

SOLUTIONS



DESKTOP AUTHORITY® AND MICROSOFT SYSTEMS MANAGEMENT SERVER

A ScriptLogic
Product
Positioning
Whitepaper

NICK CAVALANCIA

INTRODUCTION

Enterprise network administrators often express a need for a solution that manages every PC on their network. The solution needs to not only collect inventory information for improved decision-making, but must also allow administrators to centrally configure workstations and servers. If the solution does its job well, a user's PC should behave like a network appliance in which desktop configuration is achieved using the enterprise management solution.

A number of companies have developed products to provide such a solution; in this paper two products are compared: Microsoft Systems Management Server (SMS) 2003 and ScriptLogic's Desktop Authority®.

When evaluating these enterprise management products, customers often notice that SMS and Desktop Authority offer some overlapping features. Indeed, both assist with network information collection and software deployment. However, SMS and Desktop Authority meet enterprise management needs from very different perspectives, and are more complementary than competing.

This white paper demonstrates that Desktop Authority provides all the functionality needed to administer the vast majority of enterprise networks, and that in some cases, the granularity of information collected by SMS (as well as its built-in remote control feature) makes it an excellent complement to Desktop Authority. Three key areas of comparison are covered: Product Architecture, Client Management Features, and Cost of Ownership.

EXECUTIVE SUMMARY

SMS 2003 and Desktop Authority overlap in some functional areas, but actually have quite different areas of focus within an overall enterprise management system.

SMS 2003 has superior functions focused solely around application, hot fix and Service Pack deployment. Using SMS for desktop administration and configuration, however, requires skilled and trained administrators to spend considerable time writing and testing scripts.

The strengths of Desktop Authority are its short learning curve, instant access to all common desktop administration

functions, highly flexible Validation Logic, and extensive Remote Management capabilities.

Desktop Authority is extremely cost-effective, requires no formal training to use, and is suitable for companies of all sizes. Ideal candidates for Desktop Authority are organizations that need extensive network management, inventory reporting, and enhanced software deployment capabilities. Organizations that can justify the higher purchase and setup costs of SMS should also consider Desktop Authority.

This document provides a comparison of the features found in these products, and attempts to highlight areas where the capabilities of the products differ significantly. Throughout this whitepaper, comparison grids are used to demonstrate these concepts visually. **The comparison grid follows this legend:**

COMPARISON LEGEND

	Supported feature of the product. No scripting is required.
	Supported feature of the product. The product's infrastructure was designed to facilitate this task, but scripting will be required.
	The product could conceivably be used to facilitate this task, but probably isn't the best solution. A great deal of scripting will be required and reliability and/or performance may be less than adequate.
	The product does not natively support this task or feature.

This section compares the architectures of SMS 2003 and Desktop Authority, focusing on the client operating systems supported, the methods used to discover information about clients, and the location and storage requirements for the collected information.

Which Operating Systems are Supported?

SMS 2003 and Desktop Authority both require a Windows NT 4.0 or Active Directory domain. Typically, Desktop Authority is installed on a domain controller (note: installing Desktop Authority to a domain controller is not a requirement). Generally, SMS 2003 is installed on a dedicated standalone, or member server, and requires an available SQL server to store configuration information. This SQL server is generally installed on the same physical computer, but can reside on a separate machine, if required. SMS 2003 must be installed on a Windows 2000 SP3 or higher server, but is compatible with NT 4.0 or Active Directory domains.

SMS 2003 is optimized to manage Windows 2000 and higher clients using its Advanced client software. Windows NT 4.0 SP6a and Windows 98 clients are still supported with the Legacy SMS client software, but certain new SMS 2003 features such as roaming are not available. Since Desktop Authority runs on the network's domain controllers, its management subdivisions closely follow the NT or Active Directory Domain structure. The SMS 2003 architecture is subdivided based on IP Subnets or Active Directory Sites.

Discovering Your Enterprise

The task of deploying the SMS 2003 client software is divided into two processes: Client Discovery and Client Installation. Client Discovery is the process by which SMS locates resources on the network, and Client Installation is the process by which a client agent is installed on the computer to be managed.

