Identité™

TECHNICAL MANUAL

NoPass Application Server Installation

NoPass Application Server Installation
Technical Manual
Version 2.7.1
14 April 2021

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

CONTENTS

1. ABOUT THIS MANUAL

This chapter contains the following:

- **Purpose and scope**
- **Intended audience**
- **Document conventions**

1.1. 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 integration 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 content organization.
- **Before you begin**. Describes the requirements and preparations needed for a successful installation of the NoPass application server.
- **NoPass Server deployment**. Gives a view on the infrastructure on a whole and provides information on how to install, launch, and stop the NoPass application server.
- **Server deployment to AWS using Terraform**. Describes the infrastructure to be installed with the terraform script.
- **NoPass RADIUS portal**. Describes the principles of work and procedure for registering and configuring the RADIUS portal provided by NoPass for seamless integration with your corporate RADIUS server.
- **Identity provider and Server Provider management**. Provides instructions for installing Keycloak Identity and setting up the NoPass extension.
- **Web portal management**. Explains how to integrate a WEB portal with the NoPass system.
- **Licensing**. Describes the procedure of licensure.
- **NoPass Integrations**. Provides instructions on how to integrate NoPass with your corporate applications, identity providers, and cloud repositories.

1.2. 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.*

1.3. Document Conventions

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

ELEMENT	DESCRIPTION
	Note—Additional information about a subject.
	Warning—Indicates a potential obstacle or condition requiring special attention.
\	Used as a line break. Do not type.
<…>	Used to denote placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
`sudo`	Code samples, including keywords and variables within text.
Prerequisites	Cross-references to the document chapters or internal hyperlinks.
https://dev.mysql.com/	Cross-references to external hyperlinks to web pages.

2. BEFORE YOU BEGIN

This chapter contains the following:

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

2.2. 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 or proxy ports to the Virtual Machine where the NoPass application server will be launched).
3) A database.
4) Internet access for the NoPass application and mobile devices.

What to read next

System requirements
Prepare virtual machine

2.3. System requirements

HARDWARE REQUIREMENTS

Note: These hardware requirements are provided for running one instance. Resources will need to increase as the load on the instance.

- 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, see the Docker website.

- Docker Engine version 19.03.0 or higher
- Docker Compose tool version 1.24.0 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: Make sure you have included the intermediate and root CAs into the public part of certificate.

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 does not 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, see About FCM messages.

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.

2.4. 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 Linux platform and Windows platform.

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**

2.4.1. Install OS

This documentation shows how to deploy NoPass application to Linux and Windows platforms. Specifics screenshots and examples will refer to **Ubuntu Server 18.04** and **Windows 10 Professional**

For Ubuntu Server installation instructions, see the Ubuntu official tutorial.

For Windows 10 installation guide, see official Windows site.

What to read next

Allow firewall ports

2.4.2. Allow firewall ports

After that, you have to open the required ports preinstalled on the virtual machine. For information about the list of ports, see Network requirements at **Before you begin**.

LINUX PLATFORM

- Ubuntu uses UFW to protect the system.

For more information about opening ports on the UFW, see the official Ubuntu community forum.

You can disable UFW as well by running the following command:

```
$ sudo ufw disable
```

WINDOWS PLATFORM

- Windows 10 uses Windows Firewall to protect the system.

For more information about opening ports on Windows Firewall, see Windows Firewall Technologies.

What to read next

Create DNS records

2.4.3. 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:

LINUX PLATFORM

```
$ 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 PLATFORM

```
$ (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>
```

What to read next

Install docker and docker-compose tool

2.4.4. Install docker and docker-compose tool

Note: If you use the Linux platform you can skip this section and go to **Install the NoPass application server** to install the required tools automatically.

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

1) Uninstall older version if it is less than required:

LINUX PLATFORM

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

WINDOWS PLATFORM

To uninstall Docker Desktop from Windows machine:

a. From the **Windows Start** menu, select **Settings** > **Apps** > **Apps & features**.
b. Select **Docker Desktop** from the **Apps & features** list, and then select **Uninstall**.
c. Click **Uninstall** to confirm your selection.

Procedure

LINUX PLATFORM

Download a new version of Docker Desktop for Linux from Docker hub and install it. It contains Docker and Docker-compose tools.

For installation instructions, see Install Docker Engine.

WINDOWS PLATFORM

Download a new version of Docker Desktop for Windows from Docker hub and install it. It contains Docker and Docker-compose tools.

For installation instructions, see Install Docker Engine.

What to read next

Install and configure a database server

2.4.5. Install and configure a database server

The application requires a database to store and collection data.

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

- MySql — For installation instructions, see MySql documentation page.
- PostgreSQL — For installation instructions, see the PostgreSQL manual.
- Microsoft SQL — For installation instructions, see the SQL Server installation guide.

What to read next

NoPass Server deployment

3. NoPass Server deployment

This chapter contains the following:

- **Infrastructure schemes**
- **Install the NoPass application server**
- **Stop the NoPass application server**
- **Update the application server**

3.1. Infrastructure schemes

Web portal integration 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.

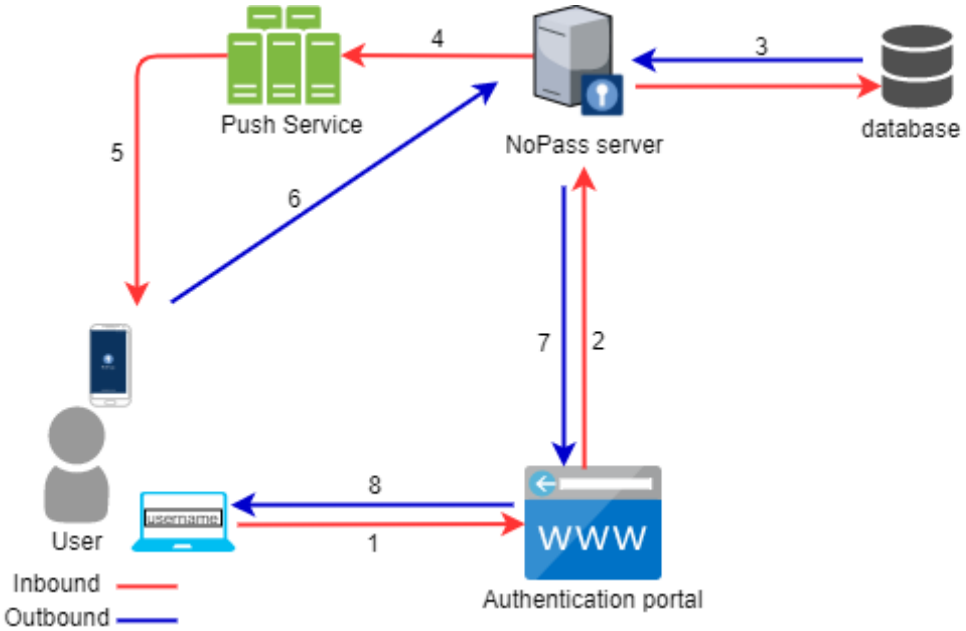


Figure 1. Web Portal Integration Scheme

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) Server generates and sends push requests to the Push service.
5) The push service receives the push request and sends a notification to the user device.
6) NoPass mobile application sends the 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.

The NoPass server works as a proxy server between your corporate RADIUS server and a RADIUS client. It means that when a user of your corporate Network tries to access WiFi, OpenVPN, RDP, or any other client integrated with your corporate Network, the request goes to the NoPass server first. The NoPass server then requests approve from the corporate RADIUS server. If the user is present in the RADIUS server database, the request is approved and the NoPass server sends a push notification to the user's mobile. When the push notification is accepted, the NoPass server sends the response to the RADIUS client. After that, the RADIUS client grants access to the user.

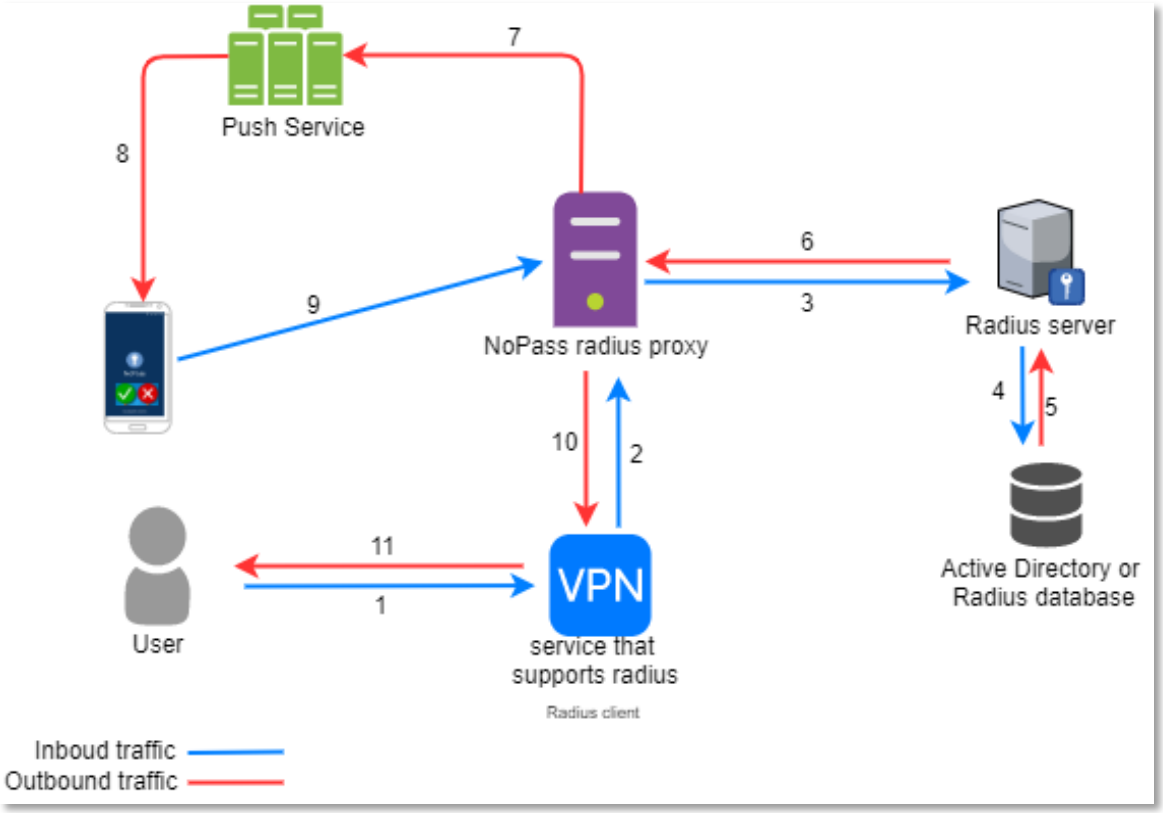


Figure 2. RADIUS Integration Scheme

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) NoPass server intercepts the response from the RADIUS server and secondary authentication via NoPass RADIUS proxy.
6) NoPass server generates and sends a push request to the Push service.
7) The Push service receives the push request and sends notification to the user device.

8) NoPass mobile application 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.

SSO-integration scheme

This authentication scheme shows how SSO clients are authenticated using NoPass. A user browses the page they want to get access to. Then Keyloak checks whether the user is authenticated or not, and if yes, logs them in to the portal or redirects them for authentication to the NoPass.

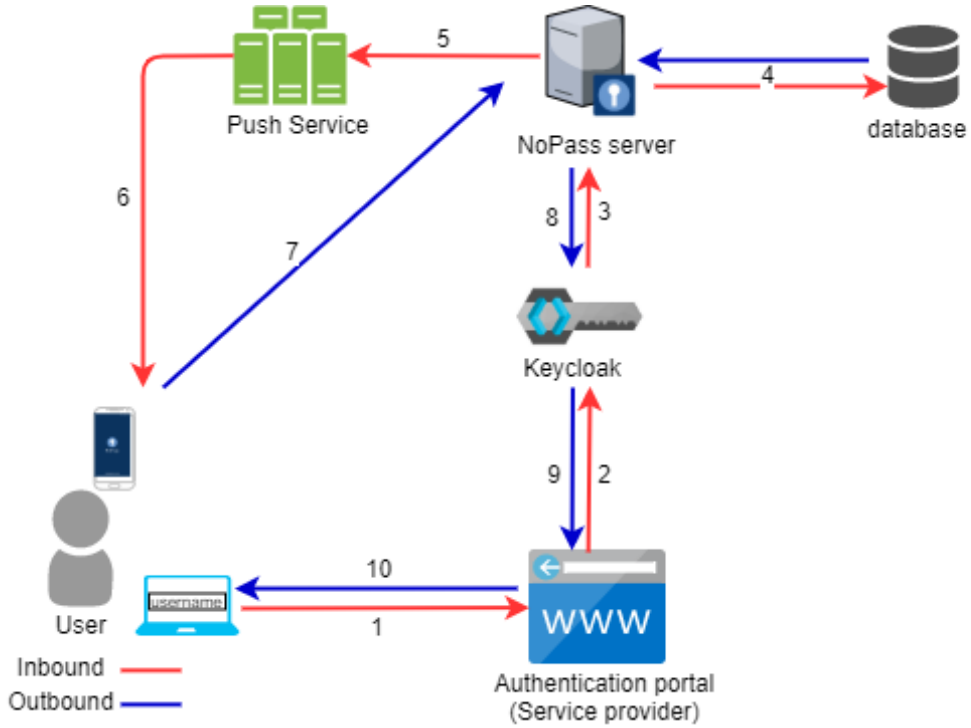
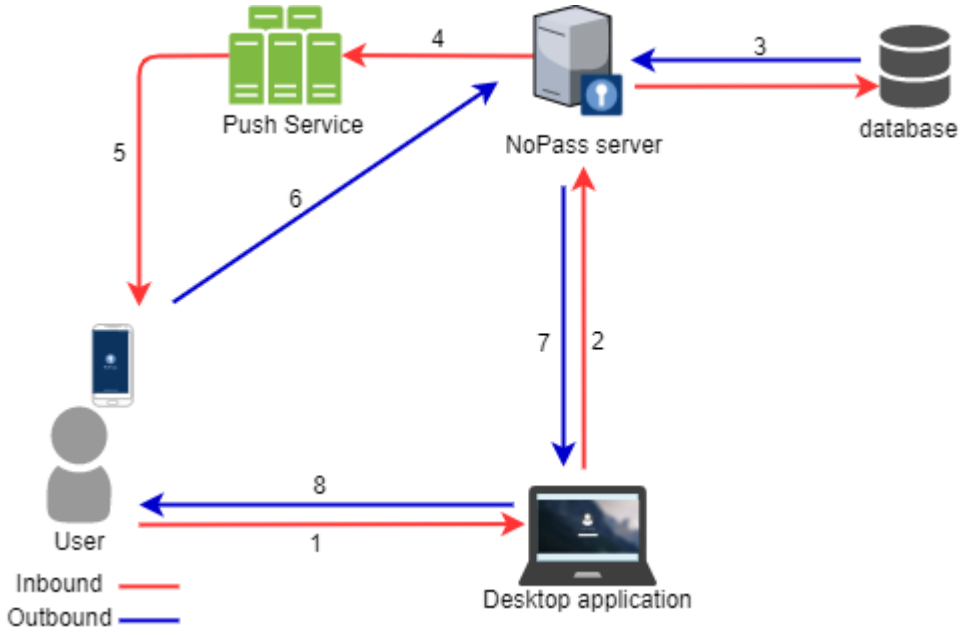


Figure 3. IDP Integration Scheme

1) Initiating primary authentication to the application or service with SSO.
2) The Service provider redirects the user's browser to send a token that contains information about the user to Keycloak.
3) Keycloak checks to see whether the user has already been authenticated and sends a request to NoPass.
4) If the user has not logged in, they will be prompted to enter their username and authenticate via NoPass.
5) NoPass server generates and sends a push request to the Push service.
6) The Push service receives the push request and sends a notification to the user device.
7) NoPass mobile application sends an authentication response from the user device to the NoPass RADIUS proxy.
8) NoPass sends a token back to Keycloak with a response message.
9) Keycloak receives the response message and authenticates or not.
10) The user is granted access to the Service Provider.

NoPass Desktop Unlock integration scheme

The following scheme describes the process of getting an access to a Windows computer using NoPass Desktop Unlock.



1) Initiation of authentication for the application.
2) The NoPass desktop application sends an authentication request to the NoPass application server.
3) The NoPass server checks the user in the database.
4) The server generates and sends push requests to the push service.
5) The push service receives the push request and sends a notification to the user device.
6) NoPass mobile application sends the 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.

What to read next

Install the NoPass application server

3.2. Install the NoPass application server

We provide preconfigured configuration files to help you install the NoPass application server.

Before you begin

- Download the configuration files for your platform from the Identite™ website.

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

Procedure

LINUX PLATFORM

1) Copy the link for Linux platforms, download the archive to your server, and unzip.

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

Unpack the archive:

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

Unpacked files look as follows:

```
root@bionic64:~# tar -xzvf nopass.tar.gz
nopass.bash.script/
nopass.bash.script/variables.env
nopass.bash.script/install.sh
nopass.bash.script/templates/
nopass.bash.script/templates/nginx/
nopass.bash.script/templates/nginx/nginx_preshop.tpl
nopass.bash.script/templates/nginx/nginx_main.conf
nopass.bash.script/templates/nginx/nginx_nopass.tpl
nopass.bash.script/templates/composes/
nopass.bash.script/templates/composes/compose_demo.tpl
nopass.bash.script/templates/composes/compose_prod_nginx.tpl
nopass.bash.script/templates/composes/compose_prod.tpl
root@bionic64:~#
```

2) Open the variable file **variables.env** and fill it according to your needs.

   For detailed information about environment variables, see **Appendix 1. NoPass server environment variables**.

Note: For demo purposes, the database will be created in the container. For production, create a database on another instance by yourself.

3) Copy SSL certificate (Public and Private keys) in this directory

4) Set execution permission to **./install.sh** script

```
$ sudo chmod +x ./install.sh
```

5) Launch the script and follow the commands

```
$ sudo ./install.sh
```

WINDOWS PLATFORM

1) Copy the link for Windows platforms, download the archive to your server, and unzip.

```
$ 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. For reference information about the environment variables, see **Appendix 1. NoPass server environment variables.**

3) Open the Nginx configuration file and path to the NoPass application server.

```
server nopass:80;
```

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

4) Change the DNS name that you created during creating DNS records.

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

5) 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;
```

6) Change the **docker-compose.yml** configuration file if you use the NoPass application server without nginx.

Note: If you want to use your own Reverse proxy server, make sure that it supports TLS 1.3.

7) Replace the row with expose port to row with publish port for NoPass directive. Replace the following:

   a. From the expose port in the Docker bridge network.

```
expose:
      - 80
```

   b. To the publish container's port on the host. You can use any other free port instead of 8001.

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

If you want to use NoPass MFA product for RADIUS authentication you must be open RADIUS ports for the container with command:

```
ports:
    - 8001:80
    - 1812:1812/udp
    - 1813:1813/udp
```

8) Log in to an Identite 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:

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

9) 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:

```
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:

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

10) Check the running application in the browser using the following link:

```
https://SERVER_URL:port/api/status
```

Server status output example:

```
errors:    []
▼ result:
    0:     "Database migration: Ok"
    1:     "Database tables: Ok"
```

What to read next

Stop the NoPass application server

3.3. 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:

LINUX PLATFORM

```
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 PLATFORM

```
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>
```

What to read next

Update the application server

3.3. 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
```

What to read next

Server deployment to AWS using Terraform

4. NoPass Server deployment to AWS using Terraform

This chapter contains the following:

- **Prerequisites**
- **Infrastructure scheme**
- **Preparation**

4.1. Prerequisites

To successfully deploy NoPass on AWS, make sure you have the following:

1) Subscription to one of the NoPass services.
   For more information about available services, see the Amazon marketplace.
2) An IAM user created with Administrative permissions. Access generated and a secret key.
   For instructions, see the Amazon knowledge center.
3) An SSL certificate issued by AWS.
   For instructions on how to request a public certificate, see the Amazon AWS Certificate Manager User Guide.
4) An SSH key generated.
   For the SSH key generation instructions, see Generating a new SSH key at GitHub docs.
5) Terraform installed.
   For instructions, see Download Terraform at Terraform Docs.

What to read next

Infrastructure scheme

4.2. Infrastructure scheme

The following scheme describes the infrastructure that will be installed using the terraform script. It contains the following main objects: VPC, security groups, instances, and databases. Besides, you can see the nonessential services that help to achieve certain security and flexibility. This scheme is relevant for deploying non-clustered infrastructure.

The VPC consists of three subnets: Public, Private, and Database. Public network has direct internet access via Internet Gateway. Private network has internet access via NAT instance that is located in the Public network. Database network does not have internet access.

NoPass server is located on the private network. It is started with the AWS ECS Service. Inbound traffic is routed to the server using AWS Application Load Balancer. It makes traffic termination from HTTPS into HTTP.

At the moment, the script supports only MySQL database installation, but the server supports MySql, PostgreSQL, MSSQL as well.

To improve security, only the networks and ports required for the application are open.

This scheme is relevant for deploying non-clustered infrastructure.

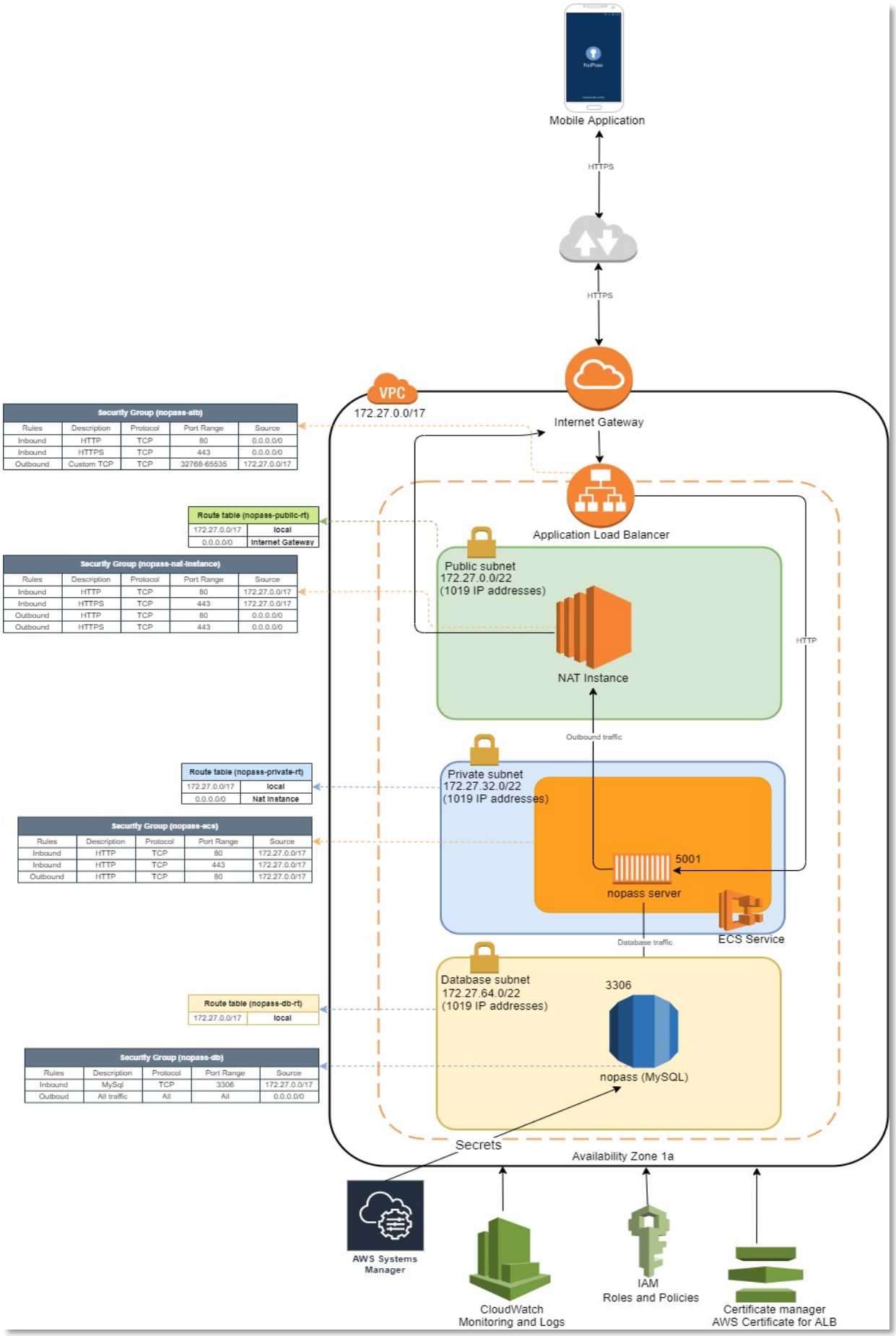


Figure 4. Infrastructure Scheme

What to read next

Preparation

4.3. Preparation

Procedure

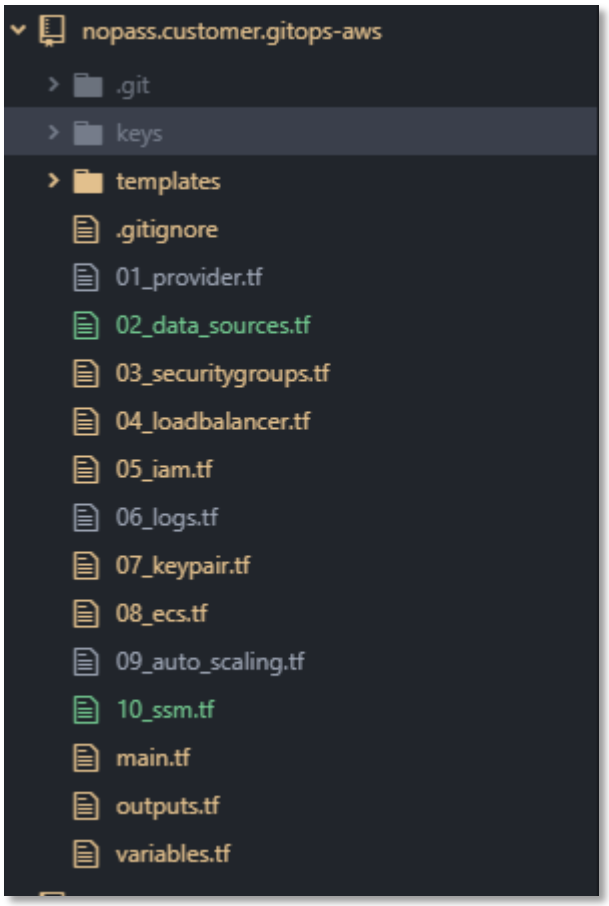
1) Clone the repository with terraform code. Credentials to authenticate:

   Username: nopass.guest02
   Password: Cvsg25xE@r

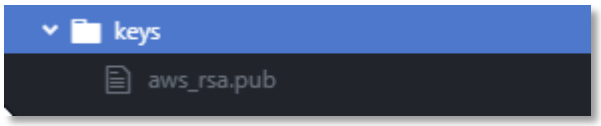
```
$ git clone http://bitgit.psa-software.com/Identite/nopass.customer.gitops-aws.git
$ git checkout tags/v1.0.0 -b v1.0.0
```

```
senko@DESKTOP-2JR687P MINGW64 /d/MyProjects
$ git clone http://bitgit.psa-software.com/Identite/nopass.customer.gitops-aws.git
Cloning into 'nopass.customer.gitops-aws'...
warning: redirecting to https://bitgit.psa-software.com/Identite/nopass.customer.gitops-aws.git/
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 18 (delta 0), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (18/18), 8.77 KiB | 147.00 KiB/s, done.
```

List of files in the repository:



2) Copy the SSH key that you generated previously to the keys folder with the name **aws_rsa.pub**.



3) Set environment variables for authentication in AWS. For more information about variables generating, see **Appendix 1. NoPass server environment variables**. The access key and secret key should have been created earlier. Set the desired region. For example:

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
$ export  AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
$ export AWS_DEFAULT_REGION=us-east-1
```

4) Open the **variables.tf** file for more detailed settings or skip this step.

5) Initialize the project.

```
$ terraform init
```

```
senkoa@BYMINPC91 MINGW64 /d/git/nopass.customer.gitops-aws (master)
$ terraform init
Initializing modules...

Initializing the backend...

Initializing provider plugins...
- Using previously-installed hashicorp/template v2.2.0
- Using previously-installed hashicorp/aws v3.13.0
- Using previously-installed hashicorp/random v3.0.0

The following providers do not have any version constraints in configuration,
so the latest version was installed.

To prevent automatic upgrades to new major versions that may contain breaking
changes, we recommend adding version constraints in a required_providers block
in your configuration, with the constraint strings suggested below.

* hashicorp/random: version = "~> 3.0.0"
* hashicorp/template: version = "~> 2.2.0"

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

6) Run the infrastructure building simulation. Enter the following values:

- AWS Certificate domain name.
- Docker image path.

- EC2 instance type

  For the AWS EC2 type list, see Amazon EC2 Instance Types.

  We recommend use t3.small < 200 RPS.
- EC2 memory limit. Specify the required memory limit for the container. For example: t3.small has 2GB memory, the limit on the container can set up at 1536.
- AWS region.

  For the AWS regions list, see What is Amazon EC2

```
$ terraform plan
```

If you get a successful result then you can run with the key apply:

```
$ terraform apply
```

Approximate setting time: 10 min
The result is as follows:

```
Outputs:

alb_hostname = nopass-1807382529.us-east-1.elb.amazonaws.com
db_password = pMnzHa28t0BU7fZQ
db_password_arn = arn:aws:ssm:us-east-1:101259527774:parameter/nopass/prod/database/password
```

Please use these values for the following purposes:

- alb_hostname: create a DNS CNAME record to this load balancer url
- db_password: password to connect to the database
- db_password_arn: password storage path in the AWS secrets

7) To destroy infrastructure, run the command:

```
$ terraform destroy -auto-approve
```

What to read next

NoPass RADIUS portal

5. Licensing

We offer licenses for the following integrations: web, RADIUS, SSO, UNLOCK, and SDK. You need to get a license prior to registering a portal or a service.

Warning: DO NOT begin registering a portal before getting the license!

Getting the license

1) Send a license request to sales@identite.us.

Make sure your request contains the following information: service type, portal domain name, service domain name. In the table below, see the example request depending on a certain NoPass product.

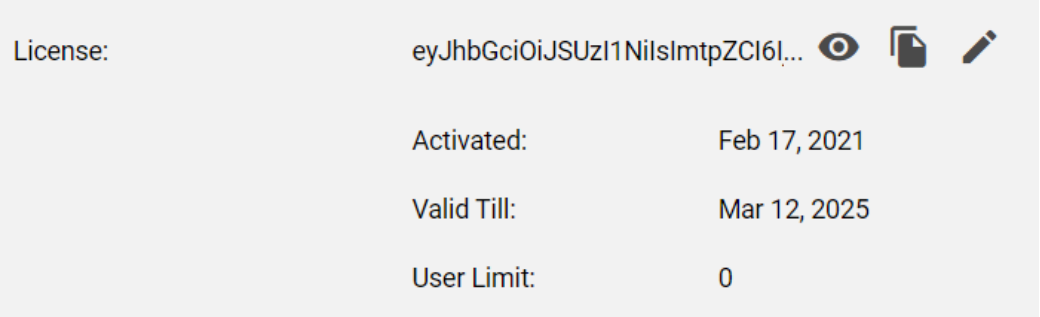
Request information	NoPass™ Consumer	NoPass™ SDK	NoPass™ Employee MFA	NoPass™ Desktop Unlock	NoPass™ Employee SSO
Service type	Portal service	SDK	RADIUS service	Unlock	Identity provider
Portal domain name	`<portal.example.com>:port`	`<portal.example.com>:port`	-	-	`https://{Keycloak URL}/auth/realms/{Realm}`
Service domain name	`nopass.<example.com>:port`	`nopass.<example.com>:port`	`nopass.<example.com>:port`	`nopass.<example.com>:port`	`nopass.<example.com>:port`
Android app package name	N/A	+	N/A	N/A	N/A
iOS app bundle ID	N/A	+	N/A	N/A	N/A

If you want to purchase a product with SDK, specify the information about the Android app package name/iOS app bundle ID in your request.

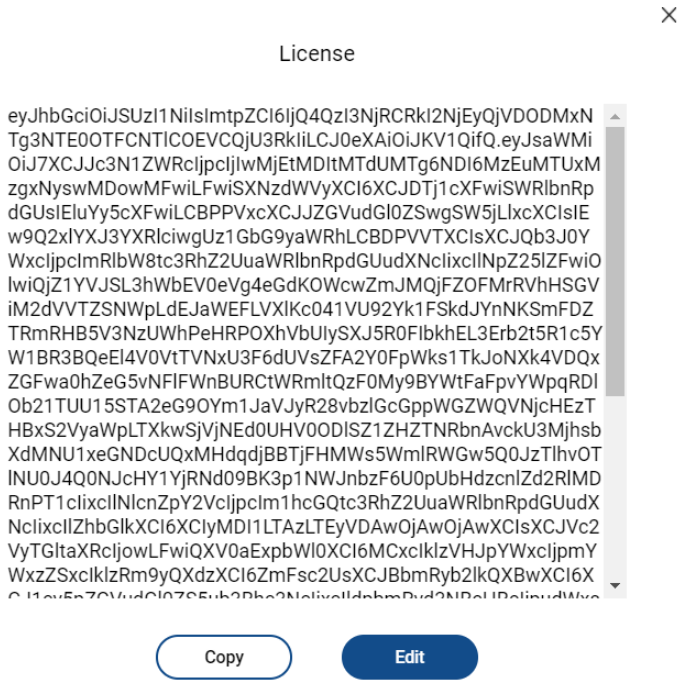
2) Check your email for the message from the NoPass team. In this email, you will receive your license.
3) Copy the license file. You will need this file during the portal registration.

Managing the license

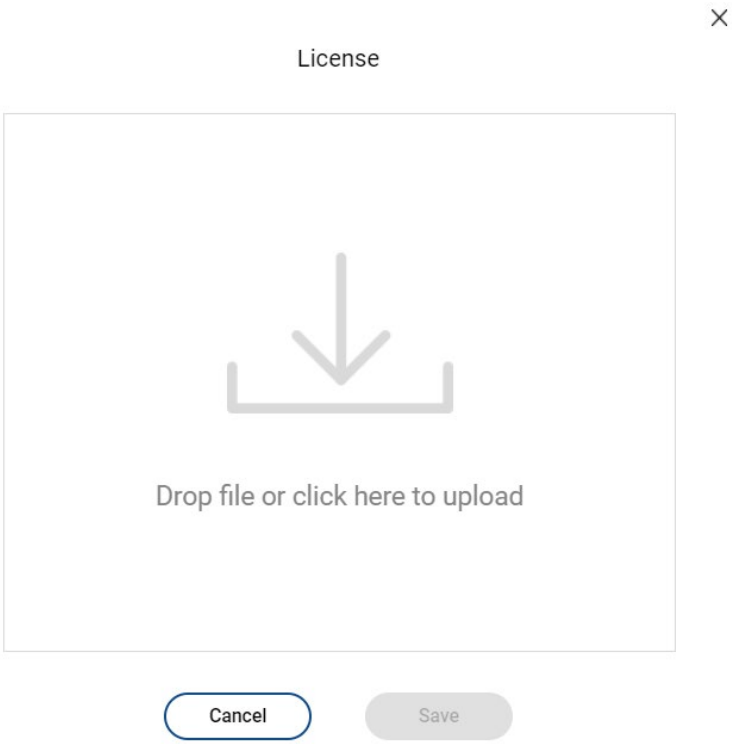
1) Go to NoPass Admin Panel.
2) On the **Settings** tab, in the **General information** group, do one of the following:



- Click **View** to view, copy or edit the license.



- click **Copy** to copy the license text
- click **Edit** to update your license and drag the new license to the window.



3) Click **Save**.
   Your license is updated.

What to read next

NoPass Integrations

6. NoPass RADIUS portal

NoPass RADIUS portal is an intermediate member that provides connection between the NoPass server and your corporate radius server to use NoPass as a 2FA when accessing corporate radius clients like WiFi, VPN, RDP, etc.

This chapter contains the following:

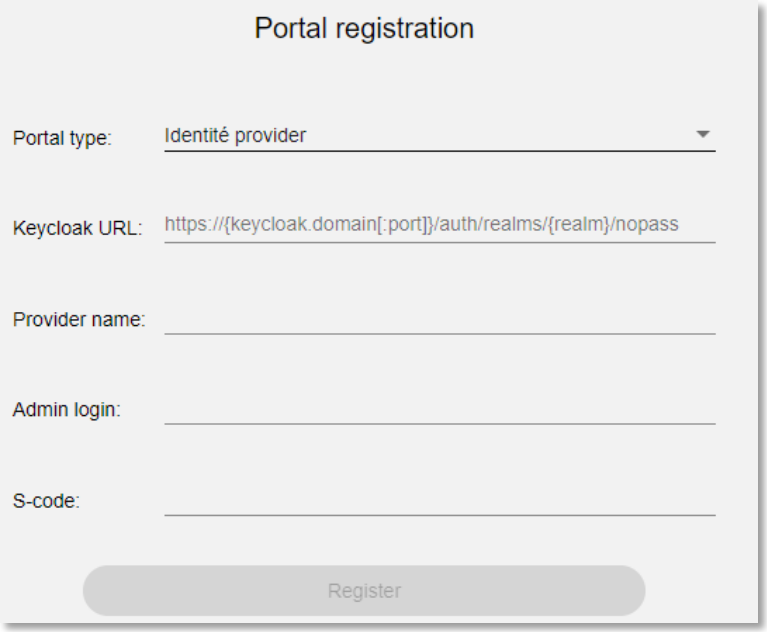
- **How to register RADIUS portal**
- **How to configure RADIUS portal**
- **How to bind a User**

6.1. How to register RADIUS portal

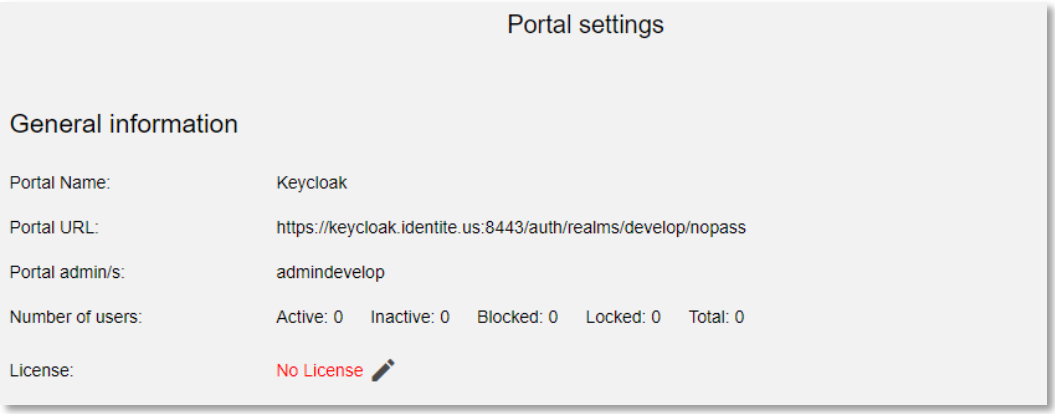
Procedure

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

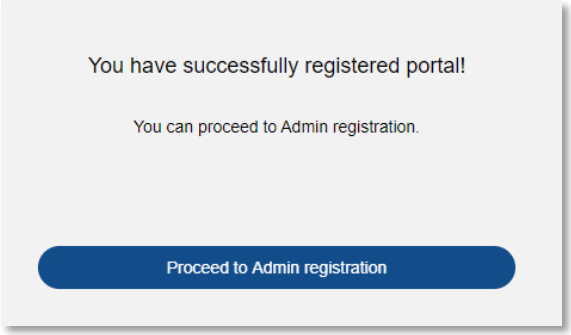
Portal type	RADIUS server
Portal name	The portal name is displayed in this field
Admin login	By default, the admin login is *<radiusadmin>*. To override this value, you can use the environment variable for the NoPass server. For more information about environment variables, see **Appendix 1. NoPass server environment variables**.
S-code	Admin password. The same as in the Admin login field. By default, it is *<radiuspassword>*.



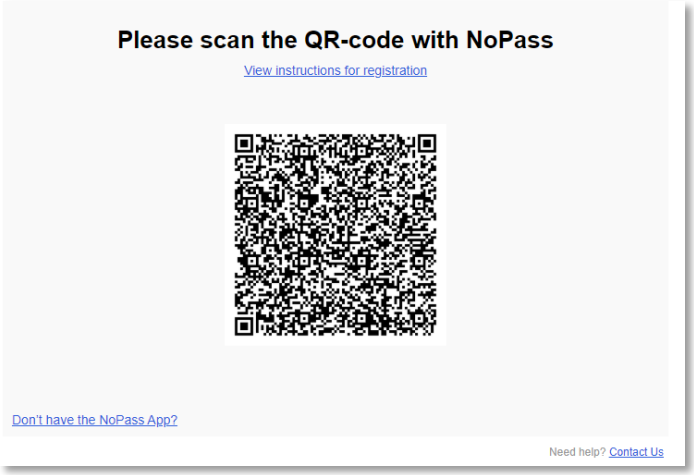
2) On **Portal settings**, configure the settings and add the license file.



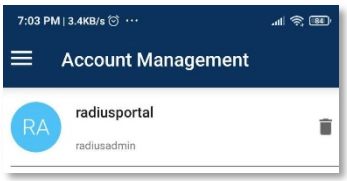
A successful result is as follows:



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



The result on your mobile phone is as follows:



What to read next

How to configure RADIUS portal

6.2. How to configure RADIUS portal

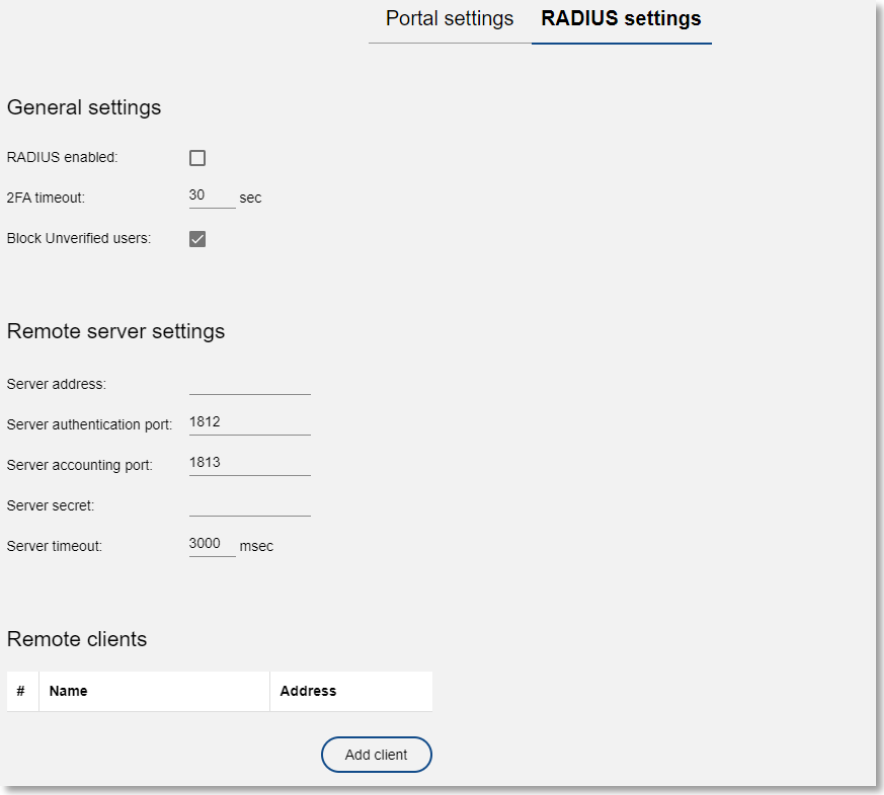
Procedure

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.

