Configuring Single Sign-on from the VMware Identity Manager Service to RSA Archer eGRC

VMware Identity Manager

JULY 2016 V1

vmware

Contents

Overview

This document provides information about configuring SAML-based single sign-on from the VMware Identity Manager service to RSA Archer eGRC.

RSA Archer eGRC solutions allow you to build an efficient, collaborative enterprise governance, risk and compliance (eGRC) program across IT, finance, operations and legal domains.

When RSA Archer eGRC is configured in the VMware Identity Manager catalog, users can sign in to RSA Archer eGRC from their VMware Identity Manager apps portal.

You must have an administrator account for the VMware Identity Manager service to configure RSA Archer eGRC. You work with your RSA Archer eGRC representative to configure VMware Identity Manager for single sign-on in the RSA Archer eGRC server.

Adding RSA Archer eGRC to VMware Identity Manager Catalog

To enable single sign-on to RSA Archer eGRC on the service, you must configure the app in the catalog.

Add RSA Archer eGRC to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the **RSA Archer eGRC** icon.
4. Click **Configuration.** The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	
Proxy Count	
Login Redirection URL	**https://sso2.archer.rsa.com/logon-egrc/def** The log in redirection URL redirects users to VMware Identity Manager for authentication.
Include Destination	
Sign Response	

<table>
<tr><td>Sign Assertion</td><td>Enabled</td></tr>
<tr><td>Include Cert</td><td></td></tr>
<tr><td>Signature Algorithm</td><td>SHA1 with RSA</td></tr>
<tr><td>Digest Algorithm</td><td>SHA1</td></tr>
<tr><td>Allow API Access</td><td></td></tr>
<tr><td>Configure Via</td><td></td></tr>
<tr><td>Assertion Consumer Service*</td><td>Automatically populated with the URL where the SAML is posted . https://sso2.archer.rsa.com/adfs/ls</td></tr>
<tr><td>Name ID Format</td><td>Transient</td></tr>
<tr><td>Name ID Value</td><td></td></tr>
<tr><td>Recipient Name*</td><td>The SP’s assertion consumer service URL populated as https:// sso2.archer.rsa.com/adfs/ls/</td></tr>
<tr><td>Audience*</td><td>The SP’s unique identifier populated with https://sso2.archer.rsa.com/adfs/services/trust</td></tr>
<tr><td>Assertion Lifetime</td><td>Populated with a value of 200 seconds</td></tr>
<tr><td>Signing Certificate</td><td></td></tr>
<tr><td>Application Parameters</td><td>Set the CompanyName and vIDMTenantName values. For example, if your RSA Archer eGRC log in URL is https://sso2.archer.rsa.com/logon-egrc/default.aspx?requested_realm=act&whr=https://xyz.com/SAAS/API/1.0/GET/metadata/idp.xml,
enter the subdomain as act and the comain name as https://xyz.com.</td></tr>
<tr><td>Attribute Mapping</td><td>Map these attributes to specific user profile values

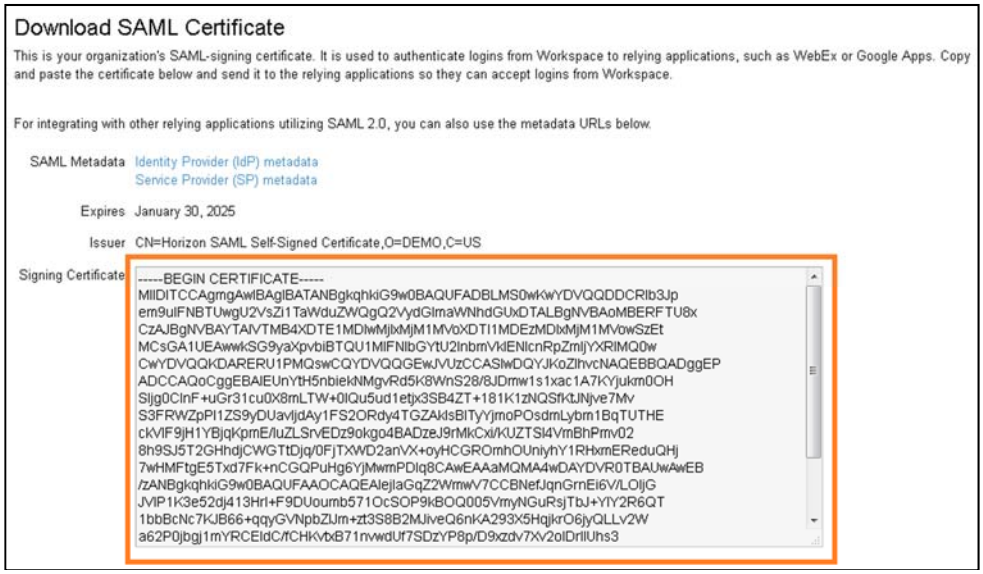
<table>
<tr><th>NAME</th><th>FOR</th><th>NS</th><th>VALUE</th></tr>
<tr><td>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn</td><td>URI</td><td></td><td>${user.userName}</td></tr>
<tr><td>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</td><td>URI</td><td></td><td>${user.email}</td></tr>
<tr><td>http://schemas.xmlsoap.org/claims/FirstName</td><td>URI</td><td></td><td>${user.firstName}</td></tr>
<tr><td>http://schemas.xmlsoap.org/claims/LastName</td><td>Basic</td><td></td><td>${user.lastName}</td></tr>
</table>
</td></tr>
</table>

