

SAP PartnerEdge

Multiple SAP Cloud ALM Tenants for Managed Service Providers

PUBLIC

March 2025



Disclaimer

The information in this presentation is solely for use of partners under the 'Managed Service Partner' (MSP) model. Unless otherwise stated, partner herein refers to the Managed Service Partner model (also as previously referred to a 'Partner Managed Cloud' (PMC) or 'Business Process Outsourcing' (BPO)).

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

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.

Content

- Context
- Multiple tenants and customer landscape
- SAP Cloud ALM tenants in the Managed Service Provider (MSP) context
- SAP Cloud ALM for implementation scenarios in the MSP context
- SAP Cloud ALM for operations scenarios in the MSP context



Context

PUBLIC



Managed Service Provider (MSP) Context (previously referred to as 'Partner Managed Cloud' or 'PMC')

Premises

A partner purchases solutions from SAP and provides them to their end customers.

The partner has subscribed to SAP cloud services.

All systems are attached to the partner customer number.

The partner receives SAP Enterprise Support, cloud editions as part of the cloud services.

The partner end-customer has:

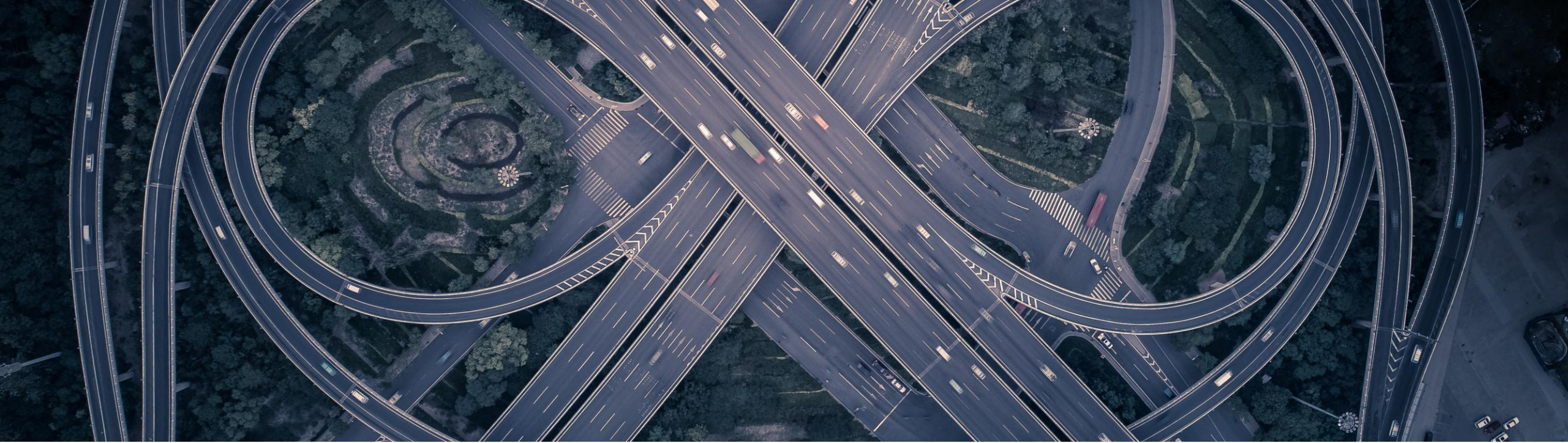
- No support entitlement from SAP
- No entitlement to SAP Cloud ALM

The partner has an entitlement for one SAP Cloud ALM tenant as part of the support across all subscribed cloud services.

The MSP may subscribe the SAP Cloud ALM, tenant extension (subject to additional fees) if further tenants are required.

Scenario for this presentation:

The MSP wants to provide access to SAP Cloud ALM to their end customers.



