

# End-Point Security

<b>CONTENT</b>		
<b>DART Number</b>	<b>DART Description</b>	<b>Page No.</b>
27	System Start-up Environment Control	3
45	Port Probe Detected	5
161	Registry Protection Management	5
174	User Logon-logoff Tracking	7
188	Email Attachment Filtering	7
189	File Download Filtering	7
192	Program Execution Control	8
225	Directory and File Protection Management	9
228	Network Packet Filtering	10
232	Intrusion Protection Control	12
233	System Start-up Environment Management	16
240	Intrusion Protection Management	18

## DART 27 - System Start-up Environment Control

### Overview

Managing and controlling system start-up helps minimize;

- Slower system boot-up
- Ongoing startup performance problems
- Unwanted intrusion, and potentially even harm to the system
- Slower system performance
- ReSOFT features complete system start-up environment management and control.

We have two DARTs that perform these functions:

- DART 27 to control the content of a system's start-up environment. Depending on its configuration, it accepts, rejects, or disables any attempt to add a new item to a system's start-up environment. If so configured, it performs all actions automatically. DART 27 can also prevent the removal of items from a system's start-up environment. In this way it neutralizes attempts to remove intrusion protection software such as virus scanners from running at system start-up.
- DART 233 to manage a system's start-up environment. DART 233 reports the content of a system's start-up environment, and disabled start-up items. It also lets you easily enable and disable start-up items on one, some, or all systems at a site.

### Triggering and detection

DART 27 is triggered by changes to the relevant registry keys and file folders. These are registry keys and file folders that are used to control which applications are run when the system starts. When these are changed, the DART runs, examines their contents to see what has changed, and takes action to allow, disable, or remove a start-up environment change based on its configuration.

Due to a limitation in Microsoft Windows 95, DART 27 cannot be triggered by registry key changes on that operating system. Because of that limitation, and in order to avoid missing a change when the client is not running, the DART also runs at system startup, and whenever the ReSOFT client starts.

DART 27 also monitors, and lets you disable or remove pending file rename operations, which execute at system start-up. Operating system files that are loaded at system startup

can't be deleted, replaced, or renamed when the operating system is running because it locks them. Pending file rename operations provide a mechanism to delete, replace, or rename these files by executing the action at system start-up before the files get loaded by the operating system. This mechanism can be exploited by someone with malicious intent.

DART 27 can also prevent the removal of items from a system's start-up environment. In this way it neutralizes attempts to remove intrusion protection software such as virus scanners from running at system start-up.

## Actions

DART 27 monitors all mechanisms that can be used to run programs at startup. The areas protected include the Startup folder, the win.ini file, the system.ini file, and the registry keys described in

<http://support.microsoft.com/default.aspx?scid=KB;en-us;q13736> and  
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;314866>

Note that the DART does not monitor the "run once" keys, since those are primarily used for system operations, and will not cause changes that permanently affect system performance.

Whenever the list of items in any one of these locations changes; the DART notifies the support provider by posting an event log on the ReSOFT server. In addition, it can take one or more of the following actions:

- Delete the item from the start-up environment so that it will no longer run at startup
- Disable the item by moving it to a "holding area"
- Ask the system's user whether or not to delete/disable the item, if the user interface configuration option is enabled
- Prevent removal of an item from the system's start-up environment
- Do none of the above

Similarly, when DART 27 detects an attempt to add a pending file rename operation, it can automatically disable it, delete it, or ignore it. If the user interface option is enabled, the end-user has control over which of these actions should be taken.

Note that DART 27 will always log the detection of a new start-up item, the removal of an item from a system's start-up environment, or the addition of a pending file rename operation on the ReSOFT server, even if it is configured to do nothing to prevent these changes from taking place.

## DART 45 - Port Probe Detected

When enabled, DART 45 monitors all IP ports on a system where the ReSOFT client is running.

It detects and reports any attempt by a device, whether on the local or other network, to open a TCP connection that is rejected by the local system because there is no process listening on that port.

Usually that indicates a "probe" or a "port scan" that could be the prelude to an unwanted intrusion.

## DART 161 - Registry Protection Management

### Overview

DART 161 is a powerful intrusion protection tool that also automatically performs a useful problem resolution function.

It lets you monitor registry keys on one, some, or all systems at a site, detect changes, and prevent them if configured to do so.

