What's New in Managing Apple Devices

Todd Fernandez, Senior Manager, Device Management
Same tools for all
Same tools for all

Balance values
Same tools for all
Balance values
Fits in and stands out
Same tools for all

Balance values

Fits in and stands out
Same tools for all
20 Accounts

- Bryan Alvarez - Content Manager - Apple Inc.
- Greg Apodaca - People Manager - Apple Inc.
- Johnny Appleseed (Me) - Administrator - Apple Inc.
- Allison Cain - Administrator - Apple Inc.
- Joe Calonje - People Manager - Apple Inc.
- Tejo Dama - 2 Roles - Apple Inc.
- Dave Elfving - Staff - Apple Inc.
- Cynthia Fong - Staff - Apple Inc.
- Janelle Gee - Staff - Apple Inc.
- Kim Kilgo - Device Manager - Apple Inc.
- Jeena Kim - Device Manager - Apple Inc.

- Sign-Ins
  - Create and send new sign-ins for people with new accounts or lost credentials.
- Account Status
  - Deactivate, reactivate or delete these accounts.
- Account Info
  - Add a new Role and Location to these accounts.
- Accounts
  - Edit the username and domain of each Managed Apple ID.
Welcome back, Johnny

Device Enrollment Program and Volume Purchase Program have a new home:

- Device Enrollment Program
  - Get Started

- Apple School Manager
  - school.apple.com

- Volume Purchase Program
  - Get Started
AppleSeed for IT

Apple Business Manager and Apple School Manager

Access with Managed Apple ID

Access software, documentation, and test plans

Associate feedback with your organization
Bring Existing iOS Restrictions to macOS Classroom

- Automatically join classes
- Request permission to leave classes
- Don’t prompt for app and device lock
- Don’t prompt for screen observation
Bring Existing iOS Restrictions to macOS

Screen viewing

Allow remote screen observation
Allow screenshot

Affects
• Remote Desktop
• Screen Sharing
• Screenshot
<table>
<thead>
<tr>
<th>Name</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaron</td>
<td>Safari</td>
</tr>
<tr>
<td>Amy</td>
<td>Books</td>
</tr>
<tr>
<td>Chris</td>
<td>Safari</td>
</tr>
<tr>
<td>Craig</td>
<td>Safari</td>
</tr>
<tr>
<td>Dallas</td>
<td>Books</td>
</tr>
<tr>
<td>Damian</td>
<td>books</td>
</tr>
<tr>
<td>Emily</td>
<td>books</td>
</tr>
<tr>
<td>Erin</td>
<td>Books</td>
</tr>
<tr>
<td>Jaden</td>
<td>Safari</td>
</tr>
<tr>
<td>Jane A.</td>
<td>Books</td>
</tr>
<tr>
<td>Jane G.</td>
<td>Pages</td>
</tr>
<tr>
<td>Ken</td>
<td>Safari</td>
</tr>
<tr>
<td>Linda</td>
<td>Safari</td>
</tr>
<tr>
<td>Luci</td>
<td>Safari</td>
</tr>
<tr>
<td>Matthew</td>
<td>Pages</td>
</tr>
<tr>
<td>Max</td>
<td>Safari &amp; Pages</td>
</tr>
<tr>
<td>Natalia</td>
<td>Books</td>
</tr>
<tr>
<td>Nicolas</td>
<td>Books</td>
</tr>
<tr>
<td>Paul</td>
<td>Books</td>
</tr>
<tr>
<td>Peter</td>
<td>Books</td>
</tr>
<tr>
<td>Raymond</td>
<td>Display off</td>
</tr>
<tr>
<td>Sam</td>
<td>Books</td>
</tr>
<tr>
<td>Stephanie</td>
<td>Books</td>
</tr>
<tr>
<td>Steveanna</td>
<td>Books</td>
</tr>
</tbody>
</table>
EXPLORE TODAY
Through the eyes of our Explorers, photographers, journalists, and filmmakers.

WORLD ENVIRONMENT DAY
Half of all land must be kept in a natural state to protect Earth.
EXPLORE TODAY
Through the eyes of our Explorers, photographers, journalists, and filmmakers.

