



Alcohol and Tobacco Tax and Trade Bureau (TTB) Virtual Desktop Implementation

Allowing Bring Your Own Device with Minimal Policy or Legal Implications

August 13, 2012

Robert Hughes
Chief Information Officer
Department of the Treasury
Alcohol and Tobacco Tax and Trade Bureau (TTB)
robert.hughes@ttb.gov

Executive Summary

The Alcohol and Tobacco Tax and Trade Bureau (TTB) decided to reduce the costs, time and effort required to refresh desktop and laptop computers used for client computing needs. TTB has a widely dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about \$2 million and disrupted the IT program and business users for several months. TTB determined that the best solution was to centralize all client computing power and applications, user data, and user settings and allow access to TTB resources by thin client computing devices. A thin client is a computing device or program that relies on another device for computational power. Currently about 70 percent of TTB personnel use thin client devices to access all TTB applications and data.

TTB desktop and laptop computers were due for refresh this year. However, the virtual desktop solution allowed TTB to avoid the expense of replacing hardware. The savings achieved paid for TTB's virtual desktop implementation – which cost approximately \$800,000 – and saved TTB \$1.2 million.

TTB realized additional savings by developing a Linux USB device that can be used to turn old desktop and laptop computers into thin client computing devices for approximately \$10 per device. The TTB virtual desktop/thin client implementation uses a small browser plugin, freely available for almost every operating system, which simply turns the end user device into a viewer and controller of the virtual desktop running in the TTB computer rooms. No data touches the end user device. As a result, the TTB virtual desktop implementation has the significant additional benefit of delivering every TTB application, with user data, to a wide range of user devices without the legal and policy implications that arise from delivering data to or allowing work to be accomplished directly on a personal device.

Challenge

TTB was created as an independent bureau in the Department of the Treasury on January 24, 2003, by the Homeland Security Act of 2002. When TTB was established, all information technology (IT) resources, including capital assets, IT personnel and the funding to procure equipment and to develop core business applications remained with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). TTB was funded at a level sufficient only to reimburse ATF for existing service. No funding was provided for the initial purchase or subsequent replacement of any of the equipment required to establish and operate TTB's IT Systems. In FY 2005 TTB established an independent IT operation with no base funding to refresh infrastructure equipment.

TTB has a very dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about \$2 million and disrupted the IT program and business users for several months. TTB decided to reduce the costs, time, and effort required to refresh client desktop and laptop computers. After considering several solutions, TTB determined that it would centralize all client computing power and applications, user data, and user settings to allow access to these resources through thin client computing devices. A thin client is a computing device or program that relies on another device for computational power.

Approach

With limited funding to invest in a completely new infrastructure for the virtual desktop implementation, TTB examined its existing hardware, software and technical expertise to determine the path most likely to succeed and achieve the objectives of providing central access to all IT resources while achieving significant savings.

TTB attained considerable success with server virtualization. Approximately 80 percent of the Windows Servers and 20 percent of the Sun Solaris servers at TTB had been virtualized. With this success in hand, TTB was confident that a virtual desktop infrastructure could be built without purchasing numerous physical servers. The infrastructure required to deliver virtual desktop could itself be largely virtualized.

Because TTB was established in 2003 with a significant number of personnel working full time from home, it was imperative from the beginning to support those personnel with a robust remote access capability. Additionally, TTB wanted to take advantage of its investment in Citrix licenses and the significant expertise its technical personnel had gained with the Citrix product suite as they supported remote access. The Citrix virtual desktop offering uses a small browser plugin called Citrix Receiver, which is freely available for download and turns most any device into a thin device. This solution was selected because the Citrix Receiver allows TTB to create thin client devices and support BYOD (initially home computers).

The currently deployed solution has 2 active sites, each with 3 physical servers. Either site can support the entire customer base. The rest of the virtual desktop servers are virtualized. In essence, TTB supports the entire population (650 personnel total in TTB, CDFI, and contractors) with 6 physical servers. Figure 1 is a conceptual view of the TTB virtual desktop.

