TECHNICAL MANUAL

NoPass Application Server Installation

Prepared By:

Identité™, Inc.
3035 Turtle Brooke
Clearwater, Florida 33761 USA
www.Identite.us

Prepared For:

Version: **1.3**
Dated: **13 October 2020**

REVISION HISTORY			
REVISION	REVISION	REVISION	REVISION
0.1	Tatsiana Kachan	Initial template	27 July 2020
1.0	Mohammad Shirazi	Author	
1.1	Artem Senko	Author	
1.2	Artem Senko	Review and update	
1.3	Elena Dubinenko	Review. Copy editing and proofreading.	13 October 2020
1.4	Artem Senko	Review and add information about installation to Windows operation system	

SIGNATURE

This **Technical Manual** documents the request for development of the NoPass Application Server Installation Project to be performed by Identité™, Inc., for **Identité™, Inc.** (“Customer”).

APPROVED BY:

Identité™, Inc. **Date**

PREPARED BY:

Identité™, Inc. **Date**

CONTENTS

ABOUT THIS MANUAL

This chapter contains the following:

- **Purpose and scope**
- **Intended audience**
- **Conventions**

Purpose and scope

This manual provides a detailed overview of the installation of the NoPass application server for conducting password less authentication. You can find all the requirements needed for the successful installation and detailed systematic instruction on the commands and configuration you will need to run the program. This manual is designed to guide you in setting up the environment and successfully installing the NoPass application server.

Aside from the general information chapter provided in the document, the document has two integration setups, which are:

- Web integration: which describes “How to install NoPass application server for Web”. up the environment to run the NoPass application server alongside its demo portal (Preshop) for demonstration purposes, by setting up this environment you will be able to witness how the NoPass password less authentication works on a demo environment. For Web intergration setup we have Test portal with configured API (Preshop) and you can download it from *https://www.identite.us/developers*.

- Radius integration: which is setting up the environment that you will be able to install the NoPass application server on your servers and connect it to your desired portal. Your user will have the ability to authenticate to your services by the help of the NoPass password-less authentication application.

This manual contains the following chapters:

- **About this manual**. Introduces the manual’s scope and proposes, targeted audience, and contents organization.
- **System requirements**. Describes the requirements and preparations needed for a successful installation of the NoPass application server.
- **Infrastructure scheme**. Contains the application installation instructions.
- Error! Reference source not found.. Shows how to activate your NoPass service via the NoPass license and the process of registration to access the NoPass administrator panel.

Intended audience

This manual is designed to be used by IT specialists with basic knowledge of computer networks, databases, operating systems, and the docker container software.

To learn more about our product, visit us at *https://www.identite.us/*.

If you need additional support, email Identitè at *support@identite.us*.

Conventions

The following guidelines present some specific conventions used in this manual.

ELEMENT	DESCRIPTION
\	Used as a line break. Do not type.
<…>	Used to denote variables.

This manual uses the following icons:

ICON	NAME	DESCRIPTION
	Note	Additional information about a subject.
	Warning	Indicated a potential obstacle or condition requiring special attention.

BEFORE YOU BEGIN

This chapter contains the following:

- **Prerequisites**
- **System requirements**
- **Prepare virtual machine**

Prerequisites

To successfully install NoPass, make sure you have the following:

1. An SSL certificate signed by Public Certification Authorities (NOT a self-signed certificate).
2. Access to the NoPass application server from an external network (Assign a public IP address or set up port forwarding on the Virtual Machine where the NoPass application server will be launched).
3. A database.
4. Internet access for the NoPass application and mobile devices.

System requirements

Hardware requirements

- CPU: 1 core or higher
- RAM: 2 GB or more
- HDD: at least 2 GB of free space

Software requirements

The application server is delivered as a docker image. It can run on any server with an existing Docker engine. For more information about the operating systems supported by Docker, go to *https://docs.docker.com/get-docker/*.

- Docker Engine version 19.03.0 or higher
- Docker Compose tool version 1.25.0 or higher

Additional services

To collect and store structured data you must have a database.

Supported databases:

- MySQL
- PostgreSQL
- MS SQL

Certificate requirements

Developing trust between two entities is established via the Secure Socket Layer (SSL) and SSL certificates. The purpose of SSL and certificates is encryption and identification to ensure that the communication exchange between the two parties is secure and trustworthy.

- SSL certificate for domain validation. You must use certificates signed by Public Certification Authorities.

Warning: **DO NOT SUPPORT** a self-signed certificate.

Network requirements

Mobile phone requirements

The mobile phone must have internet access to receive Push Notifications.

If you have a firewall to restrict traffic to or from the Internet, you need to configure it to allow mobile devices to connect with Firebase Cloud Messaging (Push service) for devices on your network to **receive messages.**

Ports to open for **incoming messages**:

- 5228
- 5229
- 5230

- 443

For **outgoing connections**, FCM doesn't provide specific IPs because their IP range changes too frequently and your firewall rules could get out of date impacting your users' experience. Ideally, you will whitelist ports 5228-5230 with no IP restrictions. However, if you must have an IP restriction, you should whitelist all of the IP addresses in the IPv4 and IPv6 blocks listed in Google's ASN of 15169. This is a large list and you should plan to update your rules monthly. Problems caused by firewall IP restrictions are often intermittent and difficult to diagnose.

Choose one of these IP configurations to allow **outgoing connections** (option #1 is preferred):

- No IP restrictions
- All IP addresses contained in the IP blocks listed in Google's ASN of 15169. Do not forget to update this at least once a month.

For more information about Firebase Cloud Messaging, go to *https://firebase.google.com/docs/cloud-messaging/concept-options*.

NoPass server requirements

The NoPass server needs internet access to communicate with third party services. If you have a firewall to restrict traffic to or from the Internet, you need to open the following ports:

For **incoming connections**:

Whitelist the following default ports:

- 443 (HTTPS)
- 1812 (Radius authentication)
- 1813 (Radius accounting)

For **outgoing connections**:

Whitelist the following ports:

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)
- 25,465 or 587 (SMTP)
- 1812 (Radius authentication)
- 1813 (Radius accounting)

To use other ports for these protocols, open them.

Prepare virtual machine

You can use various operating systems for the application that supports Docker installation. We recommend using the Ubuntu Server, which is a variant of the standard Ubuntu you already know, tailored for networks and services that brings along a high technical stability.

This guide describes how to deploy to the Ubuntu server 18.04 and Windows 10 Professional.

Workflow

1. Install OS
2. Allow firewall ports
3. Create DNS records
4. Install docker and docker-compose tool
5. Install and configure a database server

Related topics

System requirements

Install OS

This documentation will show you how to deploy to Ubuntu Server 18.04 and Windows 10 Professional.

You can find the Ubuntu Server installation guide at *https://ubuntu.com/tutorials/install-ubuntu-server#1-overview* and Windows 10 installation guide at *https://www.microsoft.com/en-us/software-download/windows10.*

Allow firewall ports

If your operating system does not have a public IP address, you need to configure a port forwarding to this server.

Procedure

- Ubuntu uses UFW to protect the system. Please see at https://help.ubuntu.com/community/UFW how to open ports on the UFW or disable it with command:

  ```
  $ sudo ufw disable
  ```

- Windows 10 uses Windows Firewall to protect the system. Please see at https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/portal how to open ports on the Windows Firewall or disable it with command:

Related topics

System requirements

Create DNS records

You will have to create DNS records type A which will point to Reverse Proxy server.

You can use the Reverse proxy server you already have. For demo purposes we provide a configured proxy server as a Docker image.

Procedure

1. To find out the public address of the server, run the following command:

Ubuntu Server 18.04

```
$ dig +short myip.opendns.com @resolver1.opendns.com
```

A successful result is as follows:

```
[root@ip-172-28-16-143 ec2-user]# dig TXT +short o-o.myaddr.l.google.com @ns1.google.com
"35.173.198.172"
[root@ip-172-28-16-143 ec2-user]#
```

Windows 10 Professional

```
$ (Invoke-WebRequest -uri "http://ifconfig.me/ip").Content
```

```
Windows PowerShell
PS C:\Users> (Invoke-WebRequest -uri "http://ifconfig.me/ip").Content
82.209.218.13
PS C:\Users>
```

2. Create a DNS binding for the NoPass application server.

Related topics

Install docker and docker-compose tool

Install docker and docker-compose tool

The NoPass application server is delivered as a container image. To deploy it, you should have a Docker Engine to run Docker containers and the Docker-Compose tool to run multi-containers.

Before you begin

Ubuntu Server 18.04

- Uninstall older versions if there are any.

```
$ sudo apt-get remove docker docker-engine docker.io containerd runc
```

Windows 10 Professional

- Uninstall older versions Docker Desktop

To uninstall Docker Desktop from your Windows machine:

1. From the Windows Start menu, select Settings > Apps > Apps & features.
2. Select Docker Desktop from the Apps & features list and then select Uninstall.
3. Click Uninstall to confirm your selection.

Procedure

Ubuntu Server 18.04

To install a new version of docker using the repository, do the following:

1. Update the apt package index.

```
$ sudo apt-get update
```

2. Install packages to allow apt to use the repository over HTTPS.

```
$ sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    gnupg-agent \
```

3. Add Docker's official GPG key.

```
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add
```

4. Verify that you now have the key with the fingerprint 9DC8 5822 9FC7 DD38 854A E2D8 8D81 803C 0EBF CD88.

```
$ sudo apt-key fingerprint 0EBFCD88
```

A successful result is as follows:

```
root@ubuntu01:~# sudo apt-key fingerprint 0EBFCD88
pub   rsa4096 2017-02-22 [SCEA]
      9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid           [ unknown] Docker Release (CE deb) <docker@docker.com>
sub   rsa4096 2017-02-22 [S]
```

5. Add a stable repository.

```
$ sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
   $(lsb_release -cs) \
```

6. Update the apt package index again.

```
$ sudo apt-get update
```

7. Install the latest stable version of Docker Engine Community and container.

```
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
```

For more information about installing Docker Engine on Ubuntu Server, go to *www.docs.docker.com/engine/install/ubuntu/.*

8. Verify the installed docker version.

```
$ sudo docker -v
```

A successful result is as follows:

```
root@ubuntu01:~# sudo docker -v
Docker version 19.03.2, build 6a30dfc
```

9. To verify that the Docker Engine Community is installed correctly, run the hello-world image.

```
$ sudo docker run hello-world
```

A successful result is as follows:

```
root@ubuntu01:~# sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
1b930d010525: Pull complete
Digest: sha256:fc6a51919cfeb2e6763f62b6d9e8815acbf7cd2e476ea353743570610737b752
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/

root@ubuntu01:~#
```

10. To download the current stable release of Docker-Compose, run the following command:

```
$ sudo curl -L "https://github.com/docker/compose/releases/down-
load/1.26.0/docker-compose-$(uname -s)-$(uname -m)" -o /usr/lo-
cal/bin/docker-compose
```

A successful result is as follows:

```
root@ubuntu01:~/git/MAPD# sudo curl -L "https://github.com/docker/compose/releases/download/1.26.0/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   651  100   651    0     0   3304      0 --:--:-- --:--:-- --:--:--  3304
100 11.6M  100 11.6M    0     0   214k      0  0:00:55  0:00:55 --:--:--  302k
root@ubuntu01:~/git/MAPD#
```

11. Create a symbolic link to usr/bin or any other directory in your path.

```
$ sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
```

12. Apply executable permissions to the binary.

```
$ sudo chmod +x /usr/local/bin/docker-compose
```

13. Verify the installed docker-compose version.

```
$ sudo docker-compose --version
```

A successful result is as follows:

```
root@ubuntu01:~# sudo docker-compose --version
docker-compose version 1.26.0, build d4451659
root@ubuntu01:~#
```

Windows 10 Professional

To install a new version of docker for Windows you will need to download Docker Desktop for Windows from Docker hub and install it. It contains Docker and Docker-compose tools. Please see at https://docs.docker.com/docker-for-windows/install/.

Related topics

Create DNS records
Install and configure a database server

Install and configure a database server

The application requires a database in which data is stored.

If you do not have an installed database server, install and configure one of the following:

- How to install and configure MySQL
- How to install and configure PostgreSQL
- How to install and configure Microsoft SQL server

Related topics

System requirements

How to install and configure MySQL

The following settings are for MySQL v.8.*

Before you begin

- Install the database server. For installation instructions, go to *https://dev.mysql.com/doc/mysql-installation-excerpt/5.7/en/*.

Procedure

To create the database and user accounts and set the following user permissions, do the following:

1. To create the database using the 'mysql' command line client, the first log into MySQL:

```
$ mysql -u root -p
```

2. Enter the password that you set during the installation.

   Successful log into MySQL is as follows:

```
root@6bdb1ee77efe:/# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.19 MySQL Community Server - GPL

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

3. Create a new database and name it 'identite' or any other name of your choice.

```
mysql>  CREATE  DATABASE  nopass  DEFAULT  CHARACTER  SET  utf8mb4  COLLATE
```

   Successfully created database is as follows:

```
mysql> CREATE DATABASE nopass DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.00 sec)

mysql>
```

4. Create a new MySQL user account. Replace the placeholder **identiteuser** with your intended new username, and placeholder **p@$$w0rd** with the user password.

```
mysql> CREATE USER ' identiteuser '@'%' IDENTIFIED BY 'p@$$sw0rd';
```

   Successfully created MySQL user is as follows:

```
mysql> CREATE USER ' identiteuser '@'%' IDENTIFIED BY 'p@$$sw0rd';
Query OK, 0 rows affected (0.01 sec)

mysql>
```

5. Grant all privileges to a user account for the database.

```
mysql> GRANT ALL PRIVILEGES ON nopass.* TO 'identiteuser'@'%';
```

Successfully granted privileges are as follows:

```
mysql> GRANT ALL PRIVILEGES ON nopass.* TO 'identiteuser'@'%';
Query OK, 0 rows affected (0.01 sec)

mysql>
```

Parent topic

Install and configure a database server

How to install and configure PostgreSQL

The following settings are for PostgreSQL v.11.*

Before you begin

- Install the database server. For installation instructions, go to *www.postgresql.org/download/*.

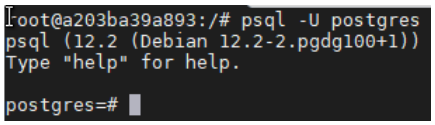
Procedure

To create a database and user account and set user permissions via console, follow these steps.

1. To create a database using the 'PostgreSQL' command line client, first log into PostgreSQL.

```
$ psql -U postgres
```

2. Enter the password that you set during installation.
   Successful log into PostgreSQL is as follows:



3. Create a new PostgreSQL user account and replace the placeholder *identiteuser* with your intended new username, and placeholder *p@$$sw0rd* with the user password.

```
postgres=# CREATE USER identiteuser WITH PASSWORD 'p@$$sw0rd';
```

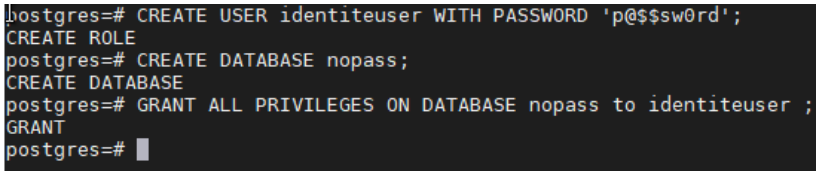
4. Create a new database and name it *nopass* (substitute with another name if required).

```
postgres=# CREATE DATABASE nopass;
```

5. Grant all privileges to a user account for the database.

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE nopass to identiteuser ;
```

   The successfully created user, database and granted permissions look as follows:



6. To allow network access, do the following:
   a. Edit configuration file:

```
$ sudo vim /etc/postgresql/11/main/postgresql.conf
```

b. Add the following line under the CONNECTIONS AND AUTHENTICATION section. You can also specify the server IP address or all Addresses.

```
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'

#listen_addresses = 'localhost'         # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
port = 5432                             # (change requires restart)
max_connections = 100                   # (change requires restart)
#superuser_reserved_connections = 3     # (change requires restart)
unix_socket_directories = '/var/run/postgresql' # comma-separated list of directories
                                        # (change requires restart)
#unix_socket_group = ''                 # (change requires restart)
#unix_socket_permissions = 0777         # begin with 0 to use octal notation
                                        # (change requires restart)
#bonjour = off                          # advertise server via Bonjour
                                        # (change requires restart)
#bonjour_name = ''                      # defaults to the computer name
                                        # (change requires restart)
```

Parent topic

Install and configure a database server

How to install and configure Microsoft SQL server

The following settings are for MS SQL v.2014.

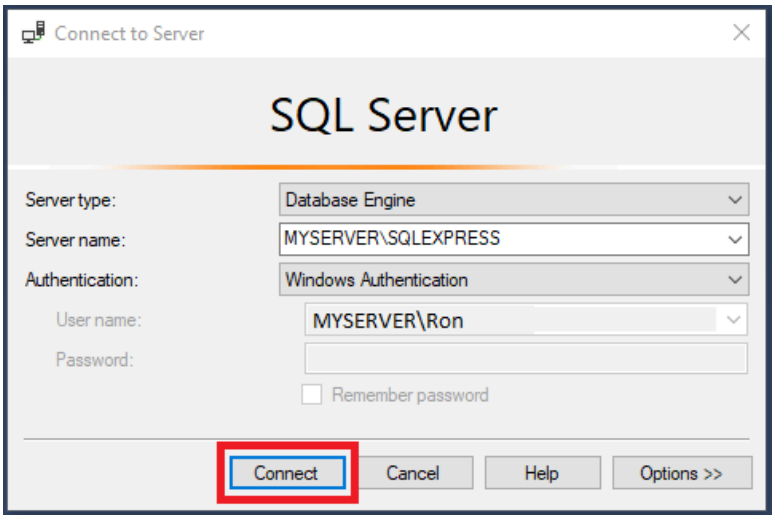
Before you begin

Install the database server. For installation instructions, go to *www.docs.microsoft.com/en-us/sql/getting-started/quick-start-installation-of-sql-server-2014?view=sql-server-2014*.

