Administrator Guide

AM.IAM Provider Discovery

Author: Dieter Steding  
 Sophie Strecke

Creation Date: 01-08-2019

Last Updated: 01-12-2020

Document Ref: OC\_DE/300516442/DO.081/0018

Version: 1.2

**Approvals:**

|  |  |
| --- | --- |
| Bundeskriminalamt |  |
| Oracle Consulting |  |

logored Copy-No. \_\_\_\_\_

## Document Control

### Change Record

| Date | Author | Version | | Change Reference |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 01-08-19 |  | 1.0 | No Previous Document | |
| 30-04-20 | Sophie Strecke | 1.1 | Picture Legends corrected | |
| 08-09-20 | Sylvert Bernet | 1.2 | Layout changes of discovery Page | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
| Rene Donner | Project Leader |
|  |  |
|  |  |
|  |  |

Contents

[Document Control ii](#_Toc59097809)

[Change Record ii](#_Toc59097810)

[Reviewer ii](#_Toc59097811)

[Introduction 1](#_Toc59097812)

[Audience 1](#_Toc59097813)

[Related Documents 1](#_Toc59097814)

[Confidentiality 1](#_Toc59097815)

[Conventions 1](#_Toc59097816)

[Requirements 2](#_Toc59097817)

[Responsive Design 2](#_Toc59097818)

[Multi-Language Support 2](#_Toc59097819)

[Provider Sharing 2](#_Toc59097820)

[Setup 3](#_Toc59097821)

[Prepare Deployment 3](#_Toc59097822)

[Installing the Application Archive 3](#_Toc59097823)

[Select Archive 3](#_Toc59097824)

[Select Target 3](#_Toc59097825)

[Application Attribute 4](#_Toc59097826)

[Deployment Settings 4](#_Toc59097827)

[Proxy Configuration 4](#_Toc59097828)

[User Interface 5](#_Toc59097829)

[Login Page 5](#_Toc59097830)

[Layout 5](#_Toc59097831)

[Navigation 5](#_Toc59097832)

[Personalization 6](#_Toc59097833)

[Coat of arms 6](#_Toc59097834)

[Configuration 10](#_Toc59097835)

[Attributes 11](#_Toc59097836)

[Operations 11](#_Toc59097837)

[Register a Provider 11](#_Toc59097838)

[List Providers 12](#_Toc59097839)

[Remove a Provider 13](#_Toc59097840)

[Register a Location 13](#_Toc59097841)

[List Locations 13](#_Toc59097842)

[Remove a Location 14](#_Toc59097843)

[Modify a Location 14](#_Toc59097844)

## Introduction

### Audience

This document is intended for people who administer the Oracle Identity and Access Management Infrastructure of the Federal Criminal Police Office in the context of federated Identity and Access Management.

The particular focus of this document is on the credential collector.

### Related Documents

For information about installing and using Oracle Access Manager, visit the following Oracle Help Center page:

* https://docs.oracle.com/en/middleware/idm/suite/12.2.1.3/index.html

### 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.

### Conventions

The following text 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. |
| *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. |

## Requirements

### Responsive Design

The pages the credential collector presents needs to be responsive.

A site designed with Responsive Design adapts the layout to the viewing environment by using fluid, proportion-based grids, flexible images, and CSS3 media queries, an extension of the @media rule.

### Multi-Language Support

The content of the site is primarily used by German-speaking users. It can be expected within international cooperation that foreign users will also use the site, so at least English must be implemented as another language.

### Provider Sharing

Not every participant will be able to provide an own infrastructure belonging to the Identity and Access Management.

Especially the Identity Provider required for authentication purpose is not available.

For this reason, Access Manager is used as an Identity Provider for those participants.

From this perspective, it must be possible that Identity Providers can be shared across items in the selection of available Identity Providers.

## Setup

The customization is packaged in a single an archive file is that contains all of the application's static files, directories, and deployment descriptor files.

| **Specification** | **Archive** |
| --- | --- |
| **Application** | idp.iam.access.module.war |

### Prepare Deployment

The web application is provided in the cluster of managed servers of the Oracle Access Manager.

For this purpose, a directory is created for storing the application archive on each participating node of the cluster.

