[MS-ADFSPIP]: Active Directory Federation Services and Proxy Integration Protocol

This topic lists the Errata found in the MS-ADFSPIP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V4.0 – 2015/06/30.

Errata Published*	Description
2016/06/27	In Section 3.8.5, Message Processing Events and Sequencing Rules, changed the resource name from Proxy/RelyingPartyTrusts/{Identity}/PublishingSettings to Proxy/RelyingPartyTrusts/{Identity}/PublishedSettings. Changed the name of Section 3.8.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings, to 3.8.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishedSettings and changed references to "PublishingSetting" throughout the section to "PublishedSettings". In Section 3.8.5.1.2, DELETE, changed references to "PublishingSetting" throughout the section to "PublishedSettings". Changed the name of Section 3.9.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings to 3.9.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishedingSettings.
2016/06/27	In multiple sections, added or updated descriptions about client TLS authentication. In Section 3.3.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the proxy MUST present the certificate on [Proxy Service State Data].TrustCertificate during client TLS authentication. Changed to: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the proxy MUST present the certificate on [Client State].TrustCertificate during client TLS authentication. In Section 3.4.5, Message Processing Events and Sequencing Rules, included the following paragraph at the end of the section: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.4.5.1.1, GET, removed the following paragraph because the content is specified in the parent section 3.4.5, Message Processing Events and Sequencing Rules:

Errata Published*	Description
	The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 400. In Section 3.4.5.2.1, GET, removed the following paragraph because the content is specified in the parent section 3.4.5, Message Processing Events and Sequencing Rules: The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. In Section 3.4.5.3.1, GET, removed the following paragraph because the content is specified in the parent section 3.4.5, Message Processing Events and Sequencing Rules: The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. In Section 3.5.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST do client TLS authentication [RFC2246] using the certificate in [Proxy Service State Data].TrustCertificate. Changed to: For all operations in this section, the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate. In Section 3.6.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.7.5, Message Processing Events and Sequencing Rules, included the following paragraph at the beginning of the section: For all operations in this section, the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate. In Section 3.8.5, Message Processing Events and Sequencing Rules, changed from:

Errata Published*	Description
	In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.9.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST use the certificate represented by [Proxy Service State Data].TrustCertificate during client TLS authentication. Changed to: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate. In Section 3.10.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the client during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the client during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. Section 3.12.5.1.5, Proxy Preauthentication for Active Clients, included the following paragraph at the end of the section: For this operation, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.13.5.2.3, Response to Active Requests, included the following paragraph about client TLS authentication: The proxy MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate.
2016/05/31	In several sections, revised quotation marks around values in the JSON definitions for complex types to accurately represent data types.

Errata Published*	Description

	In Section 2.2.2.4, Configuration, changed from:
	
	`{`
	`  "ServiceConfiguration" :`
	`  {`
	`  "ServiceHostName" : "<service-host-name>",`
	`  "HttpPort" : "<http-port-number>",`
	`  "HttpsPort" : "<https-port-number >",`
	`  "HttpsPortForUserTlsAuth" : "<user-TLS-port-number>",`
	`  "DeviceCertificateIssuers" : [ "<device-certificate-issuer>", * ],`
	`  "ProxyTrustCertificateLifetime" : "<trust-renewal-interval>",`
	`  "DiscoveredUpnSuffixes" : [ "<upn-suffix>", * ],`
	`  "CustomUpnSuffixes" : [ "<upn-suffix>", * ]`
	`  },`
	`  "EndpointConfiguration" :`
	`  [`
	`  {`
	`  "Path" : "<endpoint-uri>",`
	`  "PortType" : "<port-type>",`
	`  "AuthenticationSchemes" : "<credential-collection-scheme>",`
	`  "ClientCertificateQueryMode" : "<tls-query-behavior>",`
	`  "CertificateValidation" : "<certificate-validation>",`
	`  "SupportsNtlm" : "<support-ntlm>",`
	`  "ServicePath" : "<service-endpoint-uri>",`
	`  "ServicePortType" : "<service-port-type>"`
	`  }, *`
	`  ]`
	`}`
	
	Changed to:
	
	`{`
	`  "ServiceConfiguration" :`
	`  {`
	`  "ServiceHostName" : "<service-host-name>",`
	`  "HttpPort" : <http-port-number>,`
	`  "HttpsPort" : <https-port-number >,`
	`  "HttpsPortForUserTlsAuth" : <user-TLS-port-number>,`
	`  "DeviceCertificateIssuers" : [ "<device-certificate-issuer>", * ],`
	`  "ProxyTrustCertificateLifetime" : <trust-renewal-interval>,`
	`  "DiscoveredUpnSuffixes" : [ "<upn-suffix>", * ],`
	`  "CustomUpnSuffixes" : [ "<upn-suffix>", * ]`
	`  },`
	`  "EndpointConfiguration" :`
	`  [`
	`  {`
	`  "Path" : "<endpoint-uri>",`
	`  "PortType" : "<port-type>",`
	`  "AuthenticationSchemes" : "<credential-collection-scheme>",`
	`  "ClientCertificateQueryMode" : "<tls-query-behavior>",`
	`  "CertificateValidation" : "<certificate-validation>",`
	`  "SupportsNtlm" : "<support-ntlm>",`
	`  "ServicePath" : "<service-endpoint-uri>",`
	`  "ServicePortType" : "<service-port-type>"`
	`  }, *`
	`  ]`

