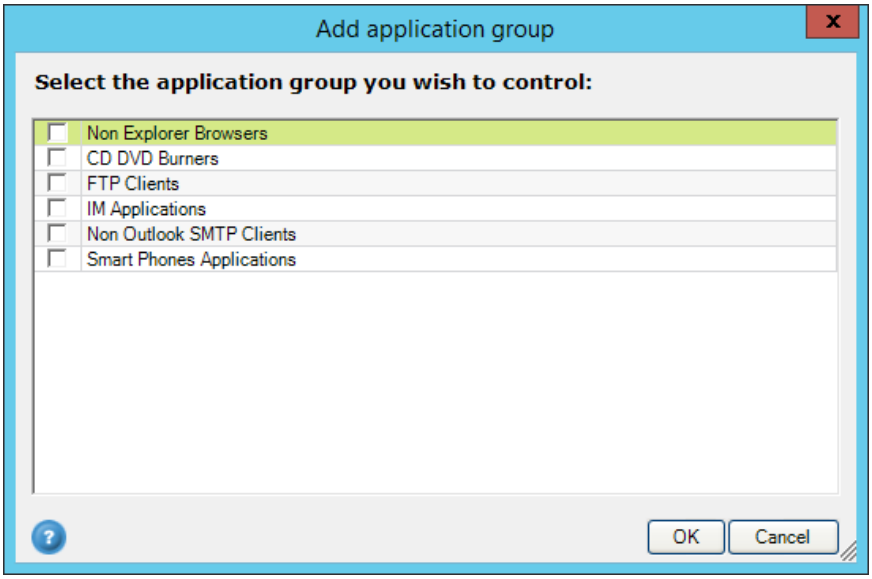
By controlling these actions, Safend Data Protection Suite controls and monitors classified data transferred out of the protected machines using such applications.

Applications are divided into logical application groups. Each application group can be added to any Data Control Security Policy, and be associated with security settings like any other protected channel. See *Application Groups* for additional information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Adding an Application Group

1. Click Add application group found at the bottom of the Data and Channels tab. The *Add application group* window is displayed.



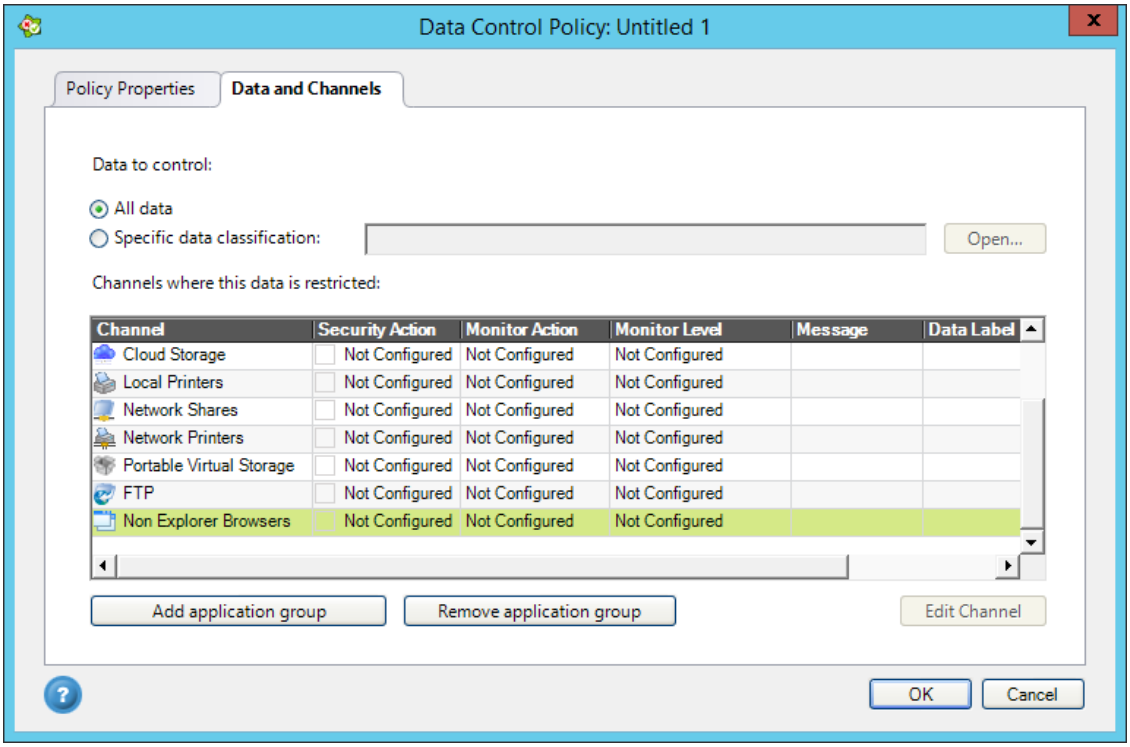
2. Select the application groups you want to add to the policy and click **OK**. The selected application groups will be added to the policy.

Editing an Application Group

After you add an application group to the list of channels it can be edited and the settings changed.

1. In the *Data and Channels* tab, choose the application group of interest, for example **Non Explorer Browsers**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. Here you directly choose the settings. You can set the *Security Action* (Allow, Block,Not Configured), *Moni*toring Action (Log, Alert, No Record, Not Configured), Monitoring Level (Incident, Text & Incident, Shadow & Incident, Not Configured) and edit the End User Messages by clicking Global.

3. Click OK to save your changes or Cancel to exit.

Editing the other application groups is very similar to the Non Explorer Browsers example. These include: CD DVD Burners, FTP Channels, IM Applications, Non Outlook SMTP Clients and Smart Phone Applications.

4.6 About Discovery Policies

Understanding where sensitive data is located is the foundation of any data protection project. Safend Data Protection Suite allows security administrators to locate sensitive data stored on organizational endpoints. This process helps identify gaps in data protection and compliance initiatives and provides insight into what policies should be implemented using other components of the Safend Data Protection Suite.

The endpoint discovery process is triggered by applying a Discovery Policy on the protected endpoint. This policy indicates which data classifications, should be searched for on the organizational endpoints. The Discovery Policy also specifies the type of log record that will be sent to the Management Server when sensitive date is discovered.

When a Discovery policy is applied on the endpoint, the Safend Data Protection Suite Agent scans and classifies all data files on the machine. When a classified file is discovered, a log record

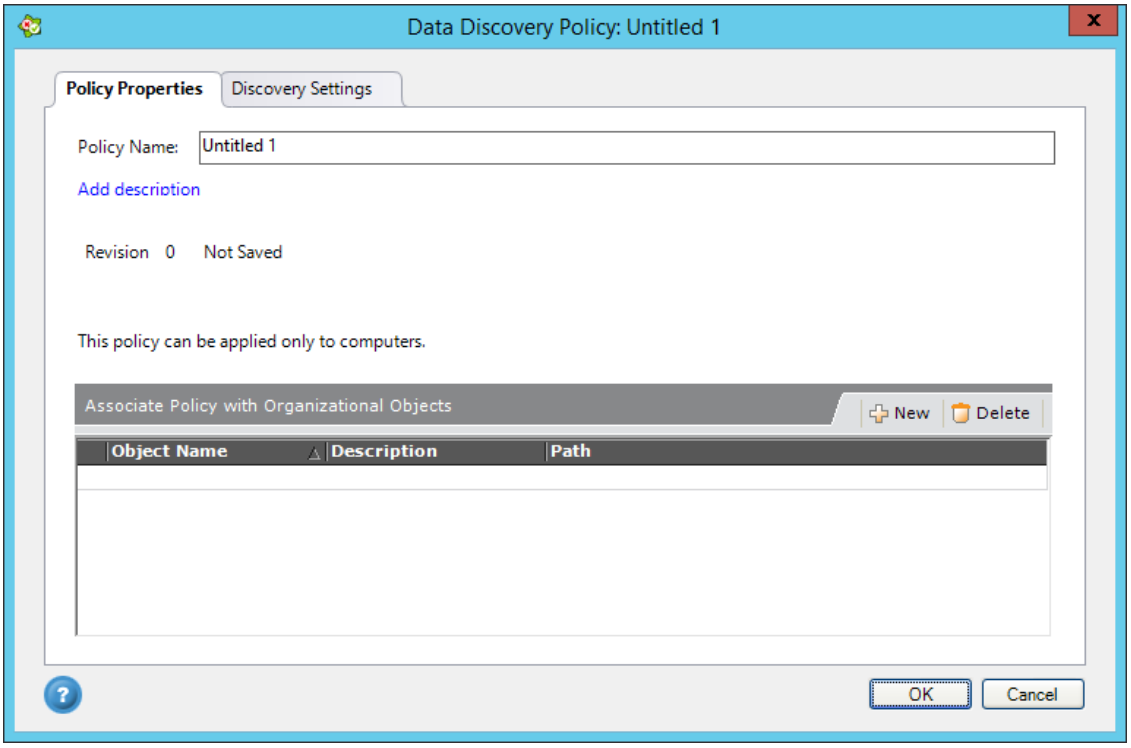
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

is sent to the Management Server. The Discovery process runs in the background, with minimal affect on endpoint performance.

The status of the Discovery process conducted on each endpoint is displayed in the Clients tab.

4.7 Creating a Discovery Policy

1. Click New in the Custom Policies toolbar. The new policy window is displayed.

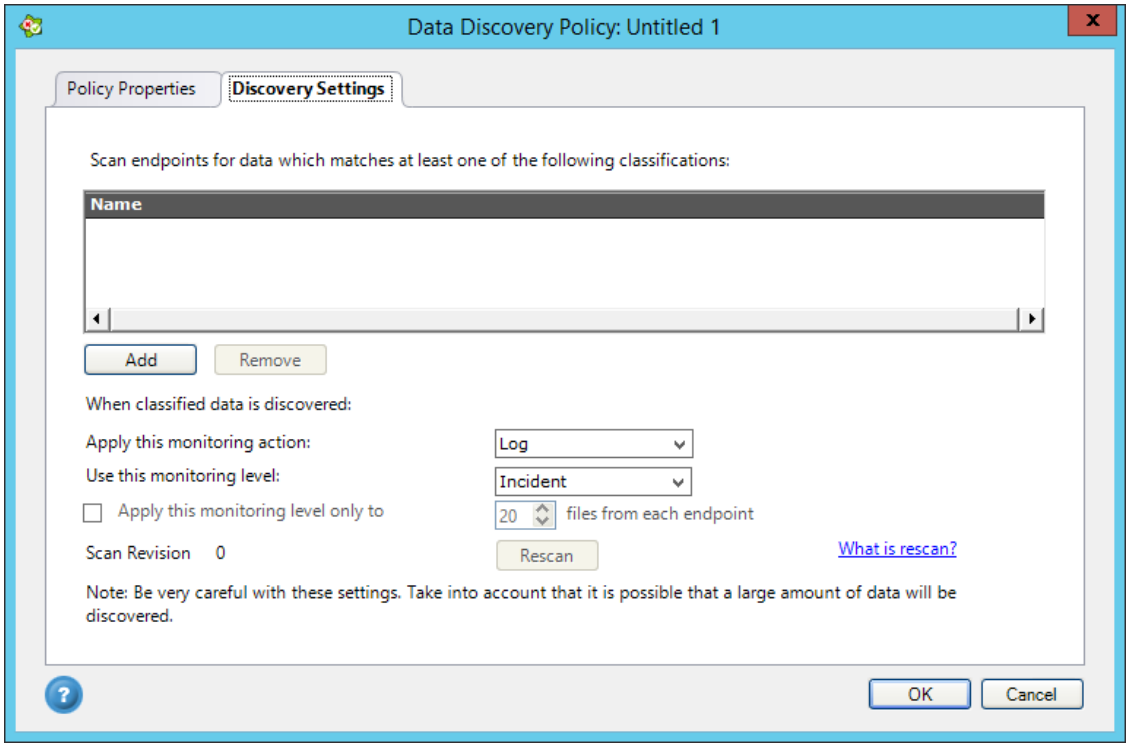


2. In the Policy Properties tab enter a Policy Name.
3. You have the option to add a description of the policy, by clicking Add description.
4. Associate the policy with Organizational objects. See Associating a Policy with Organizational Objects for a detailed description.
5. Go to the Discovery Settings tab to continue.

4.7.1 Configuring Discovery Settings

1. Click the Discovery Settings tab.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. In the Discovery Settings tab, click **Add** to add classifications to the list. The *Select Classification* dialog box is displayed. Choose a Classification to add to the list.
3. You can delete a Classification from the list by clicking **Remove**.
4. Choose in Apply this monitoring action either *Log* or *Alert*, when classified data is discovered.
5. For Use this monitoring level, choose Incident, Text & Incident or or Shadow & Incident.
6. If you select Apply this monitoring level only to, you can set the number of files from each endpoint of the specified classification, which will generate logs of the specified monitoring level. Additional classified files on the endpoint will generate a log with "incident" monitoring level only.
7. Click **OK** to begin the process

4.7.1.1 Monitoring Options

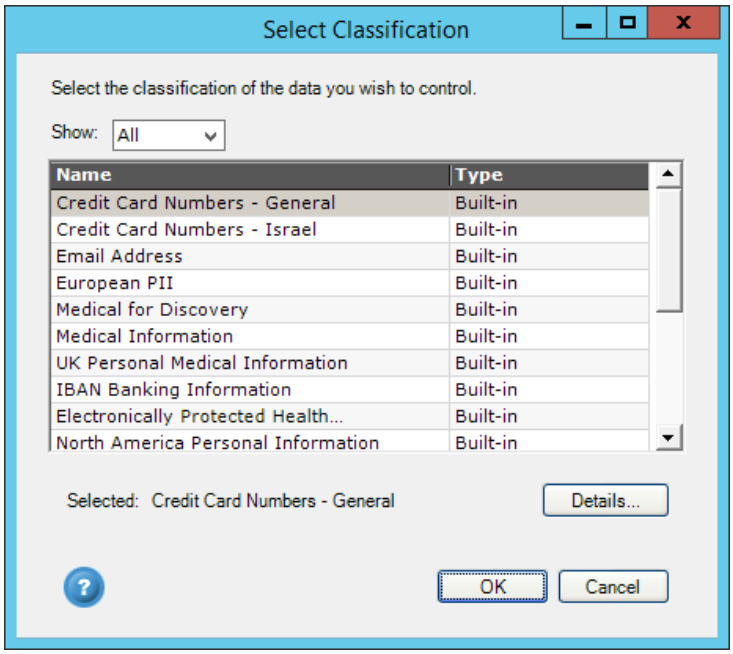
Option	Description
Monitoring Actions	
Log	Logs the incident according to the monitoring level. Sends the log in the predefined intervals.
Alert	Sends the record immediately as an alert.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Monitoring Levels	
Incident	Sends only incident details, without the content of the file.
Text & Incident	Sends the textual content of the file and file general information, together with incident details.
Shadow & Incident	Sends a copy of the file (file shadow) to the server, together with incident details.

4.7.1.2 Select Classification for Discovery Settings

1. Click **Add** in the *Discovery Settings* tab. The *Select Classification* dialog box is displayed.



2. Choose a classification from the list (Built-in or Custom).
3. Click **Details** to find out more about this classification.
4. Click **OK** and this classification is added to the list in the Discovery Settings tab.

4.7.1.3 Rescaning Endpoints

After the initial Discovery process had been completed, you may wish to repeat it again using the same policy. To initiate a scan of all endpoints associated with the Discovery Policy, even if the Discovery process already occurred, click Rescan. This will change the scanning revision, instructing all endpoints associated with the policy to repeat the Discovery process.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

5 Port and Device Control Policies

A Safend Data Protection Suite Port and Device Control policy specifies the access permissions of physical ports, wireless ports, storage device types, storage device models and distinct storage devices, as well as WiFi connections, enabling you to specify whether they are allowed, blocked, or allowed Read Only access.

A policy can also block Hardware Key Loggers that are connected to a USB or a PS/2 port. Hardware Key Loggers are devices that can be placed by a hostile entity between a keyboard and its host computer in order to log keyboard input. Your policy can specify whether hardware key loggers should be blocked when detected by the Safend Data Protection Suite.

For each port, device, storage device and WiFi connection, Safend Data Protection Suite policies also define whether its activities (such as connection or disconnection of a device) are logged, and whether these activities trigger an alert. Logs and alerts are encrypted, stored on the Safend Data Protection Suite Management Server, and can be viewed in the Logs Tab. Alerts are sent immediately to pre-defined destinations and also can be viewed in the Logs Tab.

An additional level of monitoring the activity in your organization is provided by File Type Control, which enables you to control and alert/log or save a hidden copy of files written to or read from removable media devices or CD/DVD. File logs as well can be viewed in the Logs Tab.

Note: File Type Control, controls and monitors files transferred to/from removable storage devices only according to the file type, regardless of its content. To apply a more granular policy on files transferred to removable storage devices according to its data classification, based on the file content, use Data Control Security Policies.

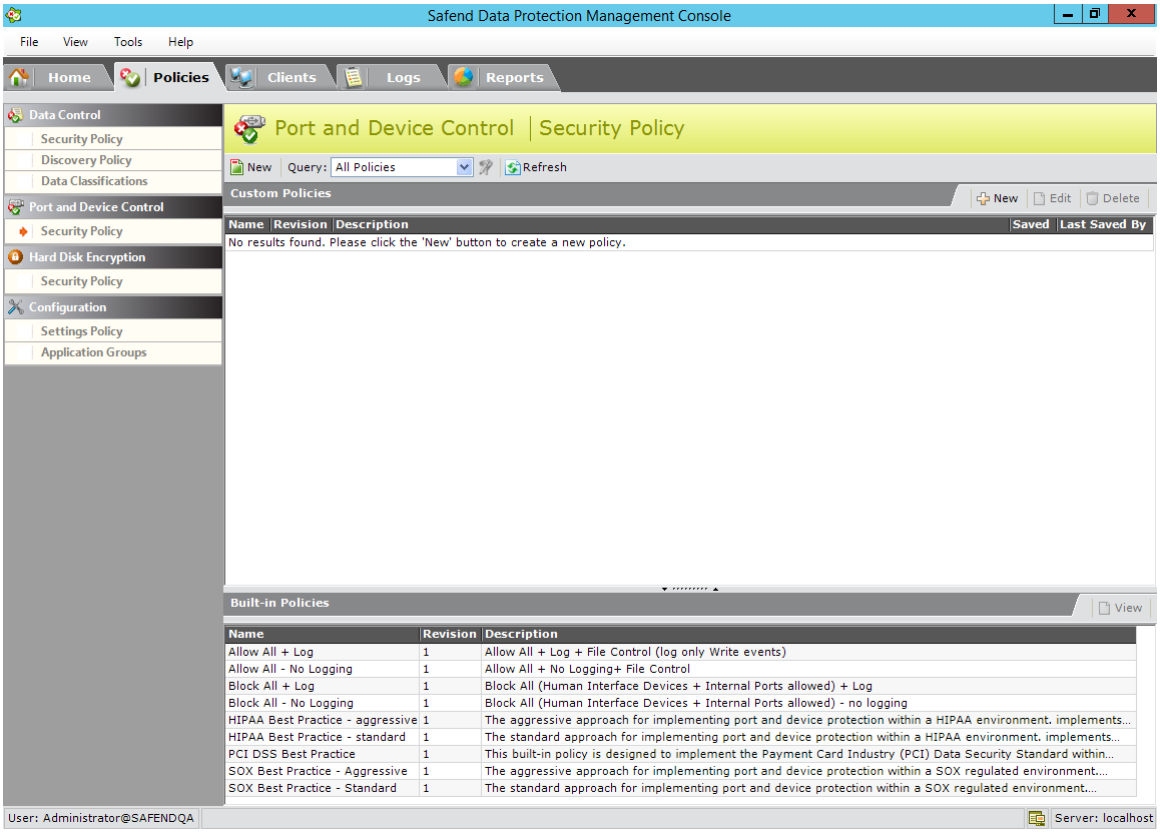
A policy can be set to require that removable media devices, including CD/DVD media and external hard disks attached to a computer protected by this policy be encrypted, so that only devices encrypted by the organization can be used. Devices encrypted by the organization can only be used by organizational computers, thereby preventing leakage of corporate data (should the need arise, there are exceptions to this rule).

5.1 About the Port and Device Control Policy Window

Accessing the Port and Device Control/Security Policy Window

Click the **Policies tab > Port and Device Control in the left pane > Security Policy**. The Port and Device Control/Security Policy window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



5.1.1.1 Workspace

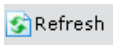
This window is divided into two sections – Custom Policies and Built-in Policies.

- Custom Policies are policies that are created by the user.
- Built-in Policies are policies that are delivered with the system that can be associated "as is" or after some adjustments.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Menus	
Option	Description
Right-click Custom Policies	
Delete	This removes the policy from the Custom Policy list.
Edit	This enables you to edit the policy.
Export	This enables you to export the policy. It opens *Save Export Result As*.
New	This enables you to create a new policy.
Built-in Policies	
Option	Description
View	This enables you to view the details of the policy.
Customize	This enables you to customize the policy according to your requirements.
Export	This enables you to export the policy. It opens Save Export Result As.

Toolbar

Button	Description
	This enables you to create a new Port and Device Control policy.
	This refreshes what is displayed on the screen.

5.1.1.2 Buttons

Button	Description
Custom Policies Buttons	
	This enables you to create a new security policy.
	This enables you to edit a selected security policy.
	This enables you to delete a selected security policy.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

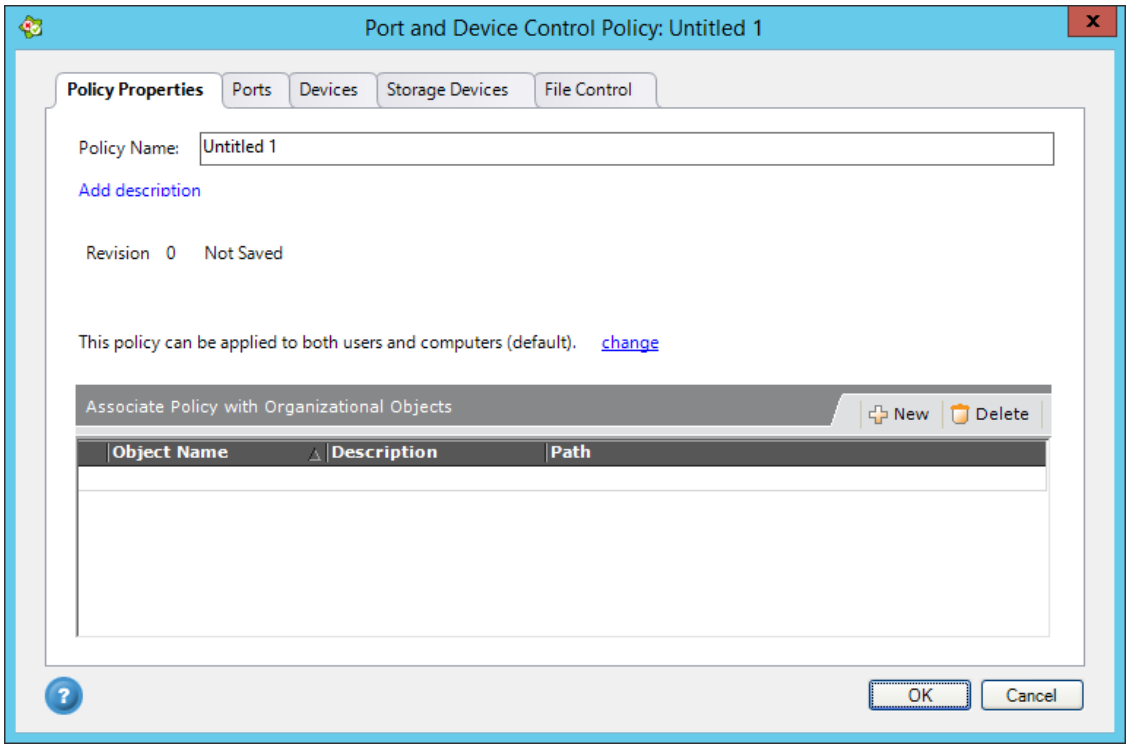
Built-in Policies	
View	This enables you to view a built-in security policy.

5.2 Port and Device Control Policy Window

This window enables you to create a new Port and Device Control policy or view or edit an existing policy.

Accessing the Port and Device Control Policy Window

Click New or select an existing policy and click Edit or View. The Port and Device Control Policy window is displayed.



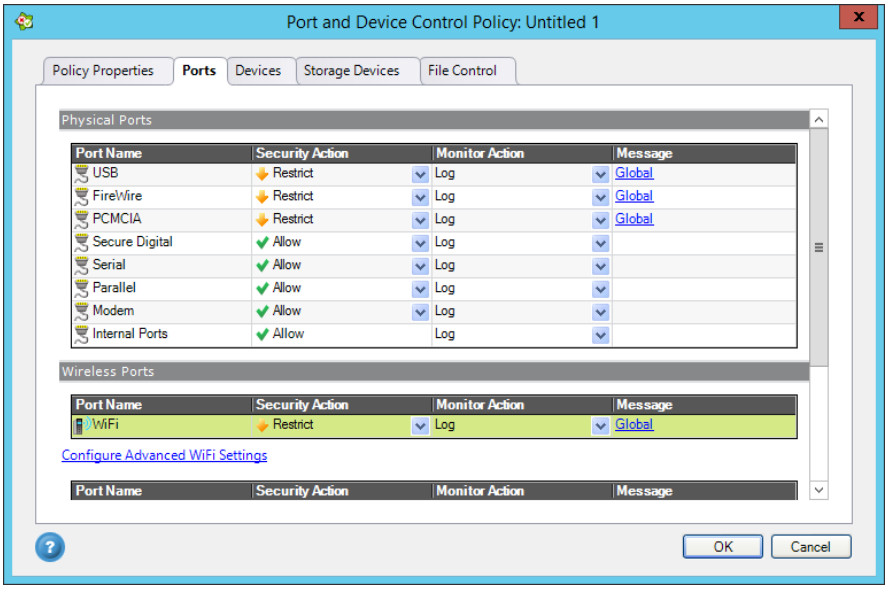
5.3 Policy Properties Tab

See Associating a Policy with Organizational Objects for a detailed description of this tab.

5.3.1.1 Ports Tab

Here you can define physical ports, wireless ports, approved WiFi networks and anti-hybrid network bridging. When you click the Ports tab, the following window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



5.3.1.2 Physical Ports

Here is where you set port permissions. For each Port Name (USB, FireWire, PCMCIA, secure digital, serial, parallel, modem, internal ports):

Option	Description
Security Actions	
Allow	This option specifies that the port can be used.
Block	This option means that no access can be performed through this port. The port is unavailable as if its wires were cut. When a port is blocked, you can specify that port initialization attempts be logged or that they trigger alerts.
Restrict	You have the option to specify that access to this port is restricted. A Restricted setting enables you to define more specifically which devices are allowed to access this port using the device tab of the policy.
Monitor Actions	
No Record	No log or alert will be generated.
Log	Enables defining whether port initialization and/or port activity are logged.
Alert	This enables you to specify whether alerts should be triggered for port events.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

5.3.1.3 Defining a physical port control

1. For each physical port you can define the *Security Action* or *Monitor Action* setting, or leave the default values.
2. For *Security Action*, choose either **Allow, Restrict** or **Block**.
3. For *Monitor Action*, choose either **No Record**, **Log** or **Alert**.

5.3.1.4 Wireless Ports

For each port WiFi, IrDA or Bluetooth you can specify the following for Security Action:

Option	Description
Allow	This option specifies that the port can be used for any purpose, without any restrictions on this communication channel.
Block	This option means that no access can be performed through this port. The port is unavailable, as if its wires were cut. When a port is blocked, you can specify that port initialization attempts be logged or that they trigger alerts.
Restrict (Available for WiFi ports only.)	You have the option to specify that access to ports of this type is restricted. A Restricted setting enables you to define more specifically (meaning with higher granularity) which connections are allowed to access the port using Advanced WiFi Settings.

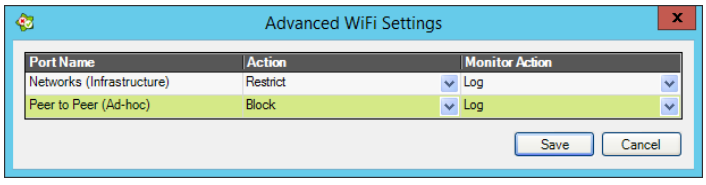
The Monitor Action options are the same as for Physical Ports.

Defining a wireless port control

1. For each Wireless Port, you can define the *Security Action* or *Monitor Action* setting, or leave the default values.
2. For *Security Action*, choose either **Allow**, **Block** or **Restrict**.
3. For *Monitor Action*, choose either **No Record, Log** or **Alert**.

Configuring advanced WiFi settings

1. Click Configure Advanced WiFi Settings (available only if the WiFi port is set to **Restrict**). The Advanced WiFi Settings window is displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. For *Act*ion, choose either **Allow** or **Restrict** and **for Monitor Action** choose either No Record, Log or Alert. Restricting networks enables you to define the specific WiFi networks which users can connect to, according to the network name, its MAC address and/or the network security settings.
3. For Peer to Peer for Action, choose either ***Allow*** or **Block** and for *Monitor Action* choose either ***No Record***, **Log** or **Alert.**

5.3.2 Approved WiFi Networks

If you chose to "restrict" WiFi networks, you can define here the specific WiFi networks which users can connect to, according to the network name, its MAC address and/or the network security settings.

1. Click **New** to add a new WiFi group. For more information, see Adding WiFi connections.
2. Click **Edit** to change the settings of a selected WiFi network. Click **Delete** to remove an existing WiFi network.

5.3.3 Anti-Hybrid Network Bridging

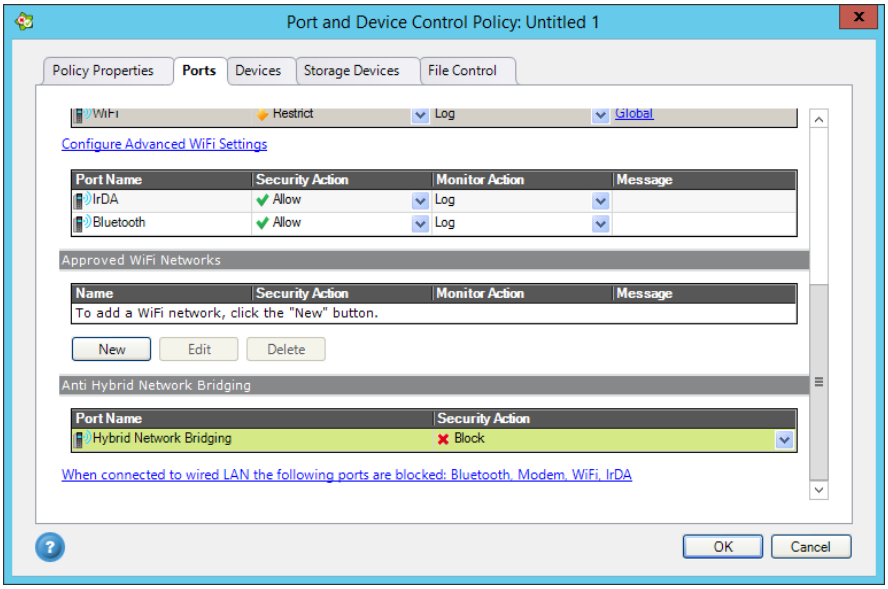
Safend Data Protection Suite allows administrators to control and prevent simultaneous use of various networking protocols that can lead to inadvertent or intentional hybrid network bridging (such as WiFi bridging and 3G card bridging). Configuring Safend Data Protection Suite Clients to block access to WiFi, Bluetooth, Modems or IrDA links, while the main wired TCP/IP network interface is connected to a network, enables users to employ certain networking protocols only when they are disconnected from the network, avoiding the creation and potential abuse of a hybrid network bridge.

For Hybrid Network Bridging, choose either **Allow** or **Block** for the Security Action.

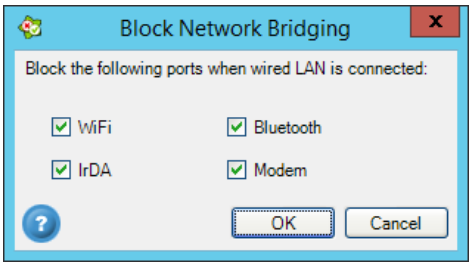
Blocking Network Bridging

The Block Network Bridging window is where you define which wireless ports should be blocked when the endpoint is connected to the wired LAN.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



1. Choose **Block** for the Security Action.
2. Click When connected to wired LAN the following ports are blocked: WiFi, IrDA, Bluetooth, Modem. The Block Network Bridging dialog box is displayed.



3. Leave checkboxes (WiFi, IrDA, Bluetooth and Modem) checked for those ports you wish to block, while connected to the wired LAN. Uncheck the checkboxes for the ports you wish to allow.

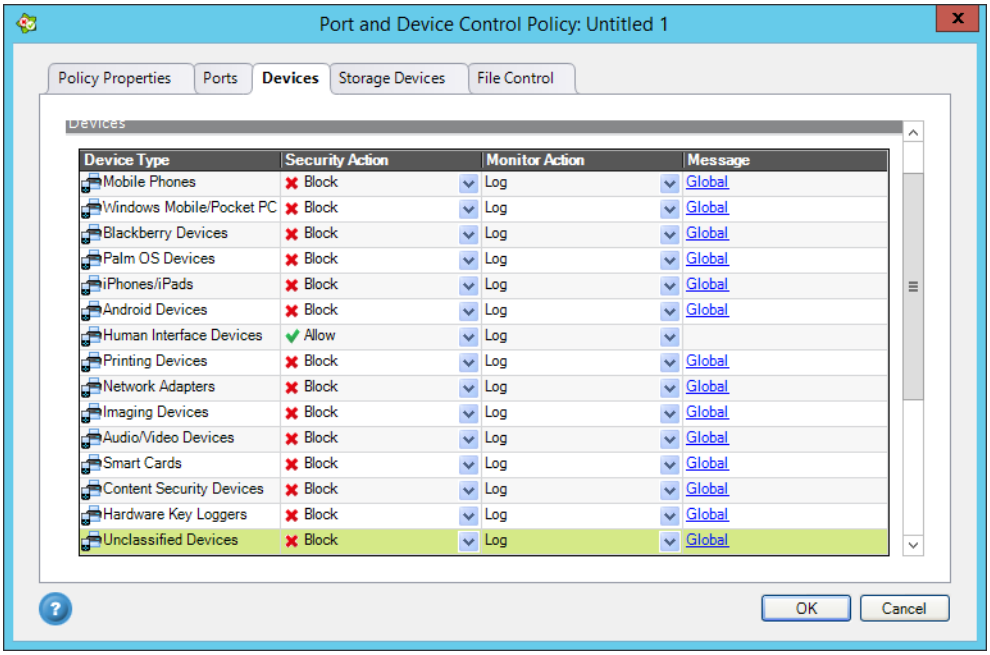
5.3.3.1 Devices Tab

This tab enables you to allow or restrict access to an endpoint according to the type of device that is connected. For example: Mobile Phones, Network Adapters, Human Interface devices (such as a mouse) or Imaging Devices. The device types available for selection are built into Safend Data Protection Suite.

The Device Control aspect of a policy is enforced for devices connected through physical ports that are restricted by policy. On a port that is Blocked, all devices are blocked, since blocking a port is similar to cutting its wires.

When you click the Devices tab, the following window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Devices

The Devices tab shows all the devices except storage devices.

Note: Content Security Devices include tokens and dongles used for software licensing.

If a device is not defined as allowed in one of the ways described below, then it is blocked.

Option	Description
Security	
Allow	Allows all storage devices of this type.
Block	All devices are blocked excluding storage devices and/or CD DVD media that you approve in the White List tab. White listed CD/DVD media are allowed Read Only access in any CD/DVD drive.
Monitor Action	
No Record	No log or alert is generated.
Log	This enables you to specify whether device usage is logged.
Alert	This enables you to specify whether alerts should be triggered for device usage.

Defining device settings

For each Device, you can define the Security Action and Monitoring Action, or leave the default values.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- For Security Action, choose either *Allow* or *Block.*
- For Monitoring Action, choose *No Record*, *Log* or *Alert*.

5.3.3.2 Device Whitelist

The Device Whitelist enables you to specify which device models or distinct devices are allowed access.

Adding a new group to the device whitelist

1. Click the **New** button. The *Select Device Type* dialog box is displayed.
2. Select the type of device and click **Next**.
3. The specific *Edit Group* dialog box will be displayed, to define further the specific group. For additional information see Approving Devices.
4. Click **Edit** to change the settings of a selected group. Click **Delete** to remove a selected group.

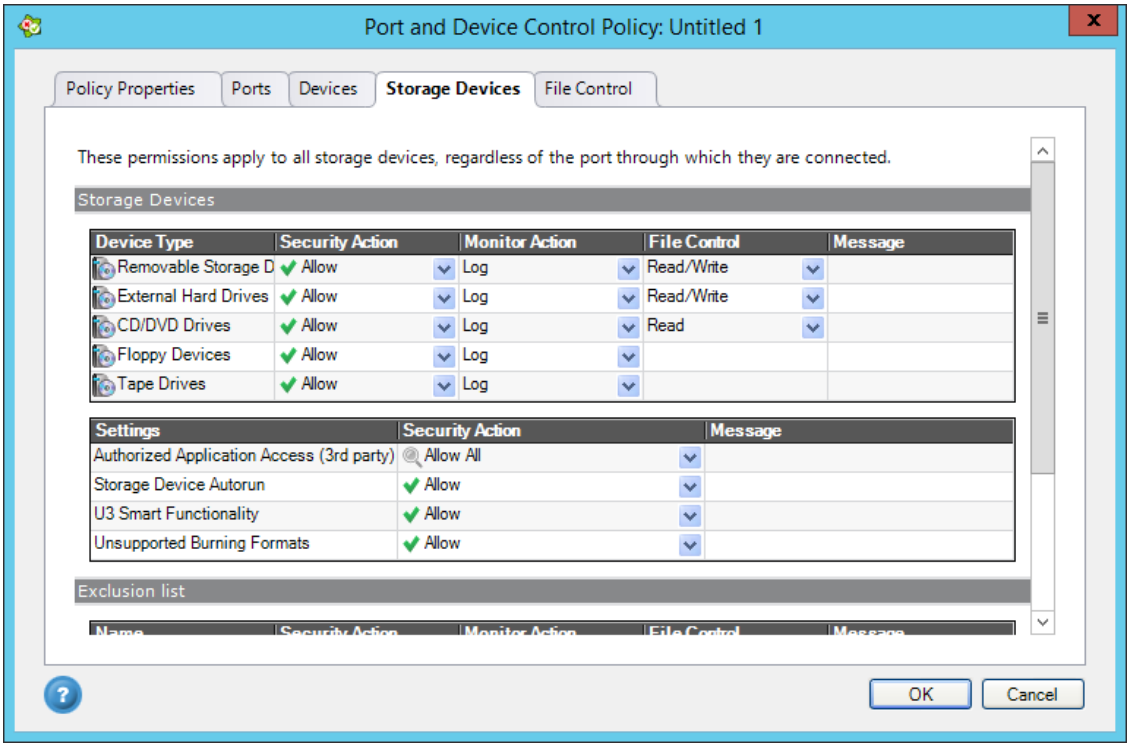
5.3.3.3 Storage Devices Tab

Storage devices may typically be the main conduits for information leakage in an organization. Safend Data Protection Suite enables you to control access by allowing full access, blocking or allowing Read Only access by any device that is identified as a storage device. This includes removable media such as USB flash drives, digital cameras and so on, as well as traditional devices, such as floppy drives, CD/DVD drives, external hard disks and tape drives. It also enables you to limit access to organizationally encrypted devices only.

The Storage Control aspect of a policy is enforced across all ports through which a storage device can connect. On a port that is Blocked all storage devices are blocked, since blocking a port is similar to cutting its wires.

When you click the Storage Devices tab, the following window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



5.3.3.4 Storage Devices

The available device types are: Removable Storage Devices, External Hard Drives, CD/DVD Drives, Floppy Devices, and Tape Drives.

The permissions apply to all storage devices, regardless of the port to which they are connected.

Option	Description
Security Action	
Allow	Allows all storage devices of this type.
Block	All devices are blocked, excluding storage devices that you approve in the White List tab.
Read Only	Allows only reading from the storage devices of this type, through unblocked ports. For CDs and DVDs, assigning Read Only means that they cannot be used for burning.
Encrypt	Access to this storage device type is allowed only if it is encrypted by the organization. If a non-encrypted device is connected, the end-user will be asked to encrypt it. If the end-user does not perform encryption, the device is blocked or set to read-only, depending on the definitions you have set. This type of permission is available for Removable Storage Devices, External Hard Disks and for a CD/DVD.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

	Note When setting the policy to require CD/DVD encryption, it is highly recommended to set "*unsupported burning formats*" to Block.
Monitor Action	
No Record	No log or alert is generated.
Log	This enables you to specify whether device usage is logged.
Alert	This enables you to specify whether alerts should be triggered for device usage.
File Control	
None	No file type control is applied.
Read	File type control settings apply to files read from storage devices.
Write	File type control settings apply to files written to storage devices.
Read/Write	File type control settings apply to files written to or read from storage devices.

Note: File Type Control, controls and monitors files transferred to/from removable storage devices only according to the file type, regardless of its content. To apply a more granular policy on files transferred to removable storage devices according to their data classification, based on the file content, please use Data Control Security Policies. In order not to use file control, choose *None*.

Defining storage device settings

1. For each Storage *Device Type*, you can define the *Security Action*, *Monitor Action* and in some cases the *File Control*, or leave the default values.
2. For *Security Action*, choose either **Allow**, **Block**, **Read only**, or **Encrypt**.
3. For *Monitor Action*, choose either **No Record**, **Log** or **Alert**.
4. For *File Control*, where applicable, choose either **None**, **Read**, **Write**, **Read/Write**.

5.3.3.5 Storage Settings

The Storage Control aspect of the policy allows you to define additional aspects of storage device behavior and storage control:

Device Virus Scan (Third Party): You can enforce a virus scan on encrypted storage devices which were used outside the protected organization to safely re-introduce them back into the

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

organization. This is in order to eliminate a virus threat being introduced into the organization, via removable storage devices. See *Device Virus Scan (Third Party)* for more information.

Storage Device Autorun: use this option to either Allow or Block CD/DVD devices from automatically launching applications after they are inserted into the machine.

U3 Smart Functionality: Certain Disk on Key devices, such as U3 devices, offer smart functionality in addition to their basic storage functionality. This functionality allows them to store and run applications once connected to a host computer. You may wish to limit these devices to their storage functionality only, and block the applications they carry. Do this by selecting Block for U3 Smart Functionality. Choose Allow to permit this functionality.

Unsupported Burning Formats: When writing to a CD/DVD, Safend Data Protection Suite can monitor burning processes that meet the following three conditions:

- The burning method is Track At Once.
- The file system is ISO-based (i.e., ISO, ISO+JOILET, ISO+UDF).
- This is the first writing session to this CD.

Burning actions that do not meet all three conditions will not be logged, and the Safend Data Protection Suite cannot verify that encryption is used if encryption is required by policy.

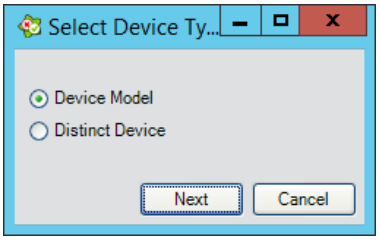
The writing of files to a CD/DVD that cannot be controlled or monitored by the Safend Data Protection Suite is blocked by default. A message is displayed to the end-user when she/he attempts to write an unsupported format.

If you wish to allow the writing of these files, set Unsupported Burning Formats to Allow.

5.3.3.6 Storage Exclusion list

The Storage Exclusion list enables you to specify a storage list with one or more device models or distinct devices that will be affected by one of the chosen Security Actions: Allow, Block, Read Only, Encrypt.

1. Click the **New** button. The *Select Device Type* dialog box is displayed.



2. Select the type of device and click **Next**. The specific Edit Group type di**alog** box is displayed, allowing definition of the specific group. See *Approving Devices more information.*
3. *Click **Edit** to change th*e settings of a selected group. Click **Delete** to remove a selected group.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

5.3.3.7 Device Virus Scan (Third Party)

The Device Virus Scan is conducted using the antivirus software installed on the endpoint. The client must have an approved antivirus program in order for the virus scan to function and integration is required to support the antivirus software. Contact Safend Support for more information.

Using Safend Data Protection Suite, security administrators can force a virus scan on removable storage devices used in the organization. The virus scan is conducted after the device is inserted by the end user but before the user is allowed to access the device, thus making sure the machine will not be infected before the virus scan is concluded.

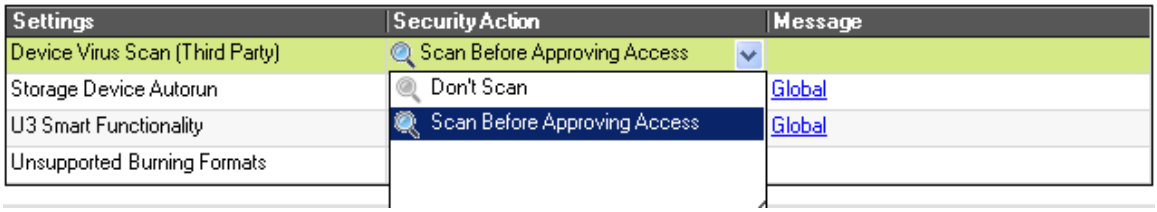
Non-encrypted removable storage devices will be scanned for viruses each time they are connected to a machine inside the protected organization. However, encrypted storage devices will only be scanned for viruses after they were used on an unprotected machine outside the organization using the Device Access Utility, in order to minimize the impact on end users in the organization.

The Security administrator can require all users to perform a "re-introduction" of encrypted devices that were used outside the organization on protected machines by running a virus scan, or limit "re-introduction" permissions to specific, trusted users. In this way, security administrators can determine that the "re-introduction" of devices which were used outside the protected organization will only be performed on specific, designated machines which are properly segmented from other machines inside the network.

Note: A virus scan only takes place in the case when the storage devices are permitted by policy settings.

Setting an automatic virus scan

When the device virus scan license is activated, this component will be displayed under Settings in the Storage Devices tab in the Port and Device Control Policy window.



Select Scan Before Approving Access, for Security Action, in order to activate this component. See ***Error! Reference source not found.*** for additional information.

5.3.3.8 File Control Tab

File Control applies to files written to or read from the following external storage devices: removable storage devices, external hard disks and CD/DVD drives (in the case of CD/DVD, File Control can be applied to files read from – but not to files written to – the device).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Safend Data Protection Suite allows you to set permissions not only for storage devices, but also for the files transferred to and from these devices. This is achieved 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.

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 to prevent data leakage.
- Prevention of the introduction of viruses/malware via external storage devices.
- Prevention of the introduction of inappropriate content, via external storage devices, e.g., unlicensed software, unlicensed content (e.g., music and movies), non-work-related content such as private pictures, etc.

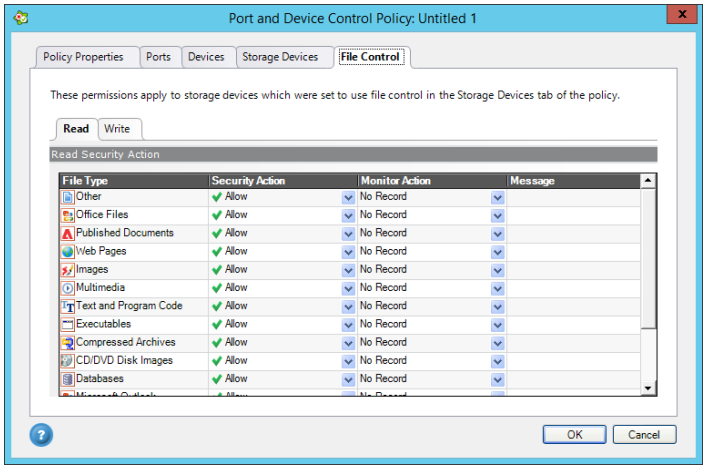
With this feature, you can define policies which approve/block specific file types on the inbound and outbound channels. This includes separate definitions for the inbound and outbound channels.

File Control is applicable to removable storage devices, external hard disks and CD/DVD media.

Note: File Type Control, controls and monitors files transferred to/from removable storage devices only according to the file type, regardless of its content. To apply a more granular policy on files transferred to removable storage devices according to their data classification, based on the file content, please use Data Control Security Policies.

Displaying the File Control tab

Click the File Control tab to view the file control options. The following window is displayed.



The File Control window includes two tabs, described below: Read, which you use to specify permissions for file types read from storage devices, and Write which you use to specify permissions for file types written to storage devices. In this window you also specify for each file type, whether you wish to log or trigger alerts relating to files of each type.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
File Type	
Allow	This allows writing files of this type without restriction.
Allow and Shadow	This allows writing files of this type, while making a copy of each file that is moved to/from external storage devices. File Shadowing is the ability to track and collect copies of the actual files that have been moved to/from external storage devices. Tip: Use this option with caution because it may influence both network utilization and storage resources. Preferably, you should initially apply it to small, well defined parts of your organization.
Block	This blocks writing files of this type.
Log Settings	
No Record	No logs or alerts are generated.
Log	If you want writing activities to be logged. If Log is checked, logs are created for each file, which can be viewed in Data Logs in the Logs Tab.
Alert	This triggers an alert.

