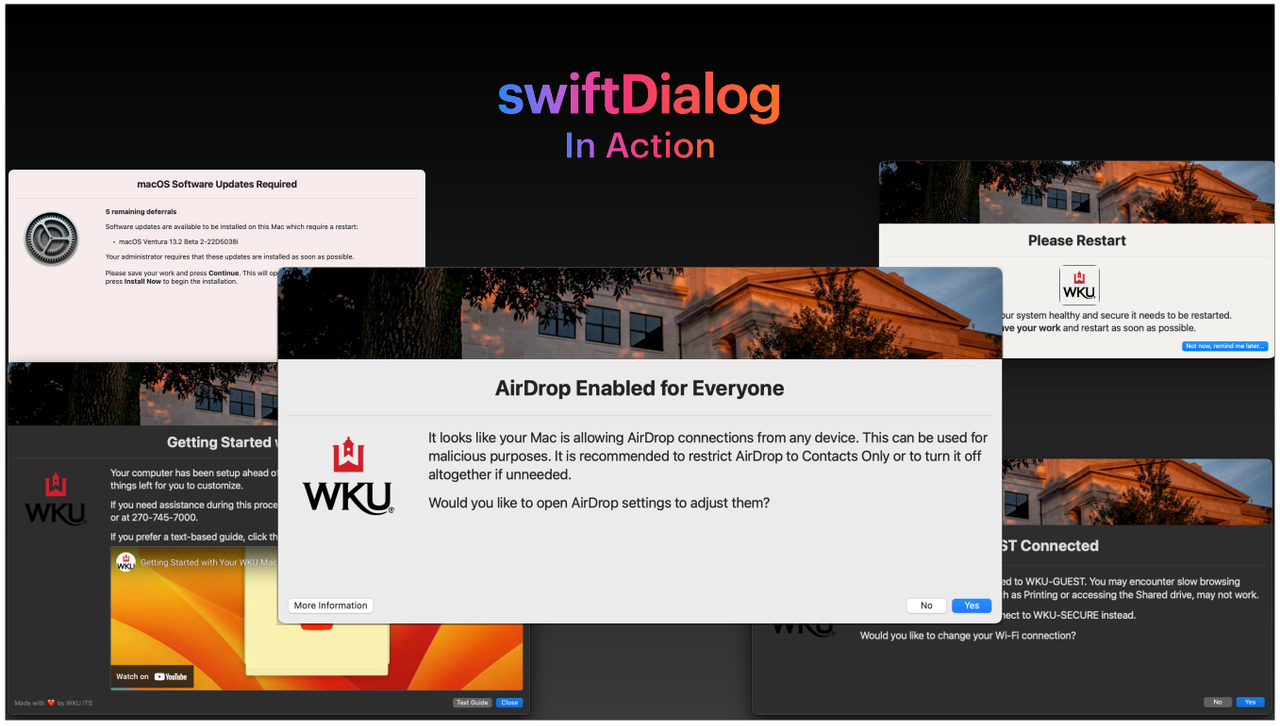
Ask audience familiarity with SD

About Me

- Systems Engineer @ Western Kentucky University
- Not a coder

@bigdoodr

WKU Mac environment



Pop-up fatigue / Jon Crain’s 2023 presentation
Timing of alerts

swiftDialog
Building It Live

- Get it: https://github.com/swiftDialog/swiftDialog/releases/latest
- Share it (AirDrop … for Everyone?)
- Install it
- Launch it: `dialog`
- Again: `dialog --builder`

An Important Message

Basic: Content

- Title: AirDrop for Everyone Enabled
- Message: It looks like your Mac is allowing AirDrop connections from any device. This can be used for malicious purposes. It is recommended to restrict AirDrop to Contacts Only or to turn it off altogether if unneeded.

  Would you like to open AirDrop settings to adjust them?

An Important Message

Basic: Window

- Window Height/Width: Leave as Default
- Window Properties>Preset Sizes: Big
- Configurations: Leave as Default
- Progress Bar: Leave Off
- Banner Image:
  - Enabled | Banner Title : Leave Off | Text Shadow : Toggle On
  - Color / Banner Height: Leave as Default
  - text Field: URL / path to file
    - https://github.com/swiftDialog/swiftDialog/wiki/Displaying-Banner-Images: *“The banner image is at most 150pt high and spans the width of the dialog window.”*

/System/Library/Desktop Pictures/.wallpapers/Sequoia Sunrise/Sequoia Sunrise.heic

An Important Message

Basic: Sidebar

- Icon:
  - Visible: toggle on
  - text field: URL / path to file
- Leave everything else as default

/System/Library/ExtensionKit/Extensions/WallpaperMacintoshExtension.appex/Contents/Resources/MacPaint.png

