RSA SECURID® ACCESS
Implementation Guide

TextMagic

Gina Salvalzo, RSA Partner Engineering
Last Modified: October 22, 2018

RSA READY

Solution Summary

TextMagic is a business text-messaging service for sending notifications, alerts, reminders, confirmations and SMS marketing campaigns. TextMagic supports multi-factor authentication through SAML 2.0 via the service-provider login page or the RSA identity provider portal.

When integrated with Identity Router (IdP), RSA provides single sign-on authentication and multi-factor authentication to TextMagic via SP or IDP initiated login. JIT provisioning is supported.

RSA SecurID Access Features	
TextMagic	
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 TextMagic 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 – TextMagic 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]
[TextMagic 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 TextMagic 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

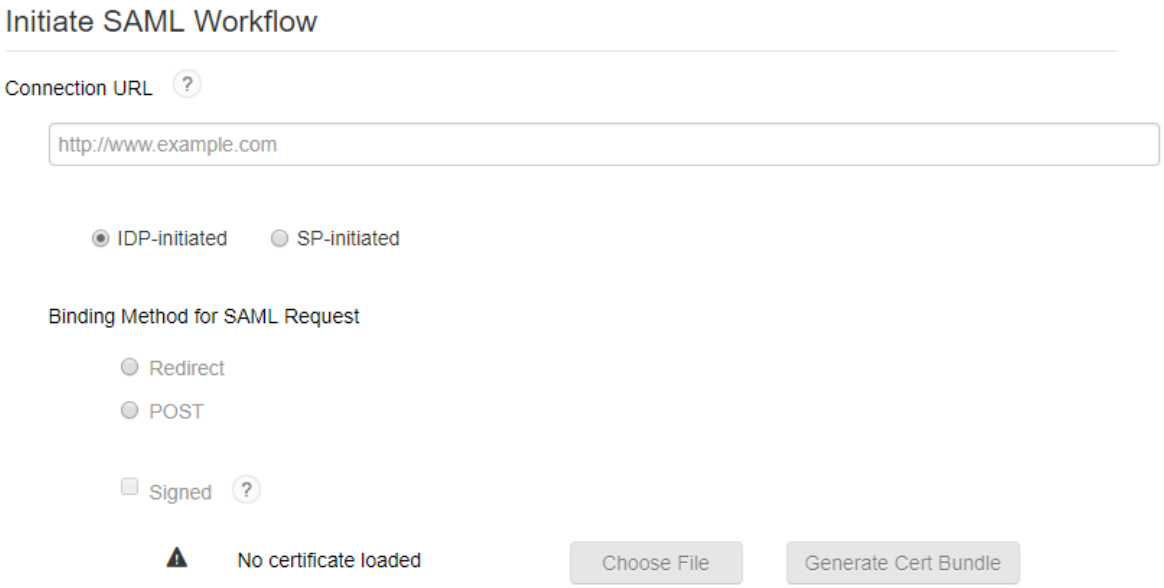
Procedure

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

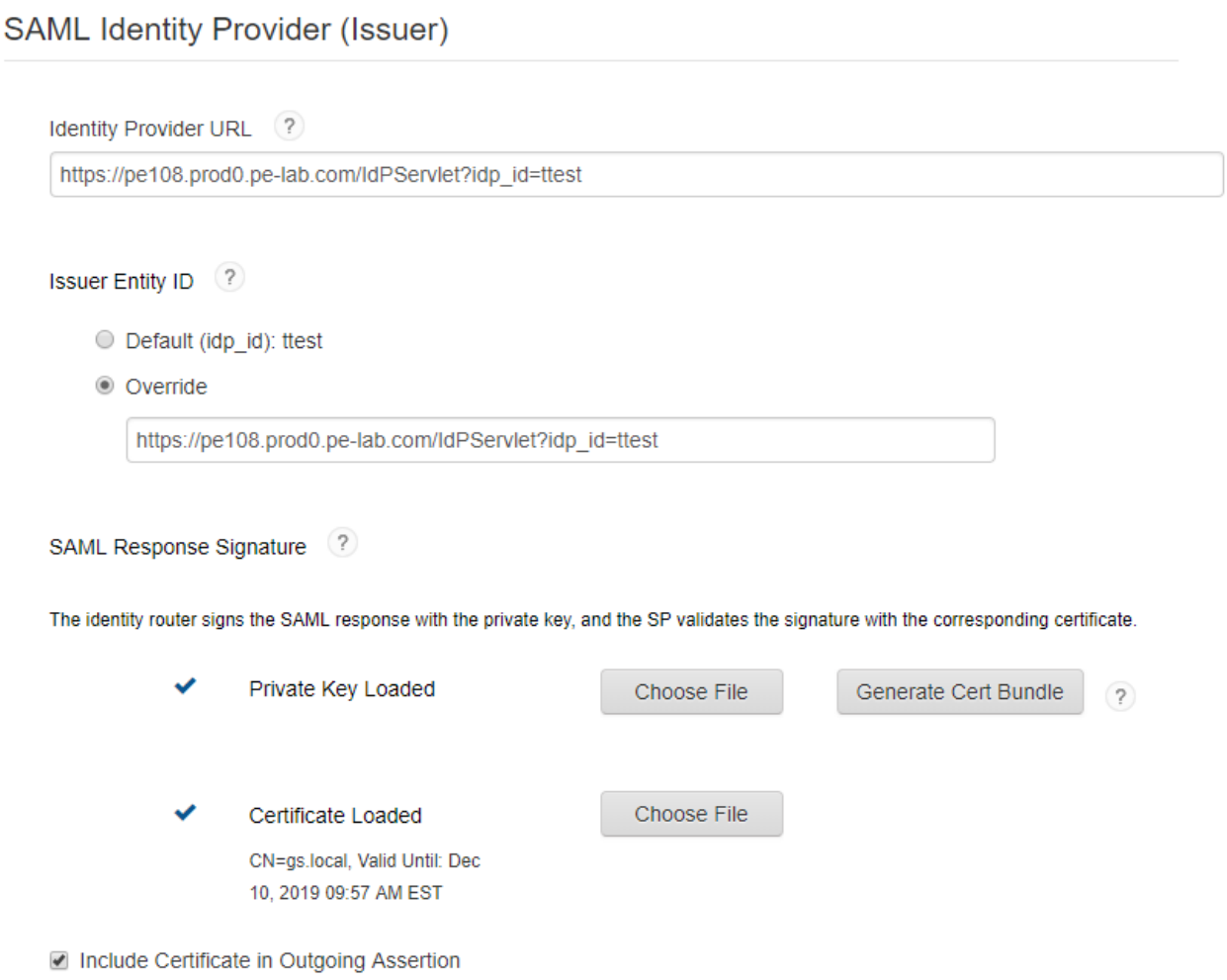
2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.

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 TextMagic connections as well.



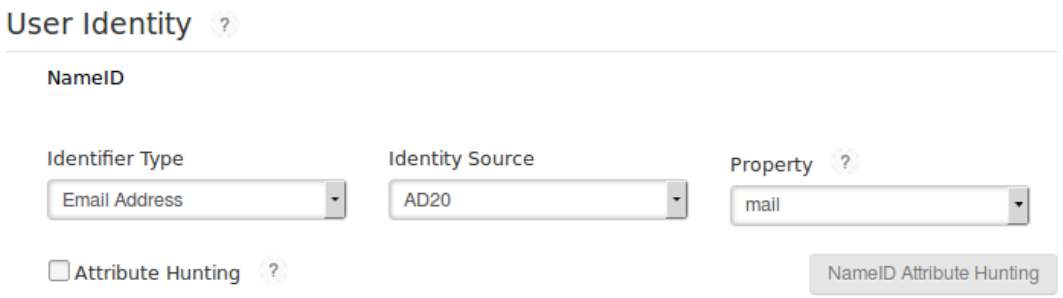
4. Scroll down to SAML Identity Provider (Issuer) section.



