RSA SECURID® ACCESS
Implementation Guide

Clever

Gina Salvalzo, RSA Partner Engineering
Last Modified: November 10, 2017

RSA READY

Solution Summary

Clever is a platform to easily connect with schools and school districts have a central location to manage their technology. Clever delivers a single sign on experience to the user through SAML. This integration supports both IdP and SP initiated authentication flows.

RSA SecurID Access Features	Clever
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 Clever 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 – Clever 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
Clever SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

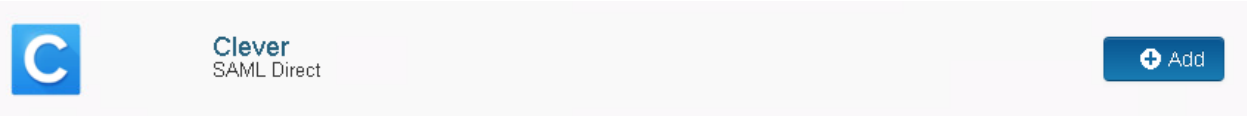
SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Clever 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

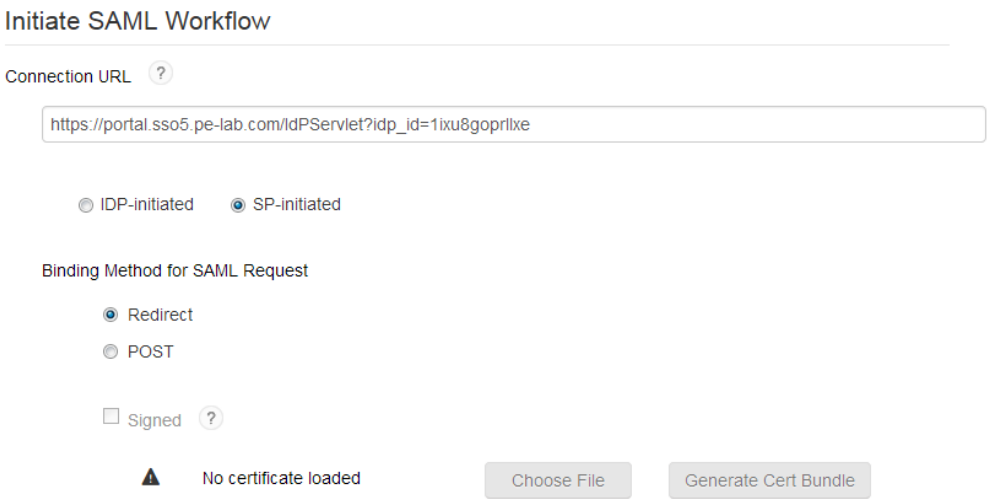
Procedure

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

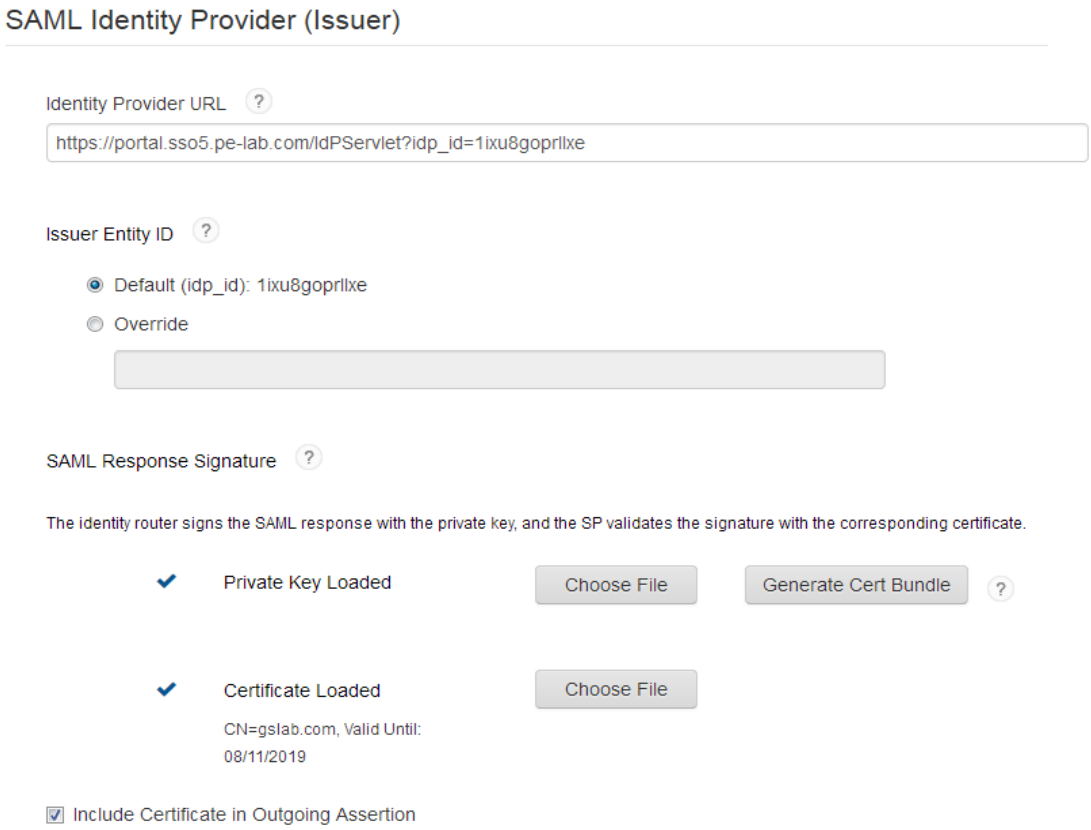


2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
    a. In the **Connection URL** field, paste the value from **Portal URL** field here.
    b. Choose **SP-initiated.** Verify that *Redirect* Binding method is selected.

Note: The following SP-initiated configuration works for IDP-initiated Clever connections as well.



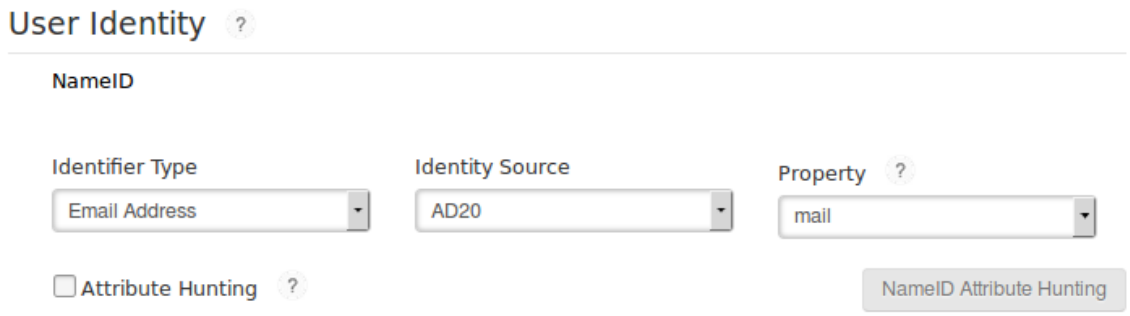
4. Scroll down to SAML Identity Provider (Issuer) section.



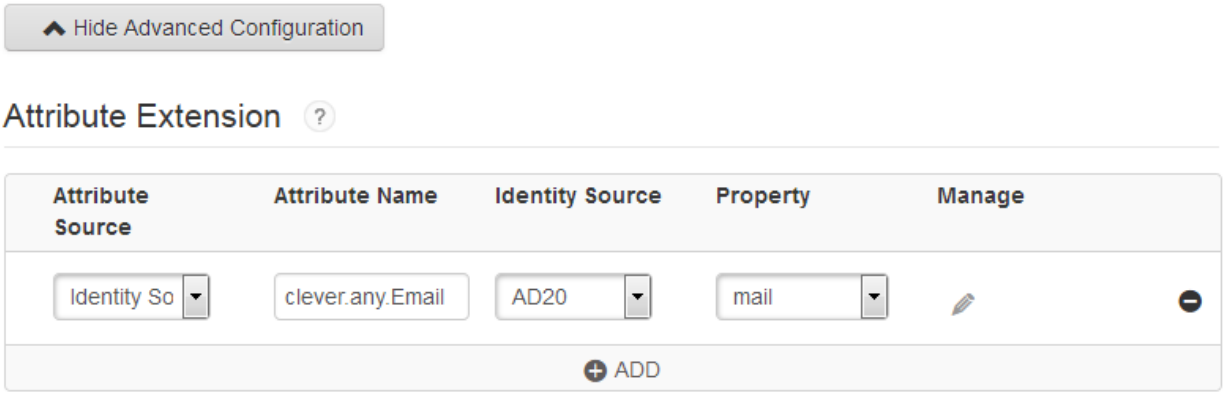
   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
   c. Select **Choose 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.