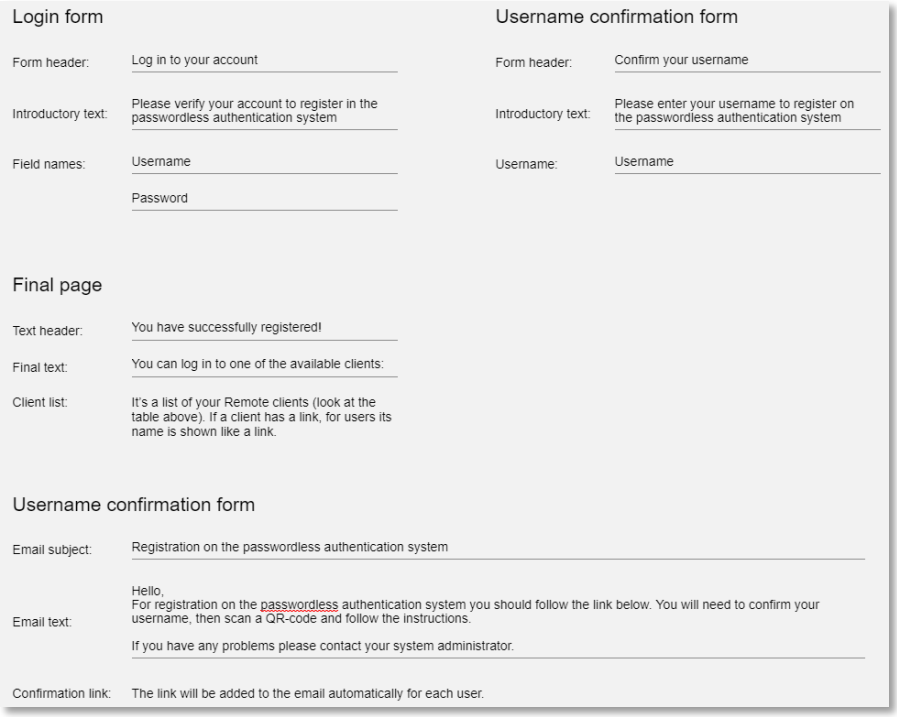


3) In the **RADIUS settings** tab, in the **General settings** group, configure the following parameters:
   a. Select **RADIUS enabled**.
   b. Set **2FA timeout**—confirmation timeout on a mobile device—less than the service connection timeout.
   c. Select **Block Unverified users** to block connection for unverified users.
4) In the **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 **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 topic

Licensing

What to read next

How to bind a User

6.3. 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.

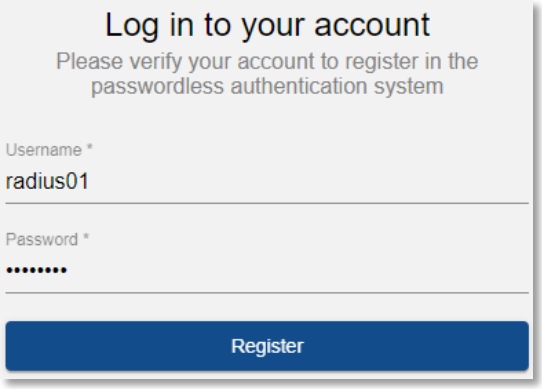
There are two ways to bind a user to the NoPass server depending on the type of RADIUS authentication protocol.

Procedure 1

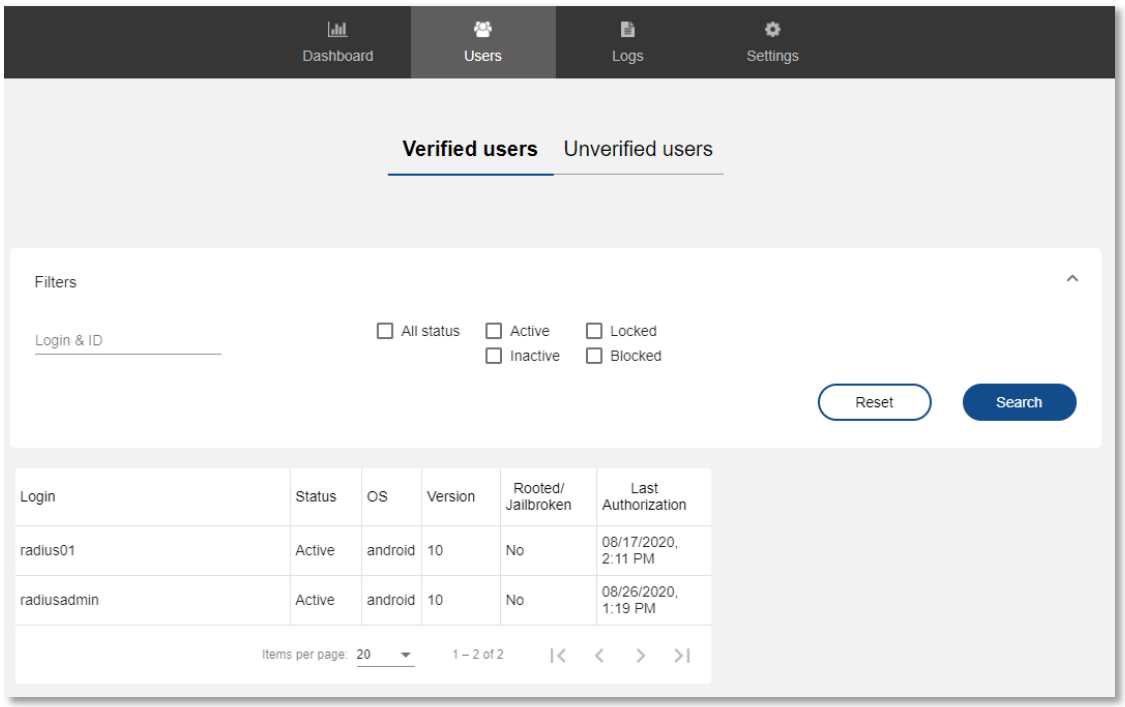
To bind a new user if the **PAP/CHAP/MS-CHAP/MS-CHAPv2** settings of your RADIUS server are enabled, do the following:

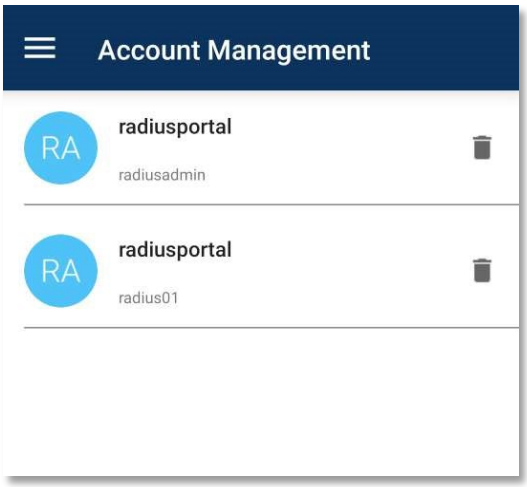
1) Register an administrator using the following link:

```
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.



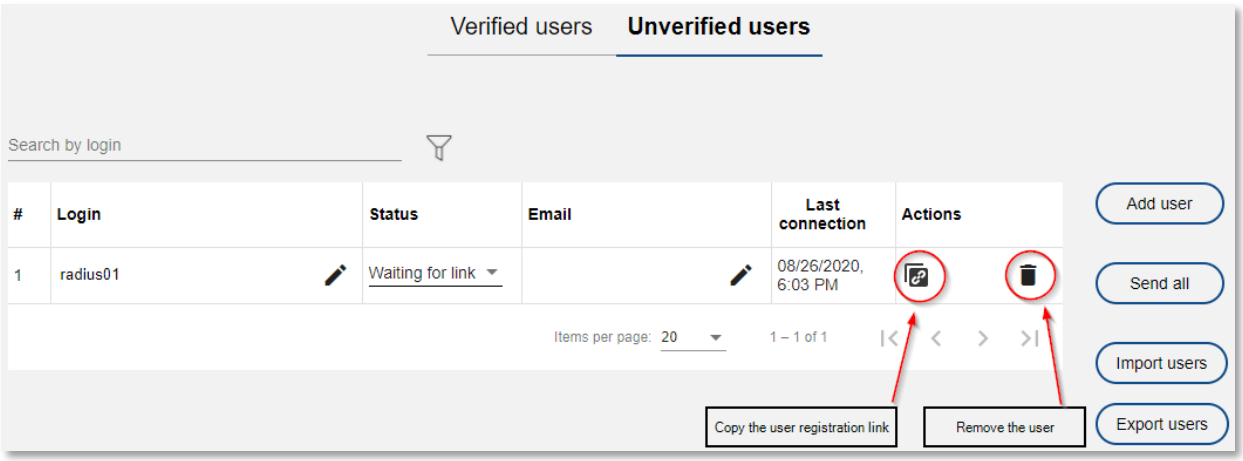


Procedure 2

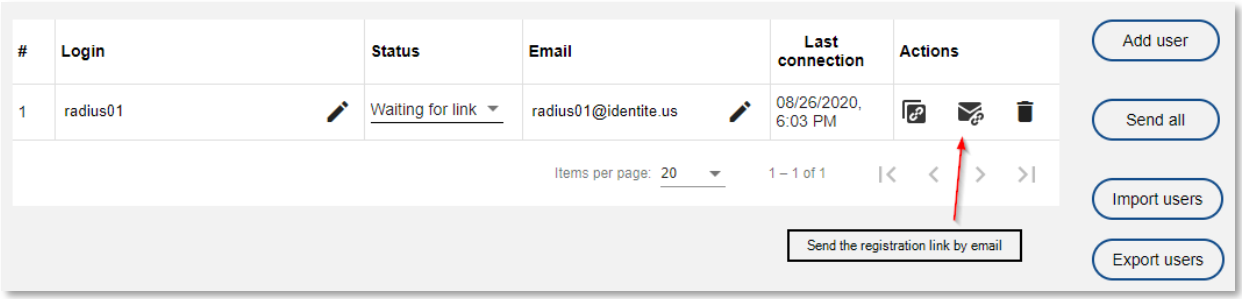
To bind a new user with any RADIUS authentication protocol, do the following:

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**.

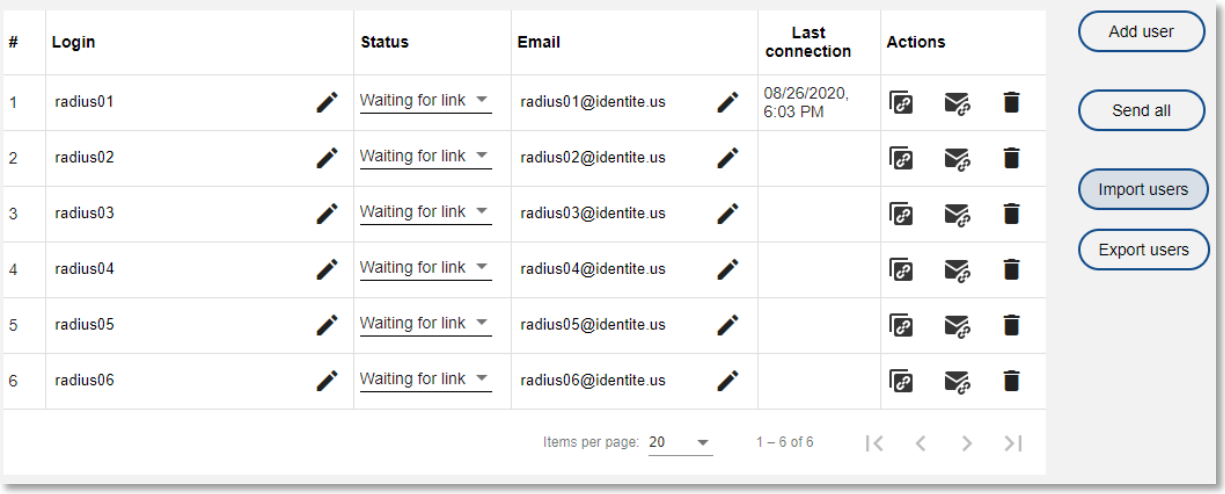


2) Send the unique registration link to the user. You can send it by email but you have to enter the email address for user.



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.

What to read next

Identity Provider and Service Provider management

7. Identity Provider and Service Provider management

This chapter contains the following:

- **Prerequisites**
- **Set up the NoPass extension**
- **Set up service providers with Keycloak**

7.1. Prerequisites

1) Download and install the Keycloak identity and access management application to integrate the NoPass application with the identity provider.
2) Download the extension and NoPass theme from the Identité Repository, and then do the following:
    a. To install the extension, copy the downloaded files to the **$keycloak_home/standalone/deployments** directory.
    b. To install the theme, unzip the archive and copy the files to the **$keycloak_home/themes/** directory.

To enter to the Identité Repository, use the credentials that you received form the Identité team by email.

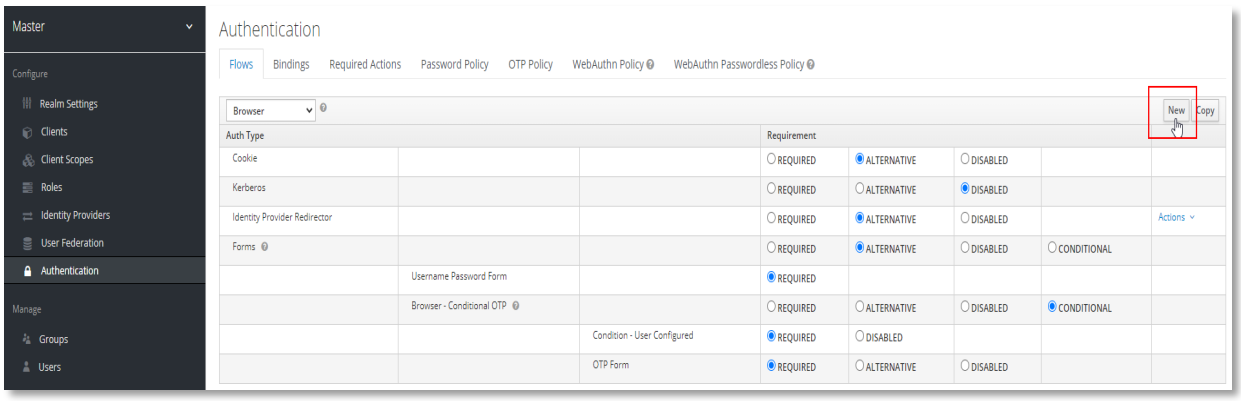
What to read next

Set up the NoPass extension

7.2. 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.



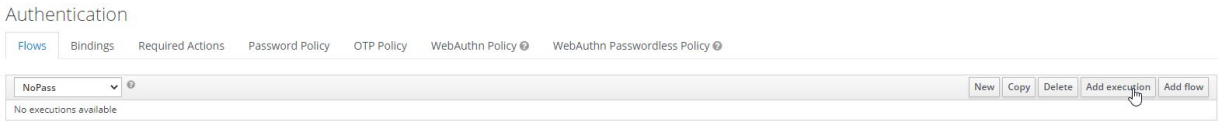
2) To identify the flow, in the **Alias** field enter the alias name.

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

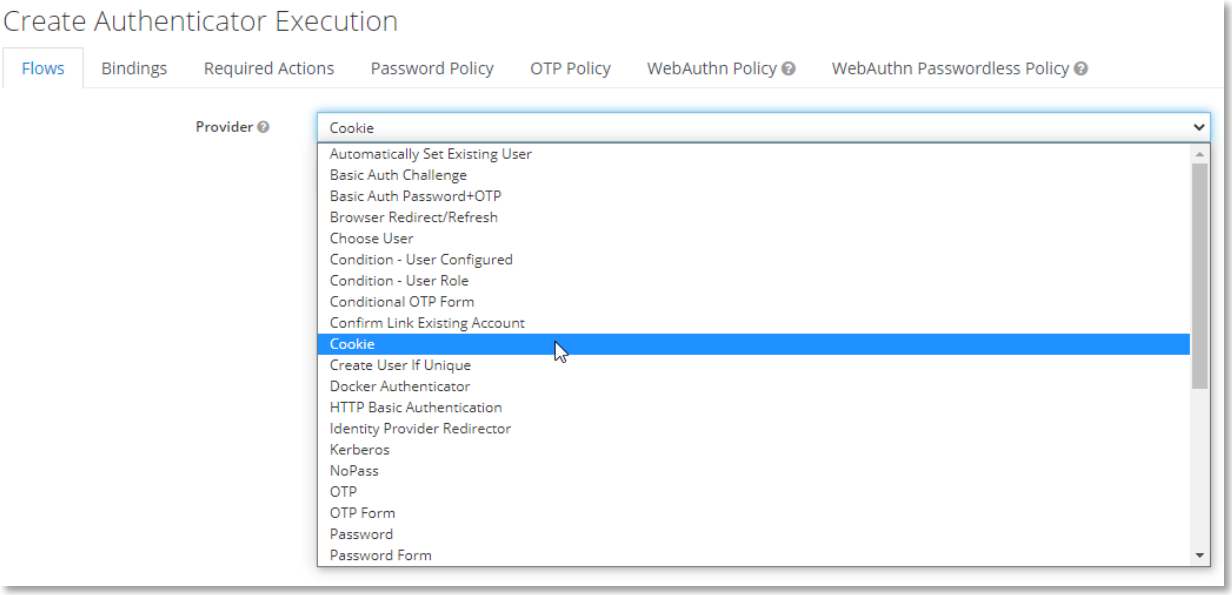
3) In the **Top Level Flow Type** box, select **generic**, and then click **Save**.

4) After you have successfully created the new flow, you need to add a new execution.

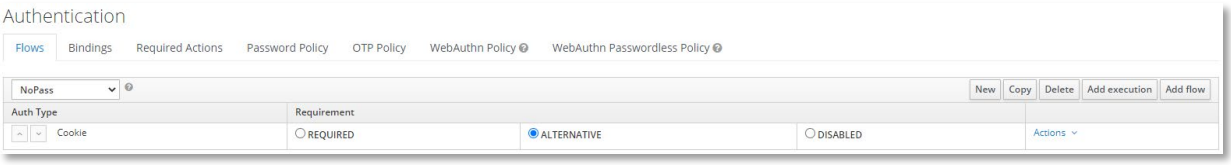
5) In the **Flows** tab, select **Add execution**.



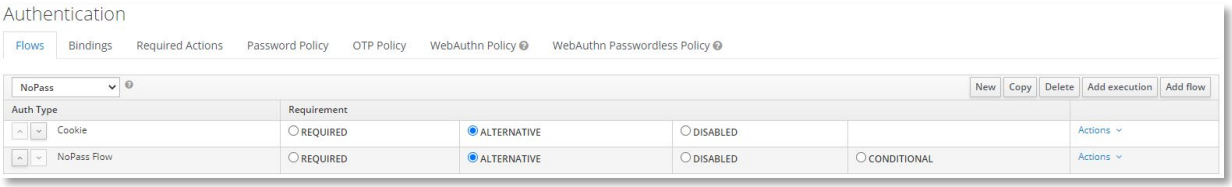
6) From the **Provider** list, select **Cookies**.



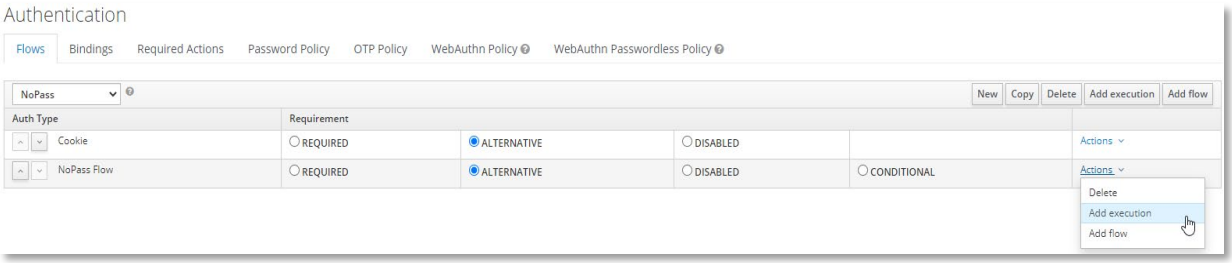
7) Select **ALTERNATIVE** to enable cookies as an alternative authentication method.

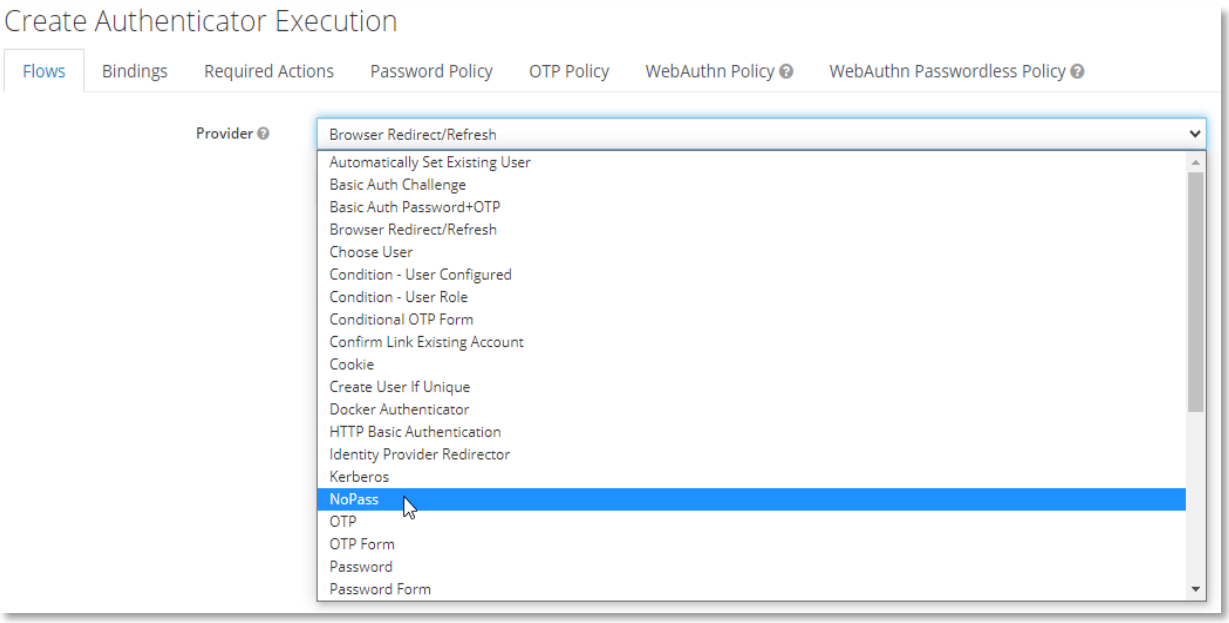


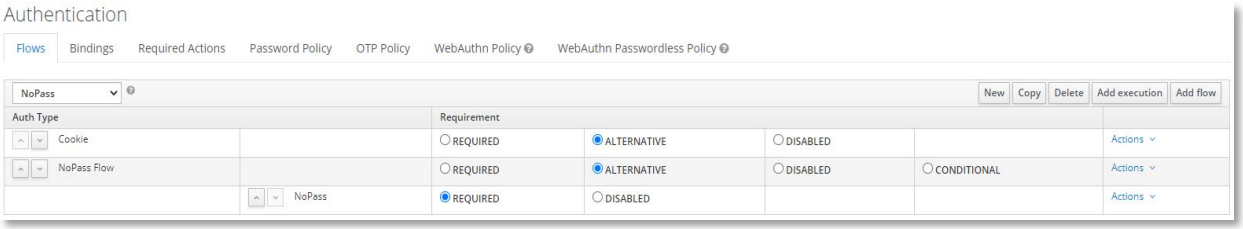
8) Add a new flow for NoPass Authentication and enable it as an alternative authentication method.



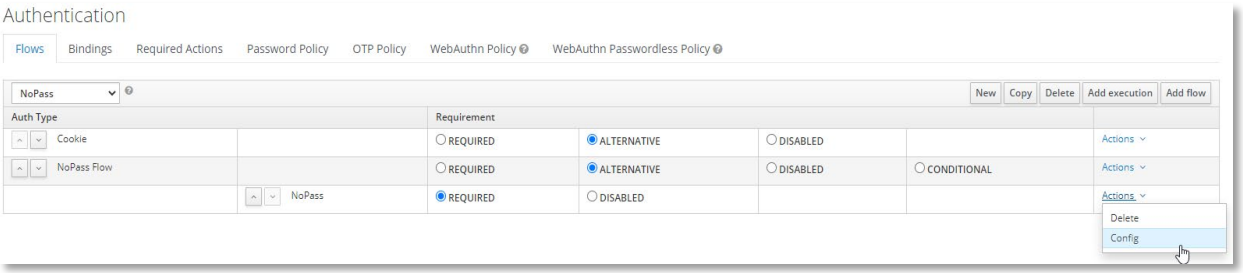
9) Under **Actions**, select **Add execution** to add the NoPass execution to the **NoPass Form** flow, and then select **REQUIRED**.







10) Under **Actions**, select **Config** to configure the extension.

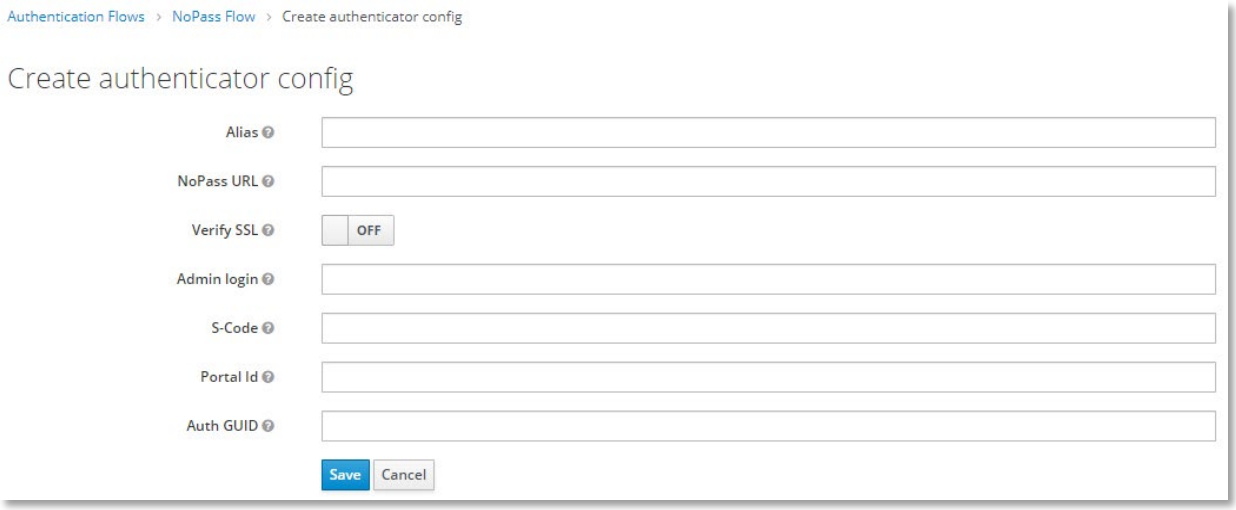


11) In the **Create authenticator config** dialog, enter the following parameters for the NoPass server, that you have installed earlier:

- **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



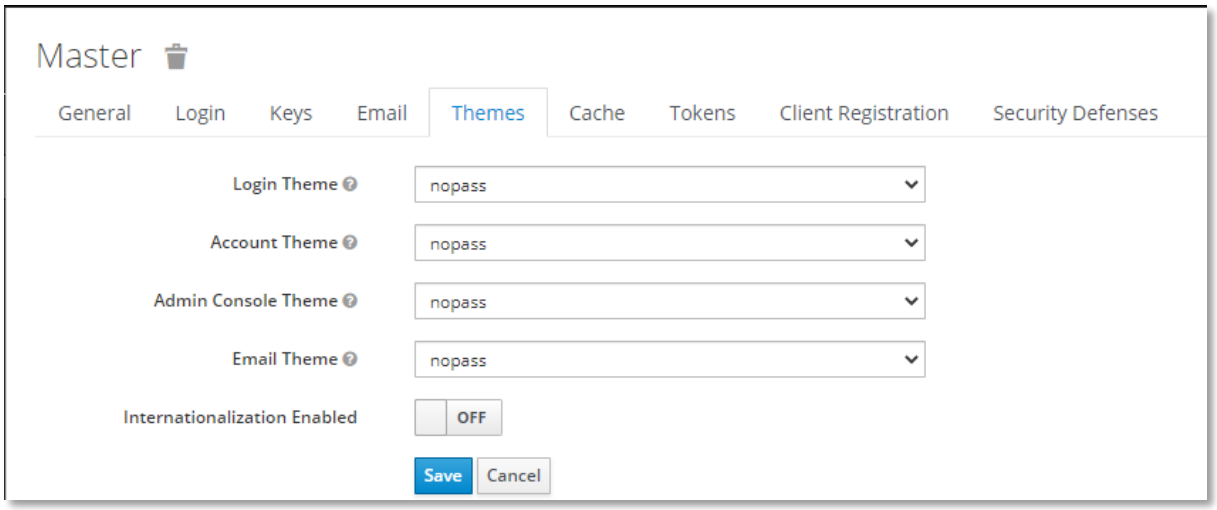
What to read next

Set up the NoPass theme

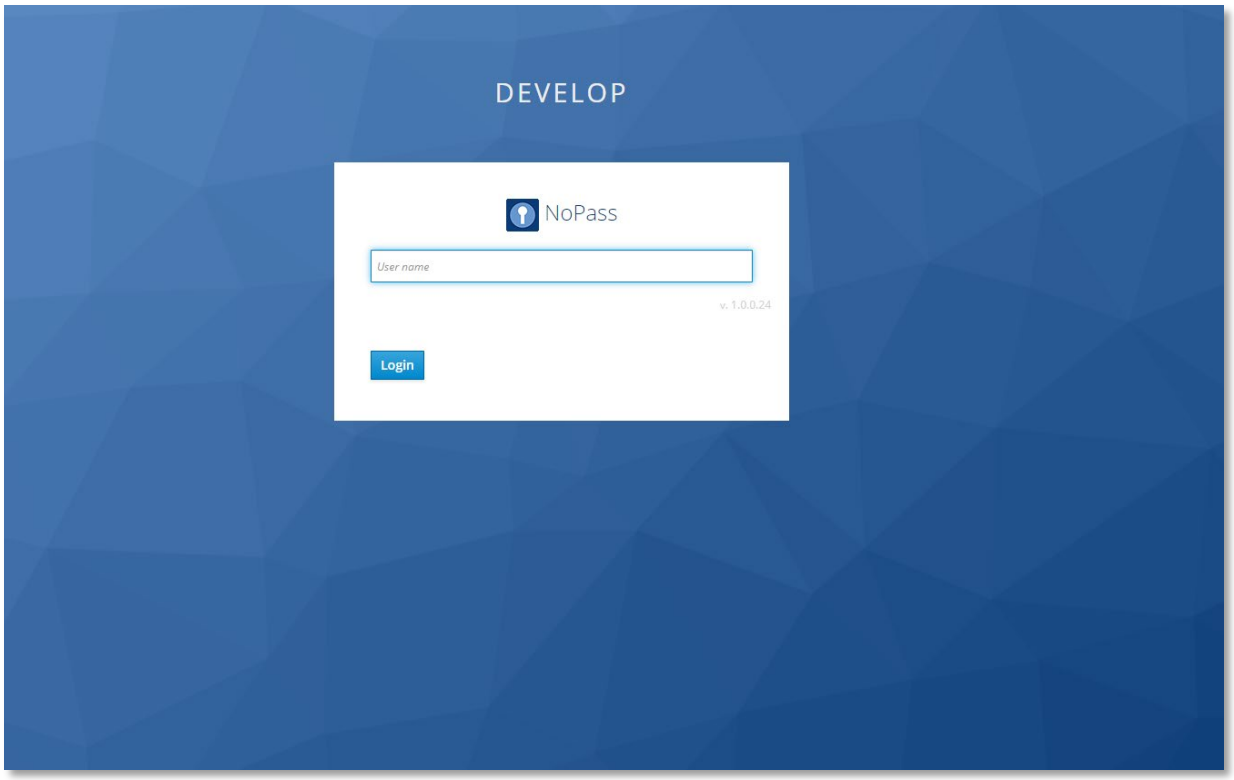
7.3. Set up the NoPass theme

To set up the NoPass theme, do the following:

1) From the Administration Console, select the required realm.
2) In the **General** tab, toggle **Enabled**.
3) In the **Themes** tab, set the following parameters and click **Save**:
    a. **Login Theme**—nopass
    b. **Account Theme**—nopass
    c. **Admin Console Theme**—nopass
    d. **Email Theme**—nopass



A successfully installed theme looks as follows:



What to read next

Set up service providers with Keycloak

7.4. 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-----
```

What to read next

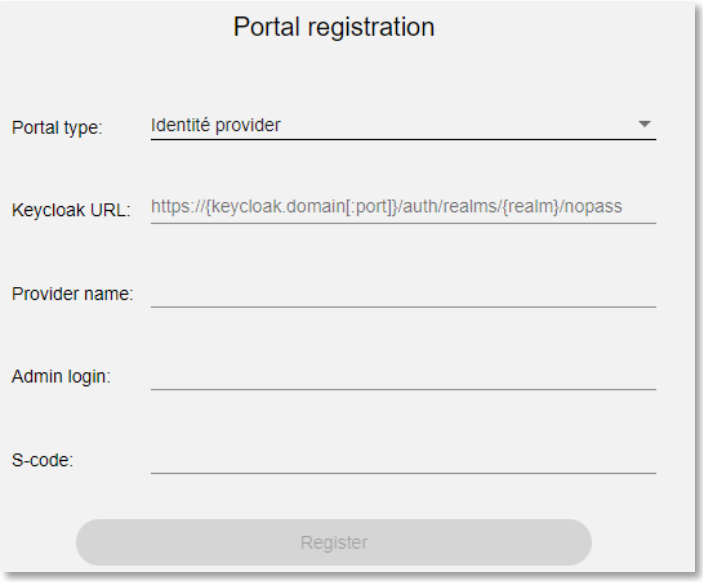
Register an Identity Provider

7.5. Register an Identity Provider

Procedure

To register an identity provider, do the following:

- 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.



Now your identity provider is registered.

What to read next

Web portal management

8. WEB PORTAL MANAGEMENT

This chapter contains the following:

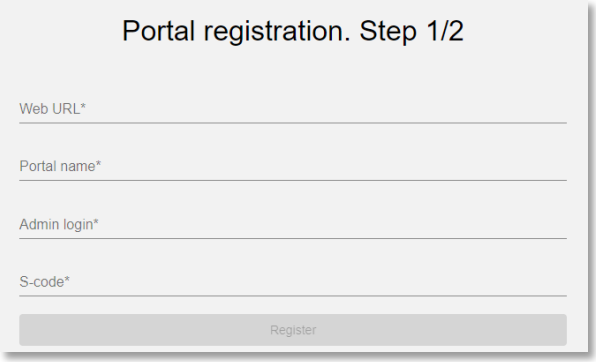
- **How to register a web portal**
- **How to register a web portal in the application server**
- **How to create an administrator account on the Preshop portal**

8.1. How to register a web portal

Procedure

To register a 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) **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.

What to read next

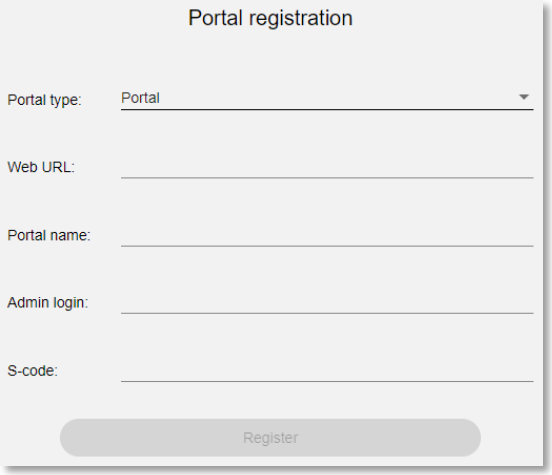
How to register web portal in the application server

8.2. How to register a web portal in the application server

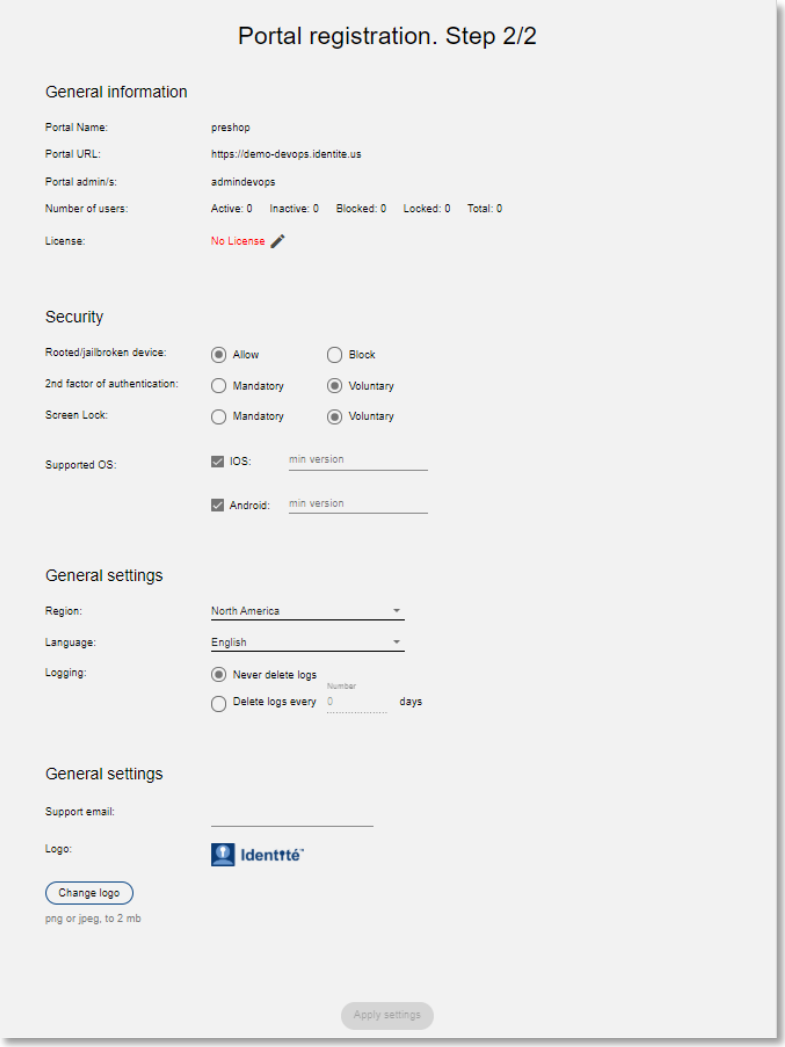
Procedure

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

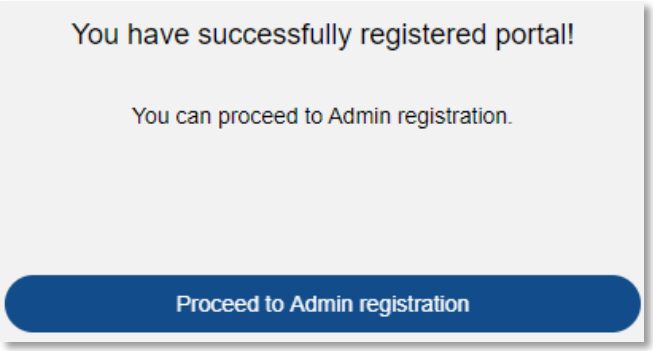
Web URL	Authentication portal
Portal Name	Unique portal name in the database
Admin login	Admin login name from the previous stage
S-code	Password that has been generated at the previous stage.



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:

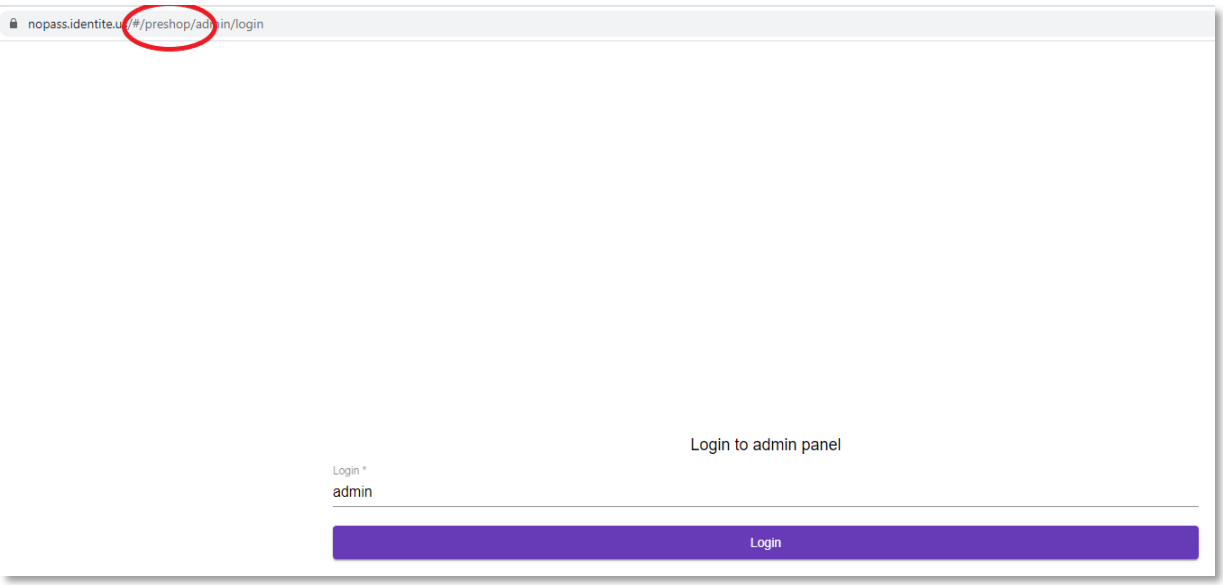


5) Click **Proceed to Admin registration**, scan the QR code, and enter the confirmation code.

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 topic

Licensing

What to read next

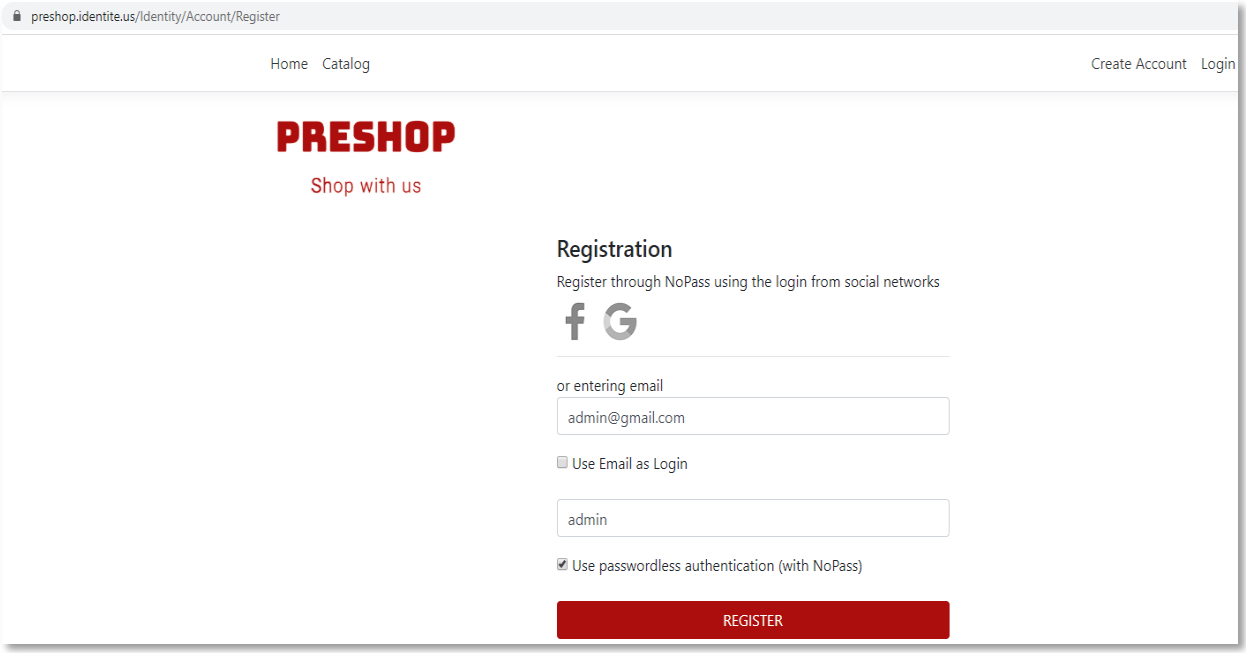
How to create an administrator account on the Preshop portal

8.3. How to create an administrator account on the 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 into the **AdminID** field in Step 2, **How to register the web portal in the application server**, and click **Register**.



