



U.S. Department of the Interior
Office of the Chief Information Officer

Active Directory Federation Services (ADFS) Relying Party Trust (RPT) Request Form User Manual

Contents

ADFS Request Form User Manual Description:	3
Section 1: Requesting Party Information	4
Section 2: New Relying Party Trust vs. Modification to an Existing Relying Party Trust	6
Section 3: “New” Relying Party Trust (RPT)	7
Section 3a) Security Related Questions	7
Section 3b) Application/service external to the DOI	8
Section 3c) SAML 2.0 Requirement	9
Section 3d) Hard Stops.....	10
Section 3e) Metadata.....	11
Section 3f) Certificate Signing and SHA-256 Requirement	12
Section 3g) LDAP Attributes.....	13
Section 3h) Transforming Claims	14
Section 3i) Custom Claims.....	15
Section 3j) Authorization Rules.....	16
Section 3k) Test URLs.....	17
Section 3l) Request to Maintain a Test Environment	18
Section 3m) Form End.....	19
Section 4) Modification to an “Existing” Relying Party Trust (RPT)	20
Section 4a) Modification Requirements	21
Section 5) Where to locate ADFS request form required information:.....	22

ADFS Request Form User Manual Description:

This user manual is designed to assist Requesting Parties/Federated Partners with understanding what information is requested and/or required to complete an Active Directory Federation Services (ADFS) Relying Party Trust (RPT) request via the intake request form. This document is broken into the following sections;

- **Section 1**, is required for all requests;
- **Section 2**, describes the difference between a “new” or “modification” of an existing relying party trust request
- **Section 3**, describes what’s requested and/or required if you’ll be submitting a new relying party trust request;
- **Section 4**, describes what’s requested and/or required if you’ll be submitting a modification to an existing relying party trust request;
- **Section 5**, provides helpful information if you’re not sure who can provide the requested and/or required information being requested in the form.

Section 1: Requesting Party Information

A DOI Sponsor is an internal DOI federal point of contact representing the Requesting Party. This role is specifically used if an external requesting party needs access to the DOI ADFS environment, but does not have a DOI Active Directory account.

Press **“Next”** to continue. If you have left a required field blank, you will not be able to continue until it is filled out.

All questions marked with a **red asterisk** are required in order to proceed

Always read the **“help text”** under the question. This will provide important information regarding what is being asked.

The form is **dynamic**, and will take you to certain sections based on your answers. Don't be overwhelmed by the number of sections. They are not all required.

Name (First and Last) *
Your answer

Telephone number *
Your answer

Your DOI Bureau/Office *
Please provide your DOI Bureau or Office name, example: OCIO/ BSEE. Your Bureau or Office should represent the Bureau or Office that this request is being submitted on behalf of.
Your answer

DOI Sponsor *
The DOI Sponsor should be the name of the individual who is either the application/system owner or the individual who is responsible for the application/system. This person must be a federal employee.
Your answer

NEXT

Page 1 of 31

Technical Point of Contact

The technical point of contact should be the individual that can answer technical questions regarding this request.

Is the Technical Point of Contact the same person as submitter of this form? *

Yes

No



If there is a point of contact that has a more technical knowledge of the ADFS RPT requirement, please provide their contact information

Technical POC Contact Information

First and Last Name *

Your answer

Telephone Number

Your answer

Email Address *

Your answer

Section 2: New Relying Party Trust vs. Modification to an Existing Relying Party Trust

A **new** Relying Party Trust refers to a request that has never been deployed into a production environment with the Department of the Interior by the Requesting Party organization

The types of questions received will vary greatly based on the selection made here

Relying Party Trust (RPT) Description

Description *
Application Request Function/Description

Your answer

New RPT or Modification to an existing RPT *
Select 'new' for RPTs that have never been in an ADFS test or production environment. Select 'modify' for RPT requests that have already been developed in a test or production environment.

New
 Modify

BACK NEXT Page 4 of 31

Never submit passwords through Google Forms.

An existing RPT refers to a current Relying Party Trust that requires some **modification** (for example additional claims, a change in authentication rules, etc.).

Section 3: “New” Relying Party Trust (RPT) details what’s necessary to complete a new RPT request.

