Recast

Deploy using Microsoft Intune (macOS – Bootstrapper 4.4)

Last Modified on 04.23.26

> **macOS only**
> The information in this article is applicable only to devices with macOS and Bootstrapper 4.4.
> The command lines and scripts in this article are just an example. When file names are specified, modify them accordingly before running the command/script.
> This guide does not cover how to create a .PKG file.

Prerequisites

Create an Entra ID identity source. For more information, see Microsoft Entra ID.

Application Workspace configurations

Create a self-signed certificate

To create a self-signed certificate:

1. In Application Workspace, navigate to **Manage** > **System** > **Device Registrations**.
2. Click on **+ Create** in the table toolbar.
3. In the **Create device registration** dialog box that opens, configure the following:
    - As the **Type**, select *Certificate* and click **Next**.
    - In **Overview**, write a name, for example *Device enrollment* and click **Next**.
    - In **Settings**, check the **Use a self signed certificate for the device registration** option. This will create a self-signed certificate for you. Click **Next**.
    - In **Self signed**, write a common name and change the days valid and key size if needed. Click **Next**.
    - In **Summary**, leave the **Modify device registration after creation** option selected. Click **Finish**.
    - In the newly created certificate that opens, navigate to the **Settings** screen and click **Download for agent registration**. You need to save this file, as you will use it when creating the .PKG file that you will later upload to Intune.

> **Certificate trust for self-hosted environments**
> If you are self-hosting Application Workspace, client devices must trust the Application Workspace server. This typically requires deploying one or more certificates to your devices.
> If your server uses a certificate issued by a public Certificate Authority (CA), no additional configuration is required.
> If you are using an internal CA or the self-signed certificate generated during the Application Workspace installation, you must export the required certificates and deploy them to client devices. This is usually done through Microsoft Intune or your preferred MDM solution.
> Depending on your setup, you may need to deploy:

The internal CA root certificate
The Application Workspace self-signed certificate

Ensure these certificates are installed in the Trusted Root Certification Authorities store on the client devices to establish a valid trust chain between the clients and the Application Workspace server.
You can create one or more Intune certificate profiles as needed, based on your environment and configuration. For guidance, see: Microsoft documentation.

Create a deployment

1. In Application Workspace, navigate to **Manage** > **Automation** > **Deployments**.
2. Click on ✚ **Create** in the table toolbar.
3. In the **Create deployment** dialog box that opens, enter the desired name and description.
    - In **Name**, write MS Intune Deployment. Click **Next** and then **Finish**.
    - In **Summary**, leave the *Modify deployment after creation* selected.
4. In the detailed view of the new deployment, configure the following:
    - In **Packages**, use the lookup field or the browse button ... to select the packages you want to deploy. Be sure to specify the *Install* action.
    - In **Assignments**, use the lookup field or the browse button ... and select an existing device collection for a targeted deployment or the *All devices* predefined collection to deploy to all devices.

Build custom .PKG

Create a folder where you will store all files that will be included in the .PKG file, namely:

- The agent bootstrapper for macOS from our downloads page https://download.liquit.com
- (Optional) The certificate is for certificate-based device registration.
- (Optional) If there are specific settings that cannot be handled by the bootstrapper, you should create an Agent.json file and add it to this folder. If you don't, the bootstrapper creates one for you during deployment. The objects that you can configure in the command line are Zone, Registration and Deployments (except for cancel, trigger, zoneTimeout). You can specify command lines for the bootstrapper in Intune, as explained later in this article.

Important notes
Make sure the files in this folder have the right permissions and attributes. Use the terminal and navigate to this folder, and make sure the bootstrapper and post-install script files are executable using the chmod +x command.
You can create the .PKG file using tools like Package Builder from Araelium https://www.araelium.com/packagebuilder
There is no need to include a post-install script. The Bootstrapper handles the log file and launch agent, including all the required post-install actions. On macOS, your only action is to run the Bootstrapper executable with the correct command-line arguments.