Multiple SAP Cloud ALM Tenants and System Landscape

PUBLIC

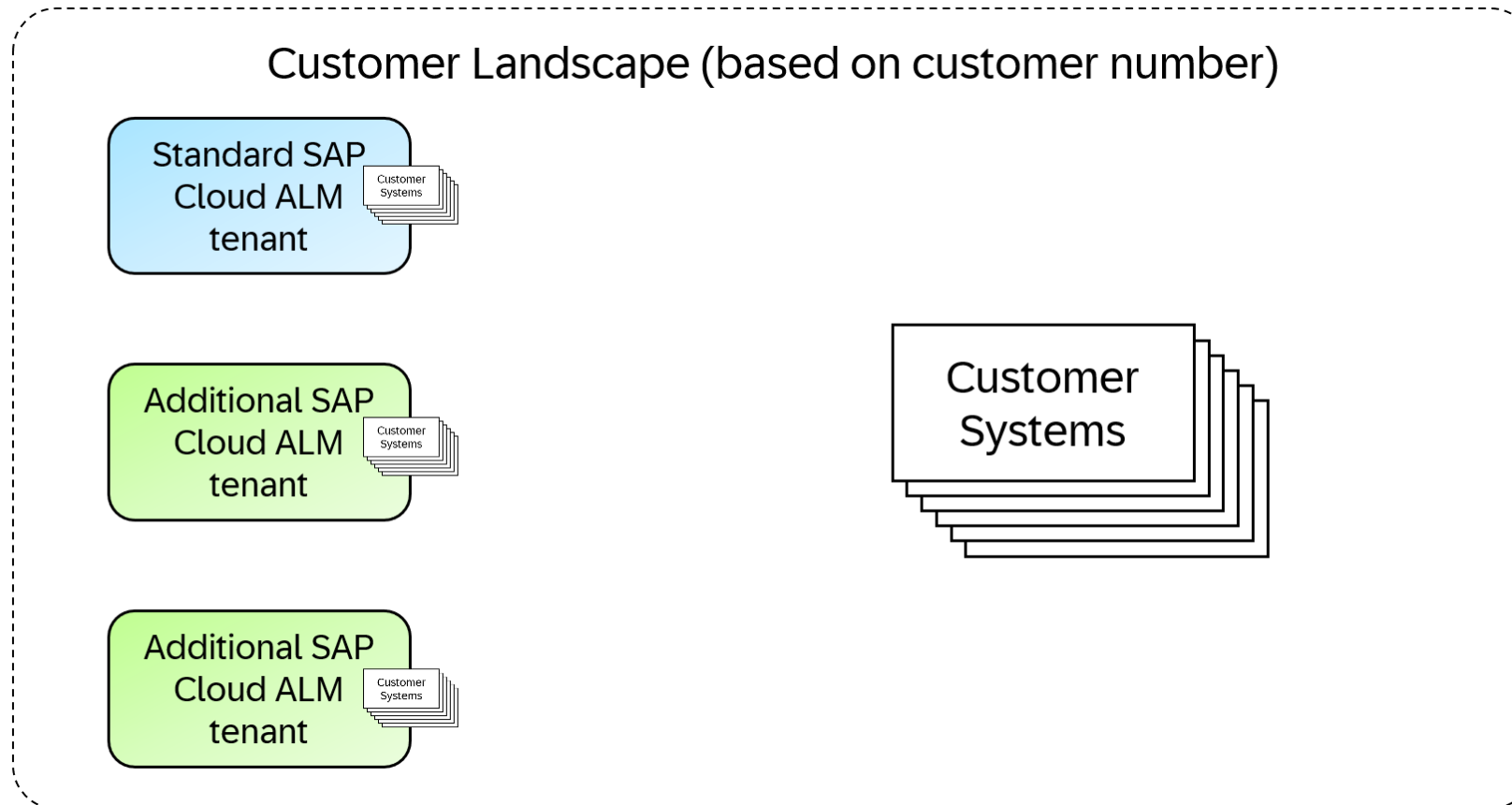


Multiple Tenants and Customer Landscape Visibility

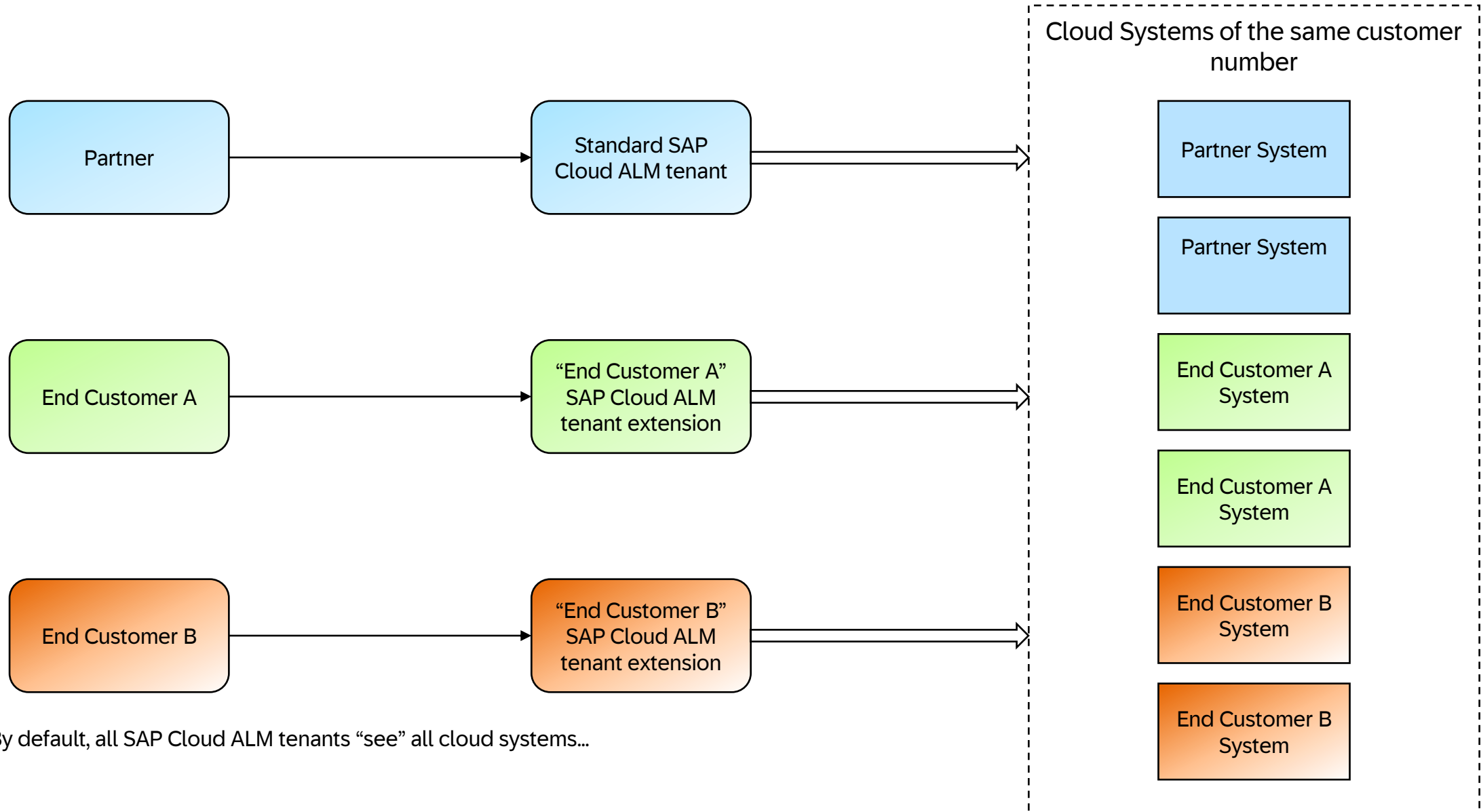
SAP Cloud ALM Landscape Management relies on the customer number assigned to SAP Cloud ALM.

Landscape Management imports all cloud services assigned to the customer number.

It happens for all SAP Cloud ALM tenants belonging to the same customer number.



