Data Realm Settings Endpoints

Introduction

Use the /data PATCH endpoints to integrate membership and profile directories, map profile properties to directory attributes, and customize global auxiliary fields.

Prerequisites

1. Complete the Enablement and Header Steps in the **Admin API Guide**
2. Have access to the application code that calls to the API endpoint(s)
3. Have a corporate directory with which to integrate for end-user membership (login) credentials
4. Have a corporate directory(s) with which to integrate for end-user profile information
5. Designate or create a SecureAuth service account in the directory with read and (optional) write access to membership and profile information

/data Endpoints

The following endpoints are prepended with the URL, **https://<SecureAuth IdP Domain>/api/v1/realms/<realm ID>**, if running **SecureAuth IdP v9.1** – in which **realm ID** is the ID number of the realm to configure –

or **https://<SecureAuth IdP Domain>/api/v2/realms/<realm ID>**, if running **SecureAuth IdP v9.2 or later**

Membership Directory Integration /data/membership PATCH Endpoint

Use this endpoint to configure the realm's Membership Directory integration. This is the information with which the end-user logs into the realm, but may not contain profile information required for authentication or assertion.

NOTE: The supported directory types are LDAP (AD and others), SQL Server, Oracle Database, Microsoft Azure AD, and Web Service (Multi-Data Store) (pulls Membership information from other SecureAuth IdP realms' Membership directory integrations).

HTTP Method	Endpoint	Example	SecureAuth IdP version
PATCH	`/data/membership`	`https://secureauth.company.com/api/v1/realms/26/data/membership`	v9.1
PATCH	`/data/membership`	`https://secureauth.company.com/api/v2/realms/26/data/membership`	v9.2 or later

Field Definitions and Accepted Values for Configuration

Defaulted values in **bold**

Field	Description	Accepted Values	Note
dataStoreType	Corporate data store from which SecureAuth IdP pulls user membership information for login purposes	• **ADSamAccountName** • ADUPN • ADAM • Domino • eDirectory • SunOne • Tivoli • OpenLDAP • OtherLDAP • SQLServer • WebService • Oracle • NoDataStore • Azure	

dataStore	Settings for selected data store	N / A	
domain	Domain name of directory	any	For LDAP directory configurations
allowAnonymousLookup	Enable directory search without requiring username or password	• true • **false**	For LDAP directory configurations
connectionMode	How SecureAuth IdP and directory connect	• **Secure** • SSL • Standard	For LDAP directory configurations
serviceAccount	Username of service account with read (and optional write) privileges for directory	any	For LDAP directory configurations
serviceAccountPassword	Password associated to service account username	any	For LDAP directory configurations
searchAttribute	ID used to search directory for user account	any, directory attribute	For LDAP directory configurations
searchFilter	What SecureAuth IdP expects for username (username=%v in string)	any, in required format based on directory selection	For LDAP directory configurations
useAdvancedAdUserCheck	Check account status of presented username	• true • **false**	For LDAP directory configurations
validateUserType	How SecureAuth IdP validates user from directory information	• **Search** • Bind	For LDAP directory configurations
userGroupCheckType	Create list of allowed or denied user groups, based on selection	• **AllowAccess** • DenyAccess	For LDAP directory configurations
userGroups	List of user groups allowed or denied access to realm (based on userGroupCheckType selection)	any	For LDAP directory configurations
includeNestedGroups	Include nested groups in group restrictions	• true • **false**	For LDAP directory configurations
groupsField	Directory attribute that contains user group information	any, directory attribute	For LDAP directory configurations
maxInvalidPasswordAttempt	Number of invalid passwords allowed before user account is locked	any, defaulted to **10**	For LDAP and SQL Server directory configurations
connectionString	String to enable communication between directory and SecureAuth IdP	any, in required format based on directory selection	For SQL Server and Oracle Database directory configurations
passwordFormat	How SQL Server password is stored in directory	• **Clear** • Hashed • Encrypted	For SQL Server directory configurations
	How Oracle password is stored in directory, also dictates which Password SP to use	• **Clear** • SHA1 • SHA2 • MD5	For Oracle Database directory configurations
allowedGroups	List of user groups allowed access to realm	any	For SQL Server, Oracle Database, and Azure AD directory configurations
deniedGroups	List of user groups denied access to realm	any	For SQL Server, Oracle Database, and Azure AD directory configurations
sprocGetUser	Name of Get User Stored Procedure (SP)	any	For SQL Server and Oracle Database directory configurations
sprocGetPassword	Name of Get Password SP	any	For SQL Server and Oracle Database directory configurations
sprocResetPassword	Name of Reset Password SP	any	For SQL Server and Oracle Database directory configurations
sprocCreateUser	Name of Create User SP	any	For SQL Server and Oracle Database directory configurations

