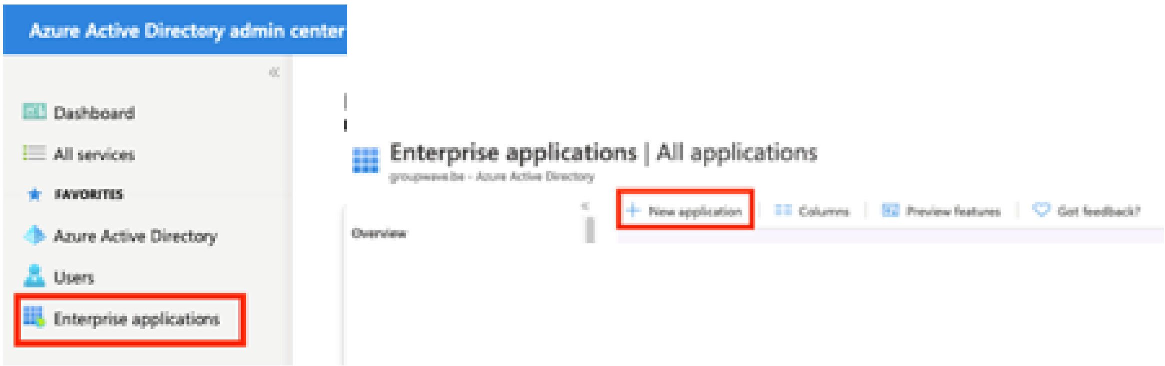
HCL Domino SSO with AzureAD

Kris De Bisschop

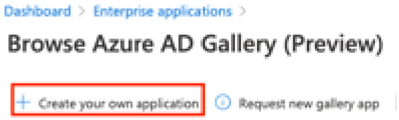
Now Domino officially supports Azure Active Directory as an Identity Provider (IDP). In this document I will explain how to set up Domino SSO with Azure AD

Azure Active Directory (AAD) settings

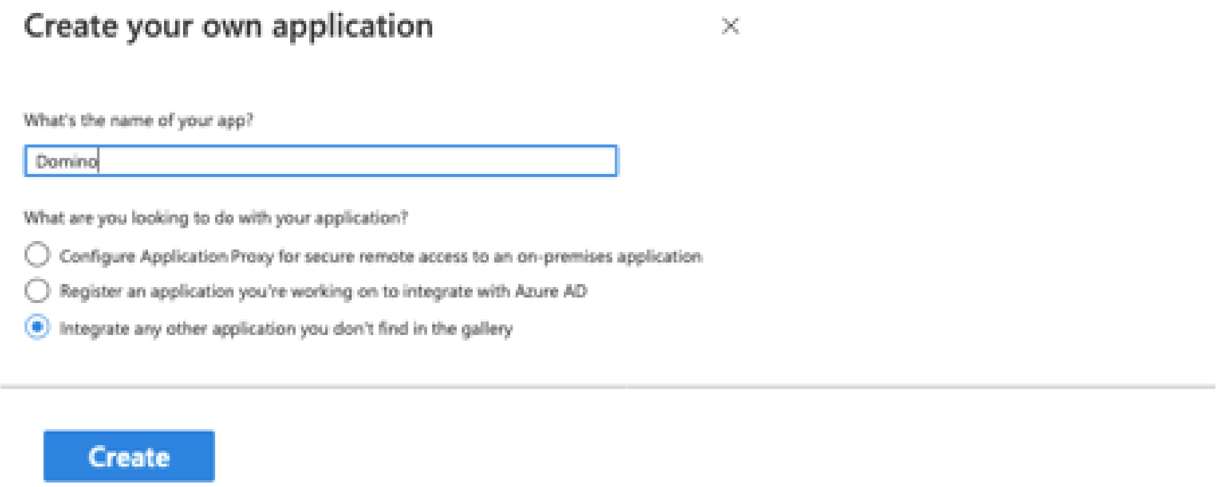
To be able to manage AAD you need to go the Azure Active Directory Admin center, https://aad.portal.azure.com Click on Enterprise applications and then on New Application to be able to register the Domino website as as an application



