

# niota – SAML configuration

**Important!** SAML authentication requires **HTTPS** connection.

Prerequisite: meta database table `et_user` must contain column `userid_saml`. Run the following commands to create column if it does not exist:

```
alter table et_user add userid_saml varchar(128) CHARACTER SET UTF8MB4;
create or replace view v_et_user as select * from et_user;
```

## Apache configuration

Add two new lines to Apache's config file `httpd.conf` – default path is `c:/Apache24x64/conf/httpd.conf` which may differ on your environment.

First define a variable for `simplesamlphp` – framework for SAML authentication used by `niota` – configuration directory path. Add the following line to the end of the file:

```
SetEnv SIMPLESAMLPHP_CONFIG_DIR
"c:/Apache24x64/htdocs/niota/app/vendor/simplesamlphp/simplesamlphp/config"
```

Take care about Apache's correct path on your environment.

Then you have to define an alias for `simplesamlphp`'s public folder. `Simplesamlphp` admin page can be accessed here even authentication process will use this folder. Path definition must be changed if Apache's path differs. Add the following line to the end of file `httpd.conf`:

```
Alias /simplesaml
"c:/Apache24x64/htdocs/niota/app/vendor/simplesamlphp/simplesamlphp/public"
```

After adding these definitions restart Apache server.

Sample result URL for `simplesamlphp` opening page. You can do nothing here. It is only a welcome page:

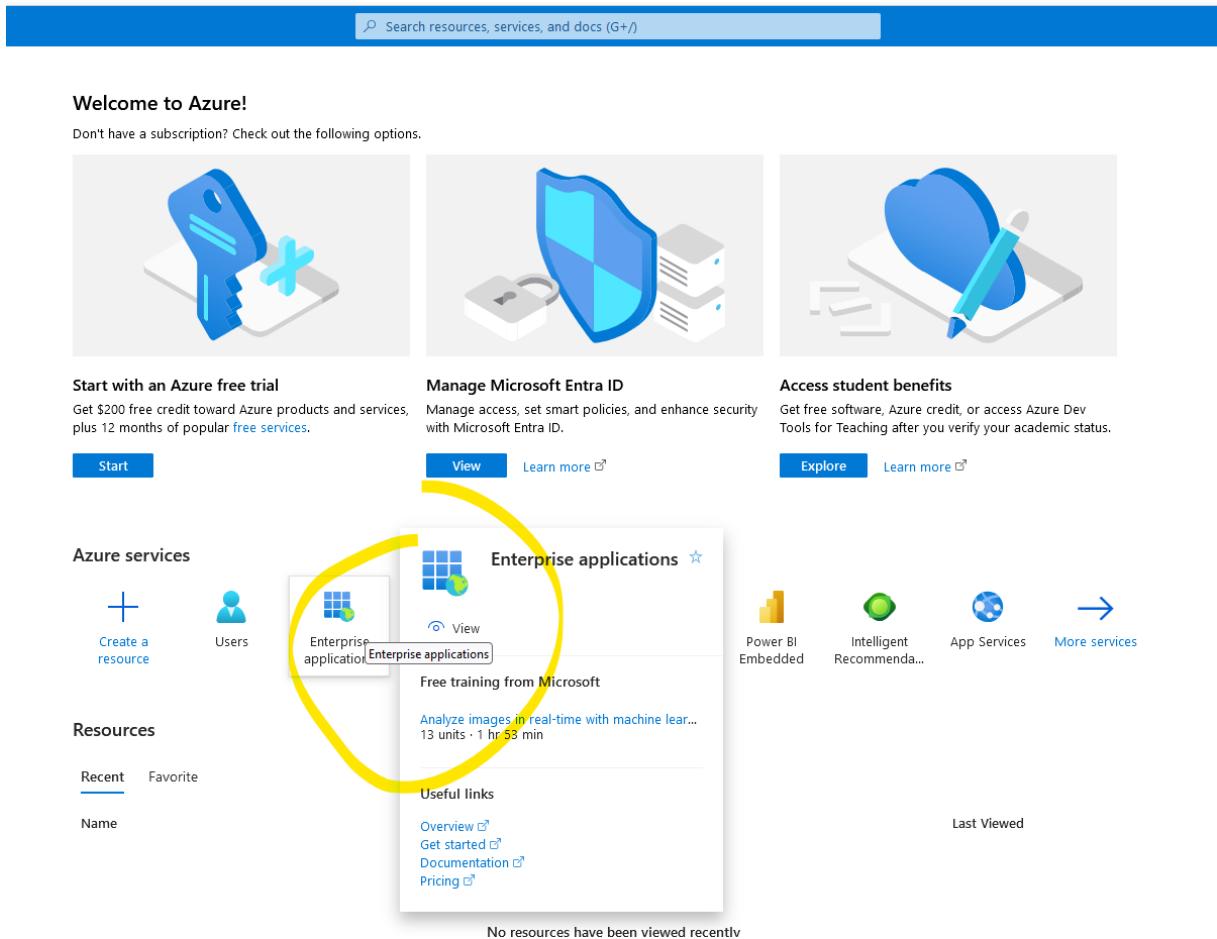
<https://office.etixpert.com/simplesaml/index.php>

