


Securing Mobile Device App Data Using Managed Apps and the Casper Suite

Technical Paper
Casper Suite v9.1 or Later
15 October 2013



 JAMF Software, LLC
© 2013 JAMF Software, LLC. All rights reserved.

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

JAMF Software
301 4th Ave S Suite 1075
Minneapolis, MN 55415-1039
(612) 605-6625

Apple, the Apple logo, and Safari 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

The Casper Suite, JAMF Software, the JAMF Software logo, and the JAMF Software Server (JSS) are trademarks of JAMF Software, LLC, registered in the United States and other countries.

All other product and service names mentioned are the trademarks of their respective companies.

Contents

Page 4	Introduction What's in This Guide Important Concepts Additional Resources
Page 5	Overview
Page 6	Requirements
Page 7	Securing Data in Transit Adding a Managed App to the JSS Creating a Smart Mobile Device Group Creating an iOS Configuration Profile with a Per-App VPN Connection Mapping the Managed App to the Per-App VPN Connection
Page 13	Securing Data at Rest Adding a Managed App to the JSS Creating a Smart Mobile Device Group Creating an iOS Configuration Profile with Restrictions Settings
Page 16	Accessing Secure Data Creating a Smart Mobile Device Group Creating an iOS Configuration Profile with Single Sign-on Settings

Introduction

What's in This Guide

This guide provides step-by-step instructions on how to secure mobile device app data using managed apps and the Casper Suite.

Important Concepts

Before you can secure mobile device app data using managed apps and the Casper Suite, you should be familiar with the concepts of managed apps. For more information, see "Understanding Unmanaged and Managed Apps" in the *Casper Suite Administrator's Guide*.

In addition, you should have a basic understanding of how smart mobile device groups work. For more information, see "Smart Mobile Device Groups" in the *Casper Suite Administrator's Guide*.

Additional Resources

For more information on related topics, see the *Casper Suite Administrator's Guide*, available at: <http://jamfsoftware.com/product-documentation/administrators-guides>

Overview

The release of iOS 7 introduces new features for the security of mobile device app data. The Casper Suite allows you to take full advantage of these new features.

This paper provides complete workflows for securing the following types of mobile device app data:

- **Data in Transit**—When a managed app connects to the internet or when a user accesses secure information in a managed app, the data is in transit on the mobile device using the internet.
- **Data at Rest**—This is data that resides on the device itself within a managed app, and is accessible even when a device is not connected to the Internet.

Additionally, this paper provides a complete workflow for how to allow users and mobile devices access to this data. This provides an additional layer of security and a seamless experience for the user.

Requirements

To secure mobile device app data using the instructions in this guide, you need:

- The JSS v9.1 or later
- Target mobile devices with iOS 7 or later

Securing Data in Transit

If a managed app requires an internet connection, you can ensure that it will connect to the internet using a specified Per-App VPN connection.

Securing data in transit involves the following steps:

1. Add a managed app to the JSS.
2. Create a smart mobile device group.
3. Create an iOS configuration profile with a Per-App VPN connection.
4. Map the managed app to the Per-App VPN connection.


Adding a Managed App to the JSS

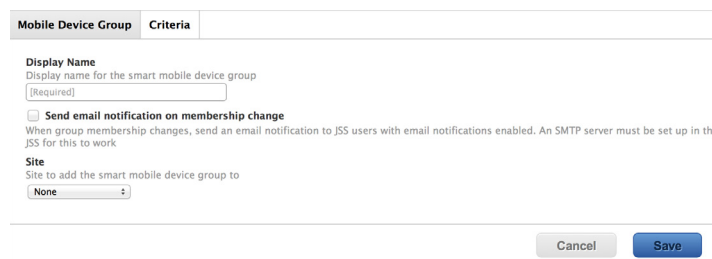
The first step to securing data in transit is to add a managed app to the JSS. This app should be the app for which you want to secure data. For instructions on adding apps to the JSS, see “In-House Apps” or “App Store Apps” in the *Casper Suite Administrator’s Guide*, available at:

<http://jamfsoftware.com/product-documentation/administrators-guides>

Creating a Smart Mobile Device Group

Create a smart mobile device group based on the managed app so you can use the group as the scope of the configuration profile.