Create your own application


Dashboard > Enterprise applications >
Browse Azure AD Gallery (Preview)
+ Create your own application
Request new gallery app

Fill in a name that you choose and select to register the application to integrate with AAD and click the create button



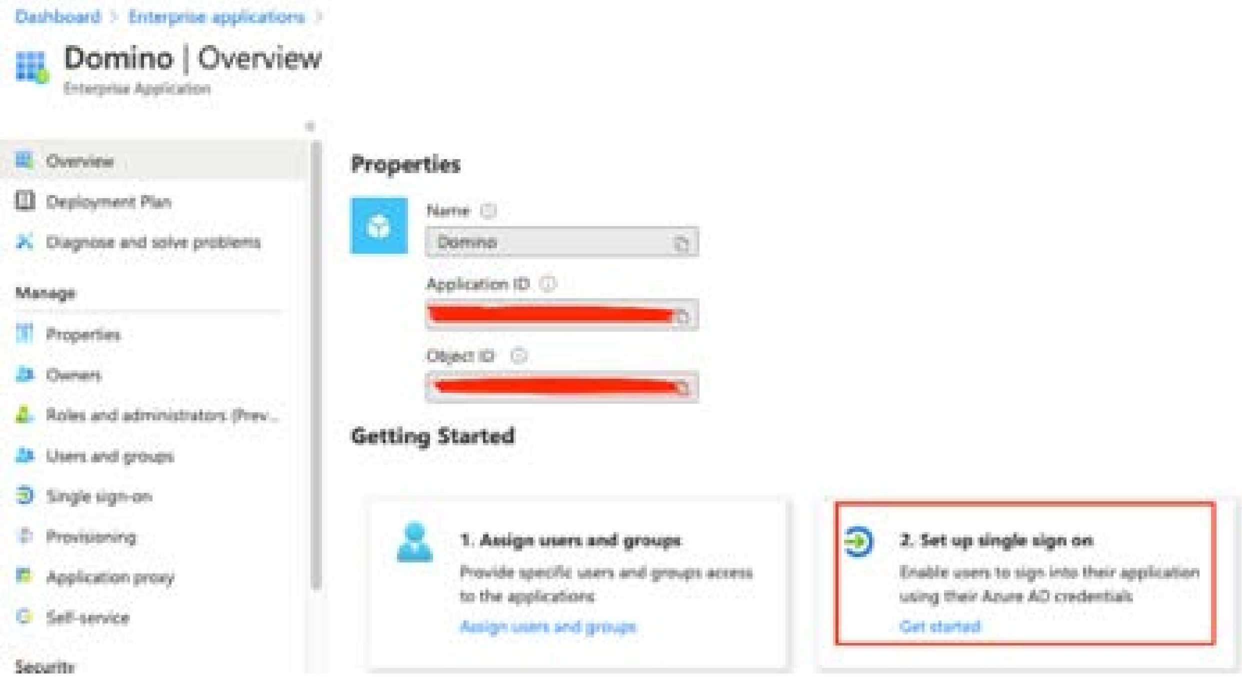
What's the name of your app?

Domino

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application you're working on to integrate with Azure AD
● Integrate any other application you don't find in the gallery

Once the application is created, you will be directed to the configuration page of the application.



Dashboard > Enterprise applications >

Domino | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators (Prev...

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Properties

Name: Domino

Application ID: [redacted]

