

Non-Employee Identity Suite - Connector Guide

Version Number 4.6.0-ni227.1

Contents

Copyright.....	v
----------------	---

Chapter 1: Configuring the SCIM 2.0 Server to Interact with IDF LDAP Gateway-based Connectors.....	6
Overview.....	7
Configuring SCIM 2.0 Server.....	7
Configuring LDAP Gateway Details.....	7
SCIM to LDAP Attribute Mappings.....	9
Non-Employee ID.....	9
Connector-specific Guidance.....	9
RACF.....	10
Epic Health.....	11

Copyright

All Rights Reserved.

All rights are reserved by IDMWORKS. No part of this software may be reproduced, duplicated or modified in any form or incorporated into any information retrieval system, electronic or any other or transmitted in any form without the prior permission of IDMWORKS.

Chapter 1

Configuring the SCIM 2.0 Server to Interact with IDF LDAP Gateway-based Connectors

Topics:

- Overview
 - Configuring SCIM 2.0 Server
 - Connector-specific Guidance
- 

Overview

This connector guide provides detailed information about configuring the SCIM 2.0 server (Account management service) to interact with IDF LDAP Gateway-based connectors.

Note: This guide assumes that LDAP Gateway and NEIS services are already installed. Please refer to <NEIS installation folder>\docs\NEIS_user_guide.pdf for installation, configurations of NEIS services.

Configuring SCIM 2.0 Server

The Account Management Service communicates with the target applications via IDF LDAP Gateway-based connectors. The configurations to connect to the IDF LDAP Gateway-based connector are present in IdPortal.json file of the Configuration service.

Configuring LDAP Gateway Details

To configure the LDAP Gateway, please follow the below steps.

Navigate to the <NEIS installation folder>\config\conf folder and modify IdPortal.json file as follows:

1. Locate the LdapServerConfig attribute and change the values of it's sub attributes wherever applicable.
 - ServerAddress - Hostname or IP address to an LDAP directory
 - ServerPort - Port number for communicating with the LDAP directory
 - BaseDn - Base DN representing the root directory that users and groups will be managed within
 - RootUserDn - Username credential in DN format for authenticating against the LDAP directory.
 - RootUserPassword - Password credential in DN format for authenticating against the LDAP directory

Example: LDAP connector

```
"LdapServerConfig" : {
    "ServerAddress" : "localhost",
    "ServerPort" : 6389,
    "BaseDn" : "dc=system,dc=backend",
    "RootUserDn" : "cn=Directory Manager,dc=system,dc=backend",
    "RootUserPassword" : "CfDJ8DnGfbZY571I1P6QeZriBfw3rtNrr09BS4Ou7"
}
```

Note: RootUserPassword must be encrypted. Please follow the <NEIS installation folder>\docs\NEIS_user_guide.pdf for how to encrypt the sensitive data using EncryptionUtility.

2. Locate the UserResourceLdapConfig attribute and change the values of it's sub attributes wherever applicable.
 - RDNResourceAttr - LDAP attribute that represents the Resource RDN (ie. cn, uid, etc). This attribute is found as part of the larger distinguished name representing the resource
 - UUIDResourceAttr - LDAP attribute that represents the globally unique identifier of the Resource (ie. entryUUID or uuid)
 - GroupMembershipAttr - LDAP attribute that represents the groups that the Resource belongs to (ie. memberof)
 - GroupMembershipIdAttr - LDAP attribute that represents the groups id that the Resource belongs to (e.g. memberofId)
 - EmailAttr - LDAP attribute that represents the email address of the Resource (ie. mail)
 - ActiveStateIdentifierAttr - LDAP attribute that represents the active state of the Resource (ie. Active)
 - SchemaPrefix - Organizational Units that the Resource will be contained within (excluding the BaseDN). Example: ou=nonemployees,ou=People
 - SearchBaseDn - Base DN representing the container that resources will be managed within (ie. ou=People,dc=system,dc=backend)
 - ObjectClasses - List of object classes that represent the resource object (ordered from general to specific)

Example:

```
"UserResourceLdapConfig" : {
    "RDNResourceAttr" : "uid",
    "UUIDResourceAttr" : "entryUUID",
    "GroupMembershipAttr" : "memberof",
    "GroupMembershipIdAttr" : "isMemberOfId",
    "EmailAttr" : "wmail",
    "ActiveStateIdentifierAttr" : "Active",
    "SchemaPrefix" : "ou=People,ou=NonEmployees",
    "SearchBaseDn" : "ou=People,ou=NonEmployees,dc=system,dc=backend",
    "ObjectClasses" : [ "top", "person", "organizationalperson",
                       "inetorgperson", "idUserOrgPerson" ]
}
```

