

ReSOFT Dashboard Overview

Table of Contents

Introduction	4
The ReSOFT Dashboard has a two-pane structure.	4
ReSOFT Dashboard.....	5
Goals	5
Views	6
Views – A closer look.....	6
Views – Important note.....	7
ReSOFT Dashboard information coverage	8
Left pane	11
View	11
Left pane navigation	11
Right pane	12
Item and events	12
View	13
Actions links.....	13
Machine group	13
Monitored item group	14
Machine	14
Monitored item	15
Profile	15
Security.....	16
Resources	17
Events	17
Maintenance.....	18
Configuring the ReSOFT Dashboard	19
Configurable items.....	19
• <i>Per user</i>	19
• <i>Per view</i>	19
• <i>Per monitored item group</i>	19
• <i>Per monitored item</i>	19
• <i>Per machine group</i>	19
• <i>Per profile item</i>	20
• <i>Per security item</i>	20
• <i>Per resource item</i>	20
• <i>Per event item</i>	20
• <i>Per maintenance item</i>	20
Configuration wizards	20
Status	21
Appendix A – Asset Profile Sample Excerpt.....	22
Appendix B – ReSOFT Dashboard Default Configuration.....	23

Default ReSOFT Dashboard configuration.....	23
Dashboard left pane configuration.....	23
Notes.....	23
Default items.....	23
Event monitoring and update intervals.....	24
Status values.....	24
Event monitoring and update intervals.....	25
Monitored item groups.....	25
• <i>Clients</i>	25
• <i>Services</i>	26
• <i>Profile items</i>	29
Intrusion protection exclusion lists.....	30
• <i>DART (Scrip) 27 (System Start-up Control) exclusion list</i>	31
• <i>DART (Scrip) 232 (Intrusion Protection Control) exclusion list</i>	32
Resource items.....	32
Event items.....	34
Event items and event filters.....	35

Introduction

The ReSOFT Dashboard is the default ReSOFT server interface. It is displayed when you log onto your ReSOFT server at

<https://ReSoftservername/main>

You can still access the individual ReSOFT facilities, events, assets, sites, Microsoft updates, provisioning, information portal, and tools, by clicking on the Use extended interface link found on the right-hand side of the ReSOFT Site and System Dashboard page above the ReSOFT Dashboard:

The screenshot shows the ReSOFT Dashboard interface. At the top left is the HandsFree Networks logo and the text 'ASI Site and System Dashboard'. At the top right, it shows the user 'admin', the date 'September 15, 2009', and a 'How to' link. Below the logo is a 'Use extended interface' link.

The main content area is titled 'Items for machine group "devsite"'. It contains a table with the following data:

Action	Site	Machine	Status	Latest Client Event
[configure] [manage] [connect] [event] [asset] [services]	devsite	tsg-4	alert	Tuesday, September 15, 2009 15:33:01
[configure] [manage] [connect] [event] [asset] [services]	devsite	tsg-1	OK	Tuesday, September 15, 2009 15:25:00
[configure] [manage] [connect] [event] [asset] [services]	devsite	pdg-1	OK	Tuesday, September 15, 2009 12:00:02

Below the table, there is a search and display options panel. The search options include dropdowns for Site (all), Machine (all), Status (all), and Latest Client Event (all). The display options include a dropdown for Page Size (10). There are 'Search' and 'Reset' buttons.

At the bottom left, there is a copyright notice: '© 2000-2008 HandsFree Networks, 159 Kinsley Street, Nashua, NH 03060'. At the bottom right is the HandsFree Networks logo.

The ReSOFT Dashboard has a two-pane structure.

In the left pane, you navigate all system based objects, sites, machine groups, and monitored item groups, via a familiar tree structure expanding and contracting system groupings by clicking on +, and - icons respectively.

Entries in the left pane at all levels are color-coded to reflect their current status, green - normal, yellow - warning, and red - alert.

Note that the ReSOFT Dashboard includes monitored item groups. These are groups of objects such as devices, MS Windows services and applications that you want to monitor. The default ReSOFT

Dashboard configuration includes the Services and Clients monitored item groups. The former includes monitoring of MS Windows services on all systems where the ReSOFT client is installed. The latter includes monitoring of all the ReSOFT clients installed at your sites.

In the right pane, you can

- View a system's asset, security, maintenance, resource, and events-of-interest item groups
- View monitored item status
- Take action on detail entries in a system's security, maintenance, resource, and events-of-interest profiles
- Configure the left pane including which groups should be included, and how they should be grouped together
- Configure a system's status snapshot including its asset, security, maintenance, resource, and events-of-interest profiles
- Configure status display parameters controlling the thresholds that define normal, warning, and alert status
- Define and configure monitored item groups

All right-pane displays have the same structure. The title of a display contains the name of the item you clicked on followed by Search Options, and a Display Options panels. Below the two panels, typically you will find a table containing top-level detail items with actions available for each item in the table.

ReSOFT Dashboard

Goals

- The ReSOFT Dashboard is designed to be easily and quickly tailored to the preferences of individual users, and requiring a minimum effort to configure. For this to be true:
- The ReSOFT Dashboard display should persist: it should be the same after the browser is closed and re-opened.
- The ReSOFT Dashboard display should be per-user: Different ReSOFT server users should be able to have different persistent dashboard displays.
- The ReSOFT Dashboard display should bring together different kinds of data into a uniform framework.
- Within one ReSOFT Dashboard display, a user should be able to define multiple views based on any criteria, showing selections of systems that may be overlapping, i.e. the same systems may be included in multiple views. The ReSOFT Dashboard should lend itself to easily drilling down to help diagnose problems.
- The ReSOFT Dashboard display should update quickly, even at the expense of the data being slightly out of date.
- Please note two ReSOFT architectural characteristics that affect the ReSOFT Dashboard:
- The information displayed on the ReSOFT Dashboard is collected via the ReSOFT client who can only have a single configuration on any given system, i.e. it cannot have multiple configurations matching the user oriented dashboard configurations.

- Systems can be in more than one machine group. This means that, for example, if a system belongs to two or more groups with different configurations we need a way to resolve potential conflicts

Views

One of the key concepts in the ReSOFT Dashboard is that of the *view*. It makes it possible to achieve the goals outlined in the *ReSOFT Dashboard goals of this* document. The best way to explain what we mean by view is by way of an example.

Suppose you offer your customers three service levels:

- Premium
- Standard
- Basic

Each service level is defined in terms of the services provided, and the *level* of each service is specified in terms of parameters such as response time to problems, types of problems covered, and their thresholds.

In this example, the *views* mechanism would let you configure the ReSOFT Dashboard to support the delivery of services to your customers based on the level of service you have contracted to provide them.

Given the three service levels defined above, you would define three views calling them, for example:

- Premium
- Standard
- Basic

To each of the views, you would add the sites, system groups and monitored item groups including the systems covered by the corresponding service levels.

For each view you could assign different threshold values for normal, warning, and alert status for each of the components of a system's status. You could also define different *events-of-interest* profiles, and different monitoring intervals.

Views – A closer look

Users can define and configure the views shown on their ReSOFT Dashboard display. Each view consists of a list of machine groups and a list of monitored item groups. You can expand a view to see what is in it, and can expand items belonging to them to see their content.

Users can define the views they want to see on their ReSOFT Dashboard display. Each user on a ReSOFT server can have a tailored ReSOFT Dashboard display.

Each view in a ReSOFT Dashboard display is configured independently both in terms of the groups of systems included, and other parameters such as status threshold.

Views can be global so that others can use them, or they can be private. Global views can only be edited by their owner (the user that created them).

Views – Important note

DART (Scrip) configurations are applied on a system-by-system basis. With group management DART (Scrip) configurations can be assigned to groups of systems defined according to any criteria. Systems can belong to multiple groups. **However, at any one point in time, for any DART (Scrip) configuration variable only one value can be assigned to one system.**

ReSOFT Dashboard displays are composed of views, and are defined per user. However, information that populates the ReSOFT Dashboard's right pane, and actions performed by clicking on links in the right pane are generated and performed via DART (Scrip) configurations.

