RSA SecurID Access Implementation Guide

Microsoft Corporation

SharePoint 2016

Certified: April 26th, 2019

Table of Contents

Solution Summary

Use Case

When integrated, Microsoft SharePoint end users must authenticate with RSA SecurID Access to sign in. Microsoft SharePoint can integrate using WS-Fed SSO Agent, RSA Authentication Agent for IIS or RSA Authentication Agent for AD FS.

Integration Types

SSO Agent integrations use SAML 2.0, HFED or WS-Fed technologies to direct users' web browsers to RSA SecurID Access for authentication. SSO Agents also provide Single Sign-On to other applications using the RSA Application Portal.

RSA Authentication Agent for IIS can be leveraged to secure access to Microsoft SharePoint server. RSA Authentication for IIS supports integration with RSA Authentication Manager.

RSA Authentication Agent for AD FS can be leveraged to secure access to Microsoft SharePoint by way of AD FS. RSA Authentication Agent for AD FS supports integration with RSA Authentication Manager and RSA Cloud Authentication Service.

For more information about RSA Authentication Agents, browse to the RSA Authentication Agents page on RSA Link.
https://community.rsa.com/docs/DOC-40601#agents

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section in this guide contains the instruction steps for how to integrate RSA SecurID Access with Microsoft SharePoint using **SSO Agent**.

Microsoft SharePoint integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	-	-	✔
LDAP Password	-	-	-	✔
Authenticate Approve	-	-	-	✔
Authenticate Tokencode	-	-	-	✔
Device Biometrics	-	-	-	✔
SMS Tokencode	-	-	-	✔
Voice Tokencode	-	-	-	✔
FIDO Token	n/a	n/a	-	✔

Microsoft SharePoint integration with RSA Authentication Manager

Authentication Methods	Authentiaction API	RADIUS	Authentication Agent
RSA SecurID	-	-	✔
On Demand Authentication	-	-	✔
Risk-Based Authentication	n/a	-	✔

✔ Supported

- Not supported

n/t Not yet tested or documented, but may be possible.

n/a Not applicable

Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate Microsoft SharePoint with RSA SecurID Access using SSO Agent.

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 RSA SecurID Access and Microsoft SharePoint components must be installed and working prior to the integration.

Links

SSO Agent

Certification Details

Date of testing: March 12th, 2019

RSA Cloud Authentication Service

Microsoft SharePoint 2016**,** Windows Server 2019

Known Issues

RSA SecurID Access related error while trying to go back to SharePoint site after sign out

Tracking Number: NGX-29120

Problem: During sign out of SharePoint site user will have the option to either "Close the browser to complete sign out" or "Go back to site". If user selects "Go back to site" option then user will get an error related to RSA SecurID access.

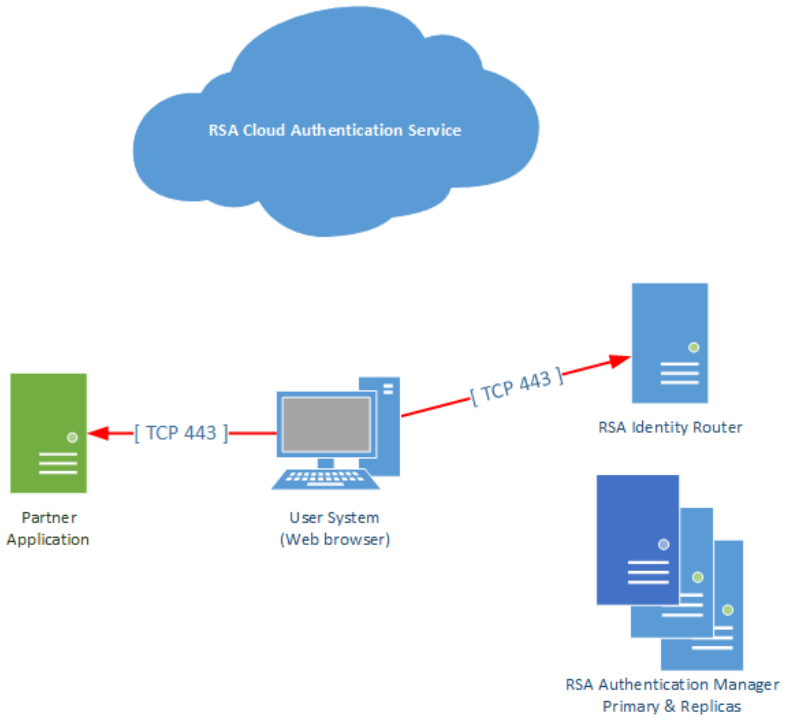
Workaround: Close the browser and relogin to access the site

