Administrator Guide

AM.IAM Konfiguration

Autor: Dieter Steding  
 Sophie Strecke

Erstelldatum: 28-01-2020

Letzte Änderung: 17-12-2020

Kontrollnummer: OC\_DE/300516442/DO.081/0016

Version: 1.0

**Freigabe:**

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

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

## Dokumentenkontrolle

### Änderungshistorie

| Date | Autor | Version | | Änderungsreferenz |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
| 28-01-20 | Dieter Steding | 1.0 | Kein vorheriges Dokument | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

### Reviewer

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

Inhalt

[Dokumentenkontrolle ii](#_Toc89671447)

[Änderungshistorie ii](#_Toc89671448)

[Reviewer ii](#_Toc89671449)

[Einführung 1](#_Toc89671450)

[Leserkreis 1](#_Toc89671451)

[Bezugsdokumente 1](#_Toc89671452)

[Vertraulichkeit 1](#_Toc89671453)

[Typografische Konventionen 1](#_Toc89671454)

[Anforderungen 2](#_Toc89671455)

[Hardware und Software Zertifizierung 2](#_Toc89671456)

[Überprüfung der Anforderungen 2](#_Toc89671457)

[Erforderliche Komponentenversionen 2](#_Toc89671458)

[Erforderliche Patches 2](#_Toc89671459)

[Konventionen Verzeichnisvariablen 2](#_Toc89671460)

[Komponenten Konfiguration 4](#_Toc89671461)

[Konfiguration Access Server 5](#_Toc89671462)

[Konfiguration Identity Store 6](#_Toc89671463)

[Federated Identity 6](#_Toc89671464)

[Allgemein 6](#_Toc89671465)

[Verzeichnis und Zugangsdaten 6](#_Toc89671466)

[Benutzer und Gruppen 6](#_Toc89671467)

[Verbindungsdetails 7](#_Toc89671468)

[Kennwortverwaltung 7](#_Toc89671469)

[Proxied Identity 7](#_Toc89671470)

[Allgemein 7](#_Toc89671471)

[Verzeichnis und Zugangsdaten 7](#_Toc89671472)

[Benutzer und Gruppen 8](#_Toc89671473)

[Verbindungsdetails 8](#_Toc89671474)

[Kennwortverwaltung 8](#_Toc89671475)

[Konfiguration Föderation 9](#_Toc89671476)

[Einstellungen 9](#_Toc89671477)

[Identity Provider 9](#_Toc89671478)

[Teilnehmer Polizei Baden‑Württemberg 9](#_Toc89671479)

[Teilnehmer Polizei Brandenburg 10](#_Toc89671480)

[Teilnehmer Bundeskriminalamt 11](#_Toc89671481)

[Teilnehmer Bundespolizei 12](#_Toc89671482)

[Teilnehmer Polizei Hamburg 13](#_Toc89671483)

[Teilnehmer Polizei Hessen 14](#_Toc89671484)

[Sonstige Teilnehmer 15](#_Toc89671485)

[Service Provider 16](#_Toc89671486)

[Netscaler Gateway 16](#_Toc89671487)

[Access Manager 16](#_Toc89671488)

[Provider Discovery 17](#_Toc89671489)

[Konfiguration 17](#_Toc89671490)

[Loopback 18](#_Toc89671491)

[Test und Diagnose 19](#_Toc89671492)

[Verwendung 19](#_Toc89671493)

[Konfiguration Authentifizierungsmodul 20](#_Toc89671494)

[Federated Identity 20](#_Toc89671495)

[Teilnehmer Polizei Baden-Württemberg 20](#_Toc89671496)

[Teilnehmer Polizei Brandenburg 20](#_Toc89671497)

[Teilnehmer Bundeskriminalamt 21](#_Toc89671498)

[Teilnehmer Bundespolizei 21](#_Toc89671499)

[Teilnehmer Polizei Hamburg 22](#_Toc89671500)

[Teilnehmer Polizei Hessen 22](#_Toc89671501)

[Identity Mapping 23](#_Toc89671502)

[Proxied Identity 23](#_Toc89671503)

[Konfiguration Authentifizierungsschema 24](#_Toc89671504)

[Federated Identity 24](#_Toc89671505)

[Teilnehmer Polizei Baden-Württemberg 24](#_Toc89671506)

[Teilnehmer Polizei Brandenburg 24](#_Toc89671507)

[Teilnehmer Bundekriminalamt 24](#_Toc89671508)

[Teilnehmer Bundespolizei 25](#_Toc89671509)

[Teilnehmer Polizei Hamburg 25](#_Toc89671510)

[Teilnehmer Polizei Hessen 26](#_Toc89671511)