DART (Scrip) configurations apply to groups of systems with only one DART (Scrip) configuration assigned to any one system at any point in time regardless of the user. DART (Scrip) configurations are user independent.

This means that the items that are included for display in a machine group are per machine group, not per view or per user. In other words, when multiple users select a machine group for a view, they all see the same information when they expand the entry for the machine group in the left pane, and also when they expand the left-pane entry for a machine within the machine group. Similarly, if a single user selects a machine group in two different views, those two views show the same information when that machine group is expanded. This is because:

- The contents of the machine group are independent of the user, so each user sees the same machines when expanding it, and
- The DART (Scrip) configuration for collecting the data that is presented has to be set up one way on a single machine, so different users can't have different configurations for it.

The best way to illustrate the constraints placed on views because DART (Scrip) configurations are per machine not per view is by way of an example. Suppose you have two machines groups, *web* and *email* with system *webmail* in common.

You configure *web* to have a resource item for network traffic, with a certain threshold (and this configures underlying DART (Scrip) in all systems in that machine group). You configure *email* to have a resource item for disk space with a certain threshold (and this configures the underlying DART (Scrip) in all systems in that machine group).

Suppose you configure one view to contain the machine group *web* and another view to contain the machine group *email*. This means that *webmail*, the machine the two groups have in common, is in both views. However, when you look at the top-level resource items for *webmail* (and any other system), with the status rolled up from the detail resource items, that list of resource items is per-machine, NOT per-view. So, the resource items will be exactly the same in both views. If, for

example, the *network* resource has an alert status, it will still cause both views at the top level to be at alert status.

The underlying assumption is that the main use of views is to aggregate groups of machines based on user defined criteria.

It's also possible to inadvertently configure the same function (DART (Scrip)) on the same system in conflicting ways. For example, suppose you have two monitored item groups that define two different machine groups, A and B, to do the monitoring, with two different schedules.

Suppose also that machine groups A and B have one system, X, in common.

It's easy to resolve the conflict caused by the fact that system X is required to monitor different systems by simply combining the two lists of systems to be monitored in the DART (Scrip) configuration for system X.

However, we cannot as easily resolve the scheduling conflict. We resolve it by selecting the schedule attached to the machine group belonging to the group category with the higher priority. If the two machine groups with conflicting DART (Scrip) configurations, in our example A and B, belong to the same category, we use the DART (Scrip) configuration value from the machine group that was created more recently.

In summary, you can use the wizards to configure data-collection settings on groups of machines. Behind the scenes, the ReSOFT server converts this into DART (Scrip) settings on individual machines, resolving any conflicts. Then, you can use the wizards to set up which groups you would like to see in your view. When you look at your view, you see those groups, and you can expand the left-pane entry for each one to explore the data that has been collected for each machine.

ReSOFT Dashboard information coverage

The ReSOFT Dashboard lets you manage and access information about the systems you have under management in an intuitive and straightforward manner. With the ReSOFT Dashboard you can:

- Access all the information about systems under management via one interface
- Customize which and how much information you view
- Configure the views and the DARTs (Scrips) used to collect information and take action reported on the ReSOFT Dashboard. ReSOFT Dashboard configuration is wizard based making the configuration process more intuitive and straightforward.

System related information covered by the ReSOFT Dashboard is sub-divided into five *Item Categories*:

- Profile
- Security
- Resources
- Events of interest

- Maintenance

In addition to the above system related item categories, there is also the *Monitoring* item category that includes information about ReSOFT client activity monitoring the availability of the ReSOFT client, MS Windows services, devices, and applications.

For each item category, you can configure the ReSOFT Dashboard to display the following information:

System Profile Summary: This is asset information that is collected by the System Survey (DART (Scrip) 61). You can select the hardware and software asset data you want included in the *Profile* item category.

Security: This is security related information included in the *Security* item category. It is extracted from the asset database, and from the information reported by the following DARTs (Scripts):

- Symantec Virus Definition Management (DART (Scrip) 12)
- McAfee Virus Definition Management (DART (Scrip) 90)
- eTrust Virus Definition Management (DART (Scrip) 242)
- Trend Micro Virus Definition Management (DART (Scrip) 247)
- Norton Anti Virus Scan Execution (DART (Scrip) 15)
- McAfee Virus Scan Execution (DART (Scrip) 175)
- eTrust EZ Antivirus Scan Execution (DART (Scrip) 243)
- Trend Micro Anti Virus Scan Execution (DART (Scrip) 249)
- Symantec Anti Virus Definition Dates Log (DART (Scrip) 238)
- McAfee Anti Virus Definition Dates Log (DART (Scrip) 239)
- eTrust EZ Antivirus Definition Dates Log (DART (Scrip) 244)
- Trend Micro Anti Virus Definition Dates Log (DART (Scrip) 250)
- System Start-up Environment Control (DART (Scrip) 27)
- Intrusion Protection Control (DART (Scrip) 232)
- System Start-up Environment Management (DART (Scrip) 233)
- Intrusion Protection Management (DART (Scrip) 240)
- In a later version, we will include event information from:
 - Network Packet Filtering (DART (Scrip) 228)
 - Port Probe Detected (DART (Scrip) 45)
 - Email Attachment Filtering (DART (Scrip) 188)
 - File Download Filtering (DART (Scrip) 189)

Device, service, and application availability: This is information about systems and services that are monitored for uptime and availability. It is used to generate the display for the Monitored item category. The device, service, and application availability information is collected using:

- Network Devices and Services Availability (DART (Scrip) 88). This DART (Scrip) directly pings or opens a connection to an IP resource or service, and reports on the success or failure of that operation.

- ReSOFT client Heartbeat (DART (Scrip) 231). This DART (Scrip) posts an event log on the ReSOFT server at regular intervals, making it possible to directly monitor the availability of the ReSOFT clients and the systems they run on.
- File Distribution and Retrieval (DART (Scrip) 100). This DART (Scrip) is similar to the Network Devices and Services Availability DART (Scrip) (#88) except that it goes further and retrieves a file from the resource, verifying that it is properly serving files. Typically, it is used to monitor the availability of Web based applications.
- Service Restart (DART (Scrip) 176). This DART (Scrip) verifies that MS Windows services are running on a system, and posts an event log if they are not. It can be configured to re-start monitored MS Windows services when they stop.

Resource utilization: This is performance related information about a system. It represents an early-warning system about potential performance related problems. This information is used to generate the display for the *Resource* item category. In future, we will be adding the capability to the ReSOFT client to report any performance information that is available in the NT performance counters, but for now, resource utilization information reported on the ReSOFT Dashboard is collected via the following DARTs (Scripts):

- Memory Statistics (DART (Scrip) 6)
- Logical Disk Statistics (DART (Scrip) 95)
- Processor Statistics (DART (Scrip) 96)
- Physical Disk Statistics (DART (Scrip) 97)
- Network Statistics (DART (Scrip) 98)

Events of interest. This is event information reported by the ReSOFT client. You can think of the *events of interest* display as the notification console for a system. Note that it is completely independent from the event notification console accessible via the extended interface. You can use any event filter to select events of interest on a system-by-system ReSOFT. The *events-of-interest* configuration wizard provides assistance in categorizing the filters.

