



Mastering macOS Management with Microsoft Intune

Okta Sari & Somesh Pathak



DELL
Technologies



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



Oktay
Sari

Modern Workplace
consultant

 @oktay_sari

 <https://www.linkedin.com/in/oktaysari>



SquaredUp



kpn
Partner Network



INS PARK



cegeka

Infrastructure Engineer
NN Group



Somesh
Pathak



@pathak_somesh



/somesh-pathak-mvp-mct



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



What Are We Going To Discuss Today?



- Platform Single Sign On
- Local Account Management
- DDM & RRS
- App Deployment
- Tip, Tricks & Treats
- Tools & Resources



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



Platform Single Sign-On

What's the buzz..."Single Sign-On: because for remembering lunch orders, not your team's memory space is better used passwords



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network

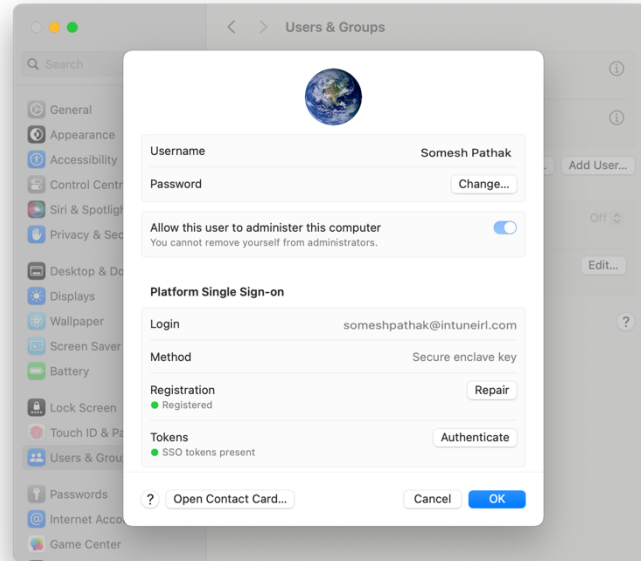


INSPARK



cegeka

How Does It Works??



MDM Configuration

- Platform SSO is enabled through the `com.apple.extensiblesso` payload
- Supports four types of authentication
- The MDM profile must be a System profile when using shared device key
- Not possible to locally create & install the profile
- Used to register encryption keys, unlock the Mac at login window & screensaver unlock



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka

MDM Configuration

Extensible Single Sign On (SSO)

Configure an app extension that enables single sign-on (SSO) for devices.

| | |
|-----------------------|--|
| Team Identifier | UBF8T346G9 |
| Extension Identifier | com.microsoft.CompanyPortalMac.ssoextension |
| Registration Token | {{DEVICEREGISTRATION}} |
| Platform SSO | |
| Account Display Name | IRL Corp Account |
| Authentication Method | SmartCard |
| Login Frequency | 64800 |
| Type | Redirect |
| URLs | https://login-us.microsoftonline.com , https://login.chinacloudapi.cn , https://login.microsoft.com , https://login.microsoftonline.com , https://login.microsoftonline.us , https://login.partner.microsoftonline.cn , https://sts.windows.net |