Defining File Control write settings

1. Click **Write**. In the first column is a list of supported file types.
2. For each file type you must select a Security Action: *Allow*, *Allow and Shadow* or *Block*.
3. For Monitor Action, select **No Record, Log** or **Alert**.

Defining File Control read settings

1. Click **Read**. In the first column is a list of supported file types.
2. For each file type you must select a Security Action: **Allow, Allow and Shadow** or **Block**.
3. For Monitor Action, select **No Record, Log** or **Alert**.

Notes:

Once Safend Data Protection Suite has logged transfer of a file to or from a specific device, it does not log it again unless one of the following conditions is met:

an hour has passed since the previous logging the computer has been restarted the device has been reconnected. This is done in order to avoid multiple log records from being written when

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

the same file is repeatedly written to the same device, such as when the end-user edits a file on a storage device and repeatedly saves it.

Logging files read from devices may produce an excessive number of log records during procedures such as software installations.

5.4 Approving Devices

The following sections explain adding approved devices to the Device Whitelist (see Device Whitelist) and adding approved storage devices to the Storage Exclusion list (see Storage Exclusion list). When differences exist between adding storage and non-storage devices, they are explained.

Permissions	Description
Device Types and Storage Types	This option, explained above, enables you to allow or restrict access to an endpoint according to the type of device that is connected. For example: Removable Media, Network Adapters, Human Interface devices (such as a mouse) or Imaging Devices. The device types and storage types available for selection are built into Safend Data Protection Suite and are found in the Devices and Storage Devices tabs of the Port and Device Control Policies window. See *Devices Tab* and Storage Devices Tab for more information.
Approved Models	This option refers to approving models of devices or storage devices, such as all HP printers or all San Disk USB flash drives.
Approved Distinct Devices	This option refers to approving distinct devices or storage devices, each with its own unique serial number, meaning each is an actual specific device. For example, if you wish to approve the use of the CEO's USB flash drive and block all other USB flash drive devices, you should set the Removable Media storage type to Block, and then enter the identifying parameters of the CEO's USB in a specific distinct device group.

This section describes how to add approved models or distinct devices, either from the list of devices whose usage was detected in your organization by Safend Auditor using the Add Approved Device wizard (see Adding a Device Using the Wizard), or manually.

The process of adding approved devices to the white list consists of the following steps:

1. Adding a device group.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

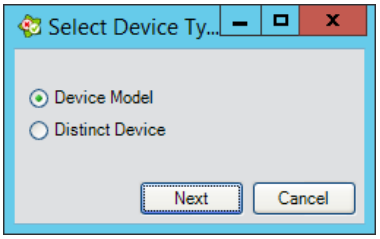
2. Adding models and distinct devices to the device group, either via the wizard or manually (copying device information from logs, or copying devices from the device inventory report).
3. Adding additional group settings (such as log and alert settings).
4. Saving the policy.

5.4.1 Adding Device Groups

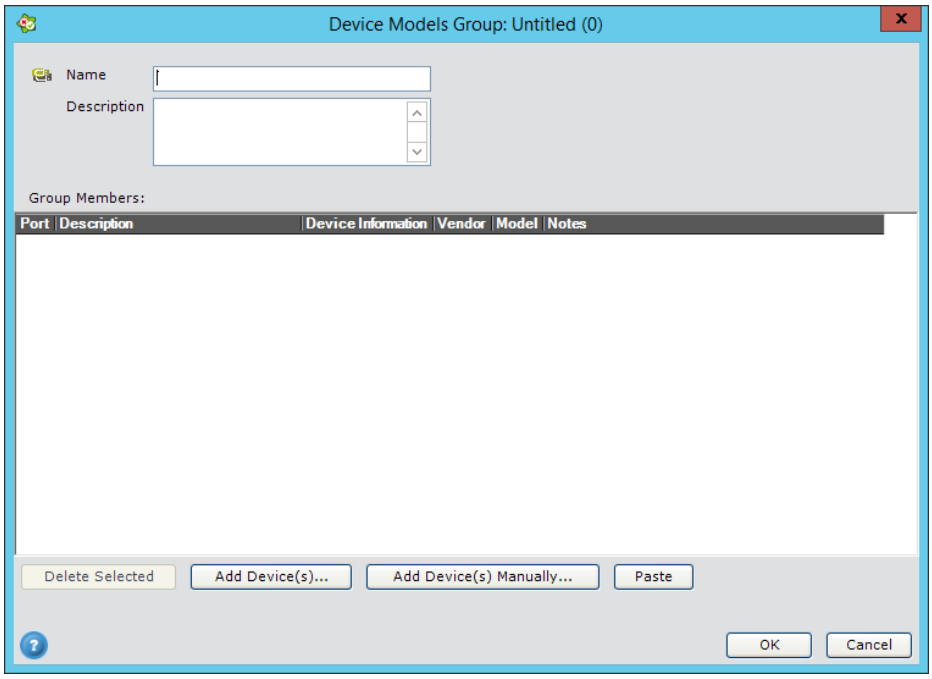
Approved models and distinct devices are arranged in groups so as to make it easier for you to manage related, same-permission devices (for instance all the devices used by the marketing group). Before adding devices you must specify device groups. You may define groups of models or distinct devices, depending on your needs.

Adding a new group

1. In the *Devices* or *Storage Devices* tabs, click New either under Storage Whitelist or Device Whitelist. The Select Device Type dialog box is displayed.



2. Select Device Model and click Next. The Device Models Group window is displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Field	Description
Name	Enter the name of the group.
Description	Add a description about the group.
Group Members	This lists all the group members that have been added. The following details are listed: Port (USB, FireWire, PCMCIA), Description (e.g., Aladdin USB Key), Device Information (e.g., HASP4 USB 1.30), Vendor (e.g., 0529), Model (e.g., 0001) and Notes if they exist.
Delete Selected	Deletes a group selected in Group Members list.
Add Device(s)	Click this in order to add a model using the wizard. See Adding a Device Using the Wizard.
Add Device(s) Manually	Click this in order to add a model manually the Add Device Model dialog box opens.
Paste	Click this in order to paste a group from the clipboard. For example, copying device information from logs, or copying devices from the device inventory report.

5.4.2 Adding a Device Using the Wizard

Once you have defined device groups, the Add Approved Storage Device Wizard is provided to walk you through the stages of adding approved devices from a list of the devices previously detected on the computers in your network by Safend Auditor. You can also add devices manually, as explained in Adding Approved Devices Manually.

The Add Approved Storage Device Wizard is comprised of three steps:

> Step 1: Get Device Information

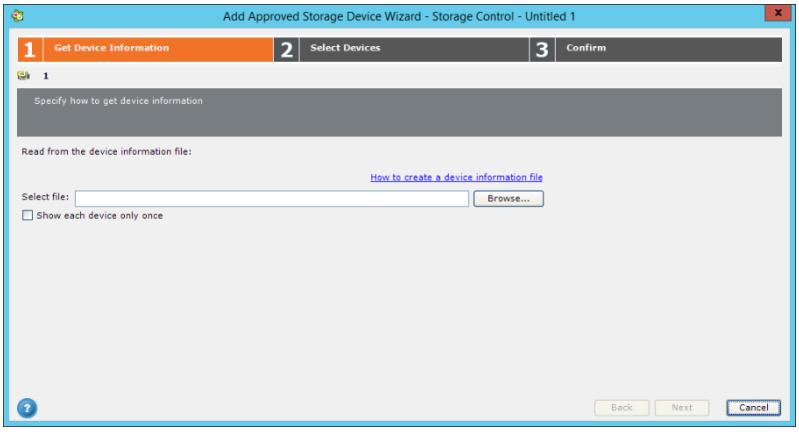
> Step 2: Select Devices

> Step 3: Confirm

5.4.2.1 Step 1: Get Device Information

When you click Add Device(s) in the Device Models Group window or when you select Add Device(s) Wizard from the right-click menu, the Add Approved Storage Device Wizard opens.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This step enables you to specify the file from which to gather the information about devices which will be added to the group, meaning the location of the Safend Auditor .XML file that contains the required device information.

Creating a Device Information File

In order to create a file that contains the information about the devices you wish to approve, use Safend Auditor to scan the required computers. Safend Auditor scans the selected computers and reports on all devices and WiFi networks currently or previously connected to those computers. The audit results are stored in an XML file. To learn about Safend Auditor refer to the Safend Auditor 3.4 User Guide.

Once you select the file using Browse..., click Next to continue to step 2.

5.4.2.2 Step 2: Select Devices

The table is divided into categories, depending on whether the group to which you are adding devices is an Approved Models group or a Distinct Devices group, and whether you are adding storage devices or non-storage devices.

Selectable devices have a checkbox beside them which you should check if you want to approve the device model or the distinct device, as the case may be. Devices that already belong to the current group are highlighted in gray, and the checkbox beside them is checked.

Note: You cannot add storage devices to the *Device* Whitelist. You cannot add devices or storage devices without a distinct ID to a Distinct Devices group.

Occasionally, a device may not be identified as a storage device by Safend Auditor. This may happen, for example, when a device class has not been embedded by the manufacturer. In this case, if you know that it is in fact storage, you may add it to your policy's storage white list. You must avoid adding storage devices to a *Device Whitelist* or adding non-storage devices to a *Storage Whitelist*, since they will be ignored by the Safend Data Protection Suite Client.

Important : When you add a device that already belongs to another device group in this policy, and the groups' permissions differ, the most permissive will apply. For example, if the Approved Models group that contains a storage device is set to **Allowed**, and the distinct device is set to

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Read Only, the **Allowed** permission will apply. Log and Alert settings will also be taken from the most permissive definition.

In cases where a device belongs to more than one group, and those groups have the same permissions, Safend Data Protection Suite will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply. Once you have selected the devices you want to add to the group click Next to continue to step 3.

5.4.2.3 Step 3: Confirm

This is where you confirm your selection and review the group with its newly added devices. To confirm your selection, click Finish, or click Back to return to the previous stage.

Adding Approved Devices Manually

You may want to add devices manually (not via the Add Approved Device Wizard), as in the case of devices that have not been connected to any endpoint in your organization and therefore do not appear in the Safend Auditor audit results or logs. Depending on whether you are adding an Approved Model or a Distinct Device, the Add Device Model or Add Distinct Device dialog box opens when you click Add Device(s) Manually in the Device Models Group and Distinct Devices Group windows or when you select Add Device Manually from the right-click menu described in Adding Devices above.

The instructions that follow apply both when adding storage devices (see Storage) and when adding non-storage devices (see Device Whitelist).

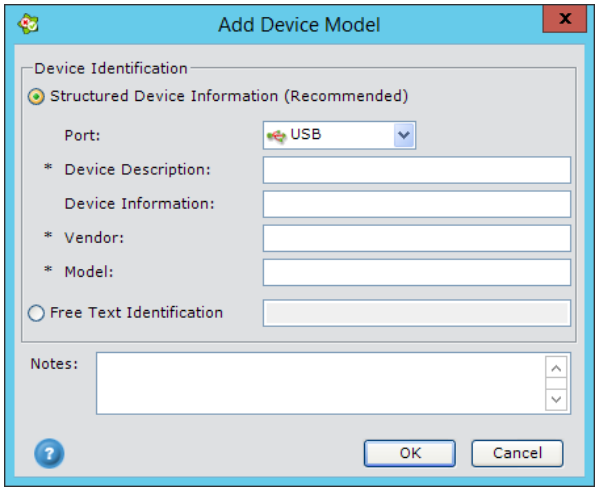
Important: When you add a device that already belongs to another device group in this policy, and the groups' permissions differ, the most permissive will apply. For example, if the Approved Models group that contains a storage device is set to **Allowed**, and the distinct device is set to **Read Only**, the **Allowed** permission will apply. Log and Alert settings will also be taken from the most permissive definition.

In cases where a device belongs to more than one group, and those groups have the same permissions, Safend Data Protection Suite will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

Adding a Device Manually

1. Click Add Device(s) Manually..., the Add Device Model window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Two options are provided for identifying the device:

Option	Description
Structured Device Information	Enables you to fill in fields that specify the information on the device that enables Safend Data Protection Suite to identify it, as described in the next section below. This is the recommended option. It is appropriate for the majority of devices, because it is based on common device information conventions that are used by most hardware vendors.
Free Text Identification	Enables you to enter free text to specify the information on the device that enables Safend Data Protection Suite to identify it. Only use this option if you cannot see the fields provided in the Structured Device Information option in the Safend Data Protection Suite.

2. In the Add Device Model window, enter the device model information as follows:

   i) Select the device identification method: Structured Information or Free text Identification.

   j) In the **Port** menu, select the port type, if you have chosen Structured Device Identification. **Note:** more than one option is available for FireWire and PCMCIA ports. If you are uncertain which port option is correct, check the Windows Device Manager or Safend Auditor scan results.

   k) Enter the required information in the following fields:

      i. Device Description (required)

      ii. Device Information (optional)

      iii. Vendor (Vendor ID) (required)

      iv. Model (Product ID) (required).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Note: Vendor ID (VID) and Product ID (PID) can be found in Safend Auditor scan results, on a sticker attached to the product itself or in Windows Device Manager.

a) Only use the Free Text Identification option when the Vendor and Model fields are empty in the logs generated by the device you wish to white list. In the Free Text Identification field, you can enter your device's Hardware ID.

Note: Hardware ID can be found in the Device Manager - Details tab.

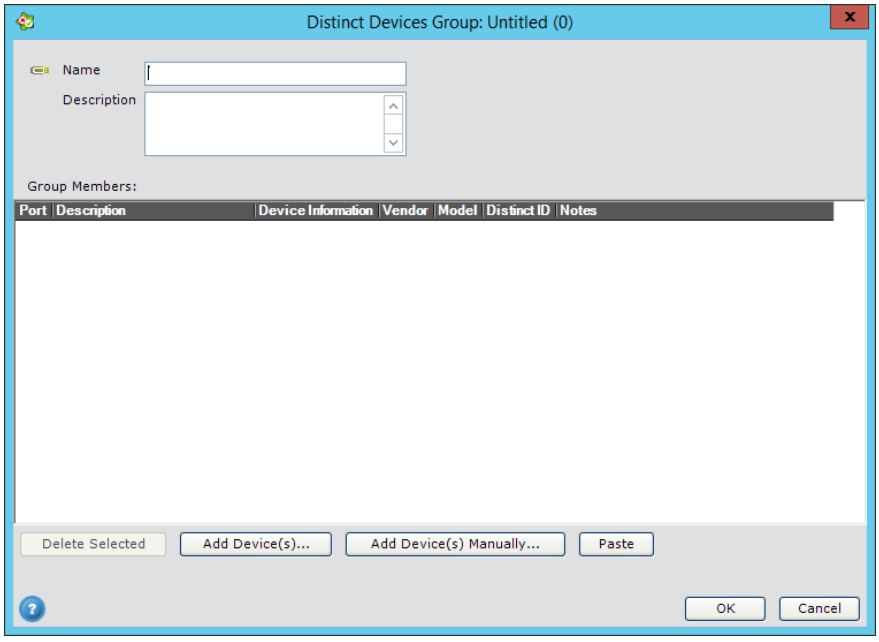
b) Enter Notes, this is optional.

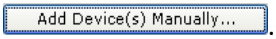
c) Double check that you have entered the correct data in all the fields and click OK.

Adding a Distinct Device

This option refers to approving distinct devices or storage devices, each with its own unique serial number, meaning each is an actual specific device.

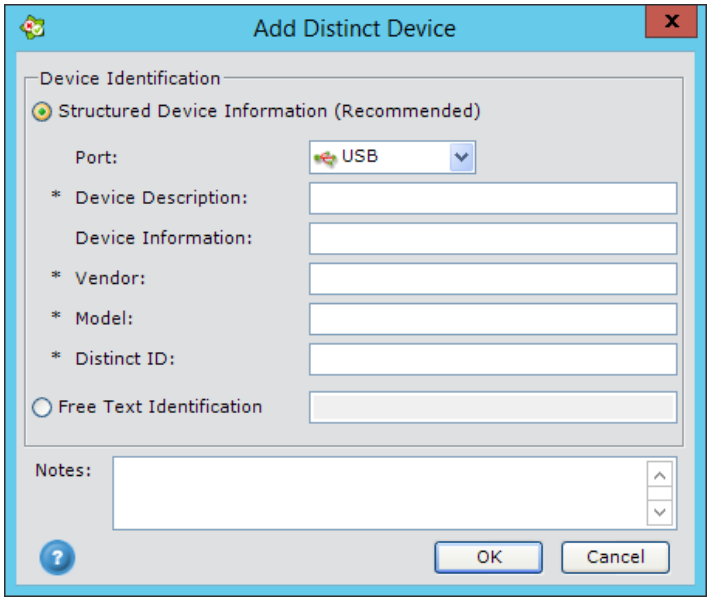
1. When you choose **Distinct Device** in Select Device Type dialog box, the following window is displayed.



2. Click 

. The Add Distinct Device window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



3. This window is the same as the Add Device Model window except that it includes an additional required field, **Distinct ID**. For a full explanation, see *Adding Approved Devices Manually*.

5.4.2.4 Additional Device Group Settings

Once you have added the desired devices to a group, you need to define a few more settings:

> Security Action

> Monitor Action (Log/Alert)

> File Control (storage devices only).

Setting security actions

In the group's Security Action, for Storage Devices select whether the group's permission is Block (✖), Allow (✔), Encrypt (🔒) or Read Only (📄). For Devices you only can select Allow or Block.

Defining log and alert settings

For each group, in Monitor Action choose No Record, Log or Alert as required.

Defining file control (storage devices only)

For each group, in File Control choose, None, Read, Write or Read/Write.

Adding WiFi connections

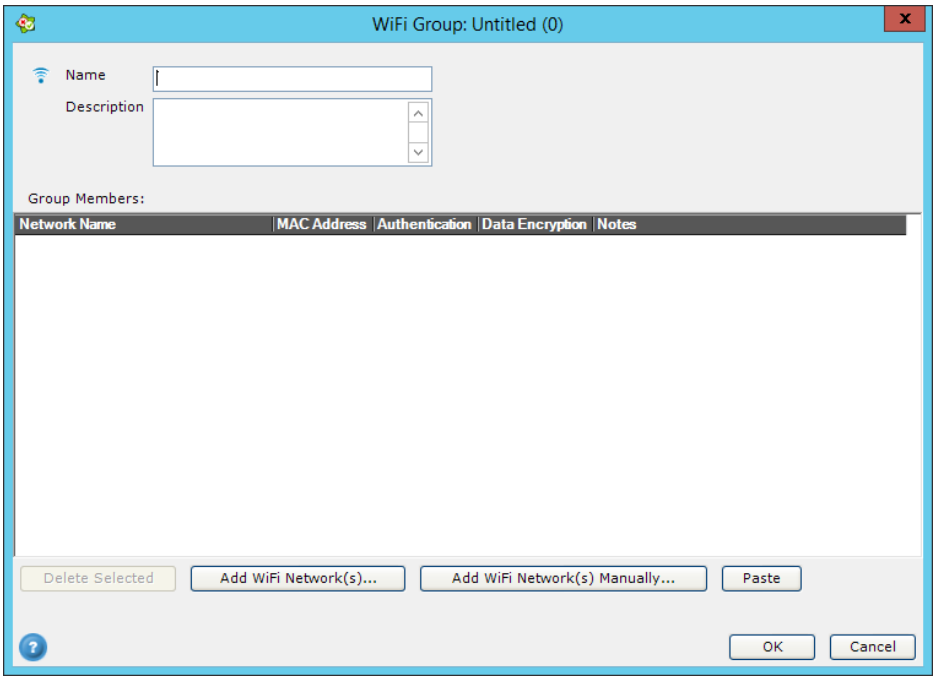
See Approved WiFi Networks for additional information.

WiFi links are added to the WiFi Control white list in much the same way this is done in the case of devices; adding WiFi groups, then adding approved links to these groups using the Add Approved WiFi Wizard, or manually (copying device information from logs, or copying devices from the device inventory report).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Adding approved WiFi links

1. Click the **Policies** tab.
2. Click **Port and Device Control** in the left pane and then select **Security Policy**. The *Port and Device Control/Security Policy* window is displayed.
3. Click **New**, or select a Custom Policy, right click on the mouse and choose either **Edit** or **New**.
4. Click the **Ports** tab.
5. Under **Wireless Ports** make sure WiFi Security Action is set to **Restrict.**
6. Under Approved WiFi Networks, click **New**. The WiFi Group window is displayed. If this option is not displayed, see *Approved* WiFi Networks and read the section before it, *To configure advanced WiFi settings*.



With the exception of adding WiFi links manually, simply follow the instructions provided for adding devices, as follows:

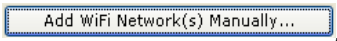
a) Adding Device Groups (no Select Device Type dialog box is displayed)

b) Adding a Device Using the Wizard

c) Additional Device Group Settings.

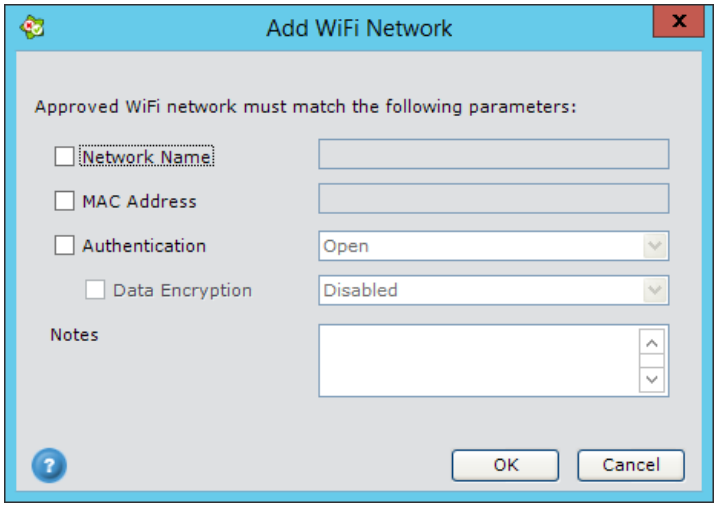
Adding a WiFi link manually

WiFi links that were not detected by Safend Auditor, and as a result cannot be added using the wizard, can be done manually.

1. Click 

, the following window opens:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



In this window you define the parameters a network must match in order for it to be approved for connection. You can identify a network by one or more of the following: its name, its MAC address or its authentication type.

2. After you enter a network authentication type, you can also specify data encryption parameters which must be matched. Only networks matching all the parameters are approved.

3. In the Add WiFi Network window, enter the network information as follows:

Adding a WiFi link manually

1. In the *Add WiFi Network* window, check one or more of the following: **Network Name**, **MAC Address** or **Authentication**.

2. If you have checked **Network Name**, enter the name and continue.

3. If you have checked **MAC Address**, enter the address and continue.

4. If you have checked **Authentication**, choose the authentication type from the menu. You may want to also define the **Data Encryption**.

   Note: The *Data Encryption* options available in the menu depend on the selected *Authentication* type. For example, for WPA authentication, the encryption options are TKIP or AES, whereas in the case of 802.1X authentication only WEP encryption is available for selection.

5. Add **Notes** (optional).

6. Double-check that you have entered the correct data in all the fields and click **OK**.

Deleting a device or WiFi group

1. In the Approved WiFi Networks list, in the Ports tab**,** right-click the group you want to delete.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. From the mouse right click menu, choose **Delete**. A confirmation window opens. Click **Yes** to delete the group.

Alternatively:

3. Select the group you wish to delete.
4. Click the **Delete** button.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

6 Hard Disk Encryption Policies

A Hard Disk Encryption Policy defines whether the data on the machine should or should not be encrypted. Safend Encryptor enforces an enterprise wide policy which protects the data stored on PC and laptop hard drives, so that sensitive data cannot be read by unauthorized users in the case of loss or theft.

Applying Hard Disk Encryption is performed with a few simple steps, described below. The encryption process is completely transparent to both end users and security administrators.

Note: After creating a new Hard Disk Encryption Policy, the new policy will take effect the next time a user logs in.

6.1 Hard Disk Encryption Process

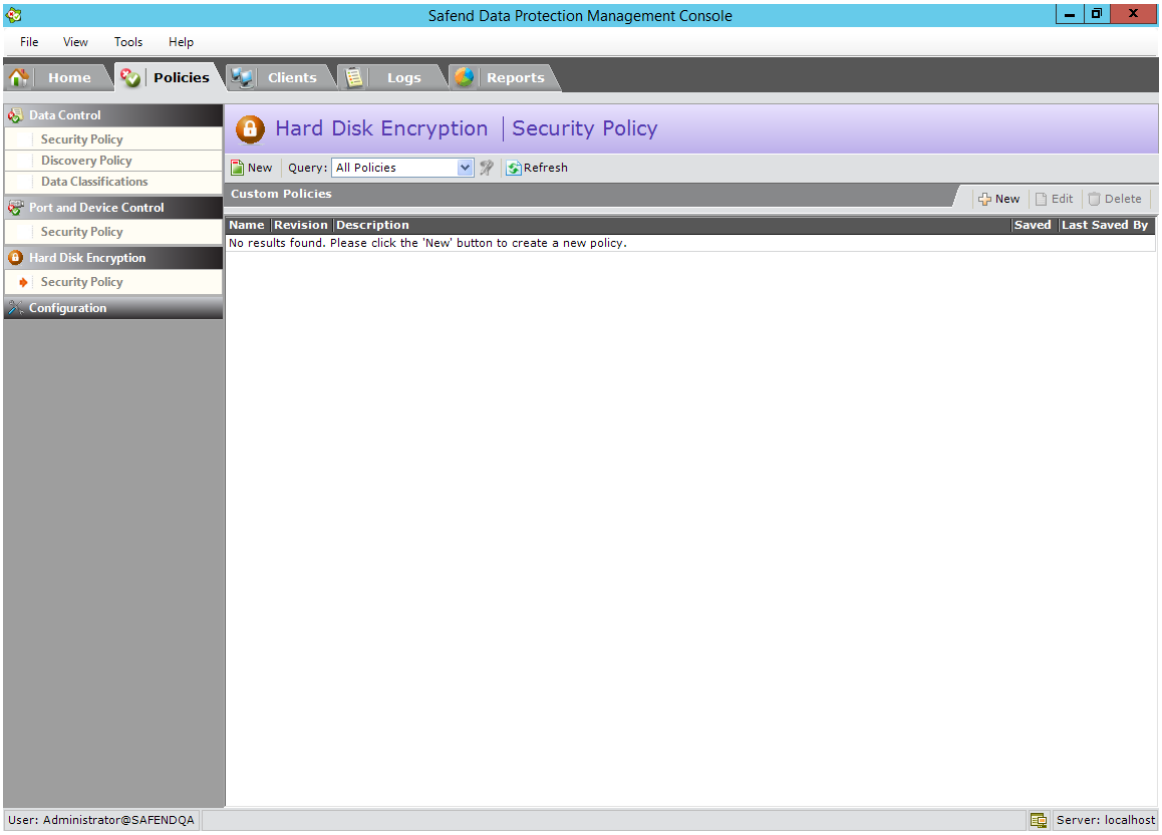
Here is a description of the Safend Encryptor encryption flow:

1. After setting the *Internal Hard Disk Encryption* to **Encrypt** the encryption policy will apply to all computers associated with the security policy.
2. Once the policy is updated on the agent, the system automatically conducts machines and user authentication. This phase is comprised of two steps:
    a) **Machine registration** – makes sure that the machine is listed only once in the domain computer list.
    b) **User authentication** – ensures that the currently logged on user is a valid domain or local user, which will be able to access the encrypted data.
3. The Safend Server creates encryption keys and securely distributes them to the agent.
4. The encryption process begins automatically. This process runs in the background, and therefore does not require any user action, and the user can continue working normally. The user can shut down or restart the endpoint during the encryption process; encryption will resume the next time the computer is powered on. The encryption status and progress is continuously updated on the Management Server, and can be viewed in the Clients Tab.
5. The machine is now protected, and secure data will not be compromised in case the computer is lost or stolen. Security administrators can view the current encryption status of organizational endpoints either through the Clients Tab or with the Safend Reporter add-on, by running the Encryption Status Report.

6.2 Quick Tour of the Hard Disk Encryption Window

Click the Policies tab. Click Hard Disk Encryption in the left pane and then select Security Policy. The Hard Disk Encryption/Security Policy window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Workspace

This window consists of Custom Policies. Custom Policies are policies that are created by the user.

Menus

Option	Description
Right-click Custom Policies	
Delete	This removes the policy from the Custom Policy list.
Edit	This enables you to edit the policy.
Export	This enables you to export the policy. It opens Save Export Result As.
New	Enables you to create a new policy.

Toolbar

Button	Description
New	This enables you to create a new security policy.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Refresh	This refreshes what is displayed on the screen.
Custom Policies Buttons	
New	This enables you to create a new security policy.
Edit	This enables you to edit a security policy after selecting it.
Delete	This enables you to delete a security policy after selecting it.

6.2.1.1 Policy Properties Tab

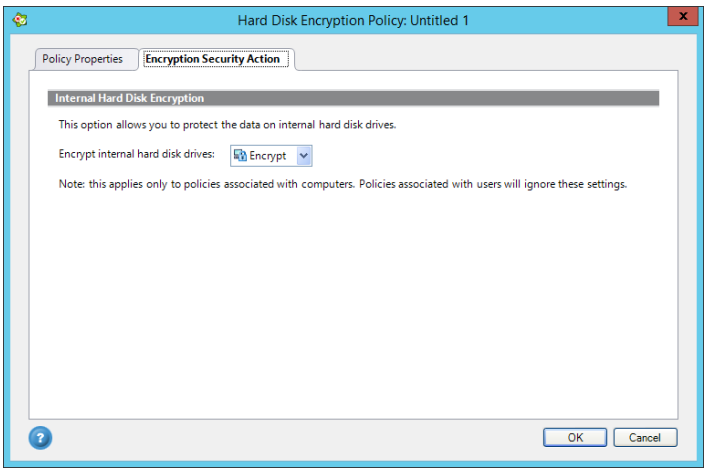
See Associating a Policy with Organizational Objects for a detailed description of this tab.

6.2.1.2 Encryption Security Action Tab

Internal hard disk encryption enables you to force encryption of a client's internal hard disks in order to protect the data on it, should it fall into the wrong hands. Access to encrypted computers is safeguarded by a Widows login password. This setting only applies to the machines with which the policy is associated and not to the users.

Setting the Encryption Security Action

In the Hard Disk Encryption/Security Policy window, click the New button. Click the Encryption Security Action tab. The following window is displayed.



The Internal Hard Disk Encryption option enables you to force encryption of a client's hard disk so that it cannot be accessed by anyone without a password.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

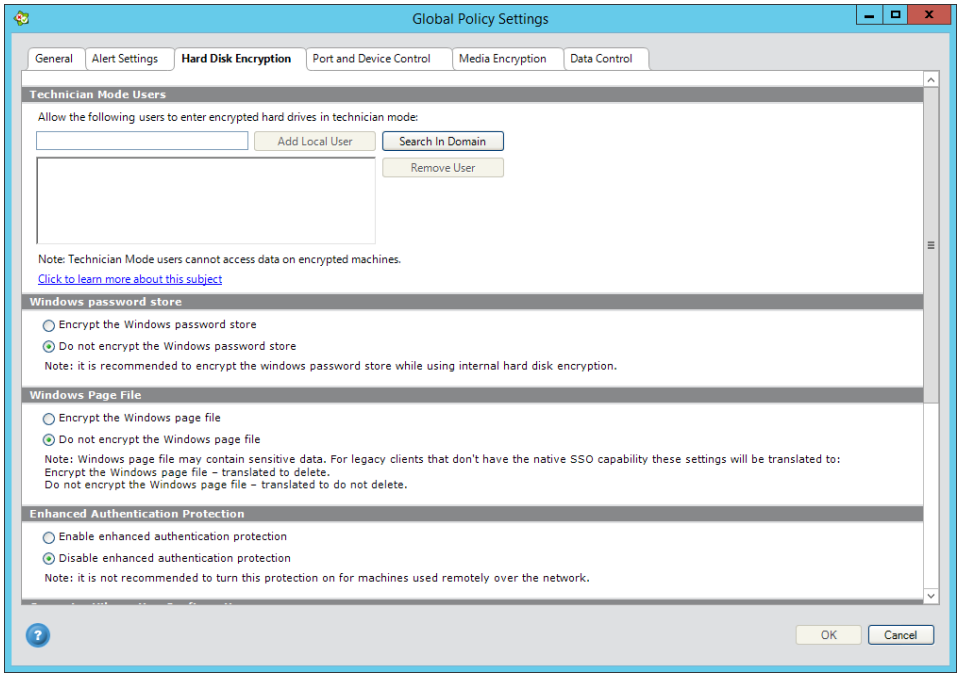
Choosing an internal hard disk encryption setting

In Encrypt internal hard disk drives, select either Decrypt or Encrypt to force encryption of a client's hard disk so that it cannot be accessed by anyone without a password.

Note: When there is more than one policy set on an endpoint, Decrypt takes precedence over Encypt.

6.2.1.3 Advanced Encryption Settings

To set the Advanced Encryption Settings, you must go to the Global Policy Settings window or Settings Policy in the Policy tab. In the Tools menu, choose Global Policy Settings. Click the Hard Disk Encryption tab. The following window is displayed.



Here you can select various advanced encryption security setting options.

Option	Description
Technician Mode Users	See Technician Mode Users for a description.
Windows password store	This gives you the option of whether or not to encrypt the password store for domain or local users.
Windows Page File	This enables you to choose whether or not to encrypt the windows page file.
Enhanced Authentication Protection	By enabling this setting, authentication will be performed each time you logoff/login. (The authentication token will be deleted during logoff.)

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Option	Description
Computer Hibernation Configuration	This enables you to choose whether or not to allow the hibernation function on endpoint computers. A Hibernation file may contain unencrypted sensitive information, so it is recommended to block hibernation while using Internal Hard Disk Encryption.
Local Users Check-In Support	Refer to Local Users Check-In Support for an explanation.
PKI Based Hard Disk Encryption User Authentication Support	This enables a user to securely authenticate to an encrypted endpoint using a Microsoft PKI-based two factor authentication device.

6.2.2 Technician Mode Users

This setting determines which local users or domain users can access encrypted machines in technician mode. Users in technician mode are able to access the system files of the encrypted machines without accessing the encrypted data.

6.2.2.1 Local Users Check-In Support

When local user check-in to an encrypted hard disk is supported, your password will be tested for password restriction compliance. If the password complies with the password restriction rules you will be authenticated/registered and will be able to access the encrypted data.

If the password does not comply with the password restriction rules, you will be logged in as a technician user and a warning message will be displayed informing you that this password does not comply with the password restriction rules, with instructions about how to amend the problem.

Choosing the Advanced Encryption Settings

1. For Technician Mode Users, Enter a user name in the text box.

   c) Click Add Local User if this user name is a local user defined on the encrypted machines.

   d) Click Search In Domain if this user name is a domain user name.

   e) Click Remove User to remove one of the users you have added.

   Note: Allowing users access in technician mode will cause their personal profile not to be encrypted (in order for them to be able to log in). Therefore, it is recommended to allow technician mode for special non-active users only.

2. For Windows Password Store, choose either Encrypt the Windows password store or Do not encrypt the Windows password store.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Note: It is recommended to encrypt the Windows Password Store when using Hard Disk encryption.

3. For Windows Page File, choose either Encrypt the Windows page file or Do not encrypt the Windows page file.

   Note: The Windows page file may contain sensitive data.

4. For Enhanced Authentication Protection, choose either Enable enhanced authentication protection or Disable enhanced authentication protection.

   Note: It is not recommended to turn this protection on for machines used remotely over the network.

5. For Computer Hibernation Configuration, choose either *Block Hibernation* or *Allow Hibernation*.

   Note: The hibernation file may contain sensitive data, so it is recommended to block hibernation while using internal hard disk encryption.

6. For Local Users Check-In Support, choose either Do not allow local user to check-in to an encrypted machine or Allow local user to check-in to an encrypted machine. (Refer to Local Users Check-In Support for more information.)

   Note: It is not recommended to allow local user to check-in to encrypted endpoints. Use this setting for non-domain environments only.

7. For PKI Based Hard Disk Encryption User Authentication Support, choose either Allow PKI Based Hard Disk Encryption User Authentication or Do not Allow PKI Based Hard Disk Encryption User Authentication.

   Note: PKI (Public Key Infrastructure) based user authentication, allows end users to be securely authenticated to an encrypted endpoint using a smart card or a USB token device.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7 Additional Configuration Settings

7.1 Global Policy Settings

Global policy settings are the default when policy-specific settings are not defined. Global settings can be modified and include general settings, log and alert definitions for events that are not policy-specific, hard disk encryption settings and port and device control settings.

Note: Modifying global policy settings is optional, and if you are only evaluating Safend Data Protection Suite at this point in time it is in fact unnecessary. Global Policy settings define the client technical configuration.

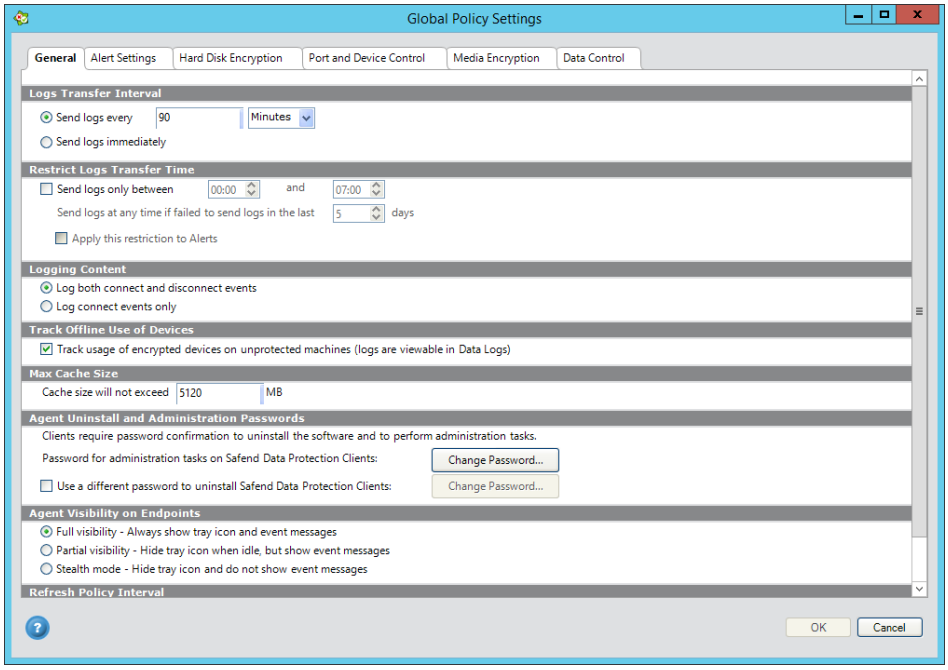
Tab	Description
General	This contains various general settings.
Alert Settings	This includes log and alert definitions for events that are not policy-specific, such as tampering attempts, policy updates, protection suspension on a Safend Data Protection Suite Client and more.
Hard Disk Encryption	This contains various advanced Hard Disk Encryption settings.
Port and Device Control	This contains the Disconnecting Active Devices option only.
Media Encryption	Encryption settings determine the system's behavior when removable storage device permissions are set to Encrypt.
Data Control	This enables you to define data sensitivity settings.

Accessing the Global Policy Settings

Global Policy Settings can be accessed from the Home Tab or from the Tools menu.

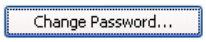
In the Home Tab in the more section click Change Global Policy Settings or in the Tools menu choose Global Policy Settings. The following window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Option	Description
Logs Transfer Interval	Choose either *Send Logs immediately* or *Send Logs Every* and choose the time interval (minutes, hours or days).
Restrict Logs Transfer Time	Leave as is, or select Send logs only between and fill in the time periods. For Send logs at any time if I failed to send logs in the last, choose the number of days. You can also choose to Apply this restriction to alerts.
Logging Content	Choose either, Log both connect and disconnect events or Log connect events only.
Track Offline Use of Devices	In order to track the use of devices, Choose Log offline activity of encrypted devices (logs are viewable in Data Logs).
Max Cache Size	You can choose the maximum value, *Cache size will not exceed* (1024 MB is the default value).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

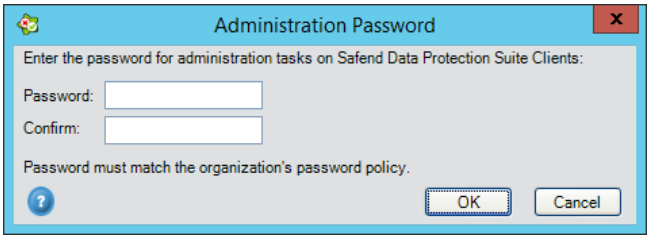
Option	Description
Agent Uninstall and Administration Passwords	Agents require password confirmation to uninstall the software and to perform administration tasks. Click  to change the password for administration tasks on Safend Data Protection Agents. Refer to *Changing an administration password* for more information. You also can choose to, Use a different password to uninstall Safend Data Protection Suite Clients. Click  beside it, to choose a password. Refer to Changing an agent uninstall password for more information.
Agent Visibility on Endpoints	Choose either: • Full visibility: Always show tray icon and event messages. In this case the end-user is always aware of Safend Data Protection Suite. This is the default mode. • Partial visibility: Hide tray icon when idle, but show event messages. In this mode the icon appears briefly when a device is connected and disappears afterwards. • Stealth mode: Hide tray icon and do not show event messages. In this mode, the end-user will never see the icon and also will never receive messages on blocked devices/ports. When using encryption in your organization, Stealth Mode should not be used in order to display the necessary messages when an unencrypted device is connected. Since removable media encryption requires end user interaction, enforcing removable media encryption or enabling device password protection on protected machines is not supported when the Safend Data Protection Agent is set to work in Stealth mode. However, devices which were already encrypted and do not require password protection on a protected machine, can be used in this mode.
Refresh Policy Interval	Set the interval for Clients to refresh a policy. Choose the time interval for *Check for updated policy every* (in seconds, minutes or hours).

Changing an administration password

This password is used to access the Administration section of the Safend Data Protection Agent. For trial versions the password is Password1 and cannot be changed. We recommend changing the administration password once you obtain your Safend Data Protection Suite license.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

1. Open Global Policy Settings (Tools>Global Policy Settings) and go to the *General* tab.
2. In the Agent Uninstall and Administration Passwords section, click Change Password... beside Password for Administration tasks on Safend Data Protection Clients. The Administration Password window is displayed.

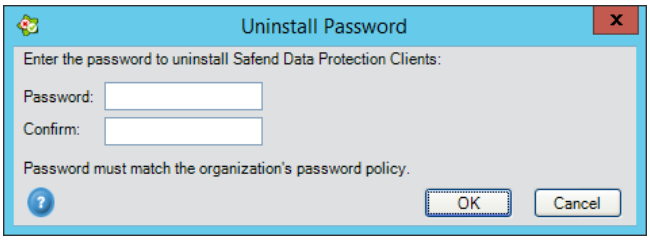


3. Enter the password in Password then enter it again in Confirm.
4. Click **OK** to save it or **Cancel** to exit.

Changing an agent uninstall password

Enter a password to uninstall the Safend Data Protection Agent.

1. Open Global Policy Settings (Tools>Global Policy Settings) and go to the *General* tab.
2. In the Agent Uninstall and Administration Passwords section, select Use a different Password to uninstall Safend Data Protection Clients.
3. Click Change Password... and the Uninstall Password window is displayed.

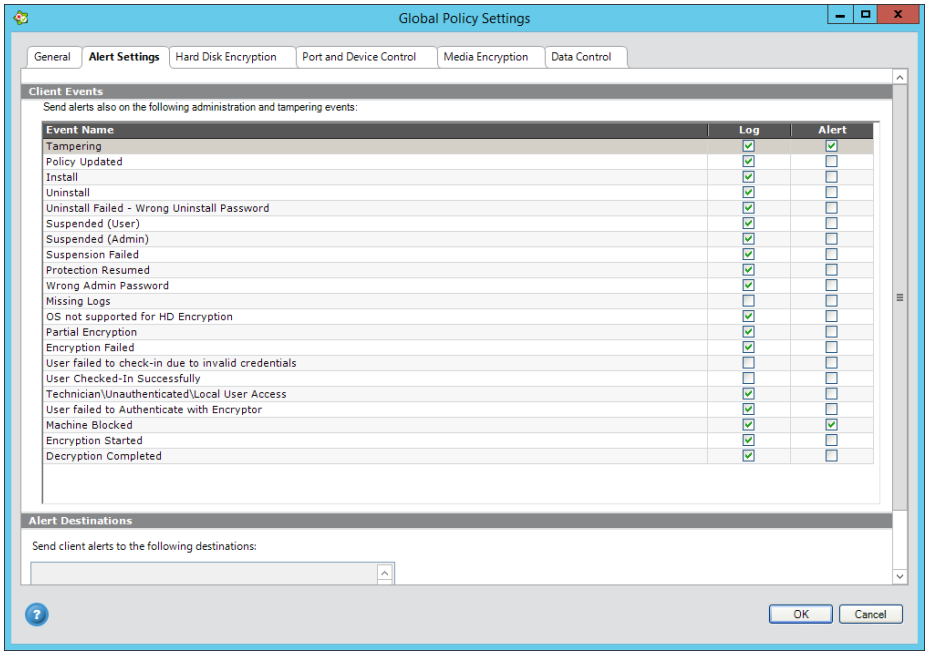


4. Enter the password in the Password field and again in the Confirm field.
5. Click **OK** to save it or Cancel to exit.

7.1.1.1 Alert Settings

Select the Client events about which you want to receive alerts or logs or both.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Event Name	Description
Tampering	This indicates a tampering attempt with Safend Data Protection Agent.
Policy Updated	This indicates that a security policy has been successfully updated on the endpoint.
Install	This indicates that a new Safend Data Protection Agent has been successfully installed.
Uninstall	This indicates that a Safend Data Protection Agent has been removed from an endpoint.
Uninstall Failed – Wrong Uninstall Password	This indicates that a wrong password has been supplied while removing the Safend Data Protection Agent.
Suspended (User)	This indicates that endpoint protection is suspended using a one time password.
Suspended (Admin)	This indicates endpoint protection is suspended using an administrator password.
Suspension Failed	This indicates that an attempt to suspend the endpoint protection has failed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Event Name	Description
Protection Resumed	This indicates that protection on an endpoint has been resumed, after it has been suspended.
Wrong Admin Password	This indicates that a user supplied an incorrect password, while trying to view the administration section on the endpoint.
Missing Logs	This indicates that some of the logs generated by endpoints are missing and did not reach the server.
OS not supported for HD Encryption	This indicates that hard disk encryption did not start on a specific machine, due to the fact that the machine OS is unsupported.
Partial Encryption	This indicates that the hard disk has been partially encrypted, meaning that the hard disk contains partitions that are unsupported for hard disk encryption (non NTFS).
Encryption Failed	This indicates that the hard disk encryption process has failed.
User failed to check in due to invalid credentials	This indicates that the hard disk encryption “check-in” process has failed due to invalid user credentials (username or password).
User Checked-In Successfully	This indicates that the hard disk encryption “check-in” process has been successful.
Technician\Unauthenticated\Local User Access	This indicates that an end-user performed logon using either technician user, unauthenticated user or local user.
User failed to Authenticate with Encryptor	This indicates that user authentication has failed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Event Name	Description
Machine Blocked	This indicates that a machine has been blocked. This could be due to the following reasons: Two encrypted machines had identical names (even momentarily). The agent has been uninstalled while not connected to the domain and had been re-installed later. A tampering attempt has been made (the encryption secrets have been copied from one machine to the machine that got blocked).
Encryption Started	This indicates that the hard disk encryption process has started.
Decryption Completed	This indicates that the hard disk has been decrypted successfully.

In Alert Destinations select which clients will receive alerts. See *Setting an Alert Destination* for further information.

7.1.1.2 Hard Disk Encryption

For a description of this tab see Advanced Encryption Settings.

7.1.1.3 Port and Device Control

This tab currently has one option: Disconnecting Active Devices. This refers to policy modifications and handling disconnected devices which are no longer approved. The options are:

> Gracefully: the active devices will not be disconnected immediately. This is the default.

> Forcefully: all the active devices will be disconnected immediately.

For more information, see Port and Device Control Policies.

7.1.1.4 Media Encryption

For a description of this tab see Media Encryption Tab.

