# RSA SecurID Access SAML Configuration for Agiloft

**Last Modified:** November 20, 2015

Agiloft is the world's most adaptable and rapidly deployed agile business and enterprise software. Agiloft makes it ease to manage your business workflow**.**

**Before You Begin**

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

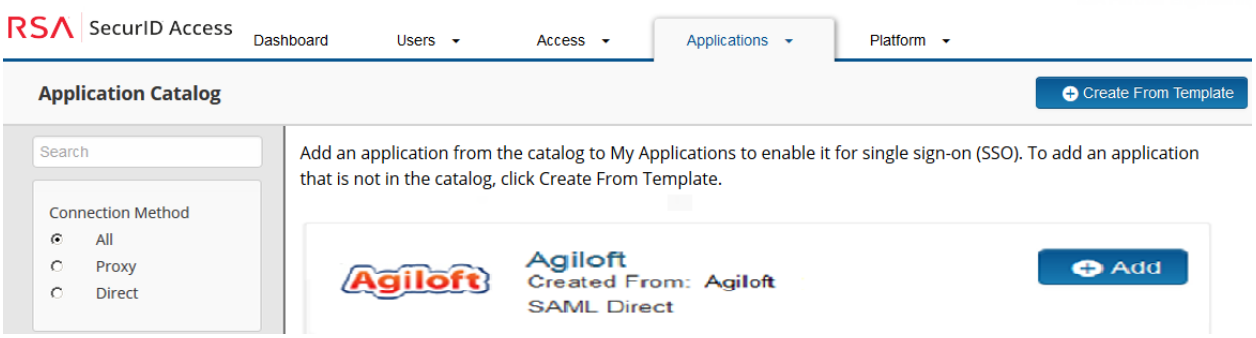
**Procedure**

1. Add the Application in RSA SecurID Access
2. Configure Agiloft to Use RSA SecurID Access as an Identity Provider

## Add the Application in RSA SecurID Access

**Procedure**

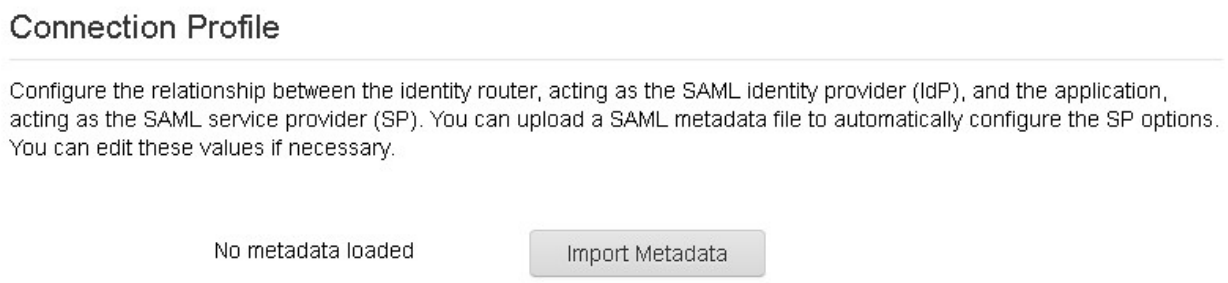
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for Agiloft and click **+Add**.



