RSA SecurID Access SAML Configuration for Sumo Logic

Last Modified: August 23rd, 2016

Sumo Logic is a cloud-based log management and analytics service that leverages machine-generated big data to deliver real-time IT insights. Headquartered in Redwood City, California, Sumo Logic was founded in April 2010 by ArcSight veterans Kumar Saurabh and Christian Beedgen.

Before You Begin

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

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

Login URL	*https://service.us2.sumologic.com/sumo/saml/get/gslab*
	https://service.us2.sumologic.com/sumo/saml/post/gslab
ACS URL	*https://service.us2.sumologic.com/sumo/saml/consume/366214111*
Service Provider Issuer ID	*https://service.us2.sumologic.com*

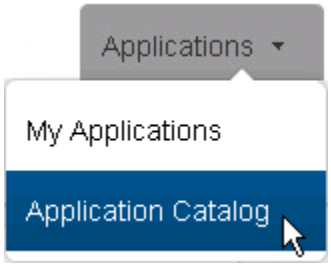
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Sumo Logic 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.

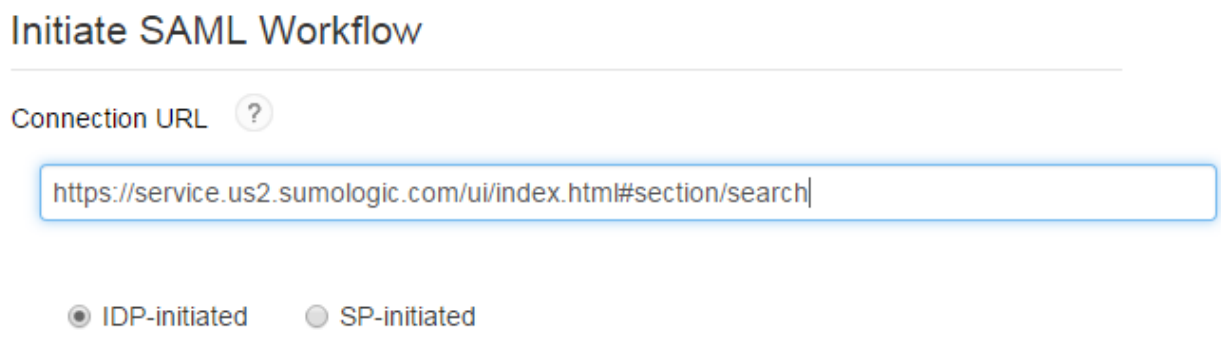


2. Search for *Sumo Logic* in the list of applications and click the **+Add** button.

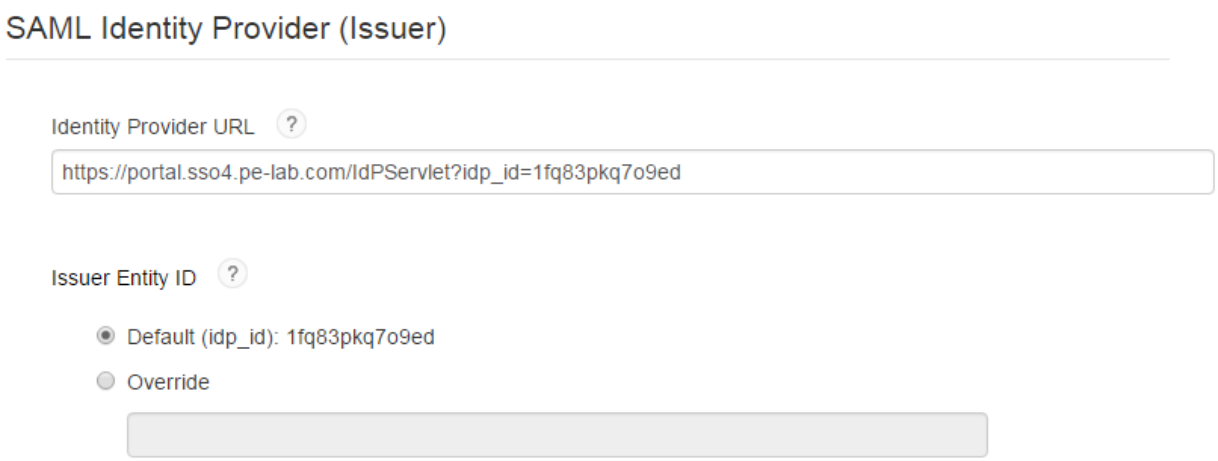
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.
4. Select the **IdP-initiated** radio button in the **Initiate SAML Workflow** section.

