

# Oracle® Enterprise Performance Management System Sicherheitskonfiguration



Release 11.2  
F28808-22  
Dezember 2023

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE®

Oracle Enterprise Performance Management System Sicherheitskonfiguration, Release 11.2

F28808-22

Copyright © 2005, 2023, Oracle und/oder verbundene Unternehmen.

Primärer Autor: EPM Information Development Team

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

# Inhalt

## Dokumentation zur Barrierefreiheit

---

## Dokumentationsfeedback

---

### 1 Informationen zur EPM System-Sicherheit

---

|   |      |
|---|------|
| Informationen zu EPM System                 | 1-1  |
| Erforderliche Kenntnisse                    | 1-1  |
| Komponenten der Sicherheitsinfrastruktur    | 1-2  |
| Benutzerauthentifizierung                   | 1-2  |
| Provisioning (rollenbasierte Autorisierung) | 1-6  |
| Shared Services Console starten             | 1-10 |

### 2 SSL-Aktivierung für EPM System-Komponenten

---

|  |      |
|--|------|
| Annahmen   | 2-1  |
| Informationsquellen  | 2-1  |
| Speicherortreferenzen  | 2-2  |
| Informationen zur SSL-Aktivierung für EPM System-Produkte        | 2-2  |
| Unterstützte SSL-Szenarios                                       | 2-3  |
| Erforderliche Zertifikate  | 2-4  |
| SSL auf dem SSL-Offloader beenden                                | 2-5  |
| Vollständiges SSL-Deployment von EPM System                      | 2-7  |
| Deployment-Architektur   | 2-7  |
| Annahmen   | 2-8  |
| Vollständige SSL-Konfiguration für EPM System                    | 2-9  |
| Allgemeine Einstellungen für EPM System neu konfigurieren        | 2-10 |
| Optional: CA-Stammzertifikate für WebLogic Server installieren   | 2-11 |
| Zertifikat auf WebLogic Server installieren                      | 2-12 |
| WebLogic Server konfigurieren                                    | 2-13 |
| HFM-Serververbindung mit SSL-fähiger Oracle-Datenbank aktivieren | 2-15 |
| Verfahren für Oracle HTTP Server                                 | 2-21 |

|   |      |
|---|------|
| Auf WebLogic Server bereitgestellte EPM System-Webkomponenten konfigurieren | 2-25 |
| Domainkonfiguration aktualisieren   | 2-27 |
| Server und EPM System neu starten   | 2-29 |
| Deployments testen  | 2-29 |
| Externe Benutzerverzeichnisse mit SSL-Aktivierung konfigurieren             | 2-29 |
| SSL auf dem Webserver beenden   | 2-30 |
| SSL für Essbase 11.1.2.4  | 2-33 |
| Essbase-Komponenten installieren und bereitstellen                          | 2-35 |
| Vertrauenswürdige CA-Zertifikate von Drittanbietern für Essbase verwenden   | 2-36 |
| Sessionbasierte SSL-Verbindung herstellen                                   | 2-44 |
| SSL für Essbase 21c   | 2-45 |
| Essbase-Komponenten installieren und bereitstellen                          | 2-47 |
| Vertrauenswürdige CA-Zertifikate von Drittanbietern für Essbase verwenden   | 2-48 |
| Sessionbasierte SSL-Verbindung herstellen                                   | 2-54 |

### 3 SSO mit Security Agents aktivieren

---

|   |      |
|---|------|
| Unterstützte SSO-Methoden   | 3-1  |
| Single Sign-On von Oracle Access Manager  | 3-4  |
| Single Sign-On für OracleAS   | 3-5  |
| Deployments testen  | 3-7  |
| OSSO für EPM System aktivieren  | 3-7  |
| EPM System-Produkte für SSO schützen  | 3-11 |
| Headerbasiertes SSO mit Identity Management-Produkten                               | 3-16 |
| EPM System für headerbasiertes SSO mit Oracle Identity Cloud Services konfigurieren | 3-18 |
| Voraussetzungen und Beispiel-URLs   | 3-18 |
| Headerbasierte Authentifizierung für EPM System aktivieren                          | 3-19 |
| Anwendung und Gateway von EPM System zu Oracle Identity Cloud Services hinzufügen   | 3-19 |
| App-Gateway konfigurieren   | 3-25 |
| Benutzerverzeichnisse für Autorisierung konfigurieren                               | 3-25 |
| SSO in EPM System aktivieren  | 3-25 |
| EPM Workspace-Einstellungen aktualisieren   | 3-26 |
| SSO für SiteMinder  | 3-26 |
| Kerberos-Single Sign-On   | 3-29 |
| EPM System für SSO konfigurieren  | 3-44 |
| Single Sign-On-Optionen für Smart View  | 3-45 |

### 4 Benutzerverzeichnisse konfigurieren

---

|   |     |
|---|-----|
| Benutzerverzeichnisse und EPM System-Sicherheit         | 4-1 |
| Vorgänge bezüglich der Benutzerverzeichniskonfiguration | 4-2 |

|  |      |
|--|------|
| Oracle Identity Manager und EPM System   | 4-2  |
| Informationen zu Active Directory  | 4-3  |
| OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren | 4-4  |
| Relationale Datenbanken als Benutzerverzeichnisse konfigurieren                    | 4-19 |
| Benutzerverzeichnisverbindungen testen   | 4-22 |
| Einstellungen der Benutzerverzeichnisse ändern                                     | 4-23 |
| Benutzerverzeichniskonfigurationen löschen   | 4-23 |
| Suchreihenfolge des Benutzerverzeichnisses verwalten                               | 4-24 |
| Sicherheitsoptionen festlegen  | 4-26 |
| Verschlüsselungsschlüssel erneut generieren  | 4-30 |
| Sonderzeichen verwenden  | 4-32 |

## 5 Benutzerdefinierte Authentifizierungsmodule verwenden

---

|   |     |
|---|-----|
| Übersicht   | 5-1 |
| Beispiele für Anwendungsfälle und Einschränkungen         | 5-3 |
| Voraussetzungen   | 5-3 |
| Überlegungen zu Design und Codierung                      | 5-3 |
| Benutzerdefinierte Authentifizierungsmodule bereitstellen | 5-9 |

## 6 Richtlinien zum Sichern von EPM System

---

|  |     |
|--|-----|
| SSL implementieren   | 6-1 |
| Administratorkennwort ändern                                   | 6-1 |
| Verschlüsselungsschlüssel erneut generieren                    | 6-2 |
| Datenbankkennwörter ändern                                     | 6-2 |
| Cookies schützen   | 6-3 |
| SSO-Tokentimeout reduzieren                                    | 6-4 |
| Sicherheitsberichte prüfen                                     | 6-4 |
| Authentifizierungssystem für starke Authentifizierung anpassen | 6-4 |
| EPM Workspace-Debugging-Utilitys deaktivieren                  | 6-4 |
| Standardfehlerseiten des Webservers ändern                     | 6-5 |
| Unterstützung für Software von Drittanbietern                  | 6-5 |

## A Beispielcodes für benutzerdefinierte Authentifizierung

---

|                               |     |
|-------------------------------|-----|
| Beispielcode 1                | A-1 |
| Beispielcode 2                | A-2 |
| Datendatei für Beispielcode 2 | A-4 |

## B Benutzerdefinierte Anmeldeklassen implementieren

---

|   |     |
|---|-----|
| Beispielcodes für benutzerdefinierte Anmeldeklassen | B-1 |
| Benutzerdefinierte Anmeldeklassen bereitstellen     | B-4 |

## C Benutzer und Gruppen benutzerverzeichnisübergreifend migrieren

---

|                            |     |
|----------------------------|-----|
| Übersicht                  | C-1 |
| Voraussetzungen            | C-1 |
| Migrationsverfahren        | C-2 |
| Produktspezifische Updates | C-5 |

# Dokumentation zur Barrierefreiheit

Informationen zu Oracles Verpflichtung zur Barrierefreiheit erhalten Sie über die Website zum Oracle Accessibility Program <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

## **Zugriff auf Oracle Support**

Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischen Support über My Oracle Support. Weitere Informationen erhalten Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>, falls Sie eine Hörbehinderung haben.