### DART 161 Operations

You can configure DART 161 to monitor registry keys continuously, in which case the DART will detect changes to directories and files as they happen, or on a schedule, in which case it will check them at the time you define in the DART's configuration parameter.

If you enable DART 161's change prevention function, the DART will make a copy of the registry keys that you want to prevent from being changed, and store all the other relevant information. If you choose to protect a registry branch, it will copy the entire branch, and all its other relevant information.

DART 161 runs when one of the following events occurs:

- When the ReSOFT client starts up. When this happens it checks for changes
- When you click on the execute button to the right of the **Check monitored items now** label in the DART's configuration page. When this happens it checks for changes.
- At its scheduled time. When this happens it checks for changes

- When monitored item(s) change. When this happens it checks for changes.
- When one of its configuration parameter changes. When this happens it updates the configuration.
- When it is enabled/disabled. When this happens it updates the configuration.
- Checking for changes means - Determining if any files or directories have been removed, added or altered, and
- Updating the stored information about any item that has changed

Updating the configuration means updating the stored information about monitored item(s) to match their current state. If any existing stored information for monitored item(s) is still relevant, then it is re-used. If a new item is added, it means recording its information.

If DART 161 is configured to prevent changes, instead of updating the stored information about any item that has changed, it will restore the item to its pre-change state by overwriting the changed item with the copy that was stored when the item was first added to the Monitored items parameter as (part of) a command line.

This means that if a protected item is corrupted because of a system's software or hardware malfunction, and does not function properly any longer, if the ReSOFT client is operational, DART 161 will restore the protected item to its working state. In this scenario, the DART can be a useful automated problem resolution tool.

## **DART 174 - User Logon-logoff Tracking**

DART 174 is enabled by default. It detects and reports all user logon and logoff events.

DART 174 tracks and reports the amount of time a user is logged onto a system, and reports all information contained in the user profile.

When users shut down or re-start their systems, DART 174 will report the event as a logoff event when the system re-starts.

## **DART 188 - E-mail Attachment Filtering**

DART 188 can be used to delete attachments from messages received on a system. You can enter the types of files you want DART 188 to delete using the DART configuration facility.

Attachments that are removed are replaced with a text file with the following content:

*"The file attached to this message that was originally named "[file name]" has been removed due to the filtering policy set up by your system administrator."*

Because DART 188 operates on the system where the ReSOFT client is installed, it protects systems from potentially damaging attachments arriving from either POP based mail services, or Web based mail services (e.g. AOL Mail, Yahoo Mail, and Hotmail).

Local execution of DART 188 also makes it possible to customize attachment filtering policies on a system-by-system basis, or for subsets of systems.

## DART 189 - File Download Filtering

DART 189 can be used to block downloading of files on a system. You can enter the types of files, or specific files, whose download you want DART 189 to prevent using the DART configuration facility.

Files whose download is prevented are replaced with a file whose name you enter in DART 189's configuration page.

If no such file name is entered, the file whose download was prevented is replaced with a file whose content is zeros.

***It's important to note that DART 189 only replaces the content of the file whose download was blocked, not its name. Unless the end-user is informed on a timely basis that the file download filtering is enabled, this can lead to repeated attempts to download a file, and consequent frustration on the part of the end-user.***

To minimize the potential for this to happen, we have included in the ReSOFT client directory a small program called block.exe (also in zipped form, block.zip) that when executed informs the end user about the file download blocking policy in effect with the following statement:

*"Sorry, per company policy download of this file type is not allowed. Please contact your system administrator with any questions. Thank you."*

You can use block.exe or block.zip as the files that replace blocked files when blocking files of type's .exe, or .zip, respectively.

## DART 192 - Program execution control

DART 192 stops the execution of programs listed in the DART's configuration page. It has two modes of operation:

- Stop List (default)
- Run List

In **Stop List** mode, DART 192 will terminate the execution of any command line listed in its **Stop List**.

In **Run List** mode, DART 192 will only allow execution of programs listed in the **Run List** of commonly running programs and of programs entered manually by the user. The **Run List** of commonly running programs is created automatically from the list of processes running on the machine for which the DART is being configured.

## DART 225 - Directory and File Protection Management

### Overview

DART 225 is a powerful intrusion protection tool that also automatically performs a useful problem resolution function.

It lets you monitor any file and/or directory on one, some, or all systems at a site, detect changes, and prevent them if configured to do so.