3. Locate the GroupResourceLdapConfig attribute and change the values of it's sub attributes wherever applicable.
 - RDNResourceAttr - LDAP attribute that represents the Resource RDN (ie. cn, uid, etc). This attribute is found as part of the larger distinguished name representing the resource
 - UUIDResourceAttr - LDAP attribute that represents the globally unique identifier of the Resource (ie. entryUUID or uuid)
 - UserMembershipAttr - Multivalued LDAP attribute that represents users who are members (ie. uniquemember)
 - UserMembershipIdAttr - Multivalued LDAP attribute that represents user id who are members (e.g. uniquememberId)
 - SchemaPrefix - Organizational Units that the Resource will be contained within (excluding the BaseDN). Example: ou=nonemployees,ou=Groups
 - SearchBaseDn - Base DN representing the container that resources will be managed within (ie. ou=Groups,dc=system,dc=backend)
 - ObjectClasses - List of object classes that represent the resource object (ordered from general to specific)

Example:

```
"GroupResourceLdapConfig" : {
    "RDNResourceAttr" : "cn",
    "UUIDResourceAttr" : "entryUUID",
    "UserMembershipAttr" : "uniquemember",
    "UserMembershipIdAttr" : "uniquememberId",
```

```

    "SchemaPrefix" : "ou=Groups,ou=NonEmployees",
    "SearchBaseDn" : "ou=Groups,ou=NonEmployees,dc=system,dc=backend",
    "ObjectClasses" : [ "top", "idOrgGroup", "groupOfUniqueNames" ]
}

```

SCIM to LDAP Attribute Mappings

The Account Management service has a default SCIM to LDAP attribute mappings file.

To modify the mappings file, navigate to <NEIS installation folder>\acctmgmt\ folder and modify the ScimToLdapAttributeMappings.xml file as follows.

This SCIM to LDAP attribute mapping file has 3 sections, one for *User* resource, one for *Group* resource and one for default custom attributes. Each attribute mapping entry has SCIM attribute name, it's corresponding LDAP attribute name and mutability.

The mutability defines whether the attribute is read only, write only or both. Valid values for mutability are - `readonly`, `writeonly` and `readwrite`.

- User - This section contains User resource SCIM attributes and corresponding LDAP attribute mappings.
- Group - This section contains Group resource SCIM attributes and corresponding LDAP attribute mappings.
- DefaultCustomAttributes - These attributes are used internally.

Note:

- Please do not modify the SCIM attribute names.
- Please do not add / delete / modify Default Custom Attributes.
- To configure custom attributes, please refer *Custom Attributes* section of the <NEIS installation folder>\docs\NEIS_user_guide.pdf.

Note: Please refer [Connector-specific Guidance](#) on page 9 for connector specific sample ScimToLdapAttributeMappings.xml file.

Non-Employee ID

When a User is created in the system using SCIM 2.0 API *POST* method (/Users), the non-employee id field is generated by default. There are scenarios where this field is not required while creating an user. To disable this feature, please follow the below steps.

Navigate to the <NEIS installation folder>\config\conf folder and modify IdPortal.json file as follows: Locate the NonEmployeeIDConfig attribute and change the values of it's sub attributes as follows.

- Generate Non-Employee ID - Represents whether to generate and assign Non-Employee ID while creating a user.
- Attribute Name - The SCIM attribute name to which non-employee id is assigned.
- Prefix - Prefix of the Employee ID.
- Suffix - Suffix of the Employee ID

Example:

```

"NonEmployeeIDConfig" : {
    "GenerateNonEmployeeId" : true,
    "AttributeName" : "ExternalId",
    "Prefix" : "NE-",
    "Suffix" : "ID"
}

```

Connector-specific Guidance

RACF

Below are RACF connector specific configurations for reference.

