



## Solving Desktop Challenges in Healthcare

A  **DESKTOP AUTHORITY**® Vertical Whitepaper

# Solving Desktop Challenges in Healthcare

---

The last decade has seen huge changes in the healthcare industry caused by population demographics, introduction of new regulations, advances in technology, increased patient choice and higher energy and transportation costs. The effect of these changes has been felt in IT departments across all healthcare providers where there has been increased pressure to work more efficiently, roll-out new projects and initiatives, deliver software updates and provide greater mobility to healthcare professionals.

This paper will address some of the key challenges presented by Windows desktop management in a healthcare environment. ScriptLogic has a long track record of helping IT professionals in healthcare, and provides solutions targeted at the over-worked, under-resourced administrator with a wide variety of responsibilities. ScriptLogic's Desktop Authority allows administrators to address these challenges with a solution that is low in complexity yet high in value. Desktop Authority provides healthcare organizations the granular control they need of all Windows desktops and applications helping them to increase efficiency, meet compliance requirements, and enhance overall security.

## The Challenge of Windows Desktops

Management of Windows desktops presents many challenges, some of which are unique to environments such as hospitals and medical centers, and others which are seen across all Windows desktop-based enterprises. Tight budgets, high ratios of users to administrators and constant pressure to "do more with less" are common burdens within healthcare IT departments, coupled with the ever-increasing focus on regulatory compliance especially the Health Insurance Portability and Accessibility Act (HIPAA) in particular.

Some of the most frequently-voiced desktop management challenges from IT professionals working in healthcare include:

- Inability to provide workers with rapid access a set of applications, resources and data as they roam between many different workstations, based on a centrally-managed policy
- Compliance with HIPAA, especially providing centralized permissions management and access restrictions around patient records
- Poor tools for providing remote assistance to user desktops, either because they require that the administrator takes over the whole desktop, or because they lack functionality and performance
- Risk of users removing sensitive data using USB drives and removable storage media
- Rising energy costs, and pressure to reduce wasted uptime

## ScriptLogic's Desktop Authority

ScriptLogic's Desktop Authority allows healthcare organizations to effectively address these issues. It is optimized for the administrator who is over-worked and covers a wide variety of IT administration tasks, offering low complexity and high value. Desktop Authority provides healthcare organizations with centralized, granular control over all Windows desktops and applications, helping them to increase IT efficiency, meet compliance requirements, and enhance overall security.

In this document we shall highlight specific features within Desktop Authority that have been used by our many existing healthcare customers to drive down costs, improve efficiency and achieve regulatory compliance:

- 1) Provide a Secure, Consistent, Task-Oriented Desktop for Users as they Roam
- 2) Reduce User Logon Times
- 3) Protect Inactive and Unattended Desktops
- 4) Secure the Desktop Environment
- 5) Excellent Remote Assistance Functionality for one-on-one support
- 6) Reduce Energy Costs with Centralized Power Management

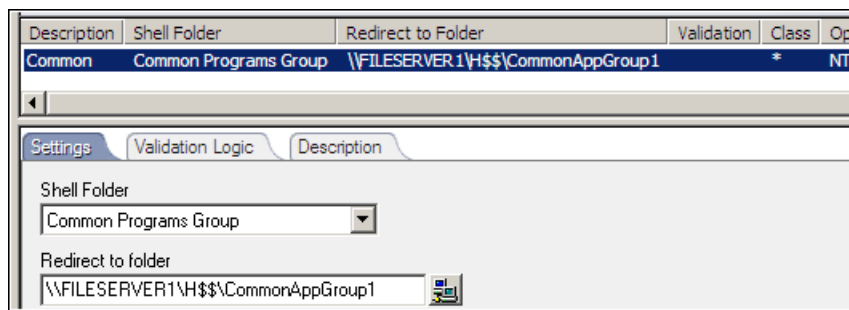
**Let's look in more detail at each of these features.**

### Provide a Secure, Consistent, Task-Oriented Desktop for Users as they Roam

Doctors, nurses and many other healthcare professionals roam between desktop locations all day. They need the ability to access important applications and resources the first time, every time. Additionally, they need a task-oriented workspace optimized for their requirements, no matter which workstation they are using.

Desktop Authority's comprehensive configuration options combined with its patented Validation Logic technology provides unlimited flexibility in providing a workspace optimized for each user, group, location and environment, as shown in the follow three examples.

