RSA SecurID Access SAML Configuration for Base

Last Modified: Feb 14, 2017

Base CRM (originally Future Simple or PipeJump) is an enterprise software company based in Mountain View, California with R&D offices located in Kraków, Poland. It provides a web-based all-in-one sales platform that features tools for email, phone dialing, pipeline management, forecasting, reporting and more. Base's platform is available on iOS and Android, and was the first full native CRM Android app available. Base also offers Apollo, a sales science platform that collects and analyzes sales activity data to generate insights for sales leaders.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and Base.
- Obtain the Base login URL, ACS URL and Service Provider Issuer ID from your Base service provider.

The instructions in this guide use the following login url, ACS URL and issuer ID (entity ID) values:

Login URL	*https://core.futuresimple.com/users/login*
ACS URL	*https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/consume*
Service Provider Issuer ID	https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/metadata

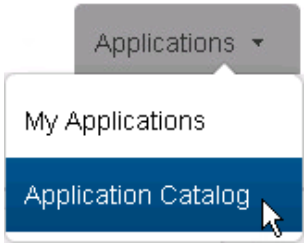
Procedure

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

Add the Application in RSA SecurID Access

Procedure

1. Log in to the RSA SecurID Access Administration Console, click the **Applications** tab and select *Application Catalog* from the **Application** tab dropdown list.

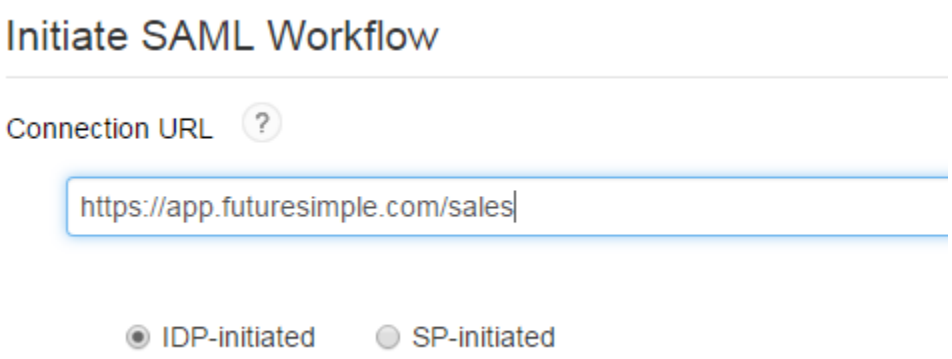


2. Search for *Base* in the list of applications and click the **+Add** button.

3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.
4. Select the **IdP-initiated** radio button in the **Initiate SAML Workflow** section.

Note: The following IdP-initiated configuration works for SP-initiated Base connections as well.

5. Enter the Base landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the Base icon.
   The URL is formatted as follows: https://app.futuresimple.com/sales



6. Scroll to **SAML Identity Provider (Issuer)** section, copy the value in the **Identity Provider URL** field and paste it into a temporary file. You will need the URL when you configure your Base service provider.
7. Please note here Issuer Entity ID is not default. Base needs Issuer ID to be proper URL, so here it is same as Identity Provider URL

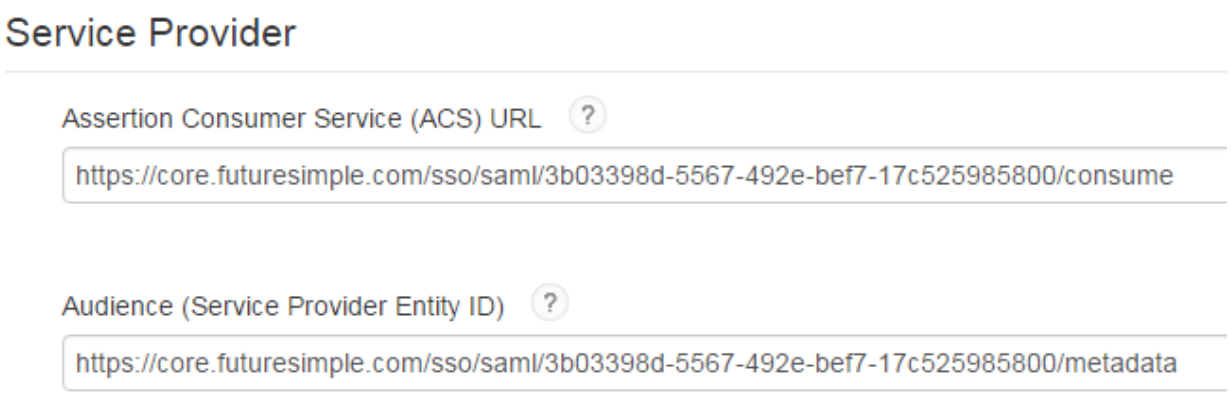
8. You must import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 9.
   a. Click the **Generate Certificate Bundle** button in the **SAML Response Signature** section.

b. In the **Common Name (CN)** field, enter the hostname of the Base service provider's HTTPS server that will be sending authentication requests.
c. Click the **Generate and Download** button, save the certificate bundle ZIP file to a secure location and extract its contents. The ZIP file will contain a private key, a public certificate and a certificate signing request. Click the **Choose File** button on the left of the **Generate Certificate Bundle** button, locate and select a private key for signing the SAML assertions and click the **Open** button.

