RSA SECURID® ACCESS
Implementation Guide

NetWitness Orchestrator

Taylor Leblanc, RSA Partner Engineering
Last Modified: July 20, 2018

RSA READY

Solution Summary

NetWitness Orchestrator an automated incident response platform to combine security orchestration, incident management and interactive investigation. This integration supports single sign on for both SAML Identity provider and Service provider initiated work flows.

RSA SecurID Access Features NetWitness 3.5.1	
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 supported use cases of RSA SecurID Access with NetWitness Orchestrator 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 – NetWitness Orchestrator 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
NetWitness SAML Configuration

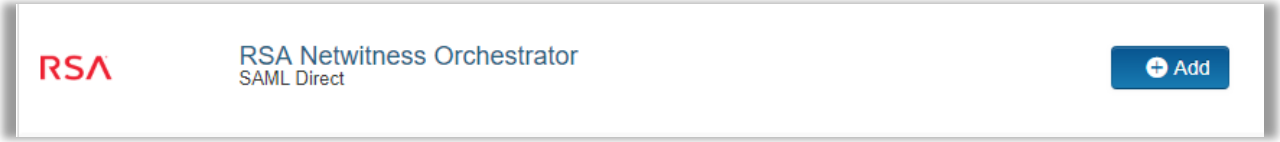
RSA SecurID Access Configuration

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 NetWitness Orchestrator 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.