Client Discovery is accomplished in several ways with SMS: Network Discovery, Logon Discovery, and Active Directory Discovery. With Network Discovery, SMS polls NT Domains, IP subnets, SNMP-enabled devices, such as routers and switches, and Microsoft DHCP Server databases to generate a list of detected subnets and resources on the network. This list of discovery records is stored in the SMS database on a specified interval, and includes both Windows and non-Windows computer systems, and IP devices, such as routers and printers. SMS also can add a discovery record to the SMS database when a client computer runs a specific script (possibly at logon or system startup). The new SMS 2003 Active Directory Discovery method downloads all computer objects, OUs, and users accounts into the SMS database on a regular schedule; in large environments, the scope of Active Directory Discovery can be restricted with LDAP queries that target only specific containers. Because Desktop Authority collects all information and configures its clients at logon and logoff, it doesn't require a discovery process.

Both SMS and Desktop Authority support automatic installation of their respective clients during the logon process. They use the same basic method of bypassing the low-rights user problem; the server logs onto the client and installs the agent remotely, using an administrative account. The SMS Client Software generally is installed on all servers and workstations; the Desktop Authority client software generally is installed only on those desktops that are to be centrally managed. The SMS 2003 Advanced Client installer is Windows Installer-based (MSI) so it can be installed using Group Policy as well as by system startup script/logon script.

SMS also has a Client Push Installation feature that detects new NT/2000/XP/Server 2003 computers as they are added to the SMS database and remotely installs the SMS client without a user logging in or logging off. This is very handy for servers or in environments where users suspend their computers at night, or never log off and back on. An administrator can enable or disable Client Push Installation for workstations, servers, or domain controllers. Note that Client Push Installation is not available for Windows 98 computers due to limitations of the operating system. Since Desktop Authority performs its desktop management functions during the logon and logoff processes, a Client Push Installation feature is not necessary.

Discovery and Client Installation

Feature	Desktop Authority	SMS
Network Discovery	✗	●
Logon Discovery	✗	●
Logon Client Installation	●	
Remote Client Installation (logon not required)	✗	●
Automatically Modifies Logon Scripts	●	
Client Rollout is controlled with Validation Logic	●	◐

Where Do You Keep Your Data?

Both SMS and Desktop Authority are database-driven. With SMS, all available information about servers and workstations, including hardware and software inventory data, is stored in the SMS database hosted by SQL Server. Everything that SMS does is related to this discovered data in some way. Likewise, all of Desktop Authority's systems management instructions are stored first in a centralized SQL database and then are generated as files on the network's domain controller servers.

SMS 2003 offers web reporting functionality with over 140 built-in reports that cover everything from computer hardware configuration to software update compliance. New custom reports can be created by anyone with experience writing standard SQL statements. Desktop Authority utilizes over 100 built-in reports with the ability to also generate custom reports.

Architecture Comparison

Design / Platform Support	Desktop Authority	SMS
Runs on Windows NT 4.0, Windows 2000 and 2003 servers	●	●
Requires SQL Server / MSDE	●	●
Manages all 32-bit Windows clients – Windows 95 through XP	●	●
Manages all 16-bit Windows clients – Windows 3.1, WFW 3.11	✗	●
Architecture based on NT or Active Directory domain structure	●	✗
Architecture based on IP or IPX subnets	●	●

CLIENT MANAGEMENT

This section looks at the features that each product offers to centrally configure workstations. Focus is on the management areas of desktop configuration, remote control, inventory logging, and software distribution.

