Mainframe Integration Guide

Version: 8.0 Patch 5

Copyright and Trademark Notices

cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Overview

SailPoint Mainframe Integration Modules deliver extended value from standard IdentityIQ deployments. SailPoint is committed to providing design, configuration, troubleshooting and best practice information to deploy and maintain strategic integrations. SailPoint has modified the structure of this document to aid customers and partner deployments. The focus of this document is product configuration and integration. For more details on design, troubleshooting and deployment best practices, refer to the Connector and Integration Deployment Center in Compass, SailPoint's Online customer portal.

This document provides a guide to the integration between the following products and IdentityIQ:

SailPoint IdentityIQ Application Modules

- Mainframe Integration Modules
    - IdentityIQ for RACF Mainframe
    - IdentityIQ for TopSecret Mainframe
    - IdentityIQ for ACF2 Mainframe
    - IdentityIQ for RACF LDAP Mainframe
    - IdentityIQ for TopSecret LDAP Mainframe

The documentation for the following products is on the compass page directly. Direct links to each of the products is provided in the following list.

- IdentityIQ for RACF Mainframe
- IdentityIQ for TopSecret Mainframe
- IdentityIQ for ACF2 Mainframe

This document is intended for the following products and IdentityIQ System Administrators and assumes an advance level of technical knowledge:

IdentityIQ for RACF LDAP Mainframe

IdentityIQ for TopSecret LDAP Mainframe

IdentityIQ for RACF LDAP Mainframe

The following topics are discussed in this chapter:

Overview

The IdentityIQ for RACF LDAP Mainframe mainly uses the LDAP interfaces to communicate with z/OS LDAP server. The IdentityIQ for RACF LDAP Mainframe supports reading and provisioning of RACF LDAP users and entitlements.

Supported Features

IdentityIQ for RACF LDAP Mainframe supports the following features:

Account Management

- Manages RACF LDAP Users as Account
- Aggregate, Refresh Accounts, Partitioning Aggregation
- Create, Update, Delete
- Enable, Disable, Change Password
- Add/Remove Entitlements

Group Management

- Aggregation

For more information on partitioning aggregation, see Defining Search Scope.

Supported Managed Systems

IdentityIQ for RACF LDAP Mainframe supports the following managed systems:

- IBM Tivoli Directory Server for z/OS 2.4 with SDBM LDAP back end
- IBM Tivoli Directory Server for z/OS 2.3 with SDBM LDAP back end
- IBM Tivoli Directory Server for z/OS 2.2 with SDBM LDAP back end

TLS communication between IdentityIQ and RACF LDAP Server

If you want secure TLS connection for RACF LDAP, TLS communication must be enabled between IdentityIQ and RACF LDAP Server. For a Java client to connect using TLS and self-signed certificates, install the certificate into the JVM keystore.

System requirements

- The following respective components for z/OS versions must be installed for TLS communication:

z/OS version	Cryptographic Services	z/OS Security Level 3
z/OS 2.2	System SSL Base: FMID HCPT420	System SSL Security Level: FMID JCPT421
z/OS 2.3	System SSL Base: FMID HCPT430	System SSL Security Level: FMID JCPT431
z/OS 2.4	System SSL Base: FMID HCPT440	System SSL Security Level: FMID JCPT441

- The CSF started task must be active.

Creating TLS communication between IdentityIQ and RACF LDAP Server

To create TLS communication between IdentityIQ and RACF LDAP Server, perform the following:

1. Implement z/OS Secured Communication to RACF LDAP Server.

   For more information on implementing the secured communication to RACF LDAP Server, see Implementing Secured Communication to RACF LDAP Server.

2. Export server CA certificate and copy the exported `.cer` file to the Java client computer (IdentityIQ computer).
3. At the client computer execute the following command from the bin directory of JDK:

   ```
   keytool -importcerts -trustcacert -alias aliasName -file <absolute path of certificate> -keystore <JAVA_HOME>/jre/lib/security/cacerts
   ```

   In the preceding command line, *aliasName* is the name of the alias.

4. Login to IdentityIQ.
5. Create the application for RACF LDAP, use TLS and provide all the required values.
6. Click on **Test Connection** and save the application.

Prerequisites

Ensure that the following prerequisites are satisfied for the directory servers:

- Set the value of the LDAP_COMPAT_FLAGS environment variable to 1

  The SDBM attributes which are in DN format are by default returned in Uppercase format. This causes duplicate entry of entitlement in IdentityIQ due to the difference in the cases of group DN fetched while aggregation and group DN fetched while group membership provisioning operation.

  To avoid the mentioned issue, the `LDAP_COMPAT_FLAGS` environment variable is set to 1 which would return the values for the mentioned attributes in mixed case format that is in the same format as of group DN returned during aggregation.

  The `LDAP_COMPAT_FLAGS` environment variable value can be specified in LDAP server environment variables file. By default, the file name is `/etc/ldap/ds.envvars`.

- RACF restriction on amount of output

When processing certain LDAP search requests, SDBM uses the RACF **R_admin** run command interface to issue RACF search commands. The **R_admin** run command interface limits the number of records in its output to 4096. This means that the RACF search command output might be incomplete if you have many users, groups, connections, or resources.