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

5. Enter the Sumo Logic landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the Sumo Logic icon.
   The URL is formatted as follows:
   https://service.us2.sumologic.com/ui/index.html#section/search



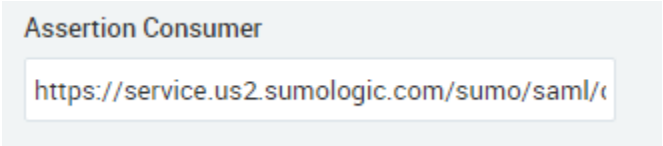
6. Scroll to **SAML Identity Provider (Issuer)** section, copy the value in the **Identity Provider URL** field and paste it into a temporary file. You will need the URL when you configure your Sumo Logic service provider.
7. Also note down **Issuer Entity ID** given default. Or you can also change default value by clicking **Override** radio button. You will need this value when you configure your Sumo Logic service provider.



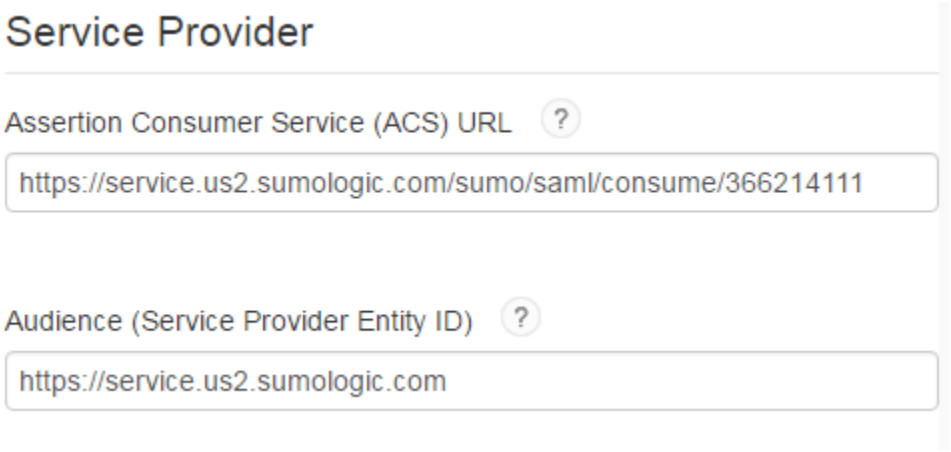
8. You must import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 8.
    a. Click the **Generate Certificate Bundle** button in the **SAML Response Signature** section.
    b. In the **Common Name (CN)** field, enter the hostname of the Sumo Logic 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.
9. 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.
10. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
11. Select the **Include Certificate in Outgoing Assertion** checkbox.

12. Scroll to the **Service Provider** section and enter your Sumo Logic ACS_URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: *https://*service.us2.sumologic.com/sumo/saml/consume/<unique_number>

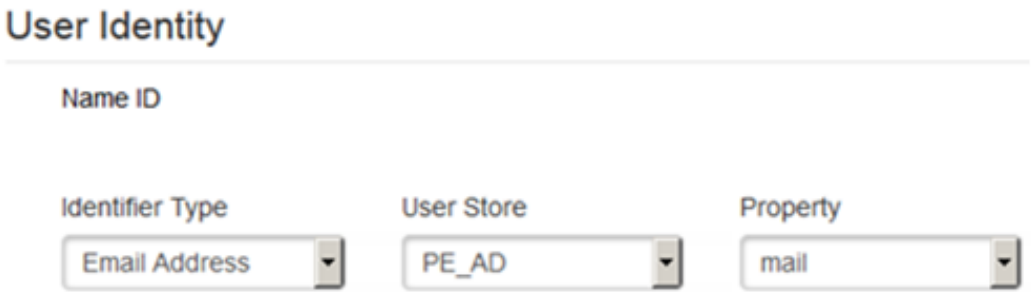
    You will find <unique_number> when you complete integration of **Sumo Logic** with **RSA SecurID Access** in the section **Assertion Consumer** at the end.



