

eXtreme Deployment: Distributing and Configuring 450 Student Laptops in Five Hours

E. Axel Larsson
Drew University
36 Madison Avenue
Madison, NJ 07940
+1 973 408 3048

elarsson@drew.edu

Russell Sprague
Drew University
36 Madison Avenue
Madison, NJ 07940
+1 973 408 3051

rsprague@drew.edu

ABSTRACT

Drew University has been recognized as a leader in Ubiquitous Computing since 1984, with the introduction of our Computer Initiative program, distributing more than 450 notebook computers to incoming students.

Drew's first Windows XP implementation did not register student computers into an Active Directory domain, instead opting for an unmanaged local account, which caused many support issues. By contract, having the computers in the domain would mean that users would not need a separate password to log in locally.

eXtreme Deployment was developed during the summer of 2003. Preloaded on the notebooks by the vendor, and built on open-source technologies, it identifies computers by their BIOS asset tag information and walks students through the process of joining the domain, and customizing settings for the user. With this, Drew is able to provide just-in-time personalization of student computers, without needing to pre-allocate them to specific students.

The Fall 2003 computer distribution using eXtreme Deployment was a success, registering over 450 computers into our domain in five hours. We have since integrated the technology into our staff computer deployment and have found the deployment technology to be quite flexible. Our paper will further explain the development and adaptability of this technology.

Categories and Subject Descriptors

K.6.4 [Computing Milieux]: Management of Computing and Information Systems – *System Management*.

General Terms

Management, Security, Human Factors, Standardization.

Keywords

Active Directory, Apache, Deployment, Imaging, Microsoft, PHP, Ubiquitous Computing, Windows, XML-RPC.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10–13, 2004, Baltimore, Maryland, USA.

Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

1. BACKGROUND

Drew's Ubiquitous Computing program (the Computer Initiative) began in 1984 when Drew's College of Liberal Arts became the first liberal arts institution to include student computers as part of tuition. The Computer Initiative budget also supplies all full-time faculty and staff with standard University desktop computers.

Drew first distributed laptops to students in 1988, and began providing email and other services via a central VMS system to students over the University's digital phone system at the same time. Ethernet networking was rolled out to student residence halls starting in 1997, with all halls wired with "one jack per pillow" in time for fall semester 1998.

Drew's primary directory service is Novell eDirectory[1], with all students, faculty, and staff having a single eDirectory login (referred to as a "uLogin" account), which provides access to all networked resources. Central file and print services are provided by a NetWare 6 (soon to be 6.5) cluster[2], with all student, faculty, and staff computers using the Novell Client software for access. Single-password, single-sign-on access to web applications such as our Webmail system and Blackboard[3] is provided by Novell iChain[4] in conjunction with a user's eDirectory login.

Prior to 2002, Drew's supported network clients consisted almost entirely of a mixture of Windows 95 and 98 systems, with a small number of Windows 2000 systems located in computer labs. No support was provided for end-users running Windows NT or Windows 2000 on their own machines, and as a result account management on user workstations and the need for a Windows domain was not a concern. Because of this, Drew was able to maintain its Novell-only environment until Windows XP was introduced to campus in 2002.

Deployment and management of the Windows 95 and 98 workstations was comparatively simple. All computers were issued having been imaged with a standard Drew configuration, including the Novell Client software, an office suite, and other standard applications. No customization of individual computers was required. Application and patch management for these workstations, including student notebooks, was accomplished using Novell ZENWorks for Desktops[5] software, primarily the Novell Application Launcher.

With the introduction of Windows XP to the campus in 2002, the scene changed markedly. Drew's first rollout of Windows XP was with the 2002-2003 student notebooks. With this initial rollout of Windows XP, very little changed in terms of the

imaging process used. To avoid having to manage local accounts, all users logged into the same local “Drew User” account with Administrator privileges as well as logging into their Novell eDirectory account via the Novell Client for networked services. This configuration most closely mirrored what we had been doing with Windows 9x and meant that the individual machines did not need to be customized in any way.

Realizing that this was not a suitable long-term solution and to support forthcoming faculty and staff Windows XP deployments, Drew created a Windows 2000 Active Directory domain in August 2002. Novell DirXML[6] was implemented to synchronize user accounts and passwords between our existing Novell eDirectory tree and the new Active Directory domain. Using DirXML, we are able to maintain the illusion of a single uLogin account and password for all network services.

