Mobile Devices in Education:

A Comprehensive Management Approach

The use of mobile devices on campus networks is exploding. According to a recent Center for Digital Education survey, 76 percent of respondents said K-12 and higher education students bring their own mobile phones or tablets to school for use on the campus network, while 84 percent of respondents said faculty and staff do the same. The accelerating adoption of mobile devices in education, both institution-owned and personal, is forcing IT departments to rethink the way they manage end-user devices.

Because tablets are powerful, versatile and reasonably priced, many educators — especially in K-12 schools and districts — are eager to purchase those mobile products for use in the classroom. At the same time, more and more students and employees — especially in colleges and universities — are asking for the chance to run academic and business applications on their personal tablets, laptops and smartphones.

As institutions add these consumer-oriented devices to the desktop and laptop computers already present on campus, IT professionals face an entirely new challenge. They need

About this Paper:

Many K-12 school districts and institutions of higher learning are embracing the reality of increased mobile device usage and bring your own device (BYOD) initiatives on their campuses, and the impact this will have on IT. Those pressed with supporting this change are wrestling with how to manage a broad assortment of end-user devices now connecting to their IT environments. These devices include consumer-oriented smartphones, tablets and laptops, as well as products designed for use within a managed environment.

This paper outlines an approach that Dell has developed and tested to meet the unique needs of education. Conceived as an easy-to-use solution for education institutions, it is designed to be simple to implement and manage, and to address a variety of mobile devices.

to make some crucial choices; deciding which mobile devices to buy or support is only one of them. Long before an institution places its first order for tablets for the media center, or allows teachers to incorporate smartphone apps into the chemistry curriculum, the IT department needs to design a sound strategy for provisioning, securing and supporting the devices that will be accessing the institution's network and resources.

When schools or campuses buy mobile devices, or when they open up their IT environment and invite students, faculty and staff to bring their own devices (also known as BYOD), the job of managing and securing the enterprise grows much more complex. Several questions need to be raised and answered so the proper IT strategy can be developed and put into place, starting with:

- How will IT accommodate the myriad end-user products running under iOS, Android and Windows 8, along with the Windows and Mac OS computers they already support?
- How can IT secure the network when it is opened to devices that the institution doesn't own?
- How can IT maintain compliance with federal, state and local laws and regulations, such as the Children's Internet Protection Act (CIPA) and section 508 Compliance, when students are accessing Web content via the institution's network?
- How can IT manage mobility network traffic and control/maintain network stability with the proliferation of mobile devices and the increased use of digital content in the learning experience?
- How will IT manage all those elements without putting new burdens on its budget and resources — especially in an era when institutions everywhere face tremendous pressure to accomplish more with less?

Policy enforcement and security are just as important for tablets and smartphones as they are for desktop and laptop computers. But managing mobile devices demands a different approach. A strong policy for institution-owned mobile devices and BYOD should cover device selection and security, and offer application controls.

Dell's education solution team has been working with IT professionals at many K-12 districts and institutions of higher learning to help address the challenges of incorporating the new generation of mobile devices into an existing IT infrastructure. To support this instruction model, Dell has developed a comprehensive approach to mobile device management based on its KACE K Series of endpoint systems solutions, as a systems management best practice to address the complex challenges that IT organizations face. This paper provides a proven approach, toolset and reference architecture (RA) that institutions can implement to manage multiple device types and operating systems (OSs). This best practice model applies regardless of the access model, whether you are implementing a BYOD initiative, purchasing mobile devices for the institution or both.

This paper also provides a detailed device management approach for institutions that are looking to adopt Windows 8 into their environment while still preserving the investments that have been made in legacy end-user mobility devices. Dell's mobility solution enables IT professionals to manage, secure and support the devices connected to their district or campus network — both fixed and mobile, and whether running Windows (including Windows 8) Mac OS, Linux, iOS or Android — all from an integrated management console.

Management, Service, Security

The Dell mobility solution for education addresses three areas of vital concern:

Device Management: This includes functions such as imaging and image management, deployment, application compatibility, user state migration, inventory and asset management, password management, patch management, reporting, desktop virtualization, and configuration and policy management. In conducting these functions, the strategy addresses both institution-owned and privately-owned devices, in order to protect the privacy of users who also keep content on their personal devices. With very few exceptions, Dell's mobility solution performs all of these device management functions for every end-user device that may be present in an education environment. Dell has thoroughly tested the solution against a broad set of common education use cases and end-user devices and documented the test results on page 9.

Service Simplification: As devices on campus proliferate in number and variety, so may the strain on the campus service desk, as end users call for help with everything from obtaining or resetting credentials and passwords to acquiring software to modifying configurations. A solution based on the K Series of appliances includes a portal through which users can easily perform many functions themselves. This significantly reduces the volume of calls that the service desk must field, while allowing users to get up and running quickly.