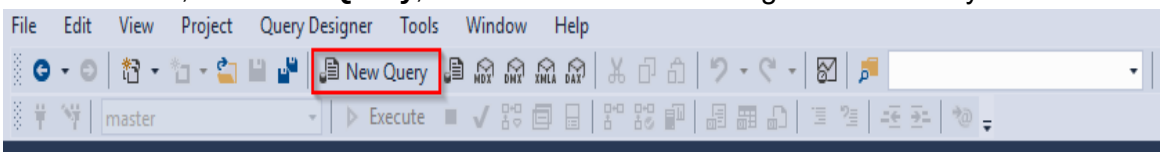
Procedure

To create a database and user account, and set user permissions via SQLQuery, do the following:

1. Open SSMS and connect to SQL Server.



2. On the ribbon, click **New Query**, to create a database using the 'SQLQuery.'

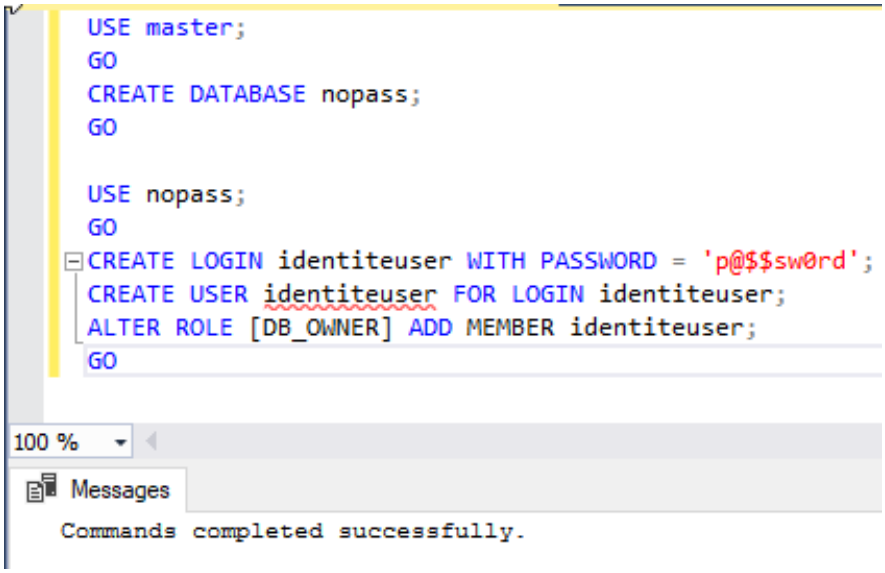


3. Create a new database named <Identite> or any other name of your choice.
4. Create a new user account and replace the placeholder *identiteuser* with your intended new username, and placeholder *p@$$sw0rd* with the password.
5. Grant all privileges to the user account for the database.

```
USE master;
GO
CREATE DATABASE nopass;
GO

USE nopass;
                                    GO
CREATE LOGIN identiteuser WITH PASSWORD = 'p@$$sw0rd';
CREATE USER identiteuser FOR LOGIN identiteuser;
ALTER ROLE [DB_OWNER] ADD MEMBER identiteuser;
GO
```

The successfully created user, database, and granted permissions look as follows:



Parent topic

Install and configure a database server

SERVER DEPLOYMENT

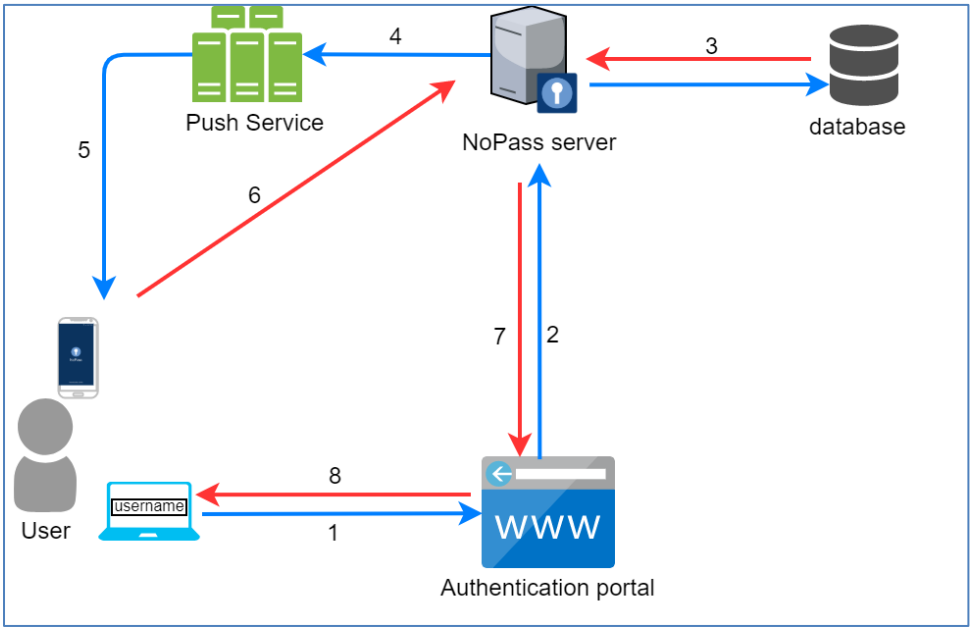
This chapter contains the following:

- **Infrastructure scheme**
- **Install the NoPass application server**
- **Configure the reverse proxy**
- **Launch the NoPass application server**
- **Stop the NoPass application server**
- **Update the application server**

Infrastructure scheme

Web portal integration scheme: shows the location of our NoPass server in the network structure and the different connections between the NoPass server and its Mobile application with the different elements of your network to provide you the ability to authenticate your users with the help of NoPass.

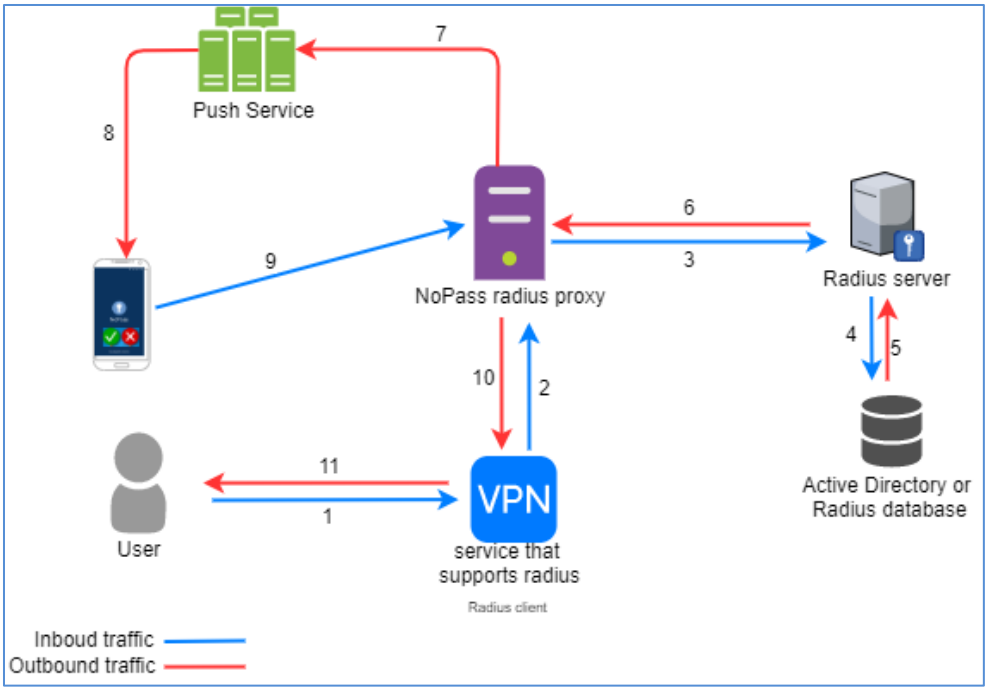
Web portal integration scheme



1. Initiation of authentication for the application.
2. Authentication portal sends an authentication request to the NoPass application server.
3. The NoPass server checks the user in the database.
4. Generates and sends push request to Push service.
5. The push service receives the push request and sends notification to the user device.
6. Send authentication response from the user device to the NoPass application server.
7. The NoPass server sends an authentication response to the Authentication portal.
8. Access to the service is provided or not.

Radius integration scheme

Radius integration scheme: here you can see how the NoPass server acts a RADIUS proxy server, its location in the network structure and different connections between the NoPass server and its Mobile application with the different elements of your network.



1. Initiating primary authentication to the application or service.
2. The application or server sends an authentication request to the NoPass proxy server.
3. The NoPass proxy server redirects the authentication request to the Radius server.
4. The Radius server does primary authentication.
5. Intercepts response from the Radius server and secondary authentication via NoPass radius proxy.
6. Generate and send a push request to the Push service.
7. The Push service receives the push request and sends notification to the user device.
8. Sends authentication response from the user device to the NoPass radius proxy.
9. The NoPass radius proxy sends an authentication response to the application or service.
10. Access to application/service is provided or not.

Install the NoPass application server

This chapter contains the following:

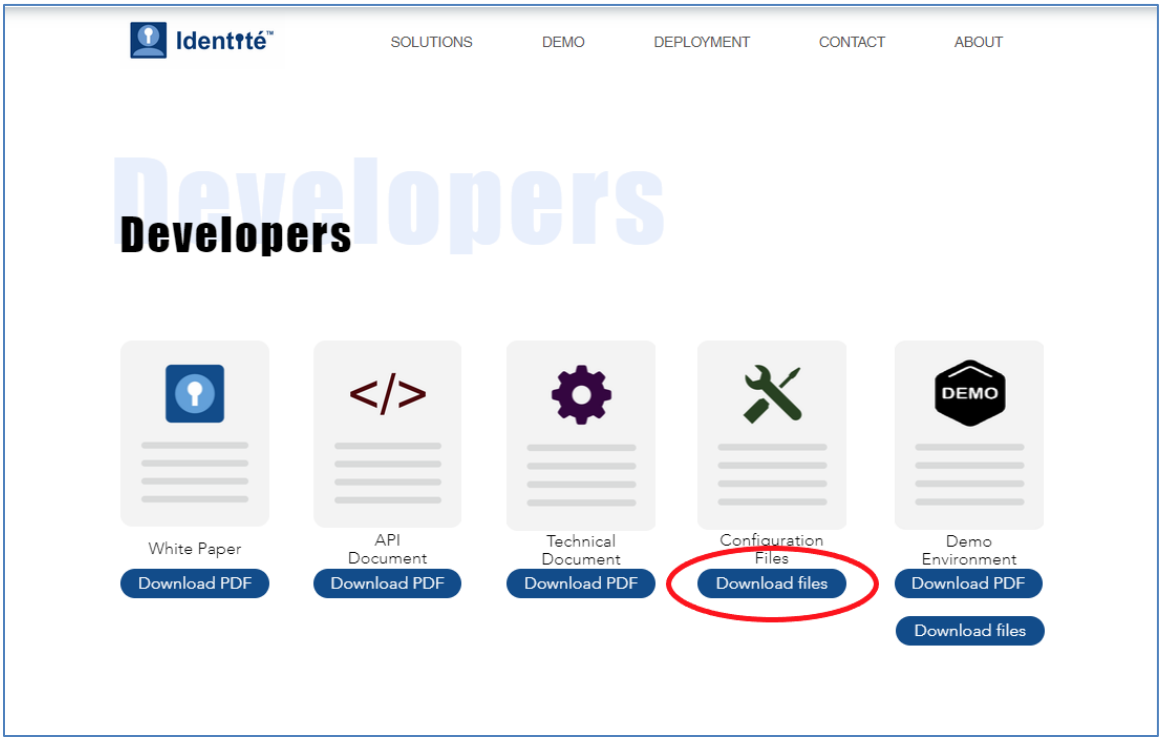
- **Prepare files**
- **NoPass server environment variables**

Prepare files

We provide pre-configured configuration files to help you install the NoPass application server.

Before you begin

- Download the configuration files from https://www.identite.us/developers.



Note: The login and password are sent to you by our team.

Procedure

1. Copy the link, download the zip archive to your server, and unzip.

Ubuntu Server 18.04

```
$ curl –LOJ https://download_link (change the link)
```

Unpacking the archive:

```
$ tar -xzvf NoPass.tar.gz
```

Unpacked files look as follows:

```
root@ubuntu01:~/NoPass# tar -xzvf NoPass.tar.gz
NoPass/
NoPass/docker-compose.yml
NoPass/nginx/
NoPass/nginx/nginx.conf
NoPass/nginx/certs/
NoPass/nginx/conf.d/
NoPass/nginx/conf.d/nopass.conf
NoPass/nopass.env
root@ubuntu01:~/NoPass#
```

Windows 10 Professional

```
$ Invoke-WebRequest -Uri https://download_link -OutFile c:\NoPass.tar.gz (change the link)
```

Unpacking the archive using 7zp. Unpacked files look as follows:

```
PS C:\Users\Administrator\NoPass> tree /f
Folder PATH listing
Volume serial number is 2E61-1B32
C:.
│   docker-compose.yml
│   nopass.env
│
└───nginx
    │   nginx.conf
    │
    ├───certs
    └───conf.d
            nopass.conf

PS C:\Users\Administrator\NoPass>
```

File description:

- **nopass.env**—environment variable file for the NoPass application server.
- **docker-compose.yml**—a configuration file to run multi-container applications.
- **nginx/conf.d/nopass.conf**—nginx server context.
- **nginx/nginx.conf**—default nginx configuration file.

2. Change variables in the **nopass.env** configuration file. The environment variables you can see below.
3. Change the **docker-compose.yml** configuration file if you use the NoPass application server without nginx. You need to change the expose port for nopass directive to publish port. Do the following:
   a. Expose port in the Docker bridge network.

   ```
   expose:
         - 80
   ```

   b. Publish a container's port to the host. You can use any other free port instead 8001.

```
ports:
    - 8001:80
```

Related topics

NoPass server environment variables
Configure the reverse proxy

NoPass server environment variables

The application will not start without the required variables. The variables with mask **EmailSettings** required to configure sending mail to your administrator.

Environment variable	Value (example)	Description
Required variables		
MAPD_DatabaseSettings__DbConnectionType	MySql	Type of database. You can use MySql, Postgre, MsSql
MAPD_DatabaseSettings__ConnectionString **OR** **MAPD_DatabaseSettings__Server=nopass_db** **MAPD_DatabaseSettings__Port=3306** **MAPD_DatabaseSettings__DatabaseName=nopass-server** **MAPD_DatabaseSettings__UserId=root** **MAPD_DatabaseSettings__Password=nopassroot!**	nopass_db;Database=nopass-server;User Id=root;password=nopassroot!;	Database connection string. You can also use a split database connection string, see below. Supported databases: MySQL, Postgre, MsSQL.
MAPD_ServerUrl	*https://nopass.example.com/*	URL of the NoPass application
Optional global variables		
MAPD_EmailSettings__Host	smtp.gmail.com	URL of an SMTP server
MAPD_EmailSettings__Port	587	SMTP port
MAPD_EmailSettings__EnableSSL	true	enable or disable SSL
MAPD_EmailSettings__EmailFrom	client.support@gmail.com	mail sender
MAPD_EmailSettings__UserName	login@gmail.com	login for mailbox
MAPD_EmailSettings__Password	pa$$w0rd	password for mailbox
MAPD_EmailSettings__Email	admin.nopass@gmail.com	recipient address
MAPD_EmailSettings__CC	sysadmins@gmail.com	copy address
MAPD_EmailSettings__Subject	Report issue	email subject
Optional variables for radius		
MAPD_RadiusProxySettings__AdminId	radiusadmin	Default login for radius administrator
MAPD_RadiusProxySettings__AdminPwd	radiuspassword	Default password for radius administrator

Related topics

NoPass server environment variables

Configure the reverse proxy

A reverse proxy terminates the HTTP request and forwards it to the application. We recommend using the Nginx server as a reverse proxy server. It will have to proxy requests to the NoPass application server and it can perform the decryption of requests and encryption of responses that NoPass application server would otherwise have to do. You can use your reverse proxy server or our pre-configured Nginx with the NoPass application server.

Before you begin

- Open the Nginx configuration file for the NoPass application server.

```
upstream nopass {
        server nopass_server:80;
}
server {
    listen 443 ssl;
    server_name nopass.example.com;
    location / {
        proxy_pass  http://nopass;
        proxy_redirect          off;
        proxy_http_version      1.1;
        proxy_set_header        Upgrade $http_upgrade;
        proxy_set_header        Connection keep-alive;
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        client_max_body_size    10m;
        client_body_buffer_size 128k;
        proxy_connect_timeout   300;
        proxy_send_timeout      300;
        proxy_read_timeout      300;
        proxy_buffers           32 4k;
    }
    ssl_certificate     /etc/certs/nopass.crt;
    ssl_certificate_key /etc/certs/nopass.key;
    ssl_ciphers              EECDH:+AES256:RSA+AES:RSA+3DES:!NULL:!RC4:!ARIA!CAMELLIA:!AES256-
SHA:!AES128-SHA;
    ssl_protocols       TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;
    ssl_session_cache   shared:SSL:10m;
    ssl_session_timeout 10m;
    ssl_stapling on;
    ssl_stapling_verify on;
    resolver 8.8.8.8 8.8.4.4 valid=300s;
    resolver_timeout 10s;
    add_header          Strict-Transport-Security: "max-age=63072000; includeSubDomains; pre-
    load";
    add_header          X-Content-Type-Options nosniff;
    add_header          X-XSS-Protection "1; mode=block";
    add_header          X-Frame-Options SAMEORIGIN;
    add_header          Referrer-Policy 'same-origin';
    add_header          Expect-CT 'enforce; max-age=3600';
    add_header          Content-Security-Policy "default-src https:; connect-src https:; font-
src https: data:; frame-src https:; frame-ancestors https:; img-src https: data:; media-src
https:; object-src https:; script-src 'unsafe-inline' 'unsafe-eval' https:; style-src 'unsafe-
inline' https:;";}
```

Procedure

1. Change your path to the NoPass application server.

```
server nopass_server:80;
```

Warning: Do not touch this directive if you want to use the installed Nginx server with the NoPass server automatically.