To avoid the mentioned search limit issue, Partition must defined to retrieve all requested objects. Partitions must be created in such a way that each Partition must not exceed the default or specified search limit. For more information on defining Partitions, see Defining Search Scope.

AdministratorPermissions

The service account configured for IdentityIQ for RACF LDAP Mainframe must have the read/write privileges over the RACF directory information tree in order to manage the RACF data, that is, the administrator user must have SPECIAL attribute to be able to manage all RACF entries. In order to limit the scope of service account, group-SPECIAL user can be created as per the requirement. Administrator user must not be a PROTECTED user that is, administrator user must have password.

Configuration Parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for RACF LDAP Mainframe uses the following configuration parameters:

> Attributes marked with * are mandatory attributes.

RACF LDAP Configuration Parameters

Use TLS

Specifies if the connection is over TLS.

When using 'Use TLS' option for RACF LDAP application, the certificate used must have FQDN of server machine as the subject under CN.

*User**

User to connect as a DN string such as Administrator.

*Password**

Password for the administrator account.

*Port**

Port number through which the server is listening.

*Host**

Host of the LDAP server.

*Connect Profile DN**

Connect Profile type DN used during group membership provisioning.

Provisioning Properties to All Connections

Sets the RACF connection properties defined in Provisioning Policy to all the RACF connections when multiple RACF Groups are requested in single operation.

Account Settings

Search Scope

Depth to search the LDAP tree.

- **Subtree**: A subtree search (or a deep search) includes all child objects as well as the base object. When referrals are followed (by default, Integration Module follow referrals) then the scope will also include child domains of the base object (when it is a parent domain) in a forest.
- **Base**: Limits the search to the base object or named object.
- **One Level**: Search is restricted to the immediate children of a base object, but excludes the base object itself.

*Search DN**

Distinguished name of the container.

Iterate Search Filter

LDAP filter that defines scope for accounts/groups from this container.

Filter String

Used to filter object as they are returned for an underlying application. Derived attributes can also be included in the filter.

Additional Configuration Parameters

racfConnectGroupName

When default group is updated from account, to retain the old default group in **racfConnectGroupName** attribute, add the following attribute in the application debug page:

```
<entry key="dropDefaultGroupConnection">
  <value>
    <Boolean>true</Boolean>
  </value>
</entry>
```

disableLDAPHostnameVerification

To disable hostname verification during LDAP Communication over TLS, configure the following attribute in the application debug page:

```
<entry key="disableLDAPHostnameVerification" value="true"/>
```

Schema Attributes

The application schema is used to configure the objects returned from a Integration Module. When an Integration Module is called, the schema is supplied to the methods on the Integration Module interface. This Integration Module currently supports two types of objects, account and group.

Account Attributes

Account objects are used when building identities Link objects.

dn

Distinguished name by which the user is known.

racfid

ID for an user on RACF.

objectClass

Describes the kind of object which an entry represents. This attribute is present in every entry, with at least two values. One of the value is **top** or **alias**.

racfAttributes

Multi-valued attribute which list keywords that describes more about the user account. For example, racfAttributes can be used to add a RACF user entry with **ADSP GRPACC NOPASSWORD** or modify a RACF user entry with **NOGRPACC SPECIAL NOEXPIRED RESUME NOOMVS**.

racfClassName

Multi-valued attribute used to specify the classes in which the new user is allowed to define profiles to RACF for protection. Classes that can be specified are USER, and any resource classes defined in the class descriptor table.

racfDefaultGroup

Represents the default group associated with the user.

racfConnectGroupName

List of groups of which this person is a member.

Example: “Sales” or “Engineering”

racfLastAccess

Information about last date-time user logged in to system.

racfProgrammerName

Users name associated with the user ID.

racfPasswordChangeDate

Last date the user changed his password.

racfPasswordInterval

Number of days during which a user's password and password phrase (if set) remain valid.

racfHavePasswordEnvelope

Information whether users password is enveloped.

racfPassPhraseChangeDate

Last date the user changed his password phrase.

racfHavePassPhraseEnvelope

Information whether users password phrase is enveloped.

racfResumeDate

Starting date when user will be allowed to access the system again.

racfRevokeDate

Starting date when user will be disallowed to access the system.

racfSecurityLabel

Users default security label.

racfSecrityLevel

Users default security level.

racfSecurityCategoryList

Multi-valued attribute contains one or more names of installation-defined security categories.

racfLogonDays

A multi-valued attribute which specifies the days of the week when the user is allowed to access the system from a terminal.

racfLogonTime

Hours in the day when the user is allowed to access the system from a terminal.

racfAuthorizationDate

Date when user was defined to RACF system.

racfInstallationData

Installation data associated the user.

racfDatasetModel

Discrete data set profile name that is used as a model when new data set profiles are created that have userid as the high-level qualifier.

racfOwner

Distinguished name of the owner of the user.

racfOperatorClass

Multi-valued attribute contains classes assigned to this operator to which BMS (basic mapping support) messages are to be routed - CICS segment.

racfOperatorIdentification

Operator ID for use by BMS - CICS segment.

racfOperatorPriority

Number from 0 - 255 that represents the priority of the operator - CICS segment.

racfTerminalTimeout

Time, in hours and minutes, that the operator is allowed to be idle before being signed off - CICS segment.

racfOperatorReSignon

Specifies whether the user is signed off by CICS when an XRF takeover occurs - CICS segment.