Defining your Desktops

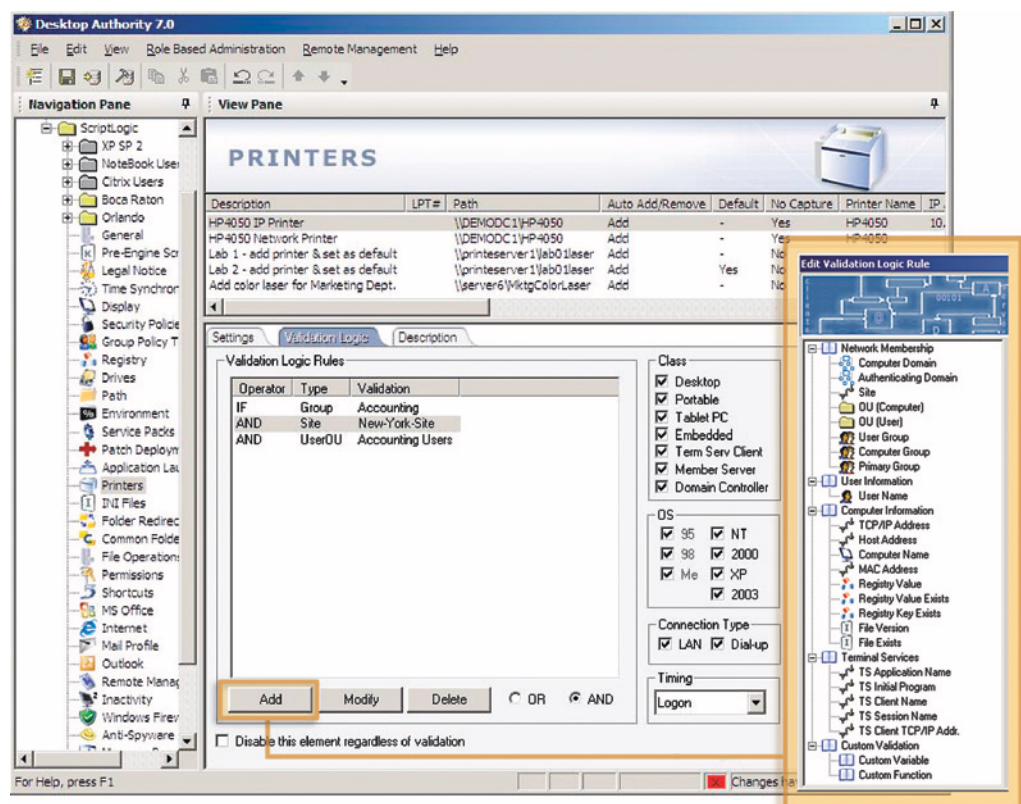
It may be surprising, but SMS 2003 actually provides very few out-of-the-box client configuration capabilities other than the patch management functionality. SMS is intended mainly as a platform or infrastructure product; almost all client-side changes must be done with custom-written scripts deployed using the SMS Software Distribution feature. Scripts must be researched, developed, tested, piloted, and finally moved into production, which means that to truly benefit from an SMS implementation, one or more skilled scripters and testers is required. From a desktop configuration perspective, SMS could be described as a development platform which trained and skilled administrators can use to generate scripts that perform specific administration tasks.

SMS allows administrators to target computers by creating collections in the SMS database. A collection can contain a list of machines directly specified by the administrator, or it can be based on a query to the SMS database. Collection memberships are evaluated on a regular basis, which allows an action to be taken on machines when they first meet particular criteria. For instance, if a particular application were advertised to a collection of all machines with 256 MB of RAM, SMS would not install the application on a PC with 128 MB of RAM. If that same PC were later upgraded to 256 MB of RAM, the computer would become a member of that collection, and SMS would install the application. Similarly, Desktop Authority can accomplish the same end result (only launching an application on machines

with 256MB of RAM) without the need for a collection using their exclusive Validation Logic along with Custom Validations, because the determination of whether the client meets the criteria to launch an application is performed at logon, rather than based on a potentially outdated value in a configuration database.

Desktop Authority provides a wealth of out-of-the-box desktop configuration options including network drive and printer mappings, Internet Explorer settings, Microsoft Office setting standardization, Outlook Profile Management, File Management, and many more. Each configuration element includes Validation Logic to ensure that each desktop is configured correctly. Validation Logic empowers the administrator to apply a specific setting to users or computers matching specific criteria, such as mapping a printer for members of a specific domain group or OU, or even sending software to only those computers with a certain speed processor. The best part is that all of these changes can be made easily within the Desktop Authority Manager interface – without requiring the administrator to do any scripting. Desktop Authority's Validation Logic provides an impressive number of options (as shown in Figure 1) covering Class of machine, OS, connection type, and 25 other criteria.

