



HCL Domino SAML

Keycloak

Version 1.0

Objectif.....	4
Présentation de Keycloak.....	5
Architecture cible.....	6
Load balancer.....	6
SSL.....	6
Sites Internet.....	6
SSO.....	6
LDAP.....	7
IPv6.....	7
Sécurité LDAP Domino.....	7
LCA étendue (xACL).....	7
Document de configuration * - Tous les serveurs.....	7
Configuration LDAP.....	7
Document serveur.....	7
Sites Internet.....	8
Firewall.....	8
Keycloak.....	9
Installation.....	9
keycloak.service.....	9
Debug.....	9
Configuration de base.....	9
Définir le nom d'hôte.....	9
Définir le certificat SSL à utiliser.....	9
Définir la version SSL.....	10
Définir le port du serveur Keycloak.....	10
Configuration LDAPs.....	10
Création du trustore.....	10
Configuration du trustore.....	11
Validation de l'installation.....	11
Fédération.....	14
Configuration LDAP sous Keycloak.....	14
Section Options générales.....	15
Section connexion et authentification.....	15
Section recherche LDAP.....	16
Section Synchronisation.....	17
Section Paramètres avancés.....	18
Mappeurs.....	18
Validation.....	19
Domaine Keycloak pour Domino.....	21

Création.....	21
Configuration.....	22
Export du fichier metadata.....	22
Domino : configuration SAML.....	24
Catalogue IdP.....	24
Intégration du fichier metadata.....	25
Fichier ID du serveur Domino.....	26
Export du fichier Service Provider.....	26
Vérification Domino.....	28
Keycloak: relation de confiance avec Domino.....	30
Onglet Settings.....	31
Onglet Keys.....	32
Onglet Client scopes.....	33
Onglet Advanced.....	35
Test Domino Web.....	38
Site Internet.....	38
Test de la configuration.....	38
Fédération Notes ou Web.....	40
Prérequis.....	40
Url ?SAMLIDLogin.....	40
Coffre d'ID.....	41
Création de la configuration de fédération côté Domino.....	41
Création de la configuration de fédération côté keycloak.....	42
Onglet Settings.....	43
Onglet Keys.....	44
Onglet Client scopes.....	45
Mise à jour de la politique Domino.....	46
Valider la fédération Web avec Verse.....	46
Valider la fédération Notes.....	47
Troubleshoot.....	49
Invalid Request.....	49
Debug Keycloak.....	49

Objectif

Configurer Domino pour utiliser Keycloak en tant qu'IdP (Identity Provider) pour SAML.

Présentation de Keycloak

Keycloak est un outil de gestion des identités et d'authentification. Son éditeur est Red-Hat et est un logiciel open-source.

Ce logiciel est utilisé pour le SSO (Single Sign-On) et permet la délégation d'identification. Il implémente plusieurs standards dont SAML (Security assertion markup language, basé sur XML) et OIDC (OpenIDConnect) tous deux utilisés par HCL Domino V12 pour SAML (Notes et Web)- et V14 pour SAML (Web et notes) et OIDC (Web uniquement pour ce dernier).

Architecture cible

L'architecture de ce document est simple n'utilise pas de load balancer, mais il est fortement recommandé d'utiliser un load balancer ou keycloak sur Docker.

Le terme anglais trustore a été utilisé dans ce document en lieu et place du terme français trusteur.

Load balancer

Si vous souhaitez utiliser un load balancer, il faut prévoir :

- Un FQDN (Fully Qualified Domain Name) pour LDAP
- Un FQDN pour les accès Web à Domino (si vous utilisez un cluster Domino pour la messagerie)
- Si le serveur de coffre n'est pas le serveur Web ou de messagerie Domino, prévoir un FQDN pour le ou les serveurs de coffre
- Planifier le SSL Off-loading : faire que le load balancer gère le certificat SSL des accès Web Domino.

SSL

En présence ou non d'un load balancer il est recommandé d'utiliser SSL pour tous les échanges :

- LDAP
- Accès Web (port 443)

Les recommandations HCL sont d'utiliser un certificat public officiel, cela simplifie les certificats de confiance (LDAP, Web, etc...).

L'utilisation de CertMgr de Domino (à partir de la version 12) est la solution la plus simple.

Cette documentation utilise les certificats Let's Encrypt (gratuits).

Sites Internet

Il est recommandé d'utiliser les sites Internet sous Domino pour simplifier la mise en œuvre.

SSO

La configuration Domino non SAML doit être fonctionnelle au niveau SSO. Ne pas activer SAML tant que la configuration SSO Domino de base (multi-serveurs) n'est pas opérationnelle.

LDAP

Avant de déployer Keycloak il est impératif d'avoir un serveur LDAP (Active Directory, Domino) fonctionnel.

La présente documentation utilise un annuaire LDAP Domino avec SSL (LDAPS).

Il est nécessaire de valider le bon fonctionnement LDAP avant de déployer keycloak.

IPv6

Si vous comptez utiliser Keycloak en IPV4, assurez-vous que le serveur LDAP est uniquement accessible en IPV4.

Si vous utilisez uniquement IPV6 avec vos serveurs Domino, il est nécessaire de désactiver IPV4 pour Keycloak via l'option :

```
JAVA_OPTS_APPEND="-Djava.net.preferIPv6Stack=true"  
(sous Linux export JAVA_OPTS_APPEND="-Djava.net.preferIPv4Stack=true")
```

Sécurité LDAP Domino

Si votre serveur LDAP est un serveur Domino, il faut le sécuriser

Sauf contraintes spécifiques, les serveurs LDAP en doivent être accessible que par Keycloak.

Pour un serveur LDAP HCL Domino, il faut configurer l'accès Anonyme au minimum afin de prévenir toute mauvaise configuration

LCA étendue (xACL)

L'utilisation d'une LCA étendue permet de mieux contrôler les accès Anonymes et les droits attribués à ce dernier.

Document de configuration * - Tous les serveurs

Si vous n'utilisez pas la LCA étendue (xACL), vous pouvez configurer les attributs accessible en mode Anonyme. Choisissez un attribut inexistant ou non essentiel.

Configuration LDAP

Document serveur

Si vous n'utilisez pas les sites Internet, configurez LDAP via l'onglet Ports > Ports Internet > Annuaire

Server: antalya/DTM antalya.dtm-france.com

Basic Security Ports... Server Tasks... Internet Protocols... Miscellaneous Ti

Notes Network Ports Internet Ports... Proxies

TLS settings

TLS key file name: keyfile.kyr

Accept TLS site certificates: Yes No

Accept expired TLS certificates: Yes No

TLS ciphers: ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030] DHE_RSA_WITH_AES_256_GCM_SHA384 [9F] ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F] DHE_RSA_WITH_AES_128_GCM_SHA256 [9E]

Modify

Web Directory Mail DIOP Remote Debug Manager Server Controller

Directory (LDAP)

TCP/IP port number: 389

TCP/IP port status: Redirect to TLS

Enforce server access settings: Yes

Authentication options:

Name & password: Yes

Anonymous: No

TLS port number: 636

TLS port status: Enabled

Authentication options:

Client certificate: No

Name & password: Yes

Anonymous: No

Sites Internet

Si vous utilisez les sites Internet, éditez les sites Internet de type LDAP.
Désactivez les accès anonyme LDAP via les sites Internet de type LDAP.

The screenshot shows the 'LDAP Site DTMLdap' configuration page with the 'Security' tab selected. The 'TCP Authentication' section has 'Anonymous' set to 'No' and 'Name & password' set to 'Yes'. The 'TLS Authentication' section has 'Anonymous' set to 'No', 'Name & password' set to 'Yes', 'Client certificate' set to 'No', and 'Bearer token (JWT)' set to 'No'. The 'TLS Options' section has 'Key file name' set to '*.dtm-france.com', 'Accept TLS site certificates' set to 'Yes', 'Accept expired TLS certificates' set to 'Yes', 'Check for CRLs' set to 'No', 'Trust expired CRLs' set to 'Yes', and 'Allow CRL search to fail' set to 'Yes'.

LDAP Site DTMLdap	
Basics Security Comments Administration	
TCP Authentication	
Anonymous:	☐ Yes ☒ No
Name & password:	☒ Yes ☐ No
TLS Authentication	
Anonymous:	☐ Yes ☒ No
Name & password:	☒ Yes ☐ No
Client certificate:	☐ Yes ☒ No
Bearer token (JWT):	☐ Yes ☒ No
TLS Options	
Key file name:	*.dtm-france.com
Accept TLS site certificates:	☒ Yes ☐ No
Accept expired TLS certificates:	☒ Yes ☐ No
Check for CRLs:	☐ Yes ☒ No
Trust expired CRLs:	☒ Yes ☐ No
Allow CRL search to fail:	☒ Yes ☐ No

Firewall

Assurez-vous que les firewalls laissent passer les flux pour les ports TCP 389 (LDAP) et 636 (LDAPS) entre le serveur Keycloak et les serveurs LDAP.

Keycloak

Installation

L'installation de Keycloak est une installation de base après son téléchargement.

keycloak.service

Pour Linux, il est nécessaire de créer un fichier keycloak.service dans le répertoire etc/systemd/system.

```
[Unit]
Description=keycloak service
After=network.service

[Service]
ExecStart=/opt/keycloak/bin/kc.sh start
PIDFile=/var/run/keycloak.pid

[Install]
WantedBy=multi-user.target
```

Debug

Pour analyser en mode debug, le plus simple est de lancer keycloak en mode TRACE avec journalisation dans un fichier de log:

```
cd /opt/keycloak
./kc.sh|.bat start --log="console,file" --log-level=ERROR -
-log-file=/var/log/keycloak.log
```

Configuration de base

Editez le fichier de configuration conf/keycloak.conf

Définir le nom d'hôte

Renseignez le nom d'hôte du serveur Keycloak

Hostname for the Keycloak server.

hostname=<**FQDN du serveur keycloak (ou du Load Balancer pour Keycloak)**>

Exemple pour ce document:

Hostname for the Keycloak server.

hostname=**adelaide.dtm-france.com**

Définir le certificat SSL à utiliser

HTTP

The file path to a server certificate or certificate chain in PEM format.

https-certificate-file=\${**kc.home.dir**}conf/server.crt.pem

Exemple:

https-certificate-file=/etc/letsencrypt/live/adelaide.dtm-france.com-0001/fullchain.pem

Définir la version SSL

TLS version

https-protocols=**TLSv1.2**

Définir le port du serveur Keycloak

Par défaut le port du serveur Keycloak est le port 443

port

https-port=**443**

Configuration LDAPs

Créez un fichier de type Trustore pour le serveur LDAP

Création du trustore

```
openssl s_client -connect <FQDN du serveur LDAP>:636
```

Exemple de résultat

```
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = antalya.dtm-france.com
verify return:1
---
Certificate chain
0 s:CN = antalya.dtm-france.com
  i:C = US, O = Let's Encrypt, CN = R3
1 s:C = US, O = Let's Encrypt, CN = R3
  i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
2 s:C = US, O = Internet Security Research Group, CN = ISRG Root X1
  i:O = Digital Signature Trust Co., CN = DST Root CA X3
3 s:O = Digital Signature Trust Co., CN = DST Root CA X3
  i:O = Digital Signature Trust Co., CN = DST Root CA X3
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIE nDCCA4SgAwIBAgISA7g045YiX4Fychgd8vvPq+u6MA0GCSqGSIb3DQEBCwUA
MDIx CzAJBgNVBAYTAiVTMR YwFAYDVQQKEw1MZXNQncyBFbmNyeXB0MQswCQY-
DVQQD
EwJSMzAeFw0yMzEwMTIxNDE3MTBaFw0yNDExMTAxNDE3MDlaMCEwH2AdBgN-
VBAMT
FmFudGFseWEuZHRtLWZyYW5jZS5jb20wdjAQBgcqhkiOPQIBBgUrgQQAIGNiAASv
HPhXsvsUKXdzsSQcVMhVppVDG1vtNBP5HKhjn0QCY5jP1SGV2OvJenVsmCTbfnOa
TnbMt8zCSOgsXaYlOa/jl8hlsef4mDYDr6ADeU4VrsssY4AnyT98/H5j+NqGtyCj
ggJpMIICZTAOBgNVHQ8BAf8EBAMCB4AwHQYDVR0lBBYwFAYIKwYB-
BQUHAAwEGCCsG
AQUFBwMCMAAwGA1UdEwEB/wQCMAAwHQYDVR0lOBBYEFMNhSCde-
fir0634a0ny3Bz2d
QgxMMB8GA1UdIwQYMBaAFBQusxe3WFbLrlAJQOYfr52LFMLGMFUGCCsGAQUFB-
```



```
wEB
BEkwRzAhBggrBgEFBQcwAYYVaHR0cDovL3IzLm8ubGVuY3Iub3JnMCIGCCsGAQUF
BzACHhZodHRwOi8vcjMuaS5sZW5jci5vcmcvMHEGA1UdEQRqMGiCFmFudGFseWEu
ZHRtLWZyYW5jZS5jb22CDmR0bS1mcmFuY2UuY29tghFteC5kdG0tZnJhbmNlNmNv
bYIXdHJhdmVsZXIuZHRtLWZyYW5jZS5jb22CEND3dy5kdG0tZnJhbmNlNmNvbTAT
BgNVHSAEDDAKMAgGBmeBDAECAATCCAQUGCisGAQQB1nkCBAIEgfYEgf-
MA8QB3ADtT
d3U+LbmAToswWwb+QDtn2E/D9Me9AA0tcm/h+tQXAAABiyR2ilAAAAQDAEgwRgIh
ANQJBPK+VItNzzcHAK1mF47MirVZbyeuuitbA9y4m9ekAiEA8CcgXLYe38zPU2kb
Anvl8BQ5sU8/1dhHUBpKOxl2h8AdgB2/4g/Crb71VHCYcz1h7o0tKTNuyncaEIK
n+ZnTFo6dAAAAYskdoqIAAAEAwBHMEUCIBXAq/WE//ral94u6SaiuLed8aR7L1Bb
LqfGocKotzVPAiEA6fy4OpQJsls+uxlxG5X6agPiYUgFMkCPJ1llA9twcR4wDQYJ
KoZlhcNAQELBQADggEBAJeA7r+EN6Cw98ntvI3264TPU2ITNhkViAayiDYCquwI
9q7VMJoP0BrmqvjsrcBztK6OpW8FS3XXpaUrPXNYMd8+AfqYh7yX22B8GX01Df5T
cSU7KxeKucMzemDvWopl5qrdCJcqBiKFWmhFq9cx0dv9IDUkE4Pq0XxtLwPttnvq
BDzB/idBLQUjayjpWwNySo+2OcsL3HsSl33b+nWzp3P4qv/KtsMbtflukHozxDfZ
Km/GlipNkuOb3klsNkgIz+Ea2P3lJ8h3fHZ3Dk3p+V1lsZERo950Adxy2BbvUDkr
OKraUTFRXvcbhURRW63HwdpbP1iZ8WDPfuzKSruLhs8=
-----END CERTIFICATE-----
```

