SailPoint Quick Reference Guide for Gateway Connectors

Version 6.4

Table of Contents

About this guide

This document provides the necessary installation and configuration steps with which to configure the Gateway Connectors as an individual application within IdentityIQ for compliance and provisioning activities.

> Note: **Gateway Connectors (Agents) residing on mainframe security systems communicate with IdentityIQ through the Connector Gateway.**

Gateway Connector Licensing

Customers who licensed IdentityIQ on or after July 15, 2013 are entitled to all IdentityIQ connectors for aggregation, provisioning and password management use cases.

Customers who licensed IdentityIQ before July 15, 2013 are entitled to use connectors for reading data (aggregation). However, entitlement to provisioning and password management functionality through the IdentityIQ connectors (whether Direct, Gateway or Agent based) requires the purchase of the SailPoint Provisioning Engine.

Related documentation

In addition to this book, you can find useful information in the publications listed in the following table. These publications are available on request from SailPoint IdentityIQ.

The following related publications supplement this book:

Document	Description
SailPoint IdentityIQ Installation Guide	Provides detailed information about the installation, deployement and configuration of IdentityIQ.
SailPoint IdentityIQ Administration Guide	Provides detailed information about Configuration, Provisioning, System Administration, and Password Management.
SailPoint Integration Guide	Provides detailed information about Provisioning Integration, Service Desk Integration and Resource Connectors.
SailPoint IdentityIQ Provisioning Connector Administration Guide	Provides the necessary installation and configuration steps to successfully configure Connectors and Connector Managers an application in SailPoint IdentityIQ for compliance and provisioning activities.

Related documentation

Chapter 1: Overview

The following topics are discussed in this chapter:

What is SailPoint IdentityIQ?

SailPoint IdentityIQ is unique and comprehensive Identity Governance solution that addresses the digital security concerns of today's global enterprises. The product provides automated analysis, monitoring and management of risk associated with access to critical or sensitive applications and data via centralized visibility to and control of identity data across the enterprise. Through the use of patent-pending technologies and annalistic, IdentityIQ improves security, lowers the cost of operations, and improves an organization's ability to meet compliance and governance demands.

SailPoint IdentityIQ is a business-oriented identity governance solution that delivers risk-aware compliance management, adaptive role management, access request management, and identity intelligence. Some of the world's largest organizations are using IdentityIQ to improve security, minimize risk and streamline their compliance efforts.

IdentityIQ minimizes the access burden placed on IT staff by empowering end users across the organization to request and manage their own access.

Organizations strive for better visibility into potential risk factors across their business. With Identity Intelligence from IdentityIQ, organizations can transform technical identity data scattered across multiple enterprise systems into centralized, easily understood and business-relevant information. The visibility and insights offered by IdentityIQ through dashboards, risk metrics and reporting provide a clear understanding of identity and access information and help to pro actively manage and focus compliance efforts strategically across even the most complex enterprise environments.

SailPoint IdentityIQ components

SailPoint IdentityIQ includes the core components illustrated in Figure 1—SailPoint IdentityIQ components.
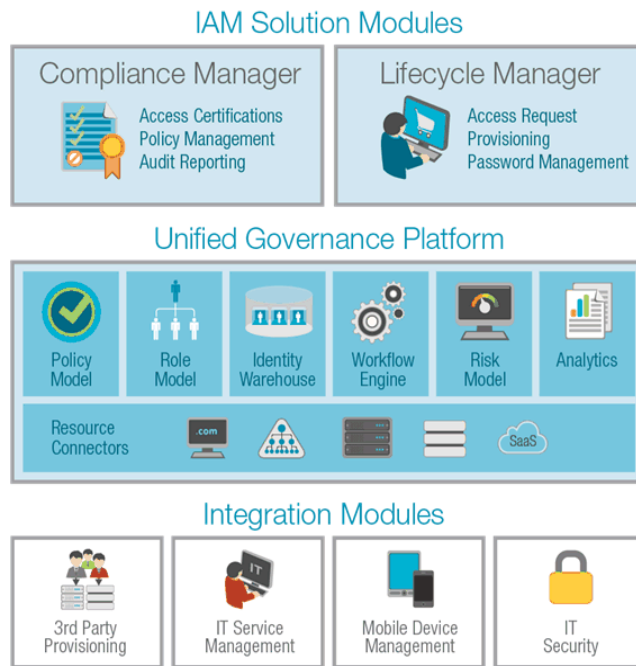
Figure 1—SailPoint IdentityIQ components

Together, these components provide a unique and comprehensive identity governance solution. The components are:

- IAM Solution Modules: The IAM Solution Modules consists of the following modules:

  - **Compliance Manager**: IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework. This allows you to streamline compliance processes and improve the effectiveness of identity governance-all while lowering costs.

