System Administrators Guide for Enterprise Management Features

WindowSMART 2013

Celebrating 10 Years – 2003-2013

Dojo North Software, LLC

49434 Tarrytown Court

Shelby Township, MI 48315

(586) 350-8117

2/27/2012

Contents

Overview

The purpose of this System Administrators' Guide to Enterprise Management Features (the "guide") is to provide system administrators with the tools necessary for deploying, licensing, managing, upgrading and uninstalling WindowSMART 2013 on end-user workstations. Many operational tasks can be scripted so that they can be installed and managed without user intervention.

WindowSMART 2013 allows the following operations to be scripted and run via batch files or a command line interface:

- Installation
- Upgrade
- Removal (Uninstall)
- License Key Deployment
- Set/Clear Custom Support Message

An Active Directory ADM template file is also available. You can deploy the ADM template into your Active Directory infrastructure for the purpose of creating Group Policy Objects (GPOs), which can be used to define (and enforce) specific settings. This can prevent users from changing WindowSMART 2013 configuration settings, and ensure a consistent set of settings is deployed across an entire organization.

Command Line Argument Preferences

All examples in this document use the slash ("**/**") character to specify command line arguments. However, because system administrators may come from different backgrounds, such as Linux, they may be used to using the dash ("-") or double dash ("--") to specify arguments.

Because of this, while the examples and instructions in this document use the slash character, using the dash and double dash are equally valid. The three example commands are all identical, so when creating your scripts, the method you use to specify the arguments is entirely your preference. (CAUTION: Windows Installer "msiexec.exe" does not recognize the double-dash.)

```
WindowSMARTEnterpriseManagement.exe /supportmessage /"message"

WindowSMARTEnterpriseManagement.exe -supportmessage -"message"

WindowSMARTEnterpriseManagement.exe --supportmessage --"message"
```

Installing, Upgrading and Removing

This section discusses how to install, upgrade and/or remove WindowSMART 2013 on end-user workstations, as well as the options available and how to interpret installation error codes.

All installation, upgrade and removal tasks must be performed by using msiexec.exe (Windows Installer). When msiexec.exe is run from a CMD, or batch, file, it will return an error code (the ERRORLEVEL value) which can be used to determine whether or not the operation was successful and, in the event of a failure, what exactly caused the failure. **NOTE:** The Microsoft Visual C++ 2010 Runtime and Microsoft .NET Framework 4 Full are prerequisites for installing WindowSMART 2013. If either of these are missing, they will be detected in the MSI and a failure code will be returned.

Installing and Upgrading the Lightweight Client

The WindowSMART 2013 Lightweight Client is intended for use on embedded devices, POS terminals, cash registers, and even servers, etc. where end users normally would not interact with the Windows operating system itself or tools that run on it. The Lightweight Client is designed so that no user interaction is required, or even allowed, and all management of WindowSMART is remote.

To install or upgrade WindowSMART 2013 Lightweight Client, you may double-click on the MSI file, or script the installation in a batch file, CMD file or PowerShell script. WindowSMART can be upgraded in place. Simply install a newer version over an older one. If you want to downgrade, however, you must uninstall the old version first.

There are no options for the Lightweight Client. Because it has no UI, there is no desktop shortcut, and the Enterprise Management tool is always installed. The below command performs a scripted (or unattended) install of the Lightweight Client.

```
msiexec.exe /i WindowSMART2013_x64_lightweight.msi /passive
```

Uninstalling the Lightweight Client

To uninstall WindowSMART 2013, use the following command:

```
msiexec.exe /x WindowSMART2013_x64_lightweight.msi /passive
```

Installing and Upgrading the Full UI Client

The WindowSMART 2013 full UI client is intended for use on laptops, desktops and even servers where end users regularly interact with them. The full UI offers rich features to end users, although like the Lightweight Client, it can still be managed remotely.

WindowSMART's full UI client offers installation options. If you would like to create a desktop shortcut, or install the Enterprise Management tool, you can specify those options. The feature names are INSTALLDESKTOPSHORTCUT and INSTALLENTERPRISEFEATURES. To install an option, set it equal to 1; to exclude the option, set it to 0. If neither option is specified, the defaults are 1 and 0 for the shortcut and Enterprise Management tool, respectively.