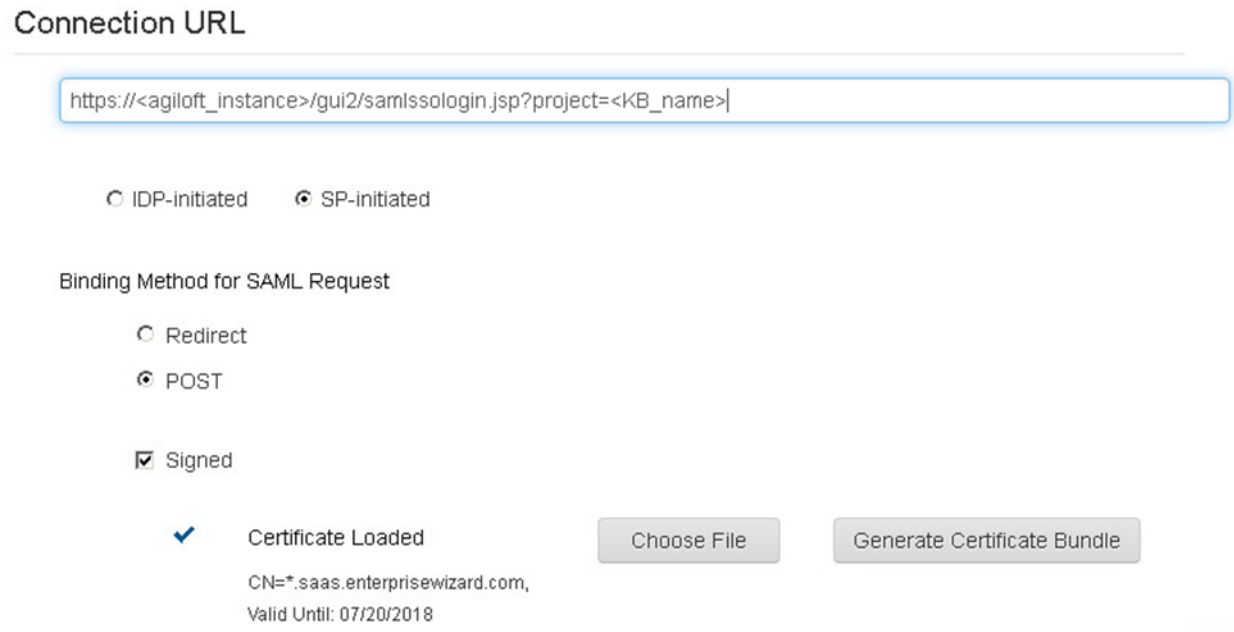
3. On the Basic Information page, specify the application name and click **Next Step**.

**Note: The following SP-initiated configuration worked for both SP and IDP connections.**

4. Select **Import Metadata** and select the xml file you downloaded from Agiloft. Edit any additional setting as show in the following configuration.



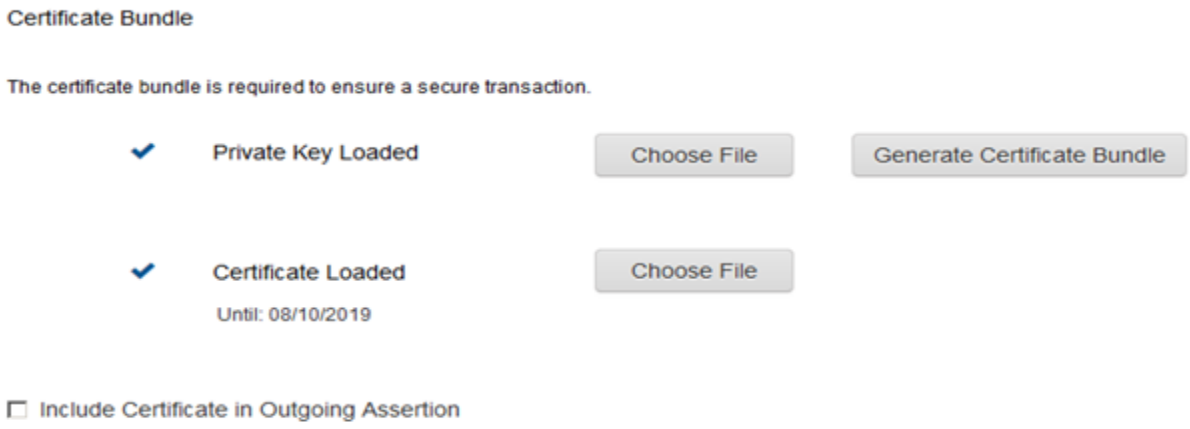

5. In the Connection URL field, enter the single sign-on login URL.
6. Select **SP-initiated** and modify the Connection URL field with your Agiloft instance and project name.