**Example 1: Simplify and customize the applications available from the start menu and the desktop.**



**Example 2: Provide predefined sets of applications and data by redirecting common folders, such as the Common Programs group. Using Validation Logic, different sets of applications and data can be provided based on the user's group memberships, location, workstation, etc.**

### FOLDER REDIRECTION

Description	Shell Folder	Redirect to Folder	Relocation
Redirect IE bookmarks to user home dir	Favorites (IE Bookmarks)	H:\ShellFolders\Favorites	Copy
Redirect My Docs to user home dir	Personal (My Documents)	H:\Documents	Copy
Redirect desktop to user home dir	Desktop	H:\ShellFolders\Desktop	Copy

---

Settings | Validation Logic | Description

Shell Folder:

Redirect to folder:

Reset to Default

Copy any files that exist in the original folder

**Example 3: Redirect user's information to centralized data stores so it is always rapidly available, even as they move around each building and between sites.**

### SHORTCUTS

Description	Action	Location	Name
Remove Program Access and Defaults	Remove Shortcut	User Start Menu	Set Program Access and Defaults
Remove Windows Catalog	Remove Shortcut	All Users Start Menu	Windows Catalog
Remove Launch Outlook Express	Remove Shortcut	User Quick Launch Bar	Launch Outlook Express
Remove Windows Update	Remove Shortcut	All Users Start Menu	Windows Update
Create User Start Menu	Create Shortcut	User Start Menu	Company Documents
Create User Quick Launch Bar	Create Shortcut	User Quick Launch Bar	Company Documents

---

Settings | Validation Logic | Description

Action:   Overwrite

Shortcut Name:

Shortcut Location:

Target:

Target Arguments:

Start In:

Shortcut Comment:

Icon File:  Index:

Shortcut Key:  Run Window:

## Fast Logons

Many organizations rely on logon scripts or large numbers of Group Policies to centrally configure desktops. These are slow, difficult to maintain and require costly expertise. Using Desktop Authority eliminates the need for logon scripts, decreases the complexity that often comes with Group Policy, and can dramatically reduce logon times.

In recent customer situations we have seen examples where Desktop Authority has reduced logon times for typical doctors and nurses **from 2 minutes down to 25 seconds!**

Desktop Authority completely replaces complex logon scripts and vast numbers of Group Policies with centralized desktop configuration from an intuitive graphical interface.

**The Desktop Authority splash screen is shown for a few seconds as the user's desktop is configured and personalized, replacing complex and slow logon scripts**



## Centralize Desktop Inactivity Policy

HIPAA regulations mandate technical safeguards for access are implemented as stated under section 164.312 (a)(1) . Healthcare professionals working in a busy environment don't always have time to log out cleanly, especially if they get called away in an emergency. Inactive desktops expose a security risk, and can leave patients' medical records in the wrong hands. With Desktop Authority's Inactivity Timer, shown in Example 4 below, all inactive desktops (defined by absence of keyboard strokes or mouse movement for a specified duration) will Lock, Logoff, Shutdown or Restart as needed. Of course, Validation Logic ensures you can define different policies for different sets of users, and apply them based on user, group, location, time of day and so on.

**Example 4: Inactivity detection allows the administrator to specify patterns of user alerts and when to Shutdown/Restart/Lock/Logoff during different times of day.**

The screenshot shows the 'INACTIVITY' configuration window. At the top, there is a table with the following data:

Comment	Elased Time	Action	Sound	Timeout	Text
Logoff 9am-6pm	10	Logoff	5	5	Your workstation is idle. If you do not respond you will be
Shutdown after 6pm	10	Shutdown	10	10	Your workstation is idle and will be shutdown if you don't r

Below the table is a 'Detection hours' grid. The grid has columns for hours 1 through 23 and rows for days of the week. A blue shaded area covers the hours from 9:00 AM to 6:00 PM on all days from Sunday to Saturday. Below the grid, the time range is set to '12:00AM to 9:00AM'. There are two radio buttons: 'Don't Monitor Inactivity' (unchecked) and 'Monitor Inactivity' (checked).