WORLD ENVIRONMENT DAY
Half of all land must be kept in a natural state to protect Earth
Desktop-Class Browsing on iPad

iPad identifies as Mac

May break MDM UI or enrollment flows

- Stop using UserAgent
Desktop-Class Browsing on iPad

iPad identifies as Mac

May break MDM UI or enrollment flows

❌ Stop using UserAgent
Platform Parity
tvOS

Managed Software Updates
Force automatic date and time
Content Caching for screen savers
Same tools for all
Same tools for all

Balance values

Fits in and stands out
Balance values
User Enrollment

Bob Whiteman, Senior Device Management Engineer
Automated Device Enrollment

SUPERVISED Device Enrollment

Acme, Inc.
server.acme.com
Verified

9:41

Remote Management

*Acme, Inc* will automatically configure your iPhone.

What does Remote Management do?

Remote management enables the administrator of *Acme, Inc* to set up email and network accounts, install and configure apps, and manage this iPhone’s settings.

About Remote Management...
Automated Device Enrollment

SUPERVISED Device Enrollment

BYOD

Device Enrollment

Automated Device Enrollment

Acme, Inc.
server.acme.com

Remote Management

"Acme, Inc." will automatically configure your iPhone.

What does Remote Management do?

Remote management enables the administrator of "Acme, Inc." to set up email and network accounts, install and configure apps, and manage this iPhone’s settings.

About Remote Management...
User Enrollment

Signing in to the Controlled Apple ID enables this organization to manage your device.

Organization: Acme, Inc.
Apple ID: johnny@acme.com

MOBILE DEVICE MANAGEMENT
Administrator will be allowed to:
- Install and remove managed applications
- Install and remove network configurations
- Install a partial VPN scoped to managed apps and accounts

INSTALL ROOT CERTIFICATE
Adding the certificate "Root Cert" will add it to the list of trusted certificates on your device.

PERSONAL INFORMATION
Personal information is data that can be used

Enroll My iPhone
Cancel & Delete Profile

Device Enrollment

Device Enrollment

Signed by: server.acme.com
Verified

Description:
iOS Mobile Services
- Mobile Device Management
- 7 Managed Apps
- 2 Password Policies
- 10 Encryption Settings
- 5 WiFi Networks
- 99 For
- 4 Device Identity Certificates
- 6 Certificates

More Details

Apps
Restrictions

Remove Management

Automated Device Enrollment

Remote Management

"Acme, Inc." will automatically configure your iPhone.

What does Remote Management do?
Remote management enables the administrator of "Acme, Inc." to set up email and network accounts, install and configure apps, and manage the device's settings.

About Remote Management...
User Enrollment

New MDM enrollment option
Better balance for BYOD
Protects privacy of personal data
Secures corporate data
Managed Apple ID
Data Separation
Management Capabilities
User Enrollment and Apple IDs

Managed Apple ID required

Apps and accounts use correct Apple ID

Unenrolling removes Managed Apple ID
Managed Apple ID

Personal Apple ID

Data Separation
Data Separation

Managed APFS volume created during user enrollment

Unenrolling destroys the volume and its cryptographic keys
How is data separated?

Managed APFS volume contains managed:

• App containers
• Notes
• iCloud Drive documents
• Keychain
• Mail attachments and full email bodies
• Calendar attachments
// Enrollment profile

<pplist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>PayloadType</key>
      <string>com.apple.mdm</string>
      <key>ManagedAppleID</key>
      <string>RickW@example.com</string>
      <key>PayloadOrganization</key>
      <string>Example, Inc.</string>
      <key>CheckInURL</key>
      <string>https://mdm.example.com:2001/checkin</string>
      <key>ServerURL</key>
      <string>https://mdm.example.com:2001/mdm</string>
      <key>CheckOutWhenRemoved</key>
      <true/>
      <key>IdentityCertificateUUID</key>

      <!-- Additional keys can be added here -->
    </dict>
  </array>
</dict>
</pplist>
// Enrollment profile

