RSA SECURID® ACCESS
Implementation Guide

HostedGraphite

Gina Salvalzo, RSA Partner Engineering
Last Modified: September 12, 2017

RSA READY

HostedGraphite

Solution Summary

Hosted Graphite is a provider of metric collection, storage and visualization services.
Hosted Graphite is a monitoring service for development teams who run applications. It takes the data produced by your apps and servers, visualize it on graphs, then let you act upon the data provided. This integration supports both IdP and SP initiated authentication flows.

RSA SecurID Access Features	
HostedGraphite	
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 HostedGraphite 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 – HostedGraphite can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
HostedGraphite 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 HostedGraphite 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.

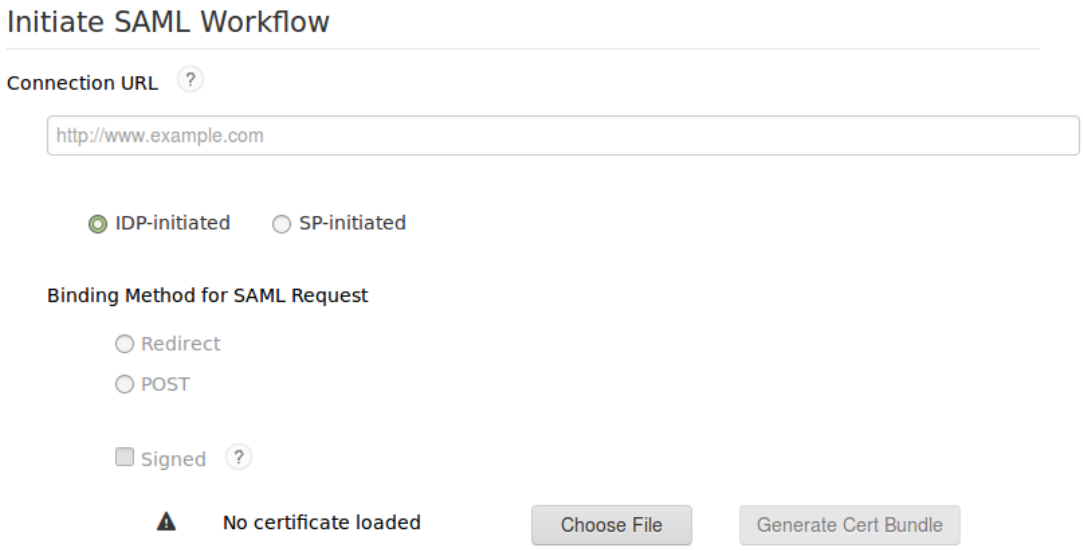
Configure RSA Identity Router SAML IdP

Procedure

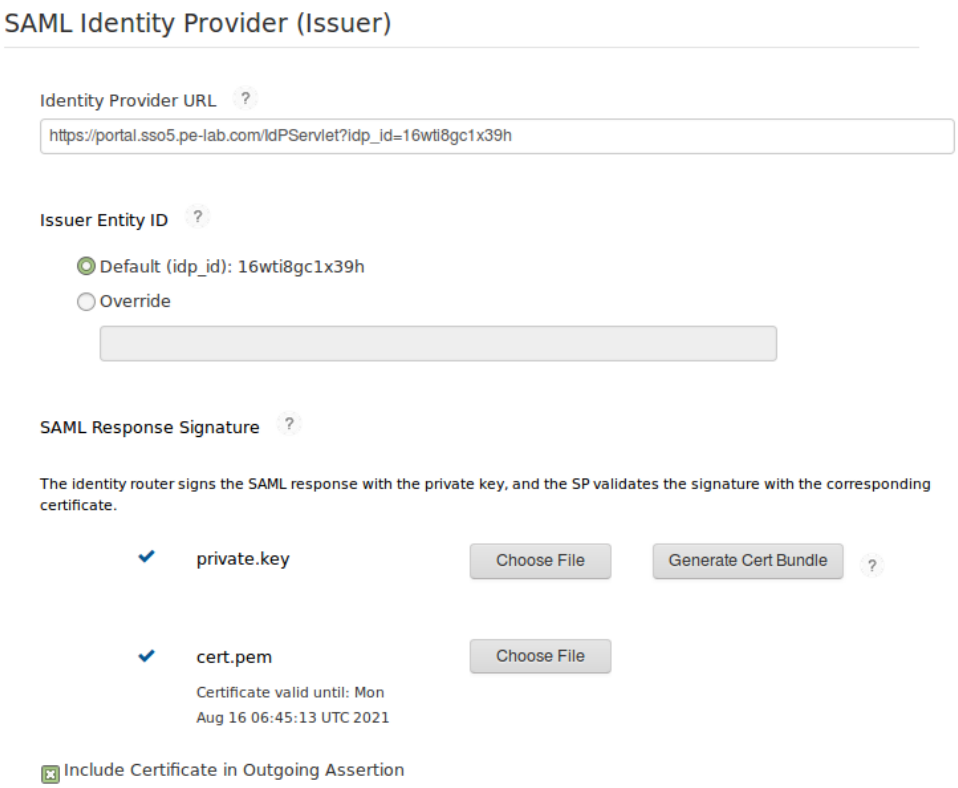
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for HostedGraphite and click **+Add** to add the connector.

