

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.

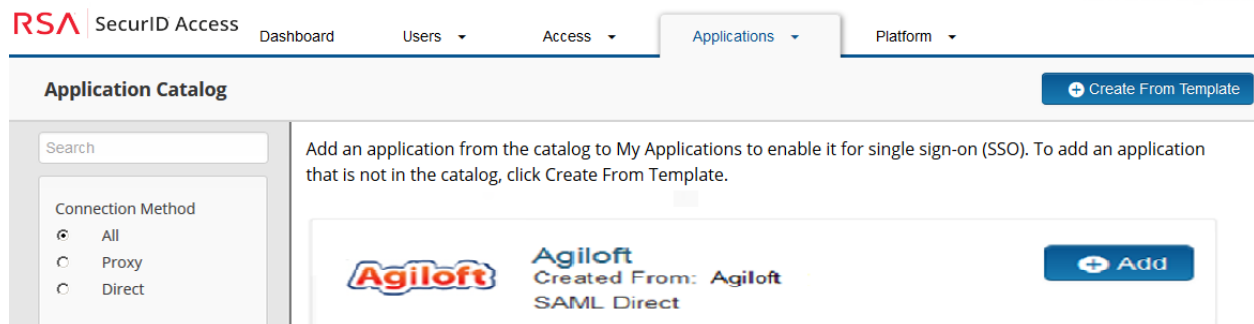
Procedure

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.

Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.

No metadata loaded

Import Metadata

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.

Connection URL

`https://<agiloft_instance>/gui2/samlssologin.jsp?project=<KB_name>`

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed



Certificate Loaded

CN=*.saas.enterprisewizard.com,

Valid Until: 07/20/2018

Choose File

Generate Certificate Bundle

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.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

- Default (idp_id): agtest
 Override

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

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

✓ Private Key Loaded

✓ Certificate Loaded

Until: 08/10/2019

Include Certificate in Outgoing Assertion

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

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

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

User Identity

Name ID

Identifier Type User Store Property

Email Address PE_AD mail

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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response Assertion within response

Signature Algorithm rsa-sha1 Digest Algorithm sha1

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

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 →

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.

Publish Changes Status:  Changes Pending

Next Steps

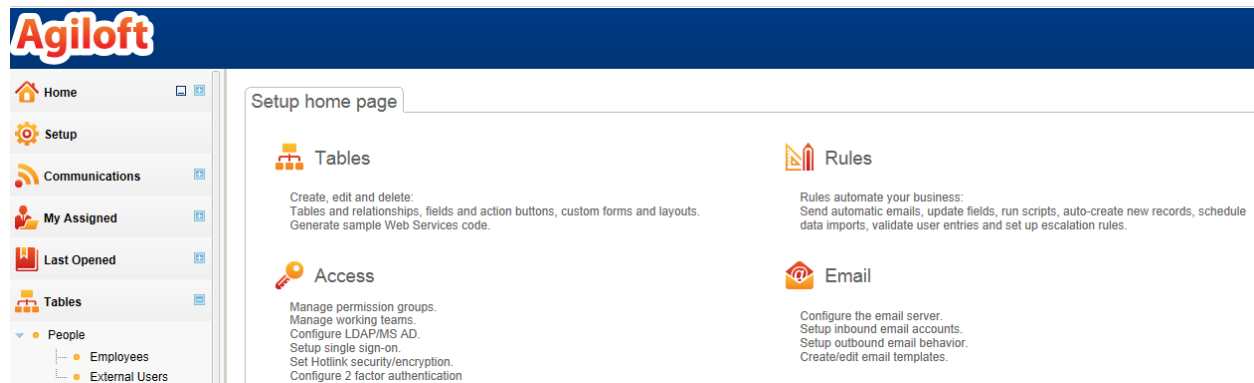
[Configure Agiloft to Use RSA SecurID Access as an Identity Provider](#)

Configure Agiloft to Use RSA SecurID Access as an Identity Provider

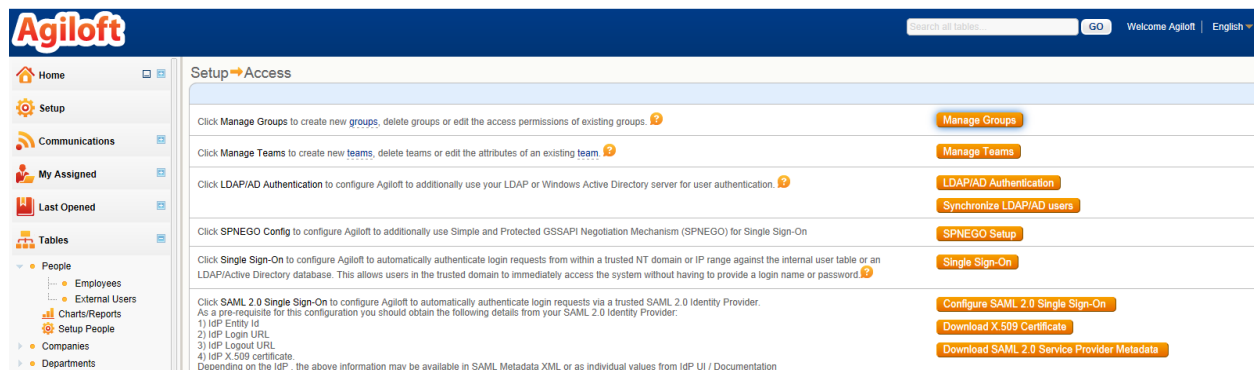
1. Login to the RSA SecurID Access console.
2. Select **Applications > My Applications**.
3. Select the **Edit** pull down for the Agiloft application and choose **Export Metadata**.



