

RSA SECURID[®] ACCESS

Implementation Guide

HostedGraphite

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

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	✓

HostedGraphite

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.




HostedGraphite
SAML Direct

+ Add

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/>

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 16wti8gc1x39h

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

?

cert.pem

Certificate valid until: Mon
Aug 16 06:45:13 UTC 2021

Include Certificate in Outgoing Assertion

- 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**.

HostedGraphite

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

Service Provider

Assertion Consumer Service (ACS) URL [?](#)

Audience (Service Provider Entity ID) [?](#)

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.

User Identity [?](#)

NameID

Identifier Type

Identity Source



Property [?](#)

Attribute Hunting [?](#)

HostedGraphite

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

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity So ▼	Email	AD20 ▼	mail ▼	 
+ ADD				

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

Access Policy


Select the access policy to determine which users are allowed to access the application.

- Allow All Authenticated Users
- Select Custom Policy ?

No Access Allowed ▼

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

Publish Changes

Status:  Changes Pending

HostedGraphite

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.

SAML Integration

1. Set up a SAML 2.0 Integration with your provider using our [documentation](#).

Entity or Issuer ID:



Assertion Consumer Service URL:



2. Enter your Identity Provider details below.

Entity or Issuer ID:

SSO Login URL:

Default User Role:

HostedGraphite

- 3. In the certificate text box, paste your [public certificate](#) which you copied earlier.
- 4. Click **Save**.

X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIICpjCCAY6gAwIBAgIGAVOIgPz2MA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMT
CWdzbGFILmNvbTAeFw0xNjAzMjMwNjEwNTIaFw0yMDAzMjMwNjEwNTIaMBQxEjAQ
BgNVBAMTCWdzbGFILmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMraYXqMGpvPa+J+rt46Nf5xG1U7Nyle5DCzTNY7uCSAXGgNou7SAN4vAlj9ZGsD
UgVQ20m8QpMkv5cmCNTnNUBAlbhlXpdkSVGcdvvHScB14GC25roNYaswGz10Qxus
F/jPypNMzZcJ6pOzCT0yuWgXlyMqbl/CKuFTo/XUFxU26Sz51Yilhhqqp8MMxpt0
hkShJExvZGH/XFj8LSt5T7rZwQGwqluYZa8oleyxbJSv7QvfiOtNCJv8ZsGgG/qn
qpwPq8lrpd/NkWvyB/+piUnPbbmVhh/gK8eExqPPPr+62KifgRziglpN6GJXJ4q
C...
-----
```

Save