### DART 225 Operations

You can configure DART 225 to monitor files and/or directories continuously, in which case the DART will detect changes to directories and files as they happen, or on a schedule, in which case it will check them at the time you define in the DART's configuration parameter.

If you enable DART 225's change prevention function, the DART will make a copy of the files that you want to prevent from being changed, and store all the other relevant information. If you choose to protect a directory, it will copy the entire directory, and all its other relevant information.

DART 225 runs when one of the following events occurs:

- ➡ When the ReSOFT client starts up. When this happens it checks for changes.

- When you click on the execute button to the right of the **Check monitored items** now label in the DART's configuration page. When this happens it checks for changes.
- At its scheduled time. When this happens it checks for changes.
- When monitored item(s) change. When this happens it checks for changes.
- When one of its configuration parameter changes. When this happens it updates the configuration.
- When it is enabled/disabled. When this happens it updates the configuration.
- Checking for changes means: Determining if any files or directories have been removed, added or altered, and
- Updating the stored information about any item that has changed.

Updating the configuration means updating the stored information about monitored item(s) to match their current state. If any existing stored information for monitored item(s) is still relevant, then it is re-used. If a new item is added, it means recording its information.

If DART 225 is configured to prevent changes, instead of updating the stored information about any item that has changed, it will restore the item to its pre-change state by overwriting the changed item with the copy that was stored when the item was first added to the **Monitored items** parameter as (part of) a command line.

This means that if a protected item is corrupted because of a system's software or hardware malfunction, and does not function properly any longer, if the ReSOFT client is operational, DART 225 will restore the protected item to its working state. In this scenario, the DART can be a useful automated problem resolution tool.

## DART 228 - Network Packet Filtering

### Overview

DART 228 performs an "in-depth" firewall function that is a last line of defense, rather than being an alternative to a corporate firewall, or to "personal" firewall products. It:

- Protects mobile machines, such as laptops, that sometimes operate outside the corporate firewall. These machines are usually unprotected when connected to a dial-up connection or a wireless connection in an airport or coffee shop.

- Limits the internal spread of a worm that gets inside the firewall. This can happen by physically bringing an infected machine into the network, or downloading and installing an infected executable.
- Reports an increase in firewall denials, which is an indicator that something is going on that merits investigation.

We don't intend to provide all the features of a "personal" firewall product. It would not add tangible values to the ReSOFT client. The major advantages that network packet filtering via DART 228 and the ReSOFT client have over those kinds of products include:

- Centralized configuration: the firewall configuration is controlled in one place, including any "exceptions". The entire facility is not open to a threat that exploits an unintentional weakness on a single machine.
- No configuration changes by end-users - Decisions on firewall policy are made by an informed system administrator who has a professional understanding of the security ramifications of the decisions, rather than being made by each end-user who just wants to complete a specific task
- Centralized reporting: All actions and events detected by DART 228 are logged on the ReSOFT server; including statistics on firewall deny operations that would alert a system administrator that the facility is under some kind of systematic attack.

## How it works

DART 228 works by applying sequences of rules, which we call chains, to a system's networking connections, which we call adapter classes.

Rules specify deny traffic or allow traffic actions for source and destination IP addresses or ports. Please refer to DART 228's configuration help file for detailed information on rules.

Once you have defined a set of rules that you want to apply to your site(s), you are ready to assemble them into chains. Chains are simply comma-separated lists of rules. DART 228 applies the rules in a chain sequentially. It takes the action specified by the first rule in a chain that is matched by the packet. If no action is specified in the matching rule, or no rules match, then the default action (a configurable parameter), which is to deny a packet, is taken. Please refer to DART 228's configuration help file for detailed information on chains.

At this point, you are ready tell DART 228 how to enforce the network packet filtering rules you have defined, i.e. how to apply chains of rules to a system's network connections as specified in its adapter classes. DART 228 supports the following adapter classes:

- Hardwired - An adapter that has a physical connection to a LAN
- Wireless - A wireless network adapter
- Dial-up - A dial-up connection through a modem
- Default - All of a system's networking connections

If you enable DART 228 and configure no adapter classes, or make a syntactical mistake in specifying rules, chains, and/or configuring adapter classes, the DART will log the configuration error and will not filter any packets.