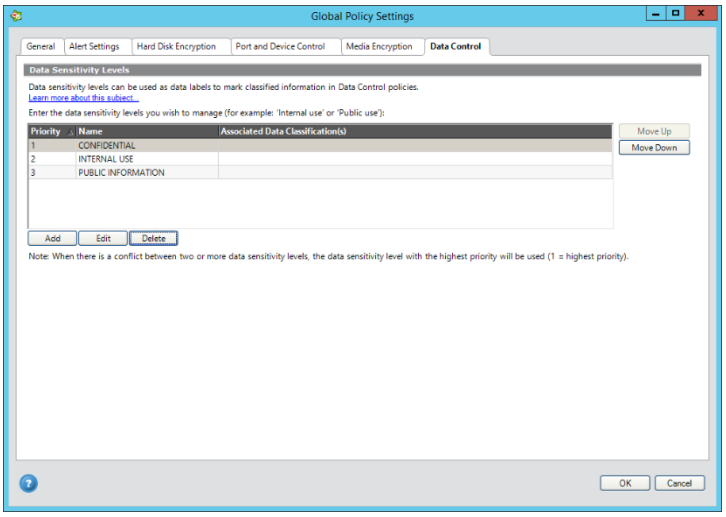
7.1.1.5 Data Control

This tab currently holds the Data Sensitivity Levels option which is used to configure data sensitivity levels for an organization. Data sensitivity levels define how an organization treats data whereas data classification describes the type of data that is being used.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

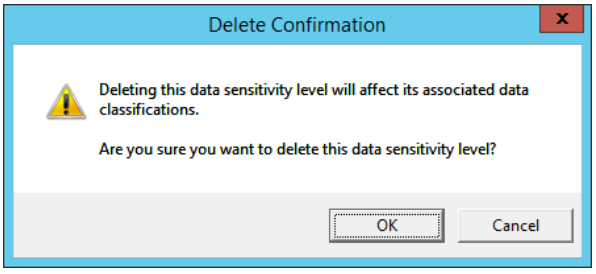
Each organization has its own data sensitivity levels which are based on the organization's business needs. For example, in a financial company it can be: normal/public/internal use, and in military organizations it can be for example: top secret/secret/confidential.

The Data Sensitivity levels you set can be used as data labels for email messages.



Column	Description
Priority	Lists the data sensitivity level (the highest level is 1). Priorities are used to determine the hierarchies of data sensitivities. The priority of the sensitivities can be changed by selecting a row and clicking either Move Up or Move Down.
Name	The name of the data sensitivity (e.g., Confidential).
Associated Data Classification(s)	Shows the data classifications names to which this data sensitivity level is associated.

1. To add a new data sensitivity to the list, click Add and enter the name. To change an existing data sensitivity name, select a row and click Edit.
2. To remove a data sensitivity level from the list, select a row and click Delete. When you go to delete a data sensitivity level the following message will be displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7.1.1.6 About Data Sensitivity

The Safend Data Protection Suite provides the ability to categorize corporate data using two key elements that enable organizations to protect their information. These elements are Data classification and Data sensitivity.

Data classification describes the category to which the data belongs, for example, medical information, personal information (PI), marketing or financial information. Each data classification contains a collection of various customizable Data Rules. Data rules are the building blocks of any data classification and are used to match and classify data according to different characteristics like specific keywords, numerical and alphabetical patterns, file properties (size, template, company, etc), file types, portions of a document (fingerprint), etc.

Data classifications are assigned with security policies to control information that matches the data classification's data rules. See *About Data Classification* for more information.

Data sensitivity presents the impact that data loss can cause to the business, for example, Public Information data sensitivity means that the data will not have any impact on the business in case the data is leaked, while Confidential data sensitivity indicates that loss of data will have serious impact on the organization. Data sensitivities are ordered by their severity, ensuring that data sensitivities with higher levels precede other data sensitivities with lower severity. While data classification answers the general question of "What is the data?, data sensitivity answers the specific question of "what is the business value of the data?".

Data sensitivities can be assigned to existing data classifications and add the "business value" dimension to the data classification. Organizations can raise data loss awareness among their users by defining data labels that will be added to outgoing data according to the data sensitivity.

7.1.1.7 Settings Policy

You can create a Settings Policy, configuring the same settings as are found in the Global Policy Settings window but for specific groups of machines.

1. In the Policies tab you choose **Configuration/Settings Policy**.
2. Click 

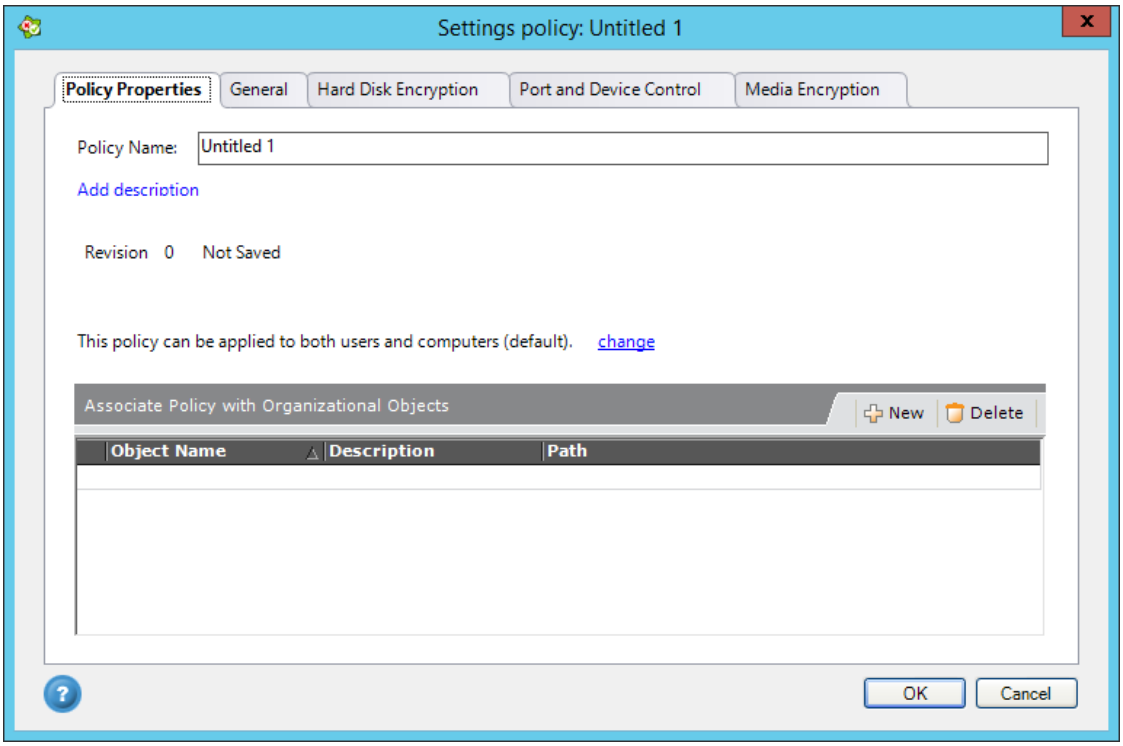
to set a new Settings Policy. The Settings policy window is displayed.

Tab	Description
Policy Properties	For a description refer to Associating a Policy with Organizational Objects.
General	These settings are described in **Error! Reference source not found.**.
Hard Disk Encryption	These settings are described in Advanced Encryption Settings.
Port and Device Control	These settings are described in Port and Device Control.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Media Encryption	Encryption settings determine the system's behavior when removable storage device permissions are set to Encrypt.

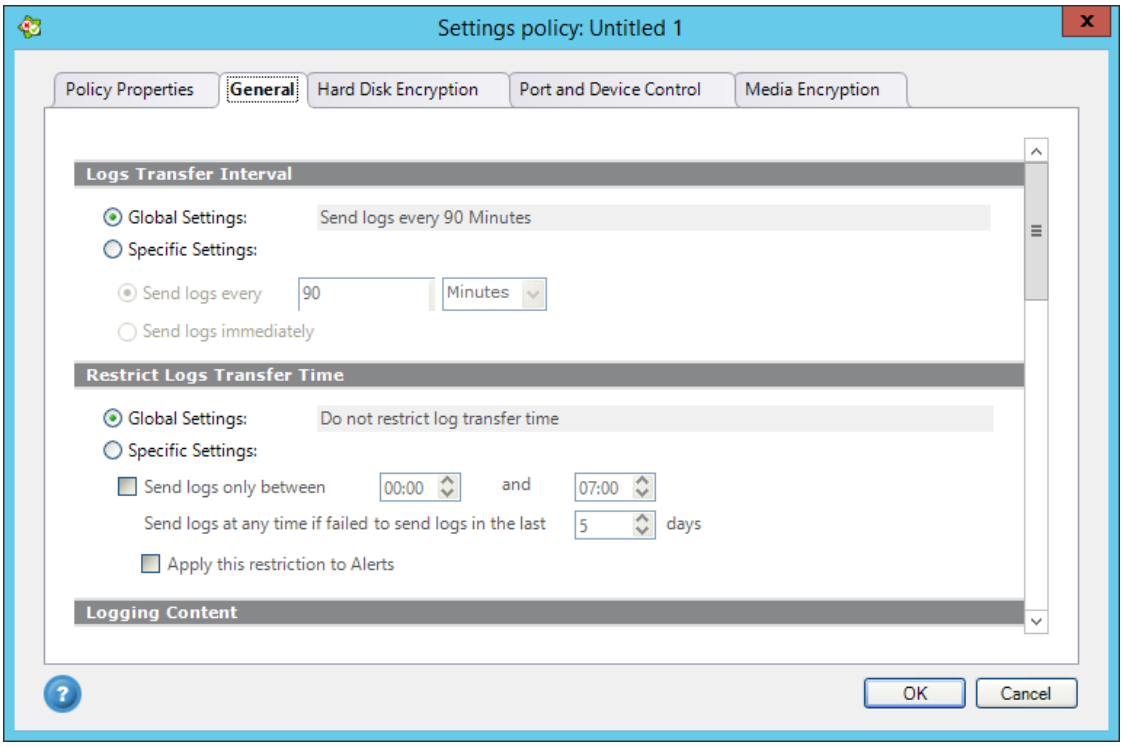
7.1.1.8 Policy Properties Tab



In this window, the user can name the policy, change its description and associate it with organizational objects. See Associating a Policy with Organizational Objects for a detailed description of this tab.

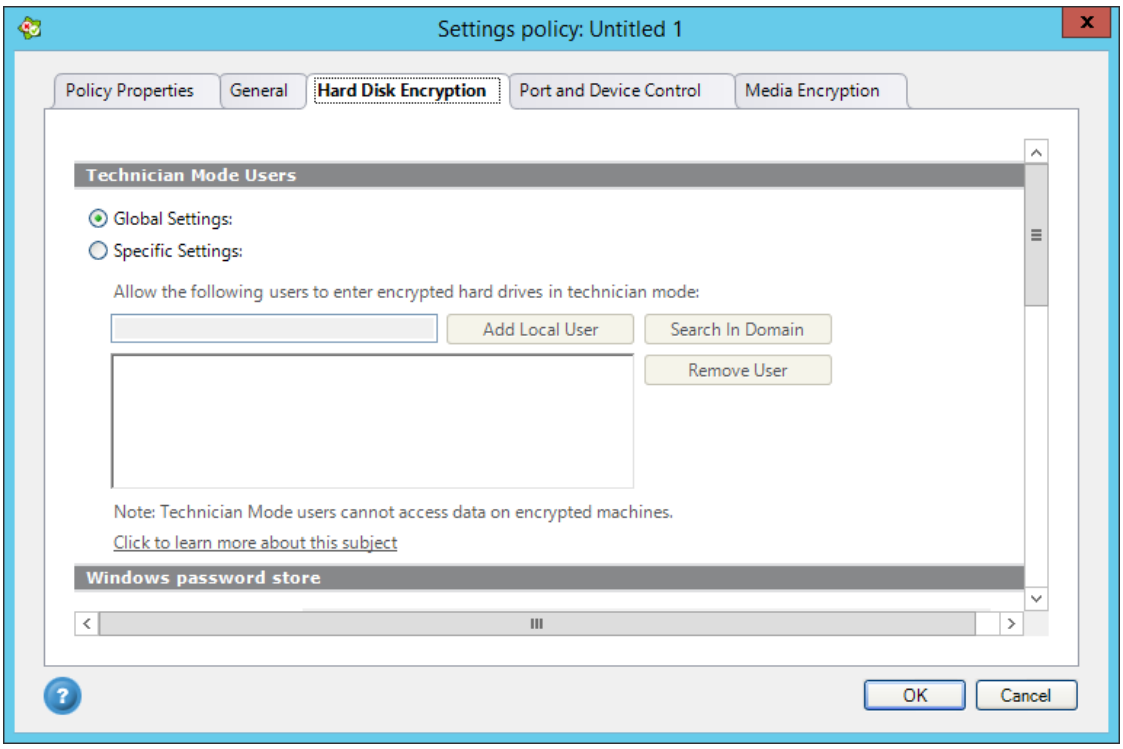
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7.1.1.9 General Tab



In this window, various general settings are found.

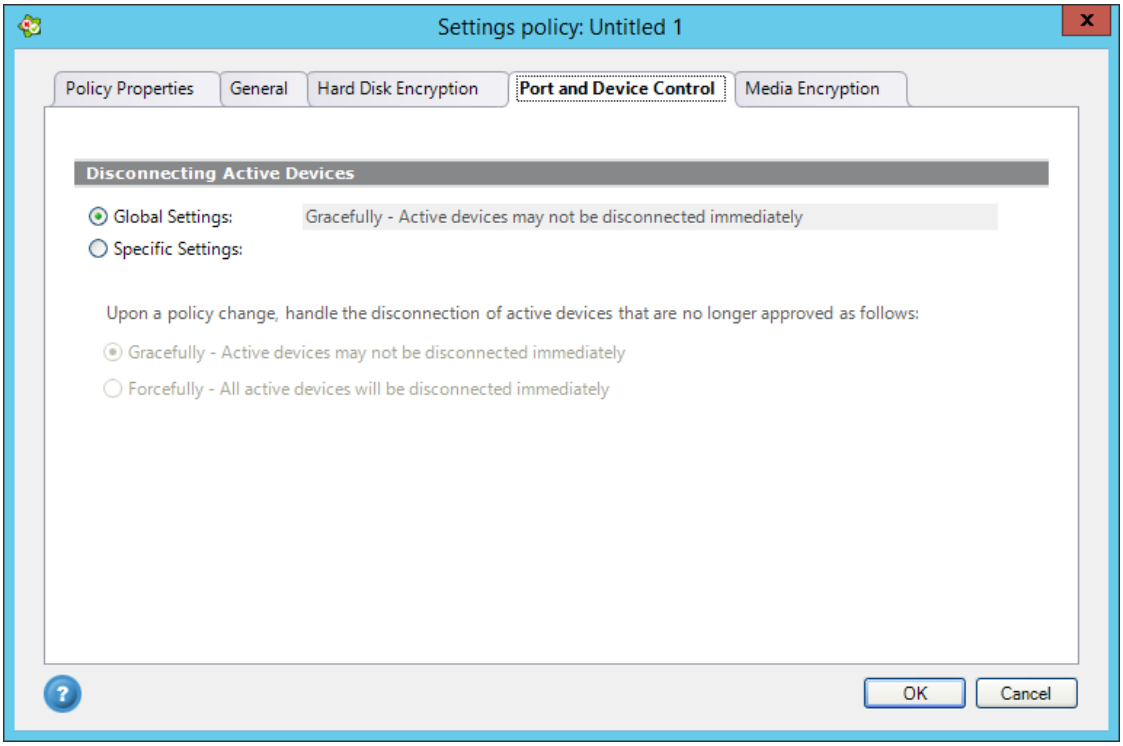
7.1.1.10 Hard Disk Encryption Tab



In this window the hard disk encryption settings are found. These settings are described in Advanced Encryption Settings.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

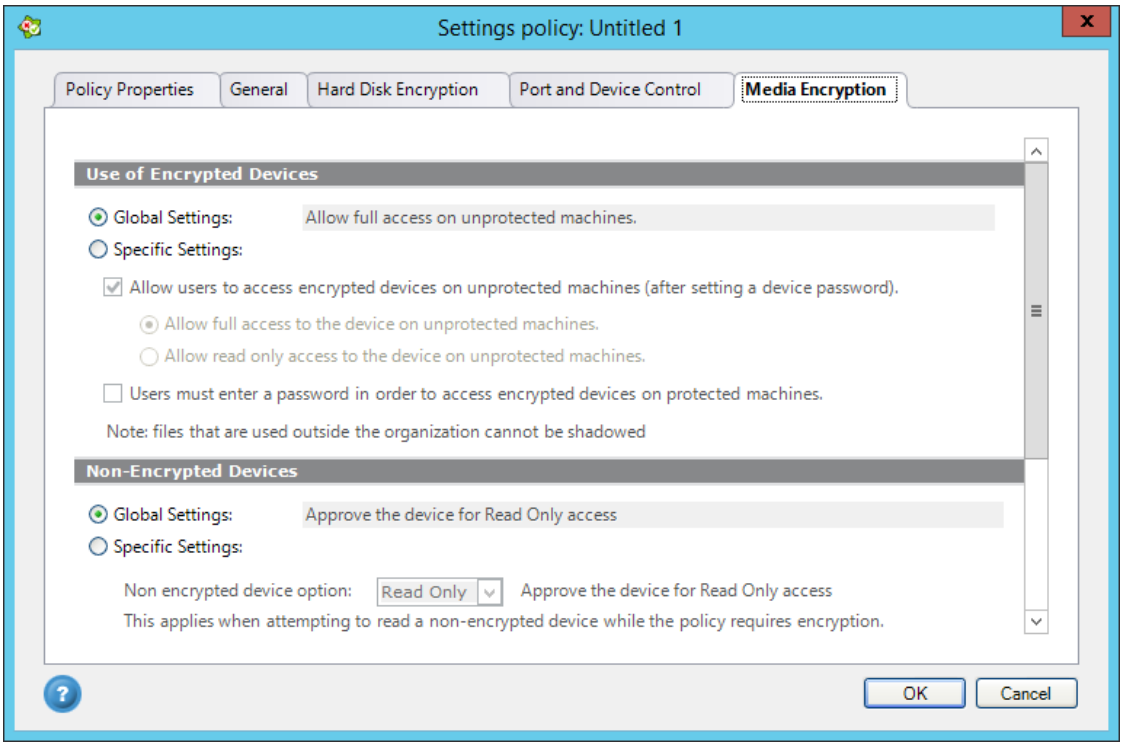
7.1.1.11 PORT AND DEVICE TAB



In this window are the port and device settings. These settings are described in Port and Device Control.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7.1.1.12 MEDIA ENCRYPTION TAB



Encryption settings determine the system's behavior when removable storage device permissions are set to Encrypt.

Setting	Description
Use of Encrypted Devices	The settings in this section determine whether the users may access encrypted removable storage devices on non-organizational computers, with full access or read only access. Also, whether one can access encrypted removable storage devices even within the organization: i.e., a password is required for access.
Non-Encrypted Devices	In this section you can determine behavior when the policy requires encryption and a non-encrypted device is detected; the device may either be blocked, allowed or permitted Read Only access.
Encryption Permissions	Here you can you choose whether to allow users to encrypt devices.
Device Re-Introduction Permissions	Here you can allow a virus scan on devices that were used outside the organization, to safely re-introduce them back into the organization. If you choose block users from using devices which were not yet re-introduced, you will not be able to re-introduce devices back into the organization after being used outside. This capability is only relevant if you chose Scan Before Approving Access for Device Virus Scan (Third Party) in Storage Control.

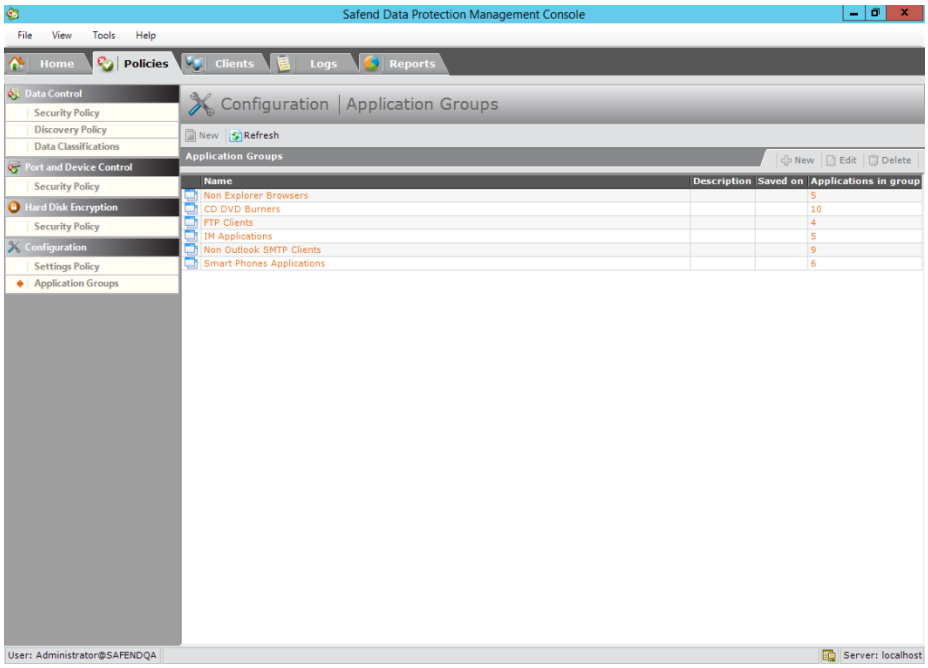
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

End-users whose effective policy requires encryption of removable storage devices should be made aware of the requirements, since their Client may display messages that require them to encrypt removable storage devices.

7.1.1.13 Application Groups

Information about various application groups can be found in the Policies tab.

Select **Configuration>Application Groups**, the following window will be displayed.



Here you can view information about a specific application group. To view this information, double click on the application group of interest in the Name column, for example Non Explorer Browsers. The following information will be displayed.

Here is displayed information about each application and executable. To search for a specific application, type the name in the Search text box and click Search.

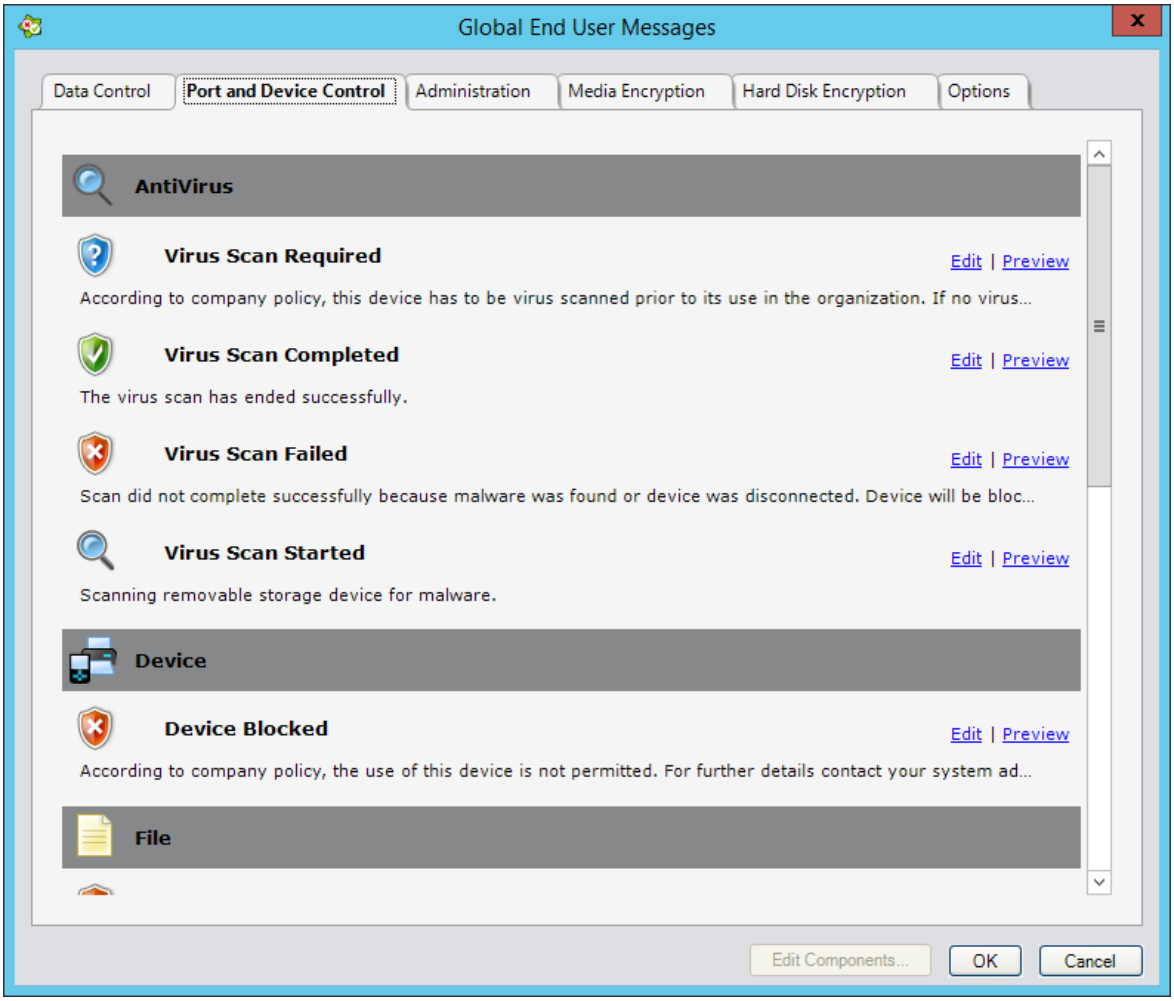
See Application Data Access Control for more information.

7.1.1.14 Configuring Agent Messages

See Safend Data Protection Suite Agent Messages for a description of each message. See for a description of another way to access the End User Message Editor.

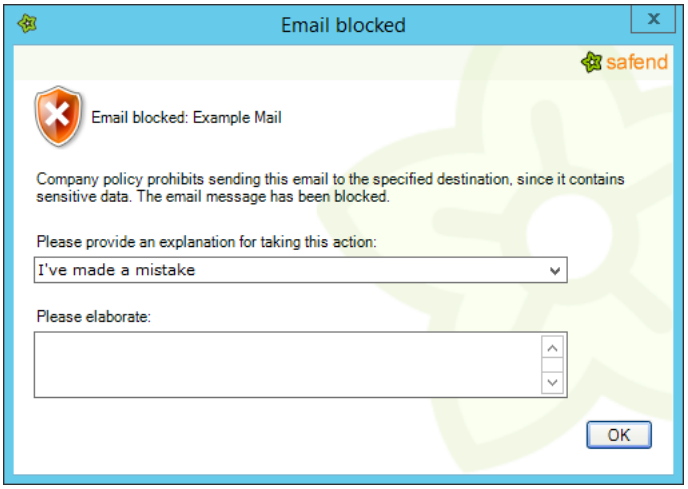
The Agent messages can be modified to meet your specifications. To modify the messages, from the Tools menu choose Global End User Messages. The Global End User Messages window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



There are five categories of messages (tabs): Data Control, Port and Device Control, Administration, Media Encryption and Hard Disk Encryption. For Data Control the following types of messages can be configured: Application Group, Email, External Storage, FTP, Local Printers, Network Printers, Network Shares, Web and Portable Virtual Storage. For Port and Device Control the following types of messages can be configured: Antivirus, Device, File, Keylogger, Port, Storage Device and WiFi. For Administration the following types of messages can be configured: Suspension and Update Policy. For Media Encryption the following types of messages can be configured: Media Encryption and Encrypted by Another Organization. For Hard Disk Encryption the following types of messages can be configured: Encryption. To view a message click Preview. Here is an example of the type of end user message which will be displayed.

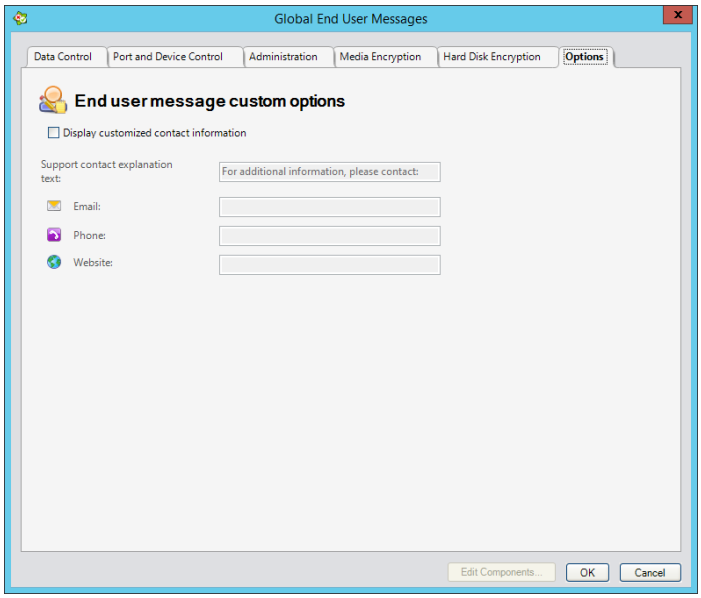
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Each message consists of a message title, the message itself, a drop-down response box for the user with several possible choices, or a text box where the user can write a free-text explanation (please elaborate).

Options Tab

You can add support contact information, if it is relevant, in the Options tab.

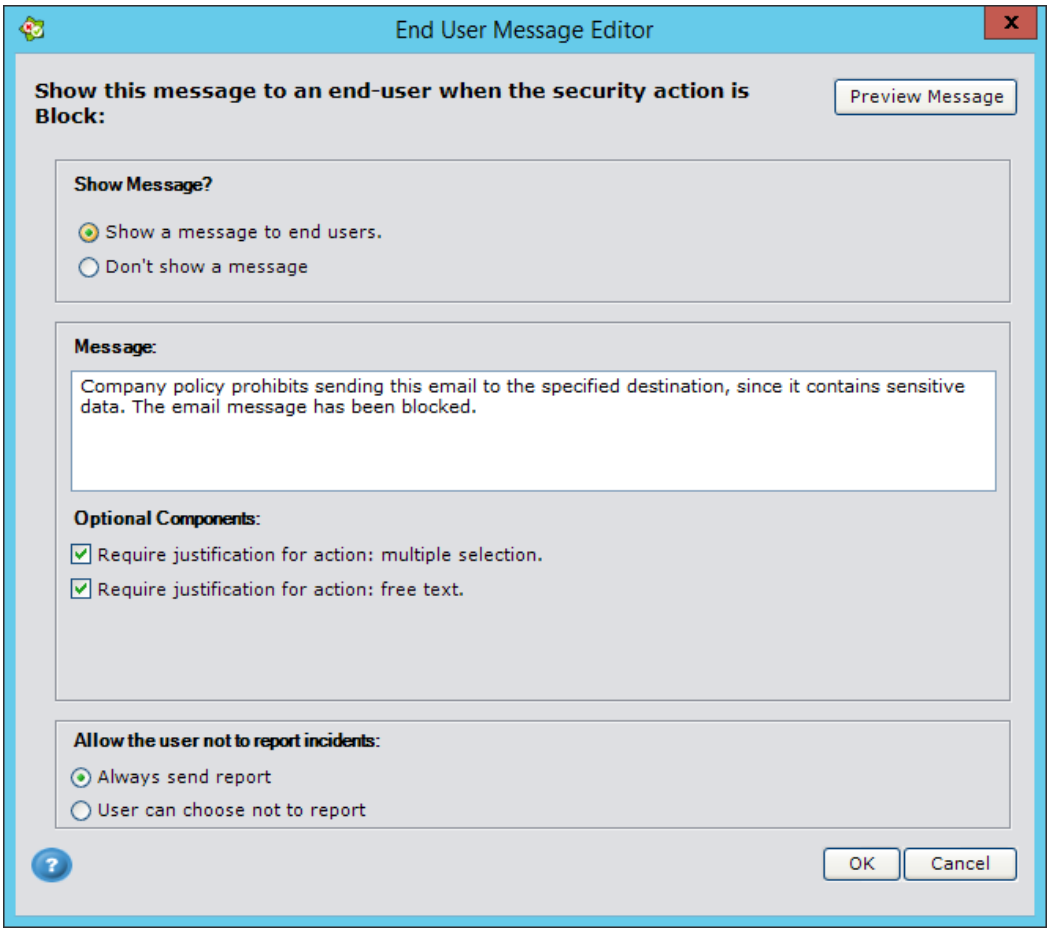


If you choose Display customized contact information, you can then add a support contact message, email, telephone and website information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Editing an End User Message

1. Click Edit beside the message you want to edit in the *Global End User Message* window. Here is an example of what is displayed which will vary according to the message.

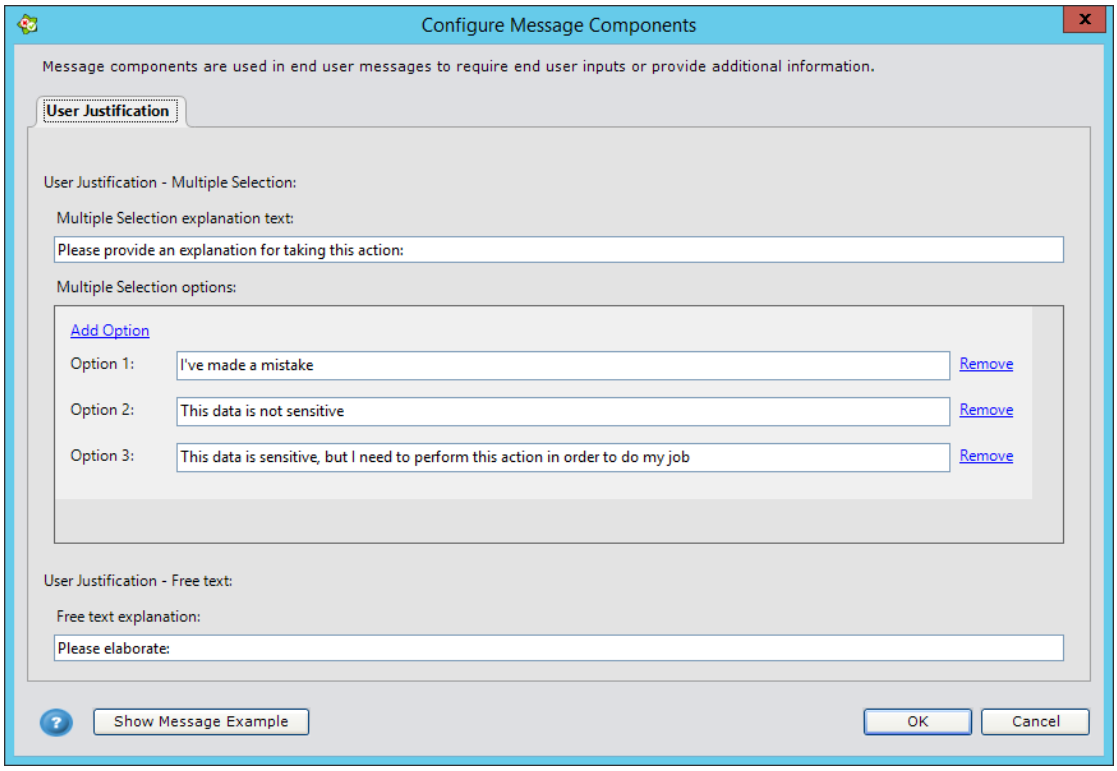


2. Click Preview Message if you want to see how this message is displayed.
3. In the Message field you can edit the text of the message. This field can present messages in different languages.
4. In Optional Components you can select a justification action: a multi-selection drop-down list and/or a free text box.
5. In Allow the user not to report incidents you can choose to send a report or have the option not to report (User can choose not to report). This option is only relevant for "block" actions.
6. In some case there is a Show Message option in which you have the option whether to show a message.
7. Click **OK** to apply all changes.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7.1.1.15 CONFIGURING MESSAGE COMPONENTS

1. You can further customize *Optional Components* in the *End User Message Editor* window, by clicking Customize Components. Alternatively, you can click **Edit Components** in the Global End User Messages window. The Configure Message Components window is displayed.



2. You can choose the Multiple Selection options you want to appear in the message and edit the Multiple Selection explanation text.
3. In addition, you can alter the text message above the Free text explanation box where the user is able to provide a detailed explanation about his actions.
4. Click **OK** to apply all changes.

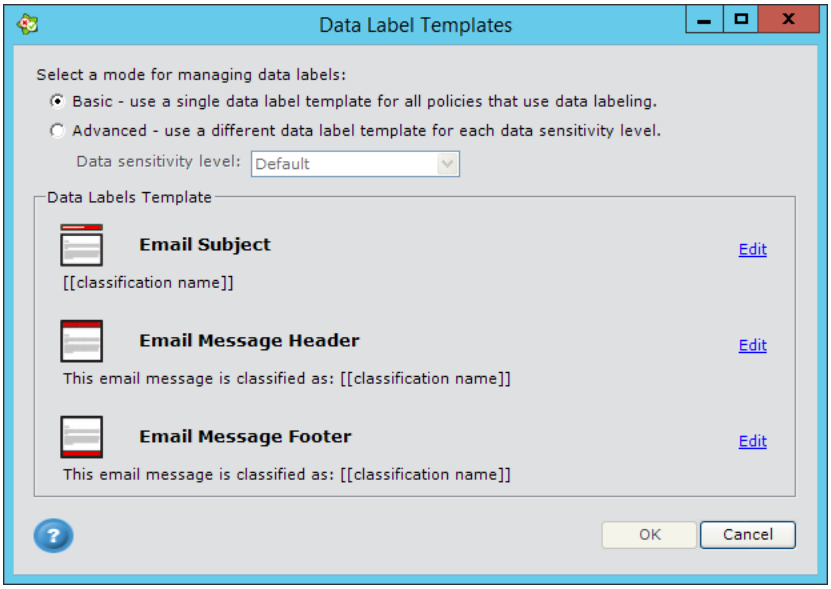
7.1.1.16 CONFIGURING DATA LABEL TEMPLATES

Note: See Email Configuration for an alternative way to access the Data Label Templates.

Labeling enables you to add pre-defined text labels to classified email messages. Labeling increases data awareness among employees in the organization and can be used along with Data Control policies to mark sensitive content and prevent its leakage. Email data labeling is supported on Outlook email clients. Data Label Templates allows you to define data labels for email messages. Labels can include a text message, Data Classifications that were matched and their Data Sensitivity.

To configure Data Label Templates, go to the **Tools** menu and choose **Data Label Templates**. The Data Label Templates window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



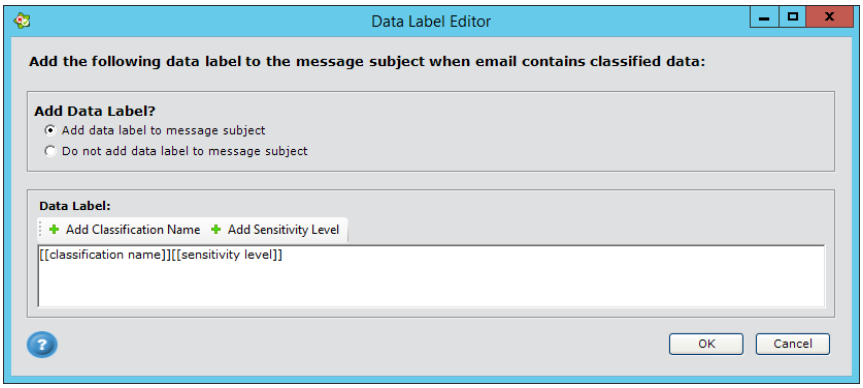
This enables you to select between 2 modes that affect the entire organization:

> **Basic mode**: you define a single (Global) data labeling template that can be used in all data control policies that require data labeling.

> **Advanced mode**: you define unique data label templates for each data sensitivity.

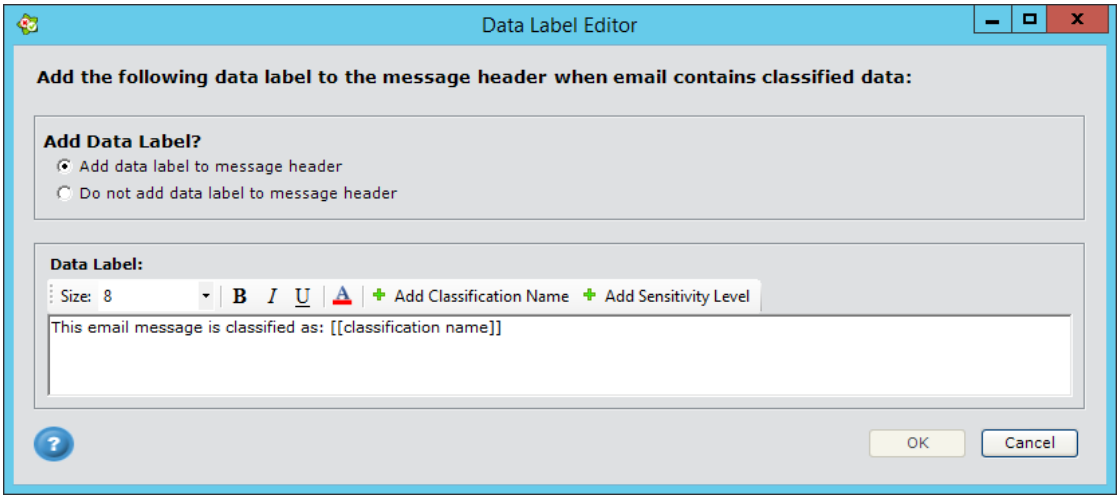
You can choose to add a label to the email subject, message header and the footer.

1. Click Edit beside *Email Subject*, *Email Message Header* or *Email Message Footer*. The following window is displayed for Email Subject.



Alternatively, if you choose Email Message Header, the following window is displayed.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



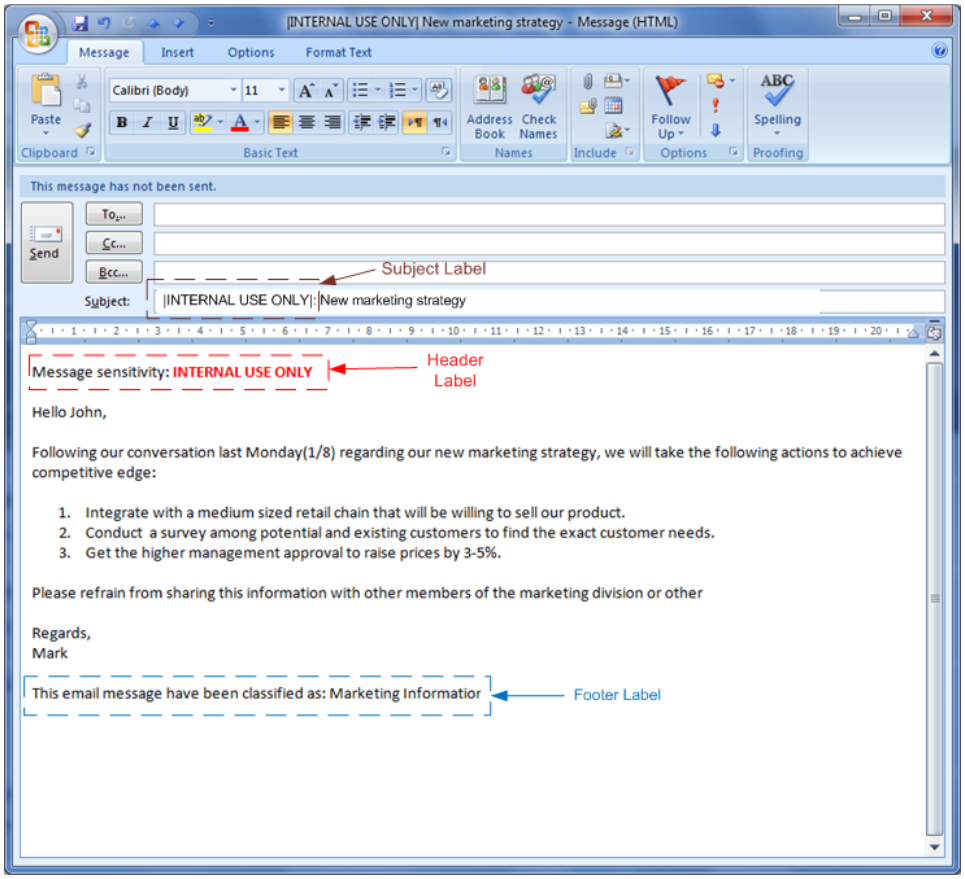
2. Select Add data label to message. The Data Label section is now enabled.

3. In the Data Label text box enter the data label for the email subject. This label will be placed at the beginning of the subject. For Message Subject you can click Add Classification Name and Add Sensitivity Level placeholders. For Message Header or Footer you have additional tools to format the rich text you add. These tools set the size and color of the text as well as whether it will be bold, italics or underlined.

   The Classification Name or Sensitivity Level placeholders must be one uniform text style (e.g., all bold) and not a mixture of styles (e.g., [[Classification Name]]). To reformat the text style of the Classification Name or Sensitivity Level, highlight the entire placeholder, including its brackets and uniformly change the style (e.g., [[Classification Name]]).

   Here is an example of how an email looks when it is data labeled. In the following example all three types of Data Labels are displayed: Subject, Message Header and Footer.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Adding an email Subject label to an email with an existing Subject label will replace the current email subject label with a new one. If the new label includes a different sensitivity than the existing label, the sensitivity with the higher priority will be applied.

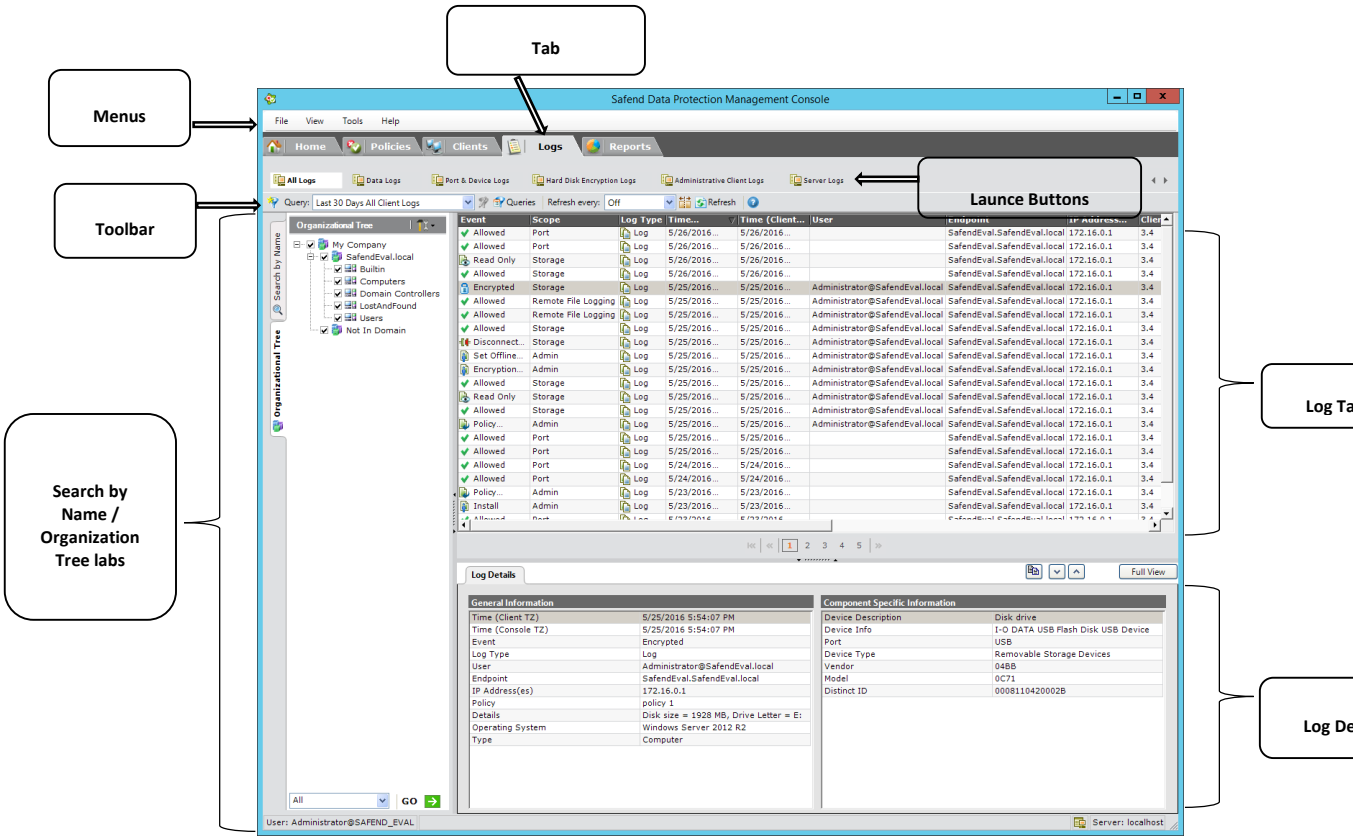
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

8 Managing Clients

The Clients Tab serves as the central location for viewing the status and details of Safend Data Protection Suite Clients, performing tasks such as updating policies on Clients and collecting logs from Clients, viewing task progress, generating a password in order to temporarily suspend protection on a Safend Data Protection Suite Client and more.

8.1 Quick Tour of the Clients Tab

Click the Clients tab. The Clients window is displayed.

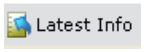
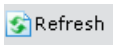
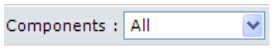


8.1.1.1 File Menu

Menu		Description
File	Export Clients	Exports the Clients table to an external file. This opens the Export Clients dialog box. You enter the Destination or click Browse.
Tools	Synchronize Virtual OU(s)	This is for importing files from a folder that contains all the Virtual OU machine lists.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

8.1.1.2 TOOLBAR

Button	Description
	Gets the most recent information from each Client by collecting logs (for details see Retrieving Latest Information from a Client).
	Grants a suspension password in order to temporarily suspend protection from a Client.
	Launches Safend Auditor (see Auditing Devices).
	Updates the Clients table according to the Organizational Tree selection and refreshes the Clients table records according to the current logs.
	Choose the end point status from the drop-down list to filter the Clients table. These include: All, Served, Not served, Blocked, Unlicensed, Encrypted and Not Encrypted.
	Choose the component from the drop-down list to filter the Clients table. These include: All, Inspector, Protector, Encryptor, Data Discovery.
	Enables you to select the fields that will be displayed in the Clients table. Refer to *Configure* Clients View for more information.
	Displays the context sensitive help of the active window and enables access to other help topics.

