TECHNICAL REFERENCE

Oracle Consulting Services

Identity Manager Deployment

Author: Dieter Steding

Creation Date: 03-06-2019

Latest Update: 28-06-2019

Control Number: OC\_DE/ 400072624/DO.070/0003

Version: 1.0.0.0

**Approval:**

|  |  |
| --- | --- |
| Oracle Consulting Services |  |
| Technical Director |  |

logored Copy-Nr. \_\_\_\_\_

## Document Control

### Change Record

| Date | Author | Version | | Change Reference |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 03-06-19 |  | 1.0.0.0 | No previous document | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
| Sophie Strecke | Security Architect |
| Melinda Nath-Richter | Principal Consultant Identity & Access Mgmt |
| Rashi Rastogi | Principal Consultant Security |
| Joao Bandeira | Principal Consultant |

### Distribution

| Copy No. | Name | Location |
| --- | --- | --- |
|  |  |  |
| 1 | Library Master | Project Library |
| 2 |  | Project Manager |
| 3 |  |  |
| 4 |  |  |

Table of Contents

[Document Control ii](#_Toc12611141)

[Change Record ii](#_Toc12611142)

[Reviewer ii](#_Toc12611143)

[Distribution ii](#_Toc12611144)

[Preface 1](#_Toc12611145)

[Audience 1](#_Toc12611146)

[Confidentiality 1](#_Toc12611147)

[Typographical Conventions 1](#_Toc12611148)

[Related Documents 1](#_Toc12611149)

[What is New in Identity Manager Deployment? 2](#_Toc12611150)

[Importing and Exporting Deployments 3](#_Toc12611151)

[Exporting Deployments 3](#_Toc12611152)

[Importing Deployments 4](#_Toc12611153)

[Managing Access Policies 5](#_Toc12611154)

[Features of Access Policies 5](#_Toc12611155)

[Provisioning 5](#_Toc12611156)

[Denying a Resource 5](#_Toc12611157)

[Creating Access Policies 5](#_Toc12611158)

[Parameters 5](#_Toc12611159)

[Modifying Access Policies 6](#_Toc12611160)

[Parameters 6](#_Toc12611161)

[Parameters specified as nested elements 6](#_Toc12611162)

[Deleting Access Policies 7](#_Toc12611163)

[Exporting Access Policies 7](#_Toc12611164)

[Importing Access Policies 7](#_Toc12611165)

[Managing Admin Roles 9](#_Toc12611166)

[Creating Admin Roles 9](#_Toc12611167)

[Modifying Admin Roles 9](#_Toc12611168)

[Deleting Admin Roles 9](#_Toc12611169)

[Managing Attribute Definitions 10](#_Toc12611170)

[Creating Attribute Definitions 10](#_Toc12611171)

[Modifying Attribute Definitions 10](#_Toc12611172)

[Deleting Attribute Definitions 10](#_Toc12611173)

[Exporting Attribute Definitions 10](#_Toc12611174)

[Importing Attribute Definitions 10](#_Toc12611175)

[Managing Lookup Definitions 11](#_Toc12611176)

[Creating Lookup Definitions 11](#_Toc12611177)

[Modifying Lookup Definitions 11](#_Toc12611178)

[Deleting Lookup Definitions 11](#_Toc12611179)

[Exporting Lookup Definitions 11](#_Toc12611180)

[Importing Lookup Definitions 11](#_Toc12611181)

[Managing System Properties 12](#_Toc12611182)

[Features of System Properties 12](#_Toc12611183)

[Creating System Properties 12](#_Toc12611184)

[Parameters 12](#_Toc12611185)

[Modifying System Properties 12](#_Toc12611186)

[Parameters 12](#_Toc12611187)

[Deleting System Properties 13](#_Toc12611188)

[Exporting System Properties 13](#_Toc12611189)

[Importing System Properties 13](#_Toc12611190)

## Preface

### Audience

This guide is intended for resource administrators and target system integration teams.

### Confidentiality

The material contained in this documentation represents proprietary, confidential information pertaining to Oracle products and methods

The audience agrees that the information in this documentation shall not be disclosed outside of Oracle, and shall not be duplicated, used, or disclosed for any purpose other than to evaluate this procedure.

