

Last Modified: July 30, 2015

SugarCRM is a cloud based solution that provides businesses with a CRM solution.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and SugarCRM.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the SecurID Access manual.

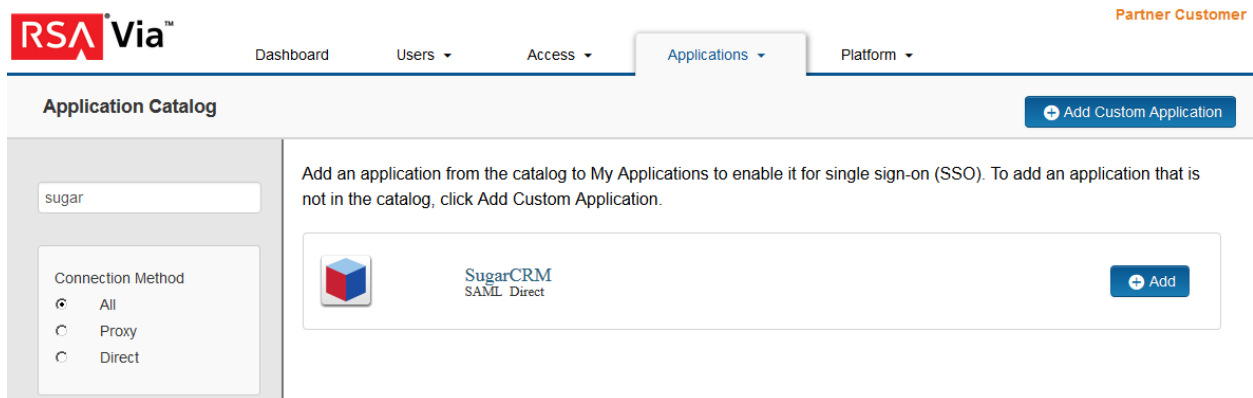
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure SugarCRM to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the application that you wish to add.



3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, fill in the Connection URL with your site's login page.
5. Select **SP –initiated** and binding method **POST**.

Connection URL

https://asrtzm2479.trial.sugarcrm.com


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

6. Scroll down to **SAML Identity Provider (Issuer)** section.
7. Take note of the Identity Provider URL it will be needed to configure SugarCRM.

SAML Identity Provider (Issuer)

Identity Provider URL

https://pe110.pe-lab.com/IdPServlet?idp_id=sugar

Issuer Entity ID

Default (idp_id): sugar

Override

- Click **Choose File** and upload the private key.

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

✓ Private Key Loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

⚠ No certificate loaded

Choose File

- Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL

<https://asrtzm2479.trial.sugarcrm.com/index.php?module=Users&action=Authenticate>

Audience (Service Provider Entity ID)

php-saml

- In the **Assertion Consumer Service (ACS) URL** field, enter https://<your_instance>/index.php?module=Users&action=Authenticate
- In the **Audience (Service Provider Entity ID)** field, enter **php-saml**.

- Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

11. Click **Next Step**.
12. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

- Allow All Authenticated Users
- Select Custom Policy


No Access Allowed

Cancel

Next Step →

13. Click **Next Step**.
14. On the Portal Display page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

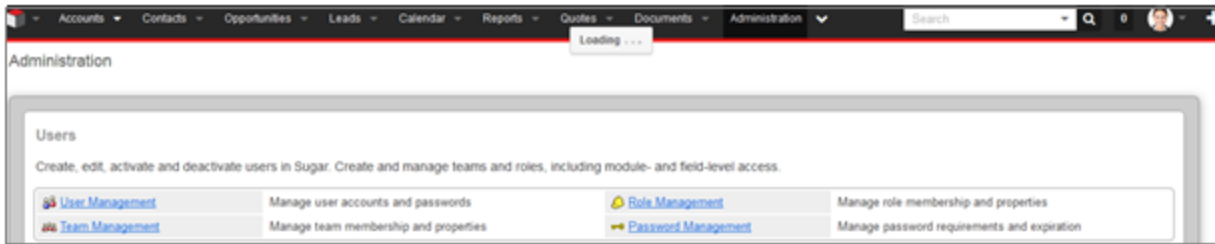
Next Steps

[Configure SugarCRM to Use RSA SecurID Access as an Identity Provider](#)