SAFAccountNumber

Users default TSO account number when logging on through the TSO/E logon panel - TSO segment.

SAFDefaultCommand

Specifies the command run during TSO logon - TSO segment.

SAFDestination

Specifies the default destination to which the system routes dynamically-allocated SYSOUT data sets - TSO segment.

SAFHoldClass

Specifies the users default hold class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.

SAFJobClass

Specifies the users default job class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.

SAFMessageClass

Specifies the users default message class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.

SAFTsoSecurityLabel

Specifies the users Security label entered or used during TSO LOGON - TSO segment.

SAFDefaultSysoutClass

Specifies the users default SYSOUT class - TSO segment.

SAFDefaultUnit

Specifies the default name of a device or group of devices that a procedure uses for allocations - TSO segment.

SAFDefaultLoginProc

Specifies the name of the users default logon procedure when logging on through the TSO/E logon panel - TSO segment.

SAFLogonSize

Specifies the default or requested region size during TSO logon - TSO segment.

SAFMaximumRegionSize

Specifies the maximum region size the user can request at logon - TSO segment.

SAFUserdata

Specifies the optional installation data defined for the user. The specified value must be 4 EBCDIC characters. Valid characters are 0 - 9 and A - F - TSO segment

Group Attributes

The group schema is used when building AccountGroup objects which are used to hold entitlements shared across identities.

dn

Distinguished name by which the Group is known.

racfid

ID for group on RACF.

objectClass

The values of the objectClass attribute describe the kind of object which an entry represents. The objectClass attribute is present in every entry, with at least two values. One of the values is either “top” or “alias”.

racfAuthorizationDate

Date when group was defined to RACF system.

racfInstallationData

Installation data associated the group.

racfOwner

Distinguished names of objects that have ownership responsibility for the object that is owned.

racfGroupNoTermUAC

Specifies that during terminal authorization checking, RACF is to allow the use of the universal access authority for a terminal when it checks whether a user in the group is authorized to access a terminal.

racfSuperiorGroup

Distinguished name of the superior group of the associated group.

racfSubGroupName

Distinguished name of the groups to which the associated group is superior group.

racfGroupUniversal

Specifies that this is a universal group that allows an effectively unlimited number of users to be connected to it for the purpose of resource access.

racfGroupUserids

Distinguished names of the users which are member of the group.

racfDatasetModel

Discrete data set profile name that is used as a model when new data set profiles are created that have group name as the high-level qualifier.

Provisioning Policy Attributes

The following table lists the provisioning policy attributes for create and update Account:

> The attributes with * are required attributes.

Create Account

*dn**

Distinguished name of the user to be created.

*password**

Password of the user to be created.

racfDefaultGroup

Default group of the user to be created. Value for this field will be the DN of the group.

racfOwner

The owner of the user to be created. Value for this field will be the DN of the group or user.

connection_racfconnectowner

Distinguished name of the connection owner.

connection_racfConnectRevokeDate

Connection Revoke Date. For example, mm/dd/yy

Update Account

connection_racfconnectowner

Distinguished name of the connection owner.

connection_racfConnectRevokeDate

Connection Revoke Date. For example, mm/dd/yy

Additional Information

This section describes the additional information related to the IdentityIQ for RACF LDAP Mainframe.

Support for PassPhrase

IdentityIQ for RACF LDAP Mainframe supports PassPhrase feature as follows:

For password change operation on RACF managed system, `racfPassword` or `racfPassPhrase` is supported. If the length of password provided is less than or equal to 8 characters then password attribute used would be `racfPassword` and if the length of password provided is greater than 8 characters then password attribute used would be `racfPassPhrase`.

Support for Connection Attributes

IdentityIQ for RACF LDAP Mainframe supports provisioning of **racfConnectionOwner** and **racfConnectRevokeDate** while provisioning entitlements. For a single entitlement request along with connection attribute values, the values of the attributes are assigned to the connection.

Provision Properties to All Connections: Select to provision same set of connection attributes values to all requested entitlements.

Implementing Secured Communication to RACF LDAP Server

Secured communication to RACF LDAP Server must be implemented using one of the following methods:

- **LDAP TLS**: Communication must be implemented on a port defined to LDAP as secured (ldaps).

  For more information, see Implementing LDAP TLS.

- **AT-TLS policy**: Communication must be implemented on a port defined to LDAP as non-secured (ldap). The TLS processing is done by TCPIP and is transparent to RACF LDAP Server.

  For more information, see Implementing AT-TLS policy for RACF LDAP communication.

The secured communication is implemented using server authentication.

Common implementation procedure

1. A valid server certificate with its associated server private key must be defined. This certificate must be signed by a trusted Certificate Authority's (CA).
2. The server certificate and the CA certificate must be connected to a key ring.
3. The CA certificate must be exported to a file, transferred (using FTP with ASCII mode) to the client and installed there to be used for certificate verification by the TLS handshake process.

> For testing purposes, a local CA can be defined for signing the server certificate.