1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. Use the Mobile Device Group pane to configure basic settings for the group.

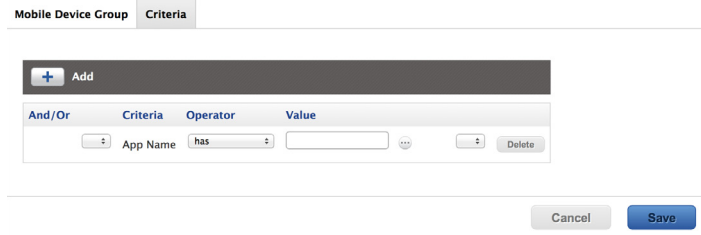


The screenshot shows the 'Mobile Device Group' configuration pane in the JSS interface. It has two tabs: 'Mobile Device Group' and 'Criteria'. The 'Mobile Device Group' tab is active. The form contains the following fields and options:

- Display Name:** A text input field with the placeholder text 'Display name for the smart mobile device group' and a '(Required)' label below it.
- Send email notification on membership change**
When group membership changes, send an email notification to JSS users with email notifications enabled. An SMTP server must be set up in the JSS for this to work.
- Site:** A dropdown menu with the text 'Site to add the smart mobile device group to' and the selected option 'None'.

At the bottom of the pane, there are two buttons: 'Cancel' and 'Save'.

6. Click the **Criteria** tab and add criteria to the group:
 - a. Click **Add**  .
 - b. Click **Choose** for "All Criteria".
 - c. Click **Choose** for "App Name".
 - d. Enter the name of the managed app in the **Value** field or browse for it by clicking **Browse**  .




- e. Choose "has" from the **Operator** pop-up menu.
7. Click **Save**.

Group memberships are updated each time mobile devices contact the JSS and meet or fail to meet the specified criteria.

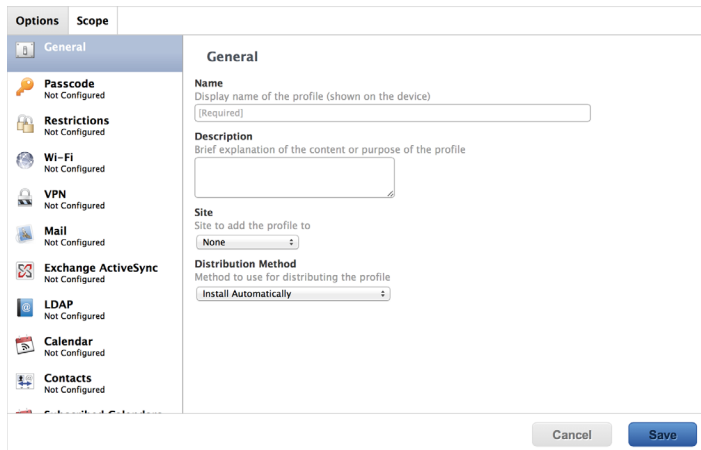
To view the group memberships, click **View**.

Creating an iOS Configuration Profile with a Per-App VPN Connection

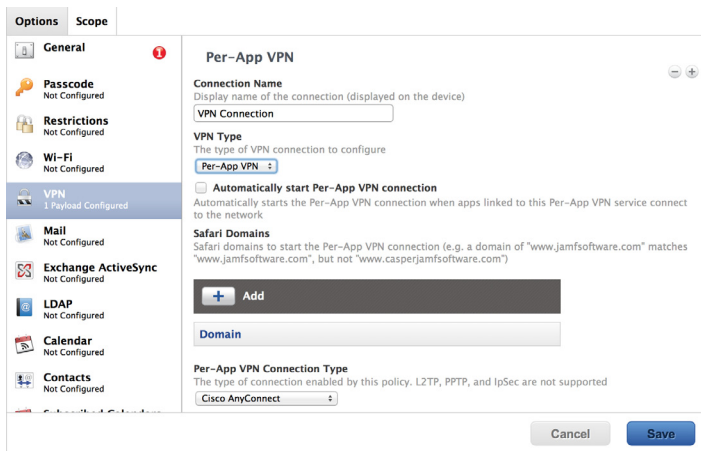
After creating the smart mobile device group, you need to create the Per-App VPN connection. This ensures that when a managed app connects to the internet, it will connect using the Per-App VPN connection.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
On a smartphone, this is in the pop-up menu.
4. Click **New**  .