The web application is then made available from this directory.

| **Specification** | **Directory** |
| --- | --- |
| **ORACLE\_BASE** | /opt/oracle/product/fmw/12.2.1/usr/apps |

|  | **Command** |
| --- | --- |
| mkdir -p /opt/oracle/product/fmw/12.2.1/usr/apps |

Be sure to save the application to the */opt/oracle/product/fmw/12.2.1/usr/apps* directory you.

|  | **Important** |
| --- | --- |
| This step has to have to repeat on each node of the cluster **oas**. |

The provision of the application archive is made via the Fusion Middleware Control.

### Installing the Application Archive

#### Select Archive

| **Option** | **Value** |
| --- | --- |
| **Scope** | Global |
| **Archive or Exploded Directory** | Archive or exploded directory is on the server where Enterprise Manager is running. |
| **Archive** | /opt/oracle/product/fmw/12.2.1/usr/apps/idp.iam.access.module.war |
| **Deployment Plan** | Create a new deployment plan when deployment configuration is done. |
| **Deployment Type** | Deploy this archive or exploded directory as an application |

#### Select Target

| **Option** | **Value** |
| --- | --- |
| **Select Target** | oas |

#### Application Attribute

| **Option** | **Value** | |
| --- | --- | --- |
| **Application Name** | idp.iam.access.module.war | |
| **Context Root of Web Modules** | **Web Module** | **Context Root** |
|  | idp.iam.access.module.war | /idp |
| **Distribution** | Install and start application (servicing all requests) | |
| **Other Options** |  | |
| **Application Source  Accessibility** | Make the application accessible from the source location that it will be deployed on. You must ensure that each target can reach the location. | |
| **Deployment Plan  Source Accessibility** | Use the same accessibility as the application. | |

#### Deployment Settings

| **Option** | **Value** |
| --- | --- |
|  |  |

### Proxy Configuration

The access to the application is proxied by an HTTP server hence following proxy rule needs to be included in the virtual host configuration

|  | **Script** |
| --- | --- |
| ###############################################  ## Entries Required by Identity Provider Discovery  ###############################################  <Location /idp>  Set Handler weblogic-handler  WebLogicHost vwasc181.zds.bka.bund.de  WebLogicPort 8009  </Location> |

## User Interface

The user interface provided consists of three parts:

1. a Discovery Page to choose an Identity Provider

The page has in common that they react to the geometry of the devices on which they are displayed (see Responsive Design).

The user interface supports multiple languages. The following languages are supported:

1. German
2. English

The control of which language is used is made via the settings of the browser.

In the following, the pages are presented anonymously.

### Login Page

#### Layout

The login page requests to choose an Identity Provider from a list of available Identity Providers.



#### Navigation

The click on a link displayed redirects back to Access Manager with the appropriate parameters to initiate the login process leveraging the chosen Identity Provider.

## Personalization

Each line introduced in the chapter above visualize a location hint

.

### Coat of arms

Following Coat of Arms are available for customization purpose:

|  |  |  |
| --- | --- | --- |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Saxony-Anhalt. |
| an-coa-s.png | an-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Brandenburg. |
| bb-coa-s.png | bb-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Berlin. |
| be-coa-s.png | be-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Federal Criminal Police Office. |
| bk-coa-s.png | bk-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Federal Police. |
| bp-coa-s.png | bp-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to (Polizei des Deutschen Bundestages) |
| bt-coa-s.png | bt-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Baden-Wuerttemberg. |
| bw-coa-s.png | bw-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Bavaria. |
| by-coa-s.png | by-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Bremen. |
| hb-coa-s.png | hb-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Hesse. |
| hb-coa-s.png | hb-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Hamburg. |
| hh-coa-s.png | hh-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Mecklenburg-Western Pomerania. |
| mv-coa-s.png | mv-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Lower-Saxony. |
| ni-coa-s.png | ni-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police North Rhine-Westphalia. |
| nw-coa-s.png | nw-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Rhineland-Palatinate. |
| rp-coa-s.png | rp-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Schleswig-Holstein. |
| sh-coa-s.png | sh-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Saarland. |
| sl-coa-s.png | sl-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Saxony. |
| sn-coa-s.png | sn-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Police Thuringia. |
| th-coa-s.png | th-coa-p.png |
|  |  | The indicator that the Identity Provider displayed in the list of available Identity Providers belongs to Customs Investigation Bureau. |
| zf-coa-s.png | zf-coa-p.png |