Sample result URL for `simplesamlphp` admin page which will be used after further configuration:

<https://office.etixpert.com/simplesaml/admin/index.php>

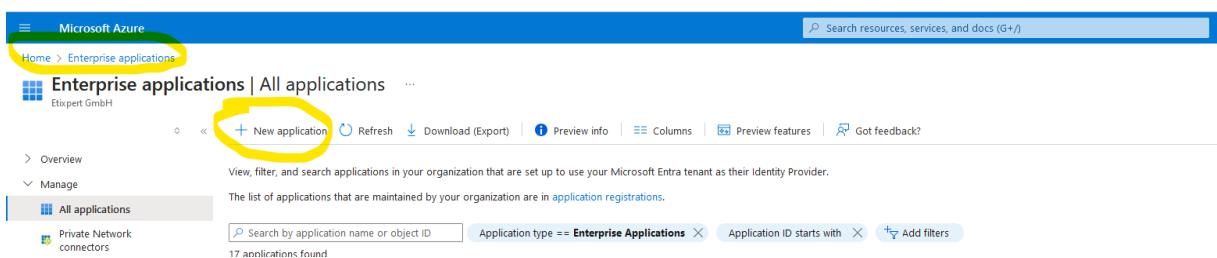
# Azure configuration

If niota application does not exist in Azure then you have to create it. Go to menu item *Enterprise applications*.



The screenshot shows the Microsoft Azure homepage. At the top, there is a search bar with the placeholder "Search resources, services, and docs (G+/" and a blue header bar. Below the header, there is a "Welcome to Azure!" message and a section for users without a subscription. Three icons are shown: a key and a plus sign, a shield and a server, and a brain and a pen. Below these are three buttons: "Start with an Azure free trial", "Manage Microsoft Entra ID", and "Access student benefits". The "Enterprise applications" menu item is highlighted with a yellow circle. The "Enterprise applications" section includes a "View" button, a "Learn more" link, a "Free training from Microsoft" section, and a "Useful links" section with links to "Overview", "Get started", "Documentation", and "Pricing". To the left, there is a sidebar with "Azure services" (Create a resource, Users), "Resources" (Recent, Favorite, Name), and "Last Viewed". To the right, there are links to "Power BI Embedded", "Intelligent Recommenda...", "App Services", and "More services".

Select menu item *New application*:



The screenshot shows the "Enterprise applications | All applications" page in Microsoft Azure. The URL in the address bar is "Home > Enterprise applications". The page title is "Enterprise applications | All applications". The top navigation bar includes "New application", "Refresh", "Download (Export)", "Preview info", "Columns", "Preview features", and "Got feedback?". The left sidebar has sections for "Overview", "Manage", and "All applications" (which is selected). The main content area shows a list of applications with a search bar at the bottom. The "New application" button is highlighted with a yellow circle.

Choose menu item *Create your own application*:

Microsoft Azure

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery ...

[Create your own application](#) | [Got feedback?](#)

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your organization to the app. For other organizations to discover and use, you can file a request using the process described in [this article](#).

Search application

Single Sign-on : All User Account Management : All Categories : All

Cloud platforms

Amazon Web Services (AWS) Google Cloud Platform Oracle SAP

Enter the name of the application then click button *Create* at the bottom of the page:

etixpert@etixpertgmbh... ETIXPERT GMBH (ETIXPERTGMBH)

### Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

Configure Application Proxy for secure remote access to an on-premises application  
 Register an application to integrate with Microsoft Entra ID (App you're developing)  
 Integrate any other application you don't find in the gallery (Non-gallery)

Cisco Secure Firewall - Secure Client (formerly Cisco AnyConnect) Cisco Webex Cisco

Create

Then select your application and define users who can use SAML authentication. Select menu item *Assign users and groups*.

Microsoft Azure

Home >

## niota-test | Overview

Enterprise Application

**Properties**

Name: niota-test

Application ID: 6ee7ed14-1222-4cc4-bd85-f...

Object ID: b57ef305-eac3-41f0-b5a3-2 ...