What to read next

Licensing

9. NOPASS DESKTOP UNLOCK

NoPass Desktop Unlock is an alternative method of interactive user authentication and access management on machines running Windows operating system.

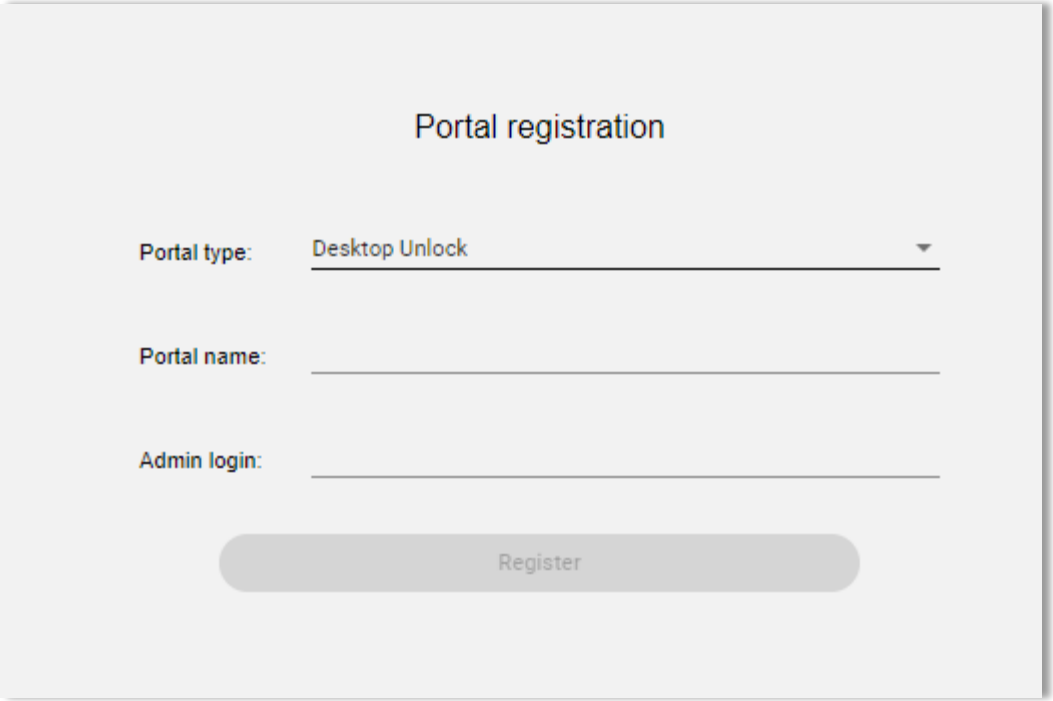
As an intermediate member, it provides connection between the NoPass server and your corporate server to provide passwordless authentication and Two-Factor authentication as an option when accessing a Windows desktop computer.

This chapter contains the following:

- **Register the portal and create an admin**
- **Installation**

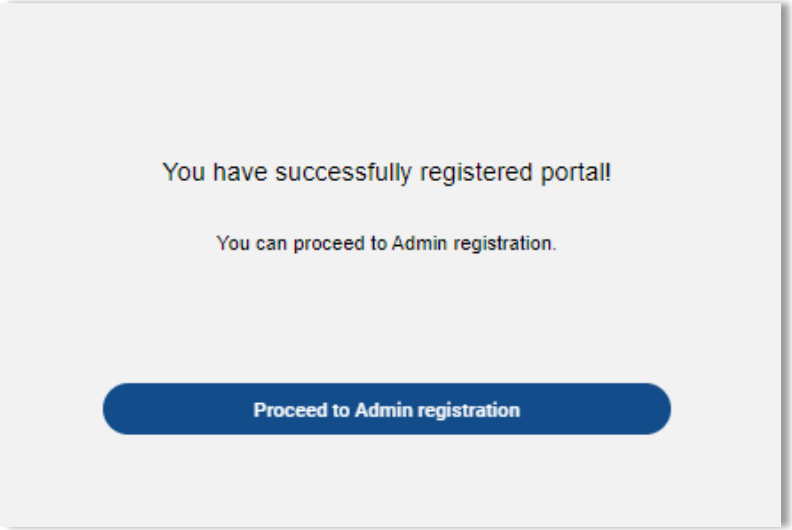
9.1. Register the portal and create an admin

1) On the portal registration page, set the following parameters, and click **Register**:
   a. From **Portal Type**, select **Desktop Unlock**
   b. In the **Portal Name** field, enter a unique name.
   c. In the **Admin login** field, enter your login.

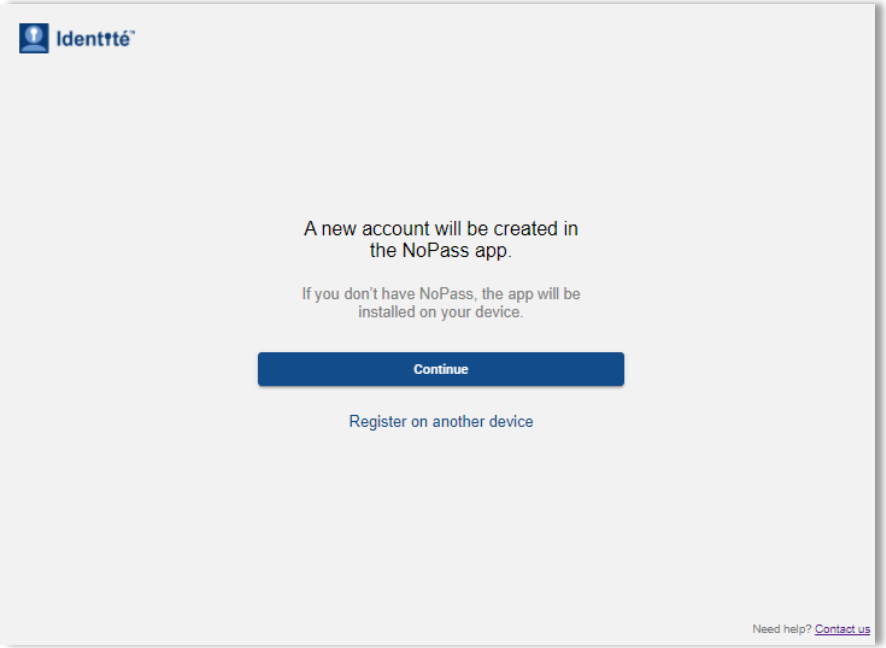


If the registration is successful, you will be redirected to the next page for licensing.

2) In the **Licensing** group, click **Edit** to add the license file.
3) Drag your license file into the window and click **Save**.



4) Click **Proceed to Admin registration** and scan the QR-code to link the account to your desktop application.

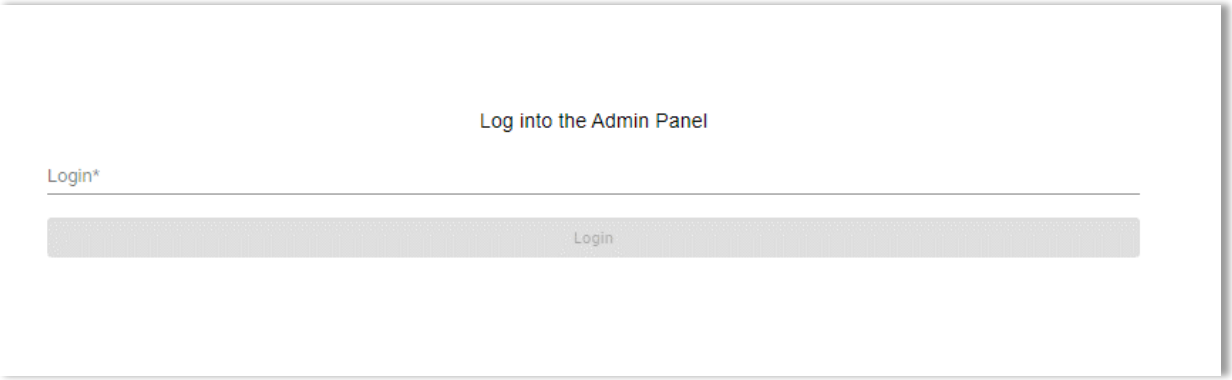


Warning: By default, the session timeout is set to 300 seconds. Make sure to register during this period of time, otherwise it will not be possible to complete the registration procedure.

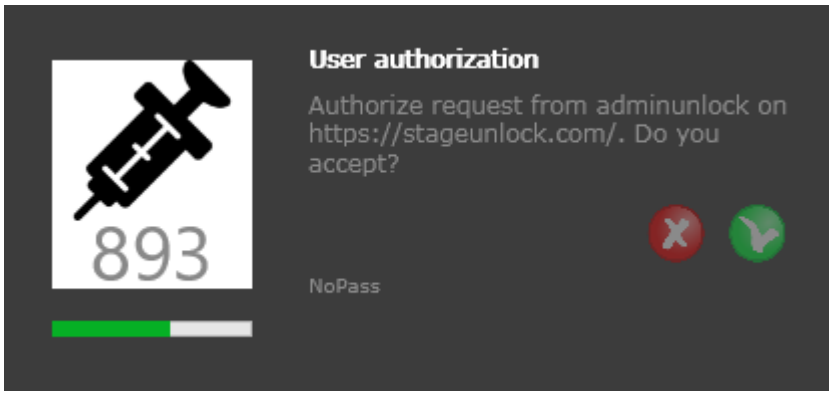
Now, you can enter the Admin Panel.

Enter the Admin Panel

1) Go to https://<*serverURL*>/#/portalname/admin/login



2) In the **Login** field, enter your admin login.
3) On a push notification, click **Accept**.



You have entered the NoPass Desktop Unlock Admin Panel.

For more information about Admin Panel controls and managing user accounts, see *The NoPass Administrator Manual*.

9.2. How to install the NoPass Desktop Application

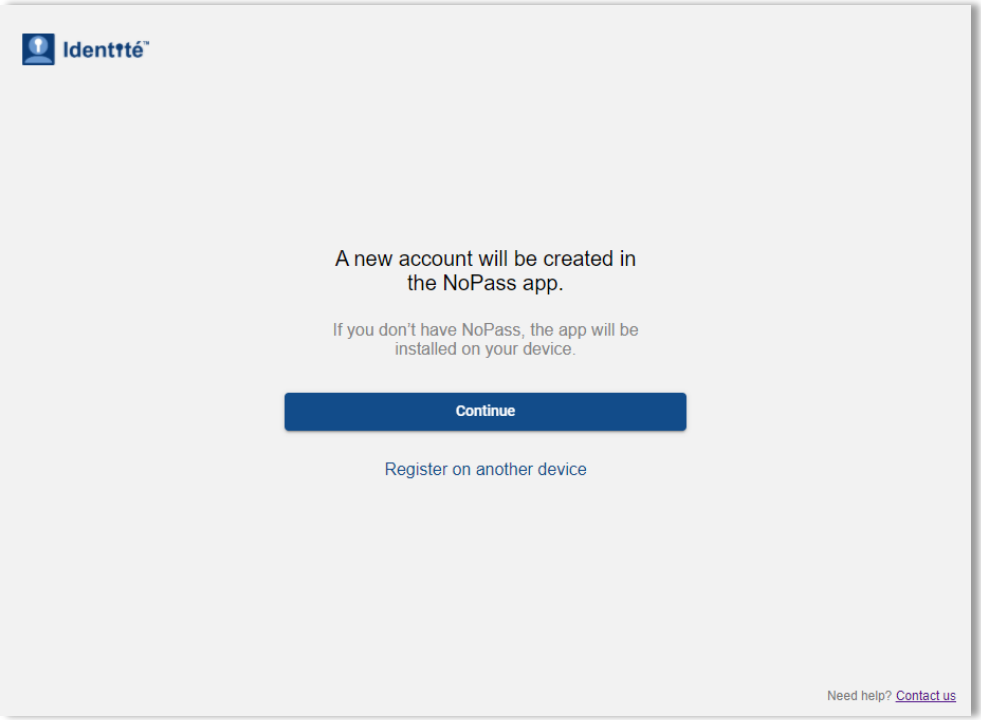
A user installs a desktop client on the computer they want to unlock using NoPass Desktop Unlock. Then, they need to register an account and synchronize it with their mobile NoPass application to be able to receive push notifications.

Prerequisites

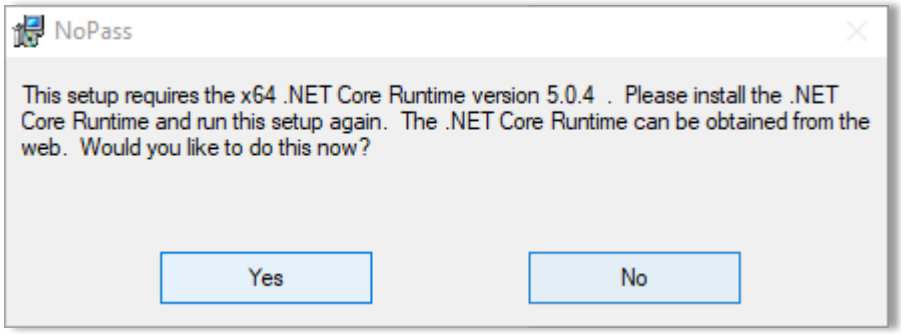
For correct work of the NoPass Desktop Unlock feature, you will need Microsoft .NET SDK 5.0.201 installed on your computer.

Install the NoPass Desktop Application

1) Go to https://*<serverURL>*/#/*<portalname>*/user-confirmation and click **Continue** to download the NoPass Desktop Application.

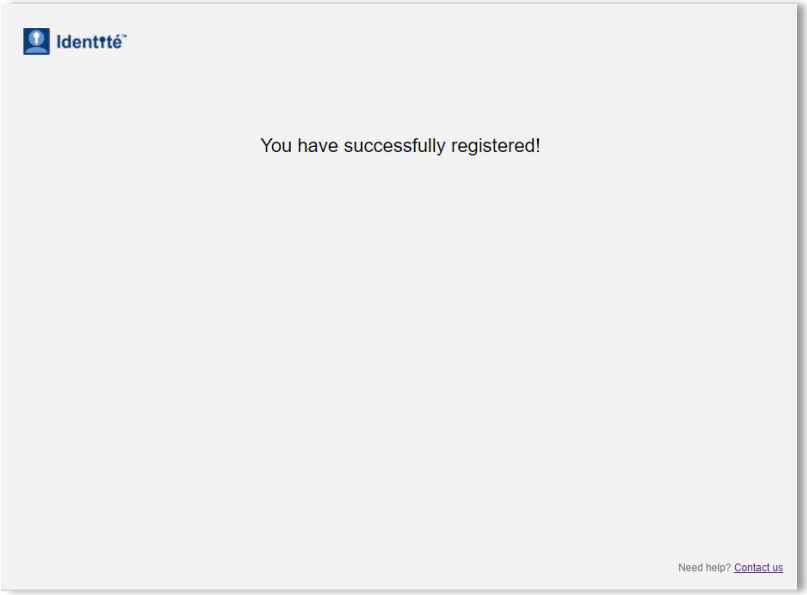


2) Follow the **NoPass Setup Wizard** instructions.



3) Locate the NoPass Setup program on your computer and launch it again to start the registration process.

The registration will be completed automatically.

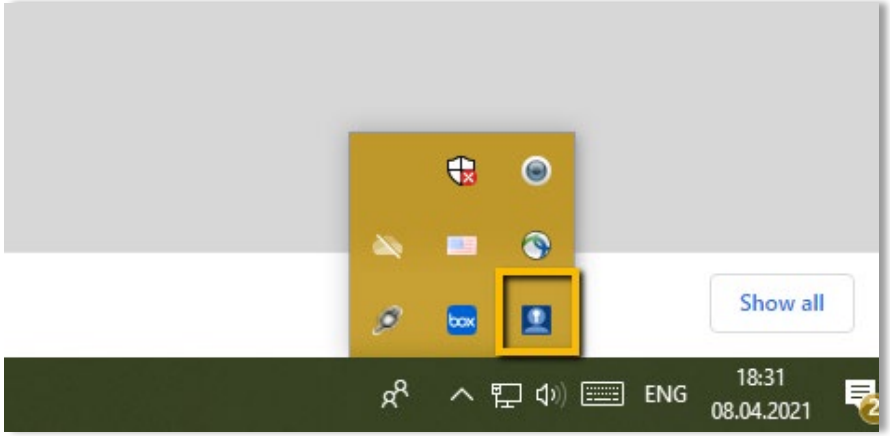


4) Close the browser window.

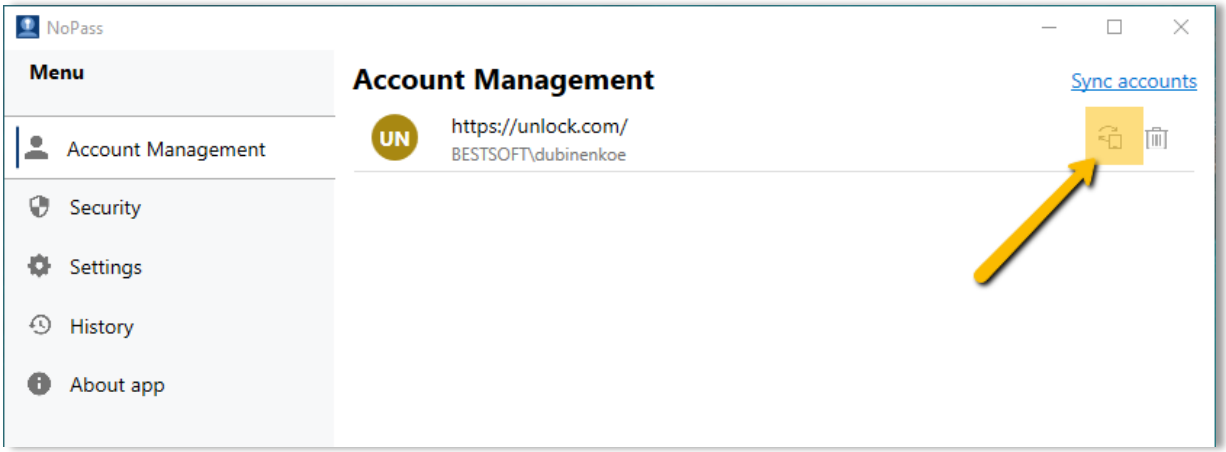
Synchronize the devices

Before you can start using the NoPass Desktop Unlock, you need to synchronize the NoPass applications on your devices to make your desktop account appear in your mobile NoPass application.

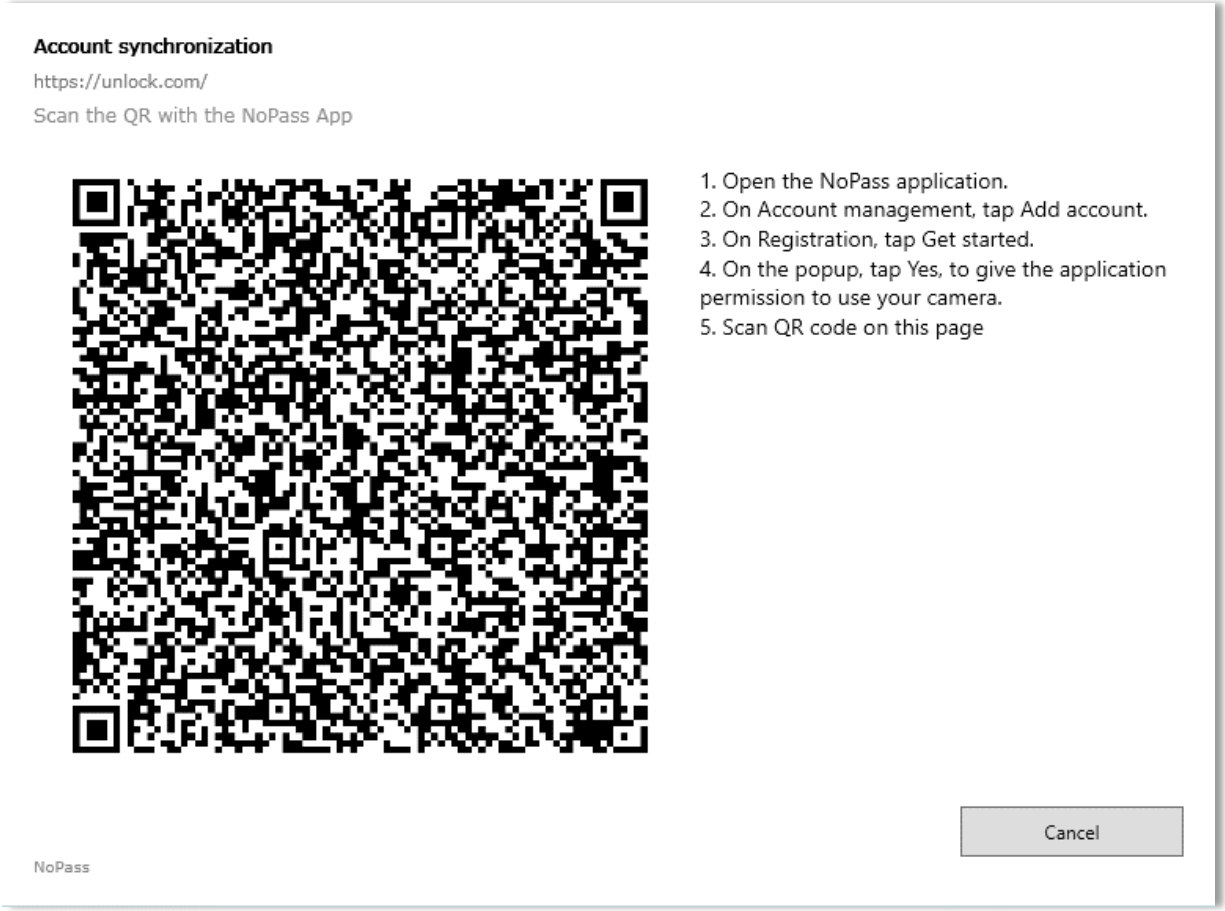
1) In the Windows notification area, click the **NoPass** icon to open the NoPass Desktop Application.



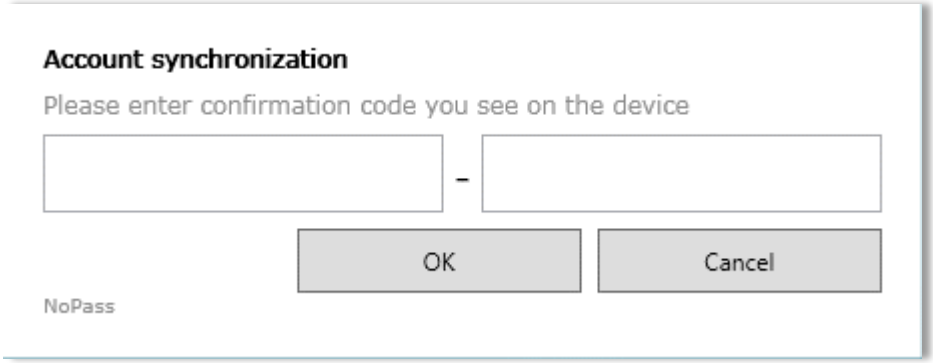
2) In the Account Management menu, click  **Synchronize** to make your account appear in your other device application.



3) Follow the instructions on the **Account synchronization** popup.



4) On the next popup, enter the confirmation code from your mobile device.



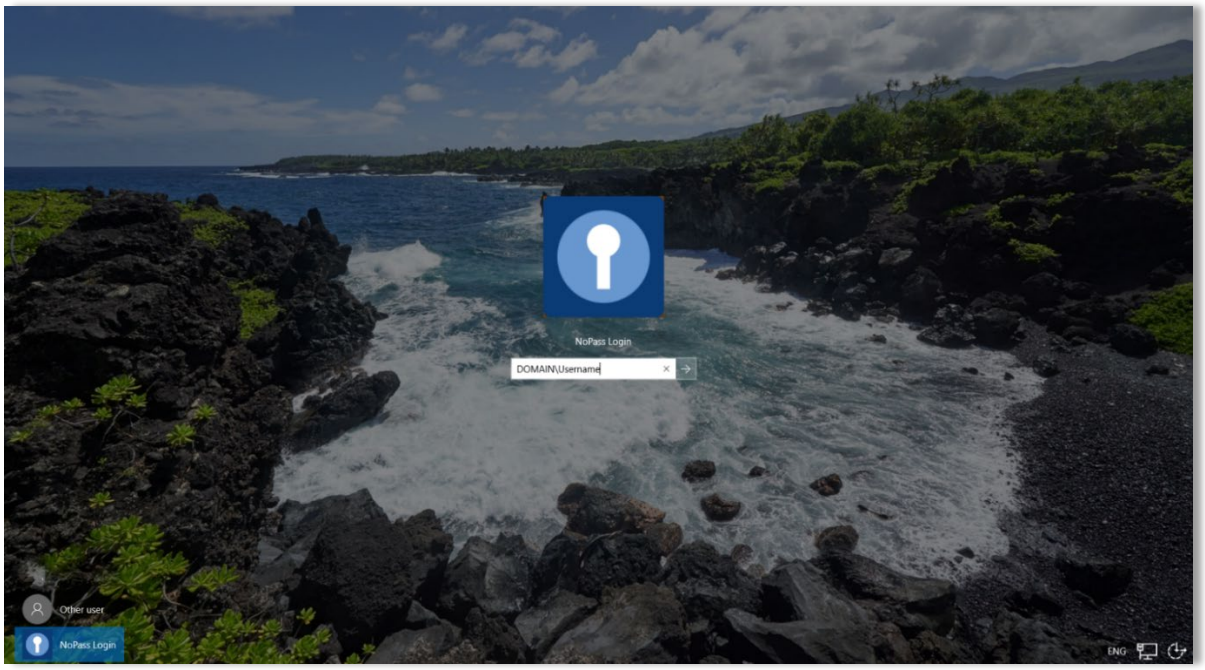
If the synchronization pedure is successful, a new account on your NoPass mobile application appears.

Now, you can use the NoPass Desktop Unlock feature.

How to unlock Windows using NoPass Desktop Unlock

When you try to open your Windows desktop computer with NoPass Desktop Unlock for the first time, you will be asked to enter your login name and password. You will be asked to do so each time you renew the password.

1) On Windows 10 Login Screen, select **NoPass Login**.



2) Accept the push notification on your other device.

You have unlocked your Windows account.

10. NoPass Integrations

This chapter contains the following:

- **RADIUS based integrations**
- **Integrations with Identity Providers**
- **NoPass integration with Box**

10.1. RADIUS based integrations

NoPass provides the ability for organizations to use NoPass as a 2nd factor authentication to manage authorization and access to on-premises applications using the RADIUS protocol.

For RADIUS integration scheme and explanation, see Section 3.1. **Infrastructure schemes**.

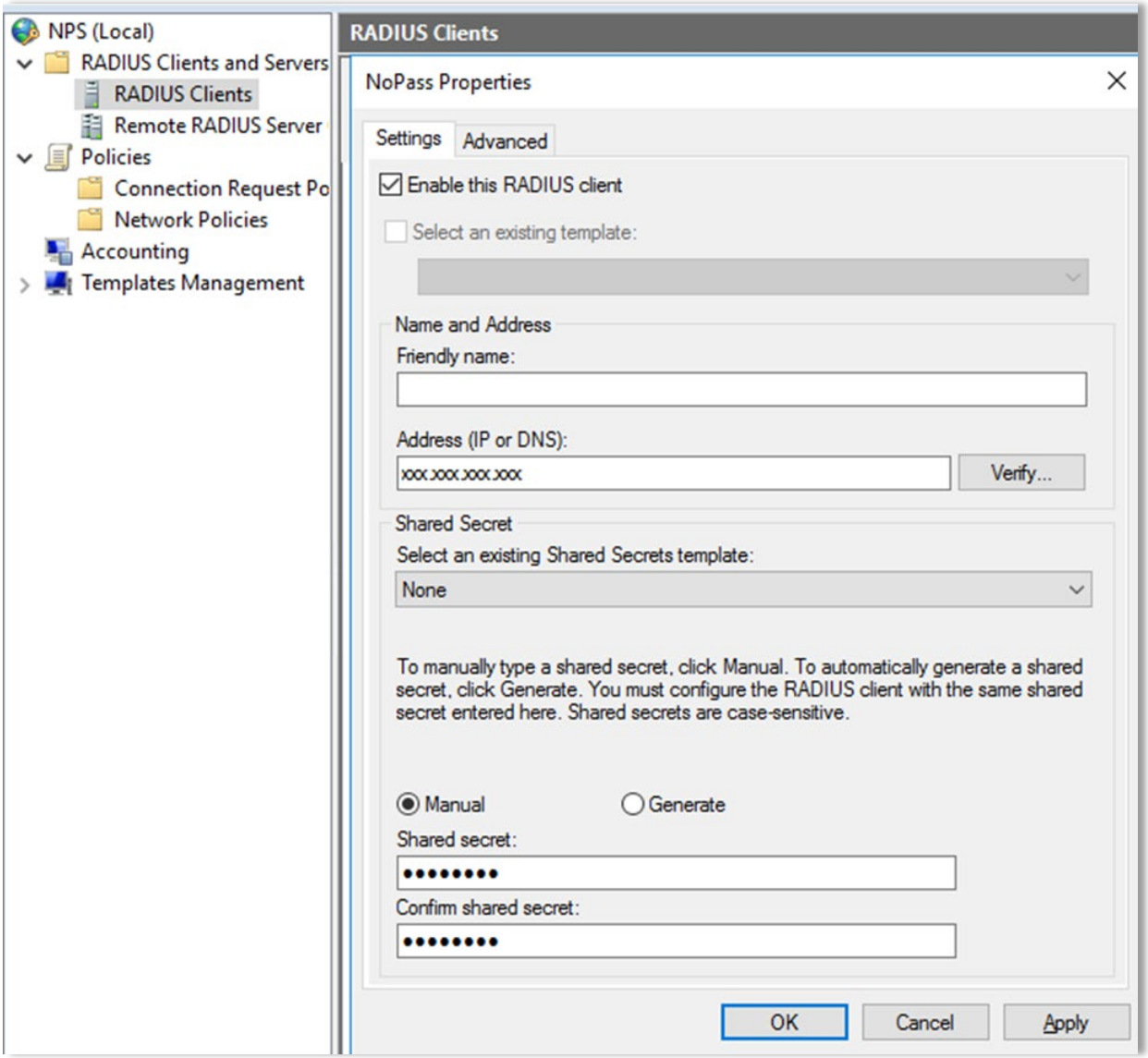
Note: The following instructions apply for Windows 2016.

What to read next

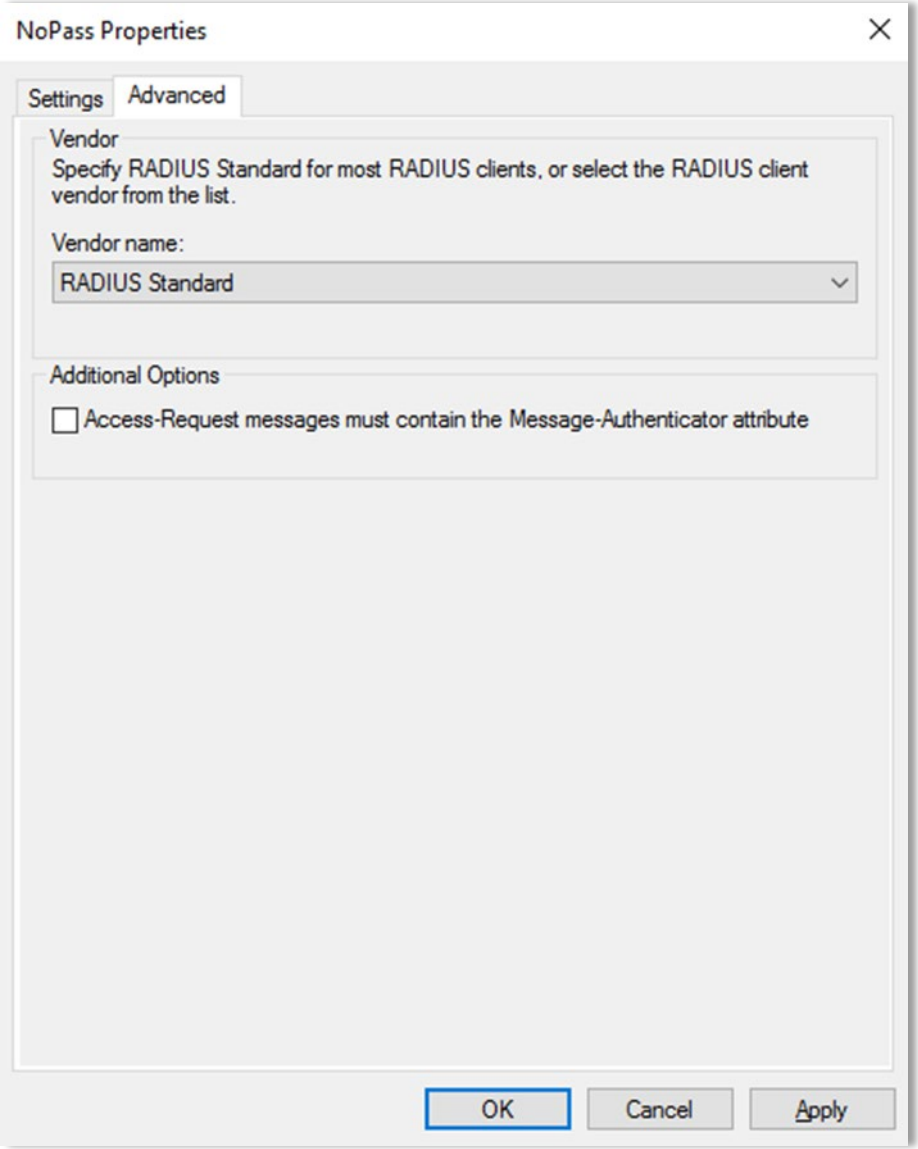
Configure RADIUS server

Configure RADIUS server

1) In the **NPS** console, add a new RADIUS client, and then do the following:
   a. In the **Address (IP or DNS)** field, enter the NoPass server IP address
   b. Form the **Shared secret** list, select the same secret as one used in the NoPass configuration.



2) The **Advanced** tab is fulfilled by default.

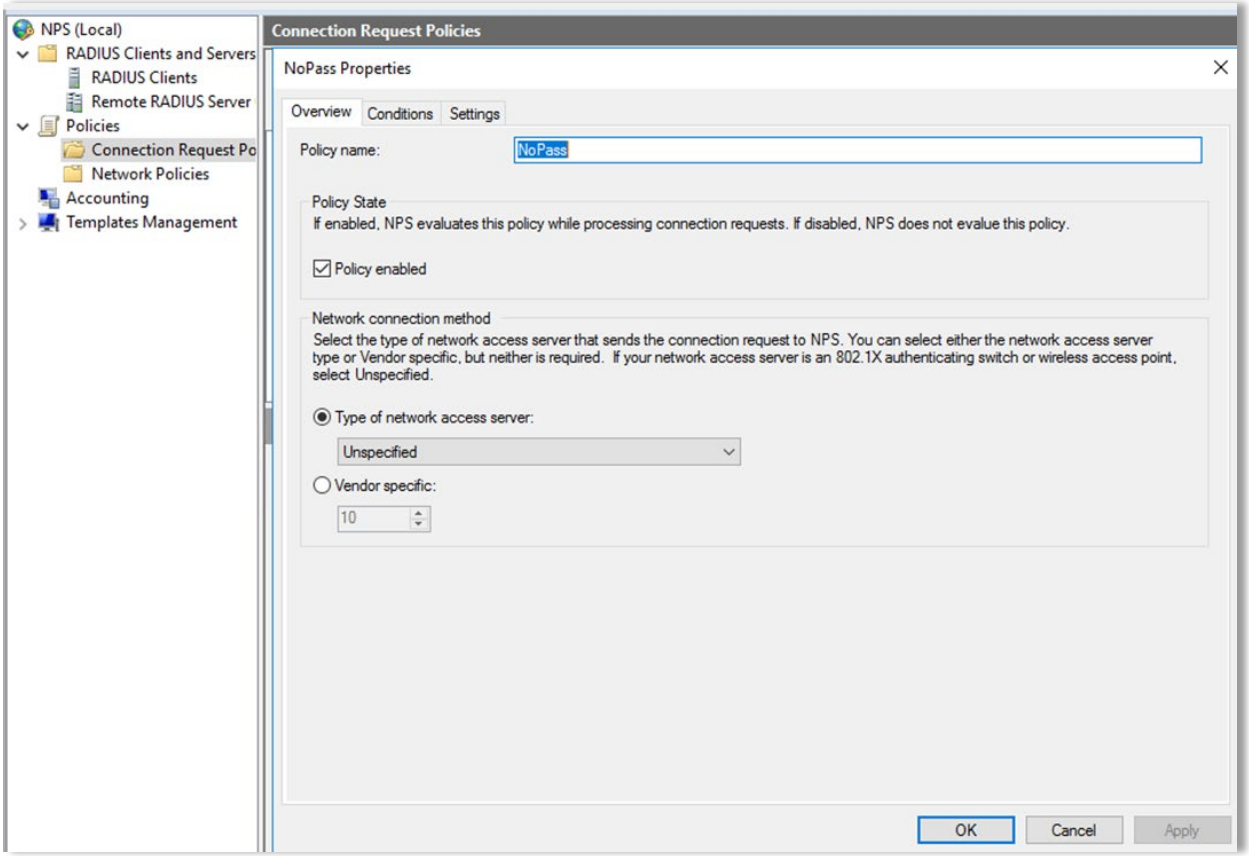


3) In the **NPS** console, select **Connection Request Policy**, and do the following:

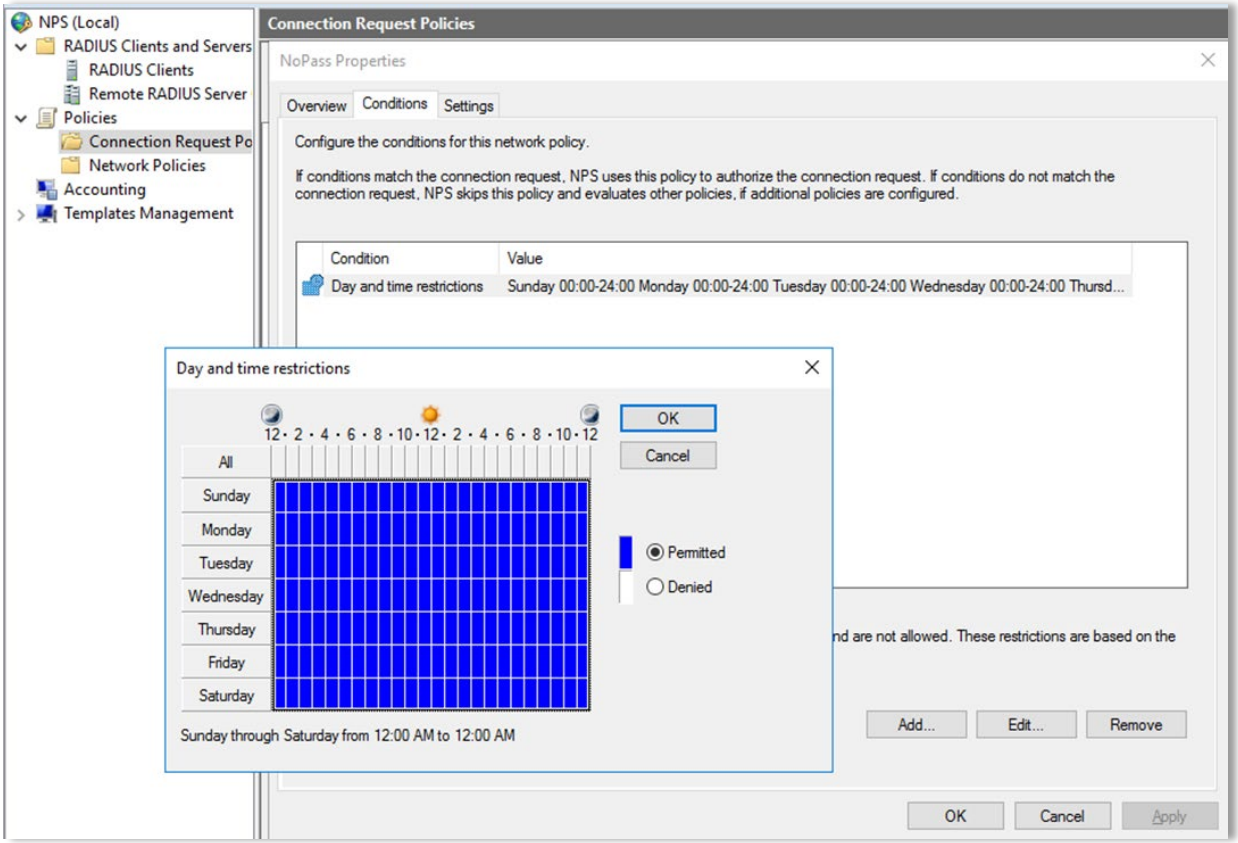
a. On the **Overview** tab, in the **Policy name** field, enter *NoPass*.

b. In **Policy State**, select **Policy enabled**.

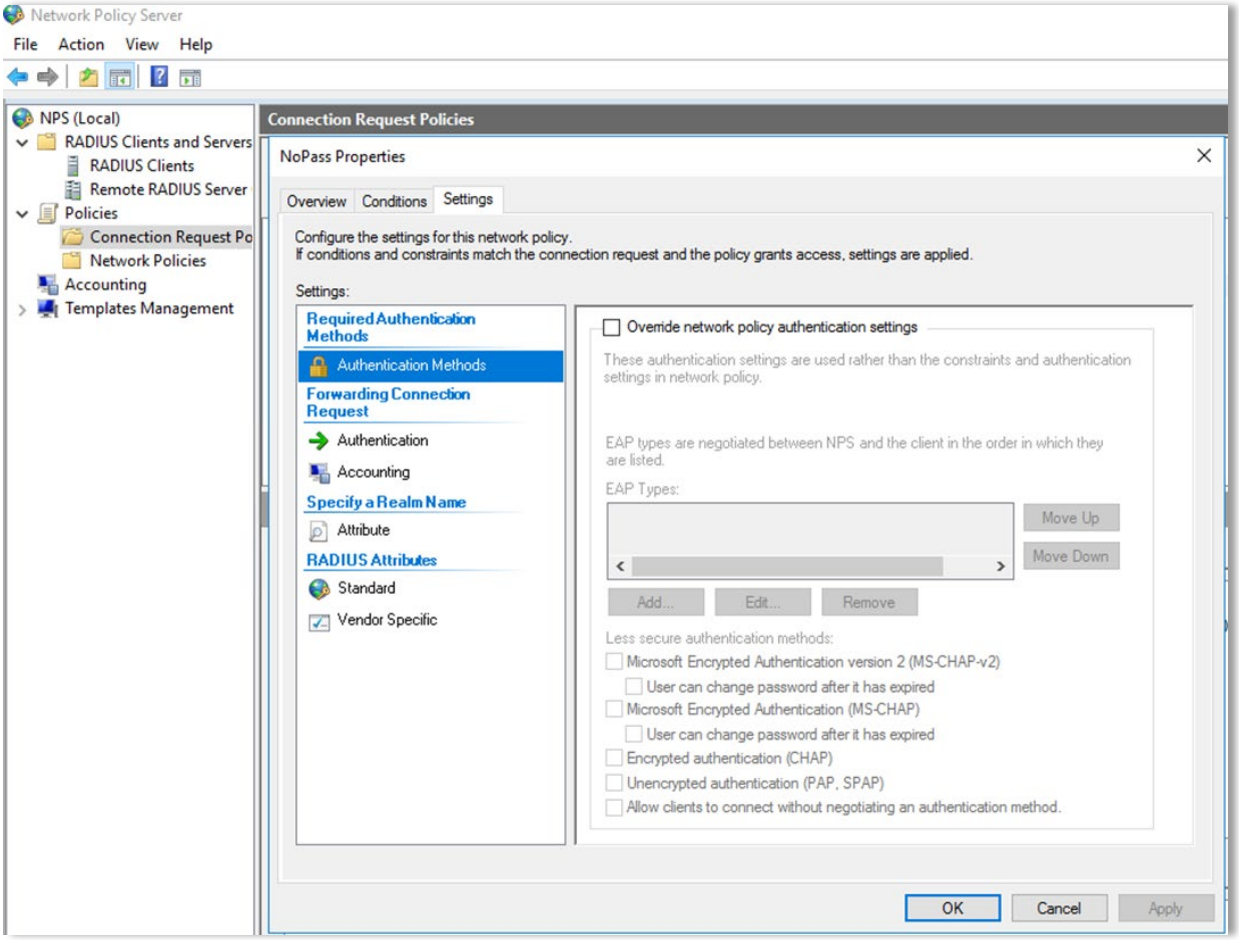
c. In **Network connection method**, select **Type of network access server** > **Unspecified**, then click **Apply**.