<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>PayloadType</key>
            <string>com.apple.mdm</string>
            <key>ManagedAppleID</key>
            <string>RickW@example.com</string>
            <key>PayloadOrganization</key>
            <string>Example, Inc.</string>
            <key>CheckInURL</key>
            <string>https://mdm.example.com:2001/checkin</string>
            <key>ServerURL</key>
            <string>https://mdm.example.com:2001/mdm</string>
            <key>CheckOutWhenRemoved</key>
            <true/>
            <key>IdentityCertificateUUID</key>
        </dict>
    </array>
</dict>
</plist>
// Enrollment profile

.plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>PayloadType</key>
        <string>com.apple.mdm</string>
        <key>ManagedAppleID</key>
        <string>RickW@example.com</string>
        <key>PayloadOrganization</key>
        <string>Example, Inc.</string>
        <key>CheckInURL</key>
        <string>https://mdm.example.com:2001/checkin</string>
        <key>ServerURL</key>
        <string>https://mdm.example.com:2001/mdm</string>
        <key>CheckOutWhenRemoved</key>
        <true/>
        <key>IdentityCertificateUUID</key>
        <string>
          NEW
        </string>
      </dict>
    </array>
  </dict>
</plist>
User Enrollment — Protocol

- Profile Service Profiles
- UDID or other persistent device identifiers
  - EnrollmentID
  - EASDeviceIdentifier
- Unlock Token in TokenUpdate
User Enrollment — Commands

- EraseDevice, ActiveSync RemoteWipe
- Managed results only:
  - InstalledApplicationList
  - CertificateList
  - ProfileList
  - ProvisioningProfileList
User Enrollment — Commands

- InstallApplication
  - App is always removed on unenroll
  - Enterprise app distribution or user-based VPP with PurchaseMethod 1
- Commands related to cellular
User Enrollment — Payloads

- Per-app VPN
  - MailDomains, ContactsDomains, CalendarDomains
- Passcode - 6 digit, non-simple
- Wi-Fi - use WPAD for proxying
- Defaults, Logging not supported
User Enrollment — Restrictions

Limited set of restrictions

- Managed Open In, allowLockScreen*, forceEncryptedBackup
- Any supervised restriction
- ratings*, allowCloud*
Demo
User Enrollment
User Enrollment — macOS

User Enrollment with Managed Apple ID
Managed APFS volume
Notes data separation
Management capabilities similar
It's time to evolve BYOD.
Certificate Transparency
iOS, macOS, tvOS, and watchOS

Security enhancement

Opt out sensitive certificates or domains

New payload

Multiple payloads unioned together
Wi-Fi payload supports WPA3 security type

- Personal
- Enterprise
Apple Push Notification Service

Support for token-based authentication
Device Enrollment Settings
iOS, macOS, and tvOS

Now always
• Supervised
• Mandatory

❌ allow_pairing deprecated
✔️ Use configuration profile restriction
Apple Remote Desktop
macOS

Enable and disable via MDM

Sets Remote Management to All Users

Enables options
- observe
- control
- show observe
Manage SecureTokens

macOS

Allow mobile accounts to boot FileVault system

MDM Server manages bootstrap token

Used to generate SecureToken when user signs in
Privacy Policy
macOS

Enable key loggers
Enable screen recording
Whitelist non-notarized internal apps
FileVault
macOS

Now requires user-approved MDM enrollment

✗ Can’t pass username/password auth to fdesetup

Changes may break scripts or MDM agents
Activation Lock
macOS

Clear Activation Lock via MDM
Same endpoint and API as iOS
MDM server APIs available soon
Service available later this summer
Deprecations
macOS

Non-UI profile installation
Parental Controls Application Access
User-channel-only enrollments
Deprecated Unsupervised Restrictions

iOS

For transition period
- Remain in effect after upgrade
- Not honored after backup and restore

MDM servers
- Don’t install on unsupervised devices
- Don’t assume they will take effect
Unlock Token

iOS

Available only in first token update after enrollment

✔ Remember it and don't count on getting one later

Also affects Apple Configurator

• Only available before passcode is set
Same tools for all
Balance values
Fits in and stands out
Same tools for all
Balance values
Fits in and stands out
Same tools for all
Balance values
Fits in and stands out
Single Sign-On
Too Many Methods, Too Many Places

OpenID Connect  2FA
Kerberos        SAML
Smart Cards     PKINIT
Cloud           OAuth
WS-Fed          Federation
Why Single Sign-On?