Copiez le Server certificate commençant par -----BEGIN CERTIFICATE----- et se terminant par --- --END CERTIFICATE----- dans un fichier ldaps.cer :

Puis générez le fichier jks en notant le mot de passe demandé à la création du keystore.jks.

```
keytool -import -trustcacerts -alias <FQDN su serveur LDAP> -file ldaps.cer -
keystore keystore.jks
```

Copiez le fichier keystore.jks dans le dossier 'conf' de keycloak

Vérifiez le fichier keystore.jks et confirmez la présence du certificat :

```
keytool -list -keystore keystore.jks
```

Configuration du trustore

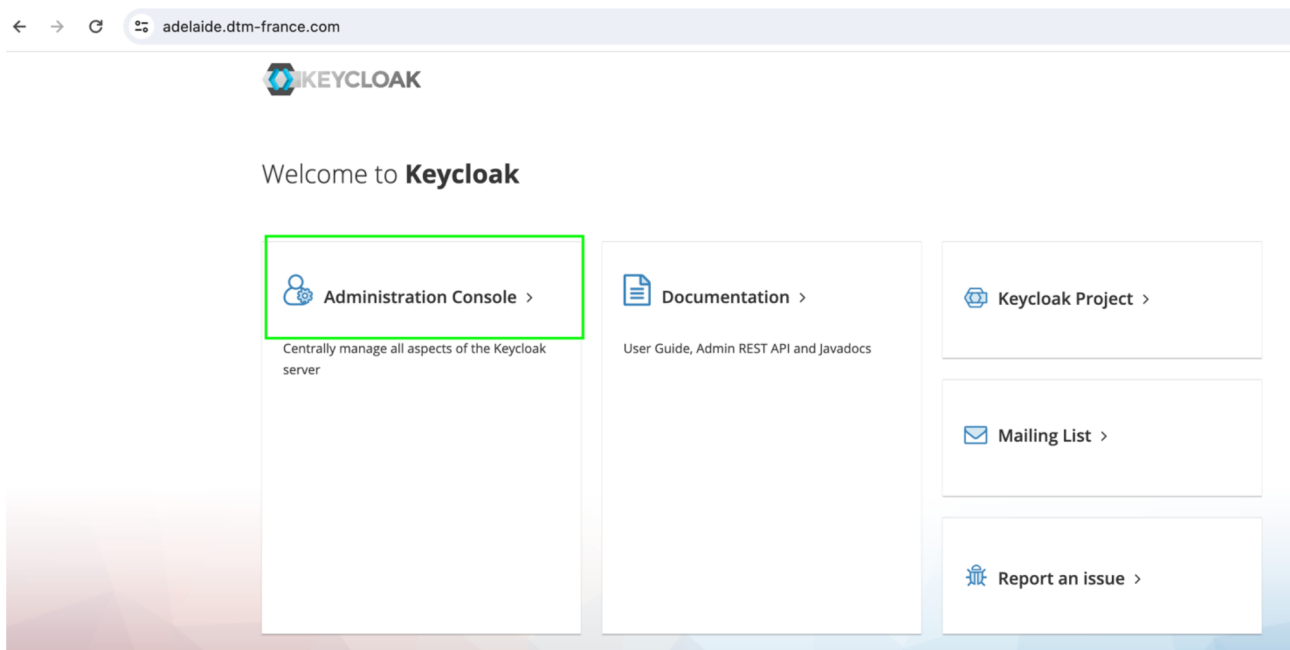
Modifier le fichier de configuration conf/keycloak.conf pour ajouter les lignes concernant LDAPs

```
# LDAPs
```

```
spi-truststore-file-file=/opt/keycloak/conf/keystore.jks
spi-truststore-file-password=<Mot de passe du fichier jks>
spi-truststore-file-hostname-verification-policy=ANY
```

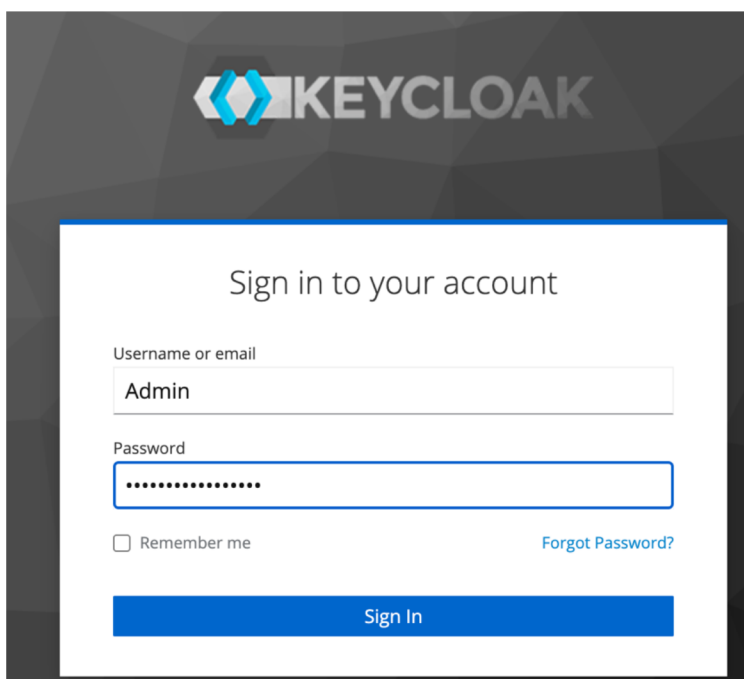
Validation de l'installation

Connectez-vous à Keycloak avec un navigateur en https.



Cliquez sur 'Administration Console'

Une fois le compte admin créé, authentifiez-vous avec ce compte 'Admin'. Par sécurité utilisez le compte local et non LDAP.



Après validation du compte et mot de passe vous êtes dirigé sur le domaine (Realm) Master.

KEYCLOAK

admin

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

master realm

Server info

Provider info

Server info

Version

21.1.0

Product

Default

Memory

Total memory

512 MB

Free memory

437 MB

Used memory

74 MB

Profile

Enabled features ⓘ

Disabled features ⓘ

ACCOUNT3 Experimental

ADMIN_FINE_GRAINED_AUTHZ Preview

CLIENT_SECRET_ROTATION Preview

DECLARATIVE_USER_PROFILE Preview

DOCKER Supported

DYNAMIC_SCOPES Experimental

FIPS Supported

MAP_STORAGE Experimental

OPENSIFT_INTEGRATION Preview

RECOVERY_CODES Preview

SCRIPTS Preview

TOKEN_EXCHANGE Preview

UPDATE_EMAIL Preview

DTM

Documentation

17/12/2023

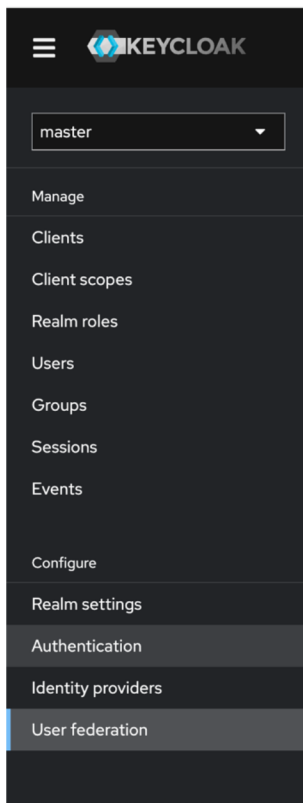
Fédération

La fédération permet de définir les annuaires LDAP utilisé par Keycloak pour l'authentification des utilisateurs.

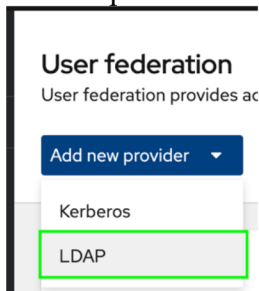
Ce document utilise un annuaire LDAP de type Domino.

Configuration LDAP sous Keycloak

Sur la page d'accueil, cliquez sur le lien 'User Federation'



Puis cliquez sur 'Add new provider' > LDAP



Section Options générales

[User federation](#) > Add LDAP provider

Add LDAP provider

General options

UI display name * ?

ldap

Vendor * ?

Active Directory

Active Directory

Red Hat Directory Server

Tivoli

Novell eDirectory

Other

Connection and authentication

Connection URL * ?

Dans le champ 'Vendor', sélectionner l'option 'Other'.

Section connexion et authentification

Connection and authentication settings

Connection URL * ?

ldaps://antalya.dtm-france.com:636

Enable StartTLS ?



Off

Use Truststore SPI ?

Only for ldaps

Connection pooling ?



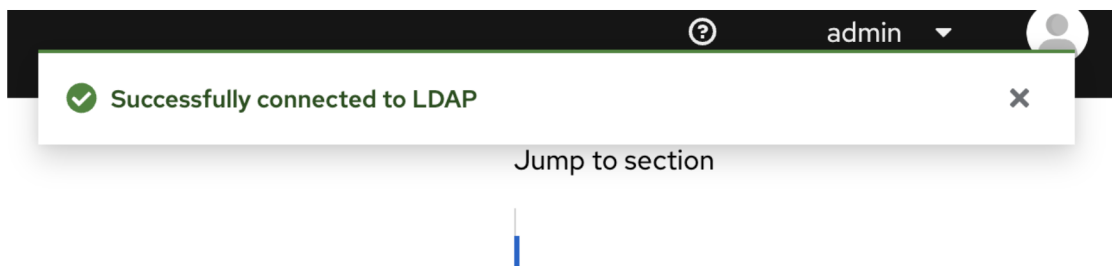
Off

Connection timeout



Test connection

Renseignez l'url ldaps au format : **ldaps://<FQDN Ldap>:636**
Définir '**Only for ldaps**' pour le trustore.

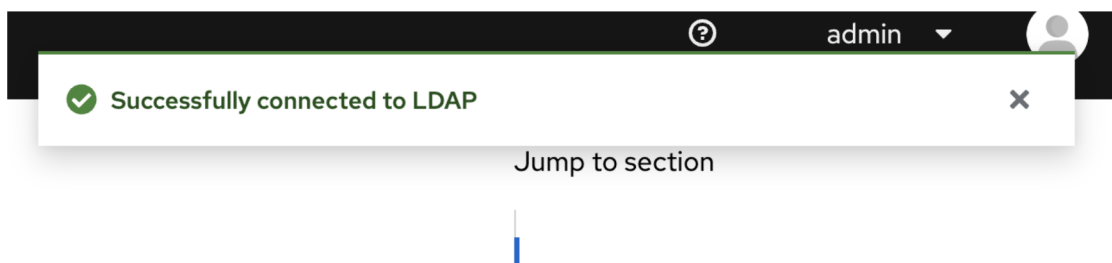


Une fois ces deux champs renseignés, cliquez sur 'Test connection' et validez qu'il n'y a aucune erreur.

Bind type * ?	simple
Bind DN * ?	cn=<compte Notes ldap lecteur>,o=<organisation Domino>
Bind credentials * ?	..

[Test authentication](#)

Renseignez les trois champs, pour le bind DN, utilisez le compte dédié LDAP de votre annuaire Domino. (Les accès en lecture sont suffisants).



Puis testez l'authentification via le bouton 'Test authentication'.

Section recherche LDAP

LDAP searching and updating

Edit mode * ?	READ_ONLY ▼
Users DN * ?	o=<Votre organisation DOMINO pour les USERS>
Username LDAP attribute * ?	uid
RDN LDAP attribute * ?	uid
UUID LDAP attribute * ?	uid
User object classes * ?	inetOrgPerson, organizationalPerson
User LDAP filter ?	
Search scope ?	Subtree ▼

Définir le mode d'édition en 'READONLY'

Définir l'organisation Domino des utilisateurs : **o=dtm** pour ce document

Section Synchronisation

Synchronization settings

Import users ?	☒ On
Sync Registrations ?	☒ On
Batch size ?	
Periodic full sync ?	☐ Off
Periodic changed users sync ?	☐ Off

Activer l'import des utilisateurs et la synchronisation.
Il est possible de planifier une synchronisation périodique.