  - **Lifecycle Manager**: IdentityIQ Lifecycle Manager manages changes to access through user-friendly self-service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

- **Unified Governance Platform**: IdentityIQ's Governance Platform lays the foundation for effective IAM within the enterprise. It establishes a single framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources. The Governance Platform also offers extensible analytics that transforms disparate, technical identity data into relevant business information. Additionally, robust resource connectivity is provided that allows organizations to directly connect to applications running in the datacenter or in the cloud.

  A unified governance platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications-in the datacenter and the cloud. SailPoint IdentityIQ applies consistent governance across compliance, provisioning and access management processes, maximizing investment and eliminating the need to buy and integrate multiple products.

- **Integration Modules**: The Integration Modules consists of the following modules:

  - 3rd Party Provisioning

  - IT Service Management

  - Mobile Device Management

  - IT Security

IdentityIQ Agent architecture

The Agent architecture diagram:
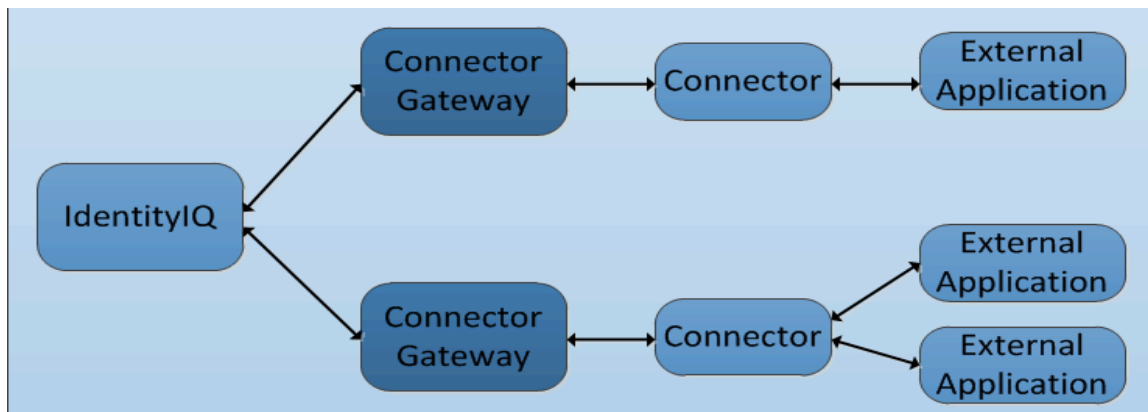
The Connector (Gateway Connectors) as shown in the above figure executes the requests (Aggregation, Provisioning Entitlements and Role Assignments, and Password Management) sent by the Provisioning Engine on the target application.

The Connector Gateway accepts concurrent requests originating from one or more IdentityIQ instances. Each request maintains its dedicated communication channel to the Connector Gateway for sending and receiving information necessary to perform the request. The Connector Gateway forwards these requests to the Connector.

The Connectors provide communications between User Administration components and the managed system. The Connectors are bound to the application they manage. Each supported application has an associated Connector. To service requests for a given application, it's associated Connector is required. Refer the "Applications supported and associated connectors" on page 6 for the complete list of the supported applications and their associated Connector.

The information exchanged between IdentityIQ and the Connector can be secured using an encrypted channel.

Before creating an application, ensure that the following components are installed and configured:

- **Connector**: installed and configured to manage the targeted application.

  For more information on individual installations of the connector, see the respective Administration Guides as follows:

    - *SailPoint IdentityIQ Connector for CA-Top Secret Administration Guide*

    - *SailPoint IdentityIQ Connector for RACF Administration Guide*

    - *SailPoint IdentityIQ Connector for CA-ACF2 Administration Guide*

- **Connector Gateway**: for each Connector, a Connector Gateway is required to communicate with the Connector.

  For more information on installation and configuration of Connector Gateway, see Chapter 2, "Installing and Configuring of Connector Gateway."

Applications supported and associated connectors

The following table lists the supported applications and associated connectors:

Table 1—Supported applications and associated connectors

Application	Connector to be used	Application Type
RACF	CONTROL-SA/Agent for RACF	RACF - Full
CA-ACF2	CONTROL-SA/Agent for CA-ACF2	ACF2 - Full
CA-TopSecret	CONTROL-SA/Agent for CA-Top Secret	TopSecret - Full

Supported features

SailPoint IdentityIQ Gateway Connectors support the following features:

- **Create/Update/Delete/Unlock/Enable/Disable on Account**: Ability for user to perform such account provisioning operations.
- **Change/Reset Password**: Ability for user to change and reset password.
- **Group provisioning**: Group provisioning is supported for all Gateway Connectors in IdentityIQ. Group provisioning supports add, delete and update group.