7. Select binding method **POST** and check **Signed**.
8. Select **Choose File** and upload the X.509 certificate that you downloaded from Agiloft.

9. Scroll down to **SAML Identity Provider (Issuer)** section.
10. Take note of the Identity Provider Entity ID; it must be provided to Agiloft.


11. Select **Choose File** and upload the RSA SecurID Access private key.
12. Select **Choose File** and upload the RSA SecurID Access public certificate.

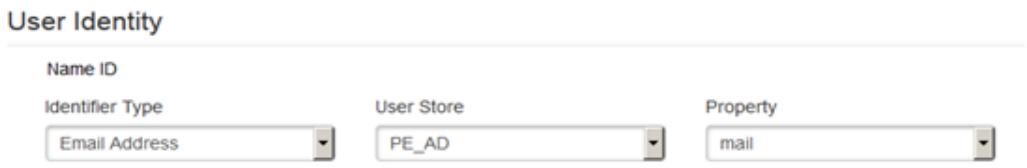



13. Scroll down to the **Service Provider** section.

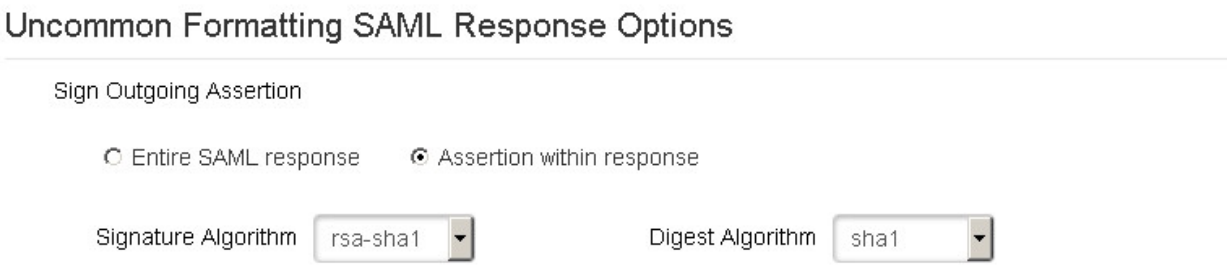

a. Modify the **Assertion Consumer Service (ACS) URL** with your Agiloft instance and project name.
Example:https://agiloft5768.enterprisewizardcom:443/gui2/spsamlsso?project=RSA

b. Modify the **Audience (Service Provider Entity ID)** with your Agiloft instance and project name.
Example: agiloft5768/RSA

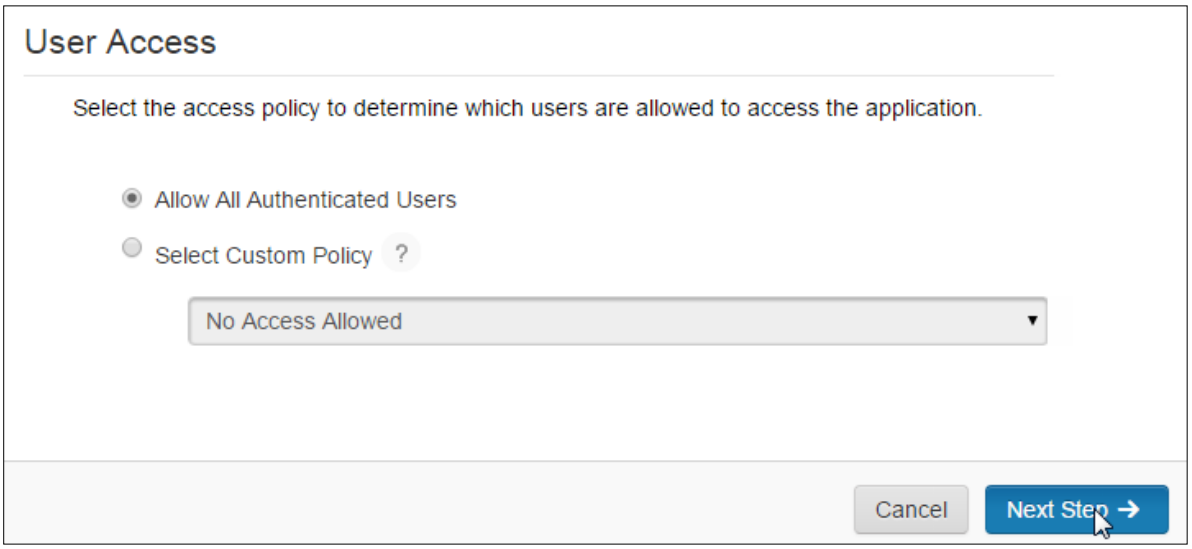
14. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.