Duration of inactivity before warning (in minutes): 10

User warning

Warning to display:  
Your workstation is idle. If you do not respond you will be to

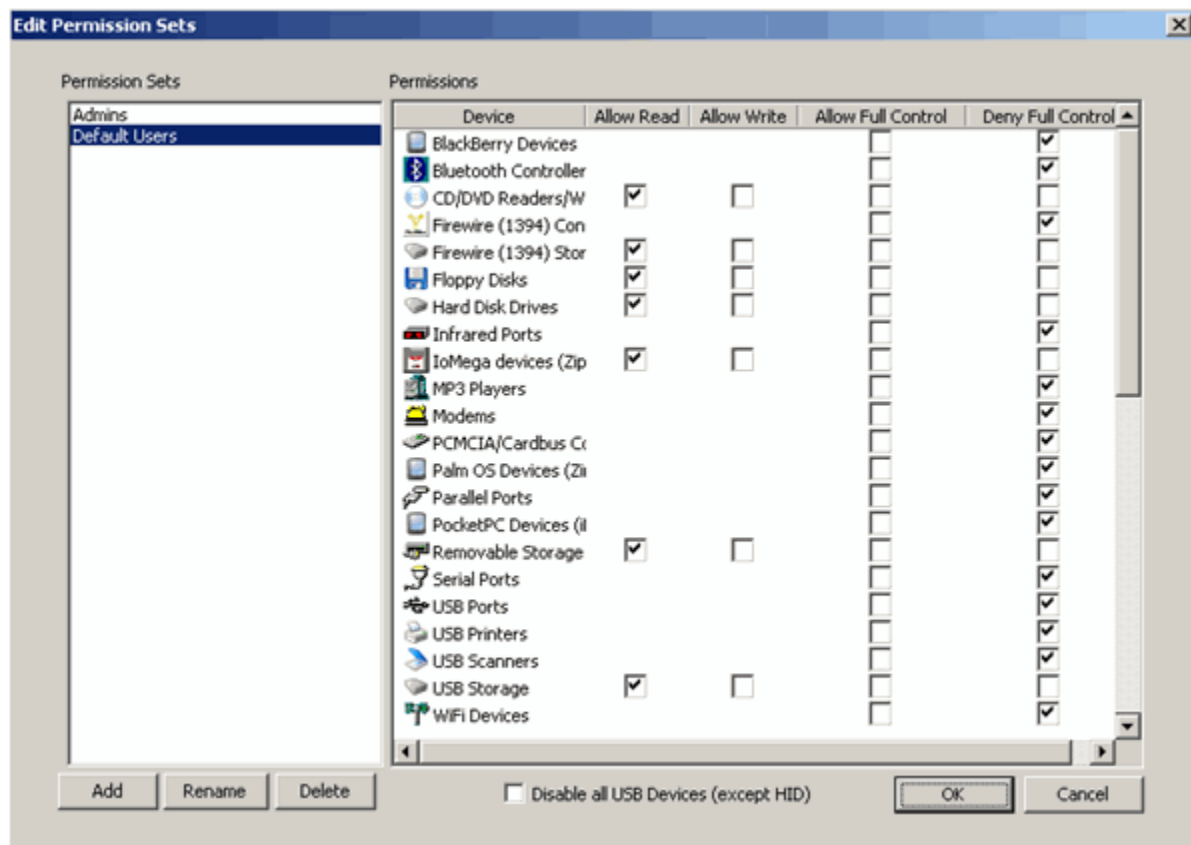
Sound to play:

