

Integrating with Microsoft Intune to Enforce Compliance on Mac Computers Managed by Jamf Pro

Technical Paper
Jamf Pro 10.17.0 or Later
23 August 2021

© copyright 2002-2021 Jamf. All rights reserved.

Jamf has made all efforts to ensure that this guide is accurate.

Jamf
100 Washington Ave S Suite 1100
Minneapolis, MN 55401-2155
(612) 605-6625

Jamf, the Jamf Logo, JAMF SOFTWARE®, and the JAMF SOFTWARE Logo® are registered or common law trademarks of JAMF SOFTWARE, LLC in the U.S. and other countries.

Apple, the Apple logo, iPad, and iPod touch are trademarks of Apple Inc., registered in the United States and other countries. App Store is a service mark of Apple Inc., registered in the United States and other countries.

IOS is a trademark or registered trademark of Cisco in the United States and other countries.

Microsoft, Microsoft Intune, Azure, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other product and service names mentioned herein are either registered trademarks or trademarks of their respective companies.

Contents

5 Introduction

- 5 What's in This Guide
- 5 Additional Resources

6 Overview

7 Requirements

- 7 Related Information

8 Manually Configure the Connection Between Jamf Pro and Microsoft Intune

- 8 Step 1: Create a new application for Jamf Pro in Microsoft Azure
- 10 Step 2: Configure Microsoft Intune to allow the Jamf Pro integration
- 10 Step 3: Configure the macOS Intune Integration setting in Jamf Pro

12 Configuring the macOS Intune Integration using the Cloud Connector

- 12 Configuring the Cloud Connector in Jamf Pro

14 Apply Device Compliance Policies to Mac Computers

- 14 Related Information

15 Deploy the Company Portal App from Microsoft to End Users

- 15 Step 1: Download the Company Portal app from Microsoft
- 15 Step 2: Upload the Company Portal app to Jamf Pro as a package
- 16 Step 3: (Optional) Identify Mac Computers that do not have the Company Portal app installed
- 16 Step 4: Deploy the Company Portal app to Mac computers
- 16 Related Information

17 Create a Policy Directing Users to Register Mac Computers with Azure Active Directory

- 18 Related Information

19 Computer Registration User Experience

22 Troubleshooting

- 23 Related Information

24 Preparing to Reassign a Computer that is Registered with Microsoft Azure and Managed by Jamf Pro

- 24 Removing Jamf Components from the Computer
- 24 Deleting a computer from the Microsoft Azure and Intune Portal

25 Best Practices for Keeping User Computers in Compliance

- 25 Related Information

26 Appendix: Inventory Information Shared with Microsoft Intune

Introduction

What's in This Guide

This guide provides step-by-step instructions for integrating with Microsoft Intune to enforce compliance on Mac computers managed by Jamf Pro 10.9.0 or later.

Additional Resources

[Conditional Access in Azure Active Directory](#)

Learn about Azure Active Directory and how to configure Conditional Access policies.

Overview

This guide provides a complete workflow for integrating with Microsoft Intune to enforce compliance on Mac computers managed by Jamf Pro.

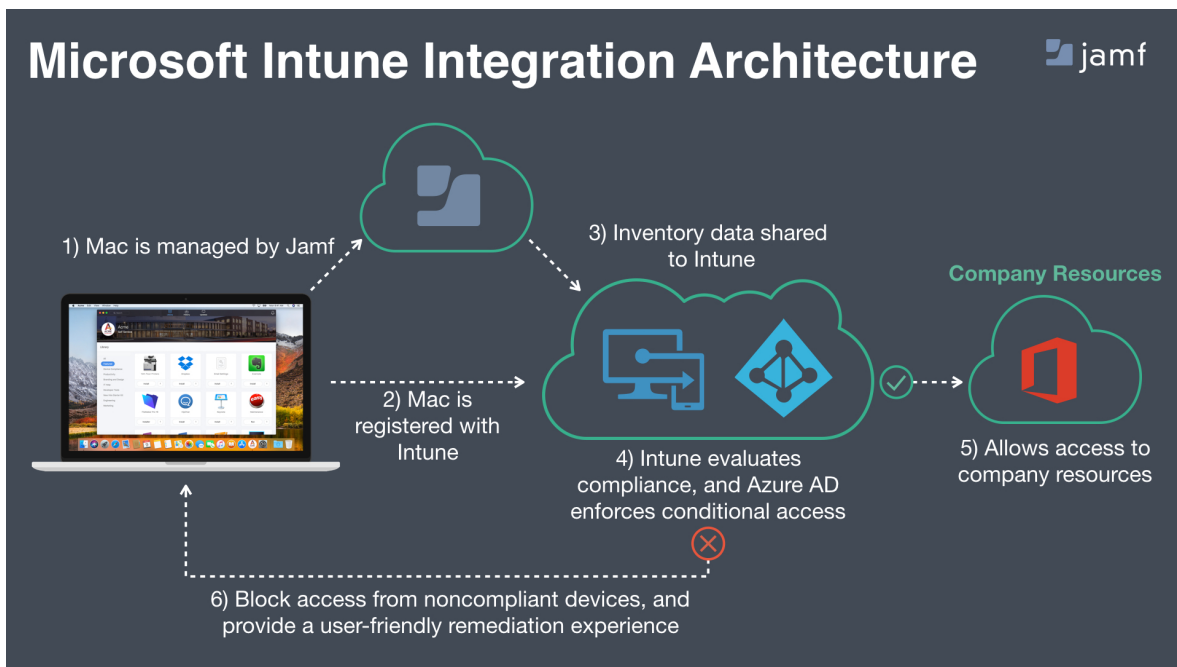
Important: You must exclude the User registration app for Device Compliance when creating the conditional access policy. Failing to exclude the User registration app for Device Compliance will prevent users from being able to register with Azure AD.

