Identity Service Integration

Table of Contents

Overview

With the integration of the Identity Service (also known as 'IDP'), it provides system defence from brute-force attacks, breaking of weak passwords, improved password policies and the ability for a Partner to integrate their Azure AD, bringing the ability for seamless sign-ins across platforms and enforcement of MFA.

Available features:

- Integration into Azure AD (AAD) for the Partner
- Set your own password policies for your own users (or inherit ours)
- Set your own password policies for child account users (customers)
- Two-factor authentication (via Google Authenticator) **BETA**

Requirements List

Name	Partner Detail	Example
Login URL (SAML2 Authentication URL)		https://login.microsoftonline .com//saml2
Logout URL		https://login.microsoftonline .com/common/wsfederation ?wa=wsignout1.0
Display Phrase of Button		“Azure AD” NOTE: It is prefixed with “Login with”, therefore specifying “Azure AD” will mean the login page button says “Login with Azure AD”
SAML2 Certificate		------BEGIN CERTIFICATE---- MIIDjjCCAnYCCQCErQYi+gB /0jANBgkqhkiG9w0BAQUFA DCBiDELMAkGA1UEBhMC-- --- END CERTIFICATE--- You will need to send this via encrypted/secure mail or upload to a site for Infinigate to download.
SAML Assertion Attribute		http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Password expiration (days) **OPTIONAL**		42 days
Required character types **OPTIONAL**		Digits, Uppercase, Lowercase, Special symbols (required/not required)
Prohibit usernamebased passwords **OPTIONAL**		Yes/No
Minimum password length **OPTIONAL**		10
Number of previous passwords to prohibit **OPTIONAL**		1
Enterprise Application in Azure AD		See below
Brand ID		61 Note: This is provided to you by Infinigate after your brand has been configured

Azure AD Integration

In order to link your Azure AD into your new CORE brand, you will need to create an enterprise application that is used to control the mapping between CORE and AAD.

1. Go to Microsoft Azure, select your tenant, and open Azure Active Directory from the menu on the left.

2. Select **Enterprise applications** and click **new application**.

3. Choose **Non-gallery application** and specify its name as "core-brand-".

4. Select Users and Groups, click Add user and add your desired group for mapping to allow Azure AD users of this group to log in to CORE.

****IMPORTANT****

This group acts as the mapping between the CORE system and Azure AD. If you add the user infinigate1@infinigate.cloud to the group/enterprise app, you will also need to arbitrarily create this user as a staff member under your Partner account inside CORE (you do not need to take note of the password) to link the mapping of the two.

5. Select Single Sign-On, then choose the SAML SSO method. In the Basic SAML Configuration tile, enter the following values:

Parameter: Value:

Identifier (Entity ID) https://<brand_domain>/auth/realms/sr<brand_id>

Parameter:	Value:
Identifier (Entity ID)	https://<brand_domain>/auth/realms/sr<brand_id>
Reply URL (Assertion Consumer Service URL)	https://%3Cbrand_domain%3E/auth/realms/sr%3Cbrand_id%3E/broker/saml/endpoint
Sign on URL	https://%3Cbrand_domain%3E/auth/realms/sr%3Cbrand_id%3E/broker/saml/endpoint

Where: is the brand identifier in CORE (please ask Infinigate if you are unsure).

6. Go to the SAML Signing Certificate tile and download the Base 64 SAML Signing Certificate (this is what is listed in the requirements table)

7. Go to the Set up core-brand-mybrand.com tile and copy the login URL value from it (this is the login URL as per the requirements table)

Considerations & Stipulations

- Azure AD Integration is preferred over Two-Factor Authentication via Googles Authenticator app. Only Partner's that do not have an Azure AD tenant should consider Google 2FA.
- You must have a brand to take advantage of Azure AD integration.
- Azure AD Integration for end-customers is not available.
- Identity Service-related features can only be managed inside the "Classic Panel" – not UX1.
- The Two-Factor authentication with the Google Authenticator is currently in BETA and therefore, could be subject to unforeseen bugs.
- You can have a password policy for your own users and/or for your child account users.
- If you do not specify any password policy details, then you will inherit the default from the platform.
- With Azure AD integration enabled, you will still be able to login with standard staff member details if required (the standard login button). It is possible to configure the identity service to redirect any visits to the brand directly to the external flow (Azure AD sign in). If you wish to have this, please specify, however bearing in mind that this will prevent any logins for users that do not have the Azure AD binding in place.
- As per the important note under step 4 of the Azure AD integration, the user log-in name inside CORE must be equal to the same login in Azure AD.

Infinigate Cloud

Delme Place
Cams Hall Estate
Delme 3
Fareham
PO16 8UX

www.infinigate.cloud