[MS-DRS] Device Registration Service

Specifies the Device Registration Join Protocol, which establishes a device identity between the physical device and an Entra ID (Azure AD) tenant.

Published Version

Date	Protocol Revision	Revision Class	Downloads
10/12/2023	0.01	New	

1 Introduction

The Device Registration Join Protocol provides a lightweight mechanism for registering personal or corporate-owned devices with an Entra ID tenant.

This protocol also defines the discovery of information needed to register devices.

2 Protocol Details

2.1 Join Service Details

2.1.1 device

The following HTTP methods are allowed to be performed on this resource.

HTTP method	Section	Description
POST	2.1.1.1	Create a new device object.

2.1.1.1 POST

This method is transported by an HTTP POST.

The method can be invoked through either the JoinEndpoint URI or the PrecreateEndpoint URI (if specifying a PreAuthorizedJoinChallenge) discovered via the Device Registration Discovery Service.

2.1.1.1.1 Request Body

The request body contains the following JSON-formatted object.

```
{
   "CertificateRequest": {
      "Type": string,
      "Data": string
   },
   "TransportKey": string,
   "TargetDomain": string,
   "DeviceType": string,
   "OSVersion": string,
   "DeviceDisplayName": string,
   "JoinType": number,
   "AikCertificate": string,
   "AttestationData": string,
   "Attributes": {
        "ReuseDevice": true|false,
        "SharedDevice": true|false
    },
    "PreAuthorizedJoinChallenge": string
}
```

CertificateRequest: A property with the following fields:

- **Type**: A property that MUST contain "pkcs10". Required.
- **Data**: A property that contains a base64-encoded PKCS#10 certificate request [RFC4211]. The certificate request MUST use anRSA public key algorithm [RFC8017] with a 2048-bit key, a SHA256WithRSAEncryption signature algorithm, and a SHA256 hash algorithm. The Certificate request SHOULD incorporate a Nonce extension as received from a Nonce Service Request. Required.
    - The OID for the Nonce extension is defined as "1.2.840.113556.1.5.284.2.1".

TransportKey: The base64-encoded JWK containing the public portion of an asymmetric key that is generated by the client. Required.

```
{
    "kty": "RSA",
    "n": "reME3...-rUsQ",
    "e": "AQAB",
    "alg": "RS256",
    "kid": "90c68066-5d9f-4de5-8615-15ac52568bc7",
}
```

TargetDomain: The fully qualified host name of the device registration service. Required.

DeviceType: The operating system type installed on the device. Required.

OSVersion: The operating system version installed on the device. Required.

DeviceDisplayName: The friendly name of the device. Required.

JoinType: The type of join operation. The value is set as defined below. Required.

JoinType	Description
0	Azure AD join.
3	Unknown.
4	Azure AD register.
6	Possibly a federated join to on-prem AD.
8	Unknown.

AikCertificate: Attestation Identity Key Certificate. Optional.

AttestationData: An exported TPMS_ATTEST structure. Optional.

Attributes: A property with the following fields:

- **ReuseDevice**: This device object may be reused. Optional.
- **SharedDevice**: This device is a shared device. Optional.
- **ReturnClientSid**: Whether to include the MembershipChanges field in the response. Optional.

PreAuthorizedJoinChallenge: A JSON Web Token (JWT). If this attribute is specified, then the join request MUST be submitted to the PrecreateEndpoint URI. Optional.

2.1.1.1.2 Response Body

If the DRS server successfully creates a device object in the directory, an HTTP 200 status code is returned. Additionally, the response body for the POST response contains a JSON-formatted object, as defined below. See section 2.1.1.1.3 for processing details.

```
{
   "Certificate": {
      "Thumbprint": string,
      "RawBody": string
   },
   "User": {
      "Upn": string
   },
   "MembershipChanges": [
      {
         "LocalSID": string,
         "AddSIDs": string array,
      }
   ]
}
```

Certificate: A property with the following fields.

- **Thumbprint**: The SHA1 hash of the certificatethumbprint.
- **RawBody**: An X.509 certificate signed by the DRS server as a base64-encoded string [RFC4648].

User: A property with the following fields.

- **Upn**: The identifier of the identity that authenticated to the Web service, or the registered owner of the device.

MembershipChanges: An array with the following fields.

