SCRIPTLOGIC

VIRTUALIZING THE DESKTOP WITH SCRIPTLOGIC DESKTOP AUTHORITY

A ScriptLogic Product Positioning Whitepaper

NICK CAVALANCIA

Information in this document is provided in connection with ScriptLogic products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in the End User License Agreement for such products, ScriptLogic assumes no liability, and ScriptLogic disclaims any express or implied warranty, relating to the products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

ScriptLogic may make changes to this document or related product specifications and descriptions, at any time, without notice. ScriptLogic makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained in this document.

Table of Contents

SCRIPTLOGIC

Virtualizing the Desktop with ScriptLogic Desktop Authority

In IT today, the term "virtualization" is so overused to define various solutions that seemingly have the same end result, that the term itself has lost much of its true meaning. Many focus the term on moving the operating system from physical hardware to a software-based (and therefore, far more portable) solution. Others focus on the ability to deliver whatever application the user needs on-demand without the need for waiting for an install to complete. Still others look to server-based computing solutions that move the users individual "desktop" to one shared among many users. Virtualizing the operating system or applications is a goal so wide with options of how to get there, that more and more vendors are dipping their toes into the virtualization waters and providing solutions that yield some form of "virtual" experience for the user.

IT Executive Summary

Desktop Authority and its family of solutions provide comprehensive coverage of the desktop lifecycle, from beginning to end, with a specific focus, unique to Desktop Authority as a desktop management platform, on the area of desktop and user configuration. While virtualization, regardless of the specific implementation, provides an OS and application workspace for the user, it lacks the management ability to cater the desktop to meet the business needs of the user beyond that of just having a copy of Office installed or streamed.

In this whitepaper, I'll provide some thought leadership on the topic of desktop virtualization by first defining the types of virtualization available today and the issues with each and then by introducing ScriptLogic's Desktop Authority solution, which can be used to complete that which today's virtualization solutions can only attempt to accomplish: **the complete virtualization of the user desktop experience**.

In addition to "virtualization", many of the terms used in this whitepaper are equally somewhat open to interpretation. So let me define a few terms I'll use throughout whitepaper so we're clear on what is being discussed.

- **Desktop** – I'll use this term to refer to the user's actual Windows desktop; the working environment in which they interact with the OS.
- **Workstation** – I'll use this term to generically mean a physical computer, whether a laptop or desktop computer.
- **Terminal Environments** – I'll generically use this term to refer to the use of Microsoft's Terminal Server and/or Citrix's Presentation Server.

Defining Desktop Virtualization

To narrow the focus from all the hype in the media today, and all the "me too" vendors claiming to have created *yet another* virtualization solution, let's concentrate on three specific, mainstream, and accepted forms of virtualization.

1) **Application Virtualization** – sometimes called "app streaming", virtualization of applications are accomplished usually through delivery of applications by streaming them from a server rather than by traditional installation onto a workstation. This is a muddied term in and of itself, as there are a myriad of solutions today that yield the same end result (instant access to a completely functioning application), but do it using varied methods.

2) **OS Virtualization** – This is most commonly associated with products like VMWare's ESX Server or Microsoft's Virtual Server. In this case, the entire client OS runs within software-based virtual hardware, resulting in the ability to run multiple "machines" on a single piece of server hardware. This can be accomplished using both workstation-based and server-based solutions. In the case of server-based OS virtualization, users will connect to the desktop using a remote control protocol, such as Microsoft's Remote Desktop protocol (RDP).

3) **Terminal Environments ("desktop virtualization")** – Microsoft's Terminal Server and Citrix's Presentation Server provide a similar experience to server-based OS virtualization, where users connect to the server to establish a desktop in which to work. Applications can be either preinstalled or streamed to provide access to needed resources.

Even these three solutions are intertwined; it is possible that you will connect to a Citrix Presentation server using a streamed version of their ICA client to run a VMWare guest OS on the Citrix desktop that uses streamed applications within the Guest OS. Sounds overly complicated, I know, but it is a reality today.

Desktop Virtualization Goals

Because the definition of "desktop virtualization" is a moving target in the industry today, I'd like to instead focus on the goals of desktop virtualization to bring all this into focus.

1) **Anytime, anywhere, on-demand access** – The core idea behind all three of the types of virtualization previously covered is to give the user instantaneous access to their working environment. App streaming gives you instant access to applications (no need to wait 45 minutes for Office to install the first time you sit down at a workstation), while OS virtualization and terminal environments give you access to an entire desktop.

2) **A secure, consistent, and functional working environment** – Creating a desktop with these characteristics means less helpdesk calls, more productive users and, therefore, more productive IT organizations. Virtualization can provide each of these aspects of a user's desktop to varying degrees. App virtualization can create this environment but only within the context of a delivered application (that is, the app itself will be secure, functional and consistent even when running on a desktop that is not). OS virtualization and thin client solutions have the ability to create this type of environment, but require the use of logon

scripts, group policies, and/or desktop configuration solutions to accomplish this goal; pretty much the same as the desktop of a physical workstation.

3) **Lower TCO** – Whatever the solution implemented, it cannot be less cost-effective than a traditional physical machine.

So the overall objective is to give the user a desktop that is not tied to a physical piece of hardware such that they have consistency in their working environment no matter where they are, and do it in a cost-effective manner. Table 1 compares the virtualization types using the goals previously mentioned.