passwordSalt	Unique string of text to append to passwords before hashed	any	For Oracle Database directory configurations; *not* applicable for **"passwordFormat:"Clear"**
sprocChangePassword	Name of Change Password SP	any	For Oracle Database directory configurations
sprocLockUser	Name of Lock User SP	any	For Oracle Database directory configurations
sprocUnlockUser	Name of Unlock User SP	any	For Oracle Database directory configurations
userName	Username of Azure AD administrator service account	any	For Azure AD directory configurations
password	Password associated to Azure AD service account username	any	For Azure AD directory configurations
tenantDomain	Domain name of Azure directory	any	For Azure AD directory configurations
clientId	Client ID of Native Client Application from Azure directory	any	For Azure AD directory configurations
username	Username provided by SecureAuth IdP for Web Service Data Store (recommended to change from default)	any	For Web Service (Multi-Data Store) directory configurations
password	Password associated to Web Service Data Store username (recommended to change from default)	any	For Web Service (Multi-Data Store) directory configurations
failover	Whether SecureAuth IdP responds in event of failure	• true • **false**	For Web Service (Multi-Data Store) directory configurations
mainUrls	Connected SecureAuth IdP realms in which IdP searches for user membership information	• realm name (SecureAuth12) for realms on the same appliance • full URL (https://secureauth.company.com/secureauth20) for realms on different appliance	For Web Service (Multi-Data Store) directory configurations
useCyberArkVault	Use CyberArk Vault to provide service account / username information	• **null** • true	For LDAP, SQL, and Oracle directory configurations
cyberArkVault	Settings for CyberArk Vault	• **null** • N / A	If **"useCyberArkVault": true**, then no configuration is required for this field, but for subsequent fields
username	Service account username of directory accessed by AIM for credential information	any	If using CyberArk Vault configurations
address	Domain of service account's directory access by AIM for credential information	any	If using CyberArk Vault configurations
safe	Name of access control where credentials are stored	any	If using CyberArk Vault configurations
folder	Name of folder in which account resides	any	If using CyberArk Vault configurations
caobject	Unique identifier for account	any	If using CyberArk Vault configurations

Parameters and Response Examples

Parameters	**Success Response**

LDAP Data Store (with CyberArk enabled)

```
{
        "dataStoreType": "ADSamAccountName",
        "dataStore": {
                "server": "LDAP://company.local/",
                "distinguishedName": "DC=company,DC=local",
                "domain": "company.local",
                "allowAnonymousLookup": false,
                "connectionMode": "Secure",
                "useCyberArkVault": true,
                "cyberArkVault": {
                        "username": "",
                        "address": "",
                        "safe": "",
                        "folder": "",
                        "caobject": ""
                },
                "serviceAccount": "service@domain.com",
                "serviceAccountPassword": null,
                "searchAttribute": "samAccountName",
                "searchFilter": "(&(samAccountName=%v)(objectclass=*))",
                "useAdvancedAdUserCheck": false,
                "validateUserType": "Search",
                "userGroupCheckType": "AllowAccess",
                "userGroups": "",
                "includeNestedGroups": false,
                "groupsField": "memberOf",
                "maxInvalidPasswordAttempt": 10
        }
}
```

SQL Server

```
{
        "dataStoreType": "SQLServer",
        "dataStore": {
                "connectionString": "-BSA-xxxxxxxx-ESA-",
                "useCyberArkVault": false,
                "cyberArkVault": null,
                "passwordFormat": "Clear",
                "allowedGroups": "",
                "deniedGroups": "",
                "maxInvalidPasswordAttempts": 10,
                "sprocGetUser": "GETUSER",
                "sprocGetPassword": "GETPASSWORD",
                "sprocResetPassword": "RESETPASSWORD",
                "sprocCreateUser": "CREATEUSER"
        }
}
```

```
{
 "status": "Success",
 "message": []
}
```