## Secure the desktop environment

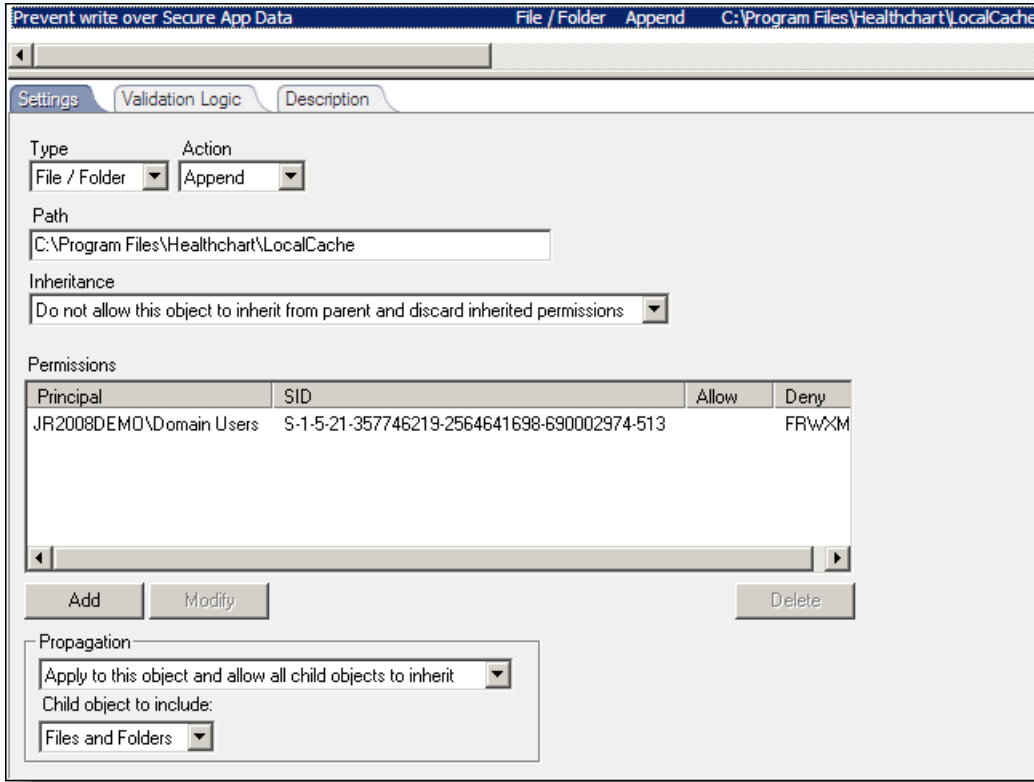
A very important aspect to healthcare compliance is avoiding data leakage. Unwanted removal of sensitive data is a huge compliance issue. And because the use of removable media devices has become one of the most widely used methods of storing data, certain measures need to be implemented to prevent this type of breach. Healthcare organizations need a system in place to prohibit or monitor the use of these devices. Copying data, introducing viruses, and installing illegal software on the company network are all issues that must be addressed, and Desktop Authority's USB & Port Security (shown in Example 5 below) tackles these issues head-on. With granular control over each device type, healthcare organizations can limit usability of certain devices to "read" but not "write" or allow users to "read" CDs or DVDs, but not "burn" them.

This granular control also allows you to set file permissions, clean out temporary folders on logoff, use Security Policies and keep desktops patched. The following examples demonstrate several features of Desktop Authority used to secure the desktop.

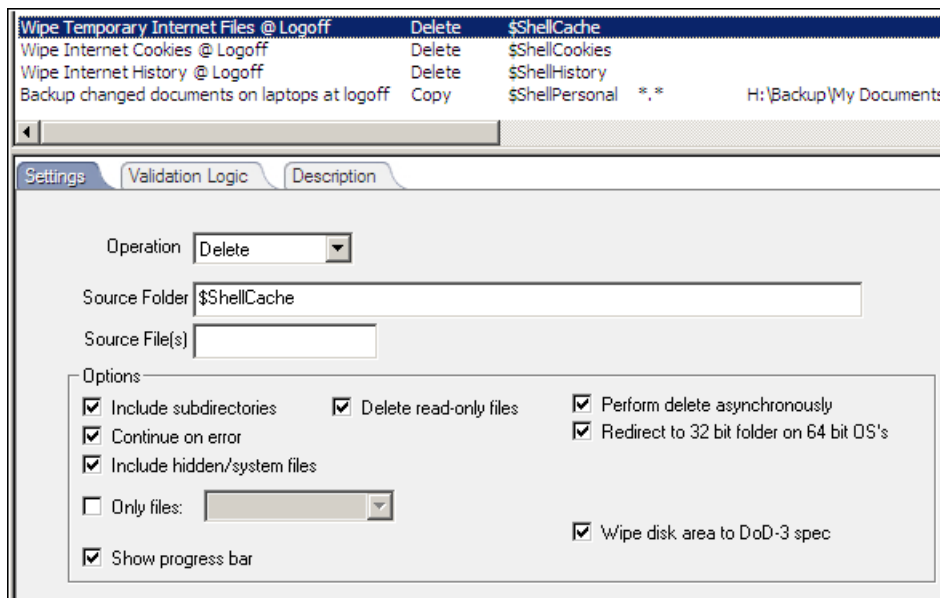
**Example 5: Desktop Authority Provides policy-based lockdown of USB, storage and communication devices with multiple levels of security to allow complete access or denial to certain device types.**