**Getting Started**

1. Assign users and groups

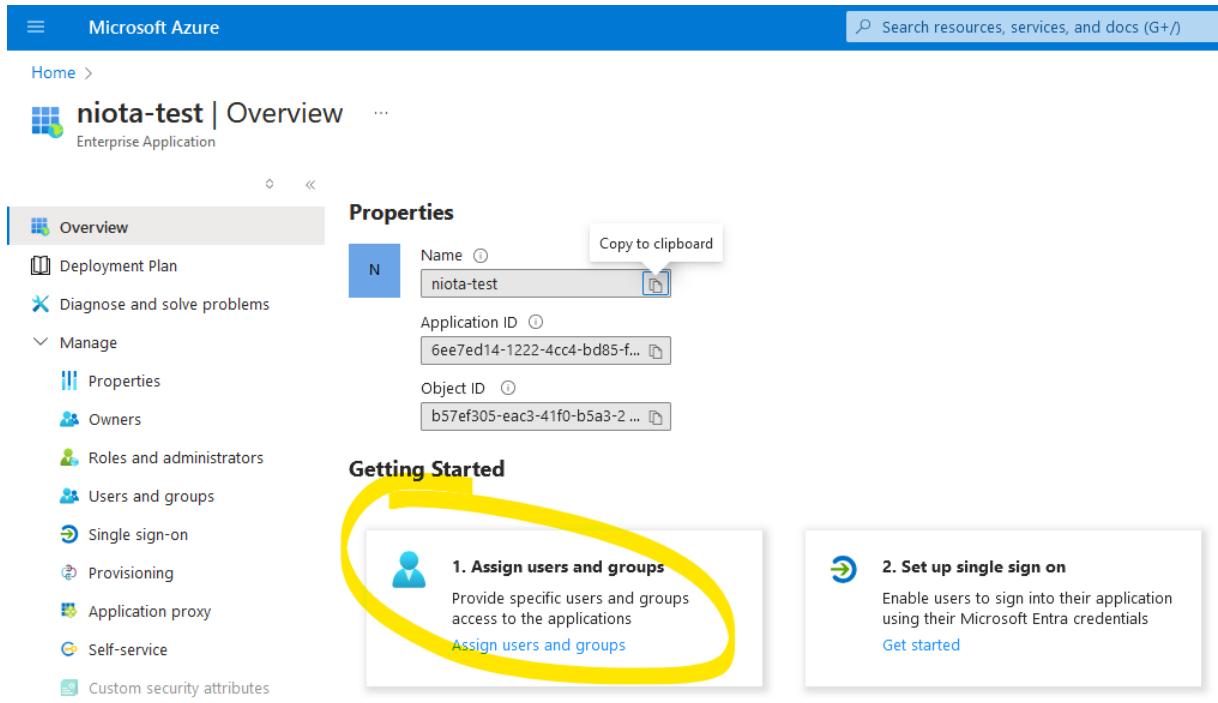
Provide specific users and groups access to the application

Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

Get started



Click item *Add user/group* to assign a user to the application

Microsoft Azure

Home > niota-test

## niota-test | Users and groups

Enterprise Application

**Overview**

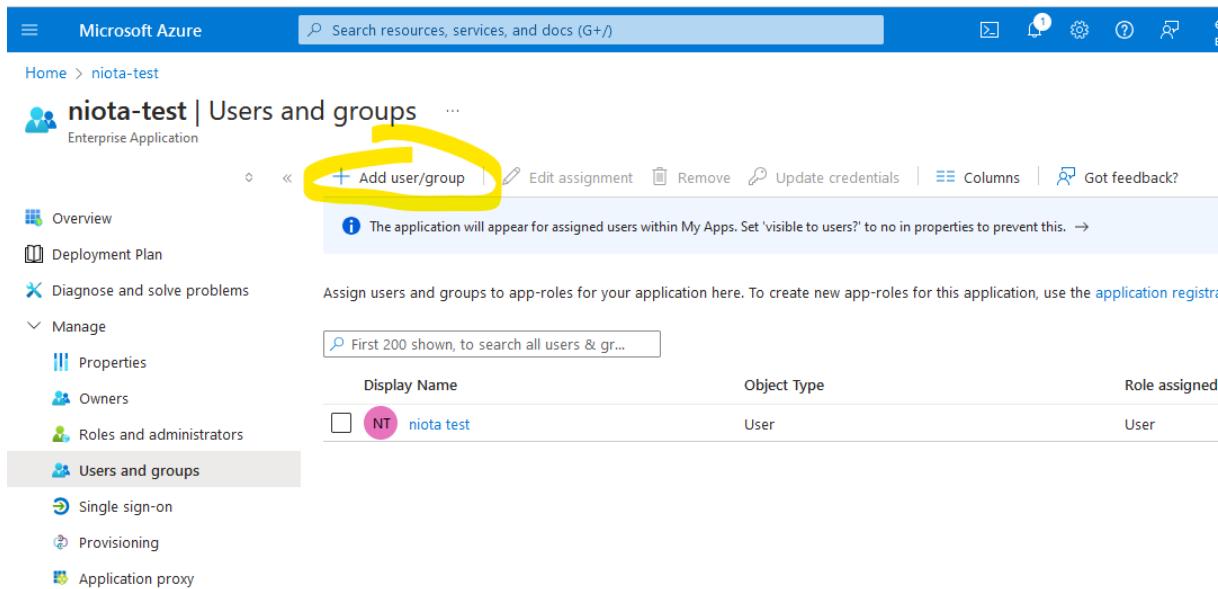
**Add user/group**

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration API.

