

**Last Modified:** October 11, 2016

HappyFox is an Online help desk providing a web based support ticketing system.

## Before You Begin

- Acquire an administrator account for both RSA SecurID Access and HappyFox.

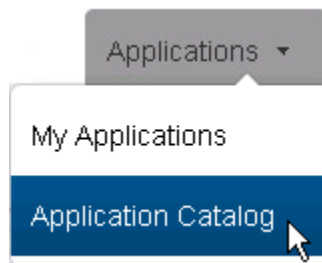
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure HappyFox 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 *HappyFox* in the list of applications and click the **+Add** button.



HappyFox  
SAML Direct



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.

---


**At the time of this testing only IdP login is supported. Contact HappyFox for SP login support.**

---

5. Leave the Connection URL field blank.

## Initiate SAML Workflow

---

Connection URL 


IDP-initiated     SP-initiated

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 this URL when you configure HappyFox.

## SAML Identity Provider (Issuer)

---

Identity Provider URL 

Issuer Entity ID 

- Default (idp\_id): 1xx3pbtsixsnp  
 Override

- 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.
- Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

✓ private.key

Choose File    Generate Cert Bundle    ?

✓ cert.pem

Choose File

Certificate valid until:  
Tue Dec 10 14:57:53  
UTC 2019

Include Certificate in Outgoing Assertion

- Scroll to the **Service Provider** section and enter your HappyFox domain in the ACS. The Assertion Consumer Service URL should be formatted as follows:

***https:// <DOMAIN>.HappyFox.com/staff/saml/callback/***

<DOMAIN> is the value of your domain name which you are using.  
example: *https://pelab3.HappyFox.com/staff/saml/callback.*

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.happyfox.com/staff/saml/callback/

Audience (Service Provider Entity ID) ?

https://www.happyfox.com

10. 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*.
11. 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.

## User Identity

Name ID

Identifier Type

Email Address

User Store

PE\_AD

Property

mail

12. Click the **Show Advanced Configuration** button.
13. Under Attribute Extension, enter Attribute Name **User.FirstName** with property **GivenName** and Attribute Name **User.LastName** with property **sn**.

## Attribute Extension ?

Attribute Source	Attribute Name Manage	Identity Source	Property		
Identity Sc	User.FirstName	AD20	givenName		
Identity Sc	User.LastName	AD20	sn		
+ ADD					

14. Click the **Next Step** button.
15. On the **User Access** page, select the **Allow All Authenticated Users** radio button.

- Allow All Authenticated Users  
 Select Custom Policy ?

No Access Allowed

16. Click the **Next Step** button.
17. Select the **Display in Portal** checkbox on the **Portal Display** page.
18. Click the **Save and Finish** button.
19. Click the **Publish Changes** button in the top left corner of the page.

**Publish Changes** Status: Changes Pending

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

Follow below steps to configure HappyFox as service provider.

## Create an Identity Provider

1. Login to your HappyFox domain as the Account Administrator.  
<https://<DOMAIN>.happfox.com/staff/welcome>
2. Go to **Manage> Integrations**.
3. Under the External section, click configuration next to SAML Integration.

Dashboard Tickets **Manage** Contacts Reports Knowledge Base

General Categories Staff Notifications Ticket Fields Contact Fields Tags Canned Actions Smart Rules SLA Satisfaction Surveys **Integrations**

Forum Multi-brand Security

### Manage Integrations Back to Tickets

#### Internal

Below is the list of all the available modules

Active	Name	Description	
X	API	Allows external applications to integrate with this help desk.	<a href="#">request access</a>
X	Web Hooks	Allows an external URL to be called whenever a ticket is created or updated	<a href="#">configure</a>
X	JSON Web Token (JWT)	Enable your clients to login via a remote authentication server	<a href="#">configure</a>
X	Support Widget	Create contact widgets that can be placed in any page on your website	<a href="#">configure</a>
X	Embed Forms	Create widgets that can be placed in any page on your website	<a href="#">configure</a>

#### External

Below is the list of all the available modules

Active	Name	Description	
X	Facebook Integration	Enables you to manage and reply to Facebook Posts and Messages via HappyFox.	<a href="#">configure</a>
X	Twitter Integration	Automatically convert your Mentions and Direct Messages into Tickets	<a href="#">configure</a>
X	SAML Integration	Allows for authentication using SAML	<a href="#">configure</a>

#### Internal/External Integrations

This page shows the list of integrations with other applications. Such integrations are classified as **Internal** and **External**. Internal integrations are the ones that we provide out of the box (based on the plan) like Embeddable forms, API etc. External integrations are those which integrate with other software services like CRM, Chat, Phone systems etc.

- Under Basic SAML Settings, select **Yes** for **SAML Integration active**.

The screenshot shows the 'SAML Integration' configuration page. At the top right is a 'Back to integrations' button. The main section is titled 'Basic SAML Settings'. It contains two dropdown menus: 'SAML Intergration active:' set to 'Yes' and 'Disable non-SAML authentication for end users:' set to 'No'. At the bottom are 'Save Settings' and 'Reset' buttons.

- Select **Save Settings**.
- Under SAML Configuration, select **Custom SAML Method** from the **Choose SSO Provider:** drop down list.
- Enter your RSA Identity Provider URL into the **SSO Target URL** field.
- Copy and paste the RSA cert.pem file into the **IdP Signature** window.
- Use the pull down to select **Yes** for those whom should authenticate via SAML.
- Click **Save Settings**.

The screenshot shows the 'SAML Configuration' page. It features a 'Choose SSO Provider:' dropdown menu set to 'Custom SAML Method'. Below it is the 'SSO Target URL' field containing 'https://portal.sso2.pe-lab.com/IdPServlet?idp'. The 'IdP Signature' field contains a long RSA certificate string. At the bottom, there are two dropdown menus: 'Authenticate helpdesk staff using SAML:' set to 'Yes' and 'Authenticate end users using SAML:' set to 'Yes'. 'Save Settings' and 'Reset' buttons are at the bottom.

- The HappyFox admin will need to approve staff's first login, by going to **Manage >> Staff >> Pending SSO accounts**.

GLS