# Dokumentationsfeedback

Um Feedback zu dieser Dokumentation abzugeben, klicken Sie unten auf der Seite eines beliebigen Themas im Oracle Help Center auf die Schaltfläche "Feedback". Sie können auch eine E-Mail an [epmdoc\\_ww@oracle.com](mailto:epmdoc_ww@oracle.com) senden.



# 1

## Informationen zur EPM System-Sicherheit

### Siehe auch:

- [Informationen zu EPM System](#)
- [Erforderliche Kenntnisse](#)
- [Komponenten der Sicherheitsinfrastruktur](#)
- [Benutzerauthentifizierung](#)
- [Provisioning \(rollenbasierte Autorisierung\)](#)
- [Shared Services Console starten](#)

## Informationen zu EPM System

Oracle Enterprise Performance Management System-Produkte bilden ein umfassendes unternehmensweites System, das modulare Suiten von Financial Management- und Planning-Anwendungen mit den umfangreichsten Business Intelligence-Funktionen für das Reporting und die Analyse integriert. Wichtige Komponenten von EPM System-Produkten:

- Oracle Hyperion Foundation Services
- Oracle Essbase
- Oracle Hyperion Financial Management
- Oracle Hyperion Planning

Informationen zu den Produkten und Komponenten der einzelnen Produktfamilien finden Sie in der Dokumentation *Oracle Enterprise Performance Management System - Installation: Beginnen Sie hier*.

## Erforderliche Kenntnisse

Diese Dokumentation richtet sich an Systemadministratoren, die Oracle Enterprise Performance Management System-Komponenten konfigurieren, sichern und verwalten. Es werden Kenntnisse in den folgenden Bereichen vorausgesetzt:

- Ein umfassendes Verständnis der Sicherheitsinfrastruktur Ihres Unternehmens. Dies umfasst Folgendes:
  - Verzeichnisserver, wie z.B. Oracle Internet Directory, Sun Java System Directory Server und Microsoft Active Directory
  - Verwendung von Secure Socket Layer (SSL) zum Sichern von Kommunikationskanälen
  - Zugriffsverwaltungssysteme, wie z.B. Oracle Access Manager und SiteMinder
  - SSO-(Single Sign-On-)Infrastruktur, wie z.B. Kerberos
- Kenntnis der EPM System-Sicherheitskonzepte, die für Ihr Unternehmen relevant sind

## Komponenten der Sicherheitsinfrastruktur

Oracle Enterprise Performance Management System integriert verschiedene Sicherheitskomponenten, um eine hohe Anwendungssicherheit zu erreichen. Wenn EPM System in eine sichere Infrastruktur integriert ist, bietet es eine Anwendungssuite, die höchsten Sicherheitsanforderungen entspricht und für Daten- und Zugriffssicherheit sorgt. Infrastrukturkomponenten, die Sie verwenden können, um EPM System zu sichern:

- Ein optionales Zugriffsverwaltungssystem, wie z.B. Oracle Access Manager, um SSO-Zugriff auf EPM System-Komponenten bereitzustellen.
- Verwendung einer integrierten SSO-Infrastruktur, z.B. Kerberos.  
Sie können die Kerberos-Authentifizierung mit dem Zugriffsverwaltungssystem (SiteMinder) verwenden, um sicherzustellen, dass sich Windows-Benutzer transparent bei SiteMinder und bei EPM System-Komponenten anmelden können.
- Verwendung von Secure Socket Layer (SSL) zum Sichern von Kommunikationskanälen zwischen EPM System-Komponenten und Clients.

## Benutzerauthentifizierung

Die Benutzerauthentifizierung ermöglicht die Single Sign-On-Funktion (SSO) über Oracle Enterprise Performance Management System-Komponenten hinweg, indem die Anmeldeinformationen der einzelnen Benutzer validiert werden, um die authentifizierten Benutzer zu ermitteln. Gemeinsam mit der komponentenspezifischen Autorisierung regelt die Benutzerauthentifizierung den Zugriff auf die EPM System-Komponenten. Der Prozess der Autorisierungserteilung wird als Provisioning bezeichnet.

### Authentifizierungskomponenten

In den folgenden Abschnitten sind die Komponenten beschrieben, die den SSO unterstützen:

- [Native Directory](#)
- [Externe Benutzerverzeichnisse](#)

### Native Directory

Native Directory ist die Bezeichnung für die relationale Datenbank, mit der Oracle Hyperion Shared Services das Provisioning unterstützt und in der Seeddata wie Standardbenutzeraccounts gespeichert werden.

Native Directory-Funktionen:

- EPM System-Standardbenutzeraccounts pflegen und verwalten
- Alle Provisioning-Informationen für EPM System speichern (Beziehungen zwischen Benutzern, Gruppen und Rollen)

Der Zugriff auf Native Directory und dessen Verwaltung erfolgt über Oracle Hyperion Shared Services Console. Informationen hierzu finden Sie unter "Native Directory verwalten" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

## Externe Benutzerverzeichnisse

Benutzerverzeichnisse bezeichnen Unternehmenssysteme zum Verwalten von Benutzern und Identitäten, die mit EPM System-Komponenten kompatibel sind.

EPM System-Komponenten werden von verschiedenen Benutzerverzeichnissen unterstützt. Hierzu gehören u.a. LDAP-fähige Benutzerverzeichnisse, wie z.B. Oracle Internet Directory, Sun Java System Directory Server (früher SunONE Directory Server) und Microsoft Active Directory. Relationale Datenbanken werden auch als Benutzerverzeichnisse unterstützt. Benutzerverzeichnisse, bei denen es sich nicht um Native Directory handelt, werden in dieser Dokumentation als "externe Benutzerverzeichnisse" bezeichnet.

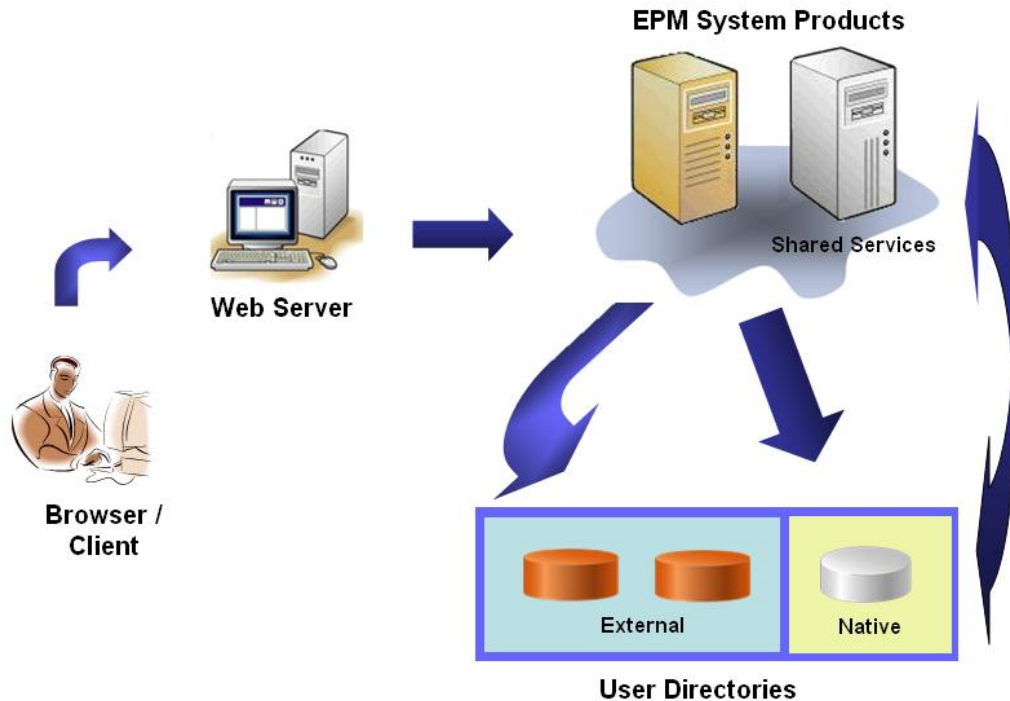
Eine Liste der unterstützten Benutzerverzeichnisse finden Sie unter *Oracle Enterprise Performance Management System Certification Matrix* auf der Seite [Oracle Fusion Middleware Supported System Configurations](#) von Oracle Technology Network (OTN).