4) On the **Conditions** tab, set **Day and time restrictions**, and click **Apply**.



5) On the **Settings** tab, configure **Authentications methods**, and click **Apply**.



6) In the **NPS** console, select **Network Policies**, and do the following:

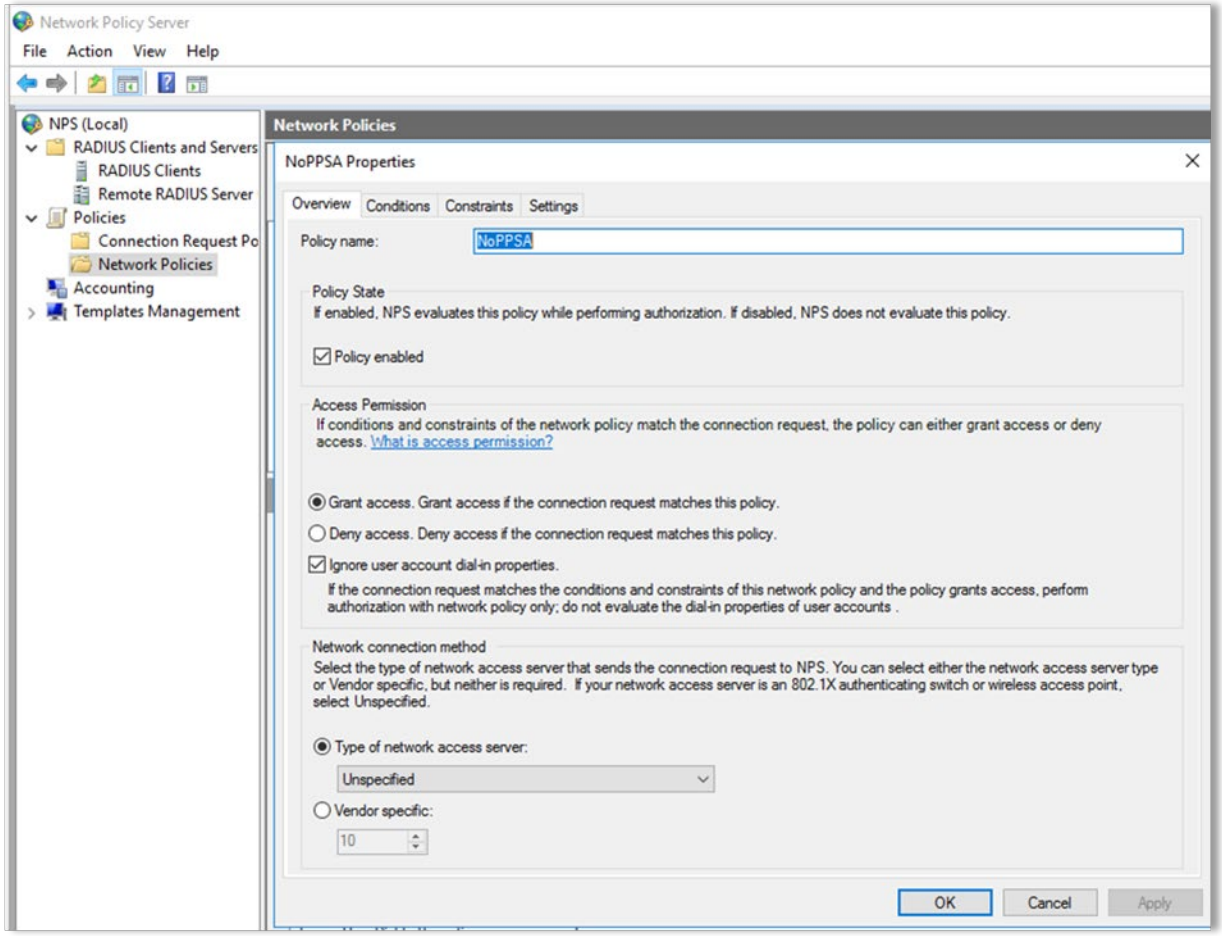
a. On the **Overview** tab, in the **Policy name** field, enter **NoPPSA**.

b. In **Policy State**, select **Policy enabled**.

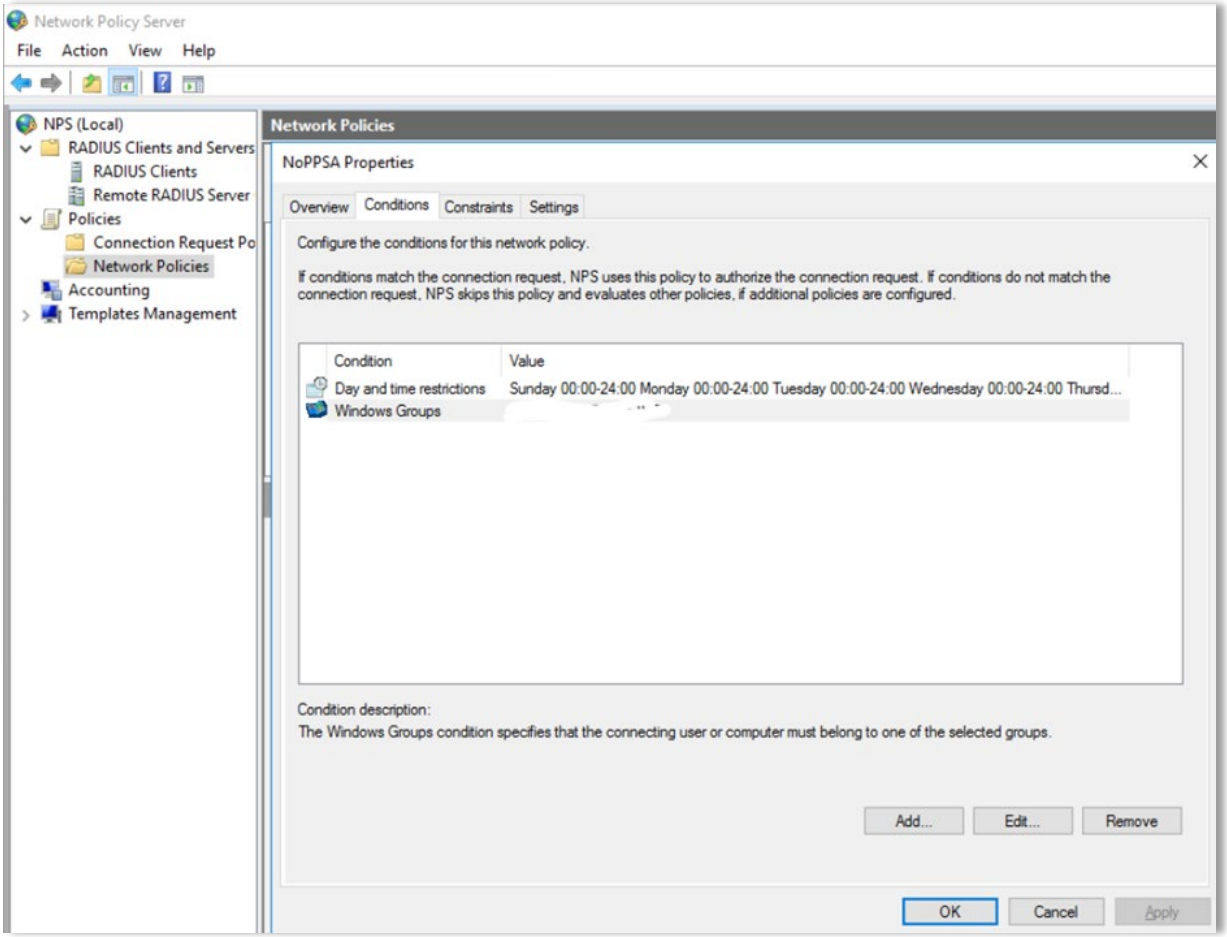
c. In **Access Permission**, select **Grant access**. Grant access if the connection request matches this policy. Select **Ignore user account dial-in properties**.

d. In **Network connection method**, select **Type of network access server**.

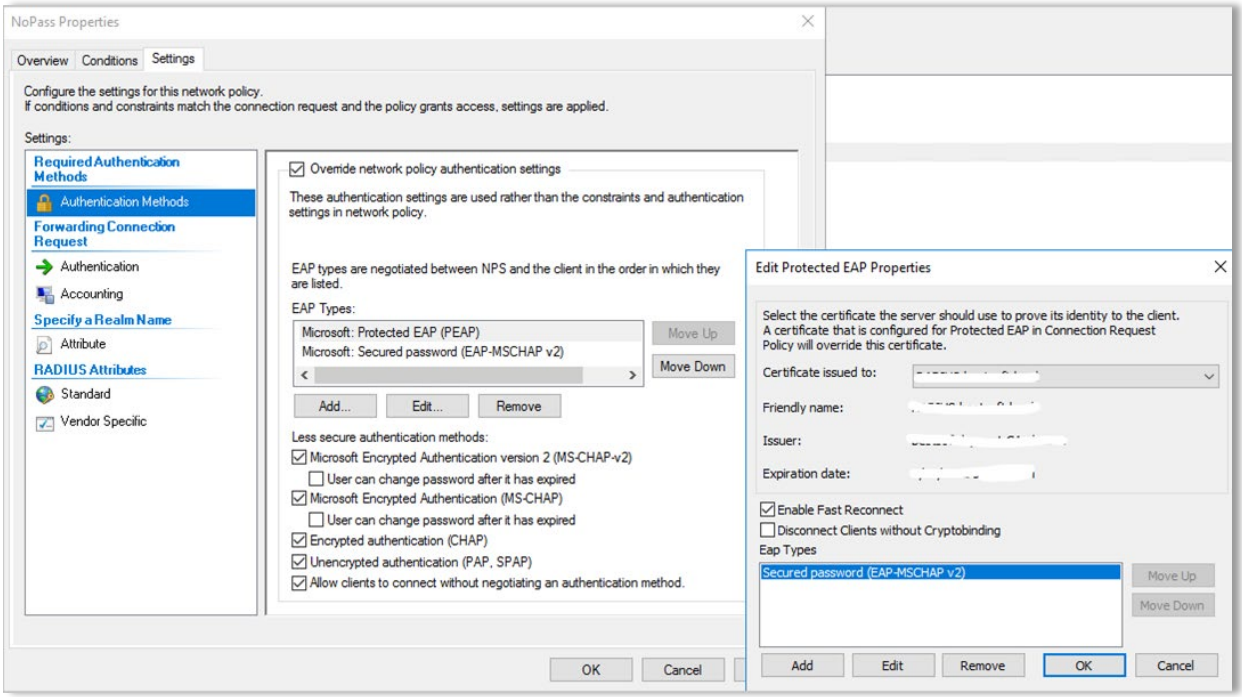
e. Click **Apply**.



7) On the **Conditions** tab, configure additional rules related to Active Directory access hierarchy. Click **Apply.**



8) On the **Settings** tab, install an appropriate certificate. Self-signed certificates are allowed here.



Now that the NoPass system is integrated with your RADIUS server, you can add RADIUS clients, such as WiFi, VPN, RDP, etc.

What to read next

Configure WiFi access point

Configure Wi-Fi access point

In your WiFi access point set the following parameters:

1) **Profile Name** — **NoPass**
2) **RADIUS Auth Server** — IP address, Port, Password/Shared Secret the same as for the NoPass server
3) **RADIUS Accounting Server** — IP address.

What to read next

OpenVPN

OpenVPN

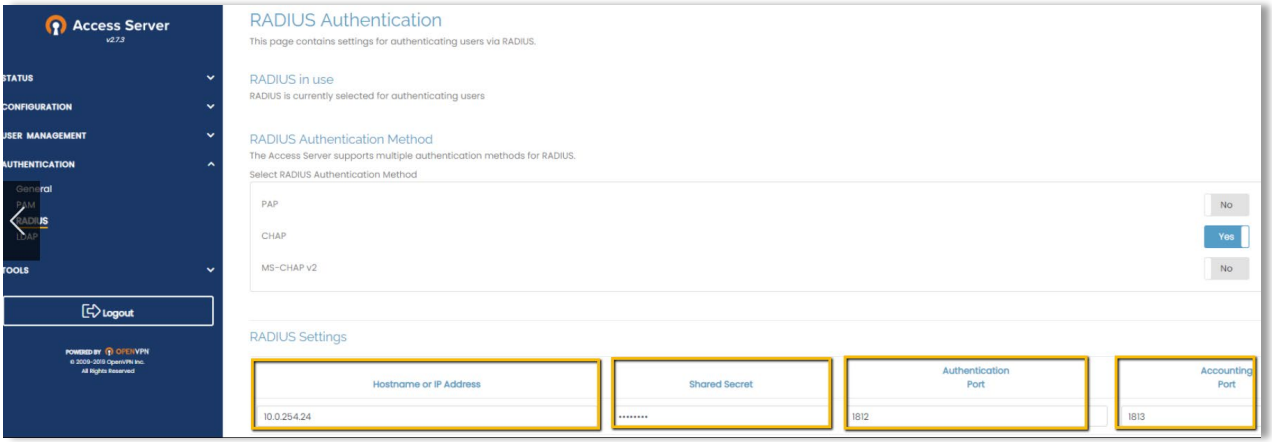
The following instructions enable you to add NoPass 2FA to your OpenVPN, which requires configuring OpenVPN Access Server and OpenVPN Connect.

Configure OpenVPN Access Server

Note: The NoPass system is currently working on OpenVPN Access Server v2.7.3.

- In the **OpenVPN Access Server** application, in **RADIUS Authentication**, enter and save the following settings: The Hostname or IP Address, Shared Secret, Authentication Port and Accounting Port.

Warning: Make sure these values are the same as in the RADIUS Admin Panel.



What to read next

Access Open VPN using NoPass 2FA: User instructions

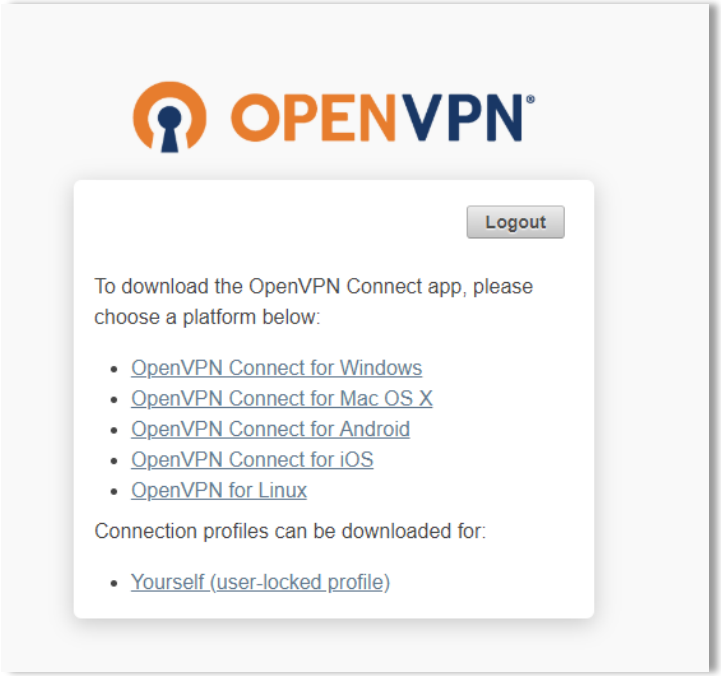
Access OpenVPN Connect using NoPass 2FA: User instructions

As an Administrator, provide the following instructions to your network users.

Install the OpenVPN Connect application

1) On the Open VPN connection page, enter your domain login and password.

2) On the next page, select the platform to download the OpenVPN application. Local administrator permissions are required.



3) Download/run the *.msi file to start the application installation.

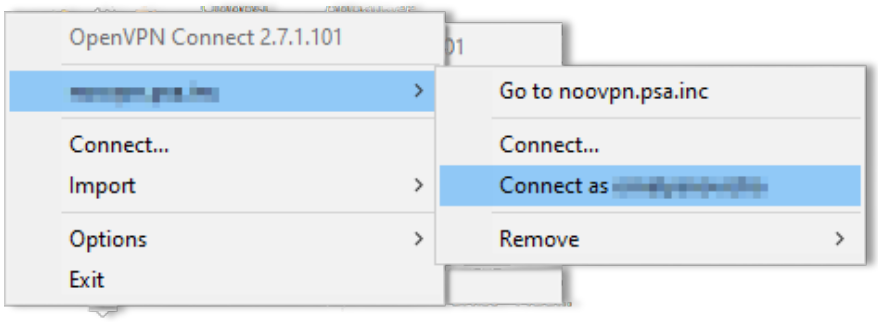
4) On the same page, select **Yourself (user-locked profile)**, download and save the configuration file.

5) After installation is completed, right-click the **OpenVPN** icon. Click **Import** and then select **From local file**.

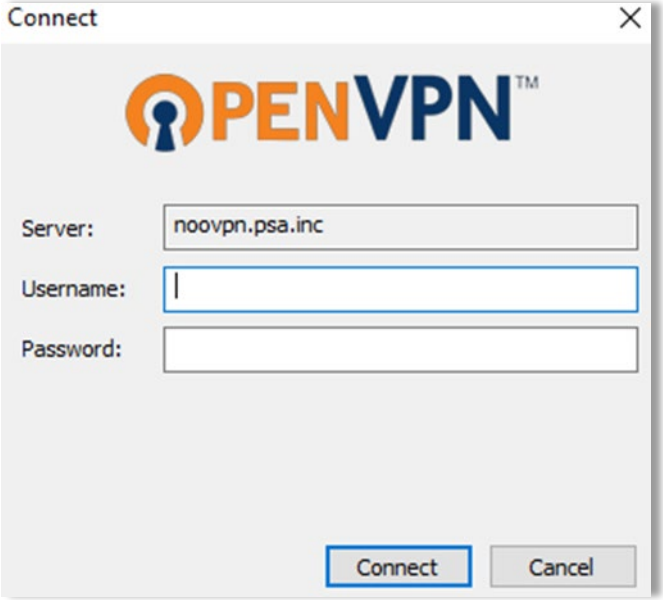
6) In the **Explorer**, navigate to the corresponding directory, and select the configuration file saved during Step 4.

Connect to OpenVPN

1) Right-click the **OpenVPN** icon. Click the corporate VPN network, and then select a user.



2) In the dialog box, enter your username and password.



3) On the **OpenVPN – Warning** popup click **Yes**, to allow OpenVPN to connect to your corporate VPN server.

4) On your smartphone with the NoPass application, accept the push authentication notification.

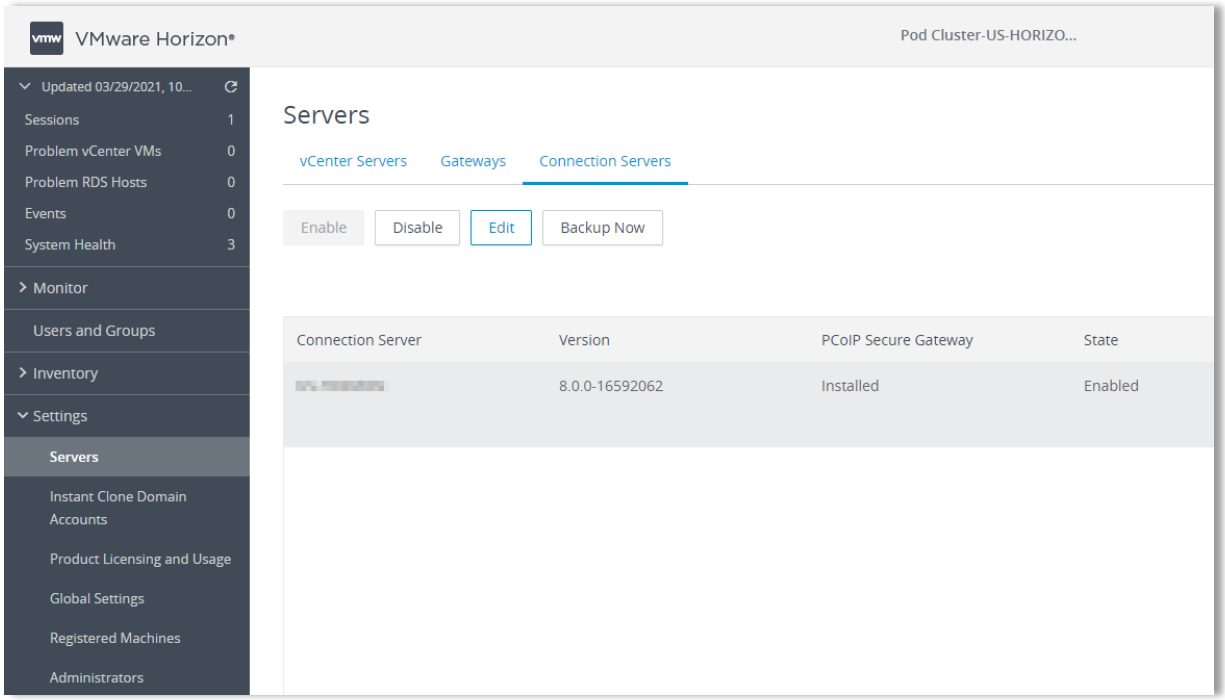
   If the connection is successful, the OpenVPN icon on your desktop changes: 

What to read next

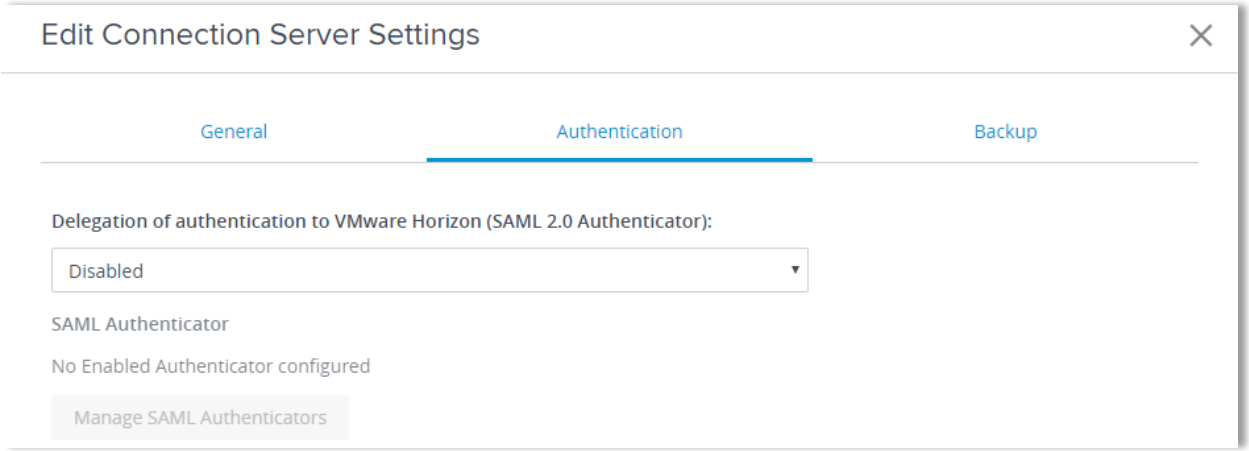
Horizon

Configure VMware Horizon

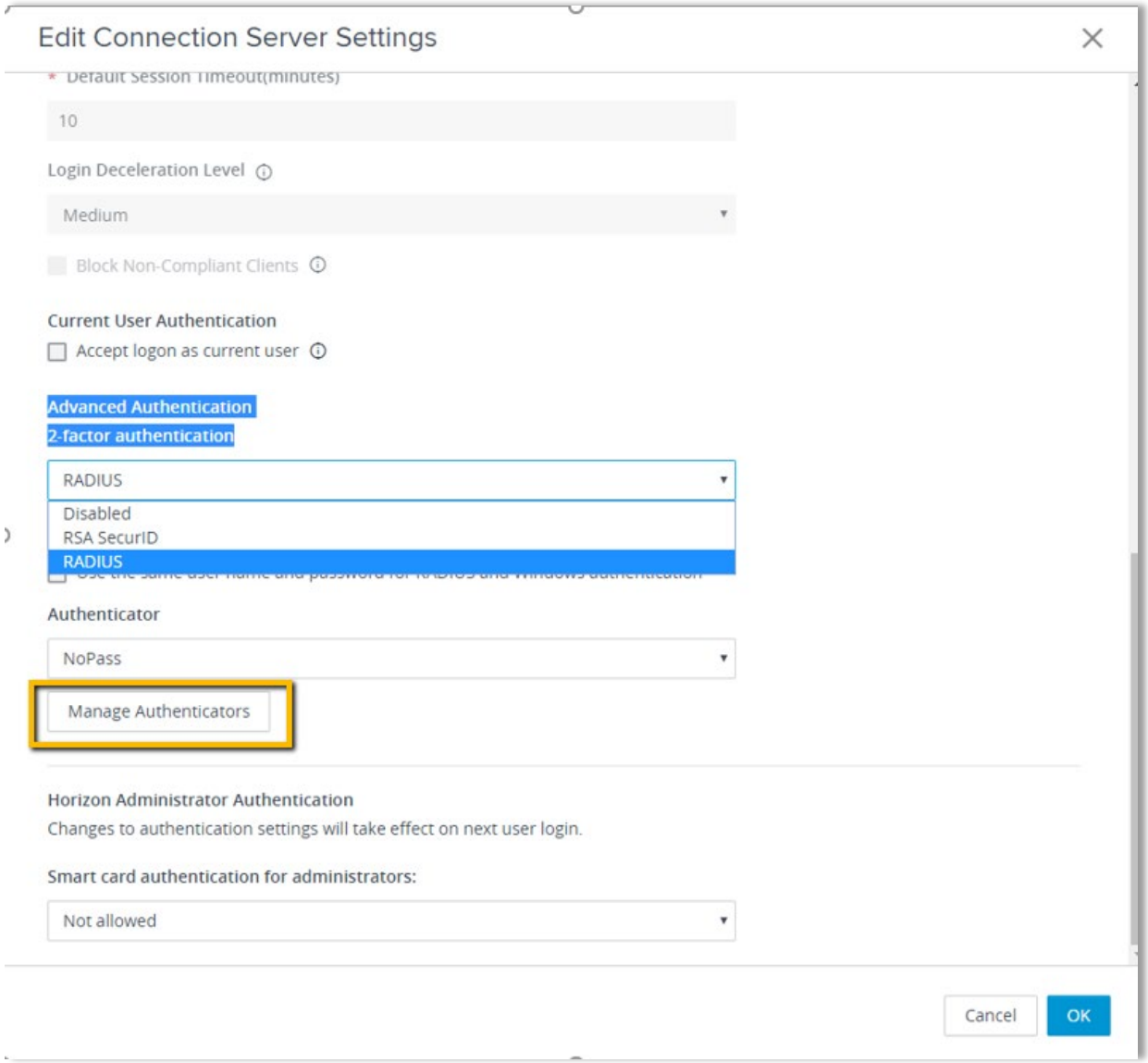
1) Go to https://*<horizon.domain.name>*/admin to enter the VMWare Horizon admin panel > **Settings** > **Servers** > **Connection Server**. Click **Edit**.



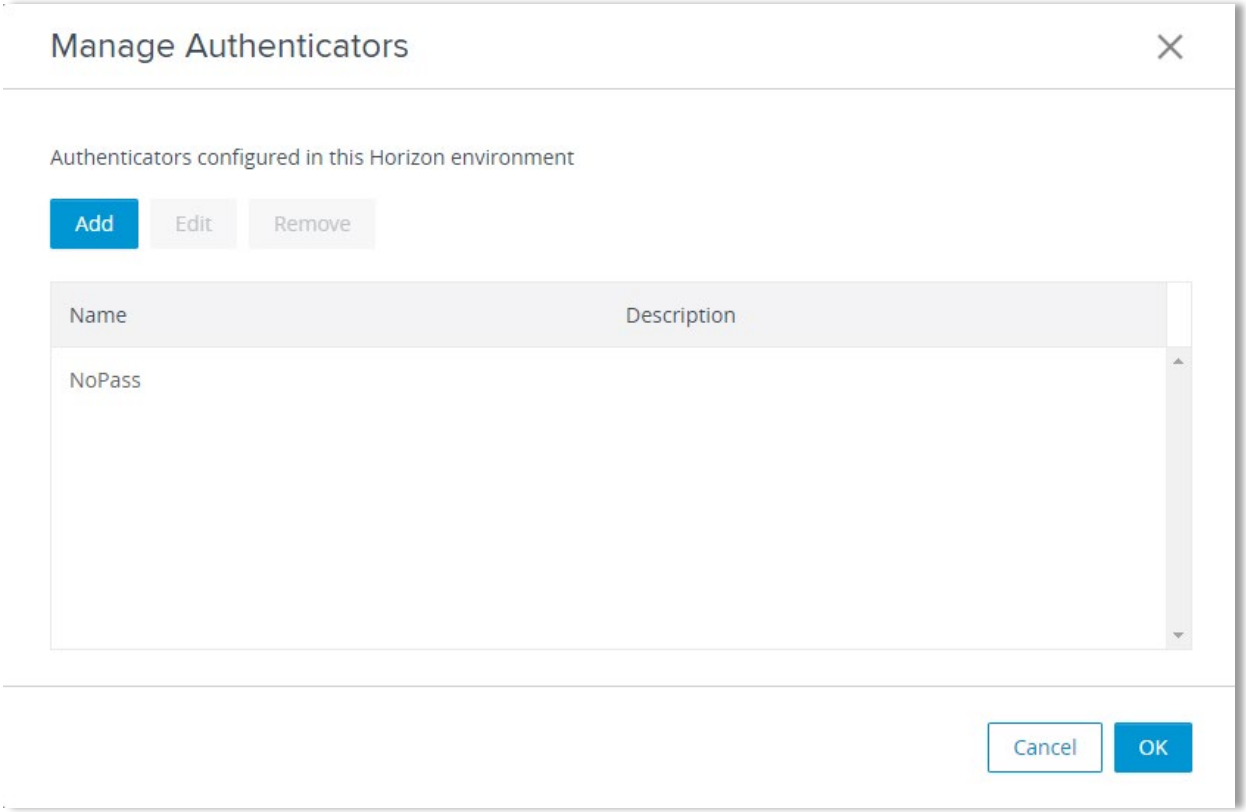
2) In the **Edit Connection Server Settings**, select the **Authentication** tab and scroll it down to **Advanced Authentication**.



3) From **Advanced Authentication 2-factor authentication**, select **RADIUS**, and then click the **Manage Authenticators** button.

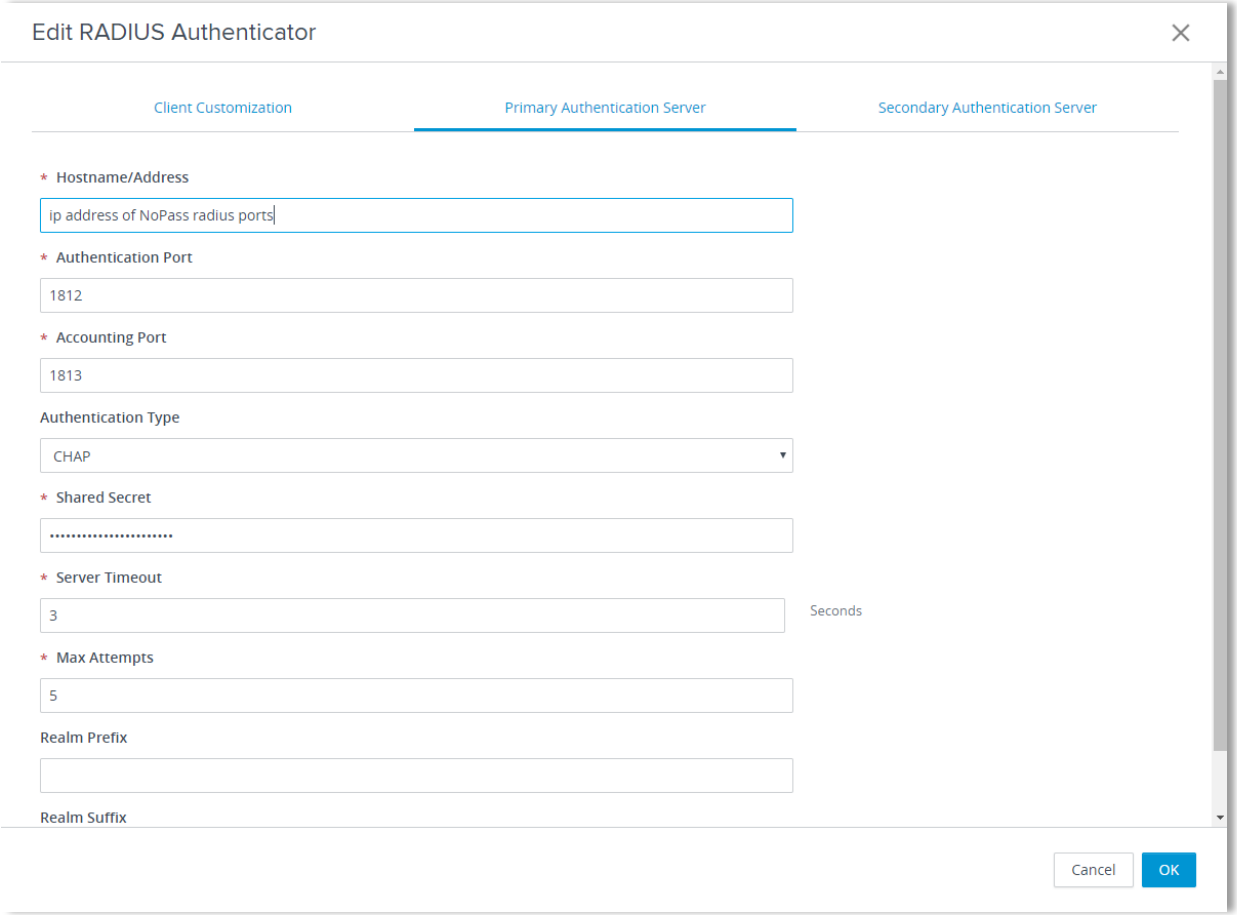


4) In the **Manage Authenticators** window, click **Add** to add a new RADIUS server.



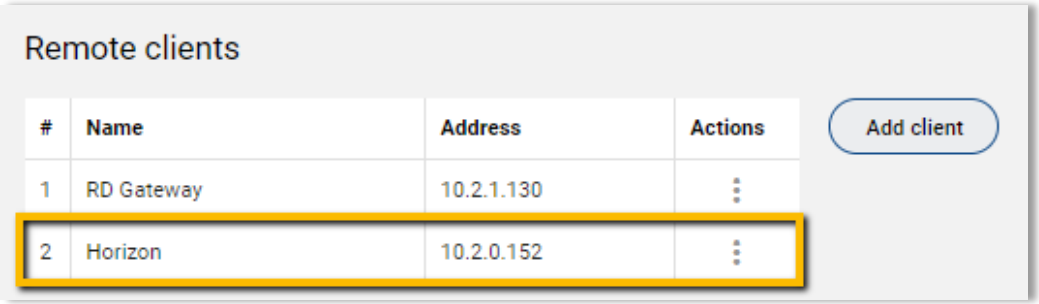
5) Click **Edit**, to configure RADIUS Authenticator, and populate the following mandatory fields with the values known from the NoPass server deployment:

- **Hostname/Address**, enter the ID address of NoPass radius ports
- **Authentication Port**
- **Accounting Port**
- **Authentication Type**
- **Shared Secret**
- **Server Timeout**
- **Max Attempts**
- **Realm Prefix**
- **Realm Suffix**



Configure the NoPass RADIUS admin panel

1) Go to the **NoPass RADIUS admin panel** > **Settings** > **RADIUS settings**.
2) In the **Remote clients** group, add Horizon as a remote client.



For more information about RADIUS settings, see *NoPass Administrator Manual*.

What to read next

IdP based integrations

10.2. IdP based integrations

For SSO integration scheme, see Section 3.1 **Infrastructure schemes**.

NoPass integration with Salesforce

Before you begin

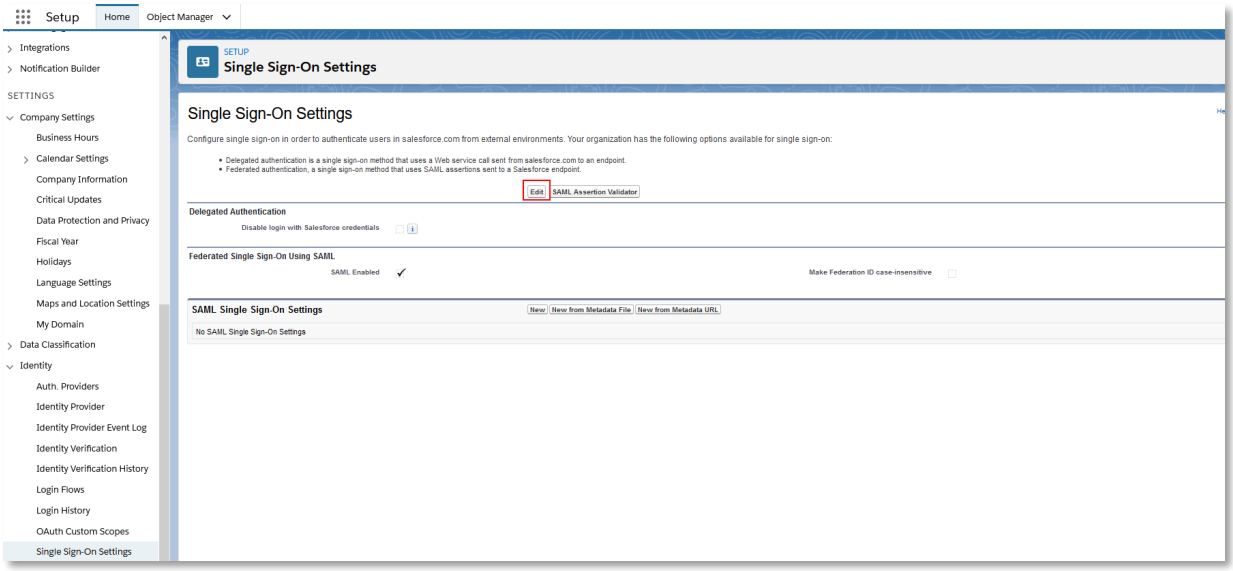
Salesforce offers the following ways to use SSO:

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

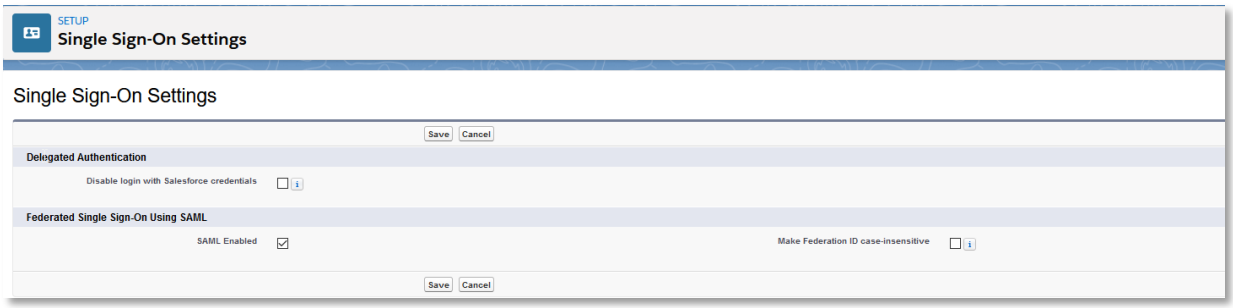
Procedure

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**.



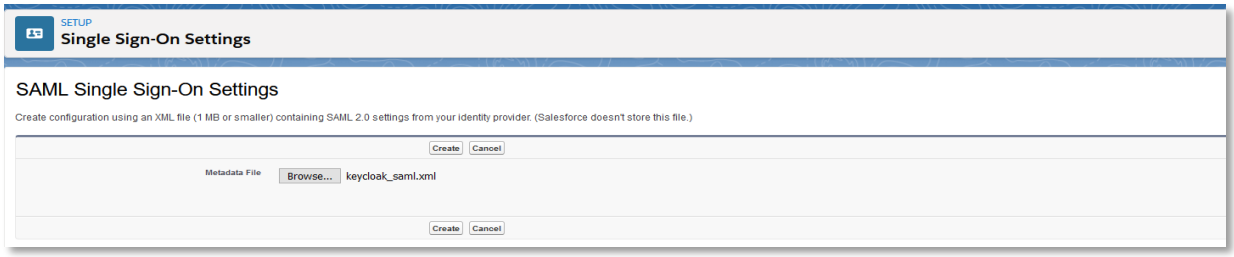
2) To view SAML single sign-on settings, select **SAML Enabled**, and click **Save**.



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.



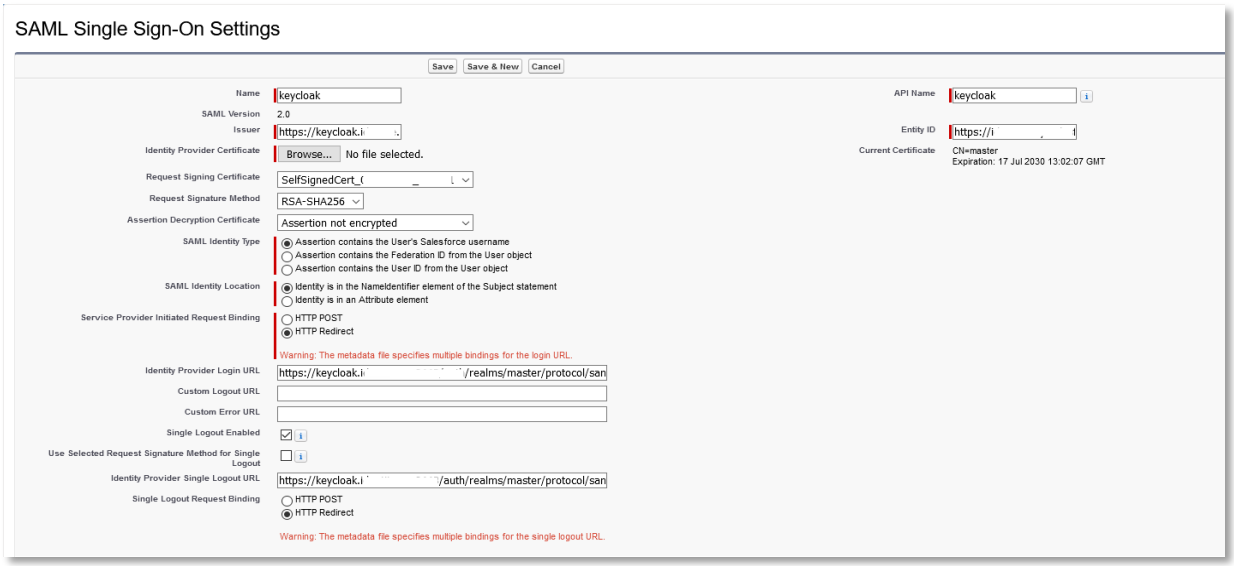
4) Name this setting for referencing within your organization. Salesforce inserts the corresponding API value, which you can customize if necessary.

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 or the custom domain for the **Entity ID**. Share this information with your identity provider.

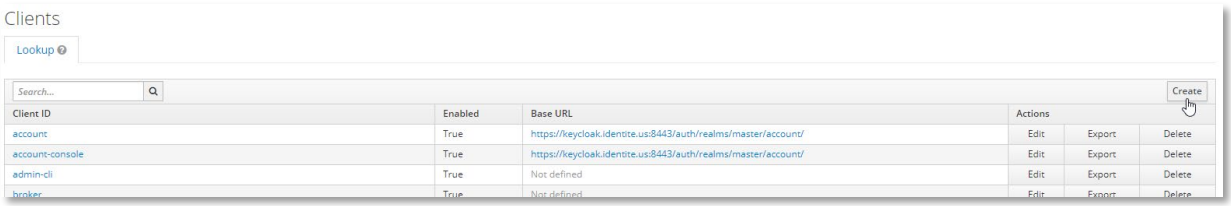
7) *Optional*. Set up Just-in-Time user provisioning. For more information, see Enable Just-in-Time user provisioning and About Just-in-Time Provisioning for SAML.