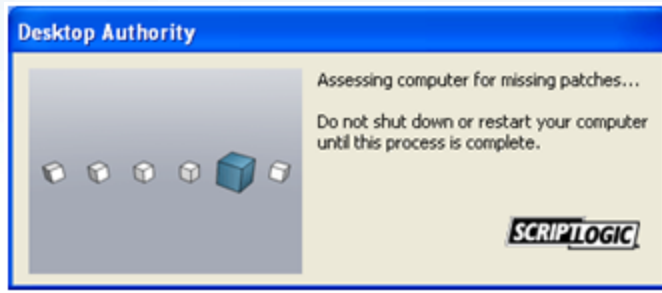
**Example 6: Prevent users from overwriting key application configuration information or data files by customizing file permissions to critical directories**



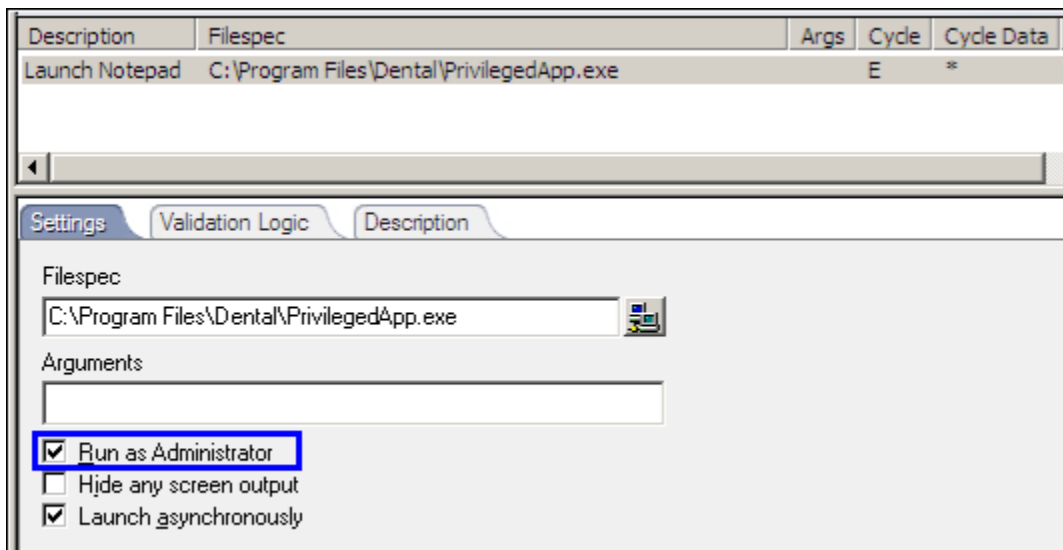
**Example 7: Prevent opening security holes for your web based applications by securely wiping browser information, including temporary files, history and browser cookies, when the user logs off.**



Example 8: Scan your users' desktops for missing patches for both Microsoft and select third-party products.



Example 9: Allow users that do not have administrative privilege on their local desktops to use applications and access resources that require a higher level of privilege.



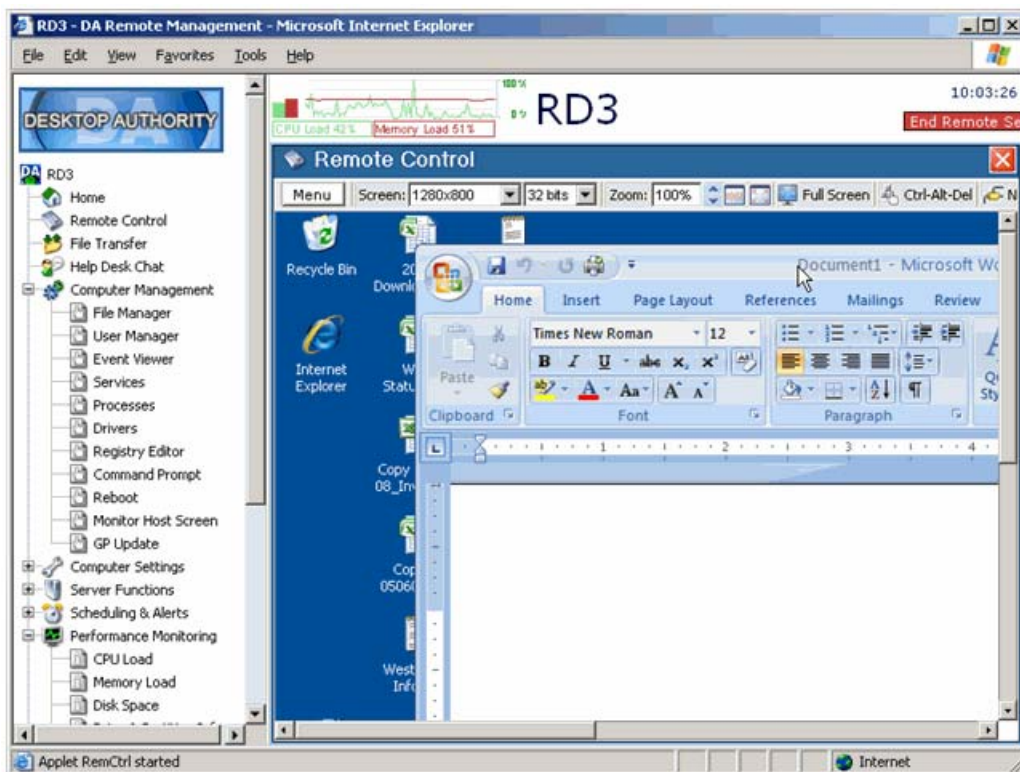
## Advanced remote assistance for individual users

