



Systems Management Buyer's Guide



Table of Contents

Executive Summary.....	3
Purpose of this Guide	3
1.0 Systems Management Buyer's Guide Feature Checklist.....	4
1.1 Inventory	4
1.2 Deployment.....	4
1.3 Power Management.....	5
1.4 Security.....	6
1.5 Asset Management.....	7
1.6 Service Desk and User Portal	8
1.7 Reporting.....	8
1.8 Remote Control and Recovery	9
1.9 Administration.....	9
1.10 Deployment and Maintenance	10
1.11 Offers Mac Support	11
1.12 Pragmatic ITIL Implementation	11
1.13 Additional Considerations.....	11
Dell KACE Corporate Background	13

Executive Summary

Now more than ever, systems management professionals in organizations of a variety of sizes are charged with doing more with less. Many systems administrators are faced with virtually the same challenges as their counterparts in the largest of enterprises, but without the number of support staff, specialized skill sets and budgets their larger-scale colleagues can afford. Time spent “fire fighting” across a variety of systems management disciplines, as well as the need to perform labor intensive manual chores, leaves little extra time to proactively tackle other strategic initiatives such as performance improvements or root cause analysis. These individuals are frequently stretched thin, with limited core teams responsible for accomplishing the bulk of the tasks necessary to achieve the IT stability critical to running the business.

Traditional software-based systems management solutions exist, but in some cases have exacerbated the systems management dilemma for the more moderately scaled organization, those typically with 100 to 20,000+ managed systems. While these traditional solutions are robust, they have been designed for the very largest of enterprises, and the investment necessary in pre-requisite software, hardware, services, maintenance and training have simply proven too costly and too complex for many who can’t afford this approach to their systems management challenges. This has left the more resource-challenged organizations to manage with either overly sophisticated software, sub-optimal point solutions or manual processes. Alternatives are available, but they need to respond to the specific criteria of the more typical systems manager who is charged with wearing many hats: the solution needs to be easy-to-use, comprehensive, and affordable, getting the administrator out of reactive problem resolution mode and into proactive systems management mode.

Purpose of this Guide

Enterprises of all sizes continue to struggle in their efforts to find and deploy an effective systems management solution scaled to their needs. In the solution evaluation process, there are both feature/function criteria as well as less tangible solution characteristics that need to be weighed in order to make an informed and appropriately calibrated decision. Dell KACE has developed this guide to help articulate that buyer’s criteria via a comprehensive feature/function checklist, and to pose additional considerations that should be made when making a decision regarding a systems management solution.

1.0 Systems Management Buyer's Guide Feature Checklist

1.1 Inventory

Hardware and software inventory represents the very core of effective systems management. Users should be able to auto-discover network-wide software and hardware configurations through managed agents or agent-less network scanning, for the most complete computer inventory possible.

- [Device discovery](#)
The solution should provide agent-less discovery of all network connected devices including PCs, servers, printers and network devices. It should report IP address, port status and SNMP inventory data for all discovered devices.
- [Hardware and software inventory](#)
The solution should perform comprehensive, agent-based inventory on PCs and Servers reporting on hardware and software data such as installed programs and patches, as well as BIOS, processor, disk drive, and memory details.

1.2 Deployment

Deployment of both operating systems and software pose one of the largest management challenges and require the greatest amount of systems administrator's time. Automation of these tasks represent a critical step beyond manual processes by allowing users to perform remote deployment and configuration of operating systems, applications, service packs, patches or virtually any digital asset to Windows, Mac and Linux desktops and servers.