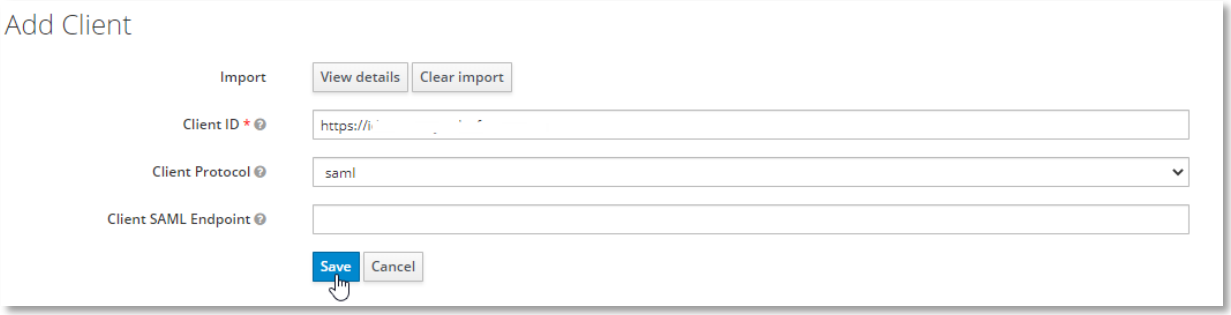
8) To download the .xml file of your SAML configuration settings, click **Download Metadata**.

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:

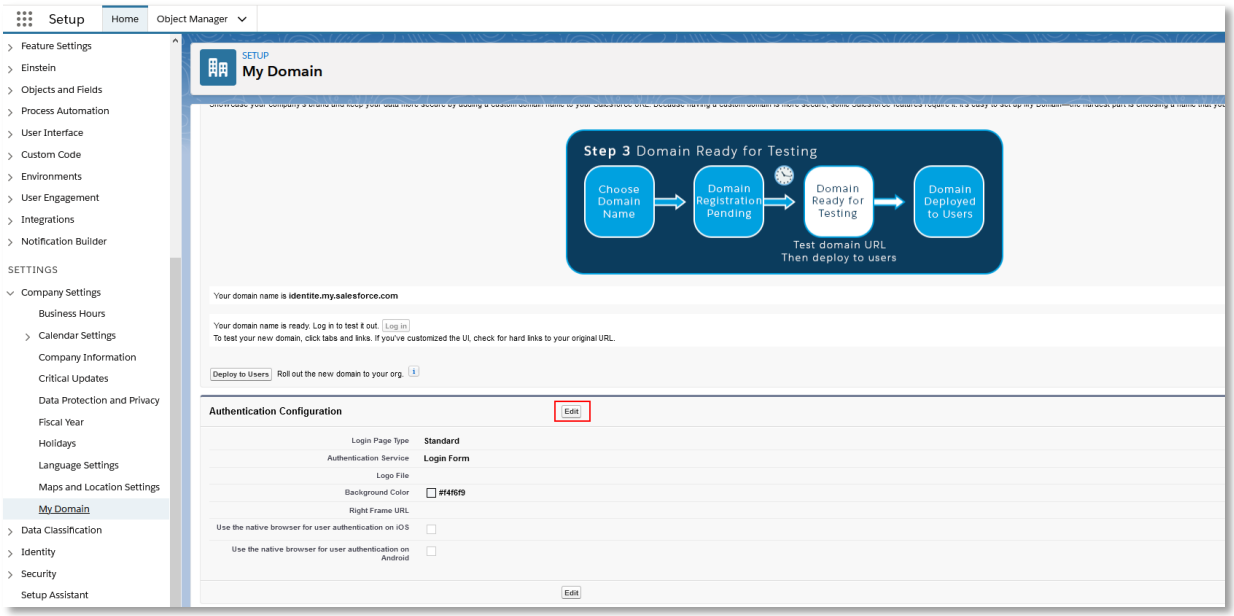
Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Consent Required	OFF
Client Protocol	SAML

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

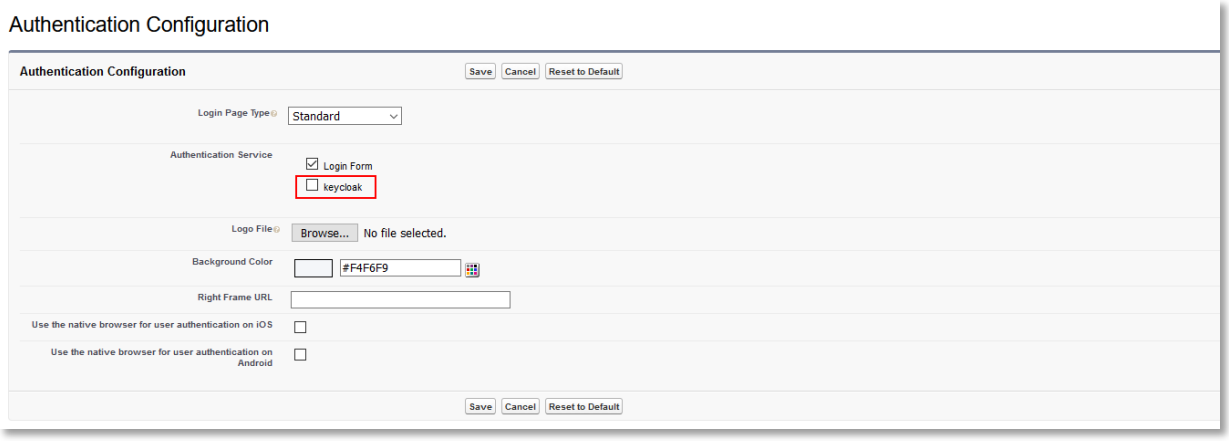
13) Under **Fine Grain SAML Endpoint Configuration**, configure the following:

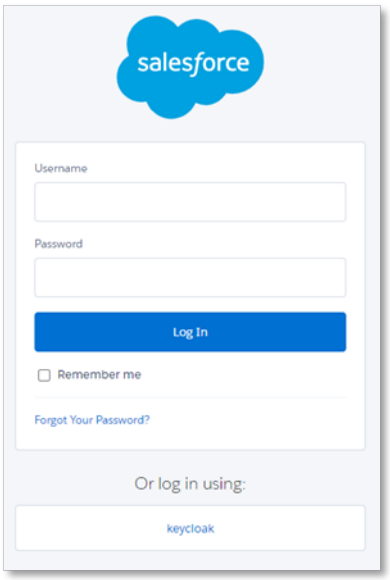
Assertion Consumer Service POST Binding UR	The ACS (Assertion Consumer Service) URL from Service Provider Metadata
Logout Service Redirect Binding URL	The Single Logout URL from Service Provider Metadata

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:





For more information about Salesforce SAML configuration, see [Configure Salesforce as the Service Provider with SAML Single Sign-On].

What to read next

NoPass integration with Confluence

NoPass integration with Confluence

Before you begin

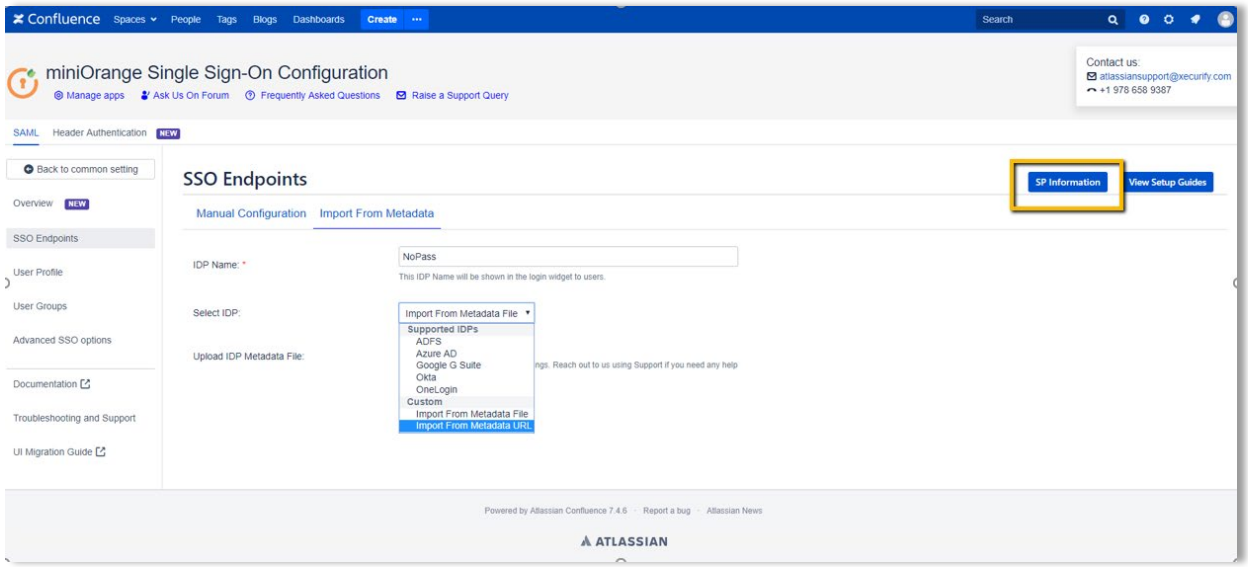
To have access to SSO in Confluence, it is necessary to install an additional application. You can download the application at Atlassian Marketplace. It is also available in the Manage apps menu of the Confluence main window.

For more information about configuring Confluence SAML, see SAML Single Sign On (SSO) into Confluence using Jboss Keycloak.

Procedure

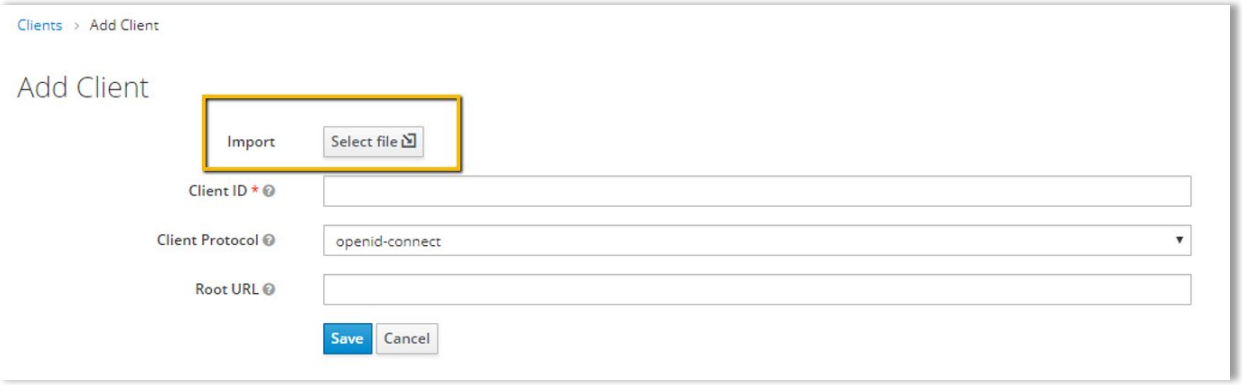
To configure SAML for SSO using Confluence SSO/Single Sign On, SAML SSO by miniOrange do the following:

1) Go to **miniOrange Single Sign-On Configuration**. In the left pane, select **SSO Endpoints** > **Import From Metadata**, and do the following:
   - Import the Keycloak metadata file into the Confluence SSO configuration application.
   - Click **SP Information** to download the miniOranges's Metadata XML (or copy the Metadata URL). You will need it later.



2) In the Keycloak admin console, go to your realm > the **Clients** tab. Click **Create** to add a new client.

3) On the **Add client** tab, click **Select file** to import the Metadata XML (or Metadata URL) from step 2, and then click **Save**.



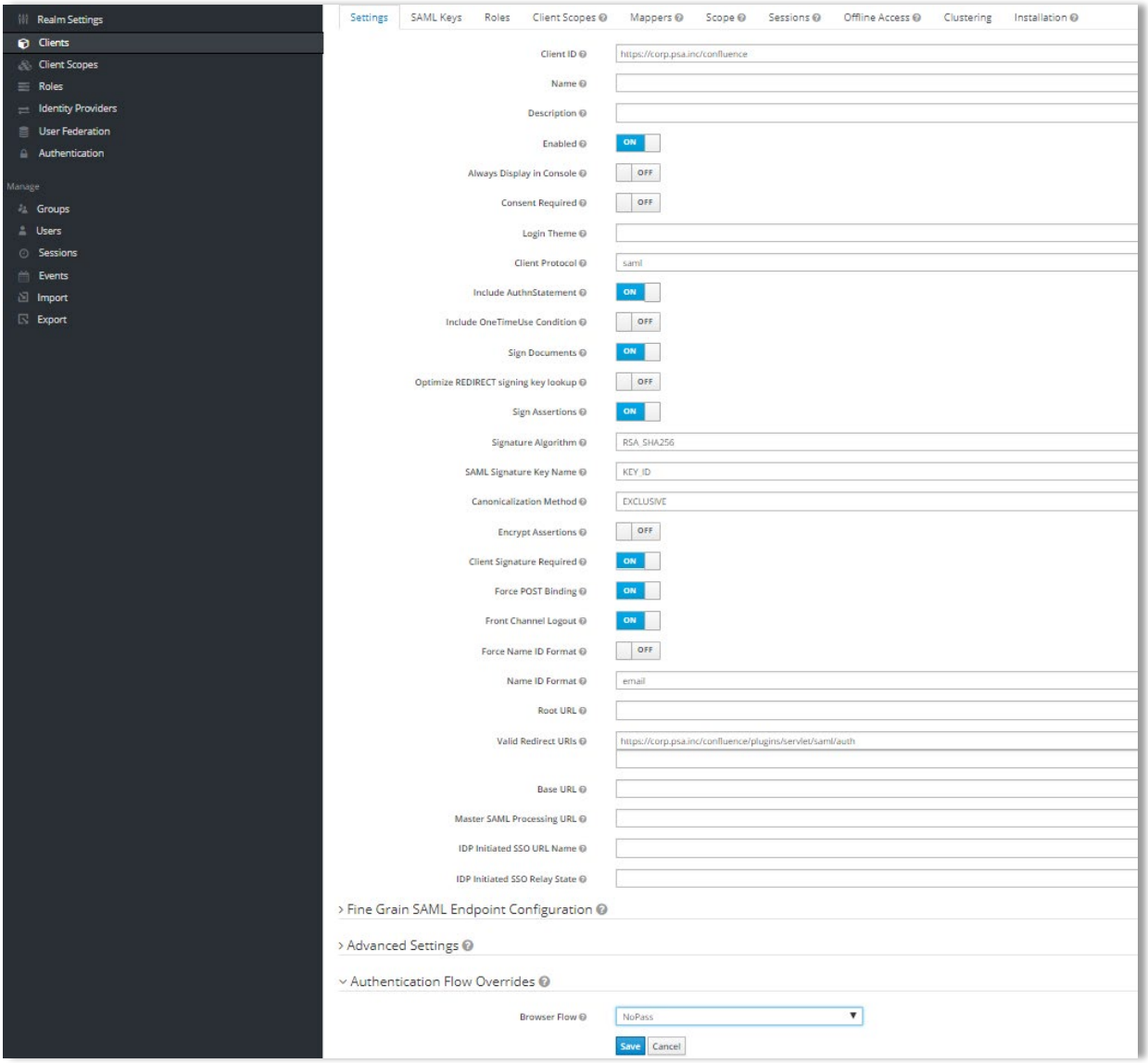
Note: If import failed, save the metadata file/URL manually, and delete the following tag from it:

```
<md:EntitiesDescriptor ...>
</md:EntitiesDescriptor>
```

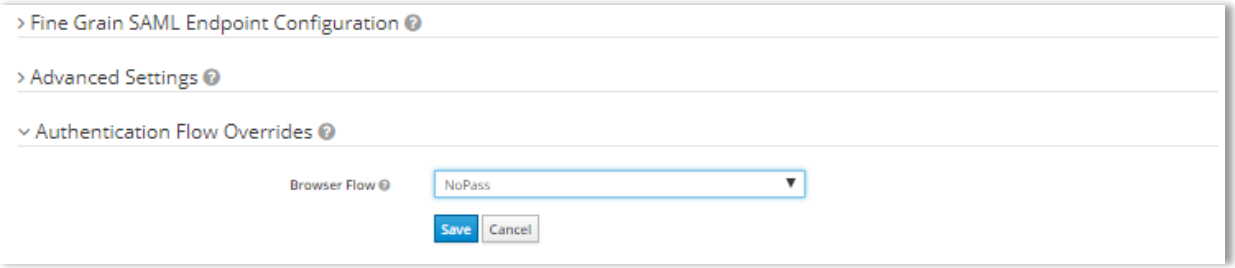
4) On the **Settings** tab, set the following parameters:

Client ID	ID from the metadata file
Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Always Display in Console	OFF
Consent Required	OFF
Login Theme	ON
Client Protocol	SAML
Include AuthnStatement	ON
Include OneTimeUse Condition	OFF
Sign Documents	ON
Optimize REDIRECT signing key lookup	OFF
Sign Assertions	ON

Signature Algorithm	RSA_SHA256
SAML Signature Key Name	KEY-ID
Canonicalization Method	EXCLUSIVE
Encrypt Assertions	OFF
Client Signature Required	ON
Force POST Binding	ON
Front Channel Logout	ON
Force Name ID Format	OFF
Name ID Format	*email*
Root URL	From the metadata file
Valid Redirect URLs	From the metadata file
Base URL	Leave empty
Master SAML Processing URL	Leave empty
IDP Initiated SSO URL Name	Leave empty
IDP Initiated SSO Relay State	Leave empty

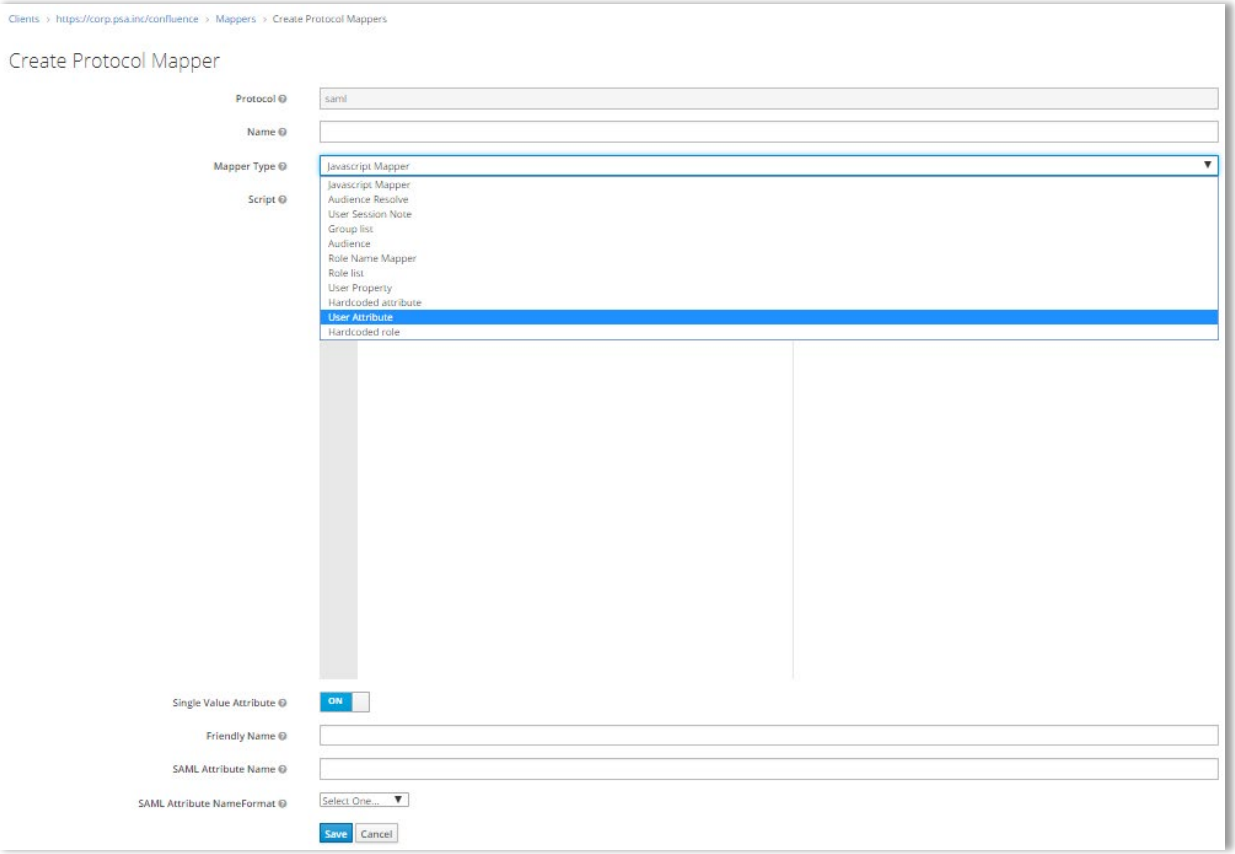


5) Click **Authentication Flow Overrides**. From the **Browser Flow** list, select **NoPass**, and then click **Save**.

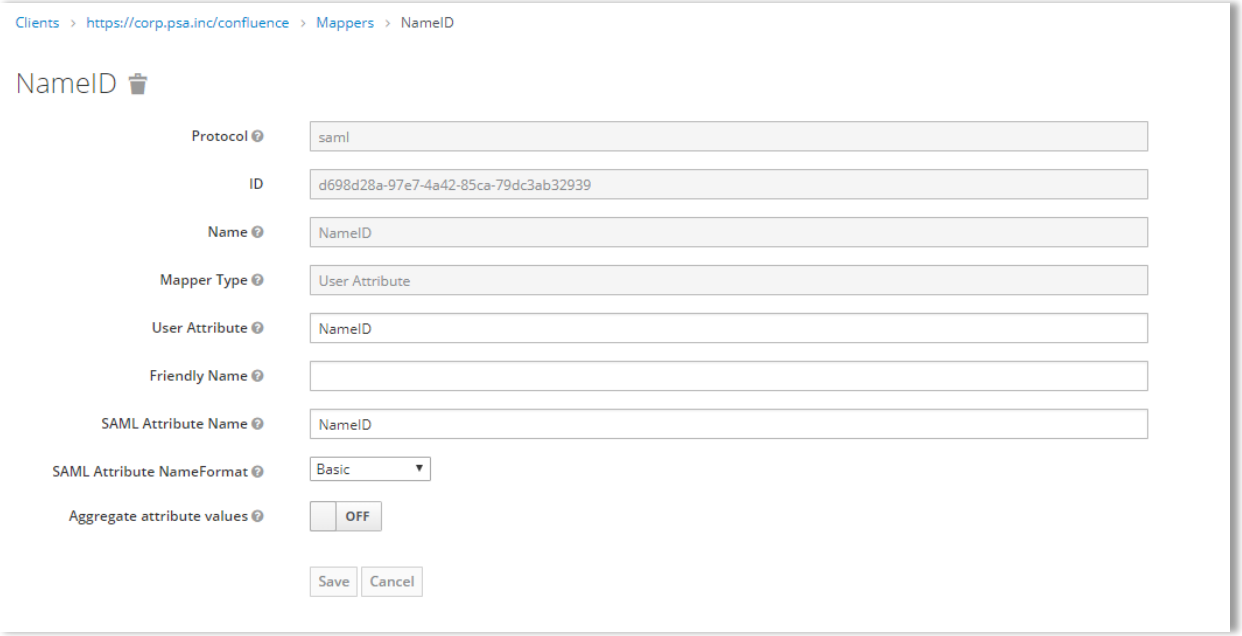


6) On the **Mappers** tab, click **Create** to add a new Mapper.

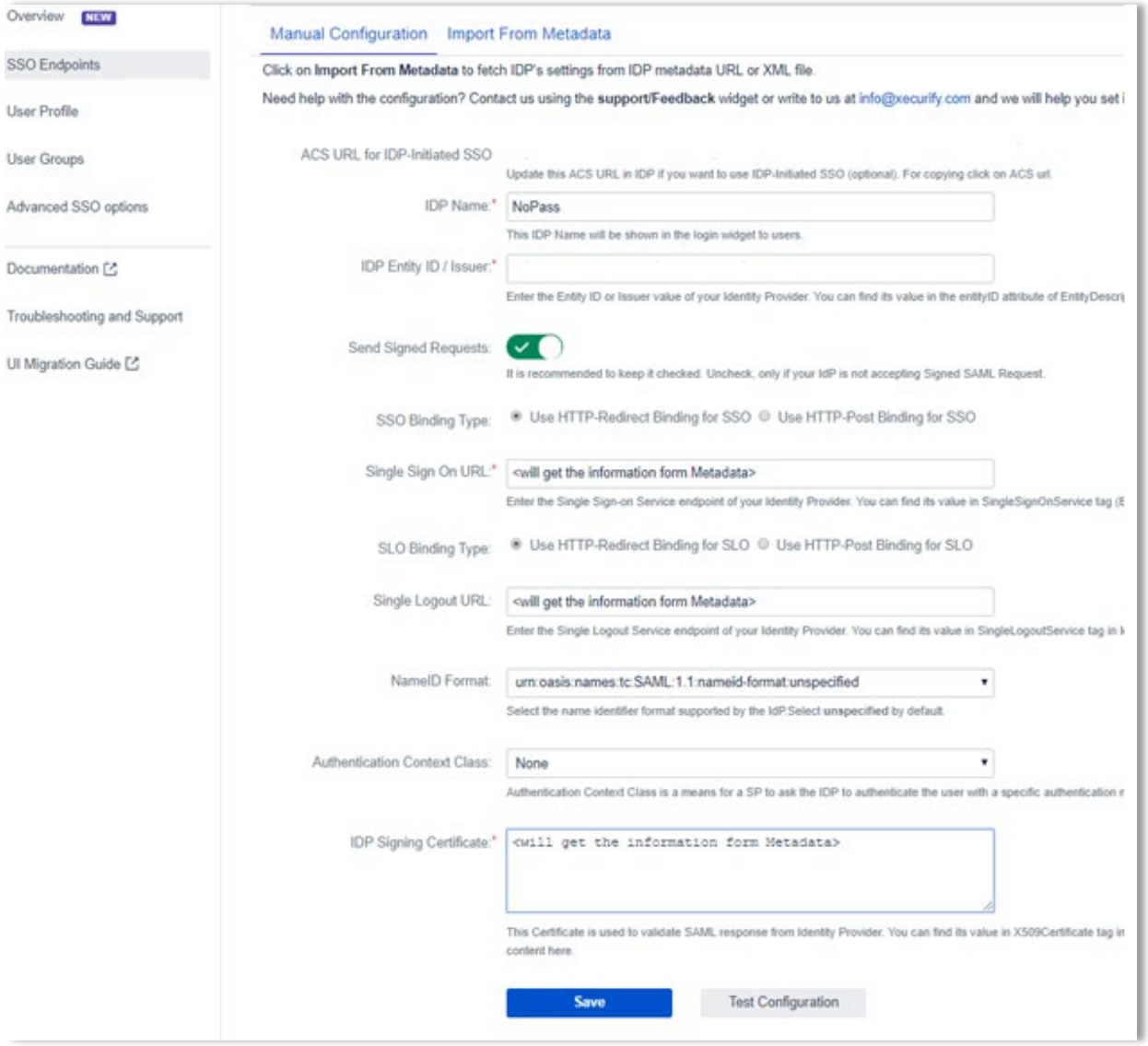
7) In the **Create Protocol Mapper** window, from **Mapper type**, select **User Attribute**, and click **Save**.



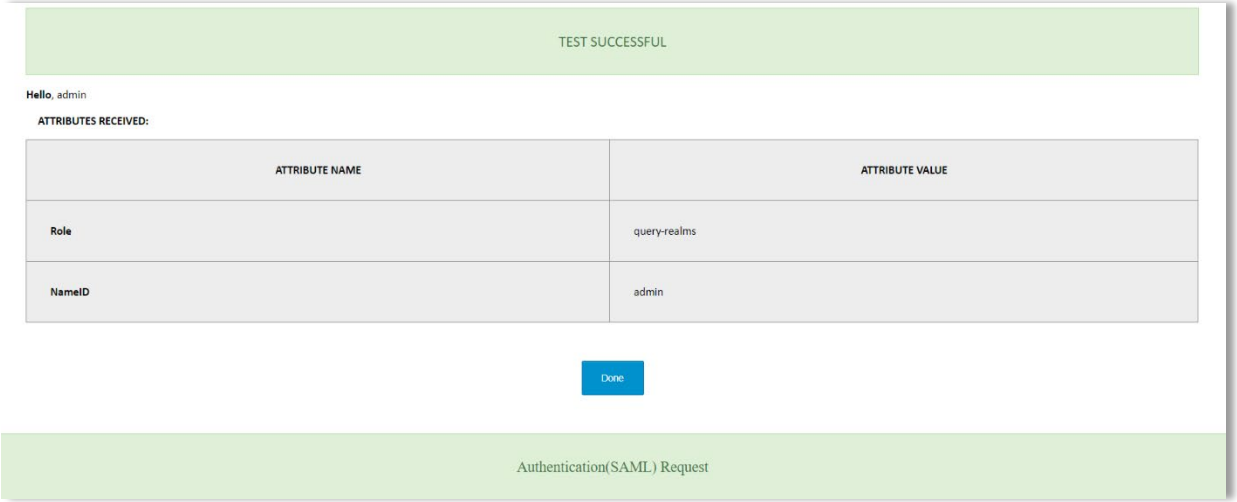
8) In the **Name** field, type *name*, and click **Save**.



9) Go to **miniOrange Single Sign-On Configuration** > **SSO Endpoints** > **Manual Configuration**. At the bottom of the page, click **Test Configuration**.



The successful result looks as follows:



Your Confluence environment is protected with NoPass now.

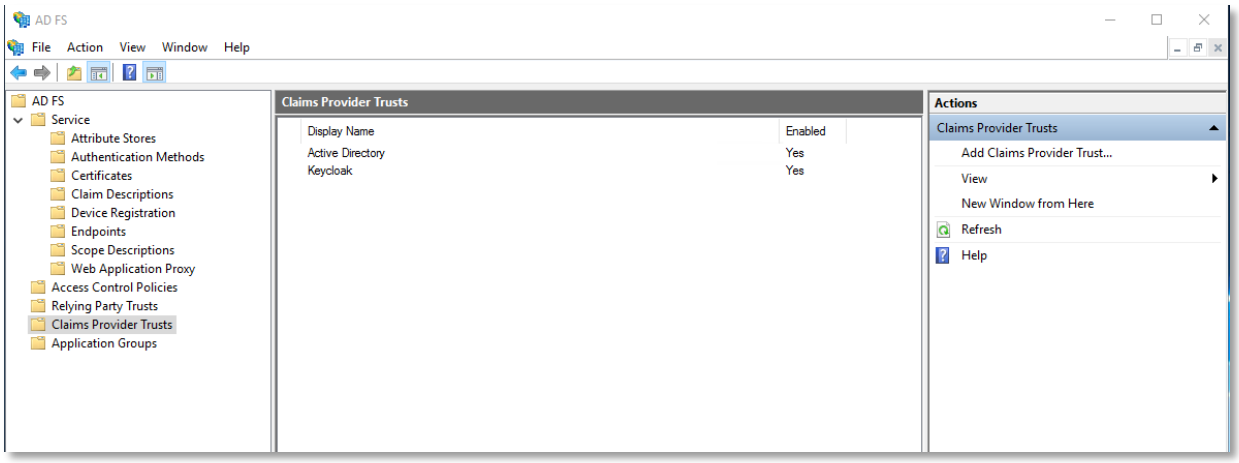
What to read next

AD FS as a service provider

AD FS as a service provider

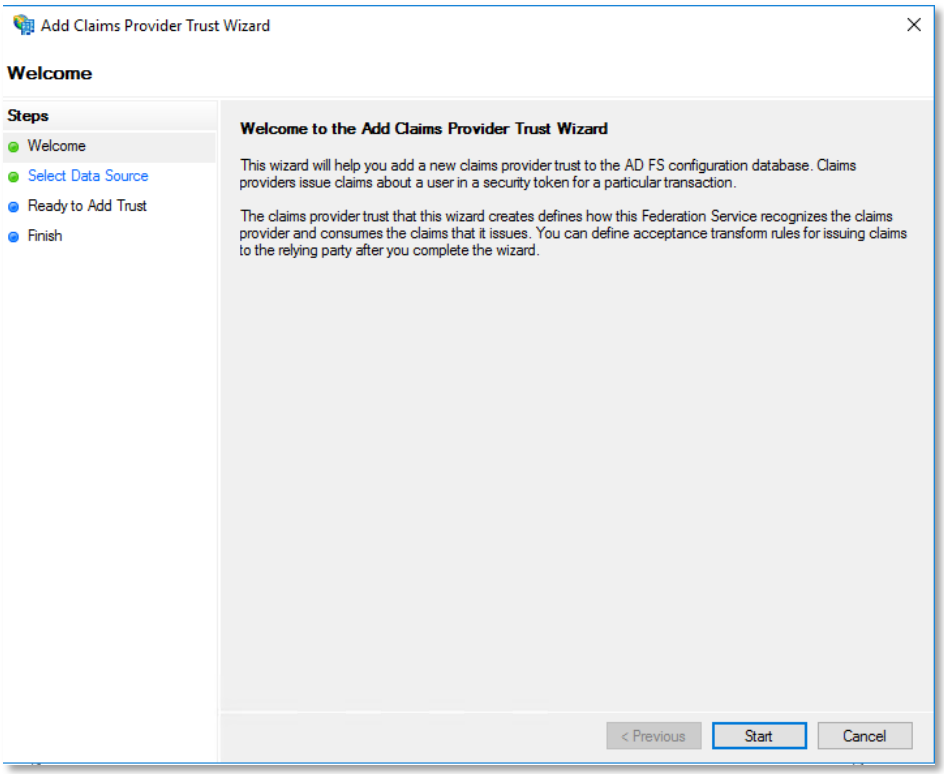
Procedure

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



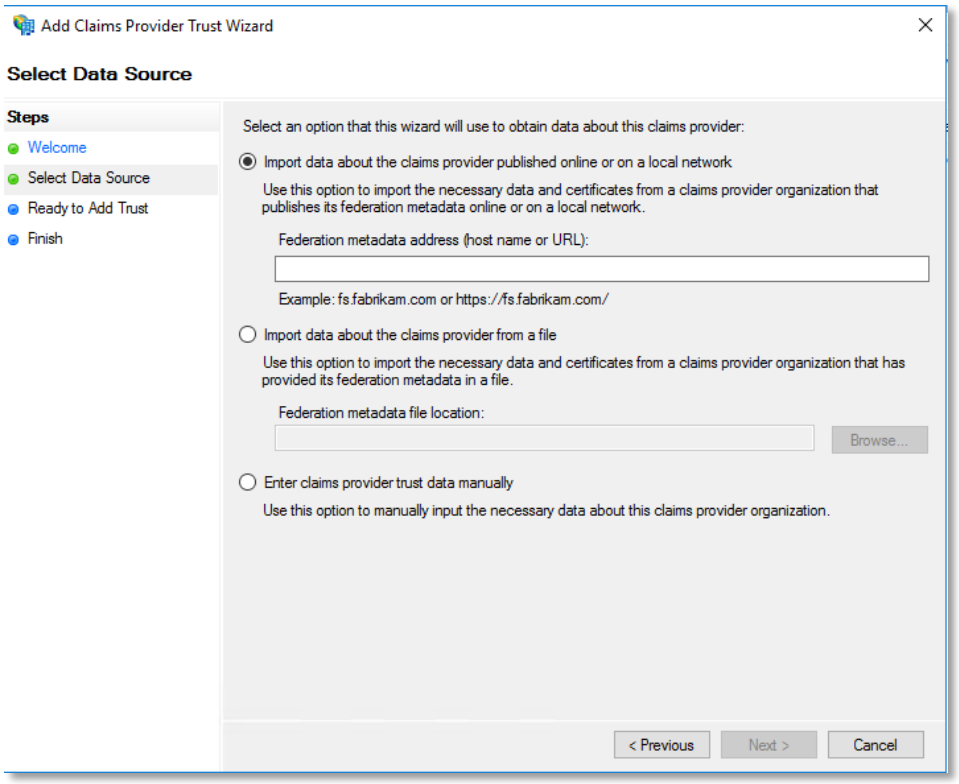
2) On the right pane, select **Add Claims Provider Trust** to open Wizard.

3) In **Welcome**, select **Start**.



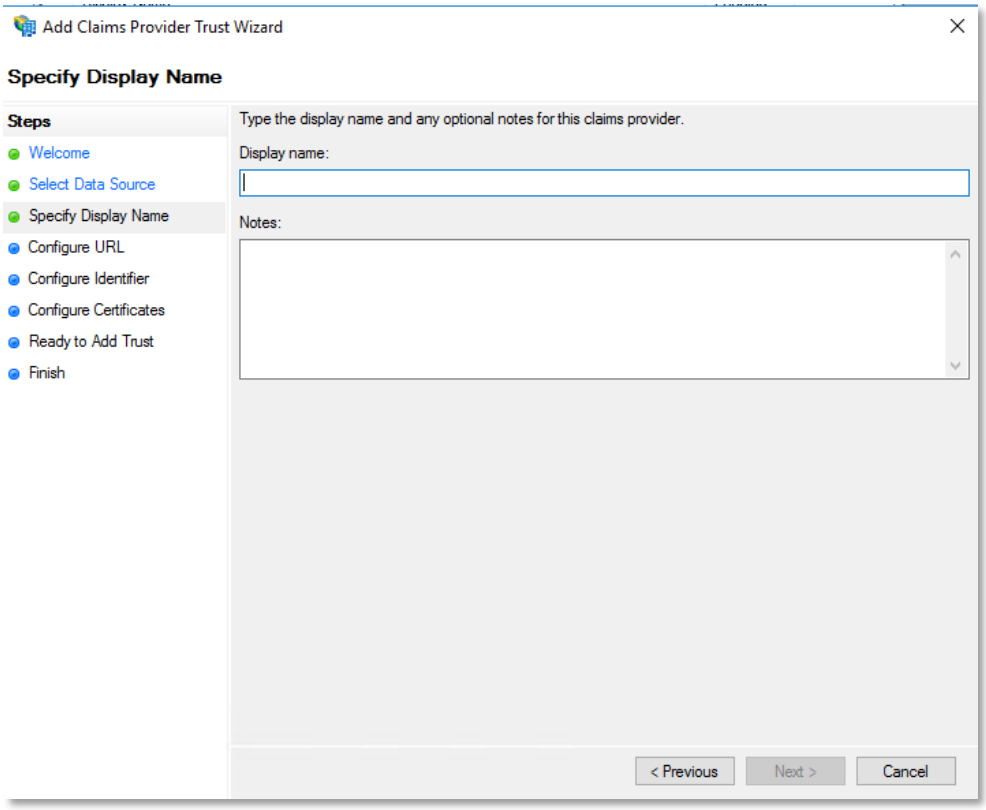
4) In **Select Data Source**, select the following options, as appropriate:

- Using metadata URL
- Using metadata XML
- Manual configuration

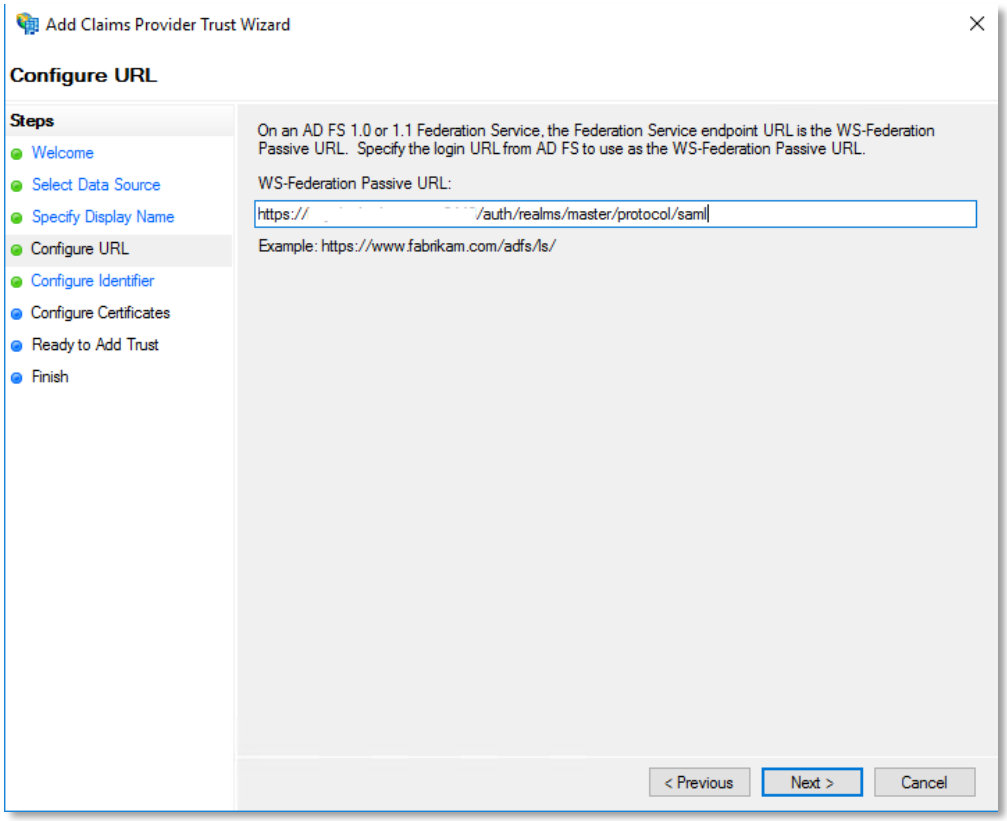


5) To configure Claims Provider Trust manually, do the following:

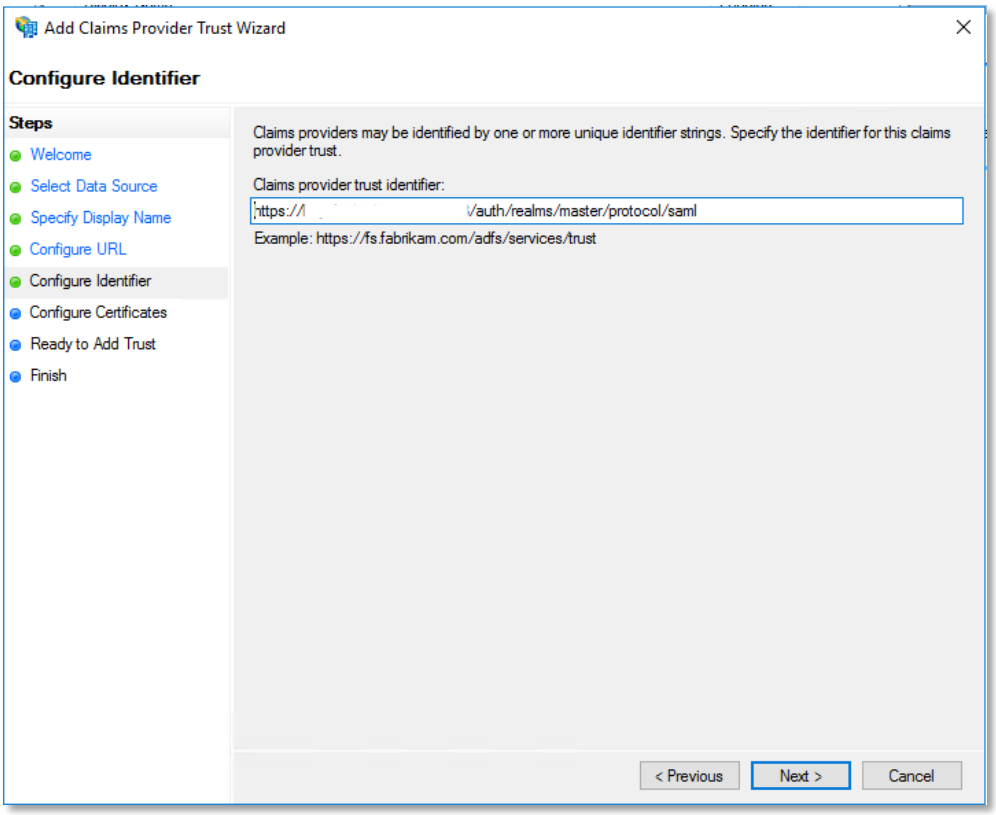
a. In the **Specify Display Name**, enter display name and notes.



