

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

Technical Paper
Jamf Pro 10.1.0 or Later
4 June 2018

© copyright 2002-2018 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

The CASPER SUITE, 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

4 Introduction

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

5 Overview

6 Requirements

- 6 Related Information

7 Configure the Connection Between Jamf Pro and Microsoft Intune

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

9 Apply Device Compliance Policies to Computers

- 9 Related Information

10 Deploy the Company Portal App from Microsoft to End Users

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

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

- 13 Related Information

14 Troubleshooting

15 Best Practices for Keeping User Computers in Compliance

- 15 Related Information

16 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 10.1.0 or later.

Additional Resources

- [Jamf Pro Administrator's Guide](#)
Find more information on Microsoft Intune Integration settings.
- [Conditional Access in Azure Active Directory](#)
Learn about Azure Active Directory and how to configure conditional access policies on computers managed by Jamf Pro.

Overview

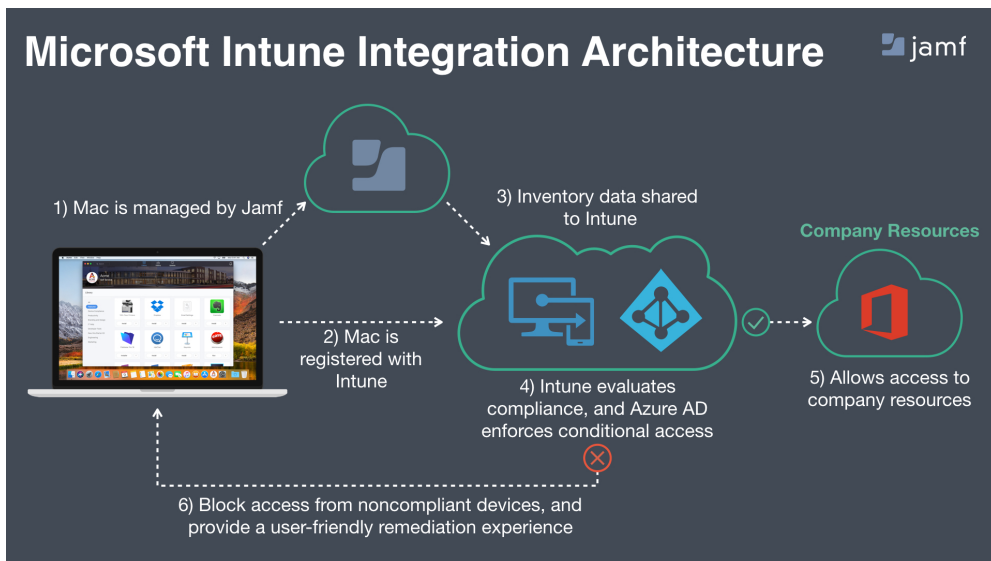
This guide provides a complete workflow for integrating with Microsoft Intune to enforce compliance on computers managed by Jamf Pro.

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

1. Configure the connection between Jamf Pro and Microsoft Intune
2. Apply device compliance policies to 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 and health 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 in 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:

- Jamf Pro 10.1.0 or later
- Microsoft Enterprise Mobility + Security (specifically Microsoft AAD Premium and Microsoft Intune)
- A Jamf Pro user account with Microsoft Intune Integration privileges
- Microsoft Intune Company Portal app for macOS v1.1
- Computers with macOS 10.11 or later

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

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

Related Information

[Jamf Pro User Accounts and Groups](#)

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

Configure the Connection Between Jamf Pro and Microsoft Intune

To enable the connection between Microsoft Intune and Jamf Pro, you must configure both Microsoft Intune and Jamf Pro.

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 Microsoft Intune Integration settings in Jamf Pro

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

1. Open Azure Active Directory, and navigate to **App Registration**.
2. Click **+New application registration**.
 - a. Enter the display name for the Jamf Pro application.
 - b. For the application type select **Web app / API**.
 - c. Specify the Sign-On URL for Jamf Pro.
 - d. Click **Create application**.
3. Select the newly created application and copy the **Application ID** field.

Note: The Application ID is required to configure the Compliance Connector in Intune and for configuring Microsoft Intune Integration settings in Jamf Pro.
4. Navigate to **Settings > API Access > Keys**, and create a new Application Key. Once a new key has been created, copy the value for the Application Key.

