RSA SECURID® ACCESS
Implementation Guide

Velpic

Gina Salvalzo, RSA Partner Engineering
Last Modified: March 07, 2018

RSA READY

Solution Summary

Velpic is a cloud-hosted learning management system designed to simplify and streamline workplace training. You can create, deliver and report on videos very easily. This integration supports single sign-on via SAML for IdP initiated and SP initiated authentication flows. Velpic application support auto-provisioning of the user.

RSA SecurID Access Features	Velpic
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 Velpic 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 – Velpic 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
Velpic 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 Velpic 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

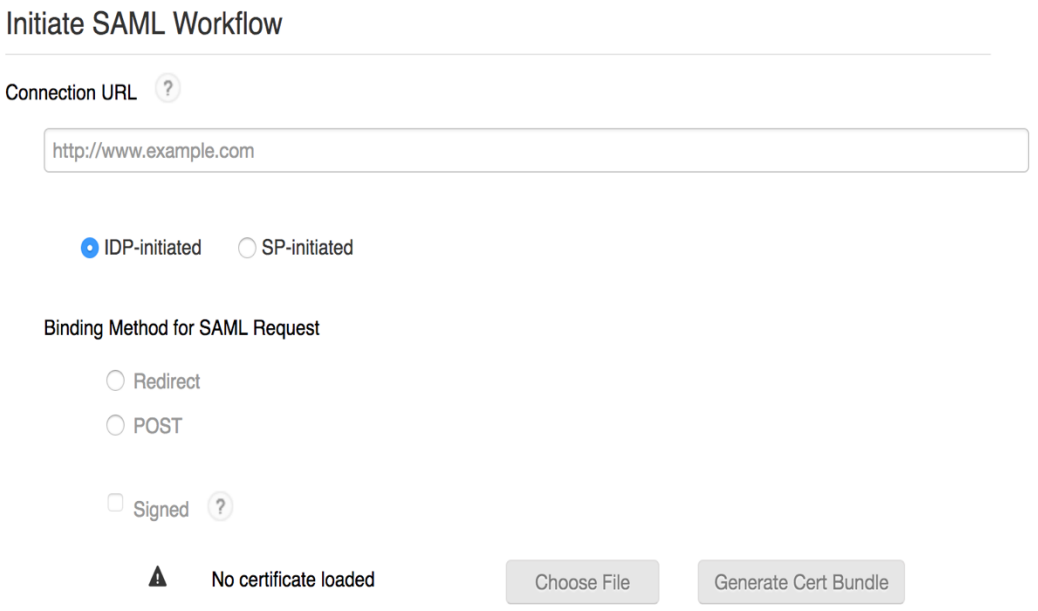
Procedure

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

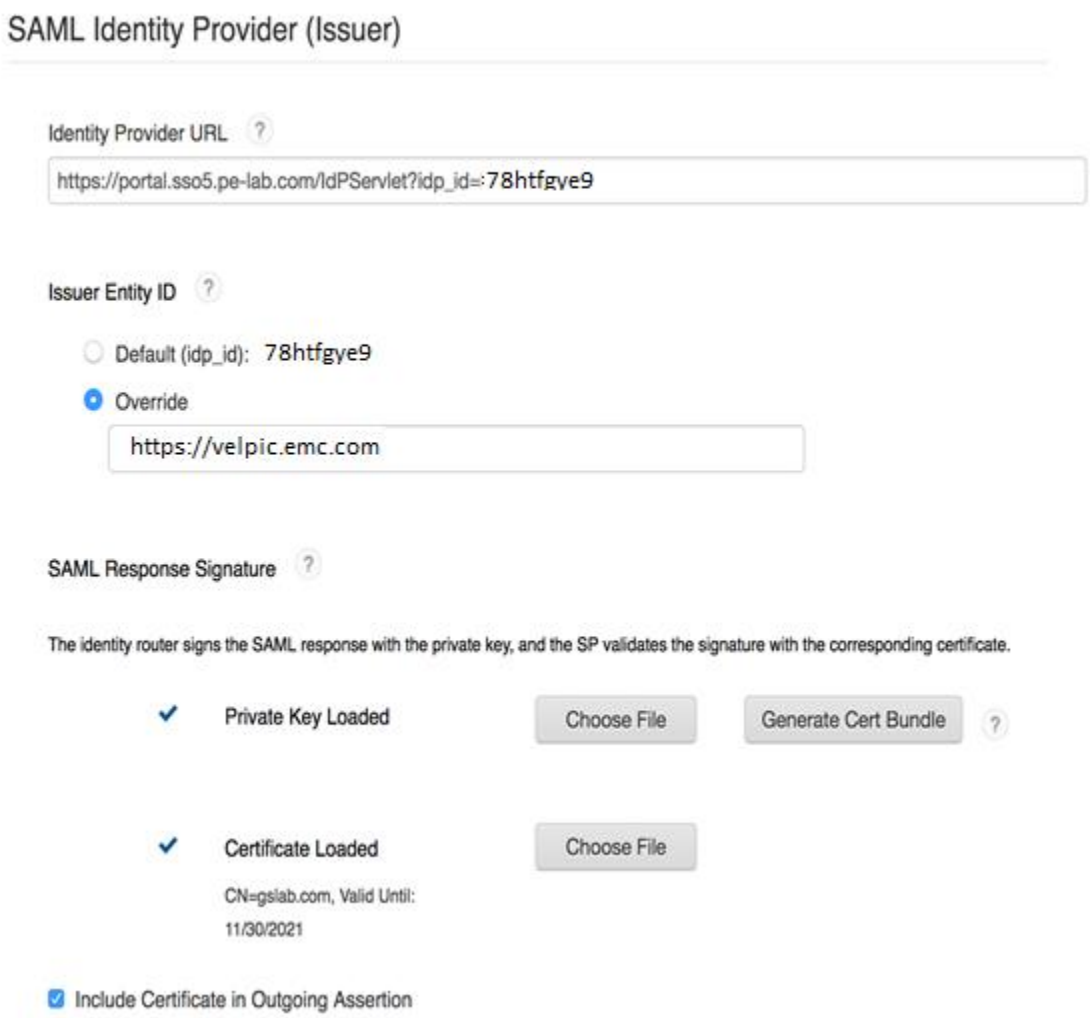
1. Enter a name for the application i.e. *Velpic* in the **Name** field on the Basic Information page and click the **Next Step** button.

2. Navigate to Initiate SAML Workflow section.
    a. In the **Connection URL** field, leave the field blank as no value is required here.
    b. Choose **IDP-initiated**.

Note: The following IdP-initiated configuration works for SP-initiated Velpic connections as well.



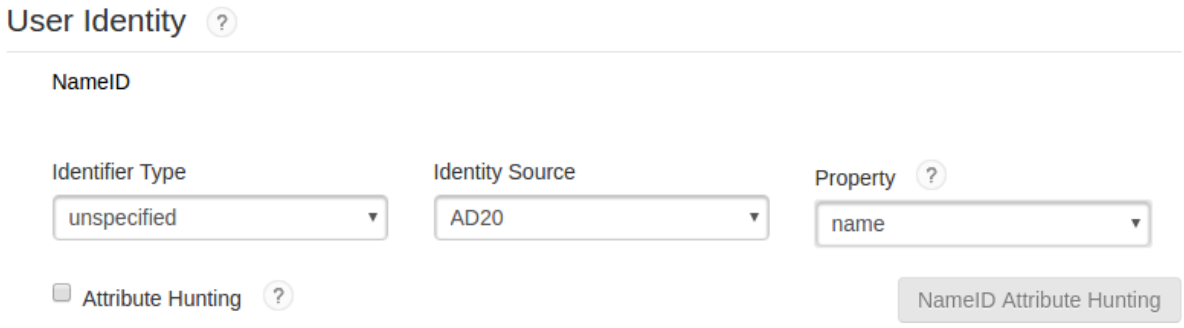
3. Scroll down to SAML Identity Provider (Issuer) section.



a. Under Issuer Entity ID, select **Override** and enter a unique https 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**.