Integrating with Microsoft Intune to enforce compliance involves the following steps:

1. Configure the connection between Jamf Pro and Microsoft Intune.
2. Apply device compliance policies to Mac computers.
3. Deploy the Company Portal app for Microsoft to end users.
4. Create a policy directing users to register computers with Azure Active Directory.
5. Troubleshoot integration issues.

Jamf Pro delivers information about the management state of computers to Microsoft Intune's device compliance engine, which integrates with Azure Active Directory (Azure AD). This allows you to identify unmanaged and non-compliant Mac computers, and remediate them using Jamf Self Service for macOS.

The following diagram shows a high-level flow of the integration architecture:



Requirements

To configure the Microsoft Intune integration with Jamf Pro, you need the following:

- (Manual connection) Jamf Pro 10.9.0 or later
- (Cloud Connector) Jamf Pro 10.18.0 or later hosted in Jamf Cloud
- Microsoft Enterprise Mobility + Security (specifically Microsoft AAD Premium and Microsoft Intune)
- A Jamf Pro user account with Conditional Access privileges
- Microsoft Intune Company Portal app for macOS v1.1 or later
- Computers with macOS 10.11 or later that are using a local or mobile account

Note: Network accounts are not supported.

Depending on your environment, you may need to add the following domain names and ports as an exception or add them to your firewall safelist:

- login.microsoftonline.com
- graph.windows.net
- *.manage.microsoft.com
- Port 80/443 (HTTP/HTTPS protocol)

Note: The JamfAAD pre-fill feature introduced in Jamf Pro 10.14.0 may cause issues with the authentication experience in environments that use both the Microsoft Intune Integration and Active Directory Federation Services to authenticate to Azure. For instructions on resolving this issue, see the [Troubleshooting the JamfAAD Pre-fill Authentication Issue](#) article.

Related Information

[Jamf Pro User Accounts and Groups](#)

Find out how to create a user account with a specific privilege.

Manually Configure the Connection Between Jamf Pro and Microsoft Intune

Manually configuring the connection between Jamf Pro and Microsoft Intune involves the following steps:

1. Create a new application for Jamf Pro in Microsoft Azure.
2. Configure Microsoft Intune to allow the Jamf Pro integration.
3. Configure the macOS Intune Integration setting in Jamf Pro.

Important: Do not attempt to use the manual connection method to connect multiple Jamf Pro instances to a single Azure AD tenant. In addition, the manual connection method should not be used in conjunction with the Cloud Connector. This will prevent the Intune Integration from working correctly.

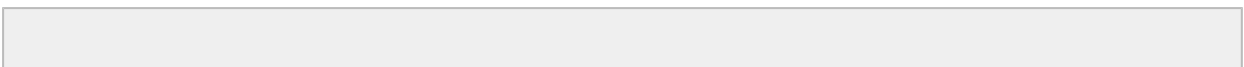
Note: When configuring the connection between Jamf Pro and Microsoft Intune, you must use the Microsoft Azure website (portal.azure.com) and not the Microsoft Azure portal desktop app.

Note: Due to changes on the Microsoft API backend permissions, changes are needed for the Microsoft and Jamf integration. Refer to [Support Tip: Intune service discovery API endpoint will require specific permissions](#) for more information from the Intune team at Microsoft.

The permission requirements for the Jamf integration enterprise apps were made in collaboration with Microsoft.

Step 1: Create a new application for Jamf Pro in Microsoft Azure

1. Open Azure Active Directory, and navigate to **App registrations**.
2. Click **New registration**.
 - a. Enter a display name for the Jamf Pro application.
 - b. Under Supported account types, select which accounts can use the application.
 - c. Specify your Jamf Pro URL as the Redirect URL.
 - d. Click **Register**.
3. Select the newly created application, copy the value from the **Application (client) ID** field and paste it to another location.



Note: The Application ID is required to configure the Compliance Connector in Intune and for configuring the macOS Intune Integration setting in Jamf Pro.

4. Navigate to **Certificates & secrets**, and click **New client secret**.
5. Give the Client Secret a description and select an expiration option. Once a new secret has been added, copy the value for the secret and paste it to another location.