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



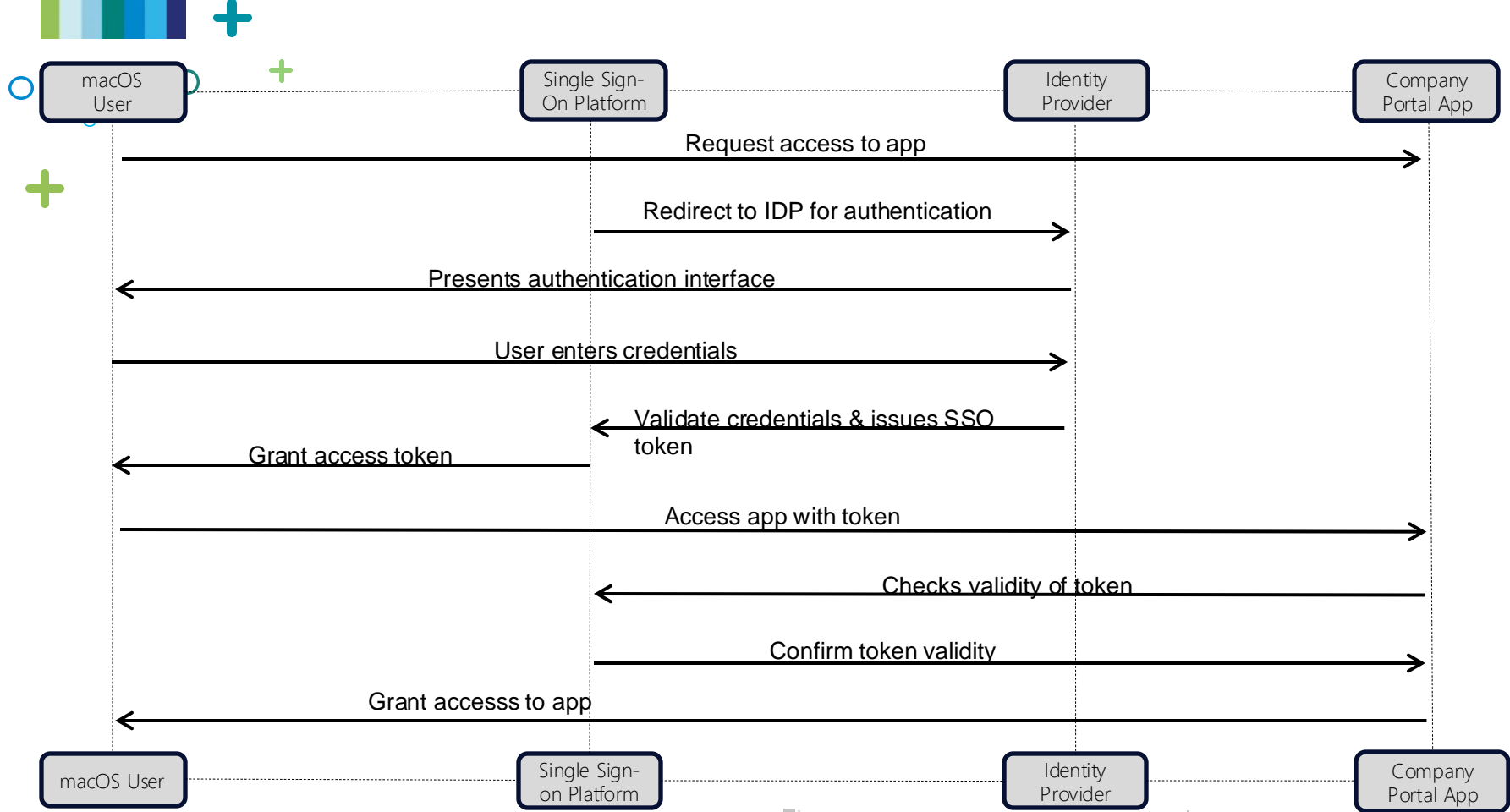
INS PARK



cegeka



Platform SSO: Behind The Scenes



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



DEMO: Platform SSO Passwordless!



Declarative Device Management

Declarative Device Management is like having a smart assistant for your devices. You tell it what the end state should look like, and voilà! It figures out the 'hows' faster than you can say 'automate my tasks, please...



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka

MDM Configuration

Declarative Device Management (DDM)

Remove category

These settings configure the declarations used by Apple's declarative device management feature. These settings are separate from older MDM settings and only apply to a device enabled for declarative management. [Learn more about declarative management at developer.apple.com](#)