Integration Configuration

SSO Agent - WS-Fed

This section contains instructions on how to integrate RSA SecurID Access with Microsoft SharePoint using a WS-Fed SSO Agent.

Architecture Diagram



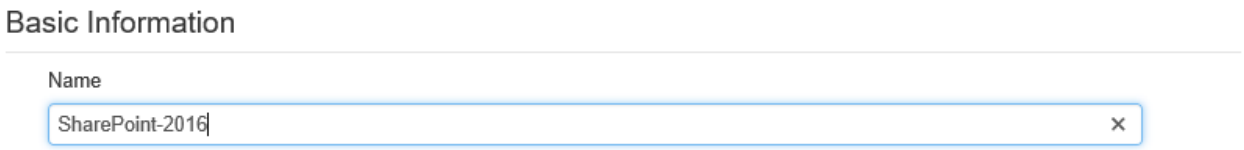
RSA Cloud Authentication Service

Follow the steps in this section to configure RSA Cloud Authentication Service as an SSO Agent WS-Fed IdP to Microsoft SharePoint.

Procedure

1. Logon to the RSA Cloud Administration Console and browse to **Applications** > **Application Catalog**, search for **Microsoft SharePoint WS-Fed** and click **+Add** to add the connector.

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



3. Scroll to the **SAML Identity Provider** section on the **Connection Profile** page and copy the value from the **Identity Provider URL** field.

4. Scroll to the top of the page and paste the identity provider URL in the **Menu URL** field.

5. You must import a private/public key pair to sign and validate SAML assertions. Follow the steps to generate a certificate bundle

a. Scroll to the **SAML Response Signature** section and click the **Generate Certificate Bundle** button.

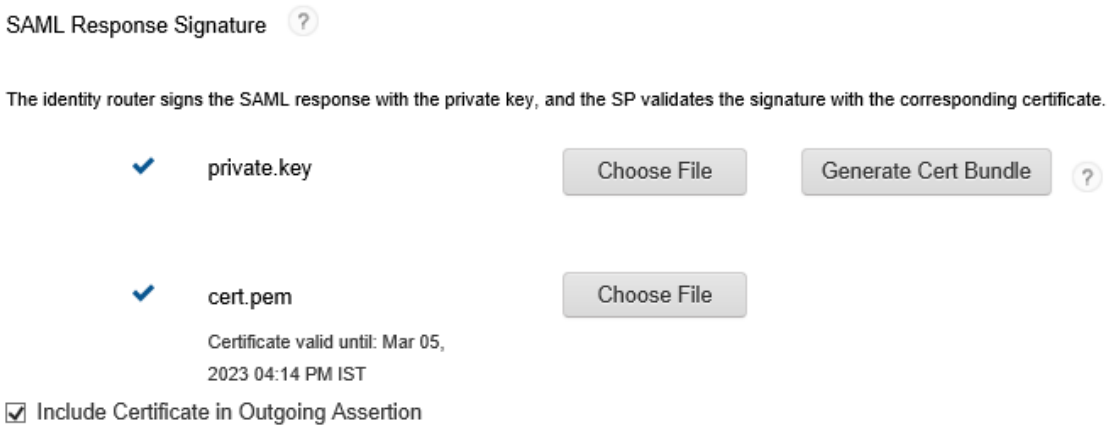
b. In the **Common Name (CN)** field, enter the host name of the SharePoint service provider's server that will be sending authentication requests.

c. Click the **Generate and Download** button, save the certificate bundle ZIP file to a secure location and extract its contents. The ZIP file will contain private key, public key, public certificate and certificate signing request.