Über Shared Services Console können Sie viele externe Benutzerverzeichnisse als Quelle für EPM System-Benutzer und -Gruppen konfigurieren. Jeder EPM System-Benutzer muss über einen eindeutigen Account in einem konfigurierten Benutzerverzeichnis verfügen. EPM System-Benutzer werden in der Regel Gruppen zugewiesen, um das Provisioning zu erleichtern.

## EPM System-Standard-Single Sign-On

EPM System unterstützt SSO in allen EPM System-Webanwendungen, wodurch authentifizierte Benutzer nahtlos von einer Anwendung zu anderen Anwendungen navigieren können, ohne die Zugangsdaten erneut eingeben zu müssen. SSO wird implementiert, indem eine allgemeine Sicherheitsumgebung für die Benutzerauthentifizierung und das Provisioning (rollenbasierte Autorisierung) in alle EPM System-Komponenten integriert wird.

Der SSO-Standardprozess ist in der folgenden Abbildung veranschaulicht.



1. Benutzer rufen über einen Browser das Anmeldefenster einer EPM System-Komponente auf und geben einen Benutzernamen und ein Kennwort ein.  
Die EPM System-Komponente fragt die konfigurierten Benutzerverzeichnisse (einschließlich Native Directory) ab, um die Benutzerzugangsdaten zu prüfen. Wenn in einem Benutzerverzeichnis ein übereinstimmender Benutzeraccount gefunden wird, wird die Suche beendet, und die Benutzerinformationen werden an die EPM System-Komponente zurückgegeben.  
Der Zugriff wird verweigert, wenn in den konfigurierten Benutzerverzeichnissen kein Benutzeraccount gefunden werden kann.
2. Mit den abgerufenen Benutzerinformationen fragt die EPM System-Komponente Native Directory ab, um die Provisioning-Details für den Benutzer abzurufen.
3. Die EPM System-Komponente prüft die Access-Control-Liste (ACL) in der Komponente, um die Anwendungsartefakte zu bestimmen, auf die der Benutzer zugreifen kann.

Sobald die Provisioning-Informationen aus Native Directory vorliegen, ist die EPM System-Komponente für den Benutzer verfügbar. An dieser Stelle wird SSO für alle EPM System-Komponenten aktiviert, für die der Benutzer über Berechtigungen verfügt.

### Single Sign-On von Zugriffsverwaltungssystemen

Um EPM System-Komponenten weiter zu sichern, können Sie ein unterstütztes Zugriffsverwaltungssystem implementieren, wie z.B. Oracle Access Manager oder SiteMinder. Dieses System kann EPM System-Komponenten die Zugangsdaten von authentifizierten Benutzern bereitstellen und den Zugriff basierend auf vordefinierten Zugriffsberechtigungen kontrollieren.

SSO von Security Agents ist nur für EPM System-Webanwendungen verfügbar. In diesem Szenario verwenden EPM System-Komponenten die Benutzerinformationen,

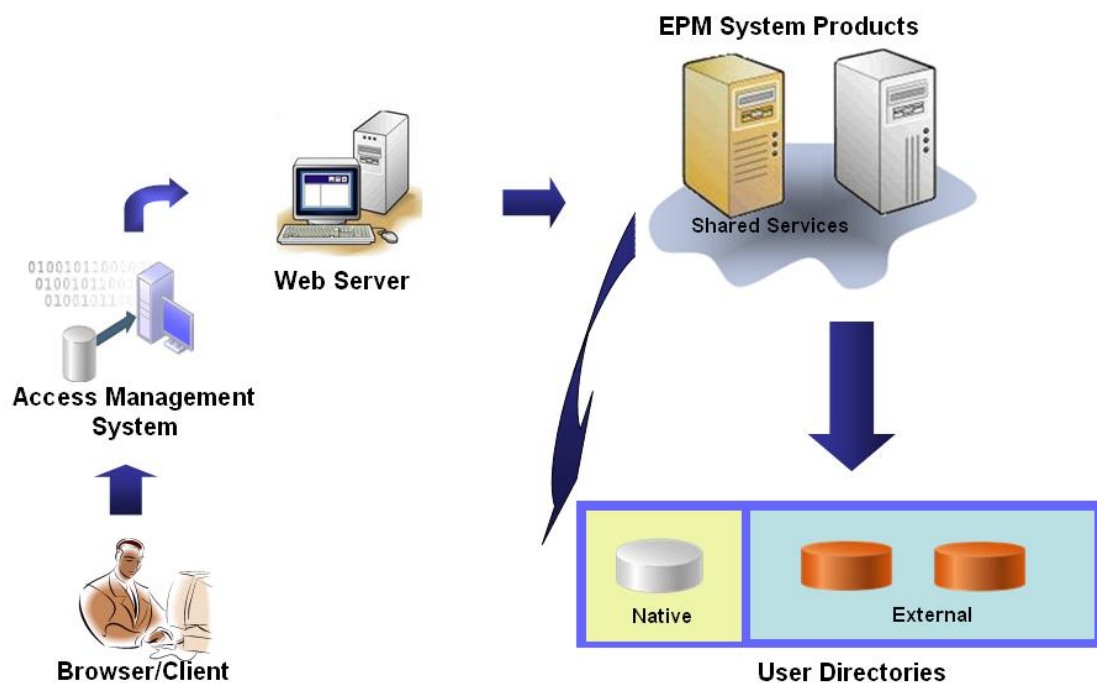
die vom Security Agent bereitgestellt werden, um die Zugriffsberechtigungen von Benutzern zu bestimmen. Um die Sicherheit zu erhöhen, empfiehlt Oracle, den direkten Zugriff auf Server durch Firewalls zu blockieren, damit alle Anforderungen über ein SSO-Portal weitergeleitet werden.

SSO von Zugriffsverwaltungssystemen wird unterstützt, indem Zugangsdaten von authentifizierten Benutzern über einen geeigneten SSO-Mechanismus akzeptiert werden. Informationen hierzu finden Sie unter [Unterstützte SSO-Methoden](#). Das Zugriffsverwaltungssystem authentifiziert Benutzer und übergibt den Anmeldenamen an EPM System. EPM System prüft den Anmeldenamen anhand der konfigurierten Benutzerverzeichnisse.

Informationen hierzu finden Sie in den folgenden Themen.

- [Single Sign-On von Oracle Access Manager](#)
- [Single Sign-On für OracleAS](#)
- [SSO für SiteMinder](#)
- [Single Sign-On für Kerberos](#)

Im Folgenden wird das Konzept veranschaulicht:



1. Benutzer fordern über einen Browser Zugriff auf eine Ressource an, die durch ein Zugriffsverwaltungssystem geschützt ist, z.B. durch Oracle Access Manager oder SiteMinder.

**Hinweis:**

EPM System-Komponenten sind als Ressourcen definiert, die durch das Zugriffsverwaltungssystem geschützt sind.

Das Zugriffsverwaltungssystem fängt die Anforderung ab und zeigt ein Anmeldefenster an. Benutzer geben einen Benutzernamen und ein Kennwort ein, die anhand der konfigurierten Benutzerverzeichnisse im Zugriffsverwaltungssystem validiert werden, um die Authentizität der Benutzer zu prüfen. EPM System-Komponenten sind auch für die Verwendung dieser Benutzerverzeichnisse konfiguriert.

Die Informationen zum authentifizierten Benutzer werden an die EPM System-Komponente übergeben, die die Informationen als gültig akzeptiert.

Das Zugriffsverwaltungssystem verwendet einen geeigneten SSO-Mechanismus, um den Anmeldenamen des Benutzers (Wert von `Login Attribute`) an die EPM System-Komponente zu übergeben. Informationen hierzu finden Sie unter [Unterstützte SSO-Methoden](#).