Software Update

Remove subcategory

1 of 4 settings in this subcategory are not configured

Target Build Version ⓘ

23F79 ✓ -

Target Date Time (UTC) * ⓘ

31/05/2024 📅 1:00 PM

Target OS Version ⓘ

14.5 ✓

Oops! I Missed The Deadline



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka



| 30 days | 14 days | 24 hours | | 1 hour |
|------------------|--------------------|---------------------|----------------------|-------------------------|
| Settings UI | Notifications | Settings UI | Notifications | Notifications |
| | | | | |
| Update available | Daily Notification | Update available | Hourly notifications | Managed install pending |
| | | | | |
| User Options | User Options | User Options | | User Options |
| Update Now | Update Now | Update Now | Update Now | 60 minutes |
| Update later | Update Later | Install on schedule | Install on schedule | 30 minutes |
| | | | | 10 minutes |
| | | | | 60 seconds |
| | | | | Update is forced |
| | | | | Reboot |



Rapid Security Response

Rapid Security Responses are a new type of software release for iPhone, iPad, and Mac. They deliver important security improvements between software updates



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka

MDM Configuration

Configuration settings [Edit](#)

^ Restrictions

Configure the Restrictions payload to enable or disable features on devices. These configurations can be used to prevent users from accessing a specific app, service or function on enrolled devices. For example, a restriction can be added that prevents an iPhone or iPad from using AirPrint. Another restriction can be added to prevent sharing of passwords over AirDrop on an iPhone, iPad and Mac. Certain restrictions on an iPhone may be restricted on a paired Apple Watch.

Allow Rapid Security Response Removal False



Allow Rapid Security Response
Installation ⓘ True



SquaredUp



infinity



kpn
Partner Network



INS PARK

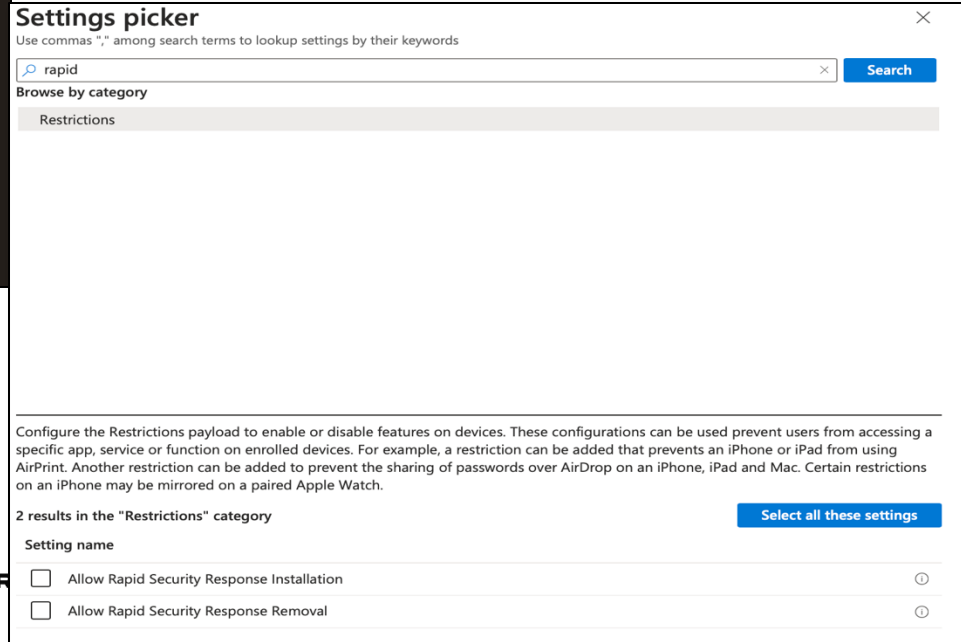
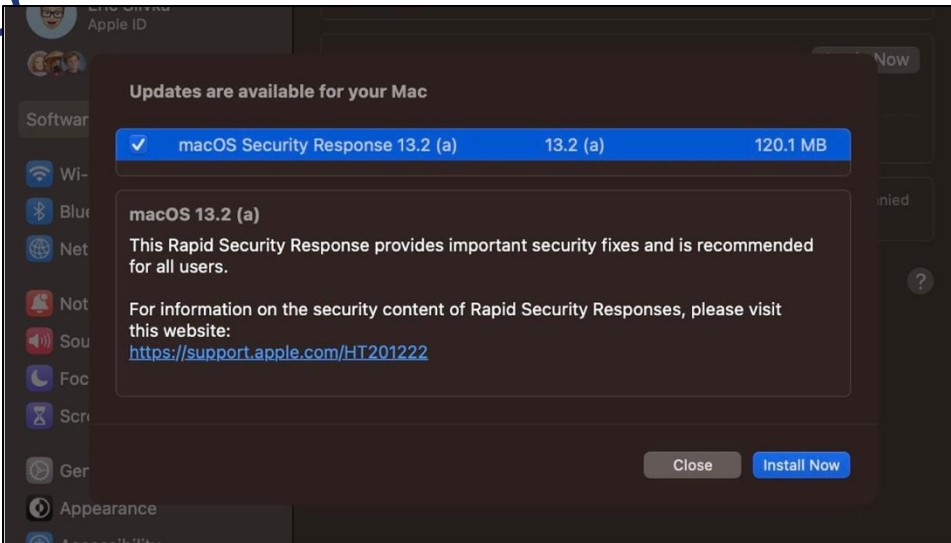