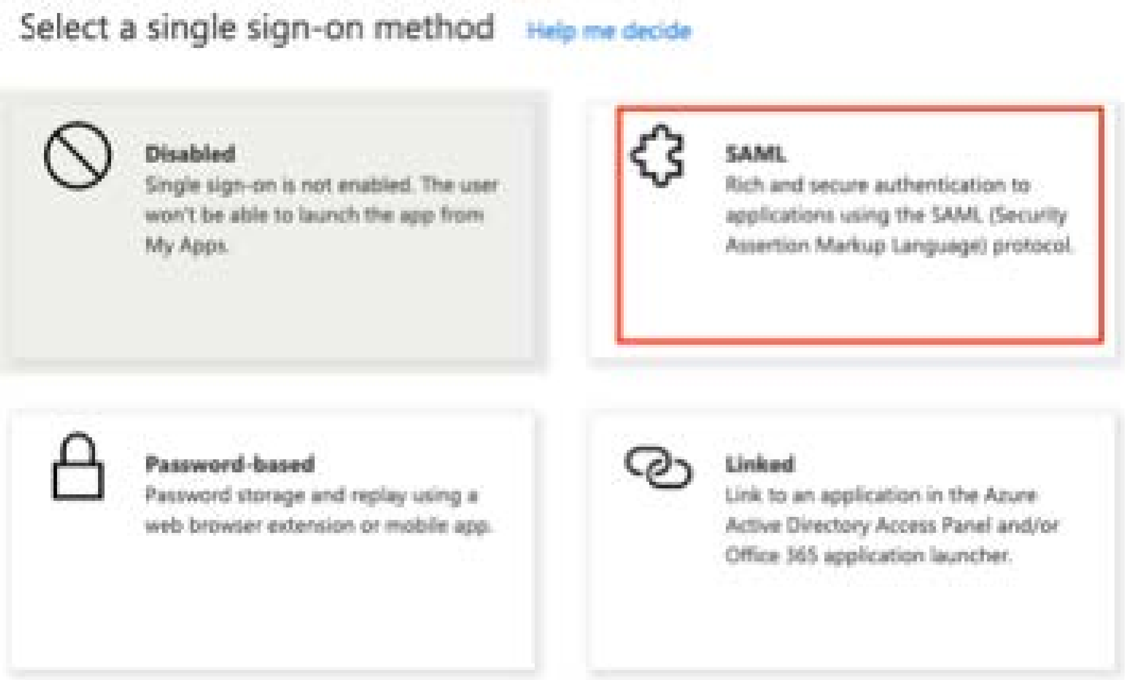
Object ID: [redacted]

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

Click on Set up single sign on and choose for SAML authentication.



Select a single sign-on method Help me decide

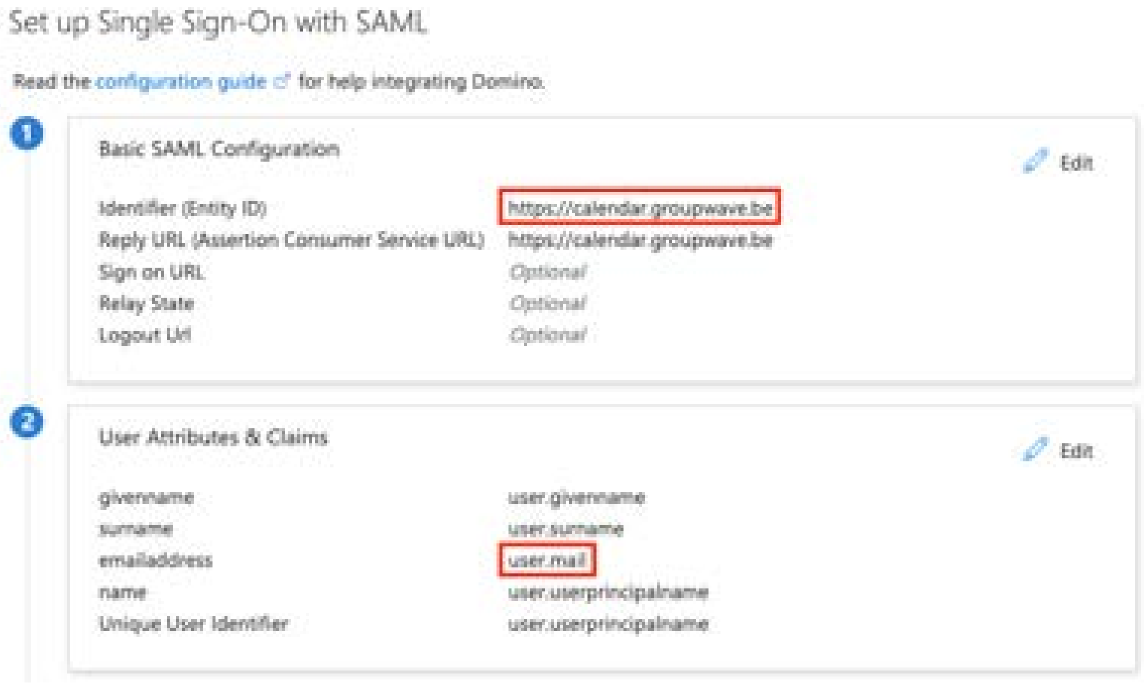
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