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

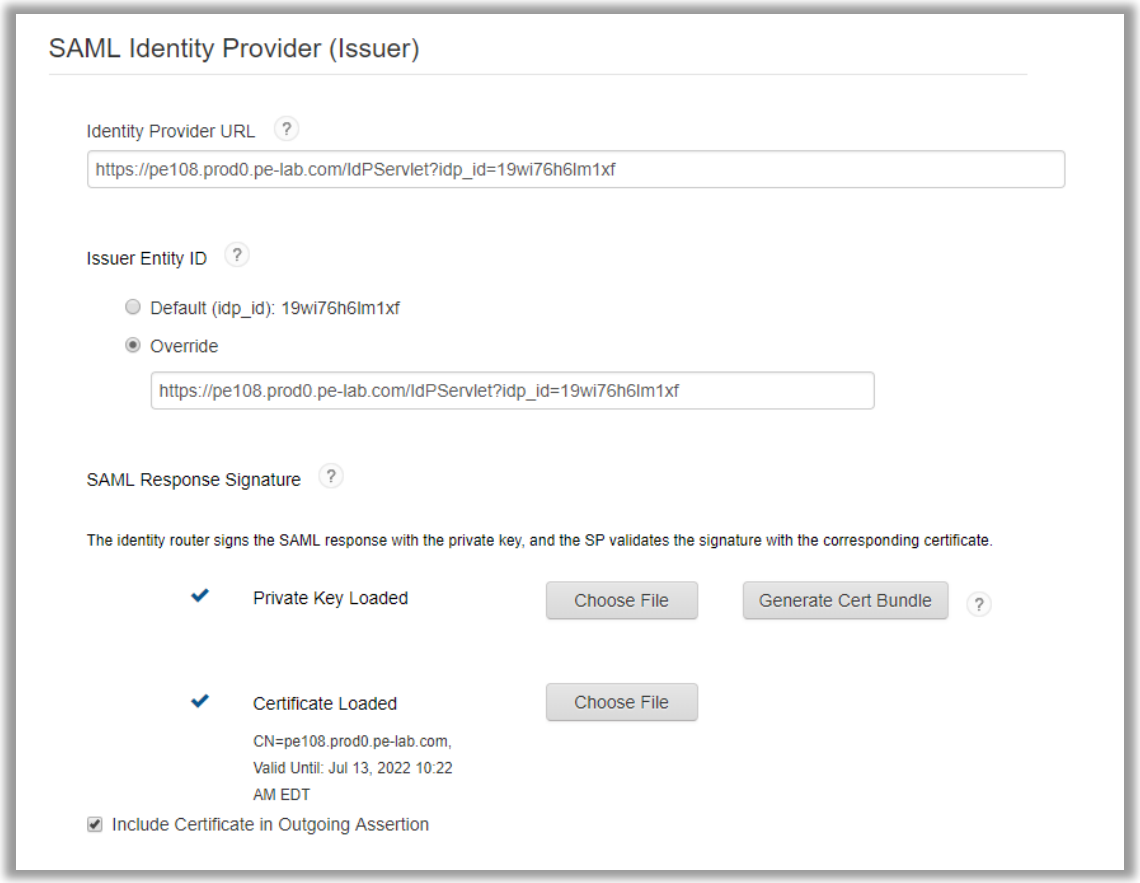


2. Enter a name for the application in the **Name** field on the Basic Information page and click the Next **Step** button.

3. Navigate to Initiate SAML Workflow section.
   a. In the **Connection URL** field, keep the field blank.
   b. Choose **IdP-initiated**.

> **Note: The following IdP-initiated configuration works for SP-initiated as well.**

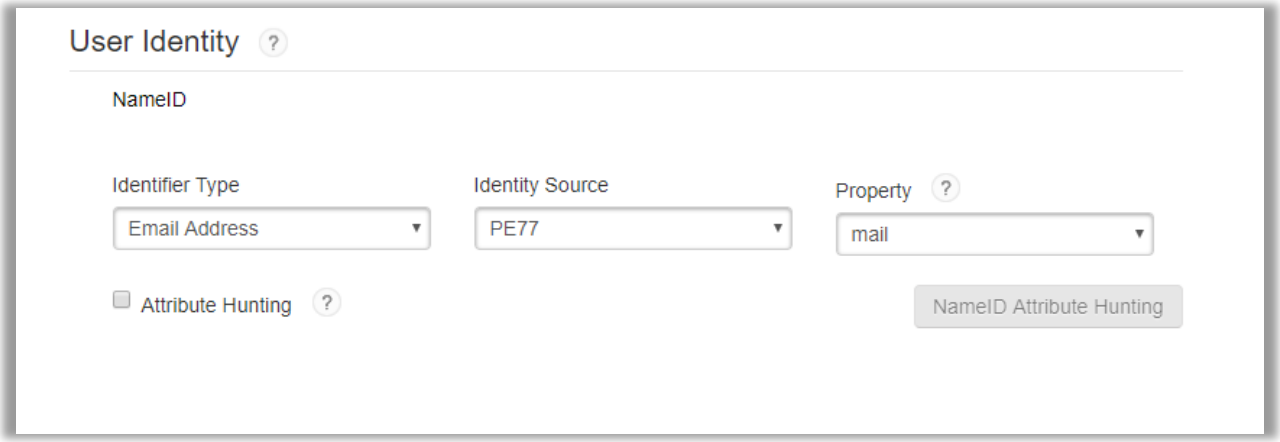
4. Scroll down to **SAML Identity Provider (Issuer)** section.



