**NetApp B2C Federation Request Form**

The NetApp identity provider for Partner and Customer interactions is Microsoft Azure Active Directory B2C. Please complete this questionnaire and submit via email to [ng-identity-federation@netapp.com](mailto:ng-identity-federation@netapp.com) with Subject *Federation Request –* *Company Name*.

**Company and Requestor Information**

|  |  |
| --- | --- |
| **First Name** | Click or tap here to enter text. |
| **Last Name** | Click or tap here to enter text. |
| **Email Address** | Click or tap here to enter text. |
| **Company** | Click or tap here to enter text. |
| **Title** | Click or tap here to enter text. |
| **Domains to Federate** | Click or tap here to enter text. |
| **Add’l Contacts (Email)** | Click or tap here to enter text. |

**Identity Federation Prerequisites**

Identity federation does not support some identity configuration. Please answer the following questions to determine if there any blockers to federation. The following items must be **No** to proceed with federation.

|  |  |
| --- | --- |
| \* Distribution lists as email addresses are not supported in federation. Unique email addresses must be used. Are you using Distribution Lists as email addresses? | Choose an item. |
| \* Email aliases for the same mailbox are not supported in federation. Are individuals in your organization using email aliases for different existing NetApp Support IDs? | Choose an item. |

If your organization is using MS Azure Active Directory, the following items must be **Yes** to proceed with federation.

|  |  |
| --- | --- |
| \* Tenant restrictions for your tenant may impact federation. Will your organization allow access to the NetApp B2C tenant if required? | Choose an item. |
| \* Some organizations restrict sign in to only UserPrincipalName (UPN) and do not allow email address sign in. Does your organization support sign in with email address? | Choose an item. |
| \* Some organizations use federation service with MS Azure AD, for example: ADFS, OKTA, or any other IDP. If this is the case, then we will proceed with configuring federation with your MS Azure AD as it will redirect to your federated IDP. | Choose an item. |
| \* Once MS Azure federation is enabled, users/admin would require providing consent for the first time. If Admin consent review is enabled, then admin must grant consent before federation can be leveraged by users. | Choose an item. |
| \* If you are using MS Azure as your IDP, then are all the users who are registered with us from your organization synced/created in Azure AD? | Choose an item. |

**Customer Identity Provider**

If all prerequisites are met, please confirm the identity provider.

|  |  |
| --- | --- |
| \* Please confirm your Identity Provider (MS Azure, Okta, ADFS, Auth0, or other). | Click or tap here to enter text. |
| \* Is your Identity Provider Microsoft Azure Active Directory, Google, or Microsoft Accounts? If so, you may skip the remainder of the questionnaire. | Choose an item. |

**SAML Federation**

If your organization would like to federate via SAML, please complete the following detail.

|  |  |
| --- | --- |
| \* Please share the Metadata URL for your IDP. | Click or tap here to enter text. |
| \* Is a specific signature algorithm required?  SHA1 is the default.  Please confirm if another algorithm is required (e.g., SHA256, SHA384, SHA512). | Click or tap here to enter text. |
| \* Does your IdP require the incoming request to be signed? | Choose an item. |
| \* Will your IdP send signed responses to Azure B2C? | Choose an item. |
| \* Will your IdP send encrypted assertions? | Choose an item. |

**OAuth or OIDC Federation**

If your organization would like to federate via generic OAuth or OIDC, please create an application with client ID and secret within your identity provider and complete the following detail.

|  |  |
| --- | --- |
| \* Please share the Metadata URL for your IDP. | Click or tap here to enter text. |
| \* Please share the Client ID. | Click or tap here to enter text. |

Please note, the client secret should only be shared with NetApp Identity and Management representative after engagement on the federation request.

**Federation Claims**

NetApp MS Azure AD B2C requires the following claims to be passed by the IDP.  Please confirm if other attributes are required by your IdP. Click or tap here to enter text.

Required OAuth/OIDC Identity Provider Claims:

* givenName        given\_name
* surname             family\_name
* displayName     name
* email                   email

Required SAML Identity Provider Claims:

* Surname            last\_name
* Given-Name      first\_name
* Email                  email
* Display-Name   displayname
* Email userPrincipalName

We look forward to engaging with you and your organization to enable federation for access to NetApp applications.