Security: Because mobile devices are at a higher risk of being lost or falling into the wrong hands than desktop systems, the IT staff must apply strong measures to protect sensitive data and user privacy. If a student, teacher or staff member loses a mobile phone or tablet, the IT department must be able to wipe institution-owned content from its memory and lock out access to enterprise content for that device. When students graduate or employees leave the institution, IT must be able to remove all enterprise content from their personal mobile devices, or remove all content from institution-owned devices before they can be reissued.

Dell's recommended solution incorporates the SonicWALL firewall, an easy-to-install next-generation firewall (NGFW) that is widely embraced in the education market. A single box that integrates all the necessary security applications, the SonicWALL firewall is deployed at the edge of the network to prevent malware, viruses and other attacks. It protects personal data on an institution's network and blocks access to unauthorized content. No school wants to land in the media spotlight because a child with a tablet has wandered onto an inappropriate site, or a hacker has stolen personal student information. The KACE K Series and SonicWALL solutions help to vastly reduce those risks, from endpoint to perimeter.

Diverse Assets, One Management Process

Dell's recommended mobility management strategy for education is delivered by the KACE K Series family of systems management appliances. The KACE approach treats mobile device management as an extension of the management process for desktop, laptop and server machines. With a single solution for all of its assets, an IT department can handle all trouble tickets through the same service desk, consolidate its reports on inventory and asset management, and apply IT policies consistently across all devices.

If you already have a systems management strategy in place, your solutions may have grown unwieldy and difficult to manage over the years — perhaps because you have customized them to address specific requirements, or because you have implemented different products to manage different types of devices. Also, your current solutions might not accommodate newer devices and operating systems. Dell's KACE-based solution can simplify or complement your overall management approach, allowing IT staff to handle all management functions through a single integrated management console. Whether you are building onto a legacy system or starting fresh, KACE appliance-based systems are easy to implement, offering rapid productivity gains and the control that is required.

The Dell KACE K Series includes:
KACE K1000 Management Appliance — a fully-integrated systems management solution for systems running the Microsoft Windows, Mac OS X and Linux OSs. In order to provide both broad visibility of all networked systems and depth of management control, the K1000 architecture supports both in-band (agentless) and out-of-band (agent-based) management. Agentless capabilities allow the K1000 to reliably

discover and inventory all systems on the network in real time, while the K1000 Management Agent provides the real depth of management capabilities required for managed systems.

KACE K2000 Deployment Appliance — a solution that automates the provisioning of systems running Microsoft Windows and Mac OS X. The K2000 core deployment functionality includes network OS installation, imaging, migration, inventory, systems recovery, pre- and post-deployment tasks, and an integrated deployment library. Plug-and-play deployment allows an institution to simply connect the K2000 to its network and immediately begin provisioning systems. The K2000 also includes its own integrated DHCP server, which speeds deployment for those institutions that do wish to utilize their existing DHCP servers for provisioning tasks. Additionally, the K2000 directly manages all PXE requests, eliminating the cost and complexity of requiring stand-alone PXE servers. The upcoming K2000 v3.5 release will include support for the UEFI boot environment for imaging.

KACE K3000 Mobile Management Appliance — a solution that integrates with other K Series appliances to detect, track and control personal and institution-owned mobile devices running both Apple iOS and Google Android in an enterprise setting. The K3000 helps IT manage both corporate and personal devices and protects sensitive content on those devices. The Dell KACE K3000 Appliance together with the Dell KACE K1000 Management Appliance offers a comprehensive, integrated, easy-to-use solution to manage all supported desktops, laptops, servers and mobile devices.

The K1000 and K2000 are available as either virtual or physical appliances. As a virtual appliance, they can each support up to 10,000 nodes. As physical appliances, they are available with three licensing options: small (0 to 1,000 nodes), medium (up to 3,500 nodes) or large (up to 20,000 nodes). The K3000 currently is available as a virtual appliance only. It supports up to 10,000 nodes. The physical appliance, available in April 2013, will scale in the same way as the physical K1000 and K2000 products.

If the user wants to enable functions that the basic KACE solution does not provide, such as private networks or single sign-ons, additional components are available to manage those activities. Dell has already engineered the necessary links, making it a simple matter to plug these components into the main solution.

A Proposed Solution for Mobility Management

To provide clear, practical information about how an education institution might implement a comprehensive systems management solution, Dell has developed a reference architecture (RA) and tested its performance in a series of use cases provided by Dell's education customers. These use cases represent a series of IT actions/activities that typically occur in education IT departments where there is a mix of devices and OSs. Figure A (on pages 6 and 7) illustrates those activities in an institution that has embraced the principle of BYOD.