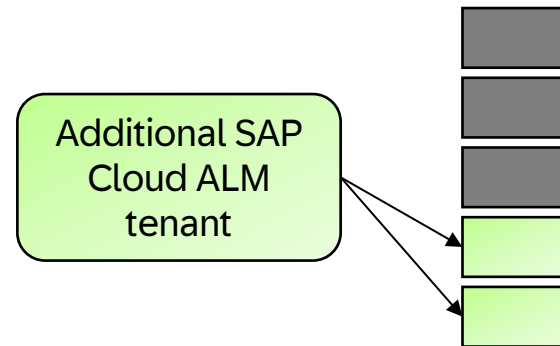
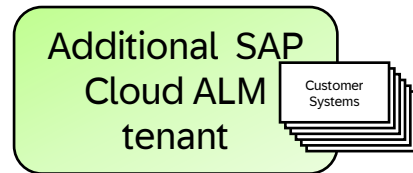
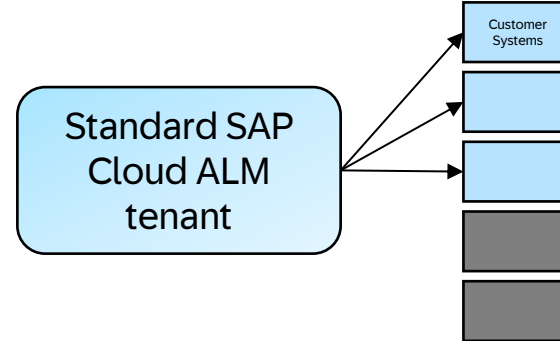
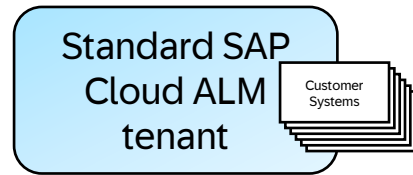
Multiple Tenants and MSP Landscape Visibility Challenge

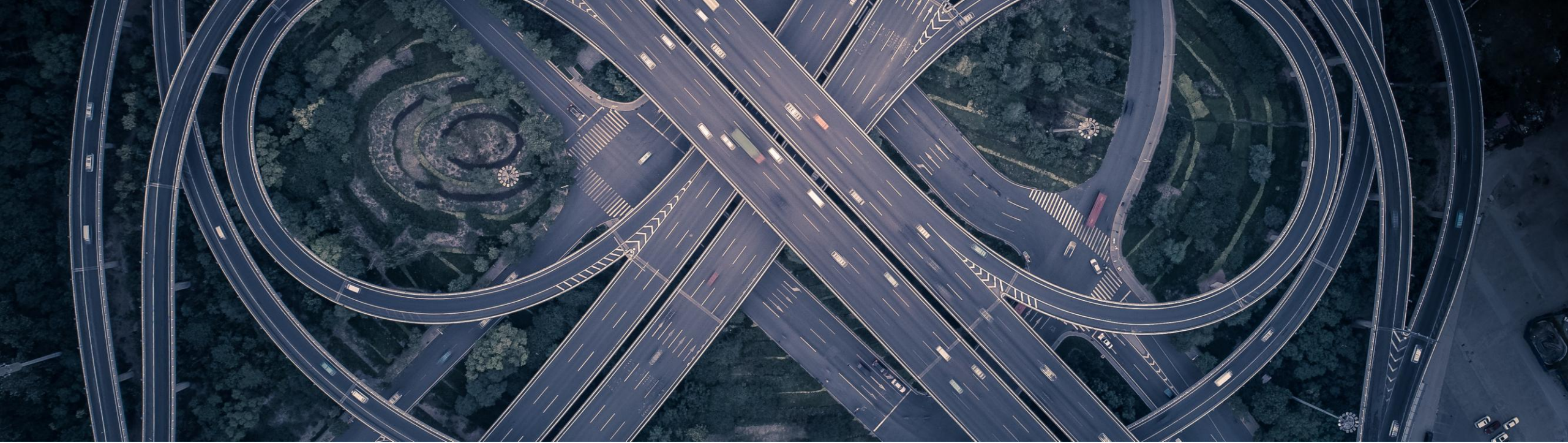


Multiple Tenants and Customer Landscape Visibility

All customer cloud services will be visible in all customer SAP Cloud ALM tenants.

Access Control in Landscape Management can be used to restrict the visibility of cloud services (details [here](#)).





