

Forward-Looking Statement Disclaimer

This presentation may contain forward-looking statements under applicable securities laws. All statements other than statements of historical facts are forward-looking statement. Forward-looking statements are based on information available to Jamf at the time they are made and provide Jamf's current expectations and projections about its financial condition, results, plans, objectives, future performance and business. You can identify forward-looking statements by the fact that they do not relate strictly to historical or current facts. Forward-looking statements may include words such as "anticipate", "estimate", "project", "plan", "intend", "believe", "may", "will", "should", "can have", "likely" and other terms of similar meaning in connection with any discussion of timing or nature of future operating or financial performance or other events.

All statements we make about our estimated and projected costs, expenses, cash flows, growth rates and financial results are forward-looking statements. In addition, our plans and objectives for future operations, growth initiatives, product plans and product strategies are forward-looking statements.

There are various factors, risks and uncertainties that may cause Jamf's actual results to differ materially from those that we expected in any forward-looking statements. These factors and risks are set forth in the documents Jamf files with U.S. Securities and Exchange Commission (SEC). These documents are publicly available on the SEC's website at www.sec.gov or on Jamf's website at ir.jamf.com.

Forward-looking statements are not guarantees of future performance and you should not place undue reliance on them. Jamf is under no obligation to update any forward-looking statements made in this presentation, except as required by law.





AI-Dentifying Methods to Manage Apple Intelligence with Jamf Pro



Lee Cacioppo

Jamf

 @ljcacioppo

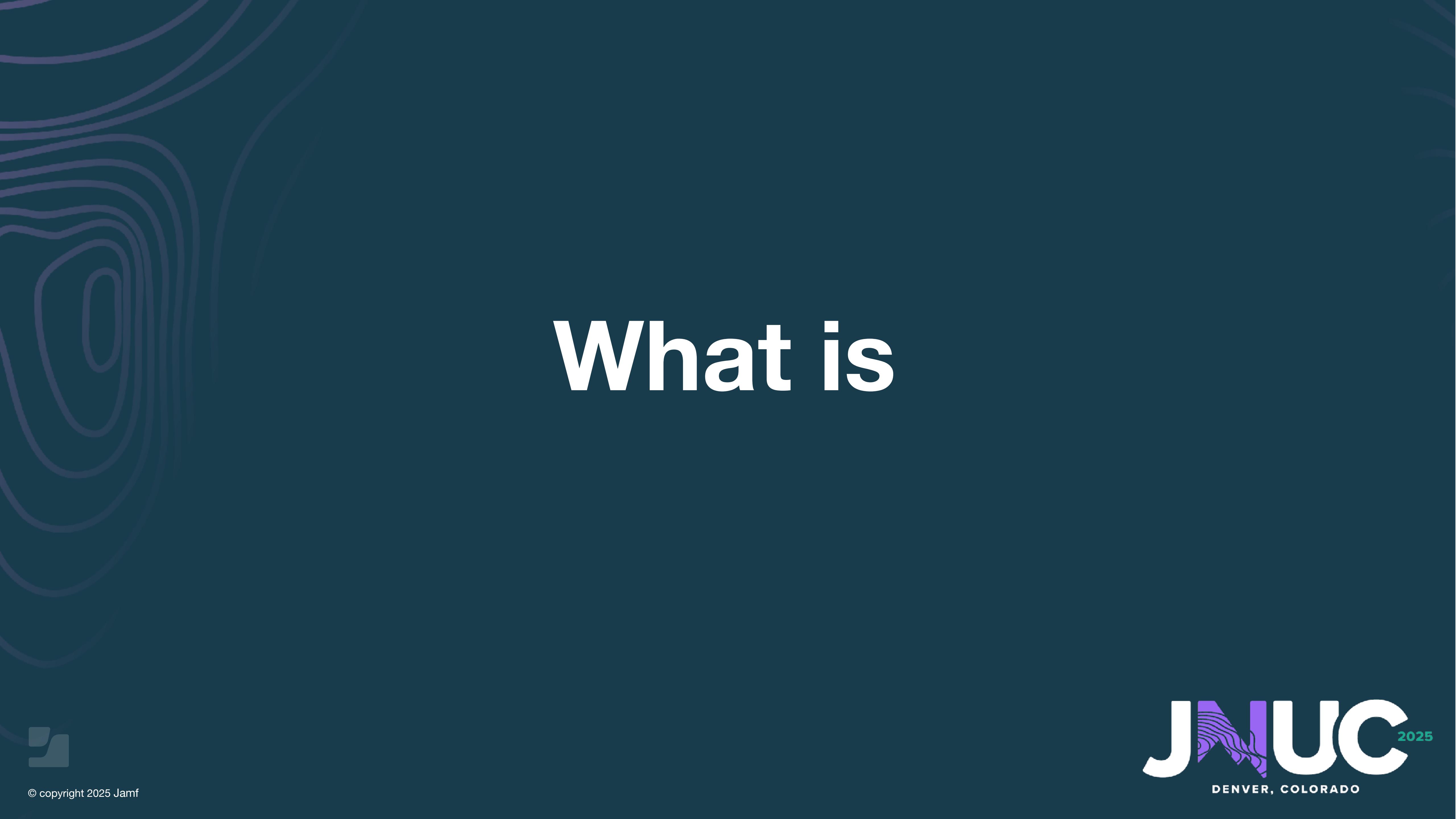


Matt Jerome

Fanatics

 @Matt Jerome





What is



What is Apple Intelligence



“ Apple Intelligence is the personal intelligence system that puts powerful generative models right at the core of your iPhone, iPad, Mac, Apple Vision Pro, and Apple Watch with incredible new features to help people communicate and work better. ”



Image Source: <https://developer.apple.com/apple-intelligence/>





© copyright 2025 Jamf

JNJC 2025
DENVER, COLORADO

Audio Recording



Summaries



Private Cloud Compute



Genemoji

Writing Tools

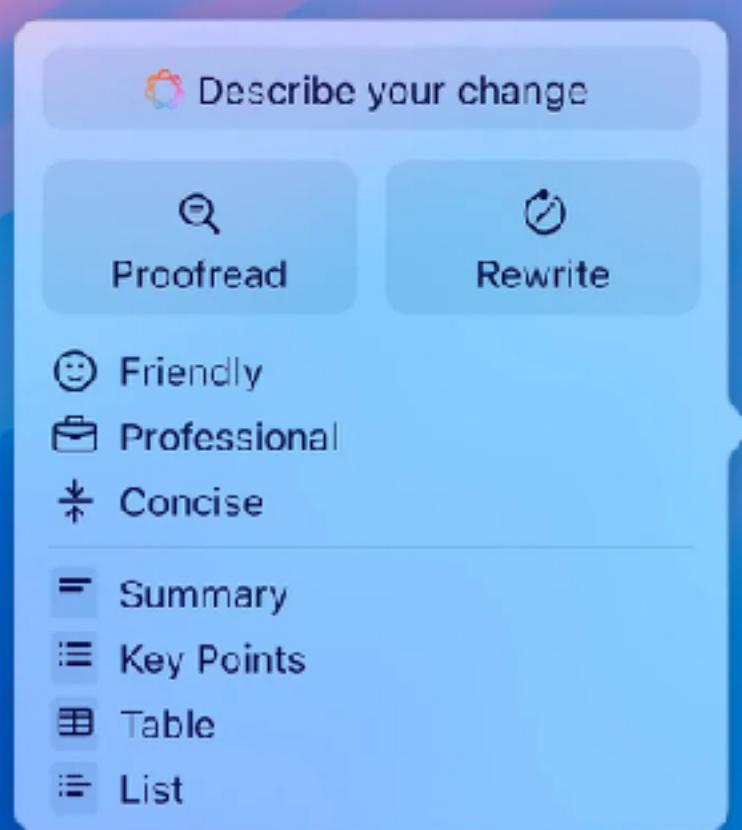


Image
Playground



Apple Intelligence

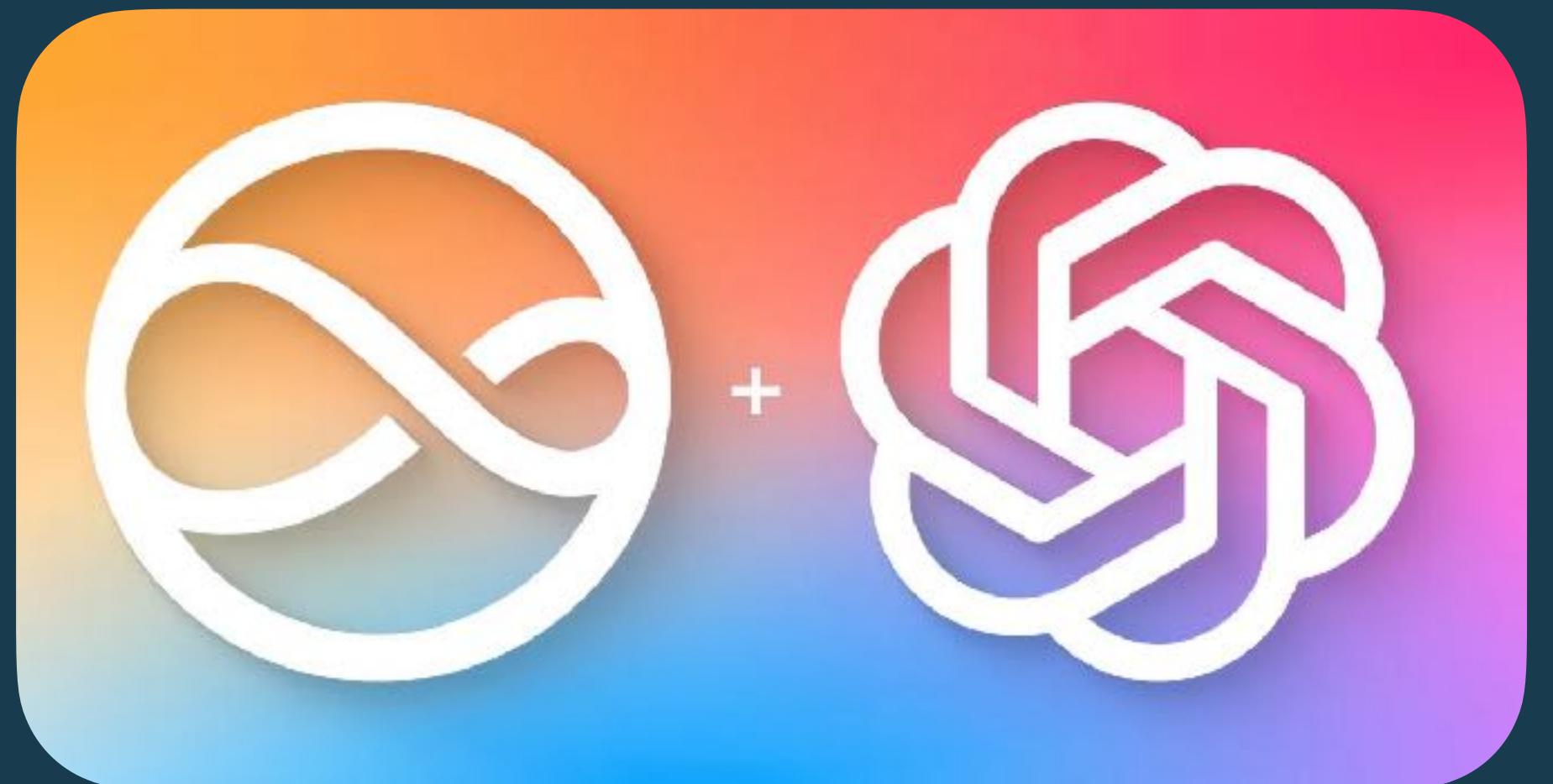


Image Wand

➡ Summaries
in Messages

eraser icon ➡ Clean Up
In Photos

JNUC 2025
DENVER, COLORADO



What is Private Cloud Compute?



Information Source: <https://security.apple.com/blog/private-cloud-compute/>

© copyright 2025 Jamf

JNUC
DENVER, COLORADO

What is Private Cloud Compute?

**Stateless Computation
on Personal User Data**



Information Source: <https://security.apple.com/blog/private-cloud-compute/>

© copyright 2025 Jamf

JNUC
DENVER, COLORADO

2025

What is Private Cloud Compute?

**Stateless Computation
on Personal User Data**

Enforceable Guarantees



Information Source: <https://security.apple.com/blog/private-cloud-compute/>

© copyright 2025 Jamf

What is Private Cloud Compute?

**Stateless Computation
on Personal User Data**

Enforceable Guarantees



No privileged runtime access

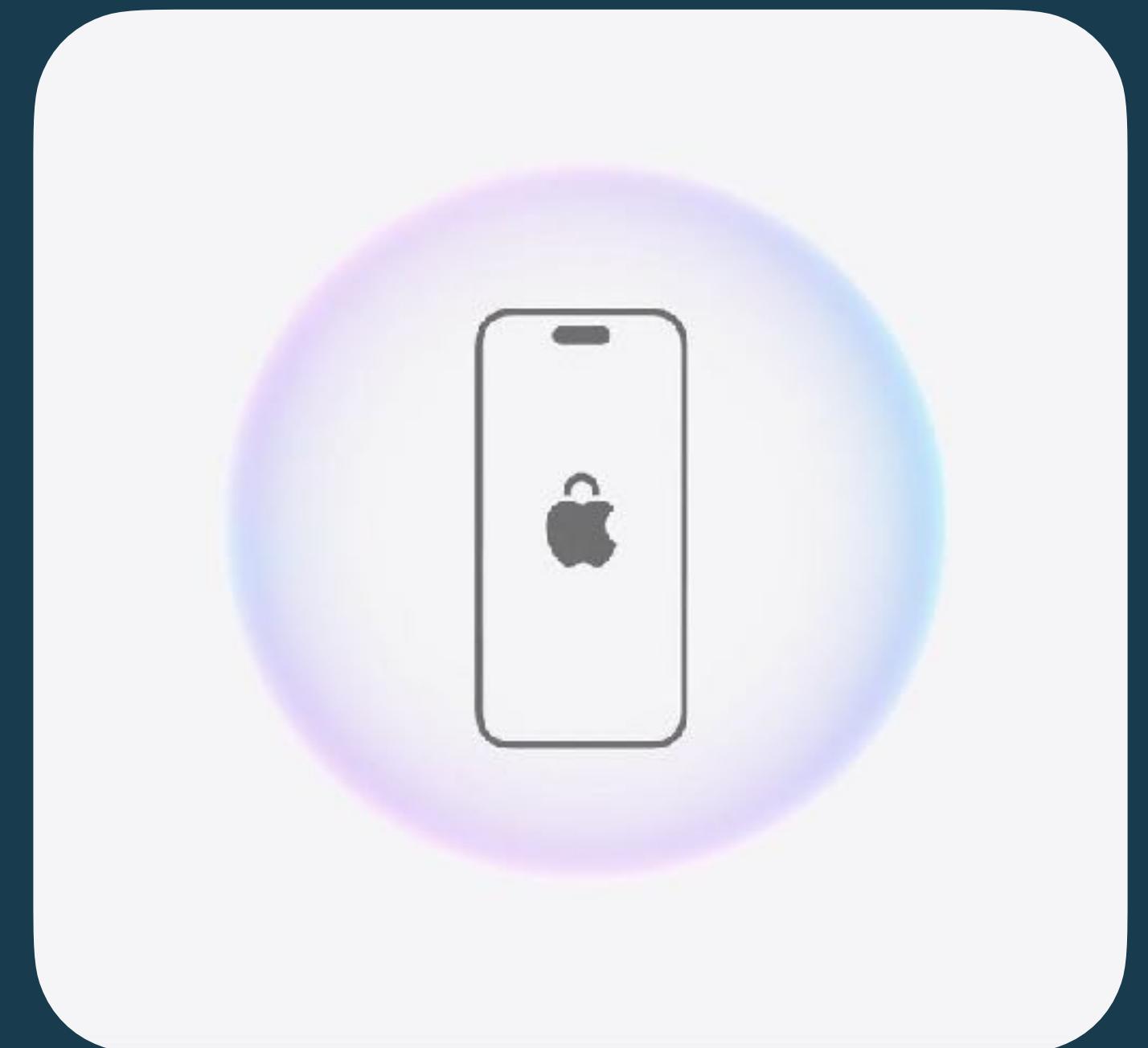


Information Source: <https://security.apple.com/blog/private-cloud-compute/>

What is Private Cloud Compute?

**Stateless Computation
on Personal User Data**

Enforceable Guarantees



Non-targetability

No privileged runtime access



Information Source: <https://security.apple.com/blog/private-cloud-compute/>

What is Private Cloud Compute?

**Stateless Computation
on Personal User Data**



Enforceable Guarantees

Non-targetability

Verifiable transparency

No privileged runtime access



Information Source: <https://security.apple.com/blog/private-cloud-compute/>

Who Do We Need?

IT Service Desk



Information Security



Jamf Pro Admin



Technology Leadership



How do we manage Apple Intelligence?



