Article - Blog Módulo CRM Web Site

Version

This article was created by SAP CDC Former(Gigya) 5.7.x Version

Brief Description

This document has the objective to exemplify how SAP CDC Gigya improve Customer Identity Security using RBA (Risk-Based Authentication). The RBA is a layer of account security that can prevent malicious attacks and hacking attempts on your site.

I hope you enjoy it!!

Author

Cláudio Goulart has been working since 1992 with the implementation of corporate solutions. Since 1999, he began his career with CRM deployments, with the most widely used Market Suites such as Vantive, PeopleSoft and Siebel. And since 2006, it has been active with SAP CRM on Premise (Interaction Center, Services, Sales, Marketing and Middleware with ECC)

Specialist in evaluation, process definition, and adherence of customer needs to SAP S4hana on Premise and Cloud solutions C4Hana.

Extensive knowledge in implementations of SAP S4hana and C4hana solutions in the areas of Call Center, Services, Marketing and Sales.

Experienced integrator of SAP on Premise Solutions (S4Hana CRM) and SAP C4Hana (Sales, Services, Marketing, Qualtrics, SAP CDC Former(Gigya)), using SAP Cloud Platform to integrate S4hana process.

Contact Data

Email: cjsgoulart@gmail.com

Blog: www.modulocrm.com.br

LinkedIn: https://www.linkedin.com/in/cgoulart/

Blog - Módulo CRM
Email: claudio.goulart@modulocrm.com.br   Page 1   **Blog - Módulo CRM**
Site: www.modulocrm.com.br

Article - Blog Módulo CRM Web Site

Content

Blog - Módulo CRM
Email: claudio.goulart@modulocrm.com.br   **Page 2**   **Blog - Módulo CRM**
Site: www.modulocrm.com.br

Article - Blog Módulo CRM Web Site

1. Customization

1.1. Description

RBA (Risk Based Authentication is used to prevent malicious attacks and hacking attempts do your web site. RBA includes two types of rules, Global and Account. Global Rules applies to all login attempts in your site. Account Rules applies to individual Accounts. SAP CDC provides several rules available out of the box, but we will test the connection with **different devices** (Computer and Mobile) using the same User Id.
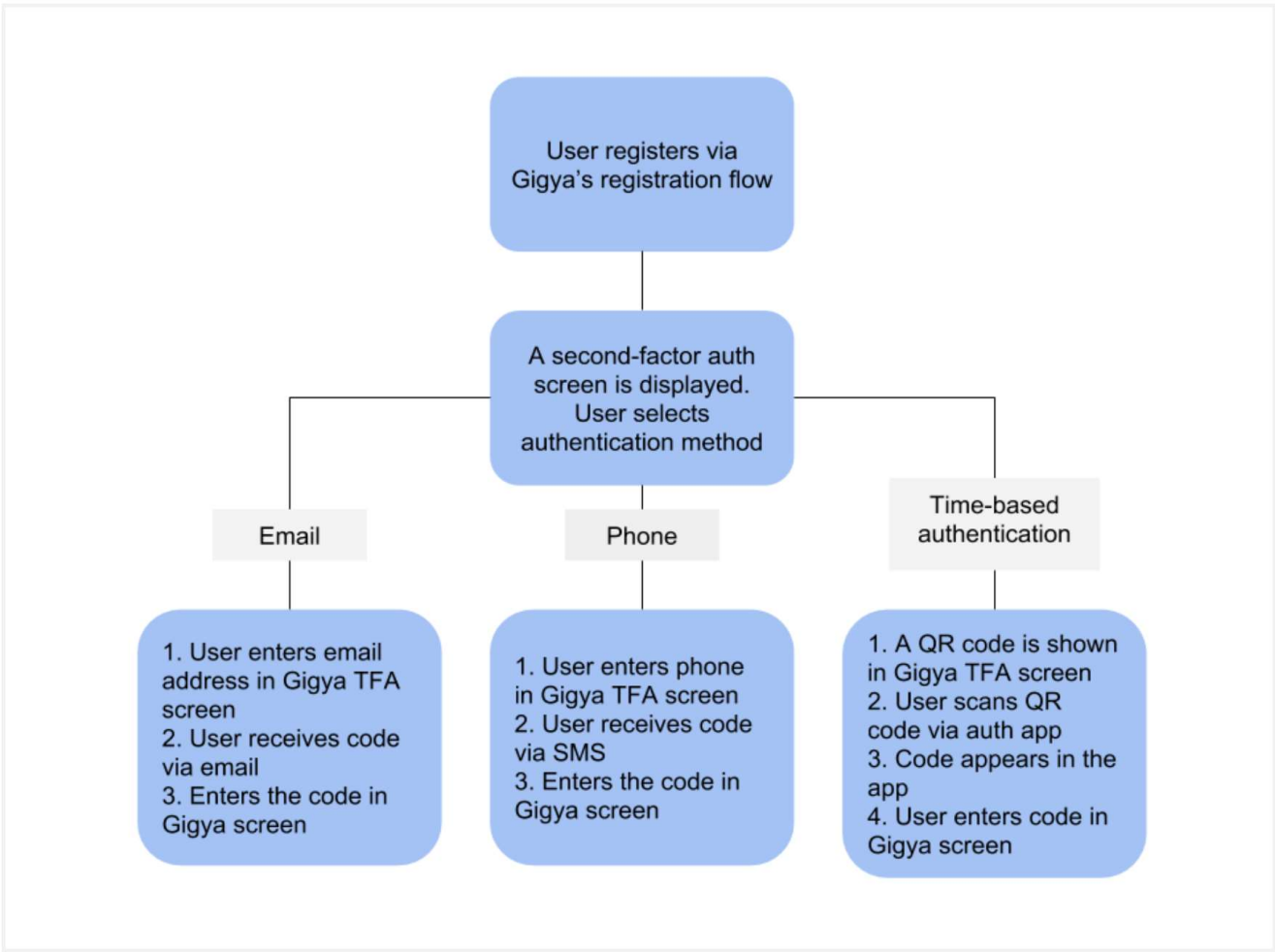
Any of the following events can trigger a requirement for a higher level of authentication:

- Failure to login after a specified number of attempts, from a specific account or IP address.
- Percentage of failed logins, triggered after a specified number of attempts
- New device used for login.
- First login from a different country.