Agent.json file example

Make sure that the Agent.json is formatted as UTF-8.

```
{
 "zone": "https://fqdn.yoursiteserver.com",
 "promptZone": "Disabled",
 "registration": { "type": "Certificate" },
 "deployment": {
 "enabled": true,
 "start": false,
 "context": "device",
 "cancel": false,
 "triggers": false,
 "autoStart": {
 "enabled": true,
 "deployment": "Your Deployment Name",
 "timer": 0
 }
 },
 "log": { "level": "Info" },
 "icon": { "enabled": true, "exit": true, "timeout": 30 },
 "launcher": {
 "enabled": true,
 "state": "Default",
 "start": "Auto",
 "tiles": true,
 "minimal": false,
 "contextMenu": true,
 "sideMenu": "Tags",
 "close": true
 },
 "restrictZones": true,
 "trustedZones": ["FQDN.yoursiteserver.com"]
}
```

Microsoft Intune configurations

Deploying the Liquit Root CA Certificate via Microsoft Intune

1. Download the Liquit Root CA certificate from our download page . If the Application Workspace Universal Agent is already installed, you can find the Liquit Root CA certificate on macOS at `/Applications/Liquit/Contents/Resources`, named Agent.pfx or download it from our download page . This certificate is part of the self-signed certificate chain and therefore needs to be trusted as well.

2. Go to the Microsoft Intune admin center.

3. Select **Devices** > **Platform** > **macOS** > **Configuration** > **Policies** > **+ Create** > **+New policy**.

4. In the Create a Profile type page that opens, under Profile type, select Template.

5. Select Trusted certificate, then click Create.

6. In the Trusted certificate page that opens, configure the following:
    - In **Basics**, fill in the necessary fields. Click Next.
    - In **Configuration settings**, set Deployment Channel to Device Channel, and in Certificate file upload the certificate from step 1.

- In **Assignments**, click Add groups and add a group of devices that should receive this certificate.
- On the **Review + create** page, review the values and settings that you entered. After you click **Create**, Intune will install the Application Workspace certificate on the group of macOS devices.

