UCONN
HEALTH

Mac – MacOS Configuration
UConn Health Standard Desktop

MacOS Standard Desktop - Initial Deployment Configuration

All accounts are granted administrator access by default unless higher levels of local account restrictions are requested. Standard accounts can be created if the department wishes to have local accounts on their Macintosh computers without administrator privileges for specific users.

The deployment begins with Configuration Profile Policies which allow the computer to communicate with the Jamf server when connected to the internet. At no time does the Jamf system allow access to Admin accounts or their data, other than the MacTech account. They allow for monitoring of system level performance such as SMART status on hard drives, temperature, battery performance, etc. Alerts can be sent to the Jamf administrator and the user warning of potential problems before they impact functionality.

Applications:

The following apps are installed onto the MacOS during the deployment process:

Adobe Acrobat Reader
Citrix Workspace
Cisco Webex Meetings
CrowdStrike Falcon
Google Chrome
Mozilla Firefox
Junos Pulse Secure – VPN
Microsoft Office (Word, Excel, Powerpoint, Outlook, Teams)
Open JDK (Java Development Kit)
Skype for Business
VLC – Media Player
WD Security – Read hard drives with WD Security installed
Zoom

Other Research apps such as R, R Studio, Image J, are available upon request. As well as assistance with how to access licensed applications with a UConn NET ID like SPSS, and purchase of other paid applications as needed.

Computer Name:

Computer name is set by the UConn Health Asset tag. DT = Desktop, LT = Laptop, plus the asset tag number.

Security Policies:

Configuration Profiles that enforce security policies allow UConn Health IT to communicate with the computer through the Jamf server when connected to the internet. In cases of loss or theft a computer can be locked out remotely, and can also be fully wiped once a backup is confirmed.

Encryption Recovery keys are stored in the Jamf sever and encryption status is sent to the Jamf server by the computer once every 24 hours to confirm the device is compliant.

Security certificates are generated and installed to allow access to NAC (Network Access Control) areas via WiFi or Ethernet cables. As well as access to the VPN system to access the UConn Health network while off campus.

Restrictions on Administrator Accounts:

- Cannot install major MacOS upgrades
- Cannot install known MacOS malware
- Cannot delete the UConn Health local Admin User Account
- Cannot deactivate encryption or remove the UConn Health Security Policies