Authentication Method	Authentication Level
Email	10
Phone	20
Time-based authentication (e.g. Google Authenticator), also known as "TOTP"	20
Push TFA (Two-Factor Authentication via mobile device push notification). Note that this method is not used in a registration flow as it requires a user to have an existing session for their second factor authentication. Instead, it is triggered by a third-party app. For more information, see below.	30

Notes:
- A new registration automatically receives an authentication level of 10.
- To be able to authenticate users via their mobile phones, you must set up an account with Twilio / LiveLink, or configure a different provider using Extensions. For more information, see below.
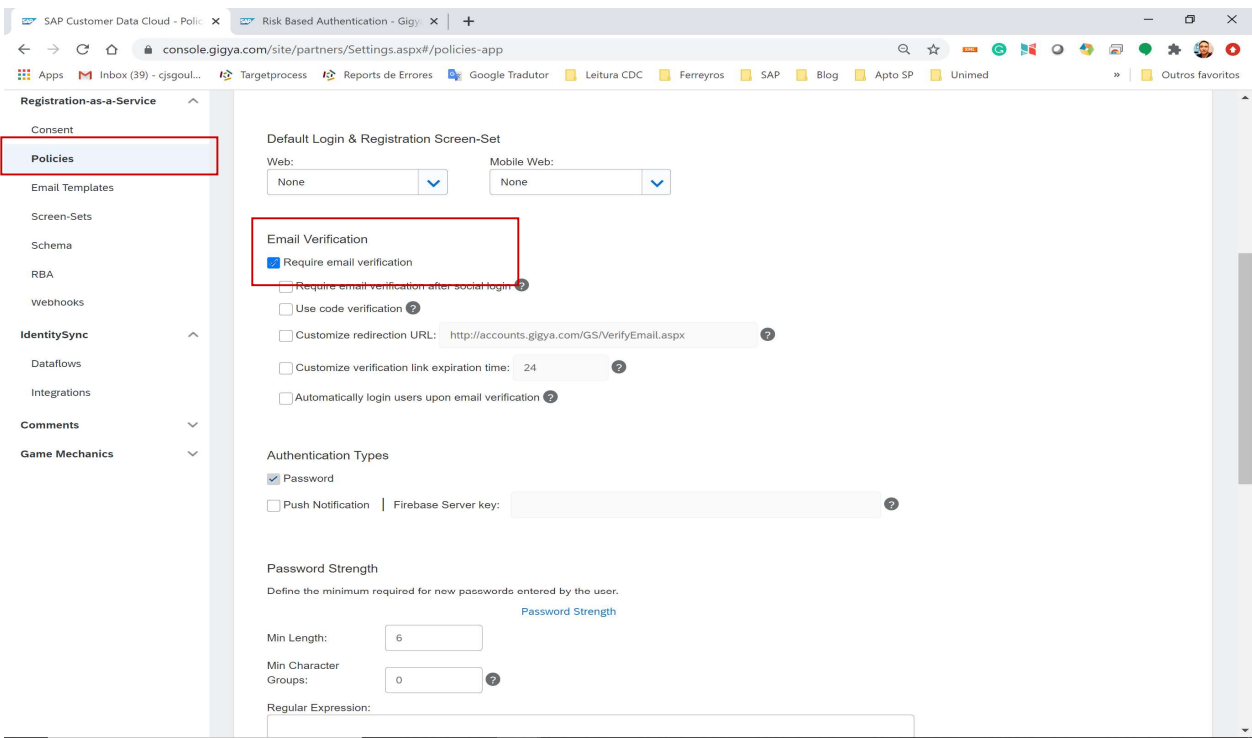

Source Data: https://developers.gigya.com/display/GD/Risk+Based+Authentication

Blog - Módulo CRM
Email: claudio.goulart@modulocrm.com.br   Page 3
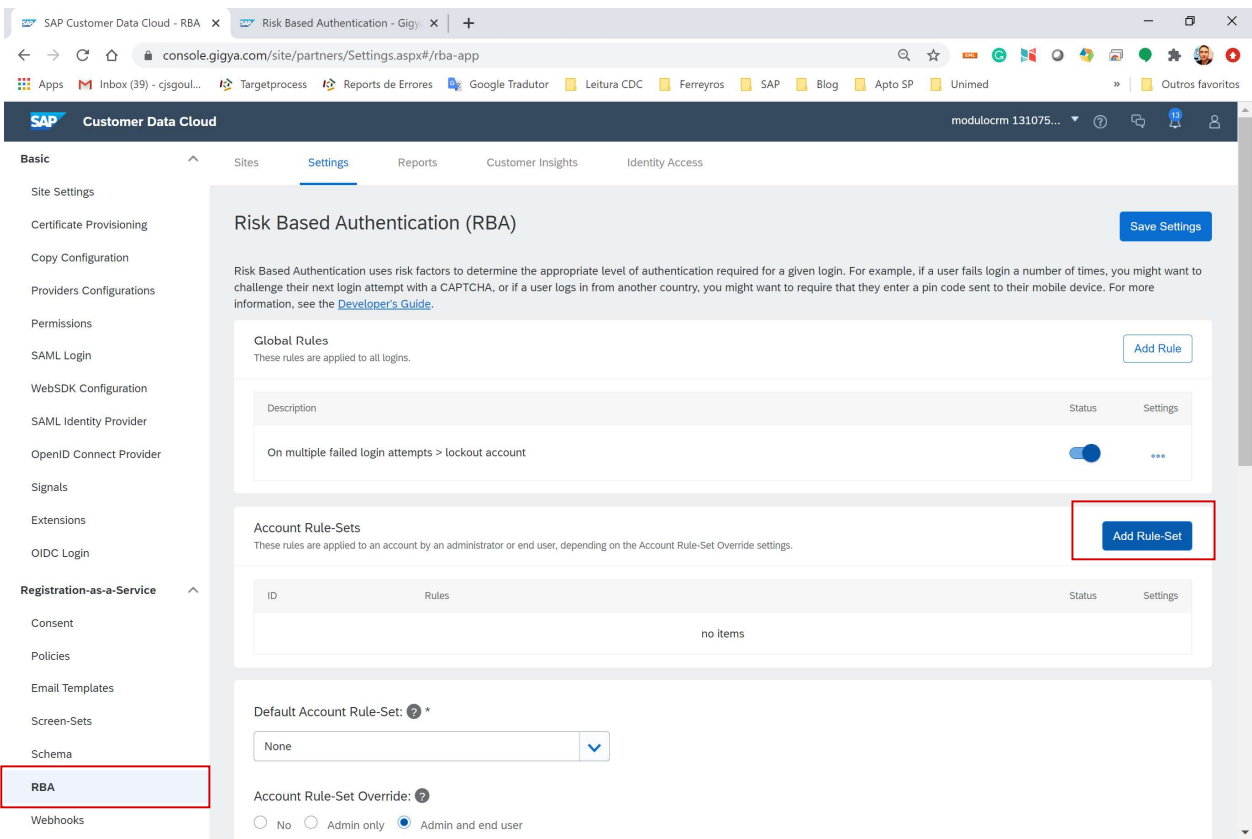Blog - Módulo CRM
Site: www.modulocrm.com.br

