IS&T Automated Device Enrollment Program for Macs

IS&T Automated Device Enrollment Program for Macs

Apple provides Automated Device Enrollment (ADE, formerly known as DEP) as a way of deploying institute-owned macOS or iOS devices. This process works by technicians providing the serial number of any device they would like enrolled into the ADE program to IS&T. IS&T will then upload the serial number to Apple and assign it to the correct Mobile Device Management (MDM) server. Once the computer has been booted, it will automatically receive any policies that have been supplied by the MDM server.

IS&T provides ADE as a service to the MIT community in conjunction with either IS&T's MDM server (Jamf Pro) or your department's own MDM server if you have one. If you are interested in our Jamf Pro offering, please visit our Jamf Pro page for more information. There is no cost associated with either the ADE or Jamf Pro services.

Please note machines must be purchased through an official MIT channel for this to work. Machines purchased through retail stores can be manually enrolled in Jamf Pro, but are not eligible to Automated Device Enrollment.

IS&T will also provide training and one-on-one time for both ADE and Jamf Pro if requested.

Contact Information

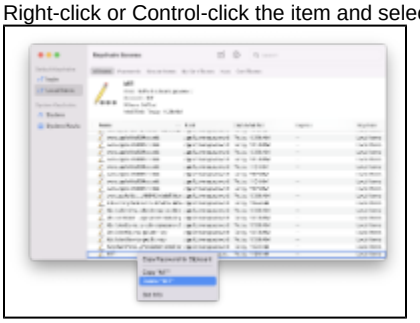
If you would like to enroll computers or have any questions regarding ADE they should be emailed to **euc-help@mit.edu**.

ADE Process

1. Send the serial numbers you'd like to enroll to euc-help@mit.edu.
2. The IS&T End User Computing (EUC) team will enroll your Mac into ADE and confirm it is enrolled.
3. Boot your new or re-imaged Mac (not before above step!).
4. Go through the Setup Assistant. If you're using a wired connection on campus, you must use on an already registered Ethernet dongle. If using Wi-Fi, you can use the "MIT" network. You can also connect from off-campus networks.
5. You will then see a screen that says *"Remote Management"*. If you do not see this screen, contact the EUC team to double check enrollment.

   ⚠ If you missed the *Remote Management* screen
   - On macOS High Sierra or newer, run `sudo profiles renew -type enrollment`

