

1GLOBAL eSIM Deployment App User Guide

[Home](#) » [1GLOBAL](#) » 1GLOBAL eSIM Deployment App User Guide 



This documentation details how JAMF Admin can configure the Webhook API for the zero touch 1GLOBAL eSIM deployment in JAMF Pro.

The API enables an organisation to distribute eSIMs from 1GLOBAL directly to end users' devices, pretty much anywhere in the World in seconds. The API call will send the right SIM to the right device in a matter of seconds and update the admin portal so names etc of the user match the 1GLOBAL portal.

Contents

- [1 Prerequisites](#)
- [2 Before you begin](#)
- [3 1GLOBAL Configuration](#)
- [4 Troubleshooting](#)
- [5 Documents / Resources](#)
 - [5.1 References](#)

Prerequisites

- JAMF Pro
- Apple eSIM compatible iOS devices
- Supervised / institutionalised iOS Devices.
- Pre-Stage Enrolment profile
- 1GLOBAL Enterprise account with eSIMs ordered as JAMF Compatible

Before you begin

This deployment method is for corporate owned devices only. This is the key to the zero-touch deployment and distributing the eSIMs direct to the user device.

eSIM deployment supported as follows:

- User by user / one at a time for new deployments
- User by user / one at a time for existing users including porting support.
- Bulk deployment for new devices / users – i.e. 2 or more, this can be hundreds or thousands of device / users.
- Bulk change from existing mobile / cellular provider to 1GLOBAL – Porting is also supported and is near seamless.

The Webhook API uses Smart Device Groups which need to be configured for those users that need an eSIM. A change in Smart Device Groups that matches an eSIM triggers the API call and the eSIM is sent to the devices EID. The EID is a unique identifier which is passed from the device in the enrolment stage to JAMF Pro and is then used by 1GLOBAL to trigger the eSIM. Note this is not possible with User Enrolment devices / BYOD.

Using Smart Device Groups means 1GLOBAL also receive a request to install the correct regional eSIM the end user receives, i.e. US users receiving an eSIM from the US and UK for the UK.

Devices need to be eSIM ready so that's all-cellular iPads from 2018 and the iPhone Xs or later. From the iPhone 13 onwards dual eSIM is also supported.

Depending on the required level of security devices can be set with a policy that only enables admin to remove and install eSIMs. This should be considered where needed but it optional. It can be used to prevent end users uninstalling eSIMs.

JAMF Pro > Devices > Configuration Policies > Restrictions > Functionality, then options for restricting:

- Modifying cellular plan
- Modifying cellular data app settings
- Modifying eSIM Settings

The Webhook also passes the username and email to update the 1GLOBAL platform for each activation.

Configuring the Smart Device Group for 1GLOBAL

Once an account with 1GLOBAL is set up (note you can have multiple accounts such as one per country), 1GLOBAL will need one Smart Device Group defined per country / account you wish to distribute SIMs to, an example below:

ABCINC_1GLOBAL_eSIM_UK

ABCINC_1GLOBAL_eSIM_NL

ABCINC_1GLOBAL_eSIM_US

JAMF Admin will need to notify the 1GLOBAL account team of the Smart Device Group name, this needs to be an exact match for the Web Hook to work correctly or the request will be ignored.

Of course, the organisation will need to define how the organisation will identify the device user groups and how users are allocated to the smart groups.

Configuring the Webhook API

This can be done by customers or 1GLOBAL offer free of charge support for initial set up.

JAMF Configuration

For 1GLOBAL to support speak engage your account team and a support call will be set up. 1GLOBAL will need permissions for read/create/delete/update webhooks only for the initial configuration you want us to do it on behalf your behalf. If the JAMF Admin is creating the webhook, we don't need those from the start.

The Webhook Event to select is: 'SmartGroupMobileDeviceMembershipChange' It is recommended to us use the 'Target Smart Device Group' and select the target group you want to send requests for.

Example is below:

Webhook Event

Event that will trigger the webhook Smart Group Mobile Device Membership Change

Target Smart Device Group

Group to receive the webhook event ABCINC_1GLOBAL_eSIM_US v

1GLOBAL Configuration

Configuration:

```
xml version="1.0" encoding="UTF-8"?>
<webhook>
<id>3</id>
<name>1GLOBAL – Mobile Device Added to Smart Group</name>
<enabled>true</enabled>
<url> https://api.1global.com/jamf-bridge/events/handle </url>
<content_type>application/json</content_type>
<event>SmartGroupMobileDeviceMembershipChange</event>
<connection_timeout>10</connection_timeout>
<read_timeout>10</read_timeout>
<authentication_type>BASIC</authentication_type>
<username>*****</username>
<password>*****</password>
<enable_display_fields_for_group_object>>false</enable_display_fields_for_group_o
bject>
<display_fields>
<size>0</size>
</display_fields>
<smart_group_id>-1</smart_group_id>
</webhook>
```

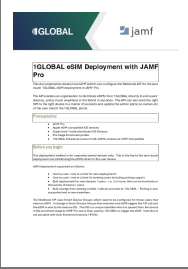
Troubleshooting

A failure of eSIMs to be delivered to the devices is normally for the below reasons:

- eSIM from 1GLOBAL already installed – An active 1GLOBAL eSIM is already installed. Either remove the SIM and re-add to the Smart Group to re-trigger or utilise the existing eSIM.
- No Profiles remaining – All the available profiles at 1GLOBAL have been used – Simply contact business.help@1global.com to request more or speak to your account team.
- Device does not have internet connection.
- User has an incorrect number – from another country / region – This is because the user was added to an incorrect Smart Group – so the wrong API has been called.
- Expired password and access – Raise a case with 1GLOBAL support team and your account team – business.help@1global.com



Documents / Resources

	<p>1GLOBAL eSIM Deployment App [pdf] User Guide iPhone Xs, iPhone 13, eSIM Deployment App, Deployment App, App</p>
----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------

References

- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.