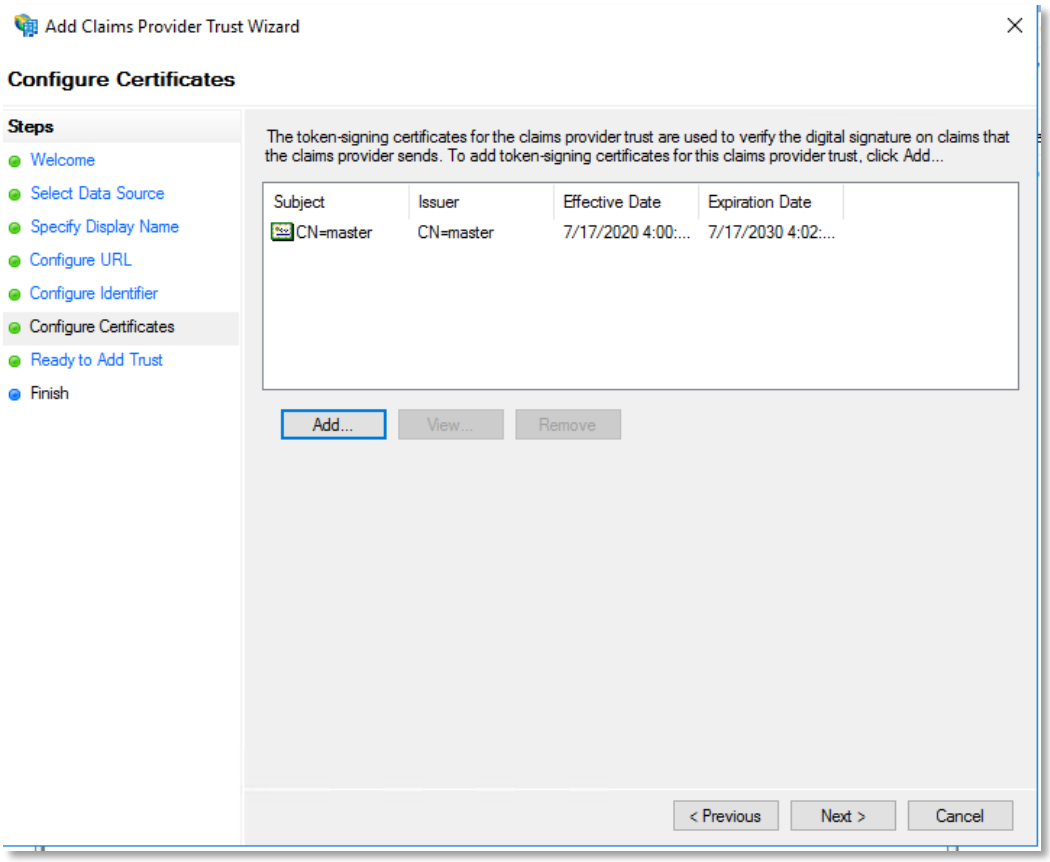
b. In **Configure URL**, enter a service provider URL.



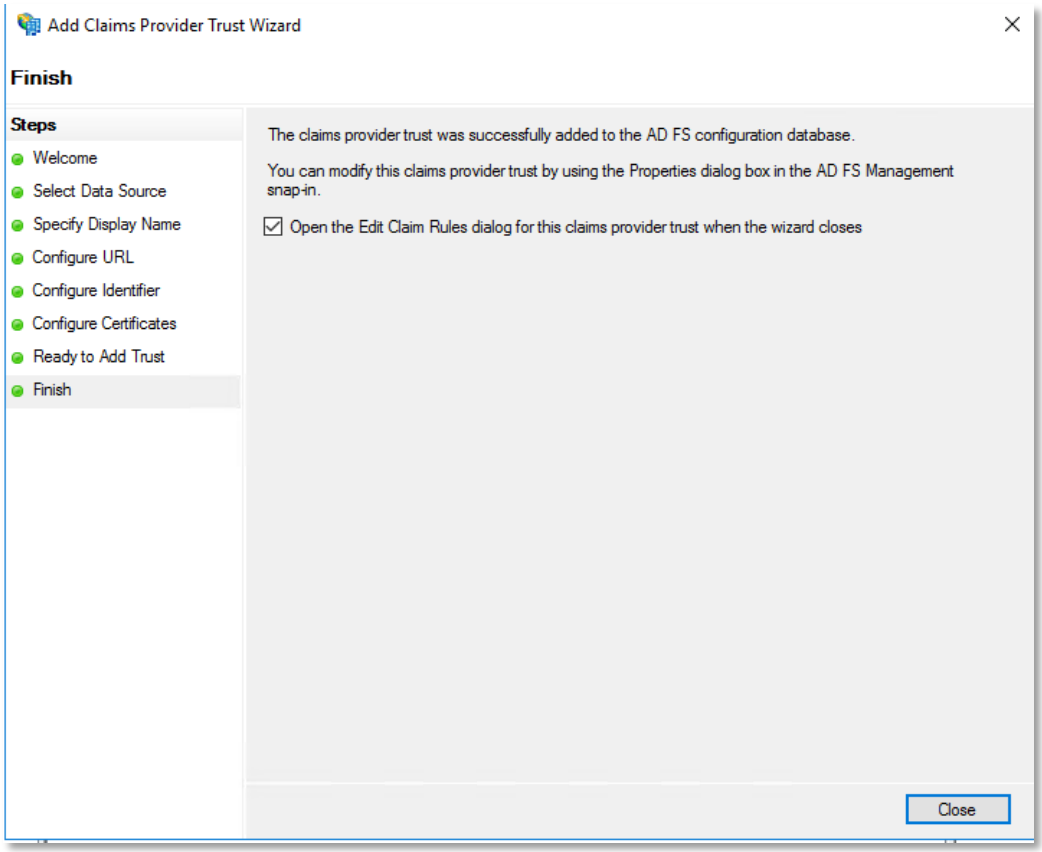
c. In **Configure Identifier**, enter claims provider trust identifier.



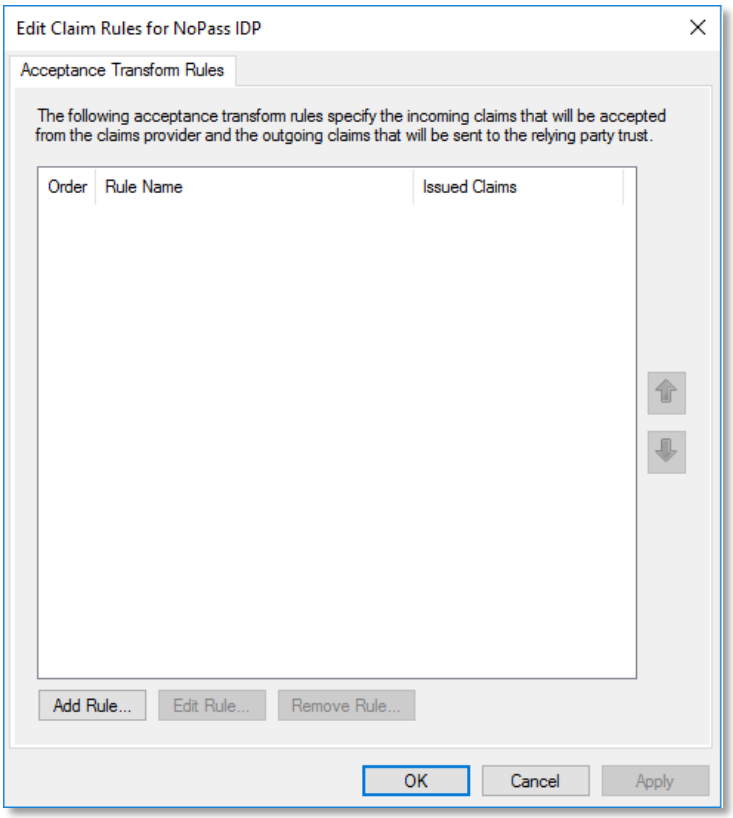
d. In **Configure Certificates**, add the token-signing certificate from Keycloak provider.



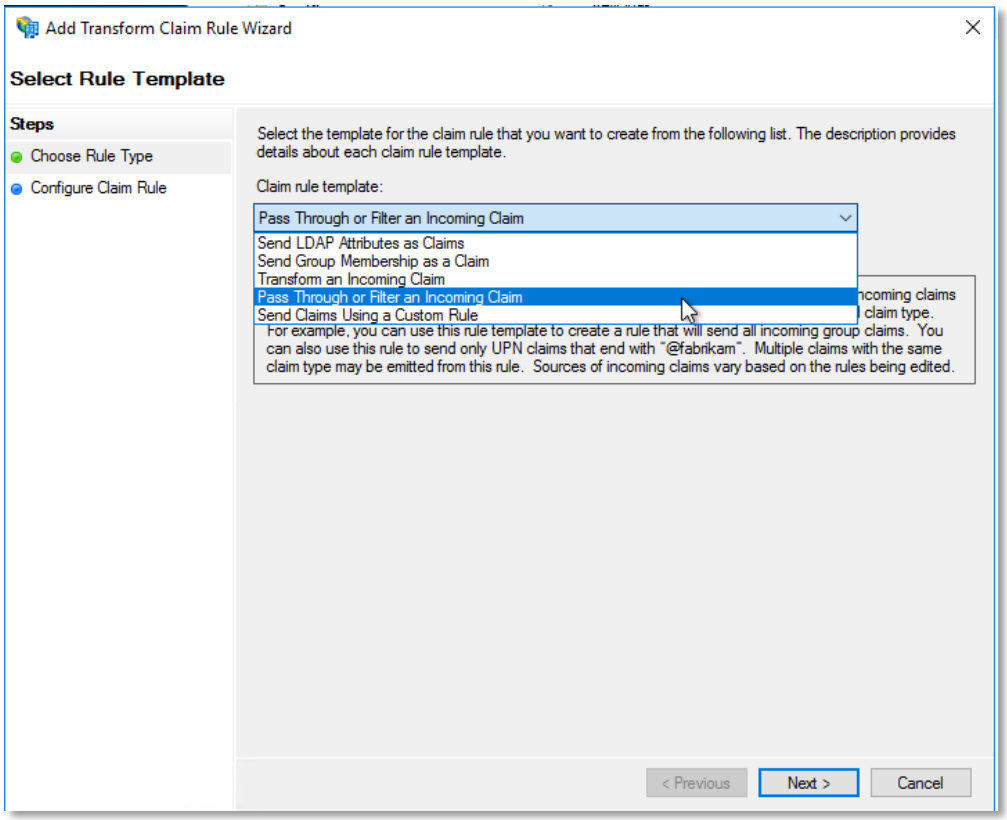
e. Check the ready status and click **Next**.
f. In **Finish**, select **Open the Edit Claim Rules dialog**…, and then click **Close**.



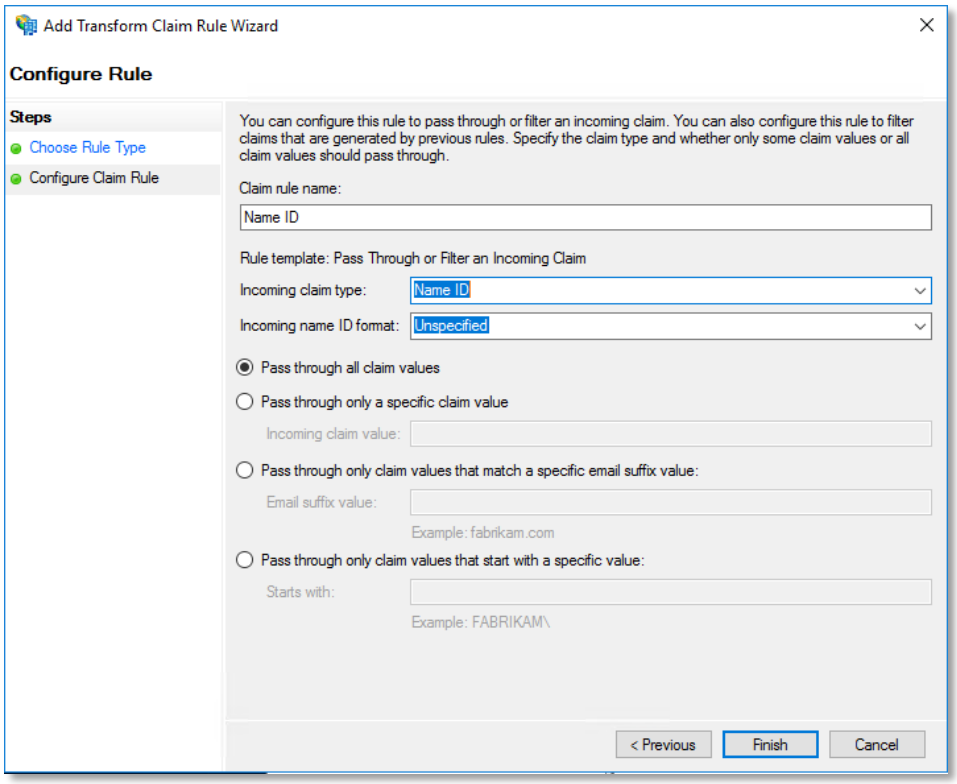
g. In the **Edit Claim Rules for NoPass IDP** dialog box, select **Add Rule**.

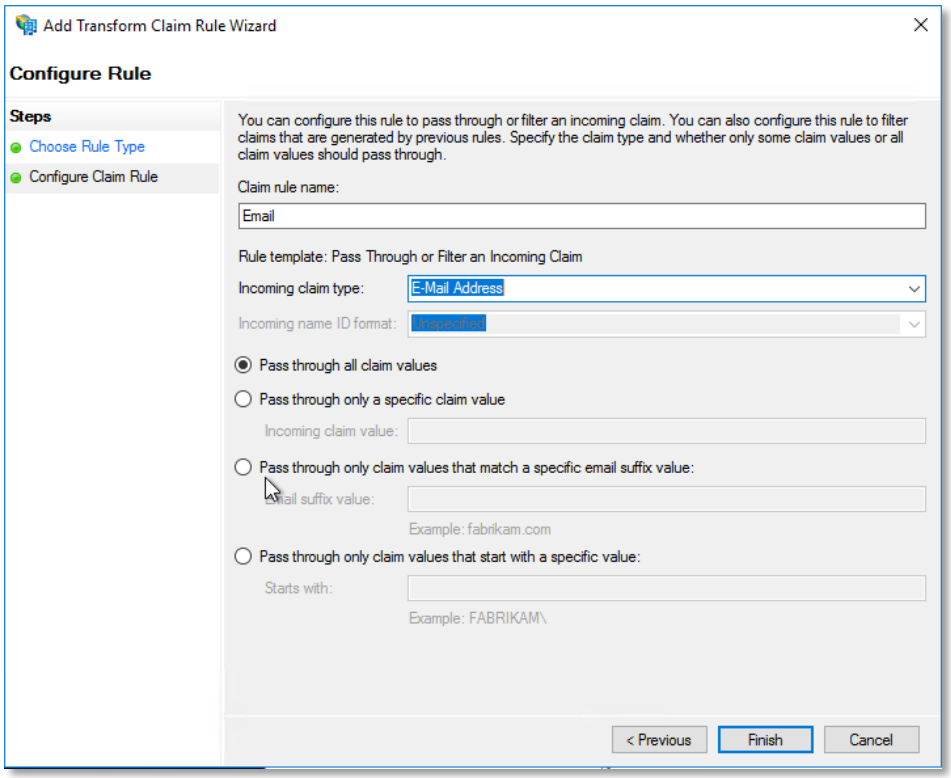


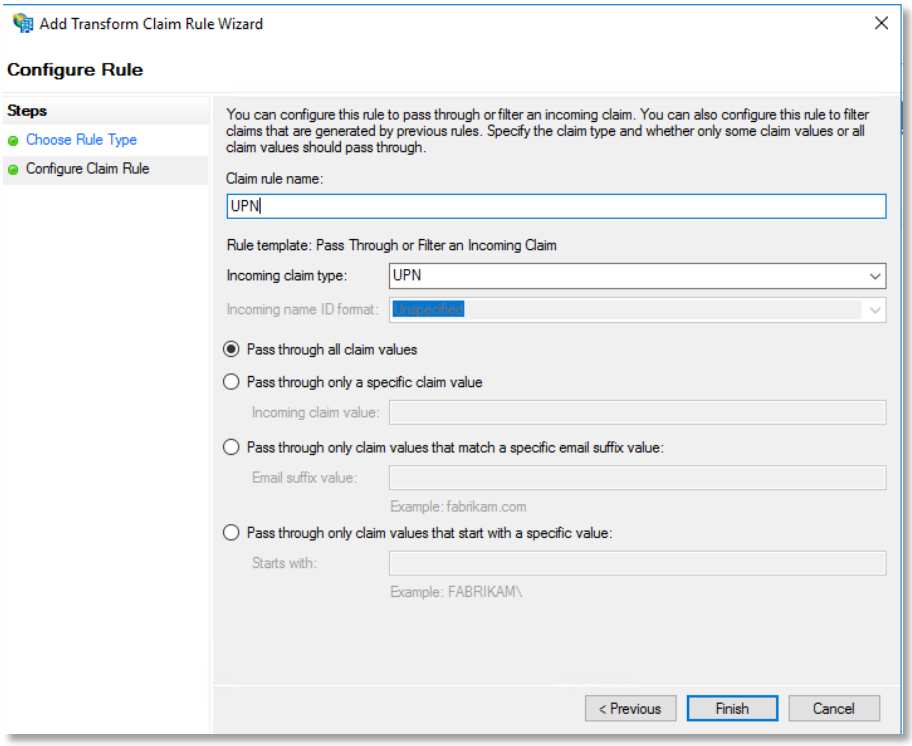
h. In **Select Rule Template**, from the **Claim rule template** list, select **Pass Through of Filter Incoming Claim**, and then select **Next**.

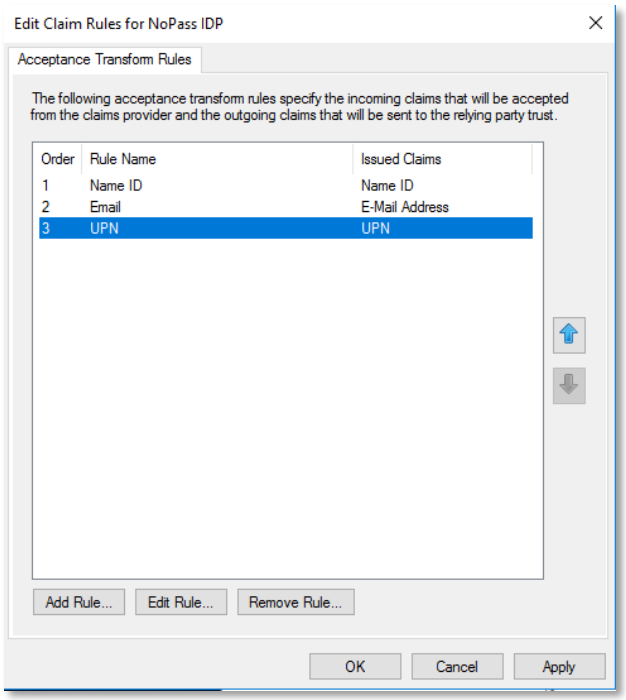


i. In the **Configure Rule** dialog box, in **Choose Rule Type**, configure the following parameters:
   - Name ID
   - Email
   - UPN

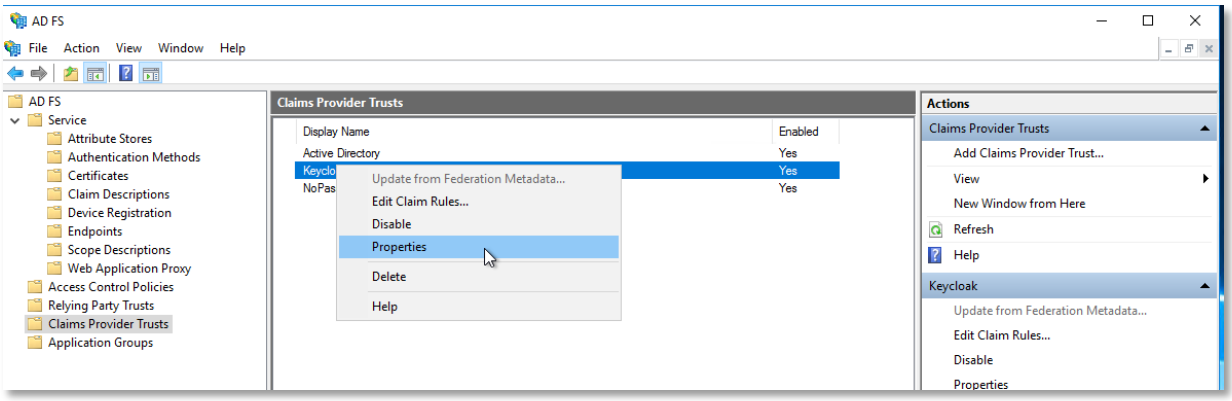

Add Transform Claim Rule Wizard
Configure Rule
Steps
Choose Rule Type
Configure Claim Rule
You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim 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:
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



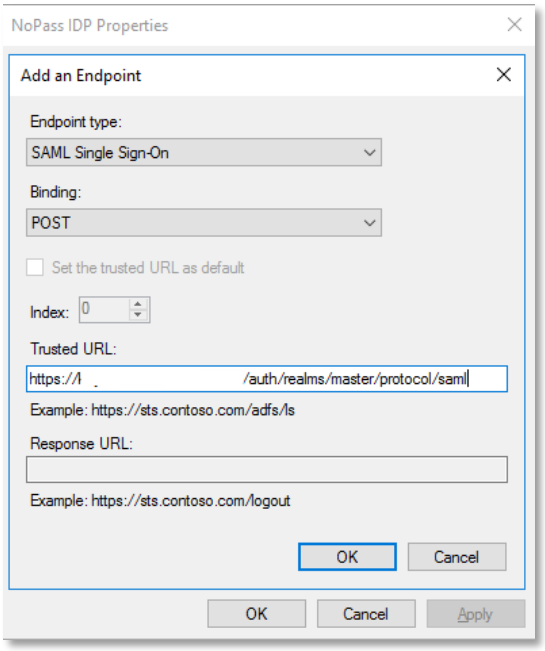


6) In the **AD FS Management** console, select the Claims Provider Trusts folder, and under Keycloak select **Properties**.

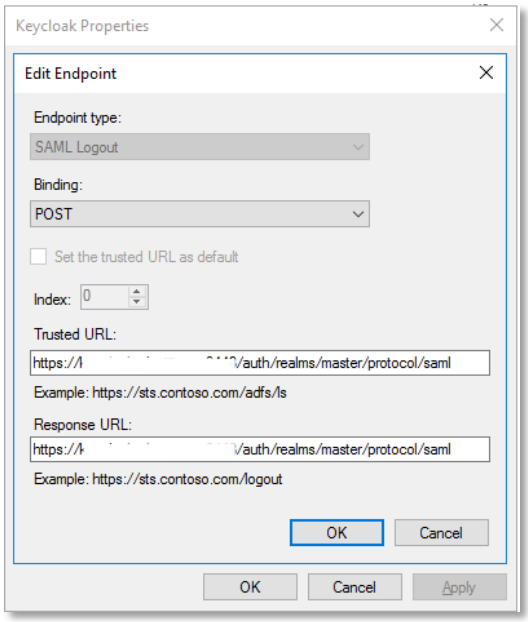


7) In the **NoPass IDP Properties**, select **Endpoints**, and add the following URLs:

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.



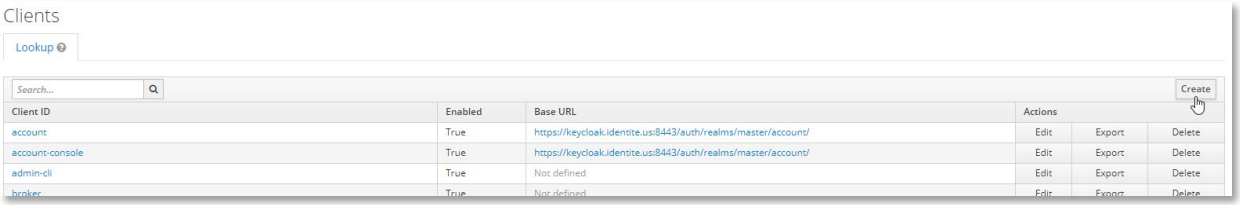
j. Export the AD FS SAML metadata to XML.

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

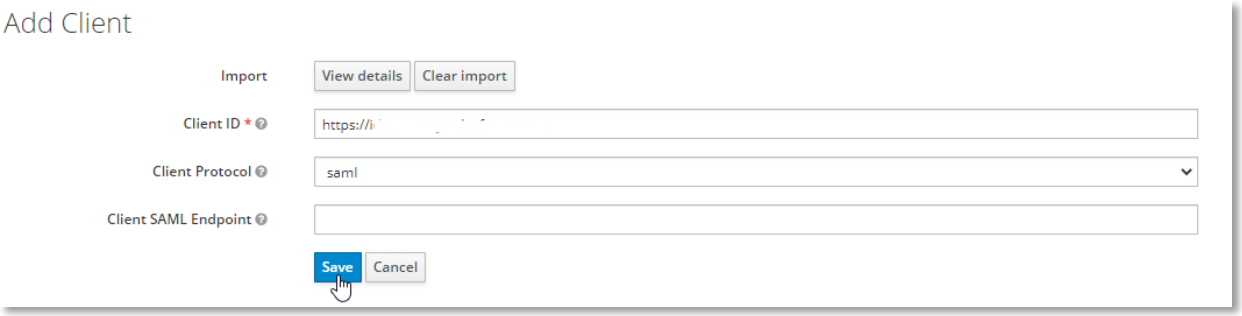
k. Import the AD FS SAML metadata to Keycloak.

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:

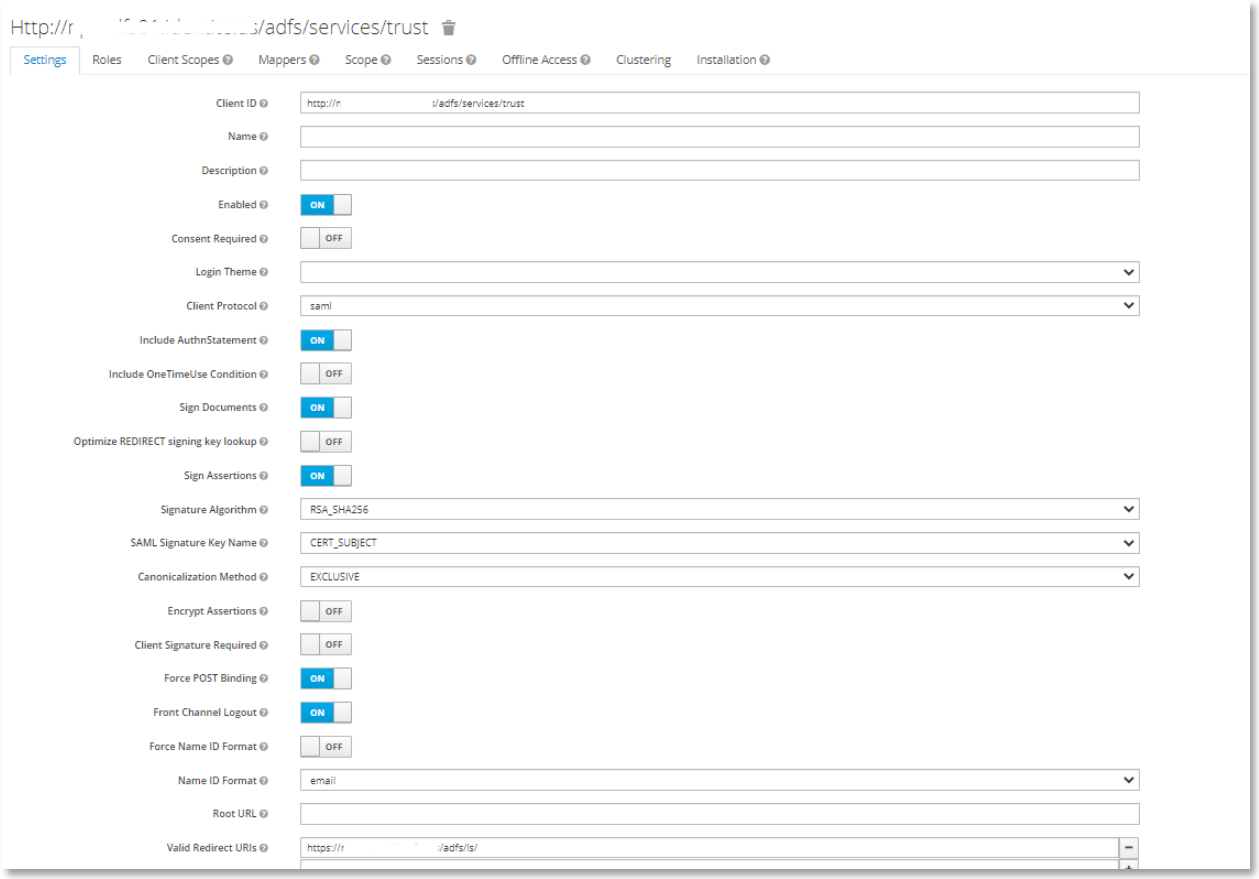
Name	Provide a name for this client
Description (optional)	Provide a description
Enabled	ON
Consent Required	OFF
Client Protocol	SAML
Include AuthnStatement	ON
Sign Documents	ON
Optimize Redirect signing key lookup	OFF
Sign Assertions	ON
Signature Algorithm	RSA_SHA256
Saml Signature Key Name	CERT_SUBJECT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



What to read next

NoPass integration with Box

NoPass integration with Box

To implement this integration, you will need preconfigured Keycloak with SAML 2.0.

For Keycloak configuration instructions, see **Set up service providers with Keycloak**.

Before you begin

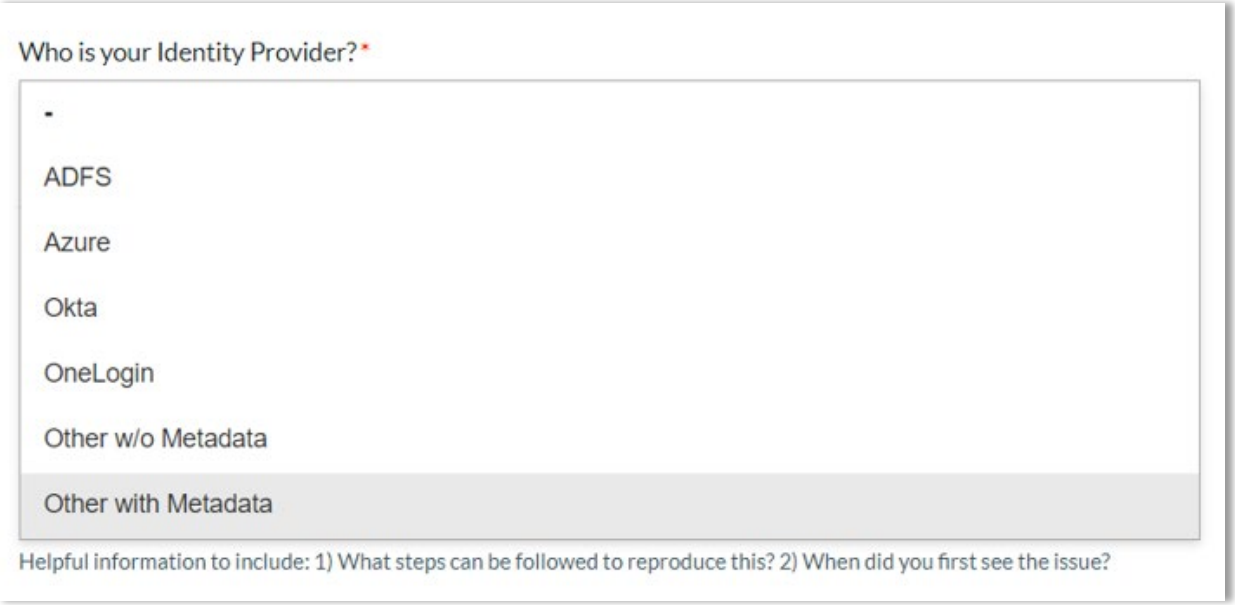
- Navigate to the **Setting Up Single Sign-On (SSO) for Your Enterprise** page at https://support.box.com/hc/en-us/articles/360043696514-Setting-Up-Single-Sign-On-SSO-for-Your-Enterprise and read the instructions.

Procedure

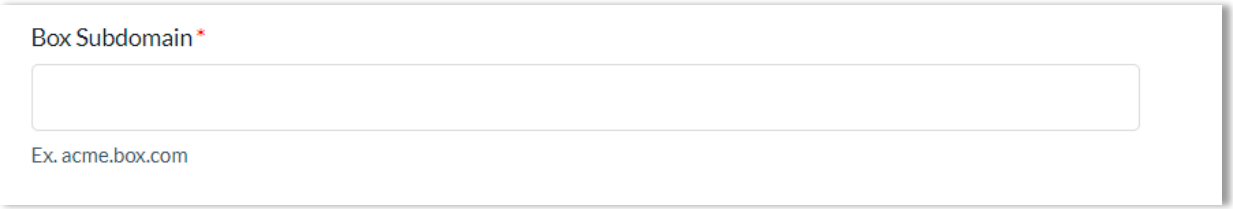
1) Form a request to Box support using one of the following:
   - On the same page, in the **What Box needs from your identity provider** table select **Other/Custom IdPs**, and follow the link:

Other/Custom IdPs	Please contact your IdP directly to assist in obtaining metadata file OR entity id, redirect URL, and signing certificate. Once obtained, use this information to fill out the Box SSO Setup Support Form.	

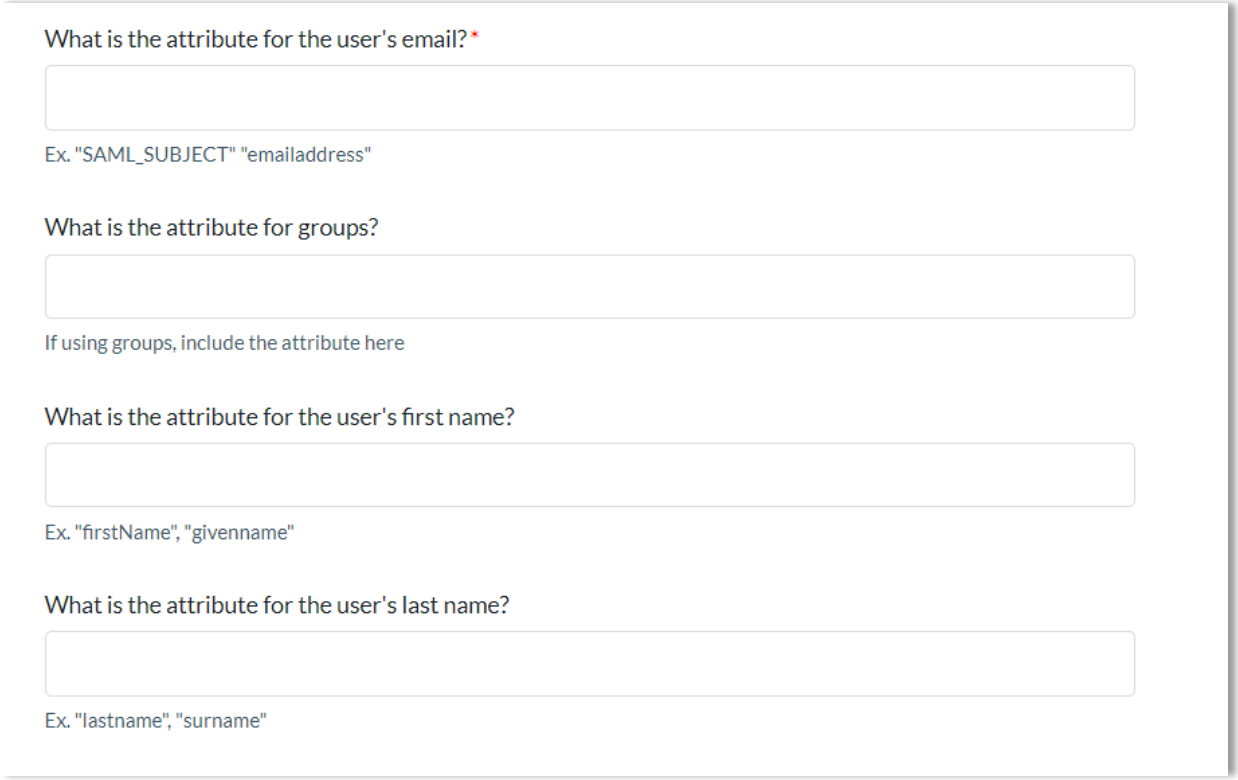
   - Go to https://support.box.com/hc/enus/requests/new?ticket_form_id=360002612594.
2) On the **Box Support** page, in the **Who is your Identity Provider** section, select **Other with Metadata** as shown



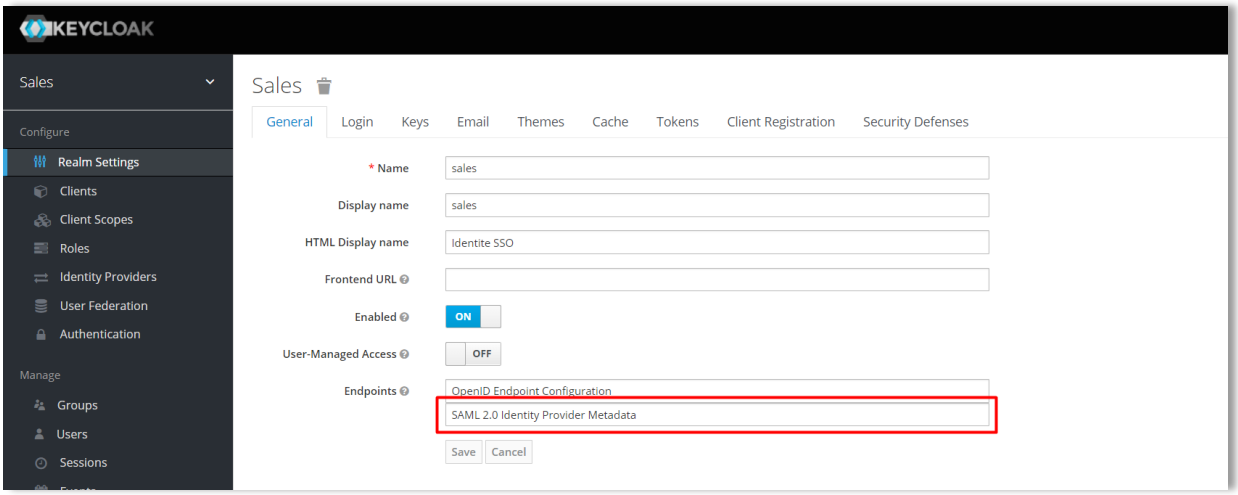
3) Enter your organization's Box Subdomain.



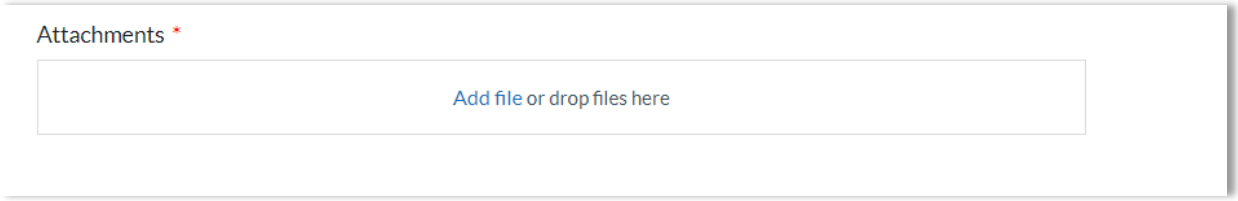
4) Fill in the required attributes, make sure you make a note of the set attributes, we will later need them to map out these attributes in Identitè Keycloak.



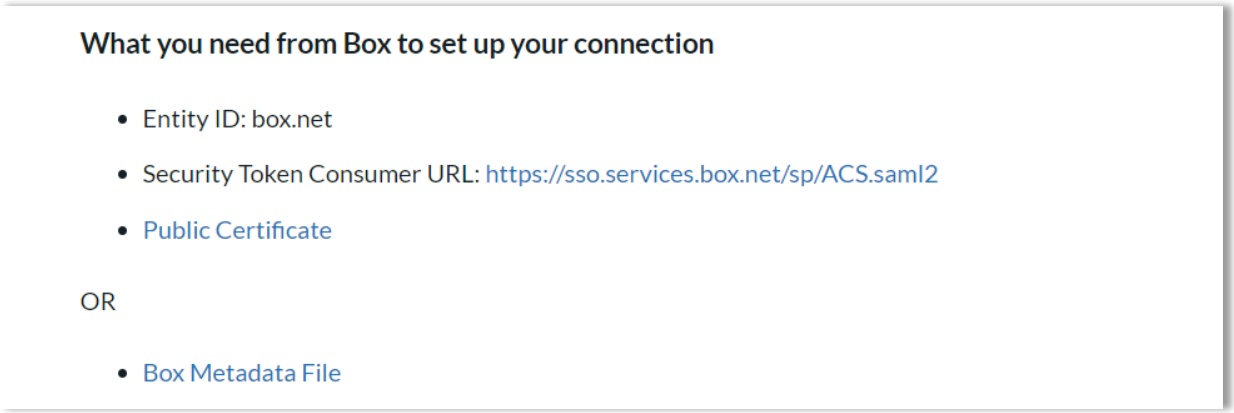
5) Log in to your Identitè Keycloak to get your Identity Provider's SAML metadata from **Realm Settings**.



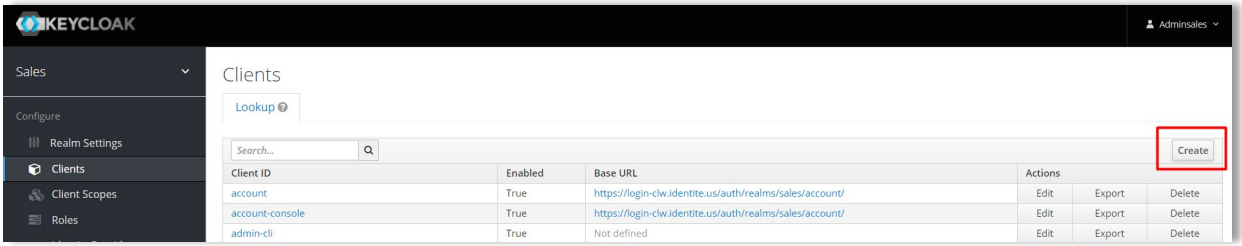
6) Upload this file into the **Attachment** section on the **Box SSO Support Form**, and then submit the form.



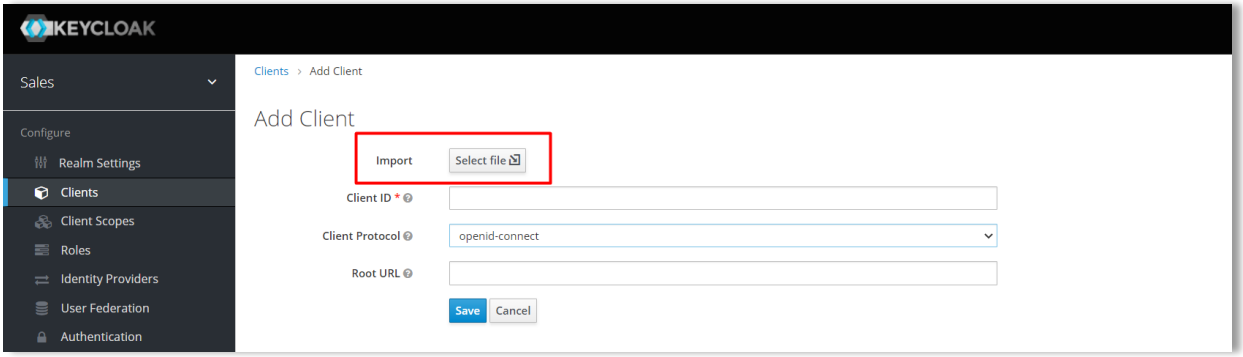
7) In Box, on the **Setting Up Single Sign-On (SSO) for Your Enterprise** page at https://support.box.com/hc/en-us/articles/360043696514-Setting-Up-Single-Sign-On-SSO-for-Your-Enterprise, click the **Box Metadata File** and save it on your computer.