The Remote Management function in Desktop Authority, shown below in Example 10, provides best-of-breed remote assistance capabilities for individual user support.

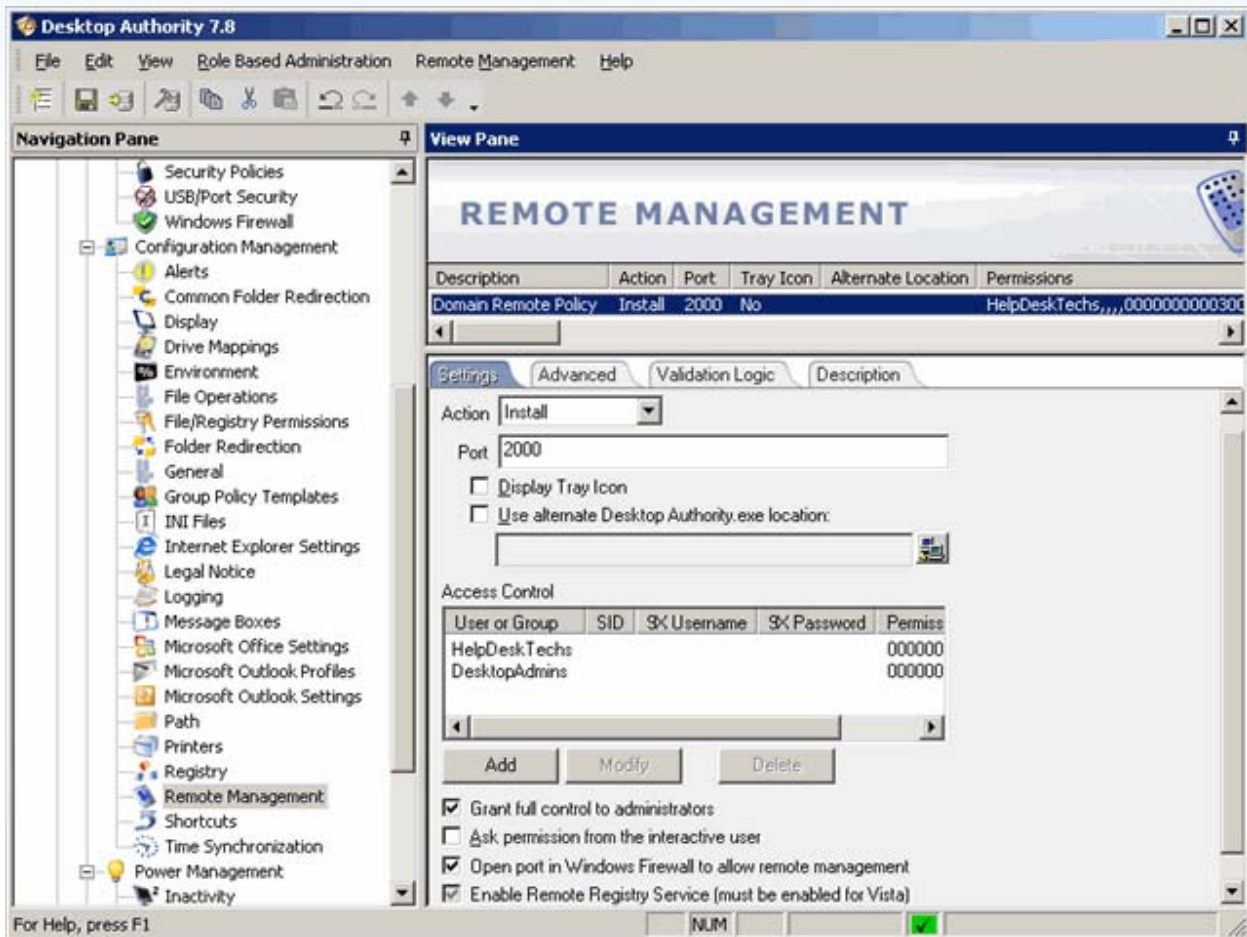
Many situations can be diagnosed and fixed without disturbing the user at all. For example, runaway processes taking 100% of CPU cycles, or services that have stopped. The administrator can explore the file system, registry and applications that have been installed, and transfer files to and from the desktop. They can run a remote command prompt to run instructions directly on the remote desktop, and then review performance statistics and health analysis. If the need to interact with the user arises, a chat function is available, or they can monitor the user's screen. And if necessary, they can take over the remote desktop completely and even blank the remote user's display if they need to perform privileged tasks.