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>
6. Navigate to **Setup > Access**.



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



8. Select **Enable SAML SSO**.

General Identity Provider Details Service Provider Details

Enable / Disable SAML SSO 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.

General Identity Provider Details Service Provider Details

The below configuration parameters should be obtained from your Identity Provider(IdP). The IdP may either provide a SAML metadata XML that contains the below parameter values or provide the values in the IdP website. You may either:
 1) Fill in the values of the parameters below in their respective input fields manually or,
 2) Paste the contents of the SAML Metadata XML provided by your IdP in this text field and let the system automatically determine the below parameter values. In this case, you may leave the below fields blank. If you provide both the SAML Metadata XML content and also enter the values manually in the respective field, then, the latter takes precedence.
 If your IdP has not provided any SAML metadata XML, leave this field blank and fill in the below values after obtaining the same from your IdP.

SAML Metadata XML contents obtained from your IdP:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="agtest"><md:IDPSSODescriptor-<md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIICRTCCA2UCBGFAT+Rz7TANBgkqhkiG9w0BAQsFADAaM
RgwFgYDVQDDA9yWwlic2ZvcnNlX3Nh
bWwHhcnMTMwODA1MTkxMQQ2WjAaMRgwFgYDVQDDA9yWwlic2ZvcnNl
X3NhbnWwggEIMA0GCSqSb3QOEBAQUAA4IBDwAwggEKAoIBAQC3wytUcGYvmpZCip8K75T-m3D
xNMc9iGckcpZwOS7P3mPirOyoRRWUli-Rckq/CG53Ljy+yth17MnPB5W/19Vy+0Sxxk1kGGh
MKCjARBMX5qXpXNTRHkHC1F7X5uQ3gT8AWhk4EiF6DEOUAcvbnY6qPbRmIz412SD4pp5T
zXLJL4Q+TQoydlchwO2hEduC8u9-BLlVfH9BjufU6e2H3+HEKASP49gP8L5SG91DQz5D
5vz2Rm4wc5XT4FG+2TopAB32S2mAg3A8qP7Foc7547rbNQBjwHBOtUlgvzRtb4HIINE1C
diCoYS9N0KqTAgMBAEwDQYJKoZlhmvcNAQELBQADggEBABNjidyVHAFgzuz30kcPymQUdgi70kLj
xaUnwVH8RAqv8XqRjJna1z2FirtxwVgKQgrwPj+2v9h+zHD5bWE68mthSKKvZrDqTU11B2Zqz
s8w7UgIc851NvPmz8y9bNt4J8Jbl+SSQhP5tVEJYGjebye8QsTegP81G85rvcdd56+6upwP
5ZwZXR6h2dt020AvdtnPhcSQqs/qpy5rvk8trAX+cNlPHFXKG-9RWZYNlUQY74c2V34fWHk
FixZWrlz5L0PisspG0jVOUazicXuhcTog0v6msUbf9MYwrcVtw+6X7+a8fgnU+e0KdzWbta8R
l7o748e=<ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent<md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-
format:transient<md:NameIDFormat><md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecialized<md:NameIDFormat><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://portal2.sso.pe-lab.com/idPService?idp_id=agtest"/></md:IDPSSODescriptor></md:EntityDescriptor>
```

Identity Provider name or a URL that identifies the IdP.

Identity Provider login URL to which Agiloft will forward the login request.

Identity Provider logout URL to which Agiloft will forward the logout assertion.

IdP Provided X.509 certificate. IdP may provide certificate as a file or as part of X.509 tag in SAML Metadata. If your IdP has provided the certificate as a file, save it on to localdisk, open the certificate in a text editor and paste the contents here. If you have already provided SAML metadata XML, you may leave this field blank.

IdP Provided X 509 certificate contents

