Administrator Guide

AM.IAM Credential Collector

Author: Dieter Steding  
 Sophie Strecke

Creation Date: 01-08-2019

Last Updated: 01-12-2020

Document Ref: OC\_DE/300516442/DO.081/0017

Version: 1.0

**Approvals:**

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

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

## Document Control

### Change Record

| Date | Author | Version | | Change Reference |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 01-08-19 |  | 1.0 | No Previous Document | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

| Name | Position |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Contents

[Document Control ii](#_Toc59098209)

[Change Record ii](#_Toc59098210)

[Reviewer ii](#_Toc59098211)

[Introduction 1](#_Toc59098212)

[Audience 1](#_Toc59098213)

[Related Documents 1](#_Toc59098214)

[Confidentiality 1](#_Toc59098215)

[Conventions 1](#_Toc59098216)

[Requirements 2](#_Toc59098217)

[Responsive Design 2](#_Toc59098218)

[Multi-Language Support 2](#_Toc59098219)

[Setup 3](#_Toc59098220)

[Prepare Deployment 3](#_Toc59098221)

[Installing the Application Archive 3](#_Toc59098222)

[Select Archive 3](#_Toc59098223)

[Select Target 3](#_Toc59098224)

[Application Attribute 4](#_Toc59098225)

[Deployment Settings 4](#_Toc59098226)

[Proxy Configuration 4](#_Toc59098227)

[User Interface 5](#_Toc59098228)

[Login Page 5](#_Toc59098229)

[Layout 5](#_Toc59098230)

[Navigation 5](#_Toc59098231)

[Error Handling 6](#_Toc59098232)

[Logout Page 6](#_Toc59098233)

[Forgot Password Page 6](#_Toc59098234)

[Layout 6](#_Toc59098235)

[Navigation 7](#_Toc59098236)

[Error Handling 7](#_Toc59098237)

[Personalization 8](#_Toc59098238)

[Discovery 8](#_Toc59098239)

[Coat of arms 8](#_Toc59098240)

[Configuration 12](#_Toc59098241)

[Attributes 13](#_Toc59098242)

[Operations 13](#_Toc59098243)

[Register a Location 14](#_Toc59098244)

[List Locations 14](#_Toc59098245)

[Remove a Locations 14](#_Toc59098246)

[Modify a Locations 14](#_Toc59098247)

## 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.

## 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** | fim.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/fim.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** | fim.iam.access.module.war | |
| **Context Root of Web Modules** | **Web Module** | **Context Root** |
|  | fim.iam.access.module.war | /ecc |
| **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 Embedded Credential Collector  ###############################################  <Location /ecc>  Set Handler weblogic-handler  WebLogicHost vwasc191.zds.bka.bund.de  WebLogicPort 8009  </Location> |

## User Interface

The user interface provided consists of three parts:

1. a Login page
2. a Logout page
3. a page to request for reset the password

All these pages have 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

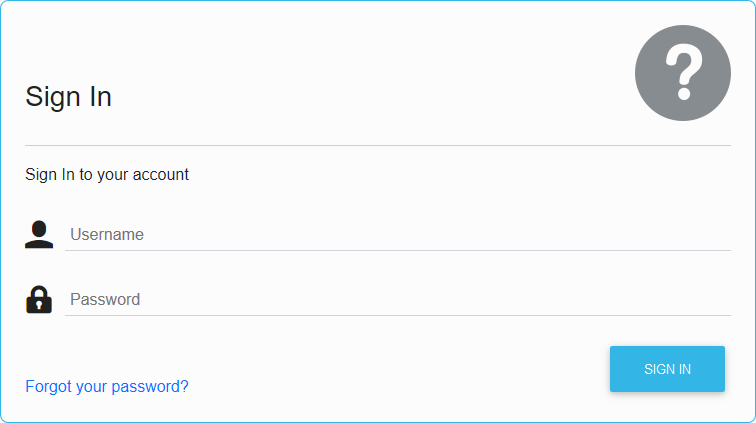
The control of which language is used is made via the settings of the browser.

In the following, the pages are presented anonymously.

### Login Page

#### Layout

The login page requests the name of the account to login and the password credential to authenticate.



The name of the account (Username) and the password credential are mandatory fields that must be entered to initiate the login process. If one of these fields is not or both are not specified, the relevant information will appear on the page.