Virtualization Goal	Application	OS	Terminal
Anytime, anywhere, on-demand access	**Yes** (limited to applications)	**Yes** (requires access to the guest OS via local storage on a laptop, USB drive, etc. or via a remote protocol such as RDP or ICA using a VPN and/or the Internet)	**Yes** (available internally and requires external access via VPN and/or the Internet)
Create a secure, consistent, functional working environment	**Yes** (limited to applications)	**No** (this method requires additional solutions such as scripts, group policies or a desktop management product)	**No** (this method requires additional solutions such as scripts, group policies or a desktop management product)
Lower TCO	**Yes** (limited to applications)	**Possible** (the addition of setup and maintenance of a virtual OS raises costs, while the potential for needing less hardware could lower costs)	**Yes** (only a single server OS needs to be installed instead of multiple workstation OSes)

Table 1: Comparing Virtualization Solutions

Desktop Virtualization: a complete failure?

<u>None</u> of the virtualization solutions today get you all the way to the goals of virtualization; app streaming is closest but is always limited to the app itself. And the OS virtualization and thin client solutions still leave you in much the same position as with physical workstations; the OS is setup, but the user experience needs to be configured.

The reason why app virtualization is so much closer to the goal of virtualization (which I believe is the reason it gets so much attention) is that the streamed application can be <u>completely configured</u> prior to streaming and can be delivered in a matter of seconds (not minutes or hours), but is limited to the app itself. With the OS virtualization and terminal solutions, the user's desktop is not configured, although it is available within an equally short timeframe. Therefore, while the hype is high, the question remains, "is a virtualized desktop possible?"

SCRIPTLOGIC

A *Virtual User Environment*: The Truly Virtualized Desktop

The answer lies in the ability to take the central configuration and instantaneous delivery strengths of application virtualization and apply that to the entire desktop in either an OS virtualization or terminal environment scenario to create what we at ScriptLogic refer to as a *Virtual User Environment*. Think about it: if you could deliver every aspect of the user's desktop in the same timeframe as a streamed application no matter where the user logged onto (be it a physical workstation, virtualized OS or terminal environment), you'd have a virtual environment where all three goals are met in one: accessing a secure, consistent and functional working environment from any machine in the world that results in a lower desktop TCO.

ScriptLogic's Desktop Authority is the only solution that can bring this virtual user environment into a reality: the anytime, on-demand access is provided by either the virtual OS or terminal environment, the instantaneous use of virtualized applications and the secure, consistent and functional working environment provided by Desktop Authority. Other "Desktop Management" or "Client Configuration" management solutions that exist on the market focus on applications and patching, but lack the ability to centrally and comprehensively configure all the desktop elements from a simple point-and-click GUI.

Defining what's in a Virtual User Environment

To be clear, let's define what needs to be immediately accessible on the desktop for a user to be productive. If we can centrally configure these aspects of the desktop and deploy them in the same way an application is streamed, you'll have a completely virtualized desktop by creating this Virtual User Environment:

- Applications
- Application Settings
- Drive Mappings, Printers
- Email Profiles
- Shortcuts (desktop, Start Menu, etc)
- Registry settings

- Security Policies
- Endpoint Device Lockdown
- Patches (both MS and 3rd party)
- File/Registry Permissions
- Windows Firewall settings
- Power Management (when applicable)

How to Create a Virtual User Environment

So let me talk about the three steps to create a Virtual User Environment: virtualizing the OS workspace, virtualizing the applications and virtualizing the user experience.

Step 1: Virtualize the OS Workspace

This can be accomplished either by truly using a virtual guest OS (a la VMWare/Virtual PC) or using a terminal environment; in either case, the OS is not tied to a physical machine in front of the user. The OS environment should be clean; not one crammed with common applications, settings, etc. Doing so only makes the OS ready for the business needs the day it was configured. Instead by using a clean OS image or terminal environment and later configuring the settings needed by the user at the time of use, the business needs of "today" can be met.

Step 2: Virtualize the Applications

While Desktop Authority does not have its own virtualization solution to facilitate immediate access to applications, third-party solutions such as Citrix's Application Streaming (www.citrix.com), Microsoft's SoftGrid (www.microsoft.com/softgrid), Thinstall (www.thinstall.com), or StreamTheory (www.streamtheory.com) can meet the need for streaming applications with varying capabilities and are compatible to be deployed via Desktop Authority.

Step 3: Virtualize the User Experience

This last step is the most critical. Without it, you simply have a desktop with applications and nothing more. If you've spent any time supporting a desktop, you know you cannot simply walk up to a user and say "I setup your new Vista machine with Office 2007… see you later!" There is so much more the user needs configured to make them productive. What is needed here is a solution that meets the virtual OS and virtual applications where they stop (which is basically at the point of deployment) and then takes over to configure each of the supporting elements of the desktop listed previously to create a completely virtualized user experience.