cegeka

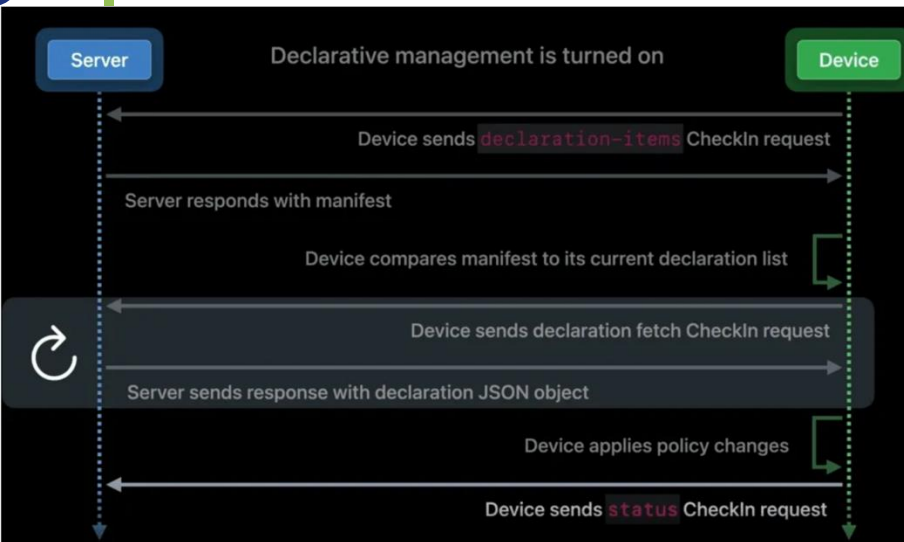


Rapid Security Response: Behind The Scenes

Rapid Security Response



Rapid Security Response



```
{  
  "Type": "com.apple.configuration.softwareupdate.enforcement.specific",  
  "Identifier": "9DF890F2-D19D-4BB0-9167-CE8281714612",  
  "ServerToken": "26EB91D1-16C2-48D8-A88C-9687D6E8AAAE",  
  "Payload": {  
    "TargetOSVersion": "14.0",  
    "TargetBuildVersion": "23A500",  
    "TargetLocalDateTime": "2023-06-05T10:00:00"  
  }  
}
```







SquaredUp



IN



Off The Press

-  **FileVault enabled during enrollment (GA)**
-  **Remote help full control (GA)**
-  **Universal Print (public preview)**
-  **Managed device attestation (private preview)**



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka

App Deployment



LOB - Managed Apps

You can wave goodbye to the app with the 'uninstall assignment type' on devices that support this feature.

