

SCIM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: USERCUBE

Website: <https://www.usercube.com/>

Name of Product: Usercube

Version: 5.1.4 Date:

29/07/2020

USERCUBE SOLUTION OVERVIEW

Usercube is an Identity Governance and Administration (IGA) solution. IGA brings together all an organization's processes to enable each identified individual to have the correct access rights at the right time for the right reasons. **This type of solution is important for several reasons:**

- Monitor everyone who has access, their missions and their locations
- Effectively manage employee arrivals, job changes and departures
- Optimize resource allocation workflows
- Increase security
- Facilitate audits with reliable and understandable data

Usercube V5.1.4 can be installed by 2 ways.

- Installed in the cloud, Usercube easily integrates with your information system without the need for specific expertise. Usercube benefits from MS-Azure's capacity. Your data is stored near you based on Azure's data-center locations, which increases the application responsiveness.
- Usercube can also be installed on-Premise, on the customer's servers. The solution allows for plug-and-play integration with cloud services as well as legacy applications.

KEY BENEFITS

Usercube builds a **repository of organizations**, sites, users and resources, from different sources, to become the centralized location for reliable and exhaustive information. The directory is powered by real-time jobs assignment of people, administration tasks and personal updates through the self-service screen. This constantly ensures a very high level of accuracy of the information contained. The repository can interface with other software to share knowledge of hierarchy and organization.

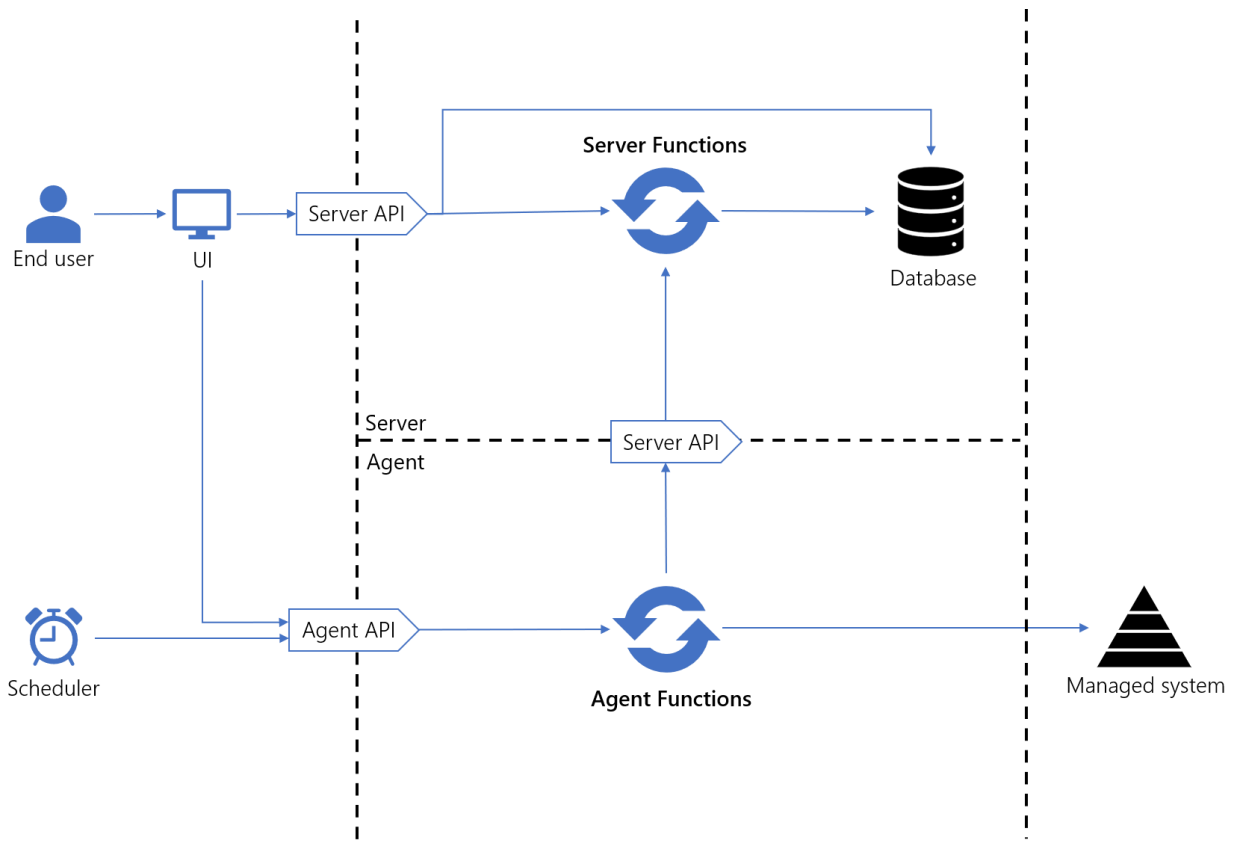
Inside organizations, people frequently move around (hires, departures, subsidiary creations, office closings, reorganizations, moves ...). Because the company's organization is defined in Usercube, workflows **notify the necessary people in real time**, making these actors more efficient and therefore reducing wasted time with each change. Additionally, the constantly updated repository and **the traceability of all requests** allows easy generation of compliance reports.