It is the combination of all three of these elements that create a comprehensive virtualized experience for the user. Figure 1 shows the relationship shared by each of these three aspects of virtualization to provide a complete virtualized user environment.
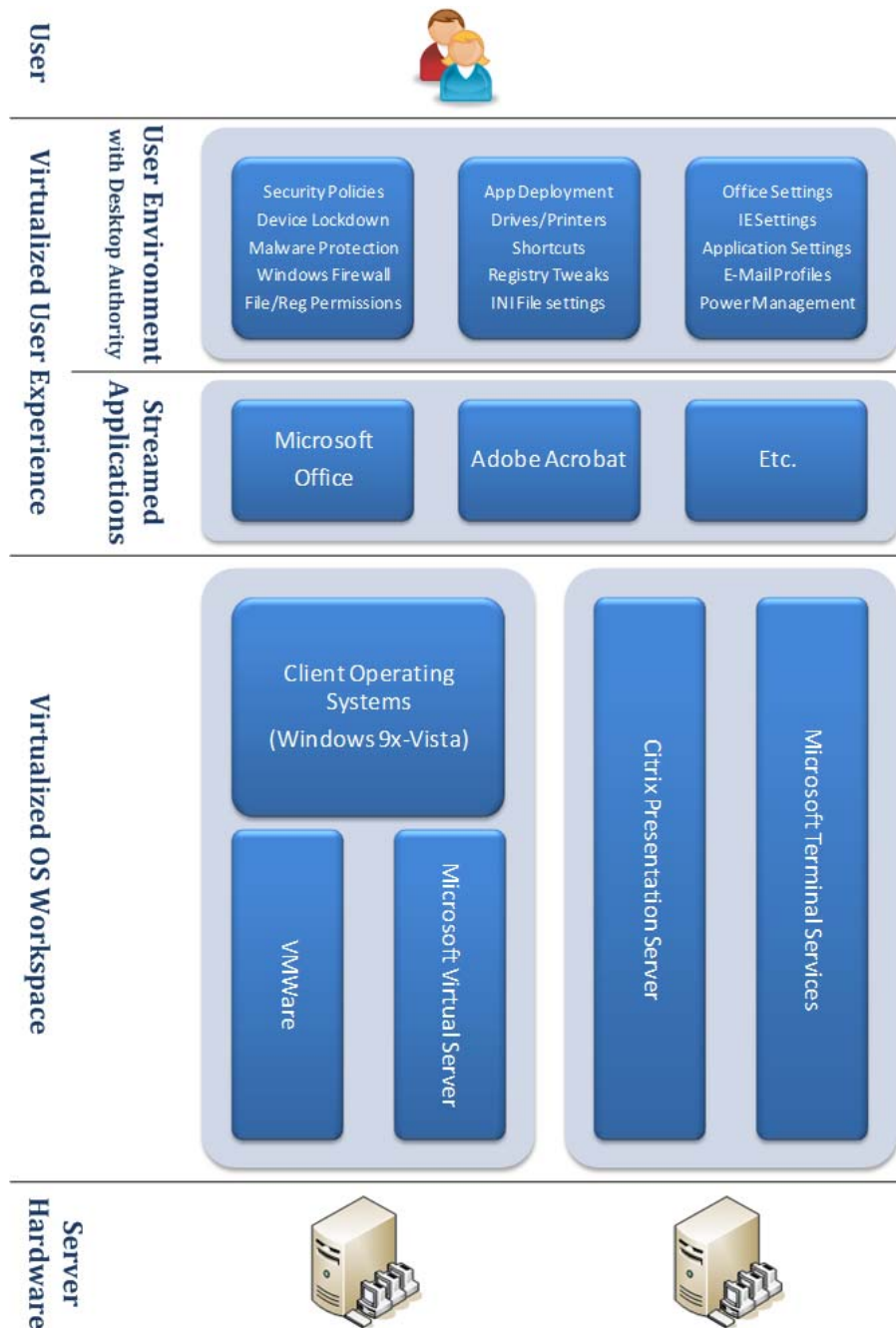
Figure 1: The Complete Virtual User Environment

By moving to either a virtual OS- or Terminal-based OS workspace, the user is no longer tied to a physical machine. By streaming the applications, they are instantly available, consistently configured, and accessible without the traditional constraint of "is it already installed" on a given machine. By virtualizing the user environment, the desktop elements that support the streamed applications actually complete the initial intent of streaming in the first place – **an instantly accessible, secure, consistent and functional working environment no matter where the user logs on.**

What about the Physical Desktop?

It should be noted that most organizations are using a hybrid approach, utilizing a mix of physical, virtual and terminal environments to facilitate user access to company resources. Streamed applications and the user environment can still be easily applied to a physical desktop as easy as the virtual. The benefits are the same: a secure, consistent, and functional working environment. All the streamed app solutions listed in this document as well as Desktop Authority work on physical desktops.

In the next section, I'll demonstrate how Desktop Authority can be used in both a virtual OS and terminal environment to complete the virtual desktop initiative started by each. I'll use the terms *physical*, *virtual*, and *terminal* to represent a physical workstation, a virtual guest OS via VMWare or Virtual PC and a Terminal Server or Presentation Server-based environment respectively.

Completing the Virtual Desktop

I'd like to cover three specific aspects of the virtualized desktop that need to be addressed beyond creating the OS environment, whether terminal or virtual, as well as beyond the accessibility to virtualized applications and show you how Desktop Authority can be used to complete the virtual desktop and create the virtual user environment by implementing a user desktop that includes:

1) **Comprehensive, Centralized Configuration** – Each of the desktop elements listed previously need to be centrally configured to ensure a consistent experience for users.
2) **Real-Time Validation** – To facilitate an experience that is functional based on the user's current needs, any validation that is used to determine whether a particular desktop element should be applied (such as deploying an application or a printer) needs to be done at the time of configuration. More on this later.
3) **Enforced Security** – Once the desktop is setup, security policies, device lockdown, patching and anti-malware initiatives needs to be put into effect to ensure the security of both the user and the network on which they are working.