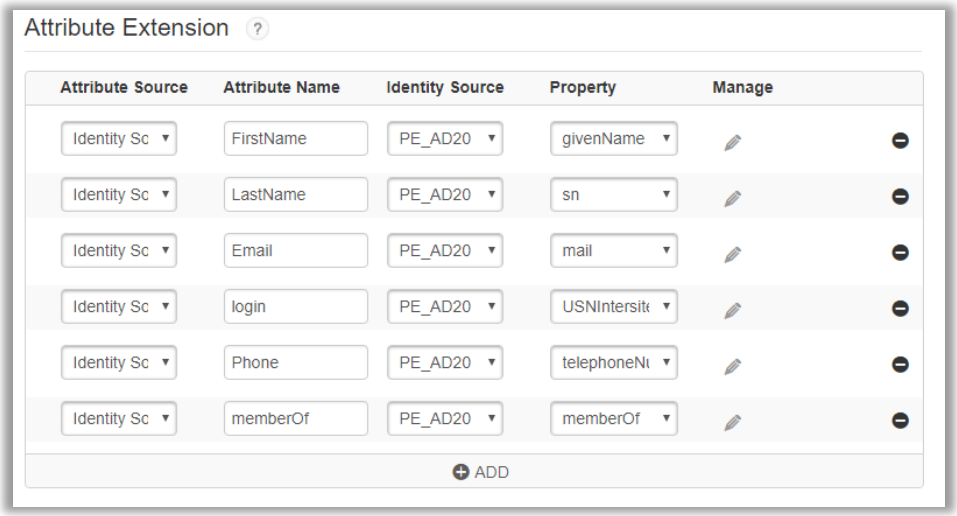
5. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   a. Select Issuer Entity ID and paste the *Identity Provider URL* in that field.
   b. Select **Choose File** and upload the *private key*.
   c. Select **Choose File** to import the *public signing certificate*.
   d. Select the **checkbox** for Include Certificate in Outgoing Assertion.

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

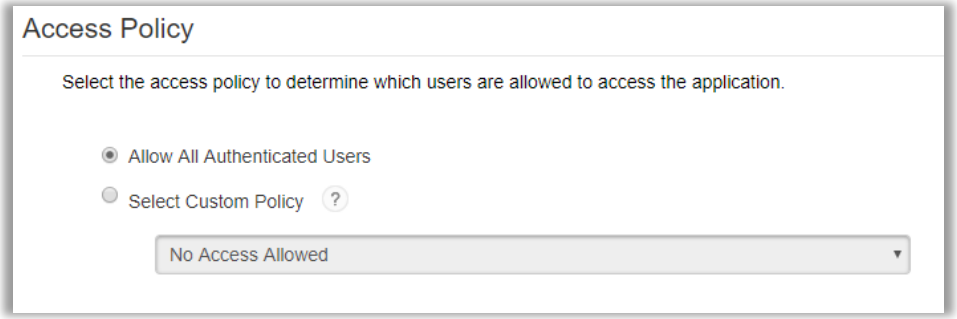
a. In the **Assertion Consumer Service (ACS) URL** field, replace *https://<SP_URL>/saml* with your NetWitness servers IP address.
b. In the **Audience (Service Provider Issuer ID)** field, replace *https://<SP_URL>/saml* with your NetWitness servers IP address.
c. Scroll down to the User Identity section. 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.



7. Click **Show Advanced Configuration**.
8. In the Attribute Extension section, map the correct property variables for NetWitness Orchestrator the default attributes are **FirstName**, **LastName**, **Email**, **Login**, **Phone** and **memberOf**.



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



11. Click **Next** Step.
12. On the Portal Display page, select **Display** in Portal.
13. Click **Save** and Finish.
14. Click **Publish** Changes.

