RSA SECURID® ACCESS
Implementation Guide

Dell Boomi

Gina Salvalzo, RSA Partner Engineering
Last Modified: August 20, 2018

RSA READY

Solution Summary

Dell Boomi specializes in cloud-based integration, API management and Master Data Management. Dell Boomi supports multi-factor authentication through SAML 2.0 via the service-provider login page or the RSA identity provider portal. Dell Boomi does not support just in time user provisioning.

RSA SecurID Access Features	Dell Boomi
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

All of the supported use cases of RSA SecurID Access with Dell Boomi require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Dell Boomi can be integrated with RSA Cloud Authentication Service in the following ways:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Dell Boomi SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Dell Boomi in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

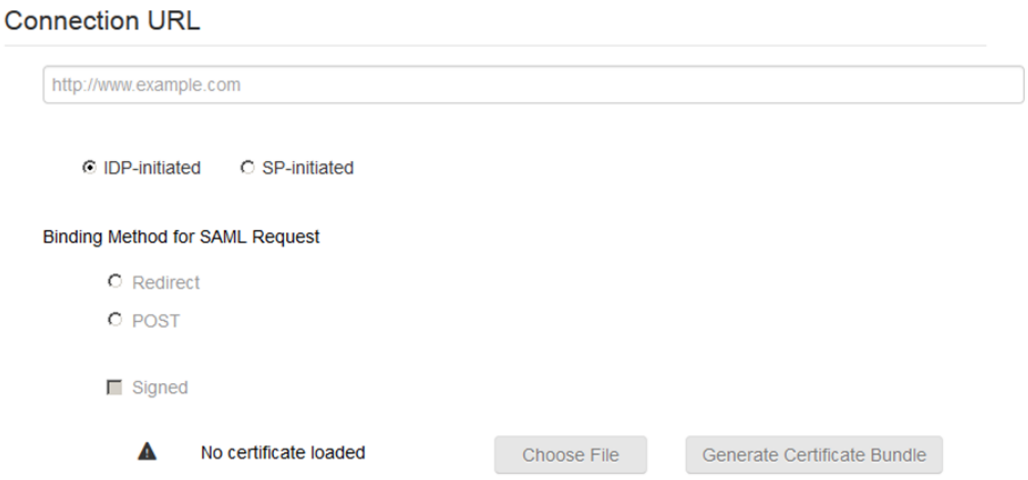
Configure RSA Identity Router SAML IdP

Procedure

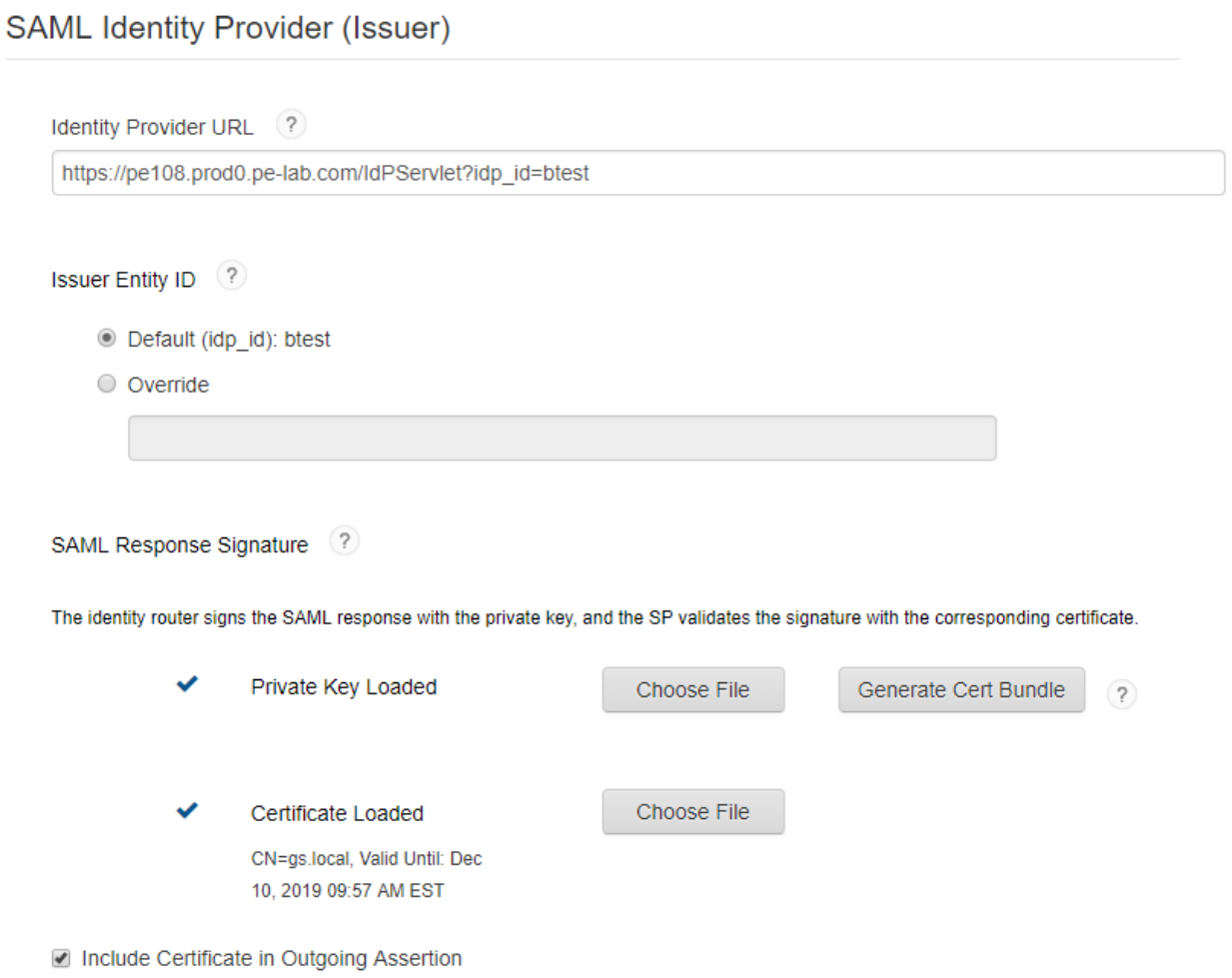
1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Dell Boomi and click **+Add** to add the connector.