2. Um die Benutzerzugangsdaten zu prüfen, versucht die EPM System-Komponente, den Benutzer in einem Benutzerverzeichnis zu finden. Wenn ein übereinstimmender Benutzeraccount gefunden wird, werden die Benutzerinformationen an die EPM System-Komponente zurückgegeben. Die EPM System-Sicherheit legt das SSO-Token fest, das SSO in allen EPM System-Komponenten aktiviert.
3. Mit den abgerufenen Benutzerinformationen fragt die EPM System-Komponente Native Directory ab, um die Provisioning-Details für den Benutzer abzurufen.

Sobald die Provisioning-Informationen für den Benutzer vorliegen, ist die EPM System-Komponente für den Benutzer verfügbar. SSO wird für alle EPM System-Komponenten aktiviert, für die der Benutzer über Berechtigungen verfügt.

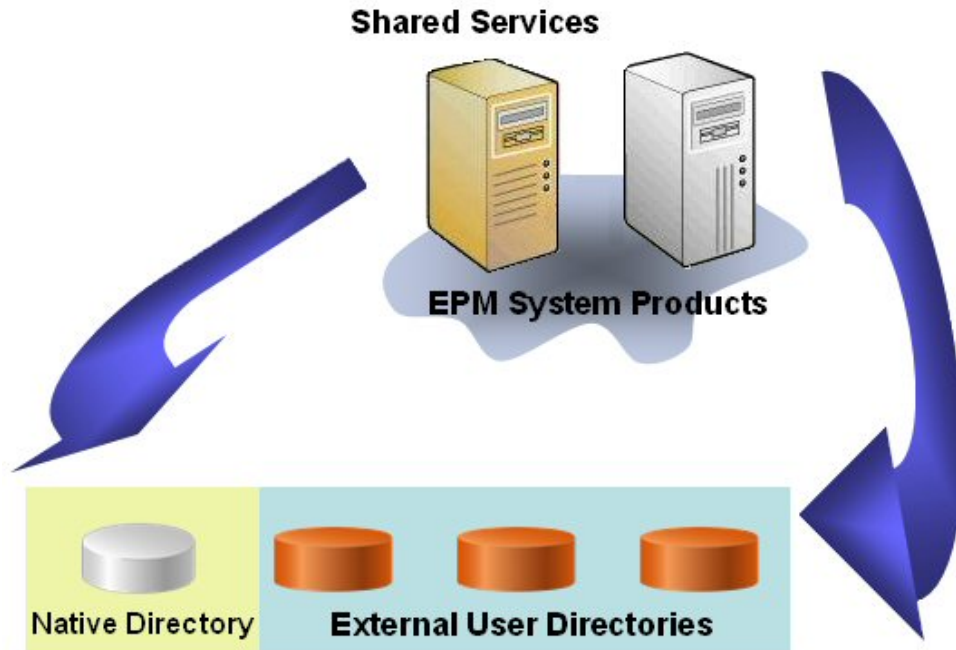
## Provisioning (rollenbasierte Autorisierung)

Die Oracle Enterprise Performance Management System-Sicherheit bestimmt den Benutzerzugriff auf Anwendungen anhand von Rollen. Dabei handelt es sich um Berechtigungen, die den Benutzerzugriff auf die Anwendungsfunktionen bestimmen. Einige EPM System-Komponenten verwenden Objektebenen-Zugriffskontrolllisten (ACLs), um den Benutzerzugriff auf Artefakte wie Berichte und Elemente weiter anzupassen.

Die einzelnen EPM System-Komponenten stellen verschiedene, an die unterschiedlichen geschäftlichen Anforderungen angepasste Standardrollen bereit. Die einzelnen Anwendungen, die zu einer EPM System-Komponente gehören, erben diese Rollen. Vordefinierte Rollen der Anwendungen, die bei Oracle Hyperion Shared Services registriert sind, sind in Oracle Hyperion Shared Services Console verfügbar. Sie können auch zusätzliche Rollen erstellen, die Standardrollen aggregieren, um bestimmten Anforderungen gerecht zu werden. Diese Rollen werden für die Zuweisung von Zugriffsberechtigungen verwendet. Der Vorgang der Zuweisung von bestimmten Rollen für EPM System-Anwendungen und ihre Ressourcen an Benutzer und Gruppen wird auch als *Zuweisung von Berechtigungen* bezeichnet.

Native Directory und konfigurierte Benutzerverzeichnisse sind die Quellen für Benutzer- und Gruppeninformationen für den Provisioning-Prozess. Sie können sämtliche Benutzer und Gruppen aller konfigurierter Benutzerverzeichnisse in Shared Services Console durchsuchen und Berechtigungen dafür zuweisen. Außerdem können Sie anwendungsspezifische aggregierte Rollen verwenden, die beim Provisioning-Prozess in Native Directory erstellt wurden.

In der folgenden Abbildung erhalten Sie eine Übersicht über den Autorisierungsprozess:



1. Nachdem ein Benutzer authentifiziert wurde, fragt die EPM System-Komponente Benutzerverzeichnisse ab, um die Gruppen des Benutzers zu ermitteln.
2. Die EPM System-Komponente verwendet die Benutzer- und Gruppeninformationen, um die Provisioning-Daten des Benutzers aus Shared Services abzurufen. Die Komponente verwendet diese Daten, um zu ermitteln, auf welche Ressourcen ein Benutzer zugreifen kann.

Die produktspezifischen Provisioning-Aufgaben, wie z.B. das Festlegen der produktspezifischen Zugriffskontrolle, werden für jedes Produkt abgeschlossen. Diese Daten werden mit den Berechtigungsdaten kombiniert, um den Produktzugriff für Benutzer festzulegen.

Diese Konzepte werden bei der rollenbasierten Zuweisung der Berechtigungen für EPM System-Produkte verwendet.

### Rollen

Eine Rolle ist ein Konstrukt (ähnlich einer Zugriffskontrollliste (ACL)), das die Zugriffsberechtigungen definiert, die Benutzern und Gruppen gewährt werden, damit diese Funktionen für die EPM System-Ressourcen ausführen können. Bei einer Rolle handelt es sich um eine Kombination aus Ressourcen bzw. Ressourcentypen (auf die Benutzer zugreifen können, z.B. auf einen Bericht) und Aktionen, die Benutzer für die Ressource ausführen können (z.B. anzeigen und bearbeiten).

Der Zugriff auf EPM System-Anwendungsressourcen ist beschränkt. Benutzer können erst darauf zugreifen, nachdem eine Rolle mit entsprechender Zugriffsberechtigung dem Benutzer oder der Gruppe zugewiesen wurde, der der Benutzer angehört. Mit auf Rollen basierenden Zugriffsbeschränkungen können Administratoren den Zugriff auf Anwendungen steuern und verwalten.

## Globale Rollen

Mit globalen Rollen, also Shared Services-Rollen für mehrere Produkte, können Benutzer bestimmte Aufgaben in allen EPM System-Produkten ausführen. Beispiel: Der Shared Services-Administrator kann Benutzern Berechtigungen für alle EPM System-Anwendungen zuweisen.

## Vordefinierte Rollen

Vordefinierte Rollen sind Rollen, die in EPM System-Produkte integriert sind. Diese Rollen können nicht gelöscht werden. Die einzelnen Anwendungsinstanzen, die zu einem EPM System-Produkt gehören, erben die vordefinierten Rollen des Produkts. Die jeweiligen Anwendungsrollen werden beim Erstellen der Anwendung in Shared Services registriert.

## Aggregierte Rollen

Aggregierte Rollen, die auch als benutzerdefinierte Rollen bezeichnet werden, umfassen mehrere vordefinierte Rollen einer Anwendung. Eine aggregierte Rolle kann andere aggregierte Rollen enthalten. Beispiel: Ein Shared Services-Administrator oder -Provisioning-Manager kann eine aggregierte Rolle erstellen, in der die Rollen "Planer" und "Anzeigebenutzer" einer Oracle Hyperion Planning-Anwendung kombiniert sind. Das Aggregieren von Rollen vereinfacht u.U. die Administration von Produkten, die mehrere spezielle Rollen aufweisen. Globale Shared Services-Rollen können in aggregierte Rollen eingefügt werden. Das Erstellen von anwendungs- oder produktübergreifenden aggregierten Rollen ist jedoch nicht möglich.