### Typographical Conventions

The following typographical conventions are used in this document.

|  |  |
| --- | --- |
| **Convention** | **Meaning** |
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. Examples include window/page titles, keywords, and interactive elements such as menus, buttons, etc.. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |
| [hyperlink](https://www.oracle..com) | A link to another section of the document or to an external document or website. |

### Related Documents

| **Nr.** | **Document** |
| --- | --- |
| 1 | For information about installing and using Oracle Identity and Access Management, visit the following Oracle Help Center page <https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html> |
| 2 | For information about Oracle Linux 7 documentation, visit the following Oracle Help Center page <https://docs.oracle.com/cd/E52668_01/index.html> |
| 3 |  |
| 4 |  |

## What is New in Identity Manager Deployment?

## Importing and Exporting Deployments

The Deployment Manager is a tool for exporting and importing Identity Manager Configurations. The Deployment Manager lets you export the objects that constitute the Identity Manager configuration. Usually, you use the Deployment Manager to migrate a configuration from one deployment to another, for example, from a test to a production deployment, or to create a backup of your system.

You can export objects from your Identity Manager system and save them in an XML file. This generated files you can later use to import to another deployment.

The following are limitations of the Deployment Manager:

|  |  |
| --- | --- |
| **Limitation** | **Meaning** |
| **Merge Utility** | The Deployment Manager is not a merge utility.  It cannot handle modifications done in both production and test environments. It replaces the object in the target system with that in the XML file. |
| **Version Control Utility** | The Deployment Manager does not track versions of imported files, and does not provide rollback functionality.  You can only use it as a means to move data between environments. |

### Exporting Deployments

The Deployment Manager Export handles the following categories of information:

|  |  |
| --- | --- |
| **Category** | **Meaning** |
| AccessPolicy | Access policies are a list of roles and the resources with which roles are to be provisioned or deprovisioned. Access policies are used to automate the provisioning of target systems to users. |
| AdminRole | An Admin Role defines the actions, also known as functional capabilities, that can be performed and the scope of control (the scope of control refers to the set of organizations managed by the admin role). |
| ApplicationInstance | Application instance is a abstraction used in Identity Manager. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). |
| ApprovalPolicy | Approval policy is a configurable entity of request management that helps associate various request types with approval processes defined in the request service only for request-level and operation-level approvals. |
| AttestationProcess | Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe entitlements of other users. |
| AttributeDefinition |  |
| CatalogDefinition |  |
| CategoryDefinition |  |
| CertificationDefinition |  |
| CertificationConfiguration |  |
| CustomResourceBundle |  |
| DataObjectDef |  |
| EmailDef |  |
| EntityAdapter |  |
| EntityPublication |  |
| ErrorCode |  |
| EventHandler |  |
| TBD complete |  |
| System Properties | System properties define the characteristics that control the behavior of Oracle Identity Manager. You can define the functionality of consoles such as the Oracle Identity Administration and Oracle Identity Manager Self Service by using system properties. |

### Importing Deployments

Objects that were exported to an XML file by using the Deployment Manager can be imported into Oracle Identity Manager by using the Deployment Manager. You can import all or part of the XML file, and you can import multiple XML files at once. The Deployment Manager ensures that the dependencies for any objects you are importing are available, either in the import or in your system.

## Managing Access Policies

Access policies are a list of roles and the resources with which roles are to be provisioned or deprovisioned. Access policies are used to automate the provisioning of target systems to users.

### Features of Access Policies

This section describes the various features offered by an access policy in the following sections:

1. Provisioning
2. Denying a Resource

#### Provisioning

Whenever an access policy is applied, the resources are directly provisioned to the user without the any request being generated.

#### Denying a Resource

While creating or modifying an access policy, you can select resources to be denied along with resources to be provisioned for roles.

If you first select a resource for provisioning and then select the same resource to be denied, then Identity Manager removes the resource from the list of resources to be provisioned.

If two policies are defined for a role in which one is defined to provision a resource and the other is defined to deny the resource, then Identity Manager does not provision the resource irrespective of the priority of the policies

### Creating Access Policies

To create an access policy you must specify the required parameter of the access policy and at least one resource to provision or deny as nested elements.

