


# BASIC Authentication

This policy enables HTTP BASIC Authentication on an API. You can use this policy to require clients to provide HTTP BASIC authentication credentials when making requests to the managed API.



Do **not** use the **BASIC Authentication** policy together with the other authentication policies [Keycloak OAuth](#) and [JWT](#). The chaining of these policies is currently not supported, but this may change in future versions.

Policy Type

BASIC Authentication Policy

BASIC Authentication Policy Configuration

Authentication Realm

Realm...

Require Transport Security

ⓘ

If this option is enabled, then requests will fail unless they come in to the API gateway via SSL (https). The API gateway must accept inbound SSL connections for this to work.

☐ Transport Security Required

Forward Authenticated Username as HTTP Header

HTTP header or leave blank to disable...

Require Basic Authentication

ⓘ

For example, you might disable this option if you want to support both BASIC auth and OAuth policies.

☐ Basic Auth Required

Identity Source

Choose an Identity Source...

Add Policy Cancel



## On this Page:

- [Configuration Options](#)
  - [Identity Source Configuration Options](#)



## Related Pages:

- [Policies](#)
  - [Assigning Policies](#)
  - [Policy Configuration](#)

## Configuration Options

Option	Type	Description	Possible Values	Default
Authentication Realm	String	Defines the BASIC Auth realm that will be used when responding with an auth challenge (when authentication is missing or fails).	-	-
Transport security required	Boolean	Enabling this will require clients to use <b>https</b> . <div><p>Please disable the TLS check if you are using Scheer PAS 21.1 or a newer version, because all PAS components are running behind a proxy server.</p></div>	true / false	false
Forward Authenticated Username as HTTP Header	String	Indicates the name of an HTTP header to send with the principal/identity of the authenticated user if authentication succeeds. Useful when the backend API needs to know the identity of the authenticated user.	-	-
Basic Auth required	Boolean	Must be set to <b>true</b> so that BASIC authentication credentials are <b>required</b> . <div><p>Make sure that this option is true if you want to use this policy for authentication.</p></div>	true / false	true
Identity Source	Object	Additionally, one of the complex properties must be included in the configuration, indicating whether API Management should use JDBC, LDAP or Static information as the source of identity used to validate provided user credentials.  Configuration details of the identity source are listed <a href="#">in the table below</a> .	Static JDBC LDAP	-


### Identity Source Configuration Options

Identity Source	Content	Type	Description	Possible Values	Default
Static		Object	Allows you to provide a static set of user names and passwords.	-	-
	Static Identities	Object	Contains a set of user names and passwords. <div> Not recommended for production.</div>	-	-
<div>  <b>Supported Databases</b>  Only PostgreSQL, MariaDB and MySQL are supported. </div>		Object	This object is included when you wish to use JDBC to connect to a database containing user and password information.	-	-
	JDBC Type	Enum	Type of JDBC connection to use. Configuration details of <a href="#">Data Source</a> and <a href="#">URL</a> see below.	Data Source URL	Data Source
	Also extract user roles from the DB	Boolean	Set to true if you also want to extract role information from the database.	true / false	false
	Roles SQL Query	String	<b>If Also extract user roles from the DB is true:</b> SQL query to use when extracting role information. The first parameter passed to the query will be the username.	-	-

#### JDBC MariaDB Example - do not use unadapted!


```
# example db
CREATE DATABASE testusers DEFAULT CHARACTER SET = 'utf8mb4';
# example table
CREATE TABLE users(id int NOT NULL PRIMARY KEY AUTO_INCREMENT COMMENT 'Primary Key',create_time DATETIME COMMENT 'Create Time',password CHAR(40) NOT NULL,name VARCHAR(255) NOT NULL) COMMENT '';
# example insert statement
INSERT INTO users(password,name,create_time) VALUES(SHA1('secret'),'test.user','2023-07-05 00:00:00');
```

#### When "JDBC Type" is Data Source

<div> <b>Data Source</b> is not available in a PAS environment.</div>	JDBC DataSource	String	The JNDI path of the datasource to use (only when type is Data Source).	-	-
--	-----------------	--------	---	---	---

#### When "JDBC Type" is URL

	JDBC URL	String	The URL to the JDBC database.	-	-
	JDBC Username	String	The username to use when connecting to the JDBC database.	-	-
	JDBC Password	String	The password to use when connecting to the JDBC database.	-	-
	JDBC Password (verify)	String	Password repetition to verify the password.	-	-

	SQL Query	String	The SQL query to use when searching for a user record. The first parameter passed to the query will be the username, the second parameter will be the (optionally hashed) password.	-	-
	Password Hash Algorithm	Enum	The hashing algorithm used when storing the password data in the database.	None SHA1 MD5 SHA256 SHA384 SHA512	SHA1
LDAP Deprecated since PAS 23.1.1		Object	This object is included when you wish to connect to LDAP when validating user credentials.	-	-
 For usage of LDAP, please use the <a href="#">Keycloak OAuth Policy</a> . Verify with the Scheer PAS support, that your LDAP server is configured as user federation inside Keycloak.	LDAP Server URL	String	The URL to the LDAP server.	-	-
	LDAP Bind DN	String	The pattern to use when binding to the LDAP server (use of \${username} is possible).	-	-
	Bind to LDAP As	Enum	Choose whether to bind directly to LDAP as the authenticating user (UserAccount), or instead to bind as a service account and then search LDAP for the user's record (ServiceAccount). Configuration details for <a href="#">Service Account</a> see below.	The inbound user A Service account	The inbound user
	Also extract user roles from the directory	Boolean	Set to true if you want to extract role information from LDAP.	true / false	false
	Group Membership Attribute	String	If <b>Also extract user roles from the directory</b> is <b>true</b> : The attribute representing the user's membership in a group. Each value should be a reference to another LDAP node.	-	-
	Role Name Attribute	String	If <b>Also extract user roles from the directory</b> is <b>true</b> : The attribute on a role LDAP node that represents the name of the role.	-	-
Only when "Bind to LDAP" is Service Account					
	Service Account Username / Service Account Password	Object	The credentials are saved as an object with two properties: <b>username</b> and <b>password</b> . The credentials are used when initially binding to LDAP as a service account.	-	-
	User Search Base DN / User Search Expression	Object	An object with two properties: <b>baseDn</b> and <b>expression</b> . Used to search for the user's LDAP record so that it can be used to re-bind to LDAP with the appropriate password.	-	-