When you decide to pull the plug on the MDM profile (remove it), it's like a clean sweep – every managed app, along with its data, gets whisked away from the device

Minimum operating system * ⓘ

macOS Ventura 13.0

Ignore app version ⓘ

Yes

No

Install as managed ⓘ

Yes

No

Included apps * ⓘ



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



Ignore App Version

NEED TO KNOW:

| Ignore App version setting | App install status on Device | App Deployment action |
|----------------------------|---------------------------------|-----------------------|
| YES | App is NOT found | Deploy the app |
| | App is installed: Other version | Do not deploy |
| NO | App is NOT found | Deploy the app |
| | App is installed: Other version | Deploy the app |



SquaredUp



infinity



kpn
Partner Network



INS PARK



cegeka

PKG Apps - Pre & Post Scripts

Home > Apps | macOS > macOS | macOS apps > Zscaler

Zscaler | Properties

Client Apps

Search

Program Edit

Overview

Manage

Properties

Monitor

Device install status

User install status

Pre-install script

```
#!/bin/bash

# Define variables
appname="Zscaler"
appfile="Zscaler.app"
log="/var/log/installzscaler.log"
installer="/path/to/Zscaler.pkg"

# Set the minimum required version
MIN_VERSION="4.1.0.161"

# Get the current version of the Zscaler app
CURRENT_VERSION=$(mdls -name kMDItemVersion
/Applications/Zscaler.app | cut -d "" -f 2)

# Compare the current version with the minimum required version
if [[ "$CURRENT_VERSION" < "$MIN_VERSION" ]]; then
    # Upgrade the Zscaler app to the new version
    echo "$(date) | Upgrading the Zscaler app to the new version" >> $log
    sudo installer -pkg $installer -target /
fi
```

Post-install script

```
#!/bin/bash
```

```
# Define variables
```

```
cloudName="zsccloud"
```

```
userDomain=""
```

```
log="/var/log/installzscaler.log"
```

```
# Configure the Zscaler app
```

```
echo "$(date) | Configuring the Zscaler app" >> $log
```

```
/Applications/Zscaler/Zscaler.app/Contents/MacOS/Zscaler --cloudName
```

```
$cloudName --userDomain $userDomain
```

```
# Check the exit status of the previous command
```

```
if [[ $? -ne 0 ]]; then
```

```
    # Return an error code if the configuration failed
```

```
    echo "$(date) | Configuration of the Zscaler app failed" >> $log
```

```
    exit 1
```

```
else
```

```
    # Return a success code if the configuration was successful
```

```
    echo "$(date) | Configuration of the Zscaler app was successful" >> $log
```

```
    exit 0
```

```
fi
```



SquaredUp



infinity

INTERSTELLAR



kpn
Partner Network



INSPIRE



cegeka



Tips, Tricks & Treats



.plist

Purpose:

Used to store settings and configuration data for applications and system components.

Examples:

- Application settings: com.apple.dock.plist
- System preferences: com.apple.systempreferences.plist

Why use plist files?

- They provide a straightforward way to store and retrieve application settings, user preferences, and other configuration data .

When to use plist files?

- Developing macOS or iOS applications that require persistent storage for configuration data.
- Configuring system preferences or settings that need to be applied across reboots.



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



.mobileconfig

Purpose:

Used to deploy configuration profiles to Apple devices, including macOS, iOS, and iPadOS, enabling centralized management of settings and policies.

Examples:

- Wi-Fi configurations, VPN settings, email accounts. For example; WiFiProfile.mobileconfig

Why use .mobileconfig files?

- A mobileconfig file is an XML file used to define settings and policies for Apple devices, which can be deployed remotely.

When to use mobileconfig files?

- When setting up new devices to ensure they meet organizational policies.
- When updating device settings remotely without needing physical access to the device.
- For enrolling devices in MDM (Mobile Device Management) solutions.



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



cegeka



Tools



PLISTWATCH

Purpose:

PlistWatch monitors real-time changes to plist files on your system. It outputs a defaults command to recreate that change.



