

RSA SecurID Access SAML Configuration for DZone AnswerHub



Last Modified: April 27, 2016

AnswerHub by DZone is enterprise Q &A software that helps people capture and share knowledge and ideas.

Before You Begin

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

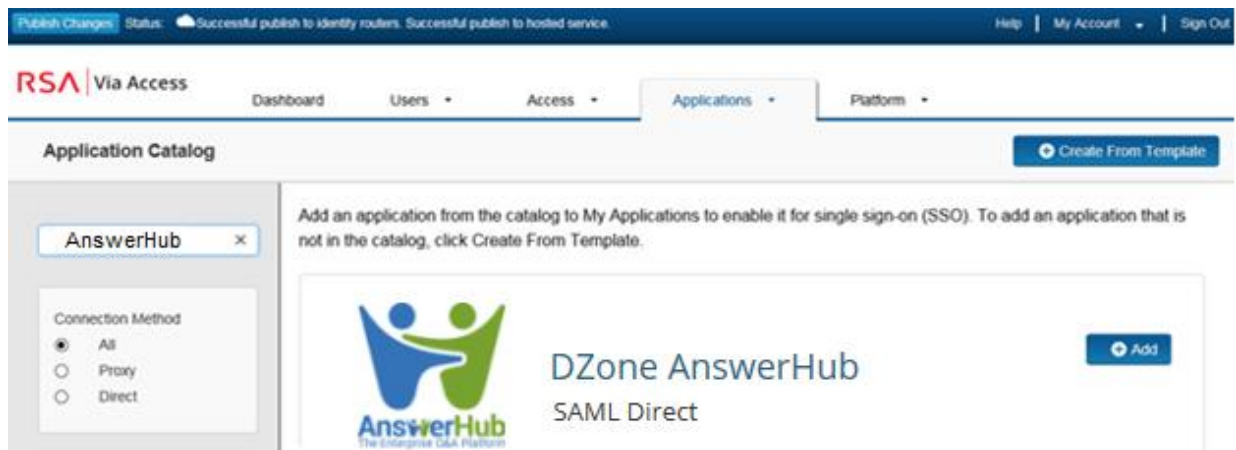
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure AnswerHub 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 SAML application that you wish to add.




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

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

4. In the Initiate SAML Workflow section, select **SP-initiated**.
5. Modify the **Connection URL** with your instance name and select **POST**.

Initiate SAML Workflow

Connection URL 

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

6. Scroll down to the **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): dzonetest

Override

SAML Response Signature ?

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

Private Key Loaded

?

Certificate Loaded

CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion

- In the **Identity Provider URL** field, copy the URL which will be needed later to configure the AnswerHub.
- Select **Choose File** and upload the RSA SecurID Access private key.
- Select **Choose File** and upload the RSA SecurID Access public certificate.

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<your_instance>.answerhub.com/saml/response.html

Audience (Service Provider Entity ID) ?

AnswerHub

- a. Modify the **Assertion Consumer Service (ACS) URL** with your instance name.
Example: <https://rsa.demo2.answerhub.com/saml/response.html>
 - b. Enter AnswerHub in the Audience field.
8. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