Figure 1:
Validation Logic



Desktop Authority isn't just limited to a single selection criteria. Validation Logic supports the use of wildcard values to extend the scope of a particular selection. For example, a TCP/IP Address value of 192.168.1.* would allow any machine on that IP subnet to pass the validation and accept the configuration change specified. When required, multiple criteria can be combined with AND/OR logic for each configuration entry within Desktop Authority, resulting in an exponentially granular selection.

Desktop Authority and SMS 2003 have similar targeting capabilities, but in practice they are quite different. With SMS, the validation is run from the database on the server

rather than evaluated on the client at run time. This has the advantage of allowing the administrator to immediately see and report on the targeted population of computers for a particular deployment, but is only as current as the last time the client reported its inventory data. Desktop Authority's Validation Logic will act always upon the current state of the machine, but the administrator cannot report necessarily on the target population ahead of time. The benefit of evaluating clients at logon time is that there is never the issue of an out-of-date database, so immediately after a configuration change is defined within Desktop Authority; clients logging on will implement the change.

Client Management	Desktop Authority	SMS
Action can be taken based on hardware or software	●	●
Natively maps network drives and printers	●	○
Natively supports Internet Explorer and MS Office Configuration	●	○
Natively supports MS Outlook Profile Management	●	○
Natively supports Security Policy Management	●	◐
Natively supports Desktop Shortcut Management	●	◐
Natively supports File System Management	●	○
Natively supports Displaying Logos and Messages at Logon	●	○
Natively supports Registry and File Permissions Management	●	◐
Natively supports Password and Drive Space Warnings	●	○
Natively supports Modifying Registry Settings	●	◐
Natively supports enterprise Anti-Spyware Management	●	○
Natively supports enterprise Patch Management	●	○
Natively supports Power Management	●	○

Remotely Accessible Clients

SMS includes a remote control product that allows an administrator to view the screen and control the mouse and keyboard of a remote Windows computer. In addition, the Remote Control client has file transfer and remote execute functionality, even on Windows 98 clients with file sharing turned off. SMS Remote Control also supports an Ask User for Permission requirement. Remote Control installation is either enabled or disabled on a site-wide basis and cannot be limited to workstations only or

according to some other company-specific requirement without performing custom scripting or configuring additional SMS sites. SMS 2003 remote control can be configured to not install on computers that support Microsoft's Remote Desktop technology – this includes Windows 2000 Server, Windows XP Professional, and Windows Server 2003 systems. For these computers, SMS defaults to the built-in Remote Desktop and Remote Assistance functionality.

Desktop Authority's remote client is not referred to as a Remote Control client because Desktop Authority's client does so much more than just remote control, so it is referred to as a Remote Management client. **In addition to basic remote control**, Desktop Authority's remote client provides administrators with comprehensive management of desktops including:

- > Services, Processes and Drivers
- > Edit File Systems and the Registry
- > Installed Applications

- > Open Files, DLLs and Registry Keys in use
- > Tasks and Alerts
- > Remote Reboots

Desktop Authority does not require a specific application to remotely manage desktops; as any standard java-enabled browser can be used. In addition, security levels can be established to limit specified groups of administrators to specific functions with Desktop Authority's Remote Management client. Figure 2 shows the Desktop Authority remote client managing a desktop. Notice the comprehensive

list of management capabilities at the left in addition to remotely controlling the desktop.

Desktop Authority's client also can be selectively deployed – using the same validation logic used for desktop configuration, administrators can choose which desktops and servers will have the remote client installed.

