



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

VMware Identity Manager

JULY 2016 V1

## Contents

Overview .....	2
Adding RSA Archer eGRC to VMware Identity Manager Catalog .....	2
Add RSA Archer eGRC to the Catalog .....	2
Download SAML-Signing Certificate.....	4
Setting up Identity Manager in RSA Archer eGRC .....	4
Testing Single Sign-on Configuration.....	4
Set up User in VMware Identity Manager for Testing.....	4
Set up a User in RSA Archer eGRC for Testing.....	5
Verify Test-User can Sign into RSA Archer eGRC.....	5
Completing the Configuration in the Catalog .....	6
Entitle Users to RSA Archer eGRC.....	6

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

<b>Sign Assertion</b>	Enabled																				
<b>Include Cert</b>																					
<b>Signature Algorithm</b>	SHA1 with RSA																				
<b>Digest Algorithm</b>	SHA1																				
<b>Allow API Access</b>																					
<b>Configure Via</b>																					
<b>Assertion Consumer Service*</b>	Automatically populated with the URL where the SAML is posted . <b>https://sso2.archer.rsa.com/adfs/ls</b>																				
<b>Name ID Format</b>	<b>Transient</b>																				
<b>Name ID Value</b>																					
<b>Recipient Name*</b>	The SP's assertion consumer service URL populated as <b>https:// sso2.archer.rsa.com/adfs/ls/</b>																				
<b>Audience*</b>	The SP's unique identifier populated with <b>https://sso2.archer.rsa.com/adfs/services/trust</b>																				
<b>Assertion Lifetime</b>	Populated with a value of <b>200</b> seconds																				
<b>Signing Certificate</b>																					
<b>Application Parameters</b>	Set the CompanyName and vIDMTenantName values. For example, if your RSA Archer eGRC log in URL is <b>https://sso2.archer.rsa.com/logon-egrc/default.aspx?requested_realm=act&amp;whr=https://xyz.com/SAAS/API/1.0/GET/metadata/idp.xml</b> , enter the subdomain as <b>act</b> and the comain name as <b>https://xyz.com</b> .																				
<b>Attribute Mapping</b>	Map these attributes to specific user profile values <table border="1"> <thead> <tr> <th>NAME</th> <th>FOR</th> <th>NS</th> <th>VALUE</th> </tr> </thead> <tbody> <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> </tbody> </table>	NAME	FOR	NS	VALUE	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	URI		\${user.userName}	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	URI		\${user.email}	http://schemas.xmlsoap.org/claims/FirstName	URI		\${user.firstName}	http://schemas.xmlsoap.org/claims/LastName	Basic		\${user.lastName}
NAME	FOR	NS	VALUE																		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	URI		\${user.userName}																		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	URI		\${user.email}																		
http://schemas.xmlsoap.org/claims/FirstName	URI		\${user.firstName}																		
http://schemas.xmlsoap.org/claims/LastName	Basic		\${user.lastName}																		

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-----**.

**Download SAML Certificate**

This is your organization's SAML-signing certificate. It is used to authenticate logins from Workspace to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Workspace.

For integrating with other relying applications utilizing SAML 2.0, you can also use the metadata URLs below.

SAML Metadata [Identity Provider \(IdP\) metadata](#)  
[Service Provider \(SP\) metadata](#)

Expires: January 30, 2025

Issuer: CN=Horizon SAML Self-Signed Certificate,O=DEMO,C=US

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLMS0wKwYDVQDDCRib3Jp
em9uIFNBTUwgU2VsZi1TaWduZWQgQ2VydGlnaWNhdGUxTALBgNVBAoMBERFU8x
CzAIBgNVBAYTAiVMB4XDTE1MDIwMjM1MjM1MDVxDTI1MDEzMDEwMjM1MjM1MjM1
MCsGA1UEAwkzSG9yaXpvaW50b291MjM1MjM1MjM1MjM1MjM1MjM1MjM1MjM1MjM1
CwYDVQKDAERERU1PMQswCQYDVQQGEwJVVzCCASwDQCYJKoZiIvcNAQEBAQADggEP
ADCCAQoCggEBAIEUyH5nbiekNMgyRd5k8WnS28/8JDrmw1s1xac1A7KjYukm0OH
Sjg0CInF+uGr31cu0x8mLTW+0lQu5ud1etj3SB4ZT+181K1zNQSFkLjNjve7Mv
S3FRWzPp11ZS9yDUavjdyA1FS2ORdy4TGZAkdsBITyYjmoPOsdmLybm1BqTUTHE
ckVIF9jH1YBjqKpmE/luZLsrEDz9okgo4BADzeJ9rMkCxiKUZTS4VmBhPmv02
8h9Sj5T2GHhdjCWGTIDjg0FjTXWD2anVX+oyHCGR0mhOUniyhY1RHxmEReduQHj
7wHMFtgE5Td7Fk+nCGQPuHg6YjMwmPDIq8CAwEAAMQMA4wDAYDVR0TBAAUwAwEB
/ANBgkqhkiG9w0BAQUFAAOCAQEAEjJaGqZ2WmwV7CCBNefJqnGmEi6V/L0lJG
JVIP1K3e52dj413HrI+9DUoumb571OcSOP9kBOQ005VmyNGuRsjTb+YIY2R6QT
1bbBcNc7KjB66+qqyGVNpbZUm+z3S8B2MjiveQ6nKA293X5HqjkrO6jyQLL2W
a62P0jbj1mYRCeIdC/CHKvxb71nwwdUf7SDzYP8p/D9xzdV7Xv2oIDrIUhs3
-----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 manager 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:

Add User Entitlement		
Type to select a user   or browse...		
User, Demo (demo)	Automatic	Remove

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

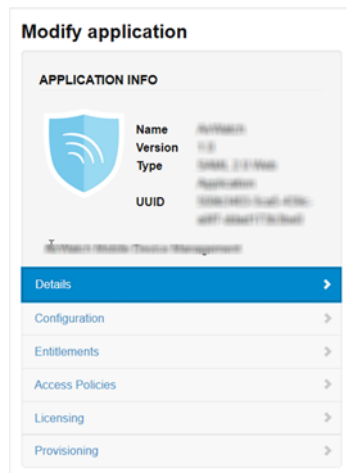
Make sure the test user you set up in VMware Identity Manager is configured in RSA Archer eGRC.

## 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**.

**Add Group Entitlement** ✕

	GROUP NAME	DEPLOYMENT TYPE
<input checked="" type="checkbox"/>	ALL USERS	Automatic <span>▼</span>

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



-----