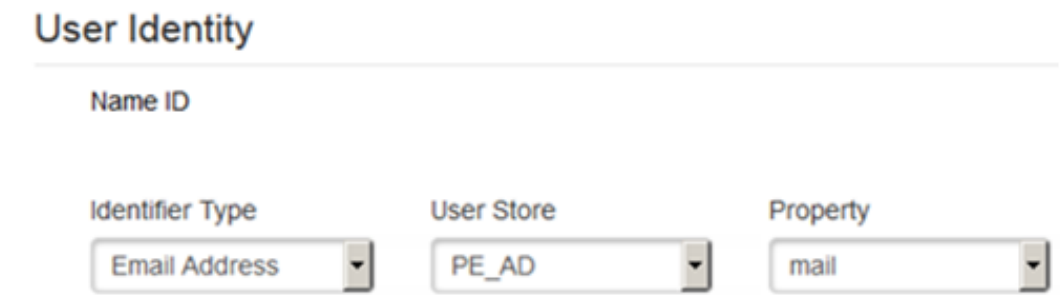
9. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
10. Select the **Include Certificate in Outgoing Assertion** checkbox.
11. Scroll to the **Service Provider** section and enter your Base ACS URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: https://core.futuresimple.com/sso/saml/<UUID>/conume

where <*UUID*> is unique per Base account.
The ACS URL in this example is https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/consume

12. Enter *https://core.futuresimple.com/sso/saml/<UUID>/metadata* in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your Base SP Issuer ID.
    where <*UUID*> is unique per Base account.
    The Service Provider Entity ID in this example is
    https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/metadata

