Table of Contents

[1 Overview 2](#_Toc511881061)

[2 Use Cases in Scope 2](#_Toc511881062)

[3 Use Case Examples 2](#_Toc511881063)

[4 Functions and Restrictions 2](#_Toc511881064)

[5 Design 3](#_Toc511881065)

[5.1 Application Extended Attributes 3](#_Toc511881066)

[5.2 Settings 4](#_Toc511881067)

[5.2.1 Single Entitlement 4](#_Toc511881068)

[5.2.2 Multiple Entitlements Different Applications 4](#_Toc511881069)

[5.2.3 Multiple Entitlements Same Application 4](#_Toc511881070)

[5.3 Conditional Rule 4](#_Toc511881071)

[5.4 Rule Configuration 4](#_Toc511881072)

[6 Data Flow 5](#_Toc511881073)

**Document Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author** | **Summary of Changes** |
| Version 1 | 3/2/18 |  | Rohit Gupta |  |
| Version 2 | 5/7/18 |  | Cathy Mallet | Minor edits |

# Overview

The purpose of this document is to explain the technical details of the New Account Dependency Entitlements feature that is bundled with the Accelerator Pack. This Feature addresses the requirement of provisioning dependent Infrastructure/Technology Entitlements after the creation of a new account for any business application. This feature is configured on an application either via the Self Service Onboarding Wizard or the IdentityIQ Administrative Wizard.

# Use Cases in Scope

The following use cases are in scope of this Feature:

* Access Requests with account “Create” operation from ”Manage Access” and “Manage Privileged Access” QuickLinks
* Manage Accounts with account “Create” operation
* Batch requests with account “Create” operation
* Lifecycle events where new access needs to be provisioned with account “Create” operation, such as JOINER FEATURE or JOINER REHIRE FEATURE.
* Automated Role assignment rules (for example, RBAC Role assignment) with account “Create” operation
* Recover Identity Access with account “Create” operation using the Operational Task QuickLink “Recover Identity Access”

