Administrator Guide

IM.IAM Konfiguration

Autor: Dieter Steding  
 Sophie Strecke

Erstelldatum: 27-11-2019

Letzte Änderung: 25-11-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0019

Version: 1.0

**Freigabe:**

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

logored Kopie-Nr. \_\_\_\_\_

## Dokumentenkontrolle

### Änderungshistorie

| Datum | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 27-11-19 | Dieter Steding | 1.0 | Kein vorheriges Dokument | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

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

Inhalt

[Dokumentenkontrolle ii](#_Toc57197721)

[Änderungshistorie ii](#_Toc57197722)

[Reviewer ii](#_Toc57197723)

[Einführung 1](#_Toc57197724)

[Leserkreis 1](#_Toc57197725)

[Bezugsdokumente 1](#_Toc57197726)

[Vertraulichkeit 1](#_Toc57197727)

[Typografische Konventionen 1](#_Toc57197728)

[Anforderungen 2](#_Toc57197729)

[Hardware und Software Zertifizierung 2](#_Toc57197730)

[Überprüfung der Anforderungen 2](#_Toc57197731)

[Erforderliche Komponentenversionen 2](#_Toc57197732)

[Erforderliche Patches 2](#_Toc57197733)

[Konventionen Verzeichnisvariablen 2](#_Toc57197734)

[Benachrichtigungen 4](#_Toc57197735)

[Kennwort Rücksetzen 4](#_Toc57197736)

[Allgemein 4](#_Toc57197737)

[Gebietsschemainformationen 4](#_Toc57197738)

[Kennwort Warnung 5](#_Toc57197739)

[Allgemein 5](#_Toc57197740)

[Text der Benachrichtigung 5](#_Toc57197741)

[Regeln für Genehmigung 6](#_Toc57197742)

[Bulk-Bereitstellung von Applikationen 6](#_Toc57197743)

[Allgemein 6](#_Toc57197744)

[Bedingungs-Builder 6](#_Toc57197745)

[Bulk-Zuweisung von Rollen 6](#_Toc57197746)

[Allgemein 6](#_Toc57197747)

[Bedingungs-Builder 6](#_Toc57197748)

[Bulk-Entfernung von Rollen 7](#_Toc57197749)

[Allgemein 7](#_Toc57197750)

[Bedingungs-Builder 7](#_Toc57197751)

[Zugriffsrichtlinien 8](#_Toc57197752)

[IDS Federation Identity 8](#_Toc57197753)

[eFBS Anwender Citrix Terminal Services 8](#_Toc57197754)

[eFBS Anwender Applikation 9](#_Toc57197755)

[Rollen 10](#_Toc57197756)

[Federation Foundation 10](#_Toc57197757)

[eFBS Anwender 10](#_Toc57197758)

[Vorlagen 11](#_Toc57197759)

## Einführung

### Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Installation der Oracle Identity und Access Management Infrastruktur befassen

### Bezugsdokumente

Informationen zur Installation und Verwendung von Oracle Identity und Access Management finden Sie auf der folgenden Oracle-Hilfeseite:

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

### Vertraulichkeit

Das in dieser Dokumentation enthaltene Material enthält geschützte, vertrauliche Informationen zu Oracle-Produkten und –Methoden.

Die Leserschaft erklärt sich damit einverstanden, dass die Informationen in dieser Dokumentation nicht nach außerhalb weitergegeben und nicht für andere Zwecke als zur Bewertung dieses Verfahrens vervielfältigt, verwendet oder weitergegeben werden.

### Typografische Konventionen

Die folgenden typografischen Konventionen werden in diesem Dokument verwendet.

|  |  |
| --- | --- |
| **Konvention** | **Bedeutung** |
| **Fettdruck** | Fettdruck kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind. |
| *kursiv* | Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhalter, für die Sie bestimmte Werte angeben. |
| monospace | Monospace kennzeichnet in einem Absatz Befehle, URLs, Code-Beispiele, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.. |

## Anforderungen

### Hardware und Software Zertifizierung

Die plattformspezifischen Anforderungen an Hardware und Software, die in diesem Dokument aufgeführt werden, sind gültig für den Zeitpunkt zu dem, dieses Dokument erstellt wurde. Da neue Plattformen und Betriebssysteme zertifiziert werden können, nachdem dieses Dokument veröffentlicht wurde, wird empfohlen die Zertifizierungsmatrix auf Oracle Technology Network heranzuziehen. Dort befinden sich die aktuellsten Aussagen zu zertifizierten Plattformen und Betriebssystemen.