Throughout the 2002-2003 academic year, Windows XP workstations were deployed and added to the Windows domain manually. Workstations were imaged with a standard Drew configuration, which had been configured to run the Microsoft Sysprep[7] “mini-setup” utility on first boot. Upon delivery of a computer to a faculty or staff member’s office, a Computing and Network Services staff member would have to manually go through the mini-setup procedure, naming and adding the computer to the domain, and adding the required domain users to the local Administrators group.

Since the summer of 2003, all Drew Windows XP computers have been configured using our eXtreme Deployment system. eXtreme Deployment is invoked automatically on first boot after imaging, and automatically configures the workstation for use in the domain based upon its BIOS serial number and configuration information containing in a central deployment database.

2. THE PROBLEM

The first year that Drew University provided laptops with Windows XP to its students was the 2002-2003 school year. We did not have an Active Directory domain on campus, and had to have students use local accounts on their laptops. Students were able to authenticate to Novell eDirectory with the Novell Client, but that only provided them access to network resources. The laptops were configured with a generic account, named Drew User, which they would log into by default.

This caused a number of problems throughout the school year. The Drew User account had no password, leaving the computers quite insecure. Students would add a password to the Drew User account, sometimes changing the Administrator account’s password as well and forgetting both, leaving them locked out of their own machine. Some students would create a new account, deleting the Drew User account, using instead an account that was not customized with a Mozilla profile and other needed settings.

Once an Active Directory domain infrastructure was put into place and configured to operate with the existing NDS framework, we were able to let students log in as themselves. An updated version of the configuration for the laptops was made using Microsoft’s Sysprep system preparation utility. Students logged in once with the same username and password, to both the Novell network and their laptop. The credentials would be cached, allowing them to continue to use it off the campus network. By being in the domain, the helpdesk had more methods to fix a laptop where the

student’s account and the Administrator account were not available. Students could no longer accidentally lock themselves out as easily.

When preparing the image for the 2003-2004 school year laptops, a new problem was recognized. When a machine had the updated configuration installed on it by the helpdesk, a student employee was there to walk the computer through the mini-setup that ran after it was first booted, finishing up Sysprep’s work. While mini-setup is fairly user friendly and self-explanatory, we could not use that for the incoming class. Students would not name their computers properly, join the domain incorrectly, or they wouldn’t be an administrator on their own machine.

A few options were considered. Having the vendor customize each laptop for an individual student was too costly. Using student employees to customize each laptop for a given student was considered. Commercial imaging software packages also required us to know ahead of time which student would be getting which exact laptop. Based on the logistics of our handout procedure, that was not an option. Methods to refine the procedure were considered, such as having students show up in a pre-assigned order, arranging the laptops physically in the same order that the students would arrive. All of these possibilities were carefully considered and deemed impractical.

Ultimately, it was decided that we needed to design our own method of deployment. One that replicated the features of Sysprep, but was automated and required as little user input as possible. It would have to be flexible enough that after computer handout, it could be customized for the student who received it.

3. THE TECHNOLOGY

eXtreme Deployment is built on top of a several open-source and commercial technologies. The major design emphasis for the project was on rapid development and ease of modification to support all of Drew’s standard computer configurations.

3.1 Server Components

The deployment server is responsible for providing deployment clients access to the deployment database. Clients communicate with the server by sending XML-RPC[8] messages over a secure (SSL) HTTP connection.

XML-RPC was chosen as a client/server protocol because XML-RPC libraries are available for a wide variety of languages. It was also chosen because it has a simplicity advantage over the competing web-services protocol SOAP[9]. In general, the usage of a web-services protocol meant that we did not need to develop our own protocol server (we used Apache on Windows), and that securing client/server communication was easily facilitated through the use of SSL.

The XML-RPC server itself is implemented in the PHP[10] scripting language running atop the Apache[11] web server on a Windows 2003 Server. PHP/Win32 was particularly well suited to this project, as it enabled us to leverage our existing in-house UNIX PHP development experience to develop a Windows server application. PHP provides the necessary COM bindings[12] that enabled us to access Active Directory via its native ADSI APIs[13] directly from within a PHP application.

The deployment database is implemented on Microsoft SQL Server 2000[14] and is actually a subset of tables within a larger

database we use for University computer asset tracking, called uTrack. There is tight integration between uTrack and the deployment system, as computer ownership information and serial numbers are obtained directly from existing asset tracking data. Our use of Microsoft SQL Server for the deployment database enabled us to take advantage of our existing investment in SQL Server for our home grown asset tracking. Integration with the asset tracking application eliminated the need for duplicate data entry between the two systems. Access to the database from the deployment server PHP scripts was accomplished via ODBC.