8.1.1.3 WORKSPACE

The Clients tab workspace is divided into three areas:

- **Organizational Tree, Search by Endpoint** and **Search by User** tabs – appear in the left pane. These tabs serve as filters for determining which records are displayed in the Clients Table. The tabs are discussed in *Filtering Clients*.
- **Clients Table** - appears in the top right pane and displays a table of the Clients in the selected Organizational Tree component. Before you make any selection in the Organizational Tree or Search By Name tabs (described below) this area is empty. Refer to *Clients* Table for more details.
- **Client Properties pane** - appears below the Client Table and displays the properties of the client selected in the Clients table. Refer to *Client Properties Pane* for more details.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

8.1.1.4 Clients Table

The Clients table displays information about the Clients protecting the organizational component(s) selected in the Organizational Tree.

The default columns displayed in the Clients table can be changed, using the Configure View button in the toolbar. Here is a description of all the possible columns.

Column	Description
Endpoint	The name of the endpoint (computer or mobile device) to which the columns in the row refer.
Domain	The Domain name.
Logged On User	If a user is logged on, displays user name and domain name.
Status	Served ( ) – protected by Safend Data Protection Suite Client or Not Served ( ) – not protected. Unlicensed ( ) – client exceeded the license seat count and therefore cannot update its policy
Software Version	The version of Safend Data Protection Suite installed on the computer.
Operating System	The name of the operating system being used.
Full Endpoint Name	The full name of the Endpoint to which the columns in the row refer, including its domain as a suffix.
IP Address	The IP address of the client machine.
Last Handshake	The date and time of the last handshake between the Client and the Management Server.
Path	The path to the Client location in Active Directory/Novell eDirectory.
Received Tampering Logs	The date and time tampering logs were last received.
Received Logs	The date and time logs were last received.
Suspension Status	Suspended - protection is suspended, otherwise Protected.
Encryption Started On	The date/time when the encryption started.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Encryption Completed On	The date/time when the encryption was completed.
Protector Effective Policy	The name of the policy which is in effect on the computer. If policies are merged on this Client, all merged policies are listed.
Protector Effective Policy Type	The effective policy type - computer ( ) or user ( ).
Protector Machine Policy	The name of the computer policy. This may be different than the Effective Policy if a user policy is in effect.
Suspension Start Time	The date and time that suspension began.
Suspension Duration	The period defined by the administrator for which this computer will be suspended.
Encryption Status	This indicates if the machine's hard disk is encrypted, and shows its progress by percent.
Encryptor Machine Policy	The name of the Hard Disk encryption policy.
Inspector Effective Policy	The name of the data control effective policy.
Inspector Effective Policy Type	This indicates if the effective data control policy applies to the machine or user.
Inspector Machine Policy	The name of the data control policy applied on the machine.
Settings Machine Policy	The name of the Settings machine policy.
Settings Effective Policy	The name of the Settings effective policy.
Last Data Security Log	The last log received from the endpoint.
Discovery Policy	The name of the Discovery policy applied.
Date of last scan	The date when the last scan was completed.
Scan Revision	The revision of the last Discovery scan or the scan that is currently running.
Discovery Status	Whether the Discovery is currently running on the machine.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

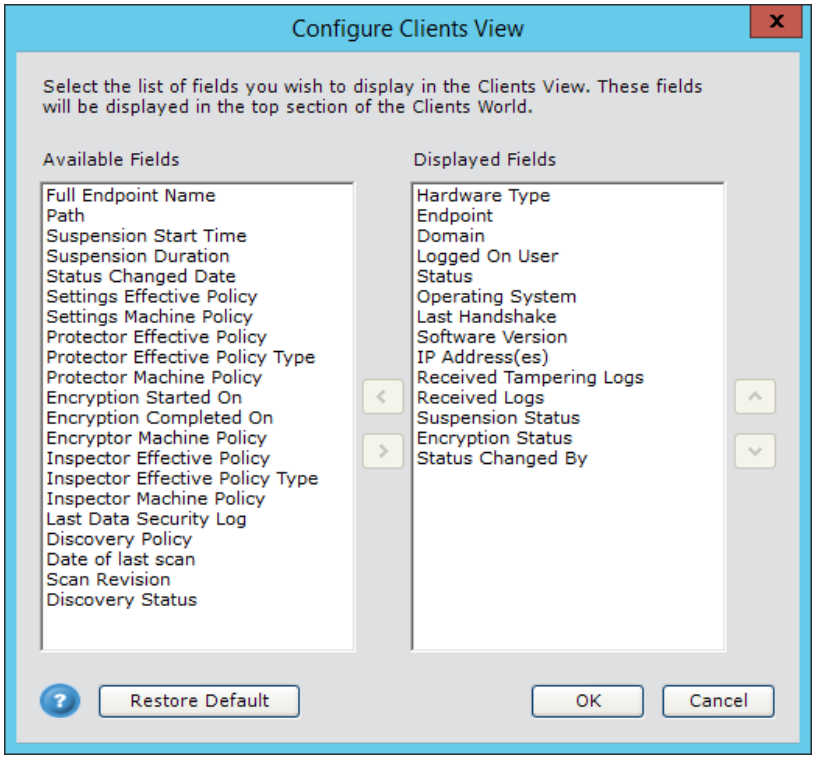
Column	Description
Status Changed By	The Management Console username that changed the endpoint status or 'System' in case the status was changed automatically.
Status Changed Date	The date on which the status was last changed.

You can modify the table view in the following ways:

- Sort the table by clicking the column heading of the column by which you wish to sort. Clicking the header again switch from ascending to descending order. You can add a secondary sort level by pressing the SHIFT key and clicking the secondary column heading.
- Modify column width by dragging the column separation lines.
- Move a column by dragging and dropping it into the desired position.

8.1.1.5 CONFIGURE CLIENTS VIEW

When you click  in the toolbar, the following is displayed.



Here you can choose the fields that will be displayed in the Clients table. Select the field and click the left/right buttons to move fields from the Available/Displayed Fields columns. Use the up/down arrows to order the fields in the Clients table.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

8.1.1.6 Client Properties Pane

The Client Properties pane appears below the Clients table and displays the properties of the client you select in the table. The details in this pane are identical to the details displayed in the table. The pane displays information regarding the selected table record, arranged in the following sections:

- **General Client Information:** displays general information about the computer and the Client. Includes an indication as to whether the Client is Served or not, a link for viewing logs for the Client and a link for viewing tampering logs for the Client. A hazard icon is displayed if this computer has been tampered with at least once.
- **Components Specific Information:** displays information about the different Safend Data Protection Suite modules.
- **Protector:** displays the Effective Policy (the Effective Policy is different from the Machine Policy when a user who has a User Policy is logged on). Machine policy: (the Machine Policy may not be the currently effective policy if a user who has a User Policy is logged on).
- **Encryptor:** shows whether the internal hard disk is encrypted or not.
- **Inspector:** displays the Effective Policy and Machine Policy.
- **Discovery**: displays the status of the discovery process, as well as the time in which the last discovery process had ended.

8.1.1.7 Filtering Clients

The left side of the Clients window includes two tabs to help you determine the computers whose information will be displayed in the Clients Table.

Filtering the Clients Table by Organizational Unit

The Organizational Tree is a tool you use to determine the Organizational Units from which Clients will be displayed in the Clients Table. This section describes how to manage the Organizational Tree and how to determine, from the Tree, which Clients are displayed in the Clients Table. The Organizational Tree tab displays the domain(s), organizational units and the Not In Domain group (which includes all computers who do not currently belong to the domain), as shown in the following figure:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Note: The Organizational Tree is applicable only if you are using Active Directory/Novell eDirectory. If you are not, only one group is displayed in the Tree – Not In Domain. Selecting this group selects all computers.

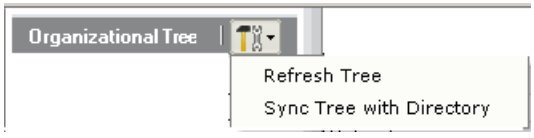
Select organizational units

If necessary, expand the Organizational Tree to view lower-level organizational units.

1. Select the required domain or organizational units by checking the appropriate checkboxes.
2. At the bottom of the Organizational Tree tab, click GO .The information now displayed in the Clients Table originates from Clients that belong to your Tree selection, and only them.

8.1.1.8 Updating the Organizational Tree

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from the Safend Data Protection Suite Management Server, or synchronize it with Active Directory/Novell eDirectory (the Directory may be more up-to-date, but may also take longer). Updating the Tree is done from the Organizational Tree Update menu (shown below) which is found at the top of the Organizational Tree tab.



> To update the Organizational Tree from the Management Server: from the Organizational Tree Update menu, click **Refresh Tree**. The Tree is updated.

> To update the Organizational Tree from the Directory: from the Organizational Tree Update menu (see previous figure), click **Sync Tree with Directory**. The Tree is updated, but this may take a while.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

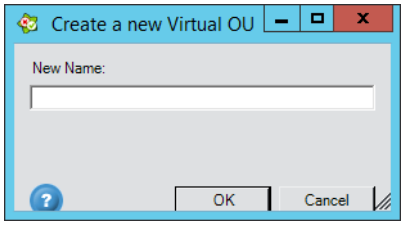
8.1.1.9 Virtual OU

Safend Data Protection Suite supports out of domain, direct policy distribution, either to the entire "out of domain" machines or only to specific out of domain machines. This involves creating virtual OUs that will function in a similar manner to directory service's Organizational Objects (OUs). The System Administrator creates virtual OUs, places "out of domain" endpoints in those virtual OUs and links machine policies directly to the virtual OUs.

Once created, these virtual OUs function in the same way as OUs: administrators are able to associate policies with them, filter queries for logs from a specific Virtual OU and run reports on OUs. They also function in the same way as OUs with regards to domain partitioning and policy hierarchy.

Creating a virtual OU

1. Right click a *Not In Domain* object in the Organizational Tree. Choose **Create a new Virtual OU** from the menu. The *Create a new Virtual OU* dialog box is displayed.



2. Type in a unique name for the virtual OU and click **OK**. If the Virtual OU name you choose is not unique, an error message will appear. The new virtual OU will be created under the Not In Domain object.

Renaming a Virtual OU

> Right-click the virtual OU in the Organizational Tree you want to rename and select the Rename Virtual OU option from the menu.

In the case of a name conflict a warning message will be displayed. This is only available when selecting a user-created Virtual OU.

Deleting a Virtual OU

1. Right-click the virtual OU in the Organizational Tree you want to delete and select the **Delete Virtual OU(s)** option from the menu. A confirmation message will be displayed asking you whether you want to delete the specific virtual OU.
2. Click **Yes** to confirm.

Movingout of domain endpoints to virtual OUs

Administrators can move Not In Domain endpoints to virtual OUs by right clicking on selected endpoints in the Clients table and choosing the Move to Virtual OU option.

If any of the endpoints are in the domain, they will not be available.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Managing virtual OUs by import

This feature provides a non directory based organization or a managed security provider the ability to synchronize multiple computer groups into the Virtual OU infrastructure.

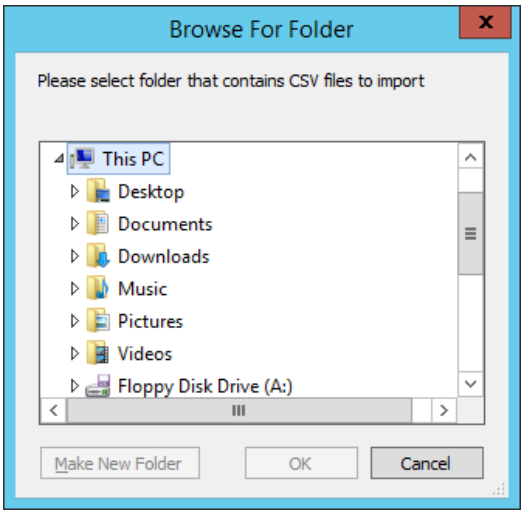
> For each vOU there is a file with the same name of the vOU it is representing.

> Such a file will contain machine lists in the following format: MachineA, MachineB
or
MachineA,
MachineB

> The files will have a CSV extension.

> If there is no vOU with that name (the name of the file), the vOU will be created.

3. In the Clients Tab Choose **Tools**>**Synchronize Virtual OU(s)** or alternatively right click on Not In Domain in the Organizational Tree and choose **Synchronize Virtual OU(s)**. The Browse for Folder window is displayed.

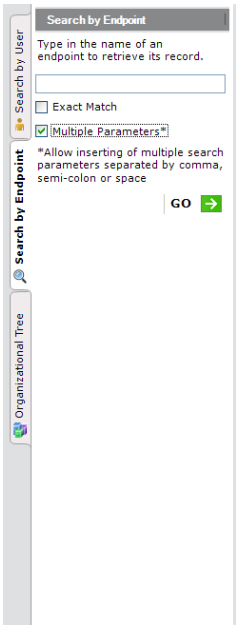


4. Select the folder that contains the CSV folder to Import these files, in order to add the machines to the vOU.

Filtering the clients table by endpoints

The Search by Endpoint tab is an additional tool that you can use to determine the endpoints whose records the Clients Table will display. This section describes how to use this tab to determine the Clients displayed in the Clients Table.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Searching for specific endpoints

1. In the text box, enter the name of the endpoint whose record you wish to display in the table. You may enter multiple names separated by a comma, semicolon or space.

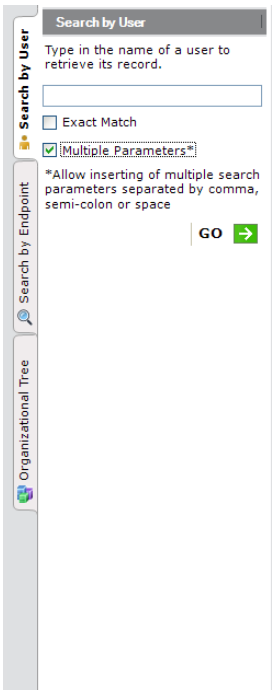
   f) Check the **Exact Match** checkbox if you want the table to display records for a computer with the name that exactly matches the string you entered in the text box. In this case you must enter the full computer name (including the domain suffix). If *Exact Match* is not selected, the Clients Table will contain records for all computers whose name contains the string that you entered.

   g) Check the **Multiple Parameters** checkbox to allow inserting of multiple search parameters separated by comma, colon or space.

2. Below the text box, click GO. The Client records now displayed in the table refer to the computer(s) whose name matches your search criteria. If no computer is found whose name matches your search criteria, the table will be empty.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

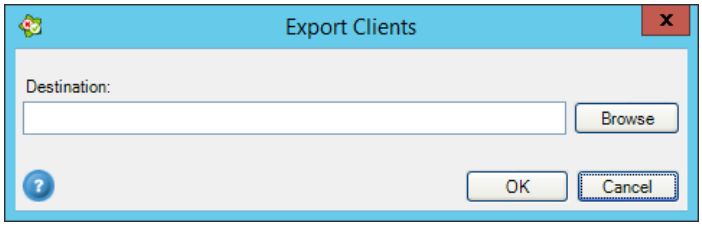
Filtering the client table by user



The procedure is very similar to Search by Endpoint, except that you enter the name of the user in the text box.

Exporting the clients table

> From the File menu, select **Export Clients**. The Export Clients window opens.



Exporting the clients table to an external file

Use this option to export the Clients Table in order to print it or perform further analysis, you can do so. The exported file is saved in XML format which can easily be opened with MS Excel, etc.

1. Click **Browse** to select a path (and type a file name) or type in the path for the exported file.
2. Click **OK**. A progress window opens and exporting begins.

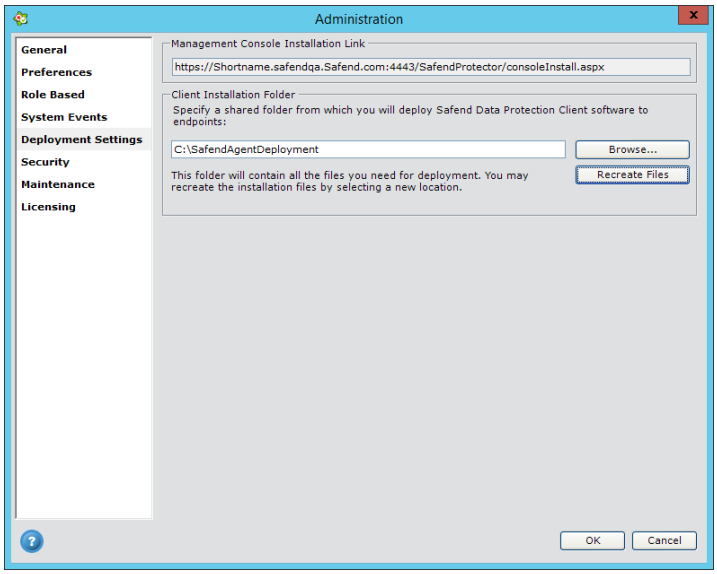
8.1.1.10 Installing Clients

Safend Data Protection Suite Client deployment (installation) is performed with a standard MSI installation package. The installation can be performed via Active Directory, various other

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

deployment tools or manually. Before performing deployment, you can check to verify that the required files are available.

From the Tools menu, choose **Administration** and click the **Deployment Settings** tab. The following window is displayed.



This window displays the current location of the Safend Data Protection Suite Client installation files. The Client installation folder should contain the following files:

> DataProtectionAgent.msi

> DataProtectionAgent_x64.msi. For a machine running 64-bit versions of Windows.

> ClientConfig.scc

> LegacyClientConfig.scc. For installing the legacy clients of v3.3.

Note: During the client installation process, the msi and scc files must be kept in the same folder. For a detailed explanation of Client installation, refer to the Safend Data Protection Suite Installation Guide.

Updating a Policy on a Client

As explained in the, policies are updated on the Safend Data Protection Suite Client by means of the Client connecting to the Management Server and checking for policy updates at predefined intervals, and updating the policy if it has changed. If you have recently edited a policy for a certain Organizational Unit or computer, you may wish to notify the relevant Safend Clients to check for an updated policy at the earliest possible opportunity.

There are two options for updating policies:

> **From the Tools menu:** this option enables you to update policies by any Organizational Unit or computer.

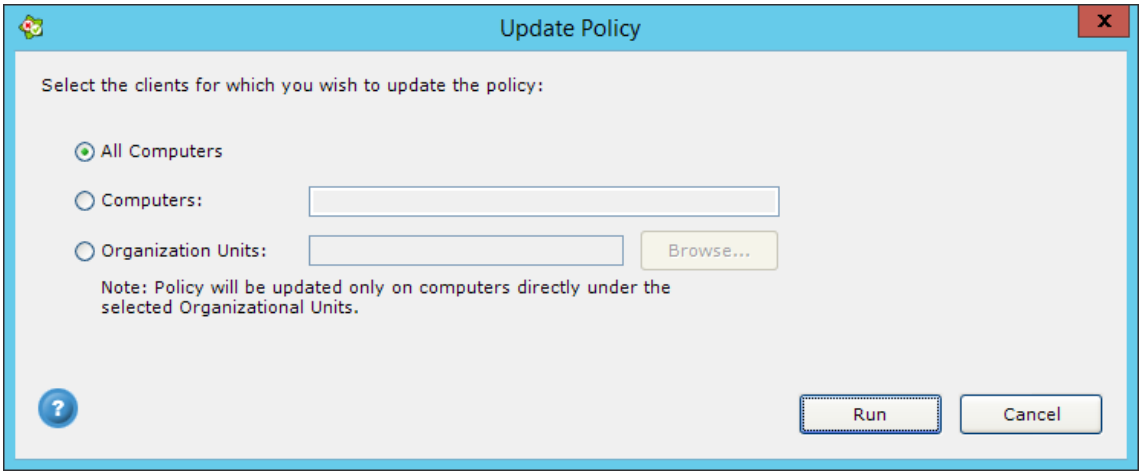
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

> **Using right-click:** this option enables you to update policies on pre-selected Clients by right-clicking Organizational Units from the Organizational Tree, or by right-clicking served Clients in the Clients table.

Updating a policy on any client

This option enables you to update a policy outside the scheduled time interval. Updating a policy is activated from the Update Policy window.

> In the Tools menu, select **Update Policy**. The Update Policy window is displayed.



Updating a client policy

If you have recently edited a policy for a certain Organizational Unit or computer, you may wish to notify the relevant Safend Clients to check for an updated policy at the earliest possible opportunity.

1. Select the required radio button option, as follows:

   a) **All Computers:** Select this option if you wish to update policies on all the computers in the organization.

   b) **Computers:** Select this option if you wish to update a policy for one or more computers and type the computer name in the field. To type more than one computer name, use a colon or a semi-colon as a delimiter.

   c) **Organizational Units:** Select this option if you wish to update policies on one or more organizational units, click **Browse**, and select the desired organizational units from the company tree. The selected units appear in the *Organizational Units* field.

2. Click **Run**. Notification is sent to the selected computers to check for a new policy, and the Client Task Progress window opens. You can track the progress of the update process in this window, as explained in *Tracking Client Task Progress*.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Updating a policy on pre-selected clients

1. In the Organizational Tree, select the desired components, or select the desired computers in the table.
2. Right–click. In the menu that appears, select **Update Policy**. Notification is sent to the selected computers to check for a new policy, and the Client Task Progress window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress*.

8.2 Hard Disk Encryption Utilities

Hard Disk Encryption Utilities contain different keys created by the administrator for specific computers that allow the end-user or other IT functions to perform different maintenance actions, such as password reset and recovery on an encrypted computer.

> Granting a one-time access key

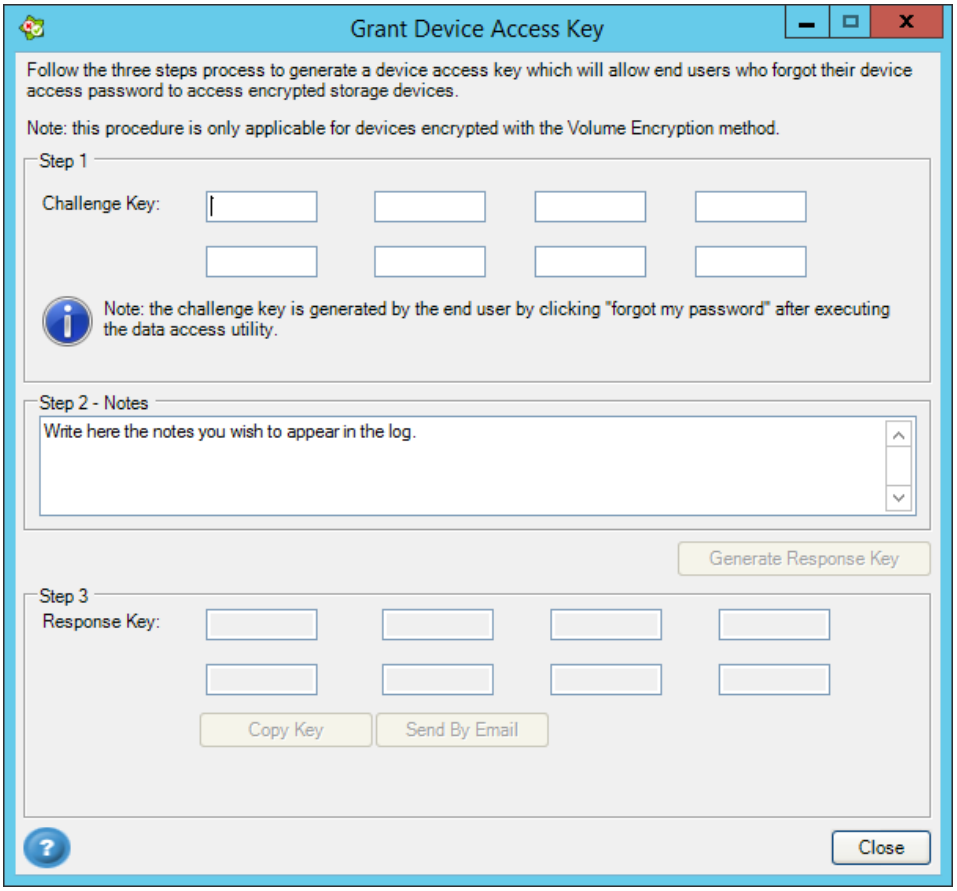
> Granting a data recovery key

Granting a one-time access key

The Grant One-Time Access Key utility allows granting an end-user one time access to an encrypted endpoint (the one time access is revoked upon rebooting or shutting down the endpoint).

1. From the Tools menu, select **Hard Disk Encryption Utilities** and then click **Grant One-Time Access Key**. The following window is displayed:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. Enter the Computer Name: the name of your computer (i.e., the computer you wish to grant one time access.). Now perform the following steps:

   a) Step 1: Challenge Key: These are numbers the Client (endpoint) enters. For each input box the characters are validated at the end of each characters sequence, if the sequence is correct the ✓ sign displayed at the right of each input box (and the input character is passed to the next characters box), if the sequence is wrong the ✗ sign is displayed and a note is displayed: "Note: incorrect challenge key was typed, please retype the challenge code."

   b) Step 2: Notes: Type in any note you want to appear in the log. This is enabled after the correct challenge key is entered. Click the Generate Response Key in order to receive a response. This is enabled after the challenge code has been typed in correctly.

   c) Step 3: Response key: These are numbers the client (endpoint) enters after receiving them from the Administrator. The same symbols as for the challenge key will be displayed for correct or incorrect input of characters. The Copy Key and Send by Email buttons are enabled after the correct challenge key is entered. These are alternative ways of receiving the response code.

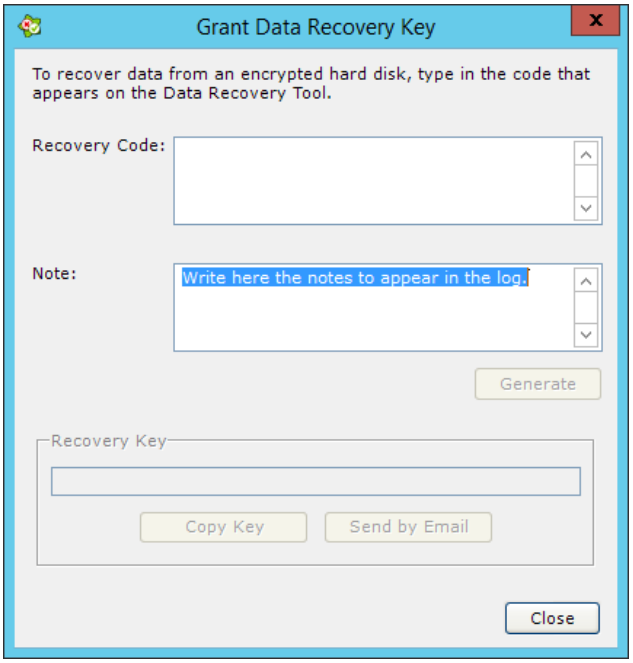
   d) Clicking the Cancel button will close the window.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Granting a data recovery key

The Data Recovery Key should be used within the Safend Recovery Tool (see Appendix A – Safend Recovery Tool for Encrypted Hard Disk for more details) by a recovery technician to decrypt an encrypted hard disk after a major technical failure.

1. From the Tools menu, select **Hard Disk Encryption Utilities**. Click **Grant Data Recovery Key**. The Grant Data Recovery Key window is displayed.



2. If serious technical failure occurs on the hard disk, the Safend Recovery Tool can be used to decrypt the information on that disk.
3. This recovery process can be performed easily using the password that was used to enable access in the Safend Data Protection Suite – Enter Access Password window each time after the computer was restarted.
4. In some cases this method cannot be used and a recovery key needs to be created by you. The technician user must first obtain the Recovery Code and send it to you (see Appendix A – Safend Recovery Tool for Encrypted Hard Disk for details). You must then enter it into the window above and click the Generate button to generate a Recovery Key that appears in the Recovery Key field at the bottom of the window.
5. You must now transfer this key to the technician. Click **Copy Key** to copy the key to the clipboard, or **Send by Email** to open a new message in your email application containing the key.
6. It is important to make sure the person receiving the key is authorized to use this specific computer.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

7. The technician should now enter this Recovery Key in the Recovery Key field in the Safend Recovery Tool, as described in Appendix A – Safend Recovery Tool for Encrypted Hard Disk section.

8.3 Retrieving Latest Information from a Client

You may at times wish to view Client information as close to real time as possible. This option enables you to collect logs and view the latest information from served computers outside the pre-defined collection times. Activating this function collects all log types.

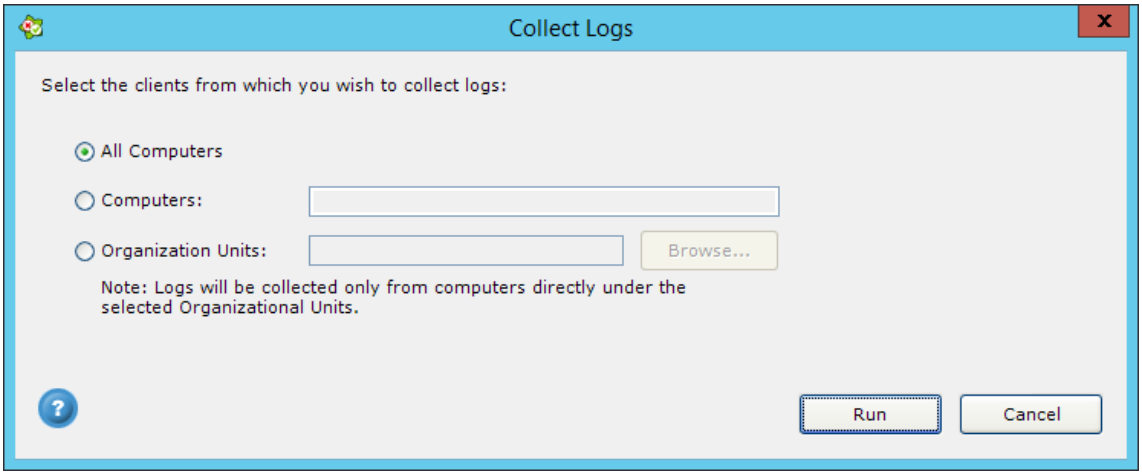
There are two ways to collect logs:

> **From the Tools menu or the toolbar**: this option allows you to collect logs by any organizational unit or computer.

> **Using right-click**: this option enables you to collect logs from pre-selected Clients by right-clicking Organizational Units from the Organizational Tree, or by right-clicking served Clients in the Clients table.

Collecting logs from any client

In the Tools menu, select Collect Logs, or click Latest Info in the toolbar. The Collect Logs window is displayed.



Collecting Logs

This option enables you to collect logs and view the latest information from served computers outside the predefined collection times. Activating this function collects all log types.

1. Select the radio button for the desired option, as follows:

   a) **All Computers:** Mark this option if you wish to collect logs from all the computers in the organization.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

b) **Computers:** Click this option if you wish to collect logs from one or more computers and type the computer name in the field. To type more than one computer name, use a colon or a semi-colon as a delimiter.

c) **Organizational Units:** Mark this option if you wish to collect logs from one or more organizational units. Click **Browse** and select the desired organizational units from the company tree. The selected units appear in the Organizational Units field.

2. Click **Run**. Log collection from the selected computers begins, and the *Client Task Progress* window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress*.

Collecting Logs from Pre-selected Clients

This option performs the same action described in the previous section, but allows you to pre-select the Clients from which to collect logs.

1. In the Company Tree, select the nodes and then right-click. A menu opens.
2. In the menu, select **Retrieve Latest Info (Collect Logs)**. The Log collection from the selected computers begins, and the Client Task Progress window opens. You can track the progress of the update process in this window, as explained in Tracking Client Task Progress.

Tracking Client Task Progress

When the application is in the process of performing tasks (such as collecting logs or updating policies), you may view the progress of these tasks in the Client Tasks Progress window.

From the View menu, select Client Tasks. The Client Tasks Progress window opens. You can view task progress in this window.

Client Tasks Progress

The Client Task Progress window displays all the tasks running at that moment, with the status of each task, and changes in this status as they occur. It displays a single line for each Client (unless a policy updating task and a log collection task for the same Client are running concurrently, in which case two lines are displayed for this Client). As the phases in the task change, so do the values in the Status column. A finished task has the status of Completed or Failed. For the case of a failed status, a reason is supplied.

The Client Tasks Progress window includes the following columns:

Column	Description
Computer	Displays the full computer name.
Task	Displays the task which the Client is performing (Collect log, Update Policy).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Status	Displays the current task status (Completed, Pending, Pushing Policy, Failed).
Details	When the Status is Failed, the reason is displayed.

Notes:

Since Safend Data Protection Suite uses WMI for performing remote client tasks, WMI ports must be open for the command to go through. See Client Tasks Failure for additional information.

If you selected Novell as your Directory in the Administration window you will be able to perform this action only if a Windows user with local administrative rights is defined on the target endpoint(s).

8.3.1.1 Client Tasks Failure

Since the Safend Data Protection Suite uses Windows WMI infrastructure for performing remote client tasks, WMI ports must be open for the command to go through. There may be 3 different types of cases where the WMI command will not function correctly. If one or more Client Tasks have failed, check the following according to the task details displayed in the Details column of the Client Tasks Progress window:

Task Details	Resolution
Access Denied	Make sure the defined Server Credentials, used for performing the scan, include local administrator privileges on the remote machine. You can refer to *Server Credentials* for more information.
The service cannot be started	Make sure that the WMI service on the remote machine is started and set to start automatically.
The RPC server is unavailable	Make sure the WMI ports are allowed on the active firewall and that "remote administration" is allowed in the Windows Firewall.

Verifying WMI connectivity on your environment

1. From the Server machine, Select **Run** from the Start menu, type wmimgmt.msc.
2. On the left-hand side, right click **WMI Control** (Local) and select connect to another computer.
3. Select another computer and enter the name of the computer with which you are trying to establish communication. Click **OK**.
4. On the left-hand side, right click **WMI Control** [hostname] and Select Properties. The application scans the remote machine using WMI.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

5. The scan result indicates the status of the WMI connectivity between the Safend Management Server and the target machine.

8.3.1.2 Temporary Suspension of Safend Data Protection Suite

At times it may be necessary to temporarily suspend Safend protection on a Client without uninstalling the Safend Data Protection Suite Client. An example might be a user who is away from the office, with a laptop that needs to have an unauthorized USB flash drive connected to it on a one-time basis, in order to view an important presentation which resides on that USB flash drive.

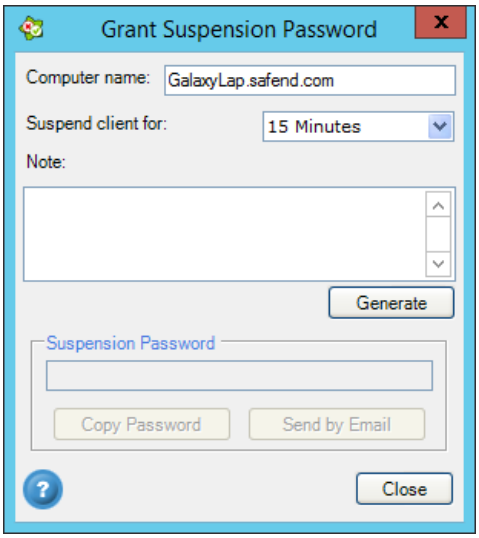
The end-user requires a password in order to perform suspension. This password is generated by the administrator and is provided to the user. Suspension begins once the user enters the password, and is pre-set for a limited period of time. Once this period ends, protection of the Client is resumed.

Once protection is resumed, Client logs are updated with information about the suspension, about devices which were connected during the suspension period and about files copied to and from those devices.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Opening the Grant Suspension Password window

In the Clients table, right-click the computer on which you wish to suspend protection, and select Grant Suspension Password. Alternatively, you can click Suspension in the tool bar, or select this option from the Tools menu. The following window opens:



Granting a Suspension Password

Use the Grant Suspension Password window to enter the necessary information about the computer on which protection is to be suspended, to enter suspension parameters and to generate a suspension password which you will provide to the user.

1. If the Computer Name field is empty (which may be the case when you open this dialog from the Tools menu or using the toolbar button), enter the required computer name.
2. In the Suspend Safend DLP Suite for field, select the suspension period from the drop-down menu.
3. In the Notes field, enter any text you desire, for example a description of the reason for suspension (optional).
4. Click **Generate**. The system generates a password and displays it.
5. Click **Copy Password** to copy the password to the clipboard, or **Send by Email** to open a new message in your email application containing all the suspension information (computer name, suspend period, notes and password).

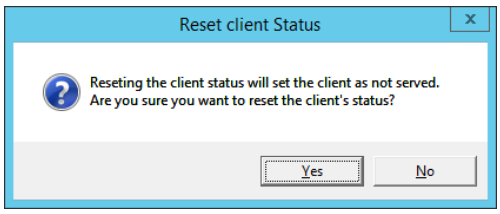
Resetting and Updating Client Status

Over time, Clients that were previously Served may not always remain Served. This option allows you to reset the status of Safend Data Protection Suite Clients which appear as Served or as blocked in the Clients table but currently may be Not Served.

1. In the Clients table, right-click the Served Client which you wish to reset, or in the Organizational tree, right-click the desired object. A menu opens.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. From the menu, select **Reset Client Status**. The following confirmation window is displayed.



Note: The **Reset Client Status** option is enabled only for Served Clients. In the Clients Table, you may select multiple Clients to reset. In the Organizational Tree, selecting an object (e.g., an OU or a domain) will reset all Clients belonging to this object.

3. From the toolbar, click **Refresh**. Client status is updated and Not Served Clients that previously appeared as Served now appear with their correct status, Not Served.

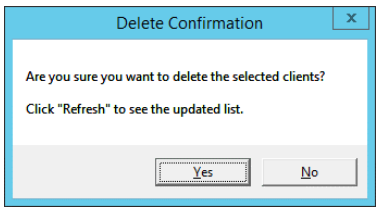
   Clients that were reset will show as Served again once they communicate with the server.

Deleting Clients that are Not in Domain

As explained earlier, the Organizational Tree may include Clients that no longer belong or never belonged to any of the tree domains and are represented in the tree under Not In Domain. Some of these Clients may no longer be relevant and you may wish to delete them from the Tree. You may choose either to delete all Not In Domain Clients (both Served and Not Served), or to delete specific Clients that are Not in Domain.

Note: A Client is added as Not In Domain as soon as it communicates with the server and is found not to belong to any Tree domain.

1. In the Organizational Tree, right-click **Not In Domain**. A menu opens.
2. From the menu, select **Delete Clients**. The following confirmation window opens:



3. Click Yes. All Clients that are Not In Domain are deleted.
4. From the toolbar, click 

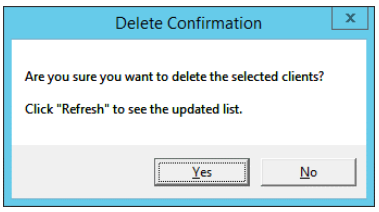
. The deleted Clients are no longer displayed.

Deleting specific clients that are not in domain

1. In the Clients table, right-click the required Client (you may delete a Client that is Not In Domain regardless of whether it is Served or Not Served). A menu opens.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. From the menu, select **Delete Clients** (Not in Domain). The following confirmation window opens:



3. Click Yes. All selected Clients that are Not In Domain are deleted.

4. From the toolbar, click Refresh. The deleted Clients are no longer displayed.

8.3.1.3 Auditing Devices

If you wish to check which devices are currently, or were previously, connected to your organization's endpoints, you may audit them. Auditing devices is done using Safend Auditor, a scanning and auditing tool described in detail in the Safend Auditor User Guide. If you want, you can launch Safend Auditor directly from the Safend Data Protection Suite.

Launching the Safend Auditor

Click the tool button. The first time you do this, you will be asked to browse to the location of your auditor.exe file. Subsequently, after you have done this once, Safend Auditor is launched and its main window opens.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

9 Viewing Logs

Events that occur on endpoints protected by Safend Data Protection Suite Clients are recorded in logs and/or alerts.

In addition to events which occur on protected endpoints, logs and alerts are also created by Safend Data Protection Suite Management Server events, such as administrator login, publishing policies and performing backups.

Logs and alerts are sent to a log repository on the Management Server at intervals as defined in the Client's policy and stored there. If necessary, they can also be collected by the administrator at other times. This chapter describes the Logs Tab, which provides various options for querying and viewing logs and alerts.

9.1 Quick Tour of the Logs Tab

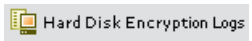
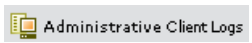
This tour refers to all logs except Server logs. The Server log windows differ in that they do not have an Organizational Tree section.

Accessing the Logs Tab

Click the Logs Tab.

The Logs window includes the tabs described in the Getting Started chapter. The launch buttons and some of the menu options are specific to the Logs Tab.

Tabs

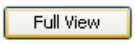
Option	Description
	This tab opens an All Logs window.
	This tab opens a Data logs window.
	This tab opens a Port & Device logs window.
	This tab opens a Hard Disk Encryption logs window.
	This tab opens an Administrative Client logs window.
	This tab opens a new Server Logs window displaying Server logs. Server logs are explained in *Logs Table*.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Toolbar

Option	Description
New Query 	Opens a new Query Properties window (for more about queries see Queries).
Query Menu	Allows query selection from a drop-down menu (for more about queries see Queries).
Edit Query 	Opens properties of the applied query for editing.
	This enables you to manage queries. It opens the Manage All Logs Queries window.
Refresh every	Refreshes the Logs Table in the active window according to the time set in the drop-down list.
Configure Logs View 	Enables you to set what fields appear in the Logs table. Refer to Configuring Logs View for more information.
	Refreshes the Logs Table in the active window.
	Displays the context sensitive help of the active window and enables access to other help topics.

Log Buttons

Button	Description
	These buttons help you navigate between entries in the table.
	This transforms the Log Details section into a separate window.
	This restores the Log Details section to its place below the Logs table.

Workspace

The workspace is divided into three areas:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- The area on the left-hand pane includes the **Organizational Tree** and **Search By Name** tabs. These tabs serve as filters for determining the origin (i.e., organizational units/computers/users) of log records displayed in the Logs Table. The tabs are discussed in *Filtering by Log Record Origin*.
  These tabs do not appear in the Server logs window, since by definition Server logs do not apply to Clients.
- The **Logs Table** appears in the upper right-hand pane and displays a table of log records received from Clients or from the Management Server. When opened initially the table displays all Client logs. The Logs table is discussed in *Logs Table*.
- **Log Details/Data View tabs** appear below the Logs table. The Log Details tab displays General Information and Component Specific Information. The Data View tab is only displayed when Data logs or All logs is selected. It displays the actual data of the incident.

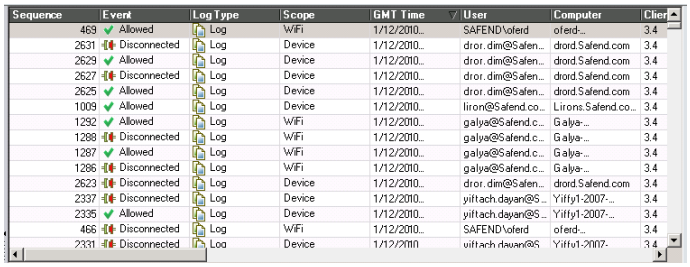
When all windows in the Logs Tab are closed, the workspace is empty. You may open a log window by clicking one of the tabs at the top of the window. Refer to Logs Table to learn about viewing logs.

9.2 Logs Table

The Logs table (shown in the figure below) displays information about events that take place in Safend Data Protection Suite Clients, Management Consoles or Management Server. There are 6 types of Logs Tables which you can view and manage:

- **All** Logs - this log displays all the log information.
- **Data** Logs - this log displays information about data.
- **Port & Device** Logs - this log displays information about ports and devices.
- **Hard Disk Encryption** Logs - this log displays information about Hard Disk encryption.
- **Administrative Client** Logs - this log displays information about administrative clients events, such as a policy update.
- **Server** Logs – this log displays information about the Management Server and administrative actions. Each record reports a specific event, such as logging into the Management Console, changing Global Policy Settings and more.

Refer to Logs Table Columns for a description of the log structure.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

The example above shows the Port and Device logs, Logs table. Each type of log displays different information in the Logs table. A detailed explanation of the table structures can be found at the end of this chapter in Logs Table Columns. You can modify the table view in the following ways:

- Sort the table by clicking the column heading of the column by which you want to sort. Clicking the header again, switch from ascending to descending order. You can add a secondary sort level by pressing the SHIFT key and clicking the secondary column heading.
- Modify column width by dragging the column separation lines.
- Move a column by dragging and dropping it into the desired position.

Whichever log type you choose to view, the number of records displayed may be overwhelming, and some of these records may not be relevant. There are, therefore, two ways in which this number can be decreased:

- **Filtering by Log Origin**: this allows you to limit log records to those originating from specific computers/users or organizational units. For an in-depth discussion of these options see *Filtering by Log Record Origin*, which discusses the Organizational Tree and the Search by Name tabs (these are not applicable to Server Logs).
- **Queries**: queries can be created in order to select records according to various parameters such as record type, time, device type and more. For an in-depth discussion of queries see
- Queries.

9.2.1 VIEWING ADDITIONAL RECORDS

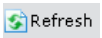
The Logs Table displays the first 1000 records that answer your query/filtering criteria. If you wish to view additional, older records, you can do so using the paging buttons that appear below the Logs Table.

Navigating to older or newer log records

Use the paging buttons that appear below the Logs Table. You may either click a specific page number, or click Next Page (»), Previous Page («) or First Page (|«) to navigate between log pages. Displaying a new page may take a while since it may require loading new data from the database. Automatic Refresh is disabled while you view pages 2 and up of the Logs Table.

Refreshing the Logs Table

The Logs Table refreshes automatically at pre-defined intervals which you determine, or as a response to an ad hoc request. The refresh process collects new data accumulated on the Management Server and then displays it in the Logs Table, in accordance with the current table sorting definition.

1. In the View menu, click Refresh, or click 

in the toolbar. New log records are added to the Logs table.

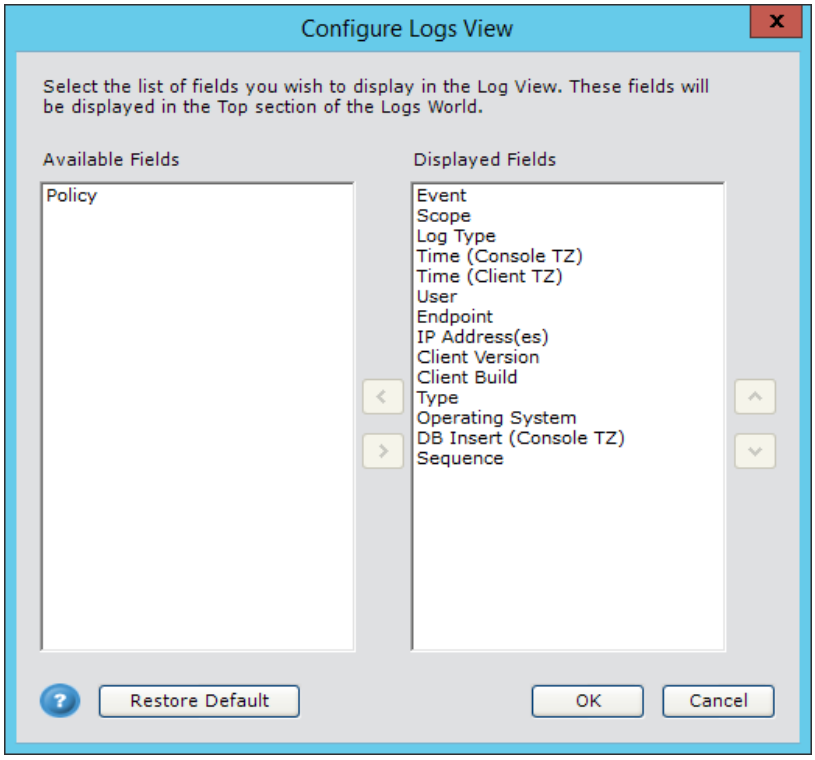
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. To set automatic refresh intervals, select the interval from the Refresh from every dropdown menu in the Toolbar.

Automatic Refresh of the Logs Table is disabled while you view pages 2 and up of the table.

Configuring Logs View

When you click in the toolbar, the following is displayed.



Here you can choose the fields that will be displayed in the Logs table. Select the field and click the left/right buttons to move fields from the Available/Displayed Fields columns. Use the up/down arrows to order the fields in the Logs table. The fields to choose from will depend on the log type selected (for example, Port & Device vs. Server logs).

Managing Shadow Files

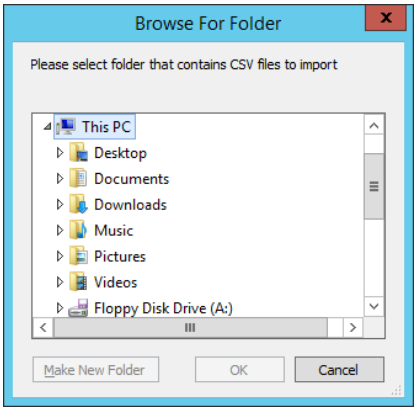
You have the ability to select multiple incidents in Data Logs and save their shadow files.