Die jeweilige Zertifizierungsmatrix für Produkte der Oracle Identity und Access Management Suite sind unter folgenden URLs verfügbar:

[Oracle® Fusion Middleware 12c (12.2.1.3.0)](https://www.oracle.com/technetwork/middleware/fmw-122130-certmatrix-3867828.xlsx)

### Überprüfung der Anforderungen

#### Erforderliche Komponentenversionen

| **Komponente** | **Version** |
| --- | --- |
| **Oracle Java Development Kit** | JDK 1.8.0\_131 oder höher |
| **Oracle Infrastruktur** | Oracle® WebLogic 12c (12.2.1.3.0) |
| **Oracle Datenbank** | Oracle® RDBMS 12c (12.2.0.1.0 oder höher |
| **Oracle Identity Governance** | Oracle® Identity Governance 12c Release 12.2.1.3.0 |

#### Erforderliche Patches

| **Komponente** | **Patch** |
| --- | --- |
| **Oracle Identity Governance** | Patch 30735905 (Oracle® Identity Governance Bundle Patch ID:200108.2108) |

### Konventionen Verzeichnisvariablen

|  |  |
| --- | --- |
| **Variable** | **Bedeutung** |
| *ORACLE\_BASE* | Das Basisverzeichnis, unter dem Oracle-Produkte installiert sind. |
| *ORACLE\_HOME* | Der Speicherort für die Binärdateien eines Produkts. Für die Host-Computer der Anwendungsebene wird sie auf einer gemeinsam genutzten Festplatte gespeichert. |
| *ORACLE\_COMMON\_HOME* | Das Verzeichnis in dem gängige Dienstprogramme, Bibliotheken und andere gängige Oracle Fusion Middleware-Produkte gespeichert sind. |
| *JAVA\_HOME* | Der Speicherort, an dem das unterstützte Java Development Kit (JDK) installiert wurde. |
| *STAGE* | Das Basisverzeichnis, unter dem Oracle-Produkt Medien aufzufinden sind. |

## Benachrichtigungen

Benachrichtigungen werden per e-Mail an die in einem Identitätsprofil oder Rollenprofil hinterlegte e-Mail Adresse versandt.

### Kennwort Rücksetzen

Diese Benachrichtigung wird an die e-Mail Adresse betroffene Identität versandt, wenn ein berechtigter Benutzer Administrator das Kennwort der Identität manuell ändert oder durch das System generieren lässt.

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Vorlagenname** | bka-password-reset |
| **Beschreibungstext** | To be sent after password has been reset by an administrator. |
| **Verfügbares Ereignis** | Kennwort zurücksetzen |

#### Gebietsschemainformationen

##### Englisch

| **Parameter** | **Wert** |
| --- | --- |
| **Codierung** | UTF-8 |
| **Betreff der Nachricht** | Reset Password |
| **Typ** | HTML |
| **Kurze Nachricht** | Reset Password |
| **Lange Nachricht** |  |

##### Deutsch

| **Parameter** | **Wert** |
| --- | --- |
| **Codierung** | UTF-8 |
| **Betreff der Nachricht** | Kennwort zurücksetzen |
| **Typ** | HTML |
| **Kurze Nachricht** | Kennwort zurücksetzen |
| **Lange Nachricht** |  |

##### Französisch

| **Parameter** | **Wert** |
| --- | --- |
| **Codierung** | UTF-8 |
| **Betreff der Nachricht** | Réinitialiser le mot de passe |
| **Typ** | HTML |
| **Kurze Nachricht** | Réinitialiser le mot de passe |
| **Lange Nachricht** |  |

### Kennwort Warnung

Diese Benachrichtigung wird an die e-Mail Adresse betroffene Identität versandt, wenn das Ablaufdatum des Kennworts einen entsprechenden Schwellwert überschritten hat.

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Vorlagenname** | bka-password-warning |
| **Beschreibung** | To be sent after password has been reset by an administrator. |
| **Event** | Reset Password |

#### Text der Benachrichtigung

## Regeln für Genehmigung

### Bulk-Bereitstellung von Applikationen

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | Provision Application Instance in Bulk Default Rule |
| **Beschreibung** | Prevent Workflow instantiation if requester is granted to system administrator. |
| **Eigentümer** | System Administrator |
| **Status** | Activated |

#### Bedingungs-Builder

##### IF

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **requester.AdminRoles** | Contains | OrclOIMSystemAdministrator |

##### THEN

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **workflow** | Equal | NO\_WORKFLOW |

### Bulk-Zuweisung von Rollen

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | Assign Role in Bulk Default Rule |
| **Beschreibung** | Prevent Workflow instantiation if requester is granted to system administrator. |
| **Eigentümer** | System Administrator |
| **Status** | Activated |

#### Bedingungs-Builder

##### IF

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **requester.AdminRoles** | Contains | OrclOIMSystemAdministrator |

##### THEN

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **workflow** | Equal | NO\_WORKFLOW |

### Bulk-Entfernung von Rollen

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | Revoke Role in Bulk Default Rule |
| **Beschreibung** | Prevent Workflow instantiation if requester is granted to system administrator. |
| **Eigentümer** | System Administrator |
| **Status** | Activated |

#### Bedingungs-Builder

##### IF

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **requester.AdminRoles** | Contains | OrclOIMSystemAdministrator |

##### THEN

| **LHS** | **Operator** | **RHS** |
| --- | --- | --- |
| **workflow** | Equal | NO\_WORKFLOW |