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, keep the field blank as the value is not required.
    b. Choose **IDP-initiated.**

Note: The following IdP-initiated configuration works for SP-initiated HostedGraphite connections as well. **https://www.hostedgraphite.com/login/saml/79980ee5/**

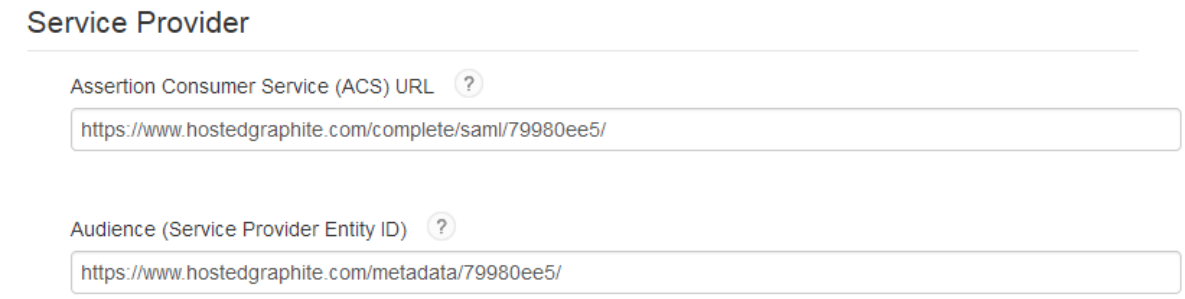


4. Scroll down to SAML Identity Provider (Issuer) section.

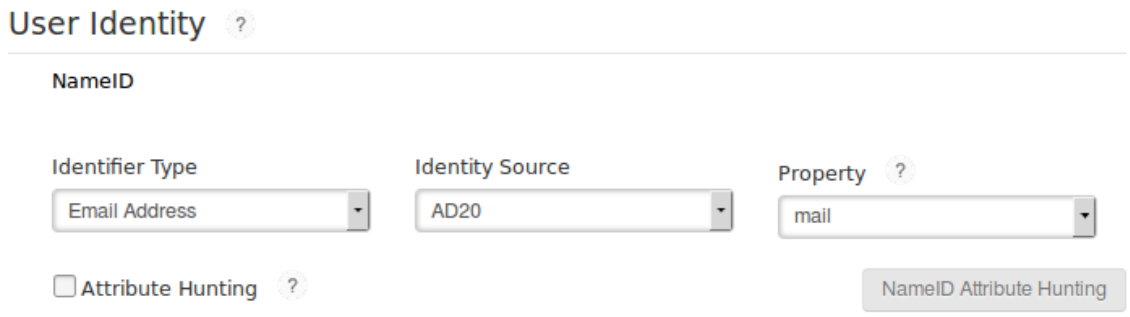


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
   c. Select **Choose File** and upload the private key.
   d. Select **Choose File** to import the public signing certificate.
   e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

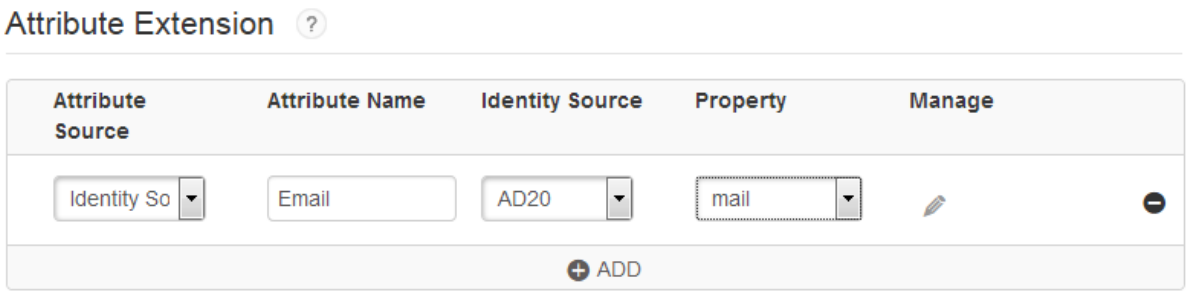
5. Scroll down to the **Service Provider** section.