1. Select multiple Data Logs incidents with the mouse, while holding the SHIFT or CTRL keyboard keys and right-click.

2. Choose from the menu **Save shadowed files**. This option will not appear when selecting incidents that do not contain shadow files. The *Save Shadowed File(s)* dialog box will be displayed.

3. Enter a path manually or click **Browse**, to specify a local or shared folder in which to save the shadowed file(s). The Browse for Folder window will be displayed if you click **Browse**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



4. Select a folder in which to save the shadowed files.

Note: Shadowed files from different incidents will be saved in separate sub-folders.

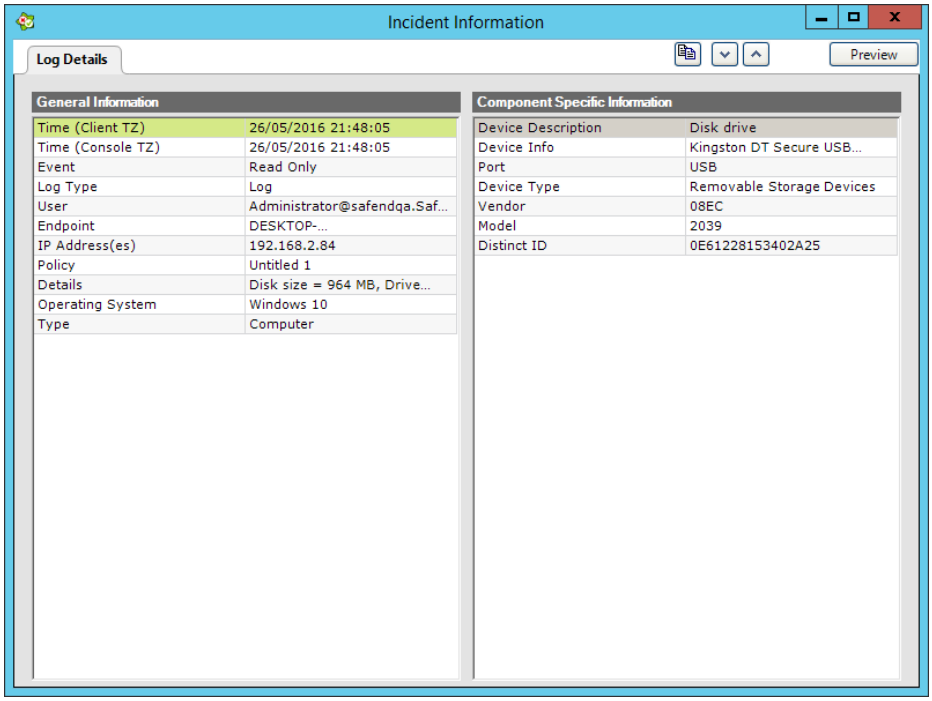
5. After choosing a folder in Browse For Folder, click **OK** in Save Shadowed File(s).

6. A message, Shadow files have been saved successfully, will be displayed if the files were saved successfully. Incident folders will contain all their shadow files, and each filename will be similar to the shadow filename in the console.

Log Details

Below the Logs table is Log Details. This displays the details for each entry in the Logs table. For each log type different information is displayed.

When you click Full View the following window is displayed.



The information provided is divided into General Information and Component Specific Information (except for Server Logs).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Viewing Log Record Properties

This option allows you to view record properties in the Log Details section, below the Logs Table, instead of scrolling across the Logs Table.

- To view record properties: Click an entry in the Logs table. The properties are displayed in Log Details.
- To copy values from Log Details to the clipboard: Right click the mouse on an entry in Logs Details and select Copy or press ctrl+ c. You can now copy the value to Notepad, etc.

Data View

The Data View tab is also displayed below the Logs table when All logs or Data Logs are selected. This displays the actual data of the incident, for each entry in the Logs table.

The lower half of the window is divided up into the Incident Tree, on the left and Classification Details on the right.

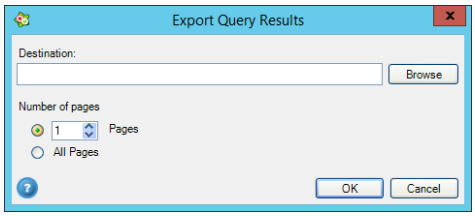
When you select an item in the Incident tree, its text will be displayed above in the upper half of the window, in Text View. You can search this text for specific words or phrases, highlight matches and open the policy or Data Classification. When you select a shadow file in the Incident Tree and click Open, the shadow file will be opened using the native default program that is defined by Windows to open the selected shadow file type.

In Classification Details all the Data rules that match the specific incidents will be displayed. Each data rule listed can be opened and viewed.

Exporting the Logs Table

The Logs Table can be exported using the Export Query Results window.

To open the Export Query Results window: From the File menu, select **Export**. The Export Query Results window opens:



Exporting Query Results

Use this option to export the Logs Table (i.e., the query results) in order to print it or perform further analysis. The file is saved in XML format which can easily be opened with MS Excel, etc.

1. Click the **Browse** button to select a path or type in the path for the exported file. You may use the default file name or change it.
2. If you want to select only the latest records of the query results, click the first radio button and select how many pages you wish to export.
3. If you want to export all query result pages, select the **All Pages** radio button.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

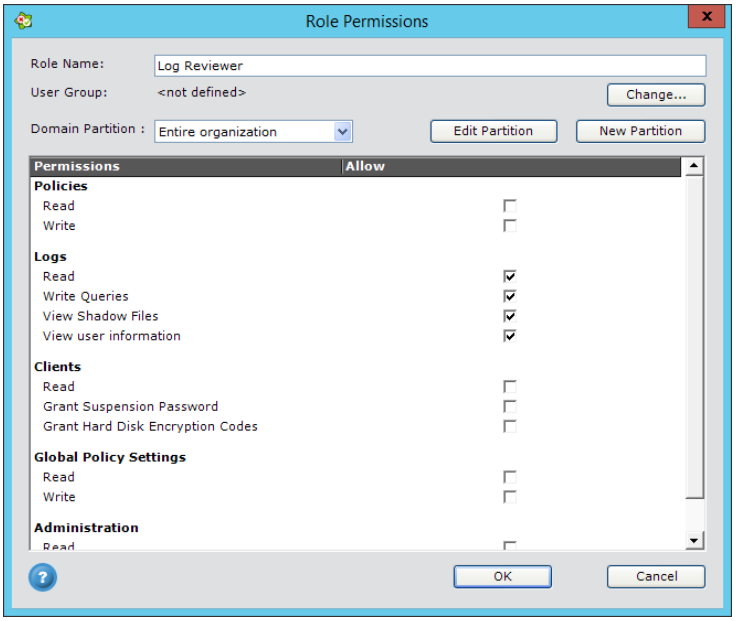
Note: Exporting the entire query may take a long time.

4. Click **OK**. A progress window opens and exporting begins.

Hiding User Information in Logs

This option enables an administrator to set privacy rules with their data protection solution, to protect employee information and privacy from being monitored by third-party groups, IT administrators or automated systems. In such cases, personal user information or any information which can be used to identify the user is hidden from monitoring systems, and only authorized personnel are able to access this information.

The privacy rule can be defined using Role Permission in Safend Data Protection Suite's role based management.



When a user, that does not have permission to view user information, logs into the console, he will not be able to view\perform the following:

- Users\Computers under Logs tab
- Users\Computers under log details
- Click "Show logs of this user\computer" context menu option
- Users\Computers information on exported logs query results (Logs Tab-->run a query-->file-->export)
- Run reports that specifically contain user\machine information
- Searching in the Logs tab according to a specific user\machine.

Filtering by Log Record Origin

This section does not apply to Server logs.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

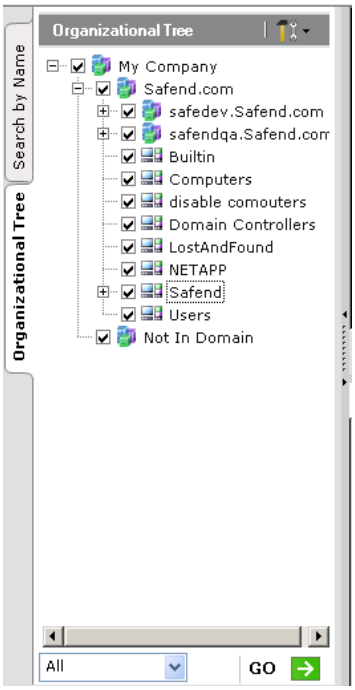
The left pane of the main Logs window includes two tabs to help you determine the organizational units or computers/users whose logs will be displayed in the Logs Table. These are the Organizational Tree and the Search by Name tabs.

Filtering the Logs Table by Organizational Unit

The Organizational Tree is a tool you use to determine the Organizational Units whose log records will be displayed in Client or File logs. Together with queries (see

Queries), selection of items in the Organizational Tree determines which records are displayed in the Logs Table (see Logs Table). This section describes how to manage the Organizational Tree and how to determine, from the Tree, which logs and alerts to display in the Logs Table.

The Tree does not appear in the Server logs window, since by definition Server logs do not apply to computers or users. The Organizational Tree tab displays the domain(s), organizational units and the Not In Domain group (which includes all computers who do not currently belong to any domain), as shown in the following figure:

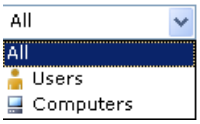


Note: The Organizational Tree is applicable only if you are using Active Directory or Novell eDirectory. If you are not, only one group is displayed in the Tree – Not In Domain. Selecting this group selects all computers.

Selecting red organizational units

1. If necessary, expand the Organizational Tree to view lower-level organizational units.
2. Select the required domain or organizational units by checking the appropriate checkboxes.
3. At the bottom of the Organizational Tree tab, select the type of objects you would like to view from the drop down menu.

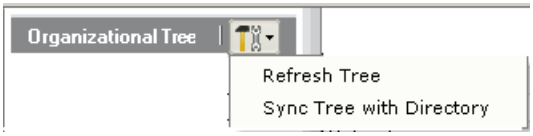
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



4. At the bottom of the Organizational Tree tab, click GO. The logs now displayed in the logs table originate from Clients that belong to your Tree selection, and only them.

Updating the Organizational Tree

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from Safend Data Protection Suite Management Server, or synchronize it with Active Directory/Novell eDirectory (the Directory may be more up-to-date, but may also take longer). Updating the Tree is done from the Organizational Tree Update menu (shown below) which is found at the top of the Organizational Tree tab.



- To update the Organizational Tree from the Management Server: From the Organizational Tree Update menu, click **Refresh Tree**. The Tree is updated.
- To update the Organizational Tree from the Directory: From the Organizational Tree Update menu (see previous figure), click **Sync Tree with Directory**. The Tree is updated, but this may take a while.

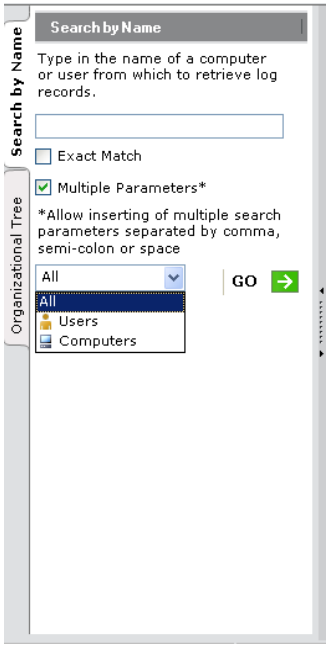
Filtering the Logs Table by Name

The Search by Name tab is an additional tool that you can use to determine the computers or users whose log records the Client or File log will display. The search criteria you enter here, along with queries (see

Queries), determine which records are displayed in the Logs Table (see Logs Table). This section describes how to use this tab to determine the logs displayed in the Logs Table.

As mentioned, this tab does not appear in the Server log window, since by definition Server logs do not apply to computers or users. The following figure shows the Search by Name tab:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Searching for specific computers or users

1. In the text box, enter the name of the computer or user whose log record you wish to display in the Logs Table. You may enter multiple names separated by a comma, semicolon or space.
2. Check the **Exact Match** checkbox if you want the Logs Table to display logs for a computer/user with the name that exactly matches the string you entered in the text box. For computers you must enter the full computer name (including the domain suffix). If Exact Match is not selected, the Logs Table will contain logs for all computers and users whose name contains the string that you entered.
3. From the Search by Name menu, select **Computers** if you want to search computer names, **Users** if you want to search user names or **All** if you want to search both computers and users.
4. Below the text box, click GO. The logs now displayed in the logs table originate from the computer/user (one or more) whose name matches your search criteria. If no computer or user is found whose name matches your search criteria the logs table will be empty.

9.3 Queries

Another method for filtering log records in the Logs Table is the use of queries. You can define queries according to various criteria, or properties, so that only log records that match your specified criteria appear in the Logs Table. Queries interact with your Organizational Tree selection to determine which records are displayed. Query types are available for all the available log types.

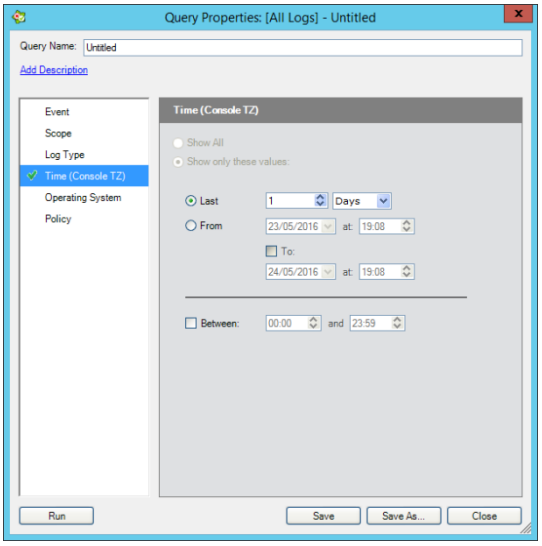
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Queries may be defined and edited on an ad-hoc basis, or saved for future use. The default query is All Logs, which displays all the log records (to be exact – those that match your Organizational Tree selection criteria).

Queries are defined in the Query Properties window. A different window is displayed for each log type (Server logs, Data logs, etc.). This section discusses this topic in general, the query properties for each log type differ.

Opening the Query Properties window

In the toolbar, click the **New Query** button . The Query Properties window opens:



The Query Properties window displayed here is for All logs and will differ for each log type. You can also open this window from the Manage Queries window by clicking the New button. (see Managing Queries). The Query Properties window has two sections:

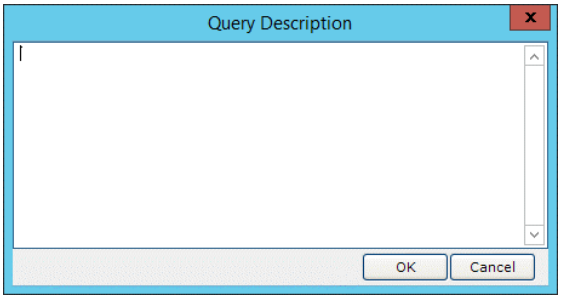
> The **left pane** displays the various tabs in which you define the query properties. Depending on the log type, these tabs will vary.

> The **main window** displays the corresponding definitions for the selection in the left pane. The definitions you make in these tabs form the criteria for deciding which records will be displayed in the Logs Table; records must match the defined criteria.

Query Properties Windows

1. At the top of the Query Properties window, in Query Name you enter the name of the Query. Below this, if you click on Add Description you can enter a description about this query in the Query Description window. Click **OK** to save your description.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



2. After entering the various Query Properties, click **Save** or **Save As** if you are changing an existing Query under a new name. Click **Close** to close the window without making any changes. Click **Run** to run the query.

The following is a description of the different types of Query Properties windows.

Category	Description
Server Logs Filters	
Event	Choose the events you want the log to display, by checking the appropriate checkbox(es).
Log Type	Select whether you would like the Logs table to display both logs and alerts, or only alerts.
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Details	Displays additional details when available: e.g., license alert details, policy name in case of Policy Published event, etc.
Port & Device Logs Filters	
Event	Choose the events you want to query. Show All the events (default) or chose Show only these options and check the events of interest (e.g., Allowed, Disconnected, Blocked).
Log Type	Specify whether the record is a log or an alert or both (Show All).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Scope	Choose to what scope the event applies. Show All (default) or chose Show only these options and check the options of interest (Port, Device, Storage, WiFi).
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Operating System	Choose Show All (default) or Show only these values and choose the relevant operating systems.
Policy	The name of the policy that applied to the reporting client. Show All (default) or chose Show only these options and type in the name of the specific policy.
Policy Type	Choose Show All (default) or Show only these options and choose the type of policy (e.g., User, Computer or Suspended).
Device Description	Show All (default) device descriptions or chose Show only these options and type in the name of a specific device description (e.g., Disk Drive, USB Human Interface Device).
Device Info	Show All (default) device info or chose Show only these options and type in specific device info (e.g., Intel(R) 945G/GZ/GC/P/PL Processor).
Port	Show All (default) ports or chose Show only these options and check the ports of interest (e.g., USB, Serial, WiFi).
Device Type	Show All (default) device types or chose Show only these options and type in the name of a specific device type (e.g., Smart Disks, Human Interface Device).
Vendor Name	Show All (default) vendor names or chose Show only these values and select a specific vendor name from the drop-down list.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Vendor	Show All (default) vendors or chose Show only these options and type in a specific vendor ID.
Model	Show All (default) models or chose Show only these options and type in a specific model ID.
Distinct ID	Show All (default) Distinct IDs or chose Show only these options and type in a specific Distinct ID.
Disk Size	Show All (default) disk sizes or chose Show only these options and choose the disk size range.
Encryption	Show All (default) encryption methods or chose Show only these options and check the encryption methods of interest (e.g., Disabled, WEP, TKIP, AES).
Authentication	Show All (default) authentication methods or chose Show only these options and check the authentication methods of interest (e.g., Open, WPA).
Details	Show All (default) details or chose Show only these options and type in specific details (e.g., Disk size).
Data Logs Filters	
Data Channel	Choose the data channel you want to query. Show All the data channels (default) or chose Show only these options and check the channels of interest (e.g., Email, Web, External Storage).
Event	Choose the events you want to query. Show All the events (default) or chose Show only these options and check the events of interest (e.g., Allowed, Blocked, Encrypted).
Log Type	Specify whether the record is a log or an alert or both (Show All).
Scope	Choose to what scope the event applies. Show All (default) or chose Show only these options and check the options of interest.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Operating System	Choose Show All (default) or Show only these values and choose the relevant operating systems.
Policy Type	Choose Show All (default) or Show only these options and choose the type of policy (e.g., User, Computer or Suspended).
Policy	The name of the policy that applied to the reporting client. Show All (default) or chose Show only these options and type in the name of the specific policy.
Device Description	Show All (default) device descriptions or chose Show only these options and type in the name of a specific device description (e.g., Disk drive).
Device Info	Show All (default) device info or chose Show only these options and type in specific device info (e.g., CBM Flash Disk USB Device).
Port	Show All (default) ports or chose Show only these options and check the ports of interest (e.g., USB, Serial, WiFi).
Device Type	Show All (default) device types or chose Show only these options and check the device types of interest (e.g., Removable Storage Devices, CD/DVD Drives).
Vendor Name	Show All (default) vendor names or chose Show only these values and select a specific vendor name from the drop-down list.
Vendor	Show All (default) vendors or chose Show only these options and type in a specific vendor ID.
Model	Show All (default) models or chose Show only these options and type in a specific model ID.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Distinct ID	Show All (default) Distinct IDs or chose Show only these options and type in a specific Distinct ID.
Disk Size	Show All (default) disk sizes or chose Show only these options and choose the disk size range.
Details	Show All (default) details or chose Show only these options and type in specific details.
File Name	Show All (default) files or chose Show only these options and type in the name of the specific file.
Extension	Show All (default) files extensions or chose Show only these options and type in a specific file extension (e.g., txt, doc).
File Size	Show All (default) files size or chose Show only these options and choose the file size range.
Created	Define the time period in which the file were created you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Modified	Define the time period in which the files were created. See the preceding description for Created.
Operation	Show All (default) operations or chose Show only these options and select the operations of interest (e.g., Write, Read).
File Type	Show All (default) file types or chose Show only these options and select the file types of interest (e.g., Microsoft Office).
Security Action	Show All (default) security actions or chose Show only these options and select the security actions of interest (e.g., Allow, Block).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Classification Name	Show All (default) classification names or chose Show only these options and type in a specific classification name.
Data Rules	Show All (default) data rules or chose Show only these options and type in a specific data rule.
User Justification	Show All (default) user justifications or chose Show only these options and type in a specific user justification (e.g., I've made a mistake).
Justification Notes	Show All (default) justification notes or chose Show only these values and type in a specific justification note.
Keywords	Show All (default) keywords or chose Show only these options and type in a specific keyword.
Destination Group	Show All (default) Destination Groups or chose Show only these options and type in a specific Destination Group.
Matched Classifications	Show All (default) Matched Classifications or chose Show only these options and type in a specific Matched Classification.
Added Classifications	Show All (default) Added Classifications or chose Show only these options and type in a specific Added Classification.
Removed Classifications	Show All (default) Removed Classifications or chose Show only these options and type in a specific Removed Classification.
Sensitivity Level	Show All (default) sensitivity levels or chose Show only these values and type in a specific sensitivity level.
Administrative Client Logs Filters	
Event	Choose the events you want to query. Show All the events (default) or chose Show only these options and check the events of interest.
Log Type	Specify whether the record is a log or an alert or both (Show All).
Scope	Choose to what scope the event applies (e.g., Admin). Show All (default) or chose Show only these options and check the options of interest.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Operating System	Choose Show All (default) or Show only these values and choose the relevant operating systems.
Policy	The name of the policy that applied to the reporting client. Show All (default) or chose Show only these options and type in the name of the specific policy.
Details	Displays additional details when available. Choose Show All (default) or Show only these options and type in, e.g., a policy name.
Hard Disk Encryption Logs Filters	
Event	Choose the events you want to query. Show All the events (default) or chose Show only these options and check the events of interest (e.g., Encryption Started, Encryption Failed).
Log Type	Specify whether the record is a log or an alert or both (Show All).
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Operating System	Choose Show All (default) or Show only these values and choose the relevant operating systems.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Category	Description
Details	Show All (default) details or chose Show only these options and type in specific details.
All Logs Filters	
Event	Choose the events you want to query. Show All the events (default) or chose Show only these options and check the events of interest (e.g., Allowed, Encrypted, Blocked).
Scope	Show All (default) or chose Show only these options and check the options of interest (e.g., WiFi, Port, Data).
Log Type	Specify whether the record is a log or an alert or both (Show All).
Time (Console TZ)	Define the time frame for the records you wish to display. Select the Last radio button to select a time period relative to the present time (hour, day, week or month). Select the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed. Select the Between checkbox if you wish to add a time window for the selected period, either for Last or From.
Operating System	Choose Show All (default) or Show only these values and choose the relevant operating systems.

Running a New Query

In the Query Properties window, after saving the query click **Run**. The query is activated and the Logs Table displays records matching your query criteria.

Note: If you do not save and name the new query before running it, it will not be available for future use once it is no longer the active query.

Saving a New Query

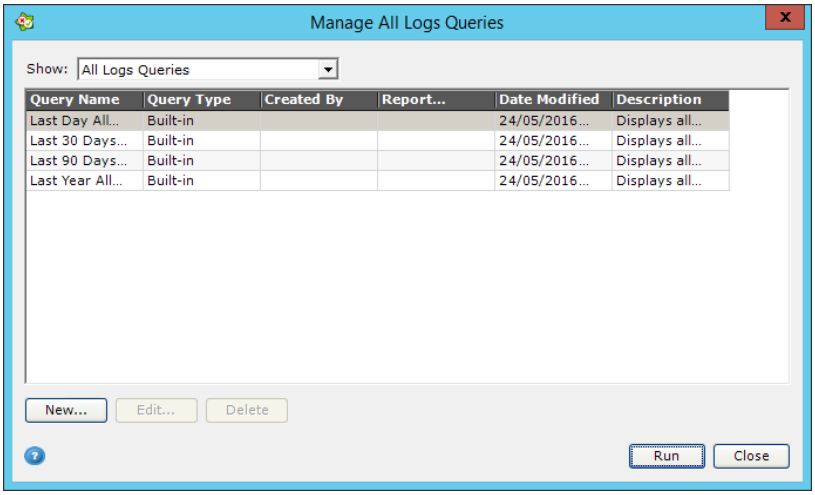
Once you have completed the query definition, you can save the query for repeated use in the future.

1. In the Query Properties window, click **Save As**. A Save As window opens.
2. In the Save As window, enter the desired Query Name and click **OK**. The query is saved and from now on can be selected from the Query menu in the toolbar.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Managing Queries

From the toolbar, click the **Manage Queries** button Queries. The Manage Queries window is displayed:



The Manage Queries window displays the built-in queries, as well as your saved queries for selected query type (Server logs, Port & Device logs, Data logs, Administrative Client logs, Hard Disk Encryption logs and All logs). In this window you can perform the following activities:

> Define new queries, explained in Creating a Query.

> Edit existing queries, explained in Editing a Query.

> Delete queries, explained in Deleting a Query.

> Rename queries, explained in Renaming a Query.

> Run queries, explained in Running a Previously Defined Query.

As a default, this window lists all queries for the active log type (Server logs, Port & Device logs, Data logs, Administrative Client logs, Hard Disk Encryption logs and All logs). If you wish, you can show and manage queries for a different log type.

Creating a Query

The process of creating a new query is explained in detail in

Queries. The Query Properties window, in which you define the new query's properties, can also be opened from the Manage Queries window by clicking the **New** button.

Editing a Query

A query can be edited when there is a need to change its properties, or when you want to use it as a template for creating a new query.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

> Either from the toolbar, click the **Edit** button . The Query Properties window opens. Make the changes.
> OR,
> in the Manage Queries window, select the query you wish to edit from the query list.

> Click **Edit**. The Query Properties window opens. Make the desired changes.
> OR,
> in the Manage Queries window, from the query list, right-click the query you wish to edit. From the right-click menu, select **Edit**. The Query Properties window opens. Make the desired changes.

Deleting a Query

1. In the Manage Queries window, select the query you wish to delete from the query list (you can use CTRL + SHIFT to select more than one query to delete).
2. Click **Delete**. A verification window opens.
3. Click **Yes** to delete the query(s), or **No** to cancel.

OR

4. From the query list, right-click the query you wish to delete (before you right-click, you can use CTRL + SHIFT to select more than one query to delete).
5. From the right-click menu, click **Delete**. A verification window opens.
6. Click **Yes** to delete the query(s), or **No** to cancel.

Renaming a Query

1. In the Manage Queries window, select the query you wish to rename from the query list.
2. Right click this query and select **Rename** form the menu.
3. The Query Name is now selected and can be edited.

Running a Previously Defined Query

Running a query applies the query criteria as you have defined them. Along with the Organizational Tree selection, this determines which records appear in the Logs Table. There are various ways in which you can run a previously defined query: from the toolbar, from the Manage Queries window using the Run button, from the Manage Queries window using the right-click menu or from the Manage Queries window by double-clicking the query.

1. To run a previously defined query from the toolbar: click the Query menu and select the query you wish to apply. The query is applied to the Logs Table.
2. To run a previously defined query from the Manage Queries window: select the query you wish to run from the query list.
3. Do either Click **Run**, right-click the query in the query list, in the right-click menu, click **Run**. The query is applied to the Logs Table.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Note: If the query belongs to a different type than the active Logs Table (for example, the active Logs Table shows Client logs and the query applies to Server logs), a new, additional Log window opens displaying the new Logs Table.

9.3.1 Collecting Logs

This option enables you to collect logs from a served computer outside the scheduled collection times, in order to view its most recent information. Activating this function collects all log types. Refer to Retrieving Latest Information from a Client in Chapter 8, Managing Clients for instructions.

9.3.1.1 Tracking Client Task Progress

When the application is in the process of performing tasks (such as collecting logs or updating policies), you may view the progress of these tasks. Refer to *Tracking Client Task Progress*, in Chapter 8 *Managing Clients for instructions*.

9.3.1.2 Logs Table Columns

- Data Logs
- Port & Device Logs
- Hard Disk Encryption Logs
- Administrative Client Logs
- Server Logs

Column	Description
Data Logs	
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.
Event	Event type.
Log Type	Specifies whether the record is a log or an alert.
Scope	Specifies what scope the event applies to (e.g., Port, Storage, Admin, Tampering).
Time	Displays the GMT time of the event, in terms of Management Console time.
User	Relevant username for the event.
Computer	Relevant computer for the event.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Client Version	The version of the client software.
Client Build	The Build number of the client software.
Operating System	The operating system being used.
Client Local Time	The event time, in terms of the time of the Client reporting the event.
DB Insert	The time the event was inserted into the database in terms of Management Console time.
Group	The group of approved devices, storage devices or WiFi connections, to which the device or connection associated with the event belongs.
Policy Type	Specifies whether the applied policy is a computer policy or a user policy.
Policy	Policy name that is applied to the reporting Client. If policies are merged on this Client, all merged policies are listed.
Device Description	Device associated with the event. (The device description is derived from the device.)
Device Info	The device associated with the event. (The information is derived from the device.)
Port	Port type of the port associated with the event.
Device Type	Device type of the device associated with the event.
Vendor	Device vendor.
Model	Device model.
DistinctID	Device distinct ID, when available.
Disk Size	Size of the device when available.
Details	Additional information when necessary: e.g., encryption type (for WiFi network encryption), tampered file name, etc.
File Name	Path and name of the logged file.
Extension	Extension of the logged file.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
File Size	Size of the logged file, in bytes.
Created	This column displays the date and time when the logged file was created.
Modified	Date and time when the logged file was modified.
Operation	Read Write Read (encrypted) Write (encrypted) Read (offline) Write (offline).
File Type	The name of the file type (e.g., Microsoft Word).
Data Channel	The channel to which the sensitive data has been transferred.
Monitoring Level	It is either, Incident, Text and Incident, or Shadow and Incident.
Classification Name	The name of the classification of which the security action was based.
Secondary Classifications	Additional classifications which match the data.
Data Rules	Classification rules which match the data.
User Justification	The user justification for the action based on the drop-down selection.
Justification Notes	The user justification for the action using free text.
Keywords	Enables the administrator to filter data logs according to specific keyword matching.
Destination Group	Enables the administrator to filter data logs according to the data Destination Group name.
The following columns relate to end-user based data classification (refer to *End-user Based Data Classification* for more information). When the user is asked to classify data he can either approve the data classification that was matched by the system, add another classification that has not been matched, or remove the suggested classification	

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Matched Classifications	Enables the administrator to filter Classify events that contain data classifications that were approved by the user.
Added Classifications	Enables the administrator to filter Classify events that contain data classifications that were manually added by the user.
Removed Classification	Enables the administrator to filter Classify events that contain data classifications that were manually removed by the user.
Port & Device Logs	
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.
Event	Event type.
Log Type	Specifies whether the record is a log or an alert.
Scope	Specifies what scope the event applies to (e.g., Port, Storage, Admin, Tampering).
Time	GMT time of the event, in terms of Management Console time.
User	Relevant username for the event.
Computer	Displays the full name (including the domain suffix) of the computer to whom the event applies.
Client Version	The version of the client software.
Client Build	The Build number of the client software.
Operating System	The operating system being used.
Client Local Time	Displays the event time in the local time of the Client that reported this event.
DB Insert	Displays the time the event was inserted into the database in terms of Management Console time.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Policy	Displays the name of the policy that is applied to the reporting Client. If policies are merged on this Client, all merged policies are listed.
Group	Displays the name of the group of approved devices, storage devices or WiFi connections, to which the device or connection associated with the event belongs.
Device Description	Displays the description of the device associated with the event. The device description is derived from the device.
Device Info	Displays the device information of the device associated with the event. The device information is derived from the device.
Port	Displays the port type of the port associated with the event.
Device Type	Displays the device type of the device associated with the event.
Vendor	Displays the device vendor.
Model	Displays the device model.
DistinctID	Displays the device distinct ID, when available.
Disk Size	Displays the size of the device when available.
Details	Displays additional information when necessary: e.g., encryption type (for WiFi network encryption), tampered file name, etc.
Hard Disk Encryption Logs	
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.
Event	Displays the event.
Log Type	Specifies whether the record is a log or an alert.
GMT Time	Displays the GMT time of the event, in terms of Management Console time.
User	Displays the name of the user to whom the event applies.
Computer	Full name (including the domain suffix) of the computer to whom the event applies.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Client Version	The version of the client software.
Client Build	The Build number of the client software.
Operating System	The operating system being used.
Client Local Time	Displays the event time in the local time of the Client that reported this event.
DB Insert	Displays the time the event was inserted into the database in terms of Management Console time.
Details	Displays additional information when necessary.
Administrative Client Logs	
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.
Event	Displays the event type.
Log Type	Specifies whether the record is a log or an alert.
Scope	Specifies what scope the event applies to (e.g., Admin, License).
Time	Displays the GMT time of the event, in terms of Management Console time.
User	Displays the name of the administrator to whom the event applies.
Computer	Displays the full name (including the domain suffix) of the computer to whom the event applies.
Client Version	The version of the client software.
Operating System	The operating system being used.
Client Build	The Build number of the client software.
Client Local Time	Displays the event time in the local time of the Client that reported this event.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
DB Insert	Displays the time the event was inserted into the database in terms of Management Console time.
Policy	Displays the name of the policy that is applied to the reporting Client. If policies are merged on this Client, all merged policies are listed.
Details	Displays additional details when available: e.g., license alert details, policy name in case of Policy Published event, etc.
Server Logs	
Event	License Admin Login/Logout Policy Saved Policy Published Policy Deleted Suspension Password Generated Global Policy Settings Changed Administration Changed Backup Succeeded Backup Failed Emergency Database Purging HD Encryption Reset Key Granted HD Encryption One-Time Key Granted HD Encryption Recovery Key Granted
Log Type	Specifies whether the record is a log or an alert.
Scope	Specifies what scope the event applies to (e.g., Admin, License).
Time	Displays the GMT time of the event, in terms of Management Console time.
User	Displays the name of the administrator to whom the event applies.
Computer	Displays the name of the Management Console to whom the event applies.
Details	Displays additional details when available: e.g., license alert details, policy name in case of Policy Published event, etc.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

10 Running Reports

Safend Reporter provides security and IT personnel with built-in reports that enable visibility into an organization's security status and operational needs. The reports can be divided into two groups: security reports and administrative reports.

- Security reports enable you to detect violations of security policies in a variety of views and levels of detail.
- Administrative reports help IT managers during the process of deployment, policy distribution, training and on-going status of asset management in the organization.

Note: This is a separate product offered as an add-on, requiring an additional license.

Security and IT personnel can view these reports from the Management Console. This information can also be exported into several standard formats to be viewed by non-technical viewers, such as the executives in the organization. Reports can also be scheduled and sent periodically by email to predefined recipients, in order to ensure continuous tracking of an organization's security status.

Each generated report includes the ability to drill down in order to view a detailed analysis of specific aspects of the report. This enables administrators to investigate suspicious patterns shown in a high-level view of the organization by drilling down to a specific incident's details and the relevant log entries.

10.1 Report Definitions

The process of defining a report involves selecting one of the Built-in reports provided by Safend Data Protection Suite, defining the parameters of the report (for example: timeframe, organizational units, devices to be included and so on) and then generating the report. Once a report has been generated you can save its settings and then generate it again in the future. Each time a report is generated, it extracts the data from the database. The Reports Tab provides a list of both the Built-in reports and the reports that were saved by Safend Administrators. You can easily re-run any of them to show the latest information.

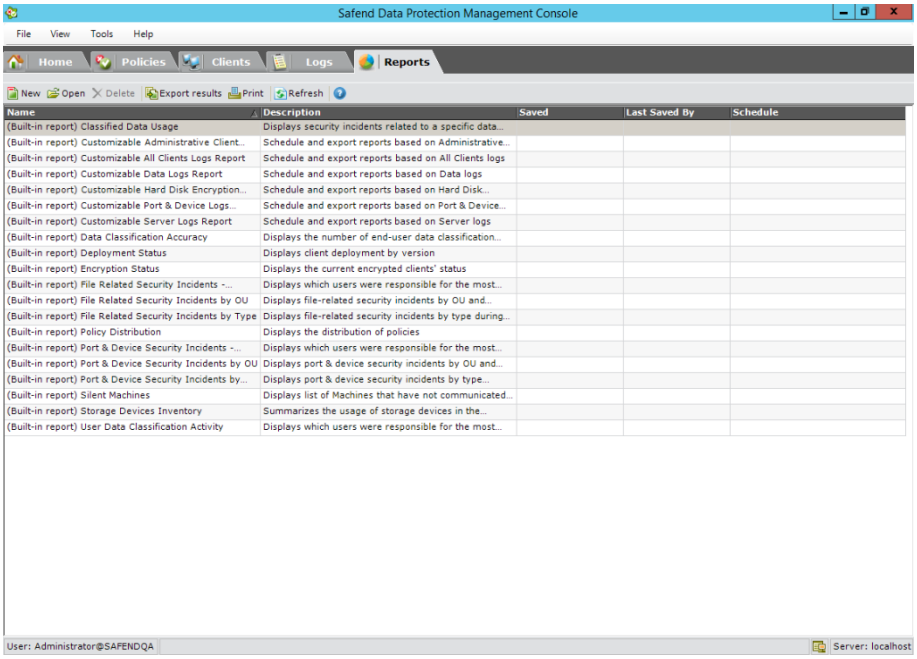
Each Built-in report in Safend Data Protection Suite is provided with a set of default parameters. You can run the Built-in report without the need to save its definitions. If you want to modify the default parameters provided with a Built-in report, then you can do so and then run the report and optionally save these definitions to be used again under a different name (the definition of the Built-in reports cannot be overwritten). You may decide to generate multiple new report definitions from the same Built-in report. This may be useful if each report covers a different part of your organization and/or different time frames.

10.2 Quick Tour of the Reports Tab

This quick tour describes the elements in the Reports Tab windows.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

To access the Reports Tab: Click the Reports tab to display the Reports window, as shown below:



Workspace

Each report that is defined in Safend Data Protection Suite is based on a Built-in report. The Report Definitions list provides a row for each Built-in report and each report definition that was modified and saved.

Menus

Option	Description
File	
Print	Generates and prints the report that is selected in the Report Definitions list. This report shows the most updated information that is specified in the report definition.
Export Results	This enables you to export the report in various file formats. It opens the Export Results As window. Here you choose a name for the report and the format in which you want to receive the report. **Note** Customizable reports can only be exported in excel (.xls) format.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Toolbar

Button	Description
	Enables you to define a new report, based on a Built-in report (See Defining a New Report).
	Generates and displays the report that is selected in the Report Definitions list. This report shows the most updated information that is specified in the report definition.
	This enables you to delete a report.
	Generates and displays the report that is selected in the Report Definitions list. This report shows the most updated information that is specified in the report definition. Click Export Results inside a report and the Export Results As window is displayed. Here you choose a name for the report and the format in which you want to receive the report. **Note**: Customizable reports can only be exported in excel (.xls) format.
	Generates and prints the report that is selected in the Report Definitions list. This report shows the most updated information that is specified in the report definition.
	This refreshes the items displayed.
	Displays the context-sensitive help of the active window and enables access to other help topics.

10.2.1.1 Built-in Reports

The following describes the features and benefits of each of the Built-in reports that come with the add-on module to Safend Data Protection Suite. Each of these is accessible by clicking the relevant report name tab that appears at the top of the window or by following the instruction provided in the Running a Report section below.

Report	Description
Classified Data Usage Report	This displays security incidents related to a specific data classification during the selected time frame.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Customizable Administrative Client Logs Report	This is a schedule and export report based on Administrative Client logs.
Customizable All Clients Logs Report	This is a schedule and export report based on All Clients logs.
Customizable Data Logs Report	This is a schedule and export report based on Data logs.
Customizable Hard Disk Encryption Logs Report	This is a schedule and export report based on Hard Disk Encryption logs.
Customizable Port & Device Logs	This is a schedule and export report based on Port & Device Logs.
Customizable Server Logs Report	This is a schedule and export report based on Server logs.
Data Classification Accuracy Report:	This displays the number of end user data classification results for a specific data classification during the selected time frame.
Deployment Status Report	This displays client deployment by version.
Encryption Status Report	This displays the current encrypted clients' status.
File Related Security Incidents by Users Watch List Report	This displays which users were responsible for the most file related security incidents during the selected time frame.
File Related Security Incidents by Users and Organizational Units Report	This displays file-related security incidents by OU and users during the selected time frame.
File Related Security Incident by Type Report	This displays file-related security incidents by type during the selected time frame.
Policy Distribution Report	This displays the distribution of policies.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Safend Inspector – Classified Data Usage Reports	This displays security incidents related to a specific data classification during the selected time frame.
Security Incidents by Users Watch List	This displays which users were responsible for the most security incidents.
Security Incidents by Users and Organizational Units Report	This displays security incidents by OU and users during the selected time frame.
Security Incident Types Report	This displays security incidents by type during the selected time frame.
Silent Machines Report	This displays a list of machines that have not communicated with the server during the selected time frame.
Storage Device Inventory Report	Summarizes the usage of storage devices in the selected organizational units during the selected time frame.
User Data Classification Activity Report	This displays which users were responsible for the most data classification activities during the selected time frame.

10.2.1.2 CLASSIFIED DATA USAGE REPORT

This report displays security incidents related to a specific data classification during the selected time frame.

- **Customizable Administrative Client Logs Report**: a schedule and export report based on Administrative Client logs.
- **Customizable All Clients Logs Report**: a schedule and export report based on All Clients logs.
- **Customizable Data Logs Report**: a schedule and export report based on Data logs.
- **Customizable Hard Disk Encryption Logs Report**: a schedule and export report based on Hard Disk Encryption logs.
- **Customizable Port & Device Logs**: a schedule and export report based on Port & Device Logs.
- **Customizable Server Logs Report**: a schedule and export report based on Server logs.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **Data Classification Accuracy Report**: displays the number of end user data classification results for a specific data classification during the selected time frame. This enables you to determine the accuracy of the classification in terms of the false positive and false negative ratio.
- **Deployment Status Report**: This report shows the progress of the Safend Data Protection Suite Client deployment process across the enterprise. The report shows the percentage of the organization's computers that are protected by the Safend Client and provides a detailed list of the computers that have not yet been protected.
  The pie chart in this report shows the distribution of Safend Data Protection Suite Client versions in the selected organizational units. The computers on which Safend Data Protection Suite is not deployed are indicated by the words Not Served.
  A table appears at the bottom of this report listing the versions of Safend Data Protection Suite Clients in each row and indicating their build number, number of clients on which it is installed and the percentage of all the clients in the report on which each Safend Data Protection Suite Client version is installed.
- **Controls for Deployment Status Report**: Organizational Tree: The Organizational Tree, located on the left, displays the domain(s), organizational units, groups, users and computers in your organization. This report enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree.
  You can use the Search option to find an organizational unit in the Organizational Tree. Enter any string and click the Search button to display a list of all the organizational units that contain or start with this string in their name. You can then check off each relevant option in the list to include it in the report.
  - **Drilldown and Linked Information from the Deployment Status Report**: The following additional information can be displayed by clicking links in this report. Some of these links show other more detailed (drilldown) reports and other links simply show more information:
  - **Not** Served**:** The **Not Served** link in the table at the bottom of the report enables you to display a list of the computers on which Safend Data Protection Suite is not deployed. This list only shows those computers that are within the range of the options that you selected in the Organizational Tree in this report.

Encryption Status Report

This report shows the encryption status of all the Clients: the percentage (number) of encrypted machines vs. unencrypted machines.

10.2.1.3 Controls for Clients Encryption Status Report

This report provides the following controls for specifying the content of the report:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **Time Frame:** Enables you to specify the timeframe in which the machines last communicated with the management server. You can specify the Last days or hours, or an exact Time Frame indicating from/to which date. You may use the Between time, to further narrow your results.
- **Organizational Tree**: The Organizational Tree enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree.

Drilldown and Linked Information from the Clients Encryption Status Report

The following additional information can be displayed by clicking links in this report:

- **Unencrypted Machines** enables you to display a list of each of the unencrypted machines, listing the **Computer Name** and **Domain Name** of each unencrypted machine.
- **Encrypted Machines** enables you to display a list of each of the encrypted machines, listing the **Computer Name**, **Domain Name** and **Encryption Completed On** (date and time) of each unencrypted machine.

File Related Security Incidents by Users Watch List Report

This report shows which users were responsible for the most file related security incidents during a specified time frame.

File Related Security Incident by Type Report

This report shows security incidents on files by incident type during a specified time frame. You can define which types of security incidents are to be shown according to the security guidelines of your organization.

This report is very similar to the Security Incident Types report, described above, except that it enables you to specify the file types to be included in the report and to specify that only files over a certain size are included in the report.

File Related Security Incidents by Users and Organizational Units Report

This report shows security incidents by users and organizational units by incident type, during a specified timeframe. You can define which users and organizational units and which types of security incidents are to be shown, according to the security guidelines of your organization. This report is very similar to the Security Incidents by Users and Organizational Units report, described on the previous pages, except that the information that it shows emphasizes the users and organizational units involved.

Policy Distribution Report

This report shows the entire range of security policies applied to the organization and its overall security policy. It also helps identify endpoints to which no valid policy has been applied. The

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

pie chart in this report shows the distribution of policies in the selected organizational units. You can select to view this chart by users or by machines.

Controls for Policy Distribution Report

This report provides the following controls for specifying the content of the report:

- **Organizational Tree**: The Organizational Tree enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree. You may refer to the *Controls for Deployment Status Report* section for more information.
- **Check Policies Apply to**: Select the **Users** or **Machines** option to specify to which of these the content of this report applies.

Safend Inspector – Classified Data Usage Reports

This report displays security incidents related to a specific data classification during the selected time frame. You define which incidents you want to view in the report.

Security Incidents by Users Watch List

This report shows which users were responsible for the most security incidents, during the selected time frame.

Security Incidents by Users and Organizational Units Report

This report shows which organizational units or specific users and computers are violating the organization security policies, or even committing an extensive amount of a*ll*owed but *susp*ici*ous* activities. This type of detailed information helps highlight unusual events and uncover malicious or reckless user behavior.

When generating a report, you are first required to define which user action is considered to be a secur*i*ty *inci*dent. For example, this may be an unapproved user action that was blocked by Safend Data Protection Suite or an allowed user action that you still want to supervise.

The bar chart in this report shows the distribution of selected organizational units and the relative number of security incidents. This enables you to immediately spot rouge departments that require further observation, training or an in-depth investigation.

A Users Watch List is also provided describing the users that have committed the most security incidents. These are the users whose behavior may require further analysis.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Controls for Security Incidents by Users and Organizational Units Report

- **Organizational Tree:** The Organizational Tree enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree. You may refer to the *Controls for Deployment Status Report* section for more information. **Note**: When you click on an Organizational Unit, the report will compare itself with the organizational units under it.
- **Incident Information:** Enables you to select the type of Safend Data Protection Suite security action that was applied in the incident, such as Blocked or Allowed and to check off the types of storage devices on which these occurred. These are the incidents that will be included in the report.

Drilldown and Linked Information from the Security Incidents by Users and Organizational Units Report

This report provides a linked (drilldown) to display the Security Incident Types Report.

Security Incident Types Report

This report shows an overview of the most common security incidents in an organization. You can define which types of security incidents are to be shown according to the security guidelines of the organization.

The information presented in this report highlights problematic procedures and work practices that should be addressed. This information can trigger an in-depth investigation into an unusually common incident type. This report can also be used to p*revi*ew a policy before its association with organizational units by checking the number of events that would have been blocked if this policy was associated with the chosen organizational units.

The bar chart in this report shows the distribution of security incidents by incident type during the selected timeframe.

A table appears at the bottom of this report listing the incident types and providing the total number of incidents, number of users involved and the number of machines involved.

Controls for Security Incident Types Report

- **Organizational Tree**: The Organizational Tree enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree. You may refer to the *Controls for Deployment Status Report* section for more information.
- **Incident Information**: Enables you to select the type of Safend Data Protection Suite security action that was applied in the incident, such as **Blocked** or **Allowed** and to check off the types of storage devices on which these occurred. These are the incidents that will be included in the report.

Note: When you select 2 device types you get results from either one of them but not both.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Drilldown and Linked Information from the Security Incident Types Report

This report provides a linked (drilldown) to display the Security incidents by OU Report.

Silent Machines Report

This report generates a detailed list of machines that have not communicated with the server during the selected time frame.

Storage Device Inventory Report

This report generates a detailed list of all the portable storage devices that were used within a defined timeframe. These devices can be copied to a policy White List in order to simplify the policy creation process.

The bar chart in this report provides a summary of the usage of storage devices in the selected organizational units during the selected timeframe.

A table appears at the bottom of this report listing the types of storage devices that were used, the number of such devices, the number of users which used those devices and the number of machines on which those devices were used. You also have the option to select to Show Specific Devices. In this case, much more detail is provided about each specific storage device that is used and it enables you to link to the Safend Data Protection Suite logs showing its usage.