2. Change the DNS name that you created during creating DNS records.

```
server_name nopass.example.com;
```

3. Copy the SSL certificate and key in the directory with the nginx server, change the path for them. If you use our Nginx server, copy the certificate to nginx/certs and change certificate names.

```
ssl_certificate     /etc/certs/nopass.crt;
ssl_certificate_key /etc/certs/nopass.key;
```

Related topics

Create DNS records

Launch the NoPass application server

Before you begin

- To download Docker images, log in to a Docker registry **hubdocker.identite.us**. Enter the credentials that we provided you.

```
$ docker login hubdocker.identite.us
```

Successful log into the Identité™ Docker registry looks as follows:

Ubuntu Server 18.04

```
root@ubuntu01:~/NoPass# docker login hubdocker.identite.us
Authenticating with existing credentials...
WARNING! Your password will be stored unencrypted in /home/senko/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
root@ubuntu01:~/NoPass#
```

Windows 10 Professional

```
Windows PowerShell
PS C:\Users\admin> docker login hubdocker.identite.us
Username: mars
Password:
Login Succeeded
PS C:\Users\admin>
```

Procedure

1. Enter the directory with the application installed. Do one of the following:
   - To start the production environment with Nginx server, run the following command:

```
$ sudo docker-compose up -d
```

A successful result is as follows:

Ubuntu Server 18.04

```
root@ubuntu01:~/NoPass_Production# docker-compose up -d
Creating network "nopass_production_network" with driver "bridge"
Creating network "nopass_production_nginx_rp" with driver "bridge"
Creating nopass_nginx_rp ... done
Creating nopass_server   ... done
root@ubuntu01:~/NoPass_Production# docker ps
CONTAINER ID        IMAGE                                  COMMAND                  CREATED             STATUS              PORTS                                      NAMES
f79d714d5043        nginx:1.17.5-alpine                    "nginx -g 'daemon of…"   4 seconds ago       Up 1 second         0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp   nopass_nginx_rp
3d4435e533d1        hubdocker.identite.us/nopass:latest    "dotnet Mapd.Server.…"   4 seconds ago       Up 2 seconds        80/tcp                                     nopass_server
root@ubuntu01:~/NoPass_Production#
```

Windows 10 Professional

```
PS C:\NoPass> docker-compose up -d
Creating network "nopass_nginx_rp" with driver "bridge"
Starting nopass           ... done
Creating nopass_nginx_rp ... done
```

   - To start the production environment without Nginx server, run the following command:

```
$ sudo docker-compose up -d nopass
```

A successful result is as follows:

Ubuntu Server 18.04

```
root@ubuntu01:~/NoPass_Production# docker-compose up -d server
Creating network "nopass_production_network" with driver "bridge"
Creating network "nopass_production_nginx_rp" with driver "bridge"
Creating nopass_server ... done
root@ubuntu01:~/NoPass_Production# docker ps
CONTAINER ID        IMAGE                                  COMMAND                  CREATED             STATUS              PORTS                   NAMES
708babe9e352        hubdocker.identite.us/nopass:latest    "dotnet Mapd.Server.…"   4 seconds ago       Up 3 seconds        0.0.0.0:8001->80/tcp    nopass_server
root@ubuntu01:~/NoPass_Production#
```

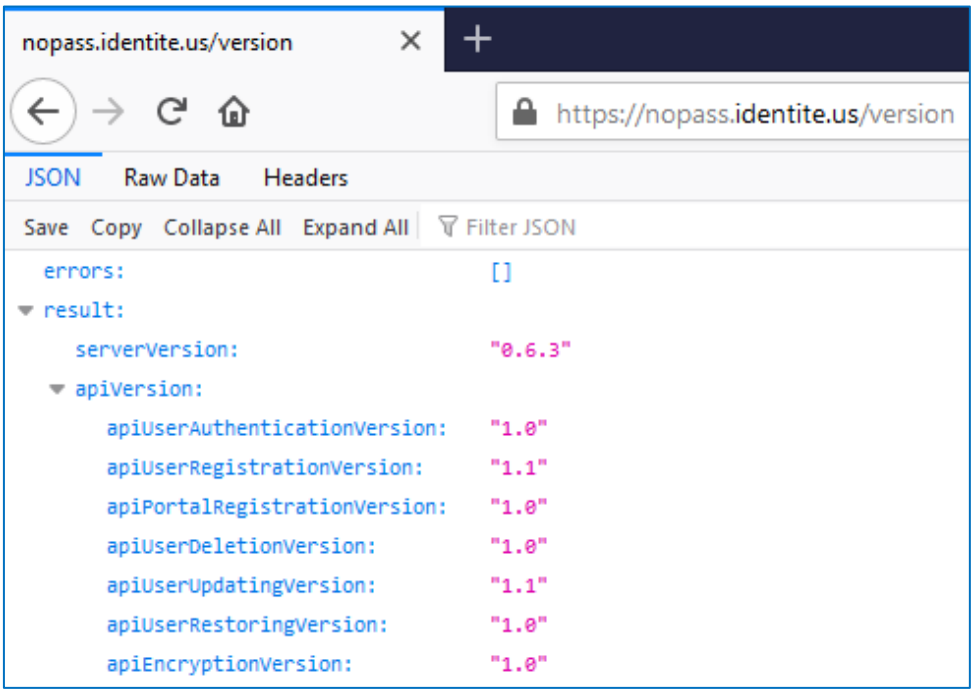
Windows 10 Professional

```
Creating network "nopass_network" with driver "bridge"
Creating network "nopass_nginx_rp" with driver "bridge"
Creating nopass ... done
PS C:\NoPass>
```

2. Check the running application in the browser using the following link:

```
https://SERVER_URL:port/version
```

Server status output example:



3. Register the portal on the NoPass application server.

Related topics

Configure the reverse proxy
Stop the NoPass application server

Stop the NoPass application server

Procedure

1. To stop the application, run the command:

```
$ sudo docker-compose down
```

A successful result for the environment with the Nginx server is as follows:

Ubuntu Server 18.04

```
root@ubuntu01:~/NoPass/NoPass# docker-compose down
Stopping nopass_nginx_rp ... done
Stopping nopass          ... done
Removing nopass_nginx_rp ... done
Removing nopass          ... done
Removing network nopass_network
Removing network nopass_nginx_rp
root@ubuntu01:~/NoPass/NoPass# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS               NAMES
root@ubuntu01:~/NoPass/NoPass#
```

Windows 10 Professional

```
Administrator: Windows PowerShell
PS C:\NoPass> docker-compose down
Stopping nopass_nginx_rp ... done
Stopping nopass          ... done
Removing nopass_nginx_rp ... done
Removing nopass          ... done
Removing network nopass_network
Removing network nopass_nginx_rp
PS C:\NoPass>
```

Related topics

Launch the NoPass application server
Update the application server

Update the application server

Procedure

To update the application server, do the following:

1. Pull a new image from the repository.
2. Restart the server.
3. Run one of the following commands:
    - For the environment with the Nginx server:

      ```
      $ sudo docker-compose pull && docker-compose up -d
      ```

    - For the environment without the Nginx server:

      ```
      $ sudo docker-compose pull && docker-compose up -d nopass
      ```

Related topics

Stop the NoPass application server
Launch the NoPass application server

IDENTITY PROVIDER AND SP MANAGEMENT

This chapter contains the following:

- **How to install Keycloak**
- **Set up the NoPass extension**
- **Set up service providers with Keycloak**

How to install Keycloak

The NoPass application has an ability to work with the Keycloak Identity and Access Management as an extension. In this manual, we will describe how to install Keycloak on Docker with MySQL database. For additional installation options, go to *https://www.keycloak.org/getting-started.*

Keycloak needs to persist and collect data to a database. Keycloak comes with its own embedded Java-based relational database called H2, but Keycloak recommends replacing it with a more production ready external database.

Prerequisites

SYSTEM REQUIREMENTS:

- At least 512M of RAM
- At least 1G of diskspace

SOFTWARE REQUIREMENTS:

- Docker Engine. For installation instructions, go to *https://docs.docker.com/engine/install/.*
- *Docker-Compose tool. For installation instructions, go to https://docs.docker.com/compose/install/.*
- A shared external database like PostgreSQL, MySQL, Oracle, etc. If you want to run in a cluster, Keycloak requires an external shared database. For more information about databases for Keycloak, go to *https://www.keycloak.org/docs/latest/server_installation/index.html#database-configuration.*

NETWORK REQUIREMENTS:

- 80/443 (HTTP/HTTPS). For additional network bindings, go to *https://www.keycloak.org/docs/latest/server_installation/index.html#_bind-address.*

Procedure

1. Create a database.
2. Create a directory where you can copy the extension and set permissions for it.

```
$ sudo mkdir extensions
$ sudo chmod -R 775 extensions/
```

3. Download the extension from https://nexus-dev.identite.us/repository/maven-public/ and copy it to the directory you created in Step 2.

Note: We provide the following docker-compose configuration file for launching Keycloak:

```
version: '3'
services:

  keycloak:
      image: quay.io/keycloak/keycloak:11.0.1
      environment:
        DB_VENDOR: MYSQL
        DB_ADDR: mysql_address
        DB_DATABASE: keycloak
        DB_USER: keycloak
        DB_PASSWORD: password
        KEYCLOAK_USER: useradmin
        KEYCLOAK_PASSWORD: userpassword
      ports:
        - 8080:8080
      volumes:
        - ./extensions:/opt/jboss/keycloak/standalone/deployments
```

4. To see the status of the container, run the command:

```
docker ps
```

A successful result looks as follows:

```
root@ubuntu01:~/keycloak# docker ps
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STATUS              PORTS                                      NAMES
19876505a1b6        quay.io/keycloak/keycloak:11.0.1   "/opt/jboss/tools/do…"   About a minute ago  Up About a minute   0.0.0.0:8080->8080/tcp, 8443/tcp           keycloak-11.0.1
```

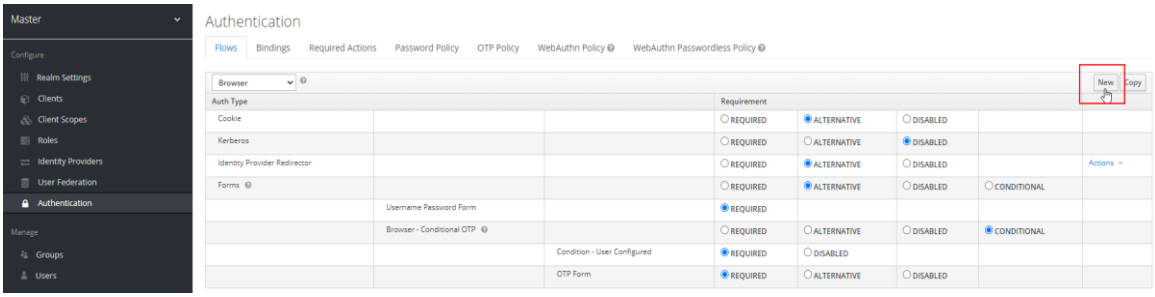
Related topics

Set up the NoPass extension
Set up service providers with Keycloack

Set up the NoPass extension

Procedure

1. From the administrative console of your Keycloak server select a realm and click **New** to create a new Authentication flow.

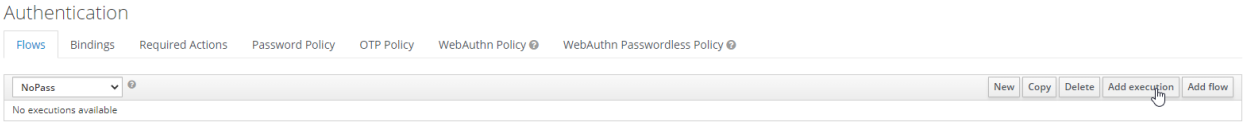


2. To identify the flow, enter the alias name.

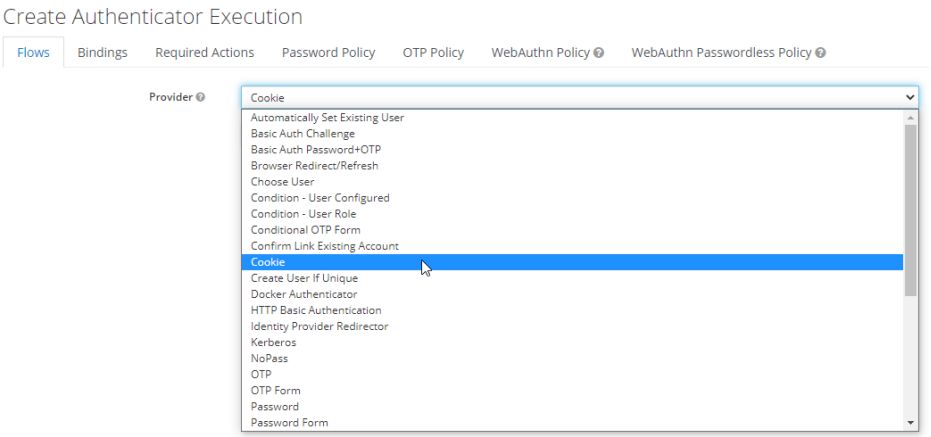
   Note: Make sure that the Alias field is set to “NoPass”.

3. In the **Top Level Flow Type** box, select **generic**, and then click **Save**.

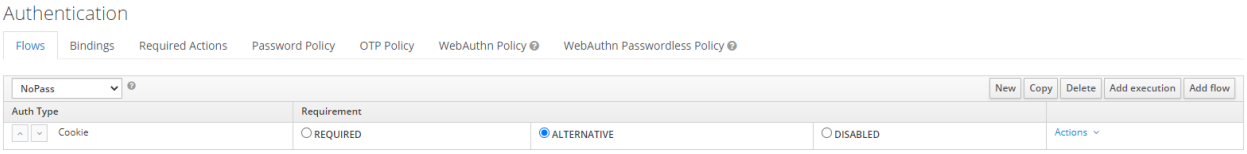
4. After you have successfully created the new flow, you need to add a new execution. In the **Flows** tab, select **Add execution**.



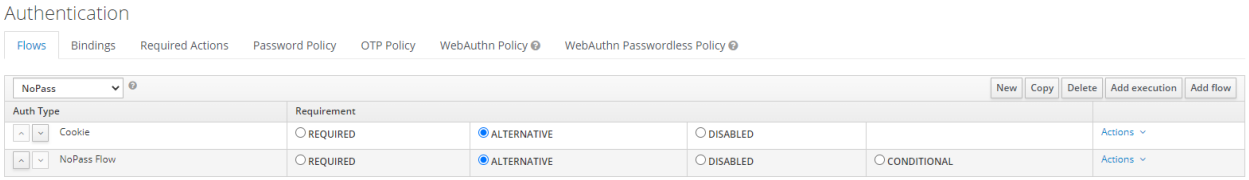
5. From the **Provider** list, select **Cookies**.



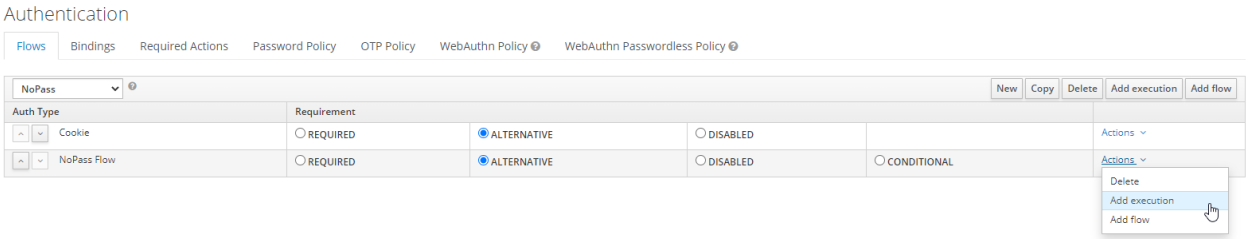
6. Select **ALTERNATIVE** to enable cookies as an alternative authentication method.

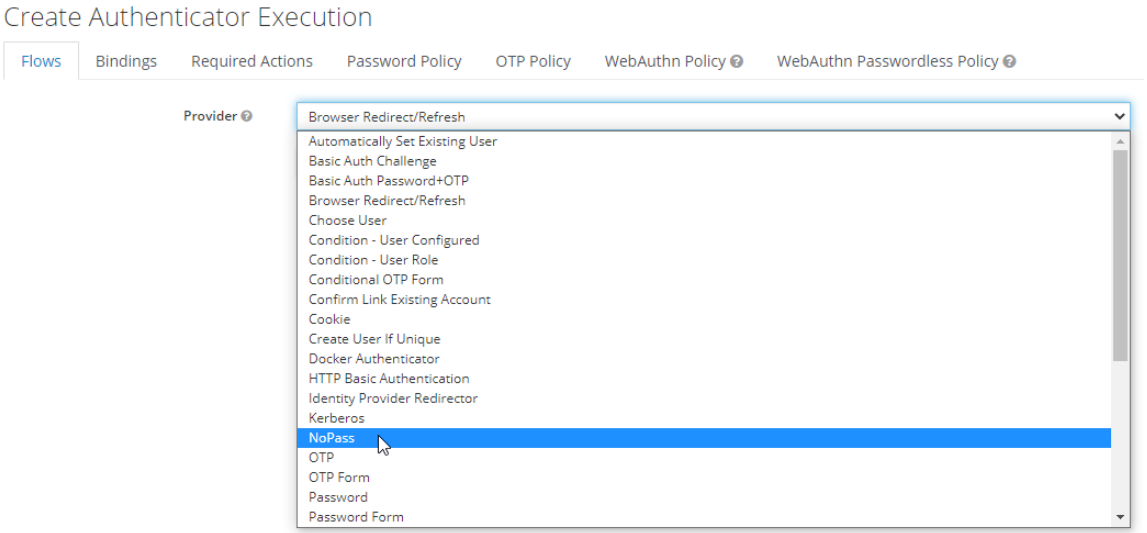


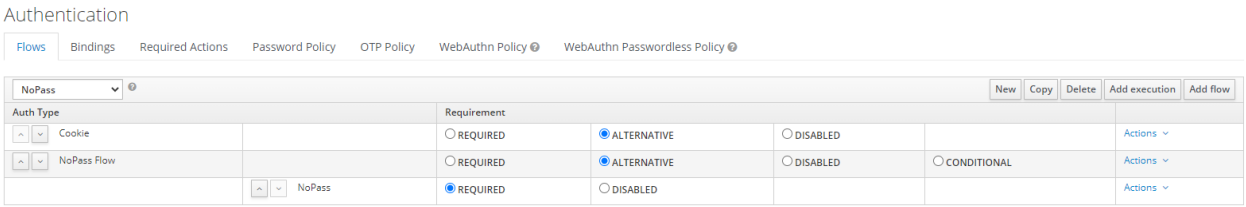
7. Add a new flow for NoPass Authentication and enable it as an alternative authentication method.



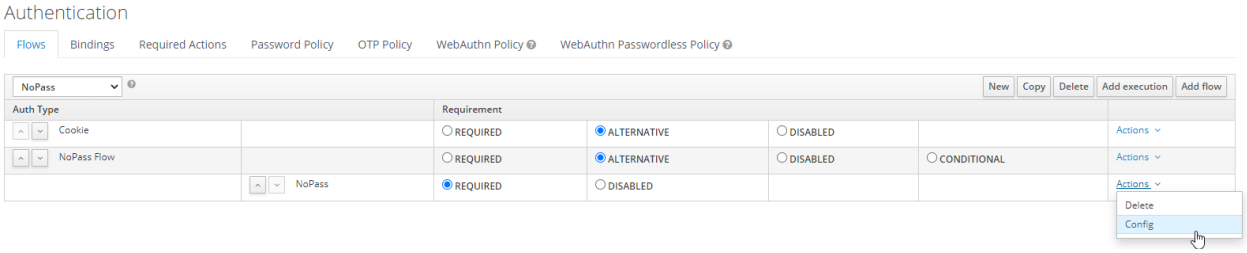
8. Under **Actions**, select **Add execution** to add the NoPass execution to the **NoPass Form** flow, and then select **REQUIRED**.







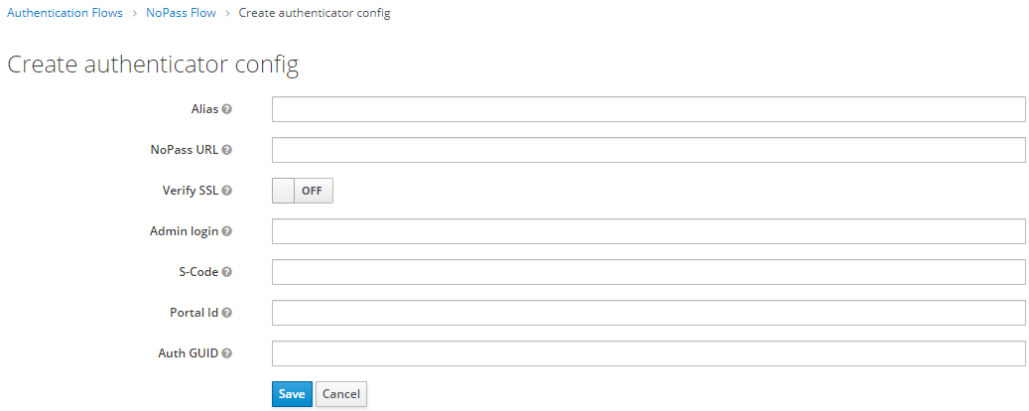
9. Under **Actions**, select **Config** to configure the extension.