6. Click the **Choose File** button on the left of the **Generate Certificate Bundle** button, locate and select a private key for signing SAML assertions and click the **Open** button.

7. Click the **Choose File** button underneath the **Generate Certificate Bundle button**, locate and select your public certificate and click the **Open** button.

8. Select **Include Certificate in Outgoing Assertion** check box.



9. Enter your relying party URL in the **Relying Party URL** field. The URL format is

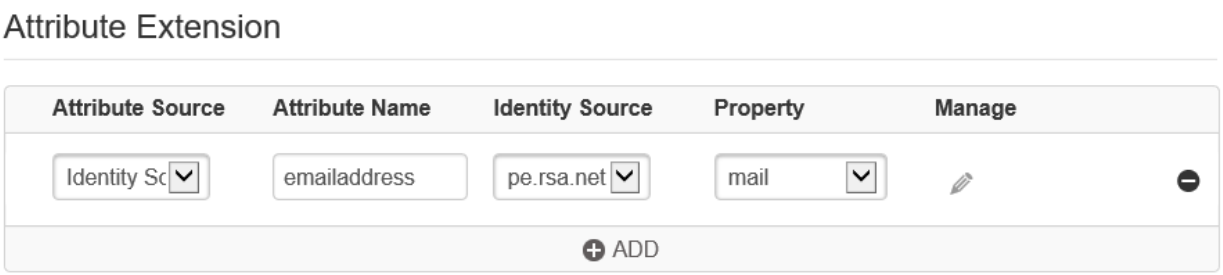
https://<SharePoint URL>:<port number>/_trust.

Note: It is necessary to configure SharePoint web application with SSL. Consult Microsoft documentation for instructions to configure SSL. If SharePoint web application is configured with default SSL port (port 443), then it is not necessary to specify port number in the Relying Party URL.

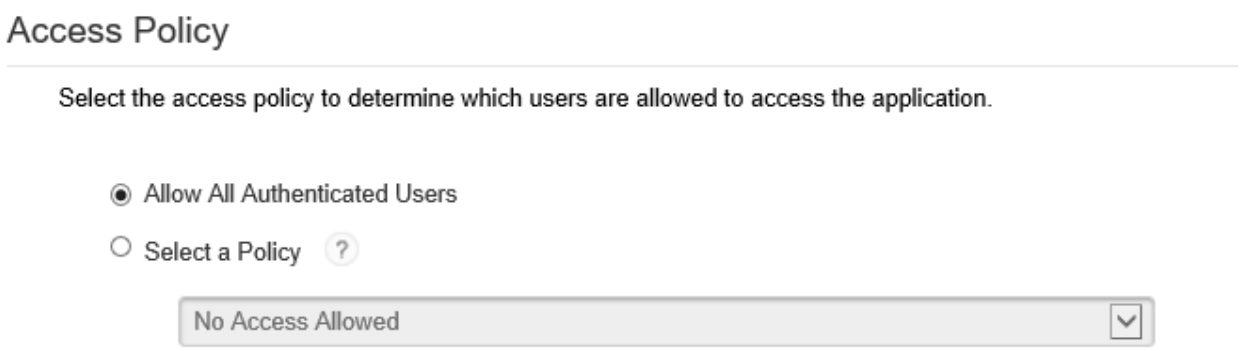
10. Enter the relying party ID in the **Relying Party ID** field. You will use this value as your SharePoint realm name. Use the format urn:<string 1>:<string 2>. You may choose any values for <string 1> and <string 2>.