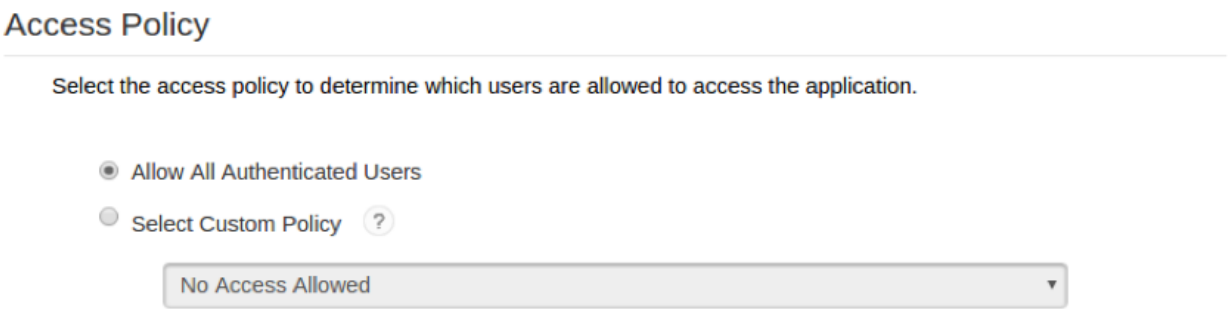
6. In the **Assertion Consumer Service (ACS) URL** field, verify the vault from the HostedGraphite SAML Setup page. Refer to page 8 step 2.
7. In the **Audience (Service Provider Issuer ID)** field, verify the value from the HostedGraphite SAML Setup page. Refer to page 8 step 2.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



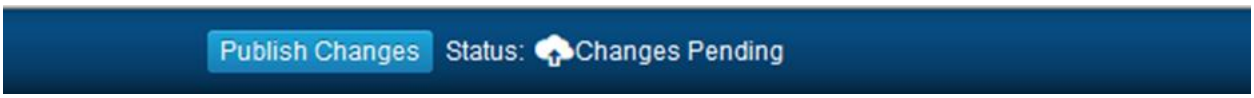
9. Moving on, select **Show Advance Configuration.**
10. In the **Attribute Extension** section, add **Email**. This is mandatory provisioning attribute needs to be forwarded at the time of SSO.



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



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



Partner Product Configuration

Before You Begin

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

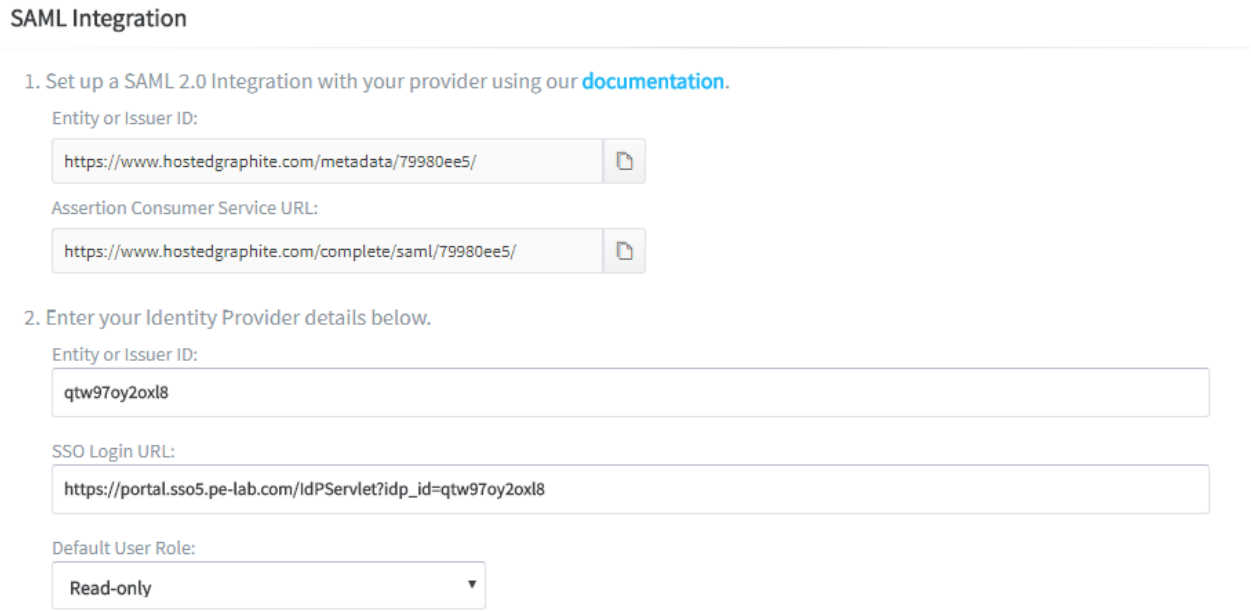
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

HostedGraphite SAML Configuration

Procedure

1. Login to your HostedGraphite application web account.
   https://www.hostedgraphite.com/accounts/login/
2. Go to the **Access > SAML setup** page to enter details from RSA SecurID Access.
   a. In the **Entity ID** field, enter RSA SecurID access's **Issuer URL**.
   b. In the **SSO Login URL** field, enter RSA SecurID access's **SSO URL**.
   c. Select the default user role for new team members.



3. In the certificate text box, paste your **public certificate** which you copied earlier.
4. Click **Save.**

Save