5. Use the General payload to configure basic settings for the profile, including a display name.

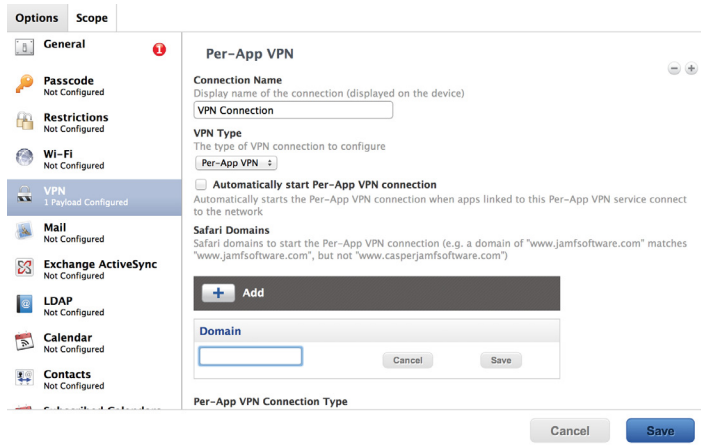



6. Choose "Install Automatically" from the **Distribution Method** pop-up menu.
7. Select the VPN payload, and then click **Configure**.
8. Enter a name for the Per-App VPN connection in the **Connection Name** field.
9. Choose "Per-App VPN" from the **VPN Type** pop-up menu.

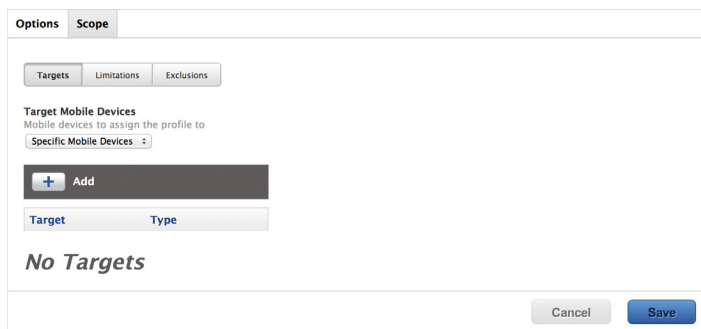


10. Select the **Automatically start Per-App VPN connection** checkbox.

11. To limit the websites that users can browse over the VPN connection, click **Add**  and then list the Safari domains.



12. Choose the type of Per-App VPN connection from the **Per-App VPN Connection Type** pop-up menu.
13. On the **Scope** pane, configure the scope:
 - a. Choose "Specific Mobile Devices" from the **Target Mobile Devices** pop-up menu.
 - b. Click **Add** .