Suite of apps and web sites

Improved user experience

No passwords

Trust score data
What is Single Sign-On?

- iOS and macOS
- Native apps and Safari
- MDM managed
- UI can be native, web, or silent
Single Sign-On ≠ Apple Sign In with Apple
Single Sign-On Components

Apps and Web Sites

Single Sign-On Extension

Identity Provider
Single Sign-On Components

Apps and Web Sites

Single Sign-On Extension

Identity Provider
Redirect Extensions

Modern authentication
OpenID Connect, OAuth, or SAML2
HTTP based
Federation
Safari — Redirect Extension
Safari — Redirect Extension
Safari — Redirect Extension

Request

Safari

Single Sign-On Extension
Safari — Redirect Extension

- Safari
- Single Sign-On Extension
- Identity Provider
Safari — Redirect Extension

Safari

Single Sign-On Extension

Identity Provider
Safari — Redirect Extension

Safari

URL Response

Single Sign-On Extension

Identity Provider
Safari — Redirect Extension

Safari
Single Sign-On Extension
Identity Provider
What Can Extensions Do?

Native screen
Multifactors
SEP generated keys
Trust score data
Federated auth
WebAuthN
Native Apps can send operations
Better fit into the app flow
Authentication library not needed
Native — Redirect Extension
Native — Redirect Extension

Native App
Native — Redirect Extension

Native App

“Login”

Single Sign-On Extension
Native — Redirect Extension

Native App → Single Sign-On Extension → Identity Provider
Native — Redirect Extension

Native App → Single Sign-On Extension → Identity Provider
Native — Redirect Extension

Native App

Single Sign-On Extension

Identity Provider

URL Response And Tokens
Native — Redirect Extension

- Native App
- Single Sign-On Extension
- Identity Provider
<dict>
  <key>PayloadType</key>
  <string>com.apple.extensible.sso</string>
  <key>ExtensionIdentifier</key>
  <string>com.example.sso.redirect</string>
  <key>TeamIdentifier</key>
  <string>4JMSJRMAD</string>
  <key>Type</key>
  <string>Redirect</string>
  <key>URLs</key>
  <array>
    <string>https://auth.example.com/connect/authorize</string>
    <string>https://auth.example.com/connect/token</string>
  </array>
  <key>ExtensionData</key>
  <dict>
    <key>UserName</key>
    <string>john.appleseed@example.com</string>
  </dict>
</dict>
Extensible SSO Profile

```
<dict>
  <key>PayloadType</key>
  <string>com.apple.extensiblesso</string>
  <key>ExtensionIdentifier</key>
  <string>com.example.sso.redirect</string>
  <key>TeamIdentifier</key>
  <string>4JMSJRMAD</string>
  <key>Type</key>
  <string>Redirect</string>
  <key>URLs</key>
  <array>
    <string>https://auth.example.com/connect/authorize</string>
    <string>https://auth.example.com/connect/token</string>
  </array>
  <key>ExtensionData</key>
  <dict>
    <key>UserName</key>
    <string>john.appleseed@example.com</string>
  </dict>
</dict>
```
<dict>
  <key>PayloadType</key>
  <string>com.apple.extensiblesso</string>
  <key>ExtensionIdentifier</key>
  <string>com.example.sso.redirect</string>
  <key>TeamIdentifier</key>
  <string>4JMSJJRMAD</string>
  <key>Type</key>
  <string>Redirect</string>
  <key>URLs</key>
  <array>
    <string>https://auth.example.com/connect/authorize</string>
    <string>https://auth.example.com/connect/token</string>
  </array>
  <key>ExtensionData</key>
  <dict>
    <key>UserName</key>
    <string>john.appleseed@example.com</string>
  </dict>
</dict>
<dict>
  <key>PayloadType</key>
  <string>com.apple.extensiblesso</string>
  <key>ExtensionIdentifier</key>
  <string>com.example.sso.redirect</string>
  <key>TeamIdentifier</key>
  <string>4JMSJJRMAD</string>
  <key>Type</key>
  <string>Redirect</string>
  <key>URLs</key>
  <array>
    <string>https://auth.example.com/connect/authorize</string>
    <string>https://auth.example.com/connect/token</string>
  </array>
  <key>ExtensionData</key>
  <dict>
    <key>UserName</key>
    <string>john.appleseed@example.com</string>
  </dict>
</dict>
<dict>
  <key>PayloadType</key>
  <string>com.apple.extensiblesso</string>
  <key>ExtensionIdentifier</key>
  <string>com.example.sso.redirect</string>
  <key>TeamIdentifier</key>
  <string>4JMSJJRMAD</string>
  <key>Type</key>
  <string>Redirect</string>
  <key>URLs</key>
  <array>
    <string>https://auth.example.com/connect/authorize</string>
    <string>https://auth.example.com/connect/token</string>
  </array>
  <key>ExtensionData</key>
  <dict>
    <key>UserName</key>
    <string>john.appleseed@example.com</string>
  </dict>
</dict>
<dict>
    <key>PayloadType</key>
    <string>com.apple.extensiblesso</string>
    <key>ExtensionIdentifier</key>
    <string>com.example.sso.redirect</string>
    <key>TeamIdentifier</key>
    <string>4JMSJJRMD</string>
    <key>Type</key>
    <string>Redirect</string>
    <key>URLs</key>
    <array>
        <string>https://auth.example.com/connect/authorize</string>
        <string>https://auth.example.com/connect/token</string>
    </array>
    <key>ExtensionData</key>
    <dict>
        <key>UserName</key>
        <string>john.appleseed@example.com</string>
    </dict>
</dict>
<key>ExtensionIdentifier</key>
<string>com.example.sso.redirect</string>