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
   a. In the **Connection URL** field, leave the field blank.
   b. Choose **IDP-initiated**.

Note: The following IDP-initiated configuration works for SP-initiated connections as well. The SSO SP login URL is https://platform.boomi.com/AtomSphere.html#build;accountId=<accountID>.



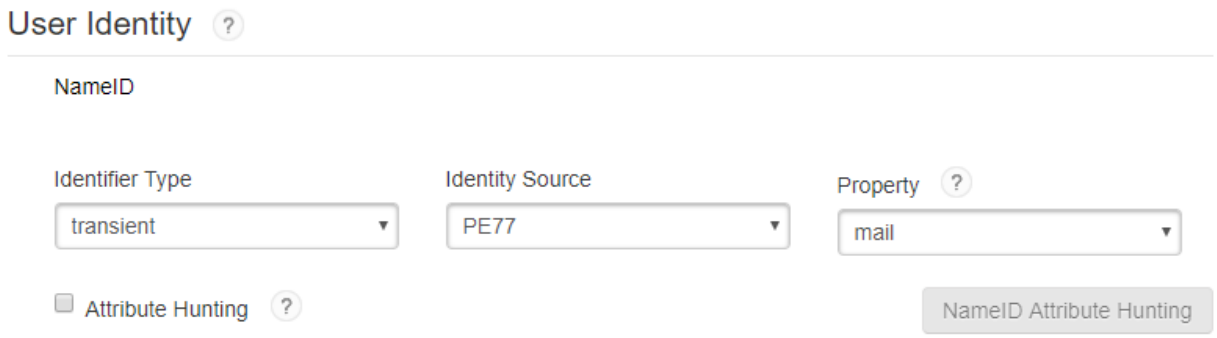
4. Scroll down to SAML Identity Provider (Issuer) section.



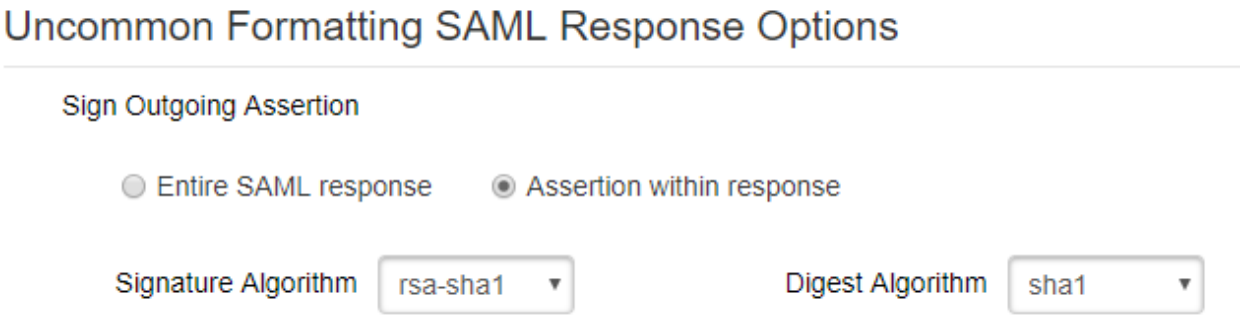
a. Take note of the **Identity Provider URL**.
b. Select **Choose File** and upload the private key.
c. Select **Choose File** to import the public signing certificate.
d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