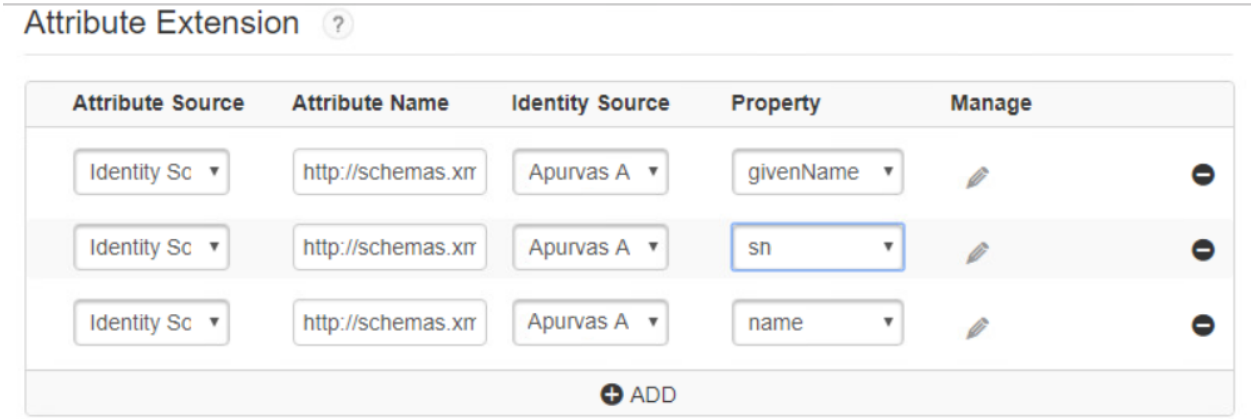
4. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field, enter the value as per provided by Velpic side which can be found during investigation. Replace <ACCOUNT_ID> value as received.
   b. In the **Audience (Service Provider Issuer ID)** field, enter the value as per provided by Velpic side which can be found during investigation. Replace <ACCOUNT_ID> value as received.
5. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username is to be presented in username format and the user account will be validated against the User Store selected.

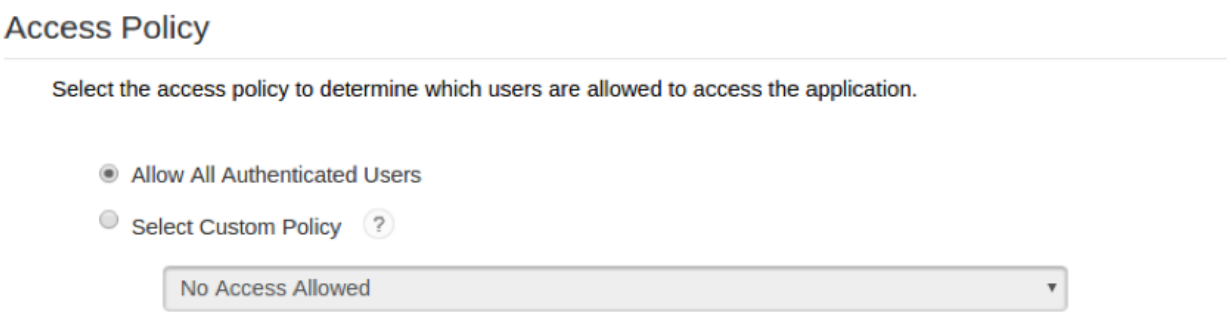


6. Click **Show Advanced Configuration**.

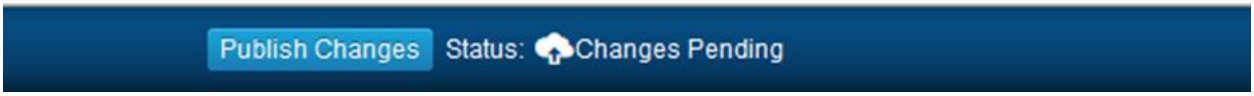
7. Scroll down to the Attribute Extension section. Map your AD attributes for givenName, surname, and username.



8. Click **Next Step**.
9. On the User Access page, select **Allow All Authenticated Users** from the available options.



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



14. Navigate to **Applications > My Applications**.
15. Locate Velpic in the list and from the Edit option, select **Export Metadata**.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Velpic 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.