- [OS deployment/imaging](#)
The solution should enable users to remotely provision any desktop, laptop or server via hardware independent network OS installation or disk imaging. Remote and unattended bare-metal provisioning should allow both pre and post provisioning tasks such as BIOS configuration and application deployment to be automated, to save administrators time and improve the reliability of deployments.
- [Windows 7 migration](#)
Beyond the necessary tasks of actual Windows 7 rollout and preservation of user data, other migration challenges include identifying which machines can be upgraded, which applications are supported on Windows 7 and assuring that license tracking is not disrupted throughout the process. The solution should help facilitate tasks such as user state migration, operating system deployment and application distribution, helping speed the move to Windows 7 and minimizing end-user downtime.
- [Software distribution](#)
The solution should enable users to push out any type of digital asset, including MSI, EXE, ZIP and batch files. It should provide remote administration, installation and distribution of any application, update, or digital asset to Windows, Mac, and Linux desktops and servers. Flexible

distribution should take the place of time consuming manual tasks, even across large distributed networks through remote administration, and updates should be managed through the use of dynamic groups which allow control over which machines are addressed and when. Additionally, the solution should provide users with direct access to application deployment best practices and technical information such as command line parameters from online systems management community websites, such as AppDeploy.com.

- **Software packaging with conflict resolution**
The solution should make it easy to distribute software applications without needing to do any repackaging. It should deploy almost any package format to Windows, Mac, and Linux systems, along with parameters or full command lines to customize installations. This will eliminate time consuming and complex repackaging. Supported packages should include: .MSI, .EXE, and .ZIP for Windows; .pkg, .app, .dmg, .zip, .tgz, and tar.gz. for Mac; .rpm, .zip, .bin, .tgz. and tar.gz for Linux.
- **Configuration and policy management**
The solution should enable administrators to automate many configuration tasks which would typically require a manual process or the advanced programming of scripts. Administrators should be provided with a script wizard to enable them to build scripts without knowing a scripting language. Shell scripts should be directly executable and scripts written in other languages should also be supported. The solution should come with preconfigured scripts and policies such as USB device control that can be used immediately. The timing and targets for scripts should be highly configurable.
- **Data settings and migration**
The solution should be compatible with 3rd party migration tools such as Microsoft® User State Migration to speed the migration of data and settings for in-place or computer to computer migration.
- **Application virtualization**
The solution should be able to be used to distribute and manage 3rd party client-based application virtualization technologies such as VMware to reduce the time and complexity of application deployment.

1.3 Power Management

Managing power consumption saves companies money, is considered a corporate responsibility and has potential for utility rebates. A comprehensive solution should provide an easy-to-use interface for developing a power control profile for an entire population of client systems, or unique profiles for specific groups of clients, whether they are Windows or Mac. The power profiles need to be deployed and enforced using configuration management capabilities. The solution should be able to implement automated client shutdown policies based upon a schedule or on system inactivity, and include features such as automated Wake on LAN (WoL) commands allowing powered-off systems to be started to allow for after-hours patching, updates and maintenance. Pre-configured and ad hoc reporting abilities are also important factors.

1.4 Security

Effective end-point security has taken on growing importance for every organization in a world of increasingly mobile systems and a dramatic increase in the number and sophistication of security threats. Security vulnerability audits, policy enforcement and remediation capabilities play a critical role not only to identify threats but also to address them.

- **Patch management**
The solution should contain comprehensive yet easy-to-use vulnerability scanning and remediation, including the ability to scan for vulnerabilities and then quickly and easily schedule their remediation via an intuitive web-based UI. Patch repositories should include patches for Windows and Mac systems as well as Microsoft and non-Microsoft applications.
- **Vulnerability scanning**
The solution should include vulnerability scanning of all managed systems. This includes setting the testing schedules and results reporting. The solution should have the ability to scan individual nodes, groups of nodes or even all nodes on a network for a complete view of vulnerabilities, and include pre-defined tests and new tests as they are defined and published.
- **Security policy management**
The solution should include wizards to create scripts for setting and enforcing security policies for browsers, firewalls and anti-virus applications. Users should be provided with wizard-based configuration of conditional, multi-dependency and multi-stage scripts and policies to allow them to create security policies that can be run on a desktop or server. The timing and targets for script deployment should be highly configurable.
- **Security remediation and quarantine**
The solution should be delivered pre-integrated with computer inventory, remote administration, patch management and software distribution functionality. This will greatly increase the ability to neutralize security vulnerabilities, allowing users to maintain security compliance and minimizing user down time across servers and desktops. In those instances where problems cannot automatically be fixed, the solution should be capable of the quarantine of offending nodes to prevent them from infecting the rest of a network or allowing additional network security intrusions.
- **Securing browsers**
Internet browsing is one of the main sources for malware. The solution should not only detect and clean up security breaches, but should proactively contain threats before they become a problem through use of such new technology as a virtual instance of an Internet browser application. By running the browser in a virtual instance, the browser and any activity resulting from its use are isolated from the endpoint, keeping the actual computer and operating system free of changes that would normally occur. Fully contained from the operating system, any changes made via browser activity are not only kept separated, but may also be quickly cleared. For even more security and control, optional white and black list entries should be available to limit what sites a user may visit and what applications the browser is permitted to launch.
- **FDCC support and SCAP scanner**
The solution should include support for the latest required Federal Desktop Core Configurations (FDCC) security settings recommended for systems connected directly to any

