Guide to deploying **ADSelfService Plus iOS mobile app in users' devices**

Table of Contents

Document summary

This guide details the mobile app deployment feature that helps admins easily install the ADSelfService Plus mobile app in end users' devices.

ADSelfService Plus mobile app deployment

What is the mobile app deployment feature?

ADSelfService Plus' mobile app helps users reset passwords and unlock accounts on the go. To simplify ADSelfService Plus installation on iOS devices, you can use the mobile app deployment feature that allows administrators to deploy mobile push management (MPM) profiles in users' devices. Once the MPM profile is installed, the administrator can remotely install and configure the iOS mobile app.

The mobile app deployment feature also allows you to:

1. Test drive the app deployment in up to 10 mobile devices using the trial mode.
2. Set up a scheduler to automatically send email notifications asking users to install the mobile push management profile.
3. Set up a scheduler to automatically install the mobile apps on MPM-configured devices.
4. Set up a scheduler to automatically update the status of app installation in each device.
5. Use the same access URL configured in the ADSelfService Plus installation for mobile apps by pushing the server settings from the product.

Note:

- To install the ADSelfService Plus app in more than ten devices, you need to complete Apple Push Notification Service (APNs) configuration.
- If you are already using an MPM or MDM provider, you need not install it again. Visit this section for steps on installing the app using your existing MPM/MDM.

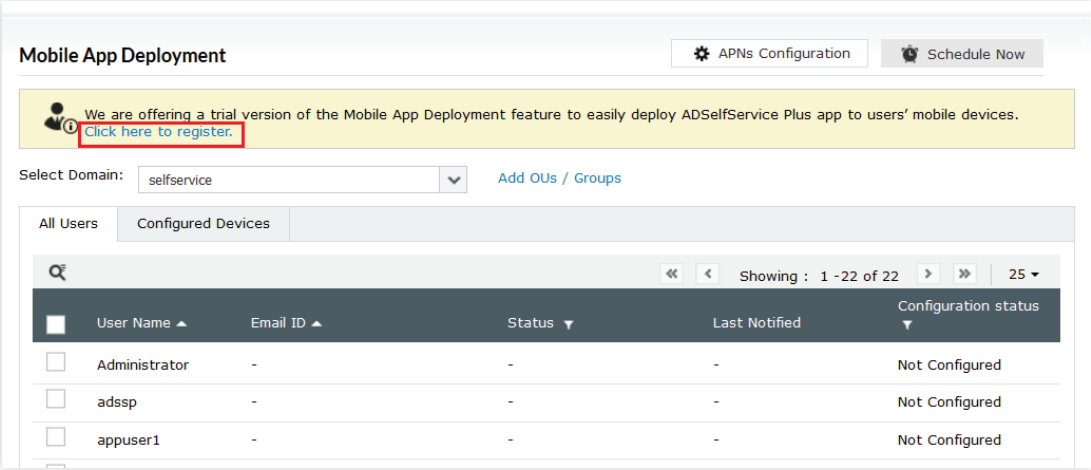
Step 1: Trial mode configuration

Prerequisite

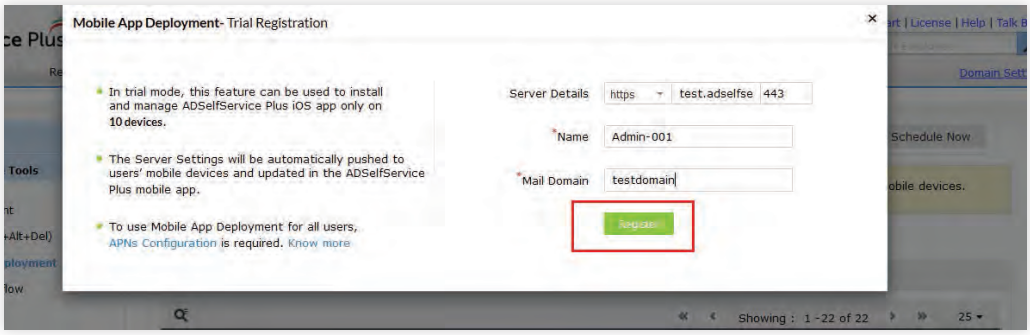
- **Allow outbound connections to creator.zoho.com:** If you're using the trial mode, please create a firewall rule to allow outbound connections to creator.zoho.com.