10. In the **Create authenticator config** dialog, enter the following parameters for the NoPass server, that you have installed earlier:
    - **Alias**—configuration name.

Note: Make sure that the Alias field is set to “NoPass”.

- **NoPass URL**—the URL of the NoPass server
- **Verify SSL**—turned off
- **Admin login**—login that is allowed to the Administrative panel
- **S-Code**—secret key necessary for the Identité administration during Keycloak registration
- **Portal ID**—ID of the Identité Provider. Generates and filles automatically
- **Auth GUID**—GUID for authentication. Generates and filles automatically



Set up service providers with Keycloak

You will need to configure Keycloak for future work with various service providers. For successful integration with NoPass, you should use those service providers that support SAML or OpenID. However, before configuring a service provider, it is necessary to configure both Keycloak and a service provider.

Before you begin

Find the Keycloak metadata at *https://{KeycloakURL}/auth/realms/{Realm}/protocol/saml/descriptor*.

Procedure

1. Extract the IdP signing certificate within the Keycloak metadata.

2. Copy the **dsig: X509Certificate** value to any text editor and save it as a .crt file. The certificate will contain the following three lines:

```
-----BEGIN CERTIFICATE-----
{Certificate}
-----END CERTIFICATE-----
```

Related topics

SalesForce: How to configure SAML for SSO
Confluence: How to configure SAML for SSO
AD FS as a service provider

SalesForce: How to configure SAML for SSO

Before you begin

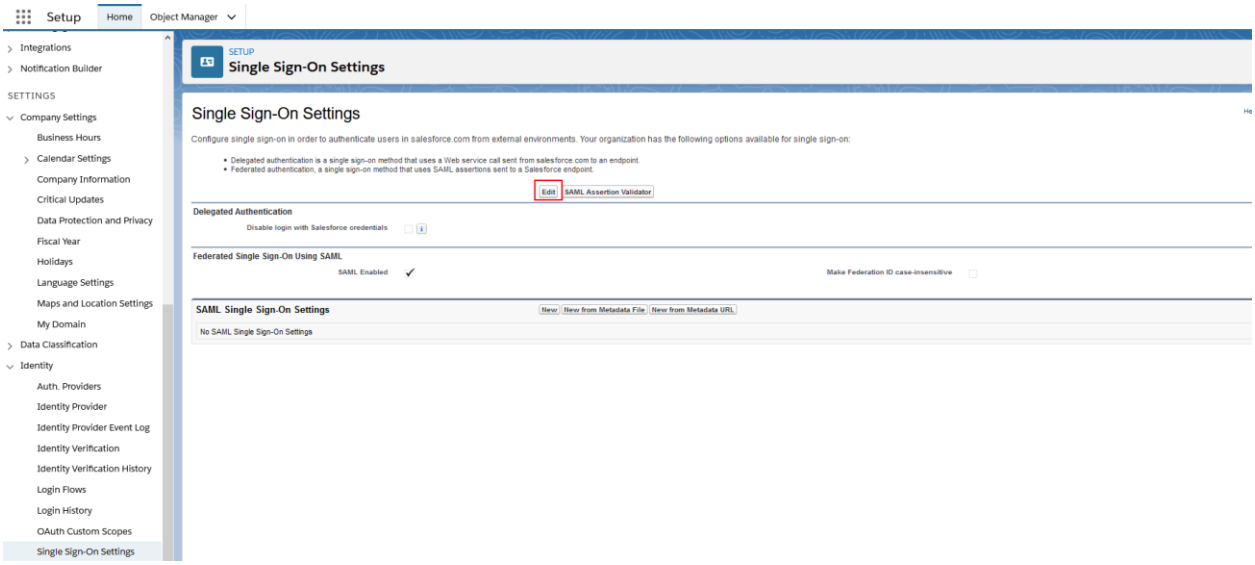
Salesforce offers the following ways to use SSO:

- Federated authentication using Security Assertion Markup Language (SAML).
- Federated authentication using OpenID Connect protocol.

Procedure

To configure SAML for SSO, do the following:

1. In Salesforce, in the **Setup** tab, in the **Quick Find** box, enter *Single Sign-On Settings*, select **Single Sign-On Settings**, and then click **Edit**.

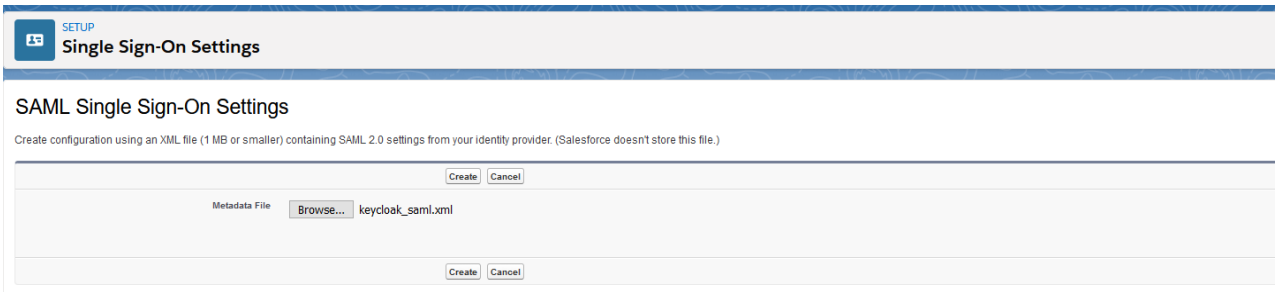


2. To view SAML single sign-on settings, select **SAML Enabled**, and click **Save**.

3. In SAML Sign-On Settings, click one of the following buttons to create a configuration:

   - **New**—to specify all settings manually.
   - **New from Metadata file**—Import SAML 2.0 settings from an XML file from your identity provider. This option reads the XML file and uses it to complete as many of the settings as possible.

- **New from Metadata URL**—Import SAML 2.0 settings from a public URL. This option reads the XML file at a public URL and uses it to complete as many of the settings as possible. The URL must be added to Remote Site Settings to access it from your Salesforce org.



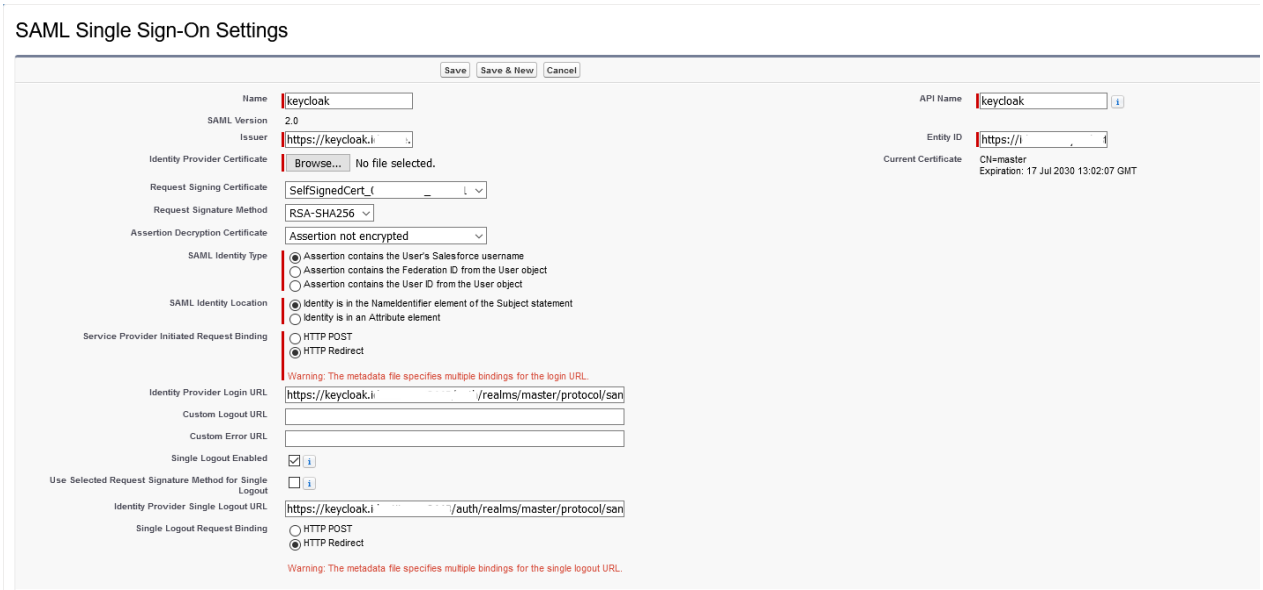
4. Name this setting for referencing within your organization. Salesforce inserts the corresponding API value, which you can customize if necessary.

5. In the **Single-On Settings**, configure the following, and then click **Save**:

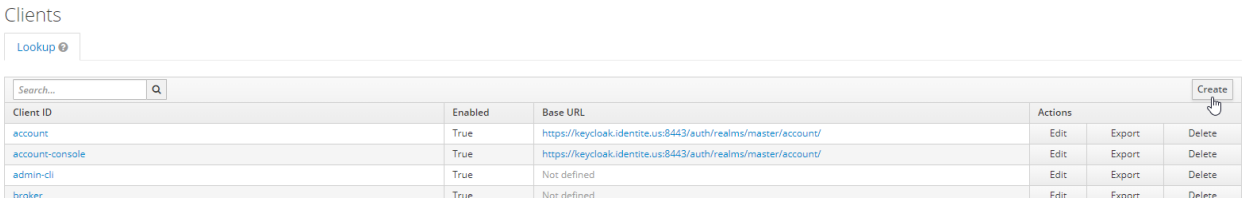
Issuer	It is often referred to as the **Entity ID for the identity provider**.
Identity Provider Certificate	Click the **Browse** button to locate and upload the authentication certificate issued by your identity provider. The certificate size cannot exceed 4 KB. If it does, try using a DER encoded file to reduce the size.
Request Signing Certificate	SELECT the certificate you want from the ones saved in your **Certificate and Key Management** settings.
Request Signature Method	Select the hashing algorithm for encrypted requests, either RSA-SHA1 or RSA-SHA256.
Assertion Decryption Certificate	*Optional*. If the identity provider encrypts SAML assertions, select the assertion decryption certificate saved in your **Certificate and Key Management** settings. This field is available only if your org supports multiple SSO configurations.
SAML Identity Type **SAML Identity Location** and other fields described in Identity Provider Values	Specify the values provided by your identity provider, as appropriate.
Service Provider Initiated Request Binding	Select the appropriate value based on the information provided by your identity provider.

Custom Error URL	specify the URL of the page that the users are directed to if there is an error during SAML login. It must be a publicly accessible page, such as a public site Visualforce page. The URL can be absolute or relative.
SAML 2.0	if your identity provider has specific login or logout pages, specify them in **Identity Provider Login URL** and **Custom Logout URL**, respectively.

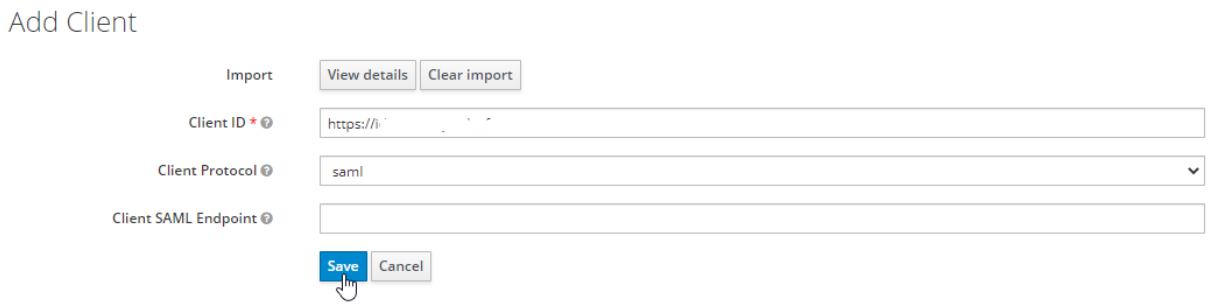
6. If your Salesforce org has domains deployed, specify whether you want to use the base domain (*https://saml.salesforce.com*) or the custom domain for the **Entity ID**. Share this information with your identity provider.
7. *Optional*. Set up Just-in-Time user provisioning. For more information, see Enable Just-in-Time user provisioning and About Just-in-Time Provisioning for SAML.



8. To download the .xml file of your SAML configuration settings, click **Download Metadata**.
9. Open the Keycloak admin console and select the realm that you want to use.
10. From the left navigation bar, click **Clients** and create a new SP application.



11. Select the file that you downloaded earlier, and then click **Save**.



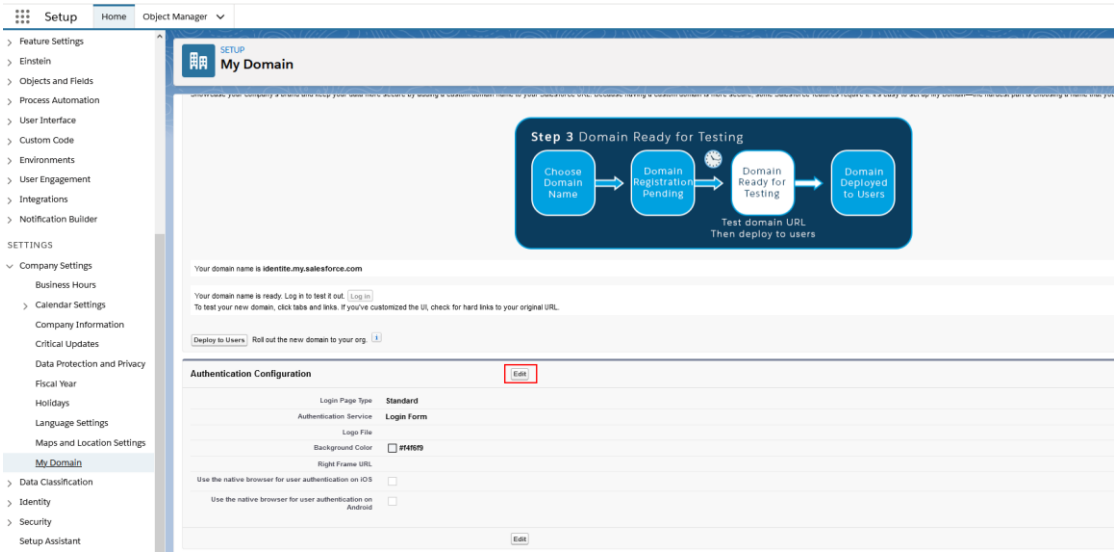
12. Configure the following parameters:

Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Consent Required	OFF
Client Protocol	SAML
Include AuthnStatement	ON
Sign Documents	ON
Optimize Redirect signing key lookup	OFF
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Encrypt Assertion	OFF
Client Signature Required	ON
Canonicalization Method	EXCLUSIVE
Force Name ID Format	ON
Name ID Format	Email
Root URL	Leave empty
Valid Redirect URIs	The Assertion Consumer Service URL from Service Provider Metadata

13. Under **Fine Grain SAML Endpoint Configuration**, configure the following:

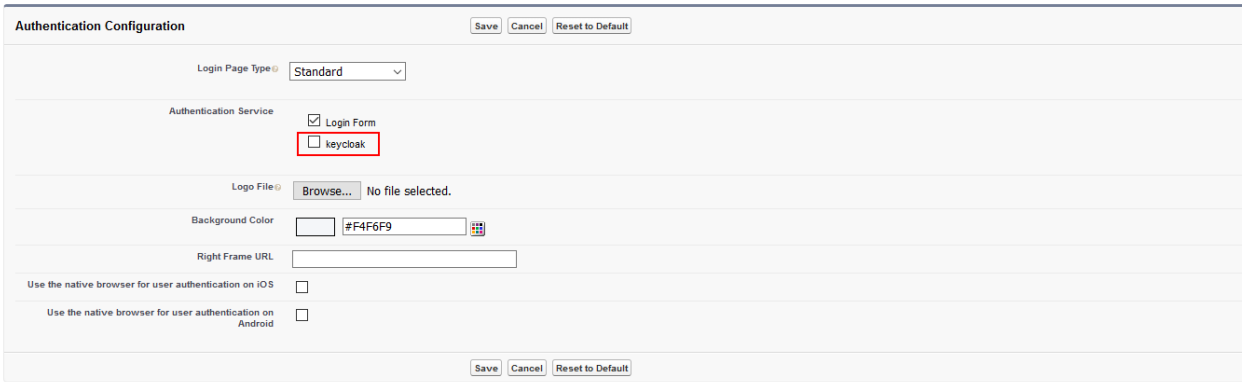
Assertion Consumer Service POST Binding UR	The ACS (Assertion Consumer Service) URL from Service Provider Metadata
Logout Service Redirect Binding URL	The Single Logout URL from Service Provider Metadata

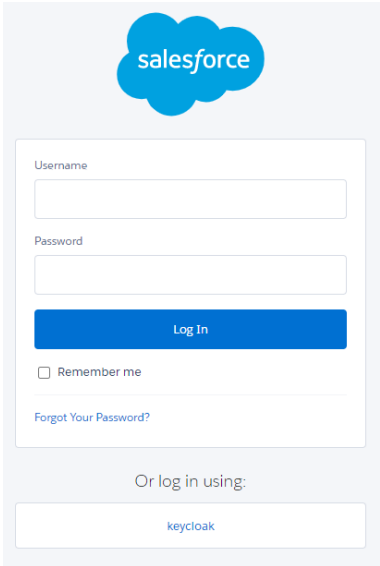
14. To redirect Salesforce login to Keycloak IdP for Single Sign On (SSO), you need to enable authentication method type. Go to **Setup**, and then select **My Domain**. In the Login Page Branding section, select **Edit**:



15. Enable another authentication type:

Authentication Configuration





For more information about Salesforce SAML configuration, go to *https://help.salesforce.com/articleView?id=sso_saml.htm&type=5*.