First 200 shown, to search all users & gr...

Display Name	Object Type	Role assigned
NT iota test	User	User



Click button *None selected* then select users from the list and submit the selection – see screenshot below:

Microsoft Azure

Home > niota | Users and groups > Add Assignment

Etixpert GmbH

Users

Groups are not available for assignment due to your Active Directory application.

None Selected

Select a role

User

Try changing or adding filters if you don't see what you're looking for.

Search

5 results found

All Users

Name	Type	Details
...	...	...
...	...	...
...	...	...
...	...	...
...	...	...

Select

Assign

Selected (0)

Reset

No items selected

## Configure SAML in Azure

Select menu item *Single sign-on* from the left menu

Home > Enterprise applications | All applications > niota-test

niota-test | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy

Upload metadata file Change single sign-on mode Test this application Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more](#).

Read the [configuration guide](#) for help integrating niota-test.

1 Basic SAML Configuration

Identifier (Entity ID)	niotasamltest
Reply URL (Assertion Consumer Service URL)	https://office.etixpert.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	https://office.etixpert.com/niota/app/login.php

Make the following configuration steps and fill the parameters:

- **Identifier (Entry ID)** – a unique identifier of the application. Entered value will be used in samlphp configuration.
- **Reply URL (Assertion Consumer Service URL)** - URL of the saml service.  
Sample URL:  
<https://office.etixpert.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp>  
The following part of the URL is fixed: `simplesaml/module.php/saml/sp/saml2-`

acs.php/default-sp”.

note: niota.etixpert.com/simpleSAML part of the URL refers to the alias set in Apache’s configuration file.

- **Logout Url (Optional)** - the page has to be loaded after logging out of Azure by using SAML in niota software. This must be the login page of niota application. Example URL: <https://office.etixpert.com/niota/app/login.php>

## simplesamlphp configuration

### config.php

Open simplesamlphp configuration file config.php, which can be found in niota installation folder:  
c:\Apache24x64\htdocs\niota\app\vendor\simplesamlphp\simplesamlphp\config\config.php

This is the general configuration file of simplesamlphp library. These settings will be used during SAML authentication.

Define setting baseurlpath according to your environment:

```
* baseurlpath is a *URL path* (not a filesystem path).
* A valid format for 'baseurlpath' is:
* [(http|https)://(hostname|fqdn)[:port]][/path/to/simpleSAML/]
*
* The full url format is useful if your SimpleSAMLphp setup is hosted behind
* a reverse proxy. In that case you can specify the external url here.
* Specifying the full URL including https: will let SimpleSAMLphp know
* that it runs on HTTPS even if the backend server is plain HTTP.
*
* Please note that SimpleSAMLphp will then redirect all queries to the
* external url, no matter where you come from (direct access or via the
* reverse proxy).
*/
'baseurlpath' => 'https://office.etixpert.com/simpleSAML/' ,
```

Note: URL part /simpleSAML/ refers to the alias set in Apache's configuration file (see at Apache configuration).

If path of your niota installation differs then the ones below, then edit the following path definitions according to your installation details:

```
/*
* The following settings are *filesystem paths* which define where
* SimpleSAMLphp can find or write the following things:
* - 'cachedir': Where SimpleSAMLphp can write its cache.
* - 'loggingdir': Where to write logs. MUST be set to NULL when using a
logging
*           handler other than `file`.
* - 'datadir': Storage of general data.
* - 'tempdir': Saving temporary files. SimpleSAMLphp will attempt to create
*   this directory if it doesn't exist. DEPRECATED - replaced by cachedir.
* When specified as a relative path, this is relative to the SimpleSAMLphp
* root directory.
*/
'cachedir' =>
'c:/Apache24x64/htdocs/niota/app/vendor/simpleSAMLphp/simpleSAMLphp/cache/' ,
'loggingdir' => 'c:/Apache24x64/htdocs/niota/app/log/' ,
'datadir' =>
'c:/Apache24x64/htdocs/niota/app/vendor/simpleSAMLphp/simpleSAMLphp/data/' ,
'tempdir' =>
'c:/Apache24x64/htdocs/niota/app/vendor/simpleSAMLphp/simpleSAMLphp/tmp/' ,
```