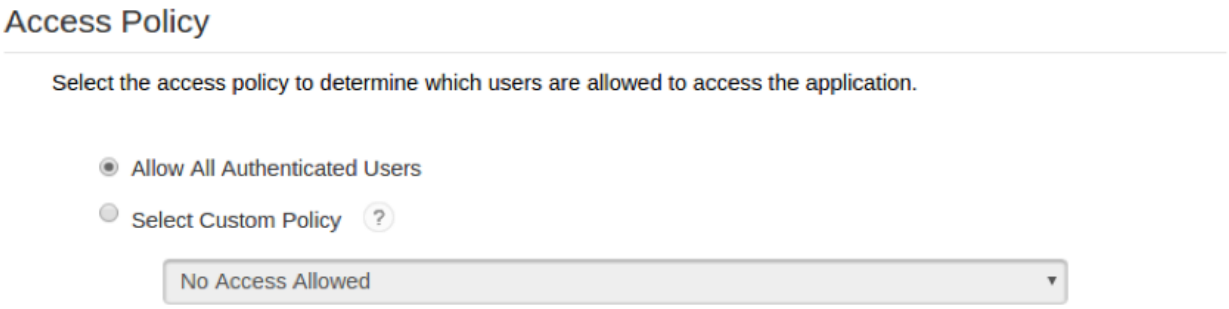
6. In the **Assertion Consumer Service (ACS) URL** field, provide the value as per received with service provider metadata.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata.
8. Scroll down to the **User Identity** section. Verify 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.



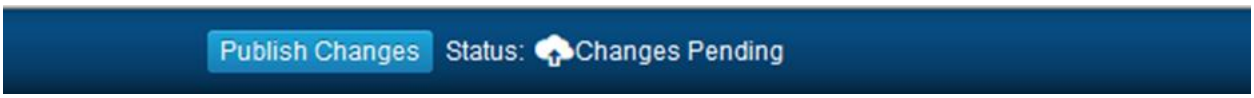
9. Select **Show Advanced Configuration**.
10. Under Attribute Extension, enter the attribute used to match the user profile to in Clever. In this example, **clever.any.Email** will be mapped to attribute **mail**.



10. Click **Next Step**.
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.



16. Navigate to **Applications > My Applications**.
17. Locate *Clever* in the list and from the **Edit** option, select **Export Metadata**.

Partner Product Configuration

Before You Begin

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

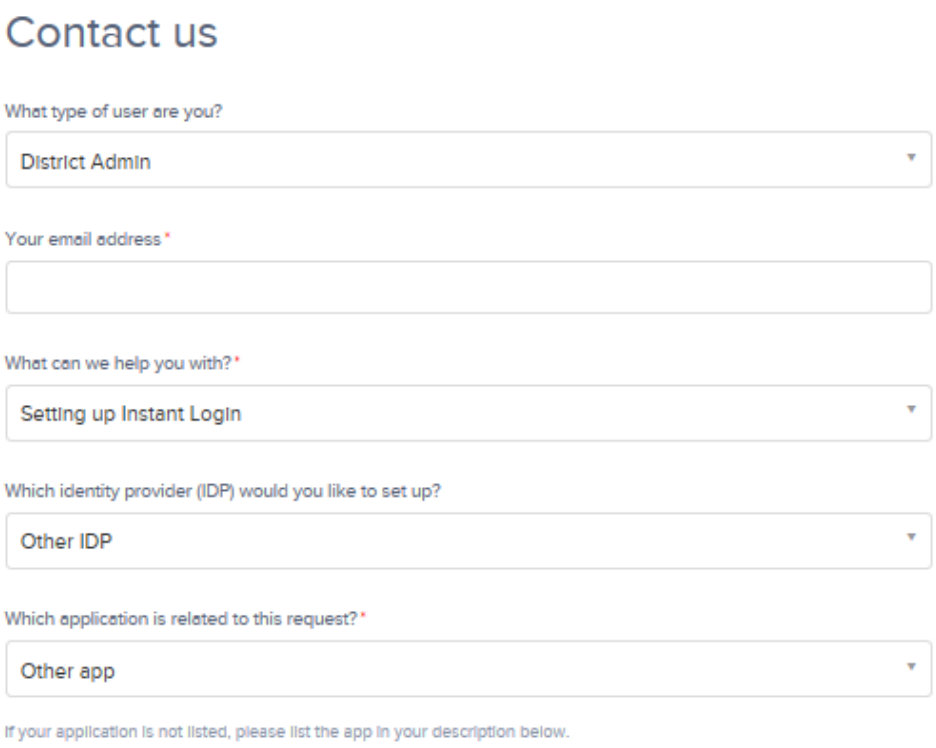
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Clever SAML Configuration