An Important Message

Buttons

- (Skip Data Entry)
- Button1: Yes
- Button 2:
  - Visible: Toggle On
  - text field: No
- Info Button:
  - Visible: Toggle On
  - Quit on Info: Toggle Off
  - Label: About AirDrop
  - Info Button Action: https://paretosecurity.com/auditor/checks/airdrop

An aside about Pareto Security

An Important Message

Advanced

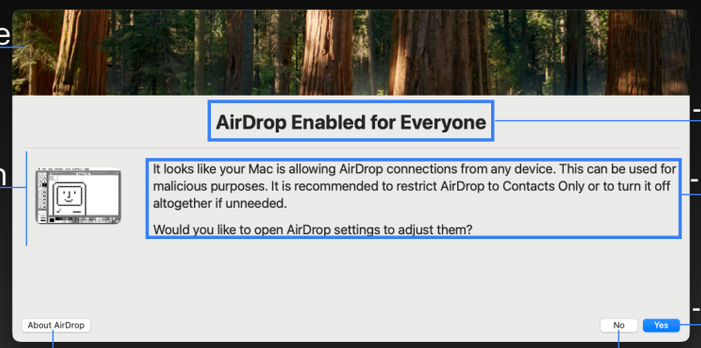
- Leave all as default

An Important Message

Output

- JSON Output
  - Generate | Copy to clipboard
- BBEdit /etc
  - ~~“builder” : “true”,~~
  - --infobuttontext “About AirDrop”
  - Save
- Quit Builder
- Back to Terminal: `dialog --jsonfile path/to/saved/file.json`

Diagram of
Our Message



- Yes / No: No logic

BBEdit

Scripting Time - Aside #1

- Security & Compliance
  - Apple IT Training
  - JAMF MSAC Tool
  - Relevant Check: `defaults read /Users/[current.user]/Library/Preferences/com.apple.sharingd.plist DiscoverableMode`
    - Possible Results:
      - Not Configured: `The domain/default pair of (Users/[current.user]]/Library/Preferences/com.apple.sharingd.plist, Discoverable Mode) does not exist`
      - No One: `Off`
      - Contacts Only: `Contacts Only`
      - Everyone: `Everyone`

Apple’s MSAC Summer Presentation:
Privacy protects the person
Security protects the device
Compliance protects the organization

BBEdit

Scripting Time - Aside #2

- Definitions and Logs
- `target_adstatus="Everyone"`
- `current_adstatus=$(defaults read /Users/[current.user]/Library/Preferences/com.apple.sharingd.plist DiscoverableMode)`
- `/private/var/log/[org.name].status.airdrop.log`
- `$( date +%Y-%m-%d\ %H:%M:%S )` (Current time)
- `x-apple.systempreference:com.apple.AirDrop-Handoff-Settings.extension` (AirDrop System Settings Path)

BBEdit

Scripting Time - For Real

https://bigdoodr.github.io/sDPres/ADforEveryone_v1

- Set the environment:

```
#!/bin/zsh
```

- Comment & Define your variables:

```
# Name the AirDrop status you want to check for
target_adstatus="Everyone"

# Get the current AirDrop status
current_adstatus=$(defaults read /Users/[current.user]/Library/Preferences/com.apple.sharingd.plist
DiscoverableMode)
```

- Define your check and remediation:

```
# Check if the current AD matches the target AD
if [ "$current_adstatus" = "$target_adstatus" ]; then
    # Make a record of it
    if [[ ! -f "/private/var/log/[org.name].status.airdrop.log" ]]; then
    touch "/private/var/log/[org.name].status.airdrop.log"
    fi
    echo "AirDrop Enabled for Everyone as of $( date +%Y-%m-%d\ %H:%M:%S )" >>
"/private/var/log/[org.name].status.airdrop.log"
    # Show a warning message
    /usr/local/bin/dialog --jsonfile /path/to/save/file.json
```

- OR long string of all options

```
    /usr/local/bin/dialog --big --title "something" --message "another thing" --icon "/icon.png" --bannerimage
"/banner.jpg" --button1text "Yes" --button2text "No" --infobuttontext "About" --infobuttonaction "URL"
```

BBEdit

Logic Cont.

-
```
    case $? in
      0)
      echo "Pressed Yes"
      # Button 1 processing here
      open x-apple.systempreferences:com.apple.AirDrop-Handoff-Settings.extension
      ;;
      2)
      echo "Pressed No (button 2)"
      # Button 2 processing here
      echo "AirDrop enabled for $target_adstatus. A warning message has been displayed." >>
"/private/var/log/[org.name].status.airdrop.log"
      ;;
    esac


else
    echo "AirDrop not enabled for $target_adstatus" >> "/private/var/log/[org.name].status.airdrop.log"
fi
```
- Save script

Let's Try It!