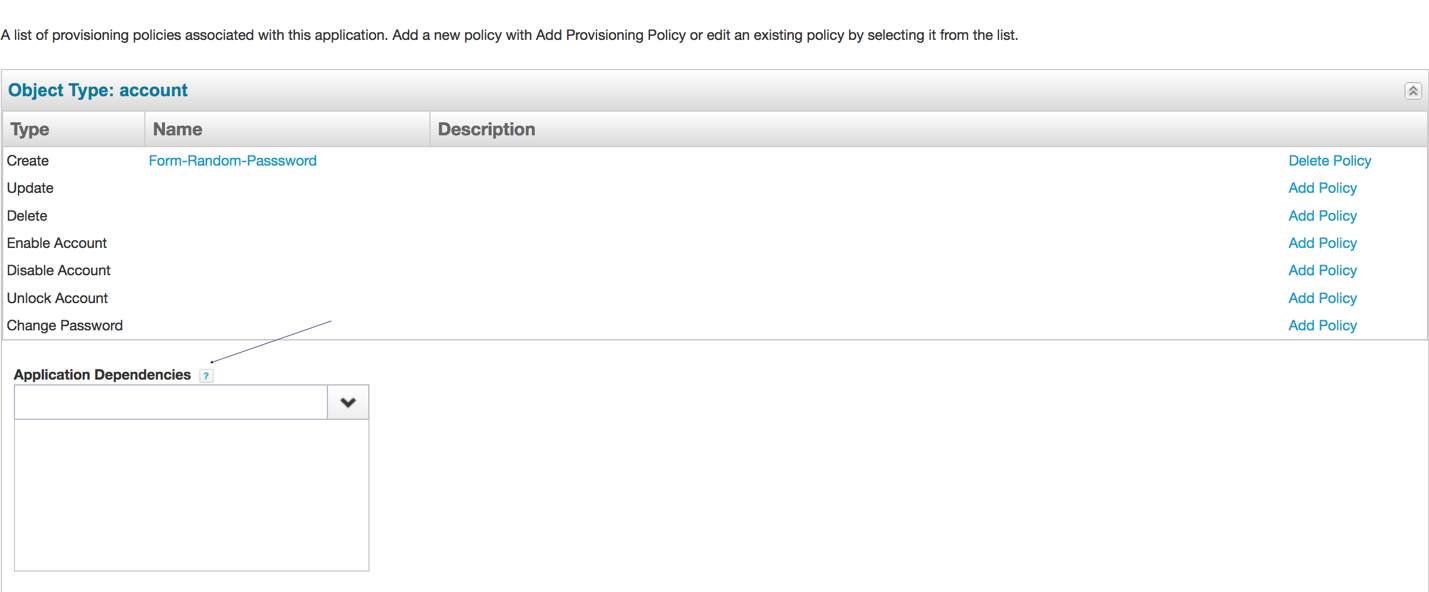
# Use Case Examples

A dependency between Business Application New Account creation and Infrastructure /Technology Authorization. For example, Business Application requires Active Directory Security Group Authorization for a new account. Accounts cannot log in to the application’s modules, portals, etc. without Active Directory Security Group Authorization.

A dependency between SSO Business Application Catalog Items and Business Application New Account creation. For example, the SSO Launchpad (VMWare Workspace ONE, Azure Single Sign-On, etc.) requires business applications to be automatically assigned to an Identity as catalog items on creation of new account on that business application.

# Functions and Restrictions

This Feature is only for provisioning additional entitlements. If a role or an entitlement requires provisioning additional application accounts (only accounts, no entitlements), then the out of the box “**Application Dependencies**” option must be used. Navigate to an Application Definition > Configuration Tab > Provisioning Policies Section to configure which application(s) to create accounts for.



**Restrictions**

* If a Business application account is already created, perhaps manually outside of IdentityIQ, but IdentityIQ is not aware of it because an aggregation has not yet run, the original access request will think that a new account is needed and try to create one. This account creation may fail because the account already exists. The provisioning of dependency entitlements always requires the original access to be provisioned successfully. In this case, since the original account creation failed, the dependency entitlement provisioning will be skipped
* If a Business application account is already created, perhaps manually outside of IdentityIQ, and IdentityIQ is already aware of it, then requesting access for a business application will not result in an account Create operation. This will cause the dependency feature to ignore any dependency entitlement provisioning. In this case, the dependency entitlements must be requested manually in a separate access request or batch request.
* Dependency entitlements cannot be configured for **Ticketing** based applications because this feature uses the application’s “After Provisioning” rule, which by design, does not execute for integration provisioning.

**Feature Functions**

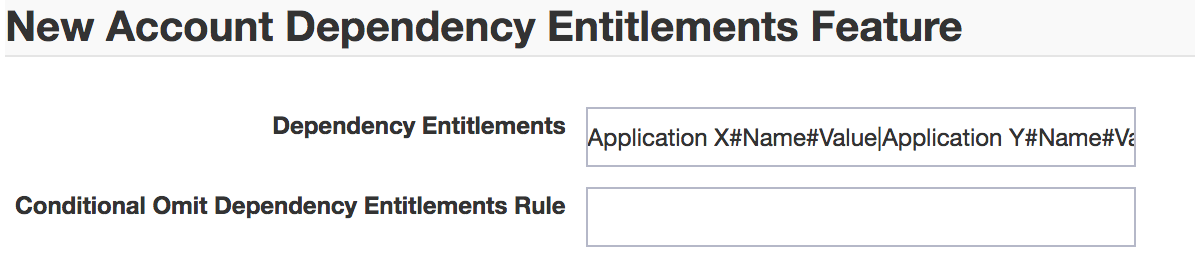
* The additional underlying Infrastructure/Technology entitlements will appear in a separate Access Request of type “REQUEST MANAGER FEATURE”. They don’t require approvals and also do not trigger email notifications.
* The dependency entitlement provisioning generates the same audit events as other provisioning events. Search for the “provisioning” audit event in advanced analytics to track them.
* If there are any errors during the provisioning, the Operations group will be notified. When troubleshooting provisioning errors, the Operations group should look for the access request of type “REQUEST MANAGER FEATURE” containing the dependency entitlements to get a complete picture of the provisioning operations
* It will also provide the option to specify a conditional rule, per application, to check additional business logic and determine whether to skip/omit its provisioning or not

# Design

This feature uses additional application extended attributes (these attributes are not indexed) as well as the “After Provisioning Rule” feature that is available out of the box on all applications.

## Application Extended Attributes

This feature will use new application extended attributes. These extended attributes will apply to all application artifacts and hold the required provisioning settings. They will be displayed in the application definition UI under a new category called “New Account Dependency Entitlements Feature”.