You will have to fill in the URL of the application that you want to link, this is the URL of your Domino internet site. As an attribute you can go with the defaults, you need to be sure that user.mail is in there so that you use the internet mail address as a unique identifier between the two directories.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Domino.

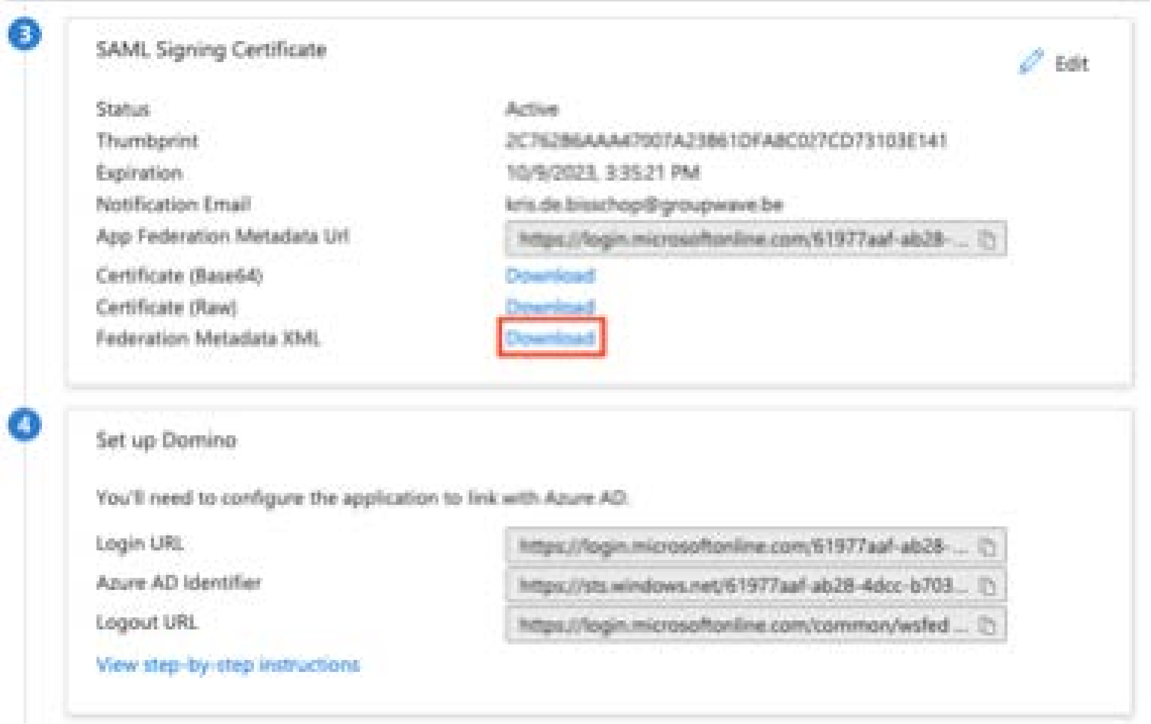
1 Basic SAML Configuration

Identifier (Entity ID)	https://calendar.groupwave.be
Reply URL (Assertion Consumer Service URL)	https://calendar.groupwave.be
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Download the federation Metadata XML file



3 SAML Signing Certificate

Status	Active
Thumbprint	2C76286AAA47007A23861DFA8C027CD73103E141
Expiration	10/9/2023, 3:35:21 PM
Notification Email	kris.de.bisschop@groupwave.be
App Federation Metadata Url	https://login.microsoftonline.com/61977aaf-ab28-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