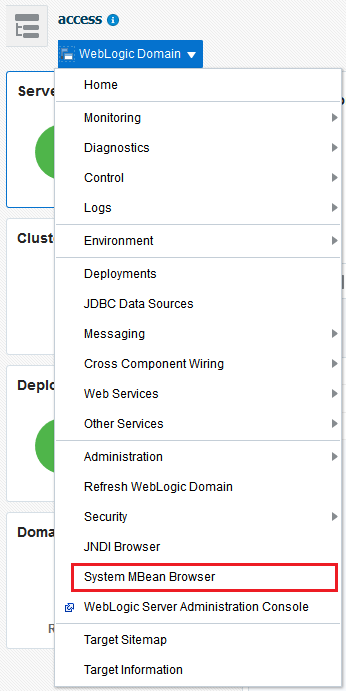
## Configuration

The configuration of the provider discovery is managed by Java Management Extensions (JMX).

The bean to configure is located in the runtime server and deployed automatically on each managed server.

The System MBean to configure the properties is accessed by Fusion Middleware Control deployed on the WebLogic Server domain access.

To configure the properties:

1. Login to Fusion Middleware Control using the credentials for an administrator or monitoring account.
2. Open the **System MBean Browser** from the **WebLogic Domain** drop-down  
     
   
3. In the **System MBean Browser** navigate in the **Application Defined MBeans** to

|  |  |
| --- | --- |
| **Entry** | **Value** |
| Node | bka.iam.platform |
| *Location (Server)* | oam (or any other member of a cluster) |
| *Application* | idp.iam.access.module |
| *Type* | idp |
| *Name* | config |

### Attributes

The bean has no attributes to configure

### Operations

To execute the view operations the attributes the role *Monitor User* is sufficient. To modify any property Administrator permissions are required

|  |  |  |
| --- | --- | --- |
| **Operation** | **Meaning** | **Role** |
| **providerRegister** | Extend the known providers and assigns one of the coats of arms to that provider and the issuer URL to redirect to the appropriate Identity Provider.  The provider itself is identified by a unique identifier obtained from the Access Manager configuration. | Administrators |
| **providerList** | Reports all configured providers registered and the coats of arms associated with them. | Monitor User / Administrators |
| **providerRemove** | Removes a particular provider | Administrators |
| **providerModify** | Associates an existing provider with a new coat of arms and the issuer URL to redirect to the appropriate Identity Provider. | Administrators |
| **locationRegister** | Extend the known networks and assigns one of the coats of arms to that network. The network itself is identified by an IPV4 address in CIDR-notation. | Administrators |
| **locationList** | Reports all configured networks and the coats of arms associated with them. | Monitor User / Administrators |
| **locationRemove** | Removes a particular network | Administrators |
| **locationModify** | Associates an existing network with a new coat of arms. | Administrators |
| **refresh** | Refresh the entire configuration by parsing the file system storage. | Monitor User / Administrators |
| **save** | Persist the changes done so far, to the file system storage. | Administrators |