Note: The Application Key is required to configure the Microsoft Intune Integration settings in Jamf Pro. The value for the Application Key is shown only once during Application Key creation. If the Application Key expires, you must create a new Application Key in Microsoft Azure and then update the Microsoft Intune Integration configuration in Jamf Pro. Microsoft Azure allows you to have both the old key and new key active to prevent service disruptions.
5. Navigate to **Settings > API Access > Required Permissions**.
 - a. Delete all permissions, including the default permissions.
 - b. Add a new required permission for the Microsoft Intune API, and then select the **Send device attributes to Microsoft Intune** checkbox. The application must only have one required permission.
 - c. Click **Grant Permissions** after saving the required permission for the application.

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 Application ID into the **Jamf Azure Active Directory App ID** field.
3. Click **Save**.

Step 3: Configure Microsoft Intune Integration settings in Jamf Pro

1. In Jamf Pro, navigate to **Settings > Global Management**.
2. Click **Microsoft Intune Integration**, and then click **Edit**.
3. Select the **Enable Microsoft Intune Integration** checkbox.
When this setting is selected, Jamf Pro will send inventory updates to Microsoft Intune. Clear the selection if you want to disable the connection but save your configuration.
4. Select the location of your Sovereign Cloud from Microsoft.
5. Click **Open administrator consent URL**, and follow the onscreen prompts to allow the Jamf Native macOS Connector app to be added to your Azure AD tenant.
6. Add the Azure AD Tenant Name from Microsoft Azure.
7. Add the Application ID and Key for the Jamf Pro application from Microsoft Azure.
8. Click **Save**.
Jamf Pro will test the configuration and report the success or failure of the connection.

Apply Device Compliance Policies to Computers

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

1. Open the Microsoft Azure portal, navigate to **Intune > Device Compliance > Policies** and create policies for macOS 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. Once you create all the required compliance policies, navigate to **Assignments** and apply the compliance policies to specified users or groups.

Note: If 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 computer with Microsoft Intune.

Deploy the Company Portal App from Microsoft to End Users

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

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 computers that do not have the Company Portal app installed
4. Deploy the Company Portal app to computers

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 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 computers that do not have the Company Portal.app from Microsoft installed.
3. Click **Save**.

Step 4: Deploy the Company Portal app to 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 with the Company Portal app.
 - d. Configure the settings for the package.
 - e. Specify a distribution point for computers to download the package from.
2. Click the **Scope** tab to specify 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 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 Computer Groups](#)

Find out how to create smart groups in Jamf Pro.

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

Once the Company Portal app is deployed to 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 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 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 computer with Azure AD.
2. Use the General payload to specify policy settings, including trigger and execution frequency.
 - a. For **Trigger**, select "Login" or "Recurring Check-in".
 - b. For **Execution Frequency**, select "Ongoing".
3. Configure the **Microsoft Intune Integration** payload.
4. Click the **Scope** tab, and scope the policy to all targeted 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 a warning, 'AccountNotOnboarded'.

Inventory information is sent to Microsoft Intune only for computers that have completed the device registration process with Azure Active Directory. Jamf Pro sends the computer inventory state of each managed computer that has checked in with Jamf Pro within the last 24 hours. For a list of the computer attributes that Jamf Pro sends to Microsoft Intune, see the [Appendix](#) in this guide.

Related Information

[Smart Computer 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.

Troubleshooting

You can verify if configured compliance policies are enforced on 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 computer managed by Jamf Pro and registered with Azure Active Directory
- On a non-compliant computer managed by Jamf Pro and registered with Azure Active Directory
- On a 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 > Microsoft Intune Integration** and click **Test** to view error messages.
- In Microsoft Intune, verify that the entered data is correct.
- In Jamf Pro and Microsoft Intune, check the logs for error messages.

Best Practices for Keeping User Computers in Compliance

Compliance can be completely enforced by Jamf Pro, as a result computers are never out of compliance as long as the computer is managed by Jamf Pro. To keep 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 computers by using the following criteria:
 - a. Computers with the Company Portal.app installed
 - b. 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., A 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](#)

For instructions on creating a policy for a computer in Jamf Pro.

[Computer Configuration Profiles](#)

For instructions on creating a macOS configuration profile in Jamf Pro.

Appendix: Inventory Information Shared with Microsoft Intune

The following computer 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	General category: Azure Active Directory ID - Computer AAD 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
Jamf Inventory State	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	General category: Azure Active Directory ID - User AAD ID
User Email	user@mycompany.com	No	User and Location category: Email Address
# of previous password to prevent reuse	1 5 NotEnforced	Yes	N/A
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	N/A
Password expiration (days)	30 NotEnforced	Yes	N/A
Password Type	Simple AlphaNumeric NotEnforced	Yes	N/A
Prevent Auto Login	TRUE FALSE	Yes	N/A
Required Passcode Length	10 NotEnforced	Yes	N/A
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