WHITE PAPER

Creating the Perfect Mac Lab in Higher Education

Modern technology for the modern student

Today's students are accustomed to leveraging technology as part of their education. For in-class learning at K-12 environments, many are offering 1-to-1 iPad programs. While some universities are moving towards a 1-to-1 iPad model, such as **The Ohio State University**, many others are relying on computer labs to offer the technical tools students need.

In order to set these young adults up for professional success, higher education institutions need to equip students with secure technology and a customized experience when they sit down at any computer in the lab.

Labs are a cost-effective and efficient way to ensure students have access to a computer with the apps they need to be successful, saving students the cost of purchasing computer hardware and software. Labs ensure digital equity for students who would not otherwise be able to afford these luxuries.

And, many university computer labs are Mac labs. Mac has a longer shelf life than PC, countless educational apps and students **simply prefer them**.

To see how Jamf amplifies the power of Mac labs in higher education, visit: **www.jamf.com**

MAKING LABS POSSIBLE FOR STUDENTS

Whether a student is writing a term paper, designing graphics or creating a mobile app, their permissions and access need to be both consistent and secure regardless of which Mac or lab they choose on a particular day.

While labs provide students with a straightforward user experience, they can present a significant technical challenge for IT and their staff.

With limited budgets that are often segmented by department, today's university IT tend to rely on traditional imaging practices to:

- Maintain the Mac lab and keep each computer current to avoid viruses and costly data breaches.
- Keep student data private, even though potentially hundreds of students are interacting with the same machine on a daily basis.
- Ensure students have access to the materials they need each time they log in.

IMAGING MACHINES AS THE DEFAULT

To get Mac labs up and running, IT has typically built a base image that includes the operating system, applications, software and settings IT deems as potentially needed by every student. This image is created leveraging an imaging tool to build a fully functioning version of macOS for each Mac.

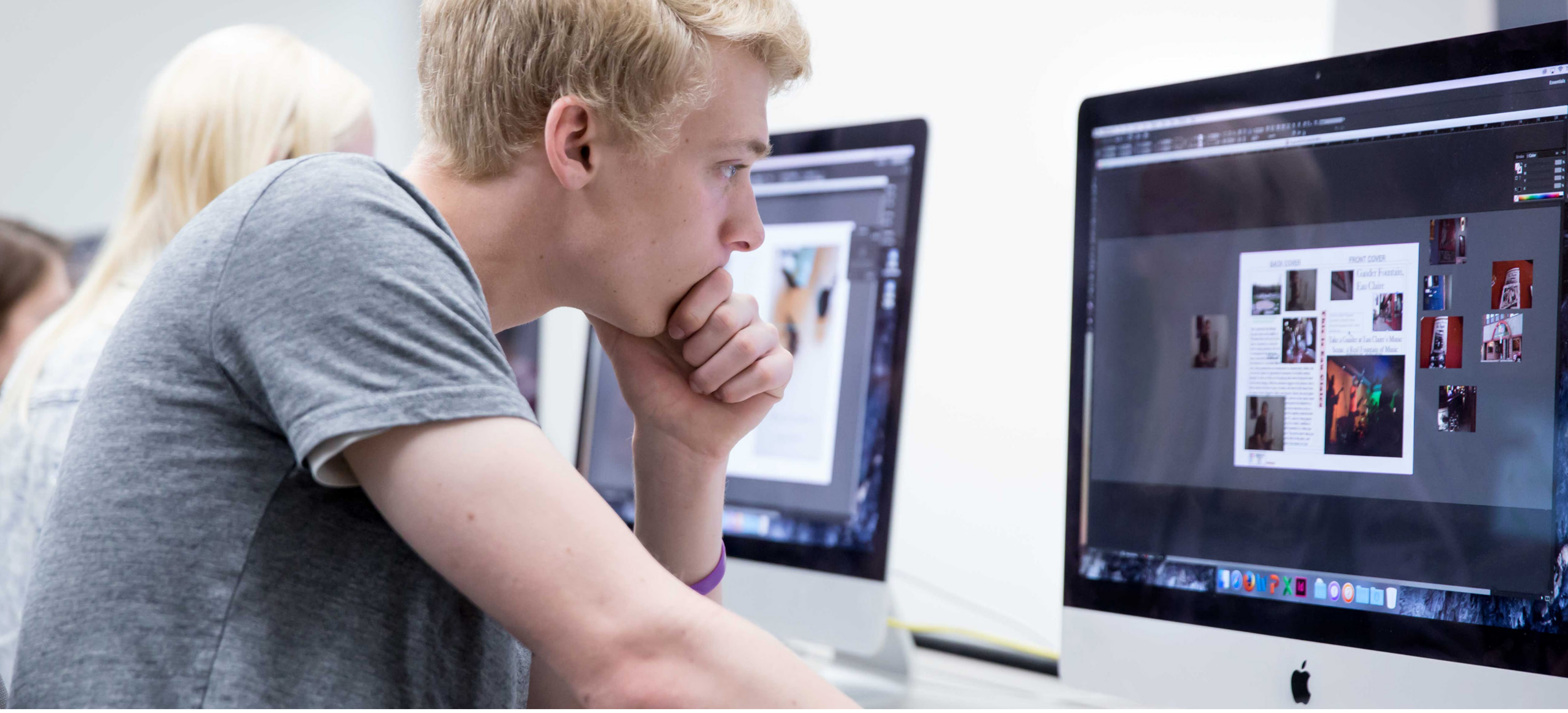
Once the base image is created, IT then manually installs the image by plugging in a thumb drive to each Mac. This requires a lot of hands-on, time-consuming work from IT. Not to mention that base images are typically large files that take a long time to load. And, while images are loading, students are unfortunately not able to access the machines.