Configuration steps

- Open ADSelfService Plus and go to **Configuration > Administrative Tools > Mobile App Deployment.**
- To register for the trial mode, select **Click here to register** displayed at the top.



- Enter the ADSelfService Plus Server details, which includes the protocol, hostname/IP, **port number, your name, and email domain name** of your organization (the domain name comes after @ in your corporate email account). Completing this step will allow the mobile users to remotely access the ADSelfService Plus server.
- After filling in these details, click **Register.**



Step 2: APNs configuration

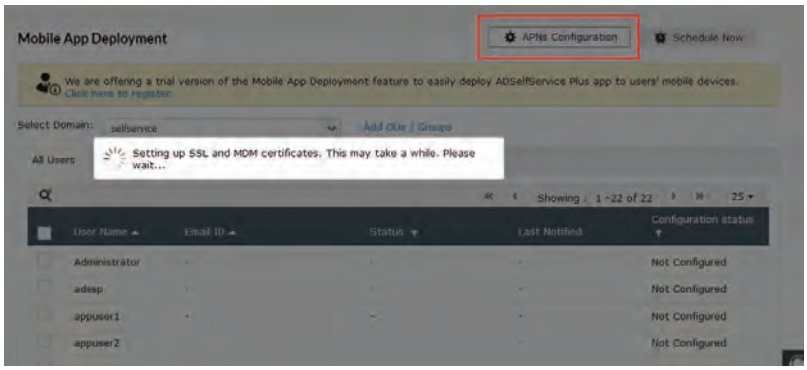
For APNs configuration, you must generate a certificate signing request (CSR), get the CSR signed by ManageEngine, and then submit the signed property list (PLIST) file to the Apple Push Certificate Portal.

Prerequisite

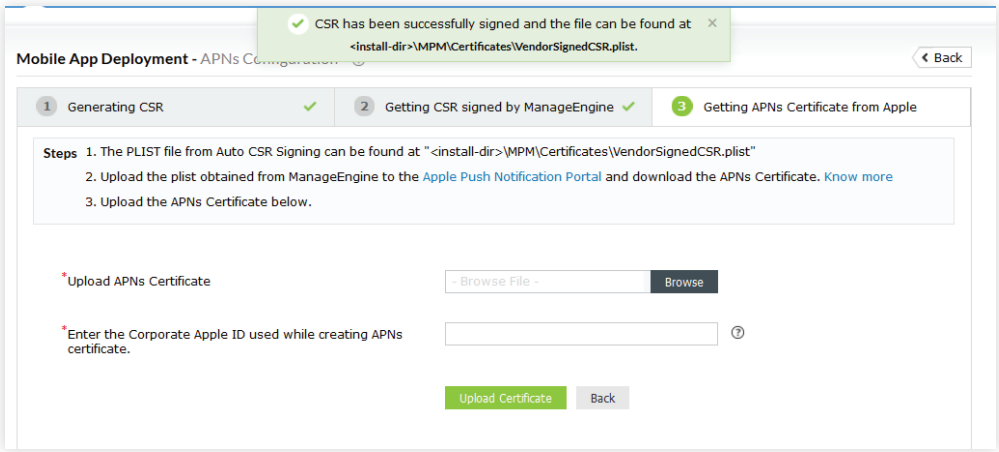
1. **Enable HTTPS:** Ensure that you've enabled HTTPS and applied a valid CA-signed SSL certificate in ADSelfService Plus.
2. **Update connection settings:** The product's self-signed certificate that was generated before build 5602 is not compatible with the Mobile App Deployment feature. If you're using such a certificate, update ADSelfService Plus to the latest build, and then navigate to the **Connection Settings,** and click **Save** to generate a compatible self-signed certificate.
3. **Open up access to the APNs Server:** In the machine where ADSelfService Plus is installed, add a firewall rule allowing connection to gateway.push.apple.com:2195 and feedback.push.apple.com:2196 so that the product can communicate with the APNs Server.