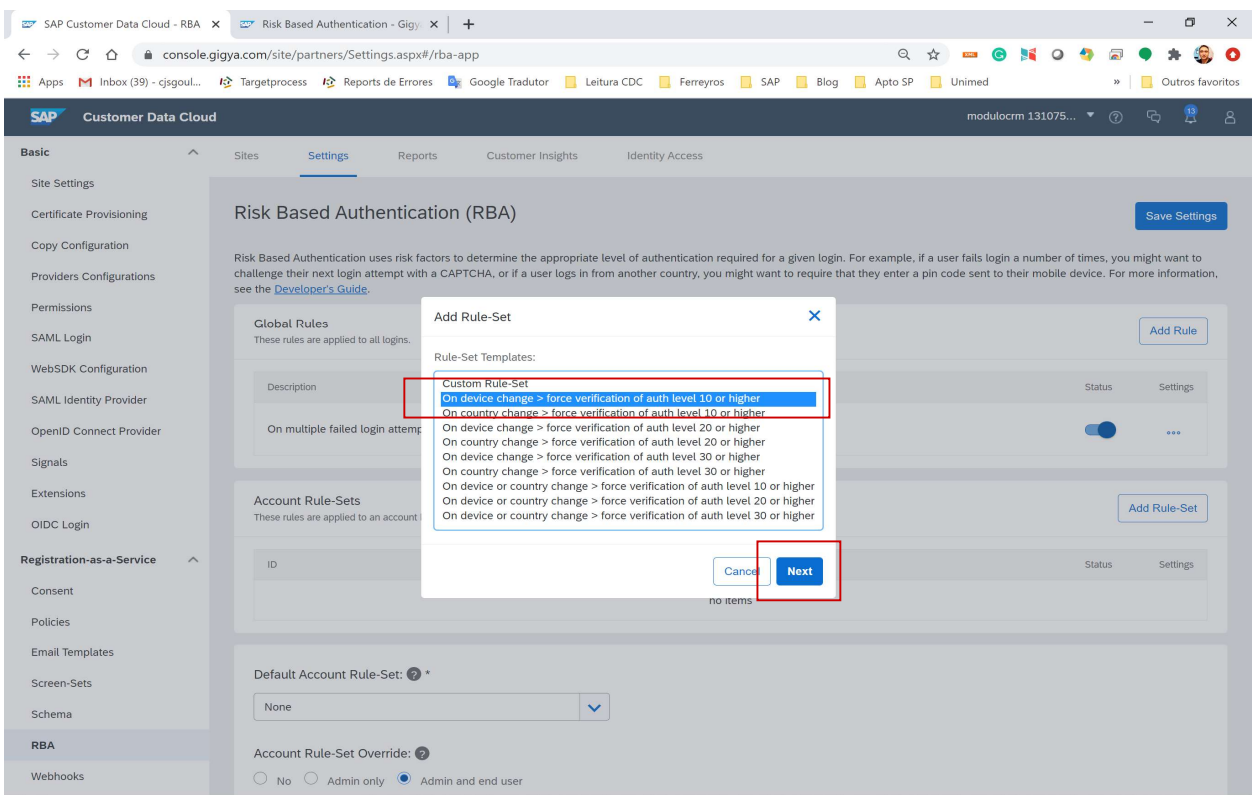# Article - Blog Módulo CRM Web Site

1.2. Customizing

First, into the policies configuration, it is necessary to check the Email Verification. Then save the configuration

Let´s go to the RBA Configuration demonstrated below. I will create our rule clicking in the button "Add Rule-Set" into the Account Rule-Sets.
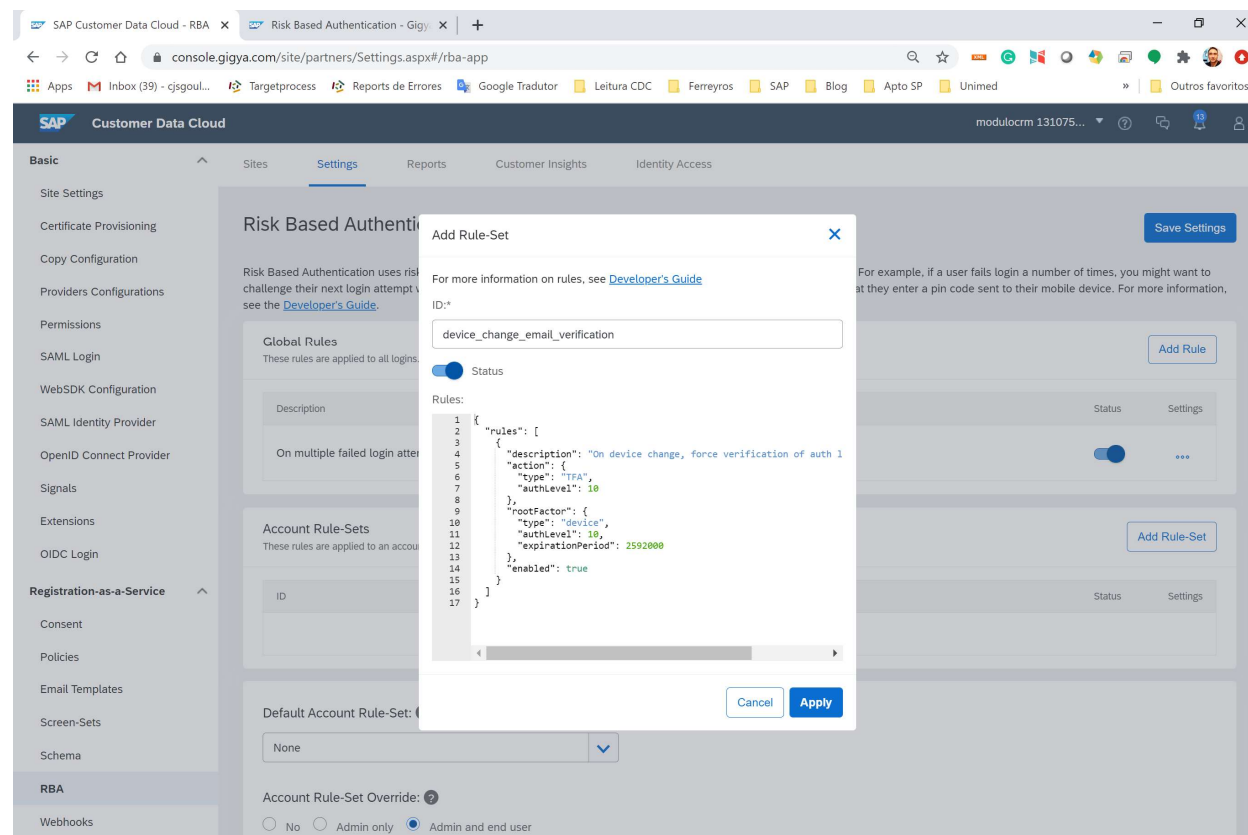