Certification directory also must be set:

```
/*
* Certificate and key material can be loaded from different possible
* locations. Currently two locations are supported, the local filesystem
* and the database via pdo using the global database configuration. Locations
```

```

* are specified by a URL-link prefix before the file name/path or database
* identifier.
*/
/* To load a certificate or key from the filesystem, it should be specified
* as 'file://<name>' where <name> is either a relative filename or a fully
* qualified path to a file containing the certificate or key in PEM
* format, such as 'cert.pem' or '/path/to/cert.pem'. If the path is
* relative, it will be searched for in the directory defined by the
* 'certdir' parameter below. When 'certdir' is specified as a relative
* path, it will be interpreted as relative to the SimpleSAMLphp root
* directory. Note that locations with no prefix included will be treated
* as file locations.
*/
'certdir' =>
'c:/Apache24x64/htdocs/niota/app/vendor/simplestsamlphp/simplestsamlphp/cert/',

```

Technical support information:

```

/*
 * Some information about the technical persons running this installation.
 * The email address will be used as the recipient address for error reports,
and
 * also as the technical contact in generated metadata.
*/
'technicalcontact_name' => 'Administrator',
'technicalcontact_email' => 'support@etixpert.com',

```

Define password for the administrative surface of simplestsamlphp. You must enter the surface later to do some further configuration steps.

```

/*
 * This password must be kept secret, and modified from the default value 123.
 * This password will give access to the installation page of SimpleSAMLphp
with
 * metadata listing and diagnostics pages.
 * You can also put a hash here; run "bin/pwgen.php" to generate one.
*/
'auth.adminpassword' => 'my-secret-password',

```

Set domain as trusted where niota is running:

```

/*
 * Array of domains that are allowed when generating links or redirects
 * to URLs. SimpleSAMLphp will use this option to determine whether to
 * to consider a given URL valid or not, but you should always validate
 * URLs obtained from the input on your own (i.e. ReturnTo or RelayState
 * parameters obtained from the $_REQUEST array).
*
* SimpleSAMLphp will automatically add your own domain (either by checking
* it dynamically, or by using the domain defined in the 'baseurlpath'
* directive, the latter having precedence) to the list of trusted domains,
* in case this option is NOT set to NULL. In that case, you are explicitly
* telling SimpleSAMLphp to verify URLs.
*
* Set to an empty array to disallow ALL redirects or links pointing to
* an external URL other than your own domain. This is the default behaviour.
*
* Set to NULL to disable checking of URLs. DO NOT DO THIS UNLESS YOU KNOW
* WHAT YOU ARE DOING!
*
* Example:
*   'trusted.url.domains' => ['sp.example.com', 'app.example.com'],

```

```
 */
'trusted.url.domains' => ['office.etixpert.com'],
```

Debug flags optionally:

```
'debug' => [
  'saml' => false,
  'backtraces' => FALSE,
  'validatexml' => false,
],
```

Set log level:

```
/*
 * Define the minimum log level to log. Available levels:
 * - SimpleSAML\Logger::ERR      No statistics, only errors
 * - SimpleSAML\Logger::WARNING  No statistics, only warnings/errors
 * - SimpleSAML\Logger::NOTICE   Statistics and errors
 * - SimpleSAML\Logger::INFO    Verbose logs
 * - SimpleSAML\Logger::DEBUG   Full debug logs - not recommended for
production
 *
 * Choose logging handler.
 *
 * Options: [syslog,file,errorlog,stderr]
 *
 * If you set the handler to 'file', the directory specified in loggingdir
above
 * must exist and be writable for SimpleSAMLphp. If set to something else, set
 * loggingdir above to 'null'.
 */
'logging.level' => SimpleSAML\Logger::INFO,
```

If you use proxy url this must be defined:

```
*****
| PROXY CONFIGURATION |
*****
```

```
/*
 * Proxy to use for retrieving URLs.
 *
 * Example:
 *   'proxy' => 'tcp://proxy.example.com:5100'
 */
'proxy' => 'tcp://office.etixpert.com',
```

## authsources.php

This is the configuration file of the service provider which is used during the SAML authentication process.

Required settings are placed inside section: `default-sp`.

Identifier (Entity ID) defined in Azure surface must be set here in setting: `entityID`.

```
// The entity ID of this SP.
'entityID' => 'niotasamltest',
```

Microsoft Azure

Home > Enterprise applications | All applications > niota-test

## niota-test | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more](#).

Read the [configuration guide](#) for help integrating niota-test.

