

# safend

Securing Your Endpoints



## Safend Protector 3.3

# Reporting – Feature Description

### Overview

Safend Protector 3.3 includes an extensive reporting mechanism, which provides a new level of visibility into the protected organization.

The different reports are designed to accommodate the security and operational needs of the organization and its security and IT personnel. The information is provided in a clear, easy to understand format, that can also benefit non-technical viewers, such as executives within the organization.

### Reports

#### Security Incidents by Users and Organizational Units

This report allows Safend Administrators to see which Organizational Units or specific users and computers are violating the organization security policies, or even committing an extensive amount of “allowed but suspicious” activities. This type of detailed information helps highlight unusual events, and uncover malicious or reckless user behavior.

When generating a report, the administrator is first required to define what user action he considers to be a “security incident”. This can be an unapproved user action that was blocked by Safend Protector or an allowed user action that the administrator still wants to supervise, such as copying Microsoft Office files above a certain size to removable storage devices.

The report will display the following results:

- A graphic chart and detailed table describing the chosen OU’s relative number of security incidents. This enables the administrator to immediately spot “rouge” departments that require further observation, education or an in-depth inspection.
- A users “Watch List” describing the users that have committed the most security incidents whose behavior may require further analysis.

### **Security Incident Types**

This report enables the administrator to see an overview of the most common security incidents in his organization. The inspected security incidents are defined by the administrator to specifically match the security guidelines of the organization.

The information presented in this report highlights problematic procedures and work practices that need to be addressed, or triggers an in-depth investigation into an unusually common incident type. This report can also be used to “preview” a policy before its association with the organizational objects by checking the number of events that would have been blocked if this policy was associated with the chosen OU’s.

### **Policy Distribution**

This report enables administrators to view the entire range of security policies applied to the organization and its overall security policy. It also helps spot endpoints that do not have a valid policy applied on them.

### **Deployment Status**

Using this report, security administrators or IT managers can see the progress of the Safend Protector Client deployment across the enterprise. The report shows the percentage of the organization machines protected by the Safend Client and provides a detailed list of the machines not yet protected.

### **Device Inventory Report**

This report generates a detailed list of all the portable devices that were used within a defined time frame. These devices can be copied to a policy White List in order to simplify the policy creation process.

### **Drill Down Options**

Each report generated also includes drill down capabilities designed to give the user a detailed analysis of specific aspects of the report. Administrators can easily investigate suspicious patterns found in the main report by drilling down from a high level view of the organization to the specific incidents’ details and the relevant log entries.

### **Export Reports**

The reports can either be viewed from within the Management Console using the newly added Report World or be exported to one of several popular formats for viewing and analysis outside of the Console.

### **Schedule Reports**

The reports can be scheduled to run periodically and their results sent by email to predefined recipients. This can help ensure the continuous tracking of the organization’s security status.