[Identity Mapping 26](#_Toc89671512)

[??? 26](#_Toc89671513)

[Proxied Identity 27](#_Toc89671514)

[Konfiguration Host Identifier 28](#_Toc89671515)

[eFBS WebDav 28](#_Toc89671516)

[eFBS Applikation Schulung 28](#_Toc89671517)

[eFBS Application Wirkumgebung 28](#_Toc89671518)

[Node 1 28](#_Toc89671519)

[Node 2 28](#_Toc89671520)

[Konfiguration Agenten 30](#_Toc89671521)

[eFBS WebDav 30](#_Toc89671522)

[Typ 30](#_Toc89671523)

[Konfiguration 30](#_Toc89671524)

[Serverlisten 31](#_Toc89671525)

[eFBS Applikation 31](#_Toc89671526)

[Typ 31](#_Toc89671527)

[Konfiguration 31](#_Toc89671528)

[Serverlisten 32](#_Toc89671529)

[Konfiguration Anwendungen 33](#_Toc89671530)

[eFBS WebDav 33](#_Toc89671531)

[Allgemein 33](#_Toc89671532)

[Authentifizierung 33](#_Toc89671533)

[Autorisierung 33](#_Toc89671534)

[Ressourcen 34](#_Toc89671535)

[eFBS Application 34](#_Toc89671536)

[Allgemein 34](#_Toc89671537)

[Authentifizierung 35](#_Toc89671538)

[Autorisierung 35](#_Toc89671539)

[Ressourcen 36](#_Toc89671540)

## Einführung

### Leserkreis

Dieses Dokument wendet sich an Personen, die sich mit der Administration 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\_133 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 Access Manager** | Oracle® Access Manager 12c Release 12.2.1.3.0 |

#### Erforderliche Patches

| **Komponente** | **Patch** |
| --- | --- |
| **Oracle Access Manager** | Patch 28922534 (Oracle® Access Management Bundle Patch 12.2.1.3.0 (ID:191201.0123.S) |

### 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. |
| *DOMAIN\_BASE* | Das Basisverzeichnis, unter dem WebLogic Domains konfiguriert werden. |

## Komponenten Konfiguration

Für die föderierte Identity und Access Management ist Access Manager entsprechend zu konfigurieren. Eine wesentliche Voraussetzung hierfür ist die Aktivierung von Access-Komponenten.

Freizuschalten sind die Dienste:

1. Identity Föderation

|  |  |
| --- | --- |
| icon-note-16 | **Hinweis** |
| Die Freischaltung des OAuth-Service ist zum gegenwärtigen Zeitpunkt nicht notwendig, da die hierfür erforderlichen Anforderungen nicht definiert sind. |

Um den genannten Dienst zu aktivieren, ist folgendermaßen zu verfahren:

1. Anmeldung als WebLogic Administrator in der Access Management Console,
2. Nach erfolgreicher Anmeldung befinden Sie im Modul **Anwendungssicherheit** des Access Managers.
3. In diesem Modul navigieren Sie über die Schaltfläche **Konfiguration** in die Ansicht Basis Konfigurationseinstellungen des Access Managers.
4. Die Aktivierung der Dienste **Identity Federation** erfolgt in der Kachel **Verfügbare Services**.
5. Im der Ansicht **Verfügbare Dienste** ist der Dienst **Identity Federation** zu aktivieren

## Konfiguration Access Server

Die nach dem Erzeugen der Domain vorzufindende Konfiguration der Access Server ist gegebenenfalls anzupassen.

Nachfolgende Tabelle für die korrekte Konfiguration für jeden Access Server auf:

| **Name** | **Instanz** | | **Proxy** | | |
| --- | --- | --- | --- | --- | --- |
|  | **Host** | **Port** | **ID** | **Port** | **Mode** |
| **oam1** | vwasc191ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |
| **oam2** | vwasc192ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |
| **oam3** | vwasc292ext.zds.bka.bund.de | 8009 | AccessServerConfigProxy | 5575 | Open |

## Konfiguration Identity Store

Die Systemkomponenten Access Manager verwendet zwei Identity Stores für die Authentisierung von Benutzer.

1. Federated Identity
2. Proxied Identity

### Federated Identity

Der Federation Identity Store ist in den Authentisierungsprozess für die Benutzer eingebunden, die über föderierte Authentisierung authentisiert werden.

Die Aufgabe dieses Identity Stores ist die Übersetzung des externen User Principal Name in den internen User Principal Name.