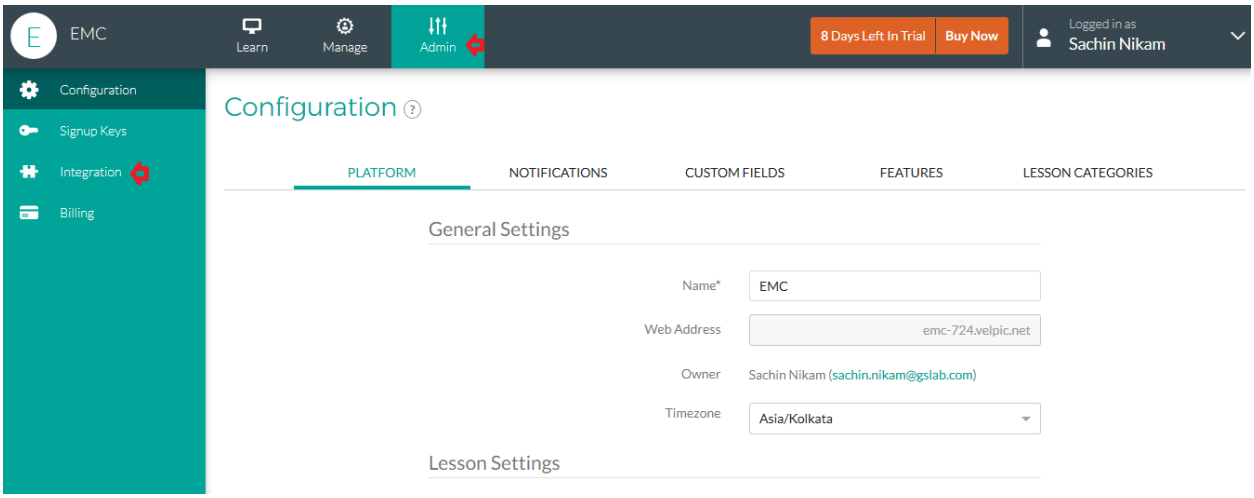
All Velpic components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Velpic SAML Configuration