Advanced settings

Enable the LDAPv3 password modify extended operation  Off 

Validate password policy  Off 

Trust email  On 

Activez l’option ‘Trust email’ afin de considérer les emails comme valides.

Mappeurs

LDAP

Settings

Mappers

 Search for mapper



Add mapper

Name

Type

email

user-attribute-ldap-mapper

first name

user-attribute-ldap-mapper

last name

user-attribute-ldap-mapper

username

user-attribute-ldap-mapper

Ne conservez que ces quatre attributs et modifiez l'attribut suivant :

- Last name => sn

[User federation](#) > [Settings](#) > Mapper details

last name

ID

a2d3eb15-7e34-41ee-bf83-ee197abacc6c

Name * ?

last name

Mapper type * ?

user-attribute-ldap-mapper

User Model Attribute

lastName



LDAP Attribute ?

sn

Pour tous les attributs vérifiez les options et adaptez les en fonction de votre site et contraintes de renommage etc....

Read Only ?



On

Always Read Value



On

From LDAP ?

Is Mandatory In LDAP



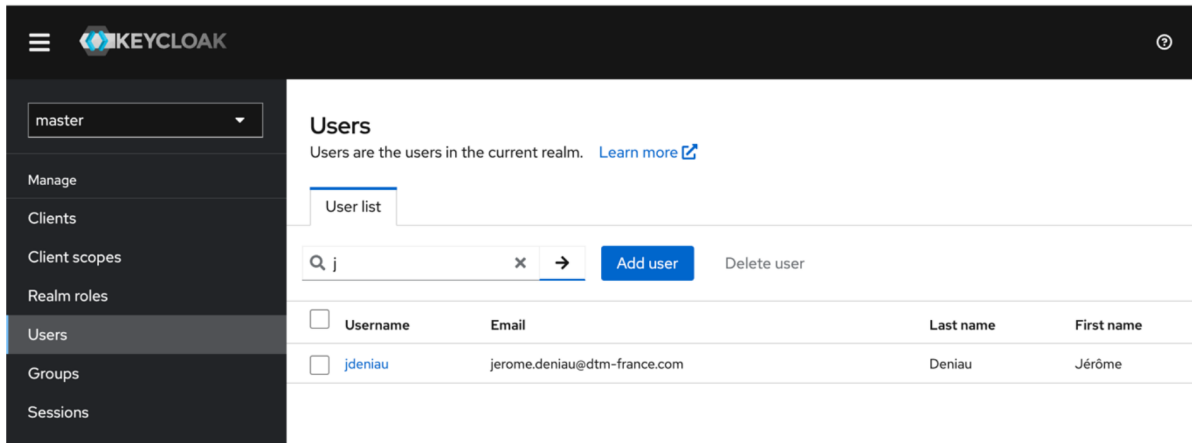
On



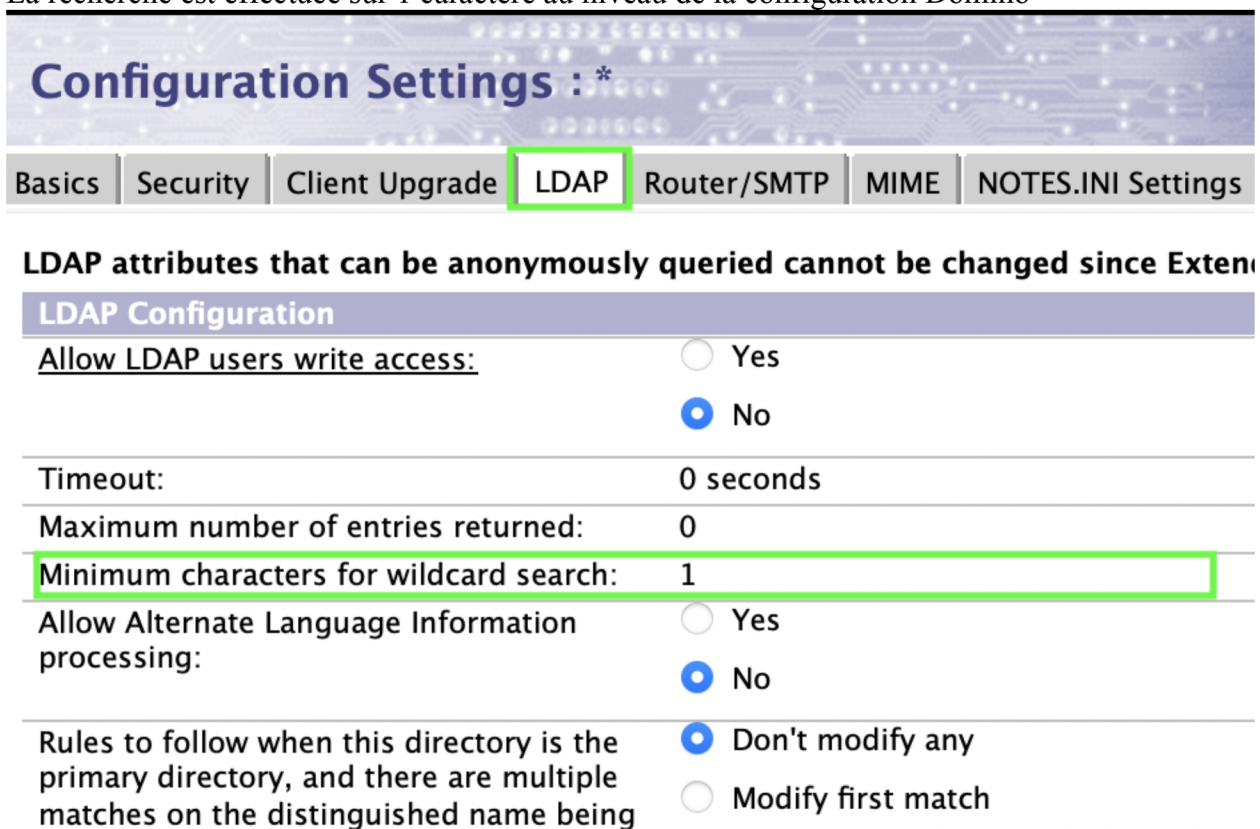
Validation

Pour vous assurer que votre annuaire est bien en ligne et opérationnel, vous pouvez effectuer une

recherche de compte LDAP à partir de Keycloak.



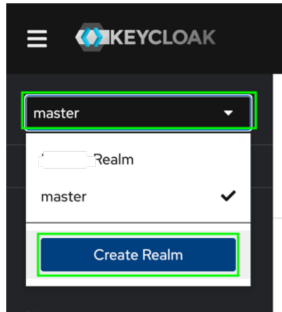
La recherche est effectuée sur 1 caractère au niveau de la configuration Domino



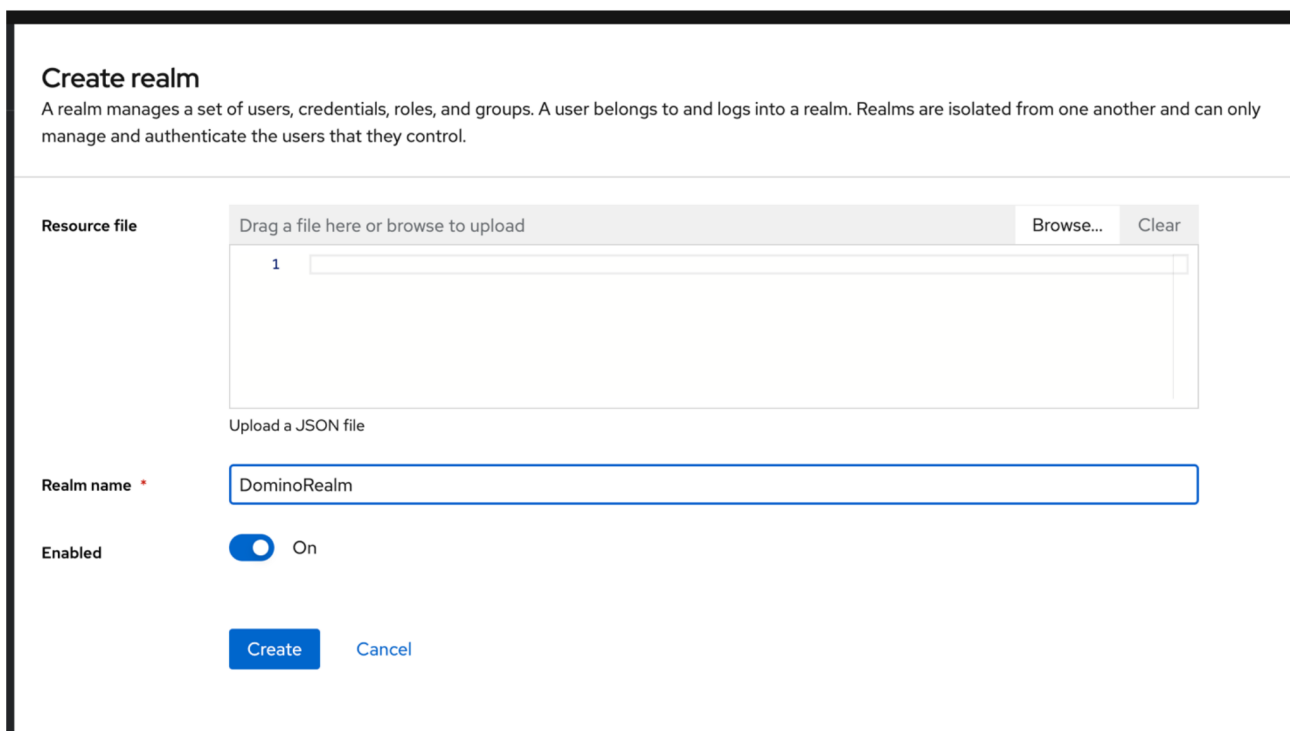
Domaine Keycloak pour Domino

Il est recommandé de créer un domaine (Realm) sous Keycloak afin de gérer les assertions SAML Domino.

Création



Pour créer le domaine pour Domino, cliquez sur Master > Create Realm.

A screenshot of the 'Create realm' form in Keycloak. The form has a title 'Create realm' and a description: 'A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.' The form contains a 'Resource file' section with a text input field containing '1' and a 'Browse...' button. Below this is a section for 'Upload a JSON file'. The 'Realm name' field is labeled 'DominoRealm'. The 'Enabled' toggle is turned 'On'. At the bottom are 'Create' and 'Cancel' buttons.

Le nom du domaine exemple est 'DominoRealm', pour désigner un domaine pour Domino, ce nom est libre (pas d'espace ni de caractères non supportés via html). Il est recommandé d'utiliser un nom court et parlant pour l'administrateur. Attention ce nom est utilisé par les urls Domino pour les authentications.

Configuration

Keycloak configuration page for the DominoRealm. The 'General' tab is selected. The 'HTML Display name' is set to 'Domino'. The 'Require SSL' is set to 'All requests'. The 'User-managed access' is set to 'Off'. The 'Endpoints' section shows links for 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'.