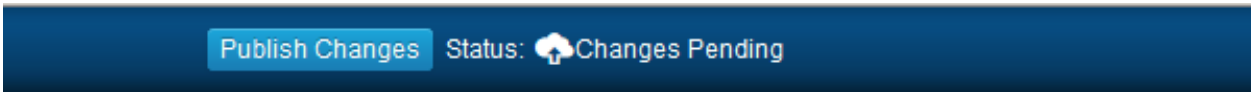

15. Scroll down to Uncommon Formatting SAML Response Options and select **Assertion within response**.




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




18. Click **Next Step**.
19. On the Portal Display page, select **Display in Portal**.
20. Click **Save and Finish**.
21. Click **Publish Changes**. Your application is now enabled for SSO.

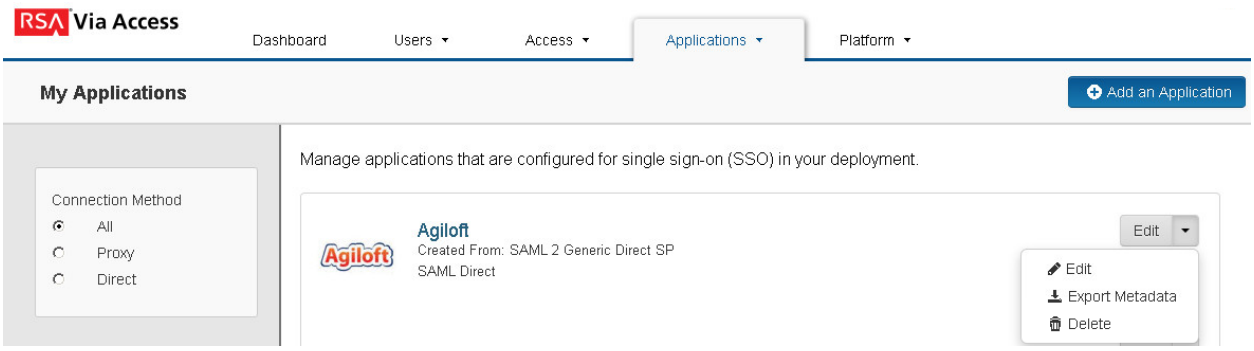


**Next Steps**

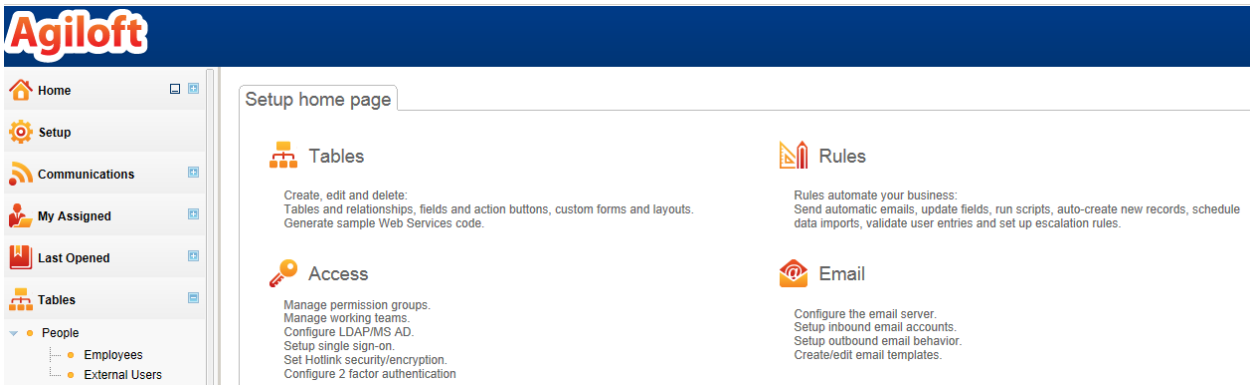
Configure Agiloft to Use RSA SecurID Access as an Identity Provider