The out-of-the-box rules will be listed, choose the rule "<u>**On Device change > force verification of auth level 10 or higher**</u>", then "Next"
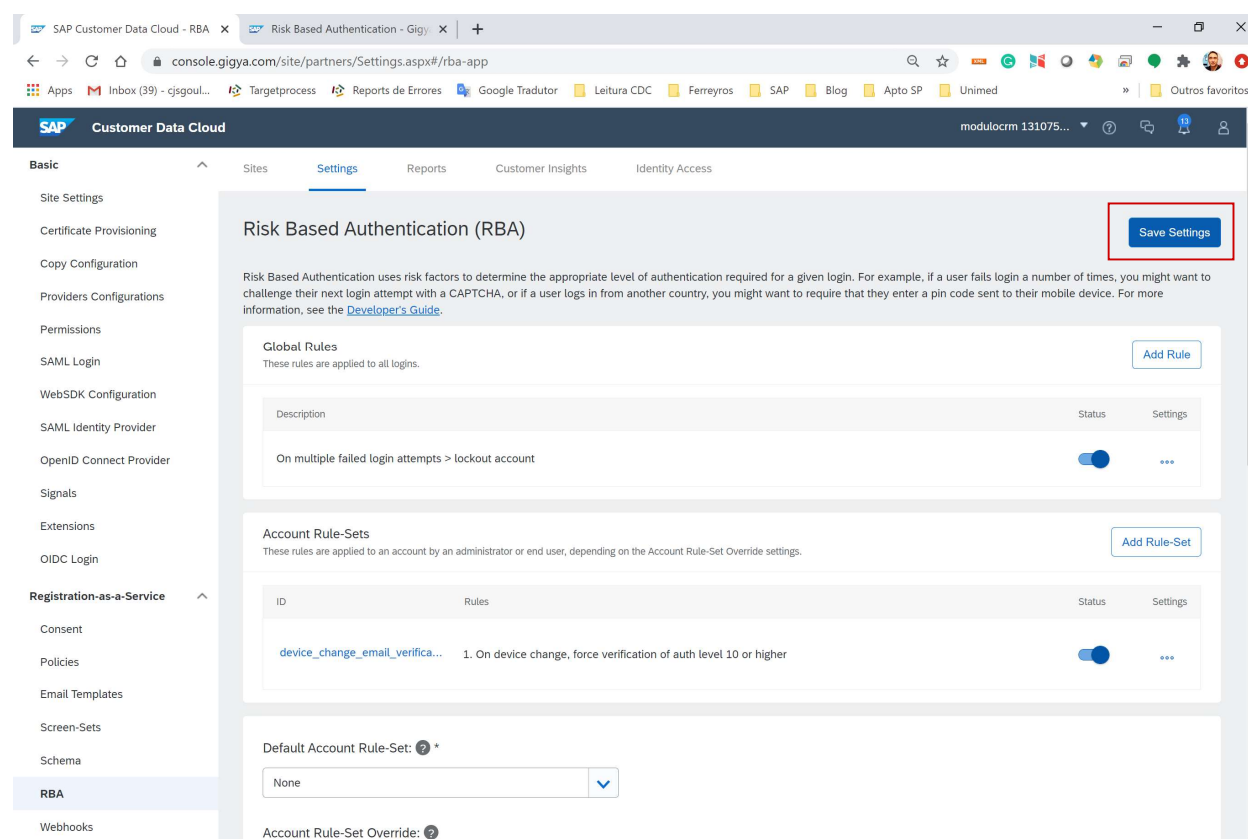
The rule "device_change_email_verification" is created automatically. Just click on the button "Apply".

Save the configuration clicking in the "Save Settings"

In the same RBA configuration, the field "Default Account Rule-Set" choose the rule that we already created, "Device_Change_Email_Verification". Then into the "Account Rule-Set Override" click in the "Admin and end user" option.
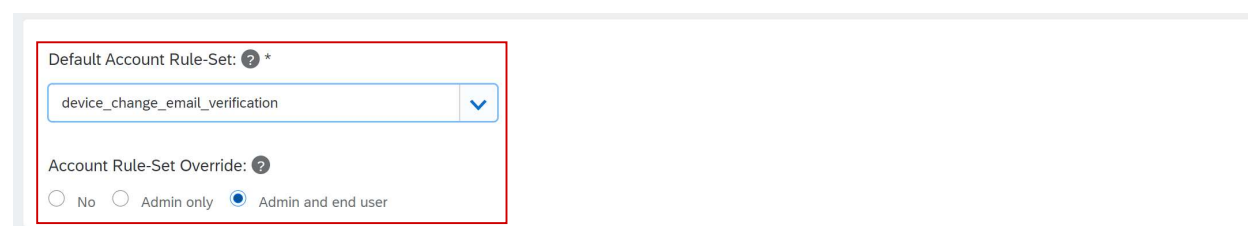
Continue in the RBA Configuration, provide the following information

➢ Auth Level 10 – Email
➢ Auth Level 20 – Authenticator App (Time-Based Authentication)
➢ Application Name (RBAModulo)

Blog - Módulo CRM
Email: claudio.goulart@modulocrm.com.br   **Page 5**   **Blog - Módulo CRM**
Site: www.modulocrm.com.br

1.3. Checking the Identity Access

Into this document, I will register a new user, then before that, I will show to you the Identity Access. There is no user created into the ModuloCRM Site.