Errata Published*	Description

	}
	
	In Section 2.2.2.5, Relying Party Trust List, changed from:
	
	[{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : "<is-web-application-published>",
	"nonClaimsAware" : "<is-a-non-claims-aware-web-application>",
	"enabled" : "<is-web-application-enabled>"
	}, +]
	
	Changed to:
	
	[{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : <is-web-application-published>,
	"nonClaimsAware" : <is-a-non-claims-aware-web-application>,
	"enabled" : <is-web-application-enabled>
	}, +]
	
	In Section 2.2.2.6, Relying Party Trust, changed from:
	
	{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : "<is-web-application-published>",
	"nonClaimsAware" : "<is-a-non-claims-aware-web-application>",
	"enabled" : "<is-web-application-enabled>",
	"identifiers" : [<web-application-identifier>, *],
	"proxyTrustedEndpoints" : [<web-application-at-proxy-endpoint-url>, *],
	"proxyEndpointMappings" :
	[{ "Key" = "<internal-url>", "Value" = "external-url" }, *]
	}
	
	…
	enabled: Boolean value specifying if the web application is enabled at the server.
	…
	
	Changed to:
	
	{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : <is-web-application-published>,
	"nonClaimsAware" : <is-a-non-claims-aware-web-application>,
	"enabled" : <is-web-application-enabled>,
	"identifiers" : [<web-application-identifier>, *],
	"proxyTrustedEndpoints" : [<web-application-at-proxy-endpoint-url>, *],
	"proxyEndpointMappings" :
	[{ "Key" = "<internal-url>", "Value" = "<external-url>" }, *]

Errata Published*	Description

	}
	
	…
	is-web-application-enabled: Boolean value specifying if the web application is enabled at the server.
	…
	
	In Section 2.2.2.9, Store Entry, changed from:
	
	{
	"key" : "<entry-key>",
	"version" : "<entry-version>",
	"value" : "<entry-value>"
	}
	
	Changed to:
	
	{
	"key" : "<entry-key>",
	"version" : <entry-version>,
	"value" : "<entry-value>"
	}
	
	In Section 2.2.2.11, Serialized Request with Certificate, changed from:
	
	{
	"Request" :
	{
	"AcceptTypes" : ["<accept-type>", *],
	"Content" : [<byte>, *],
	"ContentEncoding" : "<content-encoding>",
	"ContentLength" : "<content-length>",
	"ContentType" : "<content-type>",
	"Cookies" :
	[{
	"Name" : "<cookie-name>",
	"Value" : "<cookie-value>",
	"Path" : "<cookie-path>",
	"Domain" : "<cookie-domain>",
	"Expires" : "<cookie-expires>",
	"Version" : "<cookie-version>",
	}, *],
	"Headers" :
	[{ "Name" : "<header-name>", "Value" : "<header-value>" }, *],
	"HttpMethod" : "<http-method>",
	"RequestUri" : "<request-uri>",
	"QueryString" : [{ "Name" : "<query-param>", "Value" : "<query-value>" }, *],
	"UserAgent" : "<user-agent>",
	"UserHostAddress" : "<user-host-address>",
	"UserHostName" : "<user-host-name>",
	"UserLanguages" : ["<user-language>", *]
	},
	"SerializedClientCertificate" : "<serialized-client-certificate>",
	"CertificateUsage" : "<certificate-usage>",
	}

Errata Published*	Description

	Changed to:
	
	`{`
	`  "Request" :`
	`  {`
	`  "AcceptTypes" : [ "<accept-type>", * ],`
	`  "Content" : [ <byte>, * ],`
	`  "ContentEncoding" : "<content-encoding>",`
	`  "ContentLength" : <content-length>,`
	`  "ContentType" : "<content-type>",`
	`  "Cookies" :`
	`  [ {`
	`  "Name" : "<cookie-name>",`
	`  "Value" : "<cookie-value>",`
	`  "Path" : "<cookie-path>",`
	`  "Domain" : "<cookie-domain>",`
	`  "Expires" : <cookie-expires>,`
	`  "Version" : <cookie-version>,`
	`  }, * ],`
	`  "Headers" :`
	`  [ { "Name" : "<header-name>", "Value" : "<header-value>" }, * ],`
	`  "HttpMethod" : "<http-method>",`
	`  "RequestUri" : "<request-uri>",`
	`  "QueryString" : [ { "Name" : "<query-param>", "Value" : "<query-value>" }, * ],`
	`  "UserAgent" : "<user-agent>",`
	`  "UserHostAddress" : "<user-host-address>",`
	`  "UserHostName" : "<user-host-name>",`
	`  "UserLanguages" : [ "<user-language>", * ]`
	`  },`
	`  "SerializedClientCertificate" : "<serialized-client-certificate>",`
	`  "CertificateUsage" : "<certificate-usage>",`
	`  }`
	