## Benutzer

In Benutzerverzeichnissen sind Informationen zu den Benutzern gespeichert, die auf EPM System-Produkte zugreifen können. Sowohl bei der Authentifizierung als auch während des Autorisierungsprozesses werden Benutzerinformationen verwendet. Sie können Native Directory-Benutzer nur über Shared Services Console erstellen und verwalten.

In Shared Services Console können Sie die Benutzer aller konfigurierten Benutzerverzeichnisse anzeigen. Sie können diesen Benutzern individuell Berechtigungen zuweisen, um die Zugriffsrechte für die EPM System-Anwendungen zu gewähren, die unter Shared Services registriert sind. Oracle empfiehlt die Zuweisung von Berechtigungen für einzelne Benutzer jedoch nicht.

## Standardmäßiger EPM System-Administrator

Während des Deployment-Prozesses wird in Native Directory ein Administratoraccount mit dem Standardnamen `admin` erstellt. Dies ist der umfassendste EPM System-Account. Dieser Account sollte nur zum Einrichten eines Systemadministrators verwendet werden, der als Informationstechnologieexperte für die Verwaltung der Sicherheit und der Umgebung von EPM System verantwortlich ist.

Der Benutzername und das Kennwort des EPM System-Administrators werden während des Deployments von Oracle Hyperion Foundation Services festgelegt. Da dieser Account keinen Unternehmens-Policies für Accountkennwörter unterliegt, empfiehlt Oracle, diesen Account nach der Erstellung des Systemadministratoraccounts zu deaktivieren.

Der EPM System-Standardadministratoraccount wird in der Regel zum Ausführen dieser Aufgaben verwendet:



- Unternehmensverzeichnis als externes Benutzerverzeichnis konfigurieren. Informationen hierzu finden Sie unter [Benutzerverzeichnisse konfigurieren](#).
- Systemadministratoraccount erstellen, indem einem Informationstechnologieexperten des Unternehmens die Shared Services-Administratorrolle zugewiesen wird. Informationen hierzu finden Sie im Abschnitt zum Provisioning für Benutzer und Gruppen in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

### Systemadministrator

Der Systemadministrator ist normalerweise ein Informationstechnologieexperte des Unternehmens, der für alle Server in einem EPM System-Deployment über Zugriffsrechte zum Lesen, Schreiben und Ausführen verfügt.

Der Systemadministrator führt in der Regel folgende Aufgaben aus:

- EPM System-Standardadministratoraccount deaktivieren.
- Mindestens einen funktionalen Administrator erstellen.
- Sicherheitskonfiguration für EPM System über Shared Services Console festlegen.
- Optional Benutzerverzeichnisse als externe Benutzerverzeichnisse konfigurieren.
- EPM System durch regelmäßige Ausführung des Loganalysetools überwachen.

Die Aufgaben, die funktionale Administratoren ausführen, sind in dieser Dokumentation beschrieben.

Schritte zum Erstellen eines funktionalen Administrators:

- Unternehmensverzeichnis als externes Benutzerverzeichnis konfigurieren. Informationen hierzu finden Sie unter [Benutzerverzeichnisse konfigurieren](#).
- Einem Benutzer oder eine Gruppe die erforderlichen Rollen zum Erstellen eines funktionalen Administrators zuweisen. Informationen hierzu finden Sie im Abschnitt zum Provisioning für Benutzer und Gruppen in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

Dem funktionalen Administrator müssen folgende Rollen zugewiesen werden:

- Rolle "LCM-Administrator" von Shared Services
- Rolle "Administrator" und Rolle "Provisioning-Manager" jeder bereitgestellten EPM System-Komponente

### Funktionale Administratoren

Der funktionale Administrator ist ein Unternehmensbenutzer und ein EPM System-Experte. Dieser Benutzer ist meistens im Unternehmensverzeichnis definiert, dass in Shared Services als ein externes Benutzerverzeichnis konfiguriert ist.

Der funktionale Administrator führt EPM System-Administrationsaufgaben aus, wie z.B. das Erstellen anderer funktionaler Administratoren, das Einrichten der delegierten Administration, das Erstellen von Anwendungen und Artefakten und das Zuweisen der entsprechenden Berechtigungen sowie das Einrichten des EPM System-Auditing. Die Aufgaben, die funktionale Administratoren ausführen, sind in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit* beschrieben.

## Gruppen

Gruppen sind Container für Benutzer und andere Gruppen. Sie können Native Directory-Gruppen über Shared Services Console erstellen und verwalten. Gruppen aus allen konfigurierten Benutzerverzeichnissen werden in Shared Services Console angezeigt. Sie können diesen Gruppen Berechtigungen zuweisen, um Zugriffsberechtigungen für die EPM System-Produkte zu gewähren, die unter Shared Services registriert sind.

# Shared Services Console starten

Sie greifen über eine Menüoption in Oracle Hyperion Enterprise Performance Management Workspace auf Oracle Hyperion Shared Services Console zu.

So starten Sie Shared Services Console:

1. Rufen Sie die folgende URL auf:

```
http://web_server_name:port_number/workspace
```

In der URL steht *web\_server\_name* für den Namen des Computers, auf dem der von Oracle Hyperion Foundation Services verwendete Webserver ausgeführt wird, und *port\_number* steht für den Webserverport, z.B. `http://myWebserver:19000/workspace`.

### Hinweis:

Wenn Sie in sicheren Umgebungen auf EPM Workspace zugreifen, verwenden Sie als Protokoll `https` (nicht `http`) und die sichere Webserverportnummer. Beispiel: Verwenden Sie einen URL wie `https://myserver:19043/workspace`.

2. Klicken Sie auf **Anwendung starten**.

### Hinweis:

Popup-Blocker können das Öffnen von EPM Workspace verhindern.

3. Geben Sie unter **Anmelden** Ihren Benutzernamen und das Kennwort ein.

Zu Anfang ist der einzige Benutzer, der auf Shared Services Console zugreifen kann, der Oracle Enterprise Performance Management System-Administrator, dessen Benutzername und Kennwort während des Deployment-Prozesses festgelegt wurden.

4. Klicken Sie auf **Anmelden**.
5. Wählen Sie **Navigieren, Verwalten, Shared Services Console** aus.

# 2

## SSL-Aktivierung für EPM System-Komponenten

### Siehe auch:

- [Annahmen](#)
- [Informationsquellen](#)
- [Speicherortreferenzen](#)
- [Informationen zur SSL-Aktivierung für EPM System-Produkte](#)
- [Unterstützte SSL-Szenarios](#)
- [Erforderliche Zertifikate](#)
- [SSL auf dem SSL-Offloader beenden](#)
- [Vollständiges SSL-Deployment von EPM System](#)
- [SSL auf dem Webserver beenden](#)
- [SSL für Essbase 11.1.2.4](#)
- [SSL für Essbase 21c](#)

### Annahmen

- Sie haben die Deployment-Topologie festgelegt und die Kommunikationsverknüpfungen identifiziert, die mit SSL gesichert werden müssen.
- Sie haben die erforderlichen Zertifikate von einer Certificate Authority (CA), entweder einer gut bekannten CA oder Ihrer eigenen erhalten, oder haben selbstsignierte Zertifikate erstellt. Informationen hierzu finden Sie unter [Erforderliche Zertifikate](#).
- Sie sind mit SSL-Konzepten und -Verfahren vertraut, wie z.B. dem Importieren von Zertifikaten.

Eine Liste mit Referenzdokumenten finden Sie unter [Informationsquellen](#).

### Informationsquellen

Damit SSL für Oracle Enterprise Performance Management System aktiviert werden kann, müssen Sie Komponenten, wie z.B. Anwendungsserver, Webserver, Datenbanken und Benutzerverzeichnisse, für die Kommunikation mit SSL vorbereiten. In diesem Dokument wird angenommen, dass Sie mit den Aufgaben zur Aktivierung von SSL für diese Komponenten vertraut sind.