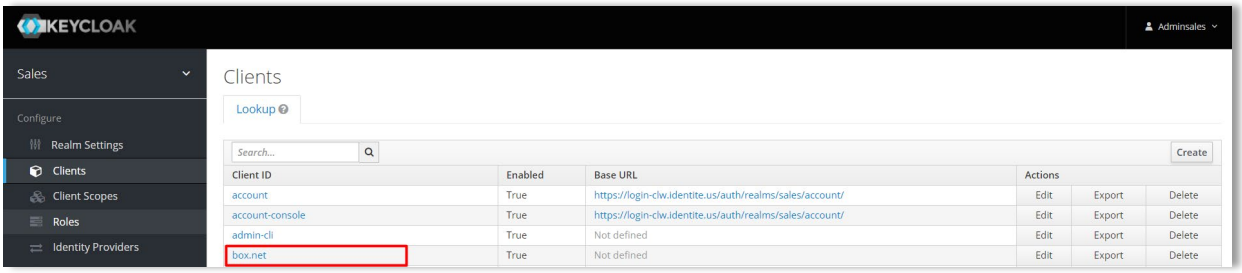
8) Enter your Identite Keycloak. On the **Clients** menu, create a new Client.



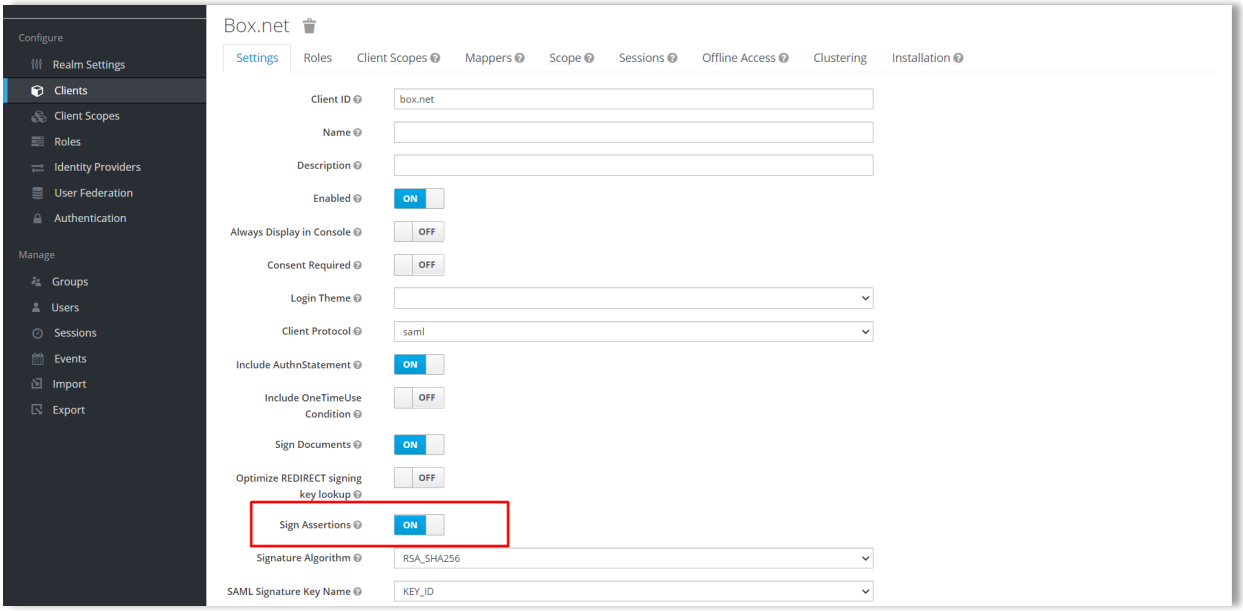
9) On the **Add Client** tab, in **Import**, click **Select file**, and locate the Box Metadata File that you saved during step 7. This file can also be found at https://cloud.app.box.com/s/9y0zm1sqgvkxe8ha2qa3dfhwoivpoyy4.



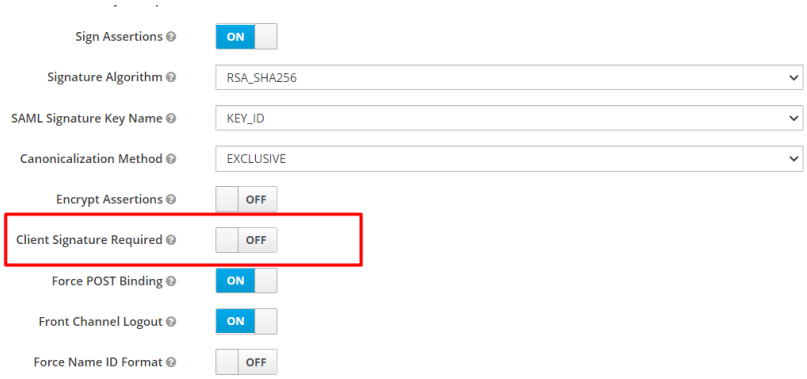
10) Once added, you will be directed to the **Box Client settings** page or you can select it manually from your **Clients** section.



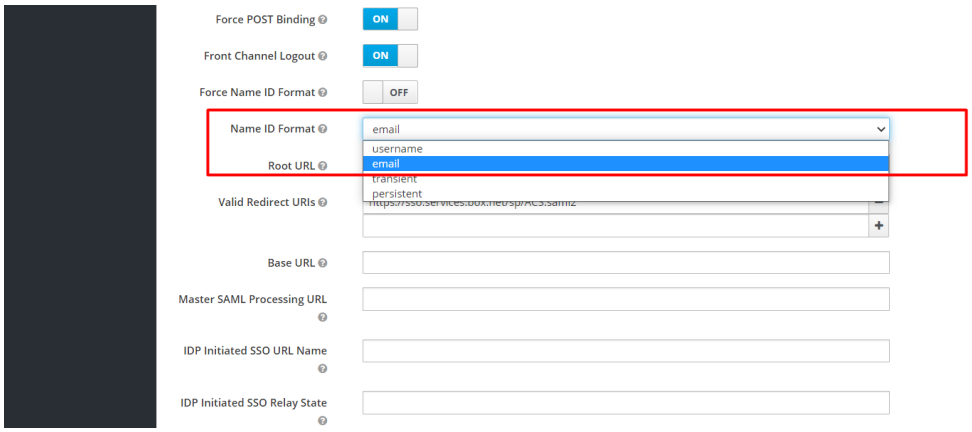
11) In the **Box Client** section, scroll down, and switch on **Sign Assertions**.



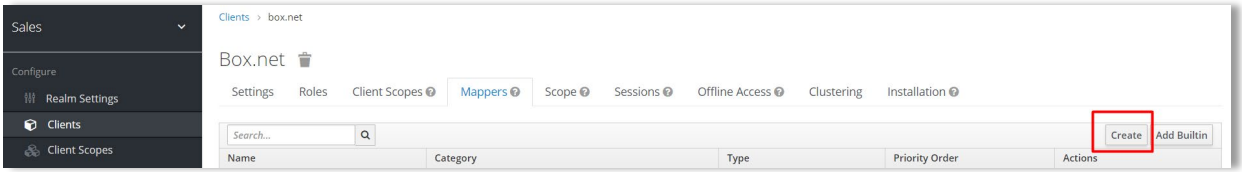
12) Scroll down and switch off **Client Signature Required**.



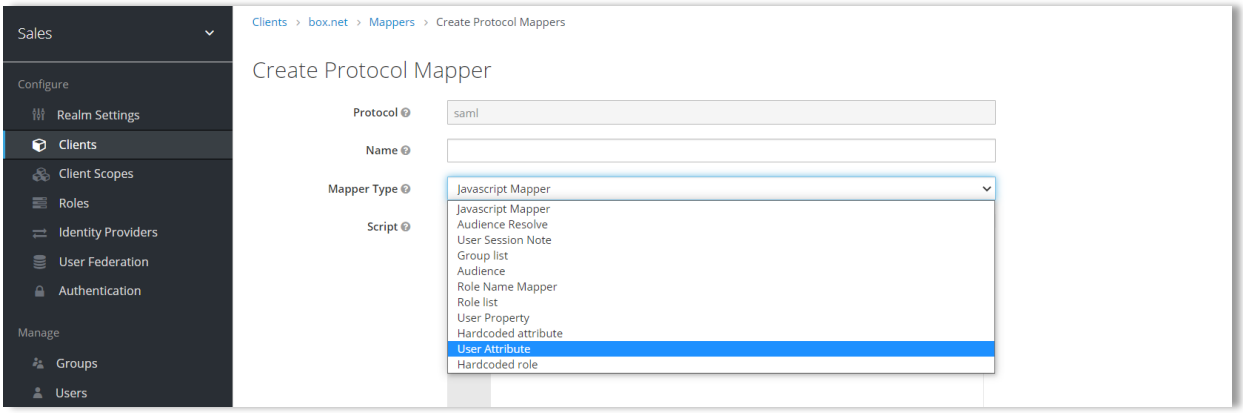
13) In **Name ID Format**, select **email**, and then click **Save**.



14) In the **Clients** menu, on the **Mappers** tab, select **Create**.



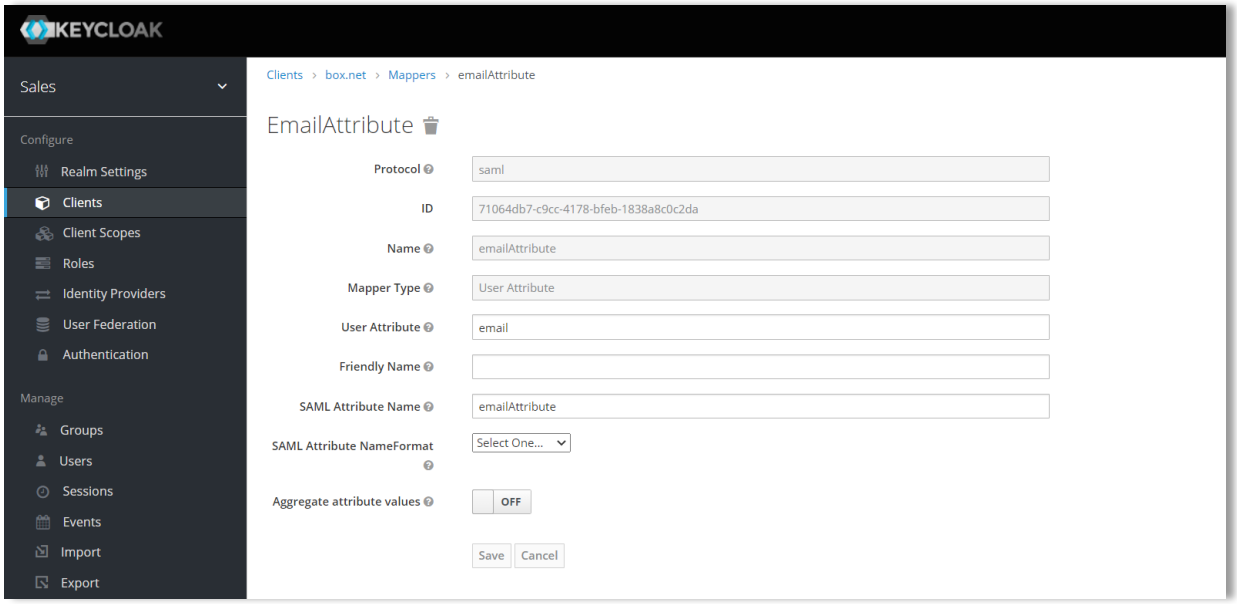
15) On **Create Protocol Mapper**, from **Mapper Type**, select **User Attributes**.

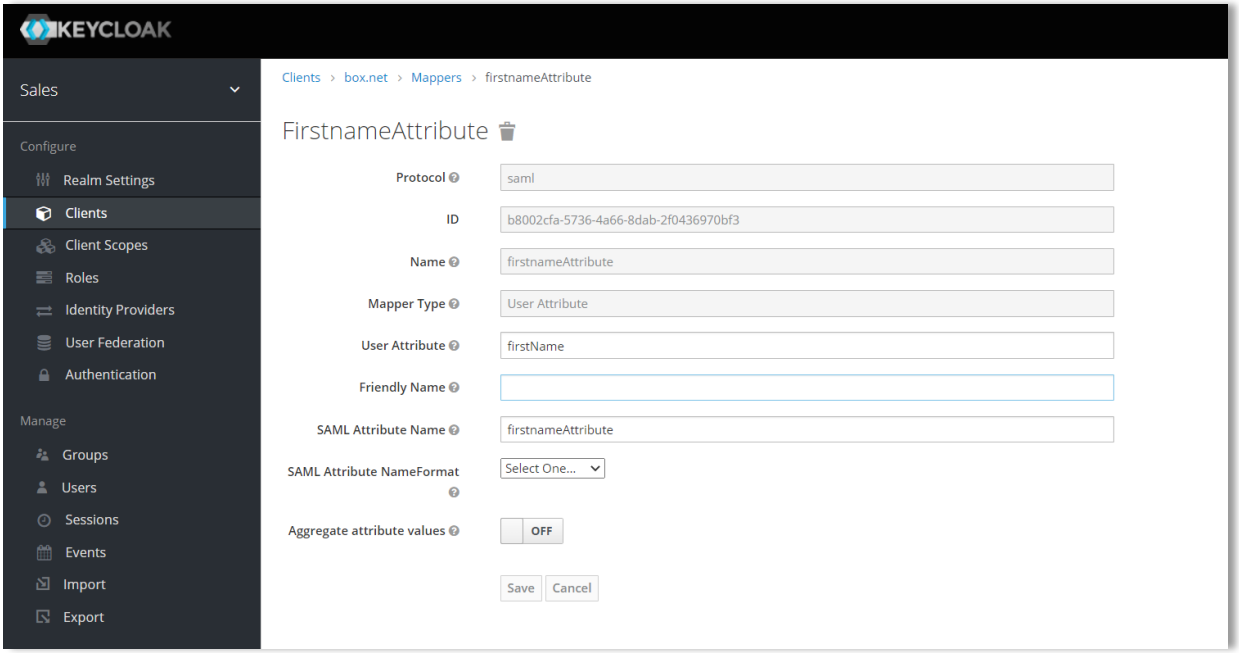


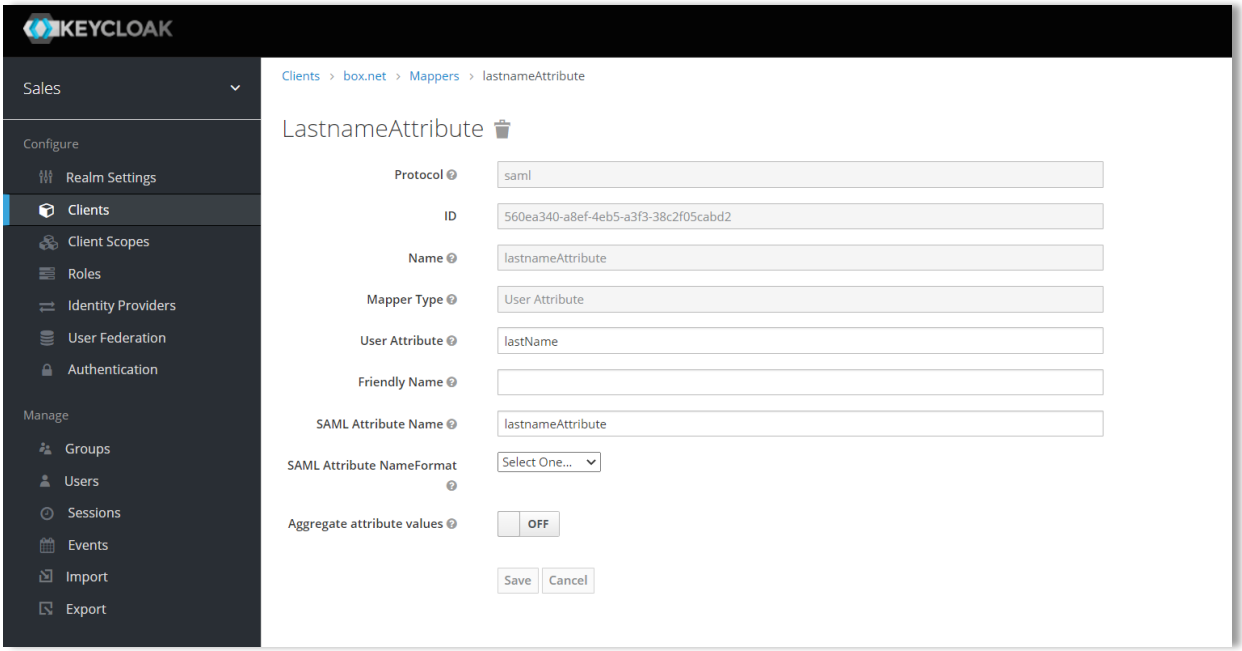
16) Create user attributes that you had set in step 5. You need to create three separate attributes:

- Email
- First name
- Last name

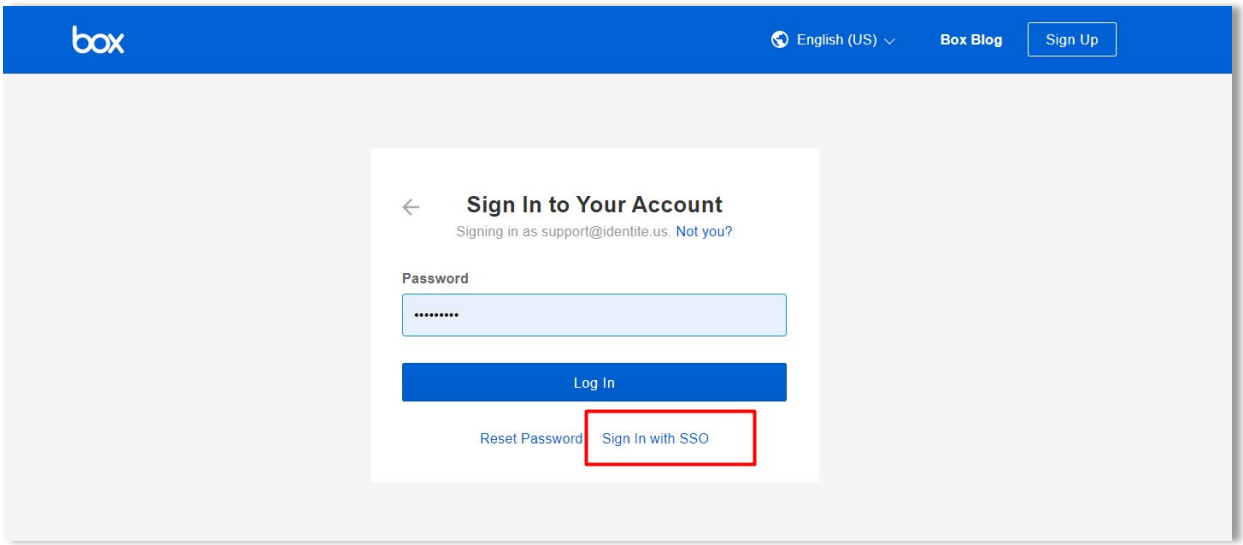
Make sure, the attributes set in step 5 are identical to **Name** and **SAML Attribute Name** on the attribute creation page and then save these attributes.


KEYCLOAK
Sales
Configure
Realm Settings
Clients
Client Scopes
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Clients › box.net › Mappers › emailAttribute
EmailAttribute
Protocol
saml
ID
71064db7-c9cc-4178-bfeb-1838a8c0c2da
Name
emailAttribute
Mapper Type
User Attribute
User Attribute
email
Friendly Name
SAML Attribute Name
emailAttribute
SAML Attribute NameFormat
Select One...
Aggregate attribute values
OFF
Save
Cancel


KEYCLOAK
Sales
Configure
Realm Settings
Clients
Client Scopes
Roles
Identity Providers
User Federation
Authentication
Manage
Groups
Users
Sessions
Events
Import
Export
Clients › box.net › Mappers › firstnameAttribute
FirstnameAttribute
Protocol
saml
ID
b8002cfa-5736-4a66-8dab-2f0436970bf3
Name
firstnameAttribute
Mapper Type
User Attribute
User Attribute
firstName
Friendly Name
SAML Attribute Name
firstnameAttribute
SAML Attribute NameFormat
Select One...
Aggregate attribute values
OFF
Save
Cancel



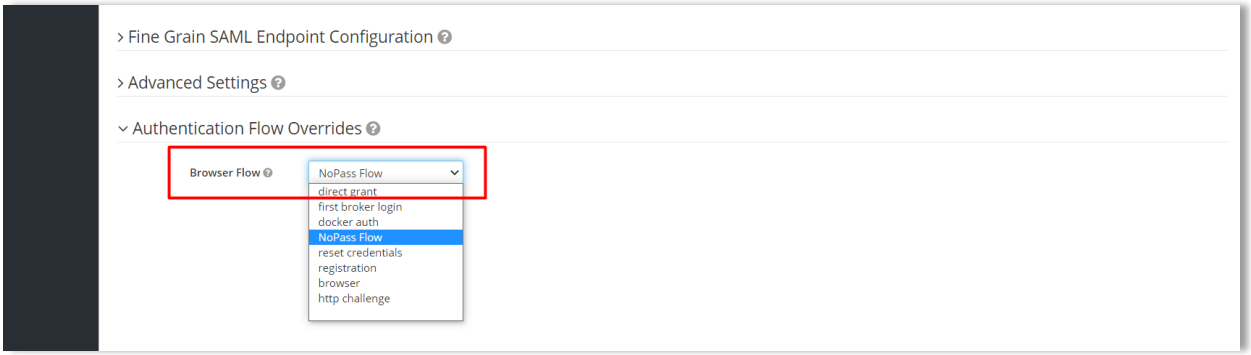
17) Go to your Box login page and test the SSO Login.



18) Once you are successfully logged in, navigate back to your Identite Keycloak, and do the following:

a. On the **Box client** tab, on the **Settings** subtab, scroll down to the bottom of the page and select the **Authentication Flow Overrides**.

b. From the drop down menu, select the **NoPass flow,** and then click **Save**.



Box SSO is now protected with NoPass.

What to read next

NoPass integration with GitLab

NoPass integration with GitLab

The following instructions enable you to use NoPass 2FA for GitLab CE and EE versions. For this purpose, you will need a preconfigured Keycloak instance with SAML 2.0.

For Keycloak configuration instructions, see Section 6.4. **Set up service providers with Keycloak.**

For detailed instructions how to configure GitLab, see SAML OmniAuth Provider.

Create SAML client in Keycloak

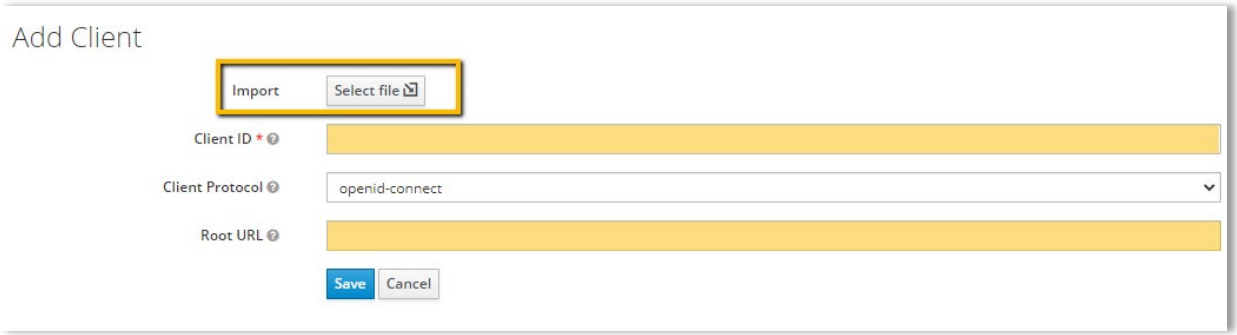
1) In the Keycloak admin console, go to your realm > the **Clients** tab. Click **Create**.

Note: The following instructions are shown for the realm called Stage. Your realm name can be different.

2) On the **Add client** tab, do the following:

   a. Import the metadata file by inserting the URL: https://*gitlab.example*.com/users/auth/saml/metadata

   b. Fill in the client information fields, and then click **Save**.



Configure the client in Keycloak for GitLab

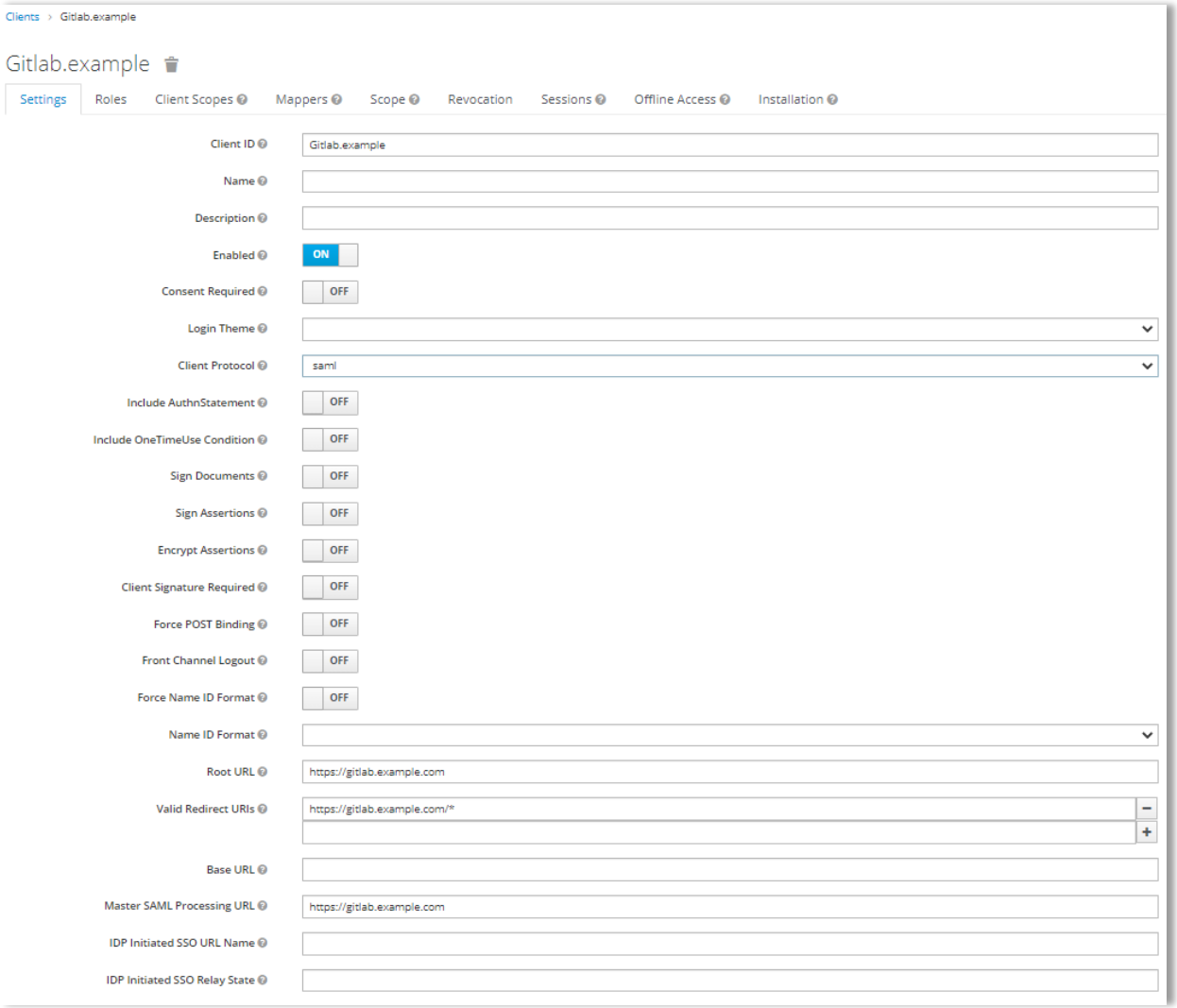
1) In the **Clients** menu, select the newly created client.

2) On the **Settings** tab, set the following parameters:

   a. **Enabled**—ON

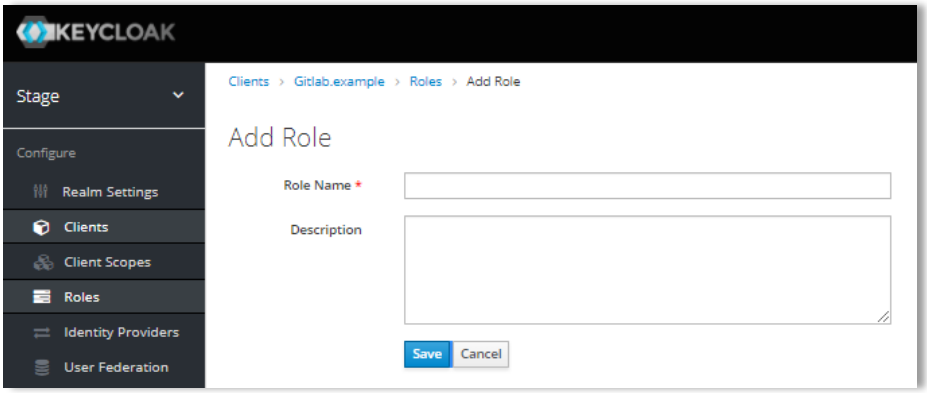
   b. **Standard flow enabled**—ON

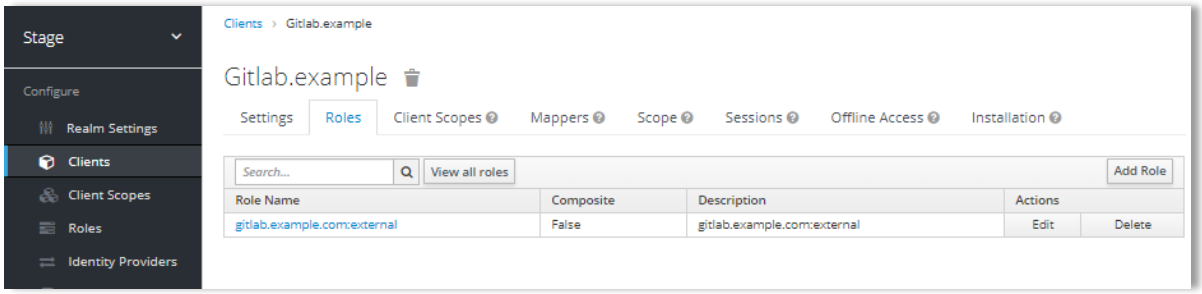
c. **Direct Access Grants Enabled**—ON



Configure roles

1) On the **Roles** tab, click **Add role** to create a group named **external** for Gitlab.
2) On the **Add role** page, fill in the following fields, and click **Save**:
   - **Role name:** *gitlab.example.com:external*
   - **Description:** *gitlab.example.com:external*





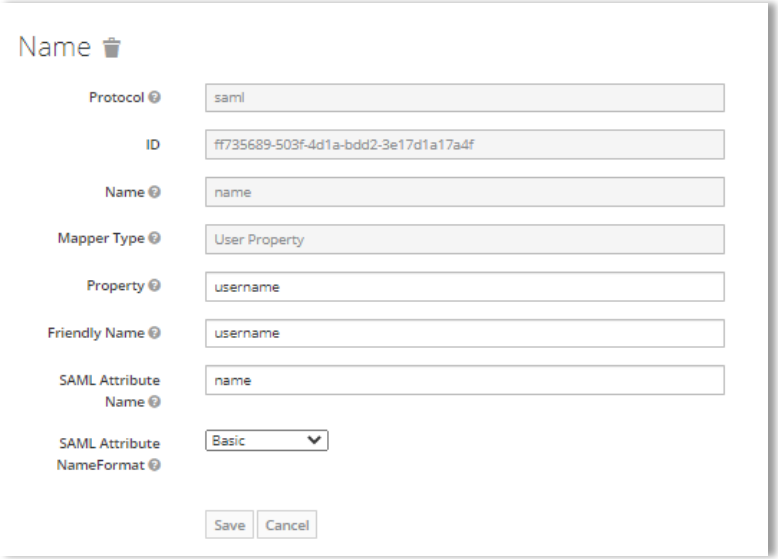
Create and configure mappers

Mappers allow to match fields from Keycloak to a service provider. For more information about SAML assertion mappings, see Keycloak Server Administration

1) On the **Mappers** tab, click **Create** to add mappers for GitLab in Keycloak.
2) On the **Create Protocol Mapper** page, fill in the following fields for the mapper, and then click **Save**:

Name	Enter **name**
Mapper type	Select **User Property**
Property	Enter **username**
Friendly name	Enter **username** or leave empty
SAML Attribute Name	Enter **name**
SAML Attribute Name Format	Select **Basic**

The successful result is as follows:



3) Repeat steps 5, 6 to create mappers for email, first_name, last_name, and roles. Populate the fields as suggested below:

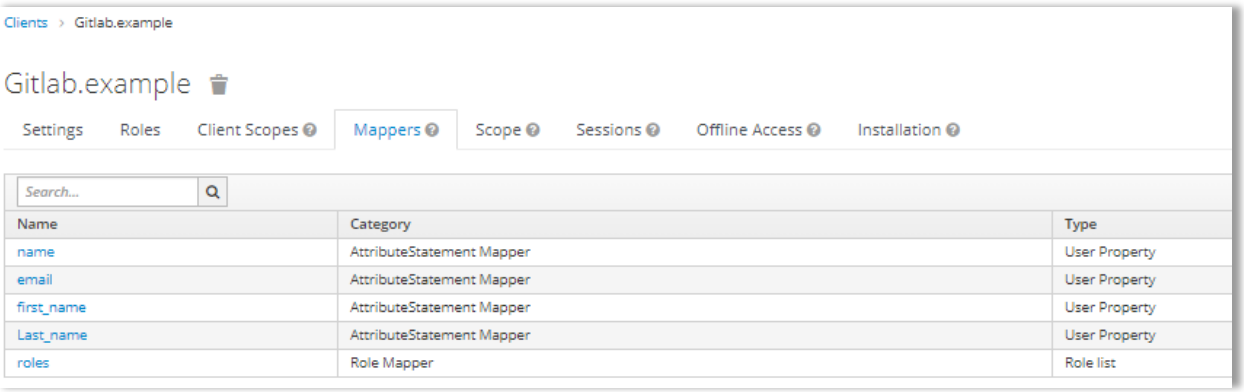
Name	Enter **email**
Mapper Type	Select **User Property**
Property	Enter **email**
Friendly name	Enter **email** or leave empty
SAML Attribute Name	Enter **email**
SAML Attribute NameFormat	Select **Basic**

Name	Enter **first_name**
Mapper Type	Select **User Property**
Property	Enter **FirstName**
Friendly name	Enter **First Name** or leave empty
SAML Attribute Name	Enter **First name**
SAML Attribute NameFormat	Select **Basic**

Name	Enter **Last_name**
Mapper Type	Select **User Property**
Property	Enter **last name**
Friendly name	Enter **last name** or leave empty
SAML Attribute Name	Enter **last name**
SAML Attribute NameFormat	Select **Basic**

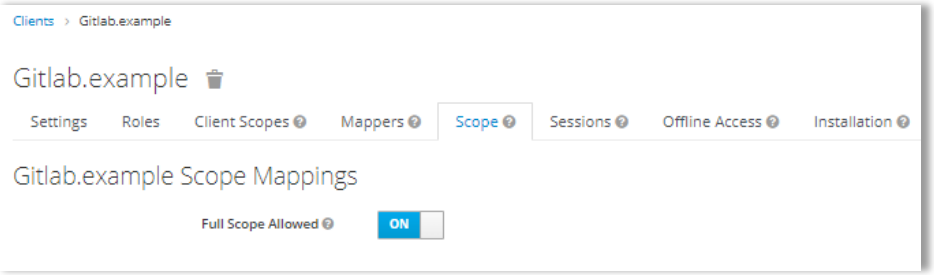
Name	Enter **roles**
Mapper Type	Select **Role list**
Role attribute name	Enter **Role**
Friendly name	Enter **Roles** or leave empty
SAML Attribute NameFormat	Select **Basic**
Single Role Attribute	Switch to **ON**

The successful result is as follows:



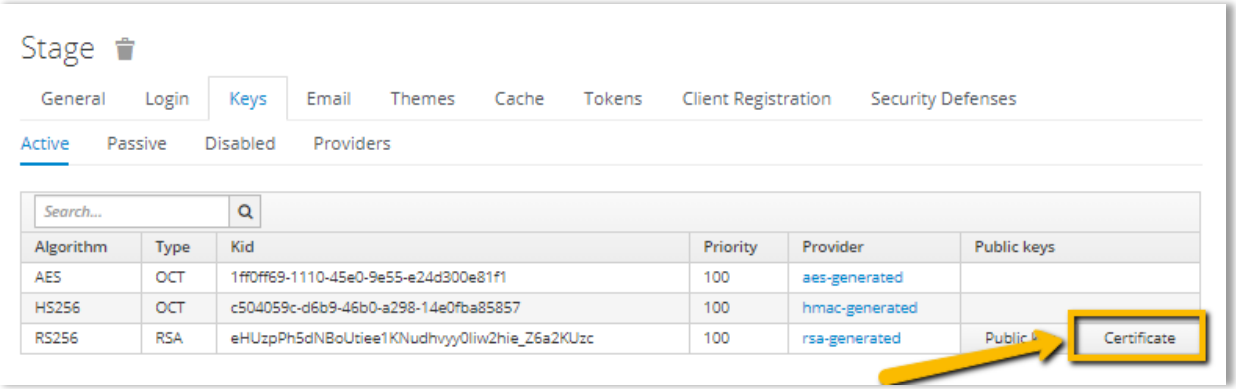
Scope tab parameters

- On the **Scope** tab, switch the **Full Scope Allowed** toggle on.



Copy the certificate

- In the **Realm Settings** menu, on the **Keys** tab, click **Certificate** to download the public certificate.



Configure GitLab

1) On your **GitLab** server, open the configuration file.

   For Omnibus package:

```
sudo editor /etc/gitlab/gitlab.rb
```

   For installations from source:

```
Cd /home/git/gitlab
Sudo -u git -H editor config/gitlab.yml
```

2) Add the provider configuration and public certificate for your GitLab instance to use for SAML:

   For example:

```
omniauth:
  providers:
    - {
      name: 'saml',
      args: {
        assertion_consumer_service_url:
'https://gitlab.example.com/users/auth/saml/callback',
        idp_cert_fingerprint: '43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8',
        idp_sso_target_url: 'https://login.example.com/idp',
        issuer: 'https://gitlab.example.com',
        name_identifier_format: 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'
      },
      label: 'Company Login'  # optional label for SAML login button, defaults to "Saml"
    certificate: '-----BEGIN CERTIFICATE-----
    <redacted>
    -----END CERTIFICATE-----',
  private_key: '-----BEGIN PRIVATE KEY-----
    <redacted>
    -----END PRIVATE KEY-----',
  security: {
    authn_requests_signed: true,  # enable signature on AuthNRequest
    want_assertions_signed: true,  # enable the requirement of signed assertion
    embed_sign: true,  # embedded signature or HTTP GET parameter signature
    metadata_signed: false,  # enable signature on Metadata
    signature_method: 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256',
    digest_method: 'http://www.w3.org/2001/04/xmlenc#sha256',
  }
}
```

3) Change the value for `assertion_consumer_service_url` to match the HTTPS endpoint of GitLab (append `users/auth/saml/callback` to the HTTPS URL of your GitLab installation to generate the correct value).

4) Change the values of `idp_cert_fingerprint`, `idp_sso_target_url`, `name_identifier_format` to match your IdP.

5) Change the value of `issuer` to a unique name, which will identify the application to the IdP.

Warning: The name specified in `issuer` must be used when registering the GitLab SP in Keycloak.

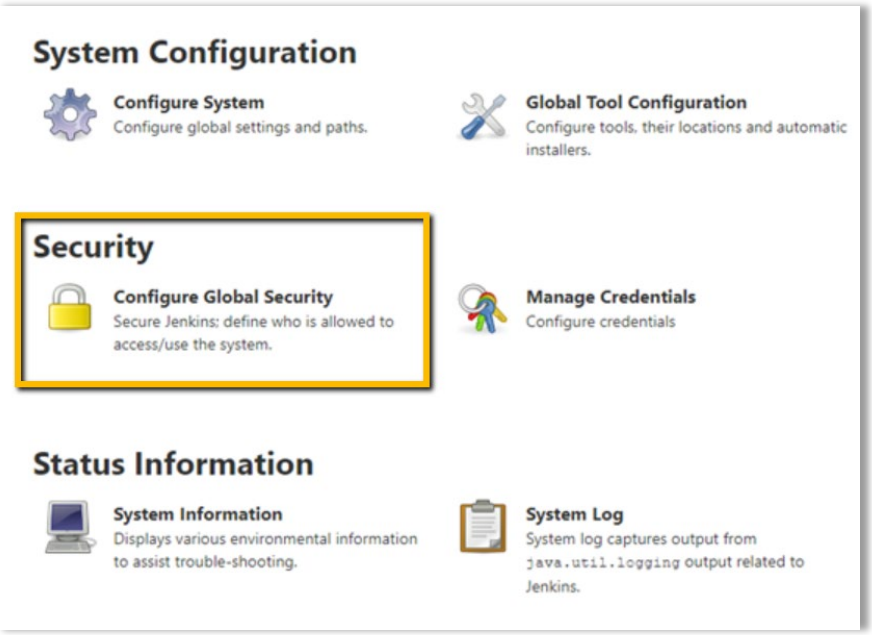
6) For the changes to take effect, reconfigure or restart GitLab.

NoPass integration with Jenkins

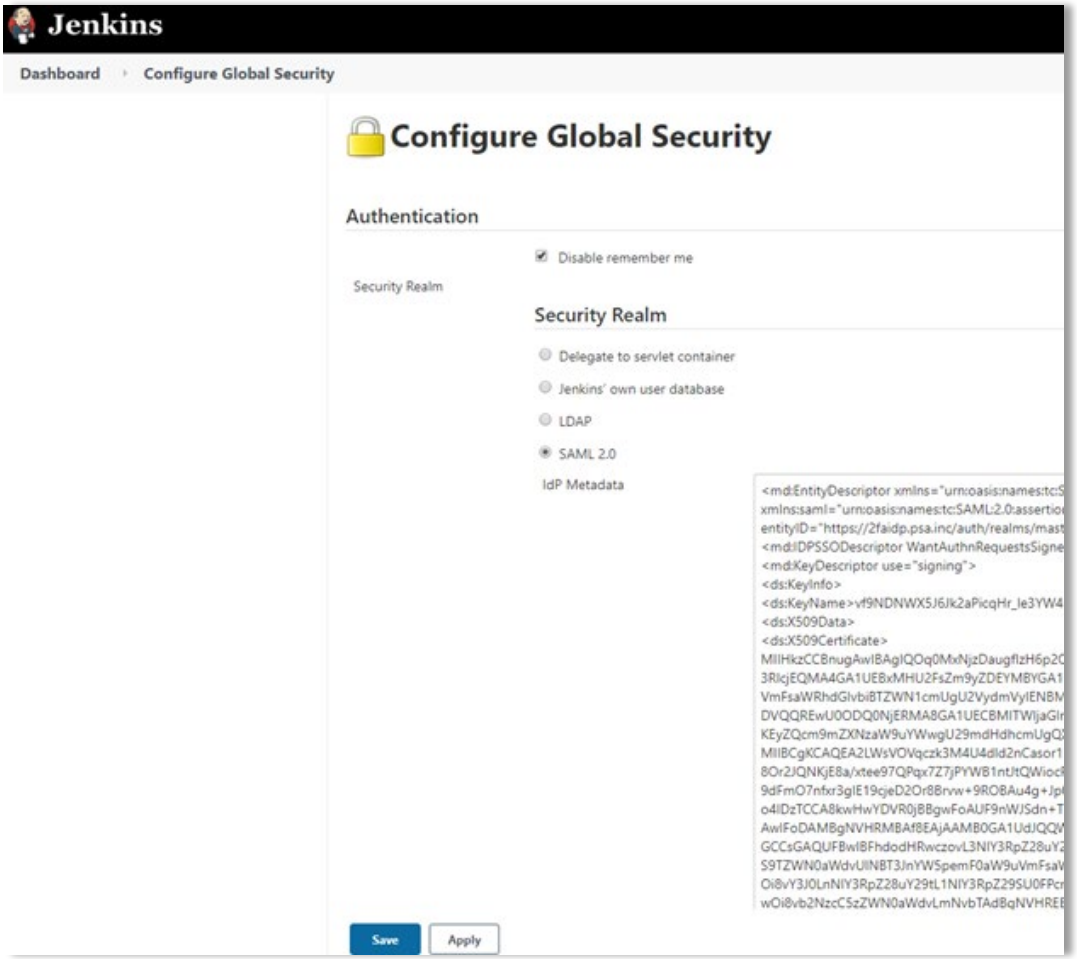
Copy the IdP Metadata from Keycloack

Configure Jenkins

1) Go to **Dashboard** > **Manage Jenkins** > **System Configuration** and select **Configure Global Security**.