Some examples on how to install WindowSMART 2013's full UI client:

```
msiexec.exe /i WindowSMART2013_x64_full.msi /passive
```

```
msiexec.exe /i WindowSMART2013_x64_full.msi /passive
INSTALLENTERPRISEFEATURES=1
```

```
msiexec.exe /i WindowSMART2013_x64_full.msi /passive
INSTALLDESKTOPSHORTCUT=0 INSTALLENTERPRISEFEATURES=1
```

Uninstalling the Full Client

To uninstall WindowSMART 2013, use the following command, regardless of installed options.

```
msiexec.exe /i WindowSMART2013_x64_full.msi /passive
```

Enterprise Management Command Line Interface

System administrators may want to deploy WindowSMART 2013 to end-user computers in a consistent manner. The unattended installation described earlier in this document causes the enterprise management feature (command line interface or CLI) to be installed. This feature allows you to deploy the WindowSMART 2013 license via a script (CMD or batch file), and also set or clear a custom support message.

The custom support message is useful if you intend for WindowSMART to report disk alerts to end users. Many system administrators don't want users to see disk alerts; instead the alerts will be sent only to the system administrator, support team or helpdesk. On the other hand, some system administrators prefer to allow end users to see disk alerts when they occur. In the latter case, you may wish to provide a support message to the user on what they should do should an alert arise. Some users may be confused or frightened when they receive a disk health alert, so providing them with instructions on what they should to can be beneficial. The support message is limited to 256 characters, so the message should be concise on what they should do. Something like this should be sufficient: "For further help regarding this disk health alert, please contact the helpdesk by calling 1-888-555-1234 option 3 or by email at support@helpdesk.somecompany.com." (This example is 163 characters long, so there are over 90 characters to spare and the action the user should take is clearly communicated.)

The enterprise management features are contained in an executable named WindowSMARTEnterpriseManagement.exe, which is contained in the WindowSMART 2013 installation folder (by default C:\Program Files\Dojo North Software\WindowSMART 2013). This executable contains the "require administrator" flag so if run interactively on a computer running a UAC-aware operating system (Windows Vista/Server 2008 or later), it will prompt for elevation.

You must run Setup with the **/unattended** argument (and optionally the **/desktopshortcut** argument) for the enterprise management feature CLI to be installed. You do **not** need to have an enterprise license to use the CLI. This CLI can be used with any WindowSMART 2013 license, including trial mode.

License Key Deployment

Unless you are licensing a handful of computers, it will be easier to script the deployment of WindowSMART 2013 licenses to end user computers. The WindowSMART 2013 license key is an XML file with a .slab file extension, hence it being referred to as a "Slab license file." You may save the Slab license file to a central location such as a file server that is accessible to end user computers. You may also copy the file locally.

The syntax of the command to apply the license is as follows:

```
WindowSMARTEnterpriseManagement.exe /key slablicensefile
```

```
WindowSMARTEnterpriseManagement.exe /key slablicensefile /autorestart
```

The **/key** argument specifies that you want to apply a license key, and the ***slablicensefile*** is the fully-qualified path of the Slab license file. The Slab license file can be located on a local drive, a mapped (lettered) drive or a UNC location.

The **/autorestart** argument instructs the WindowSMART 2013 service to automatically restart after the key is successfully applied. If the key application fails, the service restart is not performed. The service must be restarted for the changes made by application of the license key to take effect, so specifying **/autorestart** is highly recommended

Examples

WindowSMARTEnterpriseManagement.exe /key C:\temp\license.slab

This example applies the license key contained in license.slab in the C:\temp directory, without restarting the service. (The service will need to be restarted manually, or the computer rebooted.)

WindowSMARTEnterpriseManagement.exe /key \\fileserver\teamshare\license.slab /autorestart

This example applies the license key contained in license.slab on the UNC share \\fileserver\teamshare, and restarts the service when the key is applied.