If you are interested in submitting a modification to an existing RPT, please go to:

Section 3: "New" Relying Party Trust (RPT)

Section 3a) Security Related Questions

Does this service have Authorization to Operate (ATO)?

This information can typically be obtained by the requesting bureau/office security department. Additional questions regarding your ATO will be asked in the ADFS Risk Assessment Template/Questionnaire. If you have a conditional ATO, please select "yes."

Yes

No

This is not a mandatory question, but an **Authorization to Operate (ATO)** is required before your application can go into Production.

Have you filled out and submitted an ADFS Risk Assessment Template / Questionnaire? *

If you have not, you will receive a request to complete after the successful submission of this form. For more information please see "ADFS Risk Assessment Template / Questionnaire" FAQ.

Yes

No

If you have not yet filled out an **ADFS Risk Assessment**, then one will be sent to you after completion of the ADFS request form is reviewed. If you are unsure, please select **No**.

Section 3b) Application/service external to the DOI

External
Is this application/service external to DOI? e.g. cloud based or hosted by a third party?

Yes

No



If your application is an internal DOI application you will be asked about options other than ADFS that you have considered

Other Authentication *
Have other authentication options such as Windows Integrated Authentication, Native Kerberos, etc. been evaluated first?

Yes

No



Authentications Considered *
Which options have been considered and why can't they be used.

Your answer



You will not be able to continue if you have not considered other authentication options.

Stop

You can not complete the application please provide additional details of why you can not meet this requirement then Select Save on the next Screen.

There are many alternative ways to authenticate directly with AD that many applications can use such as Integrated Windows Authentication, and Kerberos that can connect directly with Active Directory and provide an even higher level of security as well as minimizing the additional resources that ADFS / SAML might require. In these instances, it is preferable to use native authentication protocols before use ADFS/SAML. Please consider using native authentication prior to submitting your ADFS request.

Section 3c) SAML 2.0 Requirement

An **application is required to support SAML 2.0** in order to obtain a Relying Party Trust with the DOI. SAML permits DOI to make assertions regarding the identity, attributes, and entitlements of user account to an external web service. Adoption of SAML is central to the agency's successful implementation of the Federal Identity, Credential, and Access Management (FICAM) strategy and corresponding two-factor PIV authentication requirements for cloud-based web applications and services. For more information regarding this requirement please see the memo "Mandatory use of Security Assertion Markup Language (SAML) 2.0 Standard for Cloud-Based, Web Application Authentication Information Exchange."

Support SAML *
Does the application/service support SAML 2.0?

Yes

No



Stop

You can not complete the application please provide additional details of why you can not meet this requirement then Select Save on the next Screen.

Connections to ADFS in DOI require the use of SAML 2.0.

Section 3d) Hard Stops

Active Directory Federation Services (ADFS) RPT Request Form

Your email address (amelia_phillips@ios.doi.gov) will be recorded when you submit this form. Not you? [Sign out](#)

STOP

If you have reached this page you will be unable to submit this record for processing. Please see the following website for information on why your application can not be processed: You can go to the next page and select submit to save your work.

<https://www.doi.gov/ocio/customers/what-ADFS-does>
<https://www.doi.gov/ocio/customers/need-more-information>

You can follow these links for more information, or to submit a question.

If you receive a hard stop, you will be able to save your responses to come back and finish it later if applicable.

Submit: Will NOT be Processed

If you click submit your record will be sent to you with an edit link to modify your saved record.

A copy of your responses will be emailed to amelia_phillips@ios.doi.gov.

BACK

SUBMIT

Page 33 of 33

Section 3e) Metadata

Is your metadata available in an exportable .xml file?
If you are unsure, select "no." *If you have a URL please select other and provide the URL. *For additional questions please see FAQs/User Manual.

Yes

No

Other : _____

If you select **Yes**, you will receive an email reminding you to attach the .xml file to an email and submit it to the Customer Support Center (CSC) helpdesk.

If you have the **url** for your metadata, please provide it in the "other" field.