**1** Basic SAML Configuration

Identifier (Entity ID)	niotasamltest
Reply URL (Assertion Consumer Service URL)	https://office.etixpert.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://office.etixpert.com/niota/app/login.php

[Edit](#)

Define URL of the SAML identity provider.

```
// The entity ID of the IdP this SP should contact.
// Can be NULL/unset, in which case the user will be shown a list of available
IdPs.
'idp' => 'https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/'
```

You can find the value to enter on Azure surface at menu item *Microsoft Entra Identifier*:

Microsoft Azure

Home > Enterprise applications | All applications > niota-test

## niota-test | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Application proxy Self-service Custom security attributes Security Activity Troubleshooting + Support

**3** SAML Certificates

Token signing certificate	Active
Status	73D83E6575DCF4B48AE025A9767505A203E1C722
Thumbprint	7/22/2027, 2:14:58 PM
Expiration	etixpert@██
Notification Email	<a href="https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/">https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/</a>
App Federation Metadata Url	<a href="#">Download</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

**4** Set up niota-test

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	<a href="https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/">https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/</a>
Microsoft Entra Identifier	<a href="https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/">https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/</a>
Logout URL	<a href="https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/">https://login.microsoftonline.com/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/</a>

**5** Test single sign-on with niota-test

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

If you use porxy you must set this flag to true. Otherwise set it as false:

```

/*
 * If SP behind the SimpleSAMLphp in IdP/SP proxy mode requests
 * AuthnContextClassRef, decide whether the AuthnContextClassRef will be
 * processed by the IdP/SP proxy or if it will be passed to the original
 * IdP in front of the IdP/SP proxy.
 */
'proxymode.passAuthnContextClassRef' => true,

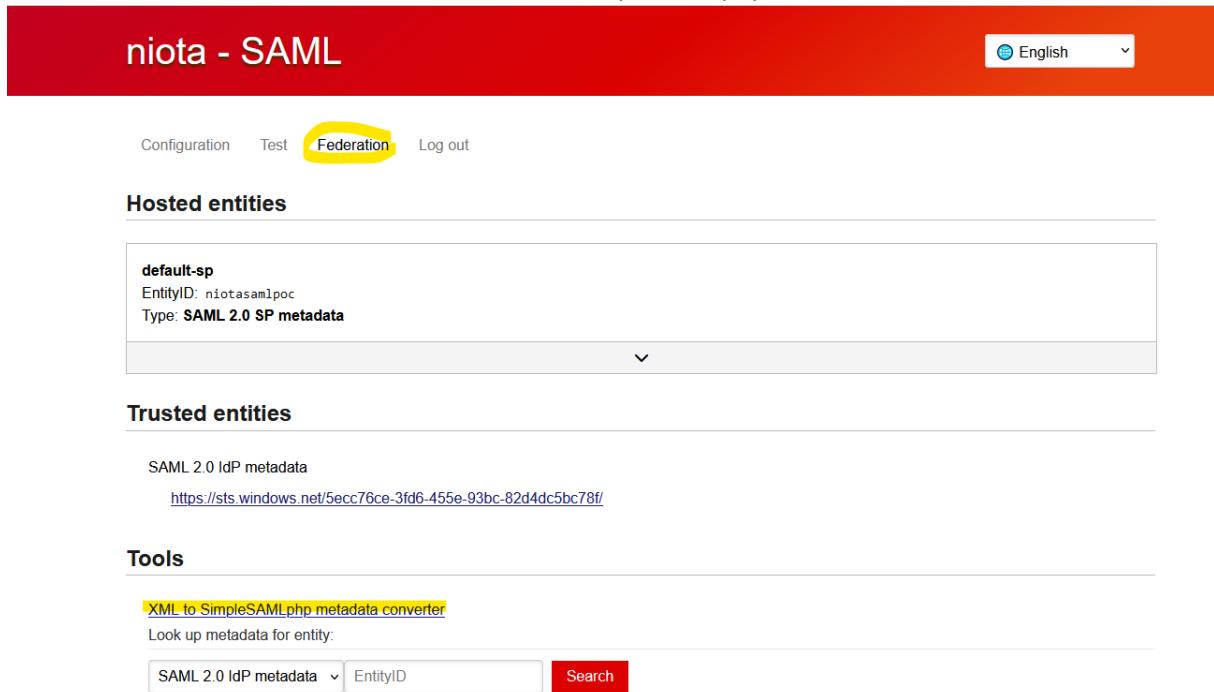
```

## saml20-idp-remote.php

Open admin surface of simplesamlphp. Sample link:

<https://office.etixpert.com/simplesaml/admin/index.php>

Enter to admin surface by using password ('`auth.adminpassword`') set in file `config.php`. Select menu item *Federation* then click on link *XML to SimpleSAMLphp metadata converter*.