LDAP Gateway Details

- **LDAP Server Configurations**

1. Please navigate to <IDF Gateway Installation>/conf folder and open customer-configuration.properties file.
2. Search for RACF connector class definition cnctr.racf.class.
3. Specify the value present for the cnctr.racf.racf1.suffix setting as the BaseDN value in IdPortal.json
4. Specify the value present for the cnctr.racf.racf1.adminUserDN setting as the RootUserDn value in IdPortal.json
5. Specify the value present for the cnctr.racf.racf1.adminUserPassword setting as the RootUserPassword value in IdPortal.json

Example

```
"LdapServerConfig" : {
    "ServerAddress" : "localhost",
    "ServerPort" : 6389,
    "BaseDn" : "dc=racf,dc=com",
    "RootUserDn" : "cn=idfRacfAdmin,dc=racf,dc=com",
    "RootUserPassword" : "CfDJ8DnGfbZY571IlP6QeZriBfw3rtNrr09BS4O"
}
```

- **User Resource LDAP Configurations**

Example

```
"UserResourceLdapConfig" : {
    "RDNResourceAttr" : "uid",
    "UUIDResourceAttr" : "uid",
    "GroupMembershipAttr" : "memberof",
    "GroupMembershipIdAttr" : "groups",
    "EmailAttr" : "wmail",
    "ActiveStateIdentifierAttr" : "revoke",
    "SchemaPrefix" : "ou=People",
    "SearchBaseDn" : "ou=People,dc=racf,dc=com",
    "ObjectClasses" : [ "top", "person", "organizationalperson",
                      "inetorgperson", "idUserPerson" ]
}
```

- **Group Resource LDAP Configurations**

Example

```
"GroupResourceLdapConfig" : {
    "RDNResourceAttr" : "cn",
    "UUIDResourceAttr" : "cn",
    "UserMembershipAttr" : "uniquemember",
    "UserMembershipIdAttr" : "uniqueids",
    "SchemaPrefix" : "ou=Groups",
    "SearchBaseDn" : "ou=Groups,dc=racf,dc=com",
    "ObjectClasses" : [ "top", "idUserGroup", "groupOfUniqueNames" ]
}
```

SCIM to LDAP Attribute Mappings

For SCIM to LDAP attribute mappings for RACF connector, please refer the `ScimToLdapAttributeMappings.xml` file present under `<NEIS installation folder>\doc\samples\connectors\RACF` folder.

Epic Health

Below are Epic Health connector specific configurations for reference.

LDAP Gateway Details

- **LDAP Server Configurations**

1. Please navigate to `<IDF Gateway Installation>/conf` folder and open `customer-configuration.properties` file.
2. Search for Epic Health connector class definition `cnctr.epichealth.class`.
3. Specify the value present for the `cnctr.epichealth.epichealth1.suffix` setting as the `BaseDN` value in `IdPortal.json`.
4. Specify the value present for the `cnctr.epichealth.epichealth1.adminUserDN` setting as the `RootUserDn` value in `IdPortal.json`.
5. Specify the value present for the `cnctr.epichealth.epichealth1.adminUserPassword` setting as the `RootUserPassword` value in `IdPortal.json`.

Example

```
"LdapServerConfig" : {
    "ServerAddress" : "localhost",
    "ServerPort" : 6389,
    "BaseDn" : "dc=epichealth,dc=com",
    "RootUserDn" : "cn=Directory Manager,dc=epichealth,dc=com",
    "RootUserPassword" : "CfDJ8DnGfbZY571IlP6QeZriBfw3rtNrr09BS4O"
}
```

- **User Resource LDAP Configurations**

Example

```
"UserResourceLdapConfig" : {
    "RDNResourceAttr" : "uid",
    "UUIDResourceAttr" : "uid",
    "GroupMembershipAttr" : "memberof",
    "GroupMembershipIdAttr" : "groups",
    "EmailAttr" : "wmail",
    "ActiveStateIdentifierAttr" : "IsActive",
    "SchemaPrefix" : "ou=EpicEmp",
    "SearchBaseDn" : "ou=EpicEmp,dc=epichealth,dc=com",
    "ObjectClasses" : [ "EpicEmp" ]
}
```

- **Group Resource LDAP Configurations**

Example

```
"GroupResourceLdapConfig" : {
    "RDNResourceAttr" : "cn",
    "UUIDResourceAttr" : "cn",
    "UserMembershipAttr" : "uniqueMember",
    "UserMembershipIdAttr" : "uniqueIds",
    "SchemaPrefix" : "ou=EpicEmp",
```

```
        "SearchBaseDn" : "ou=EpicEmp,dc=epichealth,dc=com",
        "ObjectClasses" : [ "EpicEmp" ]
    }
```

SCIM to LDAP Attribute Mappings

For SCIM to LDAP attribute mappings for Epic Health connector, please refer the `ScimToLdapAttributeMappings.xml` file present under `<NEIS installation folder>\doc\samples\connectors\Epic` folder.