Oracle Database

```
{
        "dataStoreType": "Oracle",
        "dataStore": {
                "connectionString": "<CONNECTION STRING>",
                "passwordFormat": "Clear",
                "passwordSalt": "",
                "allowedGroups": "group1",
                "deniedGroups": "group2",
                "sprocGetUser": "GETUSER",
                "sprocGetPassword": "GETPASSWORD",
                "sprocUpdateUser": "UPDATEUSER",
                "sprocResetPassword": "RESETPASSWORD",
                "sprocChangePassword": "CHANGEPASSWORD",
                "sprocCreateUser": "CREATEUSER",
                "sprocLockUser": "LOCKUSER",
                "sprocUnlockUser": "UNLOCKUSER",
                "useCyberArkVault": false,
                "cyberArkVault": null
        }
}
```

Azure AD

```
{
        "dataStoreType": "Azure",
        "dataStore": {
                "userName": "username",
                "password": *********,
                "tenantDomain": "",
                "clientId": "",
                "allowedGroups": "group1",
                "deniedGroups": "group2"
        }
}
```

Web Service (Multi-Data Store)

```
{
        "dataStoreType": "WebService",
        "dataStore": {
                "username": "FBAService",
                "password": null,
                "failover": false,
                "mainUrls": [
                        "SecureAuth12"
                        "https://secureauth.company.com/secureauth20"
                ]
        }
}
```

Profile Provider Directory Integration(s) /data/profile PATCH Endpoint

Use this endpoint to configure the realm's Profile Provider Directory integration(s). This integration(s) includes end-user profile data, which is utilized for authentication and assertion purposes.

Multiple data stores can be configured, enabling SecureAuth IdP to pull profile information from various sources; and the same directory integration used for the Membership integration can be repeated at this endpoint.

HTTP Method	Endpoint	Example	SecureAuth IdP version
PATCH	`/data/profile`	`https://secureauth.company.com/api/v1/realms/26/data/profile`	v9.1
PATCH	`/data/profile`	`https://secureauth.company.com/api/v2/realms/26/data/profile`	v9.2 or later

Field Definitions and Accepted Values for Configuration

Defaulted values in **bold**

Field	Description	Accepted Values	Note
defaultProvider	Default directory to provide user account profile information	• **LDAPProfileProvider** • SqlProfileProvider • WebServiceProfileProvider • OracleProfileProvider • AzureProfileProvider	This directory is "**source": "DefaultProvider"** in the Profile Fields section of the parameters
dataStoreType	Type of LDAP directory integration	• ADSamAccountName • ADUPN • ADAM • Domino • eDirectory • SunOne • Tivoli • OpenLDAP • OtherLDAP	If **"defaultProvider": "LDAPProfileProvider"**
ldapDataStore	Settings for LDAP profile directory	N / A	
connectionMode	How SecureAuth IdP and directory connect	• **Secure** • SSL • Standard	For LDAP directory configurations
connectionString	String to enable communication between directory and SecureAuth IdP	any, in required format based on directory selection	For LDAP, SQL Server, and Oracle Database directory configurations
searchFilter	What SecureAuth IdP expects for username (username=%v in string)	any, in required format based on directory selection	For LDAP directory configurations
searchAttribute	ID used to search directory for user account	any, directory attribute	For LDAP directory configurations
userGroups	List of user groups allowed access to realm	any	For LDAP directory configurations
connectionUsername	Username of service account with read (and optional but recommended write) privileges for directory	any	For LDAP directory configurations
connectionPassword	Password associated to service account username	any	For LDAP directory configurations
includeNestedGroups	Include nested groups in group restrictions	• true • **false**	For LDAP directory configurations
sqlDataStore	Settings for SQL Server profile directory	N / A	