Select **No**, if you do not have metadata in an exportable .xml file or url, or if you do not know. It will take you to the following questions to obtain necessary

Endpoint URL *
What is the Service Provider (SP) Endpoint URL? (Must be Valid URL starting with https://)

Your answer _____

What is the Relying Party ID (RPId)? *
The RPId is located in the Metadata and is how application identifies itself to ADFS. It's often a the URL used to access the application. For additional questions please see FAQs/User Manual.

Your answer _____

Redirect *
Are there any redirect URLs required such as specific logout, etc.?

Yes

No

Section 3f) Certificate Signing and SHA-256 Requirement

Certificate signing *
Does this RPT require certificate signing?

Yes

No

If you select **Yes**, an email will be sent reminding you to attach the signing certificate and email it to the CSC helpdesk.

The **SHA (Secure Hash Algorithm)** is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. This makes it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. **If your application does not support SHA-256 it will be rejected.**

Does this RPT support 256 bit Secure Hash Algorithm (SHA-256)? *

Yes

No

Unknown - requires testing

Stop

You can not complete the application please provide additional details of why you can not meet this requirement then Select Save on the next Screen.

Applications are required to support a 256 bit Secure Hash Algorithm (SHA-256)

Section 3g) LDAP Attributes

You can use **Send LDAP Attributes as Claims Rules** when you want to issue outgoing claims that contain actual Lightweight Directory Access Protocol (LDAP) attribute values that exist in an attribute store and then associate a claim type with each of the LDAP attributes. For more detailed information see: [https://technet.microsoft.com/en-us/library/ff678048\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/ff678048(v=ws.11).aspx)

LDAP Attributes/Outgoing Claims *

What attributes are required as outgoing claims, please fill out the specifications as illustrated on a separate line for each attribute. LDAP Attributes ----> OUTGOING CLAIM

User-Principal-Name ----> Name ID

To answer this question note the example below:

Ex: User-Principal-Name ----> Name ID

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Name ID
Given-Name	Given Name
Surname	Surname
E-Mail-Addresses	E-Mail Address
extensionAttribute5	extensionAttribute5

Section 3h) Transforming Claims

You can use **Transforming Claims** rules when you need to map an incoming claim type to an outgoing claim type and then apply an action that will determine what output should occur based on the values that originated in the incoming claim. When you use this rule, you pass through or transform claims that match the following rule logic, based on either of the options that you configure in the rule, as described in the following table. For more detailed information please see: [https://technet.microsoft.com/en-us/library/ee913567\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/ee913567(v=ws.11).aspx)

Transforming Claims *
Does the RPT require any transforming of claims? Please check all that apply and use the other field to enter any claims that are not listed.

E-mail to Name ID

UPN to Name ID

None required

Other: _____

Section 3i) Custom Claims

You write a **custom claim** rule in Active Directory Federation Services (AD FS) using the claim rule language, which is the framework that the claims issuance engine uses to programmatically generate, transform, pass through, and filter claims. By using a custom rule, you can create rules with more complex logic than a standard rule template. For more detailed information please see: [https://technet.microsoft.com/en-us/library/ee913558\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/ee913558(v=ws.11).aspx)

Custom claims *
Are any custom claims required?