Generating the PLIST file

1. Open **ADSelfService Plus** and go to **Configuration > Administrative Tools > Mobile App Deployment.**
2. Click the **APNs Con figuration** button on the top right corner.



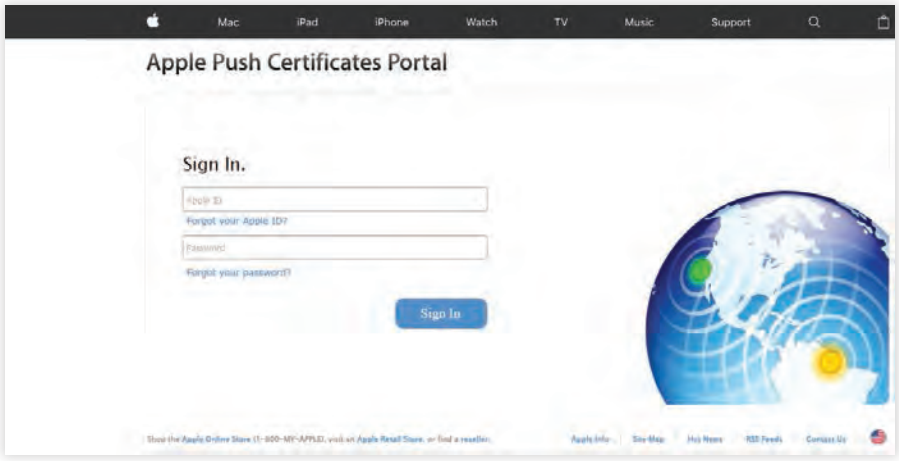
3. Now, ADSelfService Plus will auto-generate a certificate signing request (CSR) and create a PLIST file based on the SSL certificate you've applied in the product. You can find the generated PLIST file (VendorSignedCSR.plist) in this folder: <install directory>\MPM\Certificates. If, for some reason, the PLIST file is not automatically created, you'll be asked to contact ManageEngine support. In this case, the ManageEngine support team will send the PLIST file to your email.



Generating the PEM file

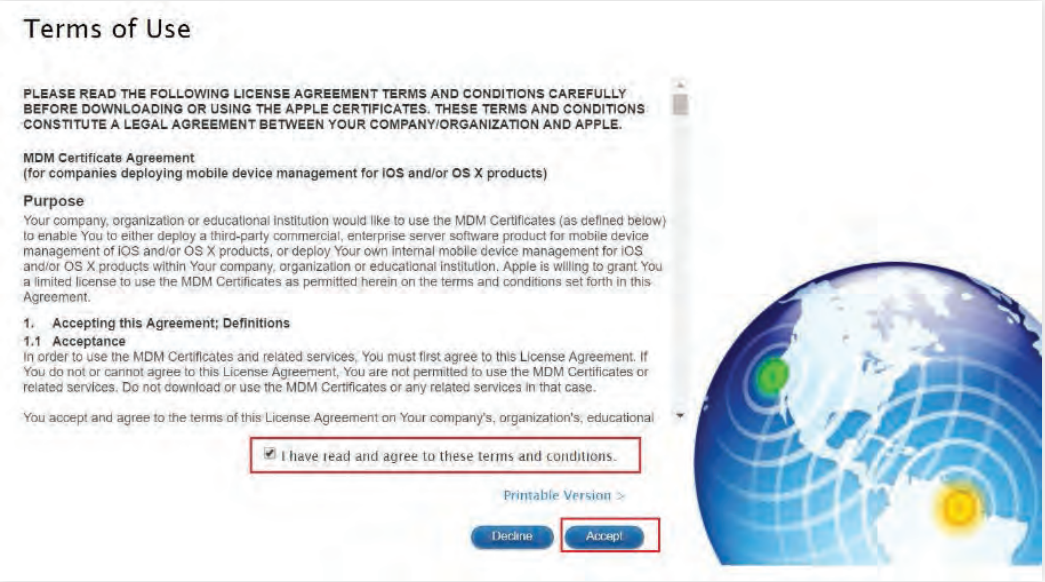
4. Go to the Apple Push Certificates Portal.

