FREJA eID

FREJA eID AZURE IdP INTEGRATION

DOCUMENT VERSION 1.0
APRIL 2020

BEFORE YOU START

The Freja eID IdP currently works with personal Freja eID on Basic, Extended or Plus level. Preconditions for successful integration are:

1. Those users wishing to access Office 365 with Freja eID must have your domain-based email address configured as their primary email address in Freja eID. For example, if your domain is hultbybruk.com and assuming a user name Joe Black, the email joe.black@hultbybruk.com should be configured as the user's primary email.

   When users register for Freja eID, the first email they use will be set as the primary email by default. If they registered with another email, they may add joe.black@hultbybruk.com and set it as their primary email via minasidor.frejaeid.com later.

2. You must configure an Azure AD that the IdP has read access to. In the Azure AD, accounts must be searchable based on email addresses with the tenant's domain name (as per the example above, @hultbybruk.com), and an Azure AD attribute needs to contain the persistent ID configured for each user in Office 365.

INTEGRATION STEPS

Once you have signed a contract to use Freja eID Azure IdP follow these steps to complete the integration:

1. Please provide the following to partnersupport@frejaeid.com:

    a. The **name** of your company (100 characters maximum);
    b. The **logo** of your company – ideally in SVG format, alternatively PNG, no larger than 1.5MB;
    c. A brief **description** of your company in English and Swedish (500 characters maximum);
    d. The **URL** you wish to be displayed to users in Freja eID e.g. your website or login page.

2. Together with Verisec Freja eID AB support team, deploy the Azure Cloud machine image of the Freja eID Azure IdP within your tenant.

3. Once you complete the deployment, send the IP address of the instance to partnersupport@frejaeid.com.

4. Provide SSH (port 22) access to the instance, at least from Verisec Freja eID AB networks.

5. Configure general TCP access on port 8443 to the IdP instance.

6. Send the IP address or DNS name of the Azure AD instance within the tenant, alongside a Read Only account username and password to partnersupport@frejaeid.com.

7. We will notify you when we have configured everything on our end. You will also receive the following parameters for PowerShell:

    a. **LogOffUri**
    b. **LogOnUri**
    c. **IssuerUri**
    d. **SigningCert**

Commands to execute:

Connect-MsolService

Then enter username/password for a user with Administrator rights in popup.

Note! In the commands below, spaces surrounding the '=' sign are important. Obviously, hultbybruk-azureidp.test.frejaeid.com should be replaced with something resembling the real customer and in prod.frejaeid.com domain, we will fine tune this with the first live customer.

$DomainName = "hultbybruk.com"

$FederationBrandName = "Hultbybruk Freja eID Demo SAML 2.0 IDP"

$LogOffUri = "https://hultbybruk-azureidp.test.frejaeid.com:8443/idp/profile/SAML2/Redirect/SLO"

$LogOnUri = "https://hultbybruk-azureidp.test.frejaeid.com:8443/idp/profile/SAML2/POST/SSO"

$IssuerUri = "https://hultbybruk-azureidp.test.frejaeid.com"

$SigningCert = @"certificate"@

<ENTER> (to get back to the command prompt)

Set-MsolDomainAuthentication -Authentication Federated –DomainName $DomainName -FederationBrandName $FederationBrandName -SigningCertificate $SigningCert -LogOffUri $LogOffUri -IssuerURI $IssuerUri -PassiveLogOnUri $LogOnUri -PreferredAuthenticationProtocol SAMLP

Get-MsolDomain -DomainName $DomainName

The output of the command should show Federated as authentication - as opposed to Managed which is the default.

Name	Status	Authentication
hultbybruk.com	Verified	Federated

VERIFYING IT WORKS

To try out whether federated authentication works:

1. Go to https://www.office.com/
2. Sign in – use the email that you previously set as your primary email in Freja eID
3. Scan the QR code or enter that email address (if on mobile)
4. Approve the transaction in Freja eID
5. You should be signed in to Office 365.