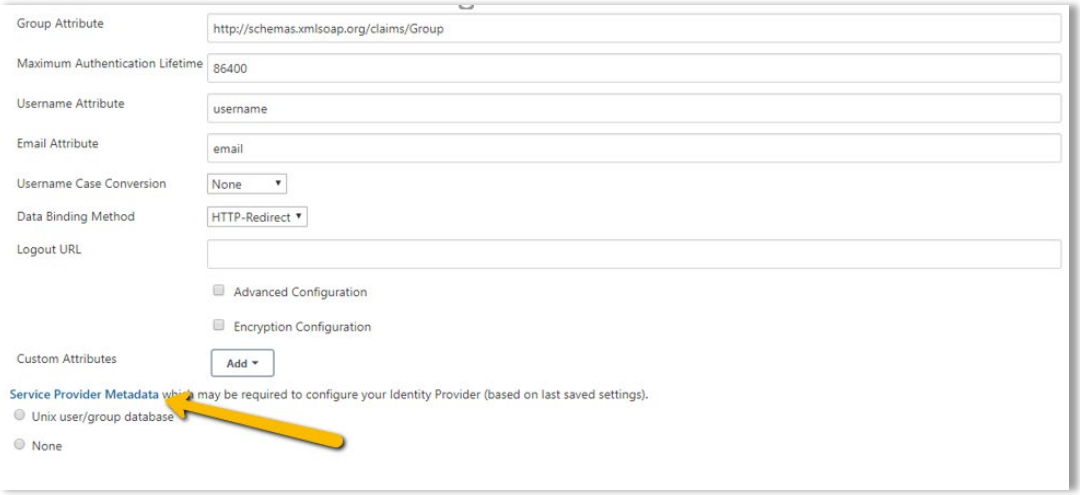


2) In the **Configure Global Security**, select **SAML 2.0** and drop the IdP Metadata file from Keycloak.



Configure Keyclok

1) In **Configure Global Security**, at the bottom of the **Authentication section**, click the **Service Provider Metadata** link to configure Jenkins as a Client on the Keycloak side.



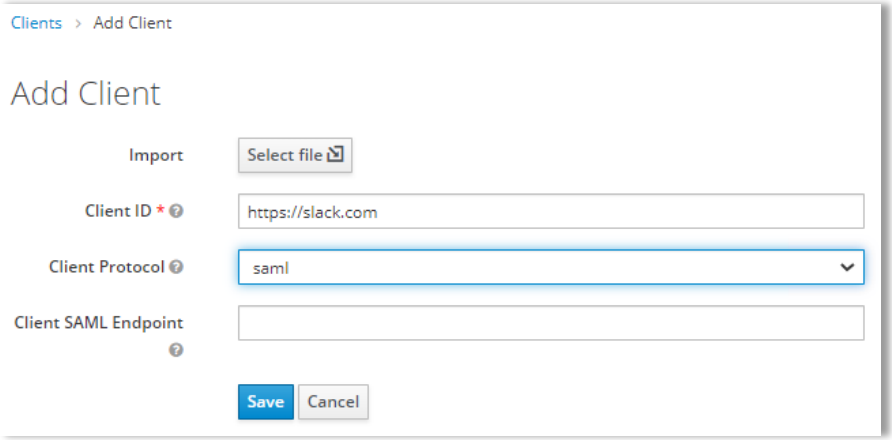
2) Go to the Keycloak admin console and repeat steps 2-5 from Section 9.2.2. **NoPass integration with Confluence**.

NoPass integration with Slack

Set up the Keycloak Client

1) Login to the Keycloak admin console at https://[kcurl]/auth/admin/master/console.
2) In the Keycloak admin console, go to your realm > the **Clients** tab. Click **Create** to add a new client.

3) On the **Add client** tab, do the following:
   - Set the **Client ID** to https://slack.com
   - Set the **Client Protocol** to SAML

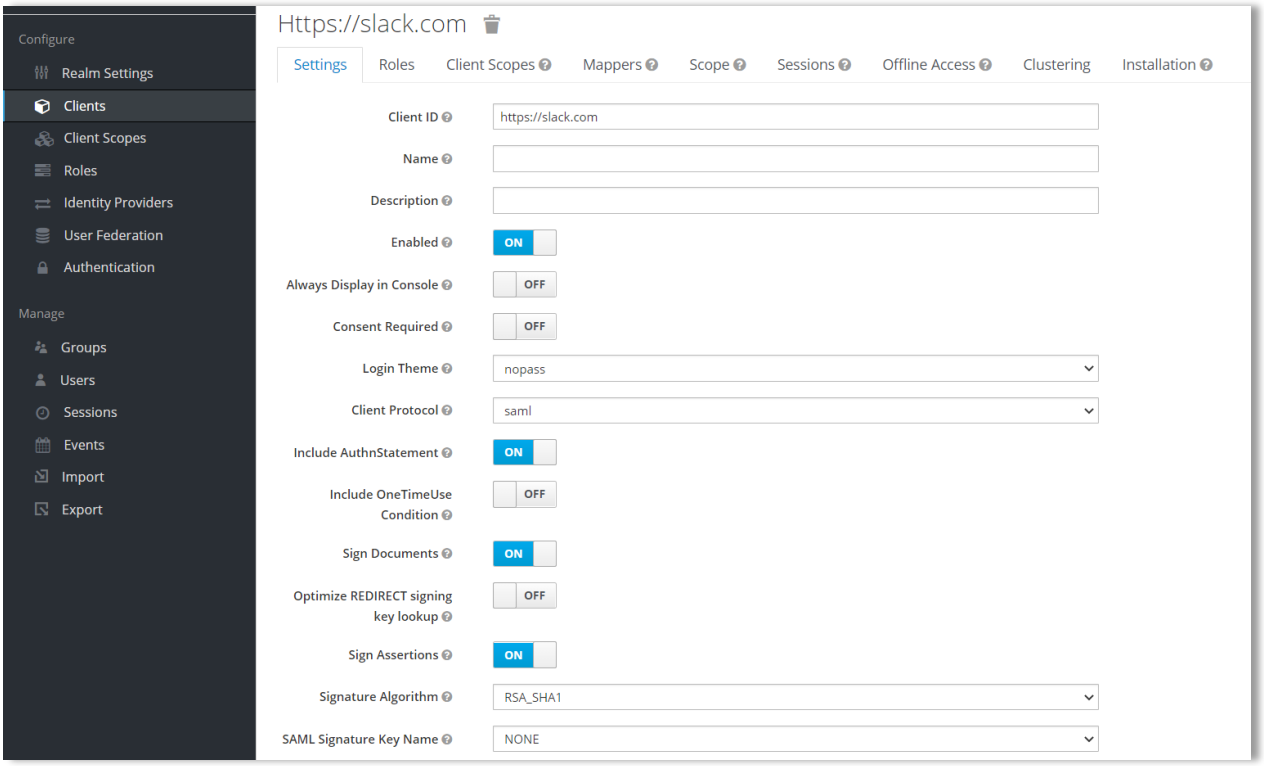


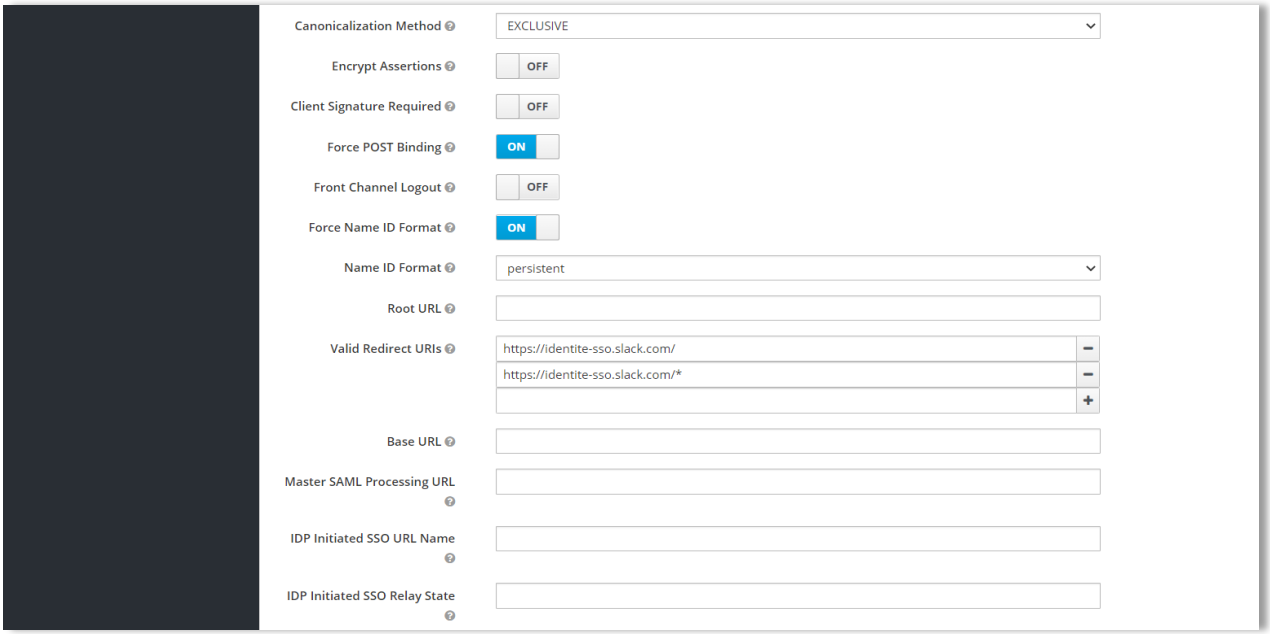
Configure the new client

1) On the **Settings** tab, set the following parameters:

PARAMETER	VALUE
Include AuthnStatement	ON
Sign Documents	ON
Sign Assertions	ON
Signature Algorithm	RSA_SHA1
SAML Signature Key Name	NONE
Force POST Binding	ON

PARAMETER	VALUE
Force Name ID Format	ON
Name ID Format	Persistent
Valid Redirect URIs	○ https://*<your-slack-url>*/ ○ https://[your-slack-url]/*

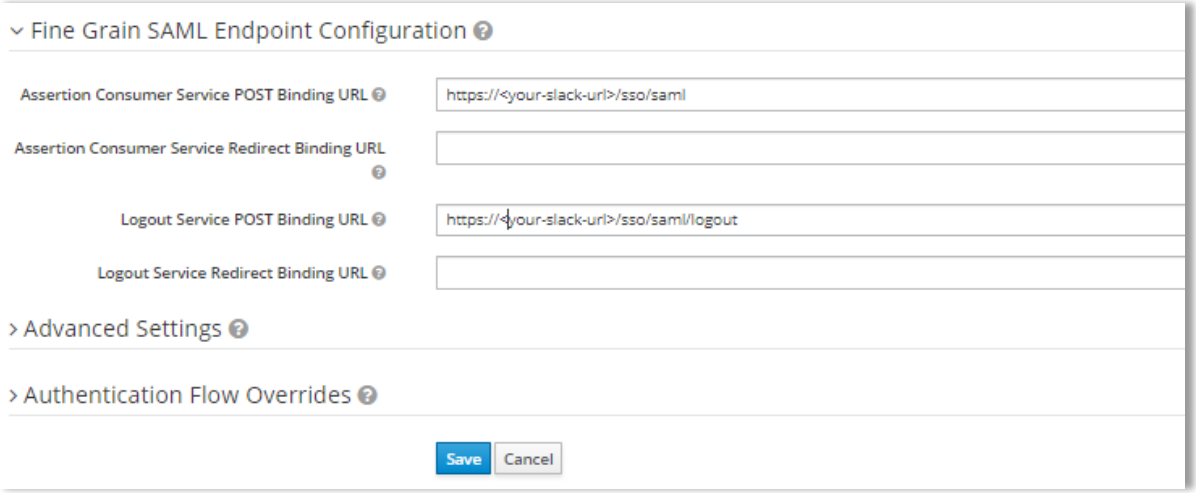




2) At the bottom of the page, in the **Fine Grain SAML Endpoint Configuration**, set the following parameters, and click save:

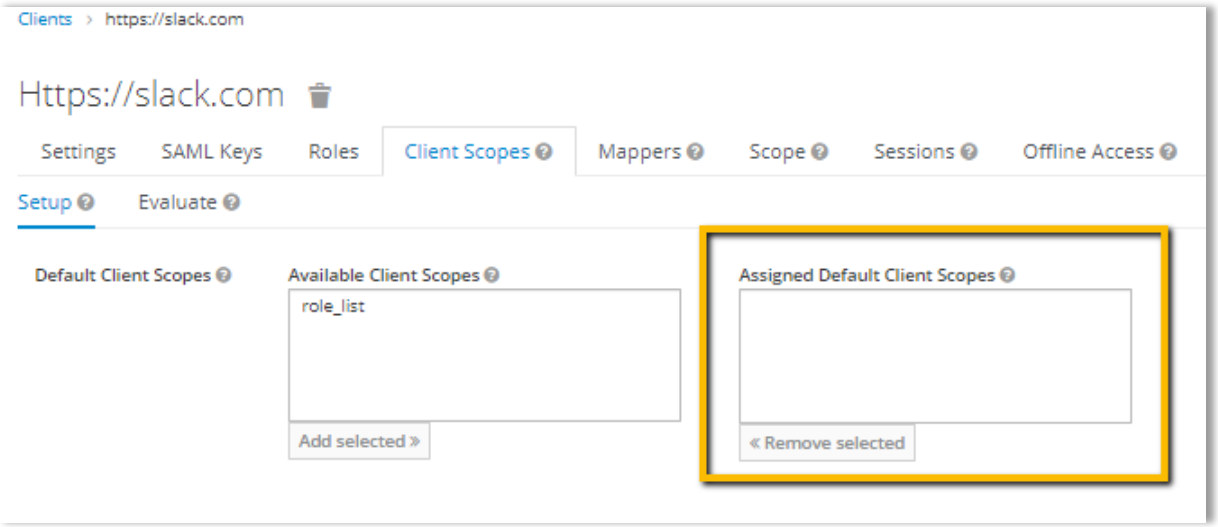
PARAMETER	VALUE
Assertion Consumer Service POST Binding URL	https://<your-slack-url>/sso/saml
Logout Service POST Binding URL	https://<your-slack-url>/sso/saml/logout

Note: The value of *<your-slack-url>* is the actual slack URL for your account, for example *homelogin.slack.com.*



Configure Client Scopes

- On the **Client Scopes** tab, remove any scopes from Assigned Default Client Scopes.



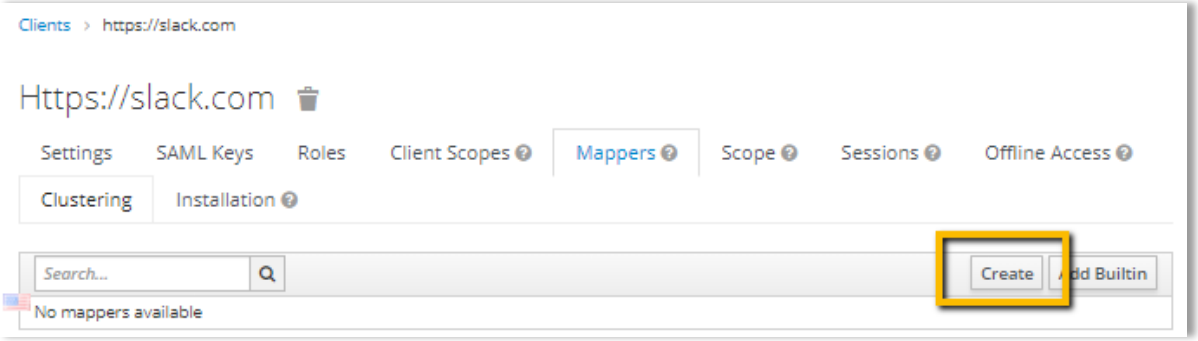
Configure Mappers

Mappers are how Keycloak handles Assertions. We will add and configure 4 mappers as described in the Slack *Custom SAML single sign-on* guide at https://slack.com/intl/en-by/help/articles/205168057-Custom-SAML-single-sign-on.

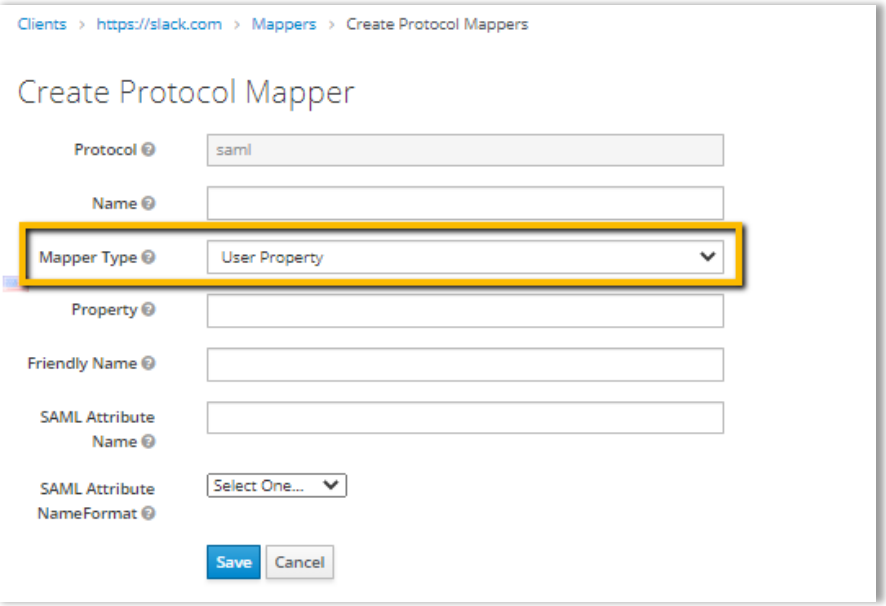
You will need to create the following mappers: email address, first name, last name, username.

Procedure

1) To add a mapper, on the **Mappers** tab, select **Create**.



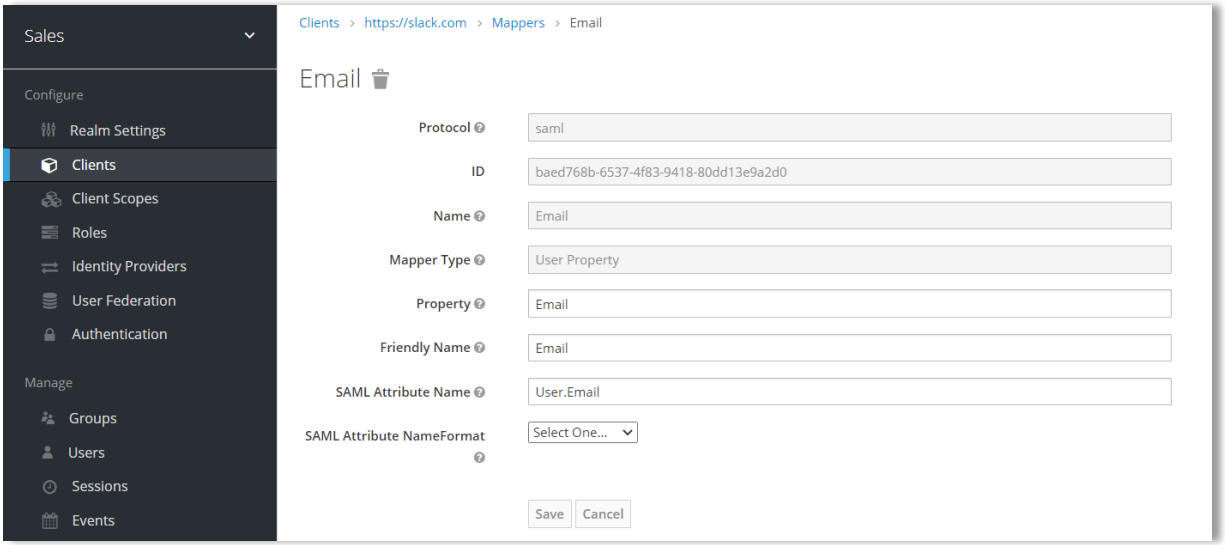
2) On the **Create Protocol Mapper**, from the **Mapper type**, select **User Property** for each mapper.



3) Fill in the following fields for mappers, and then click **Save**:

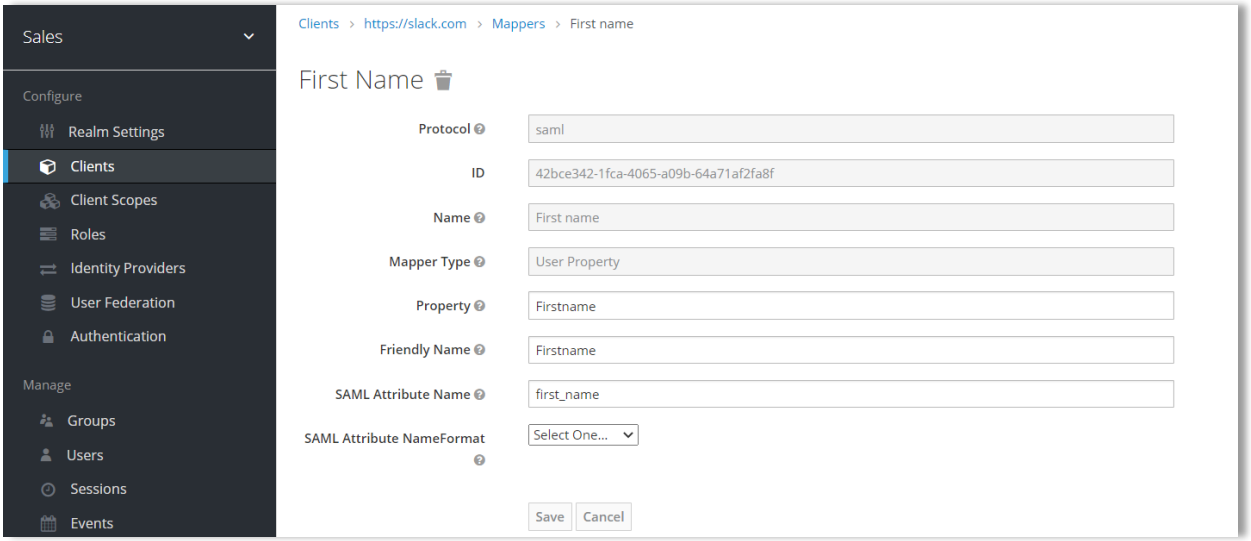
- **Email Address** (required)

PARAMETER	VALUE
Property	**Email**
Friendly Name	**Email**
SAML Attribute Name	*User.Email*



- First Name (Given Name)

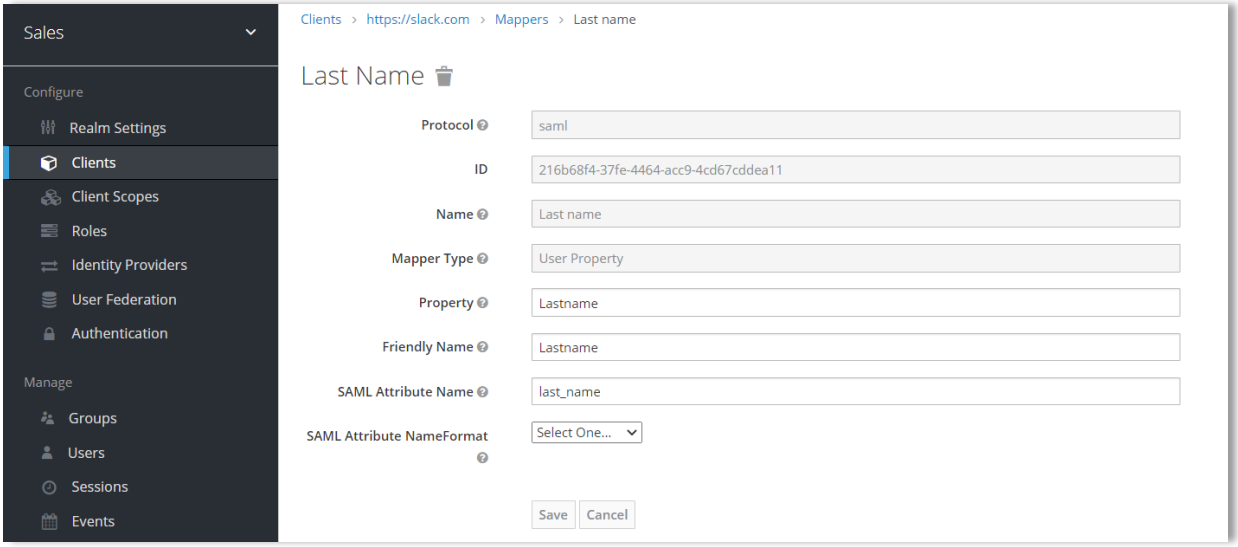
PARAMETER	VALUE
Property	**Firstname**
Friendly Name	**Firstname**
SAML Attribute Name	**First_name**



- Last Name (Surname)

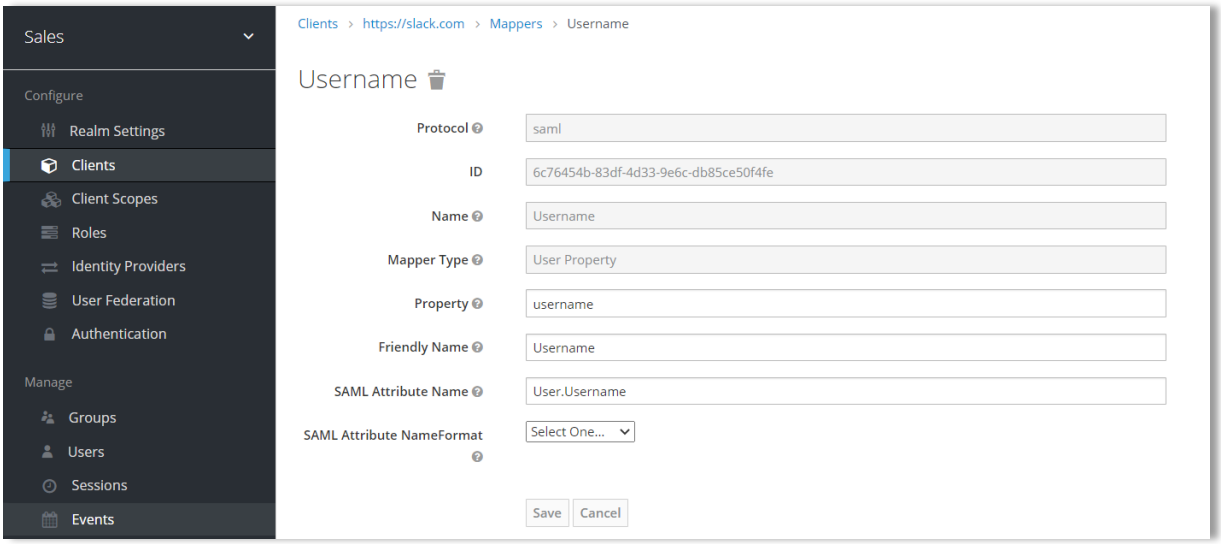
PARAMETER	VALUE
Property	**Lastname**

PARAMETER	VALUE
Friendly Name	**Lastname**
SAML Attribute Name	**last_name**



- Username

PARAMETER	VALUE
Property	**username**
Friendly Name	**Username**
SAML Attribute Name	**User.Username**



In the Slack *Custom SAML single sign-on* guide one more attribute has been mentioned as a required attribute, and that is the Name ID.

NameID (Required)

```
<saml:Subject>
 <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" NameQualifier="YOURDOMAIN.slack.com"
SPNameQualifier="https://slack.com">Your Unique
Identifier</saml:NameID>
</saml:Subject>
```

Note: To meet SAML specifications, the NameID must be unique, pseudo-random, and will not change for the user over time — like an employee ID number.

This attribute does not need to be set and is the same attribute as the Keycloak User ID that Keycloak has assigned to each user and will include it in the SAML token.

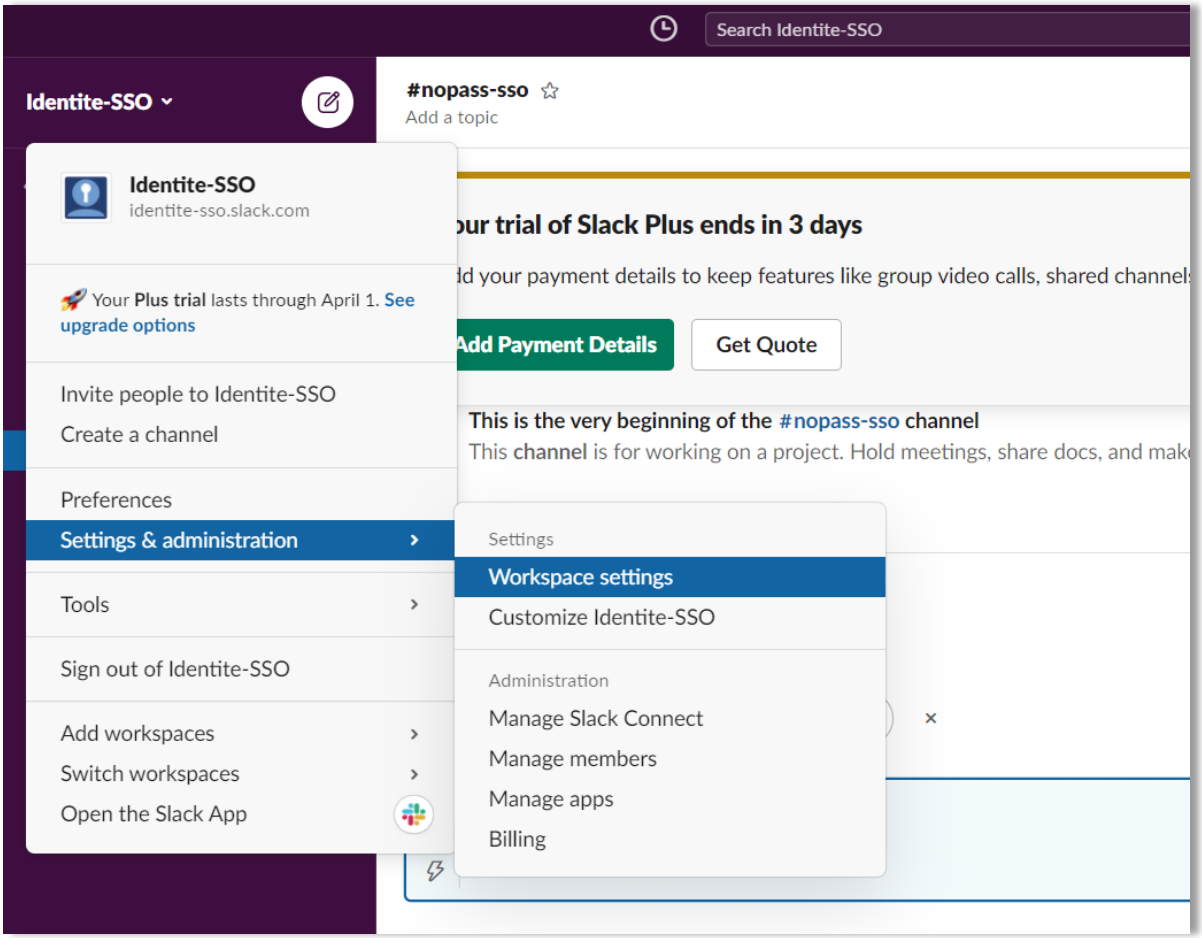
Download Keycloak Metadata

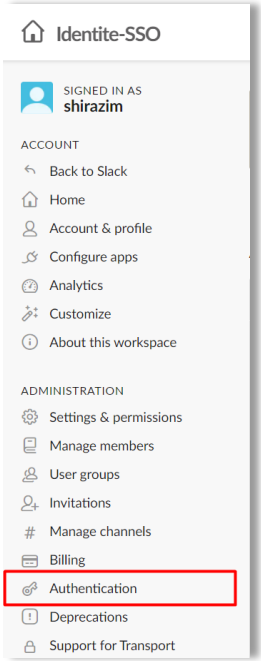
- In **Realm Settings**, on the **General** tab, select SAML 2.0 Identity Provider Metadata to download the SAML Metadata.

Note: Your URL should look similar to: https://*<keycloak-location>*/auth/realms/*<realm>*/protocol/saml/descriptor.

Configure Slack

1) Sign in to your Slack account as an admin.
2) Go to **Settings & administration > Workplace settings > Authentication > SAML SSO configurations**


Search Identite-SSO
Identite-SSO
#nopass-sso
Add a topic
Identite-SSO
identite-sso.slack.com
Your Plus trial lasts through April 1. See upgrade options
Invite people to Identite-SSO
Create a channel
Preferences
Settings & administration
Tools
Sign out of Identite-SSO
Add workspaces
Switch workspaces
Open the Slack App
ur trial of Slack Plus ends in 3 days
d your payment details to keep features like group video calls, shared channel
Add Payment Details
Get Quote
This is the very beginning of the #nopass-sso channel
This channel is for working on a project. Hold meetings, share docs, and mak
Settings
Workspace settings
Customize Identite-SSO
Administration
Manage Slack Connect
Manage members
Manage apps
Billing

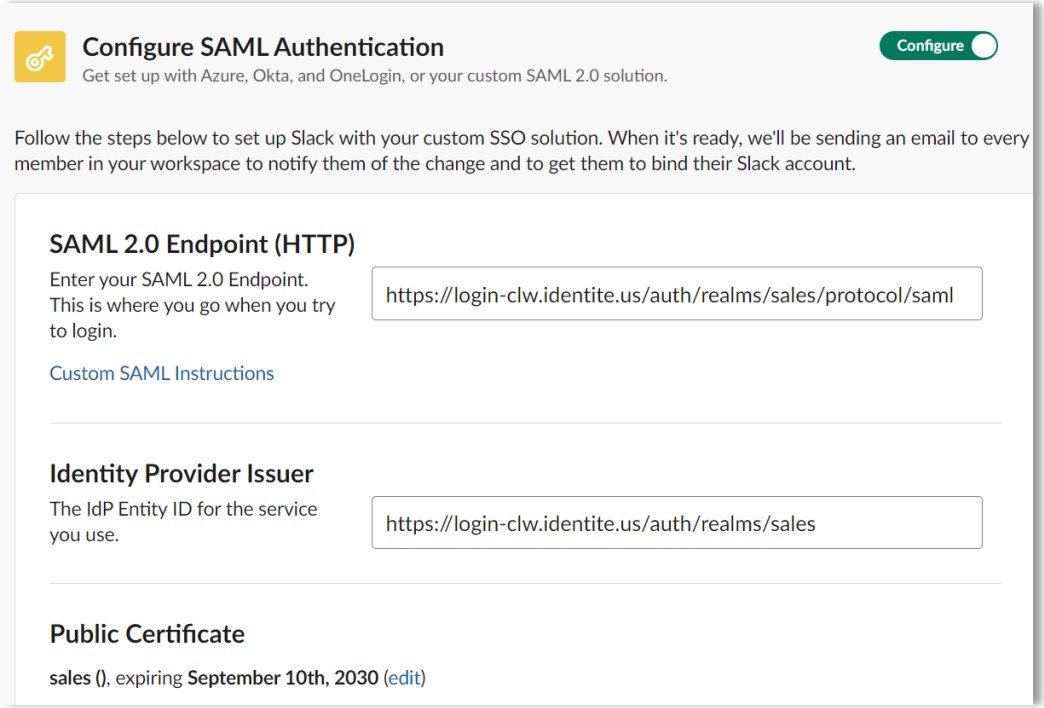

Identite-SSO
SIGNED IN AS
shirazim
ACCOUNT
Back to Slack
Home
Account & profile
Configure apps
Analytics
Customize
About this workspace
ADMINISTRATION
Settings & permissions
Manage members
User groups
Invitations
Manage channels
Billing
Authentication
Deprecations
Support for Transport

3) On the **Configure SAML Authentication** page, do the following:

- Set **SAML 2.0 Endpoint (HTTP)** to https://*<kc-base-url>*/auth/realms/*<realm-name>*/protol/saml. You can find this in the **Location** field of the **SingleSignOnService** property in the metadata.

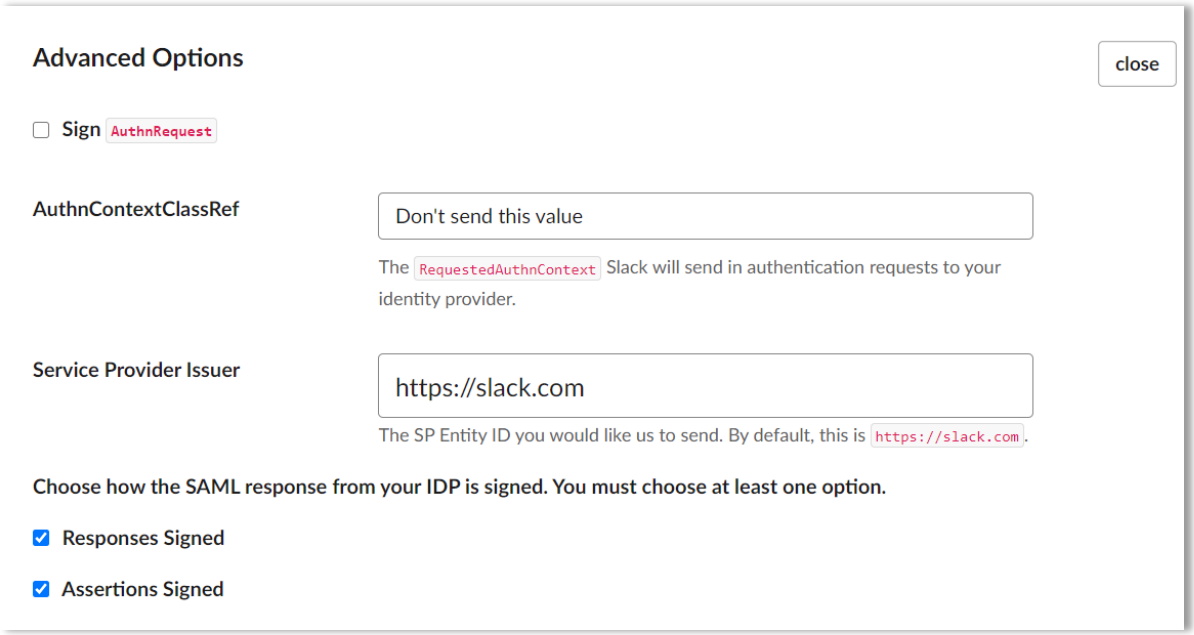
- Set **Identity Provider Issuer** to https://*<kc-base-url>*/auth/realms/*<realm-name>*. You can find this in the **entityID** field of the **EntityDescriptor** property.

- In the metadata, set **Public Certificate** to the **X509Certificate**. You do not need any extra marking, just that straight value.

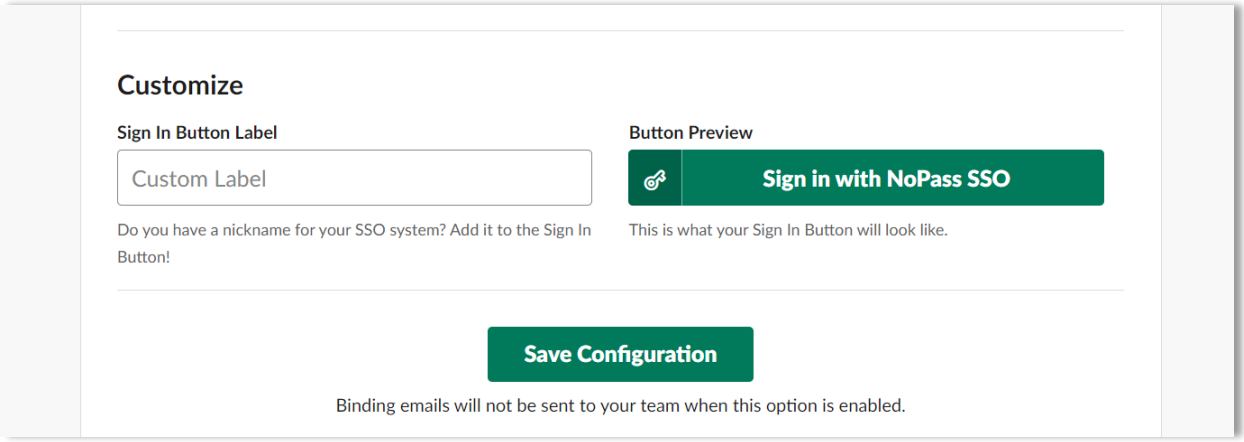


4) Under **Advanced Options**, do the following:

- Set **AuthnContextClassRef** to **Don't send this value**
- Set **Service Provider Issuer** to https://slack.com
- Select **Responses Signed**
- Select **Assertions Signed**



5) *Optional.* Customize your **Sign In Button Label**.

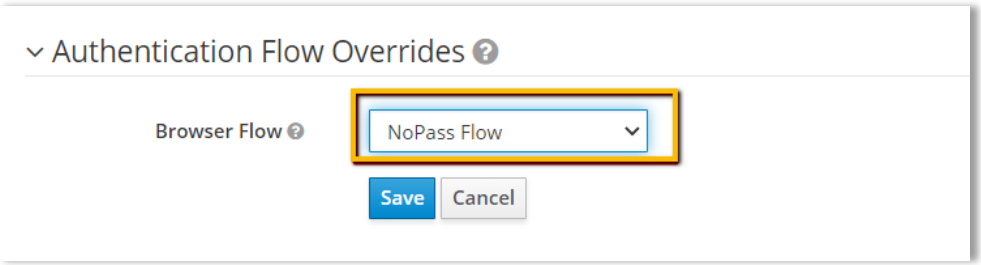


6) Click **Save Configuration**. If you are not already signed in with Keycloak, Slack will do that now to test the integration.

Enable NoPass Passwordless Authentication for Slack SSO

After Slack has tested the integration and the SSO is working, sign in to your Keycloak admin console.

On the Slack **Client Settings** tab, under **Authentication Flow Overrides**, from the Browser Flow list, select **NoPass Flow**.



APPENDIX 1. NOPASS SERVER ENVIRONMENT VARIABLES

The application will not start without the required variables. The variables with mask **EmailSettings** are 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__Server **MAPD_DatabaseSettings__Port** **MAPD_DatabaseSettings__DatabaseName** **MAPD_DatabaseSettings__UserId** **MAPD_DatabaseSettings__Password**	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

Install the NoPass application server

APPENDIX 2. CONFIGURE THE REVERSE PROXY

The 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.

```
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             ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES256-
SHA384;
    ssl_protocols       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 1.1.1.1 1.0.0.1 8.8.8.8 8.8.4.4 208.67.222.222 208.67.220.220 valid=60s;
    resolver_timeout 2s;
    add_header        Strict-Transport-Security: "max-age=31536000; includeSubDomains" always;
    add_header          X-Content-Type-OptZQvi ions 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         "default-src 'self' http: https: data: blob: 'unsafe-inline'" always;}
```

Related topics

Create DNS records
Stop the NoPass application server