The screenshot shows the 'niota - SAML' admin interface. At the top, there is a red header bar with the title 'niota - SAML'. To the right of the title is a language selection dropdown set to 'English'. Below the header, there is a navigation bar with four items: 'Configuration', 'Test', 'Federation' (which is highlighted with a yellow box), and 'Log out'. The main content area is divided into sections. The first section, 'Hosted entities', contains a table with one row. The row shows a 'default-sp' entry with EntityID: 'niotasamlpoc' and Type: 'SAML 2.0 SP metadata'. The second section, 'Trusted entities', contains a table with one row. The row shows a 'SAML 2.0 IdP metadata' entry with the URL 'https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/'. The third section, 'Tools', contains a search form. The search form has a dropdown menu set to 'SAML 2.0 IdP metadata', an input field for 'EntityID', and a red 'Search' button.

Here you must enter and parse the metadata definition in a later step. As next step you have to download metadata definition in XML format from Azure surface to be able to fill the input field of metadata parser.

Configuration Test Federation Log out

## Metadata parser

XML metadata

**Parse**

First you must download the metadata XML file from Azure surface:

Microsoft Azure

Search resources, services, and docs (G+)

Home > niota-test

niota-test | SAML-based Sign-on ...

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

**1** Overview

**2** Basic SAML Configuration

Identifier (Entity ID)	niotasamltest
Reply URL (Assertion Consumer Service URL)	<a href="https://office.etixpert.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp">https://office.etixpert.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp</a>
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	<a href="https://office.etixpert.com/niota/app/login.php">https://office.etixpert.com/niota/app/login.php</a>

**3** Attributes & Claims

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

**4** SAML Certificates

Token signing certificate

Status	Active
Thumbprint	73D83E6575DCF4B4BAE025A9767505A203E1C722
Expiration	7/22/2027, 2:14:58 PM
Notification Email	etixpert@etixpert.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/5ecc76ce-3fd6-433a-833a-0a2a2a2a2a2a/">https://login.microsoftonline.com/5ecc76ce-3fd6-433a-833a-0a2a2a2a2a2a/</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
<b>Federation Metadata XML</b>	<a href="#">Download</a>

Verification certificates (optional)

Required	No
Active	0
Expired	0

Copy and paste the content of the downloaded xml file to the Metadata parser textbox and click button Parse.

Converted metadata must be copied and pasted into file `saml20-idp-remote.php`. File path if Niota is installed in the default directory:

c:\Apache24x64\htdocs\niota\app\vendor\simplesamlphp\simplesamlphp\metadata\saml20-idp-remote.php

# niota - SAML

[Configuration](#) [Test](#) [Federation](#) [Log out](#)

## Metadata parser

---

### XML metadata

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="...8871a89-1852-4cdd-bd88-893ab033701" entityID="https://sts.windows.net/5ecc7ece-3fd5-455e-93bc-8244dc5bc785" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI="#_8871a89-1852-4cdd-bd88-893ab033701"><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></Transforms><DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /><DigestValue>7kc8V1zdTAop2Qx1QgxLB7twspwu6tQYvou0gZp1/</DigestValue></Reference><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><DigestValue>...</DigestValue></Signature><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference URI="#_8871a89-1852-4cdd-bd88-893ab033701"><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /></Transforms><DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /><DigestValue>...</DigestValue></Reference><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><DigestValue>...</DigestValue></Signature><KeyInfo><ds:X509Data><ds:X509Name>http://www.w3.org/2000/09/xmldsig#</ds:X509Name><ds:X509SubjectName>...</ds:X509SubjectName></ds:X509Data></KeyInfo><ds:X509Certificate>...</ds:X509Certificate></EntityDescriptor>
```

saml20-idp-remote.php file content will look like this (not the full content is displayed in the screenshot):

```

<?php

/**
 * SAML 2.0 remote IdP metadata for SimpleSAMLphp.
 *
 * Remember to remove the IdPs you don't use from this file.
 *
 * See: https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-remote
 */
$metadata['https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/' ] = [
    'entityid' => 'https://sts.windows.net/5ecc76ce-3fd6-455e-93bc-82d4dc5bc78f/' ,
    'contacts' => [],
    'metadata-set' => 'saml20-idp-remote',
    'SingleSignOnService' => [
        [
            'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
        ...
    ]
]

```

After these configuration steps test the authentication process:



If connection test is successful, then go to niota configuration.

## niota configuration

Open configuration file `system_defaults.php`.

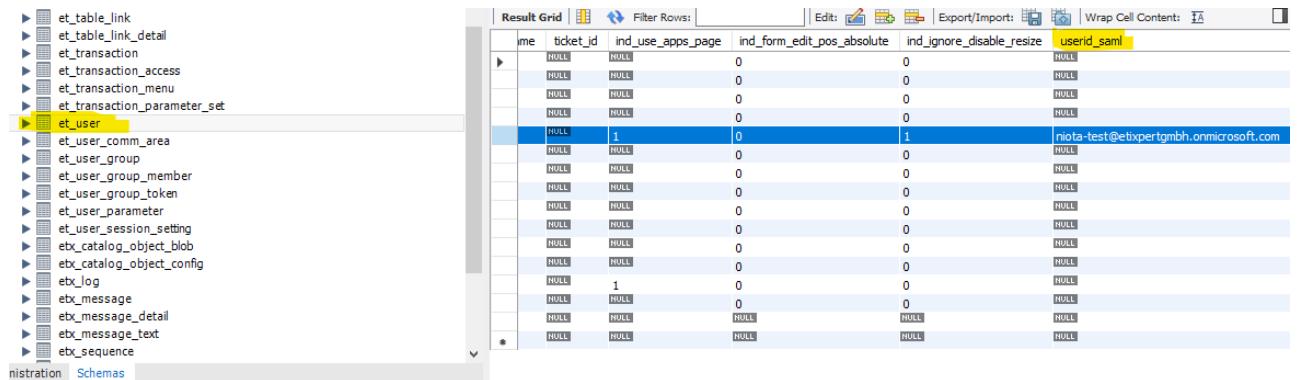
SAML authentication related constants must be copied to the client's `niota/conf/system_defaults.php` file from file `niota/app/conf/system_defaults.php` in the case of an installation update. Following section must exist in file `system_defaults.php`:

```

// --- SAML authentication
// settings affects SAML authentication behavior. SAML authentication method can
// be used only on system level.
// SAML_AUTHENTICATION_ENABLE - enables SAML authentication for users and displays
// related GUI items. Accepted values are: true/false
// SAML_AUTHENTICATION_IDPNAME - identity provider of SAML process.
//                                         Accepted values: SAML_IDP_NAME_AZURE - stands for
// 'Azure', currently the only supported IDP.
define('SAML_AUTHENTICATION_ENABLE',           true);
define('SAML_AUTHENTICATION_IDPNAME',          SAML_IDP_NAME_AZURE);
define('SAML_AUTHENTICATION_FORCESAMLOGOUT',   true);

```

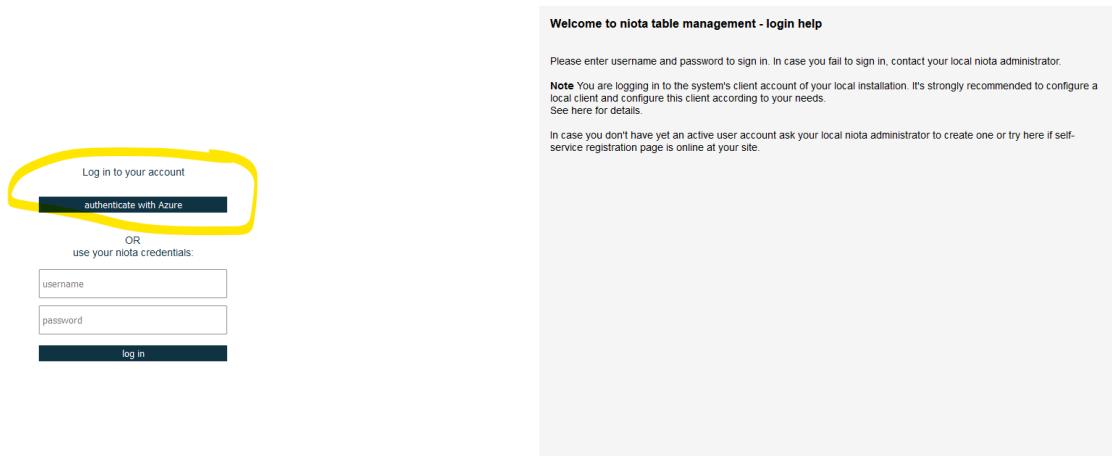
Define belonging SAML id for users in table `et_user`. SAML id is stored in column `userid_saml`. Field references to the user id used for the SAML authentication process. Without this step niota-user id cannot match with SAML-id and user cannot enter niota system.



name	ticket_id	ind_use_apps_page	ind_form_edit_pos_absolute	ind_ignore_disable_resize	userid_saml
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	1	0	1	niota-test@etxpertgmbh.onmicrosoft.com
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	1	0	0	NULL
	NULL	NULL	0	0	NULL
	NULL	NULL	NULL	NULL	NULL
	NULL	NULL	NULL	NULL	NULL

After these steps you can use SAML authentication on niota surface:

## niota dev installation



Welcome to niota table management - login help

Please enter username and password to sign in. In case you fail to sign in, contact your local niota administrator.

**Note** You are logging in to the system's client account of your local installation. It's strongly recommended to configure a local client and configure this client according to your needs.  
See here for details

In case you don't have yet an active user account ask your local niota administrator to create one or try here if self-service registration page is online at your site.

Log in to your account

**authenticate with Azure**

OR

use your niota credentials:

**log in**