Controls for Storage Device Inventory Report

This report provides the following controls for specifying the content of the report:

- **Time Frame**: Enables you to specify the timeframe in which the storage devices listed in this report were used. You can specify the Last days or hours in which they were used. Alternatively, choose an exact Time Frame indicating from/to which date and time they were used and also specify the times Between which they were used each day.
- **Organizational Tree:** The Organizational Tree enables you to select the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree. You may refer to the *Controls for Deployment Status Report* section for more information.
- **Storage Devices**: Enables you to specify the exact types of storage devices to be included in the report. Note that when you select 2 device types you get results from either one of them but not both.
- **Show Specific Devices**: Enables you to specify that much more detail is included in the report about each specific storage device that is used.
- In the Logs column, you can link to the Safend Data Protection Suite logs showing the device's usage.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

User Data Classification Activity Report

This displays which users were responsible for the most data classification activities during the selected time frame. This report tracks which users do not generate enough manual classification logs so that the administrator can choose to replace them with more active users and speed up the data leakage deployment stage.

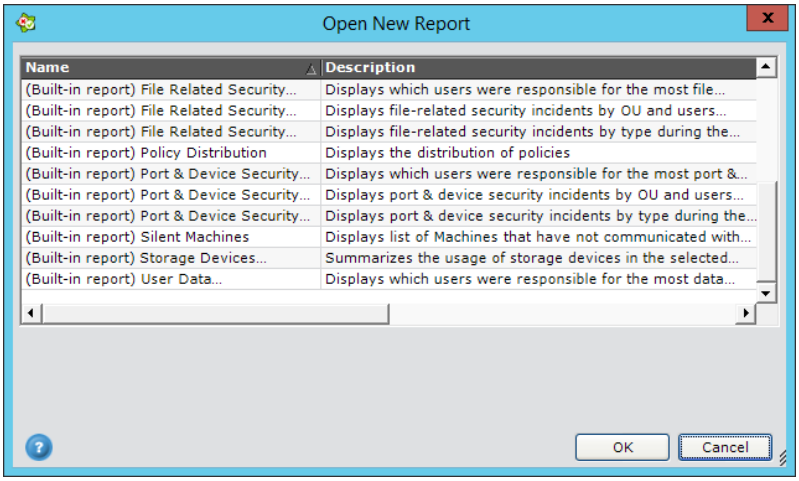
Running a Report

Safend Data Protection Suite provides a variety of Built-in reports that you can run using the default parameters or you can define a new report that is based on a Built-in report (See *Built-in Reports*) and save it in the Report Definitions list.

1. Double-click on one of the Built-in reports in the Report Definitions list to run and display the report. An example is shown below.
2. Most of the reports enable you to filter the organizational units that are included in the report by selecting the relevant checkboxes in the Organizational Tree on the left.
3. Modify any of the controls provided for this specific report. You may refer to the *Built-in Reports* section for a description of each type of report and the Built-in controls provided for it.
4. If you change the controls that are selected (such as the organizational units), you must click the Run Report button again to display the latest report information from the Safend Data Protection Suite database. You may also want to save these report definitions using the Save or the Save As tools under a different name (the definition of the Built-in reports cannot be overwritten).

Defining a New Report

Click New to display a selection of Built-in Reports, as shown below:



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Creating a New Report

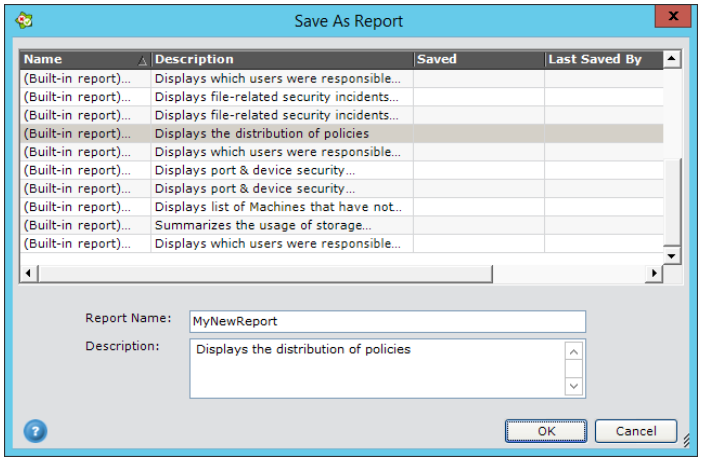
The Open New Report window lists the types of Built-in reports that can be used as a basis for creating a new report. A list of these report types and the controls that enable you to define more specifically the type of data that they include is provided in the *Built-in Reports* section. The following shows an example of one of the report windows that you can open:

1. Change the report controls to show the information that you require.
2. Optionally, you can click the **Run Report** button to display a report now. This is also recommended in order to verify that the definitions that you have specified generate the expected report information.
3. Click **Save** or **Save As** if you would like to rerun this report in the future.

Saving a Report Under a New Name

You can save a report under a new name, with a new description. This is done in the Save As Report window.

1. After running a report, click Save As at the top of the report. The *Save as Report* window is displayed.

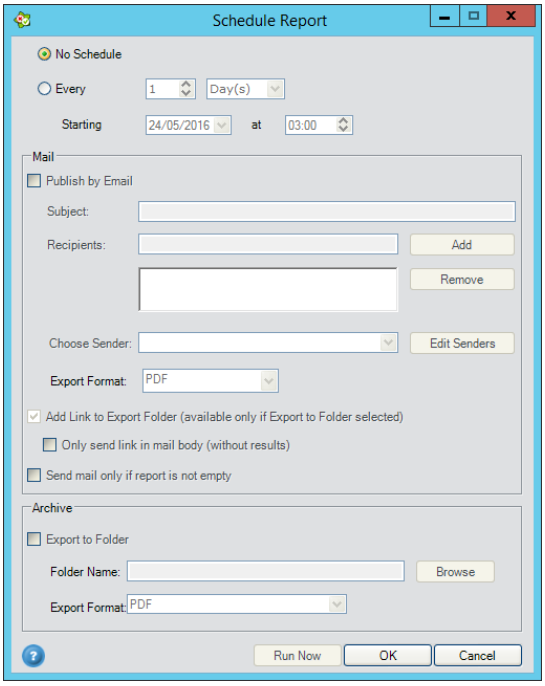


2. A list of the existing reports is displayed. In the Report Name field, save this new report under a new name. You can also add or change the description about the report in the Description field.

Scheduling a Report

Reports can be scheduled and sent periodically by email to predefined recipients or archived to a specified share folder, in order to ensure continuous tracking of an organization's security status. To open the *Schedule Report* window click the ... button in the Schedule column of the Report Definitions list or, after the report is open, click Schedule in the toolbar to display the following window.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Defining a Scheduled Report

Select the **No schedule** radio button if you would like to cancel a previously defined schedule and click **OK** to close this window or select the **Every** radio button and choose the following parameters:

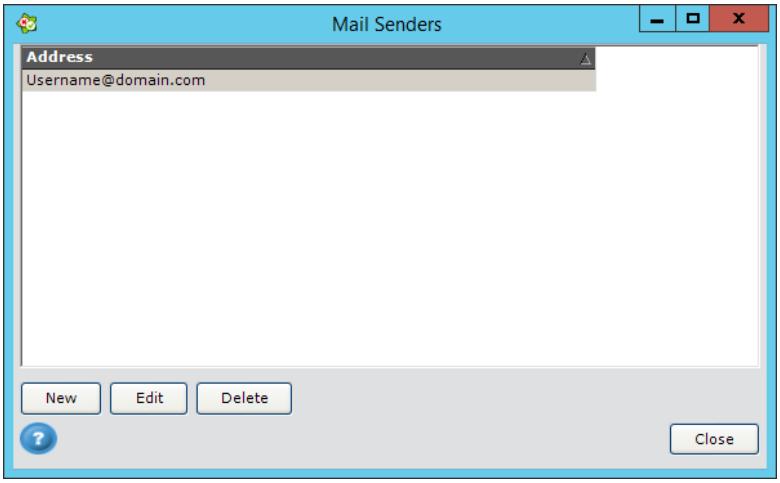
> In **Every** area:
  - Select how often to run the report by entering a number and selecting one of the following options from the drop-down menu: Days, Hours, Weeks or Months.
  - In the Starting field, specify the date and time to run the first report and then each subsequent report.

> In the *Mail* section, you can optionally define how this report is published and who are the email recipients of this report, as follows:

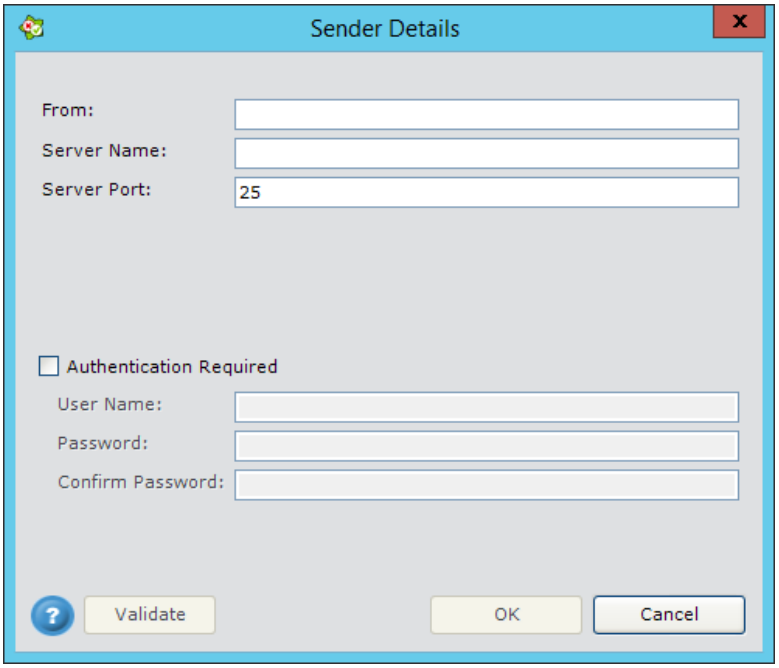
> Check **Publish by Email** checkbox to define that a report is sent by email.
  - In the *Subject* field, type in the subject of the email to be sent.
  - In the *Recipients* field, enter a list of email addresses to which to send the reports. You can type in one or more email addresses, separated by a semi-colon (;) and then click the **Add** button to add it to the list of recipients.
  - In the Choose Sender field, select the email address to be specified as the sender from the drop-down menu. The drop-down menu lists the senders that were entered previously in Safend Data Protection Suite either in this window or in the Alert Destination Repository (see
  - *Alert Destination* Repository*)*

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- You can also click the **Edit Sender** button to display the following window in which you can define a new sender, edit an existing sender or delete a sender, as shown below:



> You can click the **New** button to add a new sender in the following window:



This window contains standard email definition parameters and is similar to the window described in the

Alert Destination Repository section.

In the Export Format field select one of the various standard formats that are available: PDF, XLS, BMP, RTF, TXT, CSV or MHT.

> In the **Archive** area, you can optionally define where this report is archived, as follows:

- Check the Export to Folder checkbox to define that a report is saved each time it is run in the folder specified below.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- In the Folder Name field, specify the name of the folder into which a report is saved each time it is run. You can click the Browse button to display a window from which you can select a folder.
- In the Export Format field, specify the format of the exported report by selecting one of the various standard formats that are available: PDF, XLS, BMP, RTF, TXT, CSV or MHT.

> After completing the information in this window, do one of the following:

- Click Run Now to generate a report according to these definitions right now. The schedule is saved and reports are also generated and sent according to the defined schedule.
- Click OK to save this schedule. The report is then generated and sent according to the defined schedule.
- Click Cancel to cancel the definition of this schedule.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

11 ADMINISTRATION

11.1 Administering Data Protection Suite

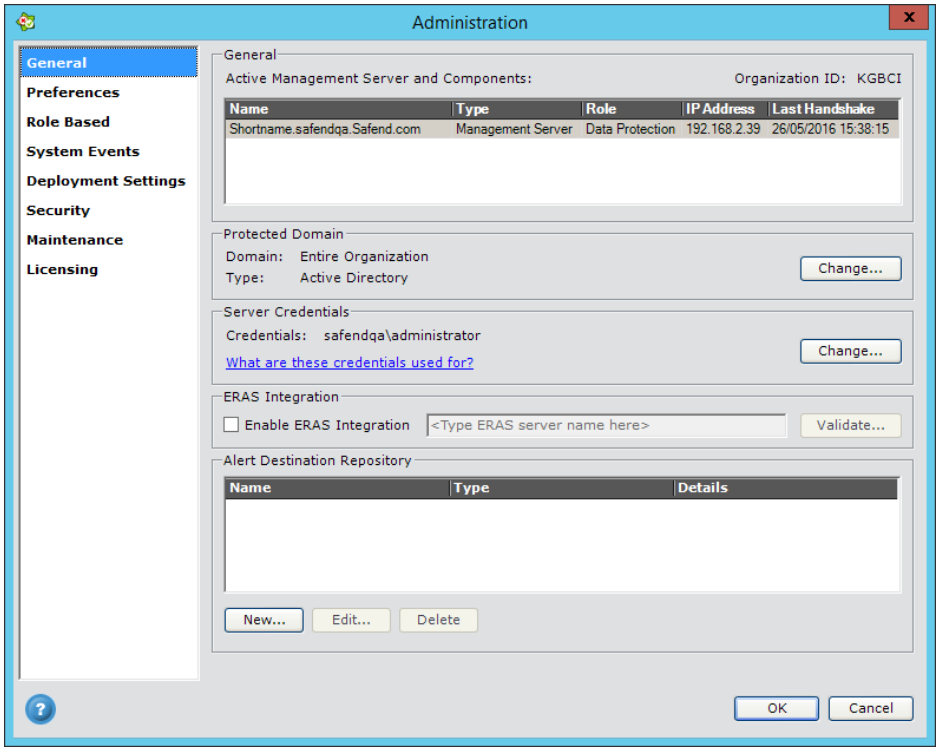
When Safend Data Protection Suite is first launched following installation, the system is initialized with default settings that may be applicable to the majority of users.

During the ongoing operation of Safend Data Protection Suite, you may want to update various administration settings. This is performed in the Administration window, as follows.

11.1.1 ADMINISTRATION WINDOW

Opening the Administration window

From the Tools menu, select Administration or in the Home Tab, in the More section, click the **Change Administration Settings** link. The Administration window opens.



The settings in the Administration window consist of eight tabs:

- **General**, described in General Tab Settings.
- **Preferences**, described in Configuring Preferences Tab Settings.
- **Role Based**, described in Configuring Role Based Tab Settings.
- **System Events**, described in Configuring System Events Tab Settings.
- **Deployment Settings**, described in Configuring Deployment Settings Tab Settings.
- **Security**, described in Configuring Security Tab Settings.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **Maintenance**, described in Configuring Maintenance Tab Settings.
- **Licensing**, described in Configuring Licensing Tab Settings.

11.1.1.1 General Tab Settings

General administration settings are defined in the General tab of the Administration window.

Configuring General Tab Settings

The General tab enables you to configure general system configuration parameters for the Safend Data Protection Suite. It contains the following sections:

- General
- Protected Domain
- Server Credentials
- Alert Destination Repository

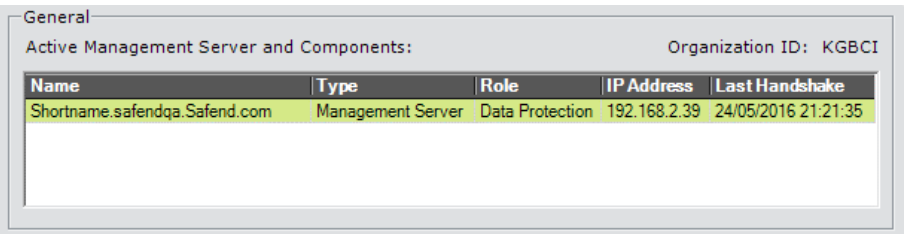
Important: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the Administration window for the modifications to apply.

General

These fields contain information about the Management Server in which Safend Data Protection Suite is managed. Each Safend Data Protection Suite Server is a computer on which you have installed the Safend Data Protection Suite Console and the Safend Data Protection Suite Management Server applications. Each Safend Data Protection Suite Console works with the Safend Data Protection Suite Management Server on which it was installed. The Management Server has multiple roles:

- It is used as a central point for communicating with Safend Data Protection Suite Clients installed on endpoints.
- It holds a database of all system configuration, policies and logs.
- It communicates with Management Consoles.

Active Management Servers and Components

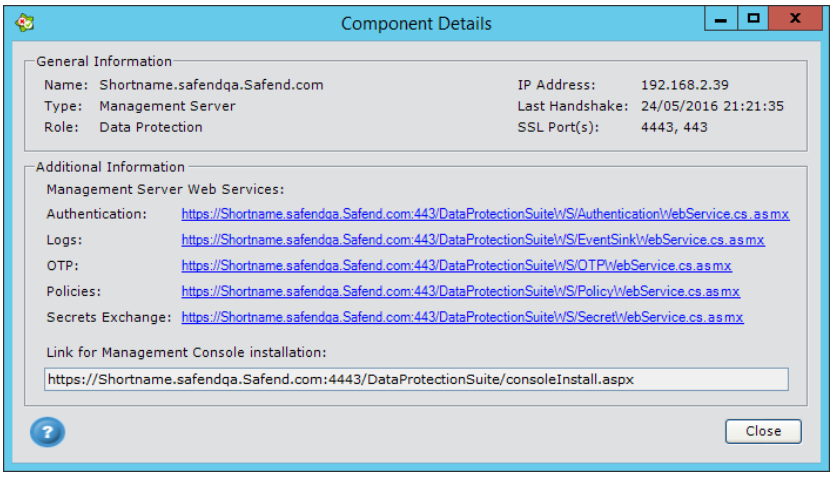


This table lists the Safend Data Protection Suite Management Servers and components that are active.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Column	Description
Name	The full name of the active Management Server or component machine.
Type	The component type: for example Server, Gateway, etc.
Role	The role of the component: for example, data protection.
IP Address	The IP address of the server or component machine.
Last Handshake	The last time the server or component communicated with the Data Protection Suite database.
SLL Port(s)	This lists the SSL ports. This information is displayed only in the Component Details window. For more information about ports see *Server Ports* which follows.

When you double click on a Server in Active Management Server and Components, the Components Details window is displayed:



Here is listed General Information which is described above and Additional Information about Management Server Web Services. At the bottom of the window is a link for installing the Management Console. See *Management Console Installation Link*.

Server Ports

The Server ports are TCP ports on which the Management Server performs its communications with the Clients (controlling and collecting logs) and with the Management Consoles (defining policies, reviewing logs, etc.). All Management Server communications performed over these TCP ports are encrypted using SSL.

During installation port 4443 is used as a default for Server-Console SSL communications and port 443 is used as a default for Server-Client SSL communications. If for any reason you want

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

to change the port number, you can change it from the Microsoft IIS settings on the Management Server machine.

Changing the port

1. Access the IIS settings from the control panel of your Management Server machine (administrative tasks → Internet Information Services).
2. Locate the Safend Data Protection Suite at the following sites:
   a) "Safend Data Protection Suite Web Site" for Management Console communications (default port 4443)
   b) “Safend Data Protection Suite Web Site WS" for Client communications (default port 443).
3. Change the SSL port(s) to your desired port(s).
4. Kill the IIS worker process on your Management Server: "w3wp.exe"
5. Access the Safend Data Protection Suite Management Console from the local machine and perform any kind of change in *Global Policy Settings* in order to cause re-publishing of all policies.

Notes:

> Since all Clients and Management Consoles use this port for communicating with the Management Server, changing the port will cause them to cease from communicating with the Server until they are notified of the new port.

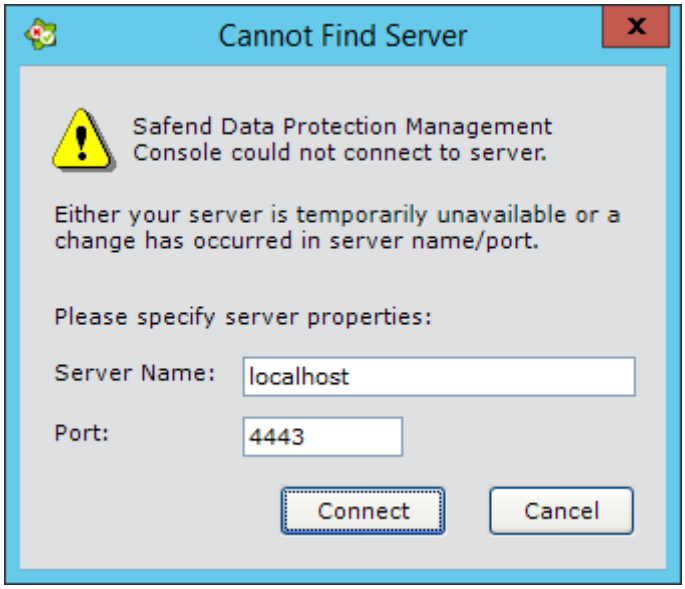
> Never change the port during active hours. If multiple Management Consoles are now in use, changing the port will cause immediate disconnection of these consoles, resulting in possible data loss.

> Safend Data Protection Suite Clients communicate with the Management Server in the communication port specified in their policy. Once you change the port, Clients will not be able to communicate with the Management Server until they receive the re-published policies.

> Management Console administrators need to be notified of the port change. You may choose one of the following options:

- Require administrators to re-install the Management Console by using the Management Console Installation web page. You will need to notify them of the new address (see the following section).
- Communicate the new port to your administrators. They will need to manually insert it the next time they open the Management Console, in the following window:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

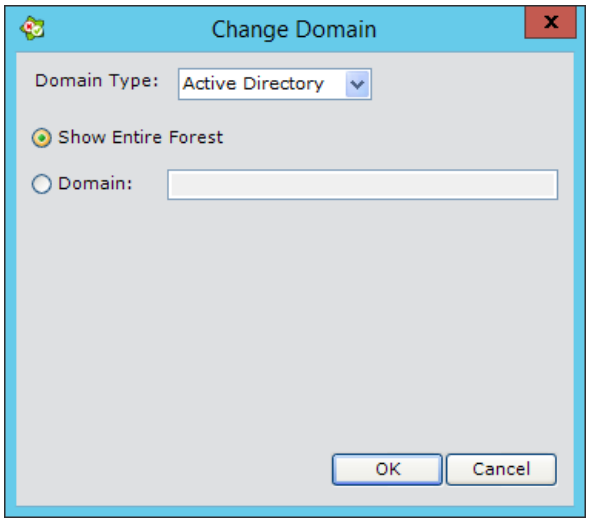


Protected Domain

This section defines the protected domain and whether it is an Active Directory or a Novell eDirectory domain. These definitions are set in the Change Domain window.

Accessing the Change Domain window

1. In the Protected Domain section, click Change. The Change Domain window opens:



2. To define domain type:
   a) In the Domain Type menu, select Active Directory or Novell eDirectory, as required.
   b) Click the appropriate radio button to select whether you want to display the entire forest or only a specific domain. If you want to display a specific domain, enter its name.
   c) Click **OK** to save and exit.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Server Credentials

For the Management Server application to perform its functions on the network, a user account with sufficient privileges is needed. This user is defined during the Management Server installation process and is crucial for the smooth operation of the whole system.

This user account must have the following privilege: WMI access to remote machines – Control messages from the Management Server to endpoints are sent over WMI. The user must have the credentials on each of the endpoints for WMI access.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

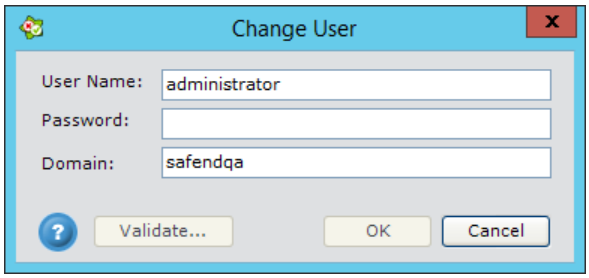
Notes:

> Safend recommends that you use an account with domain administrator privileges on your network, in order to avoid problems.

> If at any time you change the "Client Installation Folder" (see below) or choose to deploy policies as .reg files to a folder, you need to make sure this user has full access privileges to these folders (read and write).

Change Administrator Password

Change the user whenever necessary by clicking Change in the Domain Credentials section of the General tab in the Administration window. The Change User window opens:



1. Enter the credentials (User Name, Password, Domain) of the new user account.

   Note: Special characters such as: &, ^, <, >, |, are not allowed to be used in the password.

2. You may validate that the user is valid and holds sufficient privileges by clicking **Validate**. Refer to *Server Credentials* for details about this user.

3. The Validate button only validates the existence of the user in your Active Directory. In order for the Management Server to function correctly, you need to make sure that all the required privileges are given to the domain user.

Alert Destination Repository

This is where you view, edit, define and delete the destinations available in your network for sending alerts. A destination is the address to which alerts are sent.

The list of address destinations is called the Alert Destination Repository. Once you have created the repository, you can select from it the desired destinations to be used for System alerts (see *System Alert Definitions*).

Destinations can be of multiple protocol types including:

Protocol Type	Description
Email	Send to a single/multiple address(es).
Windows Event Log	Insert a log entry to a specific computer event log.

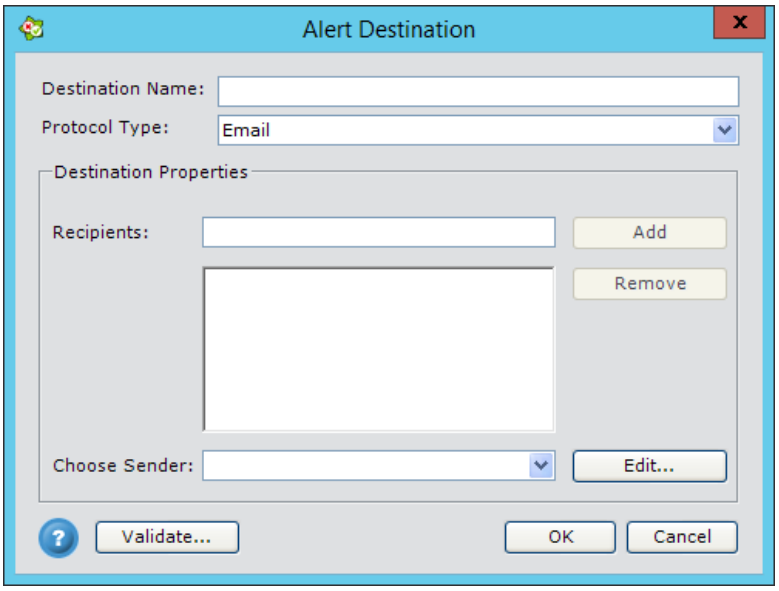
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

SNMP	Generate an SNMP trap to be sent to network monitoring systems (i.e., HP Openview, IBM Tivolli).
Executable	Run an executable which will perform any kind of action with the alert information.
Syslog	Send a message to a syslog compatible server.

Alert destinations are set in the Alert Destination window.

Opening the Alert Destination window

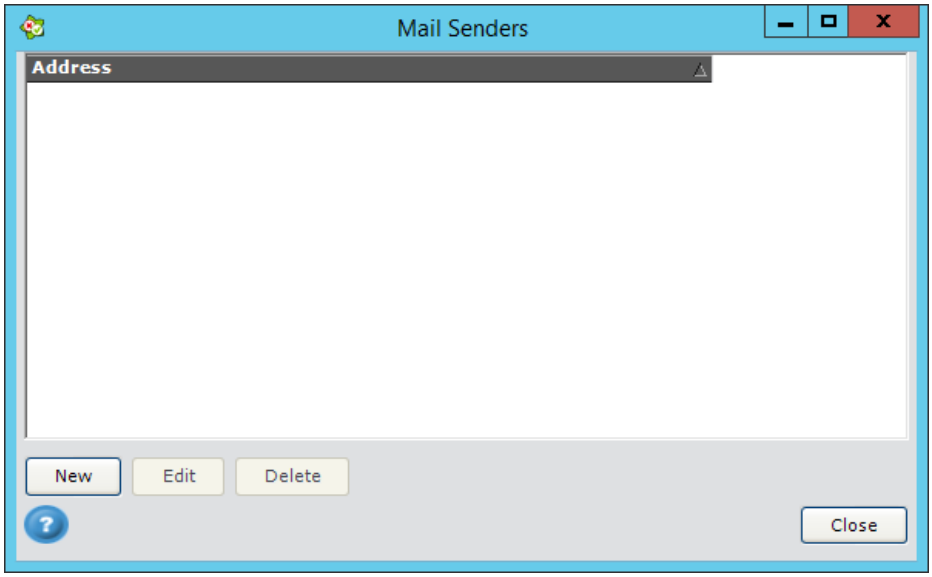
In the Alert Destination Repository section, click **New**. The Alert Destination window is displayed:



Mail Senders

A list of mail senders is displayed when you click Edit Senders in Alert Destinations.

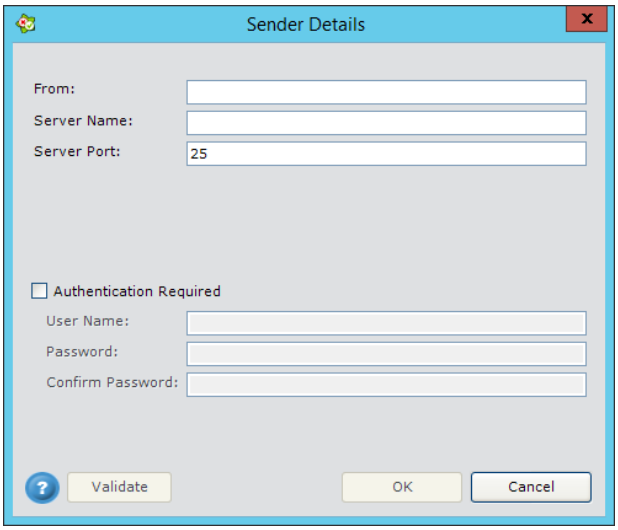
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



You can click the New button to add a new sender, Edit to edit a sender or Delete to remove a sender.

Defining a New Mail Sender

A new mail sender is defined in the Sender Details dialog box.



Field	Description
From	This field appears in the From fields of the emails that are sent.
Server Name	The host name of your outgoing email server (SMTP). You can also type an IP address.
Server Port	The TCP port for sending email. This is typically port 25. If you are using secure email, then the port may be different.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Field	Description
Authentication Required (Optional)	If your outgoing email server requires authentication, enter the following fields as well: User Name, Password/Confirm Password.

Setting an Alert Destination

Protocol Type	Destination Properties
Email	**Recipients** – type in a valid email address to which the email will be sent. You can also type several addresses, comma/semicolon separated. Select add to add the mail address you typed to the recipients list. In the Choose Sender field, select the email address to be specified as the sender from the drop-down menu. The drop-down menu lists the senders that were entered previously in Safend Data Protection Suite either in this window or in the Schedule Report window (See *Scheduling a Report*). You can also click the Edit Sender button to define a new sender, edit an existing sender or delete a sender. Note: The drop-down menu in the *Alert Destination* window lists the senders that were entered previously in Safend Data Protection Suite, either through this window or in the *Schedule Report* window (See *Scheduling a Report).*
Windows Event Log	**Host Name** – the host name on which to write Windows event logs. You can also type an IP address.
SNMP	**Server Name** – the host name of your SNMP server. You can also type an IP address. **Server Port** - the TCP port for sending SNMP traps. This is typically port 162.
Executable	Path to executable – the path to an executable to be launched by an alert, if desired.
Syslog	**Server Name** – the host name of your Syslog server. You can also type an IP address. **Server Port** – This is typically port 514.

For details about the API parameters, please contact Safend Support at: support@safend.net.

Adding an alert destination

1. In this window, enter the required details and click **OK**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

2. After you click **OK**, the system validates the destination you have entered. If not valid, check your settings and try again.

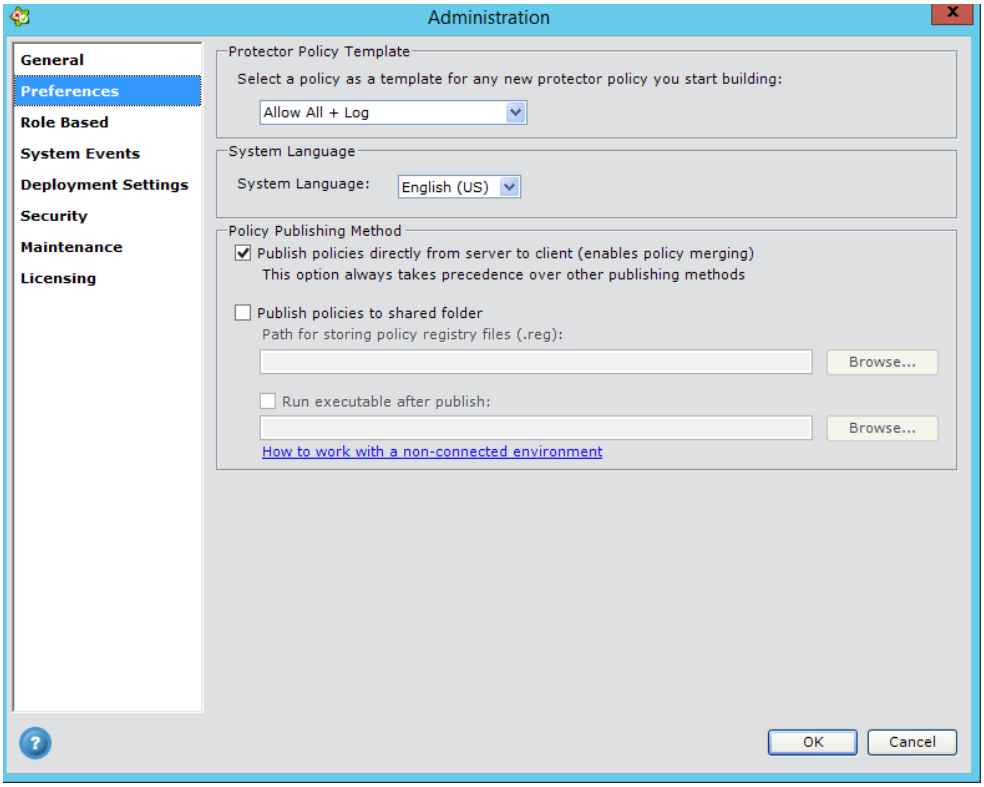
3. You can also click **Validate** to perform manual validation.

Once you have created the Alert Destination Repository, you can select from it the desired destinations to be used for System alerts (see System Alert Definitions).

Important: If you change the properties of a destination, it will affect all alerts that use this destination: the system alerts, policy-specific alerts and global policy alert settings.

Configuring Preferences Tab Settings

Preferences Administration settings are configured in the Preferences tab in the Administration window.



Preferences Settings

The Preferences tab enables you select a Policy template and choose the system language. It contains the following sections:

> Protector Policy Template

> System Language

> Policy Publishing Method

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Protector Policy Template

Each time you create a new Port and Device Control Security Policy (configuring the Protector component of the Safend Data Protection Suite), default values appear for security options (ports, devices, etc.).

With this option, you can choose to set any of the policies you have already defined as a template which replaces the default when creating new policies. This is useful when you have specific settings you prefer to start from, rather than the default.

Note: This option is disabled until you create at least one policy.

System Language

Safend Data Protection Suite allows you to customize it to your own language. With each new version additional languages are added.

This language affects the following:

- The language for the Management Console menus and buttons.
- The language for textual fields in logs.
- The language for default end-user messages.

System language is typically defined during the Management Server installation. If you wish to change it after installation, set it here.

Notes:

- After you change the language you will need to restart you Management Console for the language change to take effect.
- You cannot have multiple Consoles in different languages.
- Log information which was stored before the point of the language change is displayed in the previous language.
- The language for Safend Data Protection Suite Clients is defined during the installation of the Clients (see the *Safend Data Protection Suite Installation Guide*).

Policy Publishing Method

The Safend Administrator has the option to save Protector and Encryptor policies to registry files in order to apply policies on machines that are isolated and don't have access to the organizational network.

Choose one of the policy publishing methods:

- Publish policies directly from the Server to the Client (enables policy merging).
- **Note**: This option always takes precedence over other publishing methods.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

> Publish files to shared folder, Path for storing policy registry files (reg.). This is used to publish policies via registry files to machines in a non-connected environment. Either type in the path or click Browse and choose the appropriate folder. You can choose to run an executable after publish. Type in the path or click Browse and choose the appropriate folder.

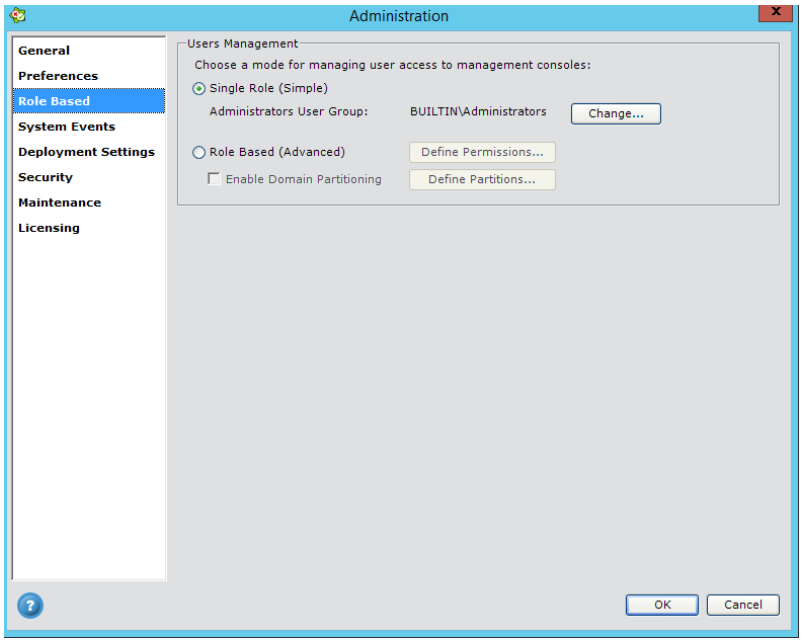
Working in an unconnected environment

Once the Administrator turns this option on (Publish files to shared folder), all Policies will be saved to a relevant folder, under the location the Administrator specified. For example if the Administrator set C:\Policies as the location where he wants to store all policies, all Policies will be saved under C:\Policies\Encryptor, C:\Policies\Protector, C:\Policies\Settings.

Existing folders will be completely overwritten (folders names will not be localized). If this option is on, every time a policy will be saved it also will be saved under the relevant folder. Existing policies will be updated. When the Administrator turns this option off, the policies will not be deleted and the files will remain on the drive.

Configuring Role Based Tab Settings

Role-based administration settings are configured in the Role Based tab in the Administration window.



Role Based Settings

The Role Based tab enables you to choose a mode for managing user access to Management Consoles.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Users Management

User access to the Management Console is restricted for security reasons. Safend Data Protection Suite does not require its own users and computers database. Instead, credentials are checked using Windows/Active Directory.

Note: If Safend Data Protection Suite is synchronized with Novell eDirectory, only local users on the Management Server can be used.

You can choose one of the following modes of operation:

- **Single Role (Simple)** – Using this mode you limit full access to the Management Console to only one group of authorized users. All of them will be able to perform all the tasks in the Console (create policies, read logs, suspend Clients, etc.).
- **Role Based (Advanced)** – Using this mode, you can add an additional level of access control by restricting users to a subset of functions within the Management Console, according to their role and permissions and to specific containers of an organization for which they are responsible.
- The default mode after installation is – Single Role (Simple).

Single Role (Simple)

Working with Multiple Management Consoles

The "Single Role" mode is designed for allowing multiple Management Consoles to access the Management Server, each with his own user and password. This is performed by validating that the user is a member of the user group defined as the "Protector Administrators User Group".

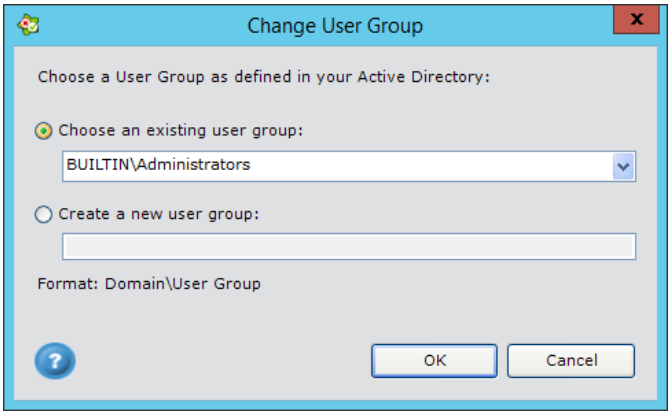
By default, after installing the Management Server this property is set to "BUILTIN\Administrators" which restricts access to the local administrators of the Server machine.

If you are planning on having multiple administrators for Safend Data Protection Suite Management Console, it is recommended that you set here a user group from your Active Directory, and add the appropriate administrators as members of this user group. This is done from the Change User Group window.

Opening the Change User Group window

In the Users Management section, click Change. The following window opens:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Changing the Safend Data Protection Suite Administrators User Group

1. Select one of your existing user groups from the drop-down menu, or create a new user group. When creating a new group, use the following format: Domain\UserGroup (for example Safend\administrators).
   If you do not enter the domain the new user group is created in the computer hosting the Safend Data Protection Suite Management Server.
2. Click **OK**. Creation of a new user group is only performed once you have confirmed changes in the Administration window and clicked **OK**.

Role Based (Advanced)

To determine how the Role Based (Advanced) feature operates, you can configure the following:

> **Defining Permissions** – This option enables you to add an additional level of access control by restricting users to a subset of functions within the Management Console.

> **Defining Domain Partitions** – This option enables you to partition the containers of an organization so that they are only accessible to the Safend Data Protection Suite Console administrators that are responsible for handling them.

Defining Permissions

Using this mode adds an additional level of access control by restricting users to a subset of functions within the Management Console. You can create multiple user roles and restrict each of them to specific functions in the Console.

For example, you can define a role as "Logs Reviewer" which would restrict users only to the Logs tab, without having the ability to view or edit policies. In the same way you can define a role as "Policy Administrators" which would restrict the user to the Policies tab, without having the ability to view logs.

In addition, you can define "Read Only" users who can only view information on the Management Console and cannot perform any changes.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

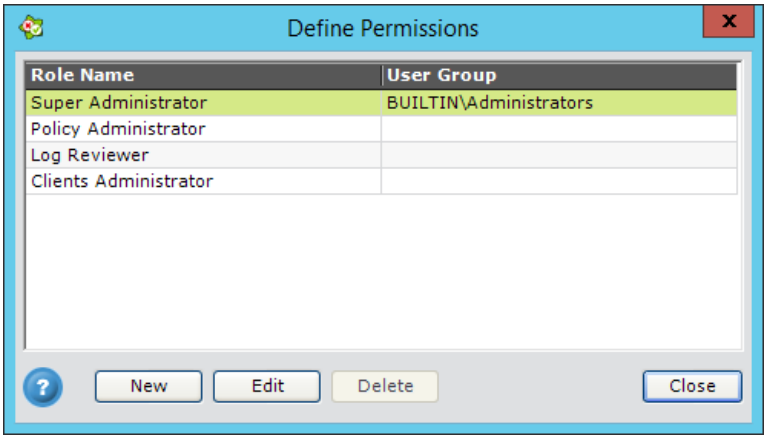
A "role" is actually a set of permissions which are associated with a user group in your Active Directory. When a user tries to access the Management Console, his/her credentials are checked with the domain, and the list of groups of which he/she is a member is retrieved. The user will be authorized to perform the functions which are defined in any of the roles to which he is associated.

For example, if the user is both a member of the "Policy Administrators" and "Logs Reviewer" in the example above, he/she is able to access both the Logs and the Policies tabs.

Role definition is defined in the Define Permissions window.

Opening the Define Permissions window

Click Define Permissions. The Define Permissions window opens:



Defining Roles

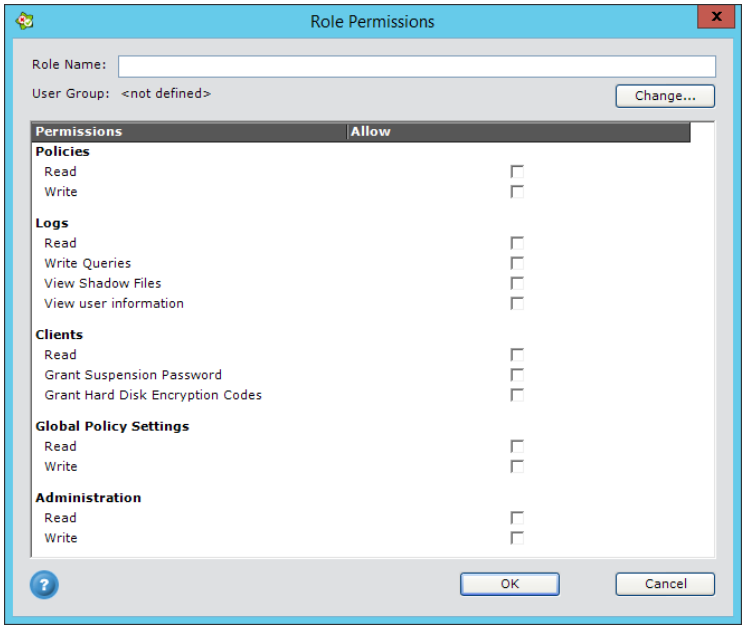
This window displays a list of the existing roles. In it you can create new roles and edit or delete existing roles. Each row displays a role, the user group with which it is associated and the domain partition to which it has been assigned (See *Defining Domain Partitions*).

The following roles are built into Safend Data Protection Suite: Super administrator, Policy Administrator, Log Reviewer, Client Administrator. If you wish to use any of the last three roles, simply Edit them and associate them with a User Group. If you do not wish to use them, you may Delete them.

Note: You cannot edit or delete the "Super Administrator" role. This role is preset from the installation of the Management Server and is given all the permissions, including the ability to edit administration settings. The user group associated with this role is derived from the group defined in the "Single Role" mode.

To create a new role, click **New**. To edit an existing role, click **Edit**. The following window opens:

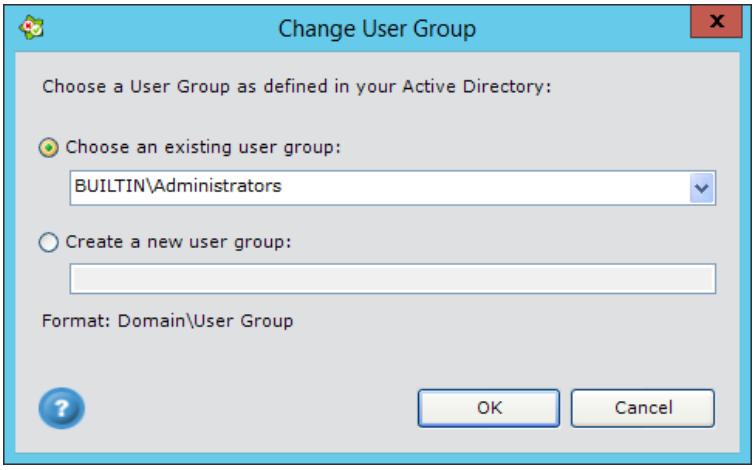
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Refer to Defining Role Permissions for an explanation of role permission definition.

Defining Role Permissions

1. If this is a new permission, enter the Role Name.
2. If you want to define or change the User Group, click **Change**. The *Change User Group* window opens:



3. Refer to Changing the Safend Data Protection Suite Administrators User Group for an explanation of this window. You must select a User Group in order to use a role definition. If you are using Novell, you can only use a local user group on the Management Server.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4. The Domain Partitioning feature enables the partition of the containers of an organization so that they are only accessible to the Safend Data Protection Suite Console administrators that are responsible for handling them. This feature affects almost all aspects of Safend Data Protection Suite's interface, so that only the containers assigned to the Domain Partition associated with a Safend Data Protection Suite user are displayed in the Safend Data Protection Suite Console. The Role permissions define which administrative actions each Safend Data Protection Suite administrator can perform and the Domain Partition settings define the clients on which they can perform these actions.
   To change the partition for this Role permission, select another one in the Domain Partition drop-down menu. If you want to define a new Domain Partition, click New Partition. To edit an existing Domain Partition, click Edit Partition. To change the partition for this Role permission, select another one in the Domain Partition drop-down menu.
5. Edit the permissions by checking or un-checking the Allow checkboxes. Each checkbox that you allow gives the allowed permission to the user group.
6. Click **OK**.

Defining Domain Partitions

Safend Data Protection Suite's Domain Partitioning enables the partition of the containers of an organization so that they are only accessible to the Safend Data Protection Suite Console administrators that are responsible for handling them. Your organization's domain can be partitioned according to its organizational structure and then different Safend Data Protection Suite administrators can be assigned to each partition.

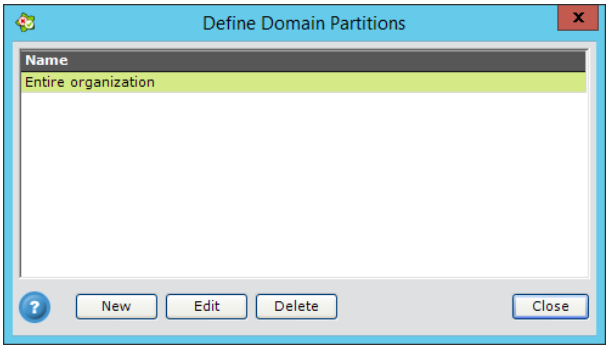
Note: Domain Partitioning is especially important when using File Shadowing. File Shadowing collects hidden copies of files that are moved to/from external storage devices, and therefore, you may want to restrict access to these sensitive files by defining which administrator is allowed to view a shadowed file according to the file's OU or origin.