1.4. Registering a new User into your Web Site (Computer)

I built a web site which is integrated with SAP CDC. This is the moment to test our configuration. Then, I am accessing my web site using my ==computer== and I will click into the "Register" link.

The Screen-Set Registration appears, then I will provide my email, name, and password. I will agree with the consents and click the button "Submit"
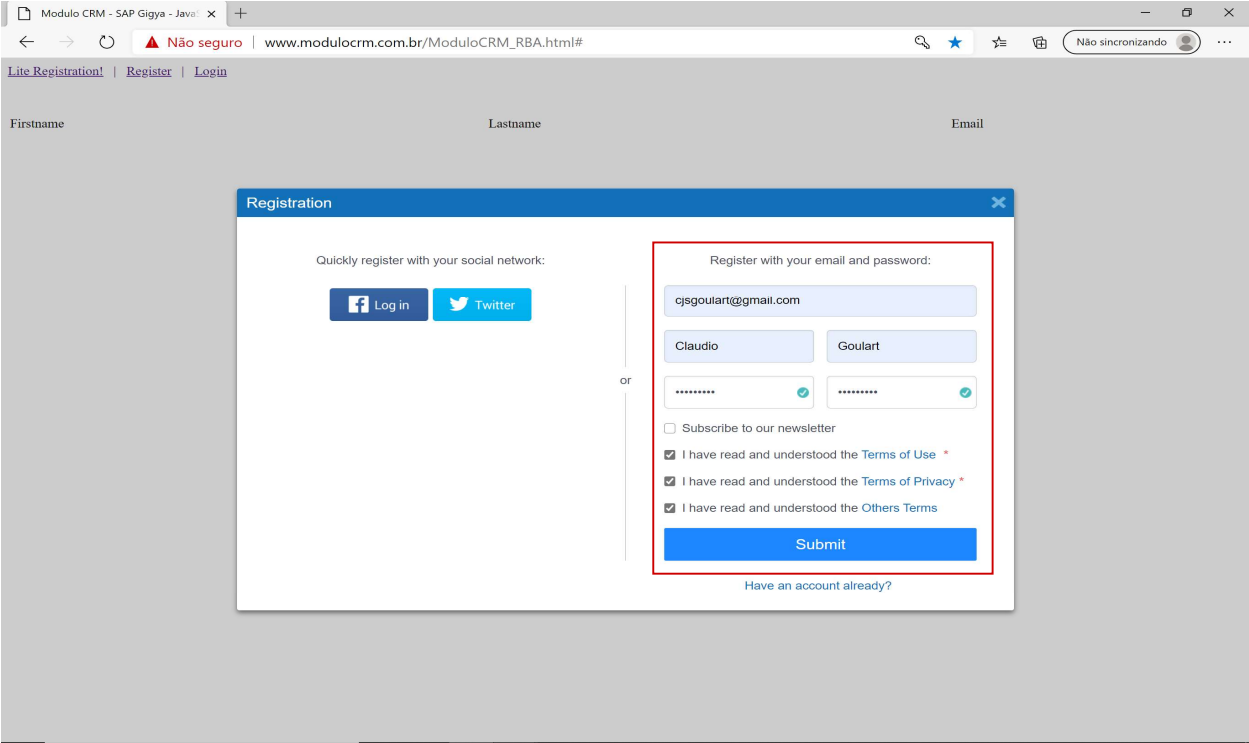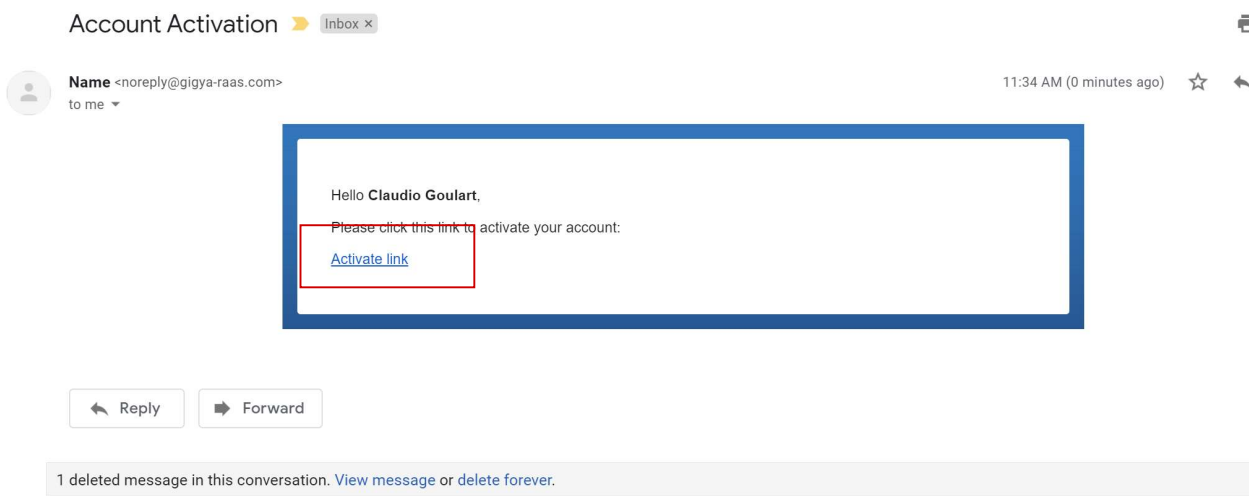