Comprehensive, Centralized Configuration

Desktop Authority touts management of over 30 different aspects of the user's desktop; each one easily configured using an intuitive and simple interface. Figure 2 shows the various configuration objects, as well as an example of adding a printer using nothing more than a UNC path to the printer.
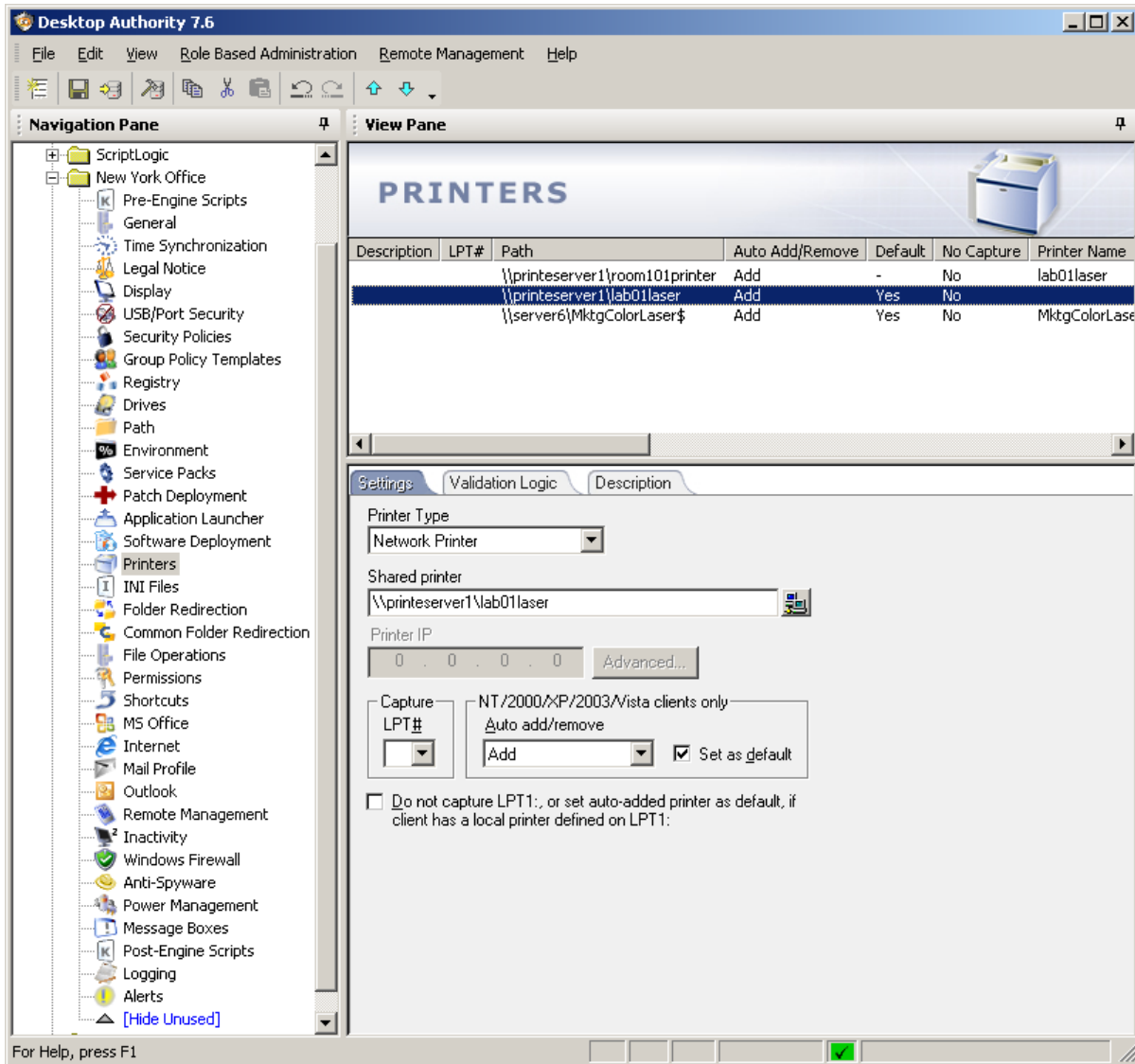
Each of these configuration objects uses a simple interface to quickly and easily configure the user's desktop, as shown in Figure 3. Each element (that is, an individual drive mapping, shortcut, registry setting, etc) is grouped together by type and then the configuration is store within a profile, which is essentially a folder used to separate configurations. Figure 2 previously shows a "New York Office" profile (at the upper left of the screenshot) that houses the configuration elements for the users of that office.
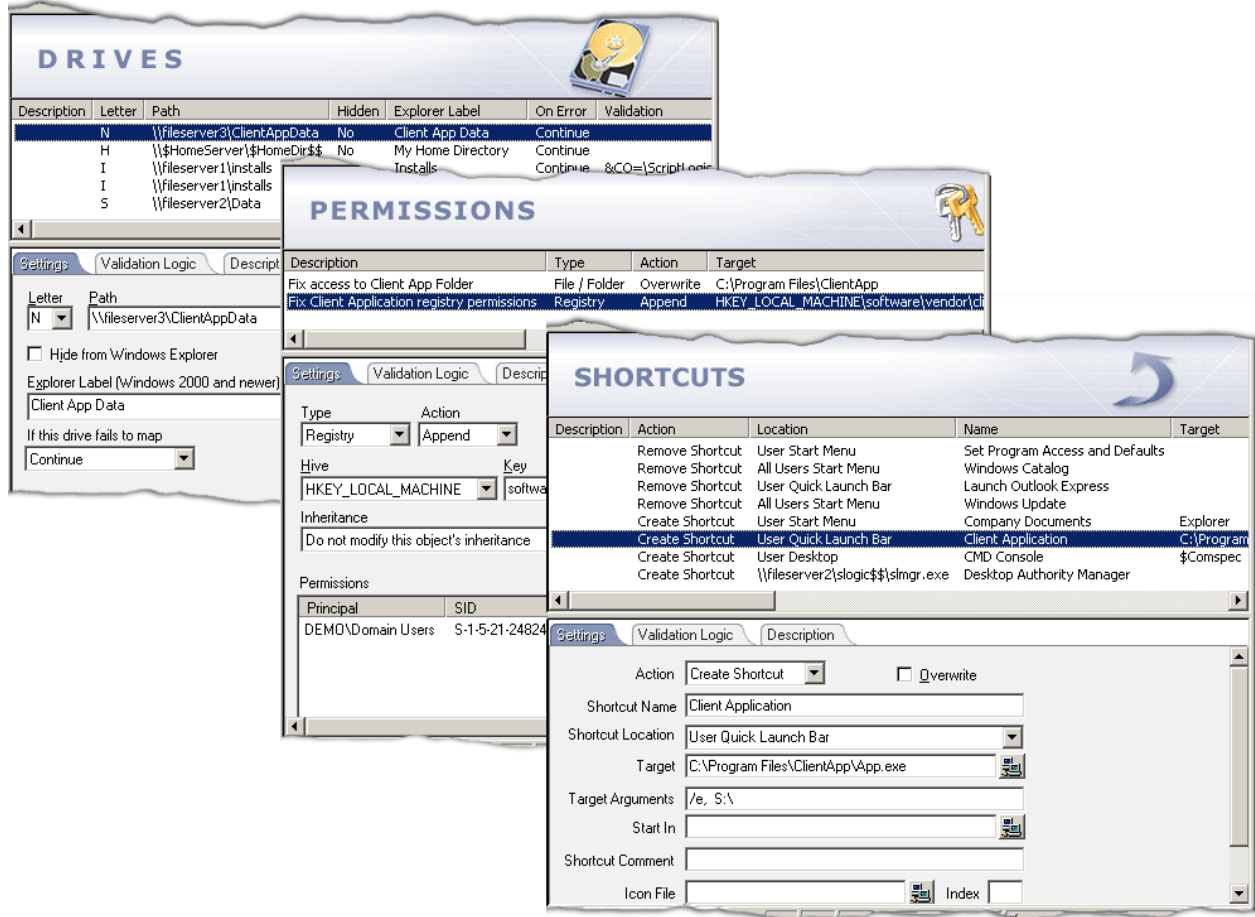
Figure 3: Configuring the desktop is simple and intuitive with Desktop Authority