## Configure Agiloft to Use RSA SecurID Access as an Identity Provider

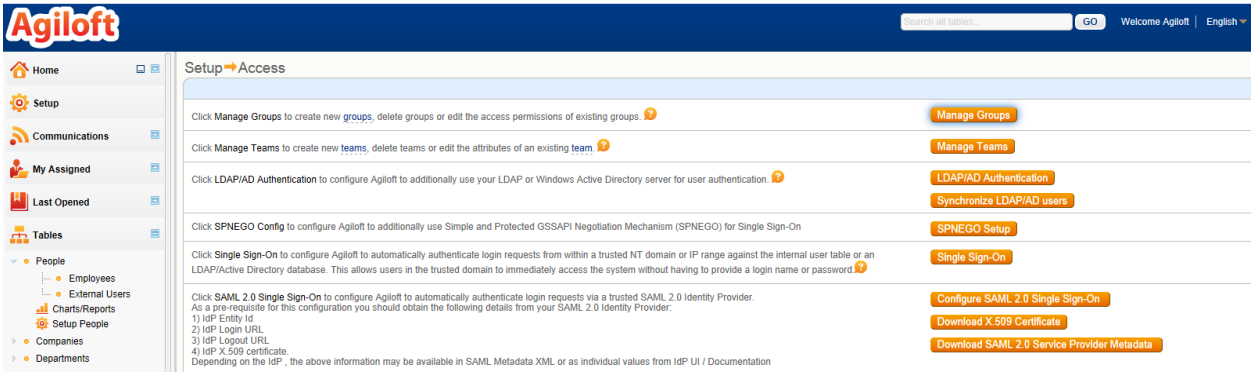
1. Login to the RSA SecurID Access console.
2. Select **Applications > My Applications**.
3. Select the **Edit** pull down for the Agiloft application and choose **Export Metadata**.




4. Contact Agiloft to setup the Agiloft certificates and provide them with the RSA SecurID Access metadata file.
5. Login to Agiloft with an admin account. [https://<agiloft_instance>/logins/<KB name>](https://<agiloft_instance>/logins/<KB name>)
6. Navigate to **Setup > Access**.