Configure SugarCRM to Use RSA SecurID Access as an Identity Provider

Procedure

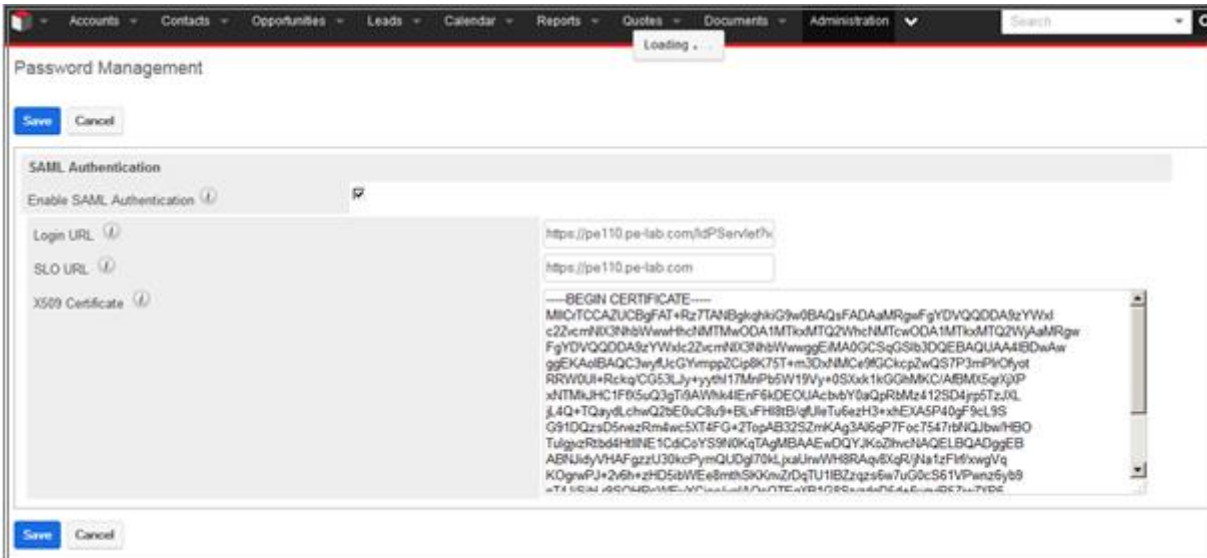
1. Login to SugarCRM.
2. Under the Admin profile pull down, select **Admin**.



3. Select **Users > Password Management**.
4. Scroll down to SAML Authentication and select **Enable SAML Authentication**.



5. The SAML Authentication window will open.
6. In the **Login URL** field, enter the SecurID Access Identity Provider URL.
7. In the x509 certification window paste the SecurID Access public certification, including the Begin and End lines.



8. Click **Save**.

9. Navigate to **Administration > Users > User Management**.
10. Select the user to edit.
11. Verify that the email address is configured.
12. Select the user's **Advanced** tab.
13. Check the **SAMLAuthenticate Only** box.

The screenshot shows the 'Advanced' tab of the 'User Settings' section. The interface includes several configuration options:

- Export Delimiter:** A text input field containing a period (.)
- Import/Export Character Set:** A dropdown menu set to 'UTF-8'
- Show Full Names:** A checked checkbox
- Default Teams:** A list containing 'Global' with a minus sign button to its right. A 'Primary' label is positioned above the list.
- SAMLAuthenticate Only:** A checked checkbox
- Notify on Assignment:** An unchecked checkbox
- Reminders:** A checked checkbox for 'Popup' and an unchecked checkbox for 'Email all invitees'. A dropdown menu next to 'Popup' is set to '30 minutes prior'.