What is Virtual Desktop

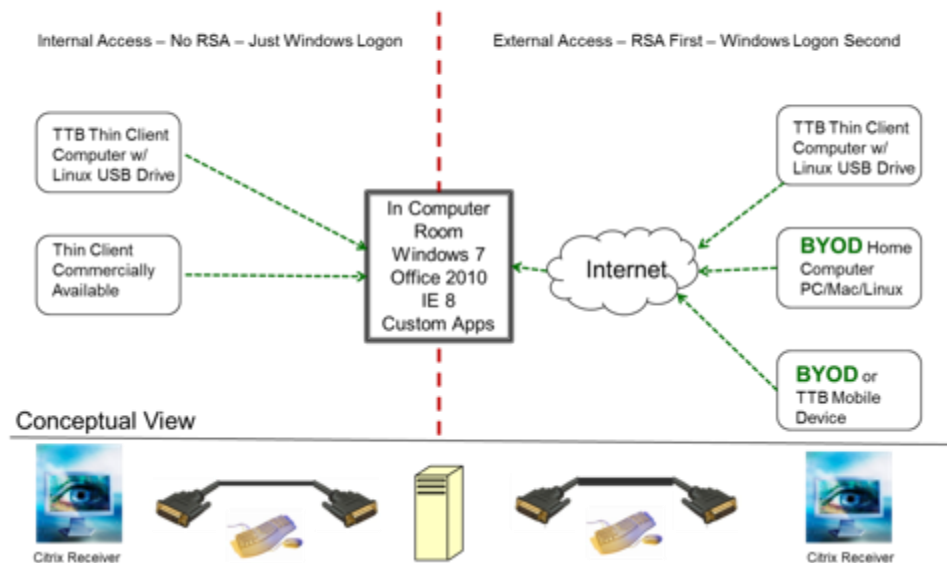


Figure 1
Results

Today about 70 percent of TTB personnel access all TTB computing resources through thin devices, provided by TTB as well as BYOD. There is no typical user setup. If the desired user configuration works, TTB allows it. As an example, a TTB attorney uses a thin client device in the office, a BYOD Mac personal computer when working from home, and a BYOD iPad device when on the road. Several TTB personnel use BYOD Kindle Fire devices for occasional access, for example, if they need to check email when out of the office or they need to approve a time card that was not ready when they were in the office.

The rapid pace of change in the mobile device market makes the virtual desktop solution particularly attractive. Because no data touches the user device, there is no need for a mobile device management (MDM) solution on a non-TTB device. When a device is made available to the public it can be used to access TTB applications and data. The Droid Razzr smart phone with a Motorola Lapdock 500 is an example of such a device. A user who has a government-provided smart phone (MDM installed) with a Lapdock would not need an additional computing device. Further, a user who had the same setup, minus the MDM, also could work full time with this BYOD. The ASUS Transformer is another example of a newly available mobile device that has a form factor usable for full-time work. The multiple-device access capability of virtual desktop allows TTB to move toward providing a single device per user.

The final result, which is likely the greatest benefit of the TTB Virtual Desktop solution relative to BYOD, is the minimization or elimination of complex legal and policy issues. Because no data touches the BYOD device and no work is physically accomplished on the BYOD equipment, all requests for discovery of information from a user's computer can be satisfied without having to recover anything from the user's personal device.

Lessons Learned

- The primary TTB BYOD lesson learned is to avoid allowing data to touch the personal device. Having all data, settings and processing in a central location and using the BYOD device simply as a viewer significantly simplifies the legal and policy implications.

Hardware/Software

- VMware for server virtualization
- 6 Dell R910 physical servers
- Citrix XenDesktop, XenApp, XenClient (pilot), Receiver, Citrix Provisioning Services
- Netscalers for remote access
- Robust Storage Area Network and Core Network required

Disclaimer

- References to the product and/or service names of the hardware and/or software products used in this case study do not constitute an endorsement of such hardware and/or software products.