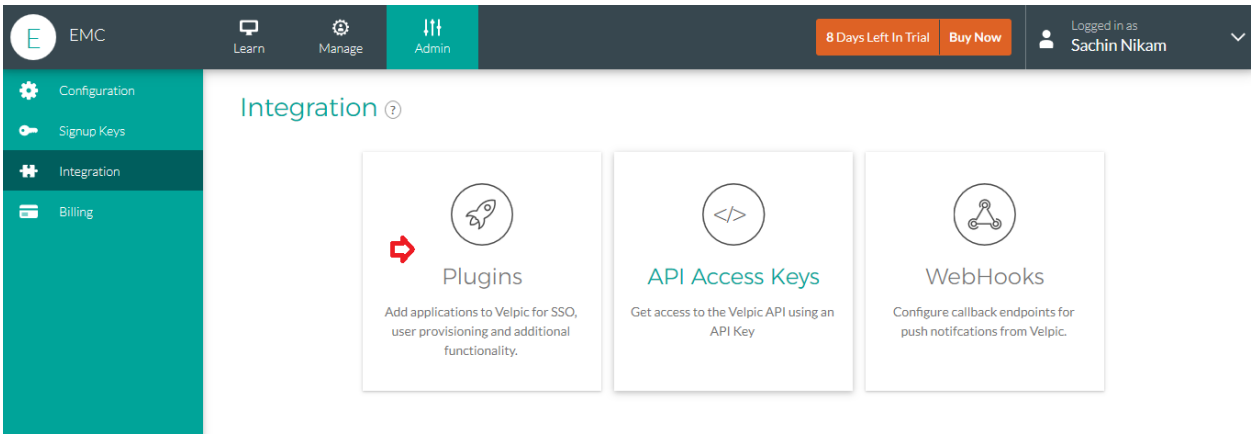
Procedure

1. Sign in to your Velpic application web account.
   https://<DOMAIN>.velpic.net/#login

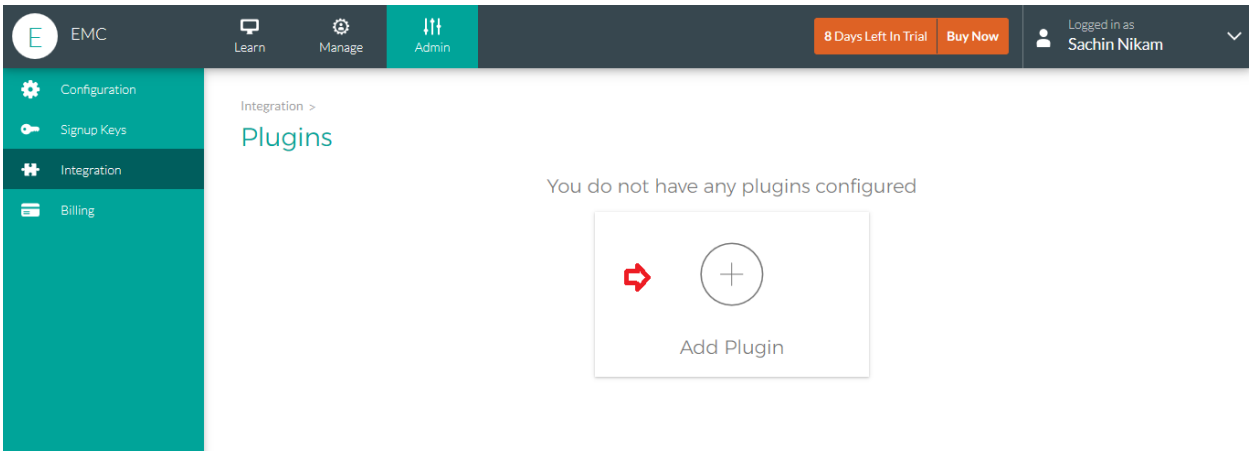
2. Following UI will be displayed. Click on *Admin* tab followed by *Integration* section.