NetWitness Configuration

Before You Begin

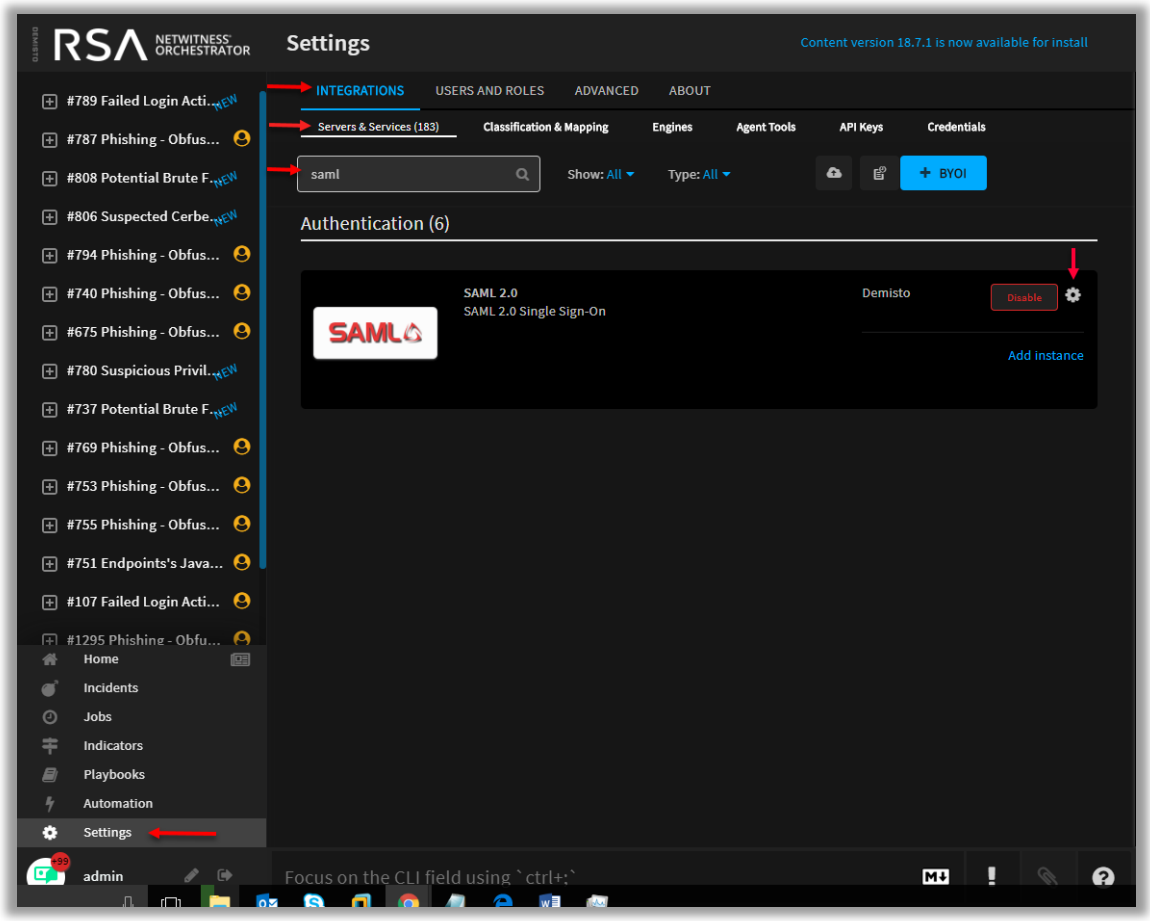
This section provides instructions for configuring NetWitness Orchestrator with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

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

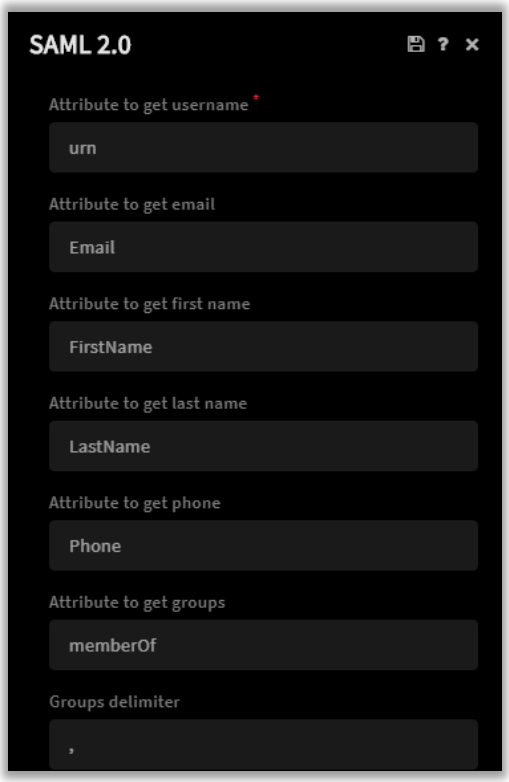
NetWitness Orchestrator Configuration

1. Login to NetWitness Orchestrator as an administrator.
    a. Navigate to **Settings > INTIGRATIONS > Servers & Services.**
    b. Type SAML into the search field and select the gear next to the service.