Setting/Clearing a Custom Support Message

If you want to set or remove a custom support message that is displayed at the end of all disk health alerts, use the following commands:

WindowSMARTEnterpriseManagement.exe /supportmessage *"message"*

WindowSMARTEnterpriseManagement.exe /supportmessage /delete

When you specify **/supportmessage** with a message you want displayed, you **must** enclose the entire message body in double quotes, unless you message consists of a single word (not recommended). If you do not enclose the message in double quotes, you will get an error.

Specifying **/supportmessage /delete** clears the custom message.

Removing Group Policy Settings

If you use the WindowSMART 2013 ADM template to enforce some or all WindowSMART configuration values, these are not stored in the Microsoft policies location in the Registry, but rather in the standard location WindowSMART has always used, which ensures interoperability by both GPO-configured and standalone WindowSMART installations. It is easier to troubleshoot and manage when configuration settings are stored in a consistent location across all deployments, rather than scattered across the Registry depending on whether group policy objects (GPOs) are used to deploy the configuration settings.

This does, unfortunately, have one significant drawback. If you decide to, at a later date, remove the GPO settings or change some policies to "not configured," this will not necessarily "unlock" the UI or enable the users to make changes. This is because when policies are not deployed in the Microsoft policies location, they are instead deployed as preferences, and therefore "tattooed" in Registry. This means that changing a policy setting to Not Configured or removing the ADM template completely will **not** remove those settings. To combat this, you can run the below command to refresh the configuration and clean out those settings. If you still have GPOs enforcing *some* settings, the next policy refresh will restore those settings.

WindowSMARTEnterpriseManagement.exe /refreshpolicy /tattoo

The **/refreshpolicy /tattoo** instructs the Enterprise Management tool to remove all tattooed settings (settings that do not exist in a non-GPO environment). This does not prevent you from restoring those settings at a later date, nor will it permanently delete GPOs you still want to enforce. Those GPOs may be temporarily removed, but the next time Windows performs a policy refresh, those settings will get restored. You can force the policy refresh by running the Windows command **gpupdate /force**.

Enterprise Management Command Line Exit Codes

When Setup exits, it returns an exit code, also known as an error code. When used in a CMD (or batch) file, the exit code is saved in the ERRORLEVEL variable, which can be used by the script to determine success or failure. Below is the list of exit codes.

CLI Exit Code	Explanation
0	The operation completed successfully. This applies to license application, setting/clearing the support message and policy refresh. This is also returned if you specify the **/?** argument for help.
1	The license key was successfully applied, but an error occurred trying to restart the service. Please restart the service manually or reboot the computer.
2	Invalid number of parameters specified. Except for the **/?** argument, the CLI takes exactly 2 or 3 arguments, no more and no less.
3	First parameter is invalid; it must be either **/key** or **/supportmessage** or **/refreshpolicy**.
4	Third argument to **/key** is invalid; if specified this argument must be **/autorestart**.
5	Unrecognized parameter was specified.
6	The Slab license file was not found at the specified location.
7	An error occurred checking for the Slab license file. This may occur if there is a typo in the file path, or if the ID being used to run the script does not have permissions to access the specified location.
8	Second argument to **/refreshpolicy** is invalid. It must be **/tattoo**.
9	Unhandled exception was thrown trying to apply the license.
10 (0xA)	XML in the specified file is malformed.
11 (0xB)	Document validator returned an empty string (should never occur).
12 (0xC)	Exception occurred in the cryptography engine.
13 (0xD)	Exception occurred injecting the license.
14 (0xE)	Exception occurred setting/clearing the support message. Most likely this is caused by a lack of permissions to set the Registry value.
15 (0xF)	The policy refresh operation threw an exception.
All Other Codes	License module specific error code. Contact Dojo North Software for assistance.

Active Directory ADMX and ADM Templates

The WindowSMART 2013 Active Directory group policy object (GPO) template can be used to customize all of your WindowSMART 2013 deployments. If you go this route, you are able to lock down the WindowSMART 2013 client so that end users are prohibited from making any changes to the

configuration. The template is designed such that each configuration area is a separate entity, so you can customize and lock down some settings while leaving others available to the users.