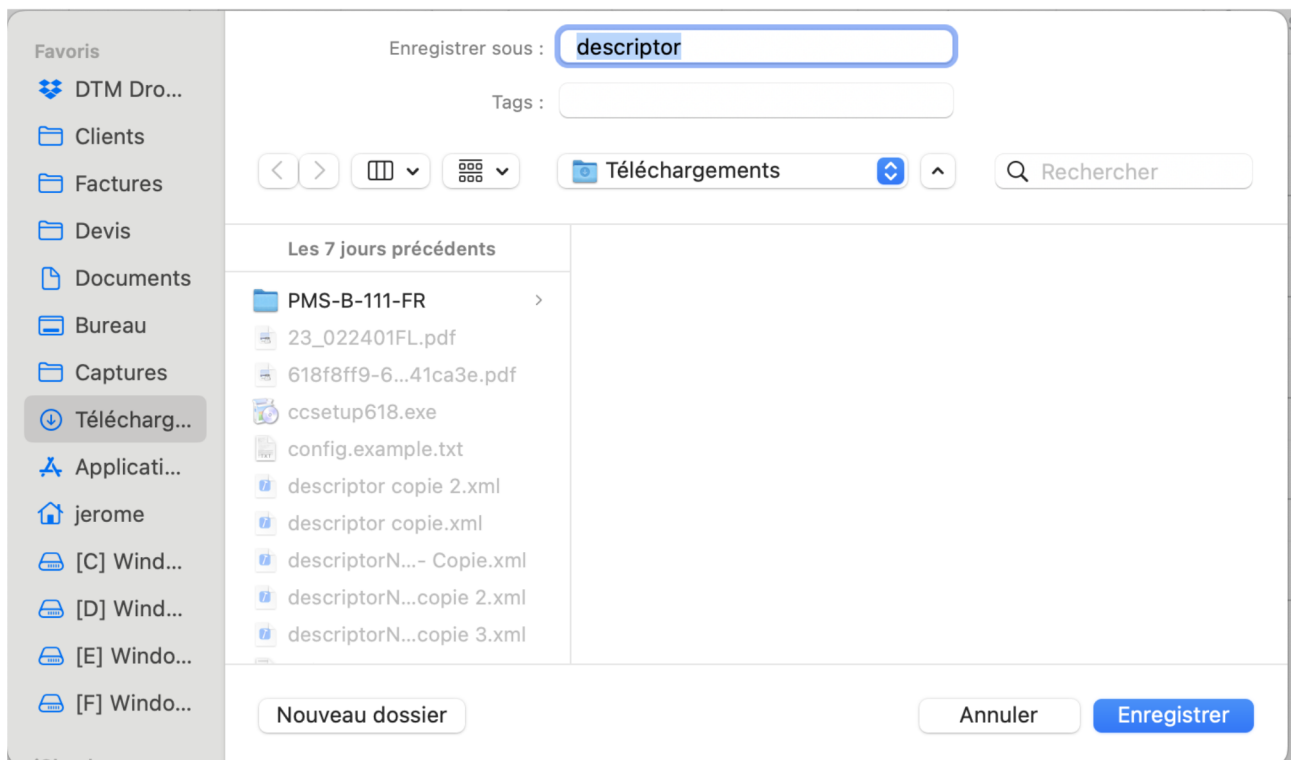
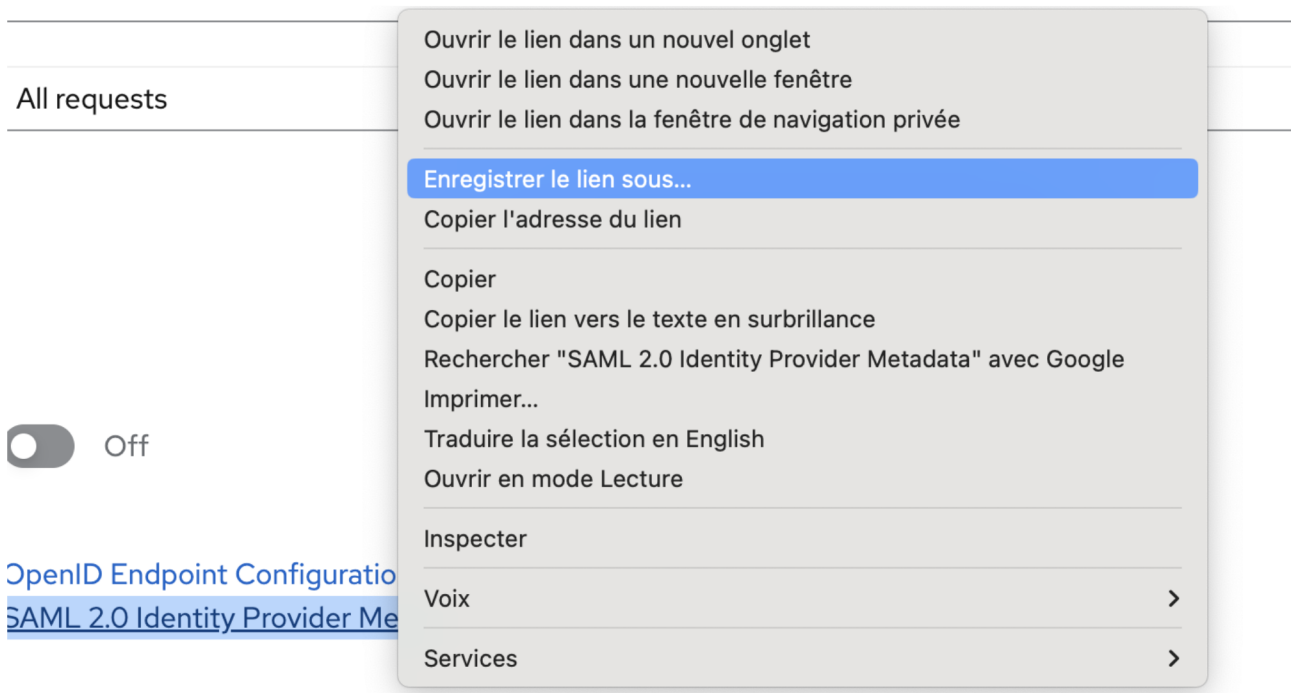
Définissez les champs d’affichage et HTML pour qu’ils soient parlants, ici nous avons utilisé ‘Domino’ pour tous les produits HCL, pour Traveler, Sametime, NomadWeb, Nomad, leap, etc...

Export du fichier metadata

Sous Keycloak, exporter le fichier metadata Descriptor.xml.

Keycloak configuration page for the DominoRealm. The 'General' tab is selected. The 'HTML Display name' is set to 'Domino'. The 'Require SSL' is set to 'All requests'. The 'User-managed access' is set to 'Off'. The 'Endpoints' section shows links for 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. The 'SAML 2.0 Identity Provider Metadata' link is highlighted with a green box.

Effectuez un click-droit sur le lien « SAML 2.0 Identity provider Metadata »



Effectuez plusieurs copies de ce fichier via votre système d'exploitation, car lors de l'import de ce fichier dans Domino, le client Notes supprime le fichier sur disque.

Domino : configuration SAML

Catalogue IdP

Il est nécessaire de créer un fichier idpcat.nsf à partir du modèle idpcat.ntf de Domino

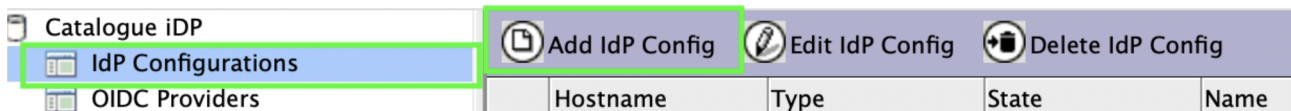
The screenshot shows two overlapping dialog boxes in the Domino configuration interface. The top dialog, titled "Specify New Application Name and Location", has fields for "Server" (antalya/DTM), "Title" (Catalogue iDp), and "File name" (idpcat). It includes buttons for "OK", "Cancel", "Encryption...", "Create full text index for searching" (unchecked), and "Advanced...". The bottom dialog, titled "Specify Template for New Application", has a "Server" field (antalya/DTM) and a "Template" list. The list includes "HCL iNotes Extension Forms (11)", "HCL iNotes Redirect", "HCL Notes/Domino Fault Reports", "HCL Notes/Domino Smart Upgrade Trackin", "ID Vault (14)", and "IdP Catalog (14.0)". The "IdP Catalog (14.0)" template is selected. Below the template list is a "File name" field (idpcat.ntf) and buttons for "About...", "Show advanced templates" (checked), and "Inherit future design changes" (checked).

Le nom du fichier doit être idpcat.nsf, quel que soit le système d'exploitation qui héberge le serveur Domino, prenez l'habitude de créer le fichier idpcat.nsf en minuscule.
Bien valider que le modèle utilisé provient du serveur et est 'idpcat.ntf'.

Si la base idpcat.nsf existe déjà, vérifier que sa structure est bien à jour avec la version du serveur Domino. Mettre à jour la structure si la base a été créée dans une version antérieure avec un remplacement de structure Notes.

Intégration du fichier metadata

Une fois la base idpcat créée, il faut créer un document et importer. Le fichier metadata.



Sélectionnez la vue 'IdP Configurations' puis cliquer sur le bouton d'action 'Add IdP Config'.

IdP Configuration

Basics | Client Settings | Certificate Management | Advanced | Administration

Import XML file

Host names or addresses mapped to this site: antalya.dtm-france.com

Protocol version: SAML 2.0

State: Enabled

Federation product: AuthnRequest SAML 2.0 compatible

Service provider ID: https://antalya.dtm-france.com

Artifact resolution service URL:

Single sign-on service URL:

IdP name (for your reference):

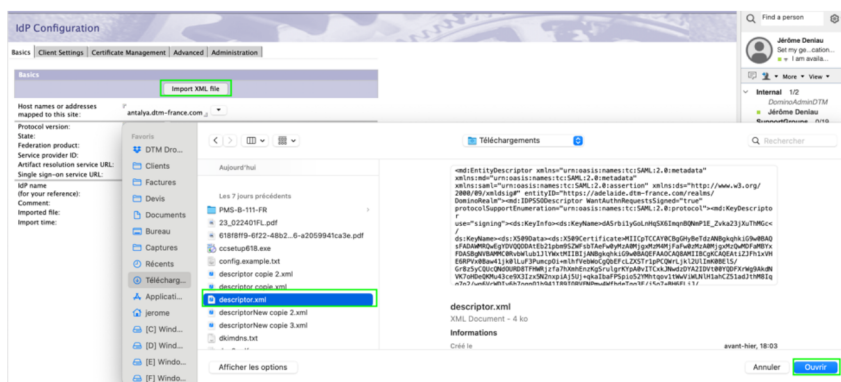
Comment:

Imported file:

Import time:

Saisissez manuellement le FQDN de votre serveur Domino (la sélection par liste n'est pas encore configurée au niveau de l'annuaire Domino : aucun document serveur ou site Internet n'est encore configuré pour utiliser SAML, d'où la saisie manuelle du nom d'hôte).

Le champ 'Service Provider ID' est important, l'url saisie est l'url de requête qui sera utilisée par Keycloak pour identifier le serveur Domino (dans le cas d'un load balancer c'est bien l'url du load balancer qui doit être saisie).



Une fois ces deux champs renseignés on peut importer le fichier XML metadata fourni par Keycloak.

Save & Close Cancel

IdP Configuration

Basics Client Settings Certificate Management Advanced Administration

Basics

Import XML file

Host names or addresses mapped to this site: antalya.dtm-france.com

Protocol version: SAML 2.0

State: Enabled

Federation product: AuthnRequest SAML 2.0 compatible

Service provider ID: https://antalya.dtm-france.com

Artifact resolution service URL: https://adelaide.dtm-france.com/realms/DominoRealm/protocol/saml/resolve

Single sign-on service URL: https://adelaide.dtm-france.com/realms/DominoRealm/protocol/saml

IdP name (for your reference):

Comment:

Imported file: - descriptor.xml

Import time: 17/12/2023 21:16

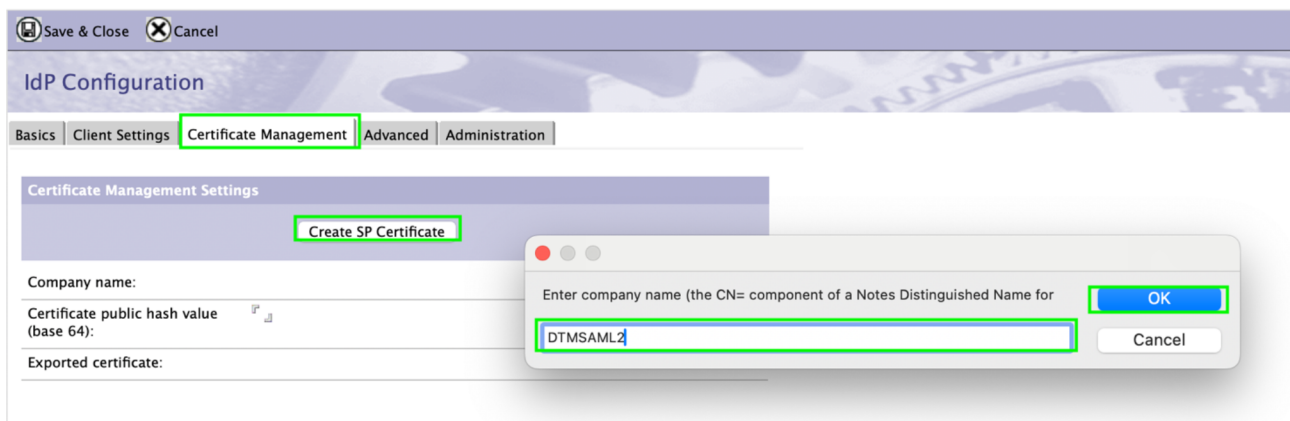
Les champs sont automatiquement renseignés et le fichier descriptor.xml est intégré au document. Cliquez sur 'Save and Close' pour enregistrer et fermer le document.