Implementing LDAP TLS

For detailed information about implementing LDAP TLS, see “Setting up for SSL/TLS” chapter of *z/OS IBM Tivoli Directory Server Administration and Use for z/OS* IBM manual.

> RACF LDAP server must be granted with permission to access the key ring containing the RACF LDAP server certificate and the CA certificate.

Implementing AT-TLS policy for RACF LDAP communication

For detailed information about implementing AT-TLS policy, see “Application Transparent Transport Layer Security data protection” chapter of *z/OS Communications Server IP Configuration Guide*.

The required policy attributes for AT-TLS policy are:

- Local Port Range – ports defined in LDAP as non-secured
- Direction = Inbound
- TLS Enabled = On
- TLS v1.1 = On
- TLS v1.2 = On
- TLS v1.3 = On
- Handshake Role = Server
- Client Authorization Type = PassThru
- Application Controlled = Off
- Secondary Map = Off
- The name of the certificate created for the secured communication and the name of the key ring to which the server certificate and the CA certificate are connected, should be specified.

> TCPIP must be granted permission to access the key ring to which the RACF LDAP server certificate and the CA certificate are connected.

> When generating certificates in RACF, users must note that TLS v1.3 requires a minimal RSA key size of 2048 bit.

Sample file for AT-TLS policy

```
# RULE for LDAP GLDSRV
############################################################
TTLSRule LDAP
{
  LocalAddr ALL
```

```
  RemoteAddr ALL
  LocalPortRange 389
  Direction Inbound
  Priority 255 # highest priority rule
  Userid GLDSRV
  TTLSGroupActionRef GrpAct_LDAP
  TTLSEnvironmentActionRef GrpEnv_LDAP
  TTLSConnectionActionRef GrpCon_LDAP
}

TTLSGroupAction GrpAct_LDAP
{
  TTLSEnabled On
  Trace 7
}

TTLSEnvironmentAction GrpEnv_LDAP
{
  Trace 7
  HandshakeRole Server
  EnvironmentUserInstance 0
  TTLSKeyringParmsRef PrmKeyRing_LDAP
  TTLSEnvironmentAdvancedParmsRef PrmEnvAdv_LDAP
}

TTLSEnvironmentAdvancedParms PrmEnvAdv_LDAP
{
  TLSv1.1 On
  TLSv1.2 On
  TLSv1.3 On
  ClientAuthType PassThru
}

TTLSConnectionAction GrpCon_LDAP
{
  HandshakeRole Server
  TTLSCipherParmsRef PrmCipher_LDAP
  TTLSConnectionAdvancedParmsRef PrmConAdv_LDAP
  CtraceClearText Off
  Trace 7
}
TTLSConnectionAdvancedParms PrmConAdv_LDAP
{
  ApplicationControlled Off
  CertificateLabel GLDSRV
  SecondaryMap Off
}
TTLSCipherParms PrmCipher_LDAP
{
# supported cipher suites - we used a wide list, that should be
decreased according # to specific needs
V3CipherSuites      TLS_DH_DSS_WITH_DES_CBC_SHA
V3CipherSuites      TLS_DH_RSA_WITH_DES_CBC_SHA
V3CipherSuites      TLS_NULL_WITH_NULL_NULL
```

```
V3CipherSuites       TLS_RSA_WITH_NULL_MD5
V3CipherSuites       TLS_RSA_WITH_NULL_SHA
V3CipherSuites       TLS_RSA_EXPORT_WITH_RC4_40_MD5
V3CipherSuites       TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
V3CipherSuites       TLS_RSA_WITH_DES_CBC_SHA
V3CipherSuites       TLS_DHE_DSS_WITH_DES_CBC_SHA
V3CipherSuites       TLS_DHE_RSA_WITH_DES_CBC_SHA
V3CipherSuites        TLS_RSA_WITH_AES_256_CBC_SHA256
V3CipherSuites        TLS_RSA_WITH_AES_256_CBC_SHA
V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_DHE_DSS_WITH_AES_128_CBC_SHA
V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
V3CipherSuites        TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites        TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites        TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites        TLS_AES_256_GCM_SHA384
V3CipherSuites        TLS_AES_128_GCM_SHA256
V3CipherSuites        TLS_CHACHA20_POLY1305_SHA256
}
TTLSKeyringParms PrmKeyRing_LDAP
{
  Keyring GLDRING
}
```

Defining Search Scope

> IdentityIQ for RACF LDAP Mainframe supports Partitioning Aggregation feature to enable faster retrieval of RACF data. In order to define search scope, enabling Partitioning Aggregation on aggregation task is not required.

In IdentityIQ for RACF LDAP Mainframe, objects can be retrieved by means of a **searchDN**, **searchFilter** and **searchScope**. IdentityIQ for RACF LDAP Mainframe partition entries are the application configuration searchDNs list with each entry of the list treated as a single partition.