- **Password Interception**: SailPoint IdentityIQ provides the capability of Password Interception, by which password of an account changed on managed system is intercepted to IdentityIQ.

  New password is intercepted and sent to IdentityIQ to be propogated to other managed systems on which the account is defined.

  For proper functioning of the Password Interception, the Password Interception settings are mandatory. For more information on setting the Password Interception from IdentityIQ, see "Settings for configuring Password Interceptor and Online Interceptor" on page 19.

- **Target aggregations**: Aggregation of permissions on objects.

  Note: **After upgrading to IdentityIQ version 6.4, perform target aggregation again and configure certifications as the old formatted permissions can not be used to revoke permissions.**

- **Auto revocation of accounts and group permissions:** SailPoint IdentityIQ provides the ability of automatic revocations of accounts and groups.

- **Online Interception:** SailPoint IdentityIQ provides the capability of Online Interception, by which any account or group or account-group connection changed on managed system is intercepted to IdentityIQ.

  For proper functioning of the Online Interception, the Online Interception settings are mandatory (Same settings as for Password Interception, so this should be defined only once in IdentityIQ). For more information on setting the Online Interception from IdentityIQ, see "Settings for configuring Password Interceptor and Online Interceptor" on page 19.

IdentityIQ Agent architecture

Chapter 2: Installing and Configuring of Connector Gateway

This chapter provides the steps for the installation and configuration of Connector Gateway.

The following topics are discussed:

Overview

> **Note:**   **Java Development Kit 1.5 (32-bit and 64-bit) or later is required.**

The Connector Gateway can be installed on the any computer with network connectivity to both IdentityIQ and the Gateway Connector (Agent).

Create an installation directory on the computer where the Connector Gateway will run and extract the contents of the `ConnectorGateway-<version>.zip` file that is included with IdentityIQ. Use the following OS-specific installation instructions located in the associated README file included in the `ConnectorGateway-<version>.zip`.

Before you begin

- Verify the Connector is not connected to any application.
- The Connector Gateway and Agent can be started / stopped in any order.
- A directory named **log** should always be present in Connector Gateway installation directory. Check the logs created in **log** directory to follow activities occurring in the Connector Gateway. If any problem arises and logs are not generated, check Windows Event viewer.
- JavaService creates a log file, `javaservice.log`. This file may be located in the root directory of the installation partition. This file can contain information about the installation and uninstallation of the Windows service as well as startup and shutdown activities of the service.
- If there is a firewall between Connector Gateway and Connector, then the port on which Connector is listening must be opened.

Additional configuration parameters

Use the following parameters defined in the IdentityIQ System Configuration object and apply to all applications:
- **syncSchema**: If set to **true**, IdentityIQ application schema will be synchronized with the Connector. Default value is **true**.
- **smReadTimeout**: Timeout value in minutes for read operations between IdentityIQ and the Connector. Default value is 10 minutes.
- **multiColumnSeperator**: The delimiter for multi-column attributes in Connector. The default value is '#'. If the default value does not work for an application, add a new separator into the application template as shown in the following example:
```
<entry key="multiColumnSeperator" value="+" />
```

- **IBMcharacterSet**: The related character set in java for code page used on agent side. Default value: IBM500. For more information, see the following link:

  http://www-01.ibm.com/software/globalization/ccsid/ccsid_registered.html
- **smSocketConnectRetry**: Controls how many times a thread tries to establish a connection with Connector Gateway to get correct read/write socket connection.

Configuring Connector Gateway

This section describes the installation and uninstalltion procedures of Connector Gateway.

Installation

This section describes the installation procedures for Windows and UNIX operating systems.

For Microsoft Windows

1. Download the `ConnectorGateway-<version>.zip` file from IdentityIQ home directory to a temporary directory.

   Note: **The Connector Gateway and the IdentityIQ version must be same.**

2. Unzip the `ConnectorGateway-<version>.zip` file in the temporary directory.
   The following files are extracted:

   - `init.xml`

   - `install.bat`

   - `log4j.properties`

   - `ConnectorGateway.jar`

   - `ConnectorGateway32.exe`

   - `ConnectorGateway64.exe`

   - `README_UNIX`

   - `README_WIN`

3. Edit the `install.bat` file and set `JDK_HOME` to the root directory of your JDK installation.

4. Run the following `install.bat` file, to install Connector Gateway on 32-bit or 64-bit:

   - (*32-bit*): `install.bat 32`

   - (*64-bit*): `install.bat 64`
   And verify if `IdentityIQConnectorGateway_<service name>` service has been installed.