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Speichername** | FederationIdentityStore |
| **Speichertype** | OID: Oracle Internet Directory |
| **Beschreibung** | Identity Store used to translate external User Principal Names to internet User Principal Names. |
| **SSL aktivieren** | <unchecked> |
| **nativen ID-Speichers verwenden** | <unchecked> |
| **Im Voraus abgerufene Attribute** | uid,mail,cn,sn,givenName,krbPrincipalName |

#### Verzeichnis und Zugangsdaten

| **Parameter** | **Wert** |
| --- | --- |
| **Verzeichnis** | fedvip.zds.bka.bund.de:7389 |
| **Bind DN** | uid=oamadmin,cn=System,dc=bka,dc=bund,dc=de |
| **Kennwort** |  |

#### Benutzer und Gruppen

| **Parameter** | **Wert** |
| --- | --- |
| **Anmelde-ID-Attribut** | cn |
| **Benutzerkennwortattribut** | userPassword |
| **Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Objektklassen für Benutzerfilter** | person |
| **Gruppennameattribut** | cn |
| **Basis für die Gruppensuche** | ou=Gropus,dc=bka,dc=bund,dc=de |
| **Gruppenfilterklassen** | groupOfUniqueNames |
| **Gruppenmitgliedschafts-Cache aktivieren** | <unchecked> |

#### Verbindungsdetails

| **Parameter** | **Wert** |
| --- | --- |
| **Minimale Poolgröße** | 50 |
| **Maximale Poolgröße** | 100 |
| **Wait Timeout (in milliseconds)** | 1000 |
| **Inaktivitätstimeout (in Sekunden)** | 0 |
| **Zeitgrenze für Ergebnisse (in Sekunden)** | 0 |
| **Anzahl Wiederholungen** | 3 |
| **Referral Policy** | <empty> |

#### Kennwortverwaltung

Die Kennwortverwaltung verbleibt deaktiviert.

### Proxied Identity

Der Federation Identity Proxy exponiert die Datenbank des Identity Managers als Verzeichnisdienst.

Über diesen Identity Stores werden all die Benutzer authentisiert, deren Teilnehmer keinen eigenen Identity Provider für eine föderierte Authentisierung bereitstellen.

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Speichername** | FederationIdentityProxy |
| **Speichertype** | OUD: Oracle Unified Directory |
| **Beschreibung** | The Identity Store providing entries to authenticate accounts where participants has not their own infrastructure. |
| **SSL aktivieren** | <unchecked> |
| **nativen ID-Speichers verwende** | <unchecked> |
| **Im Voraus abgerufene Attribute** | uid,mail,cn,sn,givenName |

#### Verzeichnis und Zugangsdaten

| **Parameter** | **Wert** |
| --- | --- |
| **Verzeichnis** | fimvip.bka.bund.de:7389 |
| **Bind DN** | uid=oamadmin,cn=System,dc=bka,dc=bund,dc=de |
| **Kennwort** |  |

#### Benutzer und Gruppen

| **Parameter** | **Wert** |
| --- | --- |
| **Anmelde-ID-Attribut** | uid |
| **Benutzerkennwortattribut** | userPassword |
| **Benutzersuchbasis** | cn=Participants,dc=fim,dc=bund,dc=de |
| **Objektklassen für Benutzerfilter** | person |
| **Gruppennameattribut** | cn |
| **Basis für die Gruppensuche** | ou=Gropus,dc=bka,dc=bund,dc=de |
| **Gruppenfilterklassen** | groupOfUniqueNames |
| **Gruppenmitgliedschafts-Cache aktivieren** | <unchecked> |

#### Verbindungsdetails

| **Parameter** | **Wert** |
| --- | --- |
| **Minimale Poolgröße** | 50 |
| **Maximale Poolgröße** | 100 |
| **Wait Timeout (in milliseconds)** | 1000 |
| **Inaktivitätstimeout (in Sekunden)** | 0 |
| **Zeitgrenze für Ergebnisse (in Sekunden)** | 0 |
| **Anzahl Wiederholungen** | 3 |
| **Referral Policy** | <empty> |

#### Kennwortverwaltung

Die Kennwortverwaltung verbleibt deaktiviert.

## Konfiguration Föderation

### Einstellungen

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Provider Id** | https://iam.bka.extraprol.de/oam/fed |
| **Signaturschlüssel** | osts\_signing\_sha256 |
| **Verschlüsselungsschlüssel** | osts\_encryption\_sha256 |

### Identity Provider

Die Identity Provider werden in der Identitätsproviderverwaltung angelegt.