Typically, the partitions can be defined as the searchDNs list as follows:

```
<entry key="searchDNs">
    <value>
      <List>
        <Map>
          <entry key="iterateSearchFilter" value="(racfid=a*)"/>
          <entry key="searchDN" value="profiletype=USER,cn=SDBM"/>
          <entry key="searchScope" value="SUBTREE"/>
        </Map>
        <Map>
          <entry key="iterateSearchFilter" value="(racfid=b*)"/>
          <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
          <entry key="searchScope" value="SUBTREE"/>
        </Map>
        <Map>
          <entry key="iterateSearchFilter" value="(racfid=c*)"/>
          <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
          <entry key="searchScope" value="ONELEVEL_SCOPE"/>
        </Map>
        <Map>
          <entry key="iterateSearchFilter" value="(racfid=d*)"/>
          <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
          <entry key="searchScope" value="SUBTREE"/>
        </Map>
……..
….. 
….. 
……
        <Map>
          <entry key="iterateSearchFilter" value="(racfid=z*)"/>
          <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
          <entry key="searchScope" value="SUBTREE"/>
        </Map>
       </List>
     </value>
       </entry>
```

Each specified partition has to be unique by way of the iterateSearchFilter value. If not, the first partition would get aggregated skipping the subsequent duplicate ones.

Partitions must be created in such a way that each partition must not exceed the default or specified search limit.

Troubleshooting

1 - When setting password/passphrase with 9 - 13 characters an error message is displayed

When setting password/passphrase with 9 - 13 characters, the following error message is displayed:

```
Invalid Password
```

Resolution: Passphrase can be 9 - 100 characters if `KDFAES` or `ICHPWX11` encryption algorithm is present on the server. If `KDFAES` or `ICHPWX11` encryption algorithm is not present on the server then the allowed number of characters for passphrase are 14 - 100.

2 - Change Password operation fails with an error

When performing a self change password operation for an account and if any one of the connection is revoked, the following error message is displayed:

```
[LDAP:error code 1 - R000208 Unexpected racroute error safRC=8 racfRC=36
racfReason=0(srv_authenticate_native_passsword:3567)]
```

Resolution: For change password operation, connections of the accounts must not be revoked.

3 - Create account request fails with an error

When create account request has multiple groups and default group is not mentioned then create account request would fail with the following error message:

```
Failed to create account. Specifying default group is mandatory when more than
one groups are requested.
```

Resolution: Ensure that the default group is specified. If Owner of the user account is not specified then default group of the user would be the owner of the user account.

4 - Error message appears for connection failure

For connection failure while performing any operation the following error message appears:

```
[ConnectionFailedException] [Possible suggestions] a) Make sure there is a smooth
connectivity between Identity Server and host. b) Ensure the host/end system is
up and running. [Error details] Failed to connect to server: simple bind failed:
<ip address>:<port>"
```

Resolution: Add the following entry in the **catalina.bat** (Tomcat) file and restart the application server.

```
set JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
```

IdentityIQ for TopSecret LDAP Mainframe

The following topics are discussed in this chapter:

Overview

The IdentityIQ for TopSecret LDAP Mainframe mainly uses the LDAP interfaces to communicate with CA LDAP server. The IdentityIQ for TopSecret LDAP Mainframe supports reading and provisioning of Top Secret LDAP users and entitlements.

Supported Features

IdentityIQ for TopSecret LDAP Mainframe supports the following features:

Account Management

- Manages Top Secret LDAP Users as Account
- Aggregate, Refresh Accounts, Partitioning Aggregation
- Create, Update
- Enable, Disable, Unlock, Change Password
- Add/Remove Entitlements

Group Management

- Aggregation

For more information on partitioning aggregation, see Partitioning Aggregation.

Supported Managed Systems

IdentityIQ for TopSecret LDAP Mainframe supports the following managed system:

- CA LDAP Server for z/OS Release 15.1.00 with CATSS_UTF back end

TLS communication between IdentityIQ and Top Secret LDAP Server

If you want secure TLS connection for Top Secret LDAP, TLS communication must be enabled between IdentityIQ and Top Secret LDAP Server. For a Java client to connect using TLS and self-signed certificates, install the certificate into the JVM keystore.

System requirements

- The following respective components for z/OS versions must be installed for TLS communication:

z/OS version	Cryptographic Services	z/OS Security Level 3
z/OS 2.2	System SSL Base: FMID HCPT420	System SSL Security Level: FMID JCPT421
z/OS 2.3	System SSL Base: FMID HCPT430	System SSL Security Level: FMID JCPT431
z/OS 2.4	System SSL Base: FMID HCPT440	System SSL Security Level: FMID JCPT441

Creating TLS communication between IdentityIQ and Top Secret LDAP Server

To create TLS communication between IdentityIQ and Top Secret LDAP Server, perform the following:

1. Implement z/OS Secured Communication to Top Secret LDAP Server.

   For more information on implementing the secured communication to Top Secret LDAP, see Implementing Secured Communication to Top Secret LDAP Server.

2. Export server CA certificate and copy the exported `.cer` file to the Java client computer (IdentityIQ computer).

3. At the client computer execute the following command from the bin directory of JDK:

   ```
   keytool -importcerts -trustcacert -alias aliasName -file <absolute path of certificate> -keystore <JAVA_HOME>/jre/lib/security/cacerts
   ```

   In the preceding command line, *aliasName* is the name of the alias.