- **LocalSID**: The security identifier (SID) of the directory administrator account. This value MUST be ignored by the client.
- **AddSIDs**: An array of sids. This value MUST be ignored by the client.

2.1.1.1.3 Processing Details

3 Protocol Examples

3.1 Device Registration Discovery Service

Discover the list of available enrollment URLs and api versions.

HTTP Request

You can address the tenant using either the**tenantId** or **domain name**.

```
GET /{tenantId}/Discover?api-version=1.9
GET /{domainName}/Discover?api-version=1.9
```

Request Headers

Name	Description

Name	Description
Content-type	application/json
ocp-adrs-client-name	The name of the client application making the request.
ocp-adrs-client-version	The software version of the client application making the request.

Request body

Do not supply a request body for this method.

Response

If successful, this method returns a 200 OK response code and a list of enrollment services in the response body.

Example

Request

The following is an example of the request.

```
GET https://enterpriseregistration.windows.net/{tenantId}/Discover?api-version=1.9
```

Response

The following is an example of the response.

```
HTTP/1.1 200 OK
Content-type: application/json

{
  "DiscoveryService": {
    "DiscoveryEndpoint": "https://{registrationServer}/{tenantId}/Discover",
    "ServiceVersion": "1.9"
  },
  "DeviceRegistrationService": {
    "RegistrationEndpoint": "https://{registrationServer}/EnrollmentServer/DeviceEnrollmentWebService.svc",
    "RegistrationResourceId": "urn:ms-drs:{registrationServer}",
    "ServiceVersion": "1.0"
  },
  "AuthenticationService": {
    "OAuth2": {
      "AuthCodeEndpoint": "https://{authServer}/{tenantId}/oauth2/authorize",
      "TokenEndpoint": "https://{authServer}/{tenantId}/oauth2/token"
    }
  },
  "IdentityProviderService": {
    "Federated": false,
    "PassiveAuthEndpoint": "https://{authServer}/{tenantId}/wsfed"
  },
  "DeviceJoinService": {
    "JoinEndpoint": "https://{registrationServer}/EnrollmentServer/device/",
    "JoinResourceId": "urn:ms-drs:{registrationServer}",
    "ServiceVersion": "2.0"
  },
  "KeyProvisioningService": {
    "KeyProvisionEndpoint": "https://{registrationServer}/EnrollmentServer/key/",
    "KeyProvisionResourceId": "urn:ms-drs:{registrationServer}",
    "ServiceVersion": "1.0"
  },
  "WebAuthNService": {
    "ServiceVersion": "1.0",
    "WebAuthNEndpoint": "https://{registrationServer}/webauthn/{tenantId}/",
        "WebAuthNResourceId": "urn:ms-drs:{registrationServer}"
    },
    "DeviceManagementService": {
        "DeviceManagementEndpoint": "https://{registrationServer}/manage/{tenantId}/",
        "DeviceManagementResourceId": "urn:ms-drs:{registrationServer}",
        "ServiceVersion": "1.0"
    },
    "MsaProviderData": {
        "SiteId": "{siteId}",
        "SiteUrl": "{registrationServer}"
    },
    "PrecreateService": {
        "PrecreateEndpoint": "https://{registrationServer}/EnrollmentServer/device/precreate/{tenantId}/",
        "PrecreateResourceId": "urn:ms-drs:{registrationServer}",
        "ServiceVersion": "2.0"
    },
    "TenantInfo": {
        "DisplayName": "{tenantName}",
        "TenantId": "{tenantId}",
        "TenantName": "{domainName}"
    },
    "AzureRbacService": {
        "RbacPolicyEndpoint": "https://pas.windows.net"
    },
    "BPLService": {
        "BPLProxyServicePrincipalId": "{UUID}",
        "BPLResourceId": "urn:ms-drs:{registrationServer}",
        "BPLServiceEndpoint": "https://{registrationServer}/aadpasswordpolicy/{tenantId}/",
        "ServiceVersion": "1.0"
    },
    "DeviceJoinResourceService": {
        "Endpoint": "https://{registrationServer}/EnrollmentServer/device/resource/{tenantId}/",
        "ResourceId": "urn:ms-drs:{registrationServer}",
        "ServiceVersion": "2.0"
    },
    "NonceService": {
        "Endpoint": "https://{registrationServer}/EnrollmentServer/nonce/{tenantId}/",
        "ResourceId": "urn:ms-drs:{registrationServer}",
        "ServiceVersion": "1.0"
    }
}
```

3.2 Nonce Service

The Nonce Service is used to request a nonce (__n__umber**once**) for crafting join requests.