Important: The Client Secret value is required to configure the macOS Intune Integration setting in Jamf Pro. The value for the secret is shown only once after the secret is added. If the Client Secret expires, you must add a new Client Secret in Microsoft Azure, and then update your macOS Intune Integration configuration in Jamf Pro. Microsoft Azure allows you to have both the old secret and new secret active to prevent service disruptions.

6. Navigate to **API permissions**.
 - a. Remove all permissions, including the default permissions.
 - b. Click **Add a permission**.
 - c. Under the Intune API, click **Application permissions**, and then select **update_device_attributes**.

Note: In GCC High environments, "Microsoft Intune API" is available in "APIs my organization uses". To add the permission, navigate to "APIs my organization uses" and search for "Microsoft Intune API". After you select it, click **Application permissions**, and then select **update_device_attributes**.

- d. Under Microsoft Graph, click **Application permissions**, and then select **Application.Read.All**.
- e. Click **Add permissions**.
- f. Under Azure AD Graph, click **Application permissions**, and then select **Application.Read.All**.
- g. Click **Add permissions**.
- h. Click the **Grant admin consent for your organization** button, and then click **Yes**.

Step 2: Configure Microsoft Intune to allow the Jamf Pro integration

1. In the Microsoft Azure portal, navigate to **Microsoft Intune > Device Compliance > Partner device management**.
2. Enable the Compliance Connector for Jamf by pasting the value you copied from the Application ID field into the **Jamf Azure Active Directory App ID** field.
3. Click **Save**.

Step 3: Configure the macOS Intune Integration setting in Jamf Pro

1. In Jamf Pro, navigate to **Settings > Global Management**.
2. Click **Conditional Access** .
3. Navigate to the **macOS Intune Integration** tab, and then click **Edit**.

4. Select the **Enable Intune Integration for macOS** checkbox.
When this setting is enabled, Jamf Pro sends inventory updates to Microsoft Intune. Clear the selection if you want to disable the connection but save your configuration.
5. (Cloud-hosted instances only) Select "Manual" under Connection Type.

Note: This setting does not display for instances hosted on-premise.

6. From the **Sovereign Cloud** pop-up menu, select the location of your Sovereign Cloud from Microsoft.
7. Click **Open administrator consent URL**, and follow the onscreen instructions to allow the Jamf Native macOS Connector app to be added to your Azure AD tenant.
8. Add the **Azure AD Tenant Name** from Microsoft Azure.
9. Add the **Application ID** and **Client Secret** (previously called Application Key) for the Jamf Pro application from Microsoft Azure.
10. Select one of the following landing page options for computers that are not recognized by Microsoft Azure:
 - The Default Jamf Pro Device Registration page

Note: Depending on the state of the computer, this option redirects users to either the Jamf Pro device enrollment portal (to enroll with Jamf Pro) or the Company Portal app (to register with Azure AD).

- The Access Denied page
 - A custom webpage
11. Click **Save**.
Jamf Pro will test the configuration and report the success or failure of the connection.



Configuring the macOS Intune Integration using the Cloud Connector

The Cloud Connector simplifies the process of connecting a cloud-hosted Jamf Pro instance with Microsoft Intune. The Cloud Connector automates many of the steps needed to configure the macOS Intune Integration, including creating the Jamf Pro application in Microsoft Intune. When the connection is saved, Jamf Pro sends computer inventory information to Microsoft Intune and applies compliance policies to computers.

Note: When configuring the connection between Jamf Pro and Microsoft Intune, you must use the Microsoft Azure website (portal.azure.com) and not the Microsoft Azure portal desktop app.

Important: Only the Cloud Connector can be used to connect multiple Jamf Pro instances to a single Azure AD tenant. Do not attempt to connect additional Jamf Pro instances using the manual connection method in conjunction with the Cloud Connector. This will prevent the Intune Integration from working correctly.

Configuring the Cloud Connector in Jamf Pro

1. Log in to Jamf Pro.
2. In the top-right corner of the page, click **Settings** .
3. Click **Global Management**.
4. Click **Conditional Access** .
5. Click **Edit**.
6. Select the **Enable Intune Integration for macOS** checkbox.
When this setting is selected, Jamf Pro sends inventory updates to Microsoft Intune. Deselect this setting if you want to disable the connection but save your configuration.
7. Select "Cloud Connector" under Connection Type.
8. From the **Sovereign Cloud** pop-up menu, select the location of your Sovereign Cloud from Microsoft.
9. Select one of the following landing page options for computers that are not recognized by Microsoft Azure:
 - The Default Jamf Pro Device Registration page

Note: Depending on the state of the computer, this option redirects users to either the Jamf Pro device enrollment portal (to enroll with Jamf Pro) or the Company Portal app (to register with Azure AD).