6. In the **Assertion Consumer Service (ACS) URL** field replace **<accountID>** with your account ID.
7. In the **Audience (Service Provider Entity ID)** field replace **<accountID>** with your account ID.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the Identity Type is **transient** and presented in **mail** format.

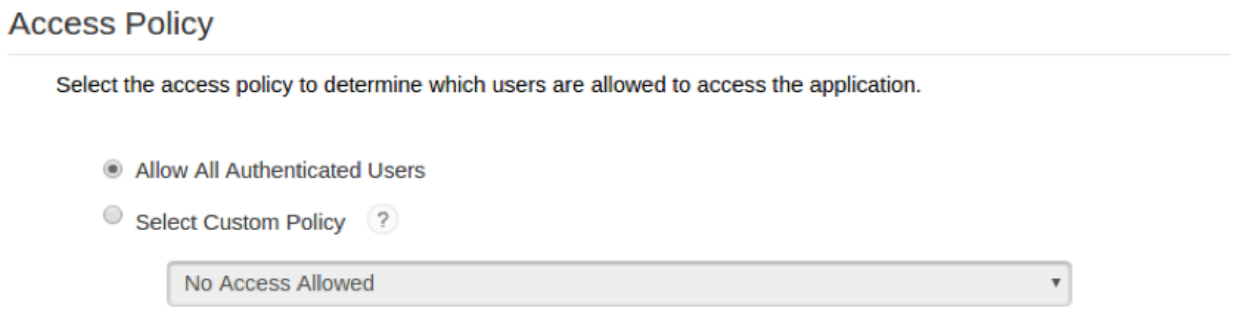


9. Click **Show Advanced Configuration**.
10. Under Uncommon Formatting SAML Response Options, select **Assertion within response**.

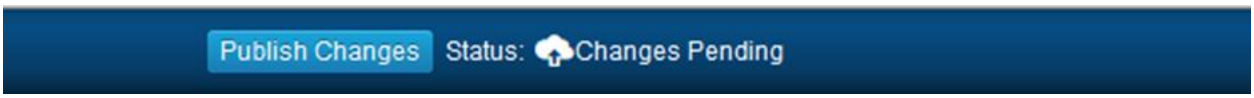


11. Click **Next Step**.

12. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



13. Click **Next Step**.
14. On the Portal Display page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.



Next Steps

[Dell Boomi SAML Configuration]

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Dell Boomi with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Dell Boomi components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

