Quest™

Desktop Authority Management Suite

Centralized, secure and consistent management of the Windows user environment

IT end users are demanding more flexibility in IT operations, but administrators must still maintain a secure and consistent user environment. They can no longer rely on the traditional model of managing only the machine; each user needs to be granted the right access to the right resources regardless of the device used. This means that even small businesses are dealing with hundreds of user environments. In addition, administrators must control application privileges appropriately, ensuring that they can run without full local administrator access.

Desktop Authority Management Suite enables admins to proactively provision and manage the Windows user environment. With the suite, you can easily create a secure, consistent environment for each user and ensure that applications run with only the privileges and access needed.

FEATURES

Desktop Authority Management Suite is comprised of two solutions:

Desktop Authority Standard

- **Real-time targeting engine —** Don't be forced to choose between "one size fits all" configurations or leaving computers unmanaged. In Desktop Authority Standard and Privilege Manager, admins can tailor settings, configurations and administrative privileges by user, computer, network address or dozens of other criteria using a patented Validation Logic targeting engine. Configuration settings and privileges are automatically updated when the user or environment changes, without any intervention by the admin.

- **Customize the user environment —** Eliminate the hassles of trying to manage configurations and profiles for users who move between physical desktops, terminal servers or VDI, or who move from office to office. Desktop Authority Standard

BENEFITS:

- Easily targets, configures and manages a secure and consistent user environment, no matter where users are or whether they use a physical or virtual desktop — even machines on and off the domain with just internet connectivity

- Ensures that users and applications have only the privileges they need with comprehensive tracking and reporting

- Customizes user configurations like drives, printers, shortcuts and Office — without logon scripts, PowerShell or WMI filtering

- Enables users to customize their computers the way they want — within the limits you specify and without giving them local admin rights

- Discovers applications that require elevated privileges and access and selectively provides what they need without granting full local administrator access

- Reduces service requests by proactively managing user configurations and administrative privileges

Desktop Authority Management Suite

Targeted configurations

- Browser settings
- Printers/drives
- Registry settings
- Ports/external devices
- Office and Outlook
- Energy settings
- Local admin privileges/accounts
- Application access

VL Validation Logic targeting
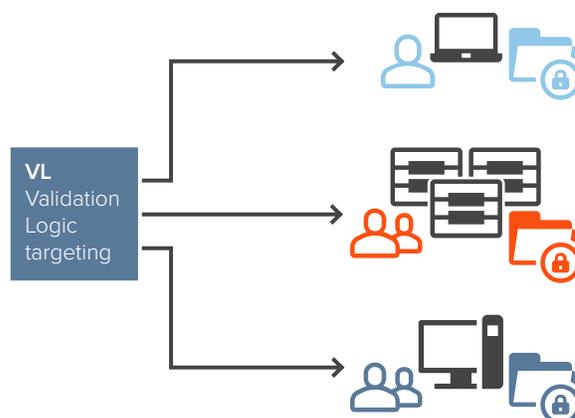
Patented Validation Logic technology targets and enforces configurations and settings for user environment management.

provides over 40 management objects that enable admins to easily provide access to company resources; manage security settings; configure Outlook profiles and settings; launch applications; customize registry settings; control power schemes and inactivity settings; and manage Internet security and browser settings.

- **Support the user —** With Desktop Authority Standard's ExpertAssist remote management system, admins can manage over 40 computer tasks without interrupting the user; for example, they can access system info, control processes, run remote command-line commands and copy files. When needed, admins can also control the mouse and keyboard remotely. ExpertAssist works over the LAN or across the Internet.

Privilege Manager

- **Elevate applications, Windows processes and ActiveX controls —** Grant users permission to install software, make desktop changes and install ActiveX controls that you deem secure—without granting them local admin rights that would

allow them to install unapproved software, copy data to flash drives or incur other risks.

- **Blacklist applications with surgical precision —** Allow administrators to selectively deny a user or group the ability to launch an installed application, even when the application requires only standard user permissions.

- **Proactively discover and manage privileges —** Discover applications that need administrative privileges, provide predefined elevation options and allow users to request their own privilege elevation.

Use cases

- Customize user configurations like drives, printers, shortcuts, MS Office and Outlook signatures without logon scripts. Provide users with the ability to customize their computers the way they want, but give admins centralized control key over key settings.

- Minimize risk by configuring browser security settings.

- Reduce risk to computers and data by eliminating local admin rights that allow users to install malware or unapproved software, copy data to flash drives, and leave computers unlocked and unattended.

- Reduce the IT burden of managing users who move from company location to location or who spend part of the time on the road and need support when they're not in the office.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

DESKTOP AUTHORITY SYSTEM REQUIREMENTS

WEB CONSOLE (MANAGER)
Windows Server 2008 and 2008 R2 (incl. x64)
Windows Server 2012 and 2012 R2

EXPERT ASSIST
Windows 7 32/64 bit and newer
Windows Server 2008 R2 (incl. x64), 2012 R2, or any SP

CLIENT
Windows 7 32/64 bit and newer
Windows Server 2008 and 2008 R2
Windows Server

HARDWARE
Minimum 2.0 GHz dual core processor
4 GB memory

SERVER PREREQUISITES
.NET Framework version 3.5 SP1
Visual C++ 2005
SQL Server 2008 R2 Express
Windows Installer 4.5
IIS 7 or above

BROWSER
Minimum IE11, Firefox 3.6 or Chrome 44, Edge 25

EXPERTASSIST
IE11, and the latest versions of Microsoft Edge, Mozilla Firefox and Google Chrome

EXPERTASSIST ADDITIONAL REQUIREMENTS
Latest Java Runtime Environment

PRIVILEGE MANAGER SYSTEM REQUIREMENTS

CONSOLE
.NET Framework 3.5 (SP1 or higher)
Microsoft Group Policy Management Console
PDF reader
Screen resolution of 1024x768 or higher

CONSOLE AND CLIENT OS S
Windows 7 32/64 bit and newer
Windows Server 2008, 2008 R2, 2012, 2012 R2 and 2016

NETWORK
Must be installed on a computer within AD domain

REPORTING DATABASE
SQL Server 2008, 2014 or 2008 R2 Express

Quest