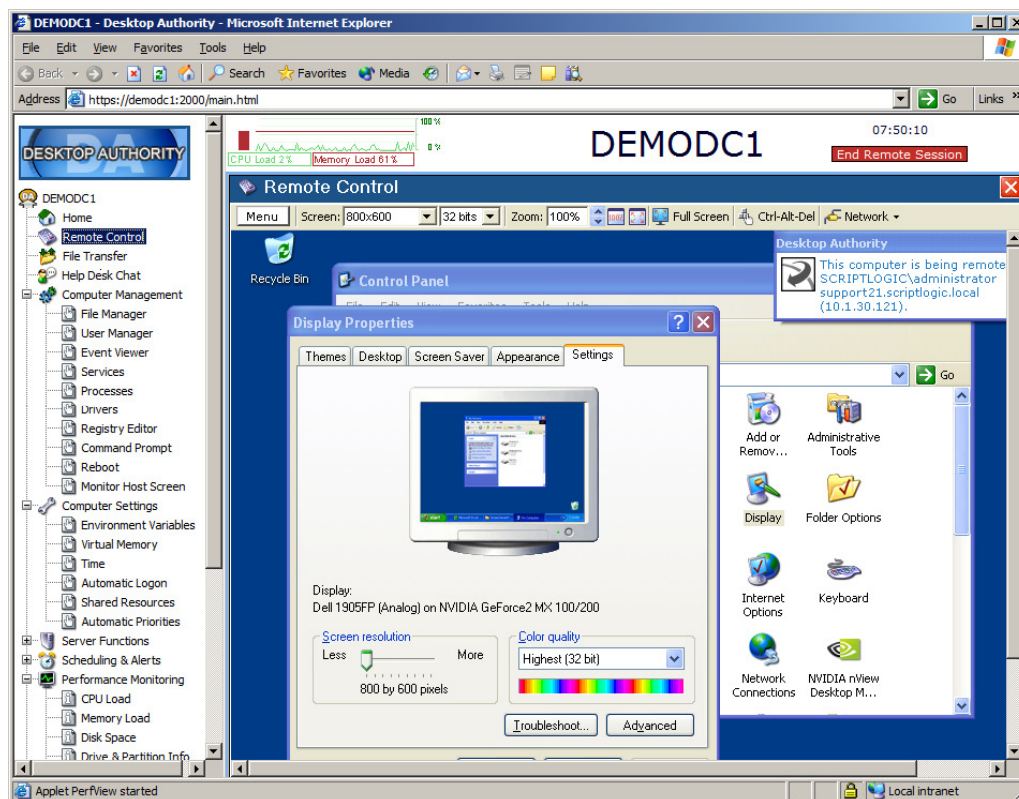


Figure 2: Desktop Authority's Remote Management Client

Inventorying your Desktops

One of the most useful features of SMS is the inventory database. Hardware and software information for all Windows computers on the network – including servers – is available for ad-hoc query and reporting, or for taking administrative action such as running a script. Desktop Authority utilizes two databases – one for storing the desktop configurations

and a second for reporting. The configuration database is used when changes are made to a configuration element within the Desktop Authority Manager. The reporting database would be the closest equivalent to SMS, in that it contains hardware and software inventory information.

Software Distribution

One of the most significant capabilities that a systems management infrastructure enables is software distribution. With automated software distribution, an enterprise can cut the immediate costs associated with technicians visiting and manually installing new software and patches on each computer involved in a rollout. In addition, centralized deployments help to ensure that each corporate computer is configured identically, which decreases support costs after a rollout is complete.

Both SMS and Desktop Authority support software distribution through MSI packaging. Packages can have user interaction, but more often are configured for quiet or silent installs, meaning that the package is pre-programmed with all of the required information. In an SMS environment, packages are often built using the SMS Installer, which is actually a simple programming language entirely geared toward the task of installing applications on a computer. SMS Installer creates a package by compiling all of the files and configuration information necessary to complete an install into a single executable. SMS Installer is included with SMS and is reasonably good at scripting most installations. Desktop Authority does not include a free packaging tool like SMS Installer, but does fully support third-party products such as Wise Package Studio or Install Shield AdminStudio. Also, many vendors now provide their setup programs in the MSI (Microsoft Installer) format, which is inherently scriptable and thus reduces the need for SMS Installer repackaging.