Multiple Tenants in the MSP-Specific Context

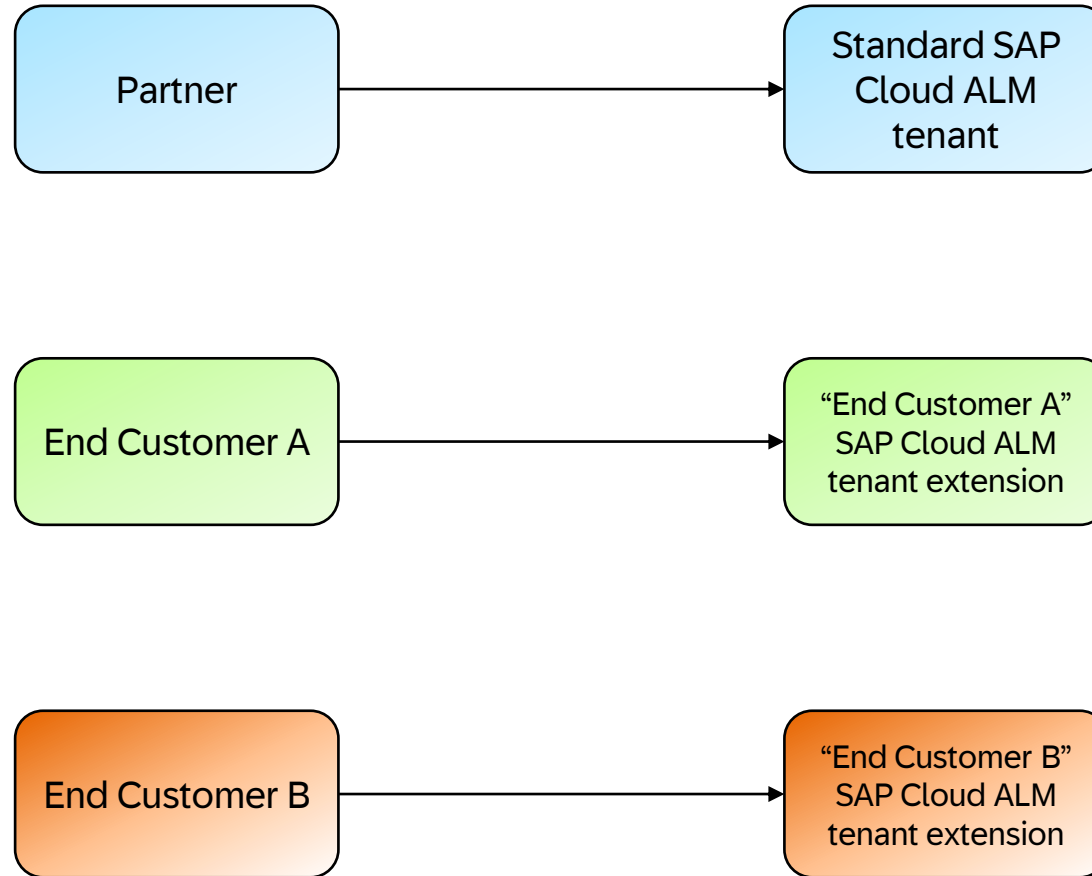
PUBLIC



Multiple Tenants for MSP Partners and Their End Customers

- The standard SAP Cloud ALM tenant (the one granted as part of SAP Enterprise Support) should be used by the **MSP ONLY**.
- The following applies if the MSP wants to provide access to SAP Cloud ALM to the end customer.
- The MSP must provision a separate tenant (SAP Cloud ALM, tenant extension) **for EACH end customer**.
- **SAP strictly advises against the usage of one SAP Cloud ALM tenant for multiple different end customers. Not following this guidance is at MSPs sole responsibility and risk.**
- **The next slides represent SAP's recommendations and limitations based on the currently available functionalities.**

MSP Landscape Recommendation for their End Customers



Overview of Scenarios Usable by End Customers in the MSP Context

Domain	Scenario	Usable by end customer?	Comment
Operations	Landscape Management	Yes	ACLs must be defined
Operations	Health Monitoring	Yes	ACLs must be defined
Operations	Real User Monitoring	Yes	ACLs must be defined
Operations	Business Process Monitoring	Yes	ACLs must be defined
Operations	Job Monitoring	Yes	ACLs must be defined
Operations	Configuration & Security Analysis	Yes	ACLs must be defined
Operations	Alert Management	Yes	ACLs must be defined
Operations	All remaining scenarios	No	ACLs are not supported, and even in display mode all landscape objects will be visible.*
Implementation	Change and Deployment Mgt.	Yes	With the correct configuration (detailed later)
Implementation	Project Management	Yes	Currently a restriction on System groups
Implementation	All other scenarios	Yes	
Services	Not relevant in the MSP scope	No	
SAP Business Transformation Center	Out of scope of this document	No	

SAP Cloud ALM Role Dispatching – Implementation Roles

Domain	Role	<u>Can be granted to end customer?</u>	Comment
Imp/Change & Deployment Mgt	Change Manager	Yes	
Imp/Change & Deployment Mgt	Deployment Manager	Yes	
Imp/Cloud Integration Automation Service	Cloud Integration Administrator	No	
Imp/Cloud Integration Automation Service	Cloud Integration Expert	Yes	
Imp/Cloud Integration Automation Service	Cloud Integration Viewer	Yes	
Imp/Cloud Transport Mgt	Transport Management Viewer	Yes	
Imp/Process Mgt	All roles	Yes	
Imp/Project Mgt	Project Administrator	No	Can view and manipulate system groups
Imp/Project Mgt	Project Lead	No	Same as above
Imp/Project Mgt	Project Member	Yes	
Imp/Project Mgt	Project Viewer	Yes	
Imp/SAP Readiness Check	Readiness Check Analysis Administrator	No	
Imp/SAP Readiness Check	Readiness Check Analysis Viewer	Yes	

SAP Cloud ALM Role Dispatching – Operations Roles

Domain	Role	<u>Can be granted to end customer?</u>	Comment
Business Process Monitoring	Process Monitoring Administrator	No	
Business Process Monitoring	Process Monitoring Consumer	Yes	
Business Process Monitoring	Process Executor	Yes	
Business Process Monitoring	Process Manager	No	
Business Process Monitoring	Process Monitoring Viewer	No	
Configuration & Security Analysis	Configuration Monitoring Administrator	No	
Configuration & Security Analysis	Configuration Monitoring Analyst	Yes	
Job & Automation Monitoring	Job Monitoring Administrator	No	
Job & Automation Monitoring	Job Monitoring Consumer	Yes	
Real User Monitoring	Real User Analyst Administrator	No	
Real User Monitoring	Real User Analyst Sensitive	Yes	
Real User Monitoring	Real User Analyst	Yes	

SAP Cloud ALM Role Dispatching – Operations Roles

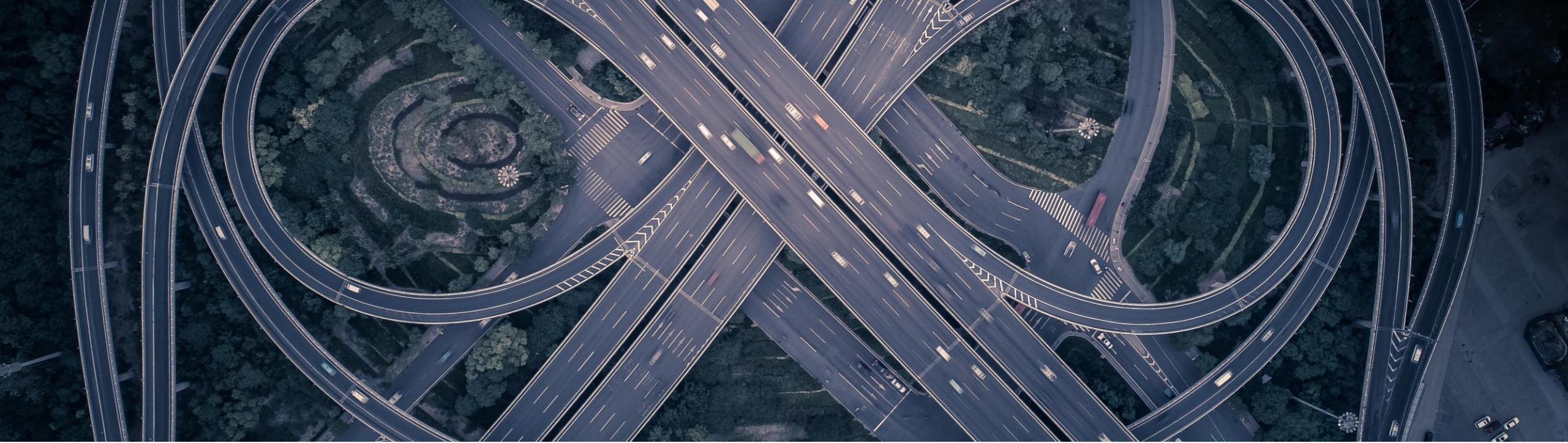
Domain	Role	<u>Can be granted to end customer?</u>	Comment
Business Service Management	All roles	No	Not ACL enabled yet
Integration Monitoring	All roles	No	Not ACL enabled yet
Synthetic User Monitoring	All roles	No	Not ACL enabled yet
Health Monitoring	Health Monitoring Administrator	No	Can deactivate the monitoring
Health Monitoring	Health Monitoring Viewer	Yes	Will only see the objects based on the ACLs defined by the MSP Admin
Monitoring Dashboards	Operations Monitoring Dashboards Administrator	No	
Monitoring Dashboards	Operations Monitoring Dashboards Configurator	Yes	
Monitoring Dashboards	Operations Monitoring Dashboards Viewer	Yes	