The WindowSMART 2013 GPO templates consist of the modern ADMX/ADML template and a classic, or legacy, ADM template. The classic template ensures compatibility with legacy Active Directory environments.

The ADMX template consists of two files – the ADMX template and the ADML language resource file. The ADML file resides in a subfolder named en-US, and for correct operation the ADML template must remain there.

Both the ADMX and ADM templates do not use the standard Windows policies keys to store its configuration data. Rather, it is stored in the standard location for any WindowSMART 2013 deployment, HKLM\Software\Dojo North Software\HomeServerSMART\Configuration. (Note that the key says "HomeServerSMART." This is because we originally developed Home Server SMART, and WindowSMART was developed later. Because they share most of their code, and to maintain backwards compatibility and support for upgrades, the registry location was not changed.) Because the Registry location is not a standard policy location, Windows will deploy it as a "preference" and not a "policy." What this means is that the settings will be "tattooed" on the clients affected by that policy; in other words, if the WindowSMART 2013 policy goes out of scope (i.e. you remove it entirely), the settings will remain on the clients. Any changes you make to the policy will still get updated on a policy refresh, but removing the policy entirely does not remove it from the clients.

If you decide to remove the WindowSMART ADMX or ADM template, it is **strongly recommended**, that you set each policy within the template to **Not Configured** and allow sufficient time for clients to detect the change. Then you can remove the template. This reduces the "tattooing" of policy settings. Of course, you can always run the Enterprise Management tool with the **/refreshpolicy** and **/tattoo** options to clean up remnants of removed policy objects.

Deploying the ADMX Template

If your Active Directory domain is set up to retrieve templates from the local computer, you must copy the ADMX and ADML files into C:\Windows\PolicySettings on each domain controller. The ADMX file goes into C:\Windows\PolicySettings and the ADML language resource file goes into C:\Windows\PolicySettings\en-US.

If Active Directory is set up to retrieve templates from the central store, you must copy the ADMX and ADML files into the **PolicySettings** folder, which you will be able to find at the location (substitute your domain name) \\fully_qualified_domain_name\SYSVOL\fully_qualified_domain_name\Policies. The ADMX goes into PolicySettings and the ADML language resource file goes into PolicySettings\en-US. Your Active Directory administrator should be able to assist you if you have questions on how to get the template deployed.

CAUTION: If you use the ADMX template, do not deploy the ADM template.

Deploying the ADM Template

To deploy the WindowSMART.adm template, you must deploy it to **each group policy** where you want it used. The location is %domainroot%\SYSVOL\domain\policies\{insert_guid_here}\Adm. A default Active Directory deployment gives you Default Domain Policy ({31B2F340-016D-11D2-945F-00C04FB984F9}) and Default Domain Controllers Policy ({6AC1786C-016F-11D2-945F-00C04FB984F9}). If you've created your own GPOs, additional GUIDs will appear and should be substituted for {insert_guid_here}. If an Adm folder does not exist, you will need to create it, and then deposit a copy of WindowSMART.adm into that location.

Once the template is deployed in the appropriate policy location(s), allow the NT File Replication Service (NTFRS) time to replicate the file to the domain controllers, and then you can configure the policy settings it provides.

CAUTION: If you use the ADM template, do not deploy the ADMX template.

Understanding Policy Settings

When you configure an Active Directory policy, you get the options of Not Configured, Enabled and Disabled. The default is Not Configured for all WindowSMART policy settings.

Not Configured

When a policy is set to Not Configured, by Microsoft's definition, "the default setting applies." What this actually means is that Active Directory is not enforcing any settings that policy governs. The user is free to change the settings, and the user's changes will not be affected by a policy refresh.

Enabled

When a policy is Enabled, Active Directory is enforcing all of the settings that policy governs. The WindowSMART 2013 service and client will detect a flag is set, and will prevent users from making changes to any of those settings. You as the administrator can customize the settings as desired, and those settings will be enforced on all clients governed by that GPO. Any changes you make to the policy are pushed to the clients on the next policy refresh.

Disabled

When a policy is Disabled, Active Directory is enforcing that the settings that policy governs are disabled and essentially unusable. Some Registry values may be removed entirely or be set to their "off" state. The WindowSMART 2013 service and client will detect a flag is set, and will prevent users from enabling those features or changing their settings.