- **Oracle WebLogic Server:** Siehe Abschnitt zur [SSL-Konfiguration](#) in der Dokumentation *Securing WebLogic Server Guide*.
- **Oracle HTTP Server:** Siehe folgende Themen in der Dokumentation *Oracle HTTP Server Administrator's Guide*:

- [Sicherheit verwalten](#)
- [SSL für Oracle HTTP Server aktivieren](#)
- **Benutzerverzeichnisse:** Siehe Dokumentation des Benutzerverzeichnisanbieters. Nützliche Links:
  - **Oracle Internet Directory:** Informationen hierzu finden Sie in der Dokumentation [Oracle Internet Directory Administrator's Guide](#).
  - **Sun Java System Directory Server:** Siehe Abschnitt zur [Verzeichnisserversicherheit](#) in der Dokumentation *Sun Java System Directory Server Administration Guide*.
  - **Active Directory:** Siehe Microsoft-Dokumentation.
- **Datenbanken:** Siehe Dokumentation des jeweiligen Datenbankanbieters.

## Speicherortreferenzen

Dieses Dokument bezieht sich auf die folgenden Installations- und Deployment-Speicherorte:

- *MIDDLEWARE\_HOME* bezieht sich auf den Speicherort von Middleware-Komponenten, wie z.B. Oracle WebLogic Server, und optional auf mindestens ein *EPM\_ORACLE\_HOME*-Verzeichnis. Das *MIDDLEWARE\_HOME*-Verzeichnis wird bei der Oracle Enterprise Performance Management System-Produktinstallation definiert. Das *MIDDLEWARE\_HOME*-Standardverzeichnis lautet `Oracle/Middleware`.
- *EPM\_ORACLE\_HOME* bezieht sich auf das Installationsverzeichnis mit den Dateien, die für EPM System-Produkte erforderlich sind. *EPM\_ORACLE\_HOME* befindet sich in *MIDDLEWARE\_HOME*. Das *EPM\_ORACLE\_HOME*-Standardverzeichnis lautet `MIDDLEWARE_HOME/EPMSysstem11R1`, z.B. `Oracle/Middleware/EPMSysstem11R1`.

EPM System-Produkte werden im Verzeichnis *EPM\_ORACLE\_HOME/products* installiert, z.B. `Oracle/Middleware/EPMSysstem11R1/products`.

Bei der EPM System-Produktkonfiguration stellen manche Produkte zusätzlich Komponenten im Verzeichnis *MIDDLEWARE\_HOME/user\_projects/epmsystem1* bereit, z.B. `Oracle/Middleware/user_projects/epmsystem1`.

- *EPM\_ORACLE\_INSTANCE* gibt einen Speicherort an, der während des Konfigurationsprozesses definiert wird und an dem manche Produkte Komponenten bereitstellen. Der Standardspeicherort von *EPM\_ORACLE\_INSTANCE* ist *MIDDLEWARE\_HOME/user\_projects/epmsystem1*, z.B. `Oracle/Middleware/user_projects/epmsystem1`.

## Informationen zur SSL-Aktivierung für EPM System-Produkte

Der Oracle Enterprise Performance Management System-Deployment-Prozess stellt Oracle EPM System-Produkte automatisch sowohl im SSL- als auch im Nicht-SSL-Modus bereit.

 **Hinweis:**

- EPM System unterstützt SSL nur über HTTP und JDBC. Andere Standards für die sichere Kommunikation, wie z.B. Thrift und ODBC, werden nicht unterstützt.
- Zum Schutz gegen die Poodle-(Padding Oracle On Downgraded Legacy Encryption-)Sicherheitslücke (Angriff auf das SSLv3-Protokoll) müssen Sie die SSLv3-Unterstützung auf Ihren Servern und in den Browsern deaktivieren, die für den Zugriff auf EPM System-Komponenten verwendet werden. Informationen zum Deaktivieren der SSLv3-Unterstützung finden Sie in Ihrer Server- und Browserdokumentation.
- EPM System-Server können möglicherweise nicht gestartet werden, wenn Sie den Nicht-SSL-Modus nach dem Konfigurieren von SSL deaktivieren. Aktivieren Sie die sichere Replikation für alle EPM System-Server in der Domain, damit sie gestartet werden, wenn der Nicht-SSL-Modus deaktiviert ist.

Beim Festlegen allgemeiner Einstellungen für EPM System geben Sie an, ob für die gesamte Server-zu-Server-Kommunikation in Ihrem Deployment SSL aktiviert werden soll.

Wenn Sie während des Deployment-Prozesses SSL-Einstellungen auswählen, wird Ihre Umgebung nicht automatisch für SSL konfiguriert. In der Oracle Hyperion Shared Services-Registry wird nur ein Kennzeichen gesetzt, mit dem angegeben wird, dass alle EPM System-Komponenten, die die Shared Services-Registry nutzen, für die Server-zu-Server-Kommunikation das sichere Protokoll (HTTPS) verwenden müssen. Sie müssen zusätzliche Schritte ausführen, um SSL für Ihre Umgebung zu aktivieren. Diese Verfahren werden in diesem Dokument erläutert.

 **Hinweis:**

Wenn Sie Ihre Anwendungen erneut bereitstellen, werden die benutzerdefinierten Einstellungen für den Anwendungsserver und für den Webserver, die Sie zum Aktivieren von SSL angeben, gelöscht.

 **Hinweis:**

In Enterprise Performance Management System Release 11.2.x wird Secure Sockets Layer (SSL) für MS SQL Server in Repository Creation Utility (RCU) nicht unterstützt.

## Unterstützte SSL-Szenarios

Die folgenden SSL-Szenarios werden unterstützt:

- SSL-Beendigung auf dem SSL-Offloader. Informationen hierzu finden Sie unter [SSL auf dem SSL-Offloader beenden](#).
- Vollständiges SSL-Deployment. Informationen hierzu finden Sie unter [Vollständiges SSL-Deployment von EPM System](#).

## Erforderliche Zertifikate

Die SSL-Kommunikation verwendet Zertifikate, um Vertrauenswürdigkeit zwischen Komponenten herzustellen. Oracle empfiehlt, Zertifikate von bekannten Drittanbieter-CAs zu verwenden, um SSL für Oracle Enterprise Performance Management System in einer Produktionsumgebung zu aktivieren.

### Hinweis:

EPM System unterstützt die Verwendung von Platzhalterzertifikaten, wodurch mehrere Subdomains mit einem SSL-Zertifikat gesichert werden können. Die Verwendung eines Platzhalterzertifikats ermöglicht Zeit- und Kosteneinsparungen bei der Verwaltung.

Wenn Sie Platzhalterzertifikate zum Verschlüsseln der Kommunikation verwenden, müssen Sie die Hostnamenüberprüfung in Oracle WebLogic Server deaktivieren.

Sie benötigen die folgenden Zertifikate für jeden Server, der EPM System-Komponenten hostet.

- Ein CA-Stammzertifikat

### Hinweis:

Sie müssen kein CA-Stammzertifikat im Java-Keystore installieren, wenn Sie Zertifikate einer bekannten Drittanbieter-CA verwenden, deren Stammzertifikat bereits im Java-Keystore installiert ist.