#### Register a Provider

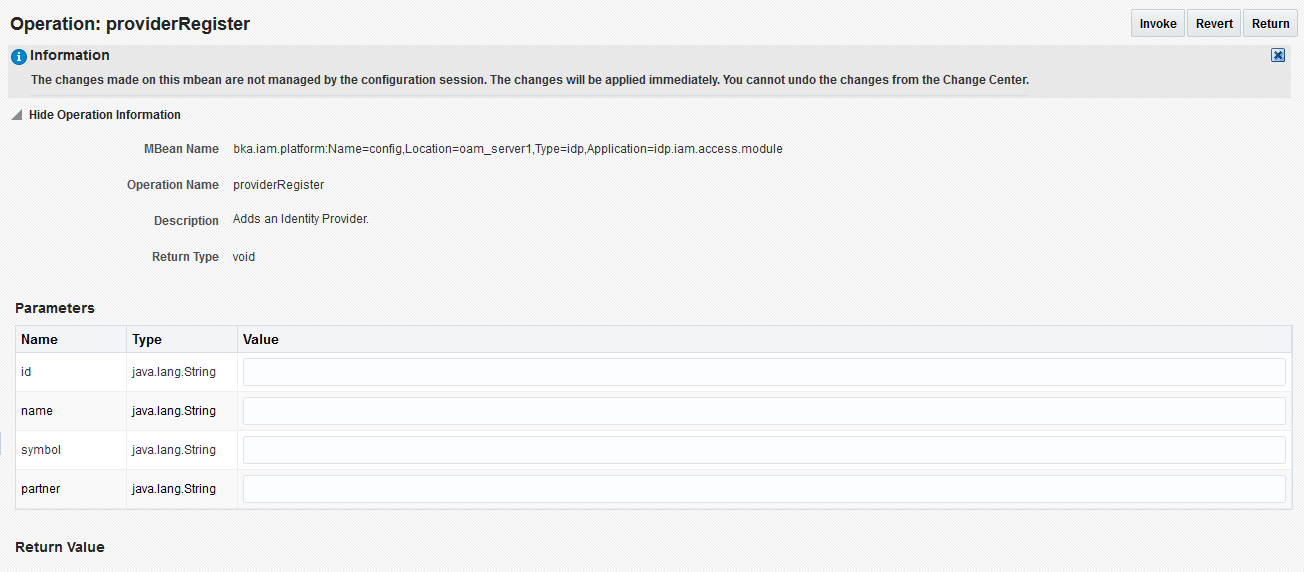
The operation providerRegister extends the known providers and assigns one of the coats of arms to that provider and the partner identifier obtained from the Access Manager configuration to redirect to the appropriate Identity Provider.

The provider itself is identified by a unique id

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| id | The internal identifier of the record |
| name | The unique name of the Identity Provider. This name is later on displayed in the graphical user interface to make this provider identifiable by end users. |
| symbol | A symbol to display in the graphical user interface in front of the unique name to support end users in identifying the partner configuration. |
| partner | The partner identifier of the provider obtained from the Access Manager configuration to redirect to the appropriate Identity Provider |

|  | **Caution** |
| --- | --- |
| The partner identifier must **exactly** match the Access Manager name of the Identity Providers configured in the Service Provider configuration. |



##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| idp.error.register | If the internal identifier of the provider to register is already registered |

#### List Providers

The operation providerList reports all configured providers and their associated properties.

##### Parameter

None

The operation providerRegister extends the known providers and assigns one of the coats of arms to that provider and the partner identifier obtained from the Access Manager configuration to redirect to the appropriate Identity Provider.

The provider itself is identified by a unique id

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| id | The internal identifier of the record |
| name | The unique name of the Identity Provider. This name is later on displayed in the graphical user interface to make this provider identifiable by end users. |
| symbol | A symbol to display in the graphical user interface in front of the unique name to support end users in identifying the partner configuration. |
| partner | The partner identifier of the provider obtained from the Access Manager configuration to redirect to the appropriate Identity Provider |

|  | **Caution** |
| --- | --- |
| The partner identifier must **exactly** match the Access Manager name of the Identity Providers configured in the Service Provider configuration. |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| idp.error.modify | If the internal identifier of the provider to modify not exists. |

#### Remove a Provider

The operation locationRemove removes a particular network

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| id | The internal identifier of the provider to remove. |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| idp.error.remove | If the internal identifier of the provider to remove not exists |

#### Register a Location

The operation locationRegister extends the known networks and assigns one of the coats of arms to that network. The network itself is identified by an IPV4 address in CIDR-notation.

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| cidr | The IPV4 address in CIDR-notation to register. |
| id | The internal identifier of a provider record to bind to the IPV4 address. |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| net.error.register | If the IPV4 address to register is already registered. |
| net.error.id | If the given id for the provider configuration is not registered yet. |

#### List Locations

The operation locationList reports all configured networks and the symbols associated with them.

##### Parameter

None

#### Remove a Location

The operation locationRemove removes a particular network

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| cidr | The IPV4 address in CIDR-notation to remove |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| net.error.remove | If the IPV4 address to remove is not registered yet |

#### Modify a Location

The operation locationModify associates an existing network with a new coat of arms

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| cidr | The IPV4 address in CIDR-notation to remove |
| id | The internal identifier of a provider record to bind to the IPV4 address. |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| net.error.modify | If the IPV4 address to modify is not registered yet |
| net.error.id | If the given id for the provider configuration is not registered yet. |