## Settings

This is a string type extended attribute called “accountCreateEntitlements” (not indexed) which holds a “|” delimited list of entitlements in the format: Application Name#Entitlement Name#Entitlement Value. This string value will be parsed into access request objects that will be added to the original provisioning plan. For LDAP based entitlements there is a need to type in the full DN for an entitlement value. Below are some of the format examples.

### Single Entitlement

LDAP Application Name#LDAP Application Attribute Name# LDAP ApplicationGroup DN

### Multiple Entitlements Different Applications

Database Application Name#Database Group Attribute Name#Database User Group Name|LDAP Application Name#LDAP Application Attribute Name#LDAP ApplicationGroup DN

### Multiple Entitlements Same Application

LDAP Application Name#LDAP Application Attribute Name#LDAP ApplicationGroup DN|LDAP Application Name#LDAP Application Attribute Name#LDAP ApplicationGroup DN

***Please Note:*** *This format is automatically set via Self Service Onboarding Wizard*

## Conditional Rule

This is a string type extended attribute “accountCreateConditionalRule” (not indexed) which holds the name of a Rule that determines if the provisioning of the underlying infrastructure, technology, or platform entitlements for this application should be provisioned or not. This field is optional. Leaving this blank will cause the provisioning of underlying infrastructure, technology, or platform entitlements for this application to always be provisioned.

The Rule receives 2 parameters (aside from the implicit “context” and “log” objects which are available to all Rule objects):

* **originalPlan**: the original ProvisioningPlan object for the Application in turn
* **appName**: the name of the Application for which the “After Provisioning” Rule is currently being executed

The Rule also must return a Boolean “true” value if the provisioning should be executed, or a “false” value if the provisioning should be skipped or omitted.

## Rule Configuration

In order for this feature to work properly, the following configuration settings are required on the applications that require additional infrastructure, technology, and or platform entitlements.

**Important Note**: When configuring dependency entitlements for **dual-channel applications**, make sure to set the configuration on the application which handles the actual provisioning.

1. The Dependency Entitlements field must be filled out with the correct values and format
2. (Optional) The Conditional Omit Dependency Entitlements Rule field can have the name of a Rule which determines if the provisioning of additional entitlements for this application should be executed or not.
3. The “After Provisioning Rule” must be configured on each application that requires additional Infrastructure/Technology, depending on one of the following use cases
   1. If the application’s “After Provisioning Rule” drop-down is not already being used by another rule, then configure it with a rule called “Rule-AccountCreation-Dependency-Framework”
   2. If the application’s “After Provisioning Rule” drop-down is already being used by another rule, or if in the future additional “After Provisioning” business logic is required, then simply edit the existing rule and add the reference to the dependency Rule Library and a call to the method which processes the dependency feature at the end of the rule’s code.
      1. Add the reference to the Rule Library “Rule-AccountCreationDependency-RuleLibrary” and “Rule-Framework-AfterBeforeProvisionRuleLibrary”in the <ReferencedRules> tag of the “After Provisioning” Rule.
      2. Add a call to the method named “addAccountCreateDependencyRequests” at the end of the code, such that it’s the last step in the business logic. This method is declared inside of the Rule Library described above, and receives 2 input parameters, which are also input parameters available to all “After Provisioning” type Rules (see the Rule’s <Signature> tag for details on its input and output parameters):

* **plan**: the ProvisioningPlan object, for the Application in turn, that was just provisioned via the application’s connector (or other provisioning integration method).
* **application.getName()**: the name of the application in turn, for which this “After Provisioning” Rule is being run.

# Data Flow

Once the “After Provisioning Rule“ and ”Conditional Omit Dependency Entitlements Rule” rules are set for the applications, the basic flow of the process is as follows.

1. The “After Provisioning Rule” executes on an application and the dependency feature is called.
2. Check if the provisioning of the original access for the application in turn was successful. If yes, then continue.
3. Check if this is an access request, Lifecycle request, Batch request, or role assignment request. If yes, then continue.
4. If the application contains a defined ”Conditional Omit Dependency Entitlements Rule”, then execute it. If the result is TRUE, then continue; otherwise skip the provisioning for that application. If no rule is specified, then continue.
5. If the identity has any dependency entitlements, then continue.
6. Inspect the original provisioning plan and see if it has an account Create operation for the specific Application in turn. If yes, then continue.
7. Create a new provisioning plan based on the Dependency Entitlements field value.
8. Launch a new instance of the Access Request Workflow to provision the entitlements.