Real-Time Validation

The challenge in configuring a virtual desktop is not the mapping of a drive or the deployment of a printer; those tasks can be scripted if necessary. The real challenge is deciding first who of the hundreds or thousands of users need the particular configuration element, as well as if the configuration is currently applicable. Here's what I mean: suppose you are deploying a Sales application out to salespeople in the field. You would first need to somehow dictate that only salespeople will get the application. The obvious method is to simply use membership within the Sales group. Additionally, you only want the sales printer deployed if the user is using a physical desktop within the organization (because they won't need it if they are connected remotely to either a virtual OS or terminal-based desktop). Here, you would need a more advanced method of determining whether a user is on a physical desktop or not.

The validation needed not only needs to be powerful, with multiple options (such as group membership and OS-type), but also needs to be determined at the time of configuration (as in the case of the printer deployment) to ensure a configuration appropriate for the user, the OS, the desktop type, etc all at the time the configuration occurs.

Desktop Authority's patented Validation Logic uses over 40 different validation types, as shown in Figure 4. These validation rules establish the configuration granularity necessary to configure the desktop appropriately for each user's needs. In addition, Boolean operators (AND and OR statements) are supported to bridge separate validation rules to create essentially 40^n levels of granularity. Desktop Authority configures the user's desktop at logon, at logoff and refreshes the configuration (by default every 60 minutes). As shown in Figure 4, each configuration element can be deployed to the user's desktop at any or all of the three times.

- **Logon** – this is perfect for establishing the user's working environment before they see the Windows desktop. So applications, drive mappings, printers, shortcuts, registry tweaks, INI file settings, Outlook profiles and more can all be setup prior to the user working.
- **Logoff** – some elements lower user productivity, such as the deployment of a Service Pack. This can be configured to deploy when the user logs off. The logoff process is suspended, Desktop Authority does its configuration and then the process is resumed.
- **Refresh** – this is perfect for those elements that need to be changed throughout the workday, those that will raise user productivity by being re-implemented should they be changed (such as a desktop shortcut that accidentally gets deleted), or those that involve enforcing security settings.
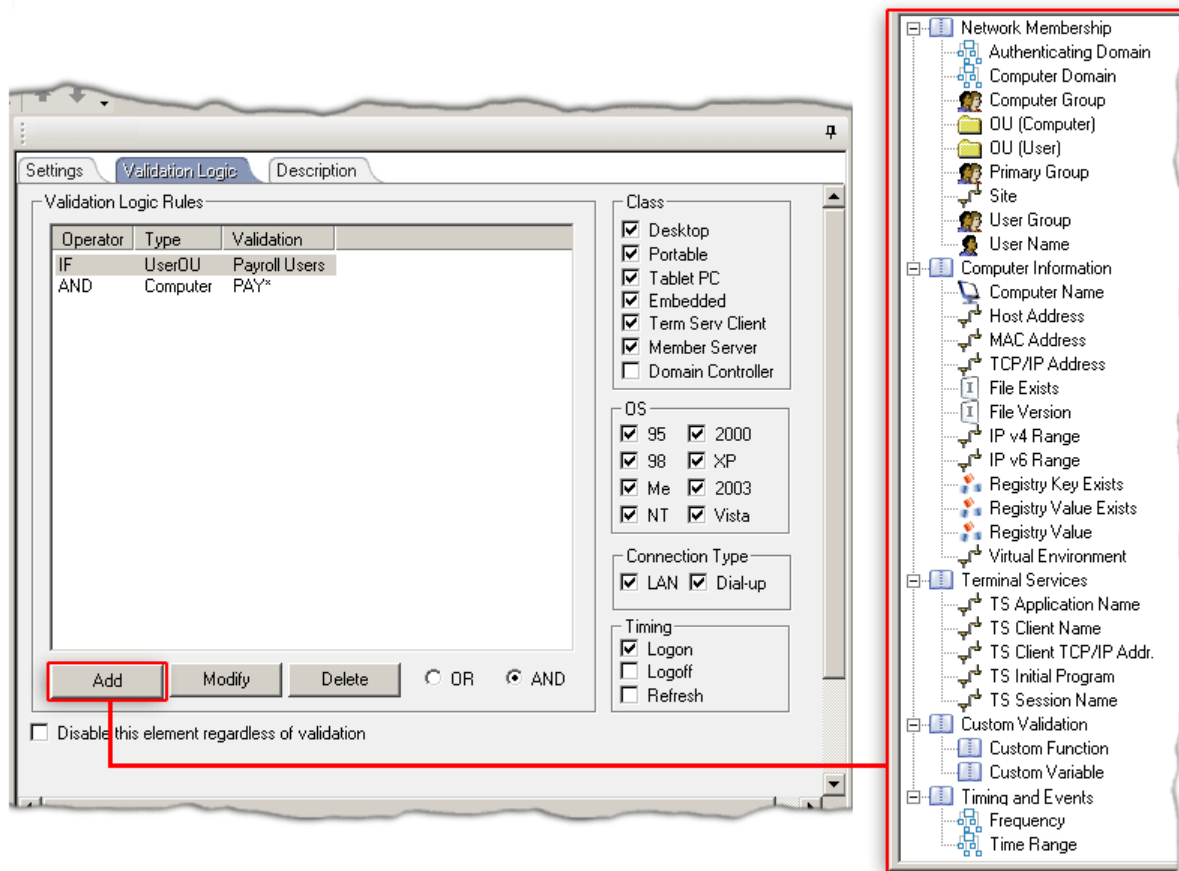