Maintenance. This is information reported by the maintenance related DARTs (Scripts). The maintenance display is like the events-of-interest display the only difference being the events it covers. Using the corresponding wizard, you can configure the *Maintenance* item category for a system to display events from one or more of the following DARTs (Scripts):

- Scandisk Execution (DART (Scrip) 9)
- Clean Folders (DARTs (Scripts) 60, 217-221)
- Scandisk Files Clean-up (MS Windows 9x and Me) (DART (Scrip) 62)
- Chkdsk Files Clean-up (MS Windows NT4, 2000, XP, and Server 2003) (DART (Scrip) 69)
- Synchronization of System Clock with Time Server (DART (Scrip) 86)
- Difference between System and Time Server Clock Exceeds Configured Threshold Since Last Checked Twelve Hours Ago (DART (Scrip) 87)
- Disk Defragmenter Execution (MS Windows 9x and Me) (DART (Scrip) 19)
- Disk Defragmenter Execution (MS Windows NT4 and 2000) (DART (Scrip) 92)
- Disk Defragmenter Execution (MS Windows XP and Server 2003) (DART (Scrip) 211)

Left pane

Items in left pane of the ReSOFT Dashboard are organized according to the following hierarchy:

View

- Group
 - Machine group
 - Monitored item group
- Item
 - Machine
- Detail category (only for machines)
 - Profile
 - Security
 - Resources
 - Events
 - Maintenance
 - Monitored item

Left pane navigation

Each item in the left pane hierarchy has a + or - next to it, for opening or closing it. When you open it by clicking on the + next to it, the items belonging to it are displayed in a tree structure below it.

Each item in the left pane is color-coded using the rolled-up status for the color selection. This means that an item will have a status equal to the highest status of one of the items belonging to it. For example, if a system group has three systems one with status normal (green), one with status warning (yellow), and one with status alert (red), the group's status will be displayed as alert (red).

Selecting an item in the left pane highlights it, and updates the display in the right pane, which is always a page with *Search Options* and *Display Options* panels listing the details for the selected item.

When nothing in the left pane is expanded, the right pane will just show the color-coded list of views available in the left pane. When a view is expanded by clicking on the + next to it, all the groups (both machine groups and monitored item groups) it contains are shown indented underneath it, and all other views continue to be shown. Similarly, when a group is expanded by clicking on the + next to it, all the items it contains are shown indented underneath it. When you click on the + next to a machine, the following five item categories will always be listed indented under it:

- Profile
- Security
- Resources
- Events
- Maintenance

Monitored items cannot be expanded because only the monitoring function is applied to them.

Right pane

In the right pane of the ReSOFT Dashboard, there are a number of possible different displays corresponding to the item you clicked on in the left pane.

Item and events

As described in the *ReSOFT Dashboard information coverage* section of this document, information managed via the ReSOFT Dashboard is sub-divided into six *item categories*:

System related

- Profile
- Security
- Resources
- Events of interest
- Maintenance
- Monitoring

Each *item category* is composed of *item types*. Each *item type* consists of:

- A DART (Scrip)
- Event filtering,
- Scope (the portion of the DART (Scrip)'s event log the event filtering is applied to), and
- Parameter extraction operation. This is the action performed to extract the information that is compared to the status threshold values, and determines the status of the item type.

When the ReSOFT Dashboard is updated, the ReSOFT Dashboard software processes all enabled item types. It retrieves the event logs for the DARTs (Scrips) in the enabled item types applying each item type's event filter to its scope. Parameter extraction is then performed, and the resulting value is compared to the status thresholds for the item type resulting in the updated status for the item type.

The ReSOFT Dashboard retains the event logs retrieved when it processes an *item type* for a period of time equal to the monitoring interval for that *item type*.

As described in the *Left pane navigation* section of this document, you can access item category information for any system by expanding the left-pane entry for a system (clicking on the + to the left of the system name), and then clicking on the desired *item category* (e.g. Security).

When you do that, the page displayed in the right pane contains a table whose entries are the enabled *item types* for that *item category*.

If you click on the *detail* link for an *item type* entry in a system's *item category* table in the right pane, a page listing all of the event logs retrieved when the ReSOFT Dashboard software processes that *item type* is displayed in a new window.

Please note that the item count for an item type could be higher than the number of event logs reported for that item type. For example, a **single** DART (Scrip) 27 (System Start-up Environment Control) could report the rejection of the attempted addition of **six** start-up items. In this case the item count for the DART (Scrip) 27 item type *change to startup environment was prevented* will be **six** while the event count will be **one**.

View

When you click on the name of a view in the left pane, the display in the right pane contains a title including the name of the view whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the groups (machine groups and monitored item groups) contained in the view. The rows are color-coded corresponding to the status as defined in the configuration of the view. Each entry (row) in the table contains the following columns:

Actions links

- **Configure:** Clicking on this link takes you to the step in the dashboard configuration wizard, where the machine group has been pre-selected.
- **Manage.** Clicking on this link takes you to the Group DART (Scrip) configuration page for the machine group. Note that there is no manage link for monitored item groups as they include systems that may not have the ReSOFT client installed.
- **Name**
- **Type** ("machine" or "monitor")
- **Status**
- **Number of items**
- **Last update.** This is the latest date and time on which information about the machine or monitored item group changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Machine group

When you click on the name of a machine group in the left pane, the display in the right pane contains a title including the name of the machine group whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the systems contained in the machine group. The rows are color-coded corresponding to the status as defined in the configuration of the view the machine group is listed in. Each entry (row) in the table contains the following columns:

- **Actions links**
 - **Configure.** Clicking on this link takes you to the step in the dashboard configuration wizard, where the machine has been pre-selected.
 - **Manage.** Clicking on this link takes you to the DART (Scrip) configuration page for this machine.
 - **Event.** Clicking on this link takes you to the ad-hoc query page selecting recent events for this machine.

- Asset. Clicking on this link takes you to the asset detail page for this machine.
- Site name
- Machine name
- Status
- Latest Client Event. This is the latest date and time on which information about the machine changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Monitored item group

When you click on the name of a monitored item group in the left pane, the display in the right pane contains a title including the name of the monitored item group whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the monitored resources contained in the monitored items group. The rows are color-coded corresponding to the status as defined in the configuration of the view the monitored item group belongs to. Each entry (row) in the table contains the following columns:

- Actions links
 - Configure. Clicking on this link takes you to the step in the dashboard configuration wizard, where the monitored item group has been pre-selected.
- Name
- Location. This is the location of the resource being monitored. This can be a NetBIOS name, IP address, domain name, or URL, depending on how it is used by the client.
- Type. This is the type of monitoring employed to monitor the resource, e.g. Ping, testing for the availability of TCP services, ReSOFT client heartbeat, fetching a file with FTP, or fetching a file with HTTP
- Monitoring machine count
- Status
- Latest Client Event. This is the latest date and time on which monitoring information about the monitored item group changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Machine

When you click on the name of a machine in the left pane, the display in the right pane contains a title including the name of the machine whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the categories of detail information (item categories) for the system whose left-pane entry you clicked on. There are five rows with the categories Profile, Security, Resources, Events, and Maintenance. The rows are color-coded corresponding to the status as defined in the configuration of the view the machine is listed in. Each entry (row) in the table contains the following columns:

- Actions links

- **Configure.** Clicking on this link takes you to the step in the dashboard configuration wizard, for the item (for example, the wizard for a security item), where the machine has been pre-selected.
- **Category**
- **Status**
- **Latest Client Event.** This is the latest date and time on which information about the machine changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Monitored item

When you click on the name of a monitored item in the left pane, the display in the right pane contains a title including the name of the monitored item whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the systems used to monitor the monitored item whose left-pane entry you clicked on.

Please note that a monitored item does not have to be a device where the ReSOFT client is installed. It could be any device with a name and IP address reachable by devices where the ReSOFT client is installed.

The rows in a monitored item table are color-coded corresponding to the status as defined in the configuration of the view the monitored item is listed in. Each entry (row) in the table contains the following columns:

- **Actions links**

Configure. Clicking on this link takes you to the step in the dashboard configuration wizard for monitored items, where the machine used to monitor the selected monitored item has been pre-selected.

Detail Clicking on this link generates a new page listing the monitoring events that provide the monitoring information about the selected monitored item generated by the ReSOFT client on the monitoring system whose detail link you clicked on. On the new page, each event has a detail link that takes you to the event detail page for the event.

- **Site name**
- **Machine name**
- **Status**
- **Latest Client Event.** This is the latest date and time on which the monitoring information about the selected monitored item changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Profile

When you click on the profile entry for a machine in the left pane, the display in the right pane contains a title including the name of the machine whose profile entry you clicked on in the left pane, the usual

Search Options and *Display Options* panels, and a table listing the asset items you selected for the profile of systems belonging to the group you accessed in the left pane

The format of the profile display is as shown in this excerpt of a *sample profile page* in Appendix A.