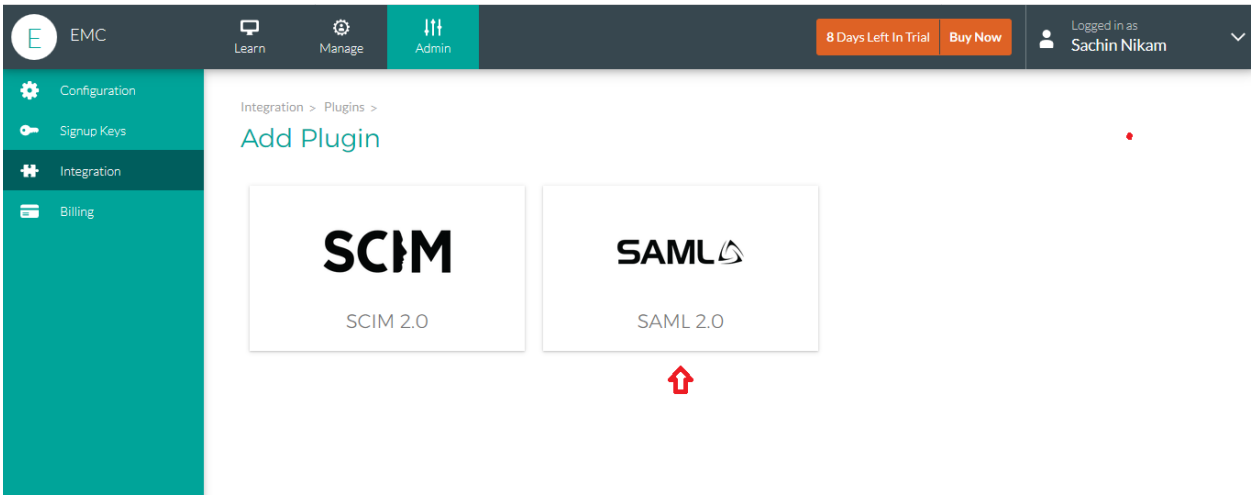
3. Following UI will be displayed. Go to *Plugins.*



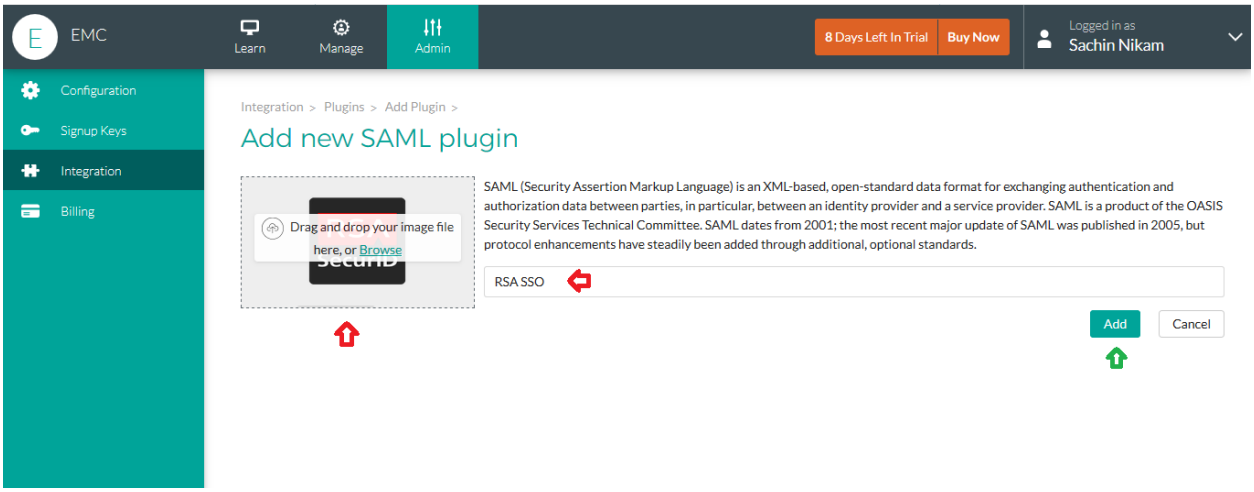
4. Following UI will be displayed. Initially, no plugin will be configured. Click *Add Plugin*.



