

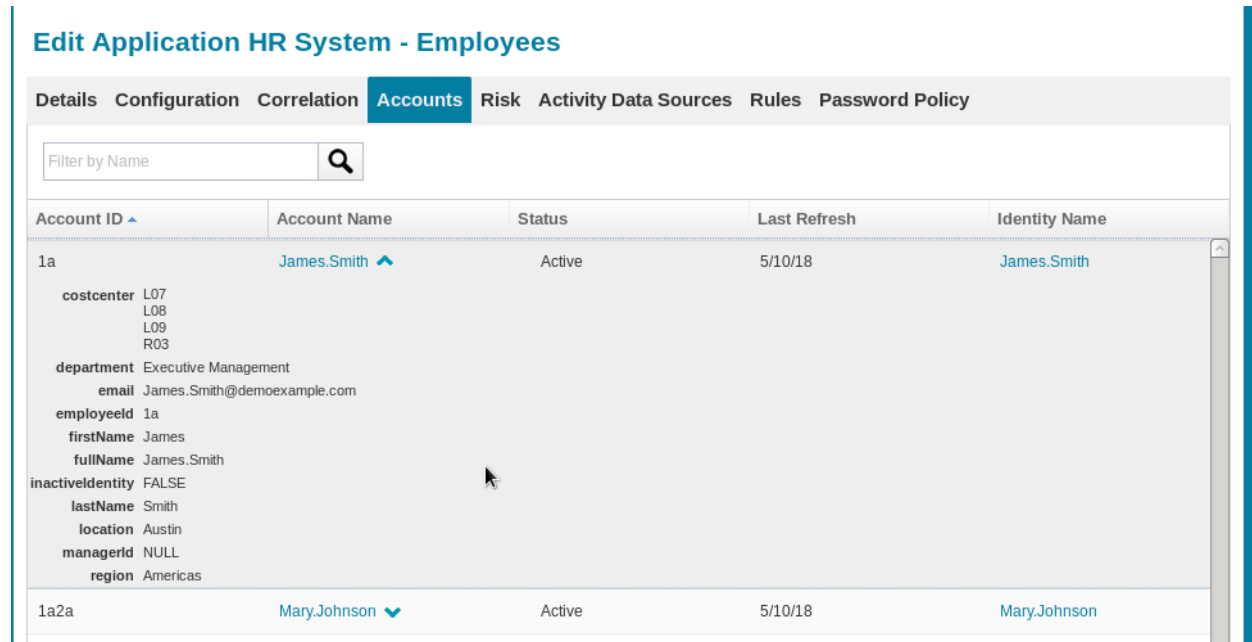
Understanding Correlation Rule, Correlation Configuration and Default Correlation

Every IIQ enthusiast has one time or the other felt the need to understand the three correlation options IIQ provides. They might have come up with questions like - which to use? Which supersedes the other? Can all three types co-exist? Can I have no correlations defined?

I have tried to break down the three types and tried to answer the questions.

Let's start.

First, let's see our Authoritative application. Name is in the format – "FirstName.LastName".



The screenshot shows the 'Edit Application HR System - Employees' interface. The 'Accounts' tab is selected, displaying a table of employee accounts. The table has columns for Account ID, Account Name, Status, Last Refresh, and Identity Name. Two accounts are visible: 1a (James.Smith) and 1a2a (Mary.Johnson). A detailed view of the 1a account is shown on the left, listing various attributes like costcenter, department, email, employeeid, firstName, fullName, inactiveIdentity, lastName, location, managerId, and region.

Account ID	Account Name	Status	Last Refresh	Identity Name
1a	James.Smith	Active	5/10/18	James.Smith
1a2a	Mary.Johnson	Active	5/10/18	Mary.Johnson

Account Details for 1a:

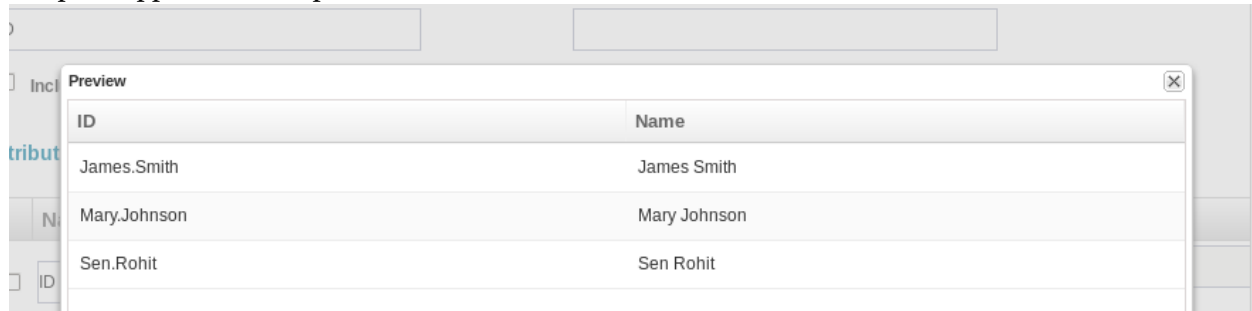
- costcenter: L07, L08, L09, R03
- department: Executive Management
- email: James.Smith@demoexample.com
- employeeid: 1a
- firstName: James
- fullName: James.Smith
- inactiveIdentity: FALSE
- lastName: Smith
- location: Austin
- managerId: NULL
- region: Americas

Ok. Let's start by creating a new application in IIQ. We will not specify any correlation configuration or rule. We will see how IIQ behaves by default.

For the use case, I am using a delimited type application. This is my delimited file:

```
File Edit View Search Term
ID,Name
James.Smith,James Smith
Mary.Johnson,Mary Johnson
Sen.Rohit,Sen Rohit
~
```

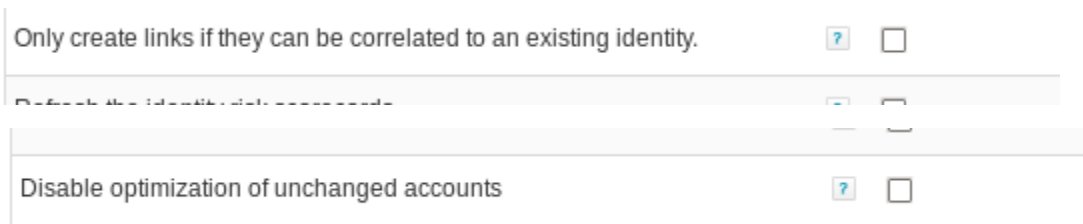
James and Mary have matching ID's with Authoritative application. Sen Rohit has no matching ID. Let's setup the application and preview accounts.



ID	Name
James.Smith	James Smith
Mary.Johnson	Mary Johnson
Sen.Rohit	Sen Rohit

Perfect.

Let's save our application and run an aggregation. Make sure the below options in task definition are unchecked.



Only create links if they can be correlated to an existing identity.

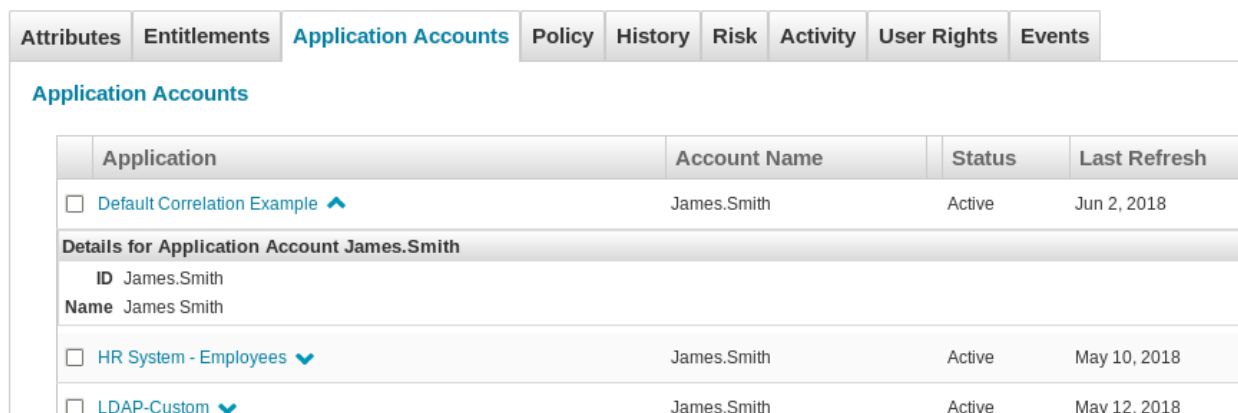
Default the identity link password

Disable optimization of unchanged accounts

Alright. Aggregation is complete. We will now open all three accounts and see what happened.