5. Edit `init.xml` and set the host and port details for the Agent and the listening port for the gateway in the Server tag.

6. Start the `IdentityIQConnectorGateway_<service name>` service.

For UNIX

1. Download the `ConnectorGateway-<version>.zip` file from IdentityIQ home directory to a temporary directory.

2. Unzip the `ConnectorGateway-<version>.zip` file in the temporary directory.
   The following files are extracted:

   - `init.xml`

   - `install.bat`

   - `log4j.properties`

   - `ConnectorGateway.jar`

   - `ConnectorGateway32.exe`

   - `ConnectorGateway64.exe`

   - `README_UNIX`

   - `README_WIN`

3. Add the `bin` directory of `Java Development Kit` to the system `PATH` variable.

4. Edit `init.xml` and set the host and port details for the Agent and the listening port for the gateway in the Server tag.

5. Run the following to start the `IdentityIQConnectorGateway` service:
   `java -jar ConnectorGateway.jar`

Uninstallation

This section describes the uninstallation procedures for Windows and UNIX operating systems.

For Microsoft Windows

1. Stop the `IdentityIQConnectorGateway_<service name>` Windows service.

2. Run following command from command prompt, to uninstall Connector Gateway installed on 32-bit or 64 bit Java run:

   - (*32-bit*): `ConnectorGateway32.exe //DS//"IdentityIQConnectorGateway_<service name>"`

   - (*64-bit*): `ConnectorGateway64.exe //DS//"IdentityIQConnectorGateway_<service name>"`

3. Manually remove the installation directory.

For UNIX

1. Stop the `IdentityIQConnectorGateway` service.

2. Manually remove the installation directory.

Chapter 3: Configuring IdentityIQ Gateway Connectors

The following topics are discussed in this chapter:

Configuration

Configuring the Provisioning Engine involves defining an Application in IdentityIQ for each of the target applications. When creating an Application within IdentityIQ, the following information is required:

- Application type
- Connector Gateway details
- Connector details
- Encryption details

> **Note:** **Version of IdentityIQ and Connector Gateway must be same.**

Application type

- Select the type of application that IdentityIQ is managing.
- See the "Applications supported and associated connectors" on page 6 for the list of supported applications and their respective application types.

Connector Gateway details

Each application IdentityIQ is managing must have a dedicated Connector Gateway. The following are details of the Connector Gateway required when defining an Application:

Attributes	Description
Connector Gateway host	Hostname/IP of the computer where the Connector Gateway for the targeted Application is installed.
Connector Gateway port	Port on which the Connector Gateway is listening.

Connector details

A single Connector manages one or more instances of an associated application type. Each instance of the application managed by a Connector requires a separate configuration to create a configuration set unique to that instance of the application. The information below is required to establish this differentiation:

Note: **The values of the attributes referenced below are case sensitive and if provided incorrectly, will cause requests from IdentityIQ to fail.**

Attributes	Description
MSCS Name	Name for the managed system configuration set that is defined when installing the Connector Manager and Connector.
Username	User account used when authenticating to the Target Application through the Connector.
Password	Password for the user account specified in Username.

Encryption details

The communication between IdentityIQ and the Connector can be secured by using either DES or Triple DES encryption algorithm. For more information on enabling secured communication, see "Enabling secured communication between IdentityIQ and Gateway Connectors" on page 18. The following information is required to enable secured communication:

- **Encryption**: the Encryption Algorithm used to secure the communication channel.
- **Encryption Key File**: fully qualified file name of the encryption key file on the IdentityIQ server. For more information on enabling secured communication, see "Enabling secured communication between IdentityIQ and Gateway Connectors" on page 18.

Click Test Connection to check if entered values are correct.

Note: **When aggregation is in progress, do not perform the test connection.**

Testing the Application

The **Test Connection** button in the Application definition web page can be used to test basic connectivity between IdentityIQ and the managed application. Additional tests can be run using the IdentityIQ integration console.

1. Launch the console by using the following IdentityIQ script in the `WEB-INF/bin` directory of the IdentityIQ installation to run IdentityIQ integration:
   ```
   iiq integration
   ```
2. When the command prompt appears enter the following:
   ```
   list
   ```
   This lists the names of all Applications created in system.
3. From the console enter the following:
   ```
   use applicationName
   ```
   This makes the Application active for further console commands.
4. Enter the following:
   ```
   ping
   ```

The following response is displayed:

`Response: Connection test successful`

Enable `log4j` tracing on this class within the Application Server using the following command:

`log4j.logger.sailpoint.connector.sm=debug`

This lets you verify the requests are transmitting over the network, and how they are being processed.