United States Federal agency. With security threats continuing to grow in sophistication, IT organizations need to take steps beyond traditional anti-malware and patch management practices to ensure proper protection.

Beyond offering FDCC support, the solution should have a Security Content Automation Protocol (SCAP) Scanner. The SCAP Scanner enables IT organizations to easily audit systems to help ensure compliance with security policies. This technology applies equally to enterprises and governments wanting to bring consistency and increased protection to computing environments.

- [PC lockdown capabilities](#)

The solution should have a PC Lockdown approach that allows flexible user privileges, which enable enterprises to enforce protective security settings, yet at the same time allows users to continue to use the applications they require to be productive on a day-to-day basis.

1.5 Asset Management

Asset management tasks gobble precious time and resource for those using manual processes to track computer and non-computer assets throughout their lifecycle. Solution capabilities need to include asset data audit, tracking, compliance and reconciliation, as well as complete reporting for both regulatory and license compliance purposes.

- [Asset creation and assignment](#)

The solution should contain asset management capabilities that unify and automate non-computer and computer inventory and asset management processes from deployment to retirement, including asset data audit, tracking, compliance and reconciliation. It should track assets in a single configuration management database (CMDB) including computers, software, phones, PDAs, teleconferencing gear and other high value assets. Computer inventory and asset data should be audited automatically and on an on-going basis.

- [Asset tracking and history](#)

The solution should contain asset management capabilities that enable asset tracking through the lifecycle including move, add, change and delete (MACD) activities. Vendor, contract, service and maintenance contracts should also be stored, ensuring accurate tracking of financial and service impacts of asset changes.

- [Asset data reconciliation](#)

As a configuration management database (CMDB), the solution should contain both the consolidated asset and vendor data to enable comprehensive asset data reconciliation.

- [Software usage management \(software metering\)](#)

The solution should contain software metering functionality that allows organizations to accurately monitor application usage and facilitate license harvesting and compliance. The number of times an application is started and cumulative application usage metrics should both be tracked by the solution.

- [Software catalog](#)
The solution should contain capabilities which provide details on discovered software applications such as software category and threat level. This information will assist organizations to quickly identify and manage all software assets.

1.6 Service Desk and User Portal

Any service desk enabled solution worthy of evaluation needs to contain capabilities that provide easy-to-use, configurable and integrated functionality for trouble ticket management, including policy-based workflow across ticket submission, tracking and resolution and pre-integration with key functionality such as inventory. User self help capabilities also extend service desk benefits for resource constrained organizations.

- [Service desk ticket creation and tracking](#)
The solution should contain service desk capabilities that provide an easy-to-use, out-of-the-box trouble ticket management system that is fully integrated with all other systems management features. Tickets should be able to be created via e-mail or the service desk user portal. The solution should also feature built in ticket queues, escalation rules, and ticket auto assignment to reduce administrative effort. The solution should also be able to meet the Information Technology Infrastructure Library (ITIL) service desk requirements for ticketing submissions, tracking and management functionality as outlined in ITIL's Service Operation book.
- [Service desk customization and workflow](#)
The service desk capability should be easily customized to match an organization's unique processes and requirements. It should also include an advanced workflow engine that can be used to automate these processes.
- [Self service user portal](#)
The solution should contain a self service portal that makes it easy for users to submit and track support requests. The integrated portal should also allow users to access a flexible knowledge base, see hardware and software inventory information on their systems, and install IT assigned and approved software packages.
- [Broadcast alerts](#)
Broadcast alerts should be included in the solution to provide a real time mechanism for communicating important information to users. Broadcast alerts can provide targeted end-user messages and eliminate time consuming voicemail broadcasts.