Summary of use cases tested using the Dell RA:

1. Enroll mobile devices into the management environment.

2. Require domain users to register a password, or
3. Enforce a mobile user device passcode when trying to access resources from devices.
4. Install or uninstall enterprise applications.
5. Wipe institution-owned applications from a device, but not personal applications.
6. Remotely wipe all applications and data from a device if it is lost, and return it to factory settings.
7. Side-load applications. Side-loading in this context refers to the capability to automate the mass distribution of apps to many devices in one process, rather than downloading to one machine at a time through an app store such as Microsoft's Windows Store, Google's Google Play Store or Apple's App Store.
8. Automatically push out corporate Wi-Fi settings to end-user devices.
9. Automatically send application and operating systems patches to Windows and Mac devices.
10. Use Quest Password Manager to allow end users to reset their Active Directory (AD) passwords via self-serve portal.
11. Deploy a pre-configured Dell SonicWALL VPN client, allowing end users to access the network remotely without any additional setup.

The mobility solutions RA diagram in Figure B (below) depicts one possible (and suggested) deployment configuration. In this configuration, admin access to the KACE appliances is directed via LAN, Internet or cloud; the AD Server provides the authentication services to the entire IT infrastructure; Quest Password Manager provides password management services tied to the AD; the managed end-points are connected via LAN, Internet or cloud; an optional Bomgar appliance provides remote access and support to the end-points; and the Dell SonicWALL Aventail SSL

FIGURE B:
THE DELL MOBILITY SOLUTION REFERENCE ARCHITECTURE

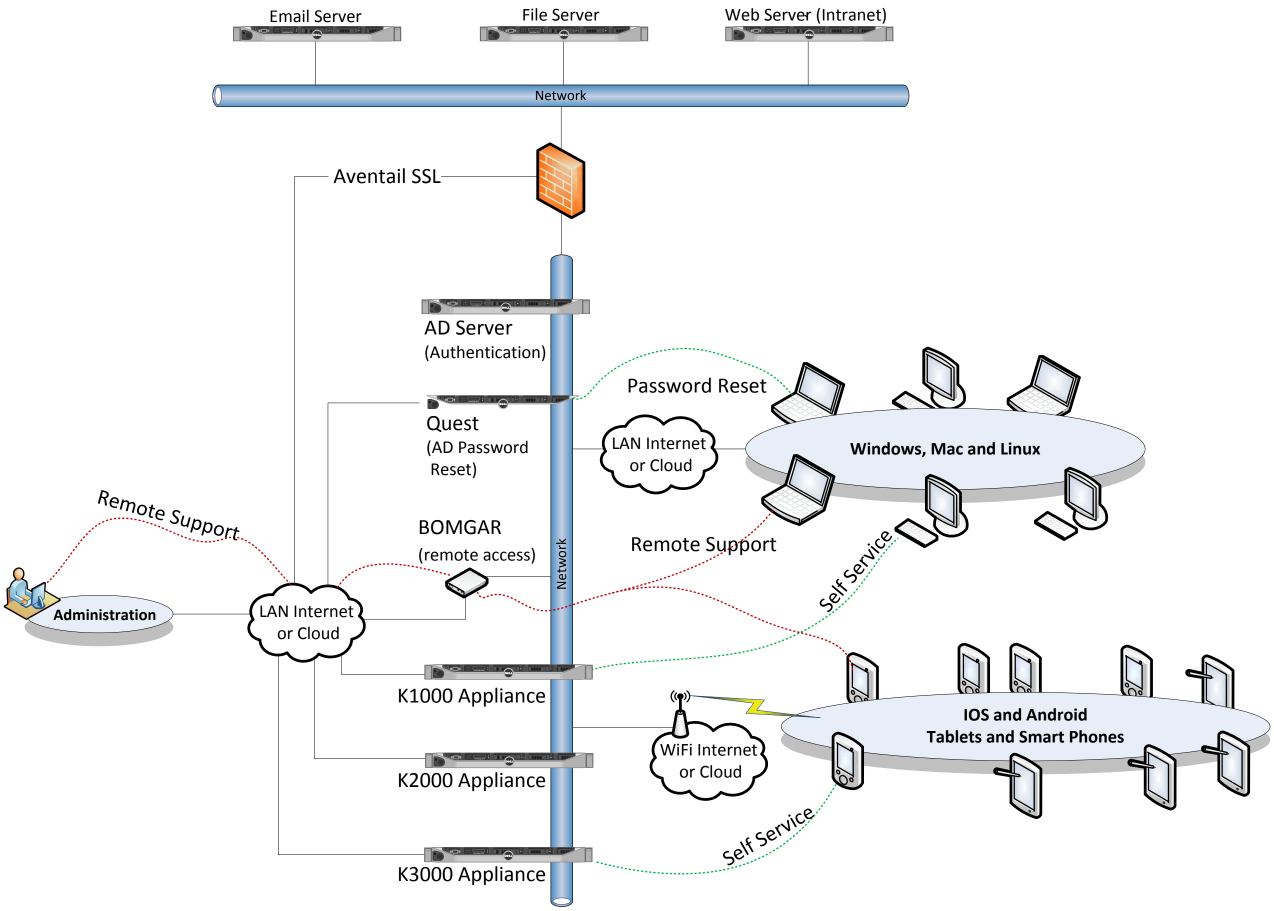


FIGURE A: MOBILE DEVICE MANAGEMENT LIFECYCLE NEEDS IN EDUCATION

DELL IDENTIFIED SEVERAL USE CASES THAT OCCUR WHEN IMPLEMENTING A MOBILE MANAGEMENT SOLUTION IN EDUCATION. TESTED TO ENSURE ITS MOBILITY SOLUTION MET THESE NEEDS.