Related topics

Set up service providers with Keycloak

Confluence: How to configure SAML for SSO

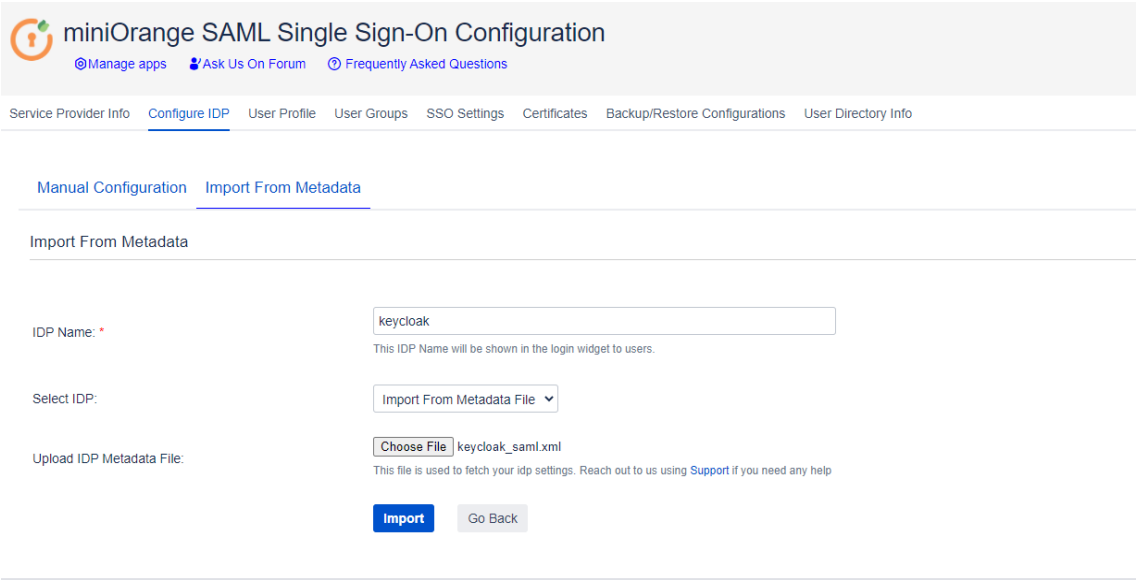
Confluence: How to configure SAML for SSO

You need to install an additional application to have access to SSO in Confluence. You can download the application at Atlassian Marketplace.

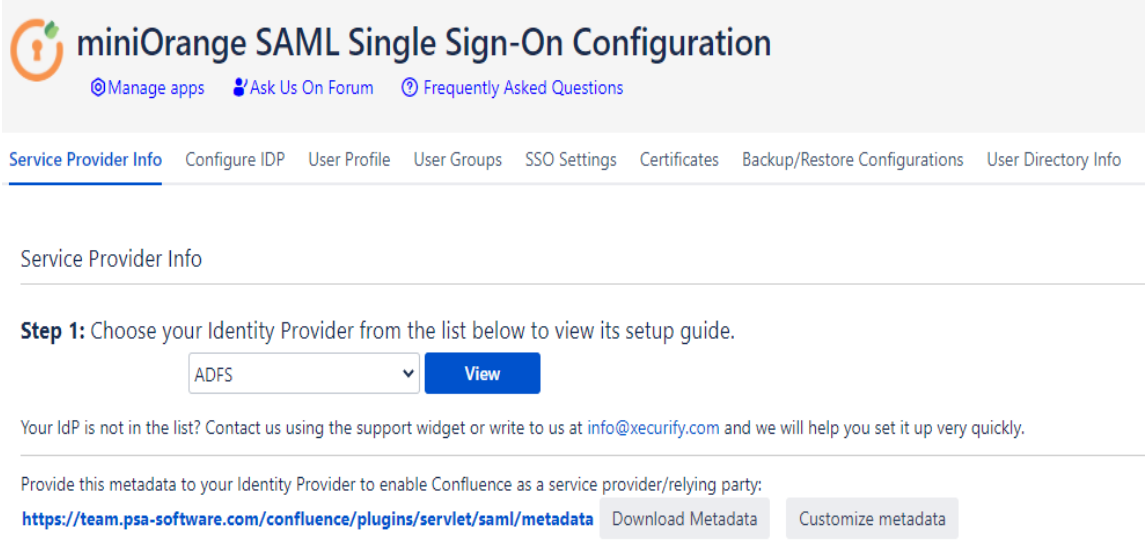
Procedure

To configure SAML for SSO using Confluence SSO/Single Sign On, SAML SSO by miniOrange do the following:

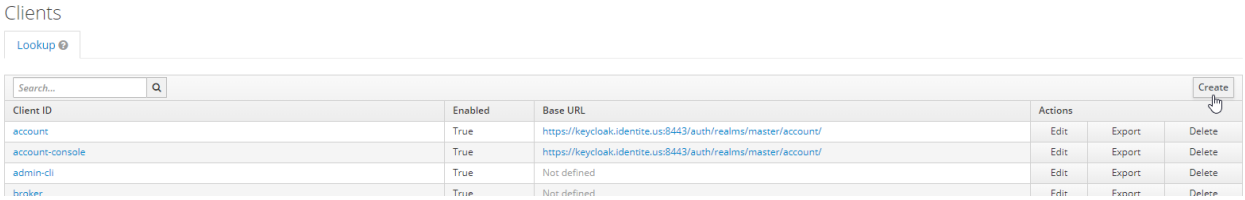
1. In the Confluence SSO configuration application, import the Keycloak metadata file.



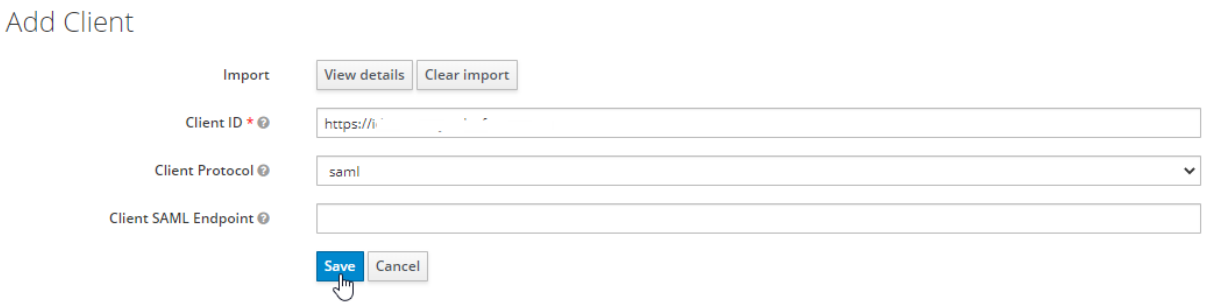
2. Download the Confluence metadata.



3. Open the Keycloak admin console and select the realm you want to use.
4. In the left navigation bar, click **Clients** to create a new SP application.



5. Select file that you downloaded earlier and click **Save**.



6. Configure the following parameters:

Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Consent Required	OFF
Client Protocol	SAML
Include AuthnStatement	ON
Sign Documents	ON
Optimize Redirect signing key lookup	OFF
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Encrypt Assertion	OFF
Client Signature Required	ON
Canonicalization Method	EXCLUSIVE
Force Name ID Format	ON
Name ID Format	Email
Root URL	Leave empty
Valid Redirect URIs	The Assertion Consumer Service URL from Service Provider Metadata

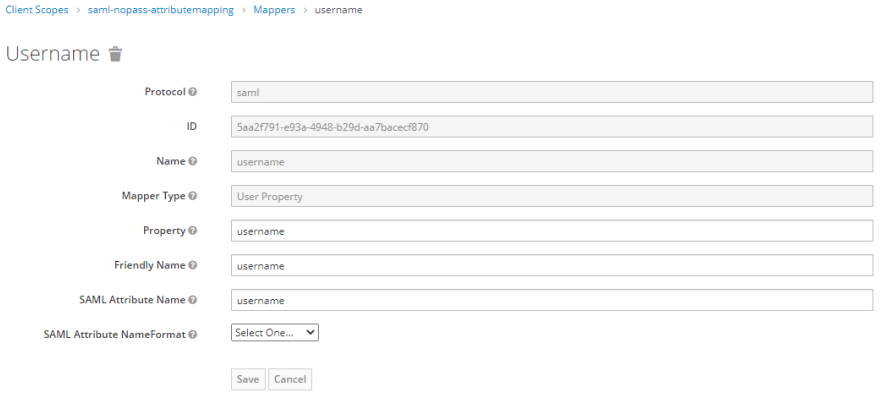
7. Under **Fine Grain SAML Endpoint Configuration**, configure the following:

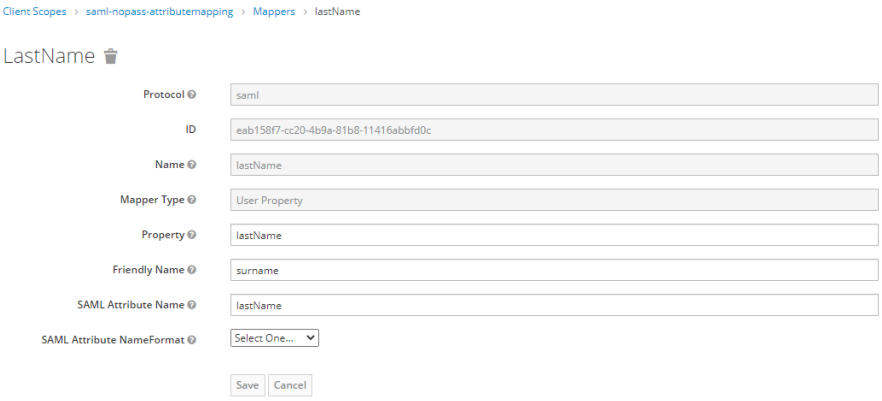
Assertion Consumer Service POST Binding UR	The ACS (Assertion Consumer Service) URL from Service Provider Metadata
Logout Service Redirect Binding URL	The Single Logout URL from Service Provider Metadata

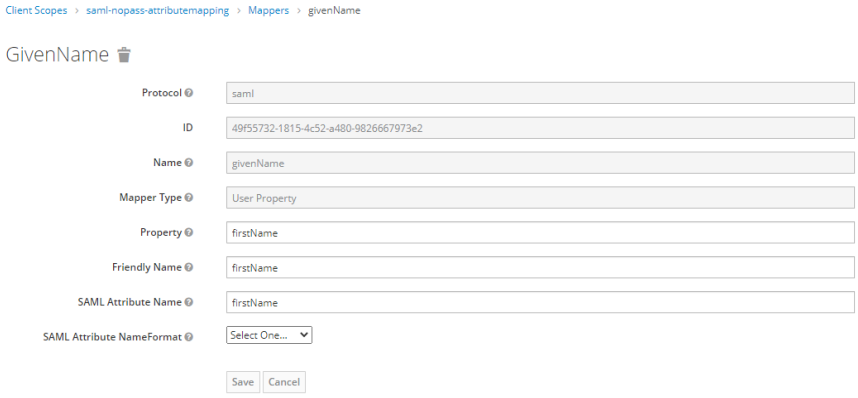
8. Add attribute mapping:

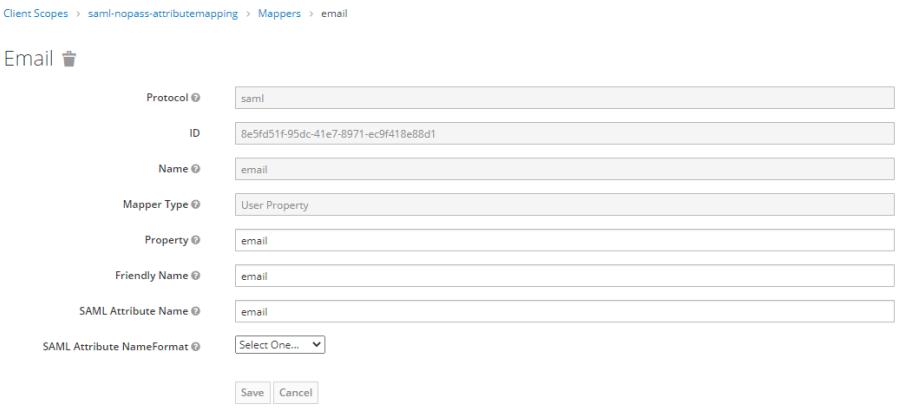
   - Username

- LastName
- GivenName
- Email



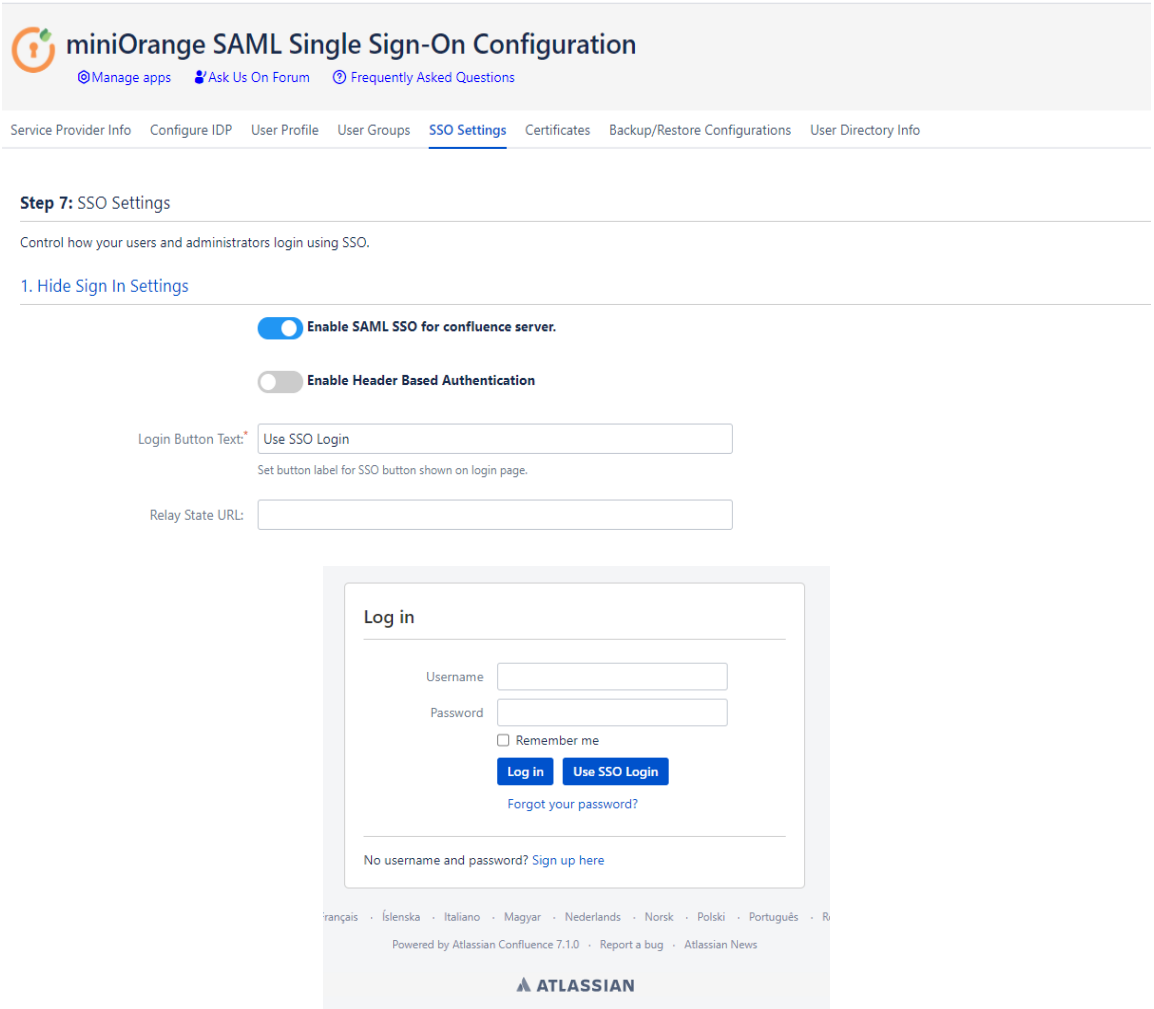






9. To redirect Confluence, login to **Keycloak IdP for Single Sign-On** (SSO) and enable an authentication method type.

In the **SSO Settings** tab, select **Enable SAML SSO for confluence server**.



For more information about configuring Confluence SAML, go to *https://plugins.miniorange.com/saml-single-sign-sso-confluence-using-jboss-keyclock*.

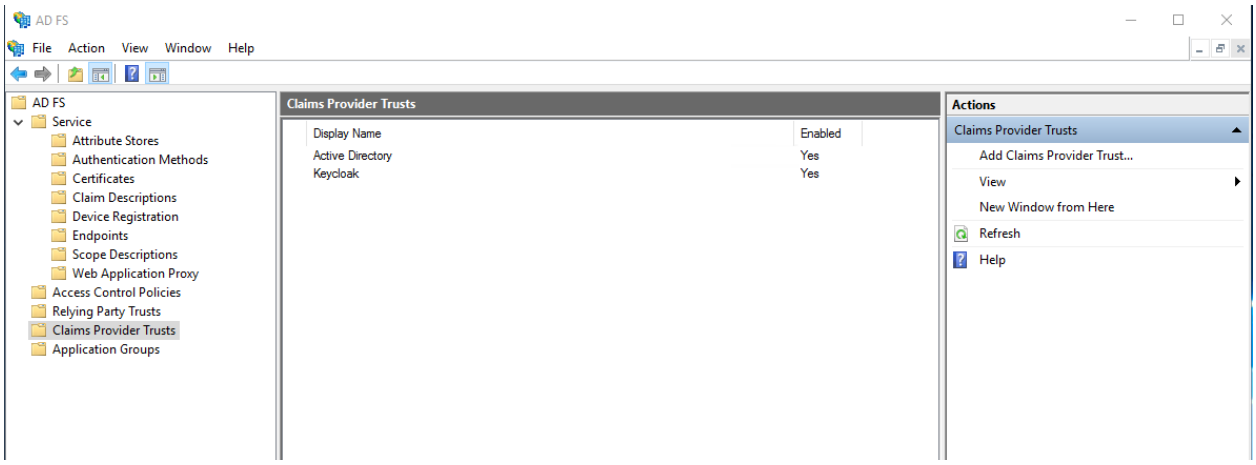
Related topics

Set up service providers with Keycloak
SalesForce: How to configure SAML for SSO
AD FS as a service provider

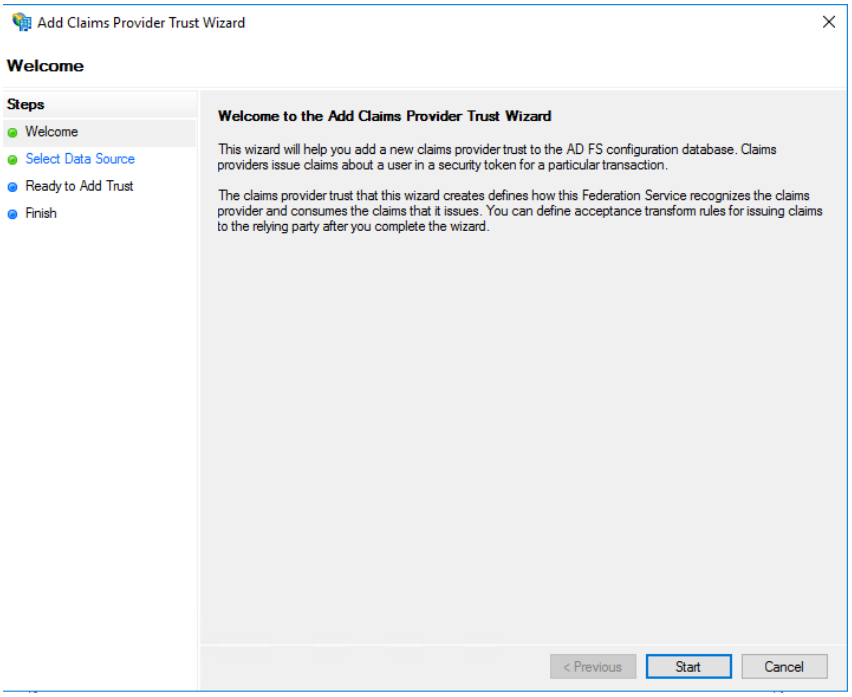
AD FS as a service provider

Procedure

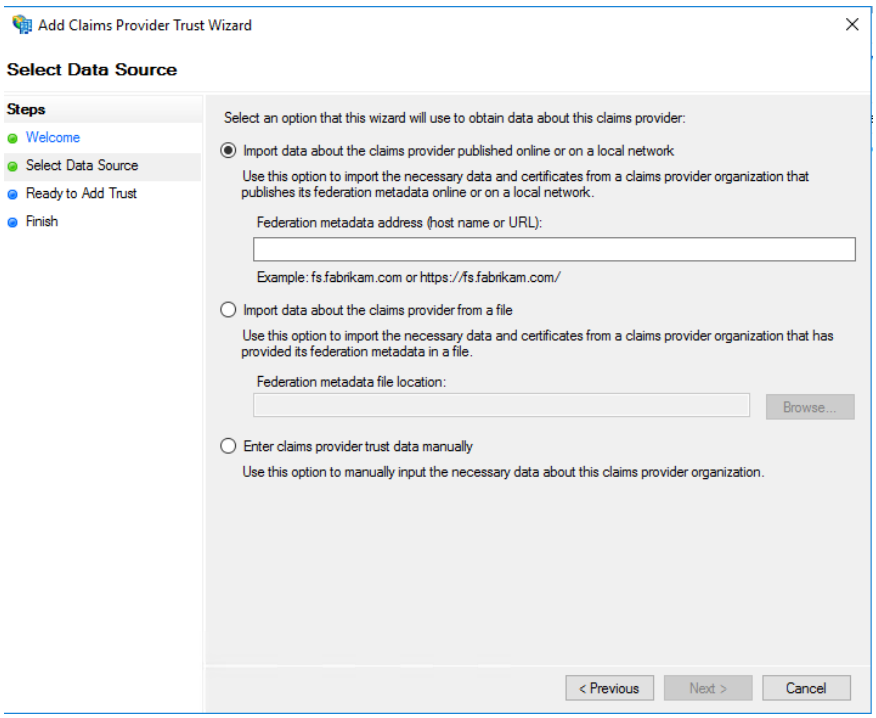
1. In the AD FS Management console, on the left pane, select the **Claims Provider Trusts** folder.