Yes

No

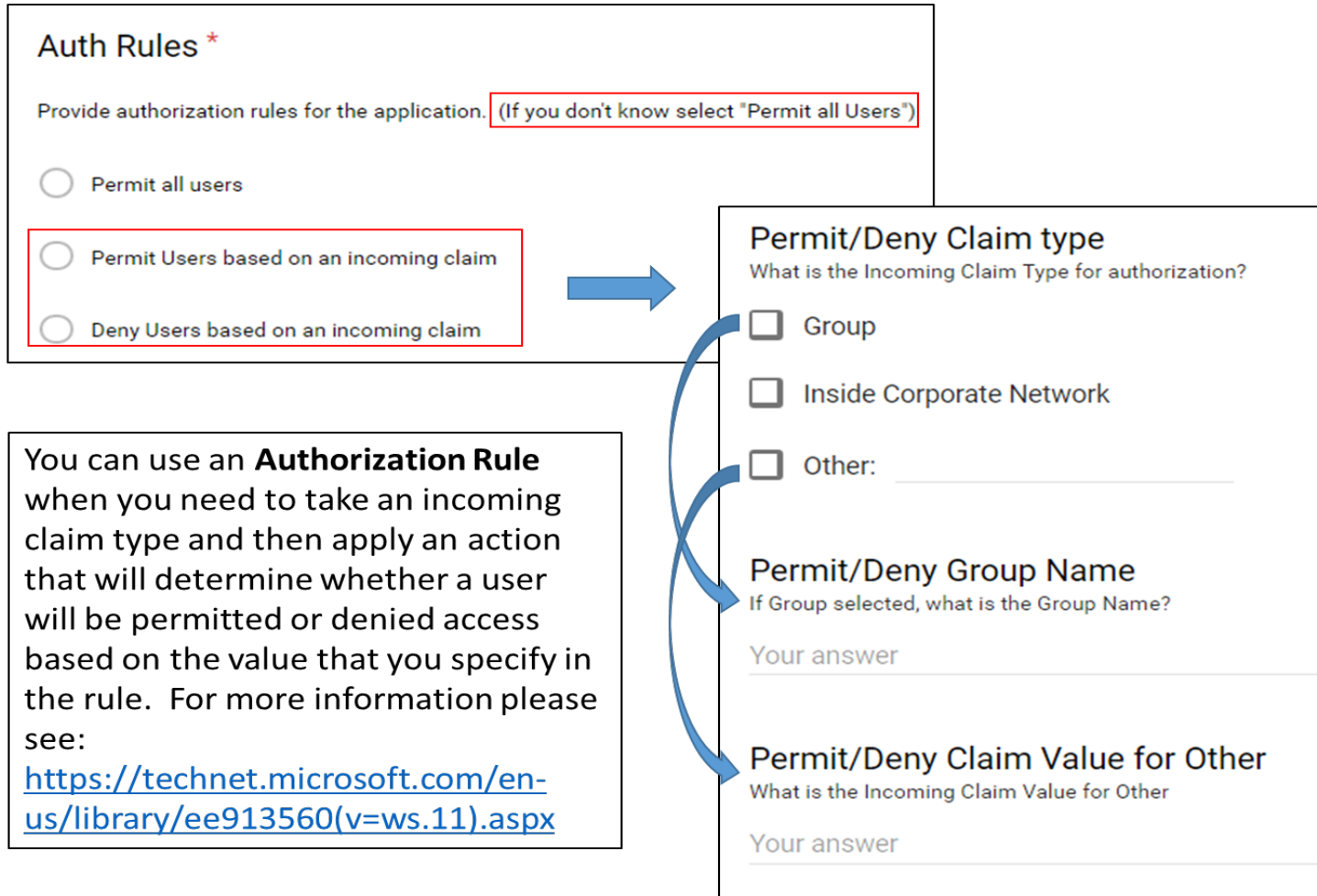


What custom claims are required?

Please use this space to enter the claim rule language below. Please describe and paste your claim language if you have it.

Your answer

Section 3j) Authorization Rules



Section 3k) Test URLs

Are Test URLs the same as Production? *

(If you don't know select yes)

Yes

No

This question is asked in order to prevent you from having to enter information in twice.

The Test Environment is where all requirements are tested prior to going live to ensure that all requirements are met, there are no bugs in the code, etc. Once all testing is complete the application can go live, by being placed in a Production Environment.



Endpoint URL *

What is the Service Provider (SP) Endpoint URL for test?

Your answer

Relying Party *

What is the Relying Party ID URLs for test?

Your answer

Redirect URL

Are there any redirect URLs required for test?

Your answer

Testing Request *

Are you requesting a test/dev environment to be maintained post deployment to production?

Yes

No

Section 3) Request to Maintain a Test Environment

Testing Request *
Are you requesting a test/dev environment to be maintained post deployment to production?

Yes

No



If you would like a Test Environment maintained after your application has gone into Production, you will give more information here.

How long should Test Environment be maintained?

1 week

2 weeks

1 month

Ongoing

Other : _____

Section 3m) Form End

This is the **end of the form!** Please provide any additional information you think would be helpful to the developers; e.g. links to technical documentation such as **SAML configuration documents**.