- The Access Denied page
 - A custom webpage
10. Click **Connect**. You are redirected to the application registration page in Microsoft.
 11. Enter your Microsoft Azure credentials and follow the onscreen instructions to grant the permissions requested by Microsoft.
After permissions have been granted for the Cloud Connector and the Cloud Connector user registration app, you are redirected to the Application ID page.
 12. Click **Copy and open Intune**. A new tab opens to the **Partner device management blade** in Microsoft Azure.
 13. Paste the Application ID into the **Specify the Azure Active Directory App ID for Jamf** field.
 14. Click **Save**.
 15. Navigate back to the original tab and click **Confirm**. You are redirected back to Jamf Pro. Jamf Pro completes and tests the configuration. The success or failure of the connection displays on the Conditional Access settings page.
 16. (Optional) Repeat this process to connect additional Jamf Pro instances to the same Azure AD tenant.

When the connection between Jamf Pro and Microsoft Intune is successfully established, Jamf Pro sends inventory information to Microsoft Intune for each computer that is registered with Azure AD (registering with Azure AD is an end user workflow). You can view the Conditional Access Inventory State for a user and a computer in the Local User Account category of a computer's inventory information in Jamf Pro.

Note: If you connected multiple Jamf Pro instances to a single Azure AD tenant using the Cloud Connector and want to disable all connections, you must deselect the **Enable Intune Integration for macOS** checkbox in the Conditional Access settings for each instance.

Apply Device Compliance Policies to Mac Computers

Once the connection between Jamf Pro and Microsoft Intune has been established, you can start applying compliance policies to Mac computers in Microsoft Intune.

1. Open the Microsoft Azure portal, navigate to **Intune > Device Compliance > Policies** and create policies for Mac computers. You may also select a series of actions (e.g., sending warning emails) that should be applied to non-compliant users and groups.
2. (Optional) Navigate to **Intune > Device Compliance > Compliance policy settings > Compliance status validity period (days)** to set the number of days before a Mac computer is marked non-compliant. Default is 30 days.
3. Once you create all the required compliance policies, navigate to **Assignments** and apply the compliance policies to specified users or groups.

Note: If Mac computers have network accounts that do not match a local account, compliance policies dealing with password complexity should not be used within Microsoft Intune as they cannot be reported correctly from Jamf Pro. Password complexity is enforced by the network account server.

Related Information

[Microsoft Intune Documentation](#)

Learn how to create a device compliance policy for a Mac computer with Microsoft Intune.

Deploy the Company Portal App from Microsoft to End Users

Before directing users to register their Mac computers with Azure Active Directory (Azure AD), it is necessary to deploy Microsoft's Company Portal app.

Deploying the Company Portal app involves the following steps:

1. Download the Company Portal app from Microsoft.
2. Upload the Company Portal app to Jamf Pro as a package.
3. (Optional) Identify Mac computers that do not have the Company Portal app installed.
4. Deploy the Company Portal app to Mac computers.

Note: It is recommended that you do not enable Conditional Access for computers with multiple user accounts. Microsoft Endpoint Manager assigns one User Principal Name (UPN) to a device record. As a result, Jamf Pro will only send active data for one AAD ID per device at a time

Step 1: Download the Company Portal app from Microsoft

On a Mac computer, download the current version of the Company Portal app for macOS from the Microsoft website.

Important: Do not install it, you need a copy of the app to upload to Jamf Pro.

The `CompanyPortal_Installer.pkg` file can be downloaded from: <https://go.microsoft.com/fwlink/?linkid=862280>

Step 2: Upload the Company Portal app to Jamf Pro as a package

1. Upload the Company Portal app to a distribution point in Jamf Pro.
2. In Jamf Pro, navigate to **Settings > Computer Management > Packages**.
3. Create a new package that includes the Company Portal app and click **Save**.

Step 3: (Optional) Identify Mac Computers that do not have the Company Portal app installed

1. In Jamf Pro, navigate to **Computers** > **Smart Computer Groups**.
2. Create a new smart group that identifies Mac computers that do not have the CompanyPortal.app from Microsoft installed.
3. Click **Save**.

Step 4: Deploy the Company Portal app to Mac computers

1. In Jamf Pro, navigate to **Computers** > **Policies** and create a policy that deploys the Company Portal app to users.
 - a. Use the General payload to configure the following settings:
 - For **Trigger**, select "Enrollment Complete" and "Recurring Check-in".
 - For **Execution Frequency**, select "Once per computer".
 - b. Select the Packages payload, and then click **Configure**.
 - c. Click **Add** for the package that includes the Company Portal app.
 - d. Configure the settings for the package.
 - e. Specify a distribution point for Mac computers to download the package from.
2. Click the **Scope** tab to specify Mac computers on which the Company Portal app should be installed. You may also use the smart computer group created in step 3.
3. Click **Save**.

Note: The policy runs on Mac computers in the scope the next time they check in with Jamf Pro and meet the criteria in the General payload.

Related Information

[Managing Packages](#)

Find out how to create a package and upload a file to a distribution point in Jamf Pro.

[Smart Groups](#)

Find out how to create smart groups in Jamf Pro.