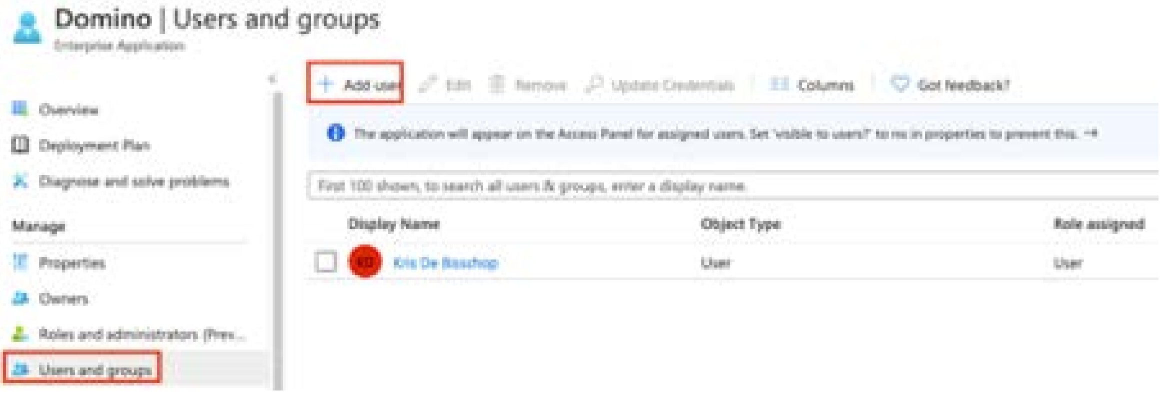
4 Set up Domino

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/61977aaf-ab28-...
Azure AD Identifier	https://sts.windows.net/61977aaf-ab28-4dcc-b703...
Logout URL	https://login.microsoftonline.com/common/wsfed ...

View step-by-step instructions

Assign a test user or a group to your application so that they can authenticate



Domino | Users and groups

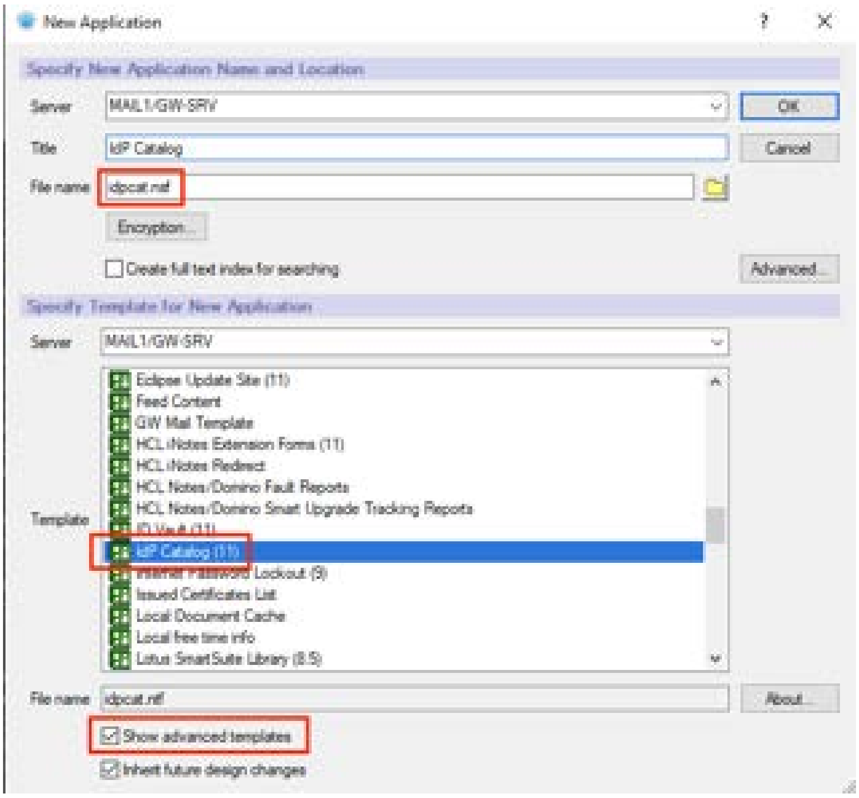
Enterprise Application

The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
Kris De Bosschop	User	User

Go to your Domino Administrator client and create and IDP Catalog database on your server. Make sure you give it the name idpcat.nsf and select Show Advanced templates to be able to see the IdP Catalog template in the list.