#### Navigation

The page provides to elements to navigate:

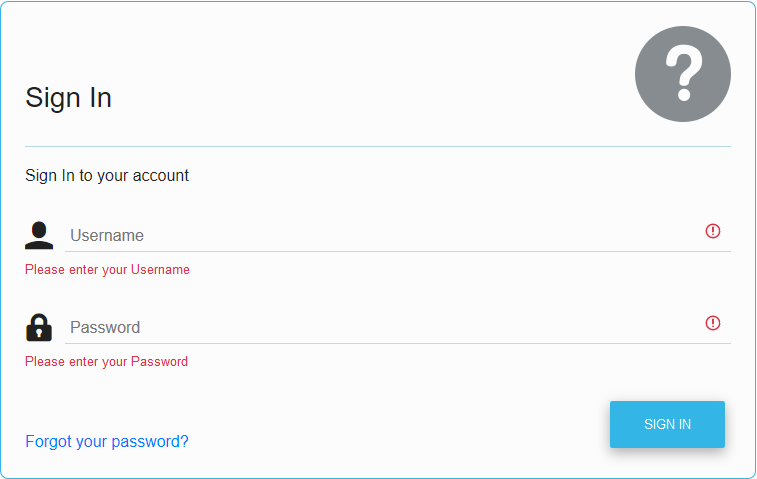
1. Forgot your password
2. Sign In

The **Sign In** button forwards the data entered after they are validated to Access Manager for authentication.

The **Forgot your password** link can be used in the event that a user has forgotten the password and wants to reset it.

#### Error Handling

##### User Input



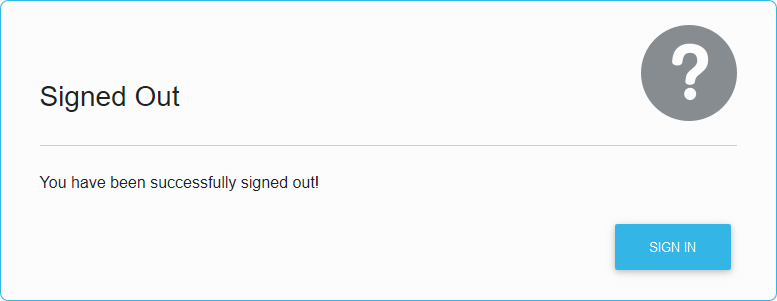
##### Authentication

The entered data is forwarded by the **Sign In** button to the Access Manager, who checks this data. In the event of an error, this is indicated on the same page and the reason for the rejected authentication is displayed.

TBD Screen Shot

### Logout Page

The logout page informs the user about the global logout. Applications must call this page if a general logout of the user account is desired.

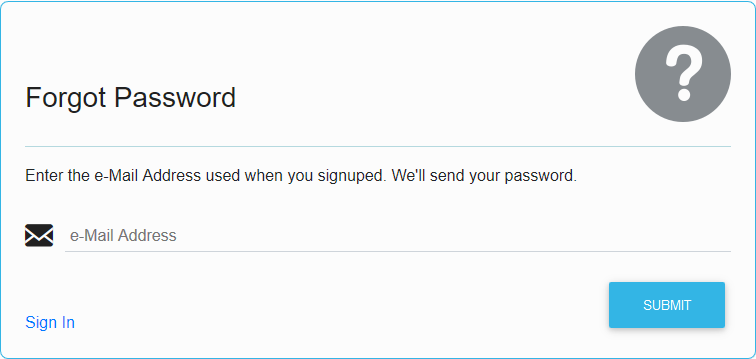


By pressing the **Sign In** button, the user returns to the user login page.

### Forgot Password Page

#### Layout

The requesting user needs to provide a valid e-Mail address.



The name of the e-Mail address is a mandatory field that must be entered to initiate the password reset process. If this field is not specified, the relevant information will appear on the page.

#### Navigation

The page provides two elements for navigate:

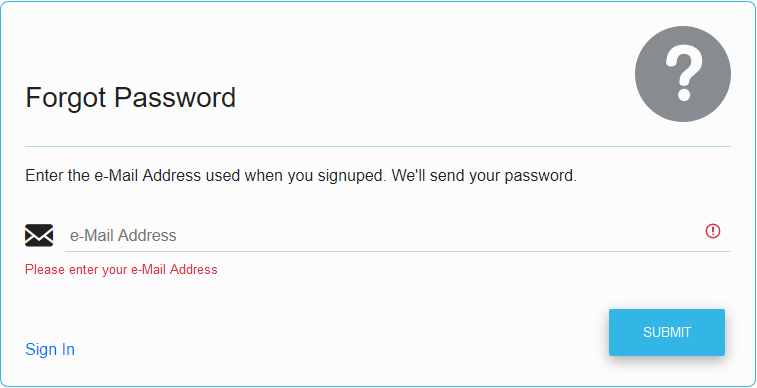
1. Sign In
2. Submit

The **Submit** button forwards the data entered after they are validated to Identity Manager to reset the password and sent it to the e-Mail address entered.