Für folgende Teilnehmer ist jeweils ein Identity Provider zu erzeugen:

1. Polizei Baden‑Württemberg
2. Polizei Brandenburg
3. Bundeskriminalamt
4. Bundespolizei
5. Polizei Hamburg
6. Polizei Hessen

Für die Teilnehmer, die keine eigene Infrastruktur zur Verfügung stellen können fungiert Access Manager als gemeinsame genutzter Identity Provider. Zu diesem

#### Teilnehmer Polizei Baden‑Württemberg

Der Identity Provider für den Teilnehmer Baden‑Württemberg wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BW-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Police Baden-Wuerttenberg |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** | BW\_FederationMedata.xml |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Teilnehmer Polizei Brandenburg

Der Identity Provider für den Teilnehmer Polizei Brandenburg wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BB-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Police Brandenburg |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** | <empty> |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Teilnehmer Bundeskriminalamt

Der Identity Provider für den Teilnehmer Bundeskriminalamt wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BK-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Federal Criminal Police Office |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** |  |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Teilnehmer Bundespolizei

Der Identity Provider für den Teilnehmer Bundespolizei wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BP-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Federal Police |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** |  |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Teilnehmer Polizei Hamburg

Der Identity Provider für den Teilnehmer Polizei Hamburg wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | HH-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Police Hamburg |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** |  |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Teilnehmer Polizei Hessen

Der Identity Provider für den Teilnehmer Polizei Hessen wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | HE-IdentityProvider |
| **Beschreibung** | Identity Provider configuration participant Police Hesse |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** |  |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

|  | **Wichtig** |
| --- | --- |
| Die Änderung des Parameters Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen, darf nur in Abstimmung mit der Implementierung im Identity Manager erfolgen, da dieser für die Befüllung der Benutzerkonten verantwortlich zeichnet. |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **idp-attribute-profile** | idp-attribute-profile |

#### Sonstige Teilnehmer

Der Identity Provider für die sonstigen Teilnehmer wird mit folgenden Parametern definiert:

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | AM-IdentityProvider |
| **Beschreibung** | Identity Provider configuration for participants without own infrastrutur |
| **Partner aktivieren** | <checked> |
| **Standard-IdP-Partner** | <unchecked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Datei** |  |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Zuordnungsoptionen

| **Parameter** | **Wert** |
| --- | --- |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |
| **DN der Benutzersuchbasis** | ou=People,dc=bka,dc=bund,dc=de |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | <selected> |
| **Assertion-Name-ID dem Benutzer-ID-Speicherattribut zuordnen** | krbPrincipalName |

### Service Provider

#### Netscaler Gateway

Allen Identity Provider gemeinsam ist ein Service Provider.

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | NetScaler-ServiceProvider |
| **Beschreibung** | Service Provider |
| **Partner aktivieren** | <checked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Manuell |
| **Provider-ID** | netscaler |
| **Assertion Consumer-URL** | https://portal.app.bka.extrapol.de/cgi/samlauth |
| **URL von Abmeldeanforderung** | https://portal.app.bka.extrapol.de/cgi/logout |
| **URL von Abmeldeantwort** | https://iam.bka.extrapol.de/oamfed/idp/samlv20 |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Name ID Format

| **Parameter** | **Wert** |
| --- | --- |
| **NameID-Format** | Persistent |
| **NameID-Value** | Benutzer-ID-Speicherattribute |
| **Expression** | ${user.attr.uid} |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **Attribute Profil** | sp-attribute-profile |

#### Access Manager

Allen Identity Provider gemeinsam ist ein Service Provider.

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | AM-ServiceProvider |
| **Beschreibung** | Service Provider for sharing the common Loopback Identity Provider |
| **Partner aktivieren** | <checked> |

##### Serviceinformationen

| **Parameter** | **Wert** |
| --- | --- |
| **Protokoll** | SAML 2.0 |
| **Servicedetails** | Aus Providermetadaten laden |
| **Provider-ID** | http://iam.bka.extrapol.de/oam/fed |

##### Signaturzertifikat

| icon-note-16 | **Hinweis** |
| --- | --- |
| Das Laden der Metadatendatei findet nach Bereitstellung durch den Teilnehmer statt. |

##### Name ID Format

| **Parameter** | **Wert** |
| --- | --- |
| **NameID-Format** | Persistent |
| **NameID-Value** | Benutzer-ID-Speicherattribute |
| **Expression** | ${user.attr.uid} |

##### Attribute Zuordnung

| **Attributprofil** | **Wert** |
| --- | --- |
| **Attribute Profil** | sp-attribute-profile |

### Provider Discovery

Dienste sind zumeist durch globale Agenten geschützt und verwenden Access Manager als Service Provider, um die föderierte Anmeldung zu initiieren.