This traditional method requires higher education IT staff to spend lots of time creating a bloated base image that will become obsolete the next time a new version of the software is available. When that happens (and it happens a lot), IT reverts back to updating their image to start the process all over again. In short, imaging equates to a vicious cycle of constantly and manually updating machines.

On top of this, and more importantly, an additional layer of security has been added to Mac in the form of the Apple T2 chip which eliminates imaging as an option. The T2 chip controls everything from power management to audio controllers and offers a new level of native security on the Mac with a feature called Secure Boot.

Per Apple: During startup, Mac verifies the integrity of the OS on the startup disk to make sure that it's legitimate. If the OS is unknown or can't be verified as legitimate, the Mac connects to Apple to download the updated integrity information it needs to verify the OS. This information is unique to the Mac and ensures that the Mac starts up from an OS that is trusted by Apple.

From a security perspective, this is fantastic news for organizations, IT and users. But, the traditional workflows of pushing OSs over the network or block copying monolithic images via cables to Mac devices is rendered incompatible on new Mac hardware with an Apple T2 chip. As such, imaging is not an Apple or Jamf recommended workflow.



OPTIONS FOR BUILDING YOUR MAC LAB

Technology is evolving and making it easier for higher education institutions to maintain secure and up-to-date Mac lab environments. For starters, IT now has options when creating and maximizing their Mac labs. We've ranked these options as OK, better and best.

1. OK: Binding to Active Directory

Active Directory (AD) is an authentication service for on-premises identity and account management. **NoMAD** is an open-source app that lets users bind to AD, however, its main purpose is to help move Mac computers off binding to AD while still getting all of the AD benefits.

By using single sign-on functionality, universities can essentially "casually bind" to AD. Users authenticate first to a local account on the Mac, then authenticate to their network account via NoMAD. NoMAD communicates with Domain Name System (DNS), Kerberos and Lightweight Directory Access Protocol (LDAP) to gather the domain record, authentication ticket, and user identity and groups. Importantly, there's no persistent directory service connection.

If you're unsure if eliminating binding is right for you, NoMAD can help you make the transition as all of NoMAD's features work while bound to AD as well. This way IT can migrate systems to the better or best options when ready.

2. Better: Just-in-time account creation

While NoMAD is great for keeping local Mac user accounts in sync with AD, **NoMAD Login** goes one step further and ensures Mac user accounts start out in sync with AD.

To do this, NoMAD Login empowers IT to manage authentication with the macOS loginwindow. This allows IT to customize the login experience for each Mac lab user and offers just-in-time user creation.

Instead of syncing Mac lab users from AD, just-in-time accounts are created and updated dynamically when the user logs in. This is accomplished by connecting the Security Assertion Markup Language (SAML) assertions sent by the higher education institution's identity provider.