## DART 232 - Intrusion Protection Control

### Overview

DART 232 detects attempted configuration changes that can be used to execute unauthorized or malicious code. It can be configured to disable or delete these changes automatically without end-user intervention. If the user interface option is enabled, it alerts the end-user of such system configuration changes giving him/her the option to reject, disable (for future re-enabling if desired), or accept such changes.

The areas monitored by DART 232 are ones that are not normally covered by anti-virus and most other intrusion protection software. DART 232 focuses particularly on how a virus or other unauthorized code may be re-activated after an end-user or system administrator tries to terminate its execution and remove it. Typically, if an end-user or system administrator discovers an unauthorized executable running they may shut down the application, remove it, and possibly remove an entry for it from the system registry.

However it is possible, using shell extension handlers for example, to run a program every time a user right-clicks on a file which checks to see if the rogue application is installed and running, and if not, re-installs it and re-runs it. This type of re-activation can be very difficult to track down.

Malicious code can also be run at startup by using the Run registry keys, the startup folders, system.ini and win.ini. DART 27, (System Start-up Executable Management) protects these areas from intrusion. Though autoexec.bat can be used to run code at startup, currently it's rarely used to do so. In autoexec.bat, we're more interested here in protecting the contents of the PATH environment variable. Rogue applications can use it to run unauthorized code. The system areas and object types currently protected by DART 232 include:

- Autoexec.bat
- Shell extension handlers Screen savers
- Open verb's command default value for executable files
- The Shell and Userinit values for the Winlogon key
- RunOnce, RunOnceEx, and RunServicesOnce registry keys
- Scrap Objects

## How it works

DART 232 creates a hidden directory in the client dir called "232". When the DART first runs it creates in this hidden directory backup files of autoexec.bat, explorer.exe, and userinit.exe, using the .bak extension. DART 232 watches these files for tampering using checksums and should one of these files change the backup file in the hidden directory will be restored if the change is rejected (either silently, by dialog box timeout, or by user action). If a file changes and the change is accepted then the backup file is updated.

Further, if one of these files change and the chosen action is "Disable" then in addition to the backup file being restored the "disabled" version is archived in the hidden directory with the extension dbl. This is so a system administrator could examine the changed file after the backup is restored.

## DART 232 coverage areas detail

In this section we describe in some detail the areas and object DART 232 protects from intrusion. For additional information on why and how configuration changes in these areas, and changes to these objects, can cause the execution of malicious code please refer to the article by Jason Fisher titled "Understand Common Virus Attacks Before They Strike to Better Protect Your Apps" at the following URL:

<http://msdn.microsoft.com/msdnmag/issues/03/05/VirusHunting/default.aspx>

**Autoexec.bat** can be used to run executable files on startup so we'll use a checksum to watch for changes in this config file. Also, the modification of the PATH environment variable is perhaps even more insidious than running executable code directly because it's less likely to be noticed as a potential risk. For example, when Microsoft Windows NT starts up it runs explorer.exe as the shell. This is because the "Shell" value of the "Winlogon" key is set to "explorer.exe". Now explorer.exe can't be replaced with a copy while Windows NT is running because it's protected by an operating system lock. However, there is no path given in the registry, so someone could replace explorer.exe with a copy stored somewhere on the

system, and change the PATH variable so that Windows NT uses the copy instead of the original. What's worse is that the real explorer.exe is no longer protected by an operating system lock so it can now be overwritten.

**Shell extension handlers** (DLLs) can be set to run whenever any number of shell actions is initiated by the user, such as right clicking on an object to bring up the context menu or dragging and dropping. Since these handlers can execute malicious code, DART 232 monitored this area of the registry detecting (and rejecting/disabling them if so configured) any new harmful codes are installed and registered.

**Screen savers.** Screen savers are executable files. They are not locked by the operating system when they are not running so they can be replaced by files in screen saver format containing malicious code. When this happens, as soon as the screen saver is activated, the malicious code is executed.

Virus writers can implement attacks that exploit screen savers in two ways. First, they can find out what the currently selected screen saver is and replace the associated file with an infected copy. They can also copy a new screen saver (infected) to the system and programmatically make it the currently selected one.

To guard against these attacks DART 232 monitors the current screen saver selection for change. It also monitors the associated file for modification. It does not create backup files for screen savers because a typical machine can have over a dozen of them and users can install many more. Saving copies of all of them would unnecessarily clutter backup directories and these files are just not important enough to warrant that.

If the current screen saver selection is changed unknown to the user, DART 232 will change it back if it is configured to do so. If the file associated with the current screen saver selection is modified it cannot restore the original file because it keeps no backup.

