

RSA SECURID[®] ACCESS

Implementation Guide

TextMagic

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



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.



TextMagic
SAML Direct




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.**

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded



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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): ttest

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 Loaded

?

✓ Certificate Loaded

CN=gs.local, Valid Until: Dec
10, 2019 09:57 AM EST

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

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.

User Identity ?

NameID

Identifier Type:

Identity Source:

Property ?:

Attribute Hunting ? NameID Attribute Hunting

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

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="Identity Sc"/>	<input type="text" value="FirstName"/>	<input type="text" value="PE77"/>	<input type="text" value="mail"/>	
<input type="text" value="Identity Sc"/>	<input type="text" value="LastName"/>	<input type="text" value="PE77"/>	<input type="text" value="sn"/>	
+ ADD				



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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

- Click **Next Step**.

- 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 ?

- Click **Next Step**.

- On the Portal Display page, select **Display in Portal**.

- Click **Save and Finish**.

- Click **Publish Changes**.

Publish Changes

Status: Changes Pending

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.

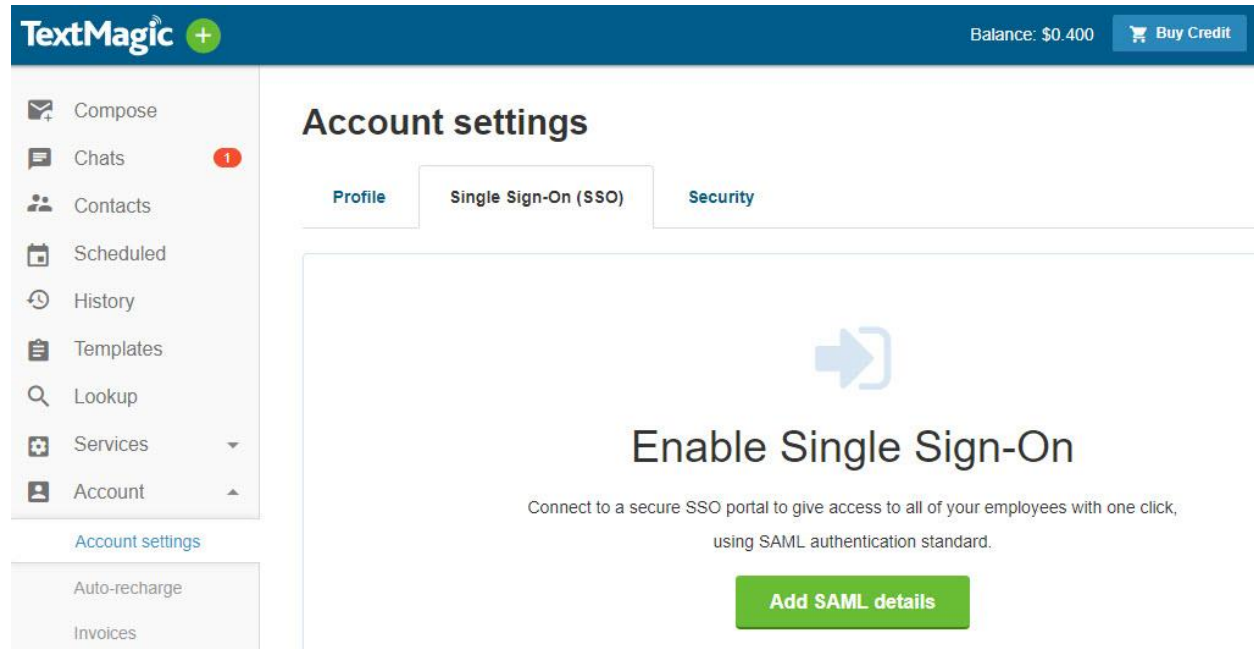
All TextMagic components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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)**.



The screenshot shows the TextMagic administration console interface. The top navigation bar includes the TextMagic logo, a balance of \$0.400, and a 'Buy Credit' button. The left sidebar contains various navigation options: Compose, Chats (with a notification badge), Contacts, Scheduled, History, Templates, Lookup, Services, and Account. The 'Account settings' section is expanded, showing 'Account settings', 'Auto-recharge', and 'Invoices'. The main content area is titled 'Account settings' and has three tabs: 'Profile', 'Single Sign-On (SSO)', and 'Security'. The 'Single Sign-On (SSO)' tab is active, displaying a large blue arrow icon and the heading 'Enable Single Sign-On'. Below the heading, there is a sub-instruction: 'Connect to a secure SSO portal to give access to all of your employees with one click, using SAML authentication standard.' A green button labeled 'Add SAML details' is positioned at the bottom of the main content area.

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**.

Account settings

[Watch tutorial](#)

Profile

Single Sign-On (SSO)

Security

SAML details

Identity provider Entity ID*	<input type="text" value="https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=ttest"/>
Identity provider SSO URL*	<input type="text" value="https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=ttest"/>
Identity provider SLO URL	<input type="text" value="https://pe108.prod0.pe-lab.com/LogoutServlet"/>
Public x509 certificate*	<pre>-----BEGIN CERTIFICATE----- MIICXzCCBgwzAQIBADCBMAUGA1UdGAAQK3fYU7Q7xRVhKMUYW/Z8aqCjpDTmho5peceqDdzZI Y9D6ZualZA9 Xl8OP0uB6s+qxwRnAJTqXa48/2i8QbPZV8SLe5l13TVwG5L48wCpx wBsoLbM0I5r XeoN8j2YCO0= -----END CERTIFICATE-----</pre>
Force SSO only	<input type="checkbox"/> Allow users to login only using Single Sign-On <small>Allow users to login to TextMagic only via SSO. Parent user will still be able to log in using SSO and regular credentials.</small>

[Cancel](#)

Save