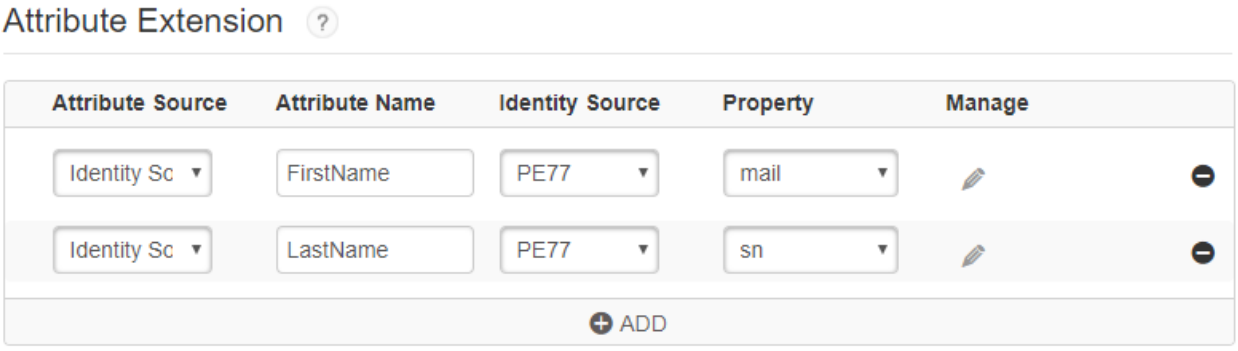
a. Take note of the **Identity Provider URL**.
b. Select the **Issuer Entity ID Override** and paste the Identity Provider URL into the field.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include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

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

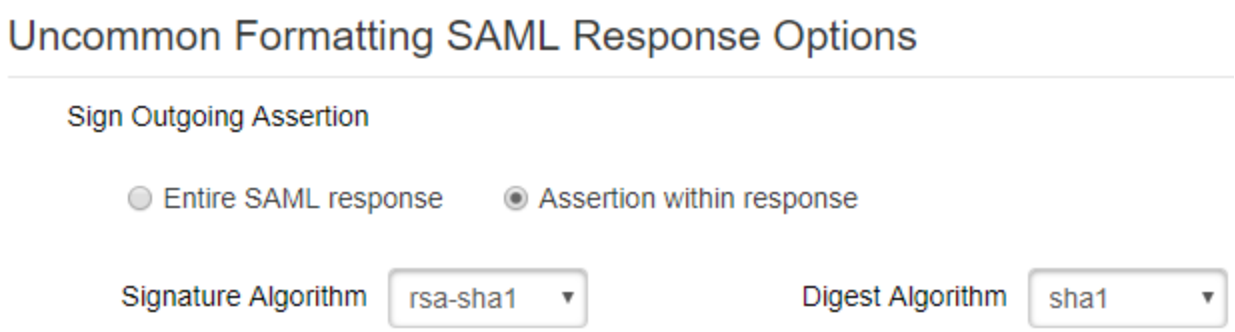
6. Verify the Assertion Consumer Service (ACS) URL field.
7. Verify the Audience (Service Provider Entity ID).
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



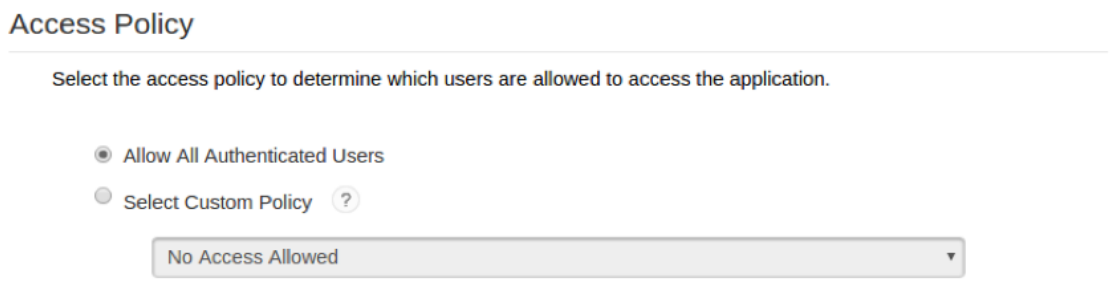
9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attributes **FirstName** and **LastName** with the correlating value from your Active Directory.