sprocGetUserProfile	Name of Get User Profile Stored Procedure (SP)	any	For SQL Server directory configurations
sprocUpdateProfile	Name of Update User Profile SP	any	For SQL Server and Oracle Database directory configurations
allowedGroups	List of user groups allowed access to realm	any	For SQL Server directory configurations
oracleDataStore	Settings for Oracle Database profile directory	N / A	
sprocGetProfile	Name of Get User Profile SP	any	For Oracle Database directory configurations
azureDataStore	Settings for Azure AD profile directory	N / A	
username	Username of Azure AD administrator service account	any	For Azure AD directory configurations
password	Password associated to Azure AD service account username	any	For Azure AD directory configurations
tenantDomain	Domain name of Azure directory	any	For Azure AD directory configurations
clientId	Client ID of Native Client Application from Azure directory	any	For Azure AD directory configurations
appKey			
webServiceDataStore	Settings for Web Service (Multi-Data Store) profile directory	N / A	
username	Username provided by SecureAuth IdP for Web Service Data Store (recommended to change from default)	any	For Web Service (Multi-Data Store) directory configurations
password	Password associated to Web Service Data Store username (recommended to change from default)	any	For Web Service (Multi-Data Store) directory configurations
allowedUserGroups	List of user groups allowed access to realm	any	For Web Service (Multi-Data Store) directory configurations
failover	Whether SecureAuth IdP responds in event of failure	• true • **false**	For Web Service (Multi-Data Store) directory configurations
mainUrls	Connected SecureAuth IdP realms in which IdP searches for user membership information	• realm name (SecureAuth12) for realms on the same appliance • full URL (https://secureauth.company.com/secureauth20) for realms on different appliance	For Web Service (Multi-Data Store) directory configurations
useCyberArkVault	Use CyberArk Vault to provide service account / username information	• **null** • true	For LDAP, SQL, and Oracle directory configurations
cyberArkVault	Settings for CyberArk Vault	• **null** • N / A	If **"useCyberArkVault": true**, then no configuration is required for this field, but for subsequent fields
username	Service account username of directory accessed by AIM for credential information	any	If using CyberArk Vault configurations
address	Domain of service account's directory access by AIM for credential information	any	If using CyberArk Vault configurations
safe	Name of access control where credentials are stored	any	If using CyberArk Vault configurations
folder	Name of folder in which account resides	any	If using CyberArk Vault configurations
caobject	Unique identifier for account	any	If using CyberArk Vault configurations
profileFields	Settings for profile property / directory attribute mapping	N / A	Refer to **LDAP Attributes / SecureAuth IdP Profile Properties Mapping** for Profile Property descriptions and appropriate directory mapping

property Name	SecureAuth IdP Profile Property name, used throughout IdP configuration	see list in parameters below	List of properties generated in realm creation (**/realms** endpoint)
source	Directory from which profile information is pulled, based on directories configured	• **DefaultProvider** • DirectoryServer • SqlServer • WebService • Azure • Oracle	
field	Directory attribute that contains required profile information, mapped to the IdP Property	any, directory attribute format	If source is LDAP directory type
dataFormat	How information is stored in directory	• **PlainText** • StandardEncryption • **AdvancedEncryption** • StandardHash • **PlainBinary** • JSON • EncryptedJSON	**AdvancedEncryption** default for **OATH Seed** **PlainBinary** default for **DigitalFP**, **PNToken**, **AccessHistory**, and **OATHToken** **PlainText** default for remainder
isWritable	Whether SecureAuth IdP can write to directory to update profile information	• true • **false**	

Add custom Profile Properties in the **profileFields** section

```
        "profileFields": [
                {
                        "propertyName": "BehaveBio",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
        {
            "propertyName": "<NEW PROPERTY NAME>",
            "source": "<PROVIDER>",
            "field": "<DIRECTORY ATTRIBUTE>",
            "dataFormat": "<FORMAT>",
            "isWritable": <T OR F>
        }
        ]
```