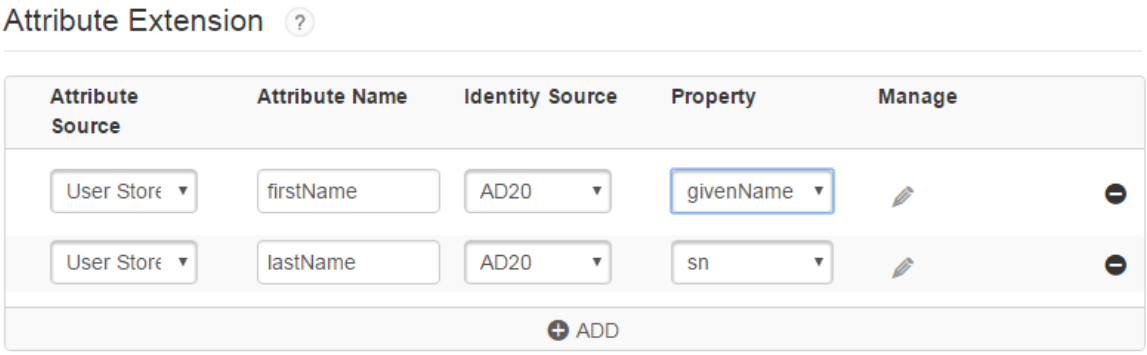
13. Enter *https://service.us2.sumologic.com* in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your Sumo Logic SP Issuer ID.



14. 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 **Identifier Source** dropdown list. In this example, user accounts are stored in an identity source named *PE_AD*.
15. 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.



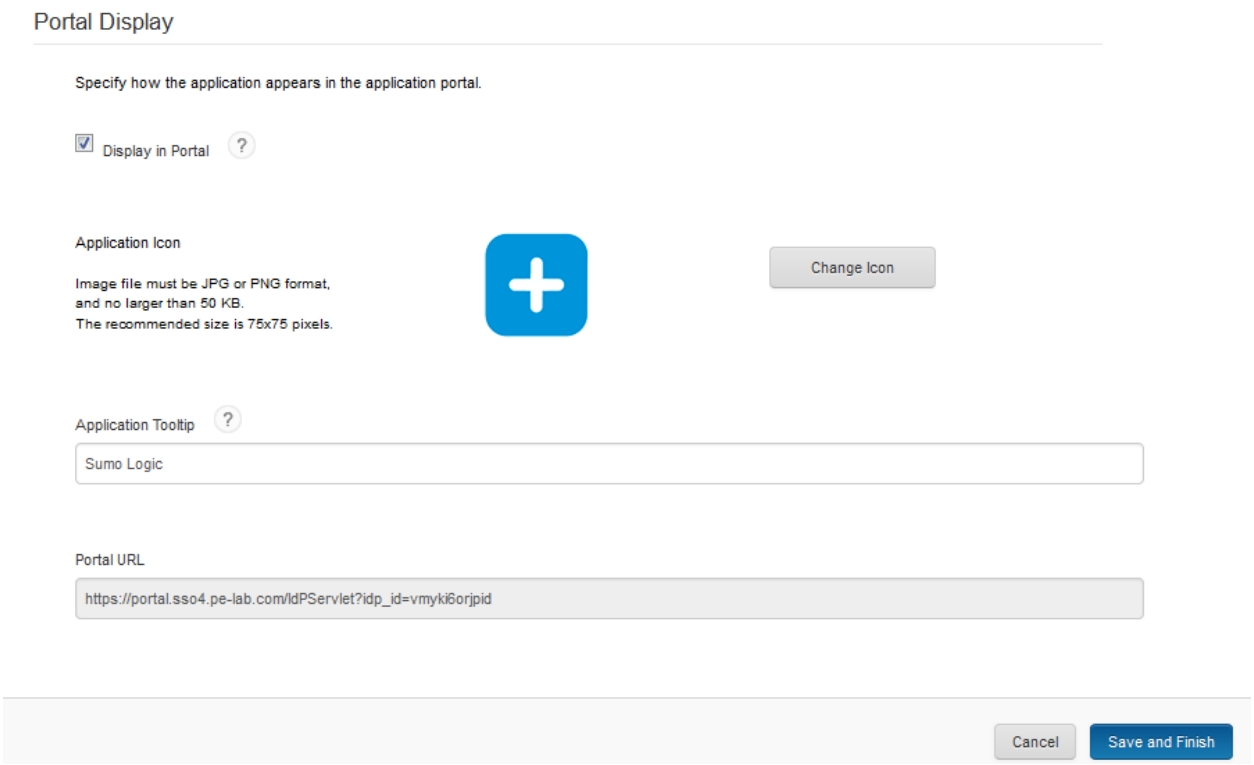
16. In **Advanced Configuration**, you can add additional attributes such as First Name, Last Name. You will need them if you want to create new users on Demand Provisioning.