Fichier ID du serveur Domino

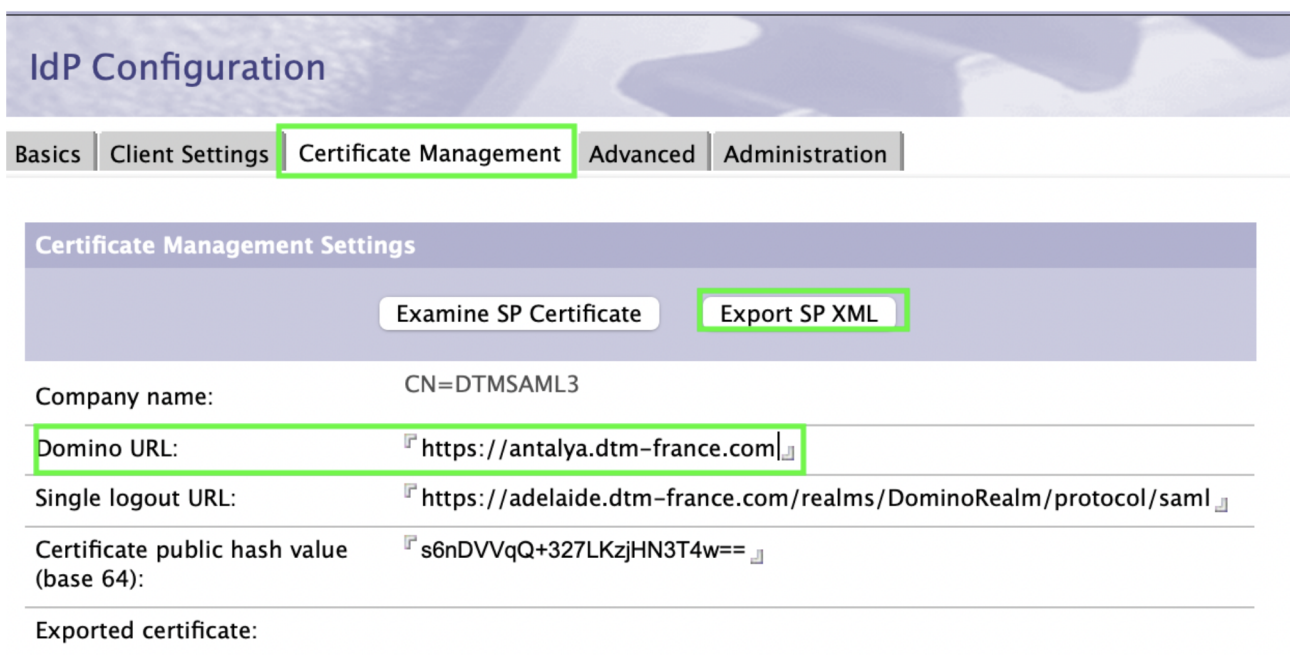
Effectuez une sauvegarde du fichier ID du serveur Domino. Il est possible de créer une clé SAML mais il est impossible de supprimer cette clé du fichier de l'ID serveur. Si une erreur de configuration nécessite de recréer une clé on ne peut la mettre à jour que manuellement via la console Domino puis modifier par la suite le document manuellement. Afin d'éviter de telles étapes, effectuez une sauvegarde du fichier ID sur le serveur via une copie du système d'exploitation.

Export du fichier Service Provider

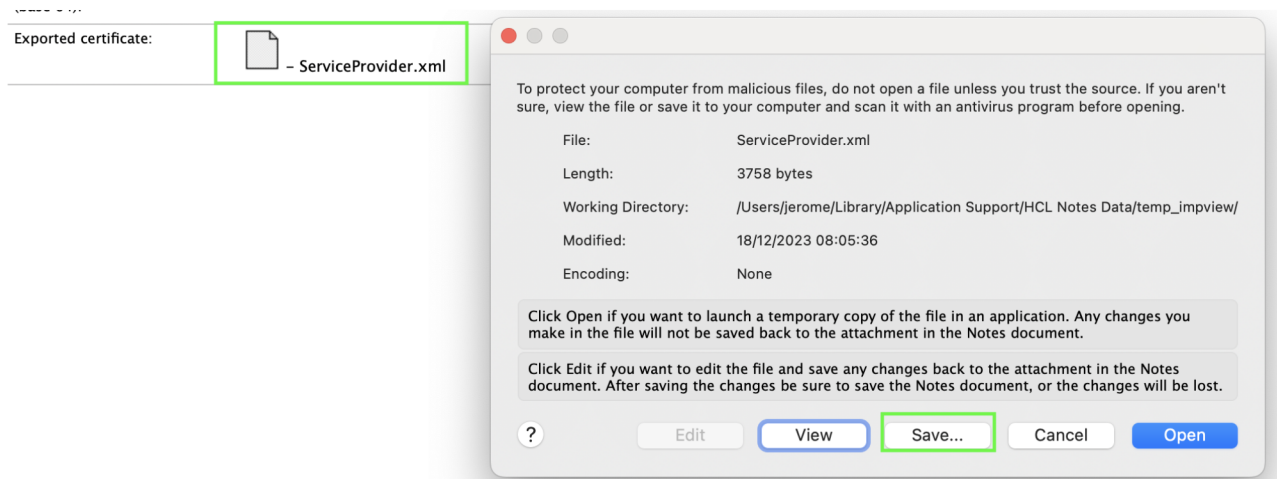
Réouvrir le document de la base idpcat.nsf créé précédemment.



Donner le nom de la clé et noter ce nom pour export dans le cas d'un cluster Domino.



Passez le document en mode édition puis accédez à l'onglet 'Certificate Management'.
Renseignez le champ 'Domino URL' (url du load balancer ou d'accès au serveur Domino si vous n'avez pas de load balancer).
Puis cliquez sur Export SP XML afin de générer le fichier ServiceProvider.xml.



Une fois le document enregistré, une pièce jointe apparaît dans le document, double-cliquez sur le fichier XML puis choisissez l'option 'Save', enregistrez le fichier sous le nom ServiceProvider.xml.

Vérification Domino

Sur la console du serveur Domino exécuter la commande 'CERTMGMT SHOW ALL' afin de lister les certificats.

Exemple:

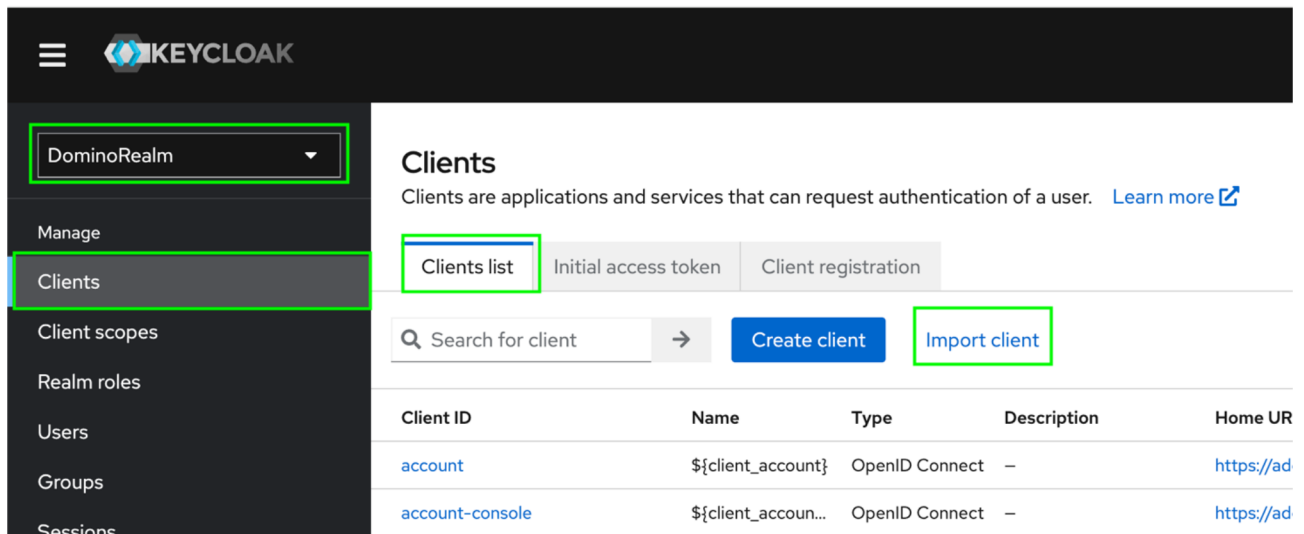
```
certmgmt show all
[1669412:000010-00007FB8CE9FF640] Certificate at index 0:
[1669412:000010-00007FB8CE9FF640] Subject Name: CN=DTMSAML
[1669412:000010-00007FB8CE9FF640] Issuer Name: CN=DTMSAML
[1669412:000010-00007FB8CE9FF640] Signature Time: 13-12-2023
17:58:31
[1669412:000010-00007FB8CE9FF640] Expiration Time: 30-11-2073
17:58:31
[1669412:000010-00007FB8CE9FF640] Key Strength: 2048
[1669412:000010-00007FB8CE9FF640] Public Key Hash: W+x0hYOJ1-
pL1C9I2igOZhg==
[1669412:000010-00007FB8CE9FF640] Key Usage: Digital Signature,
Data Encipherment
[1669412:000010-00007FB8CE9FF640] Certificate at index 1:
[1669412:000010-00007FB8CE9FF640] Subject Name: CN=DTMSAML2
[1669412:000010-00007FB8CE9FF640] Issuer Name: CN=DTMSAML2
[1669412:000010-00007FB8CE9FF640] Signature Time: 15-12-2023
11:13:07
[1669412:000010-00007FB8CE9FF640] Expiration Time: 02-12-2073
11:13:07
[1669412:000010-00007FB8CE9FF640] Key Strength: 2048
[1669412:000010-00007FB8CE9FF640] Public Key Hash: 7kIZQZFABeV1j-
ZLp5r00tg==
[1669412:000010-00007FB8CE9FF640] Key Usage: Digital Signature,
Data Encipherment
[1669412:000010-00007FB8CE9FF640] Certificate at index 2:
[1669412:000010-00007FB8CE9FF640] Subject Name: CN=DTMSAML3
[1669412:000010-00007FB8CE9FF640] Issuer Name: CN=DTMSAML3
[1669412:000010-00007FB8CE9FF640] Signature Time: 18-12-2023
```

08:04:23
[1669412:000010-00007FB8CE9FF640] Expiration Time: 05-12-2073
08:04:23
[1669412:000010-00007FB8CE9FF640] Key Strength: 2048
[1669412:000010-00007FB8CE9FF640] Public Key Hash:
s6nDVVqQ+327LKzjHN3T4w==
[1669412:000010-00007FB8CE9FF640] Key Usage: Digital Signature,
Data Encipherment
[1669412:000010-00007FB8CE9FF640] CERTMGMT command completed suc-
cessfully.

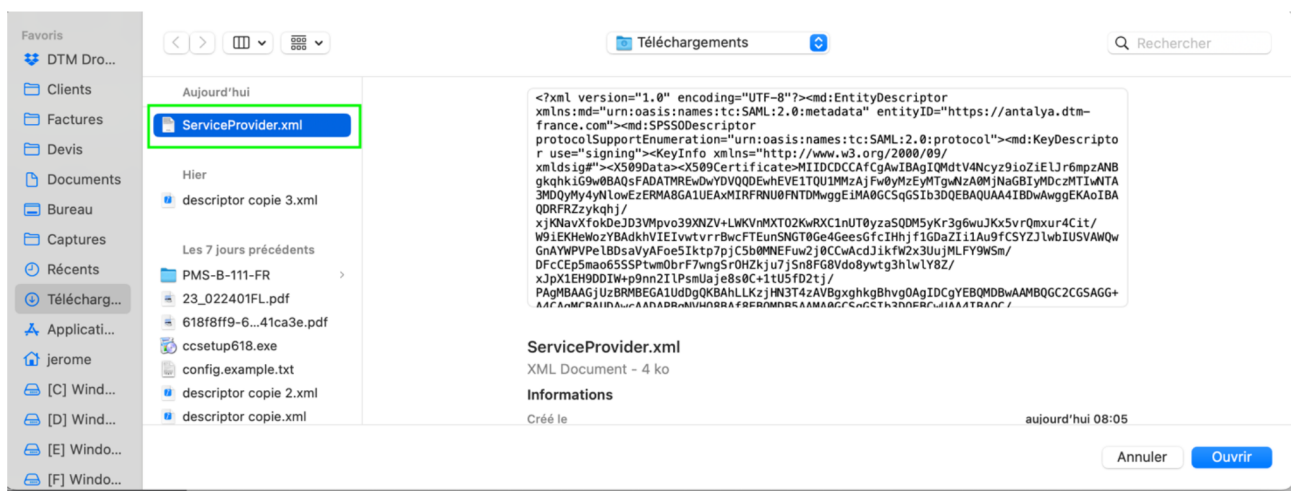
Keycloak: relation de confiance avec Domino

Désormais la configuration se fait côté Keycloak.

Il faut avoir accès au fichier ServiceProvider.xml généré à partir de Domino



Sélectionnez le domaine Keycloak DominoRealm > Clients puis dans la section 'Clients list' cliquez sur le lien 'Import client'.



Sélectionnez le fichier ServiceProvider.xml généré précédemment dans Domino via la base idp-cat.nsf.

Validez le contenu des différents écrans correspondants aux onglets

KEYCLOAK

admin

DominoRealm

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list Initial access token Client registration

Search for client → Create client Import client 1-9

Client ID	Name	Type	Description	Home URL
account	\${client_account}	OpenID Connect	—	https://adelaide.dtm-france.com/realms/DominoRealm/account/
account-console	\${client_accoun...}	OpenID Connect	—	https://adelaide.dtm-france.com/realms/DominoRealm/account/
admin-cli	\${client_admin-...}	OpenID Connect	—	—
broker	\${client_broker}	OpenID Connect	—	—
https://angstroem.dtm-france.com	—	SAML	—	—
https://antalya.dtm-france.com	Antalya	SAML	—	—
https://sametime.dtm-france.com	Sametime	SAML	Sametime connections	https://sametime.dtm-france.com
realm-management	\${client_real-...}	OpenID Connect	—	—
security-admin-console	\${client_securit...}	OpenID Connect	—	https://adelaide.dtm-france.com/admin/DominoRealm/console/

Cliquez sur le lien Client ID correspondant à votre site web.

Onglet Settings

Settings Keys Credentials Roles Client scopes Sessions Advanced

General Settings

Client ID * ?

Name ?

Description ?

Always display in UI ? ☒ On

Access settings

Root URL ?

Home URL ?