Click the Enable Domain Partitioning checkbox to enable the domain partitioning feature that allows you to divide domain partitions among roles. You can then open the Define Domain Partitions window, as described below.

Opening the Define Domain Partitions window

Click Define Partitions. The Define Domain Partitions window opens:

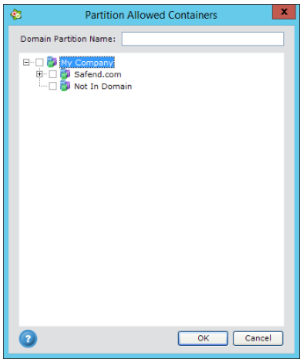
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



This window displays a list of the existing domain partitions. In it you can create new domain partitions and edit or delete existing domain partitions.

Adding a New Doman Partition

1. Click **New**. The following window opens:

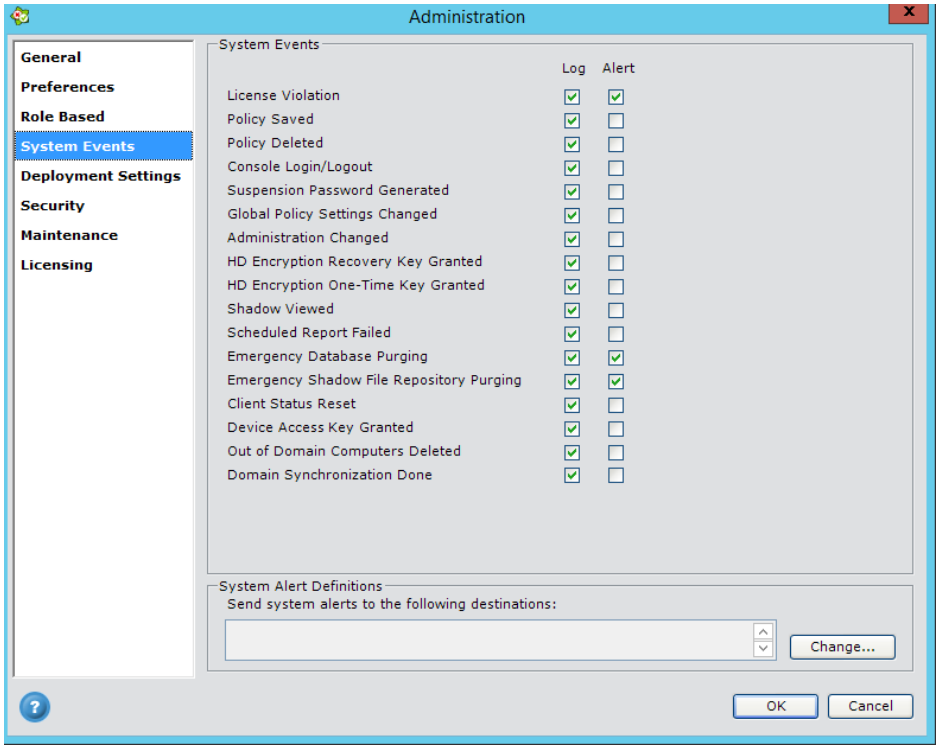


2. Enter a name for the domain partition at the top of the window.
3. Check the checkboxes of the containers that you want included in this domain. To do so, you may have to expand the tree to see the containers to be selected.
4. Click **OK**. This Domain Partition is offered for selection in the Domain Partition field of the *Role Permissions* window, as described in *Defining Roles*. To associate this partition with a group of users you must associate it with a user role in the *Role Permissions* window.

11.1.1.2 Configuring System Events Tab Settings

System Events are configured in the System Events tab in the Administration window.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



System Events Settings

The System Events tab enables you to configure log and alert definitions and alert destinations for Management Server events. It contains the following sections:

> System Events

> System Alert Definitions

Note: Whenever you modify any of the settings in this tab you must click OK at the bottom of the Administration window for the modifications to apply.

System Events

System events track events generated by the Management Server and actions performed in Management Consoles. In this section you define which events are logged (and can be viewed in Server Logs) and which also generate an alert. The following is a description of the various System Events.

System Event	Description
License Violation	This event indicates that a license violation has occurred. This can happen if the license period expires or when the system exceeds the maximum number of seats.
Policy Saved	This event indicates that a policy has been saved on the Management Server.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

System Event	Description
Policy Deleted	This event indicates that a policy has been deleted from the Management Server.
Console Login/Logout	This event indicates that a user logged in or logged out from the Management Console.
Suspension Password Generated	This event indicates that a suspension password has been generated.
Global Policy Settings Changed	This event indicates that a change in the global policy settings has been made.
Administration Changed	This event indicates that a change in administration settings has been made.
HD Encryption Recovery Key Granted	This event indicates that a hard disk encryption recovery key has been generated.
HD Encryption One-Time Key Granted	This event indicates that a one-time access key to an encrypted machine has been generated.
Scheduled Report Failed	This event indicates that a scheduled report failed to run.
Client Status Reset	This event indicates that the status of a client machine has been reset.

By default all events are logged. You can remove some of the logs or set events for which you would like the Management Server also to send an alert.

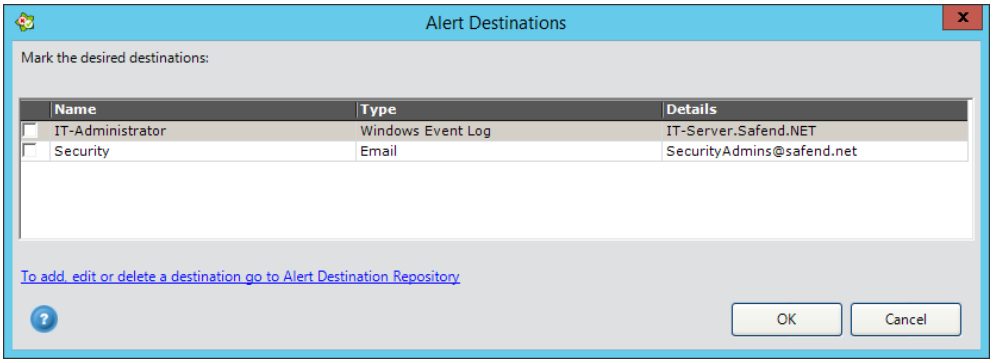
System Alert Definitions

Select here the destinations to which the Management Server sends alerts, generated as a result of systems events. Alerts are sent only for event types you have chosen in the previous section.

Adding/removing destinations

1. Click **Change**. The *Alert Destinations* window opens, displaying all available destinations defined in the Alert Destination Repository (refer to
2. Alert Destination Repository).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



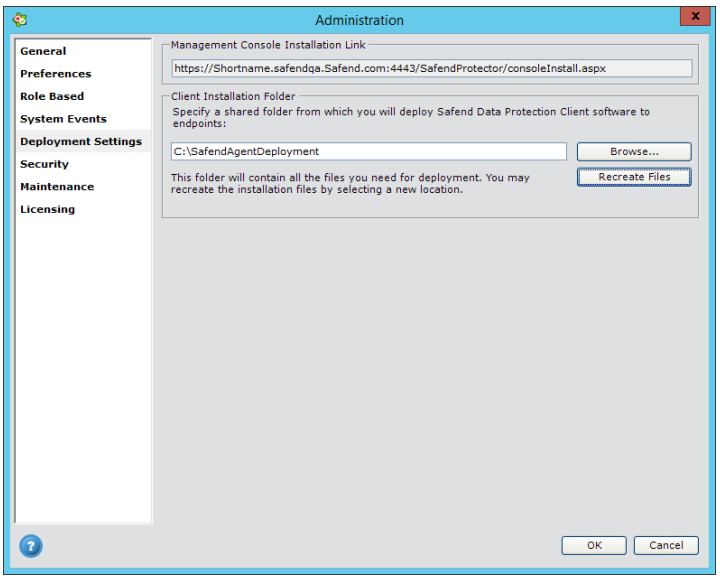
3. Select or de-select the required destinations and click **OK**.

Note: To add, edit or delete a destination, refer to

Alert Destination Repository

Configuring Deployment Settings Tab Settings

Installation settings are defined in the Deployment Settings tab in the Administration window:



11.1.2 Deployment Settings

The Deployment Settings tab enables you to specify folders and create installation files for the Console, Client.

Note: Additional Client settings such as uninstall password, log interval and Client visibility settings are set in the *Global Policy Settings* window, accessible from the *Tools* menu.

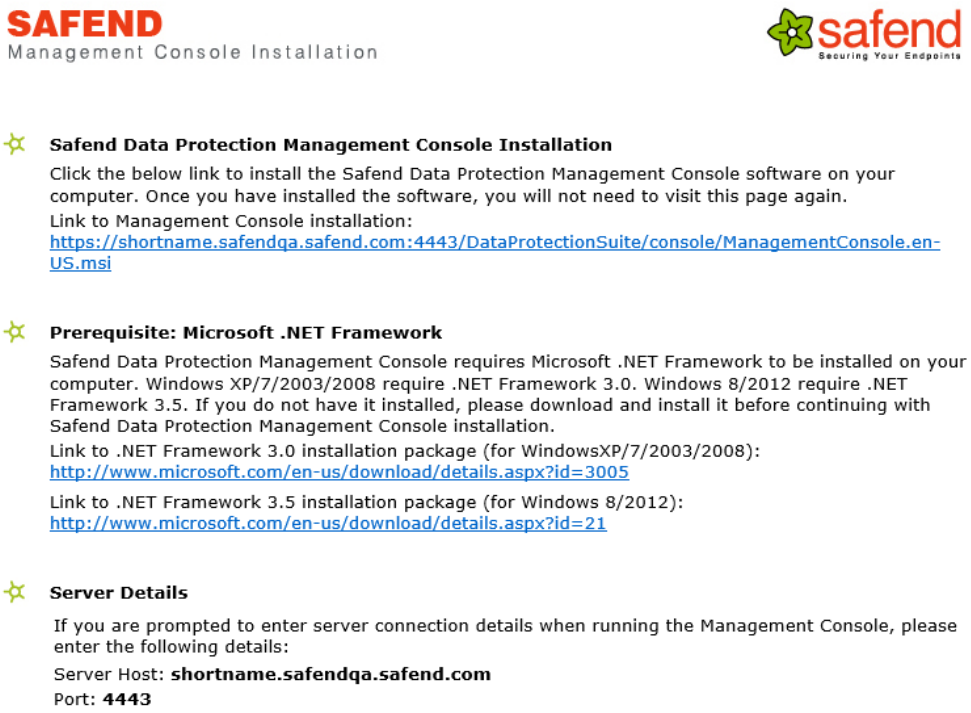
11.1.2.1 Management Console Installation Link

Typically, Management Consoles are deployed via a web page on the Management Server machines that allows users to download the Management Console installation package and install it on their machine.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

The link is in the following format:
https://<servername>:<serverport>/DataProtectionSuite/consoleInstall.aspx.

In order to install the Management Console on a new machine, all you need is to notify the user of this web page address. The installation web page appears as follows.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

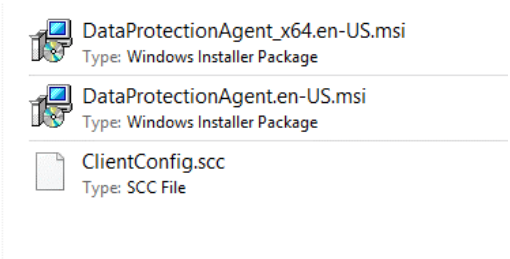
11.1.2.2 Client Installation Folder

This is the folder to which the Management Server exports the files needed for installing Safend Data Protection Suite Clients to endpoints. In order to deploy Clients, you need to define a folder for the installation files to be created. This folder should typically be a network path accessible for deploying software to endpoints.

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the Administration window for the modifications to apply.

Setting the shared folder for client installation files

1. Click **Browse**.
2. Select a network path for the shared folder and click **OK**.
3. Once you set a new path, the Server will copy the following files to the new path:
   a) DataProtectionAgent.msi. For a machine running 32-bit versions of Windows.
   b) DataProtectionAgent_x64.msi. For a machine running 64-bit versions of Windows.
   c) ClientConfig.scc
   d) LegacyClientConfig.scc. For installing the legacy clients of v3.3.



4. You also can click **Recreate Files** at any time to recreate files, if for some reason they were damaged.

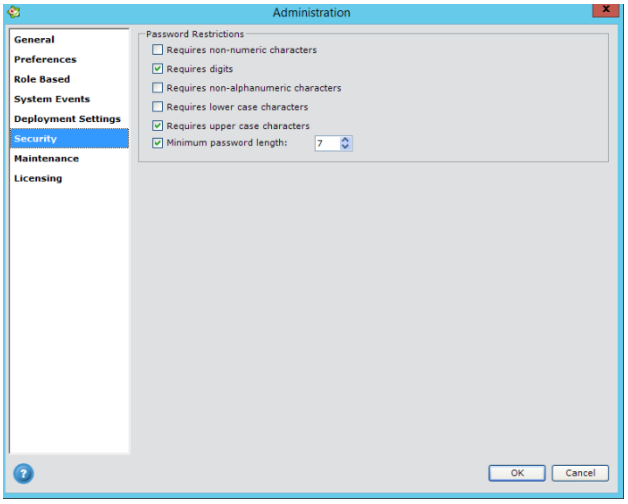
Refer to the Safend Data Protection Suite Installation Guide for instruction regarding Client deployment.

Note: Additional Client settings such as uninstall password, log interval and Client visibility settings are set in the *Global Policy Settings* window, accessible from the *Tools* menu.

11.1.2.3 Configuring Security Tab Settings

Password Restriction settings are defined in the Security tab in the Administration window:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Password Restrictions

Safend Data Protection Suite provides a number of places where its operation is password protected, such as: when uninstalling a client, when using its Offline Access Utility, when accessing the Administration on a Safend Data Protection Suite client and when using internal hard disk encryption (with Local Users Check In enabled or on legacy Encryptor 2.0 clients).

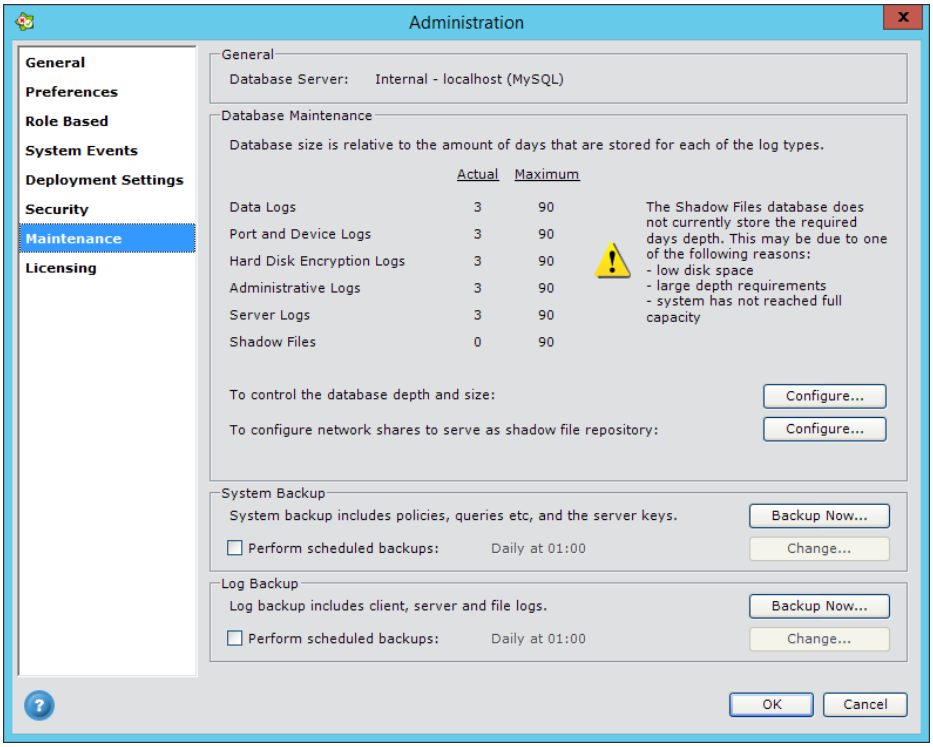
Check the relevant options in this area to control the characteristics of the passwords that can be used in Safend Data Protection Suite, such as the type and quantity of characters and the maximum password length. You can select any combination of the provided options in this section of the window.

Attention System Administrator: The password restriction you set must also adhere to the Windows password requirements in order for the internal hard disk encryption SSO (Single Sign On) feature to function (only on legacy, Encryptor 2.0 clients).

11.1.2.4 Configuring Maintenance Tab Settings

Maintenance settings are defined in the Maintenance tab in the Administration window:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Maintenance Settings

From the Maintenance tab you can perform various system maintenance activities. These allow you to define database maintenance, system backup and log backup settings. It contains the following sections:

- **Error! Reference source not found.**
- Database Maintenance
- System Backup
- Log Backup

Whenever you modify any of the settings in this tab, you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

Backups should be restored to the same DPS version from which they were made. Restoring a backup from a newer or older version of DPS may cause errors and\or failures.

This section displays the name of the database server and whether it is the Safend Data Protection Suite internal MySQL server or an external MS SQL server.

Database Maintenance

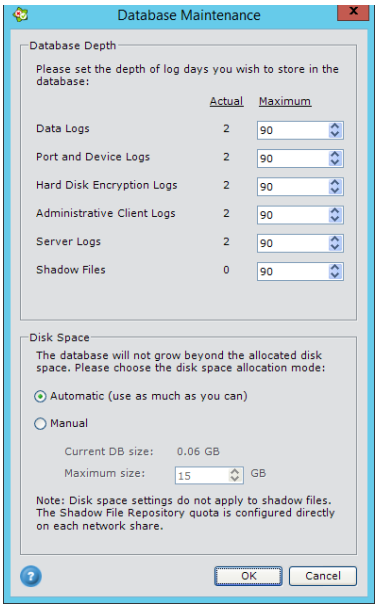
This section deals with managing the database by means of setting the number of log days (depth) you wish to store for each type of log, and defining the disk space allocated to the database, in which logs comprise the bulk of the disk space. The purpose of database management is to allow you to save the depth you require, or as close to it as possible. This is done in the Database Maintenance window, as described in the Defining Database Maintenance

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

settings section. In addition, this section allows you to configure the network shares to be used as the central repository for shadowed files, as described in the *Defining File Shadowing Network Shares* section.

Opening the Database Maintenance window

In the Database Maintenance section, click Configure beside To control the database depth and size. The Database Maintenance window opens:



Defining Database Maintenance settings

The Database Maintenance window includes two sections:

> **Database Depth**: displays the actual number of days currently stored for each log type and allows you to set the required (maximum) number of storing days for each log type.

> **Disk Space**: allows you to allocate database disk space automatically or manually. By default, disk space is managed automatically and aims to avail you of the requested depth. We recommend that you allocate disk space manually, only if you have another application running on the same server whose disk space usage is of a rapidly-growing nature.

Note: When using an external database this section does not appear, since in this case disk space is not managed by Safend Data Protection Suite.

1. In the Database Depth section, set the number of days you wish to store for each log type – Client logs, File logs, Server logs and Shadow Files.
2. Click the appropriate radio button in the Disk Space section to select whether you wish disk space to be allocated automatically or whether you prefer manual disk space allocation (current database size is displayed).
   Note: When using an external database this section does not appear, since in this case disk space is not managed by the Safend Data Protection Suite.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3. If you selected manual allocation of disk space, set the maximum disk space to be used by the database.

4. Click **OK**. Log depth and database size will now conform to these settings.

Note: When using the Safend Data Protection Suite internal database, when disk space is too low to hold the required database depth, an emergency purge is performed in which oldest records are deleted in order to free disk space. If this happens, a message appears in the *Database Maintenance* window and in the *Database* section of the Home Tab. It informs you that the database does not currently hold the required depth due to low disk space and that you should allocate additional disk space or change depth requirements.

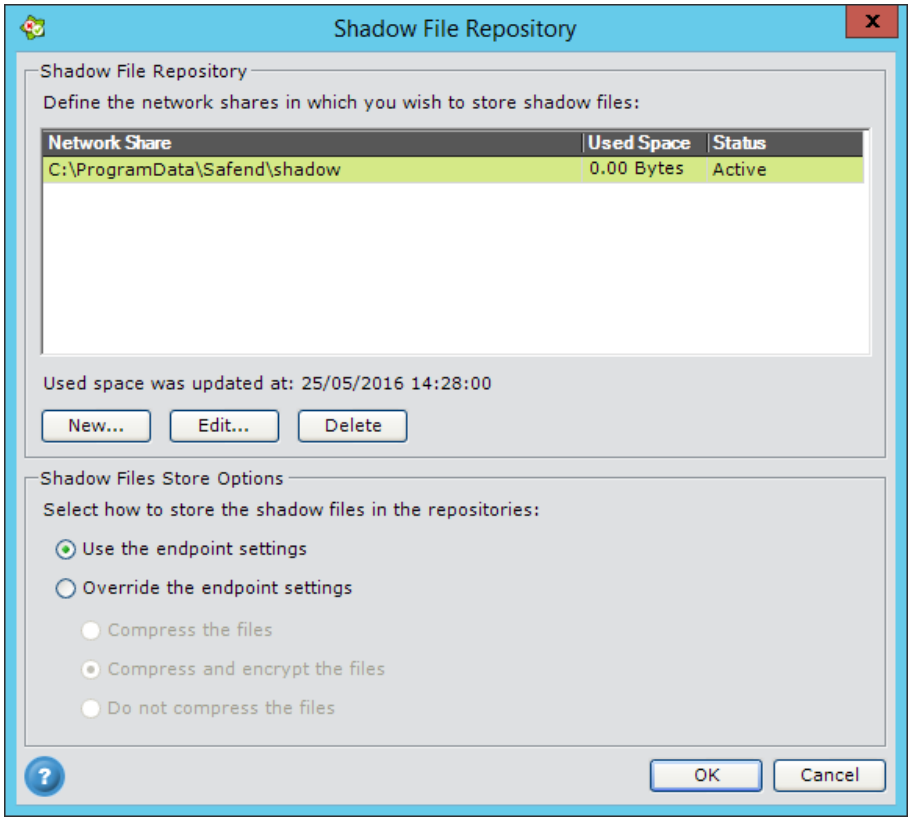
Defining File Shadowing Network Shares

This section describes how to configure the network shares to be used as the central repository for shadowed files. Security incidents which are applied with a monitoring level of "Shadow and Incident" or "Text and Incident" will be kept in this repository. One or more network shares can be defined by an administrator as the Shadowed files central repository. If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares. By default a local Shadow File Repository is defined on the Management Server machine. It is highly recommended to define another repository if a large volume of data is expected to arrive.

Configuring the File Shadowing network shares

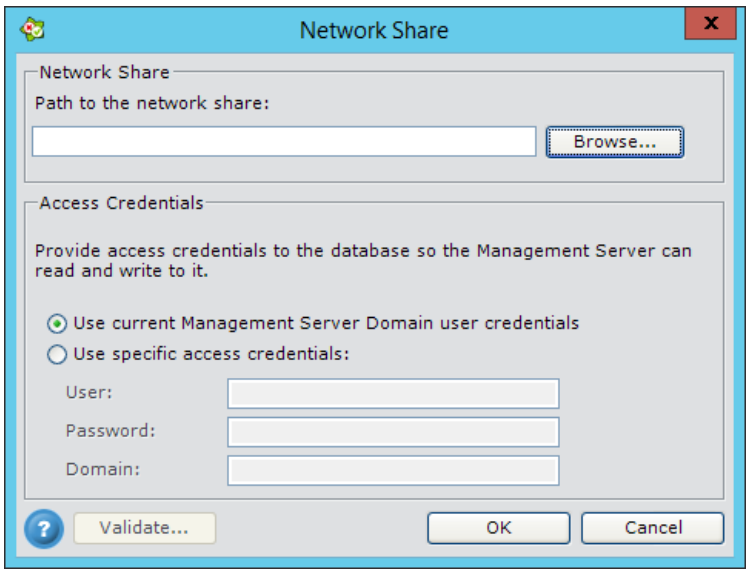
1. In the **Database Maintenance** area, to the right of the *To configure network shares as* shadow file repository field, click **Configure**. The following window is displayed listing the network shares already defined as shadowed files repository.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Note: For Shadow Files Store Options, when you choose Use the endpoint settings, the server stores the files received from the endpoint. This setting is optimal for performance.

2. Click *the* **New** button to define a new network share. The following window is displayed:



3. Click **Browse** to display a window in which you can specify the path to this network share.
4. Select this path and then click the **Make New Folder**. A window is displayed requesting the credentials to access this folder.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

5. Enter the credentials and click **Validate** to test access to the folder. Click **OK**.

   Note: If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares and that seamless failover can occur in cases of failure when accessing one of the shares.

6. *You* can compress and encrypt the files in the repository by selecting one of the following options. Only Authorized administrators are able to access encrypted files from the Management Console.

   a) Compress the files

   b) Compress and encrypt the files

   c) Do not compress the files

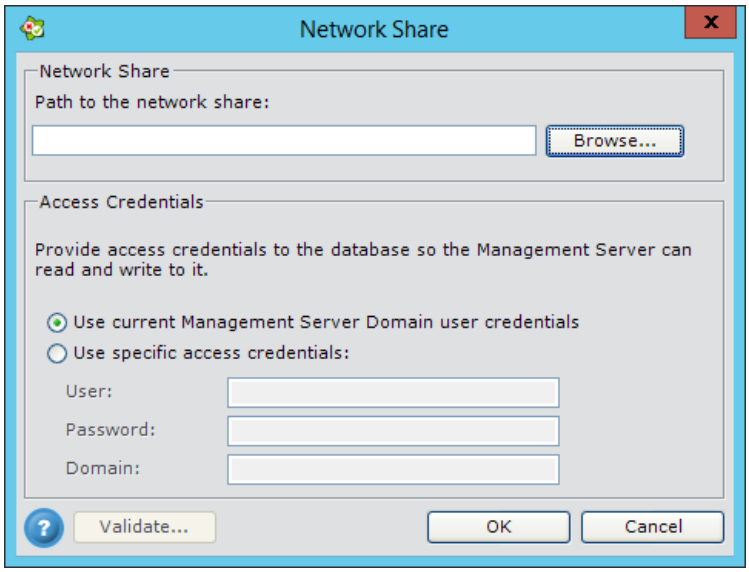
7. The added network share is defined as Active by default in the *Shadow File Repository*. You can right-click on it in the window to select the **Deactivate** option. Deactivating a network share means that shadowed files are no *longer written to it. However, files that are already in the network share can still be viewed by an authorized administrator.*

8. You can delete a network share by selecting it in the Shadow File Repository and clicking Delete. If you delete a network share, then its files can no longer be viewed by an authorized administrator.

Network Share

In Shadow File Repository you can edit or define a new file share.

1. Click **New** in Shadow File Repository. The Network Share window is displayed.



2. Click **Browse** to display a window in which you can specify the path to this network share.

3. Select this path and then click **Make New Folder**. A window is displayed requesting the credentials to access this folder.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4. Enter the credentials and click **Validate** to test access to the folder. Click **OK.**

   Note: If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares and that seamless failover can occur in cases of failure when accessing one of the shares.

5. To edit a network share: click **Edit** in Shadow File Repository. The Network Share window is displayed. Make the necessary changes.

System Backup

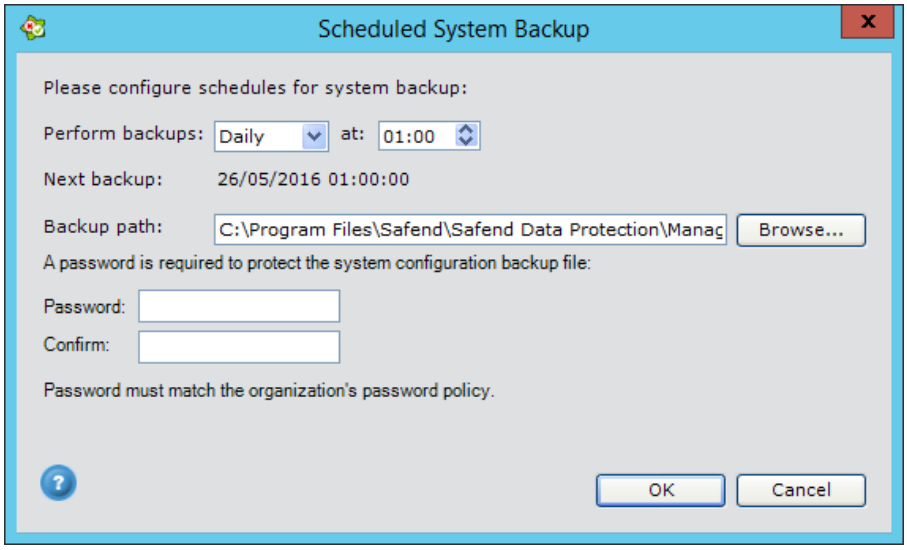
Backing up your system is also recommended, so that your existing system can be restored, should this be necessary in cases when you need to re-install the Management Server. System backup includes backing up your policy definitions, log query definitions and server keys. You may perform ad-hoc backup at any time, or schedule predefined backups.

Unscheduled backup

1. In the System Backup section, click **Backup Now**. The System Key Backup window opens.
2. Click the **Browse** button to select the desired path, to save the system backup file.
3. Enter a password and confirm the password. The password must conform to the company password policy.
4. Click **OK**. The System is backed up.

Scheduled backup

1. In the System Backup section, check the Perform scheduled backup checkbox. System backup will be performed at the scheduled times (Daily at).
2. In the System Backup section, click **Change**. The Scheduled System Backup window opens:



3. In this window you can set the interval (daily, weekly or monthly) and the time for your scheduled System backup, and the backup path.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

a) Set **Perform backups** interval and time.

b) Click **Browse** to select the backup path.

c) Enter a password and confirm the password. The password must conform to the company password policy.

d) Click **OK**. The configuration backup schedule is now set. Configuration backup files are saved under the following name convention: ConfigurationBackup01JAN2006_2359.SCB, where 01Jan2006_2359 are the time and date. The new backup file does not overwrite the current file, so that two backup files are always available.

Log Backup

When using an external database this section does not appear because backup is not managed by Safend Data Protection Suite.

In much the same way as for your configuration, you can also backup your logs. This includes Clients logs, Server logs and File logs. You can perform ad-hoc backup at any time, or schedule predefined backups.

Unschedule backup

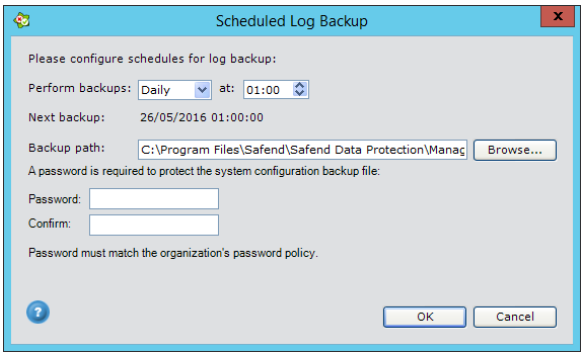
1. In the Log Backup section, click **Backup Now**. The *Select Log Backup File* window opens.
2. Select the desired path, enter the desired file name and click **Save**. Logs are backed up.

Scheduled backup

In the Log Backup section, check the Perform scheduled backup checkbox. Log backup will be performed at the scheduled times (the upcoming schedule time is displayed). If you wish to change the log backup schedule, you may do so.

Scheduling log backup

In the Log Backup section, click Change. The Scheduled Log Backup window opens:



In this window you can set the interval (daily, weekly or monthly) and the time for your scheduled log backup, and the backup path.

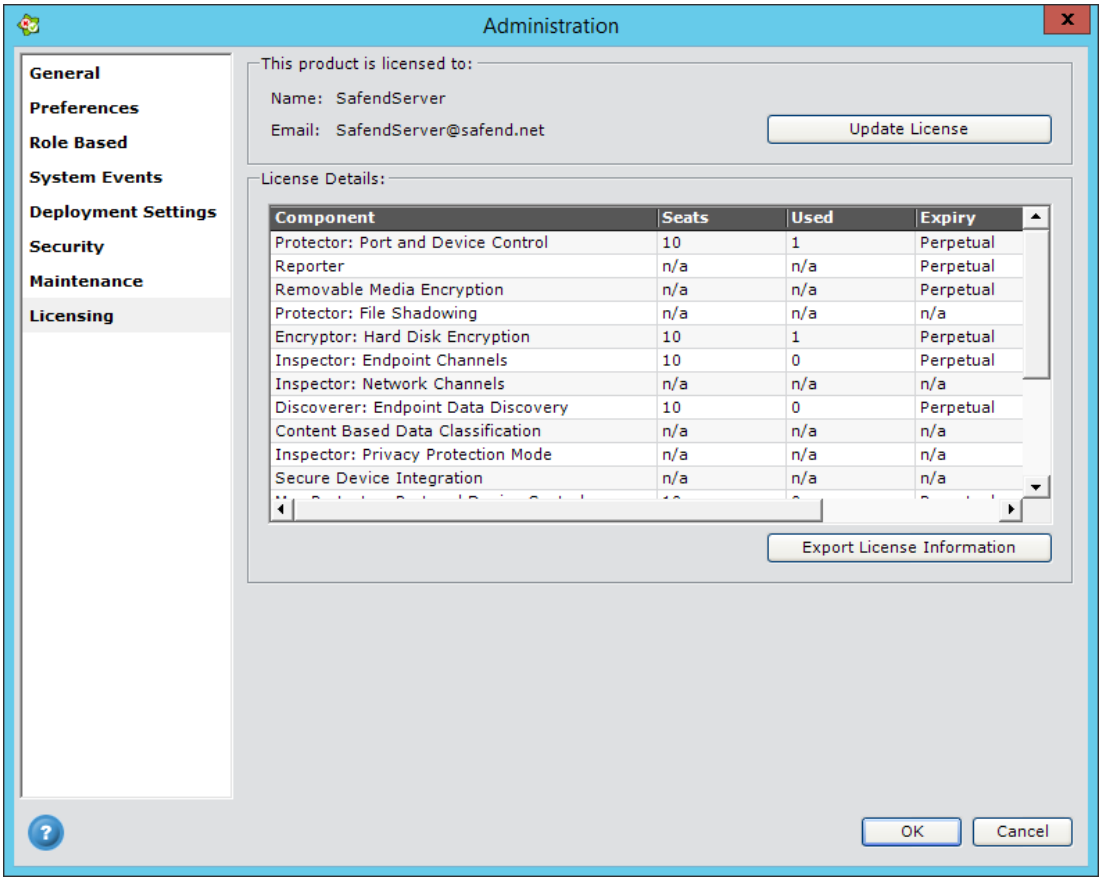
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Setting backup parameters

1. Set Perform backups interval and time.
2. Click **Browse** to select the backup path.
3. Enter a password and confirm the password. The password must conform to the company password policy.
4. Click **OK**. The log backup schedule is now set. Log backup files are saved under the following name convention: LogsBackup01JAN2006_2359.SLB, where 01Jan2006_2359 are the time and date. The new backup file does not overwrite the current file, so that two backup files are always available.

11.1.2.5 Configuring Licensing Tab Settings

Licensing details are displayed, as well as updated, in the Licensing tab in the Administration window:



The first time you open the application, a window opens to alert you that the installation will expire in 30 days. During this period you should contact Safend and purchase a license for the product. If the license has already expired, a message is displayed and you cannot perform any operations in the system until a valid license key is entered.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

The Administration window Licensing tab displays licensing details for the Safend Data Protection Suite. This license can be updated, as necessary. The Licensing tab contains the following sections:

> License Information (This product is licensed to)

> License Details

Note: Whenever you modify any of the settings in this tab. you must click **OK** at the bottom of the *Administration* window for the modifications to be applied.

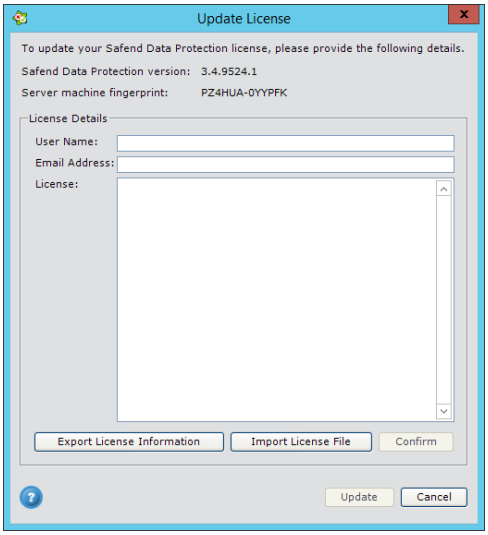
License Information (This product is licensed to)

Here is listed the name of the person the product is licensed to and their email address. You are also able to update the license.

You can enter a different license key using the Update License button. Remember that a new license overwrites the existing license. It is not appended to your current license. For example: if your current license expires in one year and you add a license for another year, you will still only have a one-year license.

Updating the license

1. Click the **Update License** button. The Update License window is displayed.



2. In order to obtain a license key, contact Safend or your local reseller and provide the Server machine fingerprint as it appears in the screen. For example, the fingerprint in the window above is: PIQOCE-64PM3H.

Using this fingerprint, a license key will be generated for you and can only be used on this specific machine.

Note: You cannot use this key on any other machine. If you wish to migrate your Management Server to another machine, please contact your local reseller or Safend Support at mailto:support@Safend.net.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

3. In the **User Name** field, enter your user name as it appears in the license key sent to you.
4. In the Email Address field, enter your email address as it appears in the license key sent to you from Safend.
5. In the Key field, enter the license key received from Safend.
6. Click **Confirm**. The License Properties are displayed, showing your updated license information, such as the allowed number of seats and the validity period of this license. In some cases, a warning message will appear after you click Confirm. This indicates an invalid or an expired license key.
7. Review the licensing information to ensure its correctness.
8. Click Up**date** to update the license.

Note: Once you have updated the license, the previous license is completely removed. Therefore, use caution when entering licensing details.

9. You have the additional option to export the license information or import the license file by clicking the relevant button.

License Details

Column	Description
Component	The name of the product (e.g., Protector, Inspector).
Seats	The number of allowed licensed Client stations.
Used	The number of seats used.
Expiry	The expiry date for using this product.

Here again you have the option to export the license information, by clicking Export License Information.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

12 End-User Experience

12.1 Safend Data Protection Suite Agents

The Safend Data Protection Suite Agent should be installed on the computers of your organization in order to protect the data on the endpoint. No setup or configuration of the agent is required, and few operations are required, except when encryption or decryption of storage devices is required.

Two indications may appear on a computer that is protected by Safend Data Protection Suite according to how the administrator configured the policy.

Note: When Client Visibility on Endpoints is set to Stealth Mode the messages and tray icon are hidden.

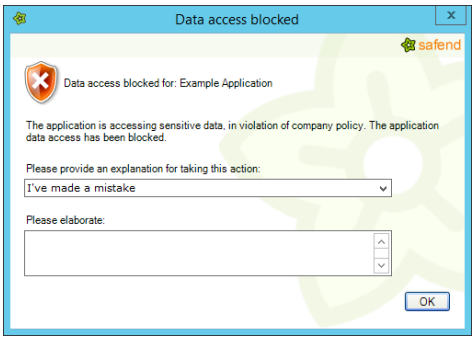
12.1.1 Safend Data Protection Suite Agent Messages

Safend Data Protection Suite messages begin appearing immediately after installation, according to the Options Settings defined for the policy applied to the computer/user. Whenever a message appears, you can click to close it, otherwise it disappears by itself after a few moments. Messages display the port name or the device model. Refer to *Configuring Agent Messages* to learn how you can modify them to suit your organization. The messages are divided into Data Control and Port and Device Control messages.

12.1.2 Data Control Messages

Here is a description of all the Data Control messages.

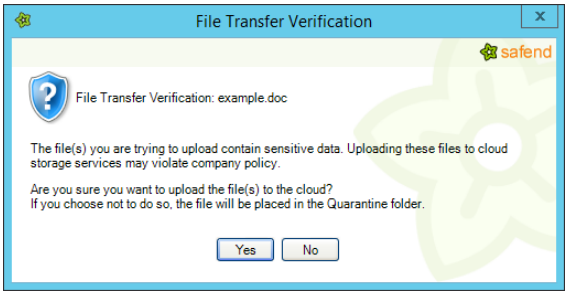
- **Application Group**: Here are the application group messages which may appear.
- **Application Group Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).
- **Application Group Blocked**: The application data access has been blocked since the application is accessing sensitive data, in violation of company policy.



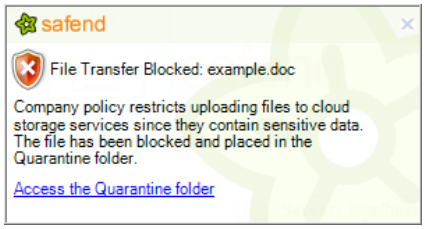
- **Cloud Storage Messages**: Here are the email messages which may appear.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

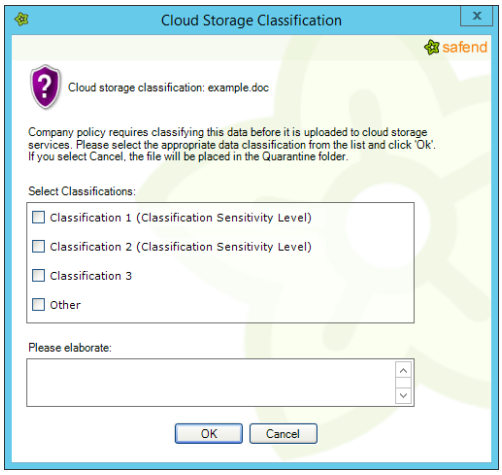
- **Cloud Storage Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).
- **Cloud Storage – Ask User**: You are asked if you want to upload file(s) to the cloud because the file(s) trying to be uploaded contain sensitive data. Uploading these files to the cloud storage services may violate company policy.



- **Cloud Storage Blocked**: File transfer has been blocked because company policy restricts uploading files to cloud storage services since they contain sensitive data.



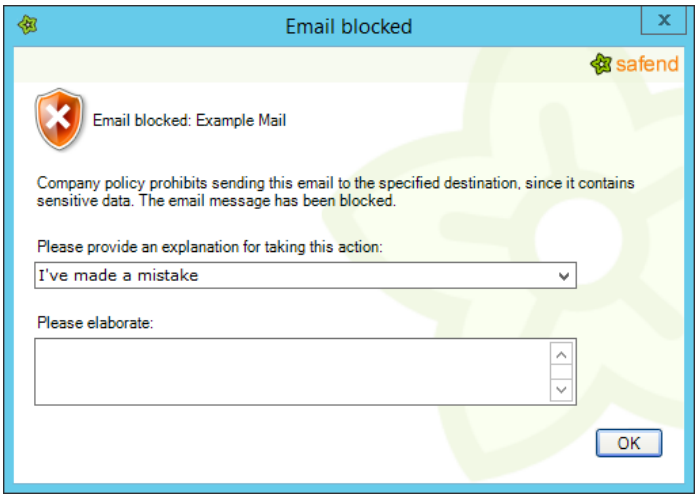
- **Cloud Storage Classify**: Here you are required to classify data before it is uploaded to the cloud storage services. You must select the appropriate data classification from the list below and click OK.



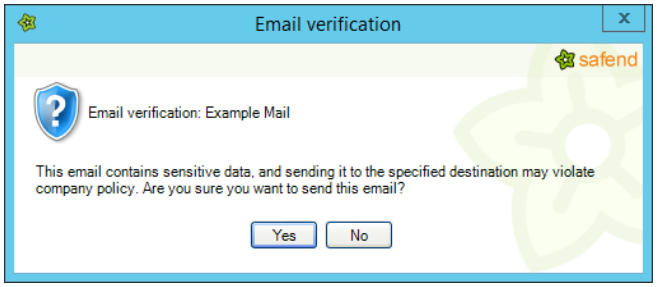
- Email messages: Here are the email messages which may appear.
- **Email Allowed and Monitored**: No message will be displayed unless you change this in the *End User Message Editor* (select, *Show a message to end users)*. This action has been recorded since company policy restricts sending this email to the specified destination, since it contains sensitive data.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

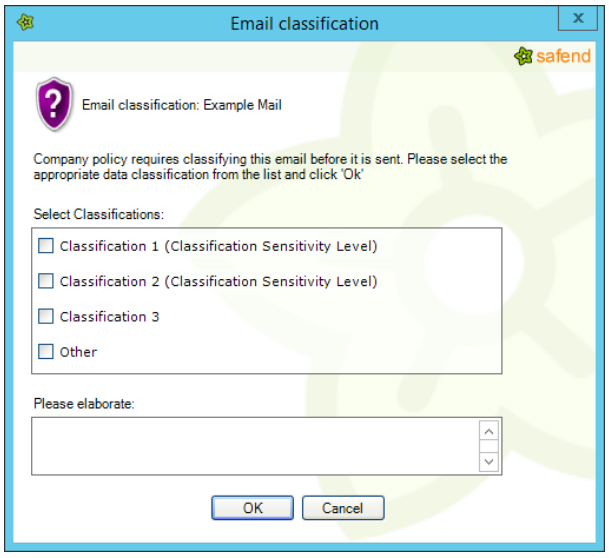
> **Email Blocked**: The email message has been blocked because it contains sensitive data that the company policy prohibits.



> **Email – Ask User**: Sending this email to the specified destination may violate company policy because it contains sensitive data. You are asked whether you are sure you want to send this email.



> **Email Classify**: This message is for when the company policy requires classifying an email before it is sent.



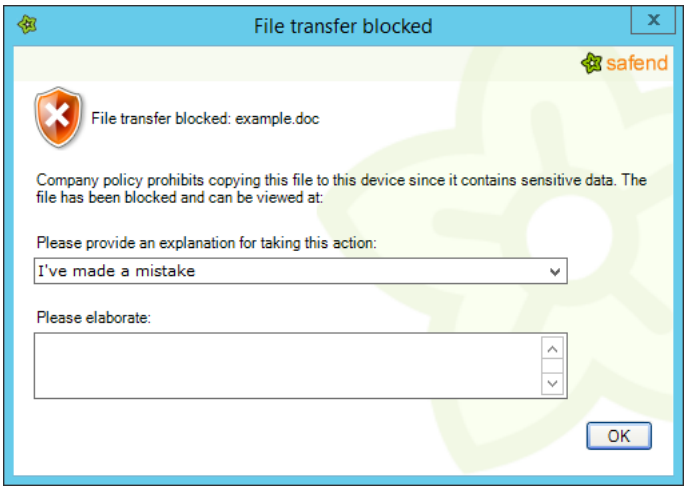
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

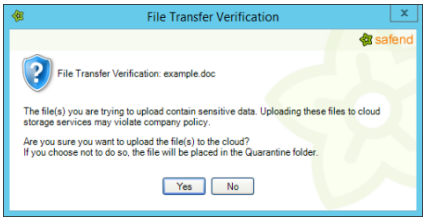
> **External Storage Messages**: Here are the external storage messages which may appear.

> **External Storage Alllowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).

> **External Storage Blocked**: This file has been blocked because company policy prohibits copying this file to this device since it contains sensitive data. A location is indicated where it can be viewed.



> **External Storage – Ask User**: Since this file contains sensitive data, and transferring it to the device may violate company policy, you are asked if you want to transfer this file to this device.

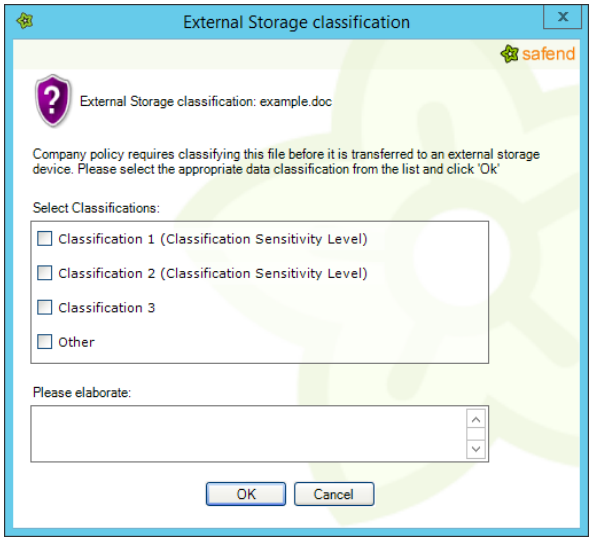


> **External Storage Encrypt**: You are asked to encrypt your device because company policy prohibits copying this file to a non encrypted device, since it contains sensitive data.