11. Decide which claim type(s) you will use to identify an authenticated user. See the link about claims-based identity https://dev.office.com/sharepoint/docs/general-development/claims-based-identity-term-definitions. This example uses http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress as claim type URL. Under **Attribute Extension** section

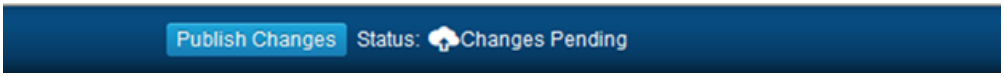
a. Select *Identity Source* from the **Attribute Source** drop-down list.
b. In the **Attribute Name** field, enter the attribute name that corresponds to your claim. The attribute name in this example is *emailaddress*.
c. Select the name of your user identity source from the **Identity Source** drop-down list.
d. Select *mail* from the **Property** drop-down list.



12. Click the **Next Step** button.
13. On the **User Access** page, configure the **Access Policy** settings and click **Next Step** button



14. On the **Portal Display page**, click **Save and Finish** button.
15. Click the **Publish Changes** button at the top of the page.



Microsoft SharePoint

Follow the steps in this section to configure Microsoft SharePoint as an SSO Agent WS-Fed SP to RSA Cloud Authentication Service

This section is divided into the following subsections:

1. Create a Trusted Identity Token Issuer for RSA SecurID Access
2. Configure a SharePoint Web Application to Use the RSA SecurID Access Token Issuer
3. Configure addtional SharePoint web applications for RSA SecurID Access Integration

Create a Trusted Identity Token Issuer for RSA SecurID Access:

1. Log into your SharePoint server host and open the SharePoint Management Shell.

2. Create a root certificate object using the signing certificate you downloaded from SecurID Access and copied to your SharePoint server. Replace c:\certs\cert.pem with the path and name of your signing certificate

```
$root_cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("c:\certs\cert.pem")
```

3. Create a trusted root authority for your token issuer and set the root certificate. Replace SECURID_ACCESS with the name you want to give to your trusted root authority.

```
New-SPTrustedRootAuthority -Name "SECURID_ACCESS" -Certificate $root_cert
```

4. Enter the command below to create (a) claim type(s) mapping (s). Replace http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress with your claim type URL (s). See the following URL for information about claims-based identity. https://dev.office.com/sharepoint/docs/general-development/claims-based-identity-term-definitions.

```
$email_claim = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -
IncomingClaimTypeDisplayName "Email Address" -SameAsIncoming
```

5. Enter the command below to create a variable to hold the name of your realm. This is the value you set as Relying Party ID in **step 10** in previous section.

```
$realm = "urn:sharepoint2016:defaultsite"
```

6. Enter the New-SPTrustedIdentityTokenIssuer command below to create a token issuer.

   a. Replace SECURID_ACCESS_IDR with a unique name to identify your token issuer.

   b. Replace "SecurID Access IDR" with a description of the issuer.

   c. Replace https://portal.sso.pe.rsa.net/IdPServlet?idp_id=v28nhhb3xb3d& with your Identity Provider URL followed

by an ampersand (&).

d. Replace http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress with your claim type URL.

```
$issuer = New-SPTrustedIdentityTokenIssuer -Name "SECURID_ACCESS_IDR" -Description
"SecurID Access IDR" -realm $realm -ImportTrustCertificate $root_cert -
ClaimsMappings $email_claim -SignInUrl
"https://portal.sso.pe.rsa.net/IdPServlet?idp_id=v28nhhb3xb3d&" -IdentifierClaim
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
```

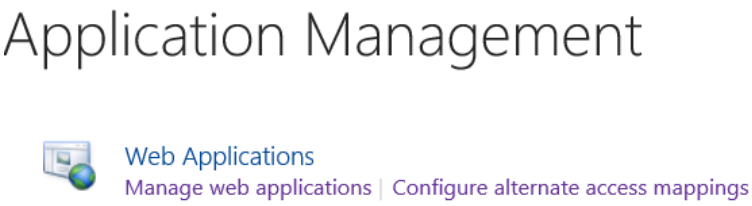
!Important: You must set the New-SPTrustedIdentityTokenIssuer command's SignInUrl parameter to your IdP URL with an & appended to the end of it. If IdP URL is https://portal.sso.pe.rsa.net/IdPServlet?idp_id=v28nhhb3xb3d, set the SignInUrl to https://portal.sso.pe.rsa.net/IdPServlet?idp_id=v28nhhb3xb3d& in the command above.