Valid redirect URIs ? + Add valid redirect URIs

Le champ 'Name' est optionnel et n'a aucun impact sur le SSO.
Activez l'option 'Always displayUI'.
Vérifier l'url de redirection en .../names.nsf?SAMLLogin

Onglet Keys

Clients > Client details

https://antalya.dtm-france.com SAML

 Enabled ⓘ

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Signing keys config

If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the client will sign their saml requests and responses. The signature will be validated.

Client signature required ⓘ  On

Certificate ⓘ

```
MIIDCCCAfCgAwIBAgIQMdtV4Ncyz9ioZiElJr6mpzANBgkqhkiG9w0BAQsFADATMREwDwYDVQQDEwhEVE1TQU1MMzAjFw0yMzEyMTgwNzA0MjNaGBlyMDczMTIwNTA3MDQyMy4yNlowEzERMA8GA1UEAxMIRFRNU0FNTDMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQRFRZzykqhj/xjKNavXfokDeJD3VMpvo39XNZV+LWKVnMXTO2KwRXC1nUT0yzaSQDM5yKr3g6wuJKx5vrQmxur4Cit/W9iEKHeWozYBAAdkhVIElvwtvrrBwcFTEunSNGT0Ge4GeesGfclHhjfIGDaZliiAu9fCSYZJlwbIUSVAWQwGnA
```

Encryption keys config

If you enable the "Encryption assertions" below, you must configure the encryption keys by generating or importing keys, and the SAML assertions will be encrypted with the client's public key using AES.

Encrypt assertions ⓘ  Off

Pour l'onglet Key, désactivez l'option 'Encryption keys config'

Onglet Client scopes

Clients > Client details

https://antalya.dtm-france.com SAML

En

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Setup

Evaluate

▼ Name

🔍 Search by name

→

Add client scope

Change type to ▼

⋮

☐ Assigned client scope	Assigned type	Description
☐ https://antalya.dtm-france.com-dedicated	none ▼	Dedicated scope and mappers for this c
☐ role_list	Default ▼	SAML role list

Cliquez sur le lien « [https ;//www.xxx.yyy-dedicated](#) » correspondant à votre URL.

Clients > Client details > Dedicated scopes

https://antalya.dtm-france.com

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

+

No mappers

If you want to add mappers, please click the button below to add some predefined mappers or to configure a new mapper.

Add predefined mapper

Configure a new mapper

Dans l'onglet 'Mappers' cliquez sur 'Add predefined mapper'.

Add predefined mappers



Choose any of the predefined mappings from this table



1 - 4 ▾



☐	Name	Description
☐	role list	Role names are stored in an attribute value. There is either one attribute with multiple attribute values,
☒	X500 email	Map a built in user property (email, firstName, lastName) to a SAML attribute type.
☒	X500 givenName	Map a built in user property (email, firstName, lastName) to a SAML attribute type.
☒	X500 surname	Map a built in user property (email, firstName, lastName) to a SAML attribute type.

1 - 4 ▾



Add

Cancel

Sélectionnez les 3 attributs X500.

[Clients](#) > [Client details](#) > Dedicated scopes

https://antalya.dtm-france.com

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope



Add mapper ▾

Name	Category
X500 givenName	AttributeStatement Mapper
X500 email	AttributeStatement Mapper
X500 surname	AttributeStatement Mapper

Cliquer sur 'Add mapper' pour ajouter l'attribut SAML NameID permettant de retourner l'attribut LDAP email à Domino (pour la fédération Notes)

User Attribute Mapper For NameID

ba0ce7be-d2ba-4c89-83ba-feaf0cd17129

Action ▾

Mapper type

User Attribute Mapper For NameID

Name * ?

NameID

Name ID Format ?

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified ▾

User Attribute ?

email

Save

Cancel

Cliquez sur ‘Save’

[Clients](#) > [Client details](#) > Dedicated scopes

https://antalya.dtm-france.com

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Q Search for mapper →

Add mapper ▾

1 - 4 ▾ < >

Name	Category	Type	Priority	
X500 givenName	AttributeStatement Mapper	User Property	0	⋮
X500 email	AttributeStatement Mapper	User Property	0	⋮
NameID	NameID Mapper	User Attribute Mapper For NameID	0	⋮
X500 surname	AttributeStatement Mapper	User Property	0	⋮

1 - 4 ▾ < >

Cliquez sur ‘Client details’ pour retourner à la page précédente

Onglet Advanced
Vérifiez les options

https://antalya.dtm-france.com SAML

Clients are applications and services that can request authentication of a user.

- Settings
- Keys
- Credentials
- Roles
- Client scopes
- Sessions
- Advanced

Fine Grain SAML Endpoint Configuration

This section to configure exact URLs for Assertion Consumer and Single Logout Service.

Logo URL ?

Policy URL ?

Terms of service URL ?

Assertion Consumer Service POST Binding URL ?

https://antalya.dtm-france.com/names.nsf?SAMLLogin

Assertion Consumer Service Redirect

**Logout Service SOAP
Binding URL** ?

**Logout Service
ARTIFACT Binding
URL** ?

Artifact Binding URL
?

https://antalya.dtm-france.com/names.nsf?SAMLLogin

**Artifact Resolution
Service** ?

Save

[Revert](#)

Test Domino Web

Une fois la configuration Keycloak terminée, il est possible de tester la mise en place de SAML, sans utiliser la fédération Domino Notes ou Web.

Site Internet

Configurer le site Internet concernant l'url définie en tant que « Service Provider ID » du document de la base idpcat.nsf. Dans notre cas <https://antalya.dtm-france.com>.

Web Site Web1

Basics | Configuration | **Domino Web Engine** | Security | Comments | Administration

HTTP Sessions

Session authentication: SAML ⌵ Open IdP Configuration

Web SSO Configuration: LtpaToken ⌵

Force login on TLS: Yes ⌵

SAML single server session expiration: 120 minutes

When overriding session authentication, generate session cookie: Yes ⌵

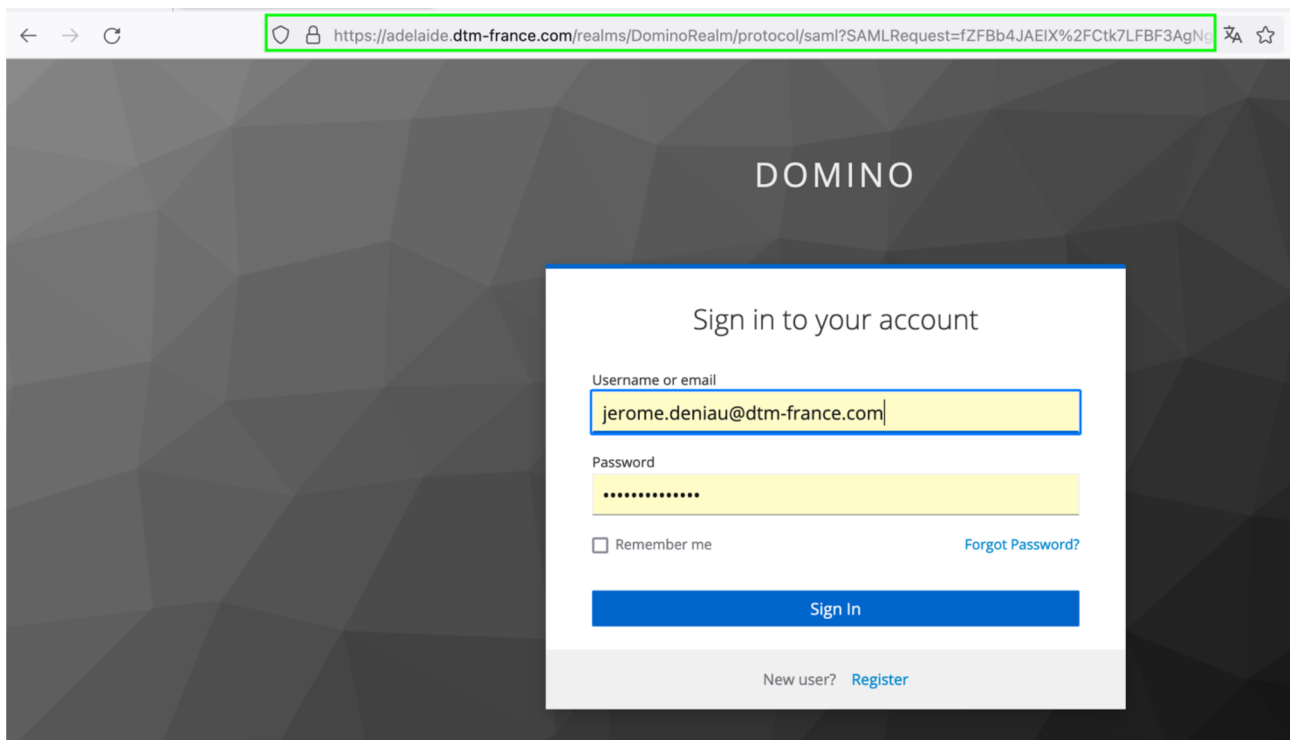
Sélectionnez 'SAML' pour le champ 'Session authentication'.

Le bouton 'Open IdP Configuration' permet de vérifier que Domino trouve bien un document de configuration IdP dans la base idpcat.nsf.

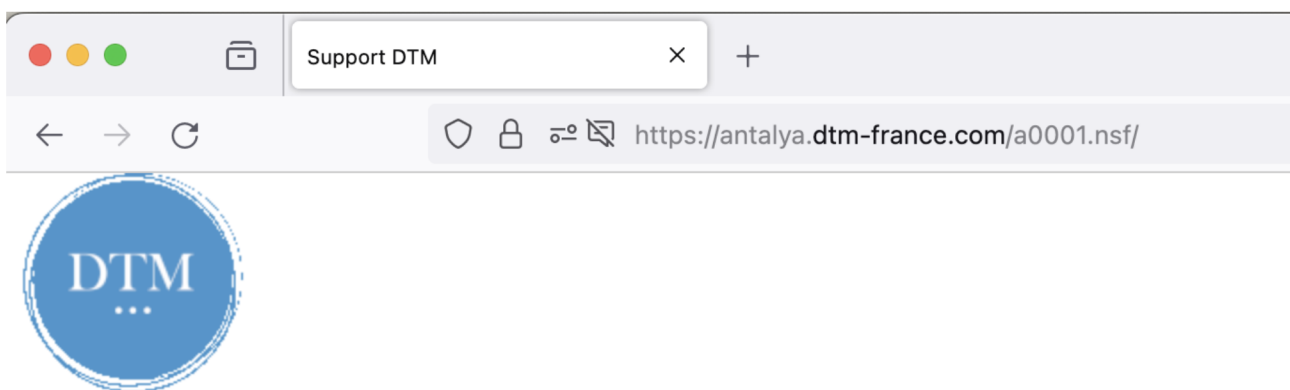
Test de la configuration

Testez l'accès à l'url Domino, vous devez être dirigé vers la page de login Keycloak par défaut. En cas d'erreur, passez à la partie troubleshoot de ce document.

Exemple avec la saisie de <https://antalya.dtm-france.com>:



Saisissez un compte et mot de passe Domino puis validez l'accès au site web.



Contrat

Ici l'accès sécurisé à la page par défaut est validé.

Fédération Notes ou Web

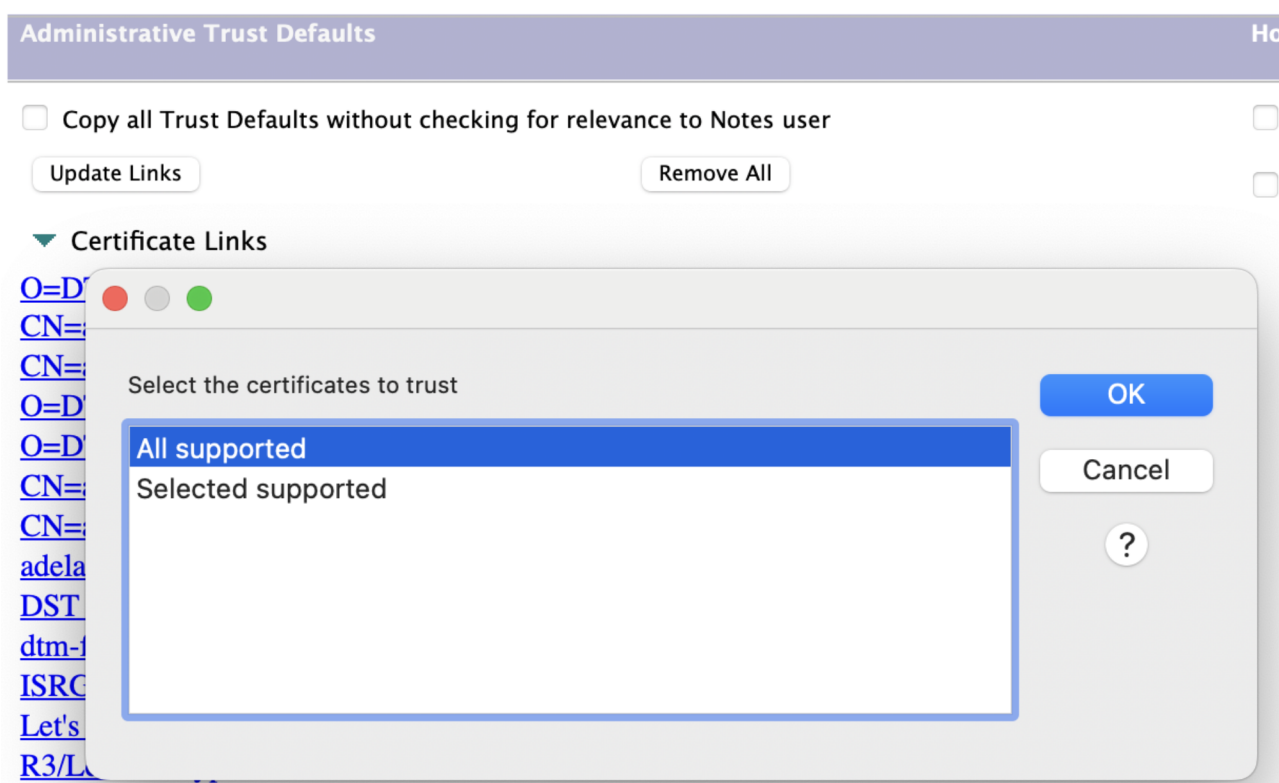
La fédération Notes ou Web est identique, dès qu'il est nécessaire d'accéder aux fichiers ID des utilisateurs il faut mettre en place la fédération Notes ou Web. La seule différence concerne le choix d'accès (Web ou Notes)

Prérequis

Vous devez propager les certificats Internet du serveur IDP au client HCL Notes.