The profile display has a single "last update" date on it. It is the latest date and time on which asset information about the selected system changed.

Security

When you click on the security entry for a machine in the left pane, the display in the right pane contains a title including the name of the site and of the machine whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the security categories of detail information configured for the system whose left-pane security entry you clicked on. The entries in the table are color-coded corresponding to the status as defined in the configuration of the view the system is listed in. Each entry (row) in the table contains the following columns:

- Actions links
 - Configure. Clicking on this link takes you to the step in the dashboard configuration wizard for security items, where the security item has been pre-selected.
 - Detail. Clicking on this link generates a new page listing the security related events for the selected security item generated by the ReSOFT client on the system whose security link you clicked on. On the new page, each event has a detail link that takes you to the event detail page for the event.
- Name. Name of entry corresponding to an item type in the Security item category
- Status
- Item Count. This is the number of occurrences of the item type whose name is entered in the Name column. Please note that the item count for an item type could be higher than the number of events reported for that item type as reported when you click on the Detail link for the entry. For example, a single DART (Scrip) 27 (System Start-up Environment Control) could report the rejection of the attempted addition of six start-up items. In this case the item count for the DART (Scrip) 27 item type change to startup environment was prevented will be six while the event count will be one.
- Criterion. This is the test applied to the event count reported for the item category type in the entry that results in the status displayed in the Status column. For example, an alert status will result if the number of disabled start-up items additions exceeds 100. For item category entries corresponding to other item types, no test is applied to the number of events reported, e.g. Anti-virus is installed. In these cases, the Criterion column is empty.
- Latest Client Event. This is the latest date and time on which the selected security related item information about the system changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Resources

When you click on the resources entry for a machine in the left pane, the display in the right pane contains a title including the name of the site and of the machine whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the resource items configured for the system whose left-pane resources entry you clicked on. The entries in the table are color-coded corresponding to the status as defined in the configuration of the view the system is listed in. Each entry (row) in the table contains the following columns:

- Actions links
 - Configure. Clicking on this link takes you to the step in the dashboard configuration wizard for resource items, where the resource item has been pre-selected.
 - Detail. Clicking on this link generates a new page listing the resource monitoring related events for the selected resource item generated by the ReSOFT client on the system whose resource link you clicked on. On the new page, each event has a detail link that takes you to the event detail page for the event.
- Name. Name of entry corresponding to an item type in the Resource item category
- Status
- Item Count. This is the number of occurrences of the item type whose name is entered in the Name column. Please note that the item count for an item type could be higher than the number of events reported for that item type as reported when you click on the Detail link for the entry. For example, a single DART (Scrip) 27 (System Start-up Environment Control) could report the rejection of the attempted addition of six start-up items. In this case the item count for the DART (Scrip) 27 item type change to startup environment was prevented will be six while the event count will be one.
- Criterion. This is the test applied to the event count reported for the item category type in the entry that results in the status displayed in the Status column. For example, an alert status will result if the number of disabled start-up items additions exceeds 100. For item category entries corresponding to other item types, no test is applied to the number of events reported, e.g. Anti-virus is installed. In these cases, the Criterion column is empty.
- Latest Client Event. This is the latest date and time on which the selected resource item information about the system changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Events

- When you click on the events entry for a machine in the left pane, the display in the right pane contains a title including the name of the site and of the machine whose entry you clicked on in the left pane, the usual *Search Options* and *Display Options* panels, and a table listing the event items that are selected by the events configuration (event filters) for the system whose left-pane events entry you clicked on. The entries in the table are color-coded corresponding to the status as defined in the configuration of the view the system is listed in. Each entry (row) in the table contains all the event database fields reported in the Event Query Results page together with the following additional columns:
 - Actions links

- Configure. Clicking on this link takes you to the step in the dashboard configuration wizard for event items, where the event item has been pre-selected.
- Detail. Clicking on this link generates a new page listing the events for the selected event item generated by the ReSOFT client on the system whose events link you clicked on. On the new page, each event has a detail link that takes you to the event detail page for the event.
- Name. Name of entry corresponding to an event of interest
- Status
- Item Count. This is the number of occurrences of the item type whose name is entered in the Name column. Please note that the item count for an item type could be higher than the number of events reported for that item type as reported when you click on the Detail link for the entry. For example, a single DART (Scrip) 27 (System Start-up Environment Control) could report the rejection of the attempted addition of six start-up items. In this case the item count for the DART (Scrip) 27 item type change to startup environment was prevented will be six while the event count will be one.
- Criterion. This is the test applied to the event count reported for the item category type in the entry that results in the status displayed in the Status column. For example, an alert status will result if the number of disabled start-up items additions exceeds 100. For item category entries corresponding to other item types, no test is applied to the number of events reported, e.g. Anti-virus is installed. In these cases, the Criterion column is empty.
- Latest Client Event. This is the latest date and time on which the selected event item information about the system changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Maintenance

- When you click on the maintenance entry for a machine in the left pane, the display in the right pane contains a title including the name of the site and of the machine whose entry you clicked on in the left pane, the usual Search Options and Display Options panels, and a table listing the maintenance items configured for the system whose left-pane maintenance entry you clicked on. The entries in the table are color-coded corresponding to the status as defined in the configuration of the view the system is listed in. Each entry (row) in the table contains all the event database fields reported in the Event Query Results page together with the following additional columns:
 - Actions links
 - Configure. Clicking on this link takes you to the step in the dashboard configuration wizard for maintenance items, where the maintenance item has been pre-selected.
 - Detail. Clicking on this link generates a new page listing the events for the selected maintenance item generated by the ReSOFT client on the system whose maintenance link you clicked on. On the new page, each event has a detail link that takes you to the event detail page for the event.
 - Name. Name of entry corresponding to an item type in the Maintenance item category
 - Status
 - Item Count. This is the number of occurrences of the item type whose name is entered in the Name column. Please note that the item count for an item type could be higher than

the number of events reported for that item type as reported when you click on the Detail link for the entry. For example, a single DART (Scrip) 27 (System Start-up Environment Control) could report the rejection of the attempted addition of six start-up items. In this case the item count for the DART (Scrip) 27 item type change to startup environment was prevented will be six while the event count will be one.

- Criterion. This is the test applied to the event count reported for the item category type in the entry that results in the status displayed in the Status column. For example, an alert status will result if the number of disabled start-up items additions exceeds 100. For item category entries corresponding to other item types, no test is applied to the number of events reported, e.g. Anti-virus is installed. In these cases, the Criterion column is empty.
- Latest Client Event. This is the latest date and time on which the selected maintenance item information about the system changed. There are two last update entries one reporting when the last update was recorded on the ReSOFT client and one when it was posted on the ReSOFT server.

Configuring the ReSOFT Dashboard

The ReSOFT Dashboard has a default configuration that lets you manage most ReSOFT functions, without needing to spend any time configuring the dashboard.

Please refer to *Appendix B* for a detailed description of the ReSOFT Dashboard default configuration.

Configurable items

Below, you will find lists of all configurable ReSOFT Dashboard items, and the level at which each item is configured.

- **Per user**
 - Which view is currently being shown.
 - Color for each status value.
 - Name for each status value.
 - Page refresh interval.
 - Implicitly, the search options and display options for each selection table.
- **Per view**
 - Which machine groups are included.
 - Which monitored item groups are included.
 - Monitoring interval.
- **Per monitored item group**
 - Which monitored items are included.
- **Per monitored item**
 - Type of monitored item.
 - Type-dependent parameters for monitoring.
 - Criteria for computing status value.
- **Per machine group**
 - List of profile items to include in system profile summary detail.
 - List of security items to include in system security summary detail.