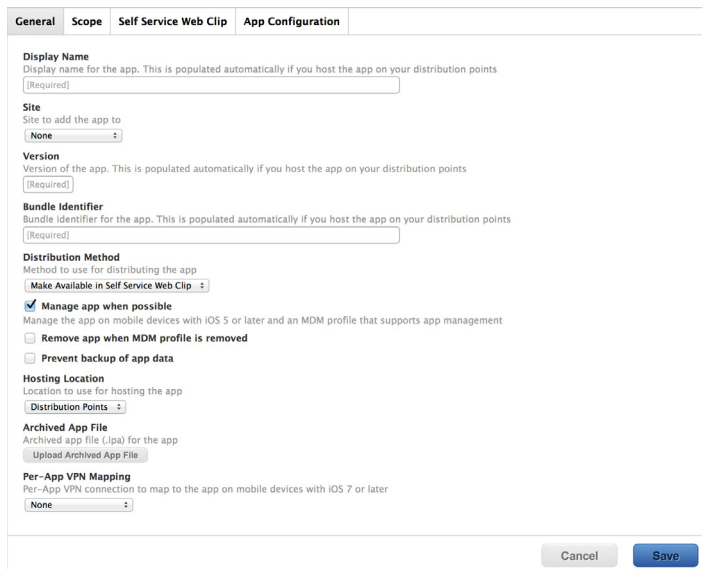
- c. Click the **Mobile Device Groups** tab.
 - d. Click **Add** next to the smart mobile device group that you previously created.
 - e. Click **Done**.
14. Click **Save**.

The mobile devices you added are displayed in a list.

Mapping a Managed App to the Per-App VPN Connection

After configuring the Per-App VPN connection, you need to map the managed app to the connection. Anytime the managed app requires an internet connection it will connect to the internet using the Per-App VPN connection.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Apps**.
On a smartphone, this is in the pop-up menu.
4. Click the managed app you want to map the Per-App VPN connection to.
5. Click **Edit**.
6. Ensure that the **Manage app when possible** checkbox is selected.




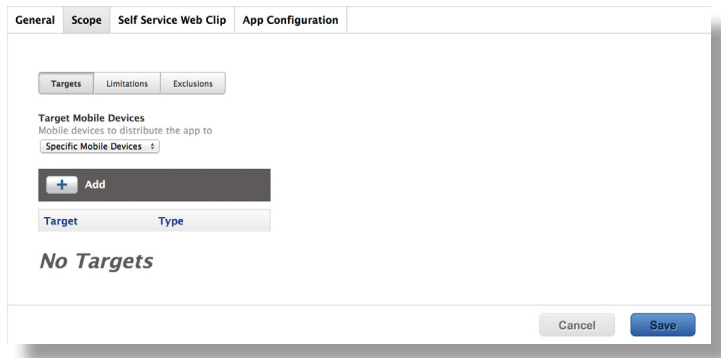
The screenshot shows the 'App Configuration' dialog box with the following sections:

- Display Name:** Text input field with a '(Required)' label.
- Site:** Dropdown menu with 'None' selected.
- Version:** Text input field with a '(Required)' label.
- Bundle Identifier:** Text input field with a '(Required)' label.
- Distribution Method:** Dropdown menu with 'Make Available in Self Service Web Clip' selected.
- Manage app when possible:** Checked checkbox.
- Remove app when MDM profile is removed:** Unchecked checkbox.
- Prevent backup of app data:** Unchecked checkbox.
- Hosting Location:** Dropdown menu with 'Distribution Points' selected.
- Archived App File:** Text input field with an 'Upload Archived App File' button.
- Per-App VPN Mapping:** Dropdown menu with 'None' selected.

Buttons for 'Cancel' and 'Save' are located at the bottom right of the dialog.

7. From the **Per-App VPN Mapping** pop-up menu, select the Per-App VPN connection that you want the managed app to connect over.

8. On the Scope pane, configure the scope:
 - a. Choose "Specific Mobile Devices" from the **Target Mobile Devices** pop-up menu.
 - b. Click **Add**  .



- c. Click the **Mobile Device Groups** tab.
 - d. Click **Add** next to the smart mobile device group that you previously created.
 - e. Click **Done**.
9. Click **Save**.

The app is distributed to mobile devices in the scope the next time they contact the JSS.

The next time the managed app requires an internet connection, it will connect to the internet using the specified Per-App VPN connection.

Securing Data at Rest

You can keep data secure by containing it in a managed app and creating restrictions settings using an iOS configuration profile.

Securing data at rest involves the following steps:

1. Add a managed app to the JSS.
2. Create a smart mobile device group.
3. Create an iOS configuration profile with restrictions settings.


