



**Keeping Everybody
Globally Connected.**

1GLOBAL eSIM deployment with Jamf Pro

1 Introduction

This implementation guide explains the configuration of Jamf Pro for automated 1GLOBAL eSIM deployment using Smart Device Group, API and Webhook settings. The integration enables organizations to deploy 1GLOBAL eSIM profiles directly to corporate-owned Apple devices with zero user friction.

The solution is designed for enterprise environments and supports scalable device provisioning, automated regional eSIM assignment, and synchronization of inventory and subscription data with the 1GLOBAL platform.

This guide is intended to be used alongside support from your 1GLOBAL representative, who can advise on eSIM deployment best practices and assist with trial onboarding and integration testing.

2 Key Benefits

- Automated zero-touch eSIM deployment.
- Centralized enterprise device management.
- Secure OAuth API authentication.
- Regional Smart Device Group assignment.
- Automated inventory synchronization.
- Reduced deployment effort for administrators and end users.

3 Prerequisites

Requirement	Details
Jamf Pro	Jamf Pro MDM with the 1GLOBAL eSIM configuration
Apple Business Manager	Automated Device Enrollment (ADE) enabled
Supported Devices	Corporate-owned eSIM compatible iPhone and iPad devices
1GLOBAL Account	Enterprise account with Jamf-compatible eSIM profiles
Internet Connectivity	Devices must have internet access during deployment

4 Before you begin

The 1GLOBAL integration is specifically designed for corporate-owned Apple devices and allows for scalable, zero-touch eSIM provisioning to devices anywhere in the world.

To utilize this integration, devices must be eSIM compatible, this includes cellular iPads from 2018 onwards and the iPhone XS or later models. Starting with the iPhone 13, Dual eSIM support was made available. Notably, the iPad Pro (M4) Cellular and iPad Air (M2) Cellular and iPhone Air models are now exclusively eSIM-only in all markets and do not support physical SIM.

5 Device Restrictions for eSIM management

In Jamf Pro supervised devices can be configured with eSIM management policies tailored to corporate security and operational requirements. The following eSIM User controls are available.

- Modifying cellular plan (iOS 11 or later, supervised).
- Modifying cellular data app settings (supervised).
- Modifying eSIM settings (iOS 12.1 or later, supervised).
- eSIM transfers to other devices (iOS 18 or later, supervised).
- Preserve eSIM on erased device (iOS 17.2 or later, supervised).

Jamf Pro path:

Devices > Configuration Profiles > Restrictions > Functionality

6 Smart Device Group configuration

Multiple Smart Device Groups can be configured to support regional or operational deployment requirements for voice services based upon location criteria.

Recommended naming convention: **<COMPANY>_<1GLOBAL>_<COUNTRY>**

- ABC_1GLOBAL_UK
- ABC_1GLOBAL_NL
- ABC_1GLOBAL_US

Important:

Smart Device Group names used must match the configuration registered with 1GLOBAL.

7 Webhook configuration

- Navigate to Settings > Global > Webhooks in Jamf Pro.
- Create a new webhook configuration.
- Enter the 1GLOBAL webhook endpoint URL.
- Set Authentication Type to Basic Authentication.
- Username and Password will be supplied by 1GLOBAL.
- Configure Connection Timeout and Read Timeout to 10 seconds.
- Select JSON as the payload format.
- Choose the 'SmartGroupMobileDeviceMembershipChange' event.
- Select the target Smart Device Group or use All Groups.

Webhook Endpoint: <https://api.1global.com/b2b/jamf-bridge/events/handle>

8 Jamf Pro API Configuration

The 1GLOBAL integration uses OAuth API authentication with dedicated API Role and Client in Jamf Pro.

Create an API Role

- Navigate to Settings > System > API Roles and Clients.
- Open the API Roles tab and select New.
- Create a role named 1GLOBAL.
- Assign the required privileges (custom privilege set).
- Save the API Role configuration.

Privilege Category	Required Permissions
Mobile Devices	Create Mobile Devices, Read Mobile Devices
Server Actions	Send Mobile Device Refresh Cellular Plans Command

Create an API Client

- Open the API Clients tab and select New.
- Create a client named 1GLOBAL.
- Assign the previously created API Role.
- Set Access Token Lifetime to 300 seconds.
- Enable the API Client.
- Generate and securely store the Client Secret.

Security Notice: The Client Secret is displayed only once. Store it securely before closing the dialog. Provide the Client and Client Secret, along with the Jamf Pro URL, to 1GLOBAL using a secure and approved method.

9 Troubleshooting

For deployment assistance, troubleshooting support, or onboarding guidance, contact your 1GLOBAL account team or email business.help@1global.com.