- List of resource items to include in resource utilization detail.
- List of event items to include in events of interest detail.
- List of maintenance items to include in maintenance detail.
- **Per profile item**
 - Name of profile item in asset data
 - Criteria for computing status value.
- **Per security item**
 - Type of security item.
 - Type-dependent parameters for item.
 - Criteria for computing status value.
- **Per resource item**
 - Type of resource item.
 - Type-dependent parameters for resource.
 - Criteria for computing status value.
- **Per event item**
 - List of event filters for item.
 - Schedule for checking events.
 - Criteria for computing status value.
- **Per maintenance item**
 - List of event filters for item.
 - Schedule for checking events.
 - Criteria for computing status value.

Configuration wizards

Like all facilities on the ReSOFT server, the ReSOFT Dashboard performs its information delivery and action taking functions via DARTs (Scrips). When you take an action on the ReSOFT Dashboard ultimately DART (Scrip) runs on the system(s) you took the action on.

At the lowest level, ReSOFT Dashboard configuration then consists of configuring DARTs (Scrips). In order to make this process easier, and more intuitive, we have implemented ReSOFT Dashboard configuration wizard's configuration wizards minimizing the need to access directly DART (Scrip) configuration pages.

ReSOFT Dashboard configuration wizards can be accessed from several locations on the ReSOFT server, and can have different options.

For example, if you start a configuration wizard from the top level navigation bar (clicking on the *wizard* link in the *dashboard* navigation bar at the top right-hand corner of any page on the ReSOFT server when you access the extended interface), the first step consists of selecting an ReSOFT Dashboard view, then a machine group, or monitored item groups in that view, then the per-machine configuration for the machines in the selected group, or the per-monitored-item configuration for the monitored items in the selected monitored item group, and so on, step by step until you complete the configuration operation with a series of point-and-click actions.

Status

The status display is a very important part of the ReSOFT Dashboard. The status of each individual item in the dashboard is determined by user-configured thresholds and conditions. These status values are rolled up to the higher-levels in the dashboard hierarchy to indicate whether or not any alert conditions exist at a lower level. The status display allows users to quickly pinpoint and drill down to any alert conditions.

In order to implement the status function efficiently, we use an integer value for status, and we use larger numbers to indicate increasing alert levels. We associate colors with different status levels. The default setup for the status levels is:

Value	Name
1	OK
2	warning
3	alert
4	Changed

Appendix A – Asset Profile Sample Excerpt

System Summary

Identification

System Manufacturer	To be Filled
System Product	To be Filled
System Version	To be Filled
System Serial Number	000000
Registered System Model	To be Filled
System UUID	Not Settable
System Wake-up Type	Modem Ring
BIOS Date	07/15/95
BIOS Version	063100
BIOS Address	0xF0000
BIOS ROM Size In kB	256

BIOS Characteristics:

Characteristics

ISA is supported
 PCI is supported
 APM is supported
 BIOS is upgradeable
 BIOS shadowing is allowed
 ESCD support is available
 Boot from CD is supported
 Selectable boot is supported
 EDD is supported
 5.25"/360 KB floppy services are supported (int 13h)
 5.25"/1.2 MB floppy services are supported (int 13h)
 3.5"/720 KB floppy services are supported (int 13h)
 3.5"/2.88 MB floppy services are supported (int 13h)
 Print screen service is supported (int 5h)

8042 keyboard services are supported (int 9h)
 Serial services are supported (int 14h)
 Printer services are supported (int 17h)
 CGA/mono video services are supported (int 10h)

Operating System Information

Operating System	Microsoft Windows 98
OS Version Number	4.10.2222

Base Board Information

Base Board Manufacturer	Supermicro Inc.
Base Board Product	Intel 440BX
Base Board Version	Rev 1.0
Serial Number	00000000

Chassis Information

Chassis Manufacturer	To be Filled
Chassis Type	Desktop
Chassis Lock	Not Present
Chassis Version	To be Filled
Chassis Serial Number	To be Filled
Chassis Asset Tag	00000000
Chassis Boot-up State	Unknown
Chassis Power Supply State	Unknown
Chassis Thermal State	Unknown
Chassis Security Status	Unknown

Appendix B – ReSOFT Dashboard Default Configuration

Default ReSOFT Dashboard configuration

It is important for the ReSOFT Dashboard to have a comprehensive set of items enabled by default with robust default values. In this way, most users will be able to use the dashboard “as is” without making any changes until they have become more familiar with the dashboard, and have a better idea of how their specific requirements can be met by the dashboard.

Please note that the complete set of ReSOFT Dashboard items is much larger than the set of the default items. Every item category (e.g. Maintenance) has sample global items that can be copied and edited. However, most items belonging to each item category are disabled. You can access all items for an item category via configuration wizards.

This document describes the list of global enabled ReSOFT Dashboard items. Note that the owner of these items is the master user for the server.

Dashboard left pane configuration

The ReSOFT Dashboard features two default views:

- Sites: all sites and machines
- Groups: all user-defined groups

Notes

Default items

The complete set of ReSOFT Dashboard default items is much larger than the set of the enabled default items. Every item category (e.g. Maintenance) has a comprehensive set of default items that can be copied and edited. However, most of the default items belonging to each item category are disabled. You can access all default items for an item category via configuration wizards.

All default ReSOFT Dashboard items are global, i.e. can be accessed by all users. However, default items cannot be changed by any users except for HandsFree Networks. Users can use default items as templates for new items. When users perform a configure action on a default item, the ReSOFT Dashboard software automatically creates a copy of the selected item. The user can then change the item (including its name) in any way he/she chooses. Users with global rights can make the copy of the default item they have created to be either local (accessible only by them), or global (accessible by all users).

Users can also define brand-new items, global or local, depending on their rights.

When users perform a configuration action on user-defined global ReSOFT Dashboard items, the ReSOFT Dashboard software automatically creates a copy of the selected global item. The user





can then change the item (including its name) in any way he/she chooses. Users with global rights can make the copy of the default item they have created to be either local (accessible only by them), or global (accessible by all users).

Event monitoring and update intervals

At the start of dashboard operation, call it time 0, event monitoring for all items will start at time 0 – the length of the event monitoring interval. Clicking on the *Reset* button for a view/item has the effect of re-starting the event monitoring interval from the time when the user clicked on the *Reset* button. The length of the first event monitoring interval after a user clicks on the *Reset* button is equal to the amount of time left in the monitoring interval when the user clicked on the *Reset* button.

Status values

We have adopted the *homeland security* colors as the ReSOFT Dashboard default status color values (we took them from the colors used by the Department of Homeland Security for the Threat Advisory System).

Value	Name	Color	Red	Green	Blue
1	Ok		0	153	102
2	warning		247	214	0
3	Alert		240	57	66
4	Changed		255	156	41

Please note that **changed** status is display-only. When, between update cycles, the status level of an item becomes higher (e.g. from **OK** to **warning**), that item's entry, the entry for the system it refers to, for the site the system belongs to, and all the groups the site belongs to are displayed in the changed color displayed in the table above.

In the tables contained in the following sections:

The column labeled *Name* contains the name of items in each item category that are enabled by default.

The column labeled Criteria contains the number of events corresponding to the item in the Name column that will cause item status to be at **warning** or **alert** level. For example, for the item Client not reporting, **one** Client not reporting event in **four hours** (i.e. an ReSOFT client not reporting to the ReSOFT server for a period of at least four hours) will cause status to be **warning**, **one** Client not reporting event in **22 hours** (i.e. an ReSOFT client note reporting to the ReSOFT server for a period of at least 17 hours) will cause status to be **Alert**.

The column labeled *Inclusion/Exclusion* contains the values for the item in the *Name* column that are either included or excluded when searching for item events. For example, when searching for *Backup Exec service stopped events*, the key words in the *Inclusion/Exclusion* column for the *Backup Exec service stopped* item will be included in the query (i.e. only events including one or more of the key words in the *Inclusion/Exclusion* column will be retrieved).

- The column labeled Monitoring Interval contains the default value of the monitoring interval for each item in the default ReSOFT Dashboard configuration

Event monitoring and update intervals

The events underlying ReSOFT Dashboard items, i.e. the events delivering the information for each item, have an update and a monitoring interval.