Additional Information

Please provide any additional information you feel would be necessary to have this created. For example: links to any technical documentation (such as SAML or application configuration documentation), etc.

Your answer

Save or Process *

If you are ready to forward this request for review select Complete. Select Save if you would like to save your work and come back and complete later. If you select Complete we ask you do not modify the record unless directed by the reviewing authority.

Save

Complete

Select **Save** to save your work and come back to it later.

Once you're ADFS RPT request has been reviewed **you'll receive a link to complete the ADFS Risk Assessment questionnaire** that must be completed prior to your application/service goes into production.

Select **Complete**, when you are ready to submit it for review to the ADFS team. **Note:** Upon successful form submission, you'll receive an email with instructions on how to submit required attachments if you indicated you have exportable metadata or SHA256 certification.

Section 4) Modification to an “Existing” Relying Party Trust (RPT)

What is the name of the application and RPid that needs to be modified? *

The RPid is located in the Metadata and is how application identifies itself to ADFS. It's often a the URL used to access the application. For additional questions please see FAQs/User Manual.

Your answer _____

The RPid is located in the Metadata, and is how the application identifies itself to ADFS. It is often the URL used to access the application.

The Rpid can be provided by whoever configured the application to SAML (this is often, but not always the vendor).

Status *

Is the existing RPT in Test or Production?

Test

Production



Production Testing

If in production has this change been tested?

Yes

No

Section 4a) Modification Requirements

Change *
What is the change you are requesting?

- Delete RPT services no longer needed
- Additional Claim
- Remove a claim
- Add/update endpoint
- Add/update RPId
- Remove endpoint
- Remove RPId
- Turn on Encryption
- Turn on Multi-factor Authentication for Internal
- Add certificate signing
- Other: _____

Select the changes you require, and then answer the applicable questions that go along with your modification request.

Additional Claim
What is the claim you need to add?

Your answer

Remove a Claim
What is the claim you wish to remove?

Your answer

Add/update endpoint
What is the new endpoint?

Your answer

Remove endpoint
What is the endpoint you wish to remove?

Your answer

Remove RPId
What is the RPId you wish to remove?

Your answer

Endpoint Type
What type of endpoint is this?

Post

Redirect

Other : _____

Add/update RPId ID
What type of endpoint is this?

Post

Redirect

Other : _____

Add/update RPId
What is the new RPId?

Your answer

Section 5) Where to locate ADFS request form required information:

If you're not sure where to acquire the requested and/or required information to submit the ADFS RPT request form, please refer to the below table.

Information	Where to locate:
Authorization to Operate (ATO)	Your bureau's security office would have the application/system's ATO. The ATO refers to permission for a product to be used in an existing system.
Metadata	The vendor or application developer can provide this information. Metadata is defined as the data providing information about one or more aspects of the data; it is used to summarize basic information about data which can make tracking and working with specific data easier.
Does Application Support SAML?	The vendor or application developer can provide this information
Does Application Support SHA-256?	The vendor or application developer can provide this information
Test URLs same as Production URLs	The bureau/office point of contact or the vendor should have this information
The RPid	The RPid is located in the Metadata, and is how the application identifies itself to ADFS. It is often the URL used to access the application. The Rpid can be provided by whoever configured the application to SAML (this is often, but not always the vendor).
Custom claim rule	A claim rule that you author using the claim rule language to express a series of complex logic conditions. You can build custom rules by typing the claim rule language syntax in the Send Claims Using a Custom Rule template.
Where can I find help configuring ADFS 3.0 to communicate with SAML 2.0?	Please follow this link for detailed instructions: http://wiki.servicenow.com/index.php?title=Configuring ADFS 3.0 to Communicate with SAML 2.0
Where can I find help configuring ADFS 3.0 to communicate with Esri	Please follow this link for detailed instructions: https://doc.arcgis.com/en/arcgis-online/reference/configure-adfs.htm

ArcGIS Online?	
Where can I find help configuring SAML for WordPress?	Please follow this link for detailed instructions: https://support.onelogin.com/hc/en-us/articles/204353160-Configuring-SAML-for-WordPress