Create a Policy Directing Users to Register Mac Computers with Azure Active Directory

Once the Company Portal app is deployed to Mac computers, you can create a policy in Jamf Pro that directs end users to initiate the device registration process by running the Company Portal app. Users will need to launch the Company Portal app from Jamf Self Service for macOS to register their Mac computers with Azure Active Directory (Azure AD) as a device managed by Jamf Pro.

Important: Prior to deploying the policy, it is recommended that you notify your end users that they will be prompted to take action.

Creating a policy that registers Mac computers with Azure AD involves the following steps:

1. In Jamf Pro, navigate to **Computers > Policies**, and create a new policy requiring users to register their Mac computer with Azure AD.
2. Use the General payload to specify policy settings. For **Execution Frequency**, it is recommended that you select "Once per computer". This prevents the policy from running multiple times on the same computer which can cause duplicate Azure AD records.
3. Configure the **macOS Intune Integration** payload.
4. Click the **Scope** tab, and scope the policy to all targeted Mac computers.
5. Click the **Self Service** tab and configure the policy to be made available in Jamf Self Service for macOS.
6. (Optional) Include the policy in the Device Compliance category in Self Service.
7. Click **Save**.

Note: The Company Portal app must be launched from Jamf Self Service to begin device registration. Launching the Company Portal app manually (e.g., from the Applications or Downloads folder) will not register the device. If an end user launches the Company Portal app manually, they will see an 'AccountNotOnboarded' warning message.

Inventory information is sent to Microsoft Intune only for Mac computers that have completed the device registration process with Azure AD. Jamf Pro sends the inventory state of each managed Mac computer that has checked in with Jamf Pro within the last 24 hours. To view inventory data sent to Microsoft Intune for each username associated with a computer, navigate to a computer's history and click the **macOS Intune Integration Logs** category. For a list of Mac computer attributes that Jamf Pro sends to Microsoft Intune, see the [Appendix](#) in this guide.

Related Information

[Smart Groups](#)

Find out how to create smart groups in Jamf Pro.

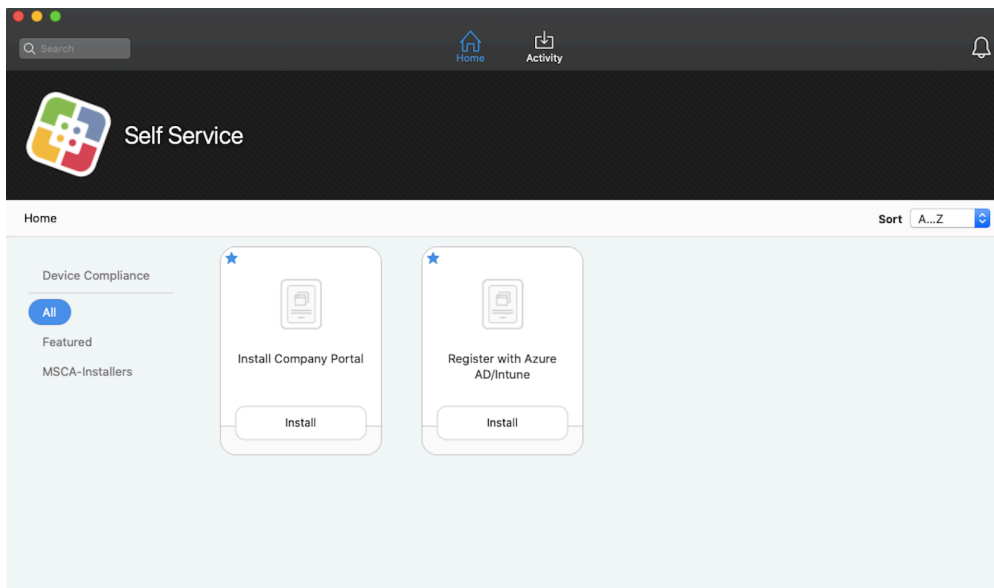
[Jamf Self Service for macOS](#)

Learn about Jamf Self Service and find out how to make items available to users.