5. Sign in to the portal using your personal or corporate Apple ID. The **Apple ID** you entered here will be used to renew the APNs certificate, so we strongly recommend using your corporate Apple ID.



6. In the Get Started page, click Create a Certificate.

7. In the *Terms of Use* page, check the **box** next to **I have read and agree to these terms and conditions,** and click **Accept.**



8. In the *Create a New Push Certificate* page, click **Choose File,** and select the **PLIST (plist_encoded) file** that was generated by ADSelfService Plus or emailed by our support team. Click **Upload.**

9. A new push certificate (MDM_ Zoho Corporation_Certificate.pem) will be generated. Click **Download,** and save the **file.**

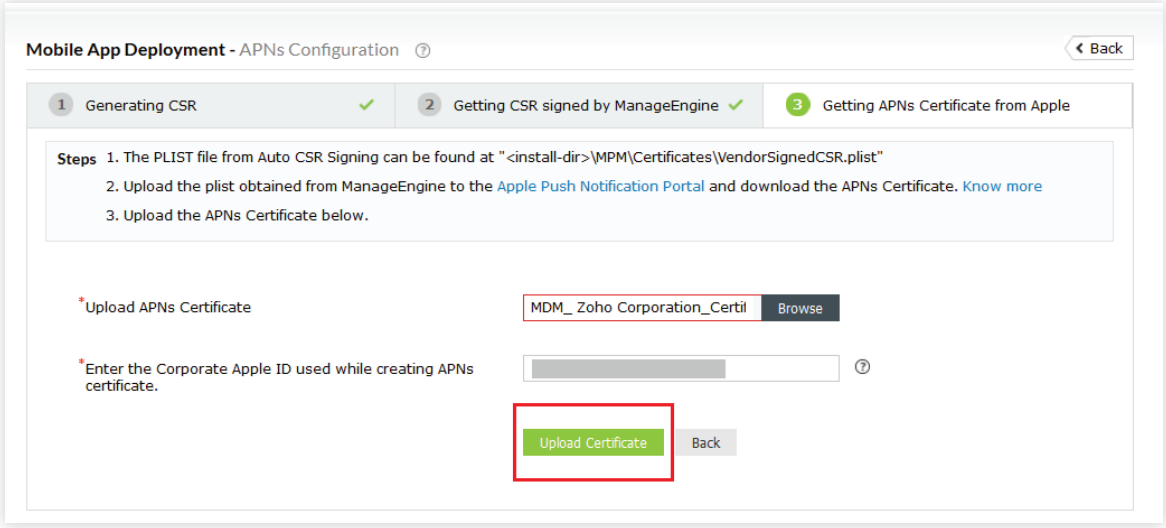
Upload the PEM file to the product

10. Now, switch back to the **Mobile App Deployment** page in *ADSelfService Plus.*

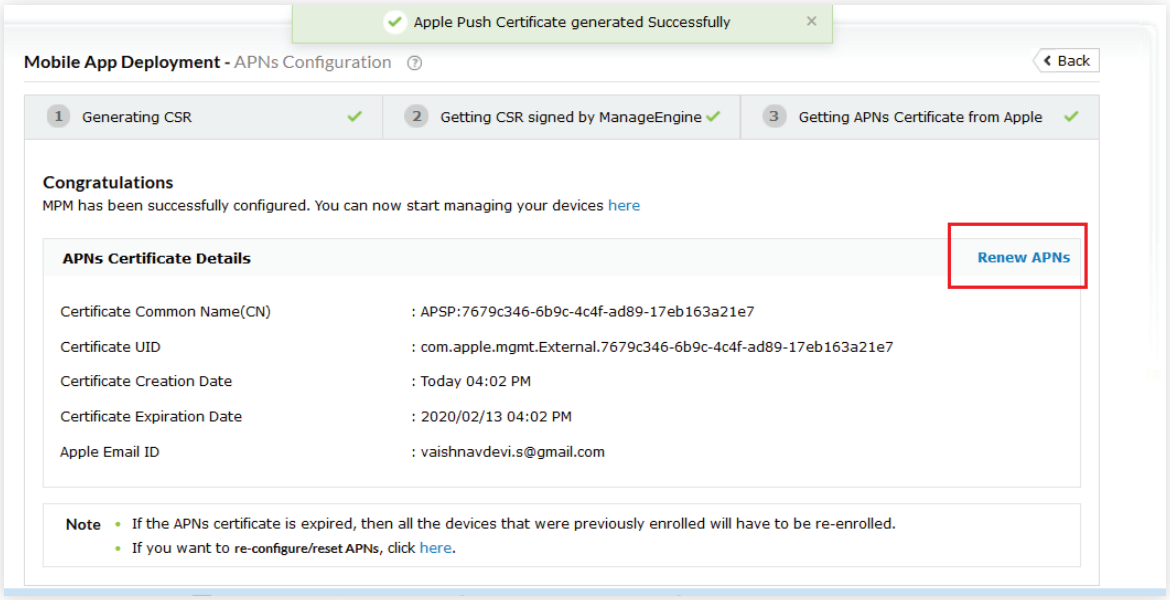
11. Click **Browse,** and upload the **APNs certificate.**

12. Enter the corporate **Apple ID** you used while creating the APNs certificate.

13. Click **Upload Certificate.**