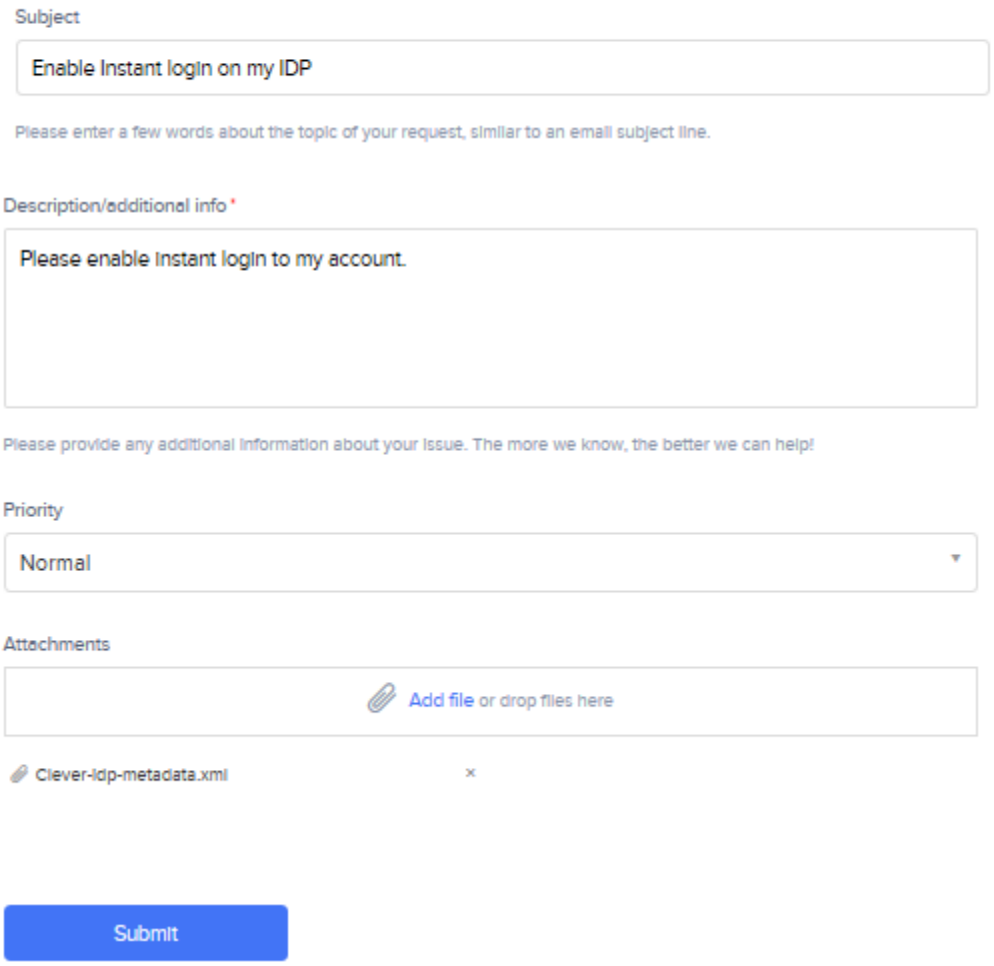
Procedure

1. Send a request to Clever Support to enable SAML SSO for student and teacher for your district by clicking on below URL.
   https://support.clever.com/hc/en-us/requests/new
2. On the displayed page, verify information is selected as below.



   a. Enter type of user as ***District Admin***.
   b. In **email address** field, enter your District Admin login email address.
   c. Select ***Setting up Instant Login*** in next field.
   d. In **IDP type** field, select ***Other IDP***.
   e. Select type of app from the dropdown in next field for whom you want to enable Instant login.

3. Scroll down to the next section.



   a. Enter Subject as ***Enable Instant login on my IDP***.
   b. In the **Description** section, enter one liner brief description to enable Instant login.
   c. In **Priority** section, select ***Normal***.
   d. In the **Attachments** section, select the **metadata file** you have exported after IDP configurations.
   e. Click **Submit**.

4. You will be notified by Clever support once your Instant login is enabled from their side.