Adding a Managed App to the JSS

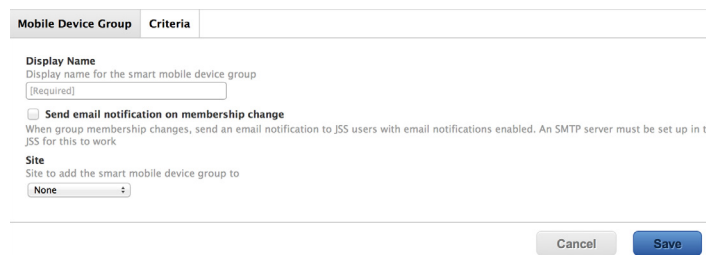
The first step to securing data at rest is to add a managed app to the JSS. This app should be the app for which you want to secure data. For instructions on adding apps to the JSS, see “In-House Apps” or “App Store Apps” in the *Casper Suite Administrator’s Guide*, available at:

<http://jamfsoftware.com/product-documentation/administrators-guides>

Creating a Smart Mobile Device Group

Create a smart mobile device group based on the managed app so you can assign the group as the scope of the configuration profile.



1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. Use the Mobile Device Group pane to configure basic settings for the group.

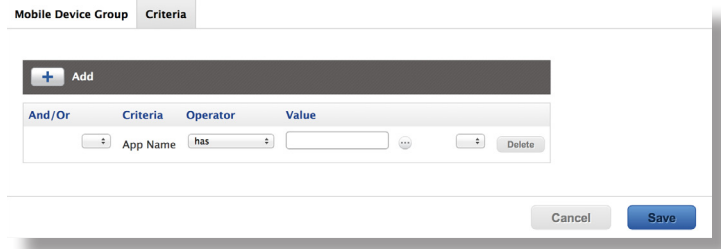


The screenshot shows the 'Mobile Device Group' configuration pane in the JSS interface. It has two tabs: 'Mobile Device Group' (selected) and 'Criteria'. The 'Mobile Device Group' tab contains the following fields and options:

- Display Name**: A text input field with the placeholder text 'Display name for the smart mobile device group' and a '(Required)' label.
- Send email notification on membership change**: A checkbox with a label. Below it is a small note: 'When group membership changes, send an email notification to JSS users with email notifications enabled. An SMTP server must be set up in the JSS for this to work.'
- Site**: A dropdown menu with the text 'Site to add the smart mobile device group to' and a selected option of 'None'.

At the bottom right of the pane are two buttons: 'Cancel' and 'Save'.

6. Click the **Criteria** tab and add criteria to the group:
 - a. Click **Add**  .
 - b. Click **Choose** for "All Criteria".
 - c. Click **Choose** for "App Name".
 - d. Enter the name of the managed app in the **Value** field or browse for it by clicking **Browse**  .




- e. Choose "has" from the **Operator** pop-up menu.
7. Click **Save**.

Group memberships are updated each time mobile devices contact the JSS and meet or fail to meet the specified criteria.

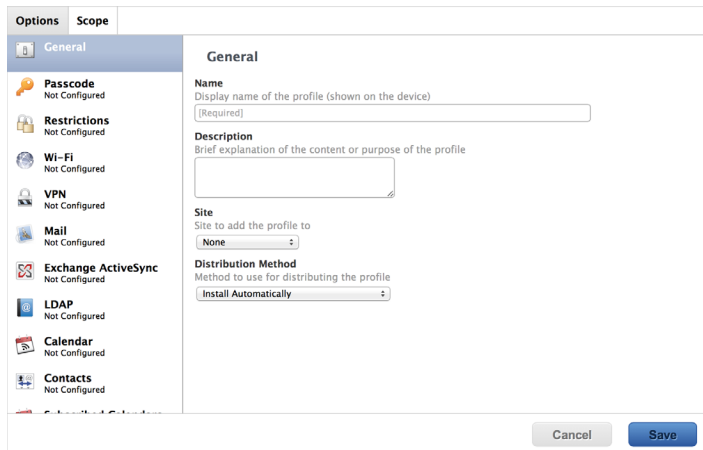
To view the group memberships, click **View**.