CHALLENGE 1:

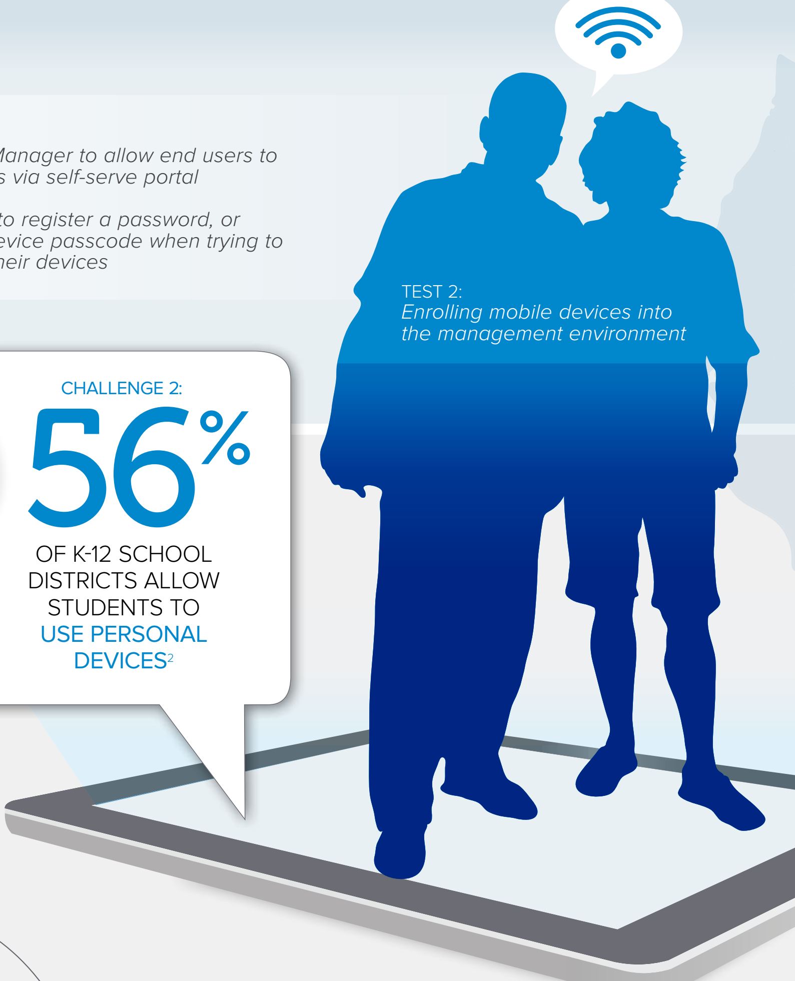
THE UNIVERSITY OF COLORADO, COLORADO SPRINGS' PASSWORD RESET REQUESTS WERE TOPPING OFF AT

2k

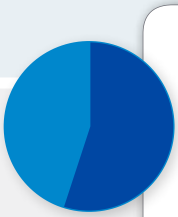
PER MONTH[1]

TEST 1:

- *Using Quest Password Manager to allow end users to reset their AD passwords via self-serve portal*
- *Requiring domain users to register a password, or enforce a mobile user device passcode when trying to access resources from their devices*



TEST 2:
Enrolling mobile devices into the management environment



CHALLENGE 2:

56%

OF K-12 SCHOOL DISTRICTS ALLOW STUDENTS TO USE PERSONAL DEVICES[2]

CHALLENGE 3:

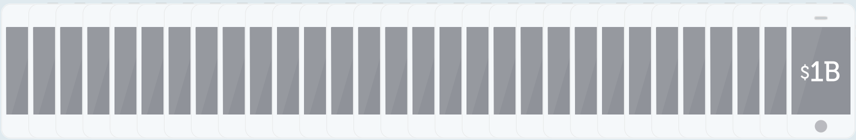
IN EARLY 2009, THERE WERE MORE THAN 3.5 MILLION LIVE@EDU HIGHER EDUCATION STUDENTS

JUST TWO YEARS LATER, THAT NUMBER MORE THAN QUADRUPLED TO MORE THAN

15M[3]

TEST 3:
Side-loading applications to many devices in one process, rather than downloading to one machine at a time from an app store

TEST 4:
Remotely wiping all applications and data from a device if it is lost, and returning it to factory settings