SAP Cloud ALM Role Dispatching – Cross

Domain	Role	<u>Can be granted to end customer?</u>	Comment
Cross Application	Global Administrator	No	Definitely not!
Cross Application	Global Auditor	No	Definitely not!
Landscape Management	Landscape Access Controller	No	Definitely not!
Landscape Management	Landscape Access Viewer	No	
Landscape Management	Landscape Administrator	No	
Landscape Management	Landscape Security Administrator	No	
Landscape Management	Landscape Security Viewer	No	
Landscape Management	Landscape Viewer	Yes	When the ACLs are properly defined.
Tag Management	Tag Administrator	Yes	
Tag Management	Tag Viewer	Yes	
Tenant Information	Tenant Information Viewer	Yes	In the future it might contain more information than needed
User & Access Management	User Administrator	No	Definitely not!
User & Access Management	User Viewer	No	

SAP Cloud ALM Role Dispatching – BTC and Service

Domain	Role	<u>Can be granted to end customer?</u>	Comment
BTC	Out of scope of this document	No	Still under review
Service	Out of scope of this document	No	Still under review



SAP Cloud ALM for Operation Scenarios in the MSP Context

PUBLIC



Multiple tenants and Customer Landscape Visibility

For the time being, ACLs only cover the following scenarios:

- Landscape Management
- Health Monitoring
- Real User Monitoring

Roadmap for the other operation scenarios to be provided soon.

We expect all the scenarios to be covered by the end of 2026*

Recommendations for MSP

1. In Landscape Management Service (LMS) create a business service for the customer (to receive downtime notifications).
2. Create a “Customer Unit” for the customer.
3. Assign only the systems and the business service for this customer to the “Customer Unit”.
4. Create an access control list for this customer and enter the customer unit as filter on the “Services & Systems” and the “Business Services” tab.
5. Assign the users of the customer to the Access Control List.
6. Test Access Control before activating it globally.
7. After the activation, the MSP admins should be excluded from the ACL restrictions so they can still access all systems.

Full details on ACLs [here](#).



Customer Business Units

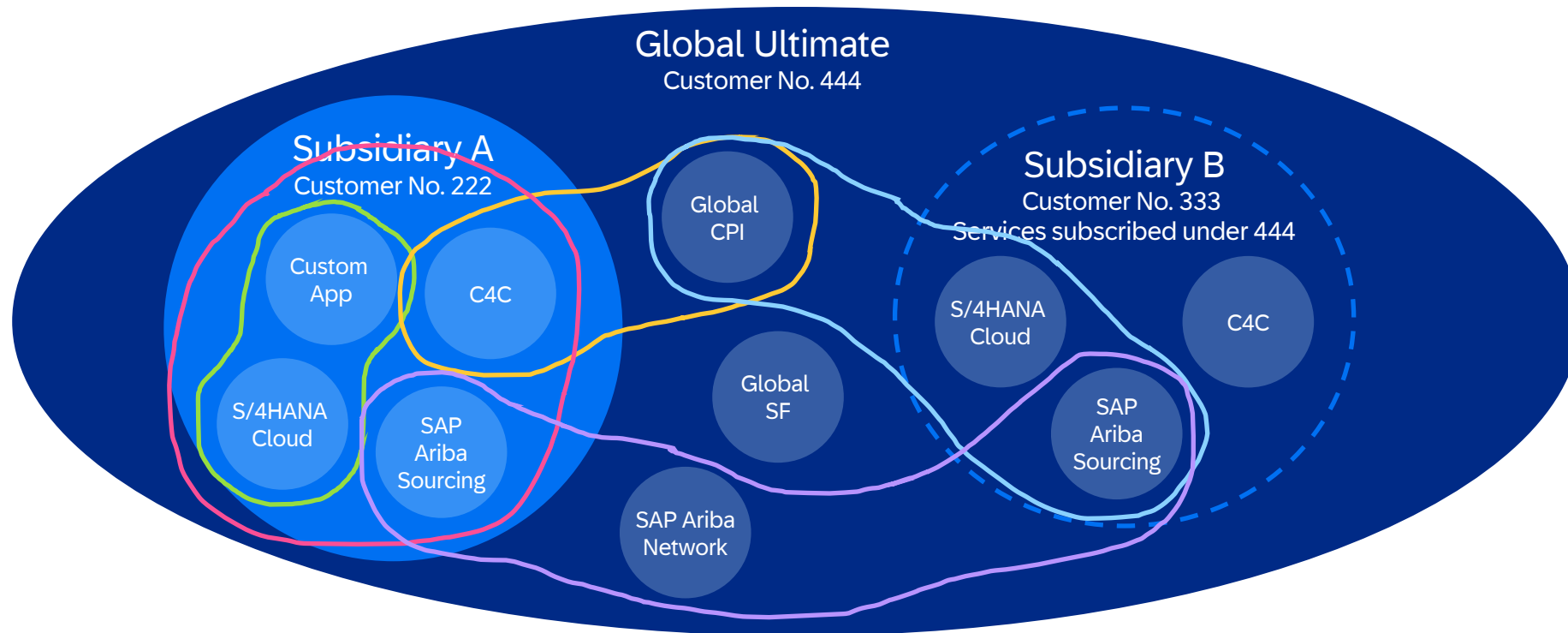
PUBLIC



Customer Business Units

Customer Business Units allow customers to group their services and systems based on their company structure even if all services are subscribed under the same customer number.