Figure 4: Ensure appropriate configurations with Desktop Authority's Validation Logic

Terminal Clients

Clients using either Terminal Server or Presentation Server environments can be configured differently from physical or virtual OS clients using a simple "Terminal Server Client" checkbox (shown previously in middle of Figure 4). Additionally, five specific terminal-related Validation Logic elements exist to further narrow the focus of a desktop configuration, also shown in middle right of Figure 4. It should be noted that while the Validation Logic section is titled "Terminal Services", those Validation logic elements apply to both Terminal Server <u>and</u> Presentation Server environments.

Virtual OS Clients

Desktop Authority currently supports detecting whether a user is logging in via a VMWare-based OS, using its "VMWare Virtual Machine" rule, shown in Figure 5. Support for Microsoft Virtual PC and Virtual Server clients will be available in future versions of Desktop Authority.
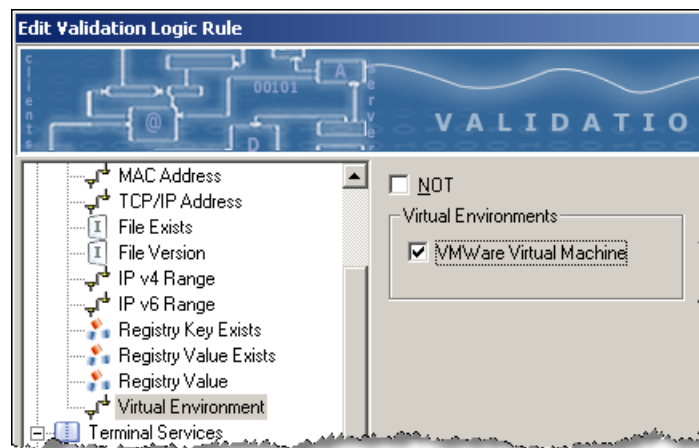

Figure 5: Desktop Authority can easily detect VMWare-based clients.

Enforcing Security

The last aspect of establishing the virtual desktop takes the last two covered and applies them to security. Providing a mechanism to lock down policies, patches, protection from malware, etc all cannot simply be done across the board; each environment (physical, virtual and terminal) has its own needs and requirements. For example, you would not initiate patching while connected to a Citrix session. Nor would you give internal users running a physical desktop the same restrictions as contractors using a VMWare-based guest OS running on the contractor's laptop when outside the building. So to bring this around full circle, you need to be able to a) comprehensively deploy security-related settings, but b) be able to easily differentiate between users logged on in a physical, virtual or terminal environment.

Desktop Authority has a number of security-related measures it uses to secure desktops, each of which can be independently established based on the client type, as well as any of the 40+ Validation Logic values:

- Group Policy-based Security Policies
- Malware Protection
- Endpoint Device Lockdown

Securing with Group Policies

Utilizing Microsoft's knowledge of their own operating systems, Desktop Authority has the ability to import Group Policy Administrative Template (ADM) files for use within Desktop Authority, as shown in Figure 6.
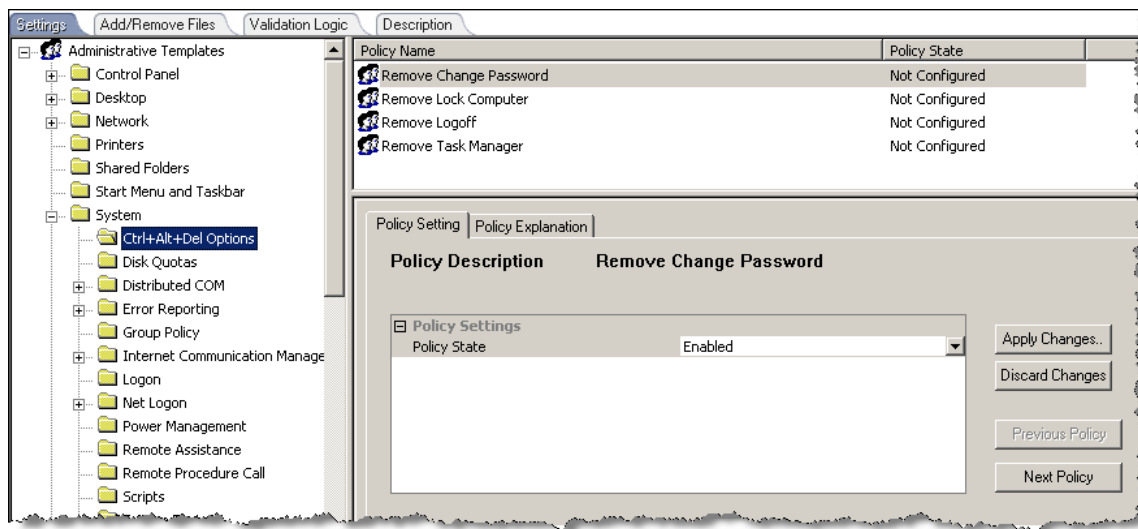