In Ausnahmefällen übernimmt ein anderweitig bereitgestellter Intermediär die Funktion des Service Providers und initiiert eigenständige den Ablauf der föderierten Anmeldung. In diesem Szenario übernimmt Access Manager die Funktion eines Federation Proxy. Agiert eine Systemkomponente eigenständig als Service Provider hängt es von den technischen Möglichkeiten dieser Komponente ab, ob eine automatische Weiterleitung an den entsprechenden Identity Provider erfolgen kann oder nicht. Aus diesem Grund ist es erforderlich dem Anwender die Auswahlmöglichkeit zu geben über welchen Identity Provider er sich authentisieren möchte.

Dazu wird im Access Manager der Identity Provider Discovery Modul aktiviert und die Seite zur Auswahl des Identity Providers durch Anwender registriert.

#### Konfiguration

##### Aktivierung

Die Aktivierung des Identity Provider Discovery Modul erfolgt über das Kommando:

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${FMW\_HOME}/oracle\_common/common/bin/wlst.sh  connect('weblogic', '<password>', 't3://<hostname>.zds.bka.bund.de:7001')  domainRuntime()  putBooleanProperty('/spglobal/idpdiscoveryserviceenabled', 'true')  putBooleanProperty('/spglobal/idpdiscoveryservicepageenabled', 'true')  exit() |

| **Option** | **Name** |
| --- | --- |
| **password** | Kennwort des WebLogic Domain Administrators |
| **hostname** | Der Name des Knotens, auf dem der Admin Server der Access Domain bereitgestellt wurde. |

| icon-note-16 | **Hinweis** |
| --- | --- |
| Zur Deaktivierung des Identity Provider Discovery Modul in obigen Kommando im Aufruf von *putBooleanProperty* der Wert *false* als Parameter für die Konfigurationseinstellung */spglobal/idpdiscoveryserviceenabled* zu übergeben. |

##### Registrierung

Die Registrierung der Seite für die Auswahl des Identity Providers durch Anwender erfolgt über das Kommando:

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${FMW\_HOME}/oracle\_common/common/bin/wlst.sh  connect('weblogic', '<password>', 't3://<hostname>.zds.bka.bund.de:7001')  domainRuntime()  putStringProperty('/spglobal/idpdiscoveryserviceurl','/idp/')  exit() |

| **Option** | **Name** |
| --- | --- |
| **password** | Kennwort des WebLogic Domain Administrators |
| **hostname** | Der Name des Knotens, auf dem der Admin Server der Access Domain bereitgestellt wurde. |

#### Loopback

Für Teilnehmer, die keine eigene Infrastruktur bereitstellen, aber trotzdem am föderierten Anmeldeverfahren teilnehmen sollen, wird Access Manager als Loopback Identity Provider eingesetzt. Hierbei ist zu beachten, dass die Anmeldung im Identity Provider und die Initiierung des Anmeldeverfahrens im gleichen Access Manager stattfindet, aber unterschiedliche Identity Stores Verwendung finden. Die Verwaltung der Sitzung im Access Manager verursacht im Standardverhalten hier einen Konflikt in der Form:

Um dieses Verhalten zu umgehen ist in den globalen Einstellungen der Parameter *ssofedfailusermismatch* entsprechend zu ändern. Die Änderung dieses Parameters erfolgt durch das Kommando:

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${FMW\_HOME}/oracle\_common/common/bin/wlst.sh  connect('weblogic', '<password>', 't3://<hostname>.zds.bka.bund.de:7001')  domainRuntime()  putBooleanProperty('/spglobal/ssofedfailusermismatch','false')  exit() |

#### Test und Diagnose

Um die Abläufe der föderierten Anmeldung testen und potentielle Fehlkonfigurationen diagnostizieren zu können, wird empfohlen die Testapplikation im Access Manager zu aktivieren. Die Testapplikation für das föderierte Anmeldeverfahren ist standardmäßig deaktiviert.

##### Aktivierung

Die Aktivierung der Testapplikation erfolgt durch folgendes Kommando:

|  | **Kommando** |
| --- | --- |
| . fmw.env  ${FMW\_HOME}/oracle\_common/common/bin/wlst.sh  connect('weblogic', '<password>', 't3://<hostname>.zds.bka.bund.de:7001')  domainRuntime()  configureTestSPEngine('true')  exit() |

| **Option** | **Name** |
| --- | --- |
| **password** | Kennwort des WebLogic Domain Administrators |
| **hostname** | Der Name des Knotens, auf dem der Admin Server der Access Domain bereitgestellt wurde. |

| icon-note-16 | **Hinweis** |
| --- | --- |
| Zur Deaktivierung der Testapplikation in obigen Kommando im Aufruf von *configureTestSPEngine* der Wert *false* als Parameter zu übergeben. |

#### Verwendung

Das Starten einer föderierten Anmeldung erfolgt nachfolgendem Ablauf:

1. Aufruf der Testapplikation in einem Browser
2. Auswahl des Identity Providers
3. Start der Operation

| **Option** | **Name** |
| --- | --- |
| **hostname** | Der Name eines der Knoten, auf denen Access Manager innerhalb der Access Domain bereitgestellt wurde. |

## Konfiguration Authentifizierungsmodul

### Federated Identity

#### Teilnehmer Polizei Baden-Württemberg

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BW-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Police Baden-Wuerttemberg |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | BW-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

#### Teilnehmer Polizei Brandenburg

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BB-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Police Brandenburg |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | BB-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

#### Teilnehmer Bundeskriminalamt

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BK-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Federal Criminal Police Office |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | BK-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

#### Teilnehmer Bundespolizei

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BP-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Federal Police |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | BP-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

#### Teilnehmer Polizei Hamburg

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BW-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Police Hamburg |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | HH-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

#### Teilnehmer Polizei Hessen

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | Authentifizierungsmodul |
| **Name** | BW-FederationModule |
| **Beschreibung** | Plugin to authenticate users via Federation SSO Participant Police Hesse |

##### Schritte

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FedAuthRequestPlugin |
| **Beschreibung** | Federation Authn Request to IdP |
| **Plugin Name** | FedAuthRequestPlugin |
| **FedForceAuthn** | <empty> |
| **Fed SSOIdP** | HE-IdentityProvider |
| **Fed Passive** | <empty> |

##### Orchestration

### Identity Mapping

##### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | LDAP-Authentifizierungsmodul |
| **Name** | BK-MappingModule |
| **Benutzeridentitätsspeicher** | FederationIdentityStore |

### Proxied Identity

| **Parameter** | **Wert** |
| --- | --- |
| **Typ** | LDAP-Authentifizierungsmodul |
| **Name** | FederationProxyModule |
| **Benutzeridentitätsspeicher** | FederationIdentityProxy |

## Konfiguration Authentifizierungsschema

### Federated Identity

#### Teilnehmer Polizei Baden-Württemberg

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BW-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Baden-Wuerttemberg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | BW-FederationModule |
| **Challenge-URL** | /pages/login.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

#### Teilnehmer Polizei Brandenburg

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BB-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Brandenburg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | BB-FederationModule |
| **Challenge-URL** | /pages/login.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

#### Teilnehmer Bundekriminalamt

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BK-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Brandenburg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | BK-FederationModule |
| **Challenge-URL** | /pages/servererror.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

#### Teilnehmer Bundespolizei

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BP-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Brandenburg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | BP-FederationModule |
| **Challenge-URL** | /pages/servererror.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

#### Teilnehmer Polizei Hamburg

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | HH-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Brandenburg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | HH-FederationModule |
| **Challenge-URL** | /pages/servererror.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

#### Teilnehmer Polizei Hessen

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | HE-FederationScheme |
| **Beschreibung** | Federation Scheme for participant Police Brandenburg |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | HE-FederationModule |
| **Challenge-URL** | /pages/servererror.jsp |
| **Kontexttyp** | customWar |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | is\_rsa=true initial\_command=NONE |

### Identity Mapping

#### ???

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | BK-MappingScheme |
| **Beschreibung** | Authentication Scheme to map external UPN to internal UPN |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | BK-FederationModule |
| **Challenge-URL** | /pages/login.jsp |
| **Kontexttyp** | default |
| **Challenge Value** | /oam |
| **Challenge-Parameters** | <empty> |

### Proxied Identity

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | FederationProxyScheme |
| **Beschreibung** | Authentication scheme for all proxied Resources |
| **Authentifizierungsebene** | 2 |
| **Standard** | <unchecked> |
| **Challenge-Methode** | FORM |
| **Challenge-Umleitungs-URL** | /oam/server |
| **Authentifizierungsmodul** | FederationProxyModule |
| **Challenge-URL** | https://iam.extrapol.bund.de/ecc |
| **Kontexttyp** | external |
| **Challenge-Parameter** | <empty> |

## Konfiguration Host Identifier

### eFBS WebDav

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwappdav-http-80 | |
| **Beschreibung** | The Host Name variations which can occur accessing eFBS WebDav domain. | |
| **Varianten** | **Host Name** | **Port** |
|  | daten.app.bka.extrapol.de | 80 |
|  | daten.app.bka.extrapol.de | 443 |
|  | IP‘s |  |

### eFBS Applikation Schulung

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwasy711-http-80 | |
| **Beschreibung** | The Host Name variations which can occur accessing eFBS application. | |
| **Varianten** | **Host Name** | **Port** |
|  | web.edu.efbs.bka.extrapol.de | 80 |
|  | web.edu.efbs.bka.extrapol.de | 443 |
|  | IP‘s? |  |