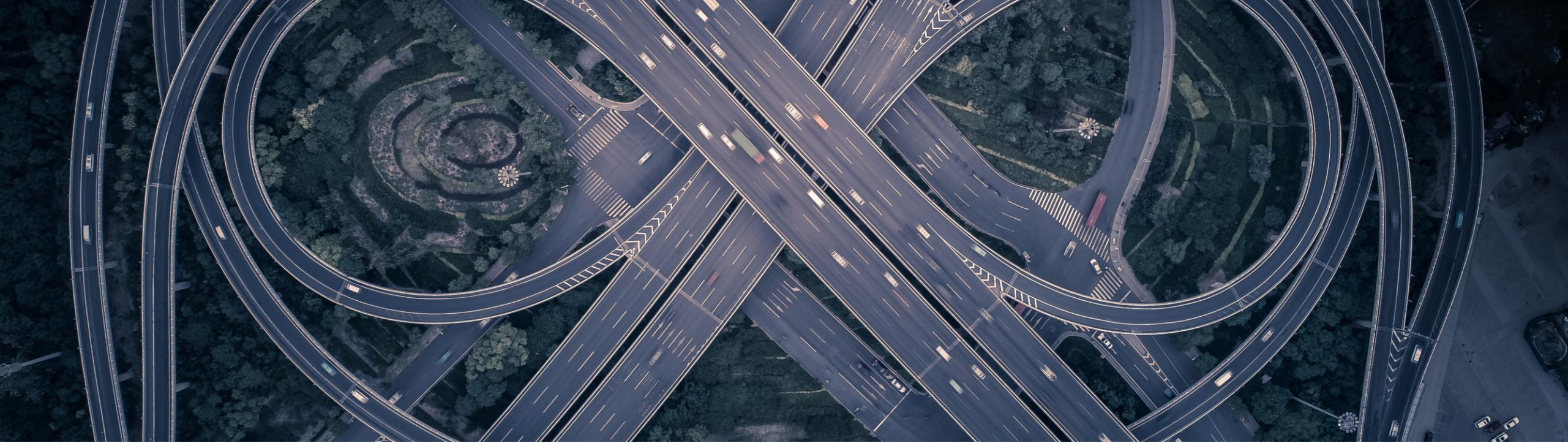
Customer Business Units can then be used to create rules in Access Control.



Customer Business Units – Maintenance and Usage

The image illustrates the configuration of Business Units in SAP BTP, showing three sequential steps:

- Step 1:** Accessing the 'Business Units' tab for a specific environment (CALM-CDM-CPI-3). The interface shows a search bar and a table of existing business units.
- Step 2:** Viewing the 'Configuration' menu, specifically the 'Customer Business Units' section. This step involves adding a new business unit.
- Step 3:** Configuring the 'Sales & Services NA' access control list. This step involves defining access rules and landscape objects for the new business unit.



Attribute-Based Access Control

PUBLIC



Motivation

Customers have **complex organizational structures with different tasks and responsibilities**. For example, the team monitoring the communication in the SAP Ariba landscape should not have access to the systems and the monitoring data on the SAP S/4HANA Cloud landscape.

The main commodity in SAP Cloud ALM is **Landscape Objects**, like cloud services, technical systems, and business services. Nearly all use cases use landscape objects one way or the other. So, landscape objects are what should be controlled when it comes to controlling the access in SAP Cloud ALM.

The current authorization concept in SAP Cloud ALM is based on SAP BTP role collections.

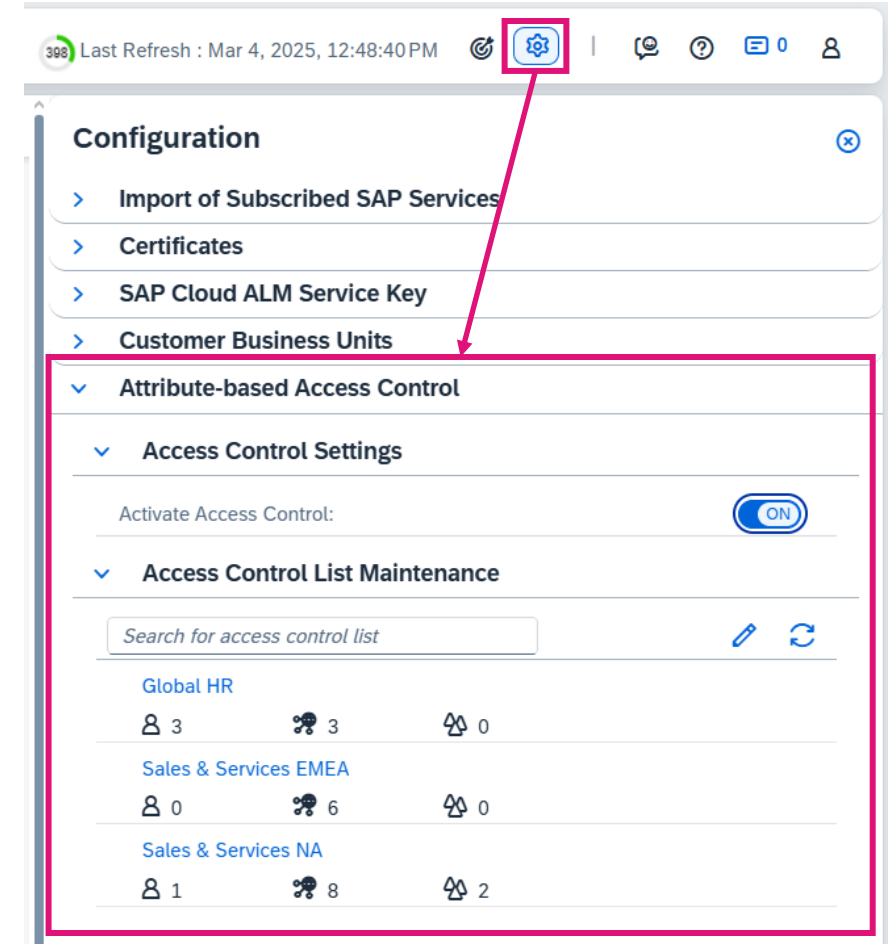
- Role collections control the access to applications and the activities that can be performed in an application.
- But role collections cannot control the access to single objects in an application.

We need an **attribute-based authorization concept**, that allows the customer to create **rules that define which user can access which services and systems**.