14. You have now successfully completed the MPM configuration. You can use the **Renew APNs** option to renew APNs certificates before they expire.



How to renew the APNs

The APNs certificates sent by Apple expire after one year. Once expired, all the mobile devices that were previously enrolled will be unenrolled, and you will have to re-enroll them once you renew the APNs certificate. Follow the steps below to renew APNs certificates before they expire, and avoid the hassle of re-enrolling all your devices:

- Click **Renew APNs.** A new PLIST file is generated under the folder: **<install-dir>\ ADSelfService Plus\MPM\Certificates\renew.**
- Log in to the **Apple Push Certificate Portal,** click **Renew,** and upload the **PLIST file** to generate a PEM file. Download the generated **PEM file.**
- Now switch back to ADSelfService Plus, and **Upload** the downloaded **PEM file.**

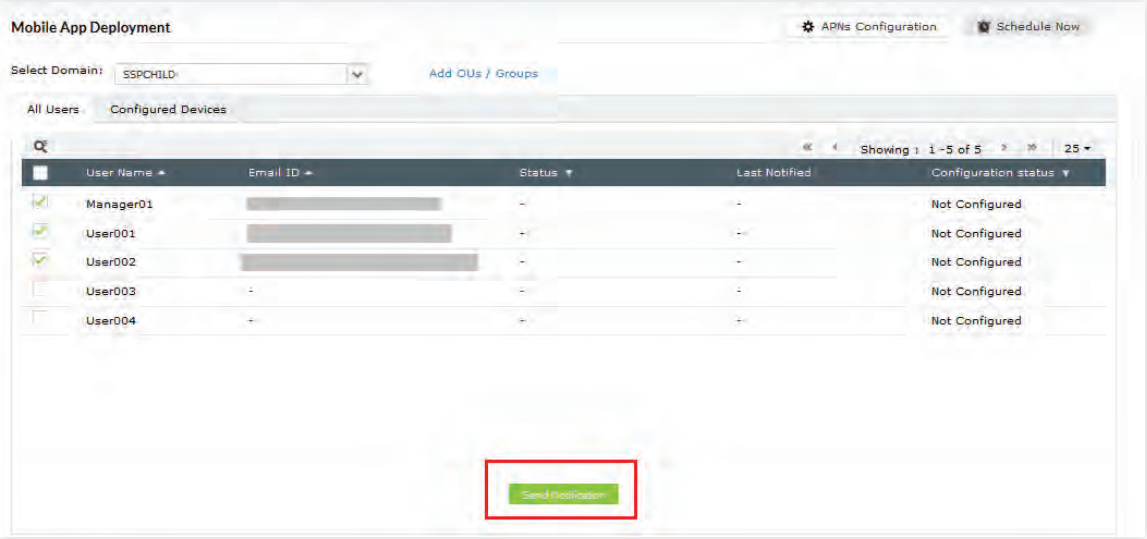
Note: If you ever change the SSL certificate used in ADSelfService Plus or the context path used in the access URL, you need to redo the steps starting at Step 2: APNs configuration for the mobile app deployment feature to continue working. Use the **reset option** available in the Note section to reconfigure APNs settings.