4. Login to IdentityIQ.

5. Create the application for Top Secret LDAP, use TLS and provide all the required values.

6. Click on **Test Connection** and save the application.

Administrator Permissions

The service account configured for IdentityIQ for TopSecret LDAP Mainframe must have the read/write privileges over the Top Secret directory information tree in order to manage the Top Secret data.

Configuration Parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for TopSecret LDAP Mainframe uses the following configuration parameters:

> Attributes with * are mandatory attributes.

Host*

Host of the LDAP server.

Port*

Port number through which the server is listening.

Use TLS

Specifies if the connection is over TLS.

When using 'Use TLS' option for Top Secret LDAP application, the certificate used must have FQDN of server machine as the subject under CN.

User*

User to connect as a DN string such as Administrator.

Password

Password for the administrator account.

Suffix*

Distinguished name of the container.

Account Filter

LDAP filter that defines scope for accounts from this container.

Additional Configuration Parameter

on

disableLDAPHostnameVerification

To disable hostname verification during LDAP Communication over TLS, configure the following attribute in the application debug page:

```
<entry key="disableLDAPHostnameVerification" value="true"/>
```

Schema Attributes

The application schema is used to configure the objects returned from a Integration Module. When an Integration Module is called, the schema is supplied to the methods on the Integration Module interface. This Integration Module currently supports three types of objects account, TopSecretProfile and TopSecretGroup.

Account Attributes

Account objects are used when building identities Link objects.

dn

Distinguished name of the Top Secret User.

ACCESSORID

Top Secret User ID.

objectClass

Top Secret User Object Classes.

AACID

Authority levels at which ACID can manage ACIDs within scope.

AdminListData

Authority to list Security File information

Misc1

Authority to perform one or more administrative functions (LCF, INSTDATA, USER, LTIME, SUSPEND, NOATS, RDT, TSSSIM, ALL)

Misc2

Authority to perform one or more administrative functions (ALL, SMS, TSO, NDT, DLF, APPCLU, WOR)

Misc3

Authority to perform one or more administrative functions (ALL, SDT, PTOK)

Misc8

Authority to list the contents of the RDT, FDT or STC or to use the ASUSPEND administrative function (LISTRDT, LISTSTC, LISTAPLU, LISTSDT, MCS, NOMVSDF, PWMAINT, REMASUSP, ALL)

Misc9

Authority to perform one or more high-level administrative functions (BYPASS, TRACE, CONSOLE, MASTFAC, MODE, STC, GLOBAL, GENERIC, ALL)

ASUSPEND

Account is suspended due to administrator action.

NODSNCHK

CA Top Secret bypasses all data set access security checks for this ACID.

SITRAN

CICS transaction CA Top Secret automatically executes after an ACID successfully signs on to a facility.

OPCLASS

CICS operator classes.

OPIDENT

CICS operator identification value equal to the ACID OPIDENT entry in the CICS SNT (Signon Table).

OPPRTY

CICS operator priority of associated ACID.

SCTYKEY

CICS security keys an ACID may use.

CONSOLE

Ability to modify control options by ACID.

CREATED

Date ACID was created.

DEPT

Department ACID.

DIVISION

Division ACID.

EXPIRE

Expiration date of ACID.

GROUPS

List of Groups a TSS User is a member.

XSUSPEND

Account is suspended due to CA-Top Secret Installation exit.

LAST-COUNT

Number of times the ACID has been used (logon times since user was defined).

MASTFAC

Multi-user facility name.

MCSAUTH

Authorize the operator commands that can be entered from the console.

PROFILES

List of Profiles a Top Secret User is a member.

MODIFIED

Last date and time when ACID was updated.

NAME

Name of ACID.

NOPWCHG

Prevent ACID from changing passwords at signon or initiation.

OIDCARD

Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.

DFLTGRP

Default group to an ACID operating under OpenEdition MVS.

HOME

Subdirectory of ACID under OMVS.

UID

Numeric UID value for security within USS.

PSUSPEND

Account is suspended due to password violation.

PHYSKEY

Physical security key to support external authentication devices.

TSOHCLASS

Default hold class for TSO-generated JCL for TSO users.

TSOJCLASS

Job class for TSO generated job cards from TSO users.

TSOLACCT

TSO Default account number.

TSOCOMMAND

Default command issued at TSO logon.

TSOLPROC

Default procedure used for TSO logon.

TSOMSIZE

Maximum region size (in kilobytes) that a TSO user may specify at logon.

TSOMCLASS

Default message class for TSO generated JCL for TSO users.

TSOMPW

Support multiple TSO UADS passwords, on a user-by-user basis.

TSOOPT

Default options that a TSO user may specify at logon

TSODEST

Default destination identifier for TSO generated JCL for TSO users.

TSODEFPRFG

Default TSO performance group.

TSOLSIZE

Default region size (in kilobytes) for TSO.

TSOSCLASS

Default SYSOUT class for TSO generated JCL for TSO users.

TSOUNIT

Default unit name for dynamic allocations under TSO.

TSOUDATA

Site-defined data field to a TSO user.

USER

User defined classes and resources.

PASSEXPD

Expiration date of password.

PASSINTV

Number of days during which password remains valid.

TYPE

ACID type (MSCA,LSCA,SCA,ZCA,VCA,MCA,USER).

VSUSPEND

Account is suspended due to access violation.