Attribute-Based Access Control in Landscape Management

Concept

- User access is controlled by Access Control Lists
 - Every list contains rules, that define which systems are part of this list.
 - Rules can be defined based on the following services and system attributes:
 - ERP Customer Number
 - Service Type
 - Customer Business Unit
 - Service/System Name or ID
 - Business Services Name or ID
- Users are assigned to the Access Control Lists which gives them access to the systems on the list.
 - User can be assigned with Read or Write access in Landscape Management.
- Other monitoring use cases inherit the Access Control Lists maintained in Landscape Management and control the use access accordingly.



Attribute-Based Access Control in Landscape Management

Access Control List maintenance

Access Control List Maintenance

Access Control Lists / SuccessFactors Monitoring EMEA

SuccessFactors Monitoring EMEA
Access for Monitoring teams for SuccessFactors Systems EMEA

Created By: [User] Changed By: [User]

General Services & Systems Business Services

Access Rules

Service Type: IS SAP SuccessFactors HCM x SAP SuccessFactors Employee Central Payroll x

Customer ERP Number: IS 12 (SAP Test Account - [User]) x

Landscape Objects

Landscape Object ID: IS I761295 x

Preview (Services & Systems in Access Control List) (5)

Name	Description	Service Type	Object Type	LMS Id
C00 [User]	C00 [User]	SAP SuccessFactors HCM	CloudService	b1 [User] /f9
C00 [User]	C00 [User]	SAP SuccessFactors HCM	CloudService	83 [User] /f9b
C00 [User]	C00 [User]	SAP SuccessFactors HCM	CloudService	5f [User] 23e
I761295	I761295	SAP Integration Suite (Cloud Integra...	CloudService	87 [User] 4ce
SFH [User]	SFH [User]	SAP SuccessFactors HCM	CloudService	2c [User] 184

Save Close

Attribute-Based Access Control in Landscape Management

User Assignment

Access Control Lists / SuccessFactors Monitoring EMEA

SuccessFactors Monitoring EMEA
Access for Monitoring teams for SuccessFactors Systems EMEA

Created By: [redacted] Changed By: [redacted] Last Change: Jul 2, 2024, 3:02:02 PM

USERS

☐	Name	Can Edit	Email	Roles
☐	E2ETests, CALM	☐	[redacted]	Cross Global Administrator, Health Monitoring Administrator
☐	[redacted] Andrea	☒	[redacted]	Cross Global Administrator, Health Monitoring Administrator

Define read/write access for each user

Assign users by selection or by email list

Add ▾ Delete ↑↓

By Selection

Mass Entry

Access Control Lists / Users / [redacted]

Andrea [redacted]

ACCESS CONTROL LISTS

User is restricted by Attribute-based Access Control ☒ YES

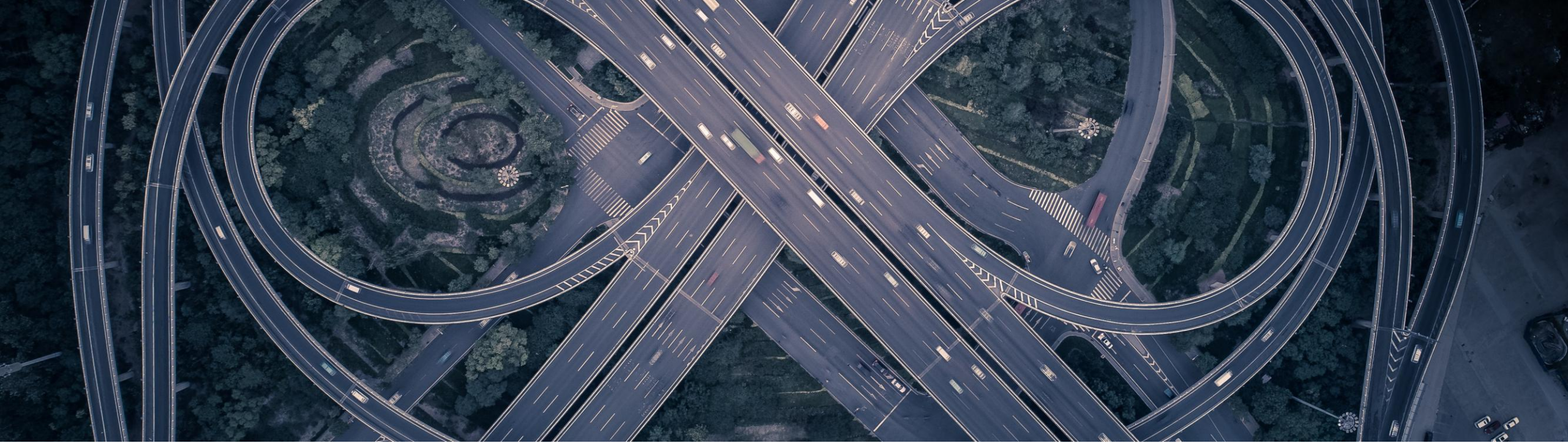
Exempt users from Access Control for a short or long time

Assign Access Control list from the user record

Live Search

Add Delete ↑↓

☐	Name	Description	Can Edit
☐	Demo Access Control List	Demo	☐
☐	SuccessFactors Monitoring EMEA	Access for Monitoring teams for SuccessFactors Systems EMEA	☒
☐	Test Case Creation Andrea New	[redacted]	☒



SAP Cloud ALM for Implementation Scenarios in the MSP context

PUBLIC



Implementation Scenarios and Impact in MSP Context

The following SAP Cloud ALM for Implementation scenarios are impacted in the MSP context:

- Project Management
- Change and Deployment Management

The following slides give details on how to use these scenarios.

The other SAP Cloud ALM for Implementation scenarios can be used without restrictions.

The following scenarios might be impacted in the future:

- Process Management
 - The processes might be linked to the systems where they are executed.
- Test Management
 - The tests might also be linked to systems.