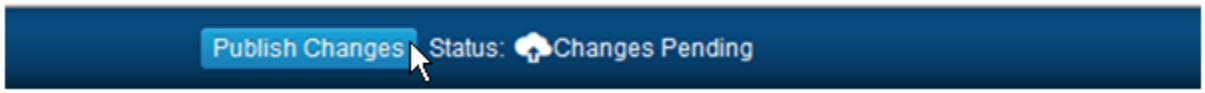
17. Click the **Next Step** button.
18. On the **User Access** page, select the access policy the identity router will use to determine which users can access the Sumo Logic service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow 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.

19. Click the **Next Step** button.
20. Select the **Display in Portal** checkbox on the **Portal Display** page.
21. 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.

22. Click the **Save and Finish** button.



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

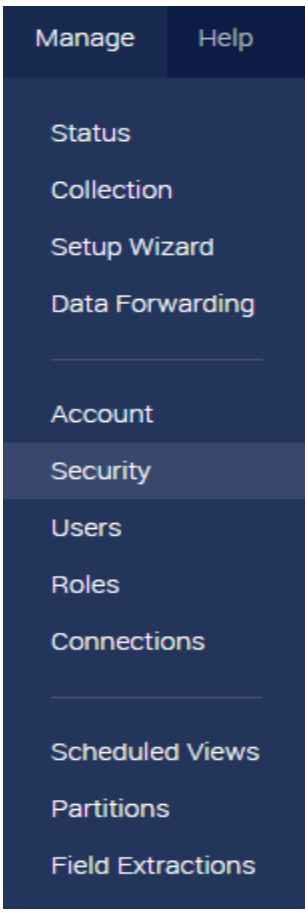


Configure Sumo Logic to Use RSA SecurID Access as an Identity Provider

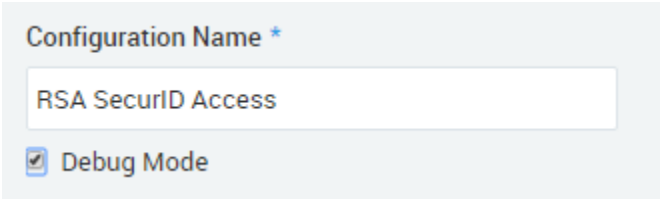
Procedure

Create an Identity Provider

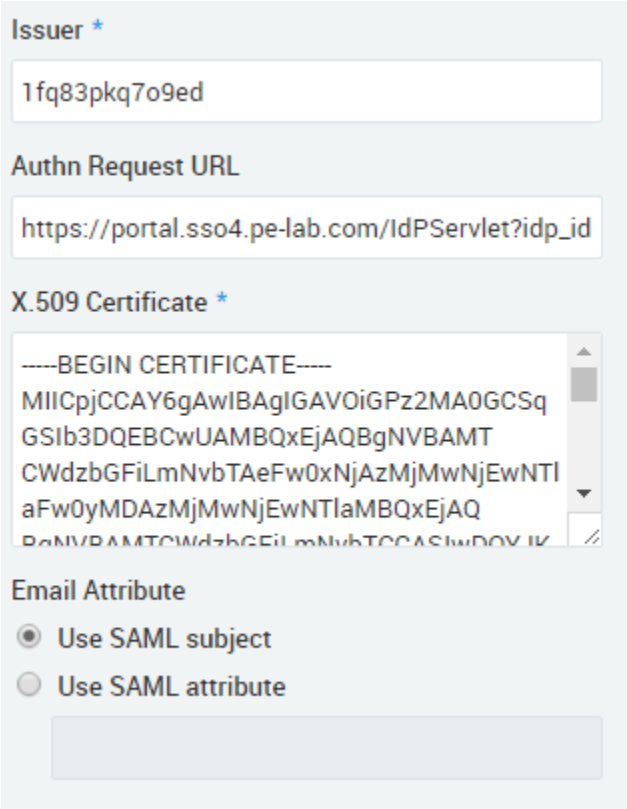
1. Log in to your Sumo Logic admin account and click *Manage -> Security*.



2. Click **SAML** button.
3. Enter name in **Configuration Name** which you want to give to this SAML configuration.
4. Select **Debug Mode** option if you'd like to view additional details if an error occurs when a user attempts to authenticate.

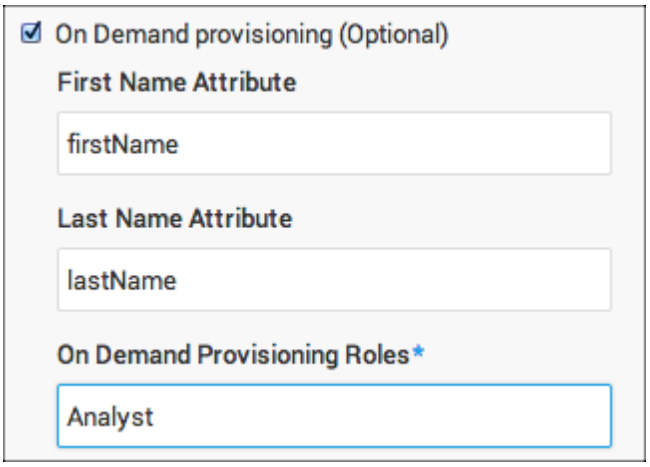


5. Enter RSA SecurID Access Issuer Entity ID in the field **Issuer**.
6. Enter your RSA SecurID Access Identity Provider URL in the **Authn Request URL** field.
7. Copy **X509Certificate** from the IdP metadata file you exported from RSA SecurID Access and paste in **X.509 Certificate** field.
8. In **Email Attribute**, select **Use SAML subject**, or select **Use SAML attribute** and type the email attribute name in the text box.



9. **SP Initiated Login Configuration** (Optional): Enter a unique identifier for your organization. You can specify any alphanumeric string, provided that it is unique to your organization.
   The identifier is used to generate a unique URL for user login. For example, if you enter "gslab", then login URL for Redirect binding and Post binding are as follows respectively:
   Redirect: https://service.us2.sumologic.com/sumo/saml/get/gslab
   POST: https://service.us2.sumologic.com/sumo/saml/post/gslab

10. **On Demand Provisioning** (Optional): Select this option and specify the following attributes to have Sumo Logic automatically create accounts when a user first logs on.
    a. **First Name Attribute** You'll need to add **firstName** attribute from Property drop down in RSA SecurID Access Attribute Extension.
    b. **Last Name Attribute** You'll need to add **lastName** attribute from Property drop down in RSA SecurID Access Attribute Extension.