---

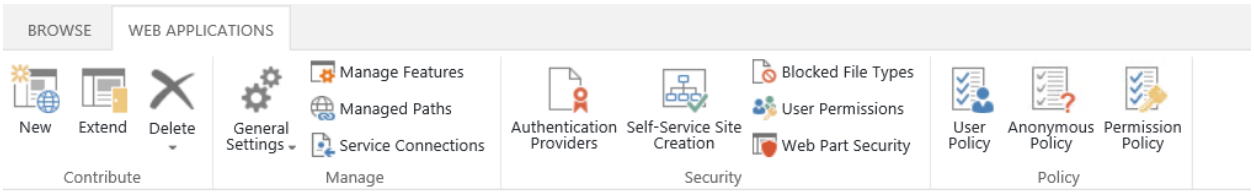
7. Follow the steps in the next section to enable RSA SecurID Access authentication on the SharePoint web application.

Configure a SharePoint Web Application to Use the RSA SecurID Access Token Issuer:

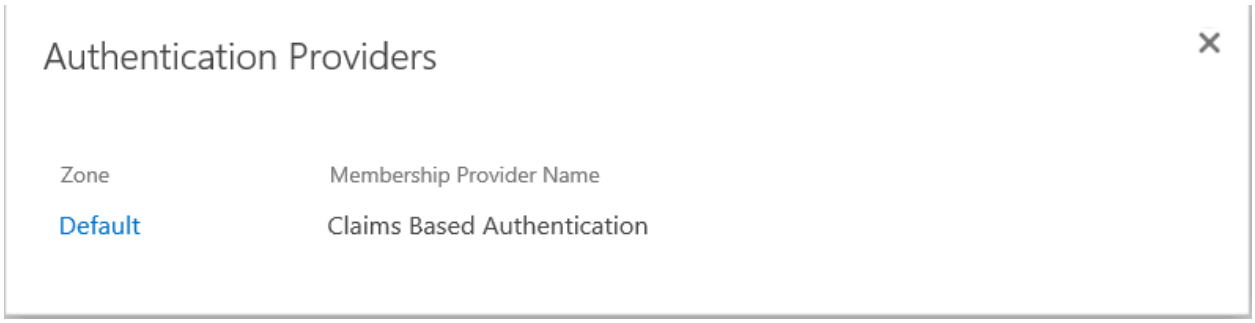
1. Open SharePoint Central Administration and click the **Manage web applications** link



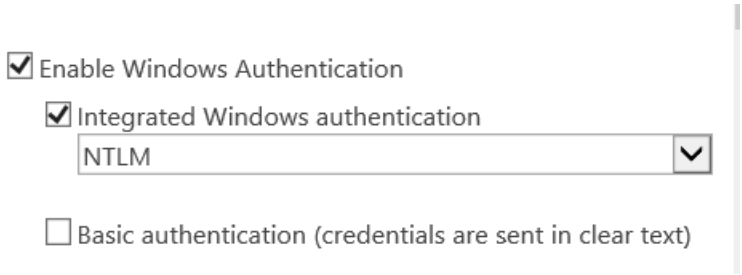
2. Highlight the web application you want to configure and click the **Authentication Providers** button



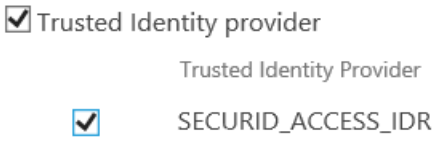
3. Click the **Default** link on the **Authentication Providers** dialog box.