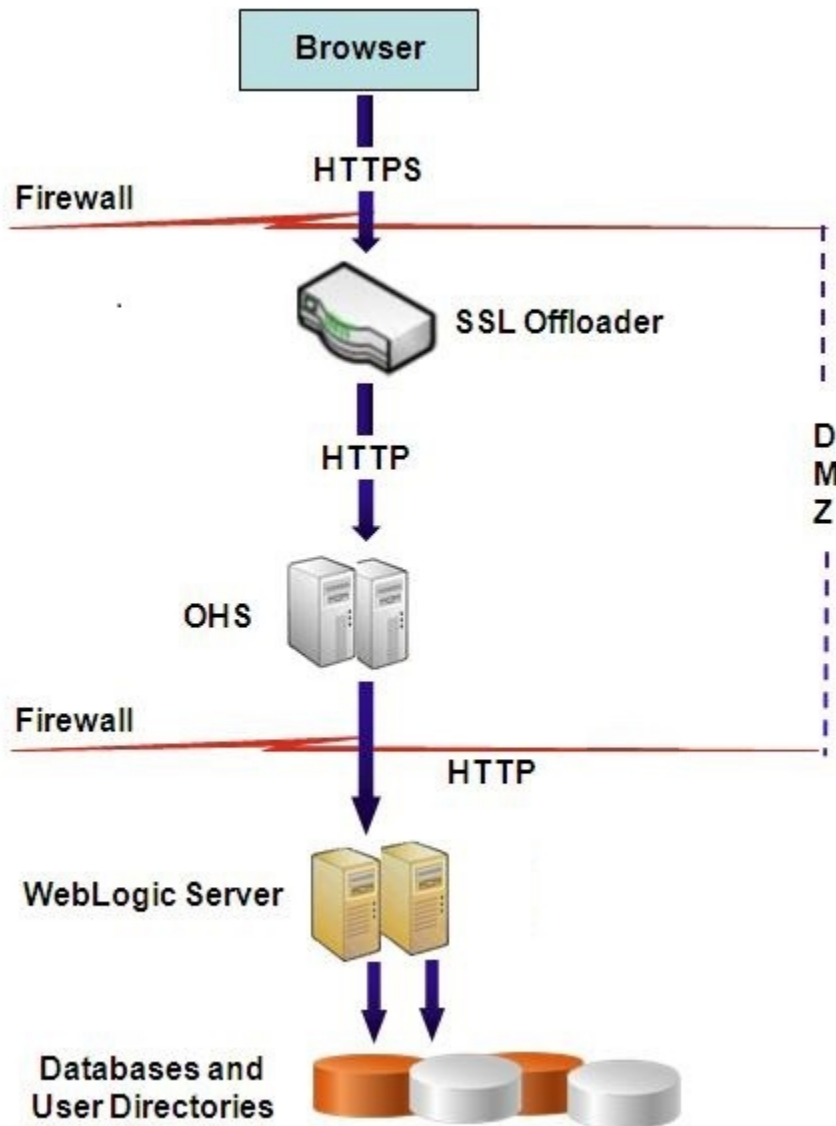
In Firefox und Internet Explorer sind bereits Zertifikate von bekannten Drittanbieter-CAs geladen. Wenn Sie selbst als CA fungieren, müssen Sie Ihr CA-Stammzertifikat in den Keystore der Clients importieren, die über diese Browser aufgerufen werden. Wenn Sie selbst als CA fungieren, können Webclients keinen SSL-Handshake mit dem Server herstellen, wenn Ihr CA-Stammzertifikat nicht in dem Browser verfügbar ist, über den der Client aufgerufen wird.

- Signierte Zertifikate für jeden Oracle HTTP Server in Ihrem Deployment
- Ein signiertes Zertifikat für den WebLogic Server-Hostcomputer. Managed Server auf diesem Computer können dieses Zertifikat ebenfalls verwenden.
- Zwei Zertifikate für den SSL-Offloader/Load Balancer. Eines dieser Zertifikate dient zur externen Kommunikation und das andere zur internen Kommunikation.

## SSL auf dem SSL-Offloader beenden

### Deployment-Architektur

In diesem Szenario wird SSL verwendet, um den Kommunikationslink zwischen Oracle Enterprise Performance Management System-Clients (z.B. einem Browser) und einem SSL-Offloader zu sichern. Im Folgenden wird das Konzept veranschaulicht:



### Annahmen

#### SSL-Offloader und Load Balancer

Ein vollständig konfigurierter SSL-Offloader mit einem Load Balancer muss in der Deployment-Umgebung vorhanden sein.

Der Load Balancer muss so konfiguriert werden, dass alle von den virtuellen Hosts empfangenen Anforderungen an Oracle HTTP Server weitergeleitet werden

Wenn SSL auf Oracle HTTP Server (OHS) oder auf dem Load Balancer beendet wird, müssen Sie wie folgt vorgehen:

- Legen Sie für jede logische Webanwendung den virtuellen Nicht-SSL-Host von Load Balancer oder Oracle HTTP Server fest (z.B. `empinternal.myCompany.com:80`, wobei "80" der Nicht-SSL-Port ist). Öffnen Sie das Fenster "Konfiguration", und führen Sie die folgenden Schritte aus:
  1. Blenden Sie die Konfigurationsaufgabe **Hyperion Foundation** ein.
  2. Wählen Sie **Logische Adresse für Webanwendungen konfigurieren** aus.
  3. Geben Sie *Hostname*, Nicht-SSL-Portnummer und SSL-Portnummer an.
- Legen Sie als externe URL den virtuellen SSL-Host von Load Balancer oder Oracle HTTP Server fest (z.B. `empexternal.myCompany.com:443`, wobei "443" der SSL-Port ist). Öffnen Sie das Fenster "Konfiguration", und führen Sie die folgenden Schritte aus:
  1. Blenden Sie die Konfigurationsaufgabe **Hyperion Foundation** ein.
  2. Wählen Sie **Gemeinsame Einstellungen konfigurieren** aus.
  3. Wählen Sie unter "Externe URL-Details" die Option **SSL-Offload aktivieren** aus.
  4. Geben Sie einen Wert für *Externer URL-Host* und *Externer URL-Port* an.

 **Hinweis:**

Wenn Sie **configtool** verwenden, um Webanwendungen erneut bereitzustellen oder den Webserver neu zu konfigurieren, werden die Einstellungen für die logische Webanwendung und für externe URLs ersetzt.

### Virtuelle Hosts

Eine Konfiguration, bei der SSL auf dem SSL-Offloader beendet wurde, verwendet zwei Serveraliasnamen auf dem SSL-Offloader/Load Balancer, z.B. `epm.myCompany.com` und `empinternal.myCompany.com`. Ein Serveralias dient zur externen Kommunikation zwischen dem Offloader und Browsern und der zweite zur internen Kommunikation zwischen EPM System-Servern. Stellen Sie sicher, dass die Serveraliasnamen auf die IP-Adresse des Computers verweisen und über DNS aufgelöst werden können.

Ein signiertes Zertifikat zur Unterstützung der externen Kommunikation zwischen dem Offloader und Browsern (über `epm.myCompany.com`) muss auf dem Offloader/Load Balancer installiert sein.

### EPM System konfigurieren

Das Standard-Deployment von EPM System-Komponenten unterstützt die SSL-Beendigung auf dem SSL-Offloader. Es ist keine weitere Aktion erforderlich.

Stellen Sie bei der Konfiguration von EPM System sicher, dass die logische Adresse für Webanwendungen auf den Alias (z.B. `empinternal.myCompany.com`) verweist, der



für die interne Kommunikation erstellt wurde. Anweisungen zum Installieren und Konfigurieren von EPM System finden Sie in den folgenden Informationsquellen:

- *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*
- *Oracle Enterprise Performance Management System - Installation: Beginnen Sie hier*
- *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide*

### Deployments testen

Prüfen Sie nach dem Abschluss des Deployment-Prozesses, ob alles funktioniert, indem Sie eine Verbindung über die sichere Oracle Hyperion Enterprise Performance Management Workspace-URL herstellen:

```
https://virtual_host_external:SSL_PORT/workspace/index.jsp
```

Beispiel: <https://epm.myCompany.com:443/workspace/index.jsp>, wobei 443 der SSL-Port ist.