DefaultIdentitySourceGroup_I

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

▼ Show Advanced Configuration

Cancel

Next Step →

9. Click **Next Step**.

10. 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 →


11. Click **Next Step**.

12. On the **Portal Display** page, select **Display in Portal**.

13. Click **Save and Finish**.

14. Click **Publish Changes**. Your application is now enabled for SSO.

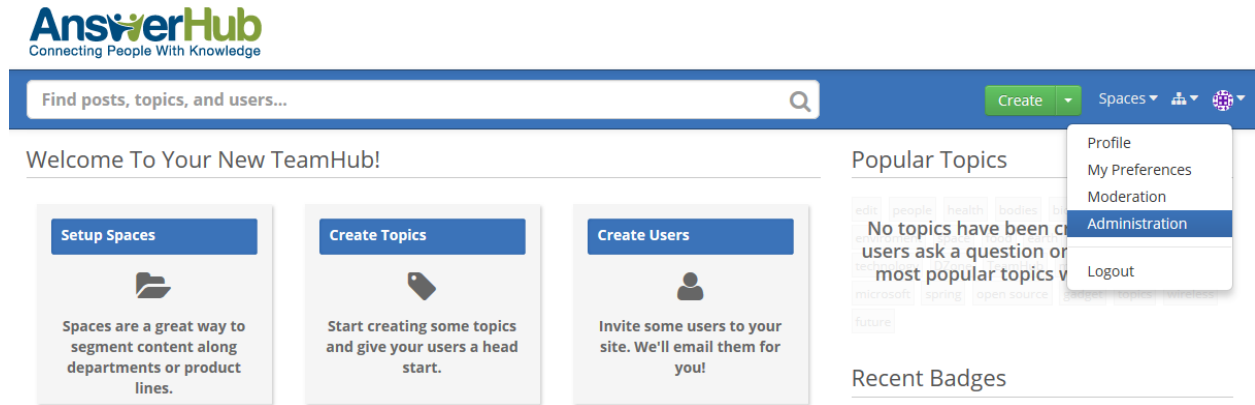
Publish Changes

Status:  Changes Pending

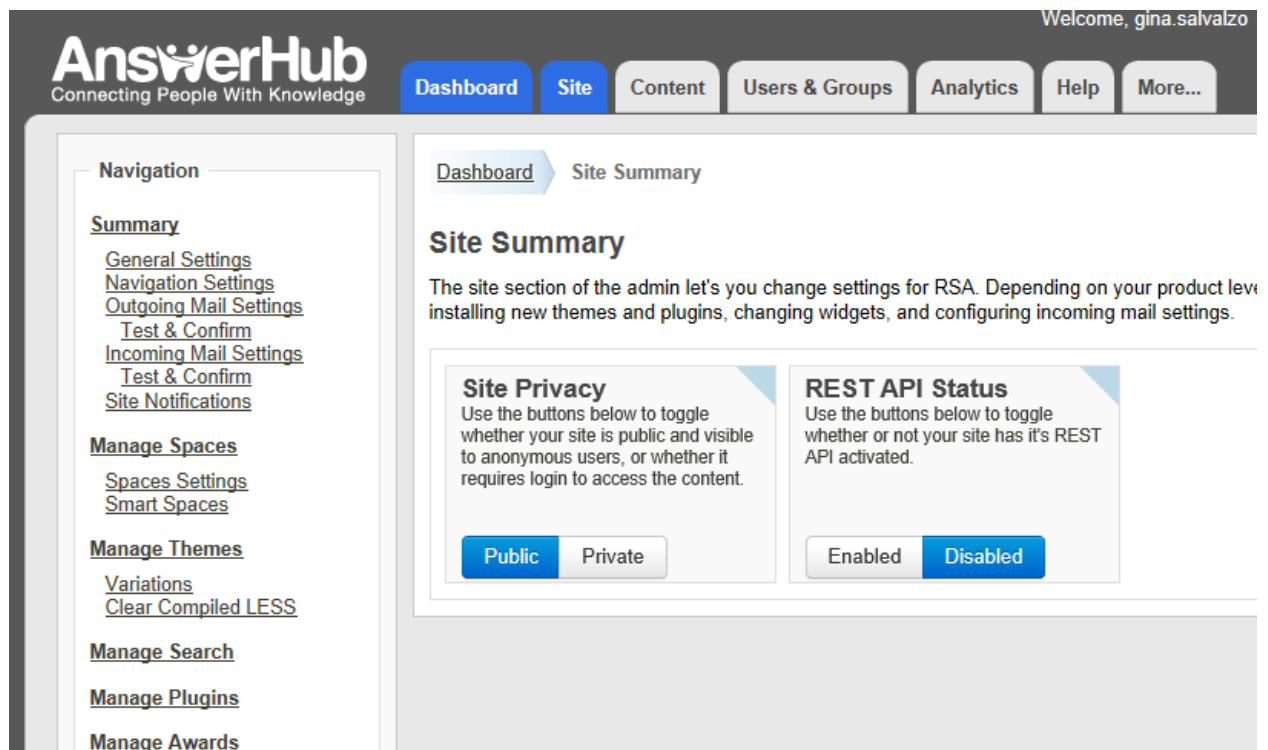
Configure AnswerHub to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the AnswerHub administration console.
https://<your_instance>.answerhub.com/users/login.html?orig=true
2. From the gear pull down pull, select **Administration**.