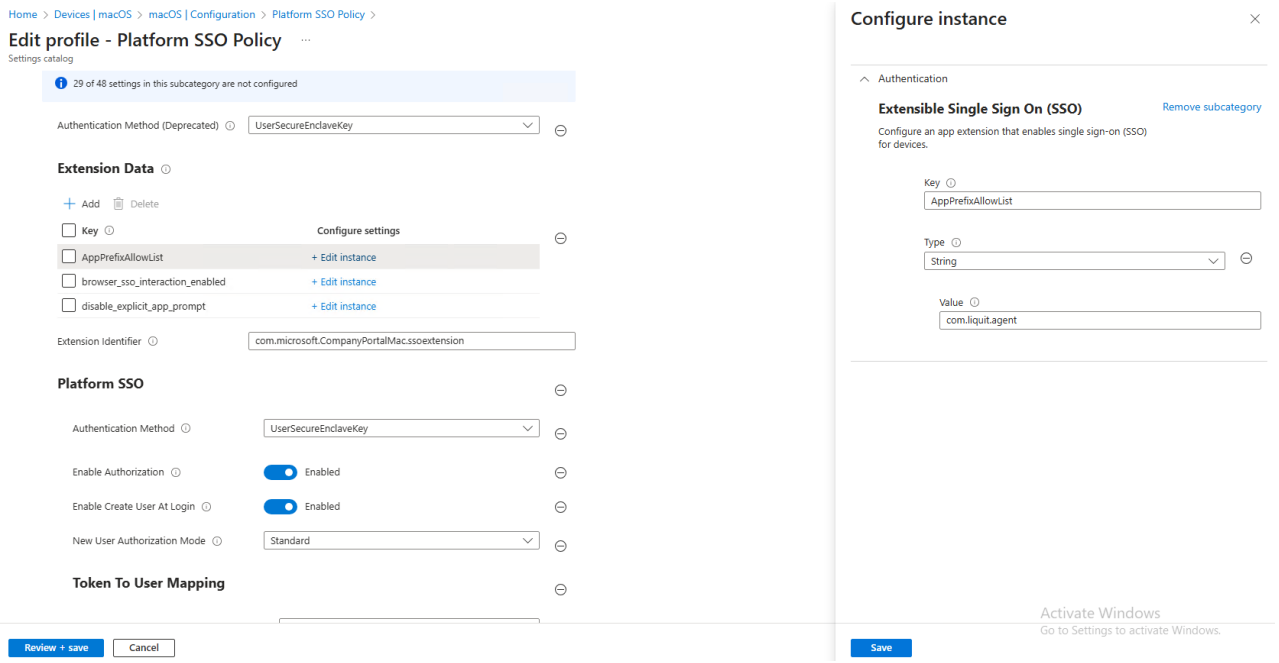
Create a macOS app in Intune

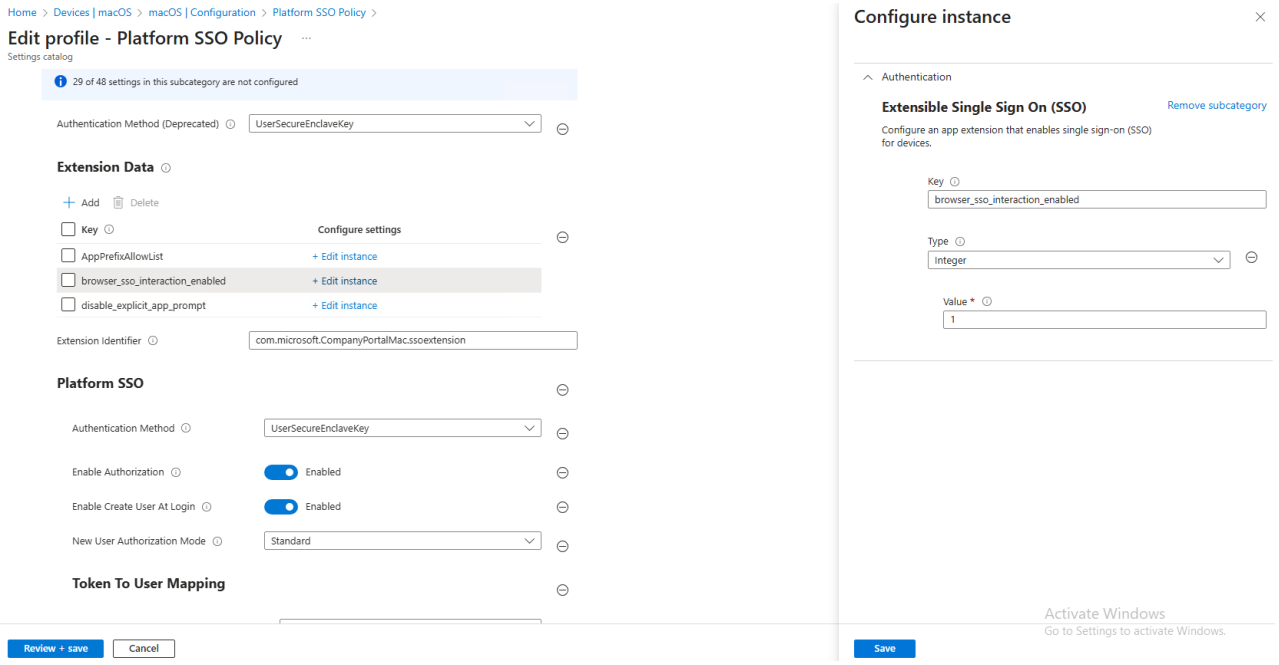
1. Go to the Microsoft Intune admin center.
2. Select **Apps** > **Platform** > **macOS** > **+ Create**.
3. On the Select app type pane that opens, under **App type**, select 'macOS app (PKG)' and then click **Select**.
4. The Add App page opens, where you configure the following:
   - On the **App information** page, click **Select app package file**.
   - On the **Add package file** page that opens, upload the .PKG file you previously prepared. Once you finish filling in all the necessary details, click **Next**.
   - On the **Program file** page, you can add the post-install script, if you did not already add it in the .pkg file itself.
   - On the **Requirements** page, choose the latest supported version of macOS.
   - On the **Detection rules** page, modify the bundle version to match the Application Workspace Agent version you intend to deploy.
   - On the **Review + create** page, review the values and settings that you entered for the app. Click **Create** to add the .pkg file to Microsoft Intune.