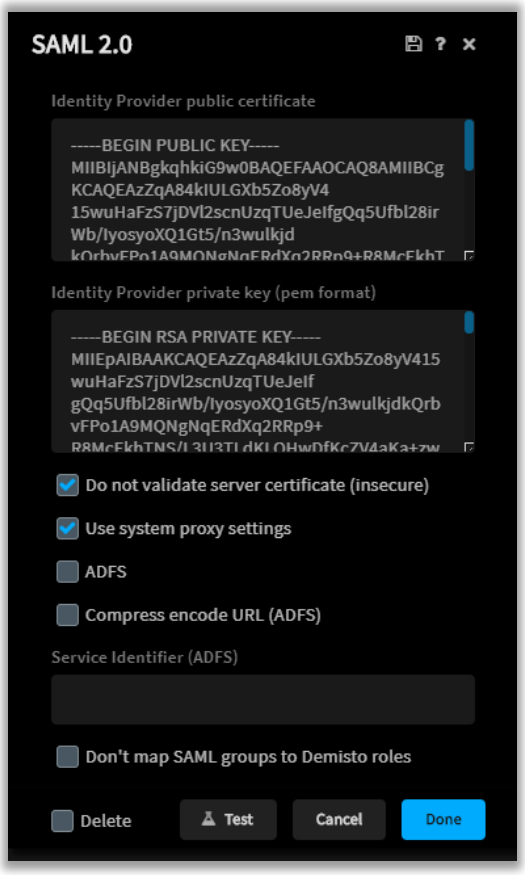


2. Within the SAML 2.0 setting menu.
   a) Enter a friendly **name** for this configuration.
   b) Within Service Provider Entity ID enter the **https://<SP_URL>/saml.**
   c) IDP metadata URL is a required field however this is not supported by RSA enter a null value.
   d) IDP SSO URL this is listed under *Identity provider URL* on the RSA SAML configuration page.

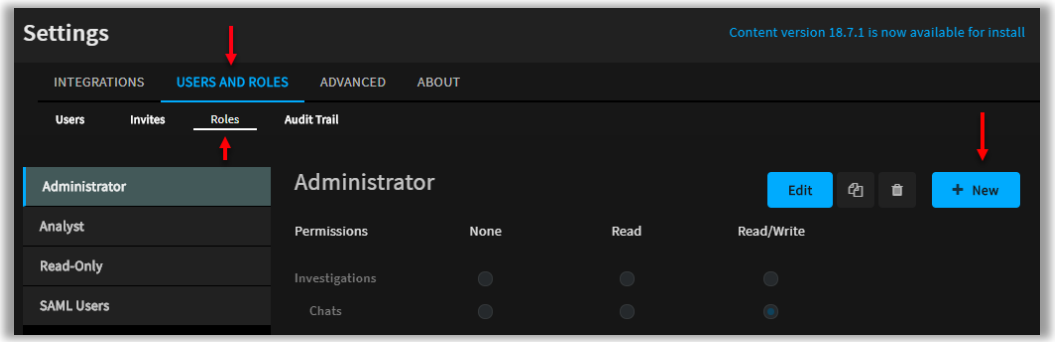
3. Continuing with in the SAML 2.0 menu keep all the default values.



4. In the SAML 2.0 configuration load the Identify Provider public certificate and the Identity Provider private key in pem format. These certificates are generated within the SAML application on in the SecurID access portal. Select *Do not validate server certificate* and select *Use system proxy settings*.



5. Navigate to the top of the and select **USERS AND ROLES** > **Roles** > **+ New.**



6. Give the new Role a friendly name and adjust the permissions according to your companies policies In the SAML Roles Mapping manually type in the memberOf group's that the end users belong to.