

DN Change Scanner

IdentityIQ Version: [Version 7]

This is the Word template for all SailPoint Services Enablement documents. Document description text, if any, goes here as DocDescription paragraph style. This might describe usage of the document, especially in the case of sample docs or templates. For example, to use this template, replace header labels and sample body text with your content or just delete of the body content and begin from scratch, applying the configured paragraph styles to your document as appropriate.

Document Revision History

|  |  |  |
| --- | --- | --- |
| **Revision Date** | **Written/Edited By** | **Comments** |
| Jan 2017 | Palle Hansen | Initial Draft |
|  |  |  |

**© Copyright 2017 SailPoint Technologies, Inc., All Rights Reserved.**

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

**Restricted Rights Legend**. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

**Regulatory/Export Compliance**. The export and reexport of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or reexport outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not 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. Government's Entities List; a party prohibited from participation in export or reexport 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.

**Trademark Notices**. Copyright © 2017 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo, SailPoint IdentityIQ, and SailPoint Identity Analyzer are trademarks of SailPoint Technologies, Inc. and may not be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

[DN Change Scanner 4](#_Toc473549420)

[Artefacts 4](#_Toc473549421)

[AuditConfig 4](#_Toc473549422)

[TaskDefinition 4](#_Toc473549423)

[Java Classes 4](#_Toc473549424)

[DNChangeScanner.java 4](#_Toc473549425)

[DNChangeHandler.java 4](#_Toc473549426)

[AuditWriter.java 4](#_Toc473549427)

[AuditConfig 5](#_Toc473549428)

[TaskDefinition 5](#_Toc473549429)

[Note: 6](#_Toc473549430)

[Use Cases 6](#_Toc473549431)

[Distinguished Name (DN) of an Account is changed natively in the target application 6](#_Toc473549432)

[Distinguished Name (DN) of a Group is changed natively in the target application 7](#_Toc473549433)

[Distinguished Name (DN) of an Account is changed in IdentityIQ 7](#_Toc473549434)

[Distinguished Name (DN) of a Group is changed in IdentityIQ 7](#_Toc473549435)

[Important 8](#_Toc473549436)

(This TOC page is optional and may be omitted for short documents.)

DN Change Scanner

Small utility designed to detect if a distinguished name (DN) has changed on a given application. In case if a change being detected it will call DN Change Handler to deal with the given change.  
The DN Change Scanner is designed to be run as a Task Definition, and is intended to be run in a sequential task definition straight after the configured applications Account-Group and Account Aggregation. So, that it can deal with any changes to distinguished name as soon as they are detected.

# Artefacts

## AuditConfig

AuditConfig called DNChangeAudit, so that all actions performed by the DNChangeScanner utility can be audited in its own custom audit entry. The default for this AuditConfig is that auditing is set to True.

The AuditConfig is delivered as a Merge File, that can either be used as is in a build repository or can be copied/merged into an existing AuditConfig file.

## TaskDefinition

A TaskDefinition called “DN Change Scanner” is delivered as an xml file designed to go into a build directory. This TaskDefinition allows configuration of all the Options for the task.

## Java Classes

The following Java Classes are delivered.

### DNChangeScanner.java

* Creates and maintains a custom database table custom\_immutable
* Compared Link DN to the previously stored DN based on an immutable ID and calls DNChangeHandler if it detects a difference.

## DNChangeHandler.java

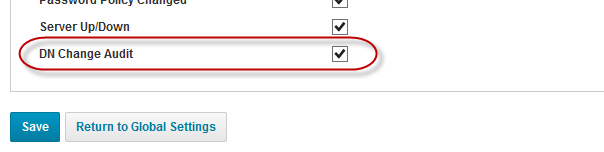
* Looks for objects in IdentityIQ where the OldDN is stored and replaces it with the NewDN