### eFBS Application Wirkumgebung

#### Node 1

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwasy111-http-80 | |
| **Beschreibung** | The Host Name variations which can occur accessing eFBS application. | |
| **Varianten** | **Host Name** | **Port** |
|  | web.prd.efbs.bka.extrapol.de | 80 |
|  | web.prd.efbs.bka.extrapol.de | 443 |
|  | IP‘s |  |

#### Node 2

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwasy211-http-80 | |
| **Beschreibung** | The Host Name variations which can occur accessing eFBS application. | |
| **Varianten** | **Host Name** | **Port** |
|  | web.prd.efbs.bka.extrapol.de | 80 |
|  | web.prd.efbs.bka.extrapol.de | 443 |
|  | IP‘s |  |

## Konfiguration Agenten

Die Agenten (WebGates) werden in einem Oracle HTTP Server 12c bereitgestellt.

Bevor diese Agenten in einem entsprechenden Oracle HTTP Server 12c bereitgestellt werden sind diese in der Konfiguration des Access Manager zu registrieren.

Es werden zwei Agenten benötigt.

1. WebDav Agent
2. Application Agent

Die Konfiguration der Agenten wird über die **Schnellstartassistenten** über den Link **SSO-Agent-Registrierung** vorgenommen.

| icon-note-16 | **Hinweis** |
| --- | --- |
| Es wird empfohlen die Registrierung über den Link **SSO-Agent-Registrierung** vorzunehmen. |

### eFBS WebDav

#### Typ

| **Parameter** | **Wert** |
| --- | --- |
| **Agent-Typ** | Webgate |

#### Konfiguration

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwappdav-http-80 | |
| **Beschreibung** | The agent which protects eFBS WebDav domain. | |
| **Basis URL** | / | |
| **Access Client-Kennwort** | <empty> | |
| **Host-ID** | vwappdav-http-80 | |
| **Benutzerdefinierte Parameter** | **Name** | **Wert** |
|  | maxSessionTimeOutUnit | minutes |
|  | cleint\_request\_retry\_attampts | 1 |
|  | EnableHostPortValidation | false |
|  | URLInUTF8Format | true |
|  | proxySSLHeaderVar | Is\_SSL |
| **Sicherheit** | Open | |
| **Virtueller Host** | <unchecked> | |
| **Policys automatisch erstellen** | <unchecked> | |
| **IP Validierung** | <unchecked> | |

#### Serverlisten

##### Primary

| **Access Server** | **Host** | **Port** | **Max. Verbindungen** |
| --- | --- | --- | --- |
| oam1 | vwasc191ext.zds.bka.bund.de | 5575 | 1 |

##### Secundary

| **Access Server** | **Host** | **Port** | **Max. Verbindungen** |
| --- | --- | --- | --- |
| oam2 | vwasc192ext.zds.bka.bund.de | 5575 | 1 |
| oam3 | vwasc291ext.zds.bka.bund.de | 5575 | 1 |

### eFBS Applikation

#### Typ

| **Parameter** | **Wert** |
| --- | --- |
| **Agent-Typ** | Webgate |

#### Konfiguration

| **Parameter** | **Wert** | |
| --- | --- | --- |
| **Name** | vwasy711-http-80 | |
| **Beschreibung** | The agent which protects eFBS application domain. | |
| **Basis URL** | / | |
| **Access Client-Kennwort** | <empty> | |
| **Host-ID** | SERVER\_NAME | |
| **Benutzerdefinierte Parameter** | **Name** | **Wert** |
|  | maxSessionTimeOutUnit | minutes |
|  | cleint\_request\_retry\_attampts | 1 |
|  | URLInUTF8Format | true |
|  | EnableHostPortValidation | false |
|  | proxySSLHeaderVar | Is\_SSL |
| **Sicherheit** | Open | |
| **Virtueller Host** | <unchecked> | |
| **Policys automatisch erstellen** | <unchecked> | |
| **IP Validierung** | <unchecked> | |

#### Serverlisten

##### Primary

| **Access Server** | **Host** | **Port** | **Max. Verbindungen** |
| --- | --- | --- | --- |
| oam1 | vwasc191ext.zds.bka.bund.de | 5575 | 1 |

##### Secundary

| **Access Server** | **Host** | **Port** | **Max. Verbindungen** |
| --- | --- | --- | --- |
| oam2 | vwasc192ext.zds.bka.bund.de | 5575 | 1 |
| oam3 | vwasc291ext.zds.bka.bund.de | 5575 | 1 |

## Konfiguration Anwendungen

### eFBS WebDav

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | eFBS-WebDav |
| **Beschreibung** | The security container to protect resources deployed in the WebDav Domain of eFBS. |
| **Timeout wegen inaktiver Session (Minuten)** | 0 |
| **Policy-Sortierung aktivieren** | <unchecked> |