Multiple levels of administrator privilege are provided so that only approved administrators can carry out privileged operations like shadowing a desktop, or deleting files, and the user's permission is usually required before the support staff see the contents of their screen.

**Example 10: Desktop Authority's best-of-breed remote assistance capabilities go far beyond traditional remote control and gives administrators complete authority over the remote desktop, including background access to the file system, services, programs and system status without interrupting the end user.**



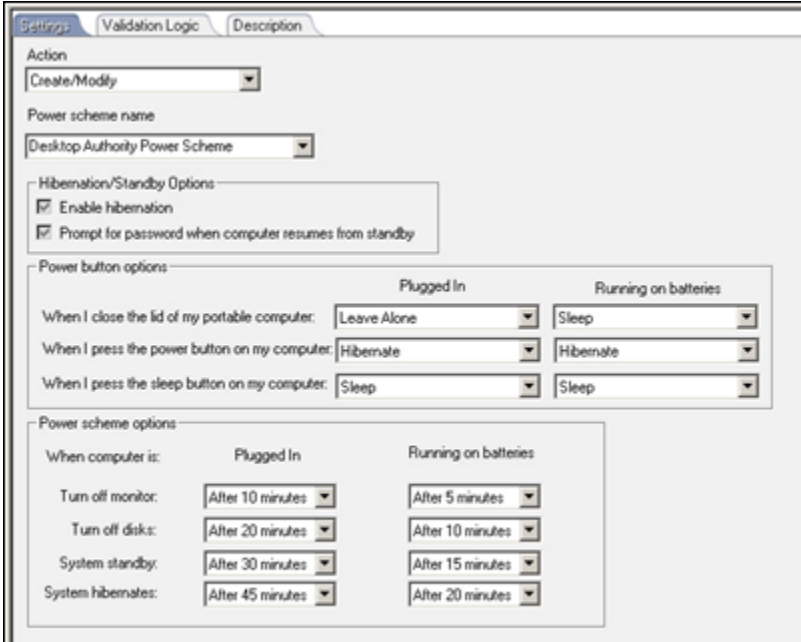
Example 11: Desktop Authority gives the administrator complete control over how the remote management agent is deployed to desktops, including configuration of role-based privileges for junior administrators.



## Power Management

The Environmental Protection Agency estimates that 58% of the time, machines are left inactive throughout the business day and only 38% are actually turned off after hours. And most healthcare organizations simply do not implement power management because they do not have the granular ability to manage it. Desktop Authority's power saving settings help alleviate this wasted energy and give more comprehensive control. The Power Management element allows administrators to easily create, modify, or remove Windows power schemes, and provides power saving options such as Standby/Hibernate and turning off monitors and disks. This setting makes it possible for organizations to ensure participation in power saving programs across the organization and in turn, save energy and money.