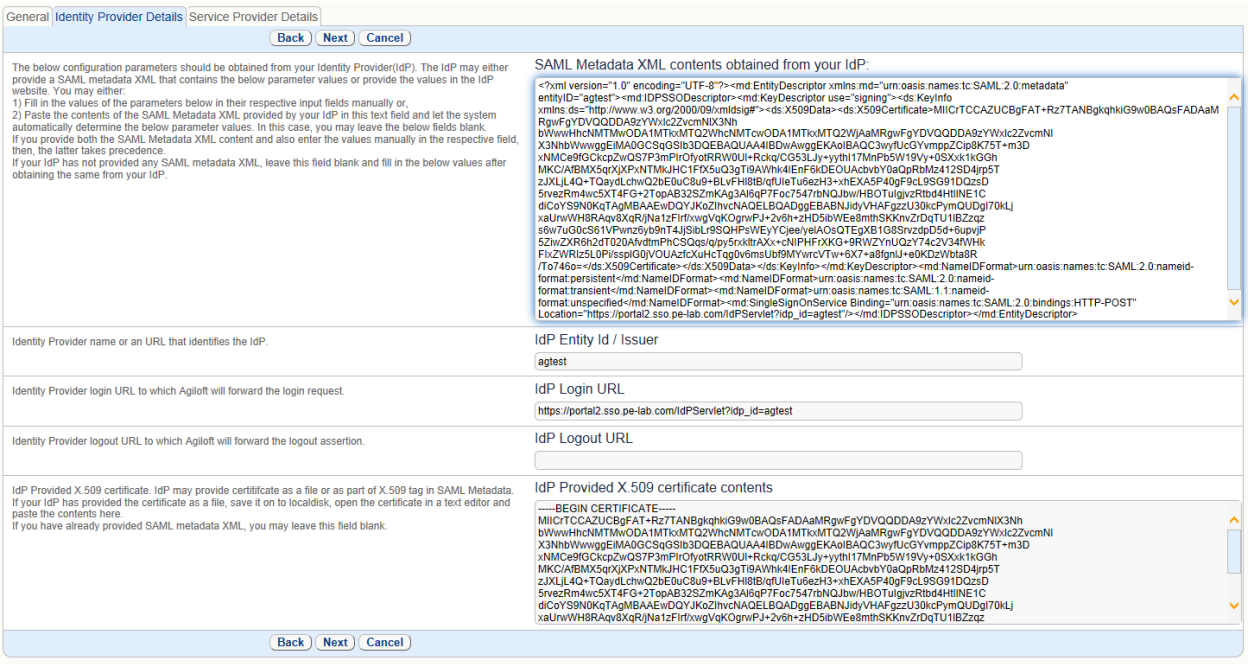



7. Select **Configure SAML 2.0 Single Sign-On.**



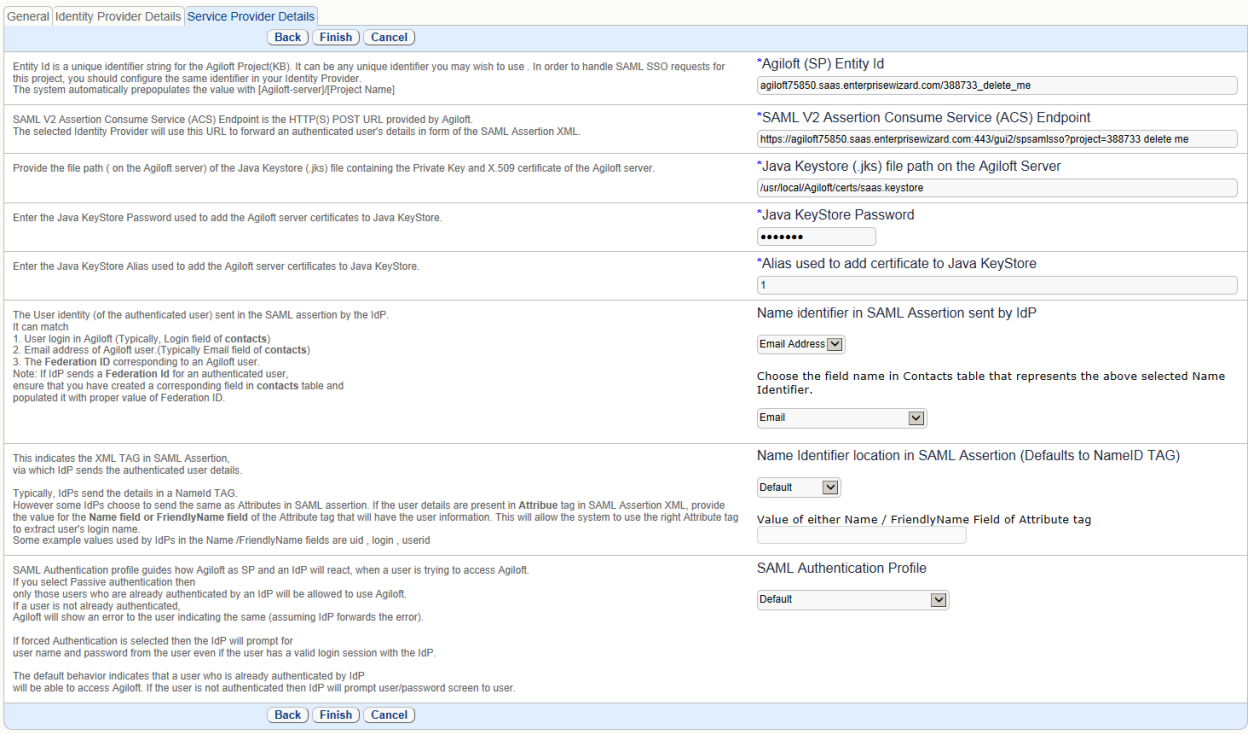
8. Select **Enable SAML SSO**.