<key>TeamIdentifier</key>
<string>4JMSJJRMAD</string>

<key>Type</key>
<string>Redirect</string>

<key>URLs</key>
<array>
  <string>https://auth.example.com/connect/authorize</string>
  <string>https://auth.example.com/connect/token</string>
</array>

<key>ExtensionData</key>
<dict>
  <key>UserName</key>
  <string>john.appleseed@example.com</string>
</dict>
</dict>
<key>ExtensionIdentifier</key>
<string>com.example.sso.redirect</string>

<key>TeamIdentifier</key>
<string>4JMSJJRMA</string>

<key>Type</key>
<string>Redirect</string>

<key>URLs</key>
<array>
  <string>https://auth.example.com/connect/authorize</string>
  <string>https://auth.example.com/connect/token</string>
</array>

<key>ExtensionData</key>
<dict>
  <key>UserName</key>
  <string>john.appleseed@example.com</string>
</dict>
</dict>
<key>ExtensionIdentifier</key>
<string>com.example.sso.redirect</string>

<key>TeamIdentifier</key>
<string>4JMSJJRMAD</string>

<key>Type</key>
<string>Redirect</string>

<key>URLs</key>
<array>
  <string>https://auth.example.com/connect/authorize</string>
  <string>https://auth.example.com/connect/token</string>
</array>

<key>ExtensionData</key>
<dict>
  <key>UserName</key>
  <string>john.appleseed@example.com</string>
</dict>
</dict>
<key>ExtensionIdentifier</key>
<string>com.example.sso.redirect</string>

<key>TeamIdentifier</key>
<string>4JMSJJRMAD</string>

<key>Type</key>
<string>Redirect</string>

<key>URLs</key>
<array>
  <string>https://auth.example.com/connect/authorize</string>
  <string>https://auth.example.com/connect/token</string>
</array>

<key>ExtensionData</key>
<dict>
  <key>UserName</key>
  <string>john.appleseed@example.com</string>
</dict>
</dict>
</dict>
</dict>
Domains authsrv:auth.example.com
Security and Privacy
Associated domains

Requires Site Association File on Server

• auth.example.com/.well-known/apple-app-site-association

```json
{
    "authsrv": {
        "apps": [ "4JMSJJRMAD.com.example.sso" ]
    }
}
```
Security and Privacy

Use managed associated domains on macOS

```xml
<key>ApplicationIdentifier</key>
<string>4JMSJJRMA.com.example.sso</string>
<key>AssociatedDomains</key>
<array>
  <string>authserv:auth.example.com</string>
</array>
```
Security and Privacy

Use managed ApplicationAttributes on iOS

<key>AssociatedDomains</key>
<array>
  <string>authserv:auth.example.com</string>
</array>
What's New in Universal Links
Credential Extensions