Figure 6: Deploy Group Policy-Based Security Settings with Desktop Authority

The benefits of using Desktop Authority instead of native Group Policies are twofold: First, a single solution can be used to push out these settings to clients instead of doing half with Desktop Authority and half with Group Policies. Second (and most important) is the use of Validation Logic to establish who will be receiving the security settings. Group Policies has essentially six levels of granularity (domain, user or computer group membership, user or computer OU and AD site) – none of which assist in separating settings for the different client types – whereas, Desktop Authority has its 40^n levels of granularity, including the previously mentioned ability to differentiate physical workstations from virtual OS clients from terminal environment clients.

Protection from Malware

Desktop Authority has two optional components to assist with keeping users safe from malicious software: Patch Deployment and Anti-Spyware. Each one can be separately configured using Validation Logic to ensure only the appropriate types of client environments should be protected by each. For example, the Anti-Spyware scans can be run on all three types of clients, but patching wouldn't be appropriate for terminal clients.

The Patch Deployment for Desktops option, shown in Figure 7, patches Microsoft and select 3rd party vendor's solutions to centrally patch the desktop. This option also includes turnkey patching-specific reports.
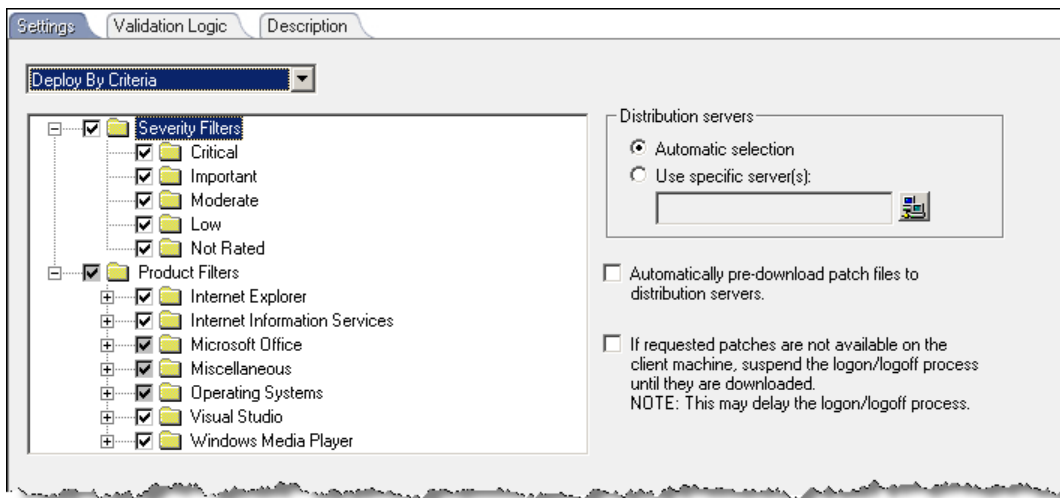

Figure 7: Desktop Authority patches Microsoft and 3rd party solutions

The Spyware Detection and Removal option, shown in Figure 8, scans the client for known spyware and can be configured to automatically remove it.
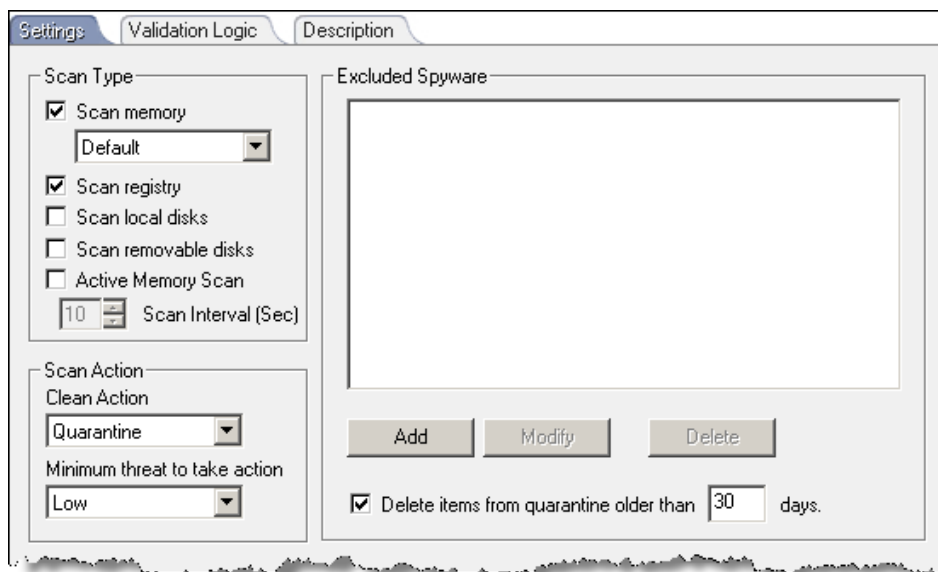