5. Click **Save**.

Download SAML-Signing Certificate

If the SAML-signing certificate from the VMware Identity Manager service is required for the RSA Archer eGRC configuration, you can retrieve the certificate from the Catalog > Settings tab.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. Copy and save the **Signing Certificate** text as a **.pem** file on your computer. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE-----.



Setting up Identity Manager in RSA Archer eGRC

Contact RSA Archer eGRC to set up single sign-on for VMware Identity Manager. Provide them with the following information.

- Your identity manger domain name
- VMware Identity Manager SAML signing certificate you saved previously

Testing Single Sign-on Configuration

Test your single sign-on configuration with a small number of users before deploying the application across your organization.

Set up User in VMware Identity Manager for Testing

1. Log in to the VMware Identity Manager administration console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list

of users.

3. In the **Catalog** page, click on the RSA Archer eGRC application.
4. Click **Entitlements**.
5. Click +**Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

7. Click **Save**, then click **Done**.
8. In the top-right corner of the page, click your user name and select **Logout**.

Set up a User in RSA Archer eGRC for Testing

Make sure the test user you set up in VMware Identity Manager is configured in RSA Archer eGRC.

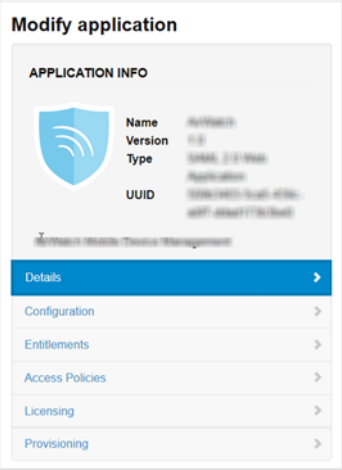
Verify Test-User can Sign into RSA Archer eGRC

1. Sign in to the user portal as the test user.
2. Click the RSA Archer eGRC icon on the My Apps page.

   You should now have single sign-on access to RSA Archer eGRC.

Completing the Configuration in the Catalog

In addition to configuring the Web application for single sign-on to the service, you can configure additional settings to add an access policy, set up app external approval requirements, and entitle users and groups to the app.



Entitlements After you configure a Web application, you can add group entitlements and entitle individual users to the Web app.

Access Policies The VMware Identity Manager service includes a default policy that is automatically assigned to the Web app when you add the app to the Catalog. If you do not want to use the default access policy, create a new access policy and in the Access Policies link, select the access policy to use for this Web application.

For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

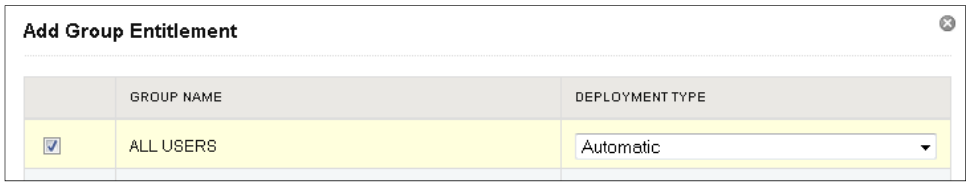
Licensing In some applications, licensing can be used to require users to request external approval before they can access the application. In addition, you can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report to see the approval information for the application.

Entitle Users to RSA Archer eGRC

You can activate single sign-on for all users.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click RSA Archer eGRC.

3. In the **Modify application** page, click **Entitlements**.
4. Click +**Add group entitlement**.
5. Select **ALL USERS** and change the DEPLOYMENT TYPE value to **Automatic**.



6. Click **Save,** then click **Done**.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com