Challenge/response authentication
Kerberos
Custom challenges
Credential Extensions

HTTP challenge

Hosts or host suffixes

Operations are supported

No associated domains
Any App — Credential Extension
Any App — Credential Extension

URLSession
Any App — Credential Extension

URLSession

SSO Extension

Challenge

Web Server
Any App — Credential Extension

URLSession

SSO Extension

Web Server

Auth Server
Any App — Credential Extension

URLSession

Web Server

SSO Extension

Auth Server
Any App — Credential Extension
Any App — Credential Extension

URLSession

SSO Extension

Web Server

Auth Server
Demo
Credential mode extension
Kerberos Extension

Included with macOS Catalina and iOS 13

Provides Active Directory password management and local password sync

Smart card and certificate-based authentication support
Single Sign-On

Summary

Enables Single Sign-On for apps and web sites

macOS and iOS

Two types available

Let’s see what you do with them!

Watch Single Sign-On video for more details
Associated Domains

Can manage via MDM

Not just for Single Sign-On!

Other service types supported
Associated Domains

Can manage via MDM

Not just for Single Sign-On!

Other service types supported
Federated Authentication

Supports Microsoft Azure Active Directory

Managed Apple ID coming to ABM

User Enrollment requires Managed Apple ID
Enrollment Customization

Provide custom web UI for enrollment

Use for
- Authentication
- Branding
- Consent text
- Privacy policy
Remote Management

Remote management enables the administrator of "Acme, Inc." to set up email and network accounts, install and configure apps, and manage this computer's settings.

"Acme, Inc." can automatically configure your computer.

Learn more about remote management

Back Continue

Remote Management

"Acme, Inc." will automatically configure your iPhone.

What does Remote Management do?

Remote management enables the administrator of "Acme, Inc." to set up email and network accounts, install and configure apps, and manage this iPhone's settings.

About Remote Management...
Acme, Inc.

Acceptable Use Policy

This policy was created by or for Acme, Inc. for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required.

If you would like to contribute a new policy or updated version of this policy, please send email to policy@acme.com.

Inteach's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Acme's established culture of openness, trust and integrity. Inteach is committed to protecting Acme's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/ Intranet/Extranet-related systems, including but not limited to...

Decline

Agree
Content Caching

Configure for best effort vs infrastructure

Tell devices to prefer specific content caches
Setup Assistant

iOS

Skip Dark Mode pane in Setup Assistant

Skip Welcome pane in Setup Assistant
Setup Assistant
macOS

Skip Screen Time pane after enrollment

Skip Screen Time or Touch ID pane in Setup Assistant payload
Exchange ActiveSync
iOS

Enable Mail, Calendar, Contacts, and Reminders individually for managed accounts
Supervised-Only Restrictions

iOS

Allow Hotspot Modification
Allow Find My Devices
Allow Find My Friends
Allow QuickPath keyboard
Allow Wi-Fi modification
Supervised-Only Restriction

tvOS

Have Apple TV always ready to AirPlay

Allow Device Sleep
Avoids iOS destination prompt

Target type must match device type
Documentation

Import new keys and values from code

Format matches developer documentation

Highlight changes in OS releases
Demo
Device Management Documentation

Graham McLuhan, Device Management Engineer
Web Service

Device Management

Remotely manage devices within your organization.

Overview

Apple devices can be securely and remotely configured after they’re enrolled in mobile device management (MDM). Users can enroll their own devices, and organization-owned devices can be enrolled using Apple School Manager or Apple Business Manager. With MDM, you can update software and device settings, monitor compliance with organizational policies, remotely erase or lock devices, and install apps and books developed in-house or purchased through Apple School Manager or Apple Business Manager.

Topics

Configuration Profiles ▶️ Using Configuration Profiles
Create and deploy configuration profiles to users within your organization.
Summary

Support Single Sign-On and Data Separation

Enable enrollment customization

Support new payloads and restrictions

Don’t rely on UserAgent

Handle newly supervised-only restrictions
### Device Management Lab

**What's New in Universal Links**

**WWDC 2019**

**Introducing Desktop-Class Browsing on iPad**

---

Friday, 1:00

WWDC 2019

Apple WWDC19