Computer Registration User Experience

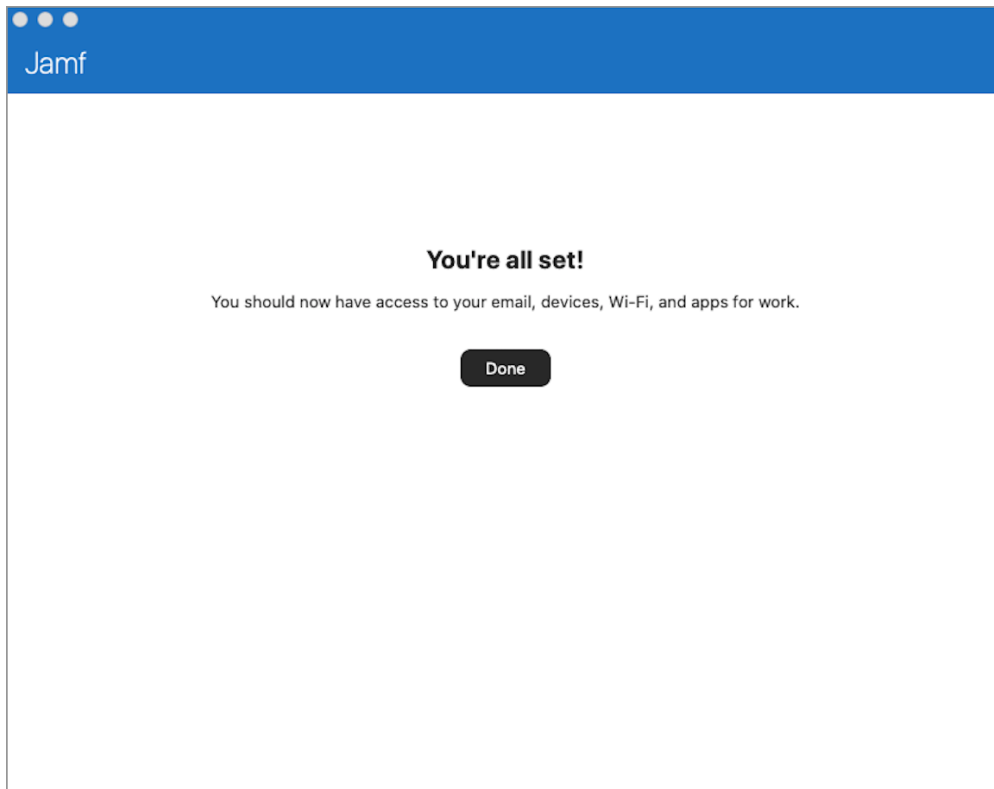
After you install the Company Portal app on the computer, users must register their computers with Azure Active Directory (Azure AD). Due to Authentication Services framework limitations, the workflow can run in one of the following web browsers: Safari, Microsoft Edge 92 or later, or Google Chrome 92 or later. The following section describes the computer registration process:

1. The user runs the registration policy from Jamf Self Service for macOS. For instructions on creating this policy, see the [Create a Policy Directing Users to Register Mac Computers with Azure Active Directory](#) section of this technical paper.

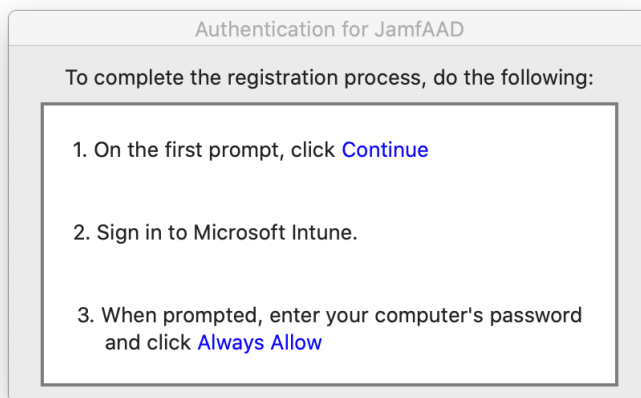


2. After the user runs the registration policy, the Company Portal app opens.
3. The user enters their Azure AD authentication credentials in the Company Portal app. Workplace Join opens after the user successfully enters their authentication credentials. This creates the computer record in Microsoft Azure. If the computer is managed by Jamf Pro and compliant, a message displays stating that registration was successful.

Note: Inventory information for the computer does not display in Microsoft Intune at this point.



4. JamfAAD opens.

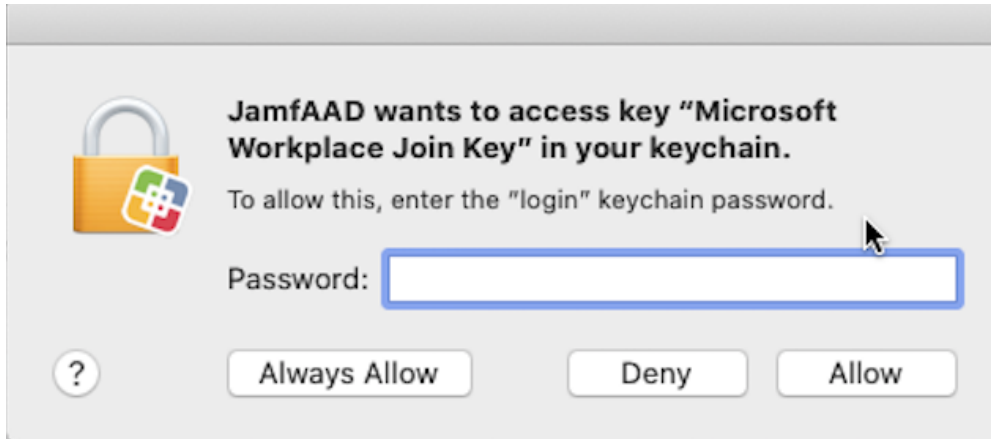


Depending on your environment, the user is asked to do one of the following:

- If your environment has Azure AD federation configured, the user is prompted to enter their authentication credentials for a second time and accept a multi-factor authentication prompt if configured.
- If your environment only uses Azure AD accounts, the user is prompted to enter their passwords again and accept a multi-factor authentication prompt if configured.