+



macOS Device Management

com.apple.applicationaccess

| Feature Name | Restriction | Minimum OS |
|-----------------------------|---|------------|
| Genemoji | allowGenemoji | macOS 15.0 |
| Writing Tools | allowWritingTools | macOS 15.0 |
| Image Playground | allowImagePlayground | macOS 15.0 |
| Mail Summary | allowMailSummary | macOS 15.1 |
| ChatGPT | allowExternalIntelligenceIntegrations | macOS 15.2 |
| | allowExternalIntelligenceIntegrationsSignIn | macOS 15.2 |
| | allowedExternalIntelligenceWorkspacesIDs | macOS 15.3 |
| Notes Transcription Summary | allowNotesTranscriptionSummary | macOS 15.3 |
| Notes Transcription | allowNotesTranscription | macOS 15.4 |
| Mail Smart Replies | allowMailSmartReplies | macOS 15.4 |
| Safari Summary | allowSafariSummary | macOS 15.4 |
| Apple Intelligence Report | allowAppleIntelligenceReport | macOS 15.4 |

macOS Device Management

com.apple.applicationaccess

| Feature Name | Restriction | Minimum OS |
|-----------------------------|--|------------|
| Genemoji | allowGenemoji | macOS 15.0 |
| Writing Tools | allowWritingTools | macOS 15.0 |
| Image Playground | allowImagePlayground | macOS 15.0 |
| Mail Summary | allowMailSummary | macOS 15.1 |
| ChatGPT | allowExternalIntelligenceIntegrations allowExternalIntelligenceIntegrationsSignIn allowedExternalIntelligenceWorkspacesIDs | macOS 15.2 |
| Notes Transcription Summary | allowNotesTranscriptionSummary | macOS 15.3 |
| Notes Transcription | allowNotesTranscription | macOS 15.4 |
| Mail Smart Replies | allowMailSmartReplies | macOS 15.4 |
| Safari Summary | allowSafariSummary | macOS 15.4 |
| Apple Intelligence Report | allowAppleIntelligenceReport | macOS 15.4 |

iOS and iPadOS Device Management

com.apple.applicationaccess

| Feature Name | Restriction | Minimum OS |
|----------------------------------|---|-----------------|
| Image Wand | allowImageWand | iOS/iPadOS 18.0 |
| Personalized Handwriting Results | allowPersonalizedHandwritingResults | iOS/iPadOS 18.0 |
| Genemoji | allowGenemoji | iOS/iPadOS 18.0 |
| Writing Tools | allowWritingTools | iOS/iPadOS 18.0 |
| Image Playground | allowImagePlayground | iOS/iPadOS 18.0 |
| Mail Summary | allowMailSummary | iOS/iPadOS 18.1 |
| Mail Smart Replies | allowMailSmartReplies | iOS/iPadOS 18.2 |
| ChatGPT | allowExternalIntelligenceIntegrations | iOS/iPadOS 18.2 |
| | allowExternalIntelligenceIntegrationsSignIn | iOS/iPadOS 18.2 |
| | allowedExternalIntelligenceWorkspacesIDs | iOS/iPadOS 18.3 |
| Visual Intelligence Summary | allowVisualIntelligenceSummary | iOS/iPadOS 18.3 |
| Notes Transcription Summary | allowNotesTranscriptionSummary | iOS/iPadOS 18.3 |
| Notes Transcription | allowNotesTranscription | iOS/iPadOS 18.4 |
| Safari Summary | allowSafariSummary | iOS/iPadOS 18.4 |
| Apple Intelligence Report | allowAppleIntelligenceReport | iOS/iPadOS 18.4 |

iOS and iPadOS Device Management

com.apple.applicationaccess

| Feature Name | Restriction | Minimum OS |
|----------------------------------|---|---|
| Image Wand | allowImageWand | iOS/iPadOS 18.0 |
| Personalized Handwriting Results | allowPersonalizedHandwritingResults | iOS/iPadOS 18.0 |
| Genemoji | allowGenemoji | iOS/iPadOS 18.0 |
| Writing Tools | allowWritingTools | iOS/iPadOS 18.0 |
| Image Playground | allowImagePlayground | iOS/iPadOS 18.0 |
| Mail Summary | allowMailSummary | iOS/iPadOS 18.1 |
| Mail Smart Replies | allowMailSmartReplies | iOS/iPadOS 18.2 |
| ChatGPT | allowExternalIntelligenceIntegrations allowExternalIntelligenceIntegrationsSignIn allowedExternalIntelligenceWorkspaceIDs | iOS/iPadOS 18.2 iOS/iPadOS 18.2 iOS/iPadOS 18.3 |
| Visual Intelligence Summary | allowVisualIntelligenceSummary | iOS/iPadOS 18.3 |
| Notes Transcription Summary | allowNotesTranscriptionSummary | iOS/iPadOS 18.3 |
| Notes Transcription | allowNotesTranscription | iOS/iPadOS 18.4 |
| Safari Summary | allowSafariSummary | iOS/iPadOS 18.4 |
| Apple Intelligence Report | allowAppleIntelligenceReport | iOS/iPadOS 18.4 |

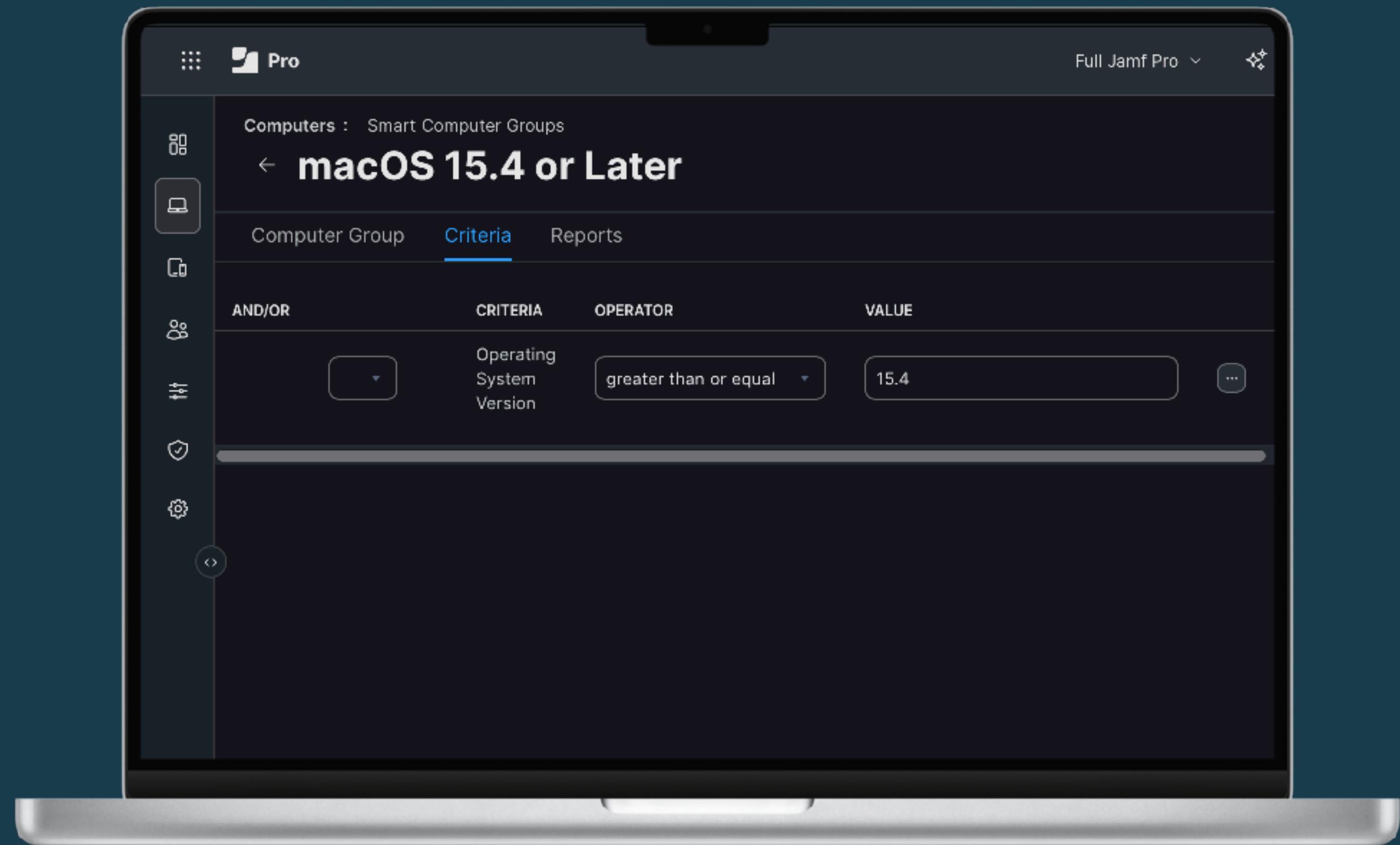
iOS and iPadOS Device Management

com.apple.applicationaccess

| Feature Name | Restriction | Minimum OS |
|----------------------------------|---|-----------------|
| Image Wand | allowImageWand | iOS/iPadOS 18.0 |
| Personalized Handwriting Results | allowPersonalizedHandwritingResults | iOS/iPadOS 18.0 |
| Genemoji | allowGenemoji | iOS/iPadOS 18.0 |
| Writing Tools | allowWritingTools | iOS/iPadOS 18.0 |
| Image Playground | allowImagePlayground | iOS/iPadOS 18.0 |
| Mail Summary | allowMailSummary | iOS/iPadOS 18.1 |
| Mail Smart Replies | allowMailSmartReplies | iOS/iPadOS 18.2 |
| ChatGPT | allowExternalIntelligenceIntegrations allowExternalIntelligenceIntegrationsSignIn allowedExternalIntelligenceWorkspaceIDs | iOS/iPadOS 18.2 |
| Visual Intelligence Summary | allowVisualIntelligenceSummary | iOS/iPadOS 18.3 |
| Notes Transcription Summary | allowNotesTranscriptionSummary | iOS/iPadOS 18.3 |
| Notes Transcription | allowNotesTranscription | iOS/iPadOS 18.4 |
| Safari Summary | allowSafariSummary | iOS/iPadOS 18.4 |
| Apple Intelligence Report | allowAppleIntelligenceReport | iOS/iPadOS 18.4 |

Smart Group Considerations

- Use the Operating System Version criteria for computers
- Use the OS Version criteria for mobile devices



Restricted Software

Computers : Restricted Software

← Block Apple Intelligence and Siri Pane

[Options](#) [Scope](#)

Process Name

Name of the process to restrict (e.g., "Chess", or "Chess.app"). The asterisk (*) can be used as a wildcard character

SiriPreferenceExtension

i When targeting a process in an application bundle, enter the name of the application bundle (e.g. "Chess.app").

Restrict exact process name
Only restrict processes that match the exact process name. The match is case-sensitive and recognizes the asterisk (*) as a literal character

Delete application
Delete the application running the restricted process

Send email notification on violation
When the process is found, send an email notification to Jamf Pro users with email notifications enabled. An SMTP server must be set up in Jamf Pro for this to work

Kill process
Terminate the process when found

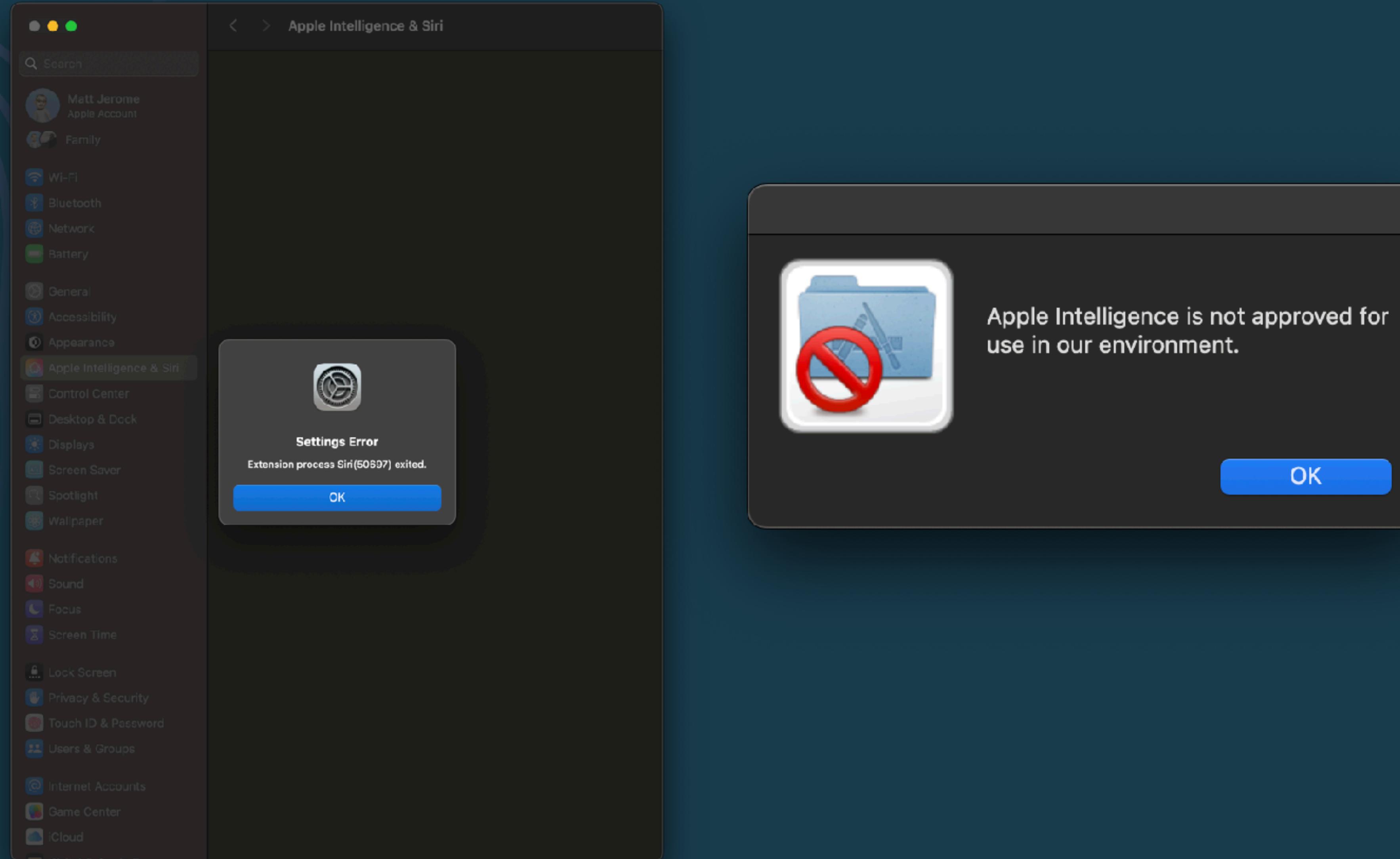
Message

Message to display to users when the process is found

Apple Intelligence is not approved for use in our environment.



Restricted Software



Deployment and Reporting

- Blueprints
- Configuration Profiles
- Prestage Enrollment Settings
- Extension Attributes



Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a blue border. The main content area is titled 'Blueprints' and contains a sub-header 'Manage your devices with our quick start solutions'. A prominent blue button in the top right corner says '+ Create blueprint'. Below this, there's a large dashed box containing a central icon with two '00' symbols and the text 'Choose a blueprint to begin'. To the right of this box, it says 'Discover an array of Declarative Data Management (DDM) configurations, tailored to address various needs.' Below the dashed box, there are four cards arranged in a 2x2 grid:

- Update software to latest version**: Keep all devices updated to the latest software version based on device eligibility. Targets iOS, iPadOS, and macOS.
- Set passcode policies**: Require users to set passcodes according to organizational requirements. Targets iOS, iPadOS, macOS, visionOS, and watchOS.
- Install disk management settings**: Configure restriction levels for external storage and network storage. Targets macOS.
- Math settings**: Configure Calculator and related math settings on devices. Targets iOS, iPadOS, and macOS.



Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option in the sidebar is highlighted with a red circle. On the main content page, the 'Blueprints' section is displayed with the title 'Blueprints' and the subtitle 'Manage your devices with our quick start solutions'. A blue button labeled '+ Create blueprint' is also circled in red. The main content area features four cards: 'Choose a blueprint to begin' (with a '00:00' timer icon), 'Update software to latest version' (with iOS, iPadOS, macOS tags), 'Set passcode policies' (with iOS, iPadOS, macOS, visionOS, watchOS tags), 'Install disk management settings' (with macOS tag), and 'Math settings' (with iOS, iPadOS, macOS tags).



Blueprints

The screenshot shows the Jamf Pro interface with the "Blueprints" section highlighted. On the left sidebar, under the "Blueprints" heading, there is a "New blueprint" dialog box. The dialog has fields for "Name" and "Description". Below the dialog, there are three cards: "Update software to last", "Install disk management settings", and "Math settings".

New blueprint

Name Enter a unique name for this blueprint.

Description Describe what this blueprint is used for.

Update software to last
Keep all devices updated and eligible.
iOS iPadOS macOS

Install disk management settings
Configure restriction levels for external storage and network storage.
macOS

Math settings
Configure Calculator and related math settings on devices.
iOS iPadOS macOS

Blueprints

The screenshot shows the Jamf Pro interface with the 'Blueprints' section selected in the sidebar. A modal window titled 'New blueprint' is open, prompting for a name and description. The 'Name' field contains 'Disallow Apple Intelligence External Integrations'. The 'Description' field is empty. The 'Create' button at the bottom right of the modal is highlighted with a red circle.

Blueprints

Manage your devices with our quick start solutions

+ Create blueprint

New blueprint

Name Enter a unique name for this blueprint.
Disallow Apple Intelligence External Integrations

Description Describe what this blueprint is used for.

Create

Cancel

Update software to last

Keep all devices updated to remain eligible.

iOS iPadOS macOS

Install disk management settings

Configure restriction levels for external storage and network storage.

macOS

Math settings

Configure Calculator and related math settings on devices.

iOS iPadOS macOS



Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a dark gray background. The main content area displays a blueprint titled 'Disallow Apple Intelligence External Integrations'. The blueprint status is 'Incomplete' with the note 'Define scope and add components'. The scope is 'Not configured' with the note 'Select groups to begin configuring this blueprint'. The recent activity shows 'Just now' (Last updated) and 'Never' (Last deployed). On the left, the 'Components library' is visible, listing four items: 'Restrictions' (Jamf | 1.0.0), 'Safari extensions' (Jamf | 1.0.0), 'Screensaver User' (Jamf | 1.0.0), and 'Service Background Tasks' (Jamf | 1.0.0). A large central box labeled 'Declaration group' contains the instruction 'Drag components from the library to add them.'



Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected and highlighted with a red box. The main content area displays a blueprint titled 'Disallow Apple Intelligence External Integrations'. The blueprint status is 'Incomplete' with the note 'Define scope and add components'. The scope is set to 'Not configured' with the note 'Select groups to begin configuring this blueprint'. The recent activity shows 'Just now' and 'Never'. The 'Components library' section lists several items, with the 'Restrictions' component circled in red. Other components listed include 'Safari extensions', 'Screensaver User', and 'Service Background'. A 'Declaration group' section is shown below the components library.

Blueprints / Disallow Apple Intelligence External Integrations

Disallow Apple Intelligence External Integrations

Status: Incomplete
Scope: Not configured
Recent activity: Just now, Never

Components library

- Restrictions (Jamf | 1.0.0) - Circled in red
- Safari extensions (Jamf | 1.0.0)
- Screensaver User (Jamf | 1.0.0)
- Service Background (Tasks)

Declaration group

Drag components from the library to add them.



Blueprints

The screenshot shows the Jamf Pro interface with the 'Blueprints' section selected in the sidebar. A modal window titled 'Restrictions' is open, showing two configuration items:

- Allow external intelligence integrations**
allowExternalIntelligenceIntegrations
If 'false', disables the use of external, cloud-based intelligence services with Siri. On iOS, this restriction is temporarily allowed on unsupervised and user enrollments. In a future release, this restriction will require supervision, and will be ignored on non-supervised devices. Available in iOS 18.2 and later, and macOS 15.2 and later.
iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence
false true
- Allow external intelligence integrations sign-in**
allowExternalIntelligenceIntegrationsSignIn
If 'false', forces external intelligence providers into anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be signed out when the next request is attempted. Available in iOS 18.2 and later, and macOS 15.2 and later.
iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence
false true

At the bottom right of the modal are 'Cancel' and 'Add' buttons.



Blueprints

The screenshot shows the Jamf Pro interface with the 'Blueprints' section selected in the sidebar. A modal window titled 'Restrictions' is open, showing two configuration items:

- Allow external intelligence integrations**
allowExternalIntelligenceIntegrations
If 'false', disables the use of external, cloud-based intelligence services with Siri. On iOS, this restriction is temporarily allowed on unsupervised and user enrollments. In a future release, this restriction will require supervision, and will be ignored on non-supervised devices. Available in iOS 18.2 and later, and macOS 15.2 and later.
 iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence
- Allow external intelligence integrations sign-in**
allowExternalIntelligenceIntegrationsSignIn
If 'false', forces external intelligence providers into anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be signed out when the next request is attempted. Available in iOS 18.2 and later, and macOS 15.2 and later.
 iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence

The 'iOS 18.2+', 'macOS 15.2+', and 'visionOS 2.4+' buttons in both sections are highlighted with a red oval.

Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a blue border. A modal window titled 'Restrictions' is displayed, showing two configuration items under the 'Apple Intelligence' category:

- Allow external intelligence integrations**
allowExternalIntelligenceIntegrations
If 'false', disables the use of external, cloud-based intelligence services with Siri. On iOS, this restriction is temporarily allowed on unsupervised and user enrollments. In a future release, this restriction will require supervision, and will be ignored on non-supervised devices. Available in iOS 18.2 and later, and macOS 15.2 and later.
 iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence
- Allow external intelligence integrations sign-in**
allowExternalIntelligenceIntegrationsSignIn
If 'false', forces external intelligence providers into anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be signed out when the next request is attempted. Available in iOS 18.2 and later, and macOS 15.2 and later.
 iOS 18.2+ macOS 15.2+ visionOS 2.4+ Apple Intelligence

At the bottom right of the modal, there are 'Cancel' and 'Add' buttons. The 'Add' button is circled in red.