Parameters and Response Examples

Parameters	Success Response

<pre>{
"defaultProvider": "LDAPProfileProvider",
"dataStoreType": "ADSamAccountName",
"ldapDataStore": {
"connectionMode": "Secure",
"connectionString": "LDAP://127.0.0.1/DC=domain,DC=com",
"searchFilter": "(&(samAccountName=%v)(objectclass=*))",
"searchAttribute": "",
"useCyberArkVault": false,
"cyberArkVault": null,
"userGroups": "",
"connectionUsername": "service@domain.com",
"connectionPassword": "***************",
"includeNestedGroups": false
},
"sqlDataStore": {
"sprocGetUserProfile": "",</pre>
	<pre>{
	"status": "Success",
	"message": []
	}</pre>

```
                "sprocUpdateProfile": "",
                "allowedGroups": "",
                "connectionString": "<CONNECTION STRING>",
                "useCyberArkVault": null,
                "cyberArkVault": null
        },
        "oracleDataStore": {
                "connectionString": "<CONNECTION STRING>",
                "useCyberArkVault": null,
                "cyberArkVault": null,
                "sprocGetProfile": "GETUSERPROFILE",
                "sprocUpdateProfile": "UPDATEUSERPROFILE"
        },
        "azureDataStore": {
                "username": "",
                "password": "",
                "tenantDomain": "",
                "clientId": "",
                "appKey": ""
        },
        "webServiceDataStore": {
                "username": "FBAService",
                "password": "",
                "allowedUserGroups": "",
                "failover": false,
                "mainUrls": [
                        "SecureAuth12"
                        "https://secureauth.company.com/secureauth20"
                ]
        },
        "profileFields": [
                {
                        "propertyName": "FirstName",
                        "source": "DefaultProvider",
                        "field": "givenName",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "LastName",
                        "source": "DefaultProvider",
                        "field": "sn",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "AuxID1",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "AuxID2",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "AuxID3",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "AuxID4",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
```

```
            "isWritable": false
        },
        {
            "propertyName": "AuxID5”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "AuxID6”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "AuxID7”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "AuxID8”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "AuxID9”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "AuxID10”,
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "Email1",
            "source": "DefaultProvider",
            "field": "mail",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "Email2",
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "Email3",
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
        },
        {
            "propertyName": "Email4",
            "source": "DefaultProvider",
            "field": "",
            "dataFormat": "PlainText",
            "isWritable": false
```

```
        },
        {
                "propertyName": "Phone1",
                "source": "DefaultProvider",
                "field": "telephoneNumber",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "Phone2",
                "source": "DefaultProvider",
                "field": "mobile",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "Phone3",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "Phone4",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "KbQuestions",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "KbAnswers",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "CertCount",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "CertResetDate",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "GroupList",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "pinHash",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
```

```
        {
                "propertyName": "MobileResetDate",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "MobileCount",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "CertSerialNumber",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "ExtSyncPwdDate",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "CertExpiration",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "HardwareToken",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "iOSDevices",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainText",
                "isWritable": false
        },
        {
                "propertyName": "OATHSeed",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "AdvancedEncryption",
                "isWritable": false
        },
        {
                "propertyName": "DigitalFP",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainBinary",
                "isWritable": false
        },
        {
                "propertyName": "PNToken",
                "source": "DefaultProvider",
                "field": "",
                "dataFormat": "PlainBinary",
                "isWritable": false
        },
        {
```

```
                        "propertyName": "OneTimeOATHList",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                },
                {
                        "propertyName": "AccessHistory",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainBinary",
                        "isWritable": false
                },
                {
                        "propertyName": "OATHToken",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainBinary",
                        "isWritable": false
                },
                {
                        "propertyName": "BehaveBio",
                        "source": "DefaultProvider",
                        "field": "",
                        "dataFormat": "PlainText",
                        "isWritable": false
                }
        ]
}
```


Global Auxiliary Fields /data/globalaux PATCH Endpoint

Use this endpoint to configure the realm's Global Auxiliary values, which are standard values that are asserted from SecureAuth IdP to the SP for each end-user without requiring directory storage.

HTTP Method	Endpoint	Example	SecureAuth IdP version
PATCH	`/data/globalaux`	`https://secureauth.company.com/api/v1/realms/26/data/globalaux`	v9.1
PATCH	`/data/globalaux`	`https://secureauth.company.com/api/v2/realms/26/data/globalaux`	v9.2 or later

Definitions

globalAux1 - 5: Any global data that can be asserted and applies to all end-users

Parameters and Response Examples

Parameter	Success Response
`{ "globalAux1": "ACME Corp.", "globalAux2": "1", "globalAux3": "false", "globalAux4": "", "globalAux5": "" }`	`{ "status": "Success", "message": [] }`

Related Documentation
Data Tab Configuration