AVERAGES OUT TO $600M WORTH OF MOBILE PHONES LOST *PER STATE*

CHALLENGE 4:

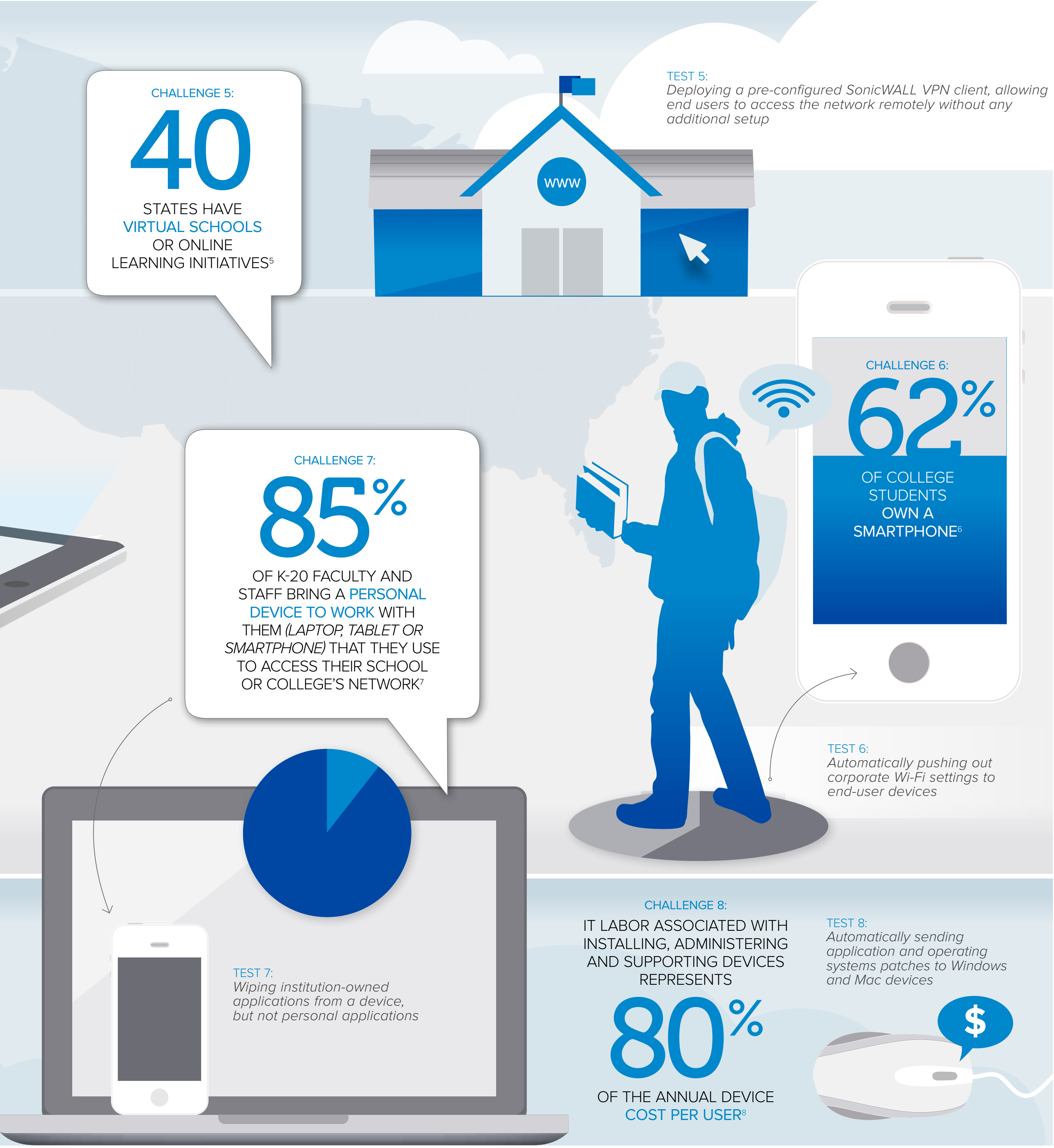
THERE ARE

$30B

WORTH OF MOBILE PHONES LOST IN THE U.S. EVERY YEAR[4]

SOURCES:
1. HTTP://DL.ACM.ORG/CITATION.CFM?ID=2382486&DL=ACM&COLL=DL&CFID=273595738&CFTOKEN=95084552 **2.** 2011-2012 CDE DIGITAL SCHOOL DISTRICTS SURVEY
3. WWW.LIBRARYSTUDENTJOURNAL.ORG/INDEX.PHP/LSJ/ARTICLE/VIEW/289/321 **4.** HTTP://MASHABLE.COM/2012/04/15/LOST-PHONE-INFOGRAPHIC/

THIS INFOGRAPHIC REPRESENTS THE CHALLENGES INSTITUTIONS FACE WHEN CONFRONTING THESE USE CASES AND WHAT DELL



CHALLENGE 5:

40

STATES HAVE VIRTUAL SCHOOLS OR ONLINE LEARNING INITIATIVES[5]

TEST 5:
Deploying a pre-configured SonicWALL VPN client, allowing end users to access the network remotely without any additional setup

CHALLENGE 6:

62%

OF COLLEGE STUDENTS OWN A SMARTPHONE[6]

TEST 6:
Automatically pushing out corporate Wi-Fi settings to end-user devices

CHALLENGE 7:

85%

OF K-20 FACULTY AND STAFF BRING A PERSONAL DEVICE TO WORK WITH THEM *(LAPTOP, TABLET OR SMARTPHONE)* THAT THEY USE TO ACCESS THEIR SCHOOL OR COLLEGE'S NETWORK[7]

TEST 7:
Wiping institution-owned applications from a device, but not personal applications

CHALLENGE 8:

IT LABOR ASSOCIATED WITH INSTALLING, ADMINISTERING AND SUPPORTING DEVICES REPRESENTS

80%

OF THE ANNUAL DEVICE COST PER USER[8]

TEST 8:
Automatically sending application and operating systems patches to Windows and Mac devices

5. HTTP://SLOANCONSORTIUM.ORG/PUBLICATIONS/SURVEY/GOING_DISTANCE_2011 **6.** WWW.EDUCAUSE.EDU/LIBRARY/RESOURCES/ECAR-STUDY-UNDERGRADUATE-STUDENTS-AND-INFORMATION-TECHNOLOGY-2012 **7.** CENTER FOR DIGITAL EDUCATION RESEARCH SURVEY, 2013 **8.** HTTP://BOICEENTERPRISES.TYPEPAD.COM/BLOG/VIRTUALIZATION/

appliance provides secure access to corporate resources such as email, files, Web applications or intranet resources. Additionally, the K1000 appliance provides a self-serve, Web-based portal for user activities (i.e., service requests or software downloads), and the K3000 appliance provides a Web-based portal for user device enrollment and information.

The specific versions used in the RA include:

- K1000 Management Appliance — version 5.1 SP1
- K2000 Deployment Appliance — version 3.4
- K3000 Mobile Management Appliance — version 1.0
- Dell Quest One Password Manager — version 5.0.1
- Dell SonicWALL Aventail SSL Appliance — version 10.6.2
- Optional: Bomgar appliance — Dell technology partner that provides an appliance-based remote end-user support solution

Dell conducted tests using the RA to determine how well the solution performed each of the use cases for the following devices:

- Dell Latitude 2120 with Windows 7 Pro
- Dell Latitude 3300 with Windows 8 Pro
- Dell Latitude 10 Tablet with Windows 8 Pro
- Apple MacBook with Mac OS 10.7.5
- Samsung Galaxy Tablet 2 with Android 4.04 (Ice Cream Sandwich)
- Apple iPad 2 Tablet with iOS 6.0
- Apple iPhone with iOS 6.0
- Motorola Droid Android phone with 2.3.4 (Gingerbread)

The testing approach assumed that all users have an AD account managed by the institution. It also assumed that for user-owned devices (BYOD), the management of those devices is contained to the management of the institution (enterprise) applications and configuration profiles.

The outcome of the tests is captured in Table 1 (page 9). All of the use cases were tested against the identified OSs and either:

- passed, as indicated by the "✓" mark;
- was not an applicable feature of the identified OS, identified by an "**O**" symbol; or
- functionality is not currently available using KACE as noted by the "■" symbol. *Note: These capabilities may be delivered using Dell partner products.*

The functional tests were conducted using two device categories:

- Notebook type device, including laptops, notebooks or tablets running supported Windows or Mac OS
- End-user mobile device, including tablets, iPads or smartphones running supported iOS or Android OS

Test and test execution details:

1. **Device enrollment**
   a. Notebook type device — mass or individual enrollment via K1000 appliance
   b. iOS and Android devices — individual enrollment via K3000 appliance
2. **Force AD password change at login**
   a. Notebook type device — Set by IT administrator via AD policy
   b. iOS and Android devices — Not a feature of these OSs to join devices to AD domains; user domain authentication may be achieved with these devices via Web interface (see #10 Quest self-service AD password reset)
3. **Set user device passcode**
   a. Notebook type device — passcode is not a feature of Windows or Mac OSs
   b. iOS and Android devices —configuration profile via K3000 appliance
4. **Install or uninstall enterprise applications**
   a. Notebook type device — mass or individual install or uninstall via K1000 appliance
   b. iOS and Android devices — mass or individual install or uninstall via K3000 appliance
5. **Wipe enterprise elements**
   a. Notebook type device — Not currently available as a standard feature set of the K1000 appliance (may be achieved via distribution, scripting and reporting modules)
   b. iOS and Android devices — via K3000 appliance
6. **Remote wipe (device lost or stolen)**
   a. Notebook type device — Not currently