New Application

Specify New Application Name and Location

Server: MAIL1/GW-SRV

Title: IdP Catalog

File name: idpcat.nsf

☐ Create full text index for searching

Specify Template for New Application

Server: MAIL1/GW-SRV

Template: IdP Catalog (11)

File name: idpcat.ntf

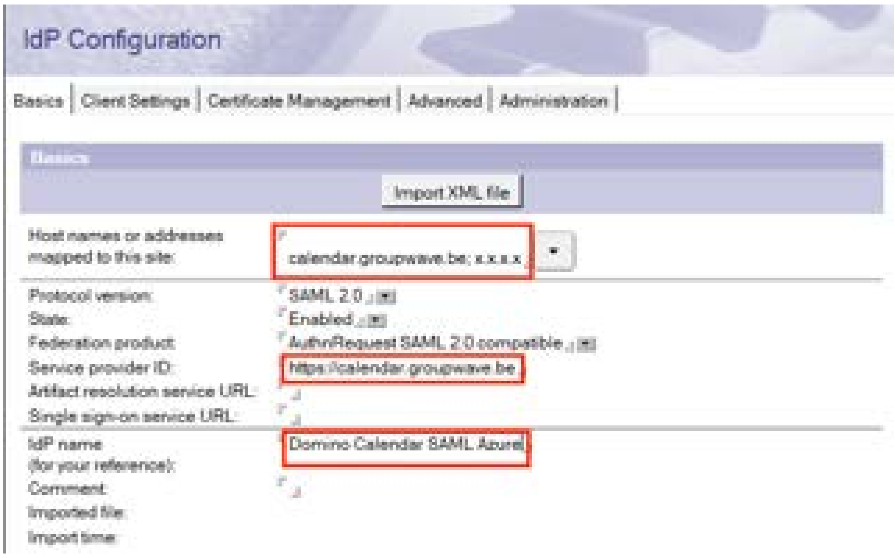
☑ Show advanced templates

☑ Inherit future design changes

In the IdP Catalog database, click on Add IdP Config and fill in the following fields

In the hostname field, fill in the name of the internet site and the IP Address that you use

In the Service Provider ID fill in the URL of the site In the IdP name field you may fill in a name as a reference for yourself, this field is just a comment.

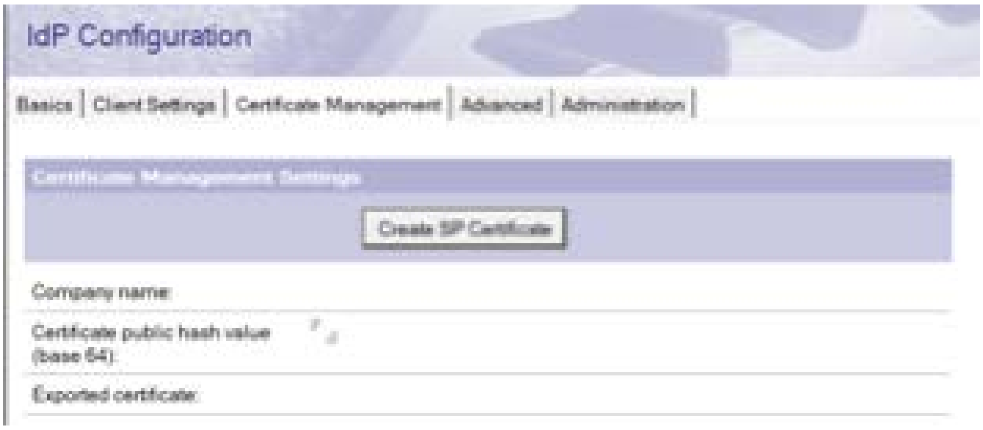

IdP Configuration
Basics | Client Settings | Certificate Management | Advanced | Administration |
Basics
Import XML file