#### Attributes

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of an access policy in Identity Manager | yes |
| **description** | A formal description of the usage of the access policy | yes |
| **priority** | A numeric attribute containing a number that is unique for each access policy you create. The lower the number, the higher is the priority of the access policy.  Identity Manager uses the highest priority policy data for an account form. | no  Defaults to -1 |
| **request** |  | no  Defaults to false |
| **retrofit** | If you select true, then the access policy is applied to all existing roles that you select during access policy creation. It means if existing user have the selected Roles then access policy will apply for those users also. | no  Defaults to true |
| **ownerType** |  | no  Defaults to User |
| **ownerName** |  | no  Defaults to xelsysadm |

### Modifying Access Policies

To modify an access policy you must specify the name of the access policy to modify.

#### Attributes

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of an access policy in Identity Manager | yes |
| **description** | A formal description of the usage of the access policy | no |
| **priority** | A numeric attribute containing a number that is unique for each access policy you create. The lower the number, the higher is the priority of the access policy.  Identity Manager uses the highest priority policy data for an account form. | no  Defaults to -1 |
| **request** |  | no  Defaults to false |
| **retrofit** | If you select true, then the access policy is applied to all existing roles that you select during access policy creation. It means if existing user have the selected Roles then access policy will apply for those users also. | no  Defaults to true |
| **ownerType** |  | no  Defaults to User |
| **ownerName** |  | no  Defaults to xelsysadm |

#### Parameters specified as nested elements

An access policy type accepts following nested elements:

| **Element** | **Description** | **Required** |
| --- | --- | --- |
| **provision** |  | no |
| **deny** |  | no |

### Deleting Access Policies

To delete an access policy you must specify the name of the access policy to delete.

|  |  |
| --- | --- |
| D:\tt\icon-restrict-16.png | Restrict: |
| This operation does not support any other parameter or nested elements. |

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of an access policy in Identity Manager | yes |

### Exporting Access Policies

Access Policies can be exported to an XML file.

|  |  |
| --- | --- |
| D:\tt\icon-tip-16.png | Tip: |
| Oracle Consulting does not recommend exporting Access Policies due to the prefix behavior of connectors regarding lookup values end entitlements.  Prefixing is based on the system identifier of an IT Resource. The system identifier is a database sequence.  It cannot be ensured that such sequence is coordinated on the same stage across environments like development, test or production.  A lot of effort is required to keep the IT Resource prefix in sync with the actual deployment of an Identity Manager instance. |

To export a access policy it is required to embed the category *AccessPolicy* in an Export Set.

|  |  |
| --- | --- |
|  | Code: |
| <object:exportSet exportFile ="0701 systemConnector ODS/xml/ods-policy-dm.xml"  description="ODS Access Policy Configuration>  <object:category value="AccessPolicy" name="ODS Basic Account"/>  <object:category value="AccessPolicy" name="ODS Administrator"/>  </object:exportSet> |

### Importing Access Policies

Access Policies can be imported to an XML file. The file needs to be a nested parameter of an Import Set

|  |  |
| --- | --- |
| D:\tt\icon-tip-16.png | Tip: |
| Oracle Consulting does not recommend importing Access Policies due to the prefix behavior of connectors regarding lookup values end entitlements.  Prefixing is based on the system identifier of an IT Resource. The system identifier is a database sequence.  It cannot be ensured that such sequence is coordinated on the same stage across environments like development, test or production.  A lot of effort is required to keep the IT Resource prefix in sync with the actual deployment of an Identity Manager instance. |

|  |  |
| --- | --- |
|  | Code: |
| <object:importSet dir="0701 systemConnector ODS/xml">  <object:importFile name="ods-policy-dm.xml"/>  </object:import> |

## Managing Admin Roles

An Admin Role defines the actions, also known as functional capabilities, that can be performed and the scope of control (the scope of control refers to the set of organizations managed by the admin role).

### Creating Admin Roles

To create an admin role you must specify the required parameter of the admin role

### Modifying Admin Roles

To modify admin role you must specify the name of the admin role to modify.

### Deleting Admin Roles

To delete an admin role you must specify the name of the admin role to delete.

|  |  |
| --- | --- |
| D:\tt\icon-restrict-16.png | Restrict: |
| This operation does not support any other parameter or nested elements. |

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of an admin role in Identity Manager | yes |

## Managing Attribute Definitions

### Creating Attribute Definitions

.

|  |  |
| --- | --- |
|  | Important: |
| Creating Attribute Definitions is not supported using Identity Manager Deployment. |

### Modifying Attribute Definitions

|  |  |
| --- | --- |
|  | Important: |
| Modifying Attribute Definitions is not supported using Identity Manager Deployment. |

### Deleting Attribute Definitions

|  |  |
| --- | --- |
|  | Important: |
| Deleting Attribute Definitions is not supported using Identity Manager Deployment. |

### Exporting Attribute Definitions

Attribute Definitions can be exported to an XML file.