Note: The JamfAAD pre-fill feature introduced in Jamf Pro 10.14.0 may cause an issue with the authentication experience in environments that use Active Directory Federation Services to authenticate to Azure. See the [Troubleshooting the JamfAAD Pre-fill Authentication Issue](#) article for instructions on resolving the authentication issue.

5. The user is prompted to unlock the login keychain in Keychain Access to grant permissions.



JamfAAD sends the token with the Azure AD information to Jamf Pro. Jamf Pro sends computer inventory information to Microsoft Intune and the computer record is created in Intune after compliance is calculated for the first time. The Azure AD information is stored in the `device_aad_information` table in the Jamf Pro database.

Troubleshooting

You can verify if configured compliance policies are enforced on Mac computers by using an end user account to access an application that is protected with a compliance policy. It is recommended that you perform this test in the following scenarios:

- On a compliant Mac computer managed by Jamf Pro and registered with Azure Active Directory.
- On a non-compliant Mac computer managed by Jamf Pro and registered with Azure Active Directory.
- On a Mac computer not enrolled with Jamf Pro.

If the integration with Microsoft Intune is not working correctly, do the following:

- In Jamf Pro, navigate to **Settings > Global Management > Conditional Access > macOS Intune Integration**, and then click **Test** to view error messages.

Note: This option is not available if you used the Cloud Connector to configure the Intune Integration.

- In Microsoft Intune, verify that the entered data is correct.
- In Jamf Pro and Microsoft Intune, check the logs for error messages.

If you failed to add the Application ID to the **Partner device management** blade in Azure when configuring the Cloud Connector, do the following:

1. In the Microsoft Azure portal, navigate to **Microsoft Intune > Device Compliance > Partner device management blade**.
2. Paste the following value in the **Specify the Azure Active Directory App ID for Jamf** field:
963a9494-54df-4554-97ac-2cb44007ff49
3. Click **Save**.
4. In Jamf Pro, navigate to **Settings > Global Management > Conditional Access > macOS Intune Integration**, and click **Edit**.
5. Deselect the **Enable Intune Integration for macOS** checkbox, and click **Save**.
6. Wait a few moments and then click **Edit**.
7. Select the **Enable Intune Integration for macOS** checkbox.
8. Click **Connect**. You are redirected to the application registration page in Microsoft.
9. Enter your Microsoft Azure credentials and follow the onscreen prompts to grant the permissions requested by Microsoft. Once all permissions have been granted, you are redirected back to Jamf Pro. Jamf Pro completes and tests the configuration.
10. Wait a few moments and then refresh the Conditional Access settings page. The success or failure of the connection displays on the Conditional Access settings page.
11. Verify that no errors exist in the **Partner device management** blade in Microsoft Azure.

Related Information

For related information on how to troubleshoot Microsoft Azure, see the [Troubleshooting Microsoft Azure Login Using JamfAAD](#) article.

Preparing to Reassign a Computer that is Registered with Microsoft Azure and Managed by Jamf Pro

Before reassigning a computer that is registered with Microsoft Azure and managed by Jamf Pro, it is recommended that you do the following:

1. Remove the Jamf-related components from the computer.
2. Delete the computer from the Microsoft Azure and Intune portals.

Removing Jamf Components from the Computer

For instructions on removing Jamf components from a managed computer, see the [Components Installed on Managed Computers](#) section in the *Jamf Pro Administrator's Guide*.

Deleting a computer from the Microsoft Azure and Intune Portal

To delete a computer that is managed by Jamf from the Microsoft Azure and Intune portals, do the following:

1. In the Microsoft Azure portal, navigate to **Azure Active Directory > Devices > All Devices**.
2. Select the device you want to delete.
3. Click **Delete**, and then click **Delete** again to confirm.
4. Navigate to **Intune > Devices > All Devices**.
5. Select the device you want to delete.
6. Click **Delete**, and then click **Delete** again to confirm.

The computer is removed from the Azure and Intune portal after Microsoft processes the request.

Best Practices for Keeping User Computers in Compliance

Compliance can be completely enforced by Jamf Pro. As a result, Mac computers are never out of compliance as long as the computer is managed by Jamf Pro. To keep Mac computers in compliance, it is recommended that you deploy a configuration profile or a policy in Jamf Pro for each compliance policy created in Microsoft Intune.

1. In Jamf Pro, navigate to **Computers > Smart Computer Groups**, and create a smart group that identifies compliant Mac computers by using the following criteria:
 - a. Mac computers with the Company Portal.app installed
 - b. Mac computers with the Azure Active Directory ID attribute
2. Deploy a configuration profile or a policy in Jamf Pro for each of your compliance policies. (e.g., Deploy a Mac computer configuration profile with the Passcode payload if you configured a password policy in Microsoft Intune or a policy with the Disk Encryption payload if you configured an encryption policy in Microsoft Intune)
3. Scope the policy or configuration profile to the smart group created in step 1.
4. Click **Save**.
5. Repeat the process for all compliance policies created in Microsoft Intune.