1.7 Reporting

Flexible reporting is critical across virtually every area of systems management. Any solution under consideration should include pre-configured reports; utilize flexible wizard-based reporting tools to easily generate routine and ad-hoc reports, and integration points for 3rd party tools.

- [Reporting and dashboards](#)
The solution should provide pre-configured reports as well as flexible wizard-based reporting tools to easily generate routine and ad-hoc reports. A wizard-based interface should be provided for quickly creating custom tabular and graphical reports that provide insight into desired management metrics. Support for 3rd party ODBC compliant reporting tools should also be part of the reporting feature, as well as scheduled and e-mailed reports to ease distribution and administration.

1.8 Remote Control and Recovery

Remote control capabilities are an important characteristic for organizations that are resource constrained, as they allow administrators to remotely fix problems without involving users, or requiring the administrator to travel or visit each effected system.

- [Remote control](#)
The solution should allow administrators to directly access any system on the network from a centralized user console. Support should also be provided for 3rd party remote control packages such as UltraVNC, Windows Remote Desktop, NetOps, Dameware and Bomgar.
- [Remote recovery](#)
The solution should include remote system recovery capabilities to allow a user to boot any system on the network via a GUI-based recovery environment. This interface will allow administrators to quickly repair systems that have become corrupted and will not boot.

1.9 Administration

Systems management that is complicated for the administrator defeats its reason to be, especially in resource-challenged environments. Foremost should be a unified, straightforward means for systems administrators of all skill levels to access and effectively perform the breadth of systems management administration tasks in an intuitive and expedited way.

- [User interface](#)
The solution should include a web based management console designed specifically for IT administrators of all skill levels. All functionality should be presented in a discoverable and easy-to-use tabbed interface. This interface should enable all administrative functions to take place from any network-allowable location. It should include a comprehensive search capability that enables search across all management data, and audit tracking that ensures key administration activities are tracked by time and activity owner, improving governance.
- [Policy groups](#)
The solution should include technology for creating policy groups. Policy groups ease administration by dynamically grouping computers by characteristics such as IP address, disk drive capacity, BIOS information or software version. Policy groups should also feature real time integration with Active Directory and LDAP. Policy groups significantly speed software distribution, patching, configuration management, asset management, alerts and security.

- [Remote replication](#)
The solution should effectively manage remote offices without the need for dedicated hardware at those locations through remote replication capabilities. These capabilities will reduce the cost and complexity by eliminating the need for dedicated hardware and IT staff in remote locations.
- [Internet connected device management](#)
The solution should have the ability to effectively provide full lifecycle management of any internet connected PCs.
- [Directory integration \(Active Directory and LDAP\)](#)
Administrator and user account creation and authentication should be capable of automation with real-time integration to Active Directory and LDAP. Account creation and authentication should also be able to be handled manually.
- [Role-based permissions – functional](#)
The solution should allow administrators' functional permissions to be tailored to their responsibilities to ensure that they only have access to those functions required to perform their duties.
- [Role-based permissions – device](#)
The solution should allow for machine assignments so that specific administrators can ensure approved administrative access.

1.10 Deployment and Maintenance

Ease of deployment and subsequent regular systems maintenance and upgrade are necessary considerations for effective installation and continued solution utilization, leading to earliest return on investment and the lowest total cost of ownership.

- [Appliance deployment](#)
The solution should offer plug and play deployment, with the ability to plug into a network and begin managing all networked systems. Solution deployment times should be measured in hours or days.
- [Nightly maintenance](#)
The solution should be self-healing and perform automatic backup and maintenance on all of its internal systems, eliminating maintenance procedures that had previously been done manually.
- [Upgrades and updates](#)
The solution should feature straightforward upgrade processes, allowing software to be quickly and easily updated.
- [Scalability](#)
The solution should scale to meet the needs of growing organizations, managing as many as 30,000 nodes from a single source.