Usercube is the solution for centralizing **requests regarding computer rights and equipment endowments**. Each user, manager or local liaison, can make a request **to obtain, modify or revoke/return** access rights or equipment for the users in his/her scope.

Access rights for customer's on-premise applications or cloud services can either be provisioned manually via notifications to resource managers, or automatically via application connectors.

Usercube makes it possible to enumerate the IT system's Security Policy regarding access right controls and can automate the exercise of these controls. Every organization is thus protected from security breaches including breaches related to the **segregation of duties** (SoD).

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Usercube is composed of five main components:

- The **Server**: it provides the APIs used by the UI. It uses Server Functions when needed.
- The **Server Functions**: they are used by the Server. They perform module-specific computations such as data loading, assignment policy enforcement, assignment review notifications. The functions are fetching their configuration and data from the database.

- The **Database**: it stores all the data needed by Usercube. This includes, but is not limited to, the applicative configuration, the resources repository, the assignment policy, and the computed assignments.
- The **Agent**: it provides Agent Functions that are used to interact with the managed systems. Only Agent Functions credentials from the managed systems and the network are necessary to read/write data from/to the managed systems.
- The **Agent Functions**: they are usually involved in the synchronization (Up or Down) process. Some functions extract data from managed systems (taking a managed system data snapshot) and send it to the server. Other functions are fetching the provisioning orders prepared by the server during the assignment policy enforcement process and execute them on the target managed systems.

Usercube's SCIM integration is part of the Agent Functions and is called a connector. By calling SCIM endpoints on the CyberArk server, Usercube can extract and modify in CyberArk data about CyberArk's users, groups and safes and then manage accounts and entitlements as described in KEY BENEFITS: Usercube can create, modify and delete user accounts and groups membership.

The connector's configuration is set in a JSON file "**appsettings.agent.json**", where we specify the server address, login, password and what information has to be extracted, and in the xml configuration.

CYBERARK SCIM SERVER INSTALLATION

To use Usercube's SCIM connector, you need a CyberArk SCIM Server in your CyberArk server. The CyberArk SCIM Server is available in CyberArk's Marketplace. To install it you may refer to CyberArk SCIM Server Implementation Guide.

USERCUBE INSTALLATION & INTEGRATION CONFIGURATION

Refer to Usercube's documentation for the installation and the xml configuration for the connector (which is available since version 5.1.4):

Step 1: Usercube installation [https://extranet.usercube.com/5.1/\[version\]>=5.1.4/Documentation/installation-guide/index.html](https://extranet.usercube.com/5.1/[version]>=5.1.4/Documentation/installation-guide/index.html) Step 2: Create SCIM connector for CyberArk

[https://extranet.usercube.com/5.1/\[version >= 5.1.4\]/Documentation/integration-guide/howtos/createconnector/](https://extranet.usercube.com/5.1/[version >= 5.1.4]/Documentation/integration-guide/howtos/createconnector/)

Step 3: Connector settings

[https://extranet.usercube.com/5.1/\[version >= 5.1.4\]/Documentation/integrationguide/connectors/scim/index.html](https://extranet.usercube.com/5.1/[version >= 5.1.4]/Documentation/integrationguide/connectors/scim/index.html)

USERCUBE'S SCIM CONNECTOR SETTINGS

The connector needs some information to collect and modify data in CyberArk.