Blueprints

The screenshot shows the Jamf Pro interface with a sidebar on the left containing navigation items: Dashboard, Computers, Devices, Users, **Blueprints**, Compliance, and Settings. The main area displays a Blueprint titled "Blueprints / Disallow Apple Intelligence External Integrations" with the subtitle "Disallow Apple Intelligence Ext". Below this, there's a "Status" section showing "Last updated Jul 2, 2021" and "Last deployed Jul 2, 2021". A "Declaration group" section is also visible. On the right, a modal window titled "Restrictions" (Jamf | 1.0.0) is open, listing three configuration options:

- Allow account modification** (allowAccountModification): If false, the system disables modification of accounts such as Apple Accounts and Internet-based accounts such as Mail, Contacts, and Calendar. Available in iOS 7 and later, macOS 14 and later, and watchOS 10 and later. Requires a supervised device in iOS and watchOS.
 iOS 7.0+ macOS 14.0+ visionOS 2.0+ watchOS 10.0+
false true
- Allow Handoff** (allowActivityContinuation): If false, the system disables activity continuation. Available in iOS 8 and later, and macOS 10.15 and later. Support for this restriction on unsupervised devices and with Managed Apple Accounts is deprecated. In a future release, this restriction will begin requiring supervision and will apply to personal Apple Accounts only.
 iOS 8.0+ macOS 10.15+ visionOS 2.0+
false true
- Allow Adding Game Center Friends** (allowAddingGameCenterFriends): If false, the system prohibits adding friends to Game Center. Available in iOS 4.2.1 and later, and macOS 10.13 and later. Requires a supervised device in iOS 13 and later.
 iOS 4.2.1+ macOS 10.13+
false true

At the bottom of the modal are "Close" and "Save" buttons.

Blueprints

Blueprints / Disallow Apple Intelligence External Integrations

Disallow Apple Intelligence Ext

Status

Last updated Jul 2, 2024

Last deployed Jul 2, 2024

Declaration group

Restrictions

Jamf | 1.0.0

Allow account modification
allowAccountModification
If 'false', the system disables modification of accounts such as Apple Accounts and Internet-based accounts such as Mail, Contacts, and Calendar. Available in iOS 7 and later, macOS 14 and later, and watchOS 10 and later. Requires a supervised device in iOS and watchOS.
iOS 7.0+ macOS 14.0+ visionOS 2.0+ watchOS 10.0+
false true

Allow Handoff
allowActivityContinuation
If 'false', the system disables activity continuation. Available in iOS 8 and later, and macOS 10.15 and later. Support for this restriction on unsupervised devices and with Managed Apple Accounts is deprecated. In a future release, this restriction will begin requiring supervision and will apply to personal Apple Accounts only.
iOS 8.0+ macOS 10.15+ visionOS 2.0+
false true

Allow Adding Game Center Friends
allowAddingGameCenterFriends
If 'false', the system prohibits adding friends to Game Center. Available in iOS 4.2.1 and later, and macOS 10.13 and later. Requires a supervised device in iOS 13 and later.
iOS 4.2.1+ macOS 10.13+
false true

Close Save

Blueprints

The screenshot shows the Jamf Pro interface with a sidebar on the left containing navigation items: Dashboard, Computers, Devices, Users, **Blueprints**, Compliance, and Settings. The main area displays a Blueprint titled "Blueprints / Disallow Apple Intelligence External Integrations" with the subtitle "Disallow Apple Intelligence Ext". Below this, there's a "Status" section showing "Last updated" and "Last deployed" both as "Jul 2, 2021". A "Declaration group" section is visible, followed by a "Restrictions" section. A modal window titled "Restrictions" is open, showing three specific restrictions: "Allow account modification", "Allow Handoff", and "Allow Adding Game Center Friends". Each restriction has a checkbox, a description, and a "false" or "true" button. The modal also includes a "Filters" section with OS Type (iOS, macOS, tvOS, visionOS, watchOS), Requirements & support (Supervised, Shared iPad), and Category (Apple Intelligence, AirDrop, AirPlay, AirPrint, iCloud, Software Update, noCategory). At the bottom of the modal are "Close" and "Save" buttons.

Blueprints / Disallow Apple Intelligence External Integrations

Disallow Apple Intelligence Ext

Status

Last updated Jul 2, 2021

Last deployed Jul 2, 2021

Declaration group

Restrictions

Jamf | 1.0.0

Restrictions

Jamf | 1.0.0

Filters

OS Type

iOS macOS tvOS visionOS watchOS

Requirements & support

Supervised Shared iPad

Category

Apple Intelligence AirDrop AirPlay AirPrint iCloud Software Update noCategory

Allow account modification
allowAccountModification
If 'false', the system disables modifications to accounts such as Mail, Contacts, Calendar, and Reminders. Available in iOS 7.0 and later, and macOS 10.10 and later. Requires a supervised device in iOS 13 and later.
false true

Allow Handoff
allowActivityContinuation
If 'false', the system disables activity continuation. Available in iOS 8.0 and later, and macOS 10.11 and later. Support for this restriction is deprecated. In a future release, this restriction will only apply to personal Apple Accounts only.
false true

Allow Adding Game Center Friends
allowAddingGameCenterFriends
If 'false', the system prohibits adding friends to Game Center. Available in iOS 4.2.1 and later, and macOS 10.13 and later. Requires a supervised device in iOS 13 and later.
false true

Close **Save**

Blueprints

Blueprints / Disallow Apple Intelligence External Integrations

Disallow Apple Intelligence Ext

Status

Last updated Jul 2, 2024

Last deployed Jul 2, 2024

Declaration group

Restrictions

Jamf | 1.0.0

Allow account modification
allowAccountModification
If 'false', the system disables modifications to accounts such as Mail, Contacts, Calendar, and Reminders. Available in iOS 7.0 and later, and macOS 10.14 and later. Requires a supervised device.

Allow Handoff
allowActivityContinuation
If 'false', the system disables activity continuation. Available in iOS 8.0 and later, and macOS 10.15 and later. Support for this restriction is deprecated. In a future release, this restriction will only apply to personal Apple Accounts only.

Allow Adding Game Center Friends
allowAddingGameCenterFriends
If 'false', the system prohibits adding friends to Game Center. Available in iOS 4.2.1 and later, and macOS 10.13 and later. Requires a supervised device in iOS 13 and later.

Category

Apple Intelligence (highlighted with a red circle)

Close Save

Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected. The main content area displays a Blueprint titled 'Blueprints / Disallow Apple Intelligence External Integrations' with the subtitle 'Disallow Apple Intelligence External Integrations'. The Blueprint status is shown as 'Last updated Jul 2, 2023' and 'Last deployed Jul 2, 2023'. A 'Declaration group' section contains a 'Restrictions' payload. The 'Restrictions' payload is set to 'Jamf | 1.0.0' and includes the following configuration:

Restrictions
Jamf | 1.0.0

Filters: Apple Intelligence

Allow Apple Intelligence
allowAppleIntelligenceReport
If 'false', the system disables App 15.4 and later.
iOS 18.4+ macOS 15.4+
false true

Allowed External Intelligence
allowedExternalIntelligence
An array of strings, but currently allows the given external integration workspace ID to be used, and requires a sign-in to make requests; the user will be required to sign in to integrations that support signing in. Multiple payloads combine using an intersect operation. This means the allowed set of workspace IDs can become the empty set if conflicting values are specified in multiple payloads.
iOS 18.3+ macOS 15.3+ visionOS 2.4+ Apple Intelligence
+ Add new item

Allow external intelligence integrations
allowExternalIntelligenceIntegrations
If 'false' disables the use of external cloud-based intelligence services with Siri. On iOS, this

Save

Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a dark grey background. The main content area displays a blueprint titled 'Disallow Apple Intelligence External Integrations'. The blueprint status is 'Incomplete' and the scope is 'Not configured'. A callout box points to the 'Scope' section with the text 'Select groups to begin configuring this blueprint'. On the right, there's a 'Recent activity' summary showing 'Just now', 'Last updated', and 'Never' for deployment status. Below the status bar, there's a 'Components library' section with a search bar and a dropdown set to 'All'. It lists four components: 'Restrictions' (Jamf | 1.0.0, Legacy payload), 'Safari extensions' (Jamf | 1.0.0, Configuration), 'Screensaver User' (Jamf | 1.0.0, Legacy payload), and 'Service Background Tasks' (Jamf | 1.0.0, Configuration). To the right of the components, there's a 'Declaration group' section and a 'Restrictions' section for 'com.apple.applicationaccess' using a 'Legacy payload'.



Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a dark grey background. The main content area displays a Blueprint titled 'Disallow Apple Intelligence External Integrations'. The Blueprint status is 'Incomplete' with the message 'Define scope'. A red circle highlights the 'Scope' section, which contains the text 'Not configured' and 'Select groups to begin configuring this blueprint'. To the right of the scope is a 'Recent activity' section showing 'Just now', 'Last updated', 'Never', and 'Last deployed'. Below the scope are sections for 'Components library' (with 'Restrictions' selected), 'Declaration group', and 'Restrictions' (specifically 'com.apple.applicationaccess'). On the left sidebar, other menu items like 'Dashboard', 'Computers', 'Devices', 'Users', 'Compliance', and 'Settings' are visible.

Blueprints

The screenshot shows the Jamf Pro interface with the following details:

- Left Sidebar:** Includes links for Dashboard, Computers, Devices, Users, **Blueprints** (selected), Compliance, and Settings.
- Current View:** Blueprint titled "Disallow Apple Intelligence External Integrations". Status: Not deployed (Blueprint ready for deployment).
- Components Library:** Shows four items:
 - Restrictions:** Jamf | 1.0.0, Legacy payload
 - Safari extensions:** Jamf | 1.0.0, Configuration
 - Screensaver User:** Jamf | 1.0.0, Legacy payload
 - Service Background Tasks:** Jamf | 1.0.0, Configuration
- Scope Tab:** Target section titled "Scope".
 - Buttons: All, Smart, Static, **Q or Later** (highlighted with a blue border).
 - Options:
 - iOS 18.2 or Later
 - macOS 15 or Later
 - macOS 15.2 or Later
 - macOS 15.4 or Later
- Bottom Right:** Buttons for Cancel and Save.



Blueprints

The screenshot shows the Jamf Pro interface with the following details:

- Left Sidebar:** Shows navigation links: Dashboard, Computers, Devices, Users, **Blueprints** (selected), Compliance, and Settings.
- Current View:** Blueprint titled "Disallow Apple Intelligence External Integrations". Status: Not deployed (Blueprint ready for deployment).
- Components Library:** Lists available components:
 - Restrictions (Jamf | 1.0.0) - Legacy payload
 - Safari extensions (Jamf | 1.0.0) - Configuration
 - Screensaver User (Jamf | 1.0.0) - Legacy payload
 - Service Background Tasks (Jamf) - Configuration
- Scope (Top Right):** Targets iOS 18.2 or Later and macOS 15.2 or Later. These two items are circled in red.
- Buttons (Bottom Right):** Cancel and Save.

Blueprints

The screenshot shows the Jamf Pro interface with the sidebar menu open. The 'Blueprints' option is selected, highlighted with a dark gray background. The main content area displays a blueprint titled 'Disallow Apple Intelligence External Integrations'. The status is 'Not deployed' (blueprint ready for deployment). The scope includes 2 Groups and 2 Devices, targeting iOS 18.2 or Later and macOS 15.2 or Later. The recent activity shows 'Just now' for last updated and 'Never' for last deployed. The components library lists 'Restrictions', 'Safari extensions', 'Screensaver User', and 'Service Background Tasks', all categorized as 'Legacy payload'. A declaration group for 'com.apple.applicationaccess' is shown, using a 'Legacy payload' component.

Blueprints

The screenshot shows the Jamf Pro interface with the 'Blueprints' section selected in the sidebar. The main view displays a blueprint titled 'Disallow Apple Intelligence External Integrations'. The status is 'Not deployed' (Blueprint ready for deployment). The scope includes 2 Groups and 2 Devices, targeting iOS 18.2 or Later and macOS 15.2 or Later. The recent activity shows 'Just now' for last updated and 'Never' for last deployed. The 'Components library' section lists 'Restrictions', 'Safari extensions', 'Screensaver User', and 'Service Background Tasks'. The 'Declaration group' section shows a 'Restrictions' component with the identifier com.apple.applicationaccess, categorized as a Legacy payload.

Blueprints

Blueprints / Disallow Apple Intelligence External Integrations

Disallow Apple Intelligence External Integrations

Deployment progress

0 Deployed • 0 Pending • 0 Error

2 Groups 2 Devices

iOS 18.2 or Later macOS 15.2 or Later

Recent activity

Just now Last updated Just now Last deployed

Components library

All

Search

Restrictions Jamf | 1.0.0 Legacy payload

Safari extensions Jamf | 1.0.0 Configuration

Screensaver User Jamf | 1.0.0 Legacy payload

Service Background Tasks Configuration

Declaration group

Restrictions com.apple.applicationaccess Legacy payload

Blueprint deployment started.



Blueprints

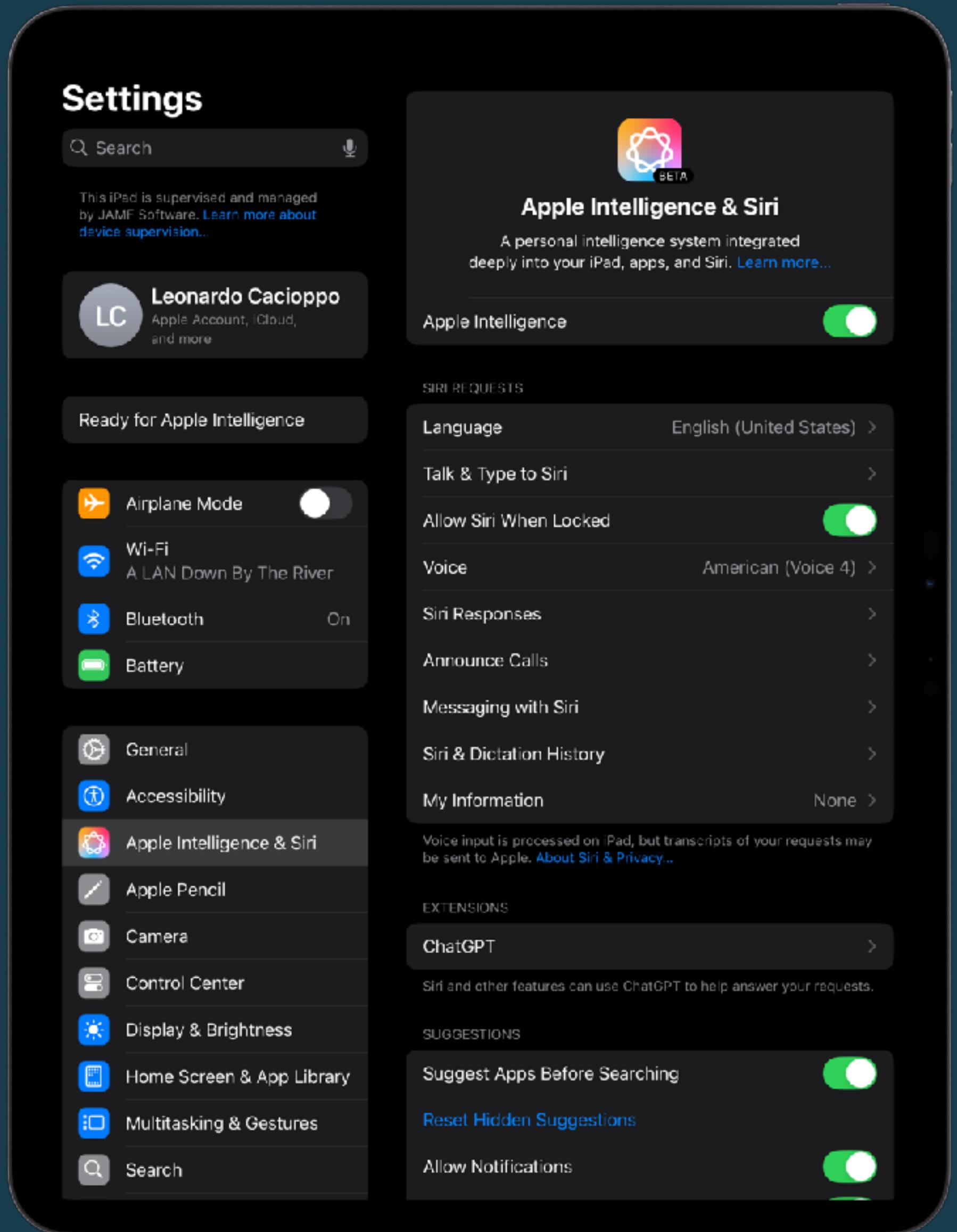
The screenshot shows the Jamf Pro interface with the 'Blueprints' section selected in the sidebar. The main area displays the title 'Disallow Apple Intelligence External Integrations' and a status summary. The status summary includes:

- Status:** Deployment progress (0 Deployed, 0 Pending, 0 Error)
- Scope:** 2 Groups, 2 Devices (iOS 18.2 or Later, macOS 15.2 or Later)
- Recent activity:** Just now (Last updated), Just now (Last deployed)

The interface also shows a 'Components library' with items like 'Restrictions', 'Safari extensions', 'Screensaver User', and 'Service Background Tasks'. A 'Declaration group' section is visible, and a success message at the bottom states: 'Blueprint deployment started.'