SquaredUp



infinity



INTERSTELLAR



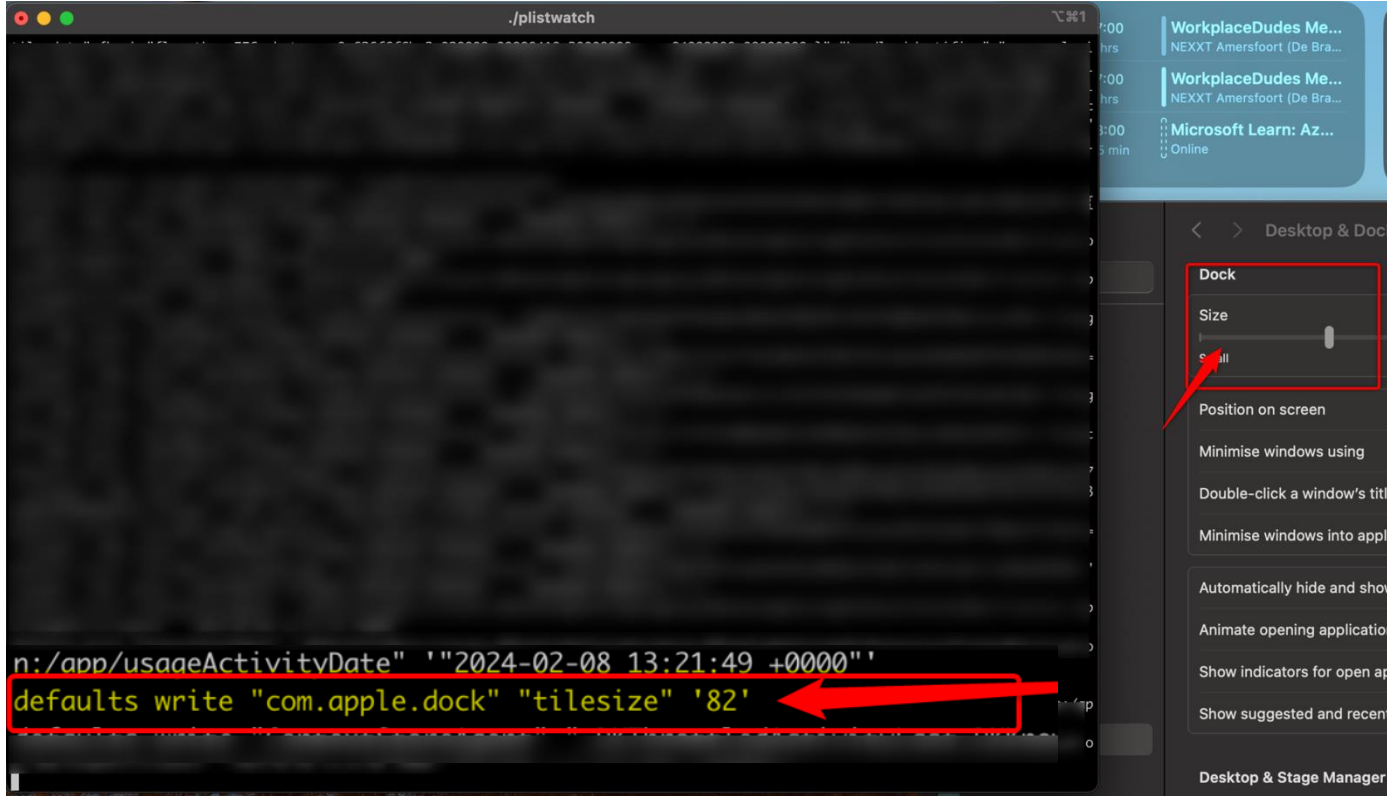
kpn
Partner Network



INSPARK



cegeka



<https://github.com/catilac/plistwatch>



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network

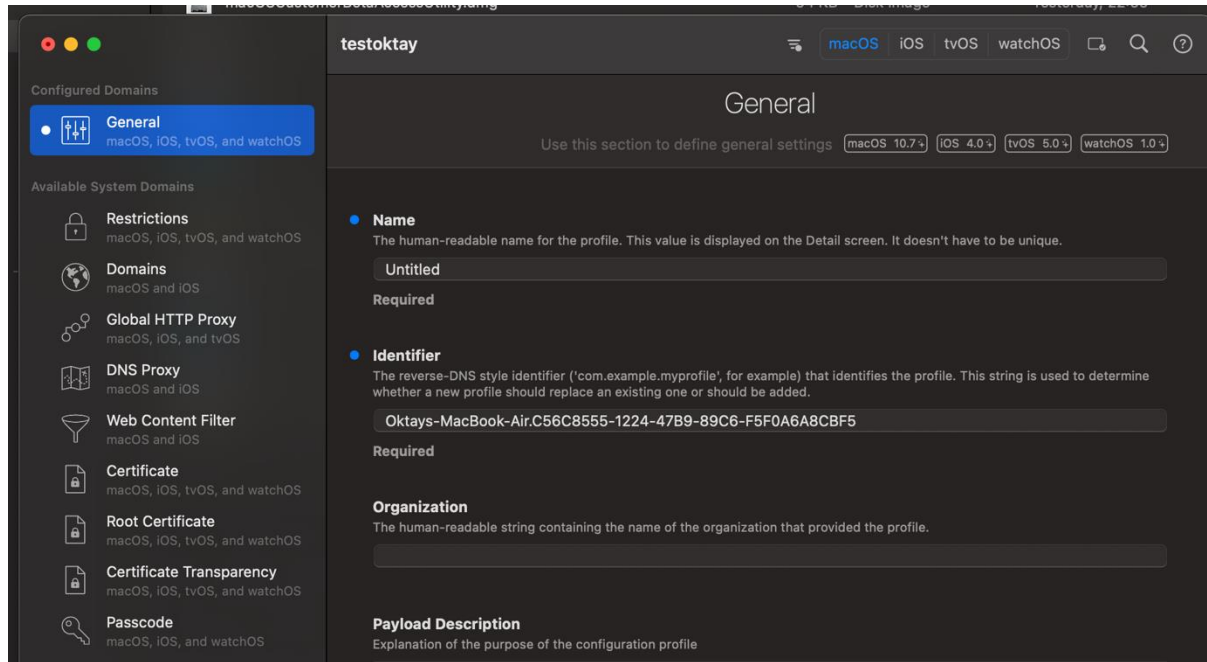


INS PARK



cegeka

iMazing Profile Editor



<https://imazing.com/profile-editor>



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INS PARK