James' account:

View Identity James.Smith



Application	Account Name	Status	Last Refresh
<input type="checkbox"/> Default Correlation Example ^	James.Smith	Active	Jun 2, 2018
Details for Application Account James.Smith			
ID James.Smith			
Name James Smith			
<input type="checkbox"/> HR System - Employees v	James.Smith	Active	May 10, 2018
<input type="checkbox"/> LDAP-Custom v	James.Smith	Active	May 12, 2018

Mary's account:

View Identity Mary.Johnson

Application	Account Name	Status	Last Refreshed
<input type="checkbox"/> Default Correlation Example ^	Mary.Johnson	Active	Jun 2, 2018
Details for Application Account Mary.Johnson			
ID	Mary.Johnson		
Name	Mary Johnson		
<input type="checkbox"/> HR System - Employees v	Mary.Johnson	Active	May 10, 2018
<input type="checkbox"/> HR System - Employees v	Mary.Johnson	Active	May 10, 2018

So far so good. Both identities have been correlated with the Authoritative identity based on their matching Name.

What about Sen Rohit's account. Let's see.

View Identity Sen.Rohit

Application
<input type="checkbox"/> Default Correlation Example v

Hard luck! The identity is uncorrelated. And account is an orphan one.

Let's analyze what happened:

1. IIQ tries to match the Identity attribute of the new application with the Identity Name of the Authoritative application.
2. If it finds a match, it correlates the identity. Else, it creates an orphan account.

Let's move on. Now let's see how the Correlation configuration option works.

Let's add some more rows to our data file. Let's add John and Patricia.

fullName	employeeId	firstName	lastName	managerId	email	department	region	location	inactiveVelder
James.S...	1a	James	Smith	NULL	James.S...	Executiv...	Americas	Austin	FALSE
Mary.Joh...	1a2a	Mary	Johnson	1a	Mary.Joh...	Regional...	Americas	Austin	FALSE
D'Arcy.O'...	1a2aX	D'Arcy	O'Mahoney	1a	D'Arcy.O'...	Regional...	Americas	Austin	FALSE
John.Will...	1a2b	John	Williams	1a	John.Will...	Regional...	Americas	Brazil	FALSE
Patricia.J...	1a2c	Patricia	Jones	1a	Patricia.J...	Regional...	Americas	San Jose	FALSE
Robert.B...	1a2a3a	Robert	Brown	1a2a	Robert.B...	Informati...	Americas	Austin	FALSE

We will add only employee codes this time for John and Patricia. Our new data file is as below:

```
ID,Name
James.Smith,James Smith
Mary.Johnson,Mary Johnson
Sen.Rohit,Sen Rohit
1a2b,John Williams
1a2c,Patricia Jones
~
~
```

Let's define a correlation configuration. ID column records of the new application should match with empId Identity Attribute. See below:

Account Correlation

To Edit the currently assigned configuration click Edit. If you want to create a New Correlation config click New.

Correlation Config Example

Attribute Based Correlation

Application Attribute	Identity Attribute
ID	empId

Condition Based Correlation

Let's run aggregation and see the changes.

John Williams is setup correctly. Nice.

View Identity John.Williams

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User R
Application Accounts							
		Application	Account Name				
<input type="checkbox"/>	Default Correlation Example ^		1a2b				
Details for Application Account 1a2b							
		ID	1a2b				
		Name	John Williams				
<input type="checkbox"/>	HR System - Employees v		John.Williams				

So is Patricia.

View Identity Patricia.Jones

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
		Application	Account Name	Status	Last Refresh			
<input type="checkbox"/>	Default Correlation Example ^		1a2c	Active	Jun 2, 2018			
Details for Application Account 1a2c								
		ID	1a2c					
		Name	Patricia Jones					
<input type="checkbox"/>	HR System - Employees v		Patricia.Jones	Active	May 10, 2018			

James and Mary are still correlated. Good.