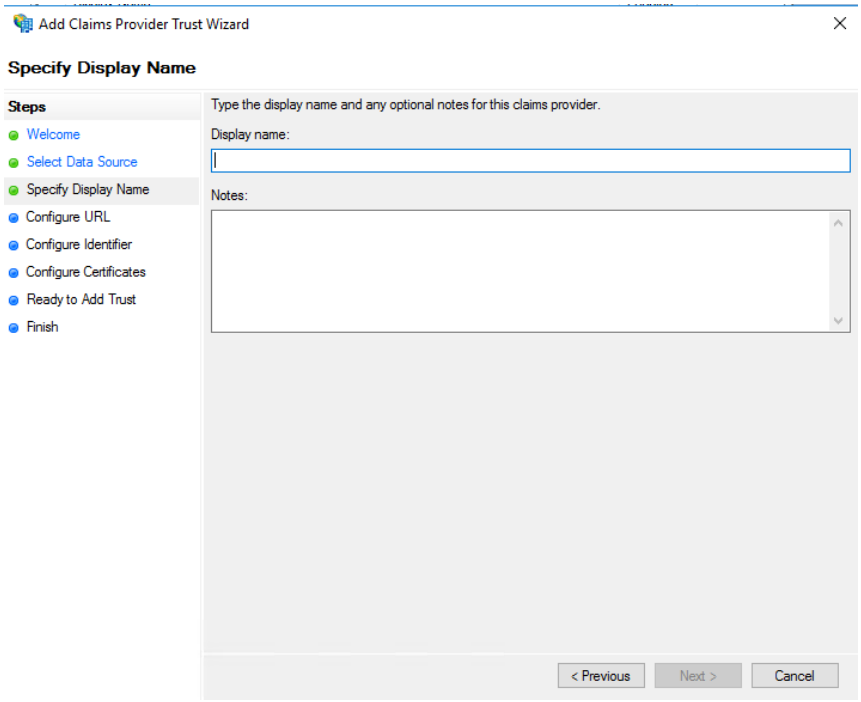
2. On the right pane, select **Add Claims Provider Trust** to open the Wizard.
3. In **Welcome**, select **Start**.



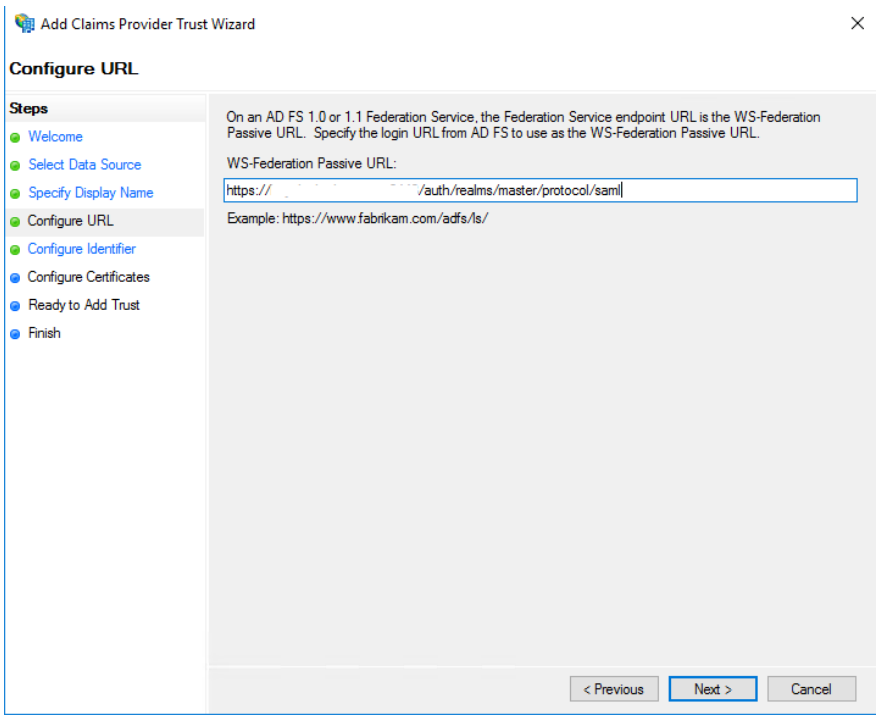
4. In Select Data Source, select the following options, as appropriate:
   - Using metadata URL
   - Using metadata XML
   - Manual configuration



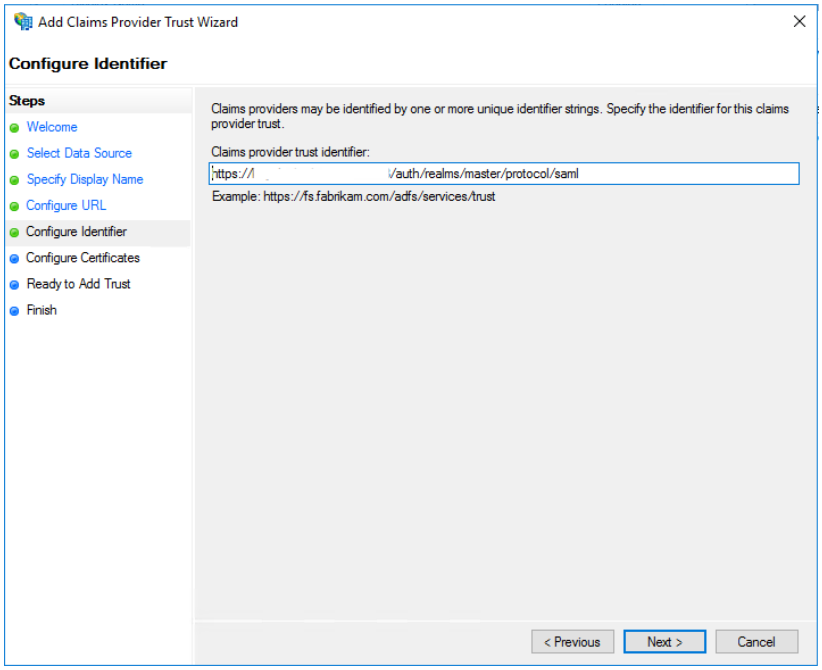
5. To configure Claims Provider Trust manually, do the following:
   a. In the **Specify Display Name**, enter display name and notes.



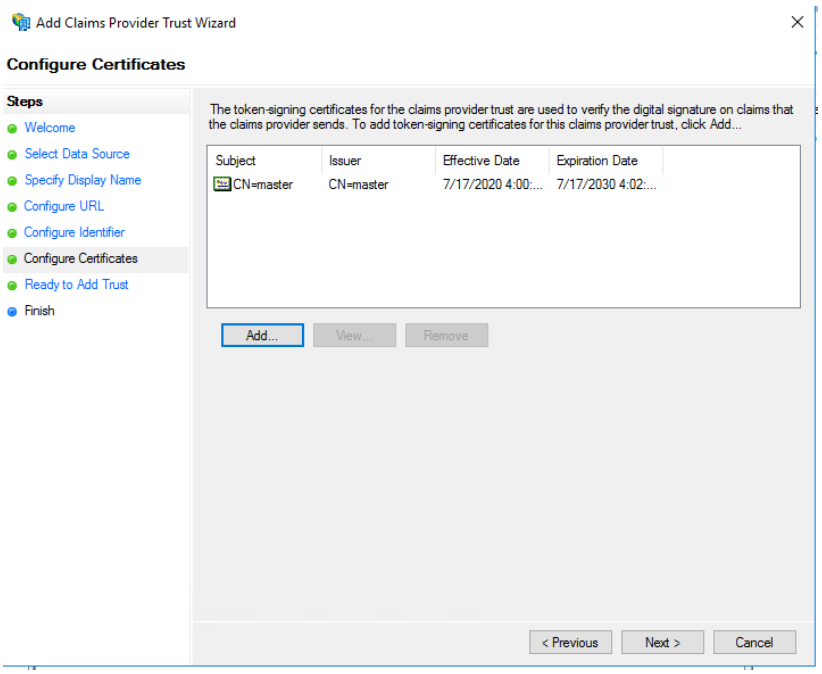
   b. In **Configure URL**, enter a service provider URL.



c. In **Configure Identifier**, enter claims provider trust identifier.

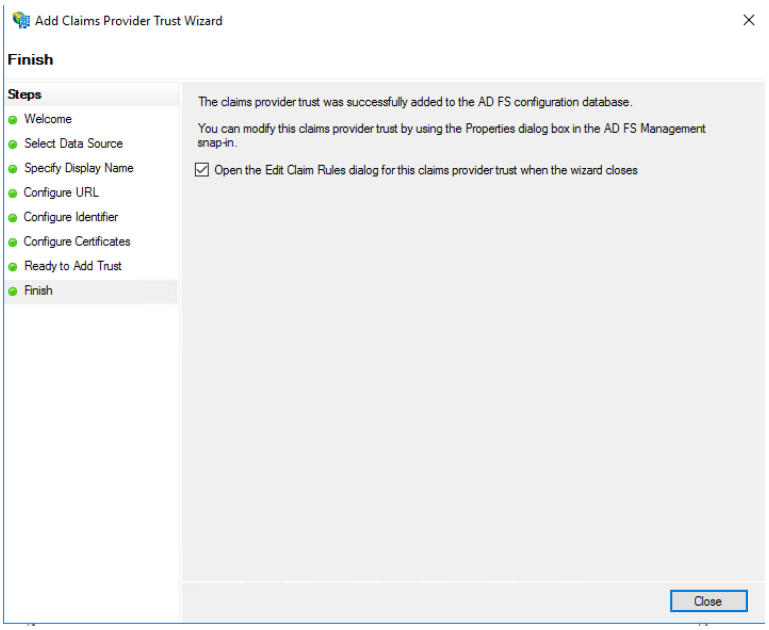


d. In **Configure Certificates**, add the token-signing certificate from Keycloak provider.

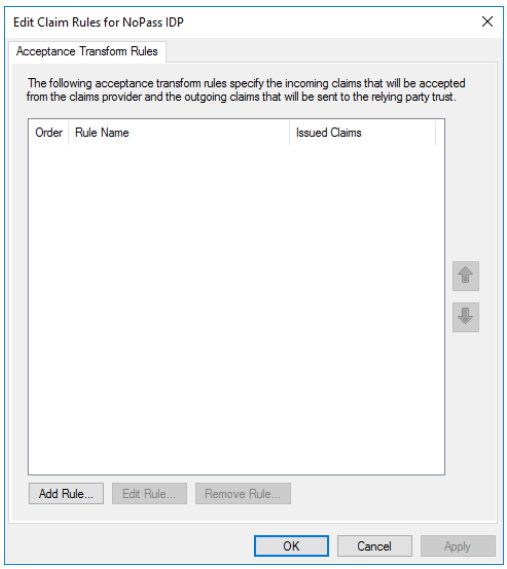


e. Check ready status and click **Next**.

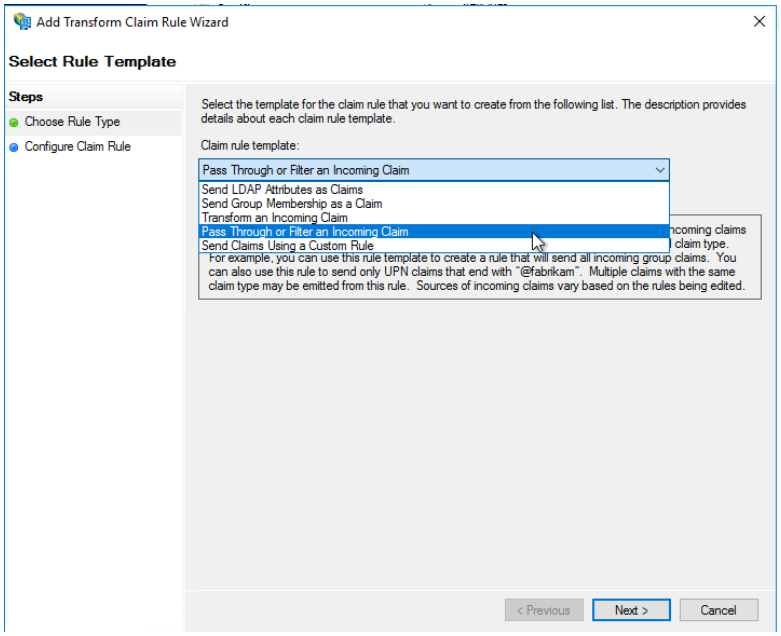
f. In **Finish**, select **Open the Edit Claim Rules dialog**…, and select **Close**.



g. In the **Edit Claim Rules for NoPass IDP** dialog box, select **Add Rule**.

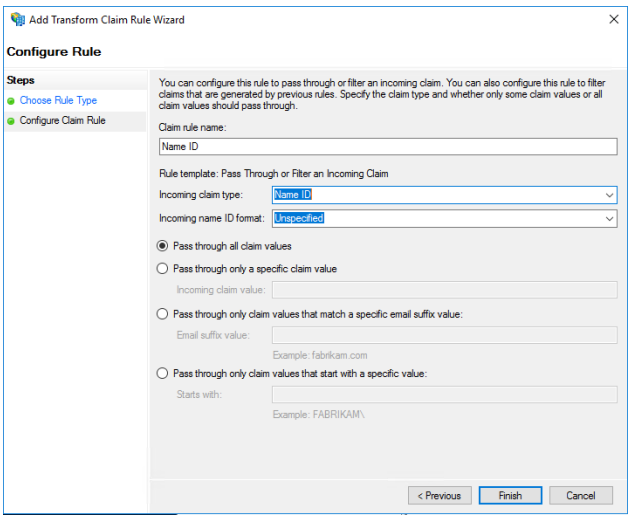


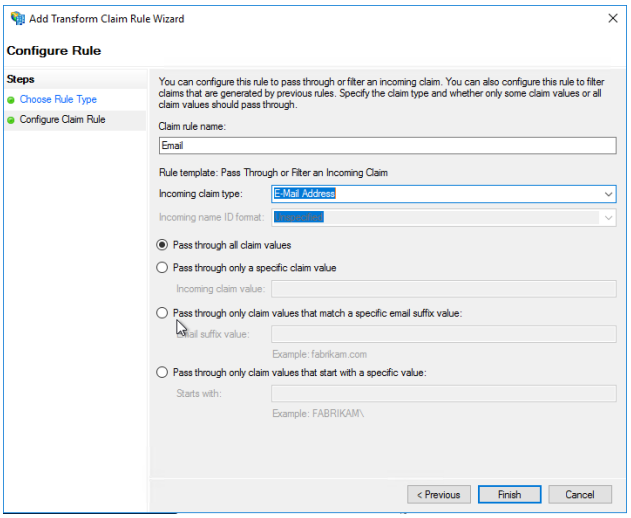
h. In **Select Rule Template**, from the **Claim rule template** list, select **Pass Through of Filter Incoming Claim**, and then select **Next**.

