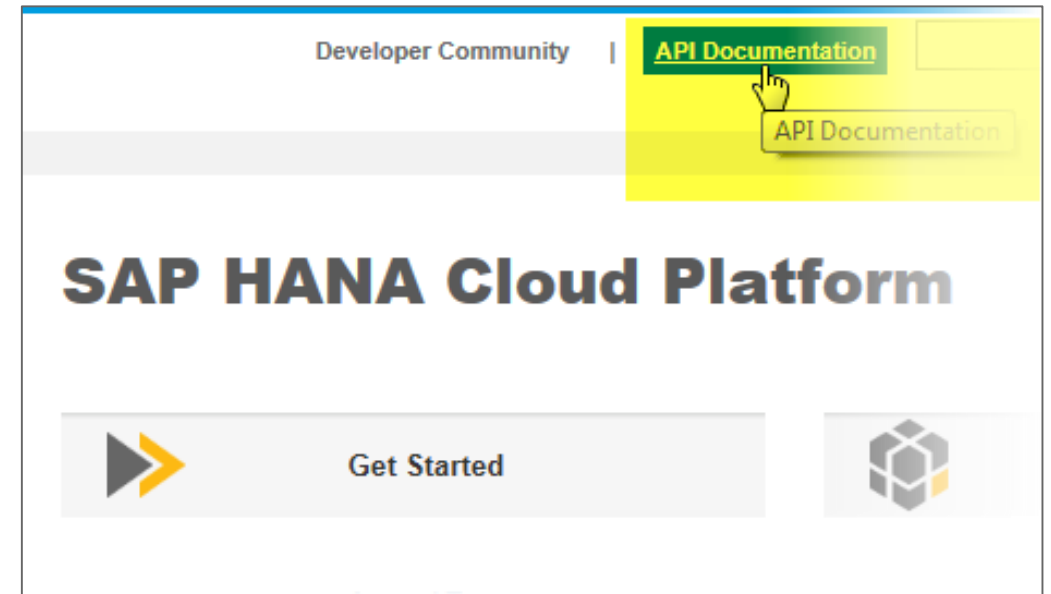


# Week 3 Unit 3: Working with the Authorization Management Platform API

# Working with the Authorization Management Platform API

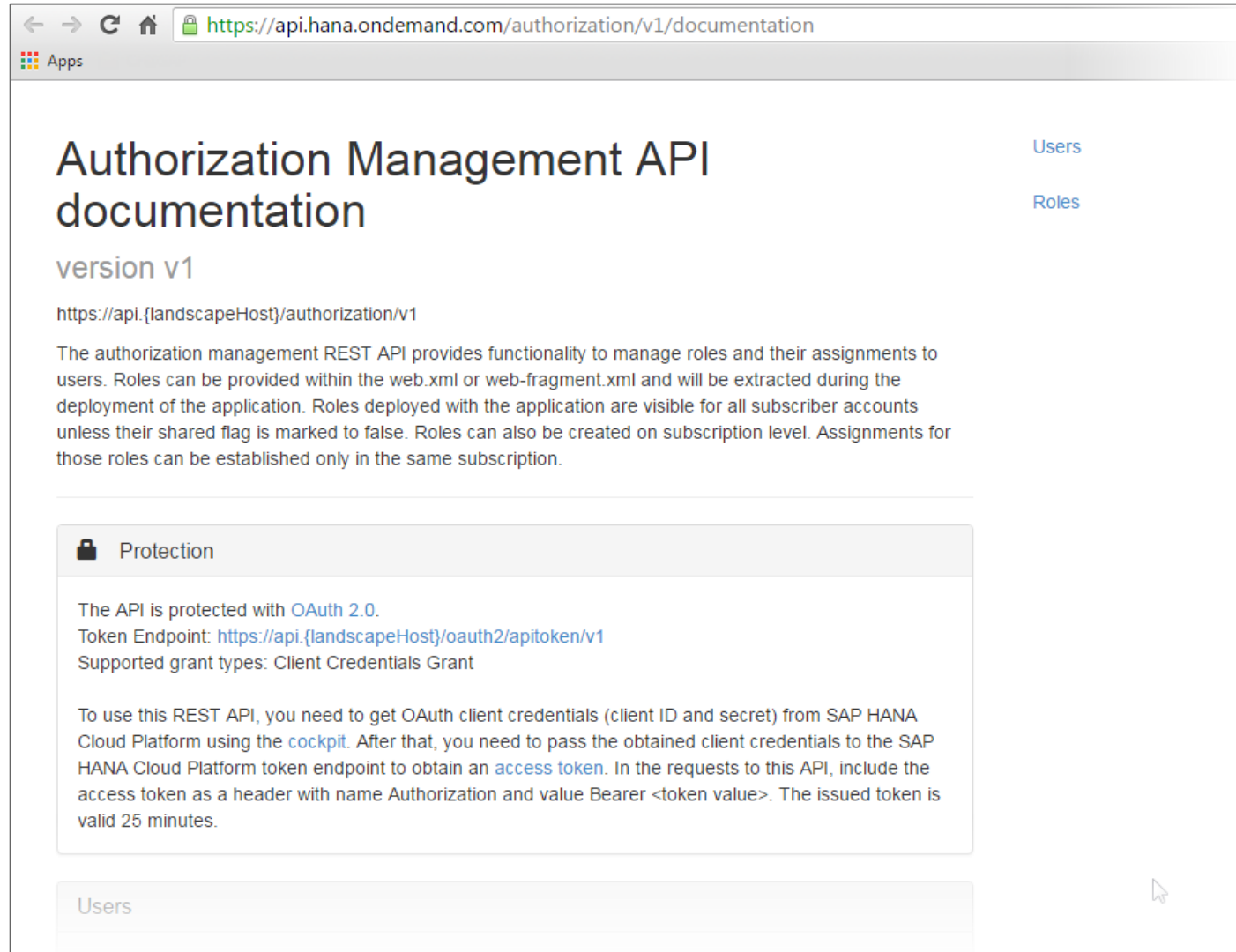
## Platform APIs – Why and what for?