The event monitoring interval is the amount of time over which an item's event logs are retained, and its status is calculated.

The event update interval is the amount of time between executions of the event queries that retrieve an item's event log. Currently, there is one event update interval for all items. By default it is set to one hour.

The event monitoring interval is a rolling interval. When event data collected when the event queries for an item run at the end of the latest event update interval are added to item event log store, the event logs collected by the oldest event update interval are deleted from the item event store.

Every time item event logs are added to an item event store, the item's status is re-calculated.

Default values

- Event monitoring interval – two days
- Event update interval – one hour

Please note that, as you will see below, the monitoring interval for a number of items differs from the default.

Monitored item groups

- **Clients**

The *Clients* monitored item group includes all systems. Its item type is handled specially. The time of the latest event and time of the last configuration synchronization are computed for each system, and the latest of those two is retained. It is used to compute a parameter representing the number of seconds since the last time the machine contacted the ReSOFT server. This number is compared with the default warning and alert thresholds for "Client not reporting" reported in the table below.

Name	Criteria	Inclusion / Exclusion	Monitoring Interval
Client not reporting	Warning – at least 1 value 4 hours or more Alert – at least 1 value 22 hours or more		22 hours

- **Services**

The *Services* monitored item group consists of all MS Windows services included in the default *Services to be monitored Services Restart DART* (Scrip) (#176) configuration parameter. Event filters consisting of "Monitored service has stopped:" followed by one of the services referenced by the item definition (see below) are used to retrieve events for monitored items in the *Services* monitored item group.

Name	Criteria	Inclusion/Exclusion	Monitoring Interval
APC PowerChute service stopped	Warning – 1-2 items Alert – 3 or more items	Include "PowerChuteNetShut", "APCPBEAgent", "APCPBEServer", "UPS"	Two days
APC PowerChute service stopped	Warning – 1-2 items Alert – 3 or more items	Include "CASDBEngine", "CASDiscoverySvc", "CASJobEngine", "CASMsgEngine", "CASSvcControlSvr", "CASTapeEngine", "CASUnivDomainSvr", "CATIRPC", "DbaRpcService", "OpenFileAgent", "RemoteDbagent"	Two days
Backup Exec service stopped	Warning – 1-2 items Alert – 3 or more items	Include "BackupExecRPCService", "BackupExecAgentAccelerator", "BackupExecJobEngine", "BackupExecDLO", "DLOAdminSvcu", "BackupExecDeviceMediaService", "BackupExecAgentBrowser", "BackupExecNamingService", "BackupExecNotificationServer", "BackupExecAlertServer"	Two days
Blackberry service stopped	Warning – 1-2 items Alert – 3 or more items	Include "BlackBerry Router", "BlackBerry Controller", "BlackBerry Synchronization Service", "BlackBerry Policy Service", "BlackBerry Attachment Service", "BlackBerry Database Consistency Service", "BlackBerry Mobile Data Server BES-SERVER1", "BlackBerry Server BES-SERVER1", "BESAlert"	Two days

Brightmail service stopped	Warning – 1-2 items Alert – 3 or more items	Include "Brightmail Agent", "Brightmail Conduit", "Brightmail Server", "Brightmail SMTP Harvester", "Brightmail Virus Cleaner"	Two days
Citrix service stopped	Warning – 1-2 items Alert – 3 or more items	Include "CdfSvc", "Cdm", "CdmService", "Citrix SMA Service", "CitrixLicensing", "Citrix_GTLicensingPro", "cpsvc", "CtxAltStr", "CtxHttp", "CTXLMC", "ctxidmn", "CtxSbx", "ctxsmcdrv", "IMAService", "MFCOM"	Two days
DHCP service stopped	Warning – 1-2 items Alert – 3 or more items	Include "DHCPServer"	Two days
DNS service stopped	Warning – 1-2 items Alert – 3 or more items	Include "DNS"	Two days
ETrust service stopped	Warning – 1-2 items Alert – 3 or more items	Include "InoNmSrv", "InoTask", "InoRT", "InoRPC", "INO_FLTR"	Two days
Executive SW Undelete service stopped	Warning – 1-2 items Alert – 3 or more items	Include "UndeleteService"	Two days
File Replication Service stopped	Warning – 1-2 items Alert – 3 or more items	Include "NtFrs"	Two days
IIS service stopped	Warning – 1-2 items Alert – 3 or more items	Include "IISADMIN", "LicenseService"	Two days
Include service stopped	Warning – 1-2 items Alert – 3 or more items	Include "Include DC Services & Mail services"	Two days
Intel service stopped	Warning – 1-2 items Alert – 3 or more items	Include "Intel File Transfer", "Intel PDS"	Two days
Intersite Messaging service stopped	Warning – 1-2 items Alert – 3 or more items	Include "IsmServ"	Two days

ISA server service stopped	Warning – 1-2 items Alert – 3 or more items	Include "isactrl", "MspFltEx", "MspNAT"	Two days
Kerberos Key Distribution Center service stopped	Warning – 1-2 items Alert – 3 or more items	Include "kdc"	Two days
McAfee services service stopped	Warning – 1-2 items Alert – 3 or more items	Include "AVExch32Service", "AVUPDService", "McAfee GroupShield", "McAfeeFramework", "McShield", "McTaskManager", "Network Associates Log Service", "Outbreak Manager"	Two days
Microsoft Search service stopped	Warning – 1-2 items Alert – 3 or more items	Include "MSSEARCH"	Two days
MS Exchange service stopped	Warning – 1-2 items Alert – 3 or more items	Include "MSExchangeIS", "MSExchangeSA", "MSExchangeMTA", "RESvc", "MSExchangeMGMT", "MSExchangeDS", "MSExchangeMT", "MSExchangeES", "IMAP4Svc", "POP3Svc", "MSExchangeSRS"	Two days
MS message queueing service stopped	Warning – 1-2 items Alert – 3 or more items	Include "MSMQ"	Two days
MS SQL Server service stopped	Warning – 1-2 items Alert – 3 or more items	Include "SQLSERVERAGENT", "MSSQLSERVER", "MSSQL\$BKUPEXEC", "MSSQLServerADHelper", "MSDTC", "MSSQL\$MWP", "MSSQL\$SHAREPOINT", "MSSQL\$SBSMONITORING", "SQLAgent\$SBSMONITORING", "MSSQL\$VAULT_LOGIX", "MSSQLServerOLAPService"	Two days
Print Spooler service stopped	Warning – 1-2 items Alert – 3 or more items	Include "Spooler"	Two days

RPC service stopped	Warning – 1-2 items Alert – 3 or more items	Include "RpcSs", "RpcLocator"	Two days
SBS service stopped	Warning – 1-2 items Alert – 3 or more items	Include "SBCore", "MSPOP3Connector"	Two days
SMTP service stopped	Warning – 1-2 items Alert – 3 or more items	Include "SMTPSVC"	Two days
Symantec service stopped	Warning – 1-2 items Alert – 3 or more items	Include "SAVSMTP", "Norton AntiVirus Server", "DefWatch", "NSCTOP", "SAVFMSE", "ccEvtMgr", "ccSetMgr", "SMSMSE", "Symantec AntiVirus", "SavRoam", "NAVAPEL", "SAVRTPEL", "SMSSMTP"	Two days
Terminal Services service stopped	Warning – 1-2 items Alert – 3 or more items	Include "TermService", "Tssdis", "TermServLicensing", "TermDD"	Two days
Trend Micro service stopped	Warning – 1-2 items Alert – 3 or more items	Include "ntrtscan", "ofcservice", "TmFilter", "tmlisten", "TmPreFilter", "VSApiNt"	Two days

- **Profile items**

The default asset profile displayed for each system in the ReSOFT Dashboard contains the following asset items:

- System Product
- Operating System
- NT Installed Service Pack
- NT Product Type
- Processor Family
- Processor Current Speed in MHz
- Processor CurSpeed in Megahertz
- Site Name
- User Name
- Physical Memory Total (Kbytes)
- IP address
- Logical Disk Name
- Logical Disk KBytes total
- Logical Disk KBytes used
- Logical Disk Percentage free
- ReSOFT UUID

Name	Criteria	Inclusion/Exclusion	Monitoring Interval
Intrusion protection startup item rejected	Warning – 50 or more items Alert -- 100 or more items	DART (Scrip) 27 exclusion list (see below)	Two days
Intrusion protection config item rejected	Warning – 50 or more items Alert -- 100 or more items	DART (Scrip) 232 exclusion list (see below)	Two days
Anti-virus is not installed	Alert – 0 items OK – >0 items		Two days
Anti-virus definition update failed to run	always OK		Two days
Anti-virus definition update ran but failed	always OK		Two days
Anti-virus definition update succeeded	always OK		Two days
Anti-virus scan failed to run	always OK		Two days
Anti-virus scan ran but failed	always OK		Two days
Anti-virus scan succeeded	always OK		Two days
Anti-virus definitions are out of date with others on the site	Warning – 7 days or more Alert – 14 days or more		Two days
Anti-virus definitions are out of date	Warning – 7 days or more Alert – 14 days or more		Two days
Intrusion management item enabled/disabled	Warning – 7 days or more Alert – 10 days or more		Two days

Intrusion protection exclusion lists

The goal of the intrusion protection items used to report rejection/disabling of attempts to add items to a system's areas protected by DARTs (Scripts) 27 (System Start-up Control) and 232 (Intrusion Protection Control) is to alert users about potential malware infiltration attempts.

The exclusion lists you will find below, include all key words used to exclude DART (Scrip) 27 and 232 rejection/disabling of items that are legitimate, and DART (Scrip) 27 and 232 actions not related to specific malware rejection/disabling. Please note that rejection/disabling of legitimate

items can be minimized by including such items in the Permitted items configuration parameter in DARTs (Scripts) 27 and 232.

- **DART (Scrip) 27 (System Start-up Control) exclusion list**

- | | | | |
|--|----------------------------|-----------------------------|---------------------------|
| - Failed to obtain the startup folder | - norton antivirus server | - easyshare.exe | - naveng |
| - Failed to obtain the system startup folder | - savrtpel | - kodak software update.exe | - ituneshelper.exe |
| - alist | - ctfmon | - aol.exe | - aolhostmanager |
| - corrupt | - mobsync | - aom.lnk | - aolacsd.exe |
| - Bad reg string value | - rpcpatch | - navex15 | - aolond~1.exe |
| - Could not find item | - dcomlaunch | - savrt | - versioncuetray.exe |
| - operation | - wscsvc | - AdobeUpdate Manager.exe | - adobe gammaloader.exe |
| - Background Intelligent Transfer Service | - ibmmessages.exe | - SAVScan.exe | - qctray.exe |
| - because it was initiated by this application | - hotsync manager | - egathdrv | - qcwlicon.exe |
| - NVSvc | - desktop.ini | - GoogleDCClient | - diskeeper |
| - WmdmPmSp | - office startup | - Connected TaskBar Icon | - spybotsnd |
| - Wmdm PmSp | - millennium agent | - ntdd.sys | - qconsvc |
| - uploadmgr | - powerreg scheduler | - msiexec.exe | - cvpnd |
| - spupdsvc | - Webshots | - cleanup | - dxdllreg.exe |
| - error occurred attempting to reject the change | - reminder-ScanSoft | - userfaultcheck | - umwdf |
| - security center | - powerword | - ikernel.exe | - wdfmgr.exe |
| - afd networking | - adcscm | - basfnd | - mm_tray.exe |
| - dcom server | - cold fusion | - wanmpsvc | - messagecenter.exe |
| - svchost.exe | - protected storage | - atwpkt2 | - navap |
| - ibm access | - Microsoft Office.lnk | - smtray.exe | - defwatch |
| - kernelfaultcheck | - symtdi.sys | - kernelfaultcheck | - symevent.sys |
| - indexing service | - tcpip.sys | - avsynmgr | - rtvscan.exe |
| - navapel | - netbt | - sndsrvc.exe | - idriver.exe |
| | - lmhosts | - naveng.sys | - eraserutildrv |
| | - policyagent | - mcupdmgr.exe | - mssql\$arrayassist |
| | - adobedownloadmanager.exe | - mcappins.exe | - symantec eraser control |
| | - acrotray.exe | - adobelmsvc | - idrivert.exe |
| | - cisco systems vpn client | - googledesktopsearch | - realonemessagecenter |
| | - atiptaxx | - aol fast start | - messagecenter.exe |
| | - directcd.exe | - aol acs | - yahooessenger.exe |
| | - ccapp.exe | - quicken | - msnappau.exe |
| | - Ad-Watch.exe | - symantec antivirus | - aim.exe |
| | - ati2evxx.exe | - ccsetmgr | - ypager.exe |
| | | - ccevtmgr | - msnmsgr.exe |
| | | - savroam | - msmsgs.exe |

- | | | | |
|-----------------------|-------------------------------------|-----------------------------|----------------------------|
| - aolond~1.exe | - usb mass storage driver | - ADUserMon.exe | - adobeupdater.exe |
| - yahoomessenger.exe | - system restore filter driver | - apdproxy.exe | - onetouch.exe |
| - realsched.exe | - adobeupdate manager | - WCESCOMM.EXE | - ucstartup.exe |
| - ituneshelper | - clpciid | - googletalk.exe | - sgtray.exe |
| - quicktime task | - Microsoft NetMeeting | - permitted items | - IBM fingerprint software |
| - tkbellexe | - IMEKRMIG.EXE | - internat.exe | - tfswctrl.exe |
| - digstream | - change was accepted automatically | - spuninst.exe | - hkcmd.exe |
| - ituneshelper.exe | - CreateCD.exe | - netfxupdate.exe | - igfxtray.exe |
| - mm_tray.exe | - SpySweeper.exe | - quicktimeupdatehelper.exe | - PWRMGRTR.DLL |
| - msgcenter.exe | | - quicktimeinstaller.exe | - SynTPEnh.exe |
| - realonemessagcenter | | | - SynTPLpr.exe |
| - msgcenter.exe | | | - EarthLink TotalAccess |
| - disk driver | | | - WMPNSCFG |

- **DART (Scrip) 232 (Intrusion Protection Control) exclusion list**

- | | | | |
|--|---------------------------|----------------------------|--|
| - because it was initiated by this application | - DragDrop Handlers | - search page | 00123456789 |
| - Yahoo! | - ContextMenu Handlers | - screen saver | 0 |
| - Google toolbar | - NavLogon -> LoginDomain | - SCRNSAVE.EXE | - 08B0E5C0-4FCB-11CF-AAA5-00401C60850 |
| - MSN apps | - Notify -> igfxcui | - searchassistant | 1 |
| - webshots | - notify -> LoginDomain | - CustomizeSearch | - 2EAF5BB1-070F-11D3-9307-00C04FAE2D4F |
| - Windows Media Player | - notify -> NavLogon | - ContextMenu Handlers | - Toolbar Extension for Executable |
| - msn toolbar | - AcroIEHlprObj Class | - 5CA3D70E-1895-11CF-8E15- | |
| - shdocvw.dll | - wgalogon | | |
| - PropertySheetHandlers | - start page | | |

Resource items

In the right pane display for resource items, Values in the "Item Count" column are equal to the number of events that meet or exceed the threshold set by the criterion of each item listed in the table below.

For example, consider the "CPU utilization" resource monitoring item. Its default configuration settings are:

Warning - 20 event logs per hour reporting 75% or higher CPU utilization

Alert - 30 event logs per hour reporting 90% or higher CPU utilization

Monitoring interval - one hour

CPU utilization is at warning level if during the current monitoring interval at least 20 (20 x 1)

1. Processor statistics event logs are produced.

CPU utilization is at alert level if during the current monitoring interval at least 30 (30 x 1) processor statistics event logs are produced.