Step 3: Installing the MDM profile

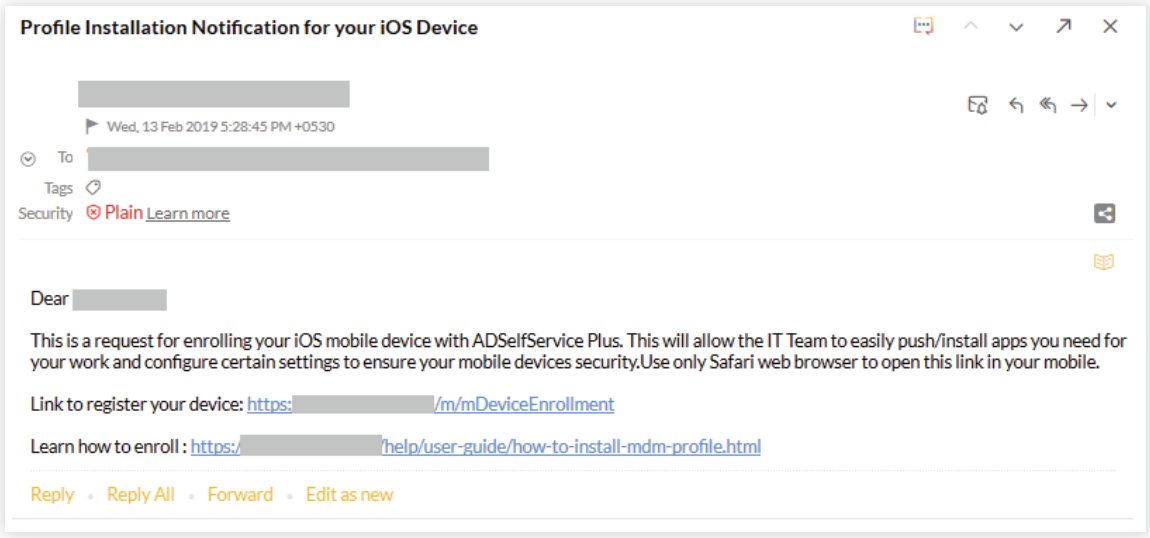
If you want to move out of trial mode or if your APNs configuration is complete, a mobile device management (MDM) profile must be installed in users' mobile devices. Only then will you be able to install the ADSelfService Plus app remotely using the Mobile App Deployment option.

Notify users to install MPM profiles in their devices

1. Open **ADSelfService Plus** and go to **Configuration > Administrative Tools > Mobile App Deployment.**
2. Select a **domain** from the *Select Domain* drop-down menu.
3. Click **Add OUs/Groups** if you want to select specific users.
4. All the users from the selected OUs and groups in the domain will be displayed under the *All Users* tab.
5. Select the desired users by checking the **box** beside their usernames.
6. Click **Send Notification.**



7. Users will receive an **email** containing the **registration link.** If you're configuring the trial mode of mobile app deployment, then a one-time password (OTP) will be sent along with the registration link. The browser will ask for this OTP in the following step as well when users open the registration link.



8. Users need to open the link in a **Safari browser** to install the profile and successfully enroll their devices for MDM.

Note:

i) The link must be opened in a Safari browser only.

ii) The ADSelfService Plus server should be accessible to the iOS devices during profile installation.