## Zugriffsrichtlinien

Für die Verwaltung von Benutzerkonten und den damit verbundenen Berechtigungen sind folgende Zugriffsrichtlinien zu erstellen:

| **Richtlinie** | **Description** |
| --- | --- |
| **IDS Federation Identity** | Verwaltung des Benutzerkontos im Identity Store des Oracle Access Managers.. |
| **eFBS Anwender Citrix Terminal Services** | Verwaltung des Benutzerkontos für Fachanwender im Microsoft Active Directorys |
| **eFBS Anwender Applikation** | Verwaltung des Benutzerkontos für Fachanwender im eFBS Anwendungssystem. |

### IDS Federation Identity

Die Richtlinie wird mit folgenden allgemeinen Attributen erstellt:

| **Attribut** | **Wert** | |
| --- | --- | --- |
| **Name** | IDS Federation Identity | |
| **Beschreibung** | Foundation account provisioned to Identities leveraging federated authentication to enable mapping of external UPN’s to internal UPN’s. | |
| **Eigentümer** | **Name** | **Type** |
|  | System Administrators | Role |
| **Retrofit** | <checked> | |
| **Prioritätsstufe** | 1 | |
| **Anwendungen** | **Name** | **Constraints** |
|  | Identity Store Account | Revoke |

### eFBS Anwender Citrix Terminal Services

Die Richtlinie wird mit folgenden allgemeinen Attributen erstellt:

| **Attribut** | **Wert** | |
| --- | --- | --- |
| **Name** | eFBS End User Citrix Terminal Services | |
| **Beschreibung** | Account provisioned to Identities that needs access to eFBS | |
| **Eigentümer** | **Name** | **Type** |
|  | System Administrators | Role |
| **Retrofit** | <checked> | |
| **Prioritätsstufe** | 1 | |
| **Anwendungen** | **Name** | **Constraints** |
|  | eFBS Citrix Terminal Services | Revoke |
| **Berechtigungen** | **Gruppe** | |
|  | TS.ADS Endpoint~CTSGRFBS-PG\_TS\_eFBS\_REF\_l\_rsClient | |
|  | TS.ADS Endpoint~CTSGRFBS-PG\_TS\_eFBS\_REF\_l\_rsClient32 | |

### eFBS Anwender Applikation

Die Richtlinie wird mit folgenden allgemeinen Attributen erstellt:

| **Attribut** | **Wert** | |
| --- | --- | --- |
| **Name** | eFBS End User Application | |
| **Beschreibung** | Account provisioned to Identities that needs access to eFBS. | |
| **Eigentümer** | **Name** | **Type** |
|  | System Administrators | Role |
| **Retrofit** | <checked> | |
| **Prioritätsstufe** | 1 | |
| **Anwendungen** | **Name** | **Constraints** |
|  | eFBS Account Education | Disable |

## Rollen

Für die Zuteilung und den Entzug von Benutzerkonten und den damit verbundenen Berechtigungen sind folgende Rollen zu erstellen:

| **Richtlinie** | **Description** |
| --- | --- |
| **Federation Foundation** | Verwaltung des Benutzerkontos im Identity Store des Oracle Access Managers.. |
| **eFBS Anwender** | Verwaltung des Benutzerkontos für Fachanwender im eFBS Anwendungssystem. |

### Federation Foundation

Die Rolle wird mit folgenden Attributen angelegt:

| **Attribut** | **Wert** |
| --- | --- |
| **Name** | basic.fed.identity |
| **Anzeigename** | Federated Identity Basic |
| **Rollen-E-Mail** | <empty> |
| **Rollenbeschreibung** | <empty> |
| **Eigentümer ist** | System Administrator |
| **Katalog** |  |
| **Genehmigerrolle** | System Administrator |
| **Kann angefordert werden** | <unchecked> |
| **Hierarchie** |  |
| **Richtlinien** | IDS Federation Identity |

### eFBS Anwender

Die Rolle wird mit folgenden Attributen angelegt:

| **Attribut** | **Wert** |
| --- | --- |
| **Name** | app.eFBS User |
| **Anzeigename** | eFBS Fachanwender |
| **Rollen-E-Mail** | <empty> |
| **Rollenbeschreibung** | <empty> |
| **Eigentümer ist** | System Administrator |
| **Katalog** |  |
| **Genehmigerrolle** |  |
| **Kann angefordert werden** | <checked> |
| **Hierarchie** | basic.fed.identity |
| **Richtlinien** | eFBS End User Citrix Terminal Services |
|  | eFBS Anwender Applikation |

## Vorlagen

Fachanwender

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | eFBS Schulung Anwender |
| **Description** | Konten für CTS, IDS und eFBS Schulung; Berechtigungen: rsClient, rsClient32 |
| **Benutzerkonten** |  |
| **Identity Store Account** |  |
| **eFBS Citrix Terminal Services** | TS.ADS.Endpoint~CTSGRFBS.PG\_TS\_eFBS\_SCHUL\_I\_rsClient |
|  | TS.ADS.Endpoint~CTSGRFBS.PG\_TS\_eFBS\_SCHUL\_I\_rsClient32 |
| **eFBS Account Education** |  |