Instead, DART 232 sets the screen saver selection to "None" so the malicious code won't execute. The DART will also post a log on the ReSOFT server warning you that the file associated with a screen saver was modified.

DART 232 only monitors the file associated with the screen saver currently selected by the end-user. To keep other (non-selected) screen saver files from being replaced, the DART I keep a list of their checksums. Whenever DART 232 runs, it compares the saved checksums with current ones. If it finds that one of the non-selected screen saver files has changed it posts a log on the ReSOFT server warning you that the file associated with a screen saver

was modified. This should be sufficient because there is no immediate danger, since the screen saver associated with the modified file is not currently selected.

**Open verb's command default value.** There is a list of executable files (.exe, .com, .bat, etc.) that will run if the user double-clicks them. This is because their "open" verb's command default value in the registry is "%1" %\*. These registry values can be changed to something like "VirusExecutable.exe %1". The result, as explained by Jason Fisher, would be this: "This allowed the virus program to run first any time the user attempted to execute any EXE program. The requested program was passed to the virus executable as a parameter, whereupon the virus could launch it, keeping the user largely in the dark about what was really going on." DART 232 monitors the open command's default value for executable files for attempts to modify them (rejecting/disabling them if so configured).

**The "Shell" and "Userinit" values for the registry key "Winlogon"** contains the name of executable files that are executed whenever a user logs on. The "Shell" value runs explorer.exe. "Userinit" runs userinit.exe on Microsoft Windows 2000, XP and 2003, and userinit.exe and nddeagnt.exe on systems running Microsoft Windows NT4. DART 232 monitors "Shell" and Userinit". If so configured, it prevents them from being changed and, as further protection, records the checksums of the .exe files in case they get replaced with copies with the same name.

**The RunOnce, RunOnceEx, and RunServicesOnce registry keys** can be used to run a malicious executable at system start-up. What makes this type of intrusion particularly insidious is that after the malicious code runs at system start-up, the registry entries are automatically deleted, thus leaving no trace.

**Scrap objects** can be created for OLE (Object Linking and Embedding) purposes. Again, we'll just quote Jason Fisher's explanation: "[Scrap objects] are extremely dangerous because they can encapsulate executable code within a compound OLE document format " Further: "There are two additional reasons these files are particularly risky, apart from the simple fact that they can hide executable code. First, they're often overlooked by antivirus software. Even if one of them is included in the list of executable application types, the other is often omitted. You should ensure that your antivirus program includes both file types. The second reason is much more subtle. As it turns out, the SHS and SHB extensions are always hidden by Explorer, even if you've configured Windows to display all file extensions.

The reason is that the registry keys for these file types include an undocumented value, "NeverShowExt." If present, this value overrides global settings in Windows. For this reason, a virus writer can create a scrap object; give it an icon corresponding to an image, and then rename it something like "Look at This Funny Picture.jpg." Its actual file name, of

course, is "Look at This Funny Picture.jpg.shs," but to the unsuspecting user it looks exactly like any other image. By the time the realization dawns that the file wasn't an image at all, the damage is done." Initially, DART 232 turns off the value NeverShowExt for scrap objects, making it less likely for a user to inadvertently execute one.

## DART 233 - System Start-up Environment Management

### Overview

Managing and controlling system start-up ensures that:

- Slower system boot-up
- Ongoing startup performance problems
- Unwanted intrusion and potentially even harm to the system
- Slower system performance is prevented.
- ReSOFT features complete system start-up environment management and control.

We have two DARTs that perform these functions:

- DART 27 to control the content of a system's start-up environment. Depending on its configuration, it accepts, rejects, or disables any attempt to add a new item to a system's start-up environment. If so configured, it performs all actions automatically.
- DART 233 to manage a system's start-up environment. DART 233 reports the content of a system's start-up environment, and disabled start-up items. It also lets you easily enable and disable start-up items on one, some, or all systems at a site.

### How it works

DART 233 runs when one of the following events occurs:

- When you click on the execute button to the right of the Update startup items now label
- When a user logs on. Having DART 233 run when a user logs on has the side effect of having it run on ReSOFT client start-up. This is because the user that is currently active is seen as a new user when the ReSOFT client starts up.
- When it is enabled/disabled. When this happens it updates the configuration.
- At its scheduled time

When DART 233 runs the **Startup items to enable and Startup items to disable** parameters are processed first. After the appropriate start-up items are enabled or disabled as per the configuration, then the content of the **currently enabled startup items on this machine and currently disabled startup items on these machine parameters** is updated.