WARNING: It is not possible to prevent a policy from being set to Disabled in an ADM template. Some WindowSMART policy settings should never be set to Disabled. For example, the "Disk Temperature Preferences and Alerts" policy contains settings for the critical, overheated, hot and warm temperature thresholds. If you set this policy to Disabled, Active Directory **removes** the Registry entries for these four temperature settings. The next time WindowSMART checks these temperature settings, they will be missing. This causes an internal error that results in WindowSMART recreating these four values with their default settings.

WindowSMART 2013 Policy Settings

When you open up GPO management, you will see the following policies. Most policies have several items within them you can configure. It will be indicated whether a policy can be safely set to the Disabled state and, if not, why it should not be set to Disabled.

Disk Polling and Analysis

These policy settings cover the WindowSMART settings found on the General tab. If you enable this policy, you specify how often the service polls the disks (in milliseconds), and whether or not an alert should be raised for Warning or Geriatric disk health events. If you leave this policy as Not Configured, the user is free to change these settings. **Do NOT** disable this policy setting. If you do, WindowSMART will use the default settings for these values (poll every 3 minutes and generate alerts for both Warning and Geriatric disk health events).

Disk Temperature Preferences and Alerts

These policy settings cover the WindowSMART settings found on the Temperatures tab. If you enable this policy, you can set the temperature display preference, the thresholds for critical, overheated, hot and warm, and whether to raise alerts for Hot and Warm disks. If you leave this policy as Not Configured, the user is free to change these settings. **Do NOT** disable this policy setting. If you do, WindowSMART will use default values. If you do not want the user making changes, enable the policy setting and specify the desired values.

You can also specify the action to take in a thermal emergency – a condition where at least one disk remains at an overheated or critically hot temperature for 3 or more consecutive polling intervals. The default action is to send an alert. Optionally, you can have the computer shut down.

NOTE: If you set a more critical temperature threshold less than that of a less critical temperature threshold (i.e. set Critical to 60 and Overheated to 61), a policy error occurs and WindowSMART will use default values. It is also a policy error to choose to ignore Hot alerts but not ignore Warm ones.

Virtual Disk Enumeration

This policy sets whether WindowSMART will attempt to enumerate (process) known virtual disks. Virtual disks do not possess SMART attributes and often lack other attributes that physical disks possess, resulting in erroneous data collection and sometimes errors raised by WindowSMART. It is recommended you do not enumerate these disks.

If you enable this setting, you can specify whether or not virtual disks are enumerated. It is recommended you set the “never enumerate known virtual disks” flag (default). If you leave this policy setting as Not Configured, the user is free to change this setting. If you disable this policy, virtual disks are never enumerated.

Allow Users to Ignore Problems

This policy sets whether a user is allowed to ignore disk problems such as bad sectors, end-to-end errors and spin retries. The purpose of ignoring problems allows a user to employ “watchful waiting” of a problem to see if it worsens. To allow a user to ignore problems, leave this policy as Not Configured or

set to Enabled. If you set this policy to Disabled, the user can never ignore problems, although problems that were ignored prior to the policy change will remain ignored.

NOTE: A user can still choose to ignore an entire disk, regardless of policy. This is because there are a number of flash drives and media card readers that expose erroneous SMART data that trigger false alerts.

Allow Users to Control the WindowSMART 2013 Service

This policy specifies whether or not the buttons on the Service Control tab are active. If you enable this policy, users are allowed to start, stop or restart the WindowSMART 2013 service. If you enable this policy, you can also control whether users are allowed to reboot or shut down the computer from within WindowSMART. If you disable this policy, users are prohibited from managing the service, and are prohibited from rebooting or shutting down the computer from within WindowSMART. (This policy setting does not necessarily preclude a user from managing the WindowSMART service via the Services control panel or rebooting or shutting down by using the Start button.) If this policy is not configured, the default behavior of enabled buttons applies.