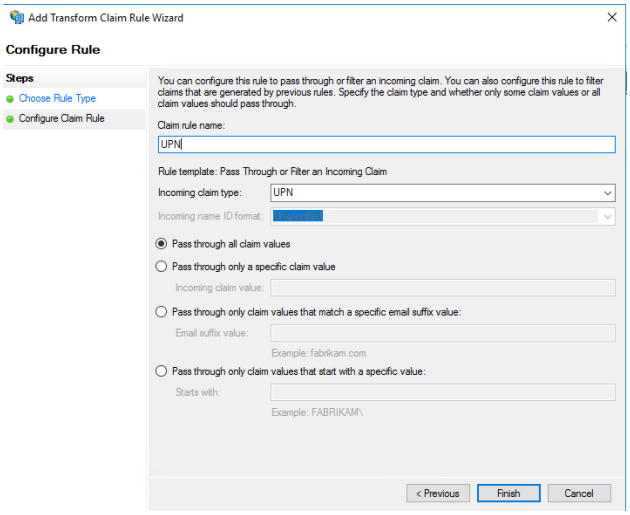


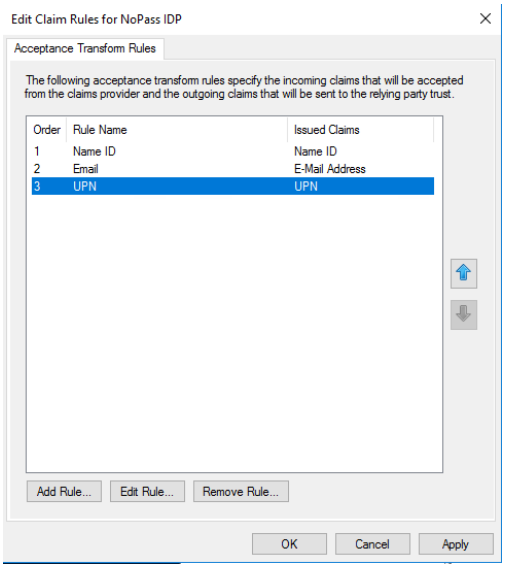
i. In the **Configure Rule** dialog box, in Choose Rule Type, configure the following parameters:

- Name ID
- Email
- UPN

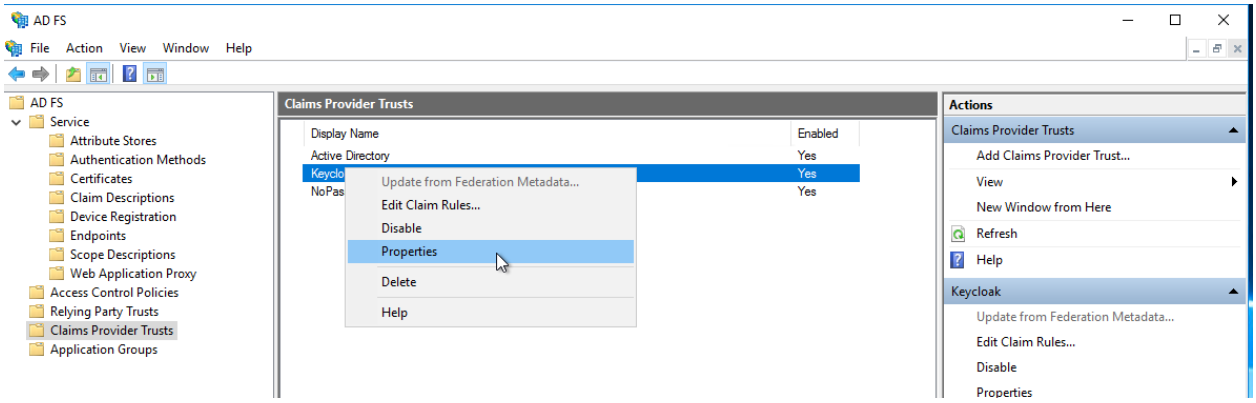

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
Claim rule name:
Name ID
Rule template: Pass Through or Filter an Incoming Claim
Incoming claim type:
Name ID
Incoming name ID format:
Unspecified
Pass through all claim values
Pass through only a specific claim value
Incoming claim value:
Pass through only claim values that match a specific email suffix value:
Email suffix value:
Example: fabrikam.com
Pass through only claim values that start with a specific value:
Starts with:
Example: FABRIKAM\
< Previous
Finish
Cancel


Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
Claim rule name:
Email
Rule template: Pass Through or Filter an Incoming Claim
Incoming claim type:
E-Mail Address
Incoming name ID format:
Pass through all claim values
Pass through only a specific claim value
Incoming claim value:
Pass through only claim values that match a specific email suffix value:
Email suffix value:
Example: fabrikam.com
Pass through only claim values that start with a specific value:
Starts with:
Example: FABRIKAM\
< Previous
Finish
Cancel

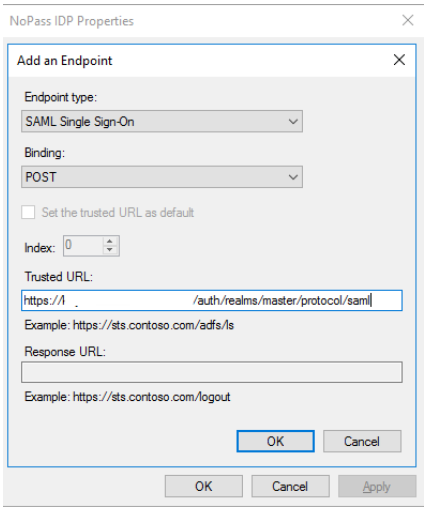

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.
Claim rule name:
UPN
Rule template: Pass Through or Filter an Incoming Claim
Incoming claim type:
UPN
Incoming name ID format:
Pass through all claim values
Pass through only a specific claim value
Incoming claim value:
Pass through only claim values that match a specific email suffix value:
Email suffix value:
Example: fabrikam.com
Pass through only claim values that start with a specific value:
Starts with:
Example: FABRIKAM\
< Previous
Finish
Cancel



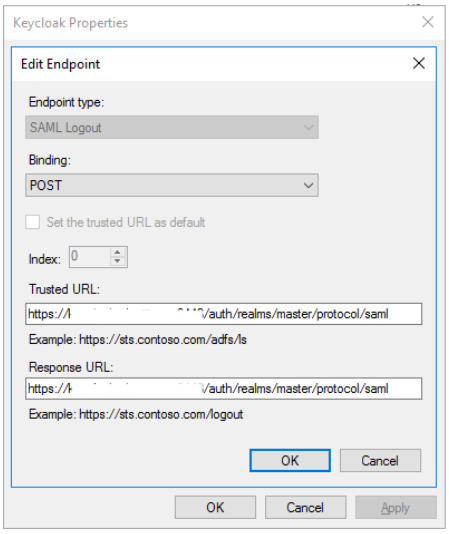
6. In the **AD FS Management** console, select the **Claims Provider Trusts** folder, and under **Keycloak** select **Properties**.



7. In the NoPass IDP Properties, select Endpoints, and add the following URLs:
   a. In **Add and Endpoint**, in the **Endpoint type** list, select **SAML Single Sign-On**. In the **Binding** list, select **POST**. In the **Trusted URL** field, enter your service provider URL.



   b. In **Edit Endpoint**, in the **Endpoint type** list, select **SAML Logout**. In **Binding**, select **POST**. In the **Trusted URL**, enter your service provider URL.

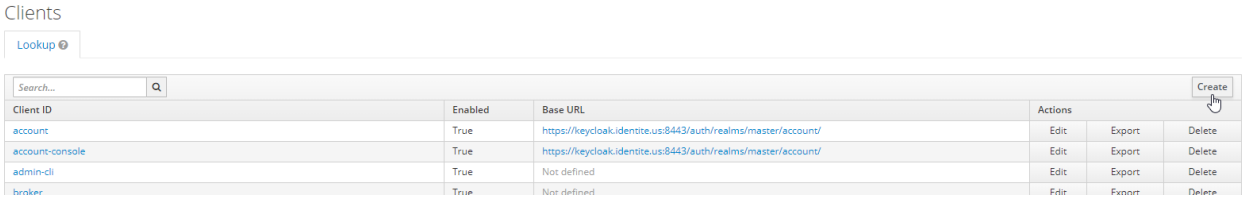


j. Export the AD FS SAML metadata to XML.

https://**adfs.domain.name**/FederationMetadata/2007-06/FederationMetadata.xml

k. Import the AD FS SAML metadata to Keycloak.

8. In the **Keycloak admin console**, select the realm you want to use.
9. In the left navigation bar, select **Clients**, and create a new SP application.



10. Select the file that you have downloaded earlier and click **Save**.

11. Configure the following parameters:

Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Consent Required	OFF
Client Protocol	SAML
Include AuthnStatement	ON
Sign Documents	ON
Optimize Redirect signing key lookup	OFF
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Saml Signature Key Name	CERT_SUBJECT
Encrypt Assertion	OFF
Client Signature Required	OFF

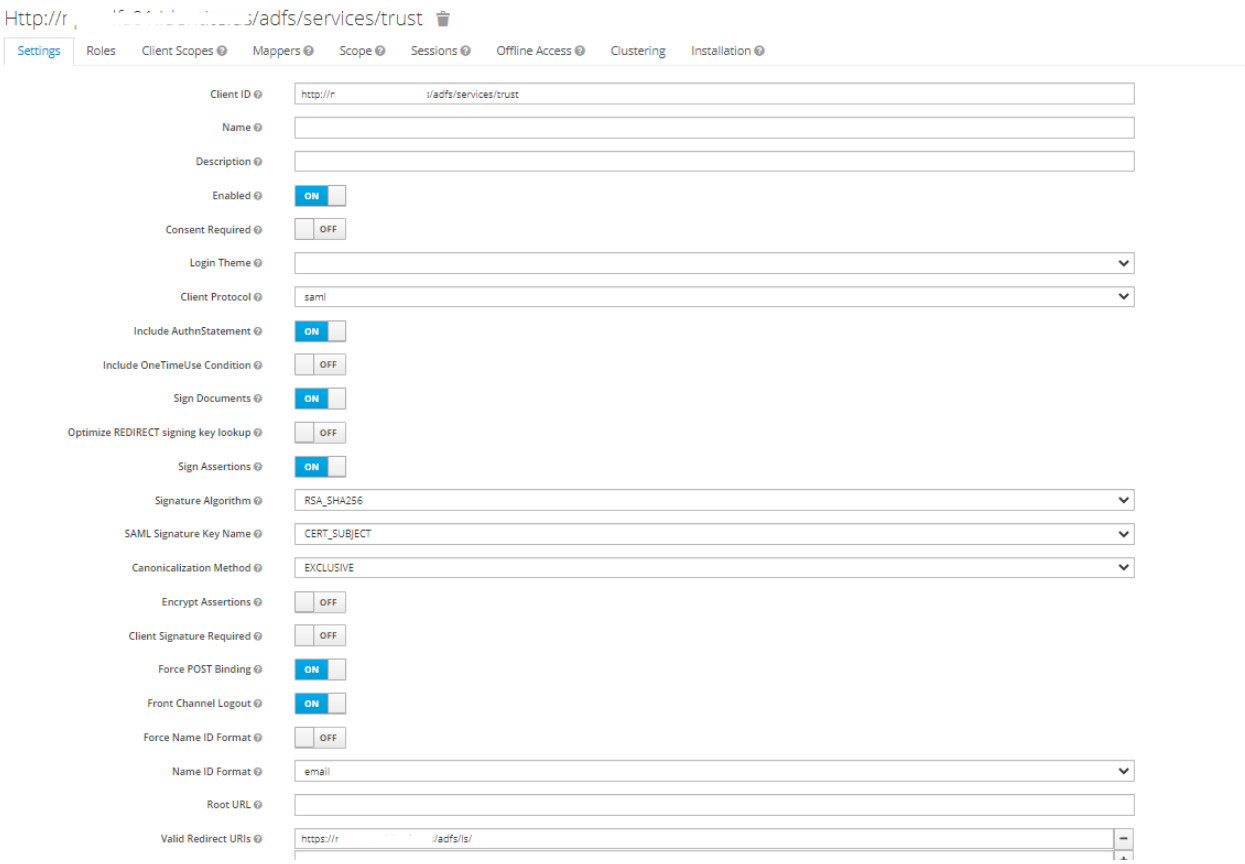
Canonicalization Method	EXCLUSIVE
Force Name ID Format	ON
Name ID Format	Email
Root URL	Leave empty
Valid Redirect URIs	The Assertion Consumer Service URL from Service Provider Metadata

12. Under **Fine Grain SAML Endpoint Configuration**, configure the following:

Assertion Consumer Service POST Binding UR	The ACS (Assertion Consumer Service) URL from Service Provider Metadata
Logout Service Redirect Binding URL	The Single Logout URL from Service Provider Metadata

Note: To login to AD FS with SSO use the following URL:

https://**adfs01.domain.name**/adfs/ls/idpinitiatedsignon



Related topics

Set up service providers with Keycloak
SalesForce: How to configure SAML for SSO
Confluence: How to configure SAML for SSO

ADMINISTRATION

This chapter contains the following:

- **Licensing**
- **Web portal**
- Error! Reference source not found.

Licensing

We offer two service types of licensing: Portal licensing and Radius licensing.

Procedure

1. Provide the following data to license NoPass:

```
Service type: Portal, Radius, Identite Provider
Portal domain name: portal.example.com:port. For radius portal name is radius.local
Service domain name: nopass.example.com:port
Valid to: 12/12/2020
UserLimit: 50
```

2. Send a license request to *sales@identite.us*.

Related topics

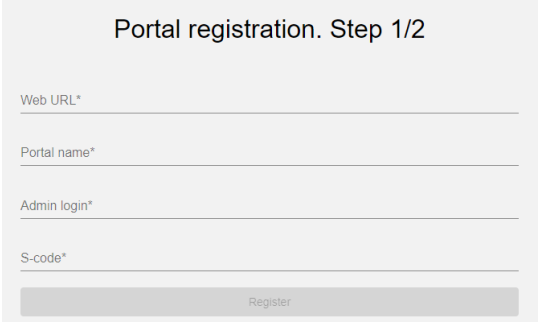
Web portal
Radius portal

Web portal

Procedure

To register the web portal, do the following:

1. On the portal registration page, enter the Admin login and S-code.



Note: choose a name for your admin login and generate a password (S-code) to bind the authentication portal to the application server. These parameters are defined by you and saved on your database. Mind the following restrictions for the credentials:

- Admin login: length is less than 64 case sensitive characters.
- Password (S-code): length is a minimum of 8 characters including capital letters and numbers or symbols.

Example of AdminID and S-code:

```
AdminID: nopass-admin
SCode: passCODE99!
```

2. Send this data into the portal response. For more information about it, see the API documentation.
3. How to register web portal in application server.
4. On the admin portal settings page, enter (import) the license code that your received from us earlier and then customize the settings.

Related topics

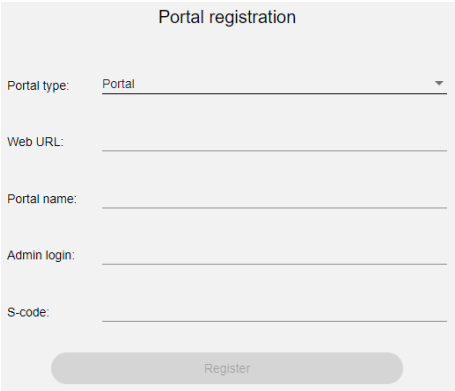
How to register web portal in application server
Error! Reference source not found.

How to register web portal in application server

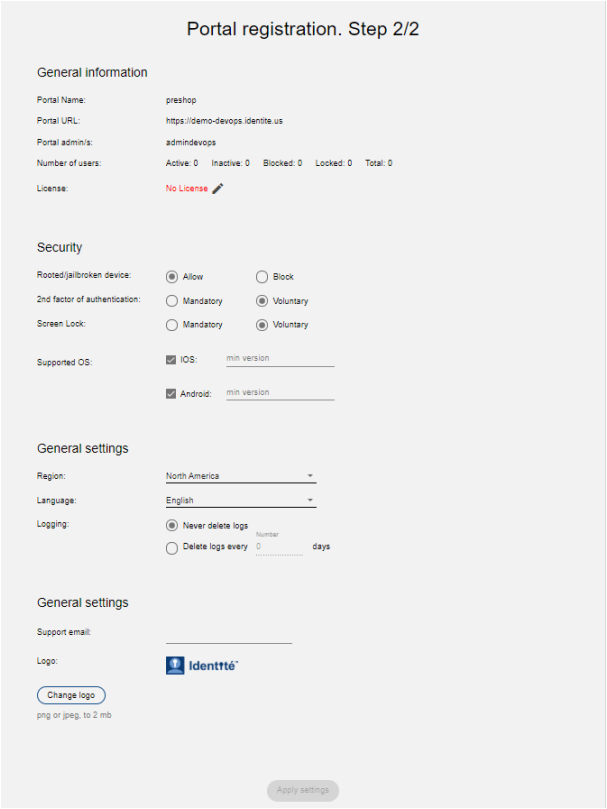
Procedure

1. Follow the WEB URL that is assigned to the application server.
2. On the **Portal registration** page, fill the following fields, and then click **Register**:

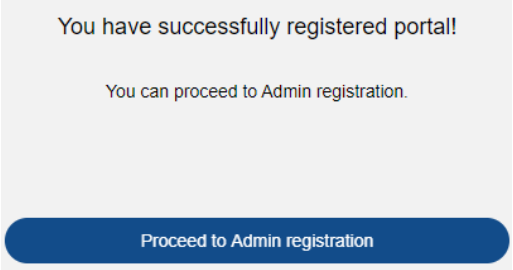
Web URL	Authentication portal
Portal Name	Unique portal name in the database
Admin login	Admin login name from the previous stage
S-code	Password from the previous stage, which was generated by you



3. In the admin portal settings page, enter or import the license code that you have received earlier.
4. Customize the following settings and click **Apply Settings**:
   a. **General information**—information created in Step 2. The license information is available after entering or importing to this page.
   b. **Security**—can be triggered or manipulated by admin for all users using our authentication system to access your services.
   c. **General settings**—information of your admin panel.



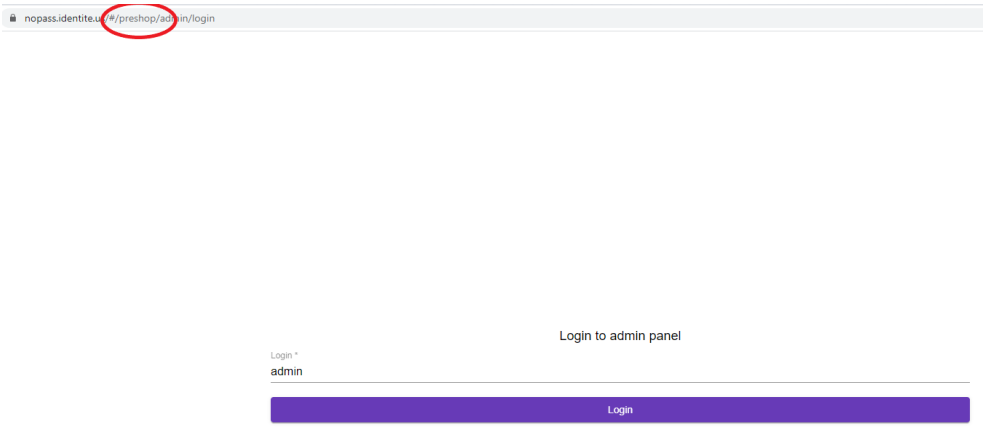
A successful result is as follows:



5. Click **Proceed to Admin registration**, scan the QR code, and enter the confirmation code.
6. On the **Admin panel login** page, save the link to the admin panel. The link consists of the NoPass application URL and Portal name that was set during the registration in Step 2.

```
https://SERVER_URL/#/PORTAL_NAME/admin/login
```

7. Enter the **Admin panel** using the link and click **Login**.



8. Go to *nopass.identite.us/#/preshop/admin/login* (the name of the registered portal is highlighted in red) and enter your AdminID.
9. After accepting the authentication attempt, by default, you will be logged into the admin panel.