3. Best: Cloud-based authentication with Jamf Connect

Building off what NoMAD and NoMAD Login offer, **Jamf Connect** provides the ideal experience for users and IT. By seamlessly integrating with a variety of cloud identity providers, such as Okta, Microsoft, Google, IBM, OneLogin and Ping, Jamf Connect allows for a simple provisioning of a user from whichever cloud identity service chosen. This is all done during the Apple provisioning workflow and is complete with multifactor authentication — no AD or LDAP necessary.

And that's a wonderful thing, since AD and LDAP:

- Allow students to change their passwords, which causes confusion and costly help desk tickets when a Mac lab user inevitably forgets their password.
- Make it extremely difficult to implement multifactor authentication to increase security protocols.
- Don't allow admins to deploy commands or scripts in the form of policy documents that apply settings to the Mac computers and users within their control. This prohibits the personal experience users crave when logging into a shared Mac.

With Jamf Connect, users simply login in on the shared Mac and can access every system-approved application after signing in with a single set of cloud identity credentials.

Benefits include:

- **Account creation:** Create local Mac accounts based on Okta, Microsoft Azure, Google Cloud, IBM Cloud and OneLogin identities, resulting in an improved login experience for users and organized fleet of Mac for IT to manage.
- **Secure enrollment:** Leverage modern authentication to track and monitor what Mac is being accessed, from where and by whom, ensuring the right student is on the right Mac before deploying anything sensitive.
- **Eliminate shared admin accounts:** Create multiple IT admin accounts leveraging permissions from the cloud identity provider, without requiring the use of shared service accounts.
- **Enforce password policies:** Admins can enforce password policies via the identity provider, maintaining consistency and security across all users.
- **Password synchronization:** Keep the Mac username and password in sync with Okta, Microsoft Azure and PingFederate credentials, leveraging a single identity for everything needed for students to be productive.

THE ROLE OF MOBILE DEVICE MANAGEMENT (MDM)

By adding a management solution such as **Jamf Pro** to the university's technical stack, IT can leverage automated mobile device management (MDM) enrollment the first time a user logs into a Mac. The process is simple and secure:

1. A user is invited to enroll in the automated MDM enrollment.
2. During the enrollment, Jamf Connect is downloaded and installed from the MDM server.
3. Users are taken directly to the Jamf Connect login window, as opposed to creating their own username and password.

The student has the same username and password for everything, creating an incredible experience while also establishing account security.

With management in place, IT can now go to work creating the perfect Mac for the individual in front of it. For starters, IT can use **Apple School Manager** to set configurations for each Mac and have these automatically in place when the machine logs in.

IT can also purchase apps in bulk from the App Store and assign them to the appropriate Mac, including all apps in the Microsoft Office suite. Leveraging an MDM tool to automate the deployment of apps is a perfect way to get the most common apps on machines and empower students to start learning the minute they log in. No Apple ID required.

For software outside of the App Store, such as Adobe Creative Suite, IT can leverage Jamf Pro to go beyond basic management capabilities and enable remote software installations. And for an even more personalized experience that equips students with the specific apps only they need, IT can leverage an MDM tool that offers a **self-service style portal** where they can place approved apps and resources students can download when they need them. With educational items on demand, students never have to submit a ticket or request an item, and IT isn't inundated with one-off software requests.

And last, but certainly not least, when it comes time to upgrade all the Mac in your computer lab, you determine when and how to do it. If you're not ready to **upgrade to macOS Catalina**, simply block and defer the upgrade for up to 90 days. Once sufficient testing has been completed, either keep data in place on all machines and upgrade or erase and start fresh.

Jamf and higher education

Searching for a better way to manage a Mac lab is how Jamf got its start. When Jamf co-founder, Zach Halmstad, was an IT admin at the University of Wisconsin—Eau Claire, he recognized the need for better workflows to manage Mac.

Seventeen years later, Apple and Jamf have made it easier than ever for higher education IT to focus on more strategic initiatives that drive education forward, instead of the manual, antiquated methods of device connection and management.

Request a free trial of Jamf Connect and/or Jamf Pro and see what happens when the time-consuming ways of maintaining a Mac lab become a thing of the past.

Start Jamf Connect Trial **Start Jamf Pro Trial**

Or contact your preferred authorized reseller of Apple devices to take Jamf for a test drive.

jamf
www.jamf.com