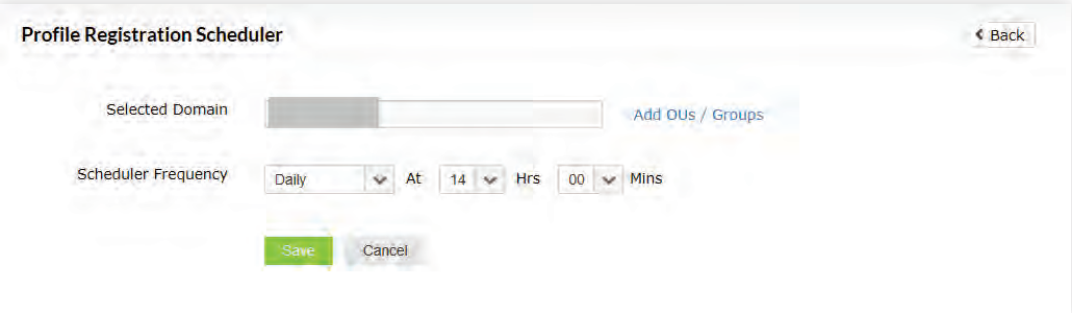
Step 4: Installing the ADSelfService Plus app

- Mobile devices in which the profile has been successfully installed will appear under the *Configured Devices* tab.
- Select the **devices** in which you want to install the ADSelfService Plus app, and click **Install.**
- Click **Update Status** to get details on the status of app installation in configured devices. It will take some time before the status is updated.
- Click the **Status** column to view the devices based on app installation status. You can choose from: installed, not installed, uninstalled, queued, cancelled, failed, and all.

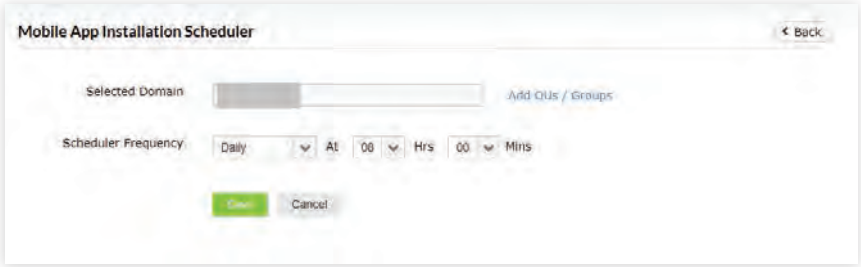
Setting up schedulers to automate profile and app installation

You don't have to manually notify new users to install the MDM profile or install the app in end users' new devices. You can automate the whole process by setting up schedulers to periodically check for new users and devices. Follow the steps below to configure the schedulers:

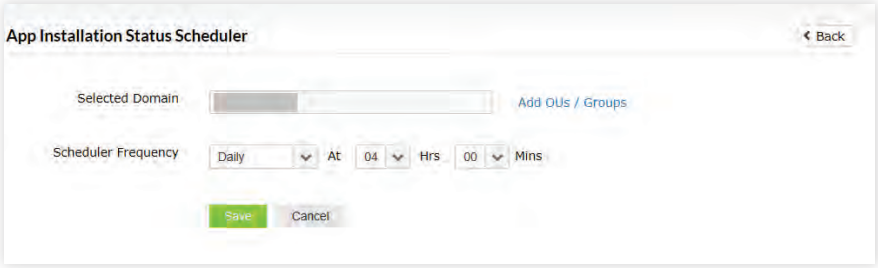
- Open **ADSelfService Plus** and go to **Configuration > Administrative Tools > Mobile App Deployment.**
- Click **Schedule Now.**
- You will be presented with three schedulers.
    - Profile Registration Scheduler: Automatically send notifications to users asking them to install the MDM profile.



    - **App Installation Scheduler:** Automatically install the ADSelfService Plus app in profile-installed devices.



- **App Installation Status Scheduler:** Automatically update the status of app installations for each device in the ADSelfService Plus web console.



- You can **Enable/Disable** schedulers.
- Click **Edit,** if you want to make any changes.
- Select the **Domain.** Click **Add OUs/Groups** link to further narrow down your selection.

  Select the **Scheduler Frequency** to specify the frequency at which the scheduler should be run.

  Click **Save.**