Email Notifications

This policy allows you to control email notifications for disk health alerts. If you want to leave this up to the user, leave the policy as Not Configured. If you would prefer to control who receives these emails, enable the policy and configure the desired recipient(s) – recommended recipients are system administrator(s), technical/field support personnel and/or helpdesk support staff. If you never want email alerts sent, set this policy to Disabled.

NOTE: If you use authentication, the username and password must be set to their **encrypted** values. The best way to do this is to configure WindowSMART on a test PC, and then copy the encrypted values from the Registry. These settings can be found in HKLM\Software\Dojo North Software\HomeServerSMART under the values MailUser and MailPassword.

iOS (iPhone/iPad/iPod Touch) Notification Via Boxcar

This policy allows you to control remote notifications via Boxcar to compatible iOS devices (and Boxcar clients running on Mac OS X), such as iPhone, iPad and iPod Touch. WindowSMART supports sending notifications to up to five (5) individual Boxcar recipients at one time. A recipient must have an email address registered with Boxcar (registration is free at boxcar.io). Leave this policy as Not Configured to allow the user to configure Boxcar notifications. Enable this policy if you want to control the recipients of Boxcar notifications, such as administrators, technical/field support or the helpdesk. Disable this policy if you never want Boxcar notifications sent.

iOS (iPhone/iPad/iPod Touch) Notification Via Prowl

This policy allows you to control remote notifications via Prowl to compatible iOS devices, such as iPhone, iPad and iPod Touch. WindowSMART supports sending notifications to up to five (5) individual Prowl recipients at one time. A recipient must have a Prowl API key (available at no charge from http://www.prowlapp.com). Leave this policy as Not Configured to allow the user to configure Prowl notifications. Enable this policy if you want to control the recipients of Prowl notifications, such as

administrators, technical/field support or the helpdesk. Disable this policy if you never want Prowl notifications sent.

Android Notification Via NMA

This policy allows you to control remote notifications via Notify My Android (NMA) to compatible Android phones and tablets. WindowSMART supports sending notifications to up to five (5) individual NMA recipients at one time. A recipient must have an NMA API key (available at no charge from http://www.notifymyandroid.com). Leave this policy as Not Configured to allow the user to configure NMA notifications. Enable this policy if you want to control the recipients of NMA notifications, such as administrators, technical/field support or the helpdesk. Disable this policy if you never want NMA notifications sent.

Windows Phone Notification Via Toasty

This policy allows you to control remote notifications via Toasty to compatible Windows Phone 7 devices, and Windows Phone 8 devices, if Toasty supports them. WindowSMART supports sending notifications to up to five (5) individual Toasty recipients at one time. A recipient must have a Toasty device ID, which is assigned by Toasty when they purchase and install Toasty on their phone. Leave this policy as Not Configured to allow the user to configure Toasty notifications. Enable this policy if you want to control the recipients of Toasty notifications, such as administrators, technical/field support or the helpdesk. Disable this policy if you never want Toasty notifications sent.

Advanced Configuration Settings

This policy allows you to control what the user is able to do on the Advanced tab (except for SmartInspect debug logging). If this policy is Not Configured, all options are available to the user. If you want to control which options are available/enforced, set the policy to Enabled and specify which options are available. For instance, you can prevent users from deleting stale disk data. You may find this useful if you have a company policy that prohibits the use of external hard drives or flash drives. If you are investigating a user for possible inappropriate activity, the stale disk data would present evidence of the user using a prohibited disk.

Do NOT set this policy to Disabled. Setting it to disabled will cause default values to be used for some options, which you may not want to allow. (Set the policy to Enabled and then disallow the specific items.)

Debug Logging

This policy allows you to control whether users can create debug logs. If this policy is Not Configured, users can create debug logs at a location of their choosing. If this policy is Enabled, you can specify whether logs are allowed (the user can turn logging on/off), mandatory (logs are always created) or forbidden (logs are never created). Regardless of the setting, you must specify a debug log path. If unsure, specify %DEFAULT% to let Windows decide (i.e. Windows 7 uses C:\ProgramData)). If this policy is Disabled, logs are never allowed or created.