Desktop Authority provides a growing library of supported install scripts for common applications such as anti-virus suites, Adobe Acrobat, and Internet Explorer. Many Desktop Authority-provided install scripts support packages that require a second administrative logon after a reboot, such as Internet Explorer 6. Microsoft provides no such repository for install scripts optimized for SMS. While Microsoft does offer notes on how to script installs of many of its own products, including those that require an administrative logon after reboot, they generally rely on the system administrator to actually write and test the script.

For example, when installing an application that was accomplished in two sections (with a reboot in the middle), an SMS script would have to be written to use the Elevated Rights Deployment tool available in the SMS 2003 Feature Pack. When properly configured, this tool performs the actions required after the reboot using administrative rights. Desktop Authority would handle the same scenario with the ScriptLogic service performing the first part of the install and starting a hidden instance of Explorer after the reboot to process the second half of the install under the context of the local Admin. This prevents the need to perform registry modifications and a logon and logoff to complete the install.

Both SMS and Desktop Authority offer a large variety of software deployment options to the system administrator. Both platforms can run install scripts that require administrator rights, even if the currently logged-on user is not an administrator. In addition, while the implementation differs somewhat, both can distribute software based on system configuration data, such as the presence of file or hardware information.

SMS can install software without a user ever logging on to a computer; Desktop Authority does not support this feature because installation instructions are not scheduled, but performed at logon. SMS also allows user-initiated optional software installations via a control panel applet or Systray icon, which Desktop Authority does not support.

Desktop Authority supports running applications at logon, logoff, or shutdown. To ensure these three events occur when needed, Desktop Authority employs an inactivity timer. This locally running application watches for the presence of keyboard and mouse movement. Specific times can be monitored and administrators have the option of logging off the user, restarting the machine, or locking the desktop. This too can selectively be done using Validation Logic. By forcing a logoff or shutdown/restart following a period of inactivity, Desktop Authority can trigger deployment of one or more applications.

SMS 2003 supports MSI source tracking functionality. A common problem with Windows Installer applications is that they often require access to the original media when they are patched, repaired, upgraded, or uninstalled. SMS can migrate user computers from the original install locations of applications (generally a server that is old or doesn't exist anymore, or a local CD-ROM drive when the user does not have the compact disc) to the SMS distribution points. As the SMS distribution points are created/moved/deleted, the clients update their MSI source location information automatically.

For low-bandwidth users, SMS supports drizzle-based deployments using a technology called Background Intelligent Transfer Services (BITS). This technology allows software to be slowly downloaded to a local cache on a machine before it is executed. The download process supports checkpoint-restart and is bandwidth aware to provide compatibility with intermittent and slow connections, respectively. This technology is also useful for packages or scripts that are run on clients on a regular basis. SMS can automatically cache such packages on client computers and run them locally rather than always having to download them from across the network. SMS also allows administrators to specify particular Active Directory Sites or IP subnets as local or remote boundaries. For each advertised program, the SMS administrator can choose the behavior for clients that are local and clients that are remote. By default, local clients

install applications directly from the distribution point and remote clients do not install the application at all, but rather wait until they are local. These behaviors can each be changed to Download and Run or remote clients can be set to Run the program directly from the Distribution Point.

In addition to software distribution, Desktop Authority includes an optional Patch Deployment for Desktops option that downloads, distributes and deploys Microsoft patches for both its Operating Systems and applications. This functionality, combined with Desktop Authority's exclusive Validation Logic gives administrators maximum control over the patch deployment process.