An information is shown informing that "A verification email with a link to verify your account has been sent to you". Then I click into the button "OK".
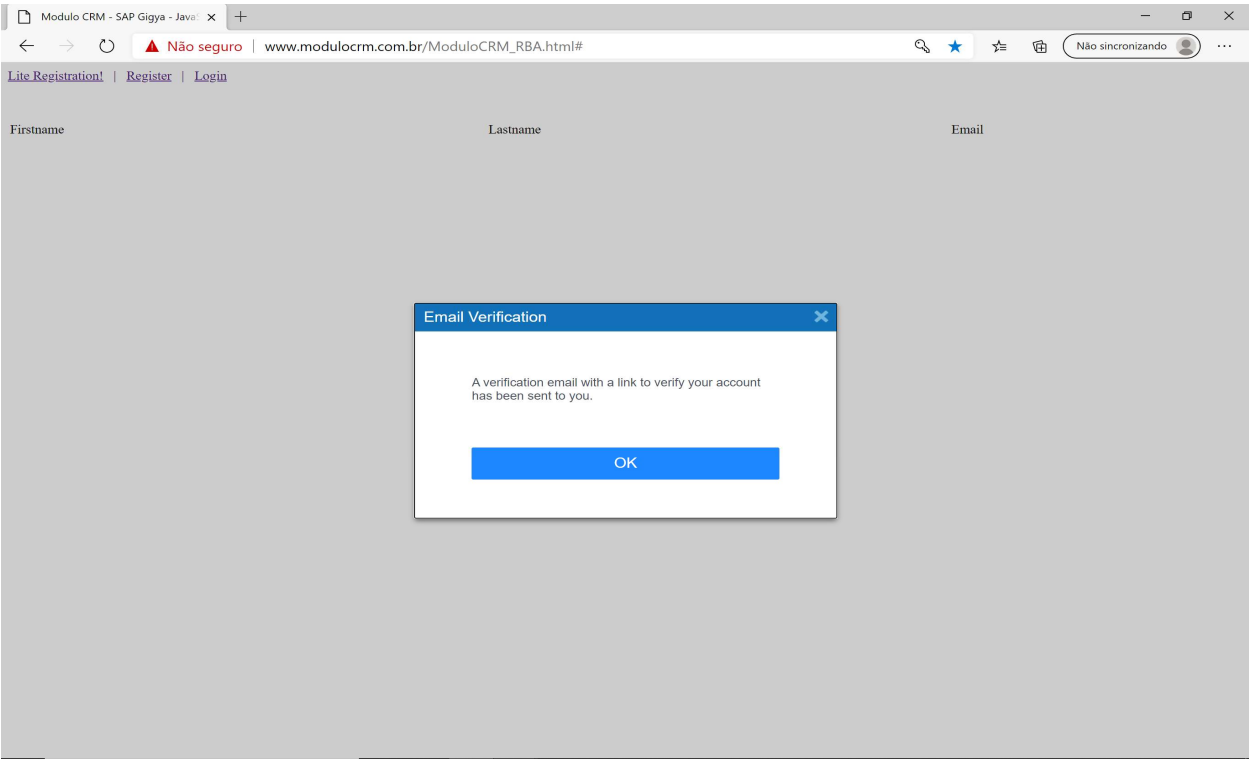
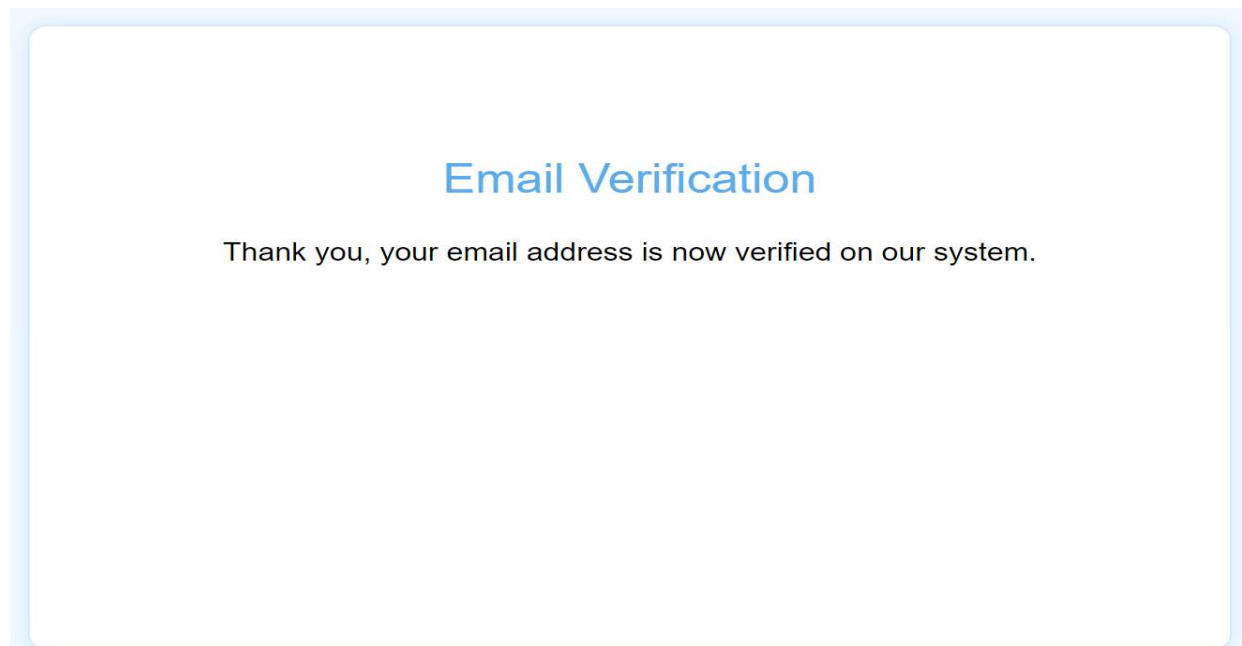## 1.5. Checking the Account Activation (Email)

As I mentioned, I will receive an email to check if my email is real. Then, I will click into the link "Activate link"

An Email Verification page will be exhibit immediately. My User was activated.

1.6.   Accessing the Web Site from different device (Mobile)

Now, let´s test if my configuration is doing exactly what I want to. I will connect into the same web site, however, using my ==cellphone==.