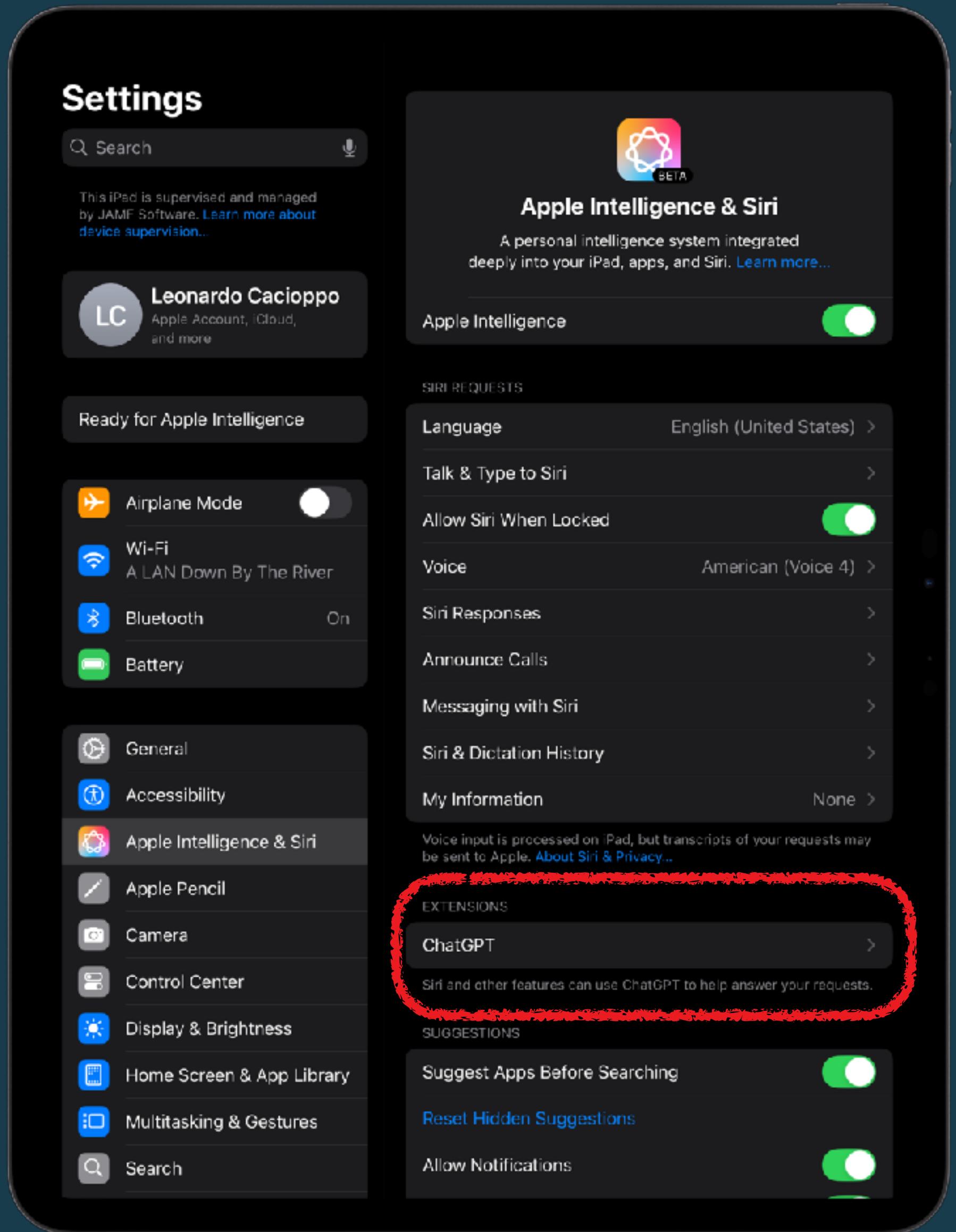
Blueprints

Restrict **Allow**



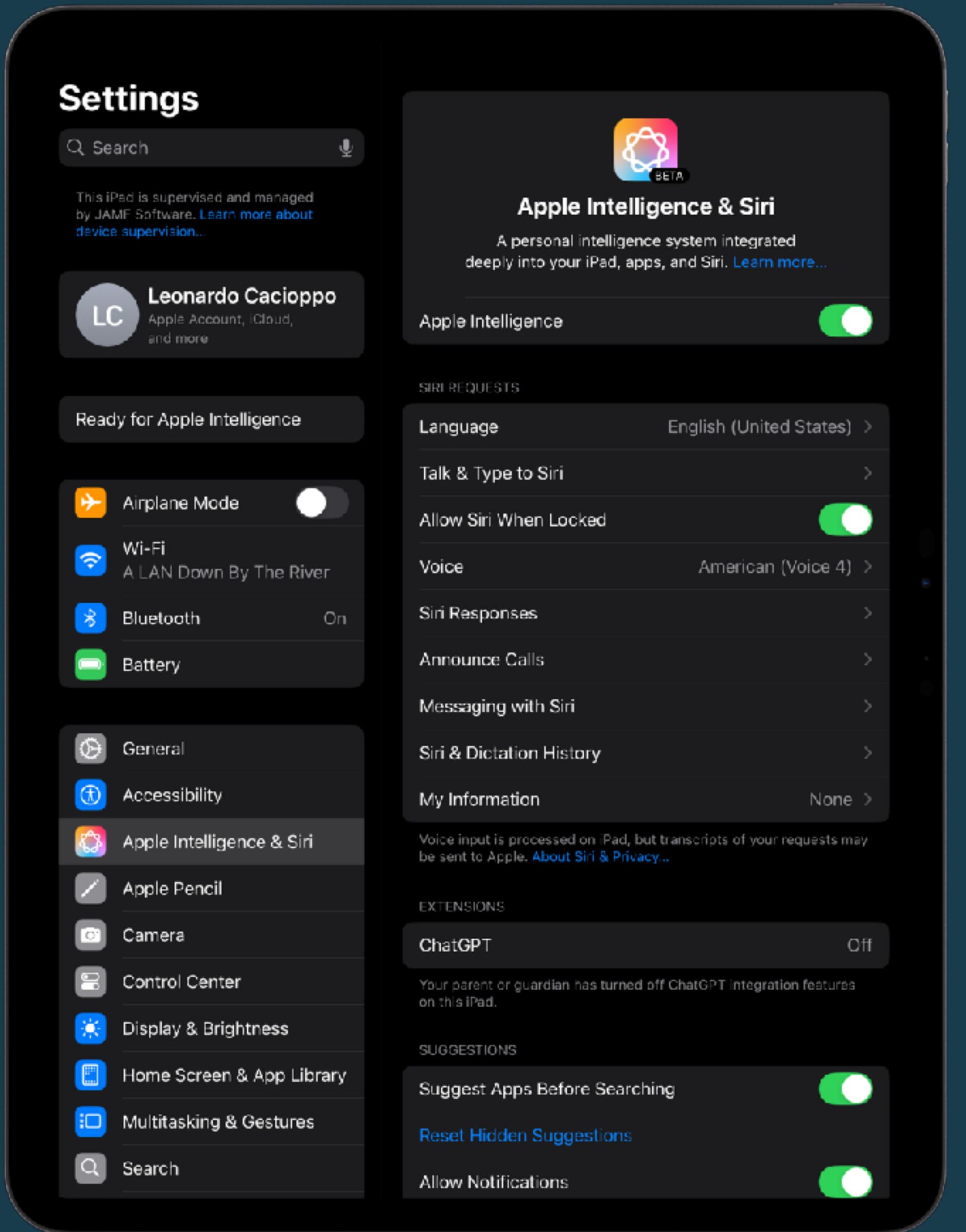
Blueprints

Restrict **Allow**



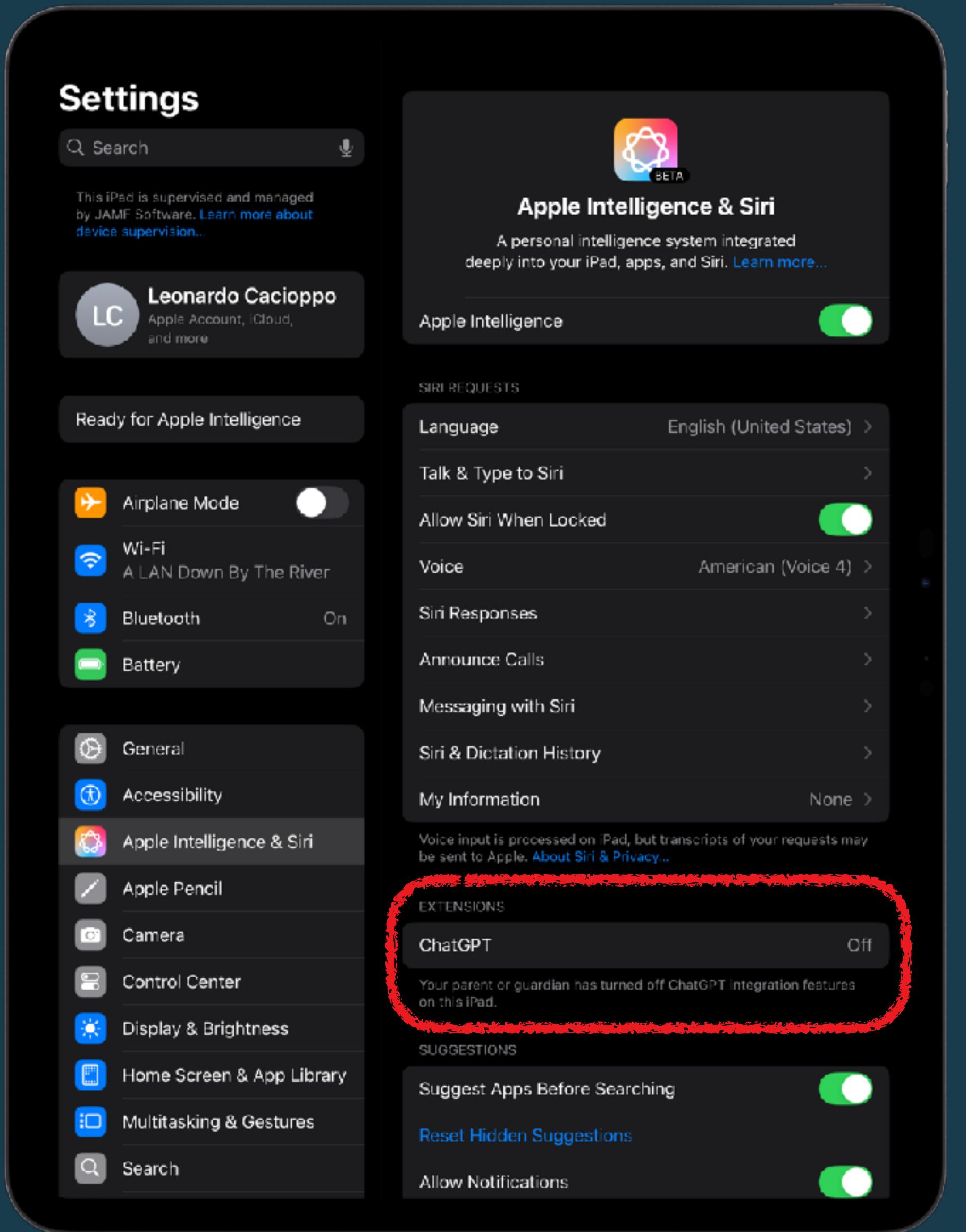
Blueprints

Restrict Allow



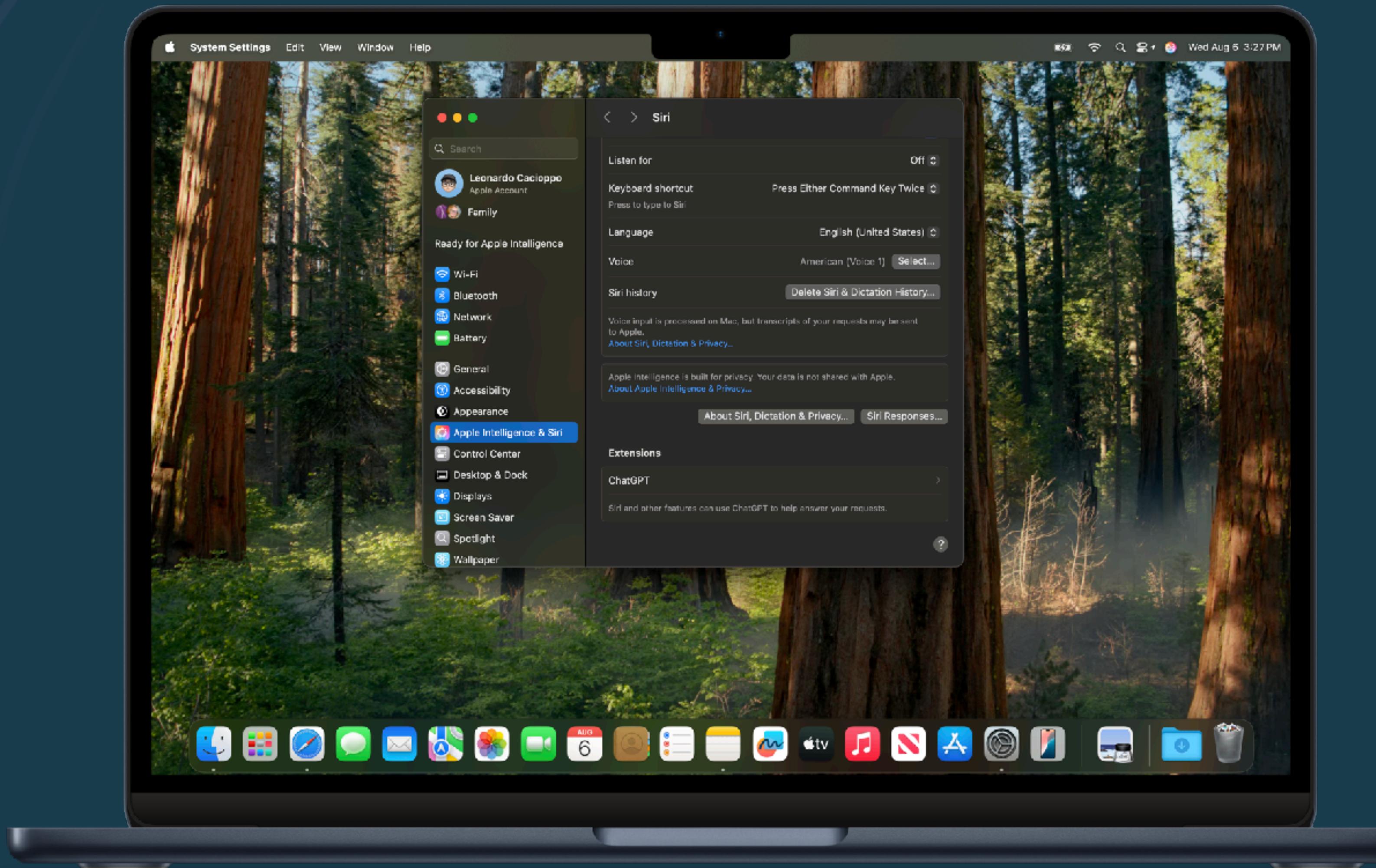
Blueprints

Restrict Allow



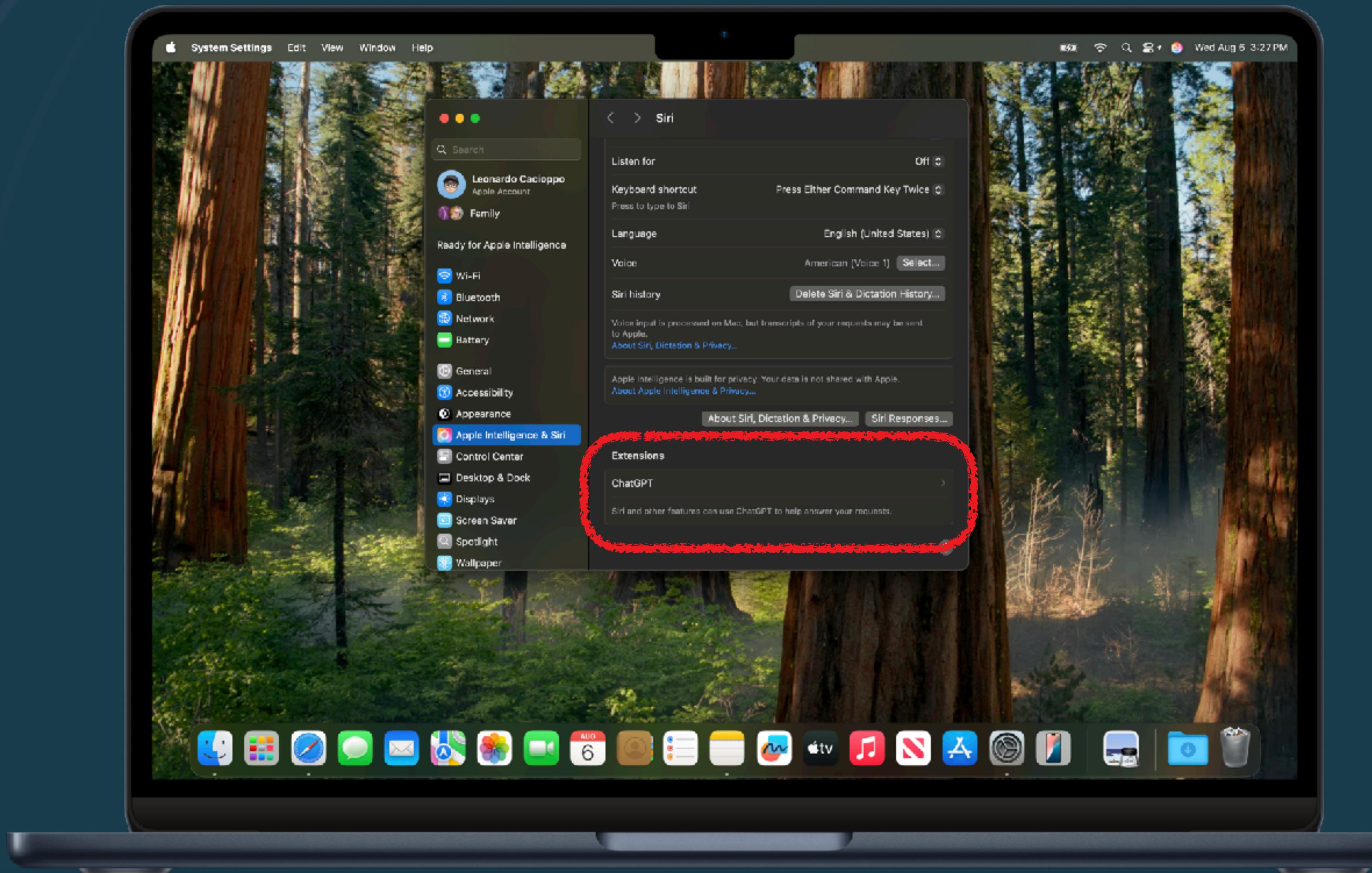
Blueprints

Restrict **Allow**



Blueprints

Restrict **Allow**



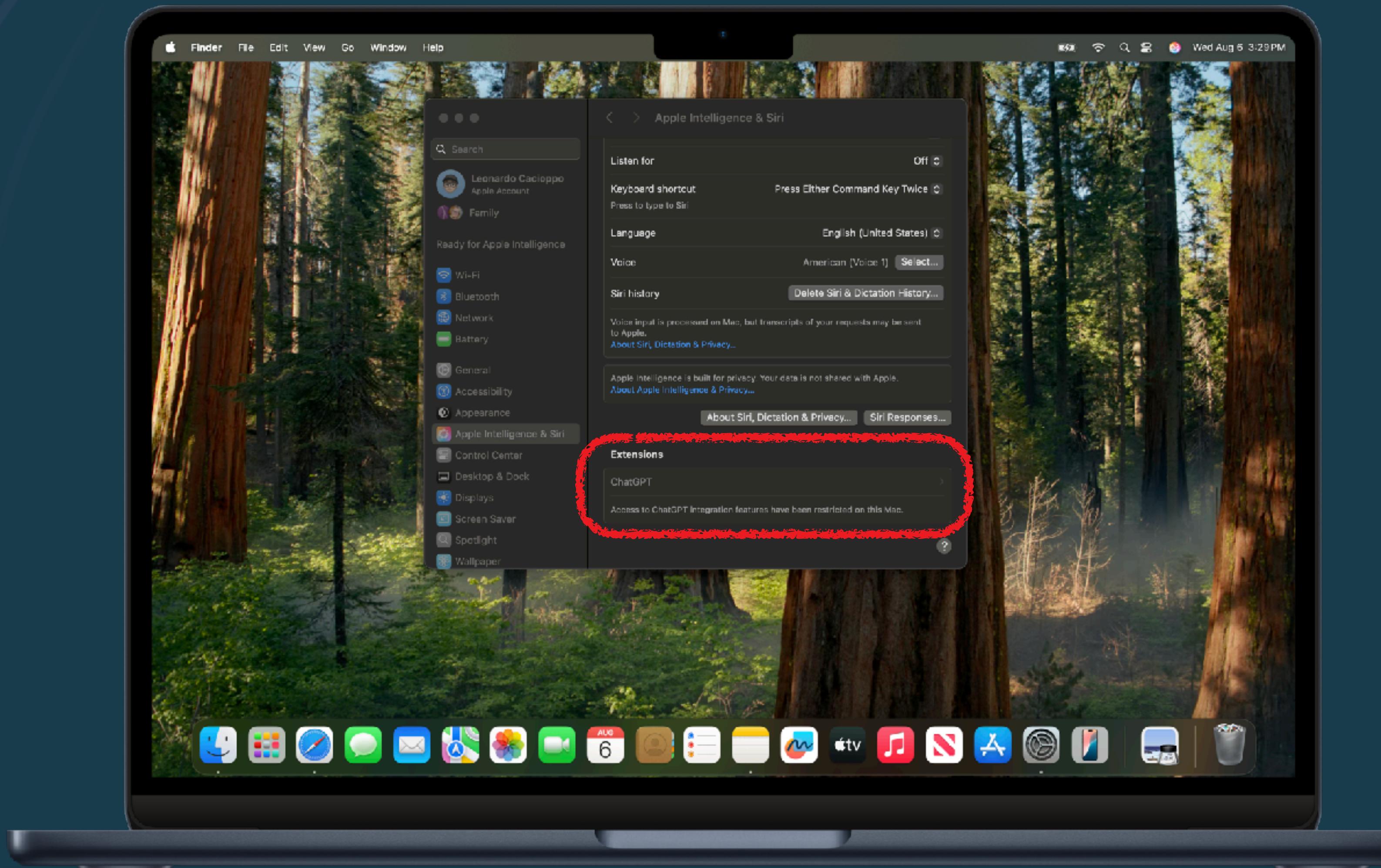
Blueprints

Restrict Allow



Blueprints

Restrict Allow



Configuration Profiles - macOS

com.apple.applicationaccess

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  </dict>
    <key>allowiPhoneMirroring</key>
    <false/>
    <key>allowGenemoji</key>
    <true/>
    <key>allowPersonalizedHandwritingResults</key>
    <true/>
    <key>allowVideoConferencingRemoteControl</key>
    <true/>
    <key>allowWritingTools</key>
    <true/>
    <key>allowMailSummary</key>
    <false/>
    <key>forceBypassScreenCaptureAlert</key>
    <true/>
    <key>allowExternalIntelligenceIntegrations</key>
    <true/>
    <key>allowExternalIntelligenceIntegrationsSignIn</key>
    <false/>
  </dict>
</plist>
```



Configuration Profiles - macOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on macOS. The left sidebar navigation includes Computers, Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management (with Policies and Configuration Profiles selected), Configuration Profiles (with Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups), and a section for Approved Kernel Extensions, Associated Domains, Certificates, Transparency, and Content Filter.

The main content area is titled "Apple Intelligence Restrictions". It displays an "Upload" section with one payload configured, labeled "com.apple.applicationaccess". This section allows defining generic settings for preference domains. The "Preference Domain" field is set to "com.apple.applicationaccess" (Required). The "Property List" field contains the following XML code:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>allowiPhoneMirroring</key>
    <false/>
    <key>allowGenemoji</key>
    <true/>
    <key>allowPersonalizedHandwritingResults</key>
    <true/>
    <key>allowVideoConferencingRemoteControl</key>
    <true/>
    <key>allowWritingTools</key>
    <true/>
    <key>allowMailSummary</key>
    <false/>
    <key>forceBypassScreenCaptureAlert</key>
    <true/>
    <key>allowExternalIntelligenceIntegrations</key>