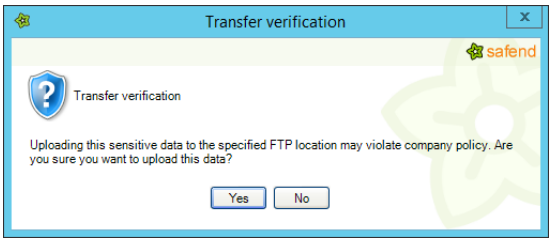
> **External Storage – Classify: This message** is for when the company policy requires classifying a file before it is transferred to an external storage device.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

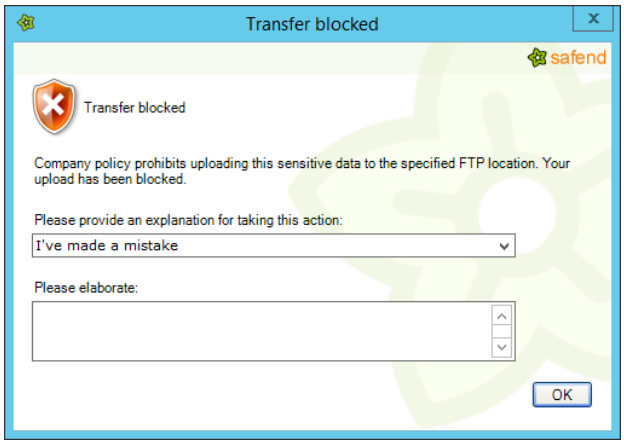


Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

- FTP Messages: Here are the FTP messages which may appear.
- **FTP Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).
- **FTP – Ask User**: You are asked whether you want to upload this data, since uploading this sensitive data to the specified FTP location may violate company policy.

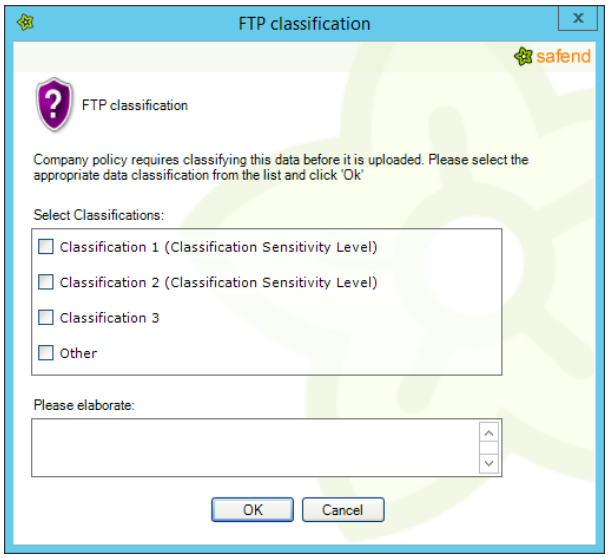


- **FTP Blocked**: This action has been blocked since company policy prohibits uploading this sensitive data to the specified FTP location.



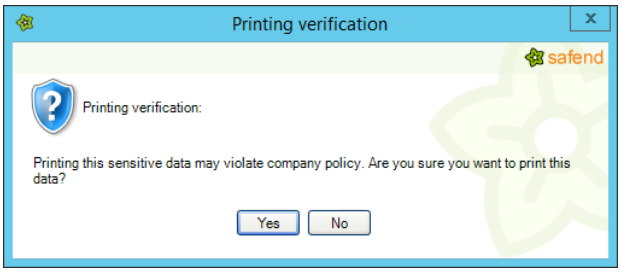
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

- **FTP – Classify**: This message is for when the company policy requires classifying this data before it is uploaded.



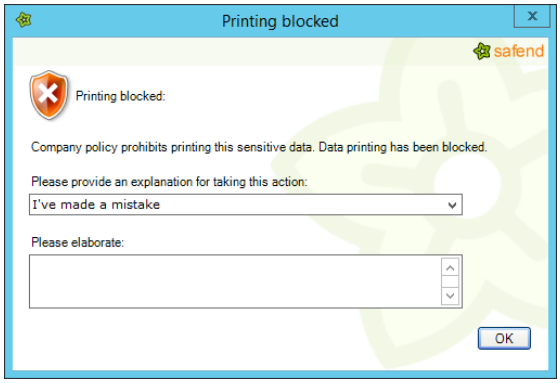
Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

- Local Printers Messages: Here are the local printer messages which may appear.
- **Local Printers Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).
- **Local Printers - Ask User**: Since printing this sensitive data may violate company policy, you are asked if you want to print this data.

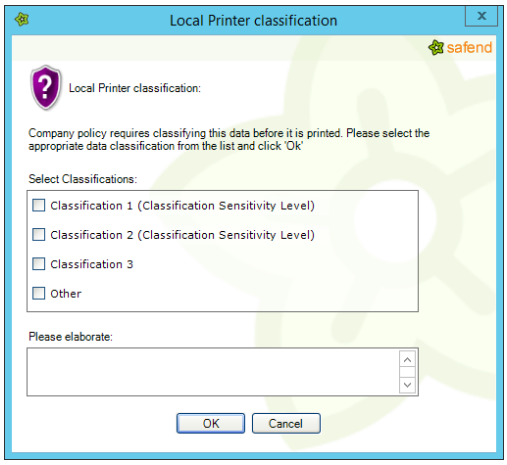


- **Local Printers Blocked**: Data printing has been blocked since company policy prohibits printing this sensitive data.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



> **Local Printers – Classify**: This message is for when the company policy requires classifying this data before it is printed.

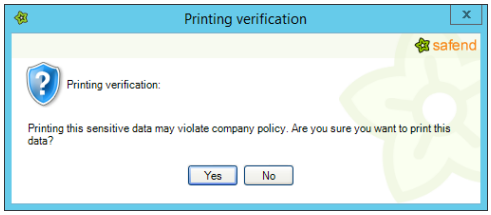


Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

> Network Printers: Here are the network printer messages which may appear.

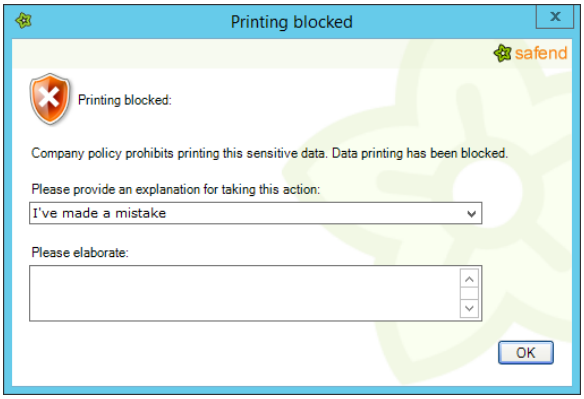
> **Network Printer Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).

> **Network Printers - Ask User**: Since printing this sensitive data may violate company policy, you are asked whether you want to print this data.

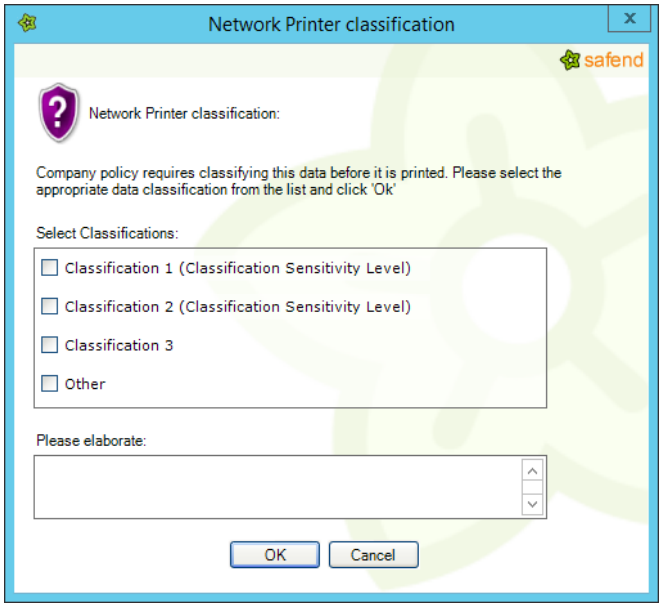


> **Network Printers Blocked**: Data printing has been blocked since company policy prohibits printing this sensitive data.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



> **Network Printers – Classify**: This message is for when the company policy requires classifying this data before it is printed.



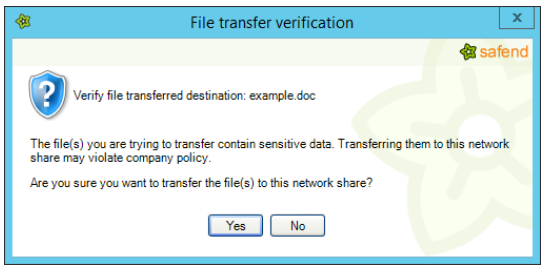
Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

> **Network Shares Messages**: Here are the network shares messages which may appear.

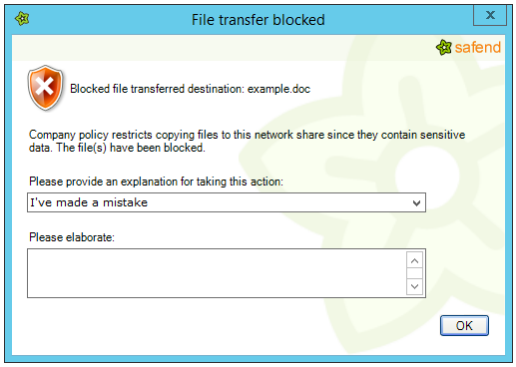
> **Network Shares Allowed and Monitored**: No message will be displayed unless you change this in the End User Message Editor (select, Show a message to end users).

> **Network Shares – Ask User**: You are asked whether you want to transfer this file to this device, since this file contains sensitive data and transferring it the network share may violate company policy.

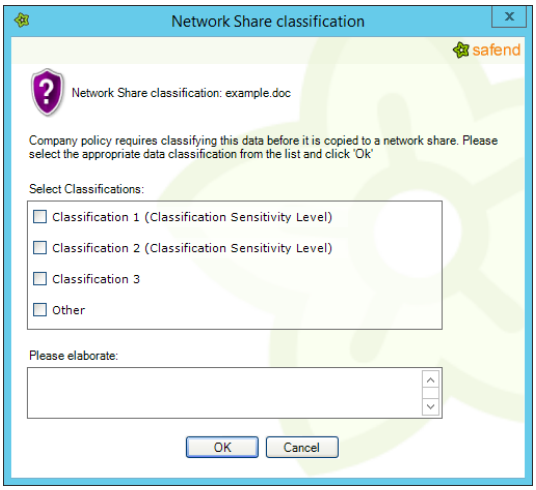
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



> **Network Shares Blocked**: The file has been blocked, since company policy prohibits copying this file to this device network share, since it contains sensitive data.



> **Network Shares – Classify**: This message is for when the company policy requires classifying this data before it is copied to a network share.



Select the relevant data classifications from the Select Classifications list. When placing the mouse over each classification, a tooltip will be displayed describing the specific classification.

12.1.2.1 Safend Data Protection Agent Options

In addition to protecting and monitoring host computers on an ongoing basis, Safend Data Protection Agent allows the end-user to perform additional actions on the host computer:

> Updating the Client's Policy

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

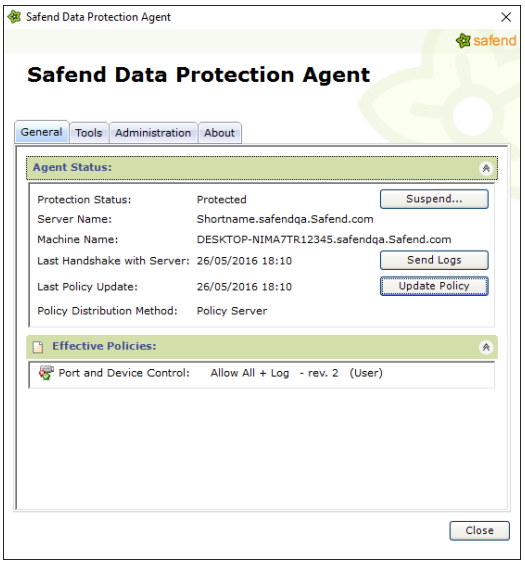
> Suspending Safend Protection on a Client

> Administrative Task

These actions are performed from the Safend Data Protection Agent window.

Opening the Safend Data Protection Agent window

Double-click the Safend Data Protection Suite tray icon or right-click the Safend Data Protection Suite tray icon and select **Options.** The *Safend Data Protection Agent* window is displayed.



Tab	Description
General	Agent Status: This displays the Protection status, Server name, Last handshake with server, Policy distribution method and the Last policy update. Suspend: to temporarily suspend protection on the client. Send Logs: to send logs outside of the pre-determined time intervals. Update Policy: to update a policy outside of the pre-determined time intervals. Effective Policies: lists the currently active policies. Hard Disk Encryption: Lists the Hard Disk Encryption and Authentication Status.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Tab	Description
Tools	Removable Media Encryption: Removable media encryption tasks are available by right clicking the removable storage devices or CD/DVD drives in My Computer. Quarantined Files: Files that were blocked and removed from the cloud storage folder by the Data Protection agent are placed in the Quarantined files folder. You can access the Quarantined files folder to recover blocked files. Note Quarantine blocked files only supports the cloud storage data channel at the moment. Agent Language: You can choose the display language of the agent.
Administration	Enables you to access administration mode with a password.
About	Provides general Safend Data Protection Suite Client information.

12.1.2.2 Updating the Client's Policy

A Safend Data Protection Suite Client's policy is updated by a process in which the Client checks the Management Server at predefined intervals and updates the policy if it has changed. Updating a Policy on a Client in Chapter 8 Managing Clients discusses how to notify Safend Protector Clients to refresh their policy at the earliest opportunity, through the Safend Protector Management Console. For a single, specific Client this also can be done from the host computer, outside of the pre-defined time interval.

Updating a policy from its host computer

From the General tab of the Safend Data Protection Agent window, click Update Policy. Alternatively, right click the Safend icon in the windows tray and choose Update Policy.

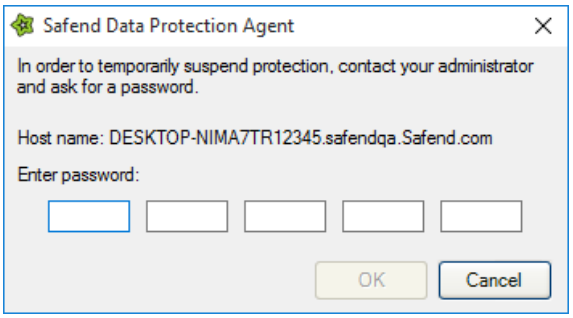
12.1.2.3 Suspending Safend Protection on a Client

As explained in Managing Clients, if you want to temporarily suspend Safend protection on a Client without having to uninstall it, you can do so in the Management Console by generating a suspension password which you give to the user and which the user in turn enters in order to lift protection. By using this option, you can suspend protection for up to a week. The next section explains what needs to be done on the Client side. In addition, the system administrator himself/herself can suspend protection ad hoc, for a short while (no longer than one day). Both options are explained below.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

12.1.2.4 SUSPENDING PROTECTION: USER

1. From the *General* tab of the Safend Data Protection Agent window, click **Suspend**. The following window is displayed.



2. Enter the Suspend Password provided by the system administrator and click OK. A message is displayed showing the period for suspension. Safend protection is suspended on the host for the period predefined by the system administrator when generating the suspension password. At the end of this period protection is automatically resumed.

12.1.2.5 ADMINISTRATIVE TASKS

Some administrative options are available on the endpoint. In the Administration tab you must enter an Administration password to carry out administration tasks. After entering the password the following is displayed.



Option	Description
Administration Mode	Indicates you are currently in Administration mode.
Agent Status	Indicates the current protection status of the agent. Click Suspend protection to suspend protection on the machine.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Anti Hardware Key Logger Protection	This option is used to approve keyboards which are suspected of being key loggers.

After you perform the required functions, click Close to close the Safend Data Protection Agent window. The next time you access the agent it does not offer administrative functions, until you type the Administrator Password.

Note: Always remember to close the *Safend Data Protection Agent* window after performing administrative tasks. Not closing the window will allow unauthorized users to perform administrative functions.

12.1.2.6 Suspend Protection on a Client by the System Administrator

If you (the administrator) need to suspend Safend protection on a Client, you can do so with the Client Administration Password.

Suspending the agent

1. Select the Administration tab.
2. Enter the *Administration password* and click **Access**.
3. In the Agent Status section click **Suspend protection**. Protection is suspended.
4. Click **Resume Now** in the Agent Status section to resume protection.
5. Close the Safend Data Protection Agent window.

Note: If you forget to resume protection, it will be resumed automatically 24 hours after suspension.

12.1.2.7 Reset Keyboards (approve keyboard hubs)

A policy can protect computers against hardware key loggers. It enables you to block a keyboard when Safend Data Protection Suite suspects that a hardware key logger is connected. In some cases when a keyboard is connected through a hub (or more than one), Safend Data Protection Suite may wrongly suspect the hub of being a key logger, and block the keyboard. Performing a "keyboard reset" as described below approves all the hubs through which the keyboard is connected at the time the reset is performed.

Note: Before resetting the keyboard you must verify that a hardware key logger is not connected, otherwise it will be approved.

1. Enter Administration mode (see Administrative Tasks).
2. In the Anti Hardware Key Logger Protection section of the Safend Data Protection Agent, click **Reset Keyboards**. The Reset Keyboards window opens.
3. Make sure that a hardware key logger is not connected between the keyboard and the computer.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4. In the Reset Keyboards window, click **Yes**. All the hubs through which the keyboard is connected are now approved, and the keyboard will resume working.

Note: Always remember to close the Safend Data Protection Agent window after performing administrative tasks. Not closing the window will allow unauthorized users to perform administrative functions.

12.1.2.8 Encryption and Decryption of Removable Storage Devices

Note: When encrypting removable storage devices containing the U3 application, the U3 application will no longer function.

Safend Data Protection Suite enables the end-user to encrypt removable storage devices and External Hard Disks and CD/DVDs. In addition to ensuring that loss or theft of the encrypted device causes no damage to the organization, this prevents leakage of information by users. As a rule, when a storage device is encrypted, it can be used only within the organizational environment, and explicit authorization is required in order to access it on non-organizational computers.

In some cases, the endpoint policy can dictate that such a storage device be encrypted, in which case encryption is mandatory. Alternatively, the end-user may choose to encrypt storage devices even when the policy does not mandate it.

When the policy requires encryption, any time a user attaches a non-encrypted device, the device is either blocked or permitted Read Only access depending on policy settings. At the same time, the user is given the ability to encrypt the device in order to use it. This is explained in Encrypting a Device.

A policy can also allow authorized users access to an organizationally-encrypted device on a non-organizational computer by means of decryption. This is explained in Accessing Encrypted Devices when Offline.

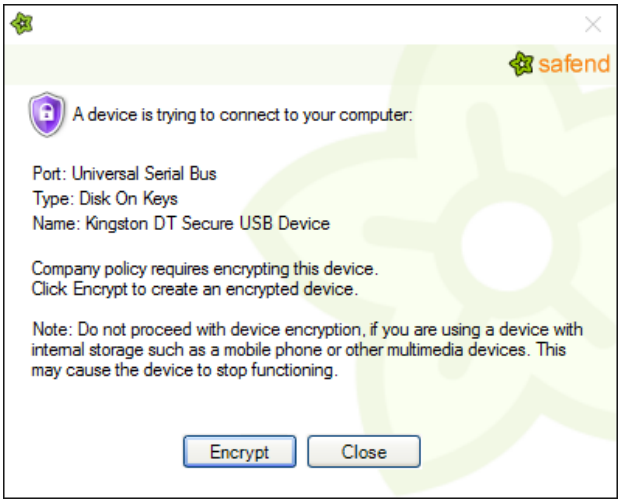
Important: Organizationally encrypted removable storage devices and external hard disks may be used on any Safend protected organizational computers, including those whose effective policy does not require encryption.

12.1.2.9 Encrypting a Device

As mentioned earlier, removable storage devices and external hard disks can be encrypted, whether or not the endpoint policy requires it.

If a policy requires encryption, and a non-encrypted device is attached to the computer, the non-encrypted device is either blocked or permitted Read Only access depending on policy settings. In order to have full use of the device, it must be encrypted by a Safend protected computer in your organization. When a non-encrypted device is connected, a window appears informing the user of this and asking him/her to encrypt the device.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

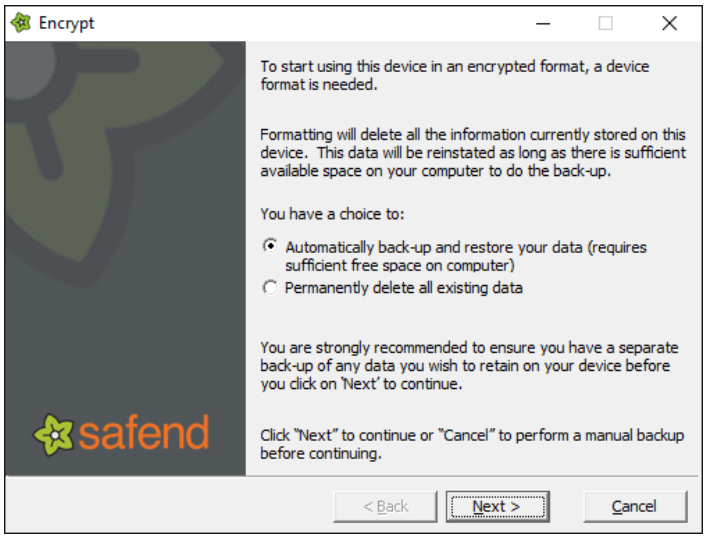


If the policy does not require encryption, the device may still be encrypted. However, in this case no end-user message appears.

Encrypting a removable storage device/external hard disk if required by a policy

Note: The steps for encrypting a removable storage device are the same whether you have selected *Device Volume Encryption* or *Device Storage Encryption*.

1. In the A Device is trying to connect to your computer window that appears when you connect the device, click **Encrypt**. The following window opens for a removable storage device:



   If you have not had enough time to click the *Unencrypted Device Connected* window and it disappears, follow the instructions below for encrypting a device when no window appears.

2. Select the appropriate radio button according to whether you wish to backup and restore the data on the device or whether you wish to delete existing data (this is necessary because encrypting the device formats it).

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

It is highly recommended to backup the information on the device before you continue with the encryption process.

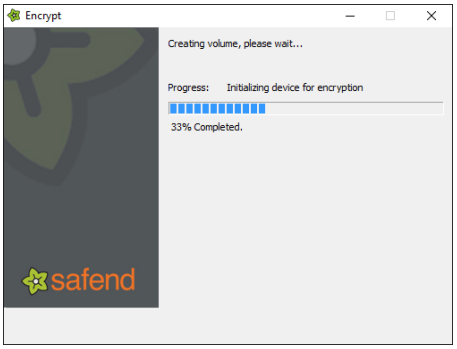
3. Click **Next**. If you have been assigned permission to set a password for accessing storage devices offline, then the following window is displayed. If not, skip this step.



4. Enter a password that will have to be entered on computers outside your organization in order to access its content. You can always set a new password in the future if desired.

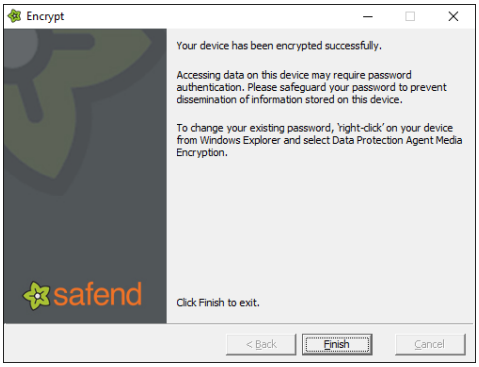
   Note: It is mandatory to set a password to enable offline access in order to use the device outside of the organization. The password that you set must adhere to the organization's password rules. The password for offline access can also be set as described in Setting an Offline Access Password.

   The encryption process (including backup and restore, if selected) begins and a progress bar appears as shown below.



5. When the encryption process is completed, the following message appears:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



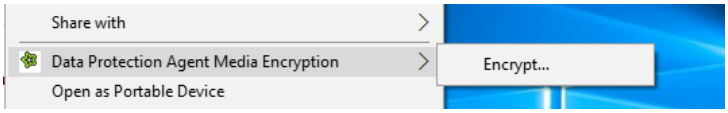
6. Click **Finish**. The device is now encrypted and the data stored on it is protected should the device be lost or stolen.

   In My Computer, encrypted devices are denoted by a special icon (a blue lock), as in Removable Disk (E:). To access the encrypted partition double click Removable Disk (E:).

   Note: When encrypting external hard drives that were formatted using advanced formatting technology (usually 3 terabyte and above), the user will be required to format the device once the encryption wizard has completed.

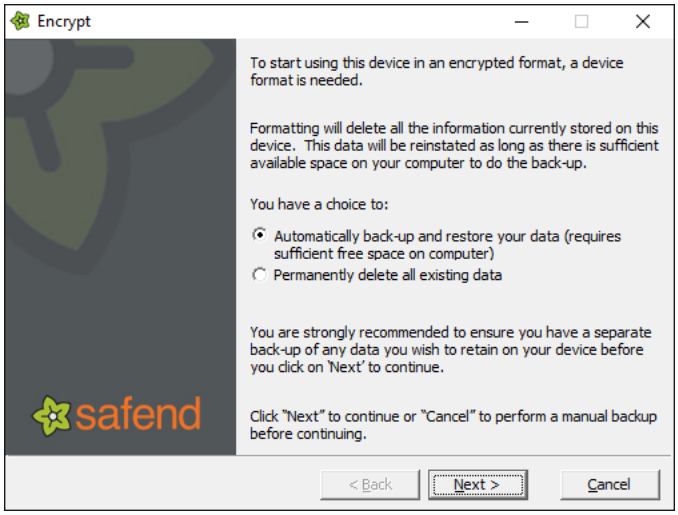
Encrypting a removable storage device when no end-user window appears

1. If the message has disappeared (it is only displayed for a few seconds), or if the policy does not mandate encryption (in which case no message appears), go to **My Computer** in Windows Explorer and right-click the device. The Data Protection Agent Media Encryption option appears in the right-click menu, and the sub-menu includes the **Encrypt** option, as shown in the following figure:



2. Click **Encrypt**. The *Encrypt* window opens:

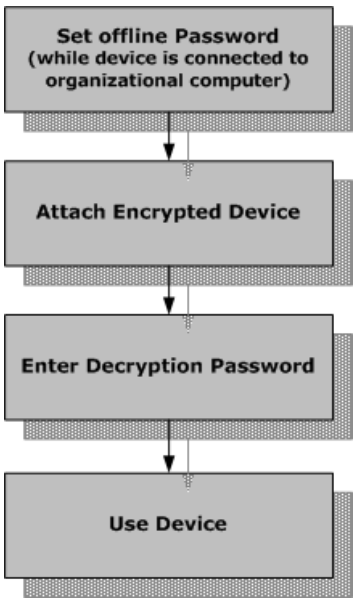
Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



3. Continue from step 2 above in Encrypting a Device.

12.1.2.10 Accessing Encrypted Devices when Offline

As a rule, organizationally-encrypted removable storage devices can be used only when connected to computers protected by the organization's Safend Data Protection Suite Clients. This rule notwithstanding, if the end-user's effective policy permits it, the user can have access to a removable storage device on non-company computers as well. The process of accessing encrypted devices on non-organizational computers includes the following steps:



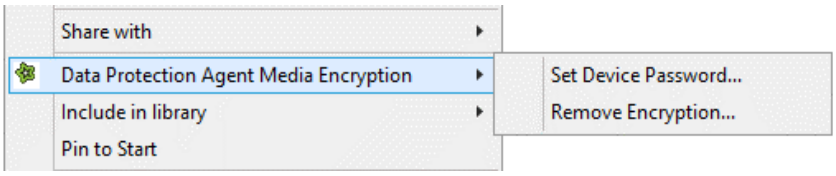
12.1.2.11 Setting an Offline Access Password: Decryption

If you choose *Set Access Password* during the encryption process this step is not necessary.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

When the end-user's effective policy permits usage of encrypted devices on non-company computers, an offline access (decryption) password can be set, which will be used to access the device offline.

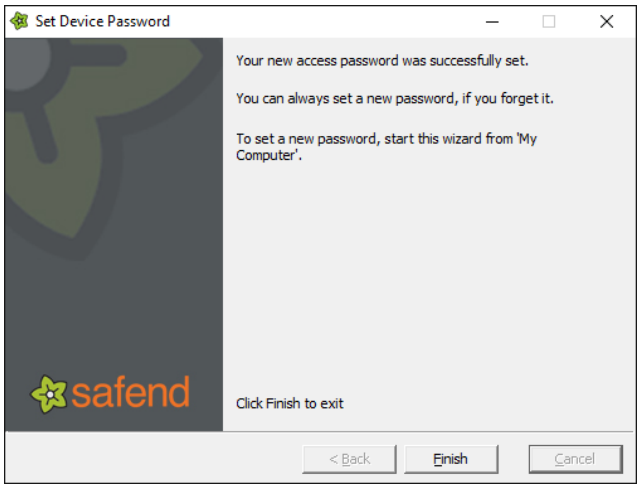
1. Connect the device you want to be able to access offline to your Safend protected computer.
2. In My Computer, right-click the device, and select the Safend Data Protection Suite shell extension:



3. Click **Set Device Password**. The Set Device Password window opens:



4. In this window, set a password, confirm it and click **Next**. The following window opens:



5. Click **Finish**. An offline access password is now set for the connected removable storage device.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

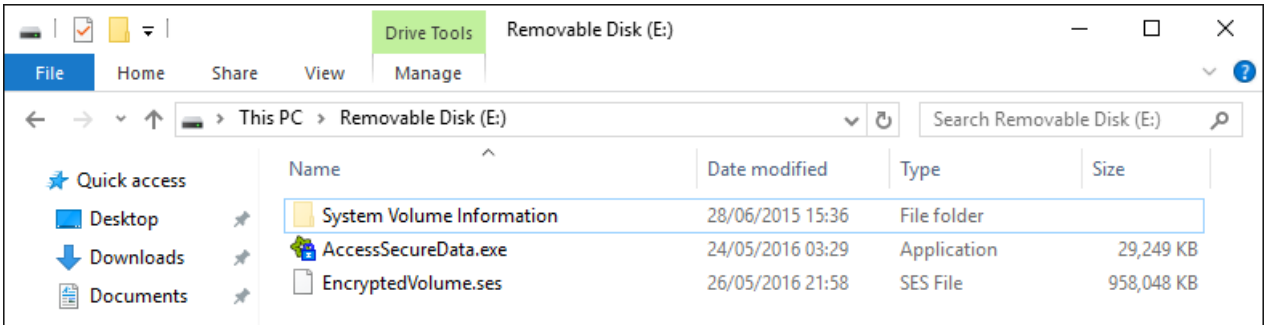
Note: The password that you set must adhere to the organization's password rules. If you forget it, or wish to change it, you may set a new offline access password at any time.

Offline Access to Encrypted Storage Devices

The Encrypted Storage Device option enables offline access to storage devices by permitted users without requiring them to have local administration rights. Files accessed in this way can only be modified and saved using the Save As option, and they cannot be accessed by another application or from a command line until Save As is performed to the local (unprotected) machine. This behavior is similar to an email attachment file or a Windows compressed folder.

Accessing an encrypted storage device offline on an unprotected machine

1. Connect the encrypted device (on which an Offline Access Password has been set) to the unprotected computer. In this drive, two files will be displayed: AcessSecureData.exe and EncryptedVolume.ses.



Note: Do not delete the container of the encrypted files from the removable storage device. Deleting the container will delete all information stored in it.

2. Double click **AcessSecureData.exe** to run the program to enable access to the data. The utility is now running and will request the offline access password (the password which was set in Setting an Offline Access Password) the first time an encrypted device is connected to the computer. What you see will depend on whether or not you have administration permission.

   a) **Administrator:** Type in your password and click **Access the device**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



A mounted volume containing the encrypted data will appear.

b) **Non-Administrator**: Type in your password and click **OK**.

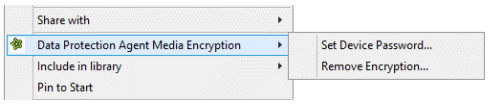


The *.ses file (encrypted volume) will open as a folder containing the encrypted files. To use the files, copy them to the desktop of the computer and when you are finished copy them back to the device.

12.1.2.12 Removing Encryption from Encrypted Devices

If you wish, you may remove encryption from encrypted devices. This is not recommended unless absolutely necessary, since the data on your device will be lost and the device will no longer be protected.

1. Connect the device. In My Computer, right-click the device and select the Safend Data Protection Suite shell extension.



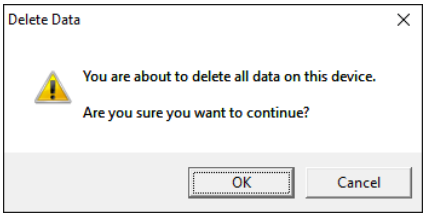
2. Select **Remove Encryption**. The following window opens:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



Important: Removing encryption formats the device, which means all data on the device will be deleted. It is highly recommended that you backup the data before removing encryption.

3. Click **Next**. The following confirmation window opens:



4. Click **OK** to begin removal of encryption. A progress bar appears. When the process ends, the following window appears:



5. Click **Finish** to exit the *Remove Encryption* wizard.

Attention System Administrator: End-users whose effective policy requires encryption of removable storage devices should be made aware of the instructions in *Encryption and*

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Decryption of Removable Storage Devices since their Client may launch a window that require them to encrypt removable storage devices. Users whose effective policy enables decryption and home usage of encrypted storage devices should, in addition, be provided the instructions in *Accessing Encrypted Devices when Offline* so that they can learn how to set an offline access password and decrypt devices.

12.1.2.13 Tracking Offline Use of Encrypted Devices

When authorized end-users use encrypted removable storage devices on non-organizational computers, you may wish to track all the file transfers they perform from/to the device. Safend Data Protection Suite enables you to do this.

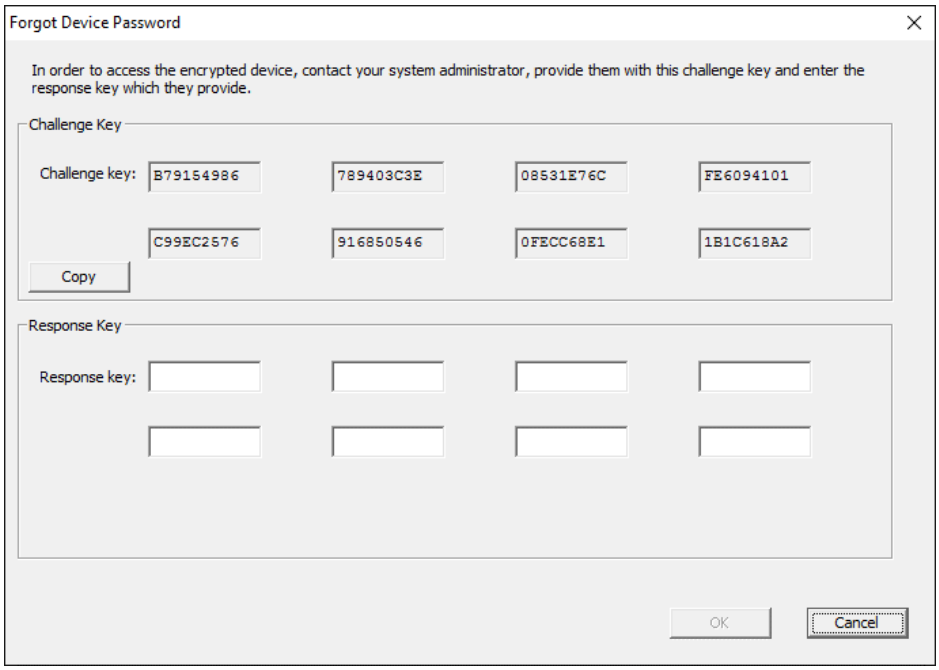
When you activate this option, all offline file transfer information is stored on the encrypted device. Once the encrypted device is reconnected to the organizational network, all the stored logs are sent to the Management Server, and can be viewed in File Logs in the Logs Tab.

12.1.2.14 Granting a Device Access Key Offline

Note: This procedure is only applicable to devices encrypted by the Volume Encryption method. An end user requires Administrator privileges to perform this operation on a computer not running Safend Protector.

The Grant Device Access Key utility allows an end-user who forgot his/her password to access an encrypted removable storage device (e.g., Disk On Key) on a computer not running Safend Data Protection Suite.

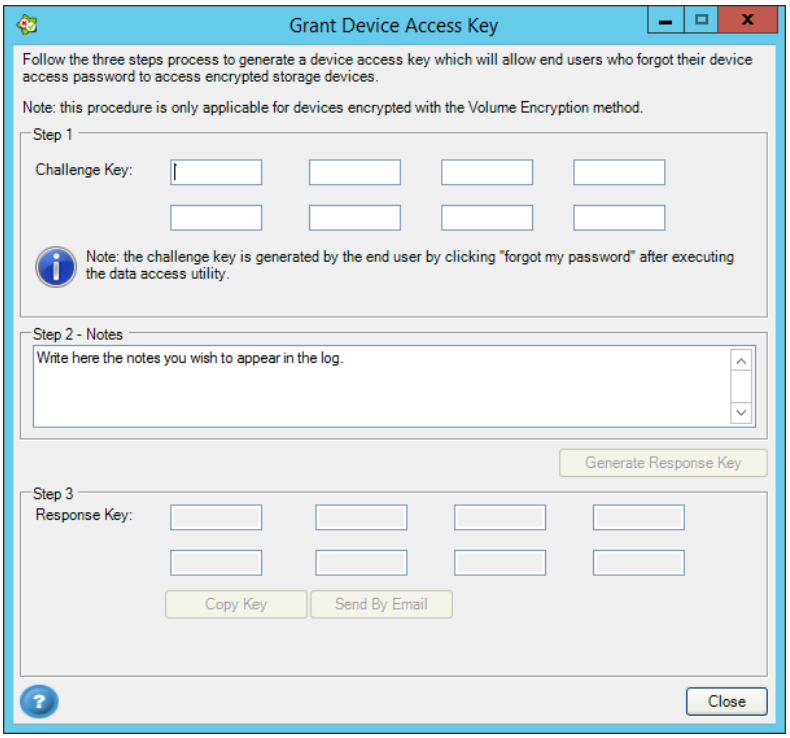
The end user when accessing the data access utility, clicks **Forgot my password**. The Forgot Device Password window is displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

Send the Administrator this Challenge Key (e.g., by email) and then enter the Response Key you are sent in response. Click the OK button. You will now have access to this device.

The administrator accesses this option from the Management Console. Click **Grant Device Access Key** from the Tools menu. The following window is displayed:



Generate a device access key

> **Challenge Key**: These are the numbers the end user provides the administrator (e.g., by email or telephone). For each input box the characters are validated at the end of each characters sequence, if the sequence is correct the ✓ sign is displayed at the right of each input box (and the input character is passed to the next characters box), if the sequence is wrong the ✗ sign is displayed and a note is displayed: "Note: incorrect challenge key was typed, please retype the challenge code."

Notes: This is enabled after the correct challenge key is entered. Type in any note you want to appear in the log. Click the Generate Response Key in order to generate a response.

> **Response key**: These are the numbers the end user enters after receiving them from the Administrator. The same symbols will be displayed, as for the challenge key, for correct or incorrect input of characters. The Copy Key button enables you to copy the response key, for example to Notepad, for later use. The Send by Email button opens a new email message containing the response key.

Click the **Close** button to close the window.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

12.1.2.15 Granting Device Access Within an Organization

When an inside organization password is enabled you will be required to enter a device access password on the protected machines. If you have forgotten the password and you want to reset the device password, do the following:

1. Suspend protection on the protected machine. See Suspending Protection: User.
2. Right click on the device in My Computer and choose **Set Password**. Then follow the wizard instructions. The protection will automatically be resumed after a pre-defined time period.

12.1.2.16 CD/DVD Encryption

Safend Protector's CD/DVD Encryption provides end-users with the ability to encrypt data on CD/DVD media.

An encrypted volume is a container into which files and folders are added when the end user is required to encrypt them. It is created through use of a simple wizard, and once its creation is completed files can be added to it or removed from it (in much the same way as files are added to or removed from a compressed archive). Any file or folder subsequently residing in this volume is encrypted.

Encrypted CD/DVDs are encrypted using organizational keys. This means that the folders and files they contain can be accessed on any organizational computer. It can also be accessed on an unprotected machine using the Access Utility.

Creating an Encrypted CD/DVD

Note: After carrying out encryption on a burned CD/DVD containing a virtual volume, no further data can be added (the CD/DVD is locked). Adding more data to the virtual volume can only be done on a protected machine.

Safend Data Protection Suite automatically launches the Create Encrypted Disc wizard which enables you to create an encrypted volume when you attempt to burn an unencrypted CD/DVD on a protected machine. It is launched in one of the following ways:

When a user who is required by policy to encrypt a CD/DVD media, inserts an empty, writeable medium to a protected machine.

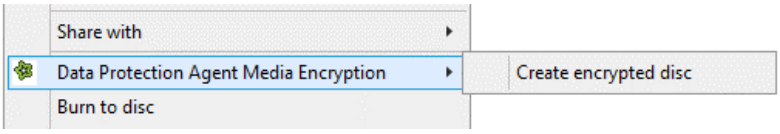
> Click **Encrypt** to display the first page of the Create Encrypted Disc wizard, as described in Creating and using an encrypted CD/DVD.

  Alternately, if you right-click on the burner drive, a menu is displayed. Select **Data Protection Agent** and then **Create encrypted disc** to open the Create Encrypted Disc wizard.

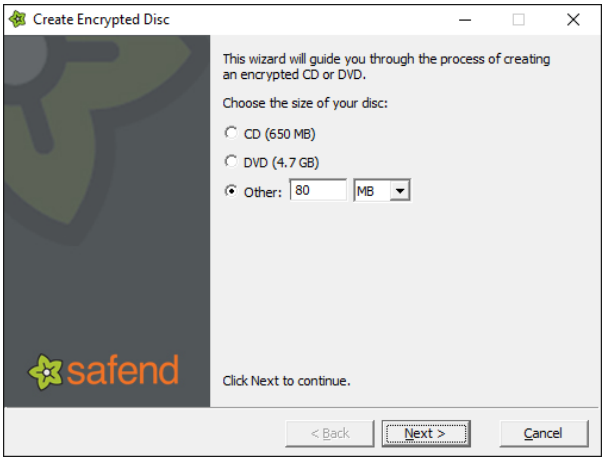
Creating and using an encrypted CD/DVD

1. Right click on a CD/DVD drive. Select **Data Protection Agent** and then select **Create encrypted disc**.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



The following wizard is displayed.



2. Specify the Disc Size. Select one of the standard sizes for a CD or DVD or enter its size in the Other field. Click **Next**.

3. If you have been assigned permission to set a password for accessing storage devices outside the organization, then the following window is displayed.



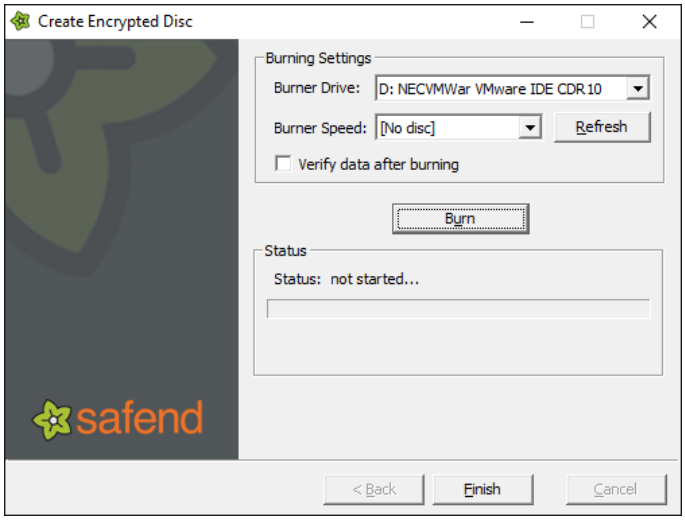
4. Choose a password that will be used on computers outside your organization in order to access its content. You can only set a password before burning the CD/DVD. **Note**: The password that you set must adhere to the organization's password rules.

5. Click **Next**. The following window is displayed:

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com



6. Click **Open Volume** and add files from your computer to the encrypted disc.
7. Click **Next**. The following window is displayed:



8. Choose the Burner Drive and Burner Speed for the CD. Click **Refresh** to change the CD or Burner. Select **Verify data after burning** if you want to check that the data is on the disc.
9. Click **Burn** to start the process. The progress will be displayed in Burning Progress.
10. Click **Finish** to exit the wizard.

12.1.2.17 Offline Access to Encrypted CD/DVDs

Access to an encrypted CD/DVD will differ depending on whether or not you have administrator privileges. See the description at the end of the section, Offline Access to Encrypted Storage Devices, for more details.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

13 Appendix A – Safend Recovery Tool for Encrypted Hard Disk

The Safend Recovery Tool can recover an encrypted hard disk that somehow was damaged and cannot be accessed properly. This tool is intended for rare hard disk failure situations, such as when the operating system has stopped functioning, or when the hard disk has experienced some faults which prevent the OS from functioning normally and there are encrypted files to be recovered.

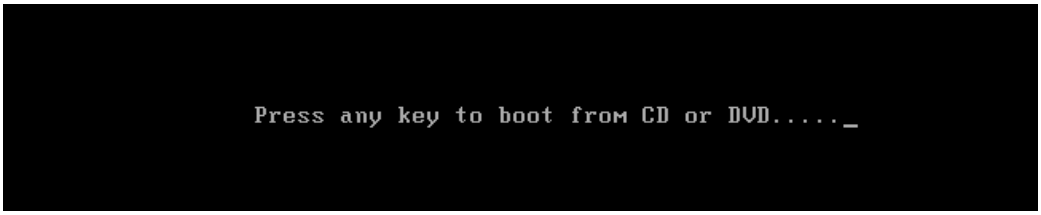
Note: When copying encrypted data for recovery on another endpoint, the entire chain of storage devices used (when there are several devices), must all be NTFS formatted. If any one of the devices are not NTFS formatted the data will not be recoverable.

13.1 Bootable CD Recovery

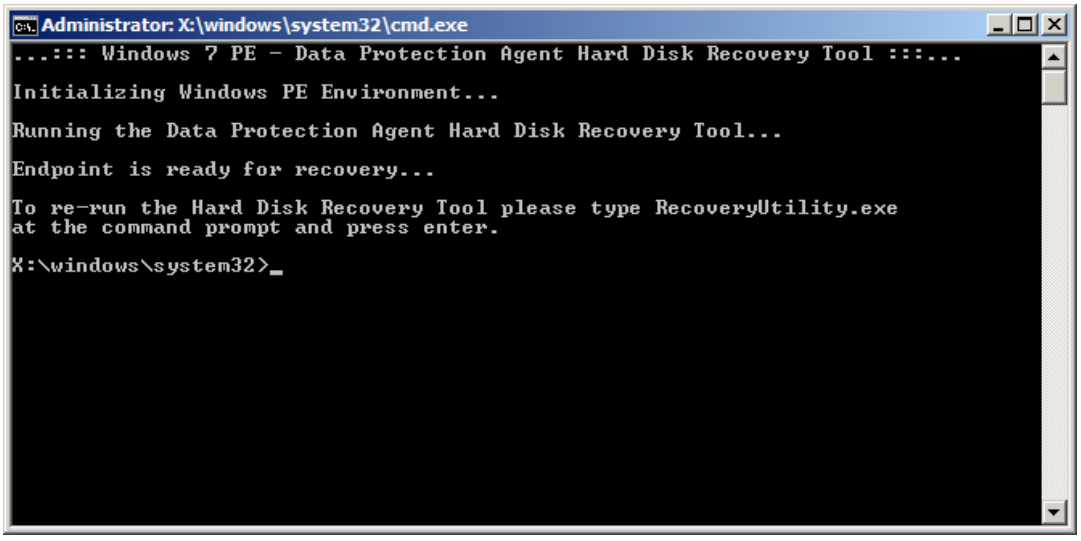
This method comes in the form of a bootable CD running the Windows PE operating system. The bootable CD can be created by burning the ISO file provided by Safend, using any CD burning software.

To access the Safend Recovery Tool supplied on a CD, do the following:

1. Place the CD in the CD drive.
2. Boot from the CD, by pressing any key after getting the following message.



3. The Windows PE operating system will now start loading. The following window will be displayed.



Copyright © 2019 **Safend All Rights Reserved** | www.safend.com

4. In the **Recovery Target** area, specify the target to be recovered. The options are, as follows:

   a) Recover the entire computer: All internal hard disks are searched and all encrypted files are decrypted.

   b) Recover specific files: Only the encrypted files found in the folder that you specify in the Source Folder field are decrypted.

   If you choose this option, you must also specify the Destination Folder into which the decrypted files will be placed.

5. Click the **Analyze** button to initiate a search for the encryption key on the hard disk. The window then indicates that it is **Searching for an encryption key** in the *Status* area at the bottom of the window.

   a) Recovery Key from Management Server: To use this option the user must get a Recovery Key generated from the Management Console. You will send the user a recovery key after the user provides you with the code displayed in the Your Recovery Code field.

   Once the user gets the Recovery code from you, he should enter it in the Recovery Key field.

6. Click the Start **Recovery** button to start the recovery process. A bar at the bottom of the window then indicates the progress of the decryption process and the **Status** area displays messages describing the current state of the process.

Copyright © 2019 **Safend All Rights Reserved** | www.safend.com