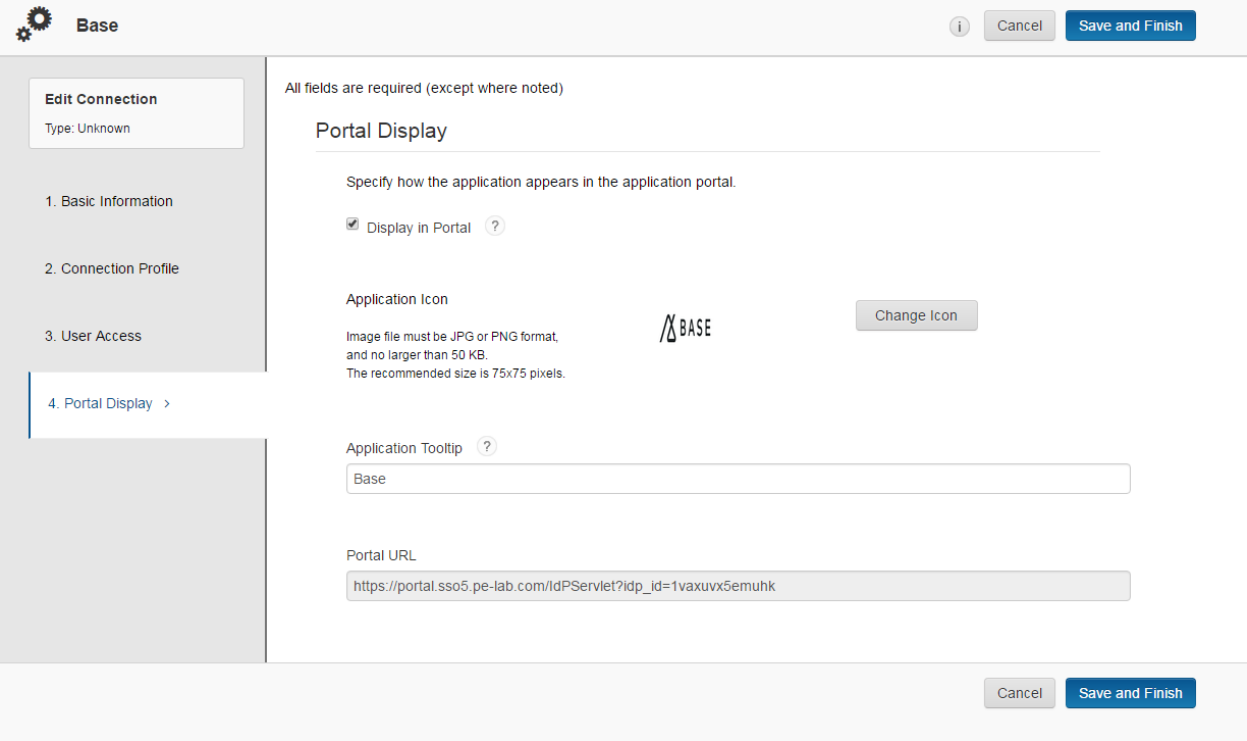


13. Scroll to the **User Identity** section, select *Email Address* from the **Identifier Type** dropdown list and select the name of your user identity source from the **User Store** dropdown list. In this example, user accounts are stored in an identity source named *PE_AD*.
14. Select the identity source's attribute that will be used as the NameID from the **Property** dropdown list. In this example, the identity source's *mail* attribute will be used to uniquely identify a user in SAML assertions.

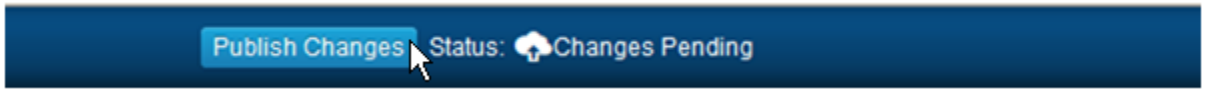


15. Click the **Next Step** button.
16. On the **User Access** page, select the access policy the identity router will use to determine which users can access the Base service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise, select the **Select Custom Policy** radio button and select the policy you want to use from the dropdown list.

17. Click the **Next Step** button.
18. Select the **Display in Portal** checkbox on the **Portal Display** page.
19. Enter descriptive text about the application in the **Application Tooltip** field. The portal will display this text when a user passes the cursor over the application's icon.
20. Click the **Save and Finish** button.



21. Click the **Publish Changes** button in the top left corner of the page.

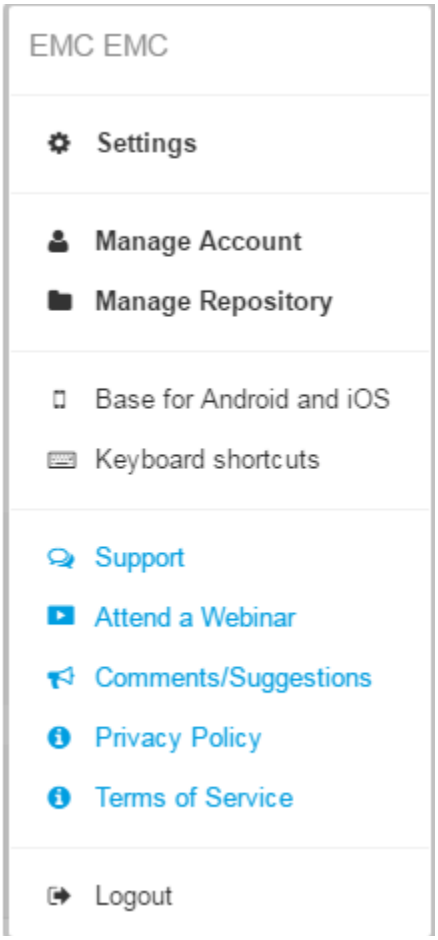


Configure Base to Use RSA SecurID Access as an Identity Provider

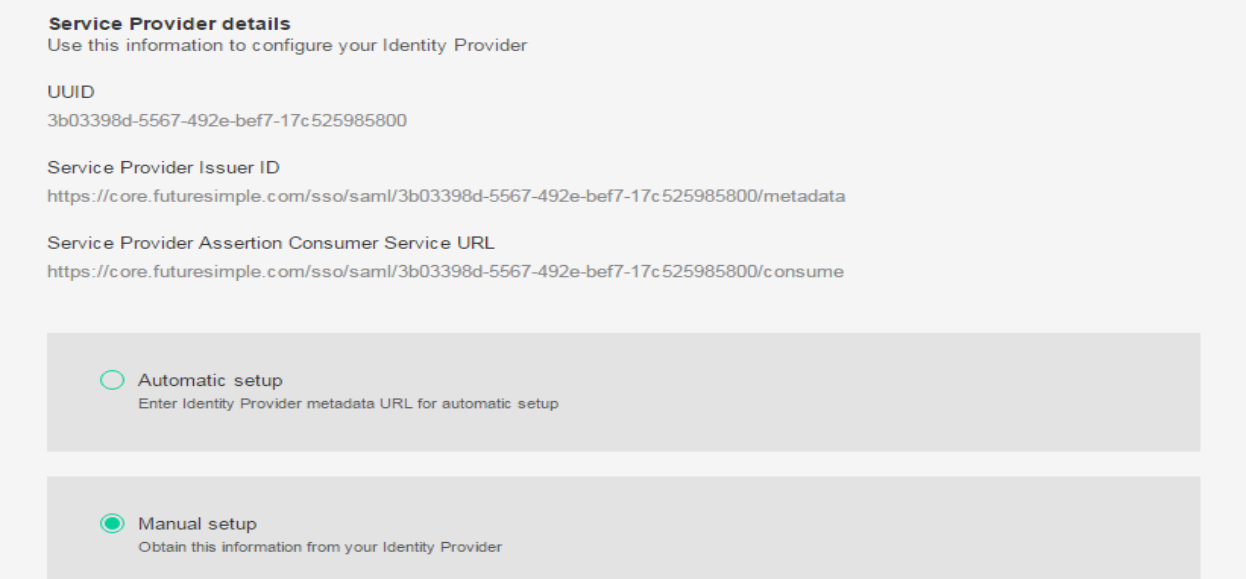
Follow below steps to configure Base as service provider.