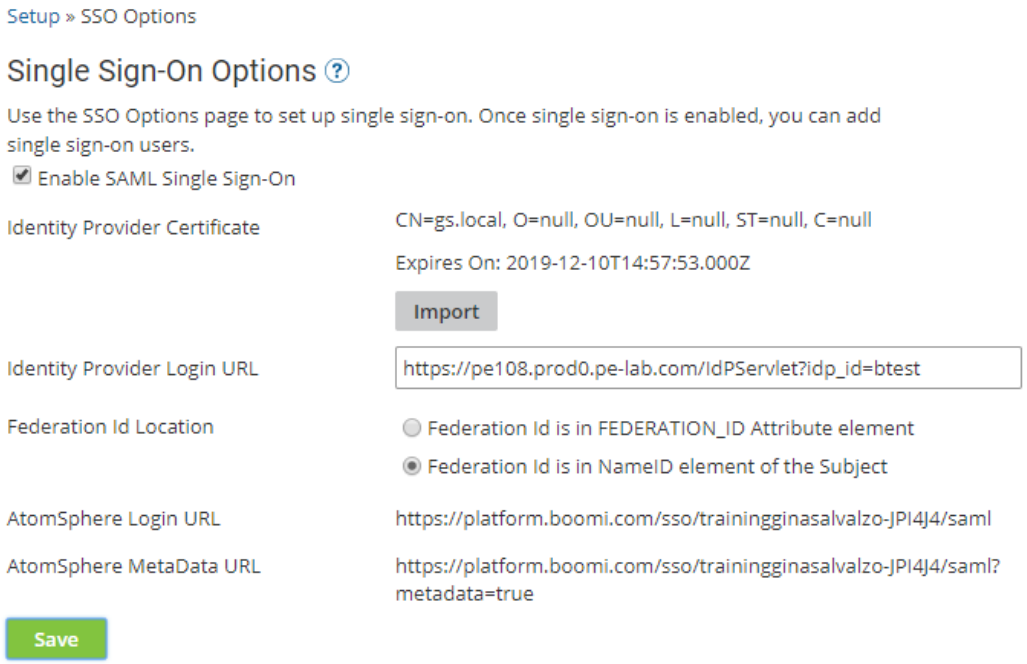
Dell Boomi SAML Configuration

Complete the steps in this section to integrate Dell Boomi with RSA SecurID Access using SAML authentication protocol.

Procedure

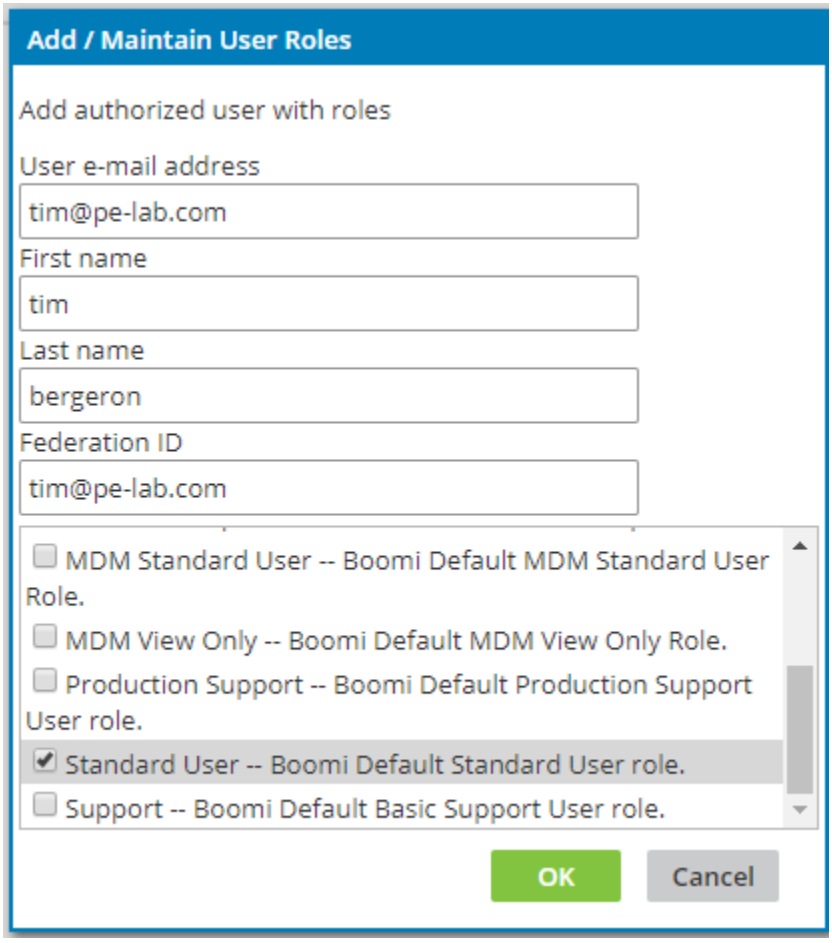
1. Login into the Dell Boomi administration console. **https://platform.boomi.com**
2. Under the account name pulldown select **Setup**.
3. Navigate to **Security Options > SSO Options**.
4. Select the checkbox for **Enable SAML Single Sign-On**.
5. Select the **Import** button and choose the **public certificate** in .cer format when configuring for IDR IDP. Choose **Signing certificate** when configuring for Cloud IDP.

6. In the Identity Provider Login URL, enter the **Identity Provider URL** when configuring for IDR IDP or enter the **Cloud IDP URL** when configuring for Cloud IDP.
7. Choose **Federation Id is in NameID element of the Subject** for the Federation Id Location option.



8. Click **Save**.

9. Navigate to **Setup > Account Access > User Management**.
10. Add a user.



11. Enter values for **User e-mail address, First name** and **Last name**.
12. Enter the user's email address as the **Federation ID**.
13. Select a role for the user.
14. Click **OK**.

Note: The SP initiated login URL is https://platform.boomi.com/AtomSphere.html#build;accountId=<accountID>.