3.2 Client Components

The eXtreme Deployment client interface is HTML based and is presented to the user in the Internet Explorer web browser operating in “kiosk” mode. This method was chosen over a standard Win32 client application, as we were able to take advantage of existing web applications development experience available in the department. Additionally, the HTML-based interface can be easily customized by non-programmers.

The web-based interface is served up to client workstations locally, using a local instance of Apache and PHP installed on each client PC. Apache is configured to listen on the loopback interface only, and only runs during the deployment process.

The deployment client also contains an updater component. The updater component runs prior to deployment and checks the deployment server for an updated version of the client components. The updater is responsible for downloading updated packages, verifying their digital signatures, and installing them as necessary.

4. THE PROCESS

During the summer, before the start of the school year, a custom configuration is developed for the laptop. The standard Drew software is pre-installed on this configuration, as is the eXtreme Deployment client. This configuration is given to the vendor, who images all of the laptops with it.

During new student orientation, incoming students receiving a computer are each given a time period in which they may pick up their laptop. Upon arriving at handout, we verify their eligibility, and they are then given a laptop and accessories. When a student is given a laptop, its serial number and the student’s ID are entered into a web application by student employees. This allocates the laptop to the student in uTrack, creates an account for the laptop in the campus Active Directory domain, and associated the notebook with its AD account and owner in the deployment database.

The student unpacks their laptop, connects it to the campus network jack in their room, and boots it. The laptop automatically logs into a local account, called Deploy, which runs the eXtreme Deployment bootstrap.

The eXtreme Deployment process contacts the deployment server, checking for newer versions of the layers present on that machine. If newer versions exist, the updated layers are downloaded and installed.

Next, a local instance of Apache is started and a full-screen web browser window is opened. The client obtains the asset tag information from the SMBIOS of the machine, and passes this to the deployment server in an XML-RPC request. The information

entered into the deployment server by the handout script is returned, giving the client all that it needs to customize the machine.

Once the student verifies the information’s validity, the computer is renamed appropriately. A SID generator utility is run to change the system’s SID, and is completed with a reboot. After the computer has been rebooted, the student enters their credentials to join the computer to the Active Directory domain account created for it.

After a second and final reboot to finish joining the computer to the domain, the student is added to the local Administrators group, the local Administrator account is given a random password, and its password is stored on the deployment server in a secure database. The auto-login of the Deploy account is disabled, its password is also randomized, and Deploy is logged out, leaving the user with a fully deployed machine.

The first time the student logs into the machine, a Mozilla profile is created for them, with customized email settings and appropriate Drew bookmarks. The Mozilla profile creation script is part of the Windows default user profile, and thus it will also be executed for any subsequent user that logs in.

5. THE RESULTS

The 2003 laptop handout was a complete success. Students living on campus brought their laptops back to their dorm rooms to deploy, while the small number of commuters quickly deployed their machines at stations we had prepared for them. A few machines locked up after joining the domain, but we believe that was due to the volume of work the servers were handling. Over four hundred and fifty machines joined the domain in five hours.

Since then, we have begun using eXtreme Deployment with all of our Windows XP configurations. The prior year’s student laptop model was the first to be upgraded, followed by the faculty and staff desktops. A web page, similar to the web application used at computer handout, is used to add machines to the deployment database as needed. Once a machine is assigned to a user in uTrack, the web form is filled out, and the computer is ready to be deployed on delivery.

eXtreme Deployment has improved workflows in the university in a variety of ways. For example, because the computer’s name and customized list of local Administrators is pre-defined in the deployment database, laptops that are loaned to customers while they are waiting for their computers to be repaired are entered into the system and are easily reset and redeployed after use. Furthermore, due to the self-updating nature of eXtreme Deployment, we have been able to update settings such as default Mozilla bookmarks or server settings after a network infrastructure change without having to update every existing configuration. Finally, during this past spring, when the Sasser worm affected machines that were deployed, we were able to easily retrieve the Administrator passwords from the secure database in order to quickly clean them while they were disconnected from the network.

This system can be easily customized for a number of environments. For example, one of the student helpdesk employees has already begun adapting it for his former school district for use in their schools. eXtreme Deployment is released under the revised BSD license, and is available for institutions

that wish to use it. A number of institutions have already expressed interest in using eXtreme Deployment.