Target Aggregation implementation in Gateway Connectors

Users can use Target aggregation feature to aggregate User, Group permissions of each mainframe based application users and group which has permissions on Mainframe resources (such as datasets , CICS...). In addition, it is also possible to revoke these permissions from IdentityIQ so the relevant Gateway Connectors will drop the relevant permission. The **Target Aggregation** functionality is supported only for the following Gateway Connectors:

- CA-Top Secret
- CA-ACF2
- RACF

Implementing Target Aggregation

To implement Target Aggregation Users must perform the following steps:

1. Synchronize keywords
2. Unstructured Target Configuration on Mainframe application
3. Execute a task to aggregate resources
4. Run certification process to revoke permissions

1 - Synchronize keywords

To aggregate the permissions, keywords for resource and ACE needs to be synchronized. Users must perform Test Connection for Mainframe application. There are three set of keywords maintained for Target Aggregation.

Users can add/remove the keywords from the list by modifying and importing respective application registry file in IdentityIQ for Mainframe connector as follows:

- RACF-Full.xml
- ACF2-Full.xml
- TopSecret-Full.xml
- **splAceAttributes**: The list that contains keywords to synchronize ACE entity.
- **splResourceAttributes**: The list that contains keywords to synchronize ACE entity.

> Note: It is recommended not to modify the list of keywords defined in **splAceAttributes** and **splResourceAttributes**.

- `splTargetPermissionsInterestingKwds`: The keywords mentioned in `splTargetPermissionsInterestingKwds` key are subset of keywords defined in `splAceAttributes` key that is used to form the permissions string. These keywords are not sent to Mainframe Connector while keyword synchronization.

If any keyword must be added/deleted in the permissions list then adding/deleting the keyword in `splTargetPermissionsInterestingKwds` tag and running target aggregation will populate value of the keyword on record.

For example, if the `splTargetPermissionsInterestingKwds` contains the following list of keywords as in `RACF-Full.xml` file:

- ACCESS
- INFO.ACC_COUNT
- WHEN.APPCPORT
- WHEN.CONSOLE
- WHEN.JESINPUT
- WHEN.PROGRAM
- WHEN.SYSID
- WHEN.TERMINAL

And if the user does not want IdentityIQ to display the fields starting with WHEN, then user must modify the list to the following in the application debug page:

- ACCESS
- INFO.ACC_COUNT

> Note: **Users can revoke only the permissions aggregated in IdentityIQ. In above scenario the permissions ACCESS and INFO.ACC_COUNT can only be revoked from IdentityIQ.**

2 - Unstructured Target Configuration on Mainframe application

1. Configure unstructured targets for the application you want to execute target aggregation.
   Provide the following details on Unstructured Target Configuration:

   - **Name**: Provide name to the created unstructured configuration.
     For example, `RACFUnstructuredTargetConfig`.

   - **Correlation Rule**: Create a correlation rule to correlate the permissions and entities in IdentityIQ.
   The following sample code can be used for correlation:

```
import sailpoint.api.Correlator;
import sailpoint.tools.xml.XMLObjectFactory;
      private String ATTR_USER_OBJECT= "USER_ID";
      private String ATTR_GROUP_OBJECT= "GROUP_ID";
      Map returnMap = new HashMap();
  if ( isGroup ) {
        returnMap.put(Correlator.RULE_RETURN_GROUP_ATTRIBUTE,"nativeIdentity");
         returnMap.put(Correlator.RULE_RETURN_GROUP_ATTRIBUTE_VALUE, nativeId);
      } else {
      returnMap.put(Correlator.RULE_RETURN_LINK_IDENTITY, nativeId);
 }
```

```
      System.out.println("Incomming ["+nativeId+"] correlated
["+XMLObjectFactory.getInstance().toXml(returnMap)+"]");
        return returnMap;
```

2. Depending on the type of the mainframe connector, select **Target Source type** and other attributes:

   - For application type **RACF Full**:

      Target Source type: **PE2 RACFCollector**

Attributes	Description
RACF Target Resource Name	Provide RACF Target Resource name.
Target Resource Type	Provide RACF Target Resource Type.
Volume	Provide RACF Target Resource volume.
Resource Get Type	Specify ID or PREFIX.
Generic Type	Specify Yes (Generic) or No (non-Generic).

   - For application type **Top Secret Full**:

      Target Source type: **PE2 TSSCollector**

Attributes	Description
TSS Target Resource Name	Provide TSS Target Resource name.
Target Resource Type	Provide TSS Target Resource Type.
Resource Get Type	Specify ID or PREFIX.