SSO configuration

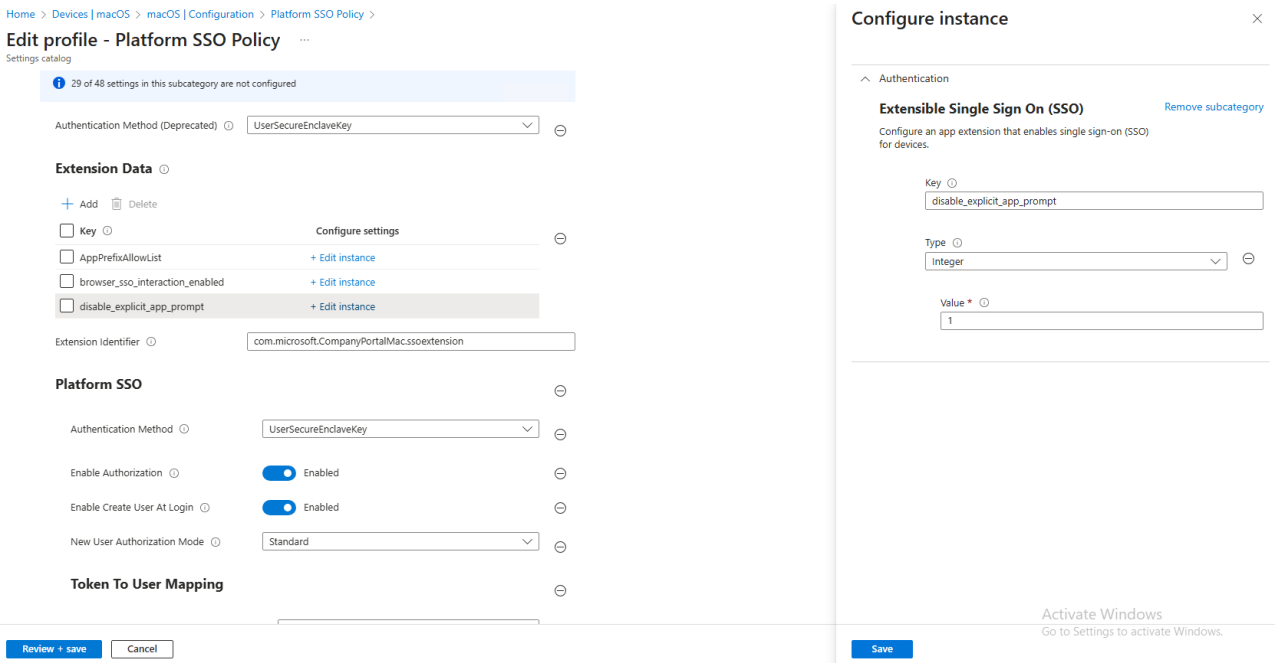
Follow Microsoft's guide to create a Platform SSO policy in Intune.
Then apply the following Application Workspace – specific settings:

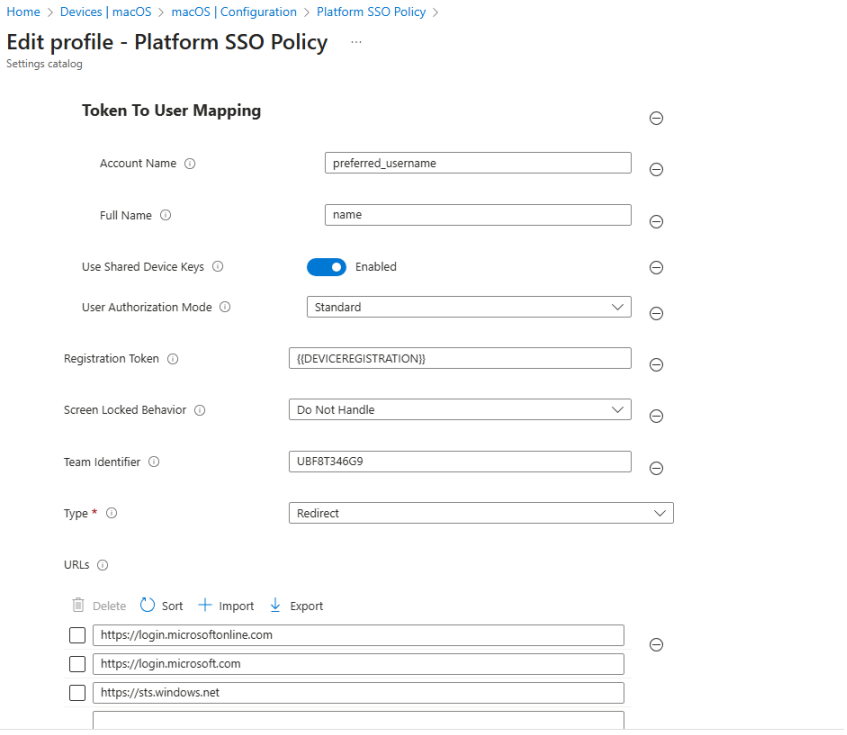
Recast


Home > Devices | macOS > macOS | Configuration > Platform SSO Policy >
Edit profile - Platform SSO Policy
Settings catalog
29 of 48 settings in this subcategory are not configured
Authentication Method (Deprecated)
UserSecureEnclaveKey
Extension Data
Add
Delete
Key
Configure settings
AppPrefixAllowList
+ Edit instance
browser_sso_interaction_enabled
+ Edit instance
disable_explicit_app_prompt
+ Edit instance
Extension Identifier
com.microsoft.CompanyPortalMac.ssoextension
Platform SSO
Authentication Method
UserSecureEnclaveKey
Enable Authorization
Enabled
Enable Create User At Login
Enabled
New User Authorization Mode
Standard
Token To User Mapping
Review + save
Cancel
Configure instance
Authentication
Extensible Single Sign On (SSO)
Remove subcategory
Configure an app extension that enables single sign-on (SSO) for devices.
Key
AppPrefixAllowList
Type
String
Value
com.liquit.agent
Save


Home > Devices | macOS > macOS | Configuration > Platform SSO Policy >
Edit profile - Platform SSO Policy
Settings catalog
29 of 48 settings in this subcategory are not configured
Authentication Method (Deprecated)
UserSecureEnclaveKey
Extension Data
Add
Delete
Key
Configure settings
AppPrefixAllowList
+ Edit instance
browser_sso_interaction_enabled
+ Edit instance
disable_explicit_app_prompt
+ Edit instance
Extension Identifier
com.microsoft.CompanyPortalMac.ssoextension
Platform SSO
Authentication Method
UserSecureEnclaveKey
Enable Authorization
Enabled
Enable Create User At Login
Enabled
New User Authorization Mode
Standard
Token To User Mapping
Review + save
Cancel
Configure instance
Authentication
Extensible Single Sign On (SSO)
Remove subcategory
Configure an app extension that enables single sign-on (SSO) for devices.
Key
browser_sso_interaction_enabled
Type
Integer
Value *
1
Save

Recast





Reboot

The device requires a reboot after the initial configuration. Until the deployment becomes inactive, the Application Workspace Agent service is disabled, and the Application Workspace Launcher is not available.

Further reading

Manage MacOS with Intune, including Apple Business Manager, Defender Enrollment, Platform SSO, and much more – The Complete Guide Part 1

Recast