Creating an iOS Configuration Profile with Restrictions Settings

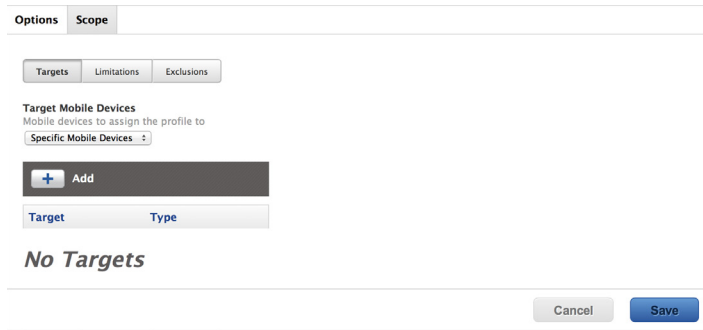
After creating the smart mobile device group, you need to create an iOS configuration profile with restrictions settings. This ensures that secure data is kept contained within the managed app.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
On a smartphone, this is in the pop-up menu.
4. Click **New**  .

5. Use the General payload to configure basic settings for the profile, including a display name.



6. Choose "Install Automatically" from the **Distribution Method** pop-up menu.
7. Select the Restrictions payload, and then click **Configure**.
8. On the **Functionality** tab, deselect the following checkboxes:
 - **Allow documents from managed apps in unmanaged apps**
 - **Allow documents from unmanaged apps in managed apps**
9. On the Scope pane, configure the scope:
 - a. Choose "Specific Mobile Devices" from the **Target Mobile Devices** pop-up menu.
 - b. Click **Add**  .



- c. Click the **Mobile Device Groups** tab.
 - d. Click **Add** next to the smart mobile device group that you previously created.
 - e. Click **Done**.
10. Click **Save**.

The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Users will only be able to access secure data in the managed app. Additionally, they will not be able to access unmanaged app data in a managed app

Accessing Secure Data


You can specify credentials that can be used to access apps and websites that contain secure data using an iOS configuration profile with Single Sign-on settings. This allows you to grant users and mobile devices access to websites and apps that contain the secure data.

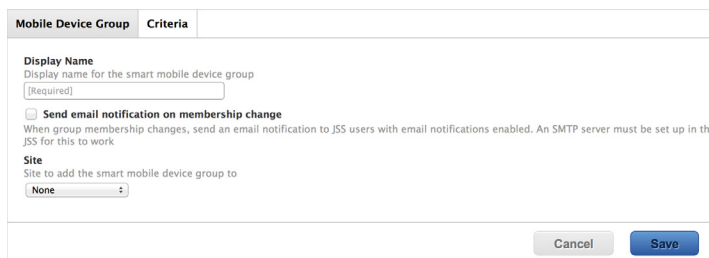
Accessing secure data involves the following steps:

1. Create a smart mobile device group.
2. Configure an iOS configuration profile with Single Sign-on settings.

Creating a Smart Mobile Device Group

The first step to allowing access to secure data is to create a smart mobile device group based on the users or mobile devices that you want to grant access to secure data. You can then assign the group as the scope of the configuration profile.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Smart Mobile Device Groups**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .
5. Use the Mobile Device Group pane to configure basic settings for the group.




Mobile Device Group **Criteria**


Display Name
Display name for the smart mobile device group
(Required)

Send email notification on membership change
When group membership changes, send an email notification to JSS users with email notifications enabled. An SMTP server must be set up in the JSS for this to work.

Site
Site to add the smart mobile device group to
None

Cancel Save

6. Click the **Criteria** tab and add criteria to the group:
 - a. Click **Add** .
 - b. Click **Choose** for the criteria you want to add.
To display additional criteria, click **Choose** for "Other Criteria".