   - For application type **CA-ACF2**:

      Target Source type: **PE2 ACF2Collector**

Attributes	Description
ACF2 Target Resource Name	Provide ACF2 Target Resource name.
Target Resource Type	Provide ACF2 Target Resource Type.
ACF2 ruleset Type	None (specific) or PREFIX or NEXTKEYS.

Modify the delimiter

The resources and permissions will be updated in the respective account as a string in delimited format. Customer can define the delimiters for field separator and list separator by modifying the following keys in respective application registry file in IdentityIQ for Mainframe connector:

```
<entry key="fieldDelimiter" value="#"/>
```

```
<entry key="listDelimiter" value=";"/>
```
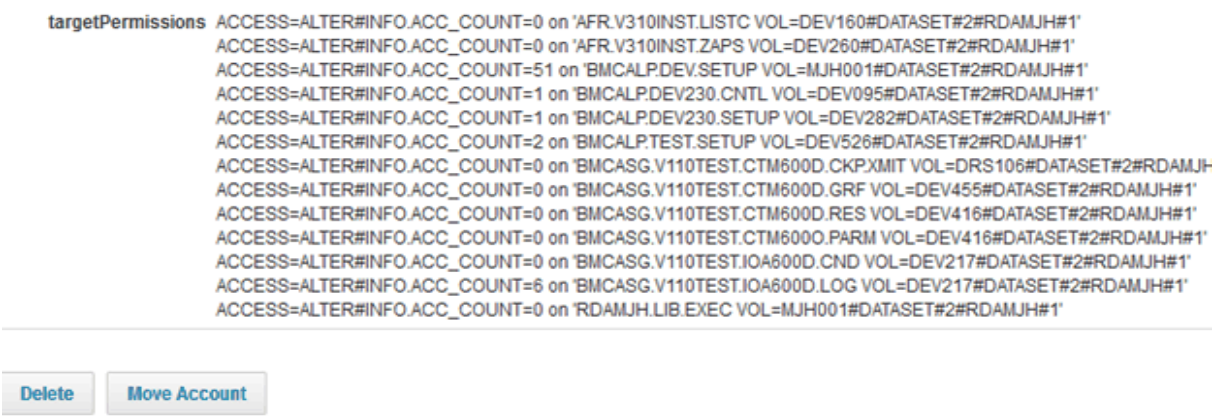
The default values for field and list delimiter are **#** and **;** respectively.

3 - Execute a task to aggregate resources

To aggregate permissions create New Target Aggregation task. Enter the name for the task and select Mainframe application to scan targets from the list and the Unstructured Target configured for the application. When the task

gets completed successfully you can view the permissions on the Account property as displayed in the following figure:

```
targetPermissions  ACCESS=ALTER#INFO.ACC_COUNT=0 on 'AFR.V310INST.LISTC VOL=DEV160#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'AFR.V310INST.ZAPS VOL=DEV260#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=51 on 'BMCALP.DEV.SETUP VOL=MJH001#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=1 on 'BMCALP.DEV230.CNTL VOL=DEV095#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=1 on 'BMCALP.DEV230.SETUP VOL=DEV282#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=2 on 'BMCALP.TEST.SETUP VOL=DEV526#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'BMCASG.V110TEST.CTM600D.CKP.XMIT VOL=DRS106#DATASET#2#RDAMJH
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'BMCASG.V110TEST.CTM600D.GRF VOL=DEV455#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'BMCASG.V110TEST.CTM600D.RES VOL=DEV416#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'BMCASG.V110TEST.CTM600O.PARM VOL=DEV416#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'BMCASG.V110TEST.IOA600D.CND VOL=DEV217#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=6 on 'BMCASG.V110TEST.IOA600D.LOG VOL=DEV217#DATASET#2#RDAMJH#1'
                   ACCESS=ALTER#INFO.ACC_COUNT=0 on 'RDAMJH.LIB.EXEC VOL=MJH001#DATASET#2#RDAMJH#1'
```

[Delete]   [Move Account]

4 - Run certification process to revoke permission

To revoke permission through certification run **Refresh Identity Cube** and **Refresh Entitlement Correlation** tasks before running certification and follow the certification process.

Enabling secured communication between IdentityIQ and Gateway Connectors

This section provides the steps used to enable secured communication between IdentityIQ and Gateway Connectors. To secure the communication channel between IdentityIQ and Gateway Connectors, IdentityIQ uses either DES or Triple DES for encrypting the exchanged data. Regardless of the type of encryption used, an encryption key file is required. You can use one common encryption key file for all the Gateway Connectors or use separate key files for each Gateway Connector.