I will click into the link "Login", then an SAP CDC login page will appear asking me my email and password. I will provide it right the way. We will se what happen.
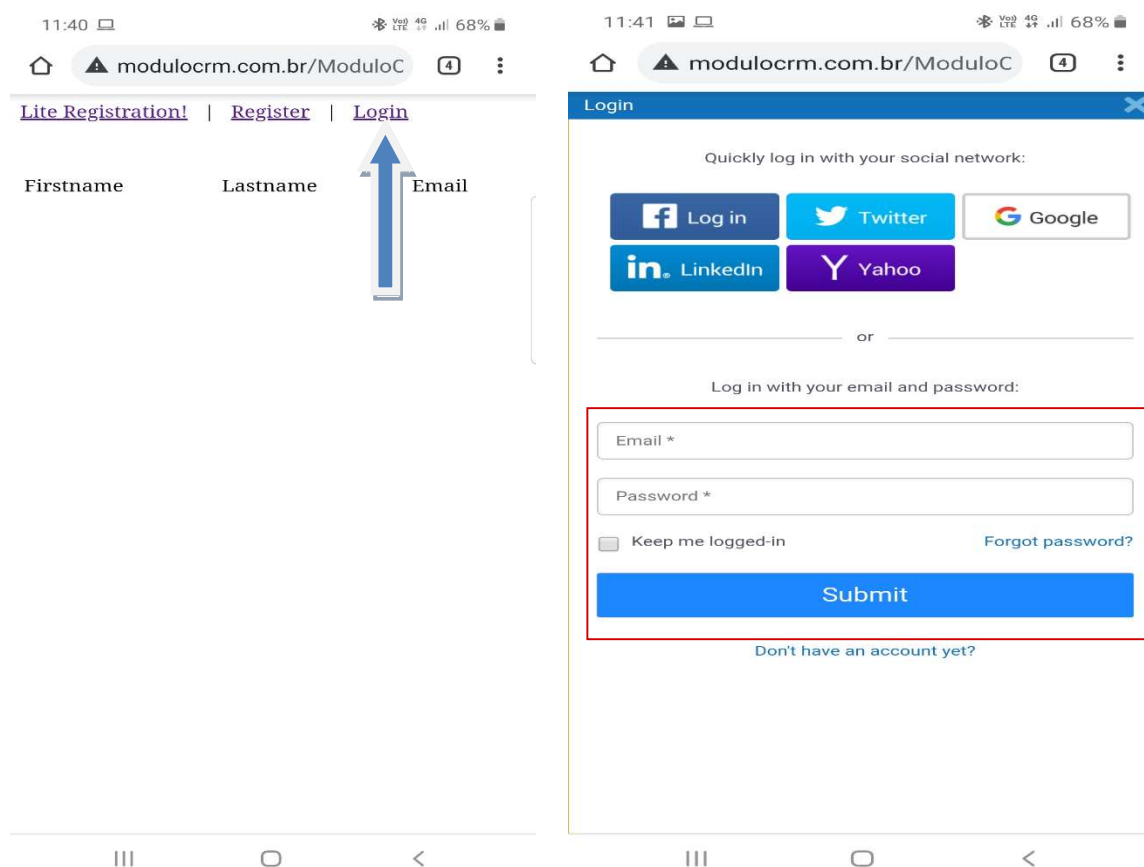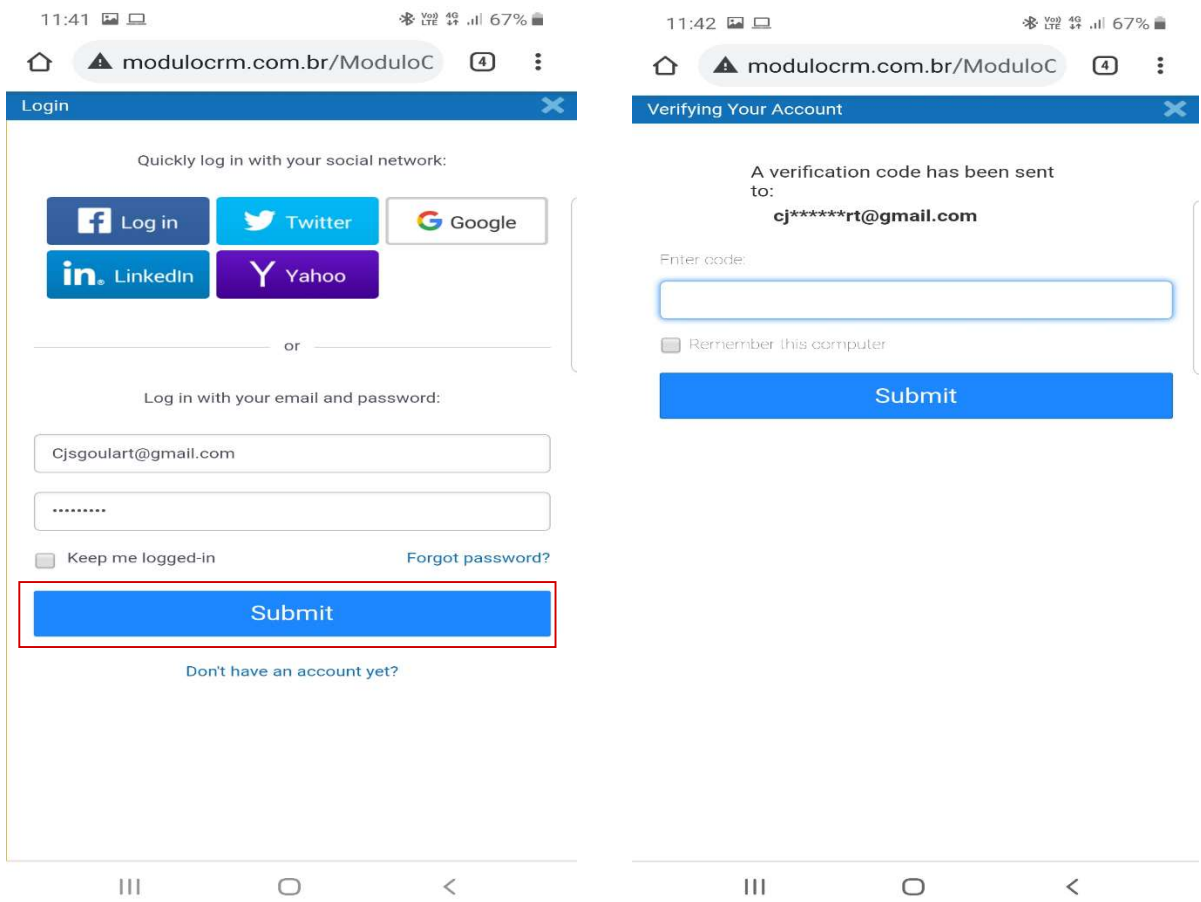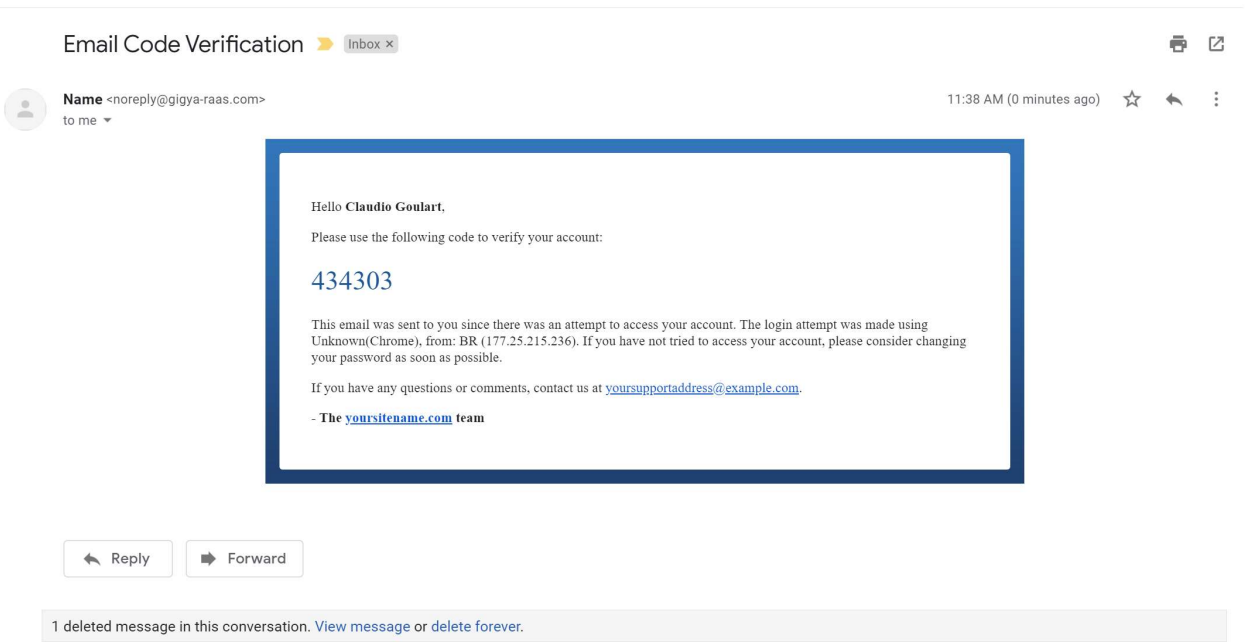
Article - Blog Módulo CRM Web Site