3. Select the **Site** tab.
4. From the left menu choose **Manage Plugins**.



5. If SAML Auth is not already in the Enabled Plugins list, select the **Disabled Plugins** tab.

[Dashboard](#) > [Plugins](#)


TeamHub Plugins

Enabled Plugins

Disabled Plugins

▼ **Advanced Analytics Package**

Description: Advanced Analytics Package
Vendor: [DZone, Inc.](#)
Plugin Version: 1.0-snapshot

 [Disable plugin](#)


Modules:

request logs interceptor	(Cannot be disabled)
advAnalyticsPersistence	(Cannot be disabled)
advAnalyticsRequestLogActionManager	(Cannot be disabled)
advTrafficAnalytics	(Cannot be disabled)
advUniqueUsersAnalytics	(Cannot be disabled)
advQuestionsAnalytics	(Cannot be disabled)
advAnswersAnalytics	(Cannot be disabled)
advSpaceActivityAnalytics	(Cannot be disabled)

6. Select **SAML Auth** plugin and click **Enable Plugin**.

▼ **SAML Auth**

Description: Provides sso integration SAML IdPs
Vendor: [DZone, Inc.](#)
Plugin Version: 1.0-snapshot

 [Enable plugin](#)

Modules:

jksKeyManager
saml-auth-settings
samlAdminController
samlMetadataController
userServiceController

7. Select the **Users & Groups** tab.
8. Select **SAML Setup** from the left menu.
9. Enter the Identity Provider URL from page 3 step 6, into the **IDP Login URL** field.

The screenshot shows a web application interface with a top navigation bar containing tabs: Dashboard, Site, Content, **Users & Groups**, Analytics, Help, and More... Below this, a breadcrumb trail shows Dashboard > Users > SAML Setup. Under SAML Setup, there are three sub-tabs: IDP Config (selected), Keys and Certificates, and Advanced. The main content area contains the following configuration options:

- If your IDP requires you to tell it the consumer URL of TeamHub, use the following:**
`https://rsa.demo2.answerhub.com/saml/response.html`
- IDP Login URL**
Text input field containing: `https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=dzonetest`
- IDP Logout URL**
Empty text input field
- IDP Login Type (post or redirect)**
Text input field containing: `post`
- IDP Name Identifier Format (emailAddress, transient, unspecified)**
Text input field containing: `emailAddress`
- Use NameID as Username?**
- NameID Is Required In Response?**
- Synchronize Profile Fields On Login?**
- Allow Email As Username?**
- Automatically Validate All Emails?**
- Automatically Create New User Groups?**
- Enable Debug Mode?**

At the bottom of the configuration area, there is a button labeled **SAML Attribute Mapping** with a right-pointing arrow. Below the configuration area is a **Save** button.

10. Enter **post** in the IDP Login Type field.
11. Enter **emailAddress** in the IDP Name Identifier Format field.
12. Select **Use NameID as Username**.
13. Select **NameID is Required in Response?**.
14. Select **Allow Email As Username?**.
15. Select **Automatically Validate All Emails?**.

16. Select **SAML Attribute Mapping**.
17. Enter **nameid** in the IDP Remote Id Attribute Mapping field.
18. Enter **mail** in IDP Username Mapping field.
19. Enter **mail** in IDP Email Mapping field.

▼ **SAML Attribute Mapping**

Use the fields below to define how the SAML attributes map to TeamHub user fields.

IDP Remote Id Attribute Mapping

IDP Username Mapping (attribute to use as TeamHub username)

IDP Email Mapping (attribute to use as TeamHub email)

IDP First Name Mapping (attribute to use as TeamHub first name)

IDP Last Name Mapping (attribute to use as TeamHub last name)

IDP Location Mapping (attribute to use as TeamHub location)

IDP Company Mapping (attribute to use as TeamHub company)

20. Click **Save**.

21. On the SAML Setting page, select the **Advanced** tab.
22. Select **Should Emails be used to match local users against IDP users?**.

IDP Config Keys and Certificates **Advanced**

AuthRequest: Issuer Value Override

AuthRequest: Relay State URL

AuthRequest: Consumer URL Override

Bypass Signature Validation?

Force Requested Authn Context?

Don't Send SPNameQualifier in NameldPolicy?

Perform Role Attribute Check?

Allow Access If No Role Attribute is Found?

Attribute to Match for Role

Regex to Verfiy Role

Redirect To Remote Site To Grant Access?

Access Grant Url

Should Emails be used to match local users against IDP users?

23. Select **Save**.