Importer le certificat Internet dans l'annuaire Domino puis dans la vue Certificats de l'annuaire Domino utiliser le bouton Actions > Créer certification croisée.

Pour propager les certificats il faut utiliser une politique sécurité



Choisissez l'option 'Selected supported' puis les certificats de confiance du certificat SSL de l'idp. D'où l'intérêt d'utiliser un certificat SSL officiel.

Url ?SAMLIDLogin

Il faut gérer l'url ?SAMLIDLogin. Dans la vraie vie des serveurs de coffre (ID Vault) sont dédiés, ces derniers doivent avoir la tâche http et il est nécessaire de les ajouter dans la base idpcat.nsf

Par convention les urls des serveurs de coffre sont préfixés par 'vault'.

Exemple : vault.antalya.dtm-france.com.

Ce FQDN ne DOIT pas être défini au niveau DNS, c'est un nom interne utilisé par Domino.

Dans ce document les serveurs Domino Web et Notes sont aussi les serveurs de coffre.

Coffre d'ID

Même si l'accès à /verse (si verse est installé) ou iNotes est fonctionnel, il faut valider l'accès aux fichier ID du coffre. Editez le document de configuration du coffre des IDs Domino de votre coffre Domino (localisé dans le dossier IBM_ID_VAULT du serveur).

The screenshot shows the 'Vault Name: DTMVault' configuration window. It has two main sections: 'IdP authenticated vault login' and 'Non IdP authenticated login'. The 'IdP authenticated vault login' section contains four rows of configurations, each with a green border: 'Notes federated login approved IdP configurations' (vault.antalya.dtm-france.com; vault.angstroem.dtm-france.com), 'Web federated login approved IdP configurations' (same), 'Nomad federated login approved IdP configurations' (empty), and 'Bearer token (JWT) approved OIDC provider configurations' (empty). The 'Non IdP authenticated login' section has a single row 'Trusted servers' with the value 'angstroem/DTM, antalya/DTM'.

Saisissez le FQDN du site Internet Domino (ici antalya.dtm-france.com) en le préfixant de 'vault', ce qui donne : **vault.antalya.dtm-france.com**.

Ce FQDN n'existe dans aucun DNS ni fichier hosts !!!

Ne pas oublier de lister les serveurs participant au coffre (Trusted servers)

Création de la configuration de fédération côté Domino

Pour simplifier l'administration un copier/coller des documents de configuration IdP a été réalisé.

The screenshot shows the 'IdP Configuration : Keycloak DTM for vaulted Antalya' page. It has a navigation bar with 'Basics', 'Client Settings', 'Certificate Management', 'Advanced', and 'Administration'. The 'Basics' tab is selected. Below the navigation bar is a section titled 'Basics' with an 'Import XML file' button. The configuration details are as follows: 'Host names or addresses mapped to this site:' (vault.antalya.dtm-france.com), 'Protocol version:' (SAML 2.0), 'State:' (Enabled), 'Federation product:' (AuthnRequest SAML 2.0 compatible), 'Service provider ID:' (https://vault.antalya.dtm-france.com), 'Artifact resolution service URL:' (https://adelaide.dtm-france.com/realms/DominoRealm/protocol/saml/resolve), 'Single sign-on service URL:' (https://adelaide.dtm-france.com/realms/DominoRealm/protocol/saml), 'IdP name (for your reference):' (Keycloak DTM for vaulted Antalya), 'Comment:' (empty), 'Imported file:' (descriptor.xml), and 'Import time:' (17/12/2023 21:16).

Bien Saisir 'vault.xxxx.yyyy' dans les deux champs 'Host names...' et 'Serice Provider ID'

IdP Configuration : Keycloak DTM for vaulted Antalya

Basics | Client Settings | Certificate Management | Advanced | Administration

Certificate Management Settings

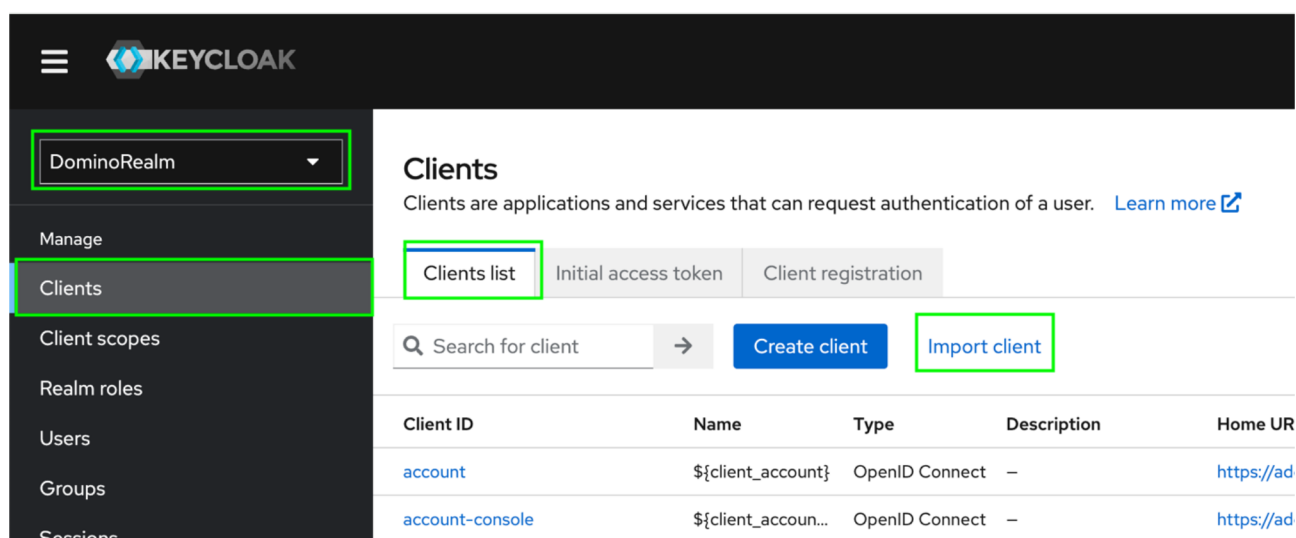
Examine SP Certificate | Export SP XML

Company name:	CN=DTMSAML3
Domino URL:	https://antalya.dtm-france.com
Single logout URL:	https://adelaide.dtm-france.com/realms/DominoRealm/protocol/saml
Certificate public hash value (base 64):	s6nDVVqQ+327LKzjHN3T4w==
Exported certificate:	 - ServiceProvider.xml

L'URL Domino doit être l'url du serveur SANS le préfixe 'vault'.
Cliquez sur 'Export SP XML' afin de mettre à jour le fichier XML
Puis enregistrez le fichier ServiceProvider.xml pour l'importer dans keycloak.

Création de la configuration de fédération côté keycloak

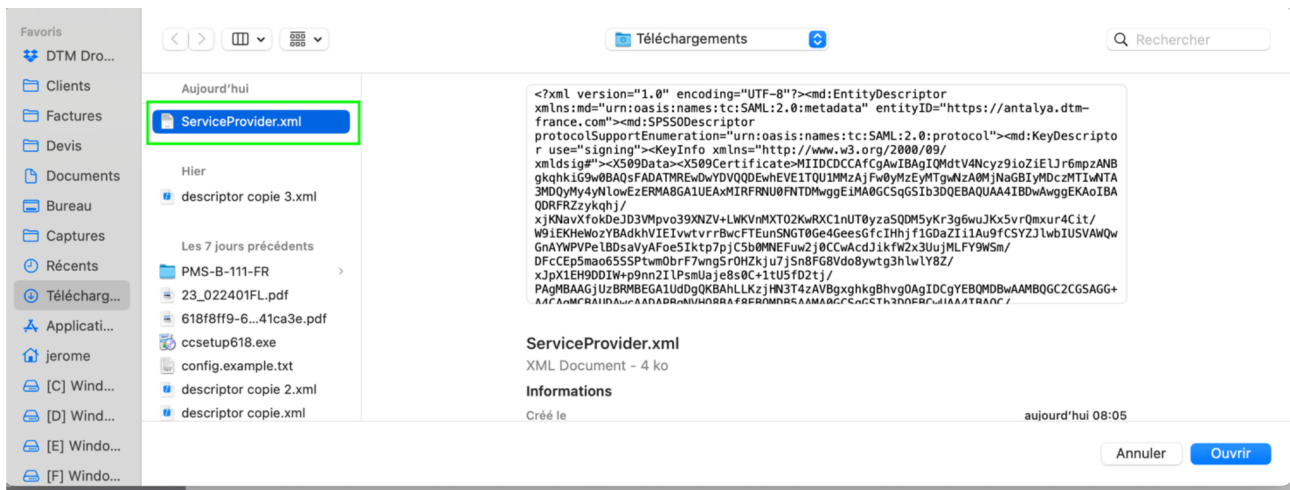
Après avoir exporté le fichier ServiceProvider.xml côté Domino, exécutez les tâches côté Key-Cloak.



The screenshot shows the Keycloak Admin Console interface. On the left, the 'DominoRealm' dropdown is selected, and the 'Clients' menu item is highlighted. The main panel shows the 'Clients' configuration for 'DominoRealm'. The 'Clients list' tab is active, displaying a table of existing clients. The 'Import client' button is highlighted with a green box.

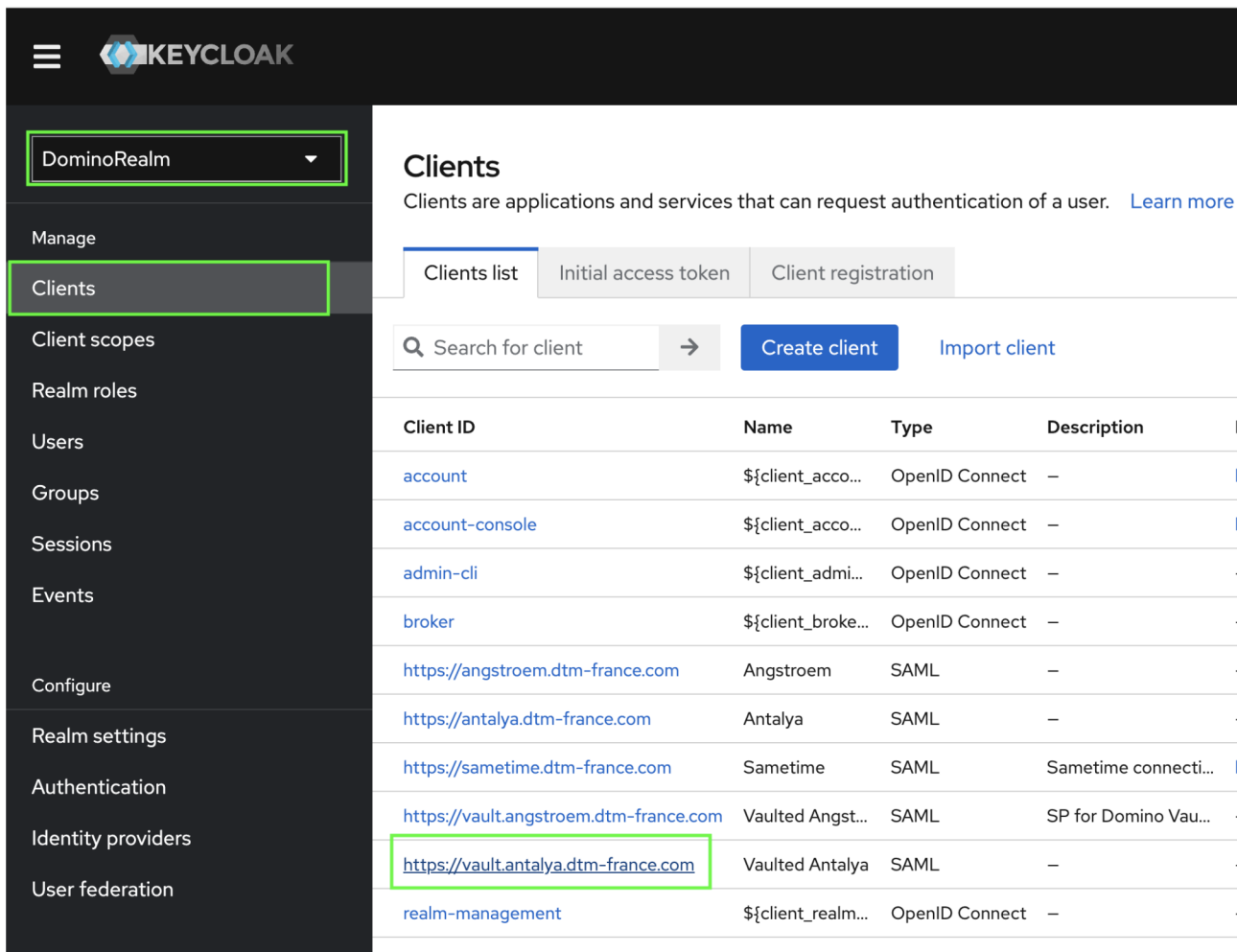
Client ID	Name	Type	Description	Home UR
account	\${client_account}	OpenID Connect	—	https://ad
account-console	\${client_accoun...}	OpenID Connect	—	https://ad

Sélectionnez le domaine Keycloak DominoRealm > Clients puis dans la section 'Clients list' cliquez sur le lien 'Import client'.