The **Sign In** link returns back to the user login page.

#### Error Handling

In case the user entered invalid data, the page is validated



## Personalization

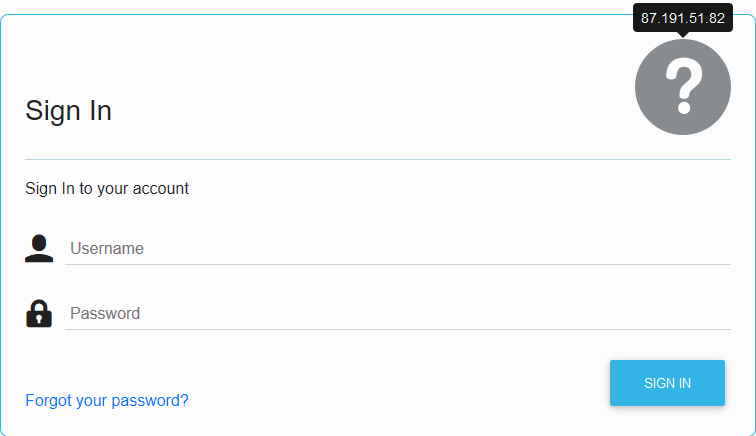
Each page introduced in the chapter above visualize a location hint. The hint use the IP address the browser agent or the forward proxy sent in the HTTP request.

### Discovery

The pages described above are shown in the anonymous mode means that the coat of arms could not be resolved because it is not mapped to a network.

To figure out the IP address the current request belongs to, hover over the image.

In a browser, the IP address the current request belongs to is displayed as a tooltip above the image.



On a mobile device tap on the image to show the IP address.

### Coat of arms

Following Coat of Arms are available for personalization purpose:

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

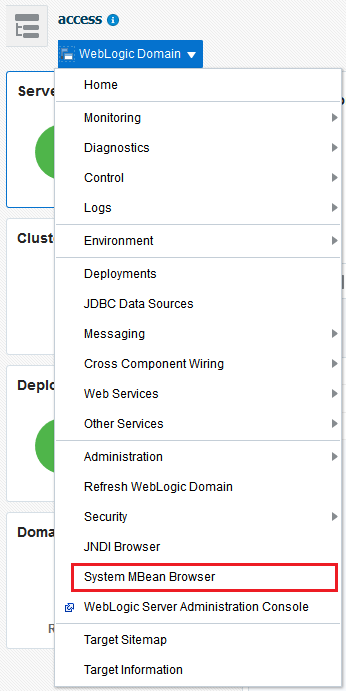
## Configuration

The configuration of the credential collector is managed by Java Management Extensions (JMX).

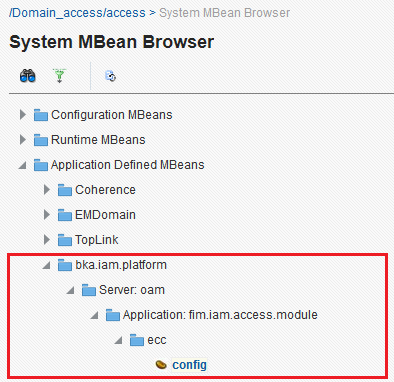
The bean to configure is located in the runtime server and deployed automatically on each managed server.

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* | fim.iam.access.module |
| *Type* | ecc |
| *Name* | config |



### Attributes

The bean provides read/write access to two attributes.

To view the attributes the role *Monitor User* is required. To update the attribute the minimum role is *Administrators*.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Meaning** | **Role** |
| *authentication* | The URI invoked from the Sign In form to authenticate a user leveraging Access Manager capabilities.  Sample: /oam/server/auth\_cred\_submit | Monitor User / Administrators |
| *resetpassword* | The URI invoked from the Forgot Password form to reset the password and send it to the specified e-Mail Address.  Sample: TBD | Monitor User / Administrators |

### 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** |
| *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, the file system storage. | Administrators |

#### Register a Location

The operation location Register 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 | IPV4 address in CIDR-notation to register |
| symbol | a symbol to display to the end users |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| err.ecc.register | If the IPV4 address to register is already registered |

#### List Locations

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

##### Parameter

None

#### Remove a Locations

The operation locationRemove removes a particular network

##### Parameter

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

##### Errors

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

#### Modify a Locations

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

##### Parameter

|  |  |
| --- | --- |
| **Name** | **Meaning** |
| cidr | IPV4 address in CIDR-notation to modify |
| symbol | a symbol to display to the end users |

##### Errors

|  |  |
| --- | --- |
| **Message** | **Meaning** |
| err.ecc.modify | If the IPV4 address to modify is not registered yet |