Software Distribution

Feature	Desktop Authority	SMS
Supports Software Distribution	●	●
Includes a Packaging Tool	✗	◐
Supports Third-Party Packaging Tools	◐	◐
Provides Supported Install Scripts	●	✗
Includes Patch Management	●	◐
Installs Software with Admin Rights	●	●
Installs Software based on Computer Configuration	●	●
Supports installs at Logon and Logoff, and Shutdown	●	●
Supports installs based on a schedule (e.g.: start at 6pm)	◐	●

READY FOR WINDOWS XP SP2

SMS 2003 can be used to automatically roll-out Windows XP Service Pack 2 using the standard package definition file mechanism that SMS uses for all service packs and hotfixes. Desktop Authority too has the same ability to roll out Windows XP SP2 using its Application Launcher, but Desktop Authority also provides the administrator with options to centrally configure SP2's security enhancements.

The biggest concern for corporate users deploying SP2 is the Windows Firewall. With the default setting of an enabled firewall, all remote access to your Windows XP-based workstation is blocked. Desktop Authority has built-in support to open and close ports blocked by the Windows Firewall, as well as a custom script to enable (or disable) the Windows Firewall.

COST OF OWNERSHIP

This last section highlights some areas that compose the cost of owning SMS and ScriptLogic: support, licensing models, and pricing.

Support Options

The first level of support should be your own staff. Supporting SMS requires classroom training and generally requires the assistance of Microsoft Consulting Services to get things up and running. Desktop Authority, on the other hand, requires neither classroom training, nor consulting to implement.

There are several support options available for both SMS and Desktop Authority beyond your own staff. Each software product has a collection of FAQs, Whitepapers, and Knowledge Base articles available on the company's website. In addition, each product can take advantage of the thriving

System-Scripting communities on the web, and of the growing SMS and KiXtart-specific communities. Microsoft offers toll-free 24x7 telephone support for SMS on a Pay-Per-

Incident basis; the fee is waived if a bug in the product caused the issue. ScriptLogic offers toll-call telephone support from 7 am to 7 pm EST, Monday through Friday.

Support Options	Desktop Authority	SMS
Online Support: Web site, FAQs, Whitepapers, KB articles	●	●
General scripting and product-specific communities	●	●
Standard telephone support	7am – 7pm	24 x 7
Annual support contracts	●	○
Fee-based support incidents	●	●

Licensing and Pricing

Both products require that a Client Access License (CAL) be purchased for each computer using the product. In addition to CALs, SMS, like other BackOffice products from Microsoft, requires the purchase of a minimum of one SMS Server License and one SQL Server License per primary site server, however SMS 2003 now supports an SMS 2003 with SQL Technology license, which offers a deep discount on the SQL Server product, but has the soft restriction that the copy of SQL Server is to be used only to host the SMS database.

If the enterprise architecture calls for more than one primary site (1000+ computers in a single location), additional SMS 2003 with SQL Technology licenses are required. Secondary sites (fewer than 1000 computers in a single location) no longer require additional SMS server licenses, though SMS client

CALs are still required. Note that many larger companies with a Microsoft Enterprise Agreement are already paying for SMS client licenses but are not using them.

Unlike SMS, Desktop Authority licensing is based solely on the number of desktops (not users) to be managed and only optionally requires licenses for SQL Servers if you choose not to use MSDE to store your data, or servers hosting Desktop Authority services. A maintenance plan is available from ScriptLogic for two or three additional years that includes product updates and priority technical support at an additional cost. Nonetheless, SMS 2003 can be roughly four to five times more expensive than Desktop Authority in similar environments, even with the three-year Desktop Authority maintenance option factored in.

SUMMARY

SMS 2003 and Desktop Authority each have a place in a well-managed Windows environment. While there is overlap in features between the products, their core strengths are quite complementary: SMS features a robust software distribution and software updates methodology, while Desktop Authority has an intuitive set of no-scripting-required desktop administration features with highly granular Validation Logic.

All organizations with Windows desktops can benefit by implementing Desktop Authority as a healthy first step toward a managed network environment. Companies who feel that the additional features of SMS such as more granular software deployment capabilities are desirable should choose to implement both products.

For information on Desktop Authority or other ScriptLogic software solutions, contact your authorized reseller or contact your ScriptLogic representative at: www.scriptlogic.com | 1.800.424.9411 | 1.561.886.2400