SSD-Specific Settings

This policy allows you to control the thresholds for raising Critical or Warning events for items specific to Solid State Disks. These items are media wearout and sector retirement. Each has a configurable critical and warning threshold. To allow the user to change the settings, leave this as Not Configured. Set to Enabled to specify the desired thresholds. **Do NOT** set this policy to Disabled. If you do, WindowSMART will use default values.

Allow User to Check for Updates

This policy allows you to control whether or not the user can click the Check for Updates button, as well as whether the WindowSMART service checks for updates automatically. Set this to Not Configured or Enabled to allow the user (and service) to check for updates. Set this to Disabled to prevent the user or service from checking for updates. (This does NOT prevent the user from visiting the Dojo North Software website and checking manually, although you may have policy that prevents users from changing installed software.)

User Interface Theme

This policy allows you to lock down the user interface theme. If your company enforces a consistent look and feel across all PCs, including how a user's desktop may look, this policy allows you to enforce how the WindowSMART UI looks. Set this policy to Not Configured to allow the user to change the theme. Set this policy to Enabled to customize the main window background and window header color (some windows have a customizable header or background).

The main window background choices are Metal Grate (default), Lightning, Cracked Glass or No Texture. The window header/help about dialogue background choices are Green (default) and Blue.

If you set this policy to Disabled, then the main window background is set to No Texture and the header is set to Green.

Custom Support Message

This policy allows you to specify a 256-character custom support message. This is the same support message that can be customized using the enterprise management CLI, discussed earlier in this document. This custom support message, if defined, is shown in email alerts and Prowl/NMA notifications. The purpose of this message is primarily for end users. It should provide instructions to what action a user should take, such as providing an email address and/or a phone number instructing them to contact technical support or the helpdesk for assistance. A message such as, "For further help regarding this disk health alert, please contact the helpdesk by calling 1-888-555-1234 option 3 or by email at support@helpdesk.somecompany.com," fits comfortably within the 256 character limit, and clearly states appropriate actions the user can take. This limit is in place because both Prowl and NMA have 1024-character limits on their notifications and some WIndowSMART alerts can consume a lot of character space.

If this policy is Not Configured, you can use the enterprise management CLI to set it on individual PCs. If this policy is Enabled, you can specify the custom message (you must specify a message if the policy is enabled). If this policy is Disabled, a custom message is never used.

Emergency Backup when Disk Failure is Detected

This policy allows you to control whether or not an emergency backup is run if a disk failure is detected. In the event a disk raises the failure flag (TEC), you can have WindowSMART back up the data to a local drive or a network shared drive.

Since temperature-related attributes like Airflow Temperature can "fail" and subsequently "un-fail," you have the option of skipping the backup if a TEC condition arises, but that condition was on the Temperature or Airflow Temperature attribute.

You also have the option to run a third-party backup program, rather than letting WindowSMART handle the backup. At your option, WindowSMART can pass a list of failing disks by their physical drive numbers or their drive letters (or both) to the backup program.

Developer Diagnostic Debugging Upload

This policy allows you to control whether or not users may generate diagnostic debugging data, including debug longs, and upload it to Dojo North Software. The diagnostic logging collects information about the computer, including the operating system, type of disks installed, USB devices and Silicon Image controllers, as well as whether any installation problems were detected.

If the user has debug logging enabled, those logs will be included in the diagnostic collection.

Users are able to upload this data to Dojo North Software to submit a bug report. Users have the option of typing additional details into a text box along with the report. The report is first compiled into an encrypted zip file, which is encrypted with WinZip-compatible AES 256-bit encryption. The password is known only to Dojo North Software. The report is then sent via secure FTP (FTP explicit SSL/TLS) to provide an additional layer of security. If the FTP operation fails, the user is presented with the option to deliver the report via standard FTP instead.

If you leave this policy disabled, the default behavior described above applies.

If you do not want users generating or sending debug reports, you should disable this policy.

If you would like to allow users to generate the reports, but want to control where the reports are sent, enable this policy, and then define the FTP server, username and password. This allows you to route reports to an internal FTP server. You will not be able to read the reports, because they are encrypted. However, some administrators may prefer this approach to give the users the impression that the reports are being sent, rather than displaying a message to the user that you are blocking the function.