6. REFERENCES

- [1] <http://novell.com/products/edirectory/>
- [2] <http://novell.com/products/netware/>
- [3] <http://blackboard.com/products/academic/lis/>
- [4] <http://novell.com/products/ichain/>
- [5] <http://novell.com/products/zenworks/>
- [6] <http://novell.com/products/nsureidentitymanager/>
- [7] *How to use Sysprep, An Introduction.* <http://microsoft.com/windowsxp/pro/using/itpro/deploying/introduction.asp>
- [8] <http://xmlrpc.com/>
- [9] <http://ws.apache.org/soap/>
- [10] <http://php.net/>
- [11] <http://httpd.apache.org/>
- [12] *PHP: COM support functions for Windows.* <http://php.net/manual/en/ref.com.php>
- [13] *Active Directory Services Interface Overview.* <http://microsoft.com/windows2000/techinfo/howitworks/activedirectory/adsilinks.asp>
- [14] <http://microsoft.com/sql/>

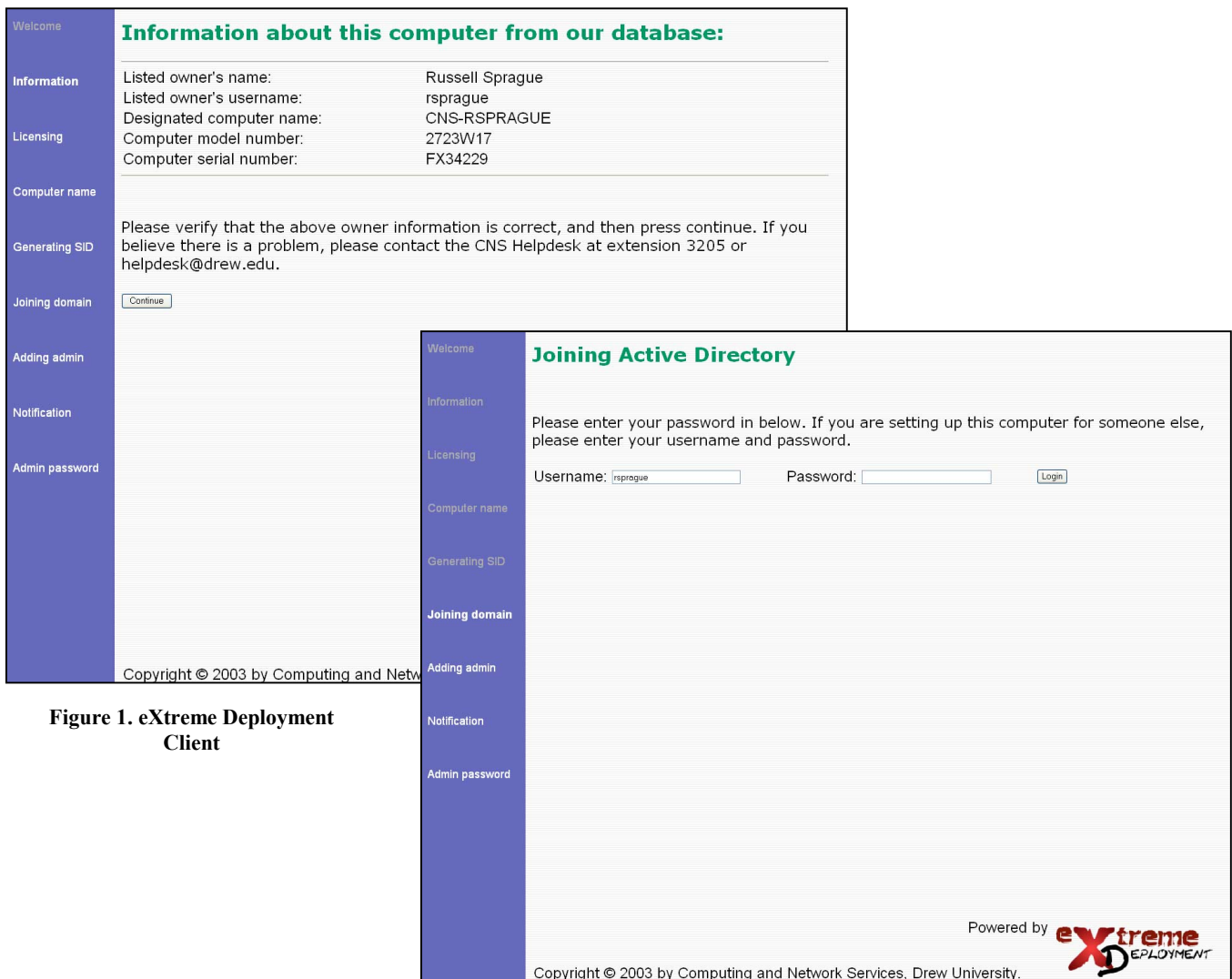


Figure 1. eXtreme Deployment Client