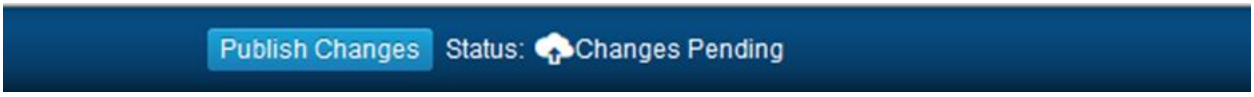
11. Under Uncommon Formatting SAML Response Options, select **Assertion within response**.



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



14. Click **Next Step**.
15. On the Portal Display page, select **Display in Portal**.
16. Click **Save and Finish**.
17. Click **Publish Changes**.



Next Steps

[TextMagic SAML Configuration]

Partner Product Configuration

Before You Begin

This section provides instructions for configuring TextMagic 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.

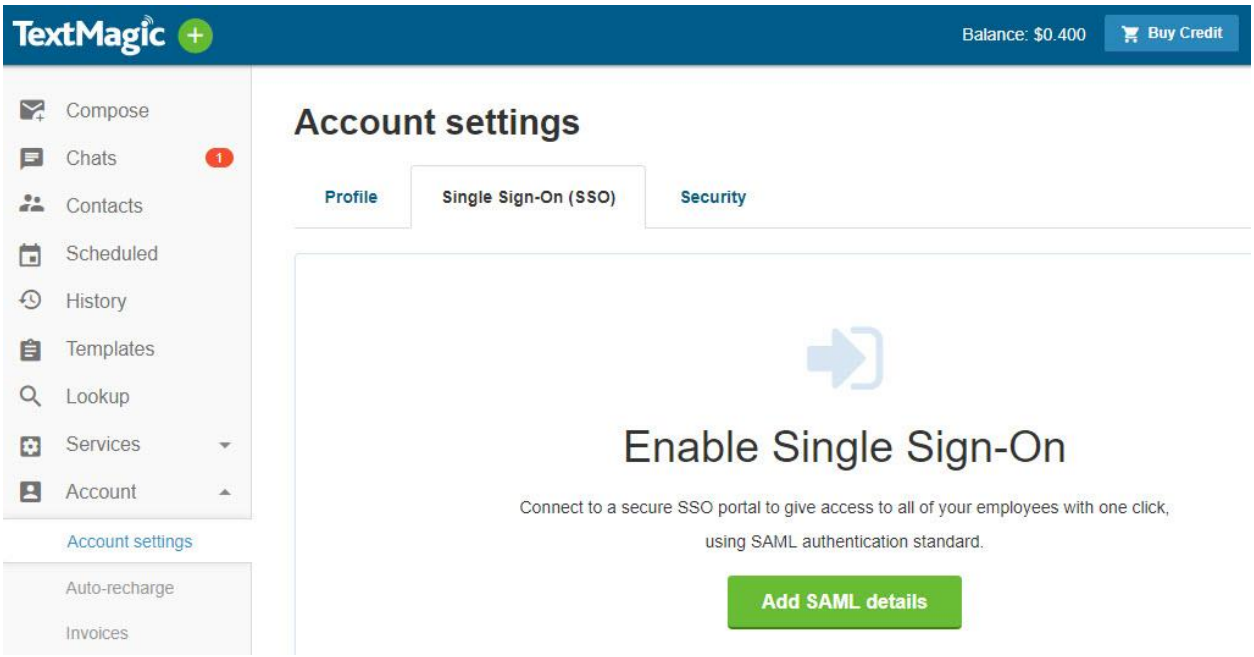
All TextMagic components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

TextMagic SAML Configuration

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

Procedure

1. Login into the TextMagic administration console. **https://my.textmagic.com**
2. Select **Account > Account settings >Single Sign-On (SSO).**



3. Click **Add SAML details**.

4. In the **Identity provider Entity ID** field paste the **Issuer Entity ID Override**.
5. In the **Identity provider SSO URL** paste **Identity Provider URL**.
6. In the **Identity provider SLO URL** enter **https://<portal>/LogoutServlet**.
7. In the Public x509 certificate field paste the **public certificate**.
8. Click **Save**.