ZONE

Zone ACID.

TopSecretProfile Attributes

The following table lists the profile attributes.

dn

Distinguished name of Top Secret Profile.

ACCESSORID

Top Secret Profile Id.

objectClass

Top Secret Profile Object Classes.

AUDIT

Allow an audit of ACID activity.

CREATED

Date ACID was created.

DEPT

DEPT ACID.

DIVISION

Division ACID.

GAP

Globally administered profile.

MODIFIED

Last date and time when ACID was updated.

NAME

Name of ACID.

NOPWCHG

Prevent ACID from changing passwords at signon or initiation.

OIDCARD

Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.

GID

Group identification for OMVS.

SOURCE

Source reader or terminal prefixes through which the associated ACID may enter the system.

LTIME

How long (in minutes) until terminal of ACID locks if CA Top Secret does not detect activity at that terminal.

TYPE

ACID type.

ZONE

Zone ACID.

TopSecretGroup Attributes

The following table lists the group attributes.

dn

Distinguished name of Top Secret Profile.

ACCESSORID

Top Secret Group Id.

objectClass

Top Secret Group Object Classes.

AUDIT

Allow an audit of ACID activity.

CREATED

Date ACID was created.

DEPT

DEPT ACID.

DIVISION

Division ACID.

GAP

Globally administered profile.

MODIFIED

Last date and time when ACID was updated.

NAME

Name of ACID.

NOPWCHG

Prevent ACID from changing passwords at signon or initiation.

OIDCARD

Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.

GID

Group identification for OMVS.

SOURCE

Source reader or terminal prefixes through which the associated ACID may enter the system.

LTIME

How long (in minutes) until terminal of ACID locks if CA Top Secret does not detect activity at that terminal.

TYPE

ACID type.

ZONE

Zone ACID.

Provisioning Policy Attributes

The following table lists the provisioning policy attributes for create Account:

> The attributes with * are required attributes.

USER DN*

Distinguished name of the user to be created.

Password*

Password of the user to be created.

Full Name*

Name of the Top Secret user to be created

Department*

DEPT of which the user would be a part.

Facilities

Permit an ACID to have access to a resource through the specified facility.

TSOLPROC

Default procedure used for TSO logon.

CONSOLE

Ability to modify control options by ACID.

Additional Information

This section describes the additional information related to the IdentityIQ for TopSecret LDAP Mainframe.

Support for PassPhrase

IdentityIQ for TopSecret LDAP Mainframe supports PassPhrase feature as follows:

For password change operation on TopSecret LDAP Mainframe managed system, `userPassword` or `PassPhrase` is supported. If the length of password provided is less than or equal to 8 characters then password attribute used would be `userPassword` and if the length of password provided is greater than 8 characters then password attribute used would be `PassPhrase`. To support self change password or passphrase on Top Secret, then appropriate logon option must be specified that is., only password or only passphrase or both.

Implementing Secured Communication to Top Secret LDAP Server

Secured communication to Top Secret LDAP Server must be implemented using one of the following methods:

- **LDAP SSL**: Communication must be implemented on a port defined to LDAP as secured (ldaps).

  For more information, see Implementing LDAP TLS.

- **AT-TLS policy**: Communication must be implemented on a port defined to LDAP as non-secured (ldap). The TLS processing is done by TCPIP and is transparent to Top Secret LDAP Server.

  For more information, see Implementing AT-TLS policy for Top Secret LDAP communication.

The secured communication is implemented using server authentication.

Common implementation procedure

- A valid server certificate with its associated server private key must be defined. This certificate must be signed by a trusted Certificate Authority's (CA).
- The server certificate and the CA certificate must be connected to a key ring.
- The CA certificate must be exported to a file, transferred (using FTP with ASCII mode) to the client and installed there to be used for certificate verification by the TLS handshake process.

> For testing purposes, a local CA can be defined for signing the server certificate.

Implementing LDAP TLS

For detailed information about implementing LDAP TLS, see *CA LDAP Server for z/OS Product Guide*.

Top Secret LDAP Server must be granted with permission to access the key ring containing the Top Secret LDAP Server certificate and the CA certificate.

Implementing AT-TLS policy for Top Secret LDAP communication

For detailed information about implementing AT-TLS policy, see “Application Transparent Transport Layer Security data protection” chapter of *z/OS Communications Server IP Configuration Guide*.

The required policy attributes for AT-TLS policy are:

- Local Port Range – ports defined in LDAP as non-secured
- Direction = Inbound
- TLS Enabled = On
- TLS v1.1 = On
- TLS v1.2 = On
- TLS v1.3 = On
- Handshake Role = Server
- Client Authorization Type = PassThru
- Application Controlled = Off
- Secondary Map = Off
- The name of the certificate created for the secured communication and the name of the key ring to which the server certificate and the CA certificate are connected, should be specified.

TCPIP must be granted permission to access the key ring to which the Top Secret LDAP Server certificate and the CA certificate are connected.

When generating certificates in LDAP, users must note that TLS v1.3 requires a minimal RSA key size of 2048 bit.