Related topics

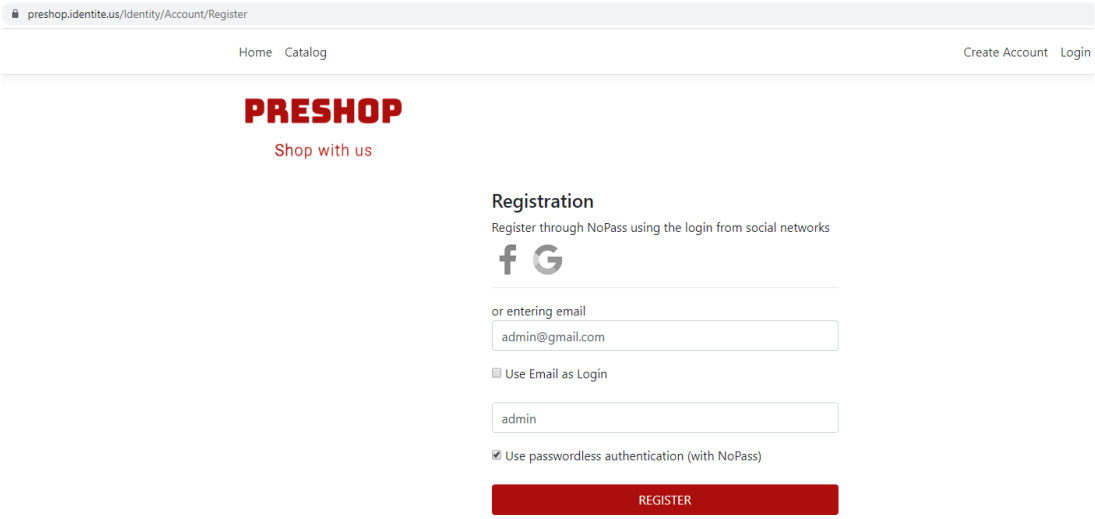
Web portal
How to create administrator account on Preshop portal

How to create administrator account on Preshop portal

You need to register and bind an administrator account to your mobile device to have access to the admin panel. If you accidentally missed this step during Web Portal Registration, you can do it on the Preshop Web portal

Procedure

1. Click Create Account.
2. On the Registration Page, enter the same login name that you entered to the AdminID field in Step 2, “How to register the web portal in the application server” and click Register.



Related topics

How to register web portal in application server

Radius portal

In this chapter you will find the following:

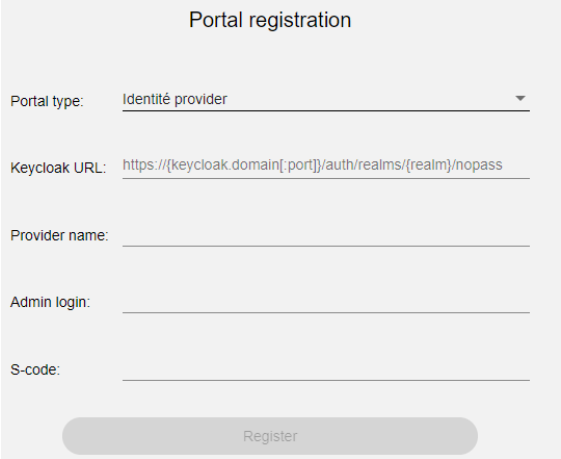
- **How to register radius portal**
- **How to configure radius portal**
- **How to bind a User**

How to register radius portal

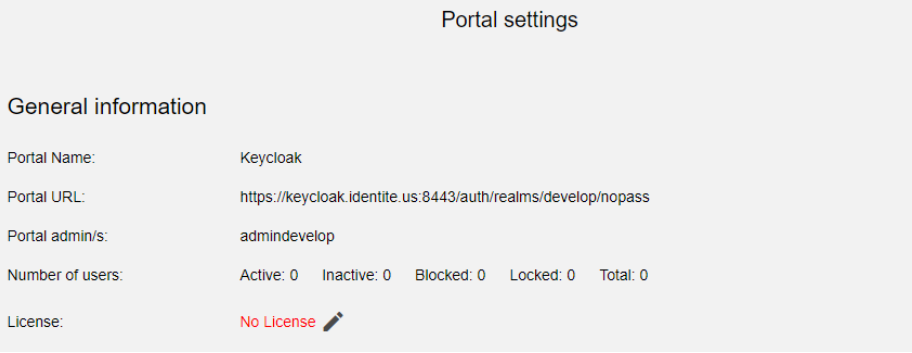
Procedure

1. To register the radius portal, on the **Portal registration** page, set the following parameters and click **Register**:

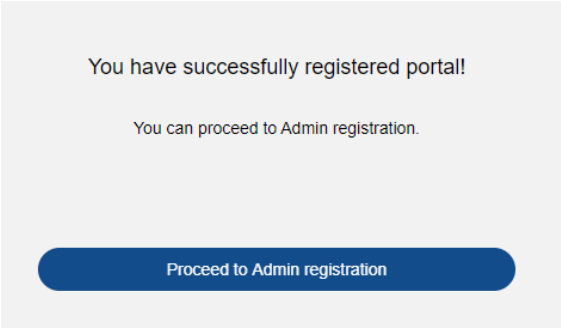
Portal type	Radius server
Portal name	The portal name is displayed in this field
Admin login	By default, the admin login is *radiusadmin*. To override this value, you can use the environment variable for the NoPass server.
S-code	Admin password. The same as in the Admin login field. By default, it is *radiuspassword*.



2. On **Portal settings**, configure the settings and add the license response file that you got during Step 2.

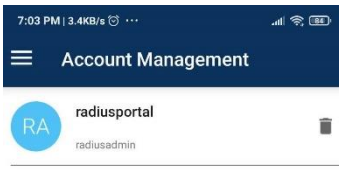


A successful result is as follows:



3. Click **Proceed to Admin registration** and scan the QR-code to link the account to your mobile phone.

The result on your mobile phone is as follows:



Related topics

How to configure radius portal
How to bind a User

How to configure radius portal

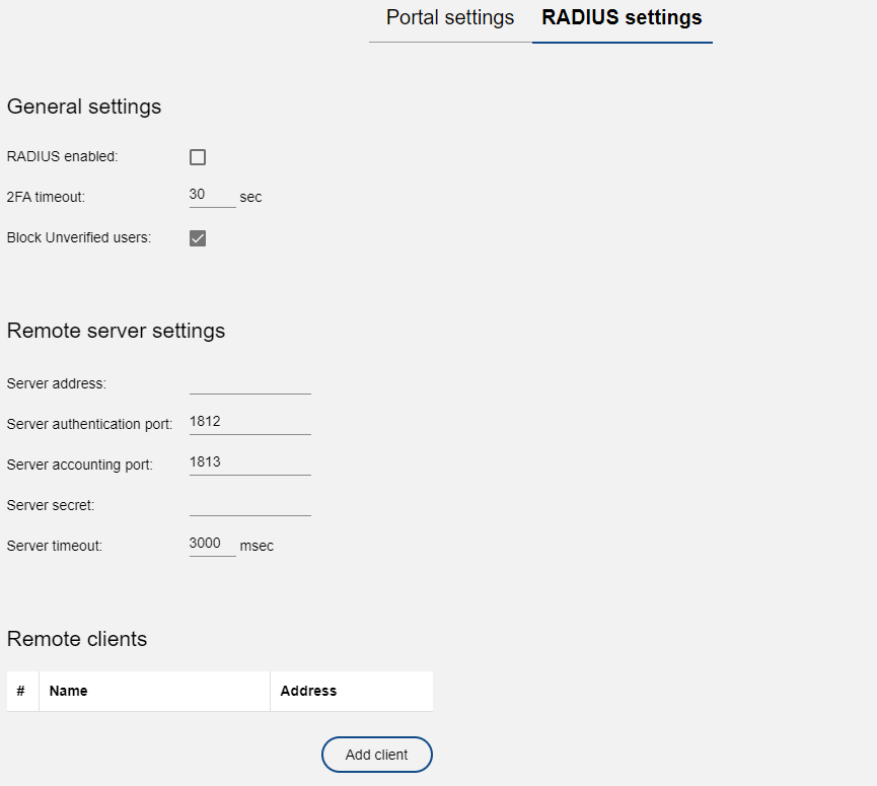
Procedure

To configure the radius portal, do the following:

1. Log in to the radius admin panel using the following link:

```
https://SERVER_URL/#/PortalName/admin/login
```

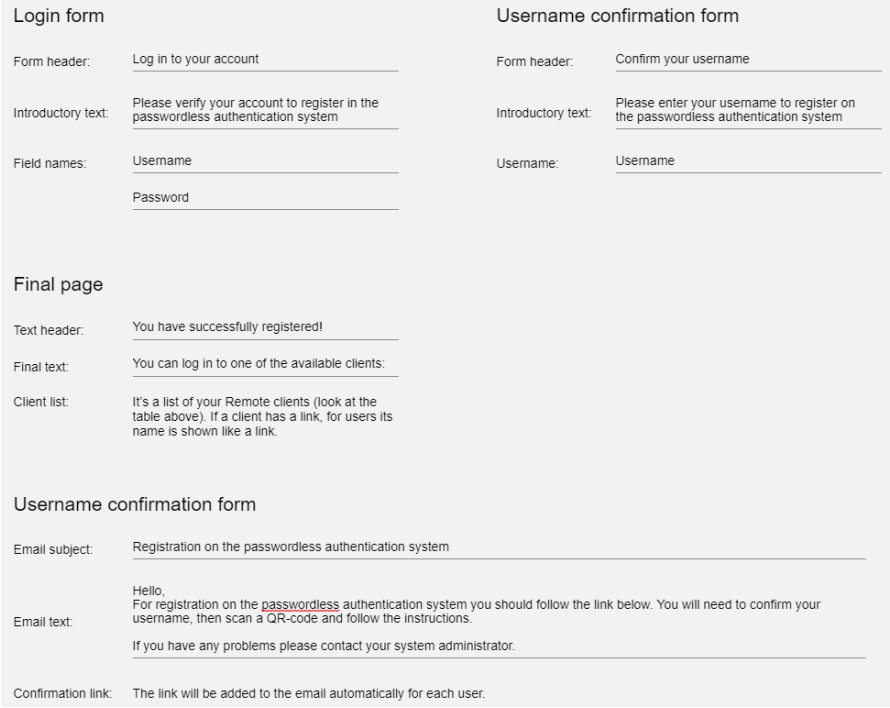
2. On the **Radius Admin** panel, select **Radius settings**.



3. In the **Radius settings** tab, in the **General settings** group, configure the following parameters:
   a. Select **RADIUS enabled**.
   b. Set **2FA timeout**—confirmation timeout on a mobile device—less than the service connection timeout.
   c. Select **Block Unverified users** to block connection for unverified users.
4. In the **Radius settings** tab, in the **Remote server settings** group, configure the following parameters:
   a. Fill the **Server address** field.
   b. Fill the **Server authentication port** field.
   c. Fill the **Server accounting port** field.
   d. In the **Server secret** field, enter the radius server secret.
   e. Set the **Server timeout** for connection timeout to radius server.
5. In the **Radius settings** tab, in the **Remote clients** group, configure the following parameters:
   a. **Name**—service display name.
   b. **Address**—service address.
   c. **Secret**—service secret.

d. **Link**—link to the server user manual.

6. *Optional*. Select **Require additional decline** if needed.
7. To customize design of the radius login page, configure the following parameters:
   a. In the **Login form** group, set **Form header**, **Introductory text**, and **Field names**.
   b. In the **Final page** group, set **Text header**, **Final text**, **Client list**.



Related topics

How to register radius portal
How to bind a User

How to bind a User

The Radius server checks that information is correct using authentication schemes such as PAP, CHAP or EAP. NoPass Proxy server supports the following radius authentication protocols: PAP, CHAP, MS-CHAP, PEAP, EAP-MSCHAPv2.

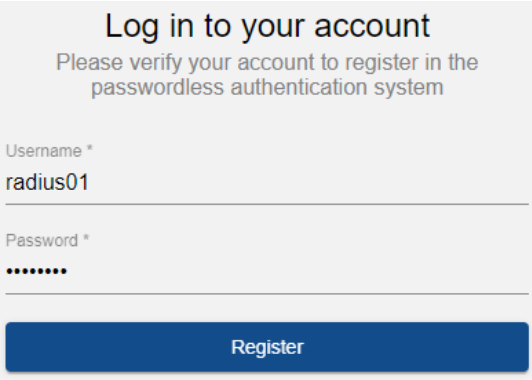
There are two ways to bind a user to the NoPass server depending on the type of radius authentication protocol.

Procedure 1

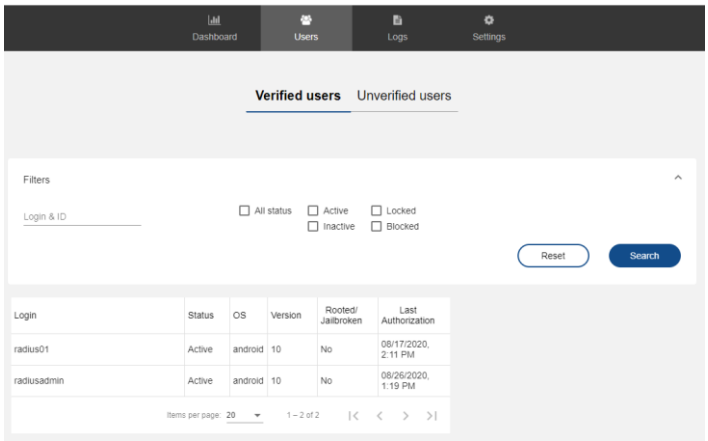
To bind a new user if the **PAP/CHAP/MS-CHAP/MS-CHAPv2** settings of your radius server are enabled, do the following:

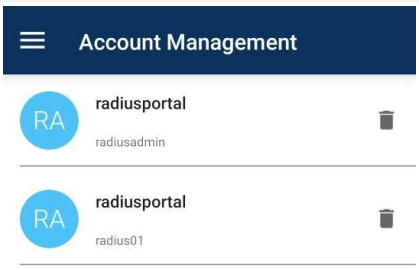
1. Register an administrator using the following link:

```
https://SERVER_URL/#/radius-user-registration
```



The user registers by the link and the administrator can see it on the verified user page in the admin panel.



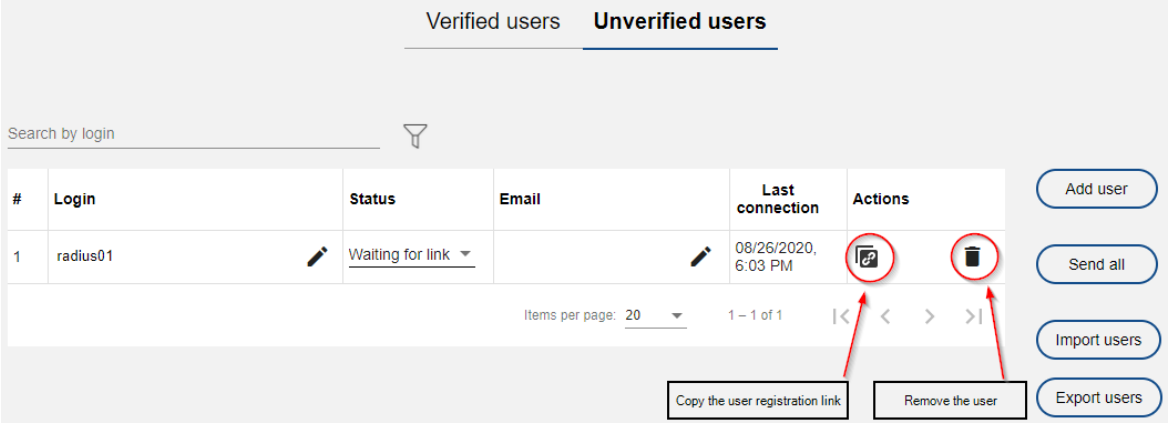


Procedure 2

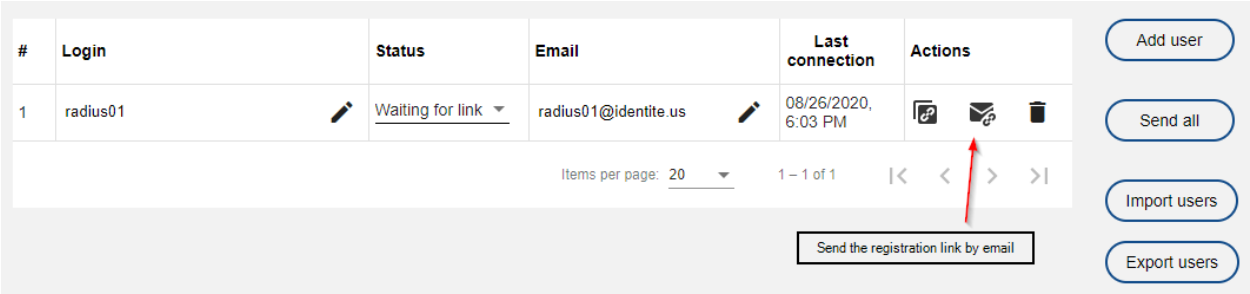
To bind a new user with any radius authentication protocol, do the following:

1. In the **Admin panel**, select **Block Unverified users**.

   Note: NoPass can proxy all connections from radius services to the radius server. When the user connects for the first time, the **Block Unverified users** checkbox appears in the **Unverified users** tab of the **Admin panel**.

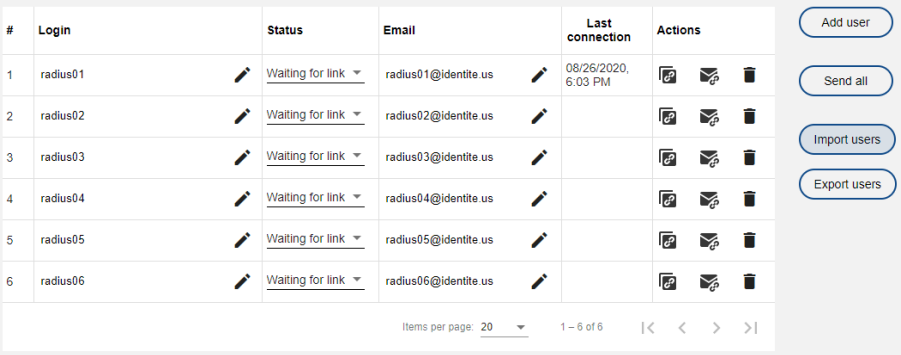


2. Send the unique registration link to the user. You can send it by email but you have to enter the email address for user.



3. *Optional*. You can import users from CSV.

```
radius02,radius02@identite.us
radius03,radius03@identite.us
radius04,radius04@identite.us
radius05,radius05@identite.us
radius06,radius06@identite.us
```



The user needs to follow the link and bind account to the NoPass Proxy server to change their status to verified users.

Related topics

How to register radius portal

How to configure radius portal

Identity Provider

In this chapter you will find the following:

- **How to register Identity Provider**

How to register Identity Provider

Procedure

To register the identity provider, do the following:

1. On the **Portal registration** page, set the following parameters and click **Register**:
    a. From the **Portal type** list, select **Identity provider**.
    b. In the **Keycloak URL** field, enter the URL of the Keycloak server.
    c. In the **Provider name** field, enter the name of identity provider.
    d. In the **Admin login** field, enter the login, which is allowed to the **Admin panel**.
    e. In the **S-code** field, enter the secret key necessary for the Identité administrator to register Keycloak.