### Enabling and disabling start-up items

The easiest way to disable a start-up item is to copy it from the **currently enabled startup items parameter**, and paste it into the **Startup items to disable** parameter. To re-enable an item you can move it from the Startup items to disable parameter to the **Startup items to enable parameter**.

While this method of enabling and disabling start-up items is certainly not the most elegant, it is straightforward and efficient.

## DART 240 - Intrusion Protection Management

### Overview

ReSOFT features complete intrusion protection management and control. We have two DARTs that perform these functions:

- DART 232 controls the content of a system's areas that could be targeted by intruders. Depending on its configuration, it accepts, reject, or disable any attempt to modify the content of these areas. If so configured, it performs all actions automatically.
- DART 240 manages a system's configuration areas potentially affected by intruders. It reports the content of a system's intrusion related configuration variables, both enabled and disabled. It also lets you easily enable and disable these variables on one, some, or all systems at a site.

### DART 240 - coverage

System configuration variables managed by DART 240 are divided into two groups manipulated via different sets of configuration parameters.

The **Currently enabled items on this machine, currently disabled items on this machine, Items to enable**, and **Items to disable** configuration parameters manage the following system configuration variables:

- Autoexec.bat
- Shell= system.ini setting for systems running Microsoft Windows 9x based operating systems
- Shell extension handlers
- RunOnce
- RunOnceEx
- RunServicesOnce registry keys
- Browser Helper Objects
- Internet Explorer Bars
- Internet Explorer Extensions
- Internet Explorer Toolbars
- Hosts file

The **Current configuration settings on this machine** and **Configuration settings** to enforce configuration parameters manage the following system configuration variables:

- Start Page settings
- Search Pages settings
- Open verb commands
- Screen saver settings
- Critical Winlogon registry keys (shell and userinit) for systems running Microsoft Windows NT based operating systems (NT4, 2000, XP, or Server 2003)

## How it works

DART 240 runs when one of the following events occurs:

- When you click on the execute button to the right of the Update intrusion protection now label
- When a user logs on. Having DART 240 run when a user logs on has the side effect of having it run on ReSOFT client start-up. This is because the user that is currently active is seen as a new user when the ReSOFT client starts up.
- When it is enabled/disabled. When this happens it updates the configuration

- At its scheduled time

When DART 240 runs, the **Items to enable, Items to disable, and Configuration settings to enforce** parameters are processed first. After the appropriate system configuration items are enabled or disabled as per the configuration, then the content of the **currently enabled items on this machine and currently disabled** items on these machine configuration parameters is updated.

## Enabling and disabling items

DART 240 is a powerful management tool because in addition to providing you with information about enabled and disabled system configuration items that could be targeted by intruders, it lets you enable and disable these system configuration items on one, some, or all systems at a site, or at all your sites making the necessary changes only once.

In addition, like all other ReSOFT DARTs, DART 240 logs and reports all events it detects and actions it takes to the ReSOFT server where you can easily set up notifications and reports to keep you and your users informed about intrusion protection management activities at your sites.

The easiest way to disable a system configuration item is to copy it from the **currently enabled items** configuration parameter, and paste it into the **Items to disable** configuration parameter. To re-enable an item you can move it (**cut and paste**) from the **Items to disable** configuration parameter to the items to enable configuration parameter.

While this method of enabling and disabling start-up items is certainly not the most elegant, it is straightforward and efficient. Depending on your needs, in order to disable a system configuration item on all systems at a site you only need to add an entry to the **Items to disable** configuration parameter on one system.

The **Configuration settings to enforce** configuration parameter provides you with a simple yet powerful tool for standardizing the value of critical system configuration settings such as browser and shell related variables at a site, and ensuring that they are protected from intruders.

The easiest way (and least prone to errors) to add to or modify the content of the **Configuration settings to enforce** configuration parameter is to copy entries with the desired value from the **Current configuration settings on this machine configuration parameter**.

To learn more about HandsFree Networks and our solution, visit [www.handsfreenetworks.com](http://www.handsfreenetworks.com), send us an e-mail or call



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

*HandsFree Networks Pvt. Ltd.,*  
4<sup>th</sup> 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.