Sample file for AT-TLS policy

Sample file for AT-TLS policy

```
# RULE for LDAP GLDSRV
#######################################################
TTLSRule LDAP
{
  LocalAddr ALL
  RemoteAddr ALL
  LocalPortRange 389
  Direction Inbound
  Priority 255 # highest priority rule
  Userid GLDSRV
```

```
  TTLSGroupActionRef GrpAct_LDAP
  TTLSEnvironmentActionRef GrpEnv_LDAP
  TTLSConnectionActionRef GrpCon_LDAP
}

TTLSGroupAction GrpAct_LDAP
{
  TTLSEnabled On
  Trace 7
}

TTLSEnvironmentAction GrpEnv_LDAP
{
  Trace 7
  HandshakeRole Server
  EnvironmentUserInstance 0
  TTLSKeyringParmsRef PrmKeyRing_LDAP
  TTLSEnvironmentAdvancedParmsRef PrmEnvAdv_LDAP
}

TTLSEnvironmentAdvancedParms PrmEnvAdv_LDAP
{
  TLSv1.1 On
  TLSv1.2 On
  TLSv1.3 On
  ClientAuthType PassThru
}

TTLSConnectionAction GrpCon_LDAP
{
  HandshakeRole Server
  TTLSCipherParmsRef PrmCipher_LDAP
  TTLSConnectionAdvancedParmsRef PrmConAdv_LDAP
  CtraceClearText Off
  Trace 7
}
TTLSConnectionAdvancedParms PrmConAdv_LDAP
{
  ApplicationControlled Off
  CertificateLabel GLDSRV
  SecondaryMap Off
}
TTLSCipherParms PrmCipher_LDAP
{
# supported cipher suites - we used a wide list, that should be
decreased according # to specific needs
V3CipherSuites      TLS_DH_DSS_WITH_DES_CBC_SHA
V3CipherSuites      TLS_DH_RSA_WITH_DES_CBC_SHA
V3CipherSuites      TLS_NULL_WITH_NULL_NULL
V3CipherSuites      TLS_RSA_WITH_NULL_MD5
V3CipherSuites      TLS_RSA_WITH_NULL_SHA
V3CipherSuites      TLS_RSA_EXPORT_WITH_RC4_40_MD5
V3CipherSuites      TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
V3CipherSuites      TLS_RSA_WITH_DES_CBC_SHA
```

```
V3CipherSuites      TLS_DHE_DSS_WITH_DES_CBC_SHA
V3CipherSuites      TLS_DHE_RSA_WITH_DES_CBC_SHA
V3CipherSuites       TLS_RSA_WITH_AES_256_CBC_SHA256
V3CipherSuites       TLS_RSA_WITH_AES_256_CBC_SHA
V3CipherSuites       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
V3CipherSuites       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_DHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_DHE_DSS_WITH_AES_128_CBC_SHA
V3CipherSuites       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
V3CipherSuites       TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites       TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites       TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites       TLS_AES_256_GCM_SHA384
V3CipherSuites       TLS_AES_128_GCM_SHA256
V3CipherSuites       TLS_CHACHA20_POLY1305_SHA256
}
TTLSKeyringParms PrmKeyRing_LDAP
{
  Keyring GLDRING
}
Partitioning Aggregation
IdentityIQ for TopSecret LDAP Mainframe supports Partitioning Aggregation feature
to enable faster retrieval of Top Secret data.
In IdentityIQ for TopSecret LDAP Mainframe, objects can be retrieved by means
of a searchDN and searchFilter. IdentityIQ for TopSecret LDAP Mainframe partition
entries are the application configuration searchDNs list with each entry of the
list treated as a single partition.
Typically, the partitions can be defined as the searchDNs list as follows:
<entry key="searchDNs">
  <value>
     <List>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=a*)"/>
           <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us"/>
       </Map>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=b*)"/>
```

```
            <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
        </Map>
        <Map>
            <entry key="iterateSearchFilter" value="(tssacid=c*)"/>
            <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
        </Map>
        <Map>
            <entry key="iterateSearchFilter" value="(tssacid=d*)"/>
            <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
        </Map>
            ……..
            ….
            ….
            ……
        <Map>
            <entry key="iterateSearchFilter" value="(tssacid=z*)"/>
            <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
        </Map>
      </List>
   </value>
</entry>
```

Partitioning Aggregation

IdentityIQ for TopSecret LDAP Mainframe supports Partitioning Aggregation feature to enable faster retrieval of Top Secret data.

In IdentityIQ for TopSecret LDAP Mainframe, objects can be retrieved by means of a **searchDN** and **searchFilter**. IdentityIQ for TopSecret LDAP Mainframe partition entries are the application configuration searchDNs list with each entry of the list treated as a single partition.

Typically, the partitions can be defined as the searchDNs list as follows:

```
<entry key="searchDNs">
  <value>
     <List>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=a*)"/>
           <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us"/>
       </Map>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=b*)"/>
           <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
       </Map>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=c*)"/>
           <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
       </Map>
       <Map>
           <entry key="iterateSearchFilter" value="(tssacid=d*)"/>
           <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
       </Map>
```

```
            ……..
            ….
            ….
            ……
        <Map>
            <entry key="iterateSearchFilter" value="(tssacid=z*)"/>
            <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us "/>
        </Map>
      </List>
  </value>
</entry>
```