## AuditWriter.java

* Small helper class to write Audit Events for the above two classes

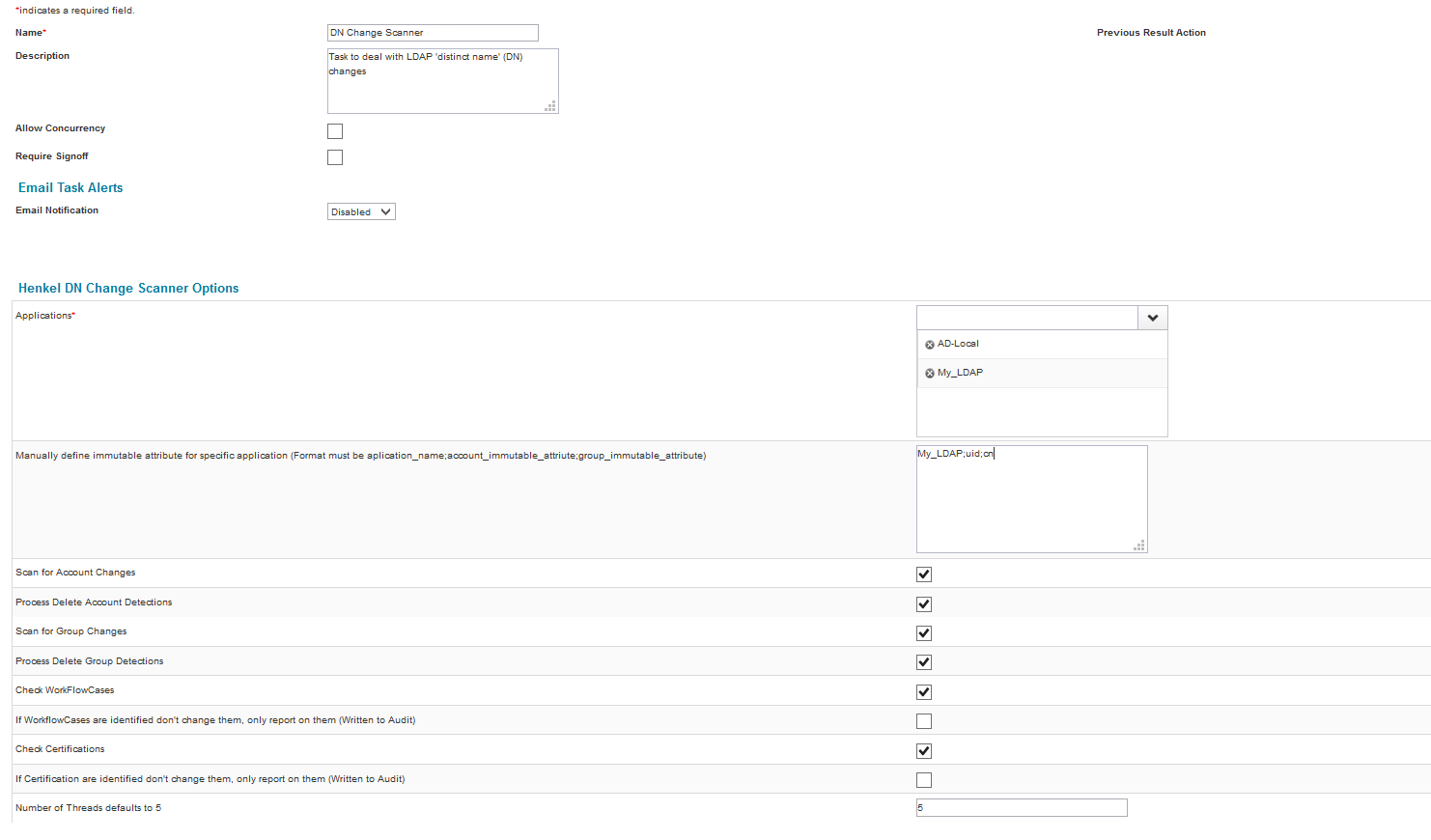
# AuditConfig

Under Gear🡪Global Settings🡪Audit Configuration there is a new entry where you can toggle audit on or off for the DN Change utility.



