Frequently Asked Questions About the Dell Kbox

What is Kbox capable of doing - and what is it not capable of doing?

The Dell Kbox is a so-called “systems management appliance” that simply allows for the management of technical aspects of multiple computer desktops from a single console, without the need to physically touch each individual computer. For example, instead of sending staff out to physically examine each of hundreds of computers for information security currency, a systems management appliance can easily keep track of information security configurations across all computers on a campus, without the need to impose on the individual computer user.

The Kbox is capable of the following:

* Information security monitoring (e.g. patch and change management)
* Computer configuration management(e.g. operating system updates)
* Software Distribution
* Asset Management (e.g. how many Apple computers do we have)
* Inventory (e.g. how many students are using SPSS)
* User Alerts (e.g. notice of unplanned downtime)
* Computer service tracking (e.g. how many times did this computer break down)
* Power management
* Desktop Dashboard (e.g. summary technical statistics on computer desktops)

The Kbox provides technical access to the capabilities of your computer that manage the above functions, but does not access any other information or data on your computer (see below).

What do you intend to use it for and which of its capabilities will not be utilized?

As noted in the attached document distributed to the Senate in January, the Kbox is being used initially as the means to ensure the campus is in compliance with our information security audit findings that require ubiquitous patch management for all campus computers. Kbox will also be used to facilitate distribution of software that’s licensed campus-wide, such as Microsoft Office. Although no specific plans have been made to use other listed features of Kbox at this time, it is likely that we will also use the asset management and inventory capabilities to provide aggregate reports regarding our campus-wide IT utilization. The user alert capabilities will very likely be tested as an enhancement to our Emergency Notification System (ENS), as this would allow emergency alerts to all campus computer stations at one time. Use of Kbox to enhance desktop power management may also be explored, if campus-wide savings can be accrued without affecting desktop usability.

**Will use of the Kbox be mandatory?**

Every campus-owned computer will have a Kbox applet installed that will allow for monitoring and update of critical information security features, such as patch management and operating system security updates. The Information Security Officer will thus have the ability to act quickly to monitor and mitigate any serious information security attack that might threaten the campus. Information security threats follow what might be called “the weakest link principle.” Hackers avoid computers that already have security updates and constantly seek out individual computers that are unprotected. Even one ‘weak link’ can compromise the entire campus. That’s why this particular aspect of use of Kbox is mandatory. However, even for information security, most non-critical computer updates will fall into the “strongly recommended,” “recommended”, or “advisable” categories, with varied levels of user control provided based on the risk involved. This is very similar to the situation with Microsoft, Apple, or cellphone vendors. On rare occasions, such vendors force mandatory software updates on our home computers and smart phones, because they know the threat is sometimes serious enough to warrant that approach. In most other cases, however, we’re provided with options for how we respond to updates (e.g. do later rather than now; choose not to do certain updates).

On very rare occasions, software used by departments or individual faculty may experience serious information security issues that Kbox may also be used to immediately mitigate. An example is the very serious compromise of a University Union software system last year, wherein dozens of computers campus-wide were being attacked from a single compromised desktop. Kbox could now be used to immediately notify the Information Security Officer of such compromises, as well as to immediately mitigate the problem. Without Kbox, many hours of manual intervention were required, causing delay, computer downtime, and greatly expanded risk and inconvenience to the campus.

As noted above, use of the Kbox will also be required for distribution and update of software that’s licensed campus-wide. However, distribution of such software will always be under the control of the college or department which owns the affected computers. In addition, individual faculty members will always have control over when and if software or software updates are placed on the computer(s) they use (with the exception of critical security updates noted above).

**Will use of Kbox interfere with my classes or instruction?**

No, all IT services are implemented with the intent of avoiding or eliminating interference with instructional activity. This principle is codified in the introduction to our campus information security policies in the following language:

The intent of these supplemental policies is to protect the campus from the risks associated with information security breaches, *while at the same time maintaining campus access to essential information technology functions and services. The application of these policies should therefore consistently consider how required information security controls can be implemented with minimal effect on user services. Whenever feasible, user input and collaboration should be obtained prior to the application of these policies to specific information security incidents.*

Even critical information security updates are scheduled during non-instructional time periods whenever possible. Non-critical software and hardware updates are always done during non-instructional periods and are also usually offered with both user notice and user control over the timing of updates. Updates to discipline-specific software would normally be under the control of college/department personnel. Kbox and its user scheduling features are available to colleges/departments, but use of Kbox for software updates and hardware maintenance is voluntary.

**If Kbox can inventory my computer, can’t it also access my email and look at my personal computer data?**

No, the Kbox provides no access to your email or personal data. It provides only a technical overview about your computer hardware and software configurations. In fact, one of the advantages of using the Kbox for systems management is that it eliminates much of the manual access to your computer that otherwise would have to take place, wherein your personal information might be exposed. The Kbox rather reports simple technical details about the university computer you use, such as the status of your security updates, the currency of your software updates, and the capabilities of your computer. These desktop statistics are used primarily on an aggregate basis, such as reporting on the number of computers of a particular type. Technical data for individual computers is only used when needed to respond to particular technical or security problems (e.g. which computers don’t have updated anti-virus protection) or which computers are due for maintenance).

April 4, 2011