- **RESTful HCP platform APIs** (will) provide programmatic access to much of the functionality available through the SAP HANA Cloud Platform Cockpit or Console Client.
- **Functionality covered by RESTful platform APIs as of today:**
  - Java Application Lifecycle Management
  - Java Application Monitoring
  - Java/HTML5 Application Authorization Management
- **Key scenarios for platform APIs:**
  - SaaS solutions with own administration user interfaces
  - Automation processes (e.g. new customer onboarding for an HCP-based solution)



# Working with the Authorization Management Platform API

## Authorization Management API



The screenshot shows a web browser window with the URL <https://api.hana.ondemand.com/authorization/v1/documentation>. The page title is "Authorization Management API documentation" with a subtitle "version v1". On the right side, there are two links: "Users" and "Roles". The main content area describes the REST API for managing roles and their assignments to users. It includes a "Protection" section with a lock icon, stating that the API is protected with OAuth 2.0 and provides the token endpoint and supported grant types. Below this, there is a detailed instruction on how to use the REST API, including obtaining OAuth client credentials from SAP HANA Cloud Platform and passing them to the token endpoint to obtain an access token. The page also features a "Users" section at the bottom.

← → ↻ 🏠 <https://api.hana.ondemand.com/authorization/v1/documentation>

Apps

## Authorization Management API documentation

version v1

[Users](#)

[Roles](#)

<https://api.{landscapeHost}/authorization/v1>

The authorization management REST API provides functionality to manage roles and their assignments to users. Roles can be provided within the web.xml or web-fragment.xml and will be extracted during the deployment of the application. Roles deployed with the application are visible for all subscriber accounts unless their shared flag is marked to false. Roles can also be created on subscription level. Assignments for those roles can be established only in the same subscription.

### Protection

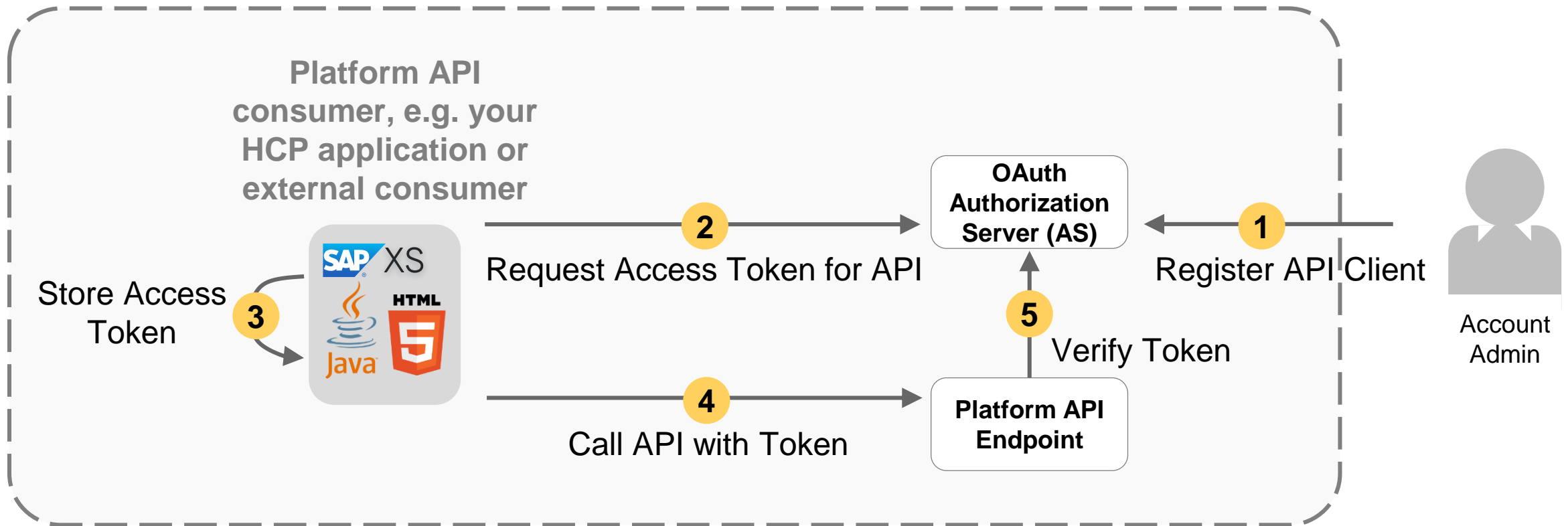
The API is protected with [OAuth 2.0](#).  
Token Endpoint: <https://api.{landscapeHost}/oauth2/apitoken/v1>  
Supported grant types: Client Credentials Grant