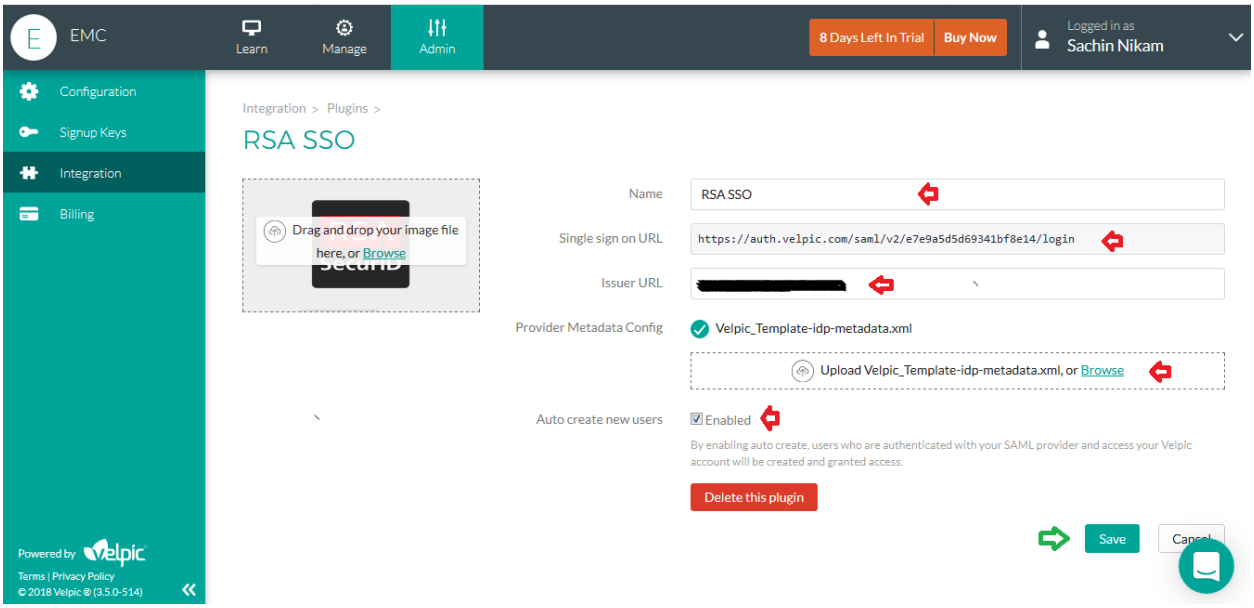
5. Following UI will be displayed. Click on *SAML* plugin to add SSO settings.



6. Following UI will be displayed to add new SAML plugin. Give convenient name to identify plugin and click on *Add* button.



7. Following UI will be displayed.



a. Make a note of *Single sign on URL*. This value will be further useful during identity provider side settings for the *Assertion Consumer Service* and *SP Entity ID* attribute values.
b. **Issuer URL** : Enter the Override *Idp Entity ID* value found in step – 3a. on page – 6. For example https://velpic.emc.com.

Note: Enter the IdP Entity ID into the Issuer URL field. This must be in URL format.

c. **Provider Metadata Config** : Provide idp metadata file here which is downloaded from step – 14 on page – 8.
d. **Auto create new users** : Click on *Enabled* checkbox to automatically create new users on the fly logging for the first time.
e. Once sure of all changes, click on *Save* button to configure SAML SSO settings.

8. Your Velpic account is now enabled for SAML SSO authentication.