```
-----BEGIN CERTIFICATE-----
MIICRTCCA2UCBGFAT+Rz7TANBgkqhkiG9w0BAQsFADAaMRgwFgYDVQDDA9yWwlic2ZvcnNlX3Nh
bWwHhcnMTMwODA1MTkxMQQ2WjAaMRgwFgYDVQDDA9yWwlic2ZvcnNl
X3NhbnWwggEIMA0GCSqSb3QOEBAQUAA4IBDwAwggEKAoIBAQC3wytUcGYvmpZCip8K75T-m3D
xNMc9iGckcpZwOS7P3mPirOyoRRWUli-Rckq/CG53Ljy+yth17MnPB5W/19Vy+0Sxxk1kGGh
MKCjARBMX5qXpXNTRHkHC1F7X5uQ3gT8AWhk4EiF6DEOUAcvbnY6qPbRmIz412SD4pp5T
zXLJL4Q+TQoydlchwO2hEduC8u9-BLlVfH9BjufU6e2H3+HEKASP49gP8L5SG91DQz5D
5vz2Rm4wc5XT4FG+2TopAB32S2mAg3A8qP7Foc7547rbNQBjwHBOtUlgvzRtb4HIINE1C
diCoYS9N0KqTAgMBAEwDQYJKoZlhmvcNAQELBQADggEBABNjidyVHAFgzuz30kcPymQUdgi70kLj
xaUnwVH8RAqv8XqRjJna1z2FirtxwVgKQgrwPj+2v9h+zHD5bWE68mthSKKvZrDqTU11B2Zqz
-----
```

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.

General | Identity Provider Details | **Service Provider Details**

[Back](#) [Finish](#) [Cancel](#)

Entity Id is a unique identifier string for the Agiloft Project(KB). It can be any unique identifier you may wish to use. In order to handle SAML SSO requests for this project, you should configure the same identifier in your Identity Provider. The system automatically prepopulates the value with [Agiloft-server][Project Name]

*Agiloft (SP) Entity Id

SAML V2 Assertion Consume Service (ACS) Endpoint is the HTTP(S) POST URL provided by Agiloft. The selected Identity Provider will use this URL to forward an authenticated user's details in form of the SAML Assertion XML.

*SAML V2 Assertion Consume Service (ACS) Endpoint

Provide the file path (on the Agiloft server) of the Java Keystore (.jks) file containing the Private Key and X.509 certificate of the Agiloft server.

*Java Keystore (.jks) file path on the Agiloft Server

Enter the Java KeyStore Password used to add the Agiloft server certificates to Java KeyStore.

*Java KeyStore Password

Enter the Java KeyStore Alias used to add the Agiloft server certificates to Java KeyStore.

*Alias used to add certificate to Java KeyStore

The User Identity (of the authenticated user) sent in the SAML assertion by the IdP. It can match

1. User login in Agiloft (Typically, Login field of contacts)
2. Email address of Agiloft user (Typically Email field of contacts)
3. The Federation ID corresponding to an Agiloft user.

Note: If IdP sends a Federation Id for an authenticated user, ensure that you have created a corresponding field in contacts table and populated it with proper value of Federation ID.

Name identifier in SAML Assertion sent by IdP

Choose the field name in Contacts table that represents the above selected Name Identifier.

This indicates the XML TAG in SAML Assertion, via which IdP sends the authenticated user details.

Typically, IdPs send the details in a NameID TAG. However some IdPs choose to send the same as Attributes in SAML assertion. If the user details are present in Attribute tag in SAML Assertion XML, provide the value for the Name field or FriendlyName field of the Attribute tag that will have the user information. This will allow the system to use the right Attribute tag to extract user's login name. Some example values used by IdPs in the Name /FriendlyName fields are uid, login, useruid

Name Identifier location in SAML Assertion (Defaults to NameID TAG)

Value of either Name / FriendlyName Field of Attribute tag

SAML Authentication profile guides how Agiloft as SP and an IdP will react, when a user is trying to access Agiloft. If you select Passive authentication then only those users who are already authenticated by an IdP will be allowed to use Agiloft. If a user is not already authenticated, Agiloft will show an error to the user indicating the same (assuming IdP forwards the error).

SAML Authentication Profile

If forced Authentication is selected then the IdP will prompt for user name and password from the user even if the user has a valid login session with the IdP.

The default behavior indicates that a user who is already authenticated by IdP will be able to access Agiloft. If the user is not authenticated then IdP will prompt user/password screen to user.

[Back](#) [Finish](#) [Cancel](#)

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

Home | Setup | Communications | My Assigned | Last Opened | Tables | **People**

Employees | External Users | Charts/Reports | Setup Employees | Companies | Departments

Employee

[Save](#) [Cancel](#) [Contact Information](#) [Job](#) [Related Records](#) [Emails](#) [History](#) << >>

ID: 399 Type: Employee

Work Status: Working [Export to Outlook](#)

Employee Information

First Name: tim Last Name: bergeron
 Title: Contract Manager Department: Sales
 Email: tim@pe-lab.com Email Pager:
 Direct Phone: 345-678-9311 Ext: Cell Phone:
 *Company: Agiloft Location Name:

User Information

*Login: tim *Password: *****
 *Confirm Password: *****