**Example 12: Centralized management of power savings policies provides complete control over desktop behavior. Different policies can be targeted at different desktops and groups of users based on their needs and work patterns.**



The screenshot shows the Windows Power Management settings window for a Desktop Authority Power Scheme. The window has three tabs: Settings, Validation Logic, and Description. The Settings tab is active. The Action is set to 'Create/Modify'. The Power scheme name is 'Desktop Authority Power Scheme'. Under Hibernation/Standby Options, 'Enable hibernation' and 'Prompt for password when computer resumes from standby' are both checked. The Power button options section has two columns: 'Plugged In' and 'Running on batteries'. For 'Plugged In', the actions are: 'When I close the lid of my portable computer: Leave Alone', 'When I press the power button on my computer: Hibernate', and 'When I press the sleep button on my computer: Sleep'. For 'Running on batteries', the actions are: 'When I close the lid of my portable computer: Sleep', 'When I press the power button on my computer: Hibernate', and 'When I press the sleep button on my computer: Sleep'. The Power scheme options section also has two columns: 'Plugged In' and 'Running on batteries'. For 'Plugged In', the actions are: 'When computer is: Turn off monitor: After 10 minutes', 'Turn off disks: After 20 minutes', 'System standby: After 30 minutes', and 'System hibernates: After 45 minutes'. For 'Running on batteries', the actions are: 'When computer is: Turn off monitor: After 5 minutes', 'Turn off disks: After 10 minutes', 'System standby: After 15 minutes', and 'System hibernates: After 20 minutes'.

## Other Functionality in Desktop Authority

The Desktop Authority family of products reduces the cost of managing the Windows desktop and eases the administrator's burden in supporting the desktop lifecycle by enabling administrators to proactively control, inventory, secure, and support desktops from a central location. This solution provides enterprises the granular control they need over Windows desktops and applications to increase IT efficiency, meet compliance requirements, and enhance security. Desktop Authority reduces the total cost of ownership for Windows desktops by reducing help desk calls, managing power more efficiently, restricting the use of removable storage, and keeping desktops patched and secured.

Desktop Authority provides the administrator with a complete set of desktop configuration features for all Windows clients including Vista. These include:

- Graphical interface which eliminates the hand-coded logon scripts
- Software and Application Installs and Updates
- Patch Management and Distribution
- Spyware Detection and Removal
- Advanced Remote Assistance
- Lock down and restrict USB and other ports
- Manage the Windows Firewall
- Centralized Power Management
- Manage connections and mappings to file servers
- Add and Remove Printers
- Manage desktop and menu shortcuts
- Manage and create Outlook profiles

Key Benefits of Desktop Authority:



**Save Time:** Implement a desktop management solution that is simple to install and does not require the purchase of additional consulting services.



**Stay Secure:** Lock unattended workstations. Control and audit activity on external drives and avoid having patient information, passwords, and other important records removed from your network.



**Reduce Cost:** Lower energy costs by implementing power management option such as standby/hibernate and turning off monitors and disks.



**Be Compliant:** Grant granular access rights to users and administrators based on security boundaries.



**Gain Control:** Customize desktops and applications based on date, time, location, OS version and many more desktop and user properties.

## Conclusion

With regulatory compliance issues on the forefront of all healthcare agendas, it is essential that certain safeguards be implemented to protect sensitive data. Tackling these compliance concerns, as well as allowing the administrator to “do more with less” addresses the never-ending problems that most healthcare organizations have in IT: manpower and budget. With ScriptLogic’s Desktop Authority, administrators of all skill levels now have the necessary tools in place to effectively secure sensitive information, provide quick access to applications for end-users, troubleshoot desktops remotely, and help reduce energy costs. So whether it’s HIPAA compliance mandates or fundamental desktop management concerns, Desktop Authority will simplify, automate, and centralize the desktop lifecycle from beginning to end.

## About ScriptLogic

ScriptLogic Corporation is a leading global provider of systems lifecycle management solutions for Microsoft Windows-based networks. ScriptLogic’s award-winning suite of Desktop management software, Server management software, Active Directory management software, and Help Desk software products help empower network administrators to proactively save time, increase security, and maintain regulatory compliance. More than 23,200 customers use ScriptLogic solutions to manage approximately 5.7 million desktops and 138,000 servers. ScriptLogic solutions benefit any size network in any industry. ScriptLogic, headquartered in Boca Raton, Florida, is a wholly owned subsidiary of Quest Software, Inc. (Nasdaq: QSFT). Reach ScriptLogic at (561) 886-2400 or on the Web at <http://www.scriptlogic.com>.

### Resources

More information on the ScriptLogic solutions listed in this document, as well as a 30-day fully-functional evaluation are available on our website.

- Desktop Authority – [www.scriptlogic.com/da](http://www.scriptlogic.com/da)
- Healthcare Vertical Solutions – [www.scriptlogic.com/healthcare](http://www.scriptlogic.com/healthcare)
- HIPAA Compliance with ScriptLogic – [www.scriptlogic.com/hipaa](http://www.scriptlogic.com/hipaa)