This information is set in the “**appsettings.agent.json**”, under InformationSystems and SCIMSetting. Here is an example:

```
"SCIM_CyberArk": {
  "Server": "http://services-uscentral.skytap.com:12345/CyberArk/scim",
  "Login": "LOGIN",
  "Password": "PASSWORD",
  "Filter": "Users;id userName active name:givenName|middleName|familyName emails:value
  phoneNumbers:value title profileUrl*ContainerPermissions;id user:value group:value
  container:value rights*Containers;id displayName type name",
  "FilterGroup": "Groups;id displayName",
  "EntryFile": "C:/UsercubeDemo/Sources/CyberArk",
  "MembersFile": "C:/UsercubeDemo/Sources/CyberArk_members",
  "SCIMSyntax": "CyberArk"
}
```

Server: Specifies the CyberArk's server endpoint for SCIM.

Login: Specifies the service account's login.

Password: Specifies the service account's password.

Filter: Specifies the non group entities and attributes you want to collect for each of them. For more information about the syntax, see Usercube's documentation.

FilterGroup: Is the same as Filter for group entities.

EntryFile: When a connector extract information from another system, it generates csv files. This attribute specifies prefix and path for these files.

MembersFile: Is the same as EntryFile for membership files.

SCIMSyntax: Specifies for what system the connector is used. In our case it is CyberArk.

DATA INTEGRATION DETAILS IN USERCUBE

Usercube is highly customizable, but here are the properties extracted and fulfilled by default.

Exported attributes in Usercube:

CyberArk Types	Properties
User	id
	userName
	active
	givenName
	middleName
	familyName
	emails
	phoneNumbers
	title
	profileUrl
	groups
	containers
Group	id
	display
	containers
Container	id
	displayName
	type
	name
	groups
	users

Fulfilled properties in CyberArk:

CyberArk's user accounts' properties

username
active
givenName
familyName
emails
titles
groups

LIMIT PROFILE MULTIPLICATION WHILE ALLOWING ULTRA-PRECISE MANAGEMENT

Usercube provides a comprehensive **role-based model** that defines the rights of users based on their identity, job functions and location.

This model can be **fine-grained** and very precise, while limiting the complexity resulting from the multiplication of possible entitlement combinations.

For easier **management of the information** system and entitlements, Usercube intelligently groups together resource types, applications, and job role. Contextual rules are also considered.

Notably, the multi-dimensional model can **also manage users with several positions without multiplying complexity**.

CERTIFY ACCESS RIGHTS BY MANAGERS AND APPLICATION OWNERS

Usercube allows compliance verification of **access rights granted based on affectation rules** in place your organization. Your organization's governance model is implemented with precise and multi-dimensional rule-based functionality. Access rights previously granted are collected and analyzed by our role mining function. Gaps between **the model and the real situation appear immediately**.

Usercube manages the model's life cycle and can simulate or apply real-time model evolutions, provisioning the information system.

Usercube can **automate certification campaigns**: managers or application/resource owners are invited to review and approve (or reject) a selection of entitlements for each of their employees or for each user of the application. The manager or application/resource owner declares the need to keep, modify, or remove access to the revised application, adding comments if appropriate.

All campaigns and the associated documentary corpus are historized and preserved in Usercube.

Business Contact	Name	DUPONT Charles
	Email	charles.dupont@usercube.com
	Tel	00 33 620 36 46 17
Technical Contact	Name	MOYERE Nicolas
	Email	nicolas.moyere@usercube.com
	Tel	
Support Contact	Name	Support
	Email	support@usercube.com
	Tel	