	In Section 2.2.2.17, Proxy Token, changed from:
	
	`{`
	`  "ver" : "<version>",`
	`  "aud" : "<audience>",`
	`  "iat" : "<issued-at>",`
	`  "exp" : "<expire>",`
	`  "iss" : "<issuer>",`
	`  "relyingpartytrustid" : "<rp-trust-id>",`
	`  "deviceregid" : "<device-registration-id>",`
	`  "authinstant" : "<auth-instant>",`
	`  "authmethod" : "<auth-method>",`
	`  "upn" : "<upn>"`
	`  }`
	
	Changed to:
	
	`{`
	`  "ver" : "<version>",`
	`  "aud" : "<audience>",`
	`  "iat" : <issued-at>,`
	`  "exp" : <expire>,`
	`  "iss" : "<issuer>",`
	`  "relyingpartytrustid" : "<rp-trust-id>",`
	`  "deviceregid" : "<device-registration-id>",`
	`  "authinstant" : <auth-instant>,`

Errata Published*	Description

	<pre>"authmethod" : "<auth-method>",
	"upn" : "<upn>"
	}</pre>
	In Section 2.2.2.21, Error Response, changed from:
	<pre>{
	"id" : "<error-id>",
	"message" : "<message>",
	"type" : "<type>",
	}</pre>
	Changed to:
	<pre>{
	"id" : <error-id>,
	"message" : "<message>",
	"type" : "<type>",
	}</pre>
	In Section 3.1.1.3, Relying Party Trust State, changed from:
	<pre>{
	"RelyingPartyTrust" : "<web-application>",
	"RedirectBasedPreauth" : "<redirect-based-preauth>"
	}</pre>
	Changed to:
	<pre>{
	"RelyingPartyTrust" : "<web-application>",
	"RedirectBasedPreauth" : <redirect-based-preauth>
	}</pre>
	In Section 6, Appendix A: Full JSON Schema, changed from:
	…
	<pre>{
	"title" : "Configuration",
	"type" : "object",
	"properties" :
	{
	"ServiceConfiguration" :
	{
	"type" : "object",
	"properties" :
	{
	"ServiceHostName" : {"type" : "string"},
	"HttpPort" : {"type" : "integer"},
	"HttpsPort" : {"type" : "integer"},
	"HttpsPortForUserTlsAuth" : {"type" : "integer"},
	"DeviceCertificateIssuers" :
	{</pre>

Errata Published*	Description

	<pre>"type" : "array",
	"items" : {"type" : "string"}
	},
	"ProxyTrustCertificateLifetime" : {"type" : "integer"}
	}
	},
	"EndpointConfiguration" :</pre>
	…
	
	Changed to:
	…
	<pre>{
	"title" : "Configuration",
	"type" : "object",
	"properties" :
	{
	"ServiceConfiguration" :
	{
	"type" : "object",
	"properties" :
	{
	"ServiceHostName" : {"type" : "string"},
	"HttpPort" : {"type" : "integer"},
	"HttpsPort" : {"type" : "integer"},
	"HttpsPortForUserTlsAuth" : {"type" : "integer"},
	"DeviceCertificateIssuers" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	},
	"ProxyTrustCertificateLifetime" : {"type" : "integer"},
	"DiscoveredUpnSuffixes" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	}
	"CustomUpnSuffixes" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	}
	}
	},
	"EndpointConfiguration" :</pre>
	…

2016/05/16	In Section 2.2.2.15, Certificate Validation, updated the values for the Certificate Validation enumeration.
	Changed from:
	<pre>…
	{
	"None"
	"User"
	"Device"
	}
	…</pre>

Errata Published*	Description

	Changed to:
	
	…
	{
	"None"
	"Ssl"
	"IssuedByDrs"
	}
	…
	
	In Section 6, Appendix A: Full JSON Schema, updated values for the CurrentEndpointConfiguration.CertificateValidation enumeration.
	
	Changed from:
	
	…
	"CertificateValidation" :
	{
	"enum" : ["None", "User", "Device"]
	},
	…
	
	Changed to:
	
	…
	"CertificateValidation" :
	{
	"enum" : ["None", "Ssl", "IssuedByDrs"]
	},
	
	…

2016/05/02	In Section 2.2.2.11, Serialized Request with Certificate, added details to clarify the purpose of the serialized request contained by this object. Changed from: … This is a JSON object containing a serialized request plus a serialized client certificate and its usage. The format of the object is as follows: … Changed to: … This is a JSON object containing a serialized HTTP request that is intended for the target service, plus a serialized client certificate and its usage. The format of the object is as follows: …
2016/04/18	In Section 3.6.5.2.4, DELETE, revised the description to call out the correct operation and behavior. Changed from: This operation modifies the value of an existing entry in the store. The operation is transported by a HTTP PUT and can be invoked through the following URIs:

Errata Published*	Description
	… Changed to: This operation removes the value of an existing entry in the store. The operation is transported by an HTTP DELETE and can be invoked through the following URIs: …

*Date format: YYYY/MM/DD