```



Configuration Profiles - macOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on macOS. The left sidebar is titled 'Computers' and includes sections for Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management, Policies, Configuration Profiles (which is selected and highlighted), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups. The main content area is titled 'Apple Intelligence Restrictions' under 'Computers : Configuration Profiles'. It has tabs for 'Options' (selected) and 'Scope'. A search bar shows 'Search... NOT configured'. Below it is a list of configuration items: 'Application & Custom Settings' (1 payload configured), 'Jamf Applications', 'External Applications', and 'Upload' (selected and highlighted with a red box). The 'Upload' section shows a payload named 'com.apple.applicationaccess' with a description: 'Use this section to define generic settings for preference domains.' It includes fields for 'Preference Domain' (set to 'com.apple.applicationaccess') and a 'Property List' containing XML code:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
</dict>
<key>allowiPhoneMirroring</key>
<false/>
<key>allowGenemoji</key>
<true/>
<key>allowPersonalizedHandwritingResults</key>
<true/>
<key>allowVideoConferencingRemoteControl</key>
<true/>
<key>allowWritingTools</key>
<true/>
<key>allowMailSummary</key>
<false/>
<key>forceBypassScreenCaptureAlert</key>
<true/>
<key>allowExternalIntelligenceIntegrations</key>
```



Configuration Profiles - macOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on macOS. The left sidebar navigation includes Computers, Inventory, Content Management (with Policies and Configuration Profiles selected), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups (with Smart Computer Groups and Static Computer Groups), and Classes. The main content area is titled "Apple Intelligence Restrictions". It displays a list of restrictions with checkboxes, many of which are checked. A search bar at the top of the list allows filtering by name.

| Setting | Description | Status |
|---|---|----------|
| Allow Apple Intelligence: Genmoji (macOS 15 or later) | Allow Apple Intelligence: Genmoji (macOS 15 or later) | Enabled |
| Allow Apple Intelligence: Image Playground (macOS 15 or later) | Allow Apple Intelligence: Image Playground (macOS 15 or later) | Enabled |
| Allow Apple Intelligence: Intelligence reports (macOS 15.4 or later) | Allow Apple Intelligence: Intelligence reports (macOS 15.4 or later) | Enabled |
| Allow Apple Intelligence: Mail smart replies (macOS 15.4 or later) | Allow Apple Intelligence: Mail smart replies (macOS 15.4 or later) | Enabled |
| Allow Apple Intelligence: Mail summaries (macOS 15.1 or later) | Allow Apple Intelligence: Mail summaries (macOS 15.1 or later) | Enabled |
| Allow Apple Intelligence: Notes transcription summary (macOS 15.3 or later) | Allow Apple Intelligence: Notes transcription summary (macOS 15.3 or later) | Enabled |
| Allow Apple Intelligence: Notes transcription (macOS 15.4 or later) | Allow Apple Intelligence: Notes transcription (macOS 15.4 or later) | Enabled |
| Allow Apple Intelligence: Safari summary (macOS 15.4 or later) | Allow Apple Intelligence: Safari summary (macOS 15.4 or later) | Enabled |
| Allow Apple Intelligence: Writing Tools (macOS 15 or later) | Allow Apple Intelligence: Writing Tools (macOS 15 or later) | Enabled |
| Allow integration with external intelligence services (macOS 15.2 or later) | Allow integration with external intelligence services (macOS 15.2 or later) | Enabled |
| Allow users to log in to external intelligence services (macOS 15.2 or later) | Allow users to log in to external intelligence services (macOS 15.2 or later) | Enabled |
| Allow Apple Intelligence: external intelligence workspace IDs (macOS 15.3 or later) | Allow Apple Intelligence: external intelligence workspace IDs (macOS 15.3 or later) | Disabled |
| Allow Apple Music | Allow Apple Music | Enabled |
| Allow Spotlight Suggestions | Allow Spotlight Suggestions | Enabled |
| Allow Touch ID to unlock device | Allow Touch ID to unlock device | Enabled |

Touch ID Timeout
A value, in seconds, that allow users to unlock a device with Touch ID before requiring a password. This setting is set to 172800 (48 hours) by default.



Configuration Profiles - macOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on macOS. The left sidebar lists various management categories, and the main pane displays the 'Apple Intelligence Restrictions' configuration.

Left Sidebar (Computers View):

- Inventory
- Search Inventory
- Search Volume Content
- Licensed Software
- Content Management**
- Policies
- Configuration Profiles** (highlighted with a red box)
- Software Updates
- Restricted Software
- Mac Apps
- Patch Management
- eBooks
- Groups**
- Smart Computer Groups
- Static Computer Groups
- Classes

Main Pane: Apple Intelligence Restrictions

Options Tab:

- Search... (Not configured)
- Passcode (Not configured)
- Printers (Not configured)
- Privacy Preferences (Policy Control, Not configured)
- Proxies (Not configured)
- Restrictions** (1 payload configured) (highlighted with a red box)
- SCEP (Not configured)
- Security and Privacy (Not configured)
- Single Sign-On Extensions (Not configured)

Scope Tab:

- Allow Apple Intelligence: Genmoji (macOS 15 or later)
- Allow Apple Intelligence: Image Playground (macOS 15 or later)
- Allow Apple Intelligence: Intelligence reports (macOS 15.4 or later)
- Allow Apple Intelligence: Mail smart replies (macOS 15.4 or later)
- Allow Apple Intelligence: Mail summaries (macOS 15.1 or later)
- Allow Apple Intelligence: Notes transcription summary (macOS 15.3 or later)
- Allow Apple Intelligence: Notes transcription (macOS 15.4 or later)
- Allow Apple Intelligence: Safari summary (macOS 15.4 or later)
- Allow Apple Intelligence: Writing Tools (macOS 15 or later)
- Allow integration with external intelligence services (macOS 15.2 or later)
 - Allow users to log in to external intelligence services (macOS 15.2 or later)
- Allow Apple Intelligence: external intelligence workspace IDs (macOS 15.3 or later)
- Allow Apple Music
- Allow Spotlight Suggestions
- Allow Touch ID to unlock device

Touch ID Timeout: A value, in seconds, that allow users to unlock a device with Touch ID before requiring a password. This setting is set to 172800 (48 hours) by default.



Configuration Profiles - macOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles on macOS. The left sidebar is titled 'Computers' and includes options like Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management, Policies, Configuration Profiles (which is selected), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups. The main content area is titled 'Computers : Configuration Profiles' and 'Apple Intelligence Restrictions'. It features tabs for 'Options' and 'Scope'. Under 'Scope', there are sections for 'Targets' (Target Computers: 'Computers to assign the profile to' set to 'Specific Computers') and 'Limitations' (Target Users: 'Users to distribute the profile to' set to 'Specific Users'). A large button labeled '+ Add' is visible. Below these sections is a table titled 'Selected Deployment Targets' with columns 'TARGET' and 'TYPE', showing 'No Targets'.



Configuration Profiles - macOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles on macOS. The left sidebar is titled 'Computers' and includes options like Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management, Policies, Configuration Profiles (which is selected and highlighted in blue), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups.

The main content area is titled 'Computers : Configuration Profiles' and 'Apple Intelligence Restrictions'. It features two tabs: 'Options' and 'Scope'. The 'Scope' tab is active, showing three tabs: 'Targets', 'Limitations', and 'Exclusions'. Under 'Targets', there are sections for 'Target Computers' (set to 'Specific Computers') and 'Target Users' (set to 'Specific Users').

The 'Selected Deployment Targets' section displays a table with columns 'TARGET' and 'TYPE'. A message 'No Targets' is shown. In the bottom right corner of this section, there is a button labeled '+ Add' with a red oval highlighting it.



Configuration Profiles - macOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles. The left sidebar is titled "Pro" and includes sections for Computers, Inventory, Search Inventory, Search Volume, Content, Licensed Software, Content Management, Policies, Configuration Profiles (which is selected and highlighted in blue), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups. The main content area is titled "Computers : Configuration Profiles" and "Apple Intelligence Restrictions". It features tabs for "Options" and "Scope". Under "Scope", there are three tabs: "Targets", "Limitations" (which is selected and highlighted in blue), and "Exclusions". A modal window titled "Add Deployment Targets" is open, showing tabs for "Computers" (selected) and "Computer Groups", "Users", "User Groups", "Buildings", and "Departments". Below these tabs is a "Filter results" input field and a message "1 - 2 of 2". Two items are listed under "GROUP NAME": "macOS 15.4 or Later" and "macOS 15.2 or Later", each with an "Add" button to the right.



Configuration Profiles - macOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles. The left sidebar is titled "Computers" and includes options like Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management, Policies, Configuration Profiles (which is selected and highlighted in grey), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups, and Static Computer Groups. The main content area is titled "Computers : Configuration Profiles" and "Apple Intelligence Restrictions". It has tabs for Options and Scope, with Scope being active. Under Scope, there are three tabs: Targets, Limitations, and Exclusions. A modal window titled "Add Deployment Targets" is open, showing tabs for Computers, Computer Groups, Users, User Groups, Buildings, and Departments. Below these tabs is a "Filter results" input field and a message "1 - 2 of 2". Two items are listed under "GROUP NAME": "macOS 15.4 or Later" and "macOS 15.2 or Later". To the right of each item is an "Add" button. The "macOS 15.2 or Later" entry has a red oval drawn around its "Add" button.



Configuration Profiles - macOS

Restrict **Allow**



Configuration Profiles - macOS

Restrict Allow



Configuration Profiles - macOS

Restrict

Allow



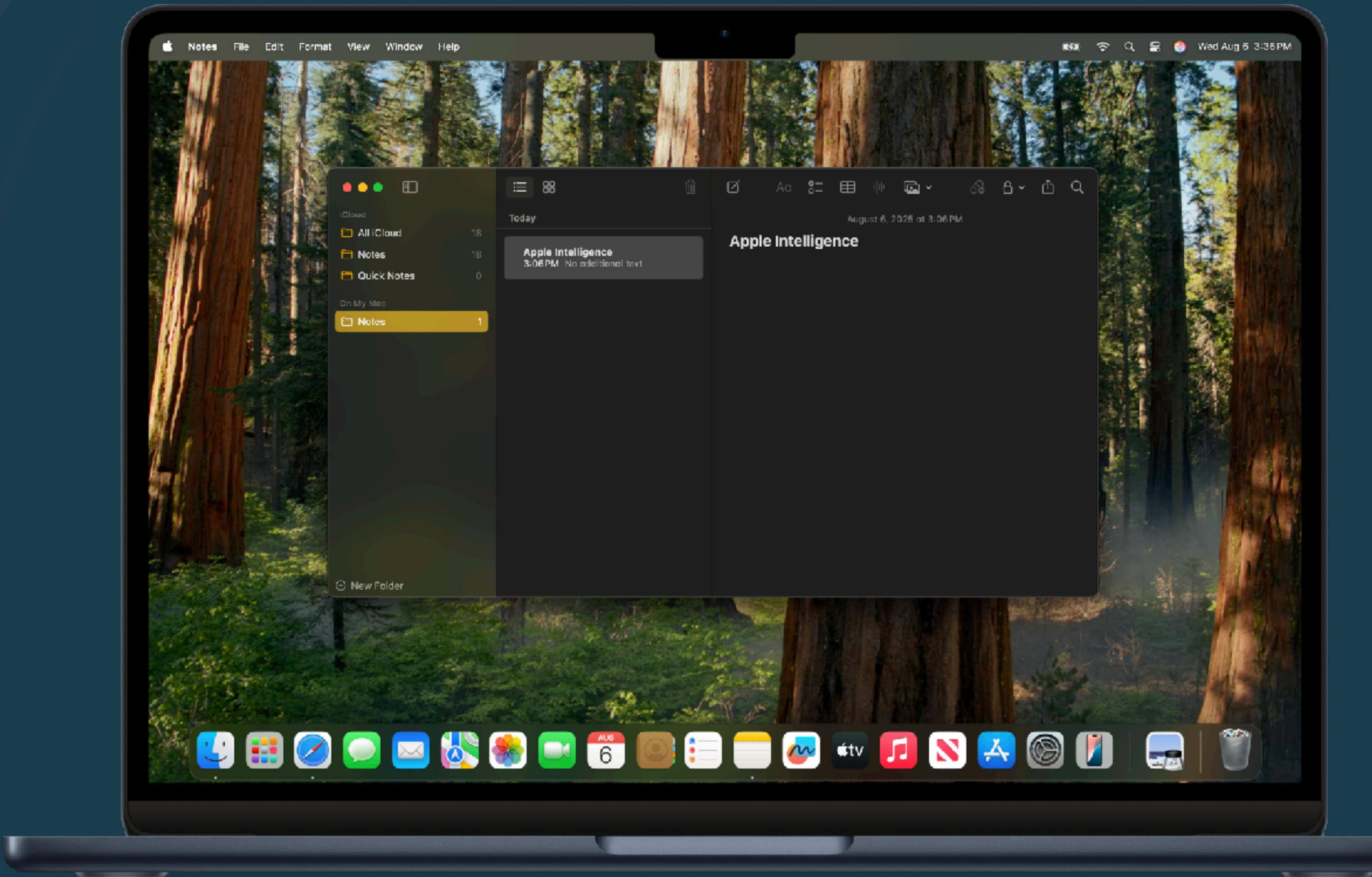
Configuration Profiles - macOS

Restrict **Allow**



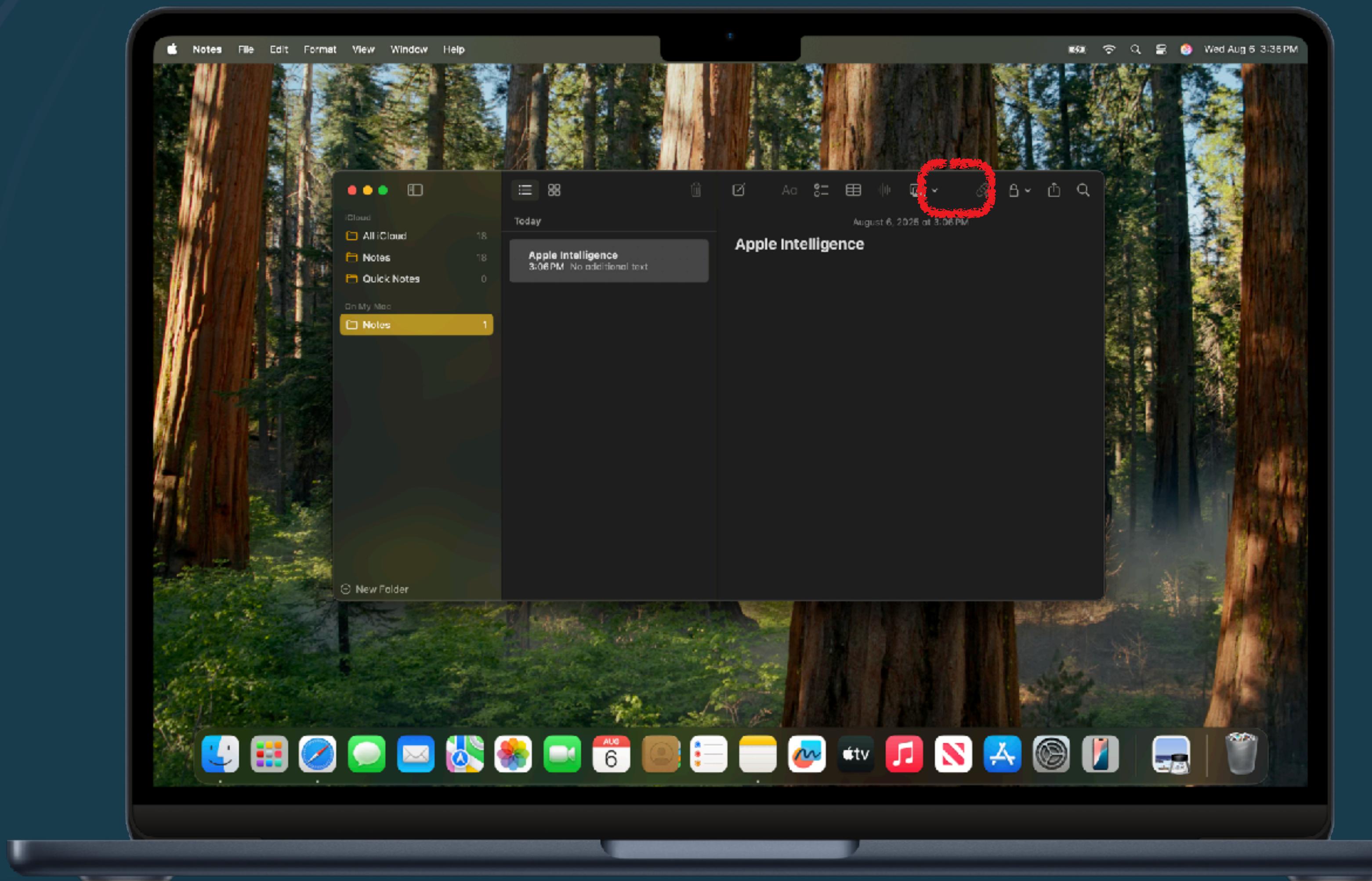
Configuration Profiles - macOS

Restrict Allow



Configuration Profiles - macOS

Restrict Allow



Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for managing mobile device configuration profiles. The left sidebar navigation includes 'Devices', 'Inventory' (with 'Search Inventory' and 'Search Volume Content' options), 'Content Management' (with 'Configuration Profiles' selected), 'Software Updates', 'Provisioning Profiles', 'Personal Device Profiles', 'Mobile Device Apps', 'eBooks', 'Groups' (with 'Smart Device Groups' and 'Static Device Groups' options), and 'Devices' again at the top.

The main content area is titled 'Apple Intelligence Restrictions' under 'Mobile Devices : Configuration Profiles'. It has tabs for 'Options' (selected) and 'Scope'. The 'General' section contains fields for 'Name' (set to 'Apple Intelligence Restrictions'), 'Description' (a brief explanation of the profile's purpose), 'Site' (set to 'None'), 'Category' (set to 'Security'), and 'Level' (set to 'Device Level'). On the right side of the General section are 'Cancel' and 'Save' buttons.

A sidebar on the right lists various configuration profile settings: 'Notifications' (Not configured), 'Passcode' (Not configured), 'Restrictions' (Not configured), 'Functionality' (with 'Apps' and 'Media Content' sections), 'SCEP' (Not configured), 'Skip Setup Items' (Not configured), and 'Single Sign-On Extensions' (Not configured).

Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for managing mobile device configuration profiles. The left sidebar is titled "Devices" and includes sections for Inventory, Content Management, Configuration Profiles (which is selected), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions" and is under the "General" tab. It includes fields for Name (set to "Apple Intelligence Restrictions"), Description (empty), Site (set to "None"), Category (set to "Security"), and Level (set to "Device Level"). On the left, a sidebar lists "Mobile Devices : Configuration Profiles" with options: Notifications (Not configured), Passcode (Not configured), Restrictions (Not configured, highlighted with a red oval), Functionality, Apps, Media Content, SCEP (Not configured), Skip Setup Items (Not configured), Single Sign-On Extensions (Not configured), and a "More" button. The top right of the screen shows "Full Jamf Pro" with a dropdown arrow, a gear icon, a bell icon, and a user profile icon.

Configuration Profiles - iOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on mobile devices. The left sidebar is titled "Devices" and includes options like Inventory, Content Management, Configuration Profiles (which is selected), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions". It displays a list of restrictions with their status and configuration options:

- Generate personalized handwriting (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.
- Apple Intelligence: Genemoji (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.
- Apple Intelligence: Image Playground (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.