- [Training required](#)
The solution should come with a comprehensive training program that includes environment specific installation instruction, as well as comprehensive web-based training. No lengthy off-site classes should be required.

1.11 Offers Mac Support

The solution should also support the Mac OSX platform, including: Mac Imaging through innovative technology which eliminates redundancies in the capture, storage and deployment of disk images during provisioning of the systems; software metering support for the Mac, helping companies manage license fees via thorough analysis of software utilization; and enhanced policy-based configuration management for Mac that enforces OS and application settings through pre-packaged policies and an easy-to-use scripting wizard.

1.12 Pragmatic ITIL Implementation

The solution should support more practical, targeted implementations of ITIL best practices, providing better service to IT users, while still maximizing IT efficiencies. Capabilities to look for include:

- Rapid implementation of the ITIL Service Transition Module with more accurate, enforceable policy-based configuration management
- Support for the ITIL Service Operations Module to help reduce problem resolution times and improved efficiencies through more accurate inventory and integrated service desk capabilities
- Ability to drive Service Implementation Plans (SIPs) by moving from a reactive operations mode to a more pro-active delivery of IT services that are responsive to business change

1.13 Additional Considerations

In addition to specific solution feature and functions, there are other key areas for consideration when selecting a systems management solution specifically calibrated to the needs of the resource-challenged organization.

- [Ease-of-use](#)
The solution should be intrinsically easy-to-use, including simple plug and play architecture, minimal administration, and an intuitive Web-based UI so that it delivers quick results even for non-IT users.
- [Cost/Total cost of ownership](#)
The solution should be more affordable than competitive solutions to acquire, with no hardware or software pre-requisites and minimal requirements for professional services. Ongoing maintenance should include straightforward software upgrades without requiring new or additional hardware, so as to lower the solution's total cost of ownership. Training should be accomplished in hours via the Web, without the cost of off-site curricula.
- [Time to ROI](#)
The solution should deliver a complete return on investment in less than one year.

- **Comprehensive functionality**
The solution should be delivered with all of the systems management functionality required. It should fulfill all of the systems management needs of an organization from initial systems deployment to ongoing management and retirement.
- **Tool matches user requirements**
The solution should be designed specifically to match the needs of an organization, where traditional software-only systems management solutions have proven too costly, complex and labor intensive.
- **Maturity of technology**
The solution should be proven and validated via industry awards, analyst validation, and have a wide reaching and robust base of reference customers.
- **Market specialization**
The solution should be industry agnostic and currently be in use across a breadth of industries, including manufacturing, health care, financial services, retail, government and education.
- **Enhancement and release schedule**
Solution customers should receive all new releases, features and enhancements, including new or revised user documentation and installation and utilization information, on a regular basis.
- **Support**
Solution customers should be provided with 24/7 customer support through a variety of web, phone and email-based support vehicles, including live support representatives, continuous information feeds, a self-service support center portal, user forums, and ongoing web-based training. Also desirable are an annual user conference and an active user community.

Dell KACE Corporate Background

Dell (NASDAQ: DELL) creates, enhances and integrates technology and services customers count on to provide them reliable, long term value. Dell provides systems management solutions for customers of all sizes and system complexity. The award-winning Dell KACE family of appliances delivers easy-to-use, comprehensive, and affordable systems management capabilities.

Dell KACE is headquartered in Mountain View, California. To learn more about Dell KACE and its product offerings, please visit <http://www.kace.com> or call 1-877-MGMT-DONE.

Helpful Links:

- [KACE Systems Management Appliances](#)
- [KACE Systems Deployment Appliances](#)
- [KACE Virtual Appliances](#)

Dell KACE Headquarters

1981 Landings Drive
Mountain View, California 94043

(877) MGMT-DONE office for all inquiries
(+1) (650) 316-1050 International
(650) 649-1806 fax
European Sales: emea@kace.com
Asia Pacific Sales: apac@kace.com

WPBG03.15.2011

While every effort is made to ensure the information given is accurate, Dell does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

Dell and KACE are trademarks of Dell Inc. Dell disclaims any proprietary interest in the marks and names of others. Microsoft and Windows are registered trademarks of Microsoft Corporation.