HTTP request

A nonce request is sent using the Nonce Service endpoint and ServiceVersion discovered during discovery in section 4.2.1.

You can address the tenant using either the**tenantId** or **domain name**.

```
GET /EnrollmentServer/nonce/{tenantId}/?api-version=1.0
GET /EnrollmentServer/nonce/{domainName}/?api-version=1.0
```

Request Headers

None.

Response

If successful, this method returns a 200 OK response code and a nonce value in the response body.

Example

Request

The following is an example of the request.

```
GET https://enterpriseregistration.windows.net/EnrollmentServer/nonce/{tenantId}/?api-version=1.0
```

Response

The following is an example of the response.

> **Note:** The response object shown here is shortened for readability.

```
HTTP/1.1 200 OK
Content-type: application/json

{
   "ReponseStatus": {
      "message": "Successfully created a nonce",
      "traceId": "c532f6ca-259a-44af-8720-1f901ec69a09",
      "time": "10/12/2023 3:05:30 PM"
   },
   "Value": "ZXlKaGJHY2lPaUpTVTBFdFQwRkZVQzB5TlRZaUxDSmxibU1pT2lKQk1qVTJSME5OS
          {...}
          ENGV1aS15WlJ4OVdDN1hhc0RrTXA4SWUyUC5KM0hoSXlUWjRDNU1La3kzZklSc253"
}
```

3.3 Device Join Service

The purpose of the Device Join Service is to enroll a device in the directory.

HTTP Request

The device join request is sent using the Device Join Service endpoint and ServiceVersion discovered during discovery in section 3.2.1.

This method is transported by an HTTP POST.

The method can be invoked through the following URI:

```
POST /EnrollmentServer/device/?api-version=2.0
```

Request headers

Name	Description
Authorization	Bearer {token}. Required.
Content-type	application/json
client-request-id	A correlation Id. Optional.
ocp-adrs-client-name	The name of the client application making the request.
ocp-adrs-client-version	The software version of the client application making the request.

The authorization token must be granted via a PublicClientApplication using the Microsoft Authentication Broker application while requesting access to the Device Registration Service application resource.

Application ID	Description
29d9ed98-a469-4536-ade2-f981bc1d605e	Microsoft Authentication Broker Application Id
01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9	Device Registration Service Application Id

Request body

In the request body, supply a JSON representation of a device registration join request, as specified in section 2.1.1.1.1.

Response

If successful, this method returns 201 Created response code and a signed certificate in the response body, as specified in section 2.1.1.1.2.

Example

The following example shows a request to the DRS server to create a device object(section 2.1.1.1.1) and the response (section 2.1.1.1.2).

Request

Here is an example of the request.

> **Note:** The request object shown here is shortened for readability.

```
POST https://enterpriseregistration.windows.net/EnrollmentServer/device/?api-version=2.0
Content-type: application/json

{
 "CertificateRequest": {
  "Type": "pkcs10",
  "Data": "MIICd...LWH31"
 },
 "TransportKey": "UlNBM...G5Q==",
 "TargetDomain": "sts.contoso.com",
 "DeviceType": "Linux",
 "OSVersion": "openSUSE Leap 15.5",
 "DeviceDisplayName": "MyPC",
 "JoinType": 4
}
```

Response

Here is an example of the response.

> **Note:** The response object shown here is shortened for readability.

```
HTTP/1.1 201 Created
Content-type: application/json

{
  "Certificate": {
    "Thumbprint": "D09A73223D16855752C5E820A70540BA6450103E",
    "RawBody": "MIID/...rQZE="
  },
  "User": { "Upn": "myuser@contoso.com" },
  "MembershipChanges": [
    {
      "LocalSID": "S-1-5-32-544",
      "AddSIDs": [
        "S-1-12-1-3792446273-1182712816-3605559969-2553266617",
        "S-1-12-1-2927421837-1319477369-3754249106-3334640282"
      ]
    }
  ]
}
```