- Apple Intelligence: Image Wand (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.
- Apple Intelligence: Intelligence reports (iOS 18.4 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.
- Apple Intelligence: Mail smart replies (iOS 18.4 or later, Supervised): Status: Off (switch is off). Options: Restrict, Allow.

At the bottom right of the configuration screen are "Cancel" and "Save" buttons.



Configuration Profiles - iOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on mobile devices. The left sidebar is titled "Devices" and includes options like Inventory, Content Management, Configuration Profiles (which is selected), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions". It lists several restrictions with their status and configuration options:

- Generate personalized handwriting (iOS 18 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow.
- Apple Intelligence: Genemoji (iOS 18 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow. This item is circled in red.
- Apple Intelligence: Image Playground (iOS 18 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow.
- Apple Intelligence: Image Wand (iOS 18 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow.
- Apple Intelligence: Intelligence reports (iOS 18.4 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow.
- Apple Intelligence: Mail smart replies (iOS 18.4 or later, Supervised): Status: Enabled (switch is on). Options: Restrict (disabled), Allow.

At the bottom right of the configuration screen are "Cancel" and "Save" buttons.



Configuration Profiles - iOS

The screenshot shows the Jamf Pro interface for managing Configuration Profiles on mobile devices. The left sidebar navigation includes Devices, Inventory, Search Inventory, Search Volume Content, Content Management, Configuration Profiles (which is selected and highlighted in blue), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions". It displays several restrictions with their status and configuration options:

- Generate personalized handwriting (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button).
- Apple Intelligence: Genemoji (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button). This item is circled in red.
- Apple Intelligence: Image Playground (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button).
- Apple Intelligence: Image Wand (iOS 18 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button).
- Apple Intelligence: Intelligence reports (iOS 18.4 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button).
- Apple Intelligence: Mail smart replies (iOS 18.4 or later, Supervised): Status: Off (switch is off). Options: Restrict (button), Allow (button).

At the bottom right of the configuration pane are "Cancel" and "Save" buttons.



Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for creating an Apple Intelligence Configuration Profile. The left sidebar navigation includes 'Devices', 'Inventory', 'Search Inventory', 'Search Volume Content', 'Content Management' (with 'Configuration Profiles' selected), 'Software Updates', 'Provisioning Profiles', 'Personal Device Profiles', 'Mobile Device Apps', 'eBooks', 'Groups', 'Smart Device Groups', and 'Static Device Groups'. The main content area is titled 'Apple Intelligence Restrictions' under 'Mobile Devices : Configuration Profiles'. It has tabs for 'Options' and 'Scope' (which is selected). Below these are three tabs: 'Targets', 'Limitations', and 'Exclusions'. Under 'Targets', it says 'Target Mobile Devices: Mobile devices to assign the profile to. Does not apply to personally owned devices' and 'Target Users: Users to distribute the profile to'. Both dropdown menus are set to 'Specific Mobile Devices' and 'Specific Users'. A large button labeled '+ Add' is available to add deployment targets. At the bottom right are 'Cancel' and 'Save' buttons.



Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for creating a Configuration Profile. The left sidebar is titled "Mobile Devices : Configuration Profiles" and lists several categories: Devices, Inventory, Search Inventory, Search Volume Content, Content Management, Configuration Profiles (which is selected and highlighted in grey), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions". It has tabs for "Options" and "Scope", with "Scope" being active. Below the tabs is a grid with three columns: "Targets", "Limitations", and "Exclusions". Under "Targets", there are sections for "Target Mobile Devices" (described as mobile devices to assign the profile to, not applying to personally owned devices) and "Target Users" (described as users to distribute the profile to). Both sections have dropdown menus set to "Specific Mobile Devices" and "Specific Users". A large button labeled "+ Add" is located at the bottom right of the "Selected Deployment Targets" section, which currently displays "No Targets". At the bottom right of the main content area are "Cancel" and "Save" buttons.



Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles. The left sidebar is titled "Mobile Devices : Configuration Profiles" and lists various management options: Devices, Inventory, Search Inventory, Search Volume Content, Content Management, Configuration Profiles (which is selected and highlighted in grey), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Apple Intelligence Restrictions" and is under the "Scope" tab. It includes tabs for Targets, Limitations, and Exclusions. A modal window titled "Add Deployment Targets" is open, showing categories: Mobile Devices, Mobile Device Gro..., Users, User Groups, Buildings, and Departments. Below these categories is a search bar labeled "Filter results" with the text "1 - 5 of 5". Under the "GROUP NAME" heading, there are five listed groups: All Managed iPads, All Managed iPhones, All Managed iPod touches, All Managed Apple TVs, and iOS 18.2 or Later. Each group has an "Add" button to its right. At the bottom of the modal are navigation arrows, a "Show: 1,000" dropdown, and "Cancel" and "Save" buttons.

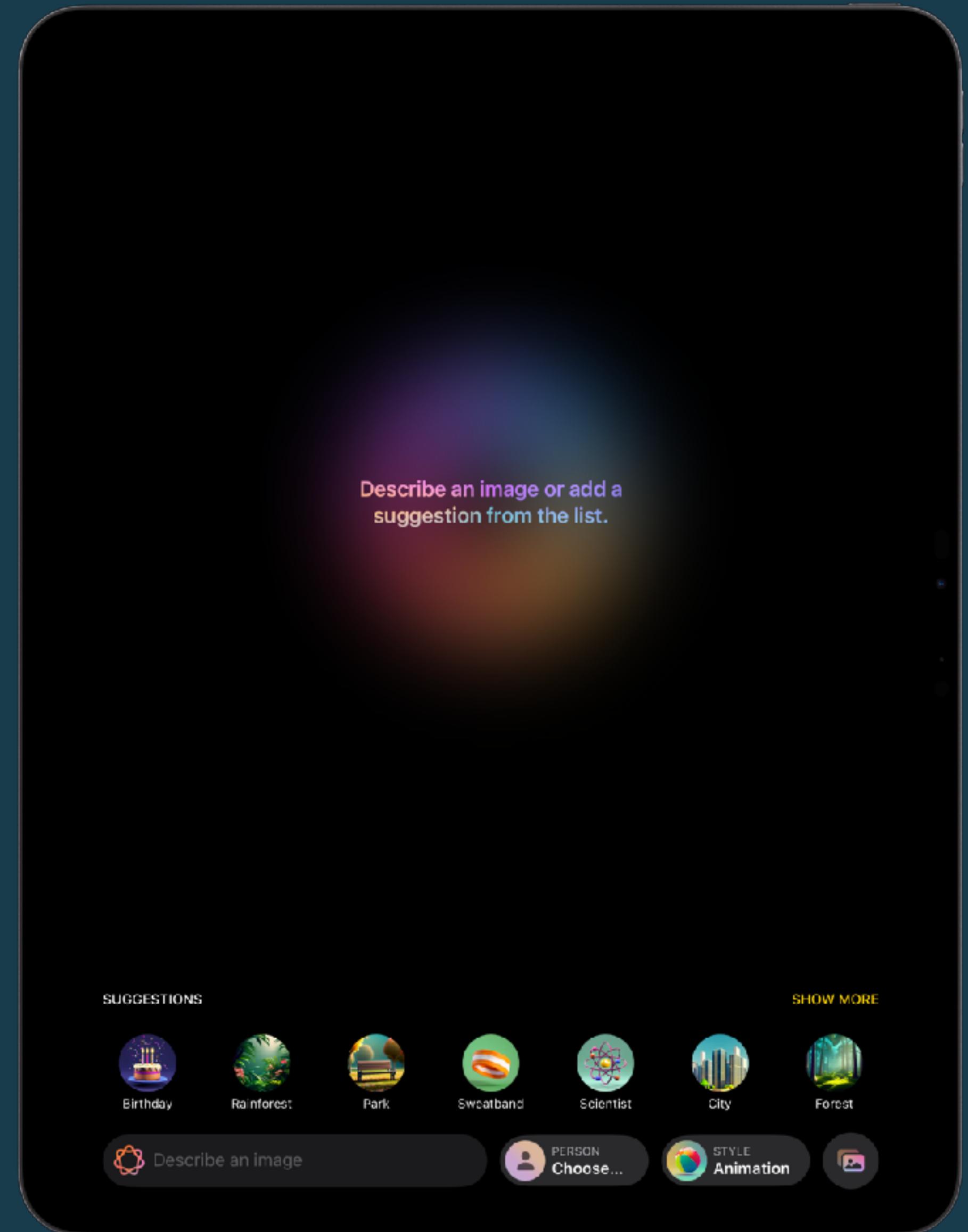


Configuration Profiles - iOS

The screenshot shows the Jamf Pro web interface for managing Configuration Profiles. The left sidebar is titled "Devices" and includes options like Inventory, Search Inventory, Search Volume Content, Content Management, Configuration Profiles (which is selected), Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, and Static Device Groups. The main content area is titled "Mobile Devices : Configuration Profiles" and "Apple Intelligence Restrictions". It has tabs for Options, Scope (Targets, Limitations, Exclusions), and Targets. Under Targets, there's a section for "Add Deployment Targets" with tabs for Mobile Devices, Mobile Device Gro..., Users, User Groups, Buildings, and Departments. A search bar shows "Filter results 1 - 5 of 5" with items: All Managed iPads, All Managed iPhones, All Managed iPod touches, All Managed Apple TVs, and iOS 18.2 or Later. The "iOS 18.2 or Later" item has a red circle around its "Add" button. At the bottom right are "Cancel" and "Save" buttons.

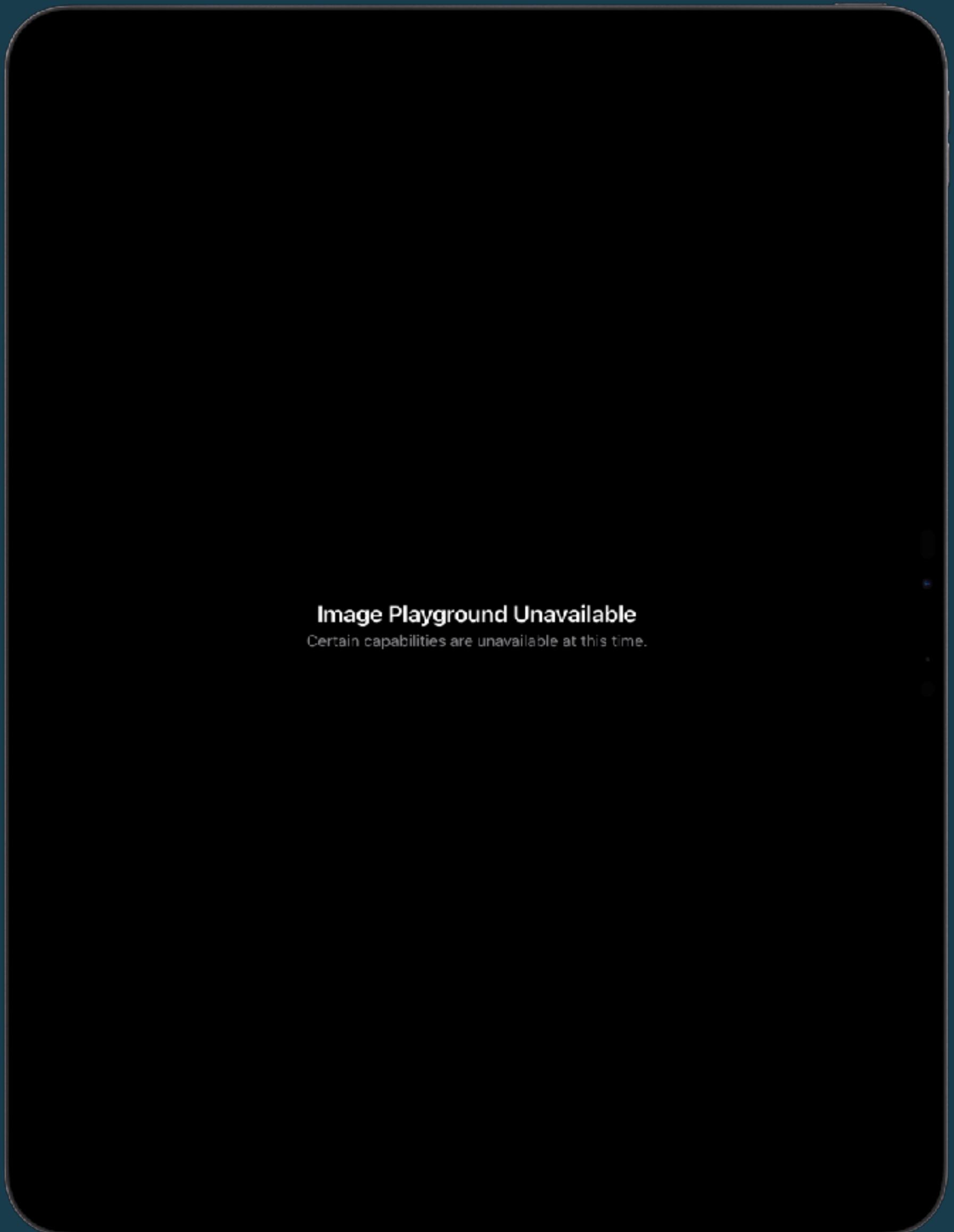
Configuration Profiles - iOS

Restrict **Allow**



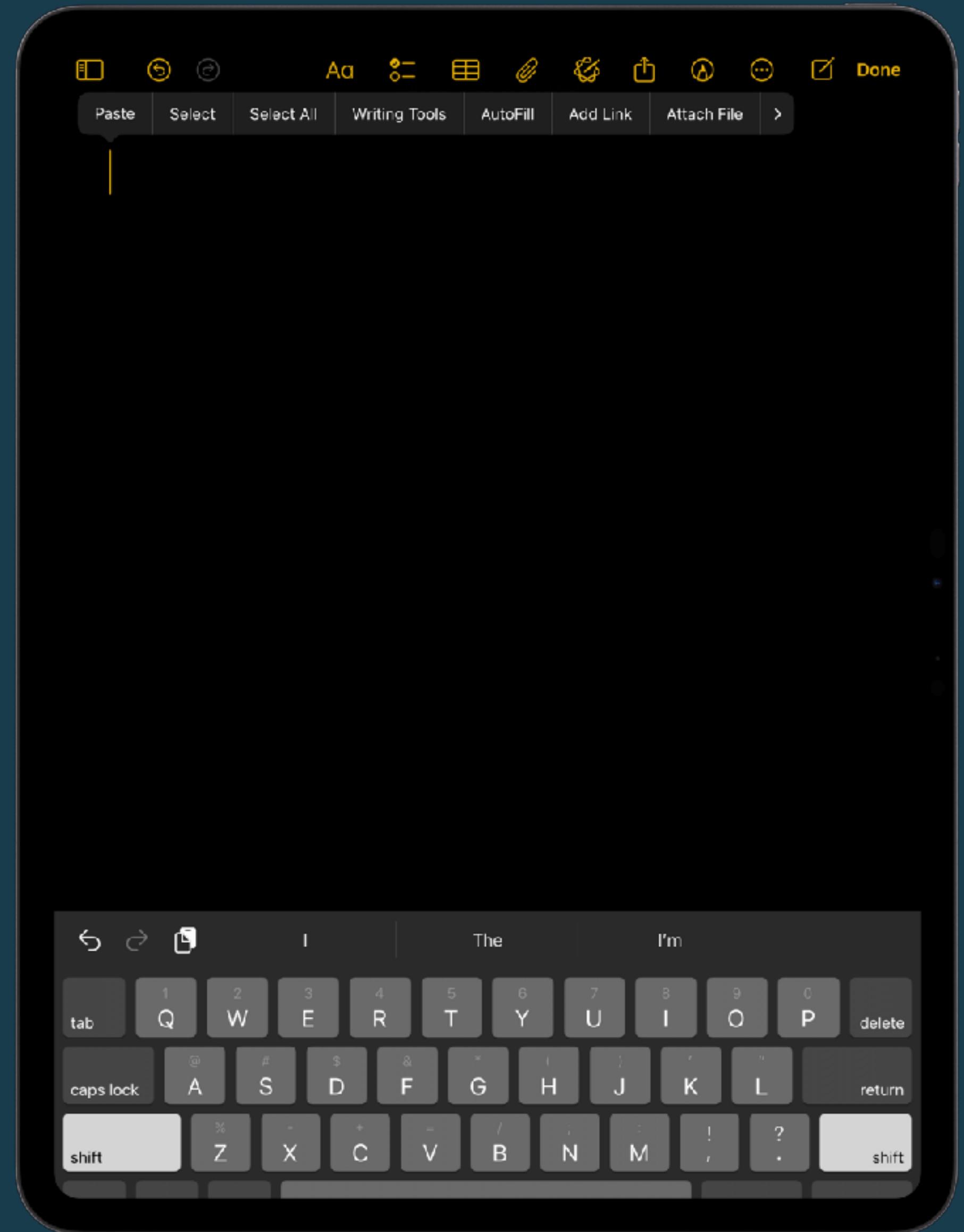
Configuration Profiles - iOS

Restrict Allow



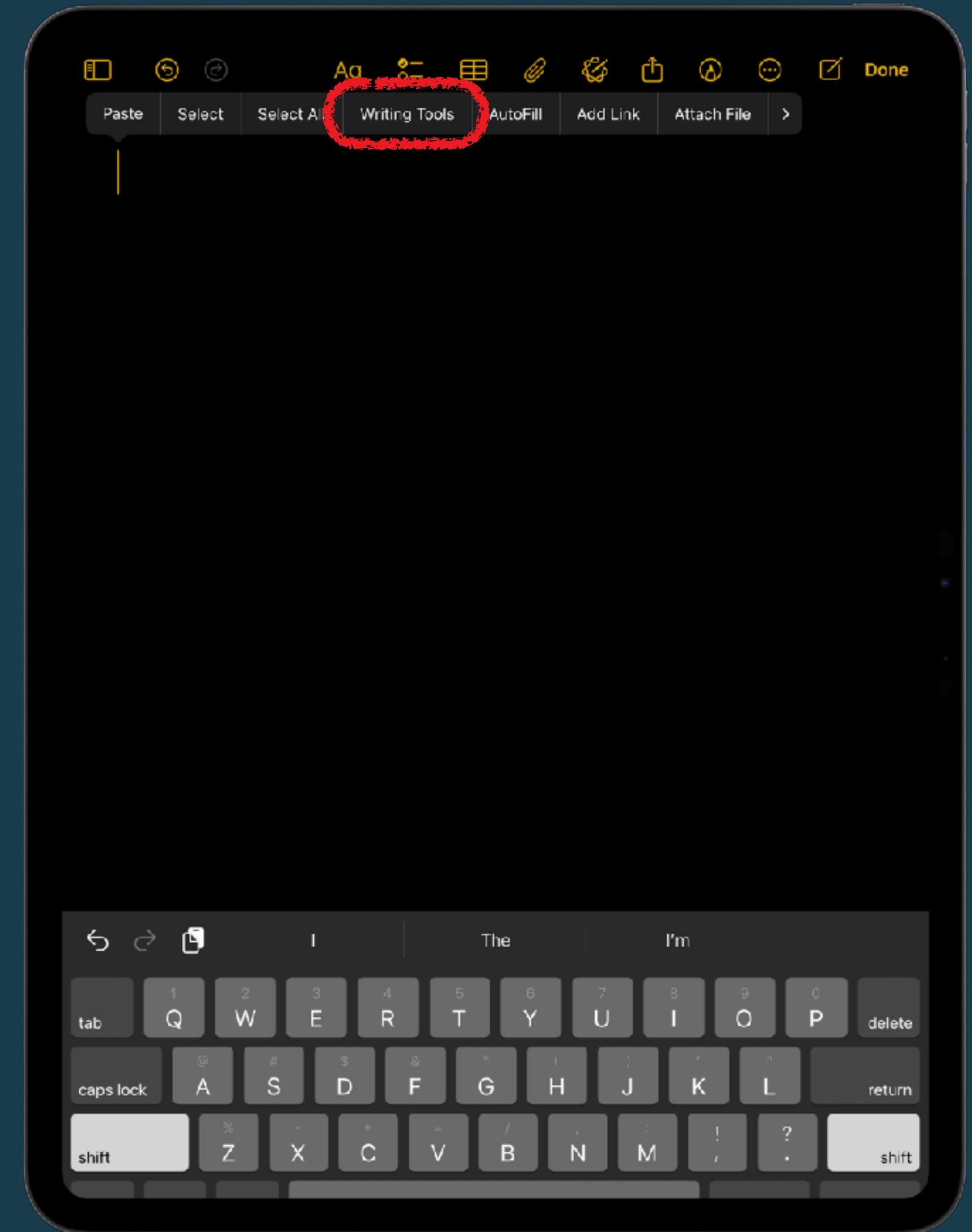
Configuration Profiles - iOS

Restrict **Allow**



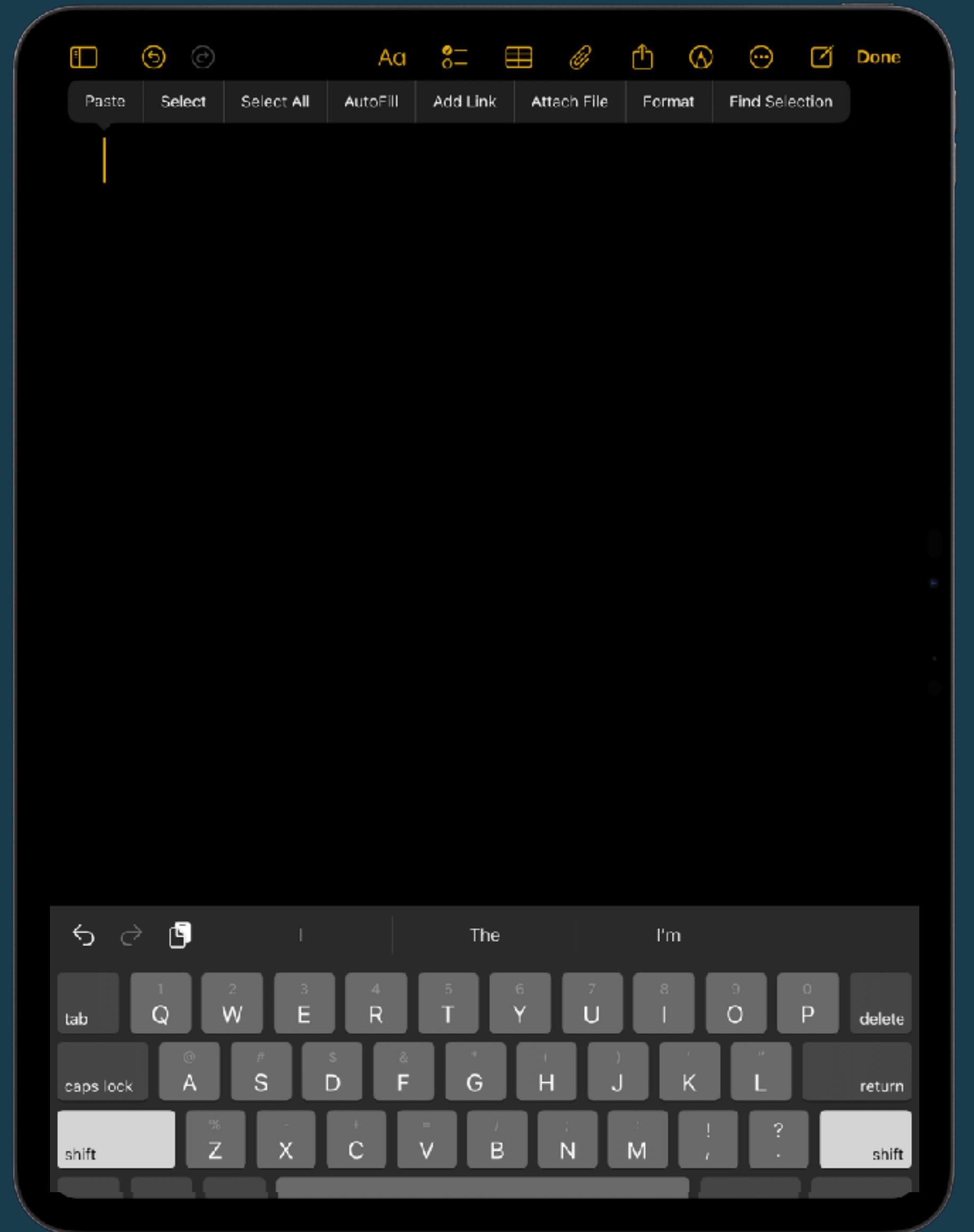
Configuration Profiles - iOS

Restrict **Allow**



Configuration Profiles - iOS

Restrict Allow



Computer Prestage - Setup Assistant Options

The screenshot shows the Jamf Pro interface for managing computer enrollment. The left sidebar lists various management categories like Computers, Policies, Configuration Profiles, etc. The 'PreStage Enrollments' option is highlighted. The main panel title is 'New Computer PreStage Enrollment'. Below it, there are two tabs: 'Options' (selected) and 'Scope'. The 'Options' tab contains several sections:

- Setup Assistant**: A checkbox for 'Automatically advance through Setup Assistant (macOS 11 or later only)' which also skips screens.
- Setup Assistant Options**: A list of items that are not displayed in the Setup Assistant during enrollment. These include 'All', 'Get Started', 'Location Services', 'Transfer Information', 'Apple ID', 'Terms and Conditions', 'Siri', 'App Analytics', 'Touch ID / Face ID', 'Enable Lockdown Mode', and 'Apple Pay'. There is also a 'Registration' option at the bottom.
- General**: A section containing icons for Account Settings, Configuration Profiles (0 profiles), User and Location, Purchasing, Attachments (0 attachments), Certificates, and Enrollment Packages (0 packages).

At the bottom right of the main panel are 'Cancel' and 'Save' buttons.

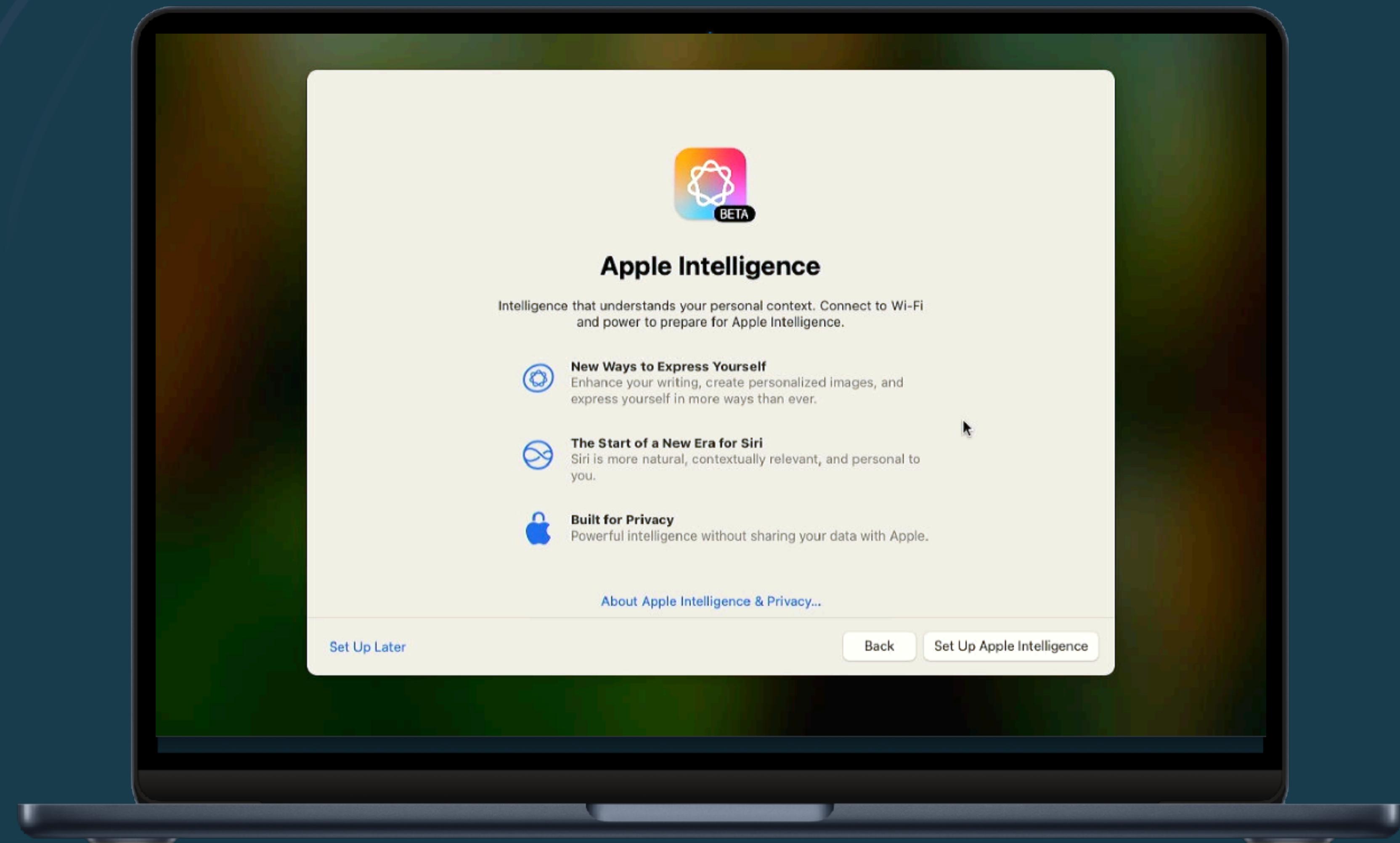


Computer Prestage - Setup Assistant Options

The screenshot shows the Jamf Pro interface for creating a new computer enrollment. The left sidebar has a 'Computers' section with various management options like Policies, Configuration Profiles, Software Updates, and Mac Apps. A 'PreStage Enrollments' option is highlighted. The main window title is 'New Computer PreStage Enrollment'. It has tabs for 'Options' and 'Scope'. Under 'Options', the 'General' tab is selected, showing sections for 'Setup Assistant' and 'Setup Assistant Options'. The 'Setup Assistant' section contains a checkbox for 'Automatically advance through Setup Assistant (macOS 11 or later only)' which is unchecked. The 'Setup Assistant Options' section lists several items with checkboxes, including 'Get Started', 'Location Services', 'Transfer Information', 'Apple ID', 'Terms and Conditions', 'Siri', 'App Analytics' (which is circled in red), 'Touch ID / Face ID', 'Enable Lockdown Mode', and 'Apple Pay'. At the bottom right are 'Cancel' and 'Save' buttons.



Computer Prestage - Setup Assistant Options



Mobile Device Prestage - Setup Assistant Options

The screenshot shows the Jamf Pro interface for creating a new mobile device enrollment. The left sidebar is titled "Devices" and includes options like Configuration Profiles, Software Updates, Provisioning Profiles, Personal Device Profiles, Mobile Device Apps, eBooks, Groups, Smart Device Groups, Static Device Groups, Classes, Enrollment, Enrollment Profiles, Enrollment Invitations, and PreStage Enrollments. The "PreStage Enrollments" option is highlighted with a red box. The main content area is titled "Mobile Devices : PreStage Enrollments" and "New Mobile Device PreStage Enrollment". It has tabs for "Options" (selected) and "Scope". Under "Options", there are sections for General (Not Configured), Mobile device names (Not Configured), User and Location, Purchasing, Attachments (0 attachments), and Certificates. To the right of these sections is a list of configuration options with checkboxes. The "Intelligence" checkbox is checked. Below it, a note says "tvOS only". The configuration options include: Software Update Completed, Emergency SOS, Safety and Handling, Terms of Address, Voice Selection, Intelligence (checked), Action Button, Camera Button, Set Up Your Apple TV, See the World Screensaver, One Home Screen for Every Apple TV, Sign In to Your TV Provider, and Where is this Apple TV? At the bottom right are "Cancel" and "Save" buttons.

Mobile Devices : PreStage Enrollments

← New Mobile Device PreStage Enrollment

Options Scope

General Not Configured

Mobile device names Not Configured

User and Location

Purchasing

Attachments 0 Attachments

Certificates

Software Update Completed

Emergency SOS

Safety and Handling

Terms of Address

Voice Selection

Intelligence

Action Button

Camera Button

tvOS only

Set Up Your Apple TV

See the World Screensaver

One Home Screen for Every Apple TV

Sign In to Your TV Provider

Where is this Apple TV?

Cancel Save

Mobile Device Prestage - Setup Assistant Options

The screenshot shows the Jamf Pro interface for creating a new mobile device enrollment. The left sidebar has a 'Devices' section with various options like Configuration Profiles, Software Updates, and Personal Device Profiles. The 'PreStage Enrollments' option is highlighted with a red box. The main window title is 'New Mobile Device PreStage Enrollment'. It has tabs for 'Options' and 'Scope'. Under 'Options', there's a 'General' section with a sub-section for 'Mobile device names' (Not Configured). Below that are sections for 'User and Location', 'Purchasing', 'Attachments' (0 attachments), and 'Certificates'. To the right is a list of setup assistant options with checkboxes. The 'Intelligence' checkbox is checked and circled in red. Other options include Software Update Completed, Emergency SOS, Safety and Handling, Terms of Address, Voice Selection, Action Button, Camera Button, and tvOS only options like Set Up Your Apple TV, See the World Screensaver, One Home Screen for Every Apple TV, Sign In to Your TV Provider, and Where is this Apple TV? At the bottom right are 'Cancel' and 'Save' buttons.

Mobile Devices : PreStage Enrollments

← New Mobile Device PreStage Enrollment

Options Scope

General

Mobile device names
Not Configured

User and Location

Purchasing

Attachments
0 Attachments

Certificates

Software Update Completed

Emergency SOS

Safety and Handling

Terms of Address

Voice Selection

Intelligence

Action Button

Camera Button

tvOS only

Set Up Your Apple TV

See the World Screensaver

One Home Screen for Every Apple TV

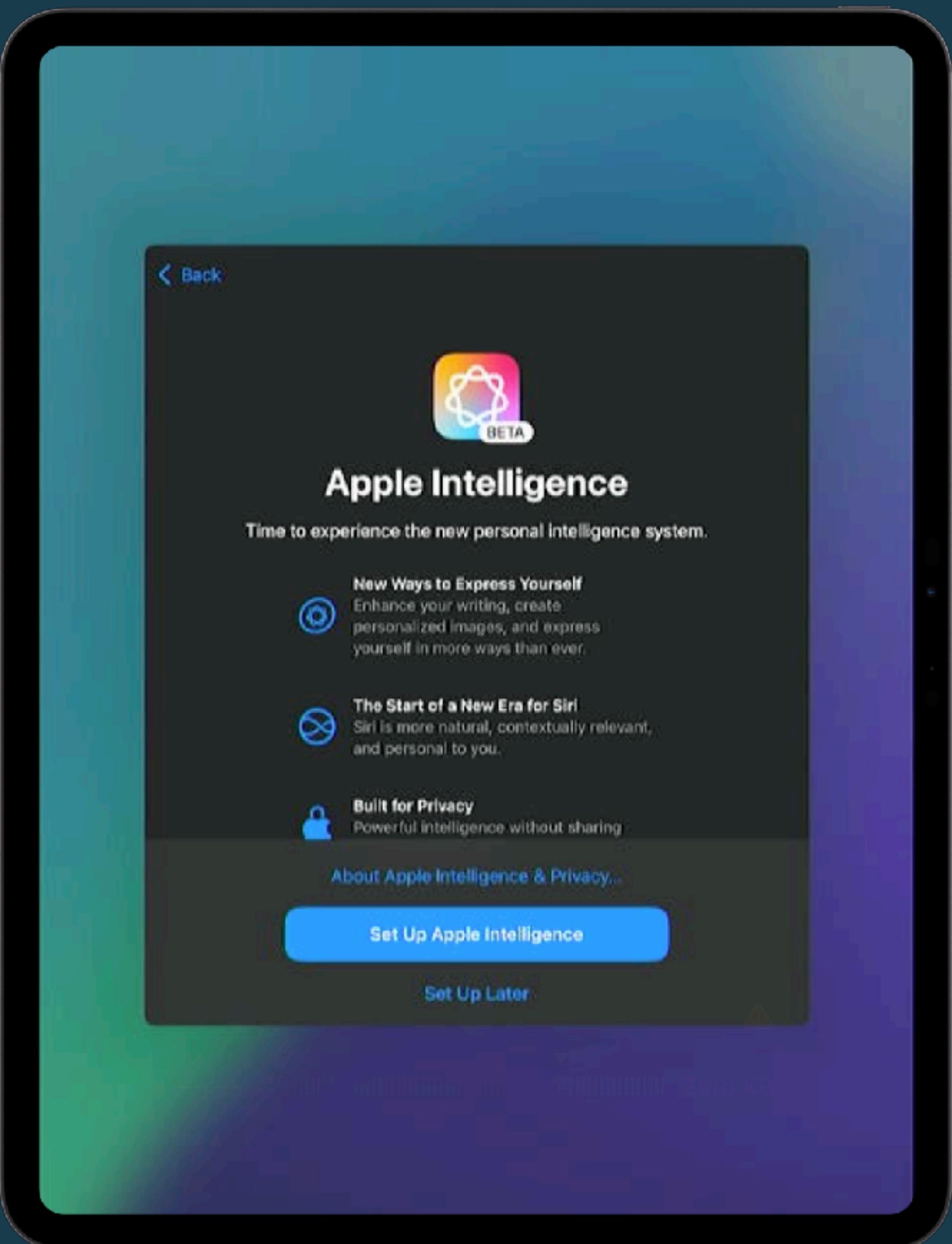
Sign In to Your TV Provider

Where is this Apple TV?

Cancel Save



Mobile Device Prestage - Setup Assistant Options



SkipSetupItems

An array strings that describe the setup items to skip

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>SkipSetupItems</key>
<array>
    <string>Intelligence</string>
</array>
</dict>
</plist>
```