So can we say that if the Correlation configuration cannot match, IIQ switches back to default configuration? Let's validate it. We will add another record with FirstName.LastName matching account name and see if the default configuration still works.

Let's add Joseph in our data file.

Edit Application HR System - Employees

Details Configuration Correlation **Accounts** Risk Activity Data Sources Rules Password Policy

Filter by Name

Account ID ^	Account Name	Status	Last Refresh	Identity Name
1a	James.Smith v	Active	5/10/18	James.Smith
1a2a	Mary.Johnson v	Active	5/10/18	Mary.Johnson
1a2a3a	Robert.Brown v	Active	5/10/18	Robert.Brown
1a2a3a4a	Joseph.Thompson v	Active	5/10/18	Joseph.Thompson

```
ID,Name
James.Smith,James Smith
Mary.Johnson,Mary Johnson
Sen.Rohit,Sen Rohit
1a2b,John Williams
1a2c,Patricia Jones
Joseph.Thompson,Joseph Thompson
```

Let's run aggregation again. Check if Joseph is correlated.

View Identity Joseph.Thompson

Attributes Entitlements **Application Accounts** Policy History Risk Activity User Rights Events

Application Accounts

Application	Account Name	Status	Last Refresh
<input type="checkbox"/> Default Correlation Example ^	Joseph.Thompson	Active	Jun 2, 2018
Details for Application Account Joseph.Thompson			
ID	Joseph.Thompson		
Name	Joseph Thompson		
<input type="checkbox"/> HR System - Employees v	Joseph.Thompson	Active	May 10, 2018

Tada! Joseph is correlated as well. So we see both default and correlation configuration is working. If correlation configuration cannot match, default correlation will occur.

Now our friend Sen Rohit is still sitting uncorrelated. Let us try to correlate it with its email attribute. Read on.

Changing the data file record for Sen Rohit to serve our purpose...

```
ID, Name
James.Smith, James Smith
Mary.Johnson, Mary Johnson
Rohit.Sen, Sen Rohit
1a2b, John Williams
1a2c, Patricia Jones
Joseph.Thompson, Joseph Thompson
defaultConfiguration.txt (END)
```

Let's try to correlate with the below authoritative identity.

The screenshot shows the IdentityIQ interface. The top navigation bar includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Setup'. The user is logged in as 'The Administrator'. The main content area is titled 'Identities'. A search bar contains the email 'Rohit.Sen@demoexample.com'. Below the search bar is a table with the following data:

User Name	First Name	Last Name	Manager	Assigned Role Summary	Detected Rc	Risk Score	Last Refresh	Status	Authoritative
Rohit.Sen@demoexa...	Robin	Lawson	Russell....	region.Asia-Pacific	TRAKK - ...	500	6/2/18 1:...	Employee	true

On the rule, let's write the code.

We will append @demoexample.com to ID field of feed file. Then compare with the User Name of existing authoritative account.

Rule Editor

```
import java.lang.String;
import java.util.*;
import sailpoint.object.*;

// Try to correlate first on Login name
// If that doesn't work try lower case "first initial" plus lower case "last name"

String login = account.getAttribute("ID");
System.out.println("Trying to correlate account: " + login);

String fullName = login + "@demoexample.com";
Identity cube = (Identity) context.getObjectByName(Identity.class,fullName);
if (null != cube) {
    // found cube
    if (cube.isCorrelated()) {
        System.out.println("Successful Correlation based on login:" + fullName);
        return java.util.Collections.singletonMap("identity", (Object) cube);
    }
}

// Nothing to correlate to
return new HashMap();
```

Rule Name

Correlation Rule Example

Rule Type

Correlation

Return Type

Map

Arguments

- log
- context
- environment
- application

Returns

- identityName
- identity
- identityAttributeName
- identityAttributeValue

Description

Identity Correlation Rules are used to find identities to which new accounts can be attached.

A correlation rule must return a Map with one of the specified Return arguments.

Ok. Let's run the aggregation and see results.