Host names or addresses mapped to this site: calendar.groupwave.be; x.x.x.x
Protocol version: SAML 2.0
State: Enabled
Federation product: AuthnRequest SAML 2.0 compatible
Service provider ID: https://calendar.groupwave.be
Artifact resolution service URL:
Single sign-on service URL:
IdP name (for your reference): Domino Calendar SAML Azure
Comment:
Imported file:
Import time:

Click on the button Import XML file and browse to the XML file you downloaded from your Enterprise Application.

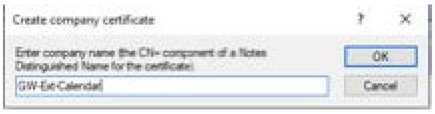
This import will fill in the Single sign-on service URL Field and the fields on the Advanced tab of the configuration document.

Save the document with Ctrl-S to be able to go to the next step. On the certificate Management tab, click on the button Create SP Certificate


IdP Configuration
Basics | Client Settings | Certificate Management | Advanced | Administration |
Certificate Management Settings
Create SP Certificate

Company name:
Certificate public hash value (base 64):
Exported certificate:

You will be asked to fill in a Company name, you may fill in whatever you want

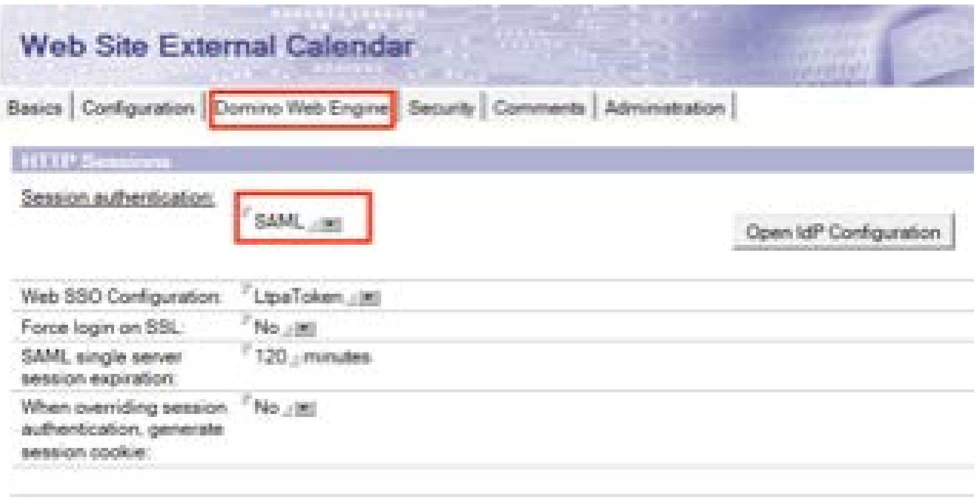


Enter company name the CN= component of a Notes Distinguished Name for the certificate:
GW-Ext-Calendar

Double click in the IdP Configuration document and fill in the Domino URL, in this case HTTPS://calendar.groupwave.be

Click on the button Export SP XML and you will see the ServiceProvider.xml file getting attached to the document. Save and Close the document and go to your internet sites view to change the affected site.

In your internet site document, go to the tab Domino Web Engine and change the Session authentication type to SAML



HTTP Sessions

Session authentication: SAML

Web SSO Configuration: LtpaToken

Force login on SSL: No

SAML single server session expiration: 120 minutes

When overriding session authentication, generate session cookie: No

When you click on the button Open IdP Configuration, you will be redirected to the correct IdP Configuration document that you created.

Save and close you Internet site document and restart the HTTP Task on your Domino Server.

Open up your browser and surf to the URL of your application. In this case it is https://calendar.groupwave.be You will see that you get redirected to Office 365 and if you were already logged in, than you will be redirected to Domino.