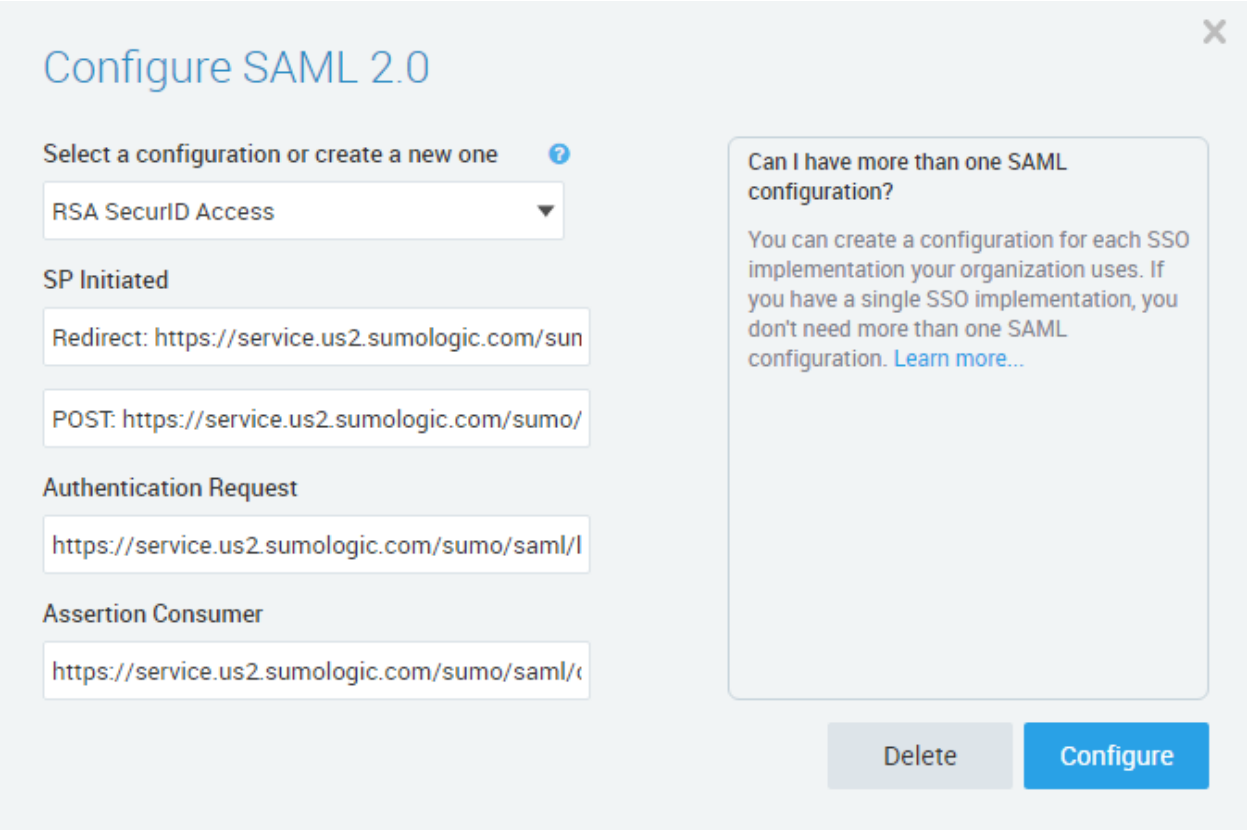


11. **On Demand Provisioning Roles** : Enter roles which you want to assign to users when they first log on. These roles also need to send as part of your assertion.
    a. Each role in the assertion must be in its own AttributeValue.
    b. The AttributeValue values of the SAML assertion must match the role names configured in Sumo Logic.
12. **Roles Attribute:** Enter the SAML Attribute Name that is sent by the RSA SecurID Access as part of the assertion.

13. Click **Save**.

Review your configuration settings:

You will find configuration information after completing all settings like below.



MD