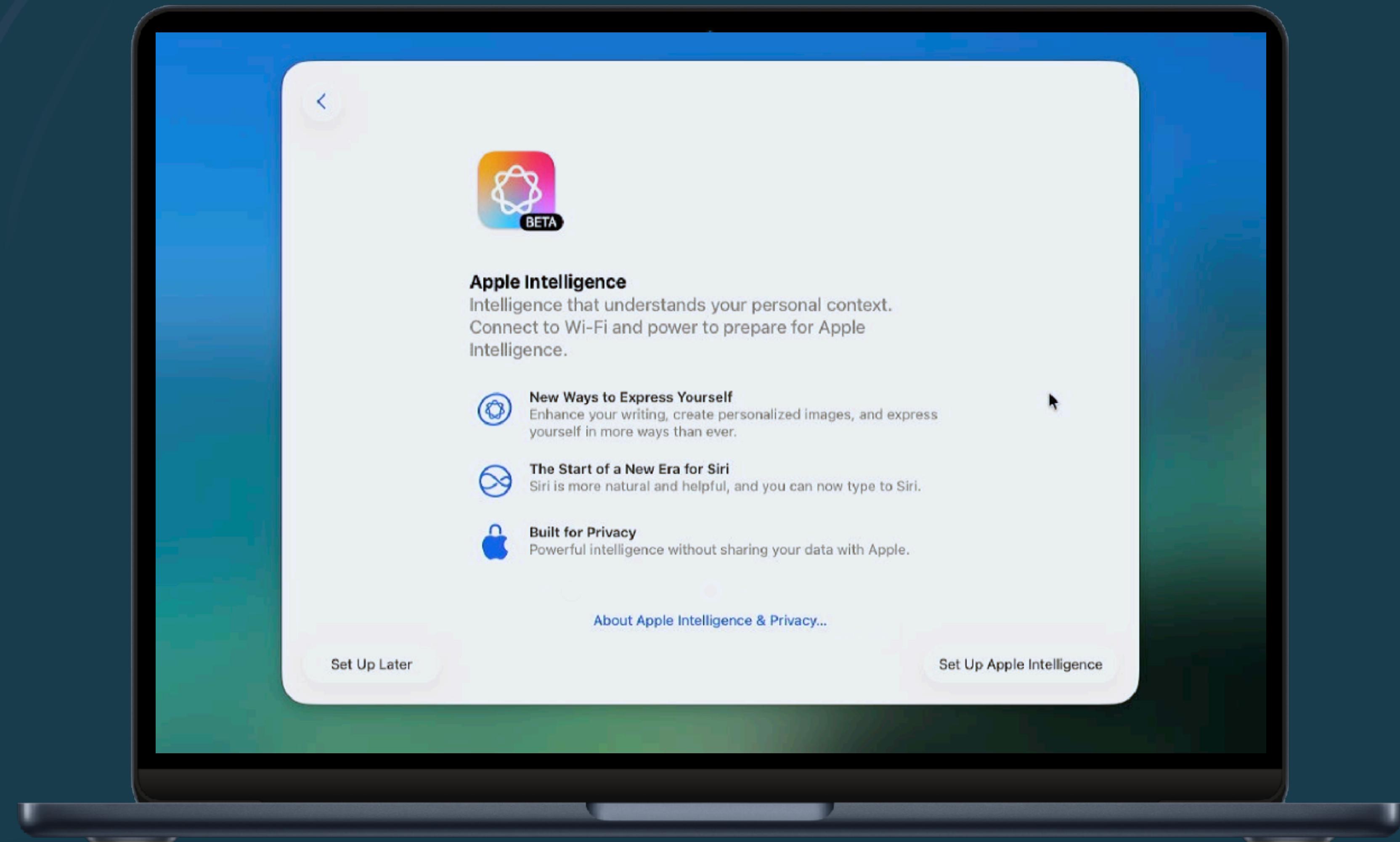
Computer Configuration Profile - SkipSetupItems