Providing my email id and password, SAP CDC automatically checks if I am connecting into my site with different Device.

SAP CDC is right; I am connecting with my <mark>Mobile</mark>. The first time it was my <mark>computer</mark>. Then SAP CDC will send to me by email a secret code and ask me to check my email inbox and confirm the secret code.
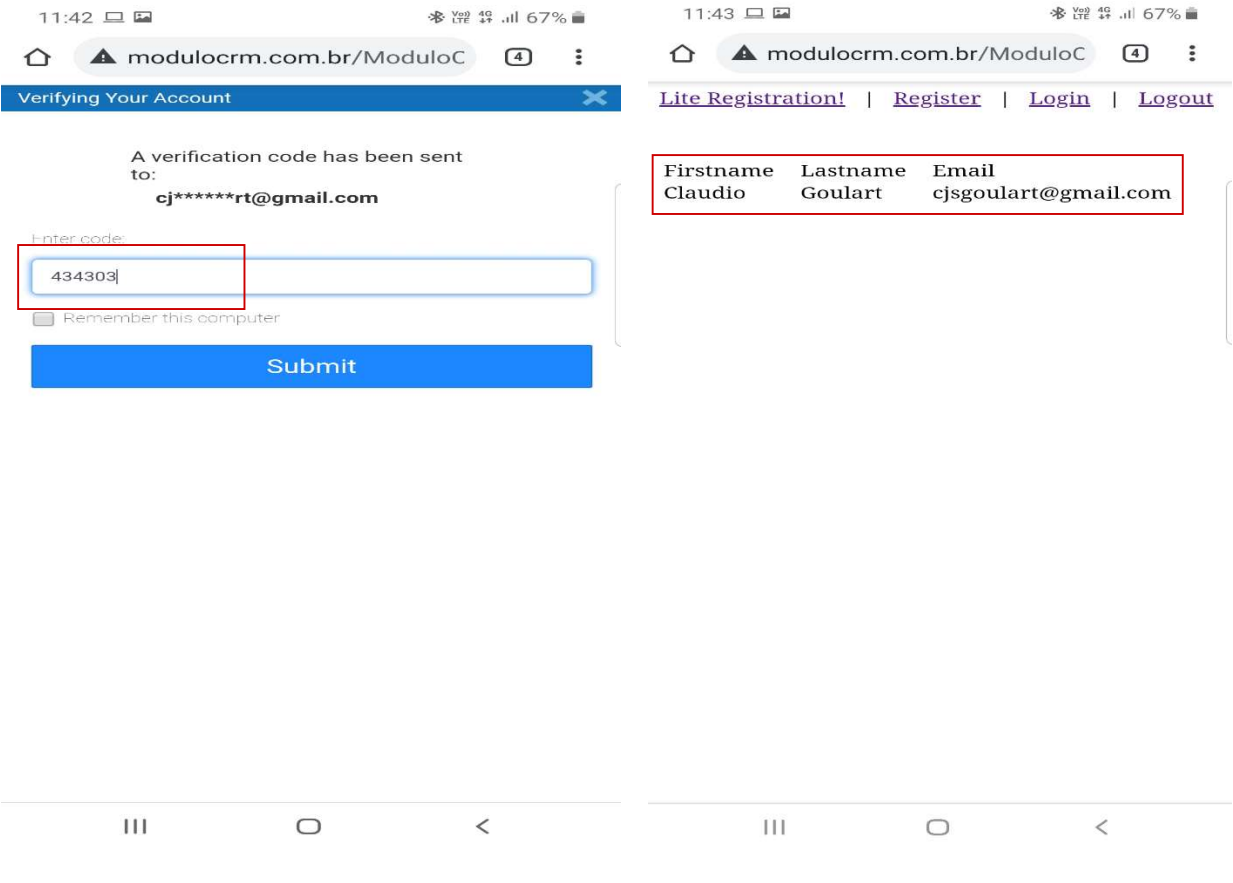

Into my email inbox, there is an email informing my secret code. Copy the code.

In the Verifying page I will provide the secret code, then I will click into the Submit Button. That´s it, SAP CDC allows me to connect into my web site now.

It was not a complex configuration, but the result is outstanding, and demonstrate how powerful this solution is.

It was nice, don´t you think?? I hope you enjoy it folks!!

Blog - Módulo CRM
Email: claudio.goulart@modulocrm.com.br   **Page 10**   **Blog - Módulo CRM**
Site: www.modulocrm.com.br