Change and Deployment Management

Regarding Transport Management:

- SAP S/4HANA on-premise and SAP S/4HANA Cloud Private Edition:
 - Managed systems need to be registered through the ALM Setup transaction.
 - HTTPS connection can be done per SAP Cloud ALM tenant.
 - In the Deployment Plan and System Groups, the correct landscape must be configured.
 - Full details [here](#).
- Cloud Transport Management:
 - CTMS instance will be connected through an SAP BTP destination in the subaccount for SAP Cloud ALM.
 - The correct CTMS instance needs to be connected per end customer.
 - In Deployment Plan and System Groups, the correct landscape must be configured.
 - Full details [here](#).
- SAP S/4HANA Public Edition:
 - A communication arrangement must be created per S/4 tenant to establish a connection to an SAP Cloud ALM tenant.
 - In Deployment Plan and System Groups, the correct landscape must be configured.
 - Full details [here](#).

Change and Deployment Management – Continued

To setup change and deployment management (previous slide), the following is required:

- In SAP Cloud ALM:
 - Setup system groups and deployment plans.
 - This is done in the Project Setup app.
 - The roles allowed to do this are: “Project administrator” and “Project lead”.
 - All systems and services are visible after performing this setup.
 - **These roles MUST NOT be assigned to end customer users.**
 - **These roles MUST be granted only to MSP users.**
 - In the future, the ACLs will also be extended to the system groups and deployment plans.*
- Outside of SAP Cloud ALM:
 - All the configuration steps from the different systems require the knowledge of the SAP Cloud ALM home URL, and credentials.
 - The end customer users could potentially perform these steps (if they are granted the necessary rights in the external system or in the BTP subaccount).
 - But they will need the credentials information to be provided to them by the MSP admin users.
 - **Pragmatically, it is recommended that the MSP admin users perform these configuration steps.**

Project Management

Overview of the roles for Project Management [here](#).

There are also specific Project User Permissions, full details [here](#).

How to create/setup the project, system groups and deployment plans:

- MSP project lead
 - creates the project, deployment plan and system groups.
 - onboards team members
 - sets up subscription (workflow, external tool integration etc.)
 - has access to project overview and analytics reports
- End customer project member
 - Manages tasks (creates and updates tasks)
 - Has access to project overview and analytics reports

Ways of working

- MSP users can have “Project Administrator” and “Project Lead” roles.
- End customer users can have “Project Member” and “Project Viewer” roles.

Test Management and Tricentis

With each SAP Cloud ALM tenant (standard and extension), a Tricentis Test Automation tenant can be provisioned.

This is bound to an administrator role, so it will have to be performed by an **MSP user**.

The prerequisites are that this user has corresponding S-user:

- with the same email address as the SAP Cloud ALM user
- with Cloud Edit rights



IAS, Roles, and Users

PUBLIC



Usage of Identity Services in the MSP Context

Most of the time, the MSP will use one dedicated SAP Identify and Authorization Services (IAS) tenant per end customer.

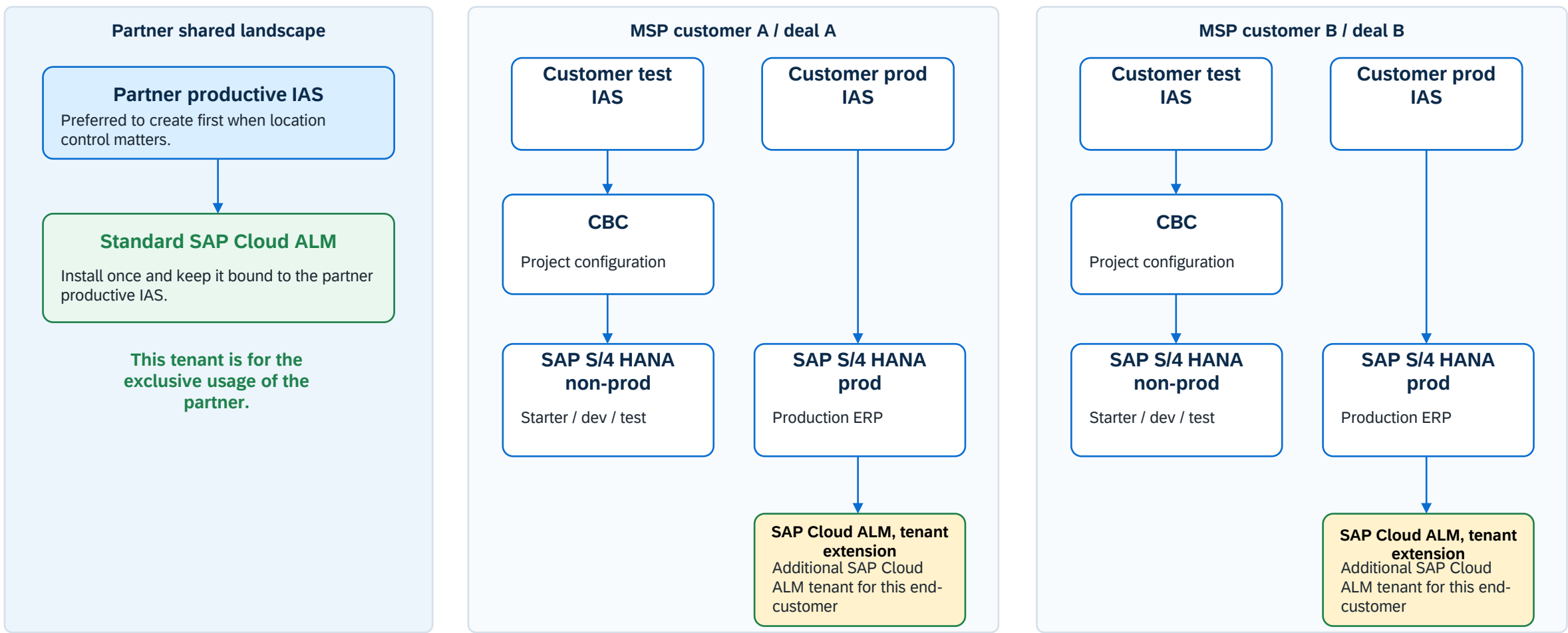
It is SAP's recommendation to **use one IAS per MSP end-customer.**

Should the MSP elect to utilize a single IAS to administer users across multiple end-customers, the MSP shall do so at its sole risk and shall be solely responsible for any and all consequences arising therefrom.

The following slide illustrates a recommended setup using SAP S/4 HANA.

Target IAS Setup

Architecture view: partner-shared SAP Cloud ALM on partner IAS, customer-specific CBC / S/4 / SAP Cloud ALM, tenant extension on customer IAS. Repeat the MSP lane for each end-customer.



Thank you.