Sélectionnez le fichier ServiceProvider.xml généré précédemment dans Domino via la base idp-cat.nsf.

Validez le contenu des différents écrans correspondants aux onglets



Onglet Settings

Assurez vous que l'url se termine bien par ?SAMLIDLogin

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

General Settings

Client ID * ?

https://vault.antalya.dtm-france.com

Name ?

Vaulted Antalya

Description ?

Always display in UI ?

On

Access settings

Root URL ?

Home URL ?

Valid redirect URIs ?

https://antalya.dtm-france.com/names.nsf?SAMLIDLogin

+ Add valid redirect URIs

Jump to

General

Access

SAML

Sign

Logins

Logo

Onget Keys

Désélectionnez l'option de chiffrement

Clients > Client details

https://vault.antalya.dtm-france.com

SAML

Enabled

Action

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Signing keys config

If you enable the "Client signature required" below, you must configure the signing keys by generating or importing keys, and the client will sign their saml requests and responses. The signature will be validated.

Client signature required ?

On

Certificate ?

MIIDCDCCAFcGAWlBAGlQMdtV4Ncyz9ioZiElJr6mpzANBgkqhkiG9w0BAQsFADATMREwDwYDVQQDEwhEVEITQUIMMzAjFw0yMzEyMTgwNzA0MjNaGBlyMDczMTIwNTA3MDQyMy4yNlowEzERMA8GA1UEAxMIRFRNU0FNTDMwggiEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDRFRZzykqhj/xjKNavXfokDeJD3VMpvo39XNZV+LWKVnMXTO2KwRXCInUT0yzaSQDM5yKr3g6wuJKx5vrQmxur4Cit/W9iEKHeWozYBAdkhVIElvwtvrrBwcFTEunSNGT0Ge4GeesGfclHhjfIGDaZliiAu9fCSYZJlwblUSVAWQwGnA

DTM

Documentation

17/12/2023

Encryption keys config

If you enable the "Encryption assertions" below, you must configure the encryption keys by generating or importing keys, and the SAML assertions will be encrypted with the client's public key using AES.

Encrypt assertions ⓘ ☐ Off

Onglet Client scopes

Cliquez sur le lien *-dedicated

[Clients](#) > Client details

<https://vault.antalya.dtm-france.com> SAML



Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Setup

Evaluate

▼ Name ▼

🔍 Search by name



Add client scope

Change type to ▼



Assigned client scope

Assigned type

Description



<https://vault.antalya.dtm-france.com-dedicated>

none ▼

Dedicated scope and mapper



role_list

Default ▼

SAML role list

Ajouter les mappeurs standards et ajoutez NameID => email pour le retour Domino

https://vault.antalya.dtm-france.com

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope



Add mapper ▾

Name	Category	Type
X500 surname	AttributeStatement Mapper	User Property
X500 givenName	AttributeStatement Mapper	User Property
NameID	NameID Mapper	User Attribute Mapper For NameID
X500 email	AttributeStatement Mapper	User Property

Mise à jour de la politique Domino

Activez l'option SAML pour Notes et WEB dans le paramètre de sécurité de votre politique. Vous pouvez commencer par l'option Web AVANT d'appliquer à Notes.

Save & Close Cancel Inheritance Enforcement How To Apply

Security Settings : DTMVaultVaultSetting

Basics Password Management Execution Control List Keys and Certificates Signed Plug-ins Portal Server ID Vault Proxies Comments Administration

Password Management Basics Notes Shared Login Federated Login

Notes Federated Login

How to apply this setting: Inherit from parent policy Enforce in child policies

Enable Notes Federated login with SAML: Yes Don't set value Inherit Enforce

Enter machine specific Formula

Activation Notification

How to apply this setting: Inherit from parent policy Enforce in child policies

How to notify users when enabled: No notification Don't set value Inherit Enforce

Custom message text:

Deactivation Notification

How to apply this setting: Inherit from parent policy Enforce in child policies

How to notify users when disabled: No notification Don't set value Inherit Enforce

Custom message text:

Web Federated Login

How to apply this setting: Inherit from parent policy Enforce in child policies

Enable Web Federated login with SAML: Yes Don't set value Inherit Enforce

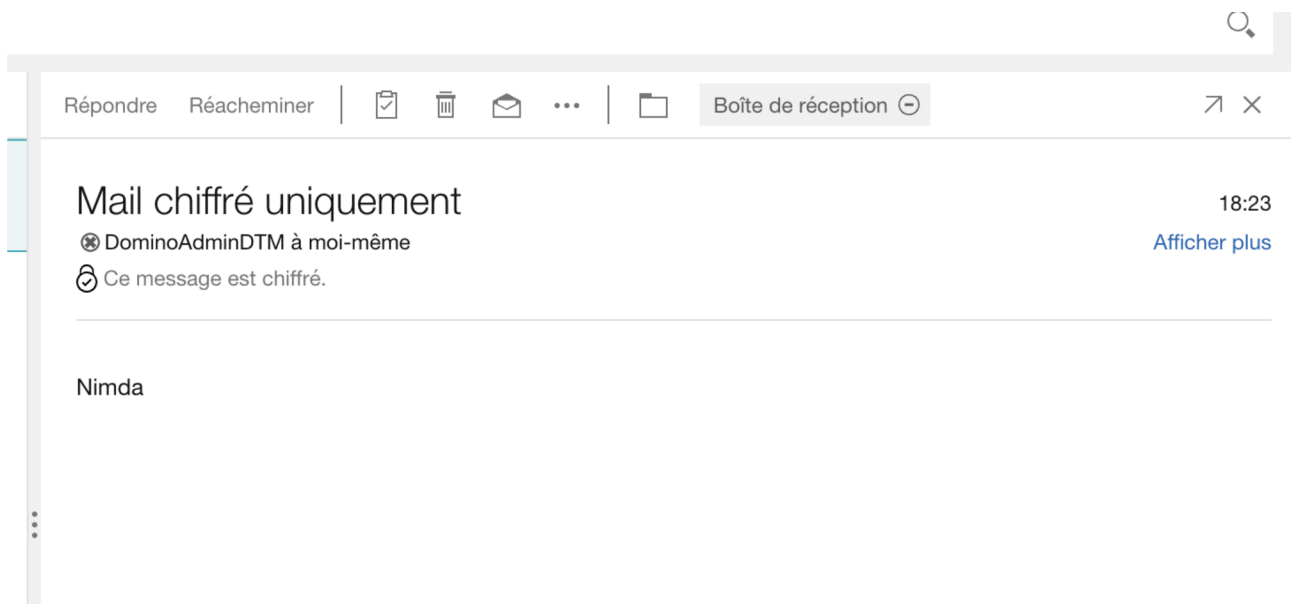
Normal Federated Login

How to apply this setting: Inherit from parent policy Enforce in child policies

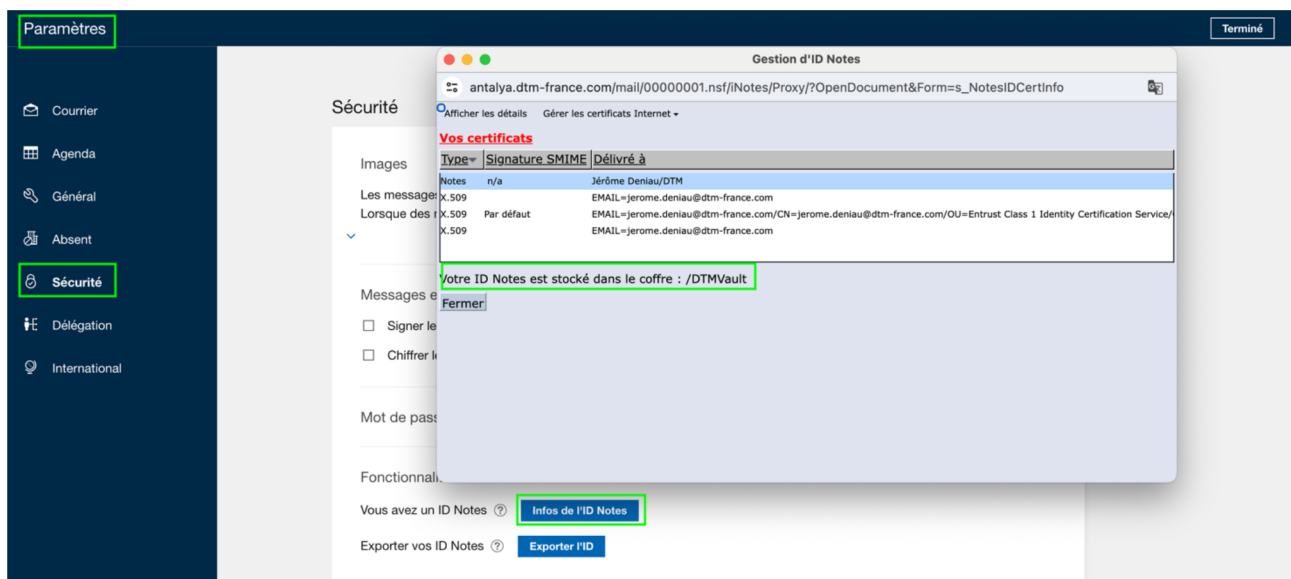
Enable Normal Federated login with SAML: No Don't set value Inherit Enforce

Activez l'option 'Enable Web Federated login with SAML' dans un premier temps pour les tests.

Valider la fédération Web avec Verse



Validez la fédération Web en utilisant Verse et un mail chiffré en réception, aucun mot de passe n'est demandé.



Vérifiez que le fichier ID provient bien du coffre dans Verse (sans saisie de mot de passe) : Paramètres > Sécurité > Infos de l'ID Notes.

Valider la fédération Notes

Pour valider le fonctionnement d'un client Notes (sans activer les notifications), il suffit de consulter le fichier ID (Fichier > Sécurité > Sécurité utilisateur...

Security Basics

Who You Are

Name: Jérôme Deniau/DTM

ID File: In memory ID file

ID File encryption strength: 128 bit AES and SHA-256

ID File expiration date: 20/12/2025

Mail Recovery ID ...

Renew...

Your ID Settings

Your ID is not stored on disk. It was downloaded from ID vault and is in memory.

☐ Log in to Notes using your operating system login

This ID file has been backed up into vault: /DTMVault

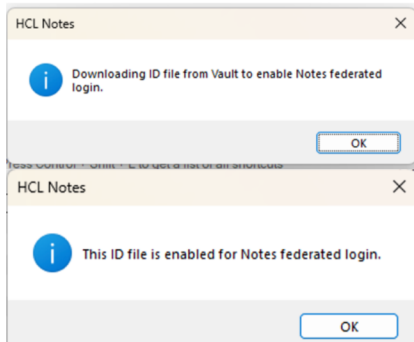
ID Vault Sync

Logout Settings

☐ Automatically lock my Notes ID after 15 minutes

OK Close

Si vous avez activé les notifications vous aurez plusieurs popups :



Troubleshoot

Ce chapitre n'est pas exhaustif.

Invalid Request

Ce message sur la page de login de keycloak indique que Keycloak n'a pas trouvé l'url (Service Provider) demandé par Domino.

Pour déboguer , ajouter les deux variables suivantes dans le fichier notes.ini :

```
set configuration DEBUG_SAML=31
set config WEBAUTH_VERBOSE_TRACE=1
```

Si le problème est lié au Web, relancez la tâche http : tell http restart (éviter d'exécuter restart task http)

Si le problème est lié à la fédération Notes, relancez le serveur Domino.

```
[1682989:000264-00007F0350081640] <samlp:AuthnRequest xmlns:samlp="urn:oa-
sis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="http://antalya.dtm-
france.com/names.nsf?SAMLLogin" Destination="https://adelaide.dtm-france.com/realms/Domi-
noRealm/protocol/saml" ID="id_8C2E240361BF1
```

Ici le problème vient du protocole (http) défini dans le champ Service Provider de la base idpcat, Keycloak ayant l'url en <https://antalya...>

Debug Keycloak

Passez temporairement keycloak en mode debug :

Arrêtez keycloak : `systemctl stop keycloak`

Puis lancez keycloak afin d'enregistrer un log dans /var/log

```
./kc.sh start --log="console,file" --log-level=DEBUG --log-file=/var/log/keycloak.log
```