

# IP Whitelisting for FormAssembly within Salesforce & Salesforce Marketing Cloud (ExactTarget)

Download the PDF of this article.

## In this Article

### Related Articles

## Introduction

When working with FormAssembly connectors, there may be times when you need to whitelist FormAssembly IP addresses in order to be able to receive information being passed from FormAssembly. In those cases, please whitelist the IP addresses listed below.

---

## IP Addresses for Whitelisting

When entering Salesforce Trusted IPs, it is required to add a start and end IP. You will enter the same IP for the start and end IPs. All plans have 2 Trusted IPs to enter per the chart below. These IPs are for customers whose instance are hosted **inside the US**.

FormAssembly Offering	Primary IP	Recovery IP
Pro & Premier accounts	34.230.105.243	18.221.37.214
Enterprise Cloud	34.231.230.11	18.217.15.195
Compliance Cloud	35.169.15.41	18.217.101.3

Please refer to the list below for customers whose instances are hosted **outside the US**.

### Frankfurt

18.196.248.135

### Paris

15.188.178.68

### London

52.56.159.99

## Singapore

13.229.172.189

## Sydney

13.210.101.251

## Montreal

52.60.131.5

---

## IP Whitelisting in Salesforce Marketing Cloud

If you are running into errors when trying to validate your Client ID and Client Secret with the Salesforce Marketing Cloud Connector, you may need to ensure that FormAssembly's IP addresses have been whitelisted within your Marketing Cloud Setup.

An example of such an error would be:

Unable to validate App Keys(ClientID/ClientSecret) provided.: Unable to validate App Keys(ClientID/ClientSecret) provided, requestToken response:  
{ "message": "Unauthorized", "errorcode": 1, "documentation": "" }

To resolve this, please ask your Salesforce Marketing Cloud administrator to follow the steps below.

---

### 1. Check your IP Whitelist Settings

Once your Salesforce Marketing Cloud administrator has logged into their account, they will need to navigate to **Admin** → **Account Settings** → **Security Settings**.

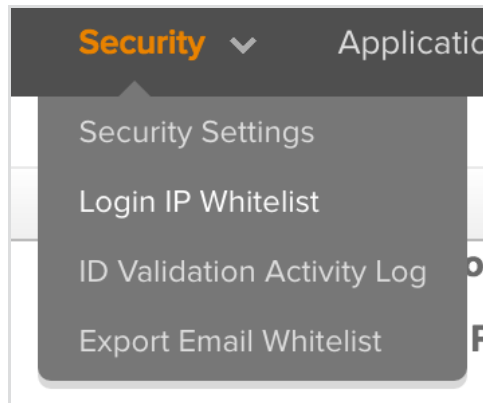
Once there, they should look under **Username and Logins** to see if "Restrict Logins by IP Address (IP Whitelisting)" is disabled.

Username and Logins	
Login Expires After Inactivity	never expires
Invalid Logins Before Lockout	3
Count Invalid Logins Across Sessions	Yes
Minimum Username Length	6 characters
<b>Restrict Logins by IP Address (IP Whitelisting)</b>	IP Whitelisting Disabled

If this feature is enabled, then you will need to add FormAssembly's IP address ranges to that list.

## 2. Update your IP Login Whitelist

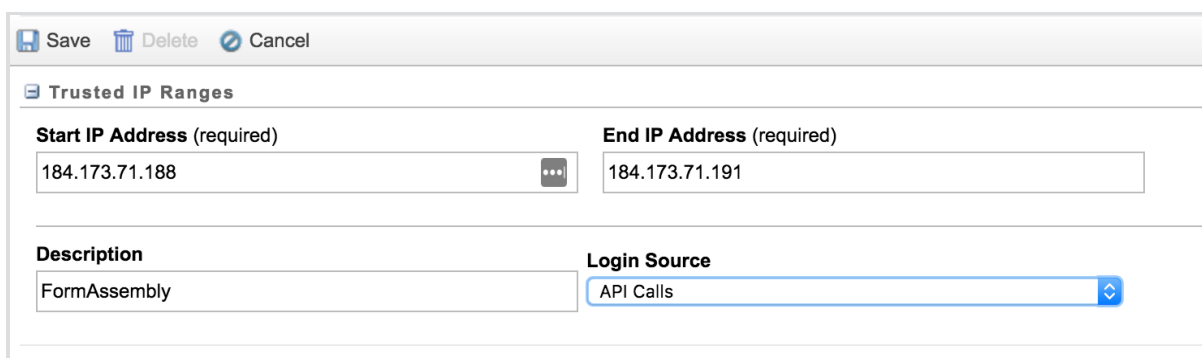
In order to add FormAssembly's IP ranges to your whitelist, you will need to navigate to **Security** → **Login IP Whitelist**.



Click on **Create** at the top left and enter the start IP address and end IP address from the list below. You will need to enter each IP.

Once you have added the Start and End IP addresses, you can add a **Description** in order to identify that this range is used for FormAssembly. You will also need to select **API Calls** from the Login Source dropdown list.

Make sure to click **Save** after each range you add in.

A screenshot of a web form titled 'Trusted IP Ranges'. At the top, there are buttons for 'Save', 'Delete', and 'Cancel'. The form has two rows of input fields. The first row contains 'Start IP Address (required)' with the value '184.173.71.188' and 'End IP Address (required)' with the value '184.173.71.191'. The second row contains 'Description' with the value 'FormAssembly' and 'Login Source' with a dropdown menu showing 'API Calls'.