# TaskDefinition

Under Setup🡪Tasks there is a new task called “DN Change Scanner”



* “Applications”: select one or more application to include when detecting changes to DN, the utility will validate the selected applications.
* “Manually define immutable attribute”: optional attribute, if this is not filled in for an application then the tool will use the database column uuid on spt\_link and spt\_managed\_attribute fot the immutable value, but if this for whatever reason is not populated or usable, then you man manually specify what Account attribute and what Group attribute to use for a given application.
* “Scan for Account Changes”: Select this option if you wish the utility to scan for Accounts on the selected applications.
* “Process Delete Account Detections” Only relevant if “Scan for Account Changes” is selected.  
  This option causes the tool to delete the following from the Identity.  
  + Role Assignment relating to the deleted account
  + Role Detection related to the deleted account
  + Attribute Assignment related to the deleted account
  + Exceptions related to the deleted account

It also terminates any WorkflowCases and IdentityRequest containing a ProvisioningPlan with the deleted account if “Check WorkFlowCases” is selected unless “If WorkflowCases are Identified don’t change them only report on them” is selected then it only reports on them.

* “Scan for Group Changes”: Select this option if you wish the utility to scan for Groups on the selected applications.
* “Process Delete Group Detections” Only relevant if “Scan for Group Changes” is selected.  
  This option causes the tool to delete and Profile from a Role where the Profile containing the deleted Group.
* “Check WorkFlowCases”: if selected then the utility will change any WorkFlowCases i.e. Access Requests etc.
* “If WorkflowCases are Identified don’t change them only report on them”: if this is checked as well as “Check WorkFlowCases” then the utility will write to the audit log what WorkflowCases would have been changed, but will not actually change anything.
* “Check Certifications”: if selected then the utility will change any non-completed Certifications
* “If Certifications are Identified don’t change them only report on them”: if this is checked as well as “Check Certifications” then the utility will write to the audit log what Certifications would have been changed, but will not actually change anything.
* “Number of Threads”: specify how many worker threads the utility should work with, it defaults to 5

### Note:

The first time the utility is run for a given Application(s) it will not do anything other than build up the content of the custom\_immutable table, if Audit is DNChangeAudit is enabled then it will write a line in the audit table for each entry it writes into the custom\_immutable table, to avoid this potentially large amount of audit data, just disable the audit configuration the first time the utility is run.  
If an application gets removed from the list then the utility will remove all rows in the custom\_immutable for the given application.

### Note2:

“Process Delete Account Detections” and “Process Delete Group Detections” should only be used if those object is expected to get deleted from the native application, ideally the delete process should be driven from IdentityIQ.

# Use Cases

## Distinguished Name (DN) of an Account is changed natively in the target application

If the utility has already been run the first time it would have created a base line. The utility will then detect that the DN has changed natively and it will then update all the references to this DN in

* The Identity
* The Link Object
* WorkFlowCases subject to configuration
* Certifications subject to configuration.

## Distinguished Name (DN) of a Group is changed natively in the target application

If the utility has already been run the first time it would have created a base line. The utility will then detect that the DN has changed natively and it will then update all the references to this DN in

* The Identity (All Identities connected to the given Group)
* The ManagedAttribute Object
* The ProfileContraints Object (Role Definition)
* WorkFlowCases subject to configuration
* Certifications subject to configuration.

## Distinguished Name (DN) of an Account is changed in IdentityIQ

Once the Provisioning is completed and successful, the following can be run to modify all the references to this DN in IIQ  
  
Instantiate the Class DNChangeHandler

DNChangeHandler ch = new DNChangeHandler(context, applicationId, newDN, oldDN)

Or

DNChangeHandler ch = new DNChangeHandler(context, applicationId, newDN, oldDN, workFlowCaseCheck, certificationCheck, workFlowCaseCheckReport, certificationCheckReport)

Then call

ch.changeAllDNReferencesForAccount(identityID);

## Distinguished Name (DN) of a Group is changed in IdentityIQ

Once the Provisioning is completed and successful, the following can be run to modify all the references to this DN in IIQ  
  
Instantiate the Class DNChangeHandler

DNChangeHandler ch = new DNChangeHandler(context, applicationId, newDN, oldDN)

Or

DNChangeHandler ch = new DNChangeHandler(context, applicationId, newDN, oldDN, workFlowCaseCheck, certificationCheck, workFlowCaseCheckReport, certificationCheckReport)

Then call

ch.changeAllDNReferencesForGroup();

# Important

This utility has only been unit tested locally, and should be properly tested before being used in a production environment.