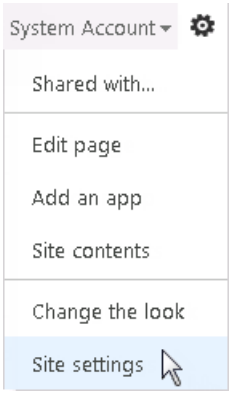
4. Confirm that the **Integrated windows Integration** checkbox is checked and that **NTLM** is selected in the dropdown list.



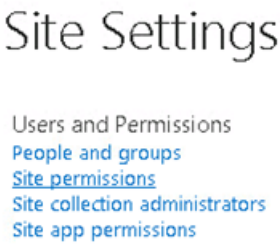
5. Check the **Trusted Identity Provider** check box.
6. Check the checkbox for the for the token issuer name you chose above.



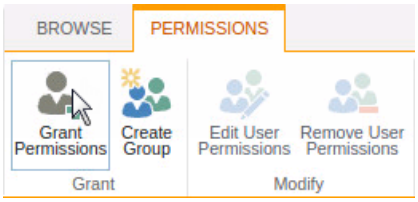
7. Click the **Save** button.
8. Log into the SharePoint site as an administrator.
9. Click the gear icon to the right of the **System Account** menu and click the **Site settings** menu item



10. Click the **Site permissions** link in the **Users and Permissions** section of the **Site Settings** page.

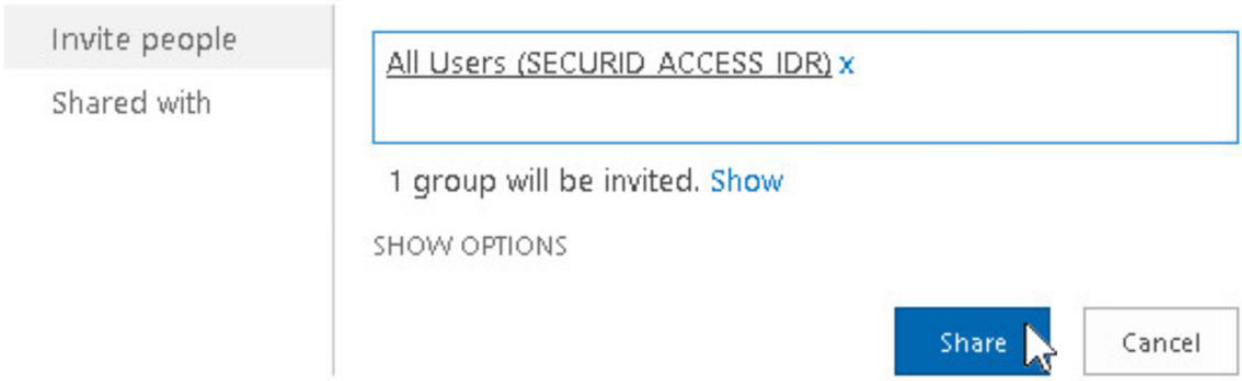


11. Click the **Grant Permissions** button at the top of the page.



12. Enter your token issuer name in the list.

13. Select the appropriate group/permission level from the dropdown based on your requirements and click the **Share** button.



Configure additional SharePoint web applications for RSA SecurID Access Integration

For configuring addtional SharePoint web applications for RSA SecurID access protection, add additional "Microsoft SharePoint WS-Fed" connectors for each web application and also create corresponding "Trusted Identity Token Issuer" for RSA SecurID Access in the SharePoint using the same procedures mentioned in **RSA Cloud Authentication Service** and **Microsoft SharePoint** configuration sections

---

Note: While creating additional "Trusted Identity Token Issuer", SharePoint does not allow to reuse the same certificate that was used to create the first "Trusted Identity Token Issuer". Regenerate public certificate again using "Generate Certificate Bundle" option and use it to create a new "Trusted Identity Token Issuer".

Configuration is complete.

Return to the main page for more certification related information.