- c. Choose an operator from the **Operator** pop-up menu.
 - d. Enter a value in the **Value** field or browse for a value by clicking **Browse** .
 - e. Repeat steps a through d to add criteria as needed.
7. Choose an operator from the **And/Or** pop-up menu(s) to specify the relationships between criteria.
 8. To group criteria and join multiple operations, choose parentheses from the pop-up menus around the criteria you want to group.

9. Click **Save**.


Operations in the group take place in the order they are listed (top to bottom).

Group memberships are updated each time mobile devices contact the JSS and meet or fail to meet the specified criteria.

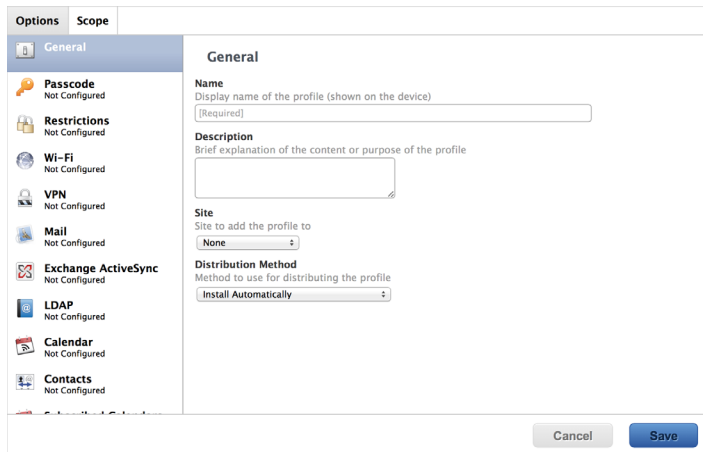
To view the group memberships, click **View**.






Configuring an iOS Configuration Profile with Single Sign-on Settings

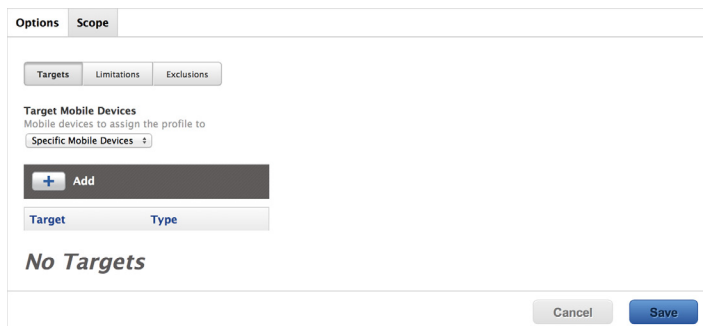
After creating the smart mobile device group, you need to configure the Single Sign-on settings. This ensures that specific users or mobile devices have access to secure data.

1. Log in to the JSS with a web browser.
2. Click **Mobile Devices** at the top of the page.
3. Click **Configuration Profiles**.
On a smartphone, this option is in the pop-up menu.
4. Click **New** .

5. Use the General payload to configure basic settings for the profile, including a display name.



6. Choose “Install Automatically” from the **Distribution Method** pop-up menu.
7. Select the Single Sign-On payload, and then click **Configure**.
8. Enter the required information where necessary.
9. If you want to limit the websites that users can access, select the **Limit this account to specific URL patterns**, and then click **Add**  .
10. If you want to limit the applications that users can access, select the **Limit this account to specific applications**, and then click **Add**  .
You can browse for an app by clicking **Browse**  , or limit the search by entering an app name in the **Bundle ID** field and then clicking **Browse**  .
11. On the Scope pane, configure the scope:
 - a. Choose “Specific Mobile Devices” from the **Target Mobile Devices** pop-up menu.
 - b. Click **Add**  .



- c. Click the **Mobile Device Groups** tab.
- d. Click **Add** next to the smart mobile device group that you previously created.
- e. Click **Done**.

12. Click **Save**.

The profile is distributed to mobile devices in the scope the next time they contact the JSS.

Users can access the secure data based on the credentials that you defined for the apps or websites. This provides a seamless experience for the user.