On IdentityIQ computer

To create an encryption key file, perform the following steps for each key file required:

1. From the command prompt change the directory to `IIQFolder\WEB-INF\bin\<OS_Flavor>`
2. Run the following command:
   `kgen <encryption_key_file_name>`

   Note: **The complete *fileName* (including the path and extension) is asked while creating an IdentityIQ Application.**

On computer where Connector is installed

Perform the following steps for each Gateway Connector.

1. Copy the encryption key file created above to `<AGENT_INSTALL>\DATA` folder.

2. Edit the `<AGENT_INSTALL>\DATA\CTSPARM.PRM` file and modify the parameters as shown below

   `FOREVERY ENCR_EXT_ACT: set the value to Y`

   `FOREVERY FILE_ENCREXT: set the value to %CTSROOT%\DATA\`*`keyFileName`*

3. Restart the Connector and the Connector Gateway.

Settings for configuring Password Interceptor and Online Interceptor

Password Interception or Online Interceptor is not enabled by default. There are few steps that need to be performed in order to enable it on Gateway Connector and IdentityIQ.

To Enable Password Interception or Online Interceptor on IdentityIQ, add the following attributes in Service definition:

1. To open the ServiceDefinitions navigate to **IdentityIQ debug page => ServiceDefinition => SMListener** and add the attribute and hostname as follows:

   • Add the following attribute in SMListener:

   ```
   <Attributes>
     <Map>
       <entry key="applications" value="Application name"/>
       <entry key="retryInterval" value="5" />
     </Map>
   </Attributes>
   ```

   Note: **To configure multiple applications for password interceptor, add multiple names in application value as follows:**
   `<entry key="applications" value="App1,App2"/>`

   • Add the hostname as follows:

   ```
   <ServiceDefinition created="1347280738108" hosts="hostName"
   id="2c9095d439b02f0b0139b030973c00e9" modified="1347285339111"
   name="SMListener">
   ```

2. To open the ServiceDefinitions navigate to **IdentityIQ debug page => ServiceDefinition => ResourceEvent** and add the hostname as follows:

   ```
   <ServiceDefinition created="1347280738124" hosts="hostName"
   id="2c9095d439b02f0b0139b030974c00ea" modified="1347285354945"
   name="ResourceEvent">
   ```

In the preceding command lines, the value of *hostName* in ServiceDefinitions of SMListener and ResourceEvent must be the name/IP of host where IdentityIQ Server is running. User must define only one IdentityIQ host if there are multiple instances of IdentityIQ Servers running. This will start **SMListener** Service on one server where the interceptors sent from Agent would be processed.

Note: If the application that is configured to receive password changes was before upgrading IdentityIQ to version 6.0 then perform the following additional steps:
   a. Navigate to the application definition page (application that is configured to receive delta changes).
   b. Re-enter the password.
   c. Save the application.
   d. Perform a **Test Connection**.

Settings for configuring Password Interceptor and Online Interceptor

When IdentityIQ starts it will start a thread per application for which password interception is enabled. This thread is responsible for receiving the delta changes from that application. If any change is made to the above attributes or if you enable or disable encryption for the application that is configured to receive password changes, the IdentityIQ server must be restarted for the changes to take effect.

Password Interceptor and Online Interception are supported for the following Gateway Connectors:

- **CA-ACF2**: To enable Password Interceptor or Online Interceptor on CA-ACF2, refer to the *SailPoint IdentityIQ Connector for CA-ACF2 Administration Guide*.

- **CA-Top Secret (TSS)**: To enable Password Interceptor or Online Interceptor on TSS, refer to the *SailPoint IdentityIQ Connector for CA-Top Secret Administration Guide*.

- **RACF**: To enable Password Interceptor or Online Interceptor on RACF, refer to the *SailPoint IdentityIQ Connector for RACF Administration Guide*.

Change Interception

Under default operation, when an account is modified on the remote system, change interception in IdentityIQ can automatically receive only the items/attributes that were changed and then merged that change into the existing IdentityIQ identity. These items/attributes were not processed through the aggregation procedures set up for the application (such as buildMap rule, customozation rule and so on).

If the processes associated with aggregation are important for these changes, you can enable the complete aggregation of single accounts, groups, or both when a change is detected, so that these additional procedures are applied to the account when a change is detected. This can be achieved by specifying the following attributes in the ServiceDefinition for the ResourceEvent:

- **getEntireAccount**
- **getEntireGroup**

The above attributes will trigger the aggregation of the accounts, groups, or both for the object on which the change is detected and ensures that any new change on accounts or groups are processed through the aggregation procedures set up on IdentityIQ for the respective applications.