Figure 8: Known malicious spyware can be detected and removed automatically

Endpoint Device Lockdown

Patching and Spyware protection are reactive measures of protection, in that they protect against known vulnerabilities. To truly protect a client, the introduction of unknown malware must be stopped before it ever occurs. This can be accomplished by locking down any mediums by which malicious code can enter the system. This includes USB sticks, CD/DVD's, Bluetooth, WiFi, FireWire

drives, and more. The USB/Port Security option in Desktop Authority, shown in Figure 9, locks down 20 different device types, allowing Read or Read/Write access to any device that can read or write (such as a USB stick or a CD Burner). Locking down these devices both prevents the introduction of malicious software, but also prevents data theft.
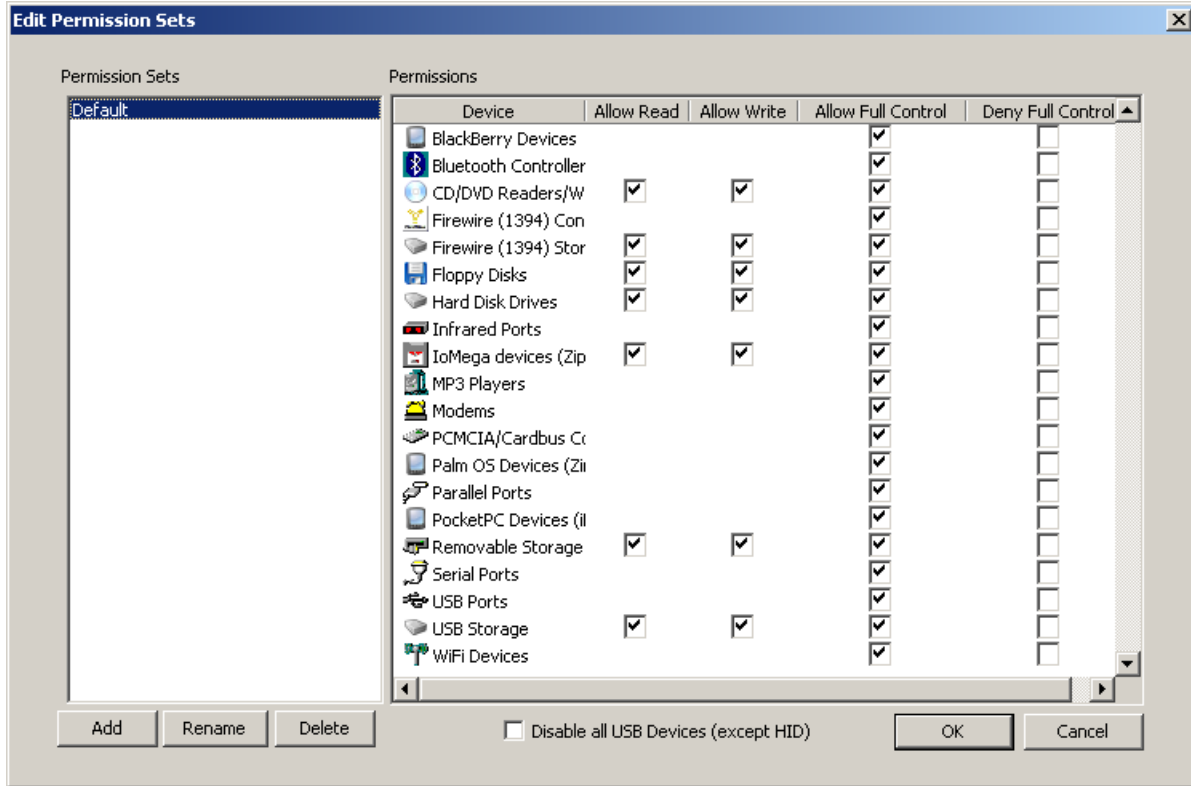

Figure 9: 20 different devices can be granularly locked down

Conclusion: Making the Virtual Desktop a Reality

So despite the hype today about creating a virtual desktop, without a solution like Desktop Authority to complete the virtualization, all you really have is yet another way to put a user at a desktop without any means of making them productive. Even with streamed applications, the user is lacking all of the supporting desktop elements that make an application truly functional.

With Desktop Authority, you will not only be able to establish a secure, consistent and functional working environment for the user regardless of what client type they log into the network with, but also be able to easily differentiate the client types and should users move from one client type to another, their configuration can be dynamically updated to use the configuration appropriate for that client type.

Resources

More information on Desktop Authority, as well as a 30-day fully-functional evaluation is available on our website. Other products listed in this document can be found at:

- Desktop Authority – www.scriptlogic.com/da
- Microsoft SoftGrid – www.microsoft.com/softgrid
- Citrix – www.citrix.com
- Thinstall – www.thinstall.com
- StreamTheory – www.streamtheory.com
- VMWare – www.vmware.com
- Microsoft Virtual Server – www.microsoft.com/virtualserver

About the Author:

Nick Cavalancia, MCSE/MCT/MCNE/MCNI, is ScriptLogic's VP of Marketing where he assists in driving innovation and the evangelism of ScriptLogic solutions. He has over 15 years of enterprise IT experience and is an accomplished consultant, trainer, speaker, columnist and author. He has co-authored and contributed to over a dozen books on Windows, Active Directory, Exchange and other Microsoft technologies, and is the author of the upcoming book "Microsoft Exchange Server 2007: A Beginner's Guide."

SCRIPTLOGIC