The screenshot shows the Jamf Pro interface for managing computer configuration profiles. The left sidebar lists various management categories like Computers, Inventory, and Configuration Profiles. The 'Configuration Profiles' section is currently selected. A specific profile, 'Skip Intelligence Setup', is displayed in the main content area. The profile has an 'Options' tab selected, showing a search bar and a list of items including Accessibility, ACME Certificate, AD Certificate, AirPlay, App-To-Per-App VPN Mapping, Application & Custom Settings, Jamf Applications, and External Applications. The 'Application & Custom Settings' item is expanded, showing its configuration details. The 'Property List' section contains the XML code for the configuration profile:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>SkipSetupItems</key>
<array>
<string>Intelligence</string>
</array>
</dict>
</plist>
```



Computer Configuration Profile - SkipSetupItems



Mobile Device Configuration Profile - SkipSetupItems

The screenshot shows the Jamf Pro interface for managing mobile device configuration profiles. The left sidebar lists various management categories like Devices, Inventory, Content Management, Configuration Profiles, and Enrollment. The main panel is titled "Skip Intelligence Setup" under the "Mobile Devices : Configuration Profiles" section. It displays a list of items with toggle switches to enable or disable them. The items are:

- Skip Intelligence (Enabled)
- Skip Location Services (Disabled)
- Skip Lockdown Mode (Disabled)
- Skip messaging activation using phone number (Disabled)
- Skip Passcode (Disabled)
- Skip payment (Disabled)
- Skip Privacy (Disabled)
- Skip Restore (Disabled)
- Skip Restore Completed (Disabled)

The "Skip Setup Items" item is highlighted with a blue selection bar at the bottom of its row.



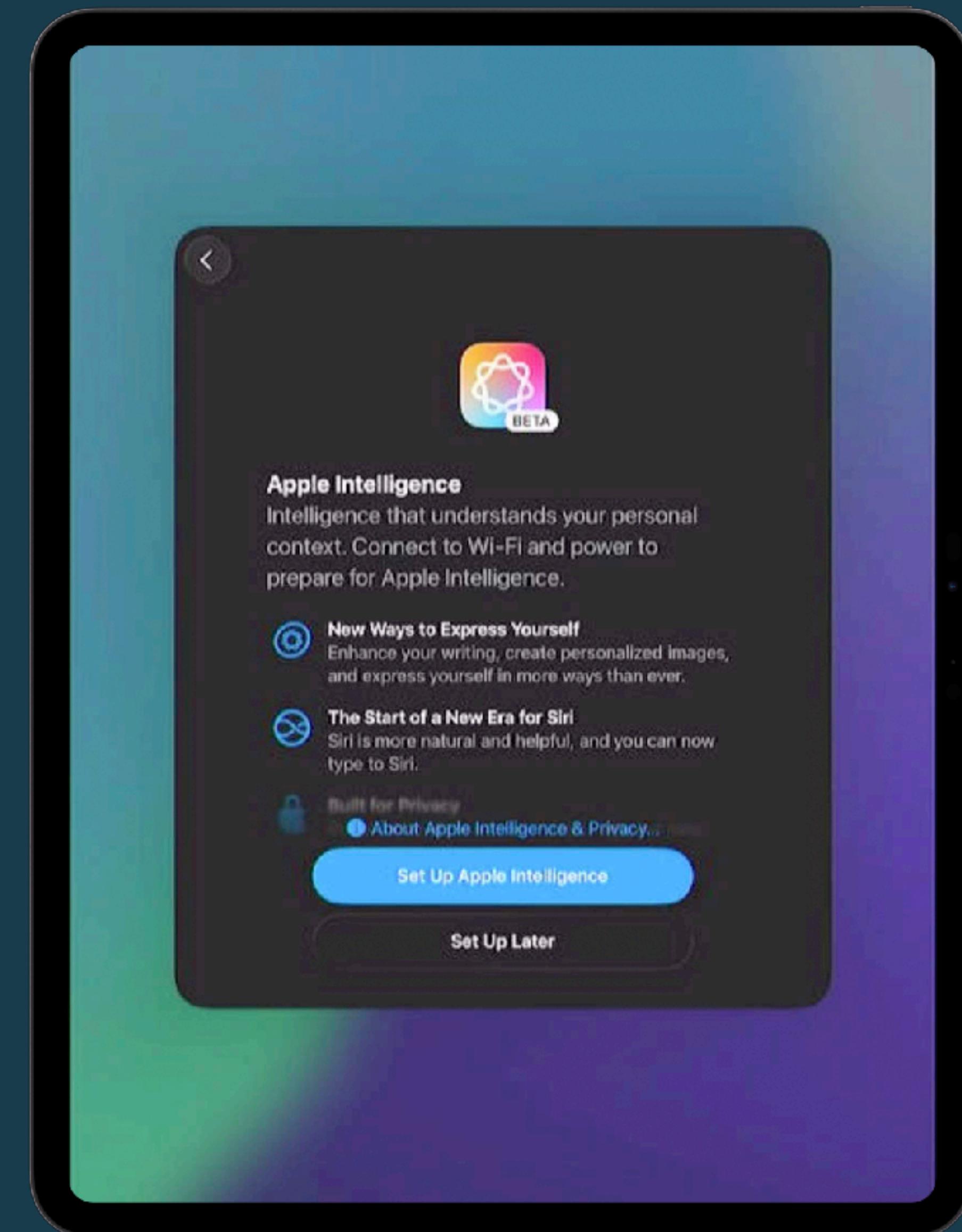
Mobile Device Configuration Profile - SkipSetupItems

The screenshot shows the Jamf Pro interface under the 'Devices' section. On the left sidebar, 'Configuration Profiles' is selected. In the main content area, the 'Skip Intelligence Setup' configuration profile is displayed. A red circle highlights the 'Skip Intelligence' setting, which is described as 'Intelligence pane (iOS 18 or later)' and has its toggle switch set to 'On'. Below it, other settings listed with their descriptions and toggle switches are: 'Skip Location Services' (Location Services screen), 'Skip Lockdown Mode' (Lockdown Mode pane (iOS 17.1 or later)), 'Skip messaging activation using phone number' (iMessage activation screen), 'Skip Passcode' (Passcode screen), 'Skip payment' (Apple Pay setup screen), 'Skip Privacy' (Privacy screen), 'Skip Restore' (Restore from Backup screen), and 'Skip Restore Completed' (Restore Completed screen).

| Setting | Description | Status |
|--|--|--------|
| Skip Intelligence | Intelligence pane (iOS 18 or later) | On |
| Skip Location Services | Location Services screen | Off |
| Skip Lockdown Mode | Lockdown Mode pane (iOS 17.1 or later) | Off |
| Skip messaging activation using phone number | iMessage activation screen | Off |
| Skip Passcode | Passcode screen | Off |
| Skip payment | Apple Pay setup screen | Off |
| Skip Privacy | Privacy screen | Off |
| Skip Restore | Restore from Backup screen | Off |
| Skip Restore Completed | Restore Completed screen | Off |



Mobile Device Configuration Profile - SkipSetupItems



Generative Assistant Settings Reporting

The screenshot shows the Jamf Pro interface for managing extension attributes. The left sidebar includes options like Dashboard, Computers, Devices, Users, Blueprints, Compliance, and Settings (which is selected). The main panel is titled "Generative Assistant Status" under "Computer management > Extension attributes". It shows an "Input type" dropdown set to "Script", a "Mode" dropdown set to "Shell/Bash", and a "Theme" dropdown set to "Default". Below these are several small icons. The central area contains a code editor with the following script:

```
16 if [[ ${osvers_major} -ge 15 ]]; then
17     if [ -f "/Users/"${currentUser}"/Library/Preferences/com.apple.siri.generativeassistantsettings.plist" ] ; then
18         chatGPTstatus=$(/usr/bin/defaults read /Users/"${currentUser}"'/Library/Preferences/com.apple.siri.generative
19         if [ $chatGPTstatus = "1" ] ; then
20             echo "<result>Enabled</result>"
21         elif [ $chatGPTstatus = "0" ] ; then
22             echo "<result>Disabled</result>"
23         else
24             echo "<result>Not configured</result>"
25         fi
26     else
27         echo "<result>Not configured</result>"
28     fi
29     exit 0
30     else
31         echo "<result>Ineligible</result>"
32     fi
33 exit 0
```

A message "Copied!" is displayed at the bottom of the code editor. At the bottom right are "Cancel" and "Save" buttons.



Generative Assistant Settings Plist

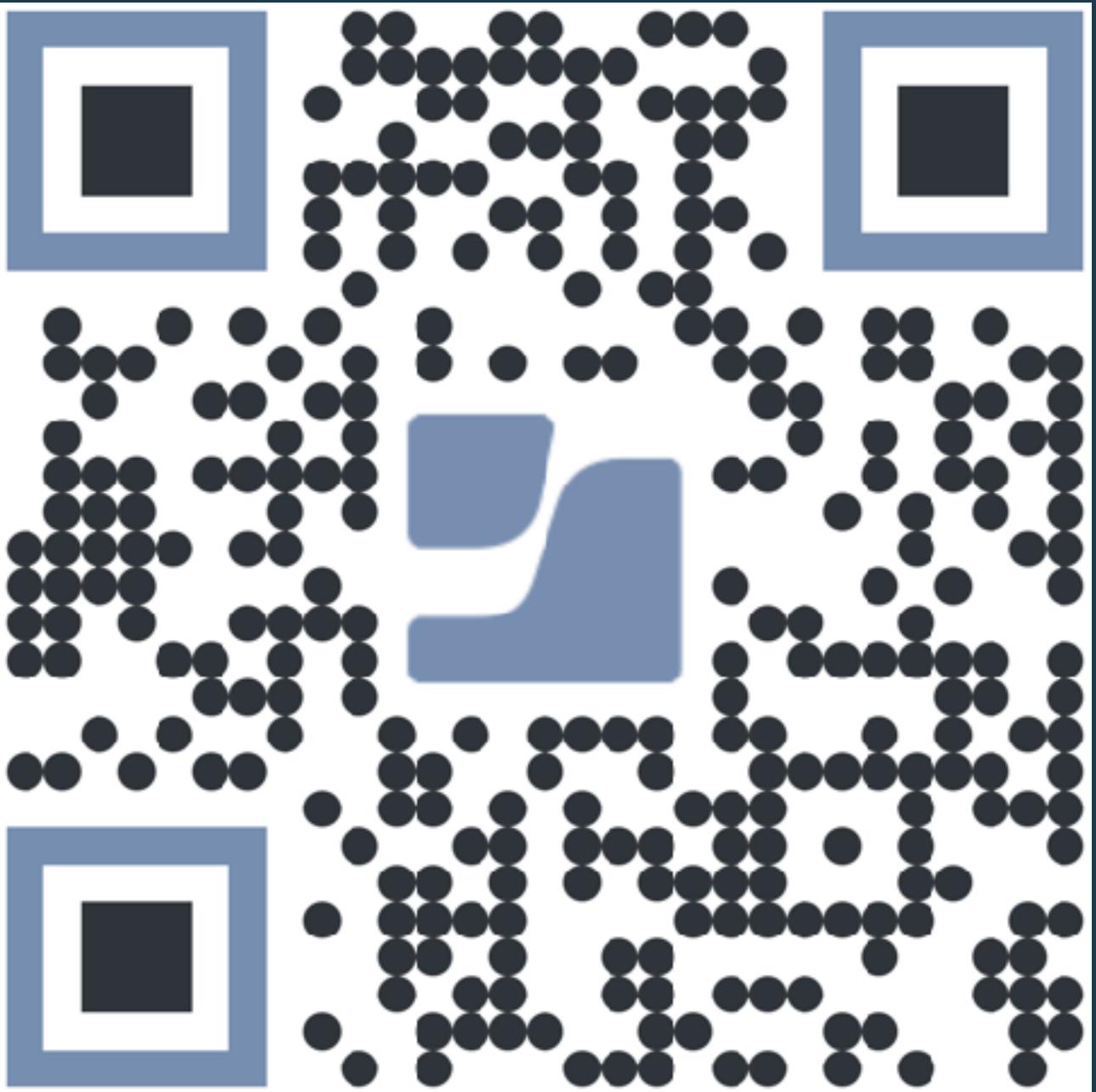
~/Library/Preferences/com.apple.siri.generativeassistantsettings.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>isEnabled</key>
  <true/>
</dict>
</plist>
```



Resources and Links

- [Apple Platform Deployment Guide](#)
- [Private Cloud Compute Security Guide](#)
- [Apple Blog - Private Cloud Compute](#)
- **Blogs**
 - Bob Gendler
 - [Raising Your IQ on Apple Intelligence](#)
 - [From Smart to Smarter: Elevating Apple IQ Even More](#)
 - Rich Trouton
 - [Managing Apple Intelligence features on macOS Sequoia 15.1](#)
 - [Managing Apple Intelligence features on macOS Sequoia 15.2](#)
 - [Managing Apple Intelligence features on macOS Sequoia 15.3](#)
 - [Managing Apple Intelligence features on macOS Sequoia 15.4](#)
 - [Suppressing the Apple Intelligence pop-up window with a configuration profile on macOS Sequoia](#)
 - Dr. Emily Kausalik
 - [Using the Applications & Custom Settings payload in Jamf Pro to manage the ChatGPT integration with Apple Intelligence](#)
 - [Skipping additional setup screens for Apple Intelligence with Jamf Pro on macOS 15.3 and iOS 18.3](#)
 - [External Intelligence Integration Status Extension Attribute](#)



Thank you!