> Note: The "getEntireAccount" and "getEntireGroup" attributes accept boolean values.

Following is an example, with the attribute values enabled:

```
<ServiceDefinition name="ResourceEvent">
  <Attributes>
    <Map>
      <entry key="correlateEntitlements" value="true"/>
      <entry key="getEntireAccount" value="true"/>
      <entry key="getEntireGroup" value="true"/>
      <entry key="noOptimizeReaggregation" value="true"/>
      <entry key="promoteAttributes" value="true"/>
    </Map>
  </Attributes>
</ServiceDefinition>
```

Setting Aggregation improvement functionality

Perform the following steps to enable aggregation improvement functionality:

1. Navigate to the debug page.
   The Application list is displayed.

2. Select the application for which you want to enable the aggregation improvement functionality.

3. Add the following new attribute in the application and save it.
   <entry key="cmOptimizedAggregation" value="true"/>

   Note: **After configuring application for Aggregation improvement, following changes are done in Aggregation algorithm:**

   - **For Group aggregation task, Connector Manager sends only group information to IdentityIQ.**

   - **For Account aggregation task, Connector Manager sends only account and connection information to IdentityIQ.**

Setting Aggregation improvement functionality

Appendix A: Troubleshooting

This appendix describes problems that may be encountered while setting and configuring the Gateway Connectors and the resolutions for these problems.

1 - Third party monitoring tool (Port Monitoring software) usage and it's implications

Resolution: When using Port Monitoring software to validate the Connector Gateway connections, use one of the following methods to enable this service to work properly:

- **Using a port monitoring solution**: Ensure that the port monitoring software is located on a server other than the IdentityIQ and/or the Connector Gateway server. The proper method of using the software is to establish a connection in the same method (as follows) as used by IdentityIQ:

  Connect first on the defined port +1, then on the defined port 2471, (for example, the port defined in `init.xml` is 2470) as this will create a valid socket connection.

- **Checking the status of Connector Gateway**: This method involves the use of two telnet sessions in the same manner as described below:

  Connect first on the defined port +1, then on the defined port 2471, (for example, the port defined in `init.xml` is 2470) as this will create a valid socket connection.

  This should be tested to ensure that this does not interfere with active connections within your environment.

- **Writing a log parser**: Write a log parser to check for socket information within the logs. If the socket connections are not performing, restart Connector Gateway. For Connector Gateway to determine the proper status, enable the DEBUG tracing. Following are the other methods to use log parser method:

  - Check the log output to see when the connection information was last updated (stale connection check), and if there are no updates from the Connector Gateway within time variable **X** (to be defined locally as it pertains to the environment), then restart Connector Gateway Service. With this the Connector Gateway would be online.

  - Write a log pareser that will validate the socket connection pairs for the transactions that are valid and are initiated from IP address of IdentityIQ host only. When using this method, ensure that the connection is misdirected, unclean or invalid.

Ensure that other unwanted traffic does not interfere with the normal communications in your network by the use of Firewalls and Routing to isolate traffic to and from only trusted and intended source machines and services.

SailPoint recommends to test the above alterantive methods in your environment using the proper Change Management methodology as specified below:

- Develop
- Test
- Promote to production after proper testing is completed

2 - During aggregation if user performs Test connection the Test connection transaction timeouts

During aggregation if user performs Test connection the Test connection transaction timeouts.

Resolution: During aggregation if user performs Test connection, the Test connection transaction timeouts as the Connector is busy in processing Aggregation. To resolve this issue, configure Multiple Transaction Servers on

Connector to perform more than one transaction at a time. For more information on the configuration changes, see the procedures documented in the respective *Connector Administration Guide*.

> **Note:** **You can set 2 or 3 multiple transaction servers to handle more concurrent operations depending on the load.**

3 - Transactions taking more time than 10 minutes.

Transactions taking more time.

Resolution: If the transaction is expected to take more than 10 minutes, perform the following:

1. Set **smReadTimeout** parameter in Configuration => System Configuration as follows:
    ```
    <entry key="smReadTimeout" value="10"/>
    ```
    Timeout value is in minutes and can be defined to read message between IdentityIQ and the Connector. The default value is 10 minutes.

4 - Why Target Permissions are not getting aggregated in IdentityIQ?

Target Permissions are not getting aggregated in IdentityIQ.

Resolution: If Target Permissions are not getting aggregated in IdentityIQ, then:
*   Verify if the application name defined in unstructured target is correct.
*   Verify if the correlation rule is pasted (by removing the extra end lines if it is copied from document) correctly.

Index