View Identity Rohit.Sen@demoexample.com

Attributes
Entitlements
Application Accounts
Policy
History
Risk
Activity
User Right

Application Accounts

Application	Account Name	Sta
<input type="checkbox"/> Default Correlation Example ^	Rohit.Sen	Activ
Details for Application Account Rohit.Sen		
ID Rohit.Sen		
Name Sen Rohit		
<input type="checkbox"/> HR System - Employees v	Robin.Lawson	Activ
<input type="checkbox"/> LDAP-Custom v	Robin.Lawson	Activ

Author: Rohit Sen
IAM Consultant

Nice! Sen Rohit is now correlated as well.

But, let's check what happened to other existing accounts. Let's open up James.

View Identity James.Smith

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
		Application	Account Name	Status	Last Refresh			
<input type="checkbox"/>		Default Correlation Example ^	James.Smith	Active	Jun 2, 2018			
Details for Application Account James.Smith								
		ID	James.Smith					
		Name	James Smith					
<input type="checkbox"/>		HR System - Employees v	James.Smith	Active	May 10, 2018			
<input type="checkbox"/>		LDAP-Custom v	James.Smith	Active	May 12, 2018			

It is as it is. So what can we infer?

Let's add more records based on Authoritative source data and check which correlation is working.

1a2b3a4b	Ruth.Gonzalez v	Active	5/10/18	Ruth.Gonzalez
1a2b3a4e	Ronald.Mitchell v	Active	5/10/18	Ronald.Mitchell
1a2b3b	Elizabeth.Taylor v	Active	5/10/18	Elizabeth.Taylor@demoexa...

Our new data file is :

```
ID,Name
James.Smith,James Smith
Mary.Johnson,Mary Johnson
Rohit.Sen,Sen Rohit
1a2b,John Williams
1a2c,Patricia Jones
Joseph.Thompson,Joseph Thompson
1a2b3a4b,Ruth Gonzalez
Ronald.Mitchell,Ronald Mitchell
Elizabeth.Taylor,Elizabeth Taylor
```

Let's run aggregation.

On checking Ruth's account, we see it is successfully correlated! Our correlation configuration has worked.

View Identity Ruth.Gonzalez

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
Application	Account Name	Status	Last Refresh					
<input type="checkbox"/> Default Correlation Example ^	1a2b3a4b	Active	Jun 2, 2018					
Details for Application Account 1a2b3a4b ✕								
ID 1a2b3a4b								
Name Ruth Gonzalez								
<input type="checkbox"/> HR System - Employees v	Ruth.Gonzalez	Active	May 10, 2018					
<input type="checkbox"/> LDAP-Custom v	Ruth.Gonzalez	Active	May 12, 2018					

Let's open Ronald.

Amazingly, Ronald is also correlated. So, our default configuration is also working.

View Identity Ronald.Mitchell

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
Application	Account Name	Status	Last Refresh					
<input type="checkbox"/> Default Correlation Example ^	Ronald.Mitchell	Active	Jun 2, 2018					
Details for Application Account Ronald.Mitchell								
ID Ronald.Mitchell								
Name Ronald Mitchell								
<input type="checkbox"/> HR System - Employees v	Ronald.Mitchell	Active	May 10, 2018					
<input type="checkbox"/> LDAP-Custom v	Ronald.Mitchell	Active	May 12, 2018					

Let's open Elizabeth.

Voila!

View Identity Elizabeth.Taylor@demoexample.com

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
Application	Account Name	Status	Last Refresh					
<input type="checkbox"/> Default Correlation Example	Elizabeth.Taylor	Active	Jun 2, 2018					
Details for Application Account Elizabeth.Taylor								
ID Elizabeth.Taylor								
Name Elizabeth Taylor								
<input type="checkbox"/> HR System - Employees	Elizabeth.Taylor	Active	May 10, 2018					
<input type="checkbox"/> LDAP-Custom	Elizabeth.Taylor	Active	May 12, 2018					

All three are correlated. Our rule too has correlated the account successfully.

So, we can easily infer that all three correlation types are equally important. Rule is used to correlate accounts based on logic out of scope of Correlation configuration.

Yes, the rule supersedes the correlation config and correlation config supersedes the default correlation. The general behavior of IIQ is to find returned map first from rule; if it does not return anything it falls back on Correlation configuration. If correlation configuration too does not return anything, it falls back on default correlation. If default correlation fails, it creates an orphan account.