9. Select **Next**.
10. Paste the RSA SecurID Access metadata file in the **SAML Metadata XML contents from your IdP** window. This will auto fill the remaining fields.

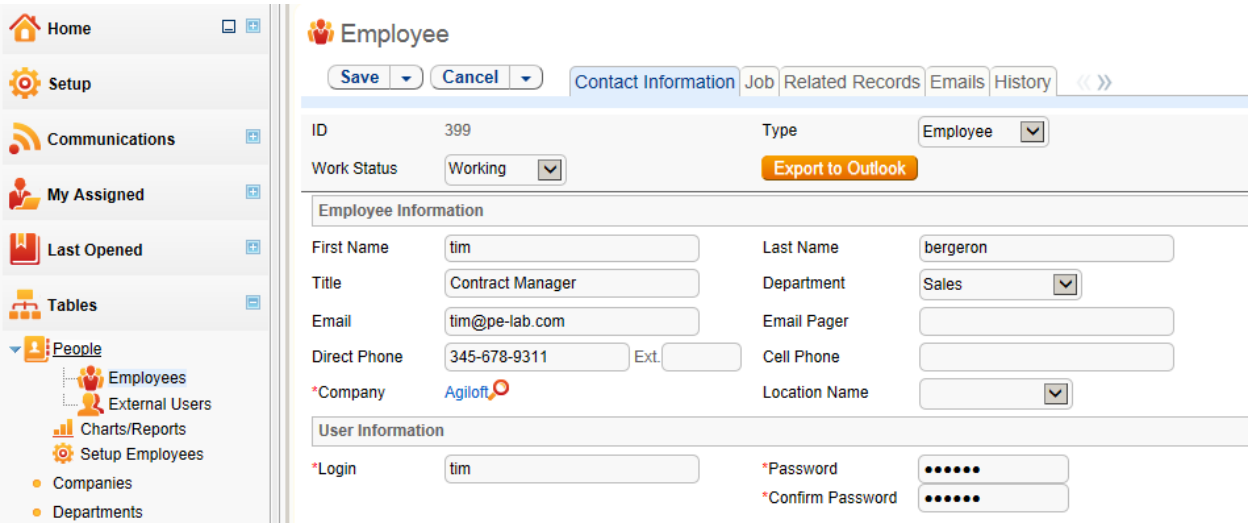



11. Select **Next**.

12. On the Service Provider Details page, use the pull down to select **Email Address** for Name identifier in SAML Assertion sent by IdP.
13. Select **Email** in the Choose the Field name in Contacts field.




14. Click **Finish**.
15. From the left side menu choose **People** to add a user.
16. Enter all the required fields for the user.




GLS