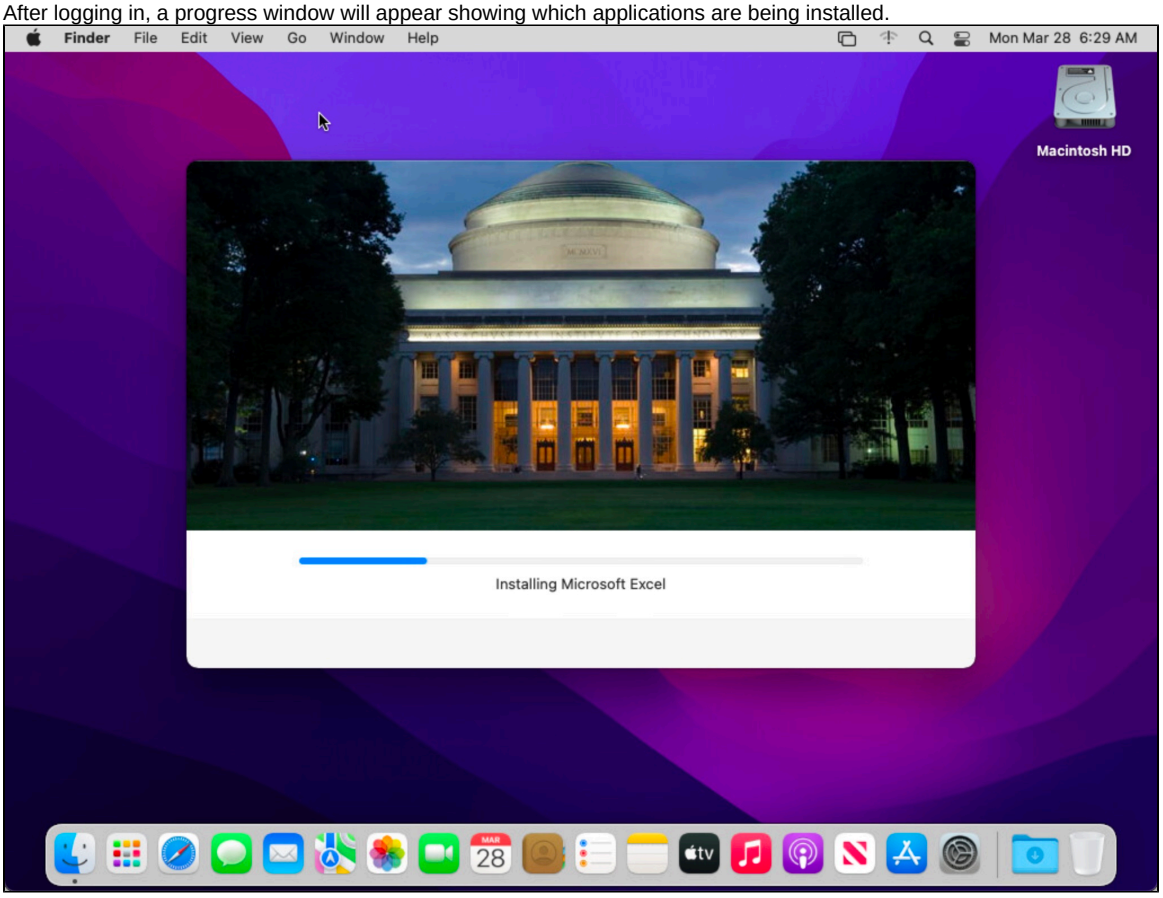
6. Create an account and log in.
7. **If you are configuring this device for another user, you should remove your saved Wi-Fi credentials from the "Local Items" keychain in Keychain Access**, following these steps:
   a. Open Keychain Access in /Applications/Utilities
   b. Select "Local Items" from in the sidebar.
   c. Scroll down and find the item matching your Wi-Fi network name, such as "MIT" or "MIT SECURE".
   d. Right-click or Control-click the item and select Delete.

   e. The ADE process will run a script to automatically remove MIT and MIT SECURE from the Login and System keychains for you. If you have joined a different network, then repeat the above steps with the "Login" and "System" keychains as well.
8. The below policies will apply if you are using IS&T Jamf Pro.
   - Software Installs
     - Adobe Reader
     - CertAid
     - Code42/CrashPlan
     - CrowdStrike Falcon
     - Dropbox

    - Firefox
    - Google Chrome
    - GlobalProtect VPN
    - Kerberos Extras
    - Microsoft Office
    - Rosetta 2 (on Apple Silicon-based Macs)
    - Slack
    - Sophos Central
    - VLC
    - Zoom
    - Apple Software Updates
- Configurations
    - Enable Filevault 2 file encryption
    - Add dock icons for Office, Firefox, and Crashplan
    - Enable firewall
    - Create a local admin account
    - Change hostname to serial number
    - Set password policy to minimum 8 characters
    - Force password change on next login
    - Configure 802.1x authentication for ethernet

After logging in, a progress window will appear showing which applications are being installed.



When setup is complete, the computer will shut down, and the user will be prompted to change their password and begin encryption the next time they log in.

You can also set up machines to have additional software/scripts/printers installed through our Jamf offering, or your own MDM policies if you have an MDM server.

Removal of machines from ADE

Machines that will be leaving MIT should be removed from ADE. Send any serial numbers to euc-help@mit.edu for removal, and specify whether this should be permanent or temporary. Computers being sold or recycled should be removed permanently, while repairs being sent back to Apple should be removed temporarily so they can be re-added when they come back to MIT.

Retired devices should be wiped completely after being removed from ADE. This will ensure that no MIT data is present on the machines, and if it's purchased by the user, it will allow the user to secure their FileVault encryption key with their personal AppleID instead of through MIT's MDM server.