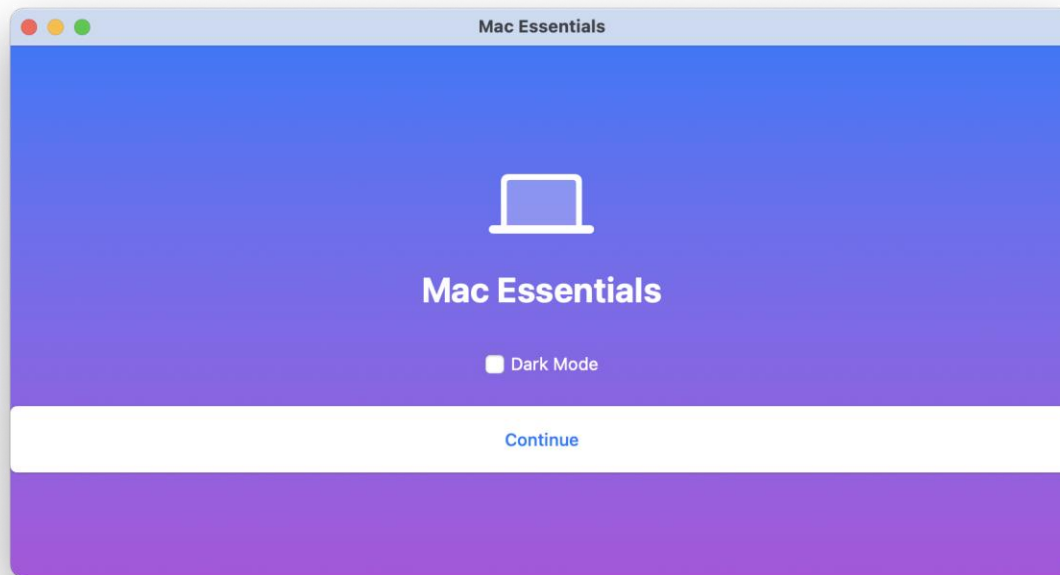
cegeka



Treats



Mac Essentials



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network

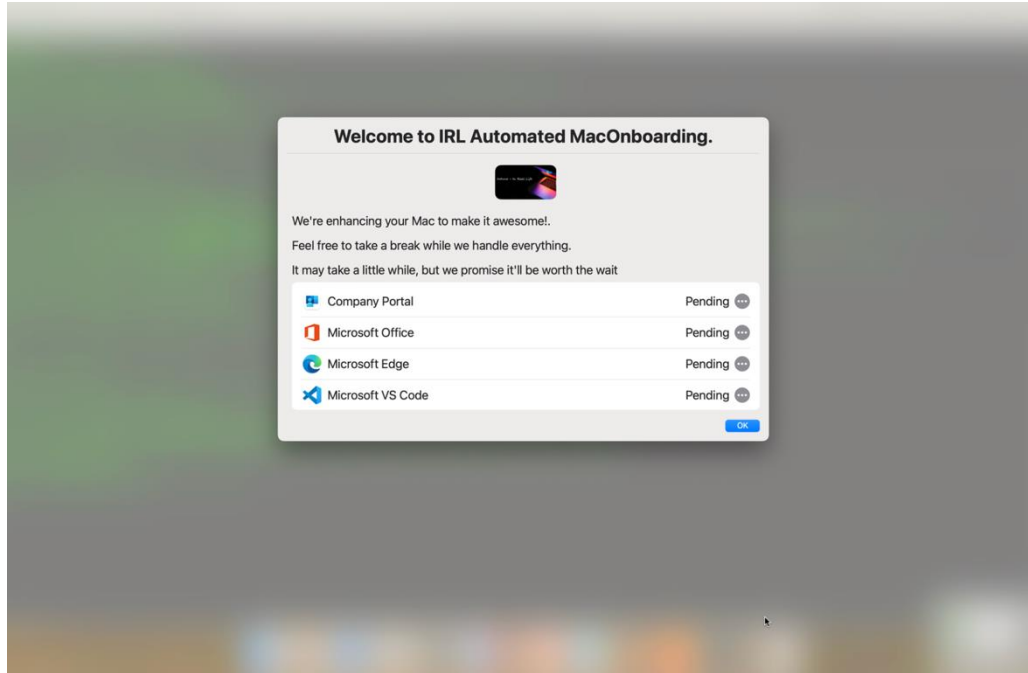


INS PARK



cegeka

Swift Dialog Video





Resources



Resources

- 🧑 **Apple Platform Deployment Guide**
- 🧑 **Apple Security Guide**
- 🧑 **Apple Seed for IT**
- 🧑 **Community Channels**
- 🧑 **Microsoft Learn**



SquaredUp



infinity



kpn
Partner Network



INS PARK



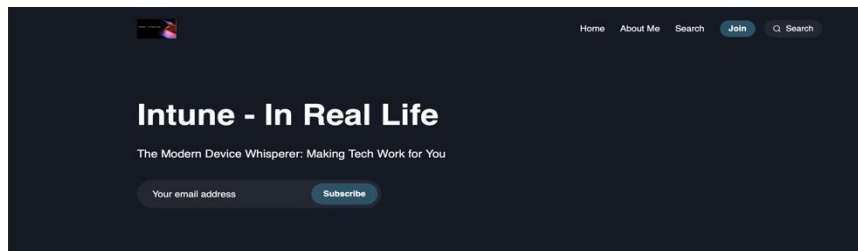
cegeka



Resources

Intune In Real Life

<https://www.intuneirl.com>



AllThingsCloud

<https://allthingscloud.blog>



SquaredUp



infinity



INTERSTELLAR



kpn
Partner Network



INSPARK



cegeka



Please evaluate this session in the App.

THANK YOU

Are there any questions?