To export a lookup definition it is required to embed the category to export in an Export Set.

|  |  |
| --- | --- |
|  | Code: |
| <object:exportSet exportFile ="0101 entityCustomization/xml/ocs-identity-dm.xml"  description="OCS Standard Entity Configuratio>  <object:category value=" User Metadata " name="division"/>  <object:category value=" User Metadata " name="department"/>  </object:exportSet> |

### Importing Attribute Definitions

Attribute Definitions can be imported from an XML file. The file needs to be a nested parameter of an Import Set

|  |  |
| --- | --- |
|  | Code: |
| <object:importSet dir="0101 entityCustomization/xml">  <object:importFile name="ocs-identity-dm.xml"/>  </object:import> |

## Managing Lookup Definitions

### Creating Lookup Definitions

.

|  |  |
| --- | --- |
|  | Important: |
| Creating Lookup Definitions is not supported using Identity Manager Deployment. |

### Modifying Lookup Definitions

|  |  |
| --- | --- |
|  | Important: |
| Modifying Lookup Definitions is not supported using Identity Manager Deployment. |

### Deleting Lookup Definitions

|  |  |
| --- | --- |
|  | Important: |
| Deleting Lookup Definitions is not supported using Identity Manager Deployment. |

### Exporting Lookup Definitions

Lookup Definitions can be exported to an XML file.

To export a lookup definition it is required to embed the category to export in an Export Set.

|  |  |
| --- | --- |
|  | Code: |
| <object:exportSet exportFile ="0100 systemFramework/xml/ocs-lookup-dm.xml"  description="OCS System Lookup Configuration>  <object:category value="Lookup" name="OCS.YesNo"/>  </object:exportSet> |

### Importing Lookup Definitions

Lookup Definitions can be imported from an XML file. The file needs to be a nested parameter of an Import Set

|  |  |
| --- | --- |
|  | Code: |
| <object:importSet dir="0100 systemFramework/xml">  <object:importFile name="ocs-lookup-dm.xml"/>  </object:import> |

## Managing System Properties

System properties define the characteristics that control the behavior of Oracle Identity Manager. You can define the functionality of consoles such as the Oracle Identity Administration and Oracle Identity Manager Self Service by using system properties.

### Features of System Properties

This section describes the various features offered by a system property in the following sections:

### Creating System Properties

To create a system property you must specify the required parameter of the property.

#### Parameters

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of a system property in Identity Manager | yes |
| **value** | A value mapped at name in Identity Manager | yes |
| **description** | A formal description of the usage of the system property | no |
| **loginRequired** | Specifies whether or not a login is required to access the system property. The default value of this field is 1, which means that a login is required to access the system property. | no |

### Modifying System Properties

To modify a system property you must specify the name of the system property to modify.

#### Parameters

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of a system property in Identity Manager | yes |
| **value** | A value mapped at name in Identity Manager | no |
| **description** | A formal description of the usage of the system property | no |
| **loginRequired** | Specifies whether or not a login is required to access the system property. The default value of this field is 1, which means that a login is required to access the system property. | no |

### Deleting System Properties

To delete a system property you must specify the name of the system property to delete.

|  |  |
| --- | --- |
| D:\tt\icon-restrict-16.png | Restrict: |
| This operation does not support any other parameter or nested elements. |

| **Attribute** | **Description** | **Required** |
| --- | --- | --- |
| **name** | The unique identifier of a system property in Identity Manager | yes |

### Exporting System Properties

System Properties can be exported to an XML file.

### Importing System Properties

System Properties can be imported to an XML file.

|  |  |
| --- | --- |
| D:\tt\icon-restrict-16.png | Restrict: |
|  |

|  |  |
| --- | --- |
|  | Important: |
|  |

|  |  |
| --- | --- |
| D:\tt\icon-caution-16.png | Caution: |
|  |

|  |  |
| --- | --- |
| D:\tt\icon-warning-16.png | Warning |
|  |

|  |  |
| --- | --- |
| D:\tt\icon-note-16.png | Note: |
|  |

|  |  |
| --- | --- |
| D:\tt\icon-tip-16.png | Tip: |
|  |