TABLE 1:
MOBILITY SOLUTION USE CASE TESTING RESULTS

	Windows 7	Windows 8 X86	MAC OSX	iOS	🤖
Device provisioning/enrollment	✓	✓	✓	✓	✓
Force AD password change at login of domain connecting devices	✓	✓	✓	○	○
Set user device passcode	○	○	○	✓	✓
Install or uninstall enterprise applications	✓	✓	✓	✓	✓
Wipe enterprise elements	■	■	■	✓	✓
Remote wipe	■	■	■	✓	✓
Side-loading applications	○	■*	○	✓	✓
Configure Wi-Fi settings	✓	✓	✓	✓	✓
Patch applications & OS by remote action	✓	✓	✓	○	○
Quest self-service AD password reset	✓	✓	✓	✓	✓
Deploy SonicWALL VPN client	✓	✓	✓	✓	✓

○ Not a feature of the device operating system ■ Not currently available

Notes:

- *Application management on Windows 8 devices is currently designed to work for desktop mode only*
- *K3000 is not designed to initiate a full wipe on BYOD devices*
- *Dell SonicWALL deployment is without pre-configuration on iOS and Android*
- *Windows 7 and Windows 8 devices based on x86 architecture were tested*

* *You can install LOB Windows Store apps that are not signed by the Windows Store. The apps must be cryptographically signed and follow Microsoft deployment documentation. See Microsoft technote: http://technet.microsoft.com/en-us/library/hh852635.aspx*

available as a standard feature set of the K1000 appliance (may be achieved via third-party solutions)

b. iOS and Android devices — Full wipe (reset to factory settings) via K3000 appliance

7. **Side-load applications**

   a. Notebook type device — Not a feature of Windows x86 or Mac OSs

   b. iOS and Android devices — via K3000 appliance

8. **Configure Wi-Fi settings**

   a. Notebook type device — via Group Policy or Script via K1000 appliance

   b. iOS and Android devices — via profile K3000 appliance

9. **Patch applications and OS**

   a. Notebook type device — mass or individual patching via K1000 appliance

   b. iOS and Android devices — Not a feature of these OSs for mass deployment (users may enable automatic updates on individual devices)

10. **Quest self-service AD password reset**

    a. Notebook type device — via Quest Password Manager self-service portal

    b. iOS and Android devices — via Quest Password Manager self-service portal

11. **Deploy SonicWALL VPN**

    a. Notebook type device — deployment of a pre-configured client to eliminate the need for end-user manual configuration via script K1000 appliance

    b. iOS and Android devices — deployment of a VPN client via K3000 appliance (SonicWALL pre-configured client not available at this time)

Dell developed the RA and conducted the tests to provide a clear path for customers to implement an end-point management solution that will support an institution's mobility initiatives. As with all technology evolutions, the ongoing development of mobility technology presents some notable challenges. In designing an OS for mobile products, manufacturers have primarily focused on the needs of the end user and have not fully considered centralized management of these devices. Not all vendors have embraced certain capabilities, such as the ability to mass-deploy applications (side-loading). Nor do existing APIs allow for automated application and OS updates on mobile devices.

Direct customer application distribution of ISV applications for Windows 8 also presents some unique challenges that need to be considered. Currently, there is no way to effectively purchase a modern Windows application directly from an ISV and load it to a Windows 8 device outside of the Windows Store. Today, the only way to purchase apps is through the Microsoft Windows Store, which limits distribution to five devices owned by the same Microsoft Account. The supported modes of application distribution are evolving for this Windows 8 platform and are expected to support an effective side-loading approach in the near future.

In addition, for customers looking to leverage the UEFI standard to image devices over the network, the UEFI specification regarding network booting has not been finalized, so as such, there is no standard for native network UEFI booting. If network boot is required, Dell recommends setting UEFI-based machines to emulate old BIOS and to use PXE to boot them for image management functions.

Which Solution Meets Your Needs?

K-12 schools and institutions of higher learning take different approaches to supporting mobile devices. While some are not yet supporting them at all, many have purchased devices, or are allowing users to bring their own. The ideal route for integrating mobile devices depends a great deal on an institution's current situation, as well as its technology goals. Whatever an institution's particular needs, there is a solution available for managing and securing all end-user devices simply and efficiently.

Here are five typical scenarios, with recommended solution paths.

1. The Greenfield

The Situation: The college, university or school district has deployed desktop machines in its computer labs but has not yet created a mobile learning environment. It might be a new school, or it might simply be waiting for technologies to mature before adopting a mobile technology strategy.

The Challenge: The administration wants to give students mobile devices that its curriculum officials have recommended and that the IT department can manage easily.

Proposed Solution: The school purchases Dell Latitude 10 Windows 8 or Windows 8 Pro tablets for student use, supporting them with K1000 and K2000 management appliances.