Related Information

[Managing Policies](#)

Find out how to create a policy for a Mac computer in Jamf Pro.

[Computer Configuration Profiles](#)

Find out how to create a Mac computer configuration profile in Jamf Pro.

Appendix: Inventory Information Shared with Microsoft Intune

The following Mac computer inventory attributes are collected and shared from Jamf Pro to Microsoft Intune:

Attribute	Example Data Sent to Microsoft Intune	Used in Compliance	Jamf Pro Computer Inventory Location and Attribute
Tenant ID	0012166F-5DB5-41F7-B832-D8763D641274	Primary key	N/A
Device AAD ID	0012166F-5DB5-41F7-B832-D8763D641274	Primary key	Local User Accounts category: Computer Azure Active Directory ID
Last Check-In Time	2017-06-07T13:32:42Z	No	Timestamp of last recurring check-in by device to Jamf Pro (in UTC timezone) Important: This is not the time of the last inventory update.
Architecture Type	x86_64	No	Hardware category
Available RAM Slots	0	No	Hardware category
Battery Capacity	91%	No	Hardware category
Boot ROM	MB81.0164.B18	No	Hardware category
Bus Speed	1.10 Ghz	No	Hardware category
Cache Size	4MB	No	Hardware category
Device Name	User's MacBook Pro	No	General category: Computer Name
Domain Join	Likewise: ad.jamf.com Centrify: ad.jamf.com ad.jamf.com FALSE	No	Operating System category: Active Directory Status
Jamf ID	140 143 (any integer)	No	General category: Jamf Computer ID

Attribute	Example Data Sent to Microsoft Intune	Used in Compliance	Jamf Pro Computer Inventory Location and Attribute
Conditional Access Inventory State <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> Note: This attribute was called "Jamf Inventory State". </div>	0 1 2	Yes; no direct setting in compliance; internal logic	Calculated 0 == activated in Jamf Pro (new or coming back from unresponsive); 1 == deactivated (deleted /retired from Jamf Pro); 2 == unresponsive (time of last recurring check-in is more than 24 hours ago)
MAC address	C4:B3:01:C5:F5:61	No	Hardware category: Primary MAC Address
Make	Apple	No	Hardware category
Model	15-inch Retina MacBook Pro (Mid 2015)	No	Hardware category: Model
Model Identifier	Macbook8,1	No	Hardware category
NIC Speed	N/A	No	Hardware category
Number of Cores	2	No	Hardware category
Number of Processors	1	No	Hardware category
OS	macOS	No	Operating System category: Operating System
OS Version	10.12.4 10.10.3	Yes	Operating System category: Operating System Version
Platform	macOS	No	General category: Platform
Processor Speed	1.10 Ghz	No	Hardware category
Processor Type	Intel Core M	No	Hardware category
Secondary MAC Address	A1:23:4F:56:78:9J	No	Hardware category
Serial Number	J01A234MFJA5	No	Hardware category
SMC Version	2.25f87	No	Hardware category
Total RAM	8.0 GB	No	Hardware category

Attribute	Example Data Sent to Microsoft Intune	Used in Compliance	Jamf Pro Computer Inventory Location and Attribute
UDID	0012166F-5DB5-41F7-B832-D8763D641274	No	Hardware category
User AAD ID	0012166F-5DB5-41F7-B832-D8763D641274	Yes	Local User Accounts category: User Azure Active Directory ID
User Email	user@mycompany.com	No	User and Location category: Email Address
# of previous password to prevent reuse	1 5 NotEnforced	Yes	Local User Accounts category: Password History
Encrypted (FileVault 2)	TRUE FALSE	Yes	Disk Encryption category: Boot Partition: FileValult 2 Partition Encryption State
Gatekeeper	App store only App store and developer ID FALSE	No	Security category: Gatekeeper
Minimum # of character sets	2 NotEnforced	Yes	Local User Accounts category: Minimum Number of Complex Characters
Password expiration (days)	30 NotEnforced	Yes	Local User Accounts category: Maximum Passcode Age
Password Type	Simple AlphaNumeric NotEnforced	Yes	N/A
Prevent Auto Login	TRUE FALSE	Yes	Security category: Disable Automatic Login
Required Passcode Length	10 NotEnforced	Yes	Local User Accounts category: Minimum Passcode Length
Start screensaver after inactivity	5 20 NotEnforced	Yes	N/A

Attribute	Example Data Sent to Microsoft Intune	Used in Compliance	Jamf Pro Computer Inventory Location and Attribute
System Integrity Protection	TRUE FALSE NOTAPPLICABLE	Yes	Security category: System Integrity Protection FALSE = not collected status (could happen on first enrollment or very recent upgrade of Jamf Pro agent) or Disabled status; NOTAPPLICABLE is displayed for a macOS version earlier than macOS 10.11