#### Authentifizierung

##### authn-public

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | authn-public |
| **Beschreibung** | Authenticate access to public resources in WebDav Domain efBS. |
| **Erfolgs-URL** |  |
| **Fehler-URL** |  |
| **Authentifizierungsschema** | AnonymousScheme |

##### authn-protected

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | authn-protected |
| **Beschreibung** | Authenticate access to protected resources in WebDav Domain efBS. |
| **Erfolgs-URL** |  |
| **Fehler-URL** |  |
| **Authentifizierungsschema** | BK-MappingScheme |

#### Autorisierung

##### authz-public

| **Parameter** | **Wert** | | |
| --- | --- | --- | --- |
| **Name** | authz-public | | |
| **Beschreibung** | Authorize access to public resources in WebDav Domain eFBS. | | |
| **Erfolgs-URL** | <empty> | | |
| **Fehler-URL** | <empty> | | |
| **Bedingungen** | **Name** | **Type** | **Beschreibung** |
|  | TRUE | True | This condition always evaluates to true. |
| **Regeln** | **Zulassen** | | **Ablehnen** |
|  | TRUE(True) | |  |

##### authz-protected

| **Parameter** | **Wert** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Name** | authz-protected | | | | |
| **Beschreibung** | Authorize access to protected resources in WebDav Domain eFBS. | | | | |
| **Erfolgs-URL** | <empty> | | | | |
| **Fehler-URL** | <empty> | | | | |
| **Bedingungen** | **Name** | **Type** | | **Beschreibung** | |
|  | TRUE | True | | This condition always evaluates to true. | |
| **Regeln** | **Zulassen** | | | **Ablehnen** | |
|  | TRUE(True) | | |  | |
| **Responses** | **Type** | | **Name** | | **Value** |
|  | Header | | OAM\_USER | | $user.attr.cn |

#### Ressourcen

| **Parameter** | **Wert** | | | |
| --- | --- | --- | --- | --- |
| **Typ** | HTTP | | | |
| **Beschreibung** |  | | | |
| **Host Identifier** | vwappdav-http-80 | | | |
| **URI** | **URL** | **Abfrage** | | |
|  |  | **Name** | | **Wert** |
|  | /\*\* |  | |  |
| **Schutz** | **Authentifizierungs-Policy** | | **Autorisierungs-Policy** | |
| **Geschützt** | authn-protected | | authz-protected | |

### eFBS Application

#### Allgemein

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | eFBS-Application |
| **Beschreibung** | The security container to protect resources deployed in the application domain of eFBS. |
| **Timeout wegen inaktiver Session (Minuten)** | 0 |
| **Policy-Sortierung aktivieren** | <unchecked> |

#### Authentifizierung

##### authn-public

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | authn-public |
| **Beschreibung** | Authenticate access to public resources in application domain eFBS. |
| **Erfolgs-URL** |  |
| **Fehler-URL** |  |
| **Authentifizierungsschema** | AnonymousScheme |

##### authn-protected

| **Parameter** | **Wert** |
| --- | --- |
| **Name** | authn-protected |
| **Beschreibung** | Authenticate access to protected resources in application domain eFBS. |
| **Erfolgs-URL** |  |
| **Fehler-URL** |  |
| **Authentifizierungsschema** | BK-MappingScheme |

#### Autorisierung

##### authz-public

| **Parameter** | **Wert** | | |
| --- | --- | --- | --- |
| **Name** | authz-public | | |
| **Beschreibung** | Authorize access to public resources in application domain eFBS. | | |
| **Erfolgs-URL** | <empty> | | |
| **Fehler-URL** | <empty> | | |
| **Bedingungen** | **Name** | **Type** | **Beschreibung** |
|  | TRUE | True | This condition always evaluates to true. |
| **Regeln** | **Zulassen** | | **Ablehnen** |
|  | TRUE(True) | |  |

##### authz-protected

| **Parameter** | **Wert** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Name** | authz-protected | | | | |
| **Beschreibung** | Authorize access to protected resources in application domain eFBS. | | | | |
| **Erfolgs-URL** | <empty> | | | | |
| **Fehler-URL** | <empty> | | | | |
| **Bedingungen** | **Name** | **Type** | | **Beschreibung** | |
|  | TRUE | True | | This condition always evaluates to true. | |
| **Regeln** | **Zulassen** | | | **Ablehnen** | |
|  | TRUE(True) | | |  | |
| **Responses** | **Type** | | **Name** | | **Value** |
|  | Header | | OAM\_USER | | $user.attr.cn |

#### Ressourcen