- Adjust your AirDrop settings
- Maybe set `target_adstatus="Contacts Only"`

Deployment 🤔

- What can your MDM do?
- Do you save the script and host/push it? Do you dump everything into your MDM's script/custom command profile?
- Host the json file and point to it
- Push the json file to the device
- Run with the options inline
- Frequency of the check—hourly, daily, weekly, monthly, just once? LaunchDaemon or MDM-defined? On-Demand via Self-Service?
- Update the current_adstatus line to target the proper path

Shall We Go Further?

With More Logic?

- Let's clean things up:

https://bigdoodr.github.io/sDPres/ADforEveryone_v2

```
#!/bin/zsh

################################################
#              Reused Variables                #
################################################
target_adstatus="Everyone"
banner="/path/to/banner.jpg"
logo="/path/to/logo.png"
ibutton="About AirDrop"
iaction="https://paretosecurity.com/auditor/checks/airdrop"
log="/private/var/log/[org.name].status.airdrop.log"
#                                              #
#                                              #
#                                              #
################################################
```

```
# Get the current AirDrop status
current_adstatus=$(defaults read ~/Library/Preferences/com.apple.sharingd.plist DiscoverableMode)

# Check if the current AD matches the target AD
if [ "$current_adstatus" = "$target_adstatus" ]; then
    # Make a record of it
    if [[ ! -f "$log" ]]; then
    touch "$log"
    fi
    echo "AirDrop Enabled for Everyone as of $( date +%Y-%m-%d\ %H:%M:%S )" >> "$log"
    echo "AirDrop Enabled for Everyone as of $( date +%Y-%m-%d\ %H:%M:%S )
```

Shall We Go Further?

Yes, More Logic

```
    # Show a warning message
    /usr/local/bin/dialog \
        --big \
        --title "AirDrop Enabled for Everyone" \
        --message "It looks like your Mac is allowing AirDrop connections
from any device. This can be used for malicious purposes. It is recommended
to restrict AirDrop to Contacts Only or to turn it off altogether if
unneeded.\n\nWould you like to open AirDrop settings to adjust them?" \
        --icon $logo \
        --bannerimage $banner \
        --button1text "Yes" \
        --button2 \
        --button2text "No" \
        --infobuttontext $ibutton \
        --infobuttonaction $iaction
```

```
    case $? in
      0)
      echo "Pressed Yes"
      # Button 1 processing here
      open x-apple.systempreferences:com.apple.AirDrop-Handoff-
Settings.extension
      /usr/local/bin/dialog \
          --big \
          --title "Continue When Ready" \
          --message "Once you have updated the AirDrop settings, press
Continue below"  \
          --icon $logo \
          --bannerimage $banner \
          --button1text "Continue" \
          --infobuttontext $ibutton \
          --infobuttonaction $iaction
      current_adstatus=$(defaults read
~/Library/Preferences/com.apple.sharingd.plist DiscoverableMode)
      if [ "$current_adstatus" ≠ "$target_adstatus" ]; then
      /usr/local/bin/dialog \
          --big \
          --title "AirDrop Updated" \
          --message "Thank you for changing your AirDrop settings to
$current_adstatus." \
          --icon $logo \
          --bannerimage $banner \
          --button1text "Close"
```

Shall We Go Further?

Last Bit of Logic

```
      else
        /usr/local/bin/dialog \
             --big \
             --title "AirDrop Unchanged" \
             --message "AirDrop is still enabled for Everyone. If you need assistance updating the settings, please contact
Support."  \
             --icon $logo \
             --bannerimage $banner \
             --button1text "Close" \
             --infobuttontext $ibutton \
             --infobuttonaction $iaction
        echo "AirDrop settings not changed." >> "$log"
        echo "AirDrop settings not changed."
      fi
      ;;
      2)
      echo "Pressed No (button 2)"
      # Button 2 processing here
      echo "AirDrop enabled for $target_adstatus. Settings were not changed. A warning message has been displayed." >> "$log"
      echo "AirDrop enabled for $target_adstatus. Settings were not changed. A warning message has been displayed."
      ;;
    esac


else
    echo "AirDrop not enabled for $target_adstatus."
fi
```

Q & A
And Resources

- swiftDialog Wiki
- Graham Pugh's Nice-Updater
- SecondSon/BigMacAdmin's Renew
- Jon Crain's swiftDialog 2023 MAC Session: GH Repo | YT Video
- 512 Pixels | Inside the Macintosh Screen Saver
- Pareto Security GH Repo
- Apple IT Training: Mac Security Compliance
- Jamf Compliance Editor
- shellcheck.net
- carbon.now.sh

https://bigdoodr.github.io/25macpres

https://bit.ly/psumac25-862807

sD Wiki: Expand Pages ToC