Create an Identity Provider

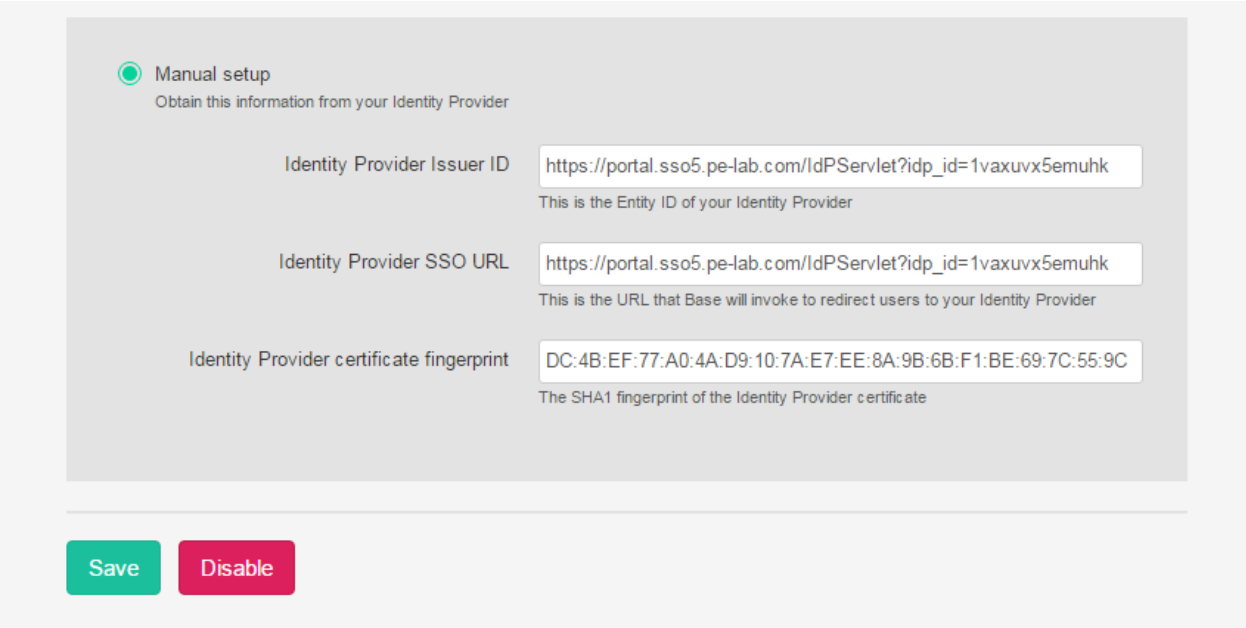
1. Log in to your Base account and select **Settings** from the Side Pane in the upper left corner of the page.



2. Click **Single Sign-On** option from side tabs.
3. Check **Manual Setup**.



4. In **Identity Provider Issuer ID** provide RSA SecurID Access Identity Provider URL as Base needs proper URL for Issuer ID.
5. In **Identity Provider SSO URL** text box provide RSA SecurID Access Identity Provider URL which you copied earlier.
6. In **Identity Provider certificate fingerprint** text box Fingerprint of the Certificate which you imported while configuring the connector earlier.
7. Then click **Save**.



8. From the left side menu select **Manage Users**.
9. Select **Add New User**.
10. Fill in the *Full Name* and *Email* fields. Select the access level and click **Save**.
11. An email will be sent to the user to complete registration.

Appendix

Your Base account's ACS URL is: https://core.futuresimple.com/sso/saml/<UUID>/consume

The ACS URL in this example is https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/consume

Your Base account's Entity ID is https://core.futuresimple.com/sso/saml/<UUID>/metadata

The ACS URL in this example is https://core.futuresimple.com/sso/saml/3b03398d-5567-492e-bef7-17c525985800/metadata

MD