2. Adding Windows 8 Computers to Existing Mobile Devices

The Situation: The school or district has purchased iPads or Android tablets for student use, or it is allowing individuals to use their personal devices. Administrators/faculty want to add Windows 8 devices to the mix, but they need a solution that will allow IT to manage all devices from a single integrated management console.

The Challenge: The existing collection of consumer-oriented devices is difficult to manage. For example, each time the IT department needs to distribute a new application to multiple devices, it has to buy the software through the appropriate app store. Since those stores make no provisions for volume purchases, IT must give each student a voucher to download the application individually. It has no control of these downloads and no way to confirm whether students have completed them successfully — or used the vouchers to buy something else entirely. Because there is no enterprise-level management capability, securing the mobile devices is a challenge. Also, because each device can support only one user profile and login, sharing devices among students is difficult.

Proposed Solution: To complement the Apple and/or Android devices already in use, the school purchases Dell Latitude 10 tablets with Windows 8 or Windows 8 Pro. It uses the K1000, K2000 and K3000 management appliances to manage all of these devices (Windows, iOS, Mac OS X and Android) from one integrated KACE management console.

3. One Device Per Student

The Situation: The institution has provided each student with his or her own device to support a blended or personalized learning initiative.

The Challenge: Institutions in this scenario face the same range of challenges as schools in scenario 2. The devices are difficult to manage, users must download applications individually from an app store, the institution can't control or confirm those downloads, the institution lacks the enterprise management capability to properly secure the mobile devices and devices are not easily shared among students.

Proposed Solution: The institution implements a device management solution such as KACE K1000, K2000 and K3000 to manage the Windows, Mac, iOS and Android devices present on campus, all from a single integrated management console.

4. One Device Per Many Students

The Situation: The school has purchased a limited number of mobile devices to be shared by all of its students. The school utilizes a homeroom model or a cart model for device deployment during the school day.

The Challenge: Schools in this scenario face many of the same challenges as in scenarios 2 and 3. The devices are difficult to manage, users must download applications for non-Windows devices individually from an app store, the school can't control or confirm those downloads, the school lacks the enterprise management capability to properly secure the mobile devices and devices are not easily shared among students.

Schools in this situation face other challenges as well. When students share devices, it is extremely difficult to manage their progress. For example, if Student A is working on Chapter 3 of a program and Student B is working on Chapter 6, the next time Student A receives a tablet and starts work on the program, the software might automatically jump to Chapter 6, causing confusion. Also, when a student enters personal information on a device, there is no way to wipe that information before the device passes into another student's hands.

Proposed Solution: The school implements a device management solution such as KACE K1000, K2000 and K3000 to manage all devices from a single integrated management console. Dell highly recommends Windows 8 or Windows 8 Pro devices for this kind of environment, since this OS allows the school to maintain an individual learning profile for each student, rather than one learning profile per device.

5. Bring Your Own Device (BYOD)

The Situation: The institution allows students, faculty and staff to bring personally-owned devices to campus. Users connect these devices to the campus network to access resources, applications and systems that the institution owns.

The Challenge: The large variety of devices and OSs present on campus creates a challenge for an IT department that needs to give users secure access to the enterprise network and resources. The IT department must implement basic password protection on each privately-owned end-user device. IT needs a simple, consolidated method for distributing in-house applications, as well as purchased applications, to Windows and non-Windows devices.

It must do this without relying on app stores, which don't allow for volume purchases and downloads. The IT department must be able to distribute software licenses to end users and harvest unused licenses for reuse. If a user's device is lost or stolen, IT must be able to remotely wipe all enterprise-owned software and data from that asset. In addition, IT must ensure that the student's personal device — which becomes an institution resource in a BYOD context — is not being used to access inappropriate content.

Proposed Solution: The institution implements a device management solution such as KACE K1000, K2000 and K3000 to manage Windows, Mac, iOS and Android devices from a single integrated management console. This approach ensures that all data passing to and from all devices will go through the appropriate firewalls and security measures, keeping data and enterprise assets safe and allowing IT to maintain content controls.

Conclusion

As BYOD and mobility initiatives become commonplace in education, institutions find themselves needing to manage a mix of end-user devices in the IT environment. To do this effectively, the devices require a comprehensive mobility management solution. Providing access to institution networks and resources while ensuring that the correct security, services and management capabilities are in place — all while minimizing risk — is a complicated task. Obtaining the right resources, processes and tools to drive a successful program requires careful planning.

Whether you are just starting a mobility or BYOD initiative at your institution, or you have already made progress in that direction, several key questions can help you determine the information you need to successfully implement the right solution:

1. What is the current and projected device profile that you will support in your environment?
2. Will the tools and processes currently in place be flexible enough to support the anticipated growth of your program?
3. What use cases will you need to support?
4. How can technology help you scale your IT resources while minimizing costs and additional IT management overhead?

Dell's mobility management specialists can help you explore these questions and tailor a strategy for your institution. For more information, contact your Dell account manager or salesperson.