Suppose the status for the "CPU utilization" item for a system is warning (yellow). When you review the CPU utilization item entry for that system in the right pane, you see that the CPU utilization warning (yellow) item count is 25 (25 > 20), the alert item count is 20 (20 < 30), and the OK (green) item count is 75. This means that during the past hour there have been 25 event logs reporting CPU utilization at 75% or higher but lower than 90%. 20 event logs reported CPU utilization 90% or greater, and 75 CPU resources event logs reported CPU utilization lower than 75% and were triggered by another CPU resource monitoring threshold (e.g. processor queue length. The status of the item is determined by the highest status threshold which has been exceeded. In this example, the CPU utilization status of the system is at warning level (yellow) because that's the CPU utilization status threshold which has been exceeded.

Name	Criteria	Monitoring Interval
CPU utilization	Warning - at least 20 values 75% or more Alert - at least 30 values 90% or more	One hour
CPU interrupt rate	Warning - at least 20 values 3000 or more Alert - at least 30 values 5000 or more	One hour
CPU queue length	Warning - at least 20 values 10 or more Alert - at least 30 values 18 or more	One hour
Physical memory percent free	Warning - at least 20 values 2% or less Alert - at least 30 values 0%	One hour
Virtual memory percent free	Alert - at least 30 values 2% or less	One hour
Swap space percent free	Alert - at least 30 values 2% or less	One hour
Page read rate	Warning - at least 80 values 300 or more Alert - at least 120 values 500 or more	Four hours
Disk space free percent	value 10% or less warning, value 5% or less alert	Four hours
Network utilization	Warning - at least 80 values 50% or more Alert - at least 120 values 75% or more	Four hours

Network transmit bandwidth	Warning - at least 80 values 50000 or more Alert - at least 120 values 100000 or more	Four hours
Network receive bandwidth	Warning - at least 80 values 50000 or more Alert - at least 120 values 100000 or more	Four hours

Event items

MS Windows Error Event Logs Events of Interest		
Name	Criteria	Monitoring Interval
win log unexpected shutdown	Warning - 50 Alert - 100 Alert - >=1	Two Days Four hours

Mass Storage Related Events of Interest		
Name	Criteria	Monitoring Interval
disk array status change	Warning - <=2 Alert - >=3	Two days
disk controller error	Warning - <=2 Alert - >=3	Two days
disk did not respond	Warning - <=2 Alert - >=3	Two days
mass storage device has bad block	Warning - <=2 Alert - >=3	Two days
Compaq physical drive failure	Warning - <=2 Alert - >=3	Two days
FT disk unavail	Warning - <=2 Alert - >=3	Two days
Disk port timeout	Warning - <=2 Alert - >=3	Two days
Disk not ready	Warning - <=2 Alert - >=3	Two days
Disk controller error	Warning - <=2 Alert - >=3	Two days
Disk parity error	Warning - <=2 Alert - >=3	Two days

FT disk failed	Warning - <=2 Alert - >=3	Two days
Disk bad block	Warning - <=2 Alert - >=3	Two days

General Events of Interest		
Name	Criteria	Monitoring Interval
resource issues	Warning - 10 Alert - 50	Two days
printing issues	Warning - 10 Alert - 50	Two days
appl error	Warning - 10 Alert - 50	Two days

Event items and event filters

You can change the event reported for the event items in the categories listed above, MS Windows Error Event Logs Events of Interest, Mass Storage Related Events of Interest, and General Events of Interest, by simply changing the event filters used to retrieve the events for each event item.

For each event item covered included in the categories listed above, MS Windows Error Event Logs Events of Interest, Mass Storage Related Events of Interest, and General Events of Interest, the table below lists the corresponding event filter accessible via the ReSOFT event filter module found at <https://ReSoftservername/main/event/search.php>.

Name	Event Filter
win log	Windows event log change detected
unexpected shutdown	Windows event log - unexpected shutdown
disk array status change	disk array status change
disk controller error	disk controller error
disk did not respond	disk did not respond
mass storage device has bad block	mass storage device has bad block
Compaq physical drive failure	Compaq physical drive failure
Resource issues	Resource issues
Printing issues	Printing issues - filtered

Appl error	Unexpected application errors
FT disk unavail	disk - ft set cannot be used
Disk port timeout	disk - port timeout due to prolonged inactivity
Disk not ready	disk - not ready for access
Disk controller error	disk - drive detected a controller error
Disk parity error	disk - parity error
FT disk failed	disk - ftdisk failed
Disk bad block	mass storage device has bad block - disk

MS Outlook Events of Interest
Name
add-in could not be installed
Outlook error - cannot start outlook
Outlook errors - error processing requested tasks
Outlook errors - exchange server not available
Outlook errors - exchange svr net problems
Outlook error - is in use and could not be access
Outlook errors - inbox folder could not be found
Outlook error - info store could not be opened
Outlook errors - item could not be moved
Outlook errors - msg interf returned unknown err
Outlook errors - name could not be resolved
outlook errors - unable to open dflt e-mail folder
outlook errors - your ms exchange svr is unavailable
Outlook errors - failed to start correctly
Outlook errors - no permission to log on
Outlook errors - server not available
Outlook errors - stationery not installed yet
Outlook errors - ms word mail could not be started

For all of the above:

- Warning – 50
- Alert – 250
- Monitoring interval – Two days

This means that the above thresholds apply to the total number of events retrieved using all of the above filters.

Connectivity Related Events of Interest
Name
conn - access denied filters
Conn - authentication failed
conn - cannot bind socket for incoming request
conn - cannot connect to printer
conn - cannot connect to the Citrix server
conn - computer or share name could not be found
conn - connection has not been restored
conn - device not available filters
conn - error while trying to connect to network
conn - error in connection
conn - error on the network
Conn - error occurred while reconnecting
conn - error writing to printer
conn - connection with firewall timed-out
conn - Limited or no connectivity
Conn - local device name already in use
conn - location unavailable
conn - there may be problem with net connection
conn - network access denied
conn - network connection may have been lost
Conn - net connection could not be found
conn - network error has occurred
conn - network location cannot be reached
conn - network name cannot be found
conn - specified net name is no longer available
conn - network path was not found
conn - net resource or device no longer avail
conn - system couldn't log you into network
conn - no domain server available
conn - not accessible
conn - client could not connect to remote comptr
conn - client could not connect to terminal server
conn - path cannot be found
conn - permanent connection not available

conn - specified remote comptr couldn't be found
conn - remote general
Conn - timed out waiting for authenticn
Conn - timed out waiting for vpn server
conn - unable to browse network
conn - unable to connect to host
conn - unable to connect
conn - unable to establish vpn connection
conn - windows cannot connect to the printer
conn - windows can't find computer or share name
Conn - wireless connection repair

For all of the above:

- Warning – 100
- Alert – 500
- Monitoring interval – two days

This means that the above thresholds apply to the total number of events retrieved using all of the above filters.

Name	Criteria	Monitoring Interval
Defrag failed	Warning – 1 or more items Alert - 4 or more items	Two days
Defrag succeeded	Alert – 0 items OK – >0 items	Two days
File cleanup	always OK	Two days
Clock sync ran but failed	Warning – 1 or more items Alert - 4 or more items	Two days
Clock sync succeeded	Alert – 0 items OK – >0 items	Two days
System clock has drifted	Warning – 1 or more items Alert - 4 or more items	Two days



To learn more about HandsFree Networks and our solution, visit www.handsfreenetworks.com

HandsFree Networks Inc.
1021 Main Campus Drive, Suite 300
Raleigh, NC 27606 (US)

HandsFree Networks Pvt. Ltd.
4th Floor, Concorde Block, UB City
Vittal Mallya Road, Bangalore -560001 (INDIA)

HandsFree Networks and related HandsFree Networks Inc. logos are registered trademarks of HandsFree Networks Inc. Copyright ©2009 HandsFree Networks. All rights reserved. All other company, product and brand names are trademarks of their respective owners.

Find out how HandsFree Networks can automate
your software support process.