To use this REST API, you need to get OAuth client credentials (client ID and secret) from SAP HANA Cloud Platform using the [cockpit](#). After that, you need to pass the obtained client credentials to the SAP HANA Cloud Platform token endpoint to obtain an [access token](#). In the requests to this API, include the access token as a header with name Authorization and value Bearer <token value>. The issued token is valid 25 minutes.

### Users

# Working with the Authorization Management Platform API

## Setup process to consume a platform API





# Working with the Authorization Management Platform API

## What you've learned in this unit

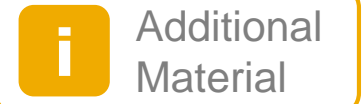
---

- Platform APIs provide programmatic access to core platform functions, such as user-to-role assignments using the Authorization Management API.
- Platform APIs enable services and (SaaS) applications to integrate deeply with the platform.
- The platform API consumer needs to obtain a valid OAuth access token from HCP to call the API.

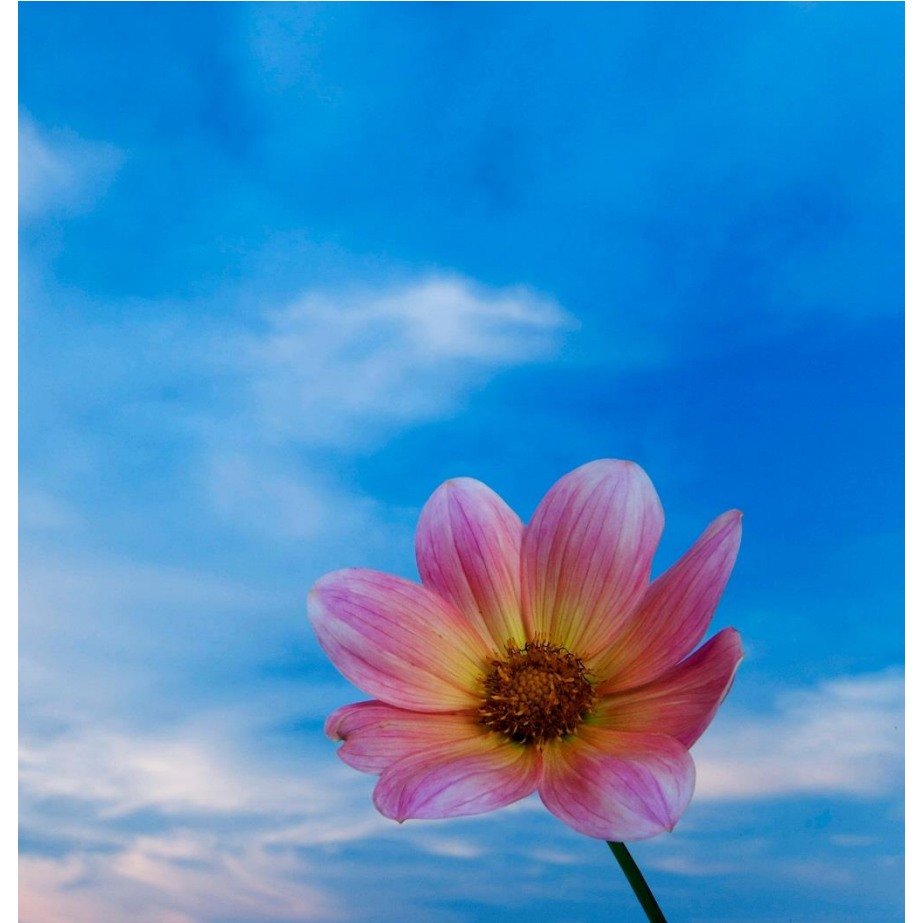


# Working with the Authorization Management Platform API

## Further Reading



- Authorization Management API Documentation:  
<https://api.hana.ondemand.com/authorization/v1/documentation>





# Thank you

Contact information:

[open@sap.com](mailto:open@sap.com)

open**SAP**

# © 2016 SAP SE or an SAP affiliate company. All rights reserved.

---

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.