## Vollständiges SSL-Deployment von EPM System

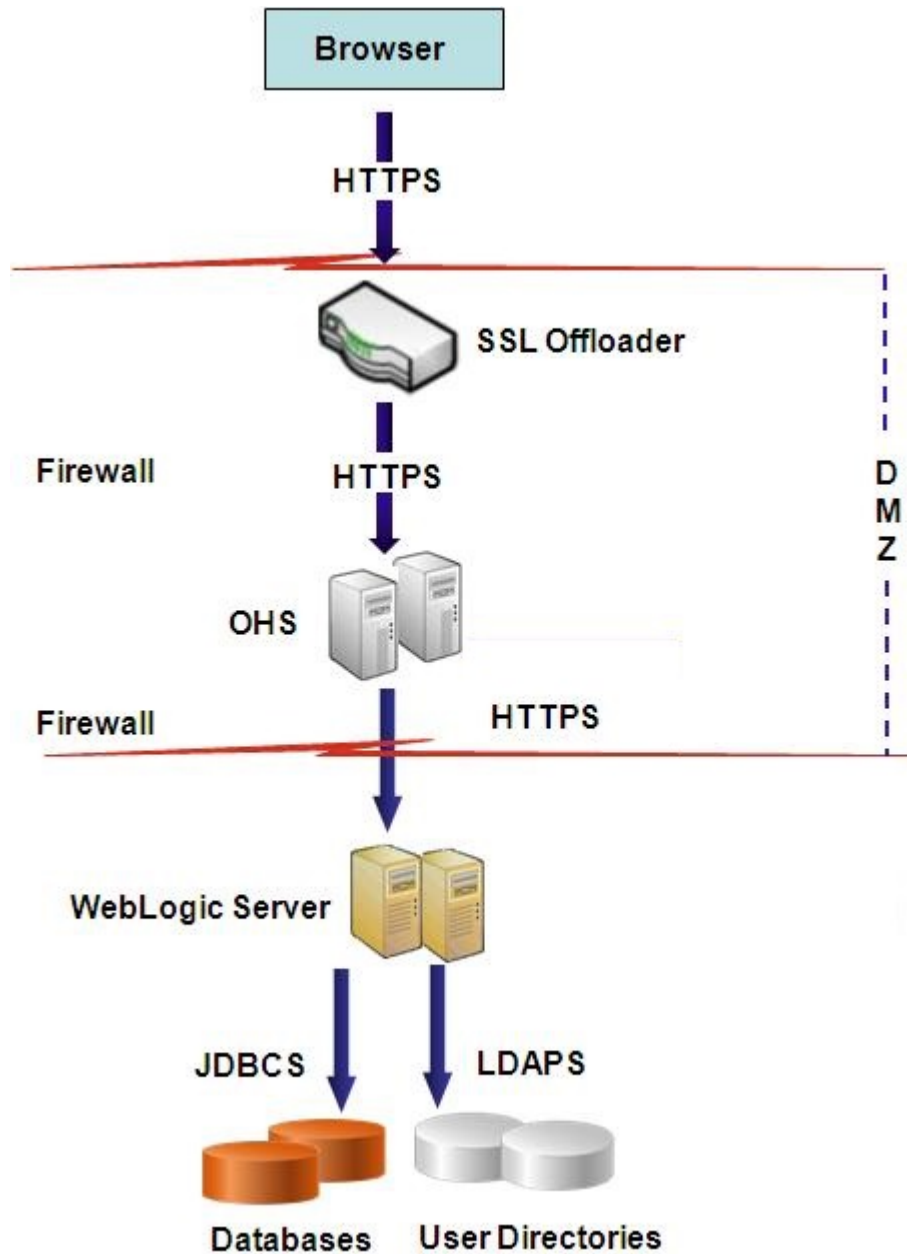
### Siehe auch:

- [Deployment-Architektur](#)
- [Annahmen](#)
- [Vollständige SSL-Konfiguration für EPM System](#)

## Deployment-Architektur

Im vollständigen SSL-Modus wird die Kommunikation in allen sicherbaren Kanälen mit SSL gesichert. Hierbei handelt es sich um das sicherste Deployment-Szenario für Oracle Enterprise Performance Management System.

Im Folgenden wird das Konzept veranschaulicht:



## Annahmen

### Datenbanken

Für die Datenbankserver und -clients ist SSL aktiviert. Informationen zur SSL-Aktivierung für den Datenbankserver und -client finden Sie in Ihrer Datenbankdokumentation.

### EPM System

Oracle Enterprise Performance Management System-Komponenten, einschließlich Oracle WebLogic Server und Oracle HTTP Server, sind installiert und bereitgestellt. Darüber hinaus wurde Ihre EPM System-Umgebung getestet, um sicherzustellen,

dass alles im Nicht-SSL-Modus funktioniert. Informationen hierzu finden Sie in folgenden Quellen:

- *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*
- *Oracle Enterprise Performance Management System - Installation: Beginnen Sie hier*
- *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide*

Wenn Sie SSL für die Datenbankverbindungen aktivieren möchten, müssen Sie während der Konfiguration in jedem Fenster für die Datenbankkonfiguration auf den Link **Erweiterte Optionen** klicken und die erforderlichen Einstellungen angeben. Dies umfasst Folgendes:

- Wählen Sie **Sichere Verbindung zur Datenbank verwenden (SSL)** aus, und geben Sie eine sichere Datenbank-URL ein. Beispiel:  
`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=myDBhost) (PORT=1529) (CONNECT_DATA=(SERVICE_NAME=myDBhost.myCompany.com)))`
- **Vertrauenswürdiger Keystore**
- **Kennwort für vertrauenswürdigen Keystore**

Details finden Sie in der *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*.

### SSL-Offloader und Load Balancer

Ein vollständig konfigurierter SSL-Offloader mit einem Load Balancer muss in der Deployment-Umgebung vorhanden sein.

Bei einer vollständigen SSL-Konfiguration werden im SSL-Offloader zwei Serveraliasnamen verwendet, z.B. `epm.myCompany.com` und `empinternal.myCompany.com`. Ein Alias dient zur externen Kommunikation zwischen dem Offloader und Browsern und der andere zur internen Kommunikation zwischen EPM System-Servern. Stellen Sie sicher, dass die Serveraliasnamen auf die IP-Adresse des Computers verweisen und über DNS aufgelöst werden können.

Der Load Balancer muss so konfiguriert werden, dass alle von den virtuellen Hosts empfangenen Anforderungen an Oracle HTTP Server weitergeleitet werden

Die beiden signierten Zertifikate müssen auf dem Offloader/Load Balancer installiert sein. Das eine Zertifikat unterstützt die externe Kommunikation zwischen dem Offloader und Browsern (über `epm.myCompany.com`) und das andere die interne Kommunikation zwischen Anwendungen (über `empinternal.myCompany.com`). Oracle empfiehlt, diese Zertifikate an Serveraliasnamen zu binden, um die Offenlegung von Servernamen zu verhindern und die Sicherheit zu erhöhen.

## Vollständige SSL-Konfiguration für EPM System

**Siehe auch:**

- [Allgemeine Einstellungen für EPM System neu konfigurieren](#)
- [Optional: CA-Stammzertifikat für WebLogic Server installieren](#)
- [Zertifikat auf WebLogic Server installieren](#)
- [WebLogic Server konfigurieren](#)
- [HFMSerververbindung mit SSL-fähiger Oracle-Datenbank aktivieren](#)

- Verfahren für Oracle HTTP Server
- Auf WebLogic Server bereitgestellte EPM System-Webkomponenten konfigurieren
- Domainkonfiguration aktualisieren
- Server und EPM System neu starten
- Deployments testen
- Externe Benutzerverzeichnisse mit SSL-Aktivierung konfigurieren

## Allgemeine Einstellungen für EPM System neu konfigurieren

Während dieses Prozesses wählen Sie die Einstellungen aus, mit denen die Verwendung der SSL-Kommunikation durch Oracle Enterprise Performance Management System-Komponenten erzwungen wird.

### Hinweis:

**Bei Aktivierung von SSL für den Oracle Hyperion Financial Management-Webserver:** Bevor Sie Financial Management konfigurieren, müssen Sie das Cookie als sicher definieren, indem Sie session-descriptor von HFM WebApp in der Datei `weblogic.xml` bearbeiten.

1. Blenden Sie das Financial Management-Webarchiv mit einem Tool wie 7-Zip ein. Die Datei `weblogic.xml` befindet sich im Archivverzeichnis `EPM_ORACLE_HOME\products\FinancialManagement\AppServer\InstallableApps\HFMWebApplication.ear\HFMWeb.war\WEB-INF\weblogic.xml`.
2. Schließen Sie die folgende Anweisung in session-descriptor von HFM WebApp in der Datei `weblogic.xml` ein:  
`<cookie-secure>true</cookie-secure>`
3. Speichern Sie die Datei `weblogic.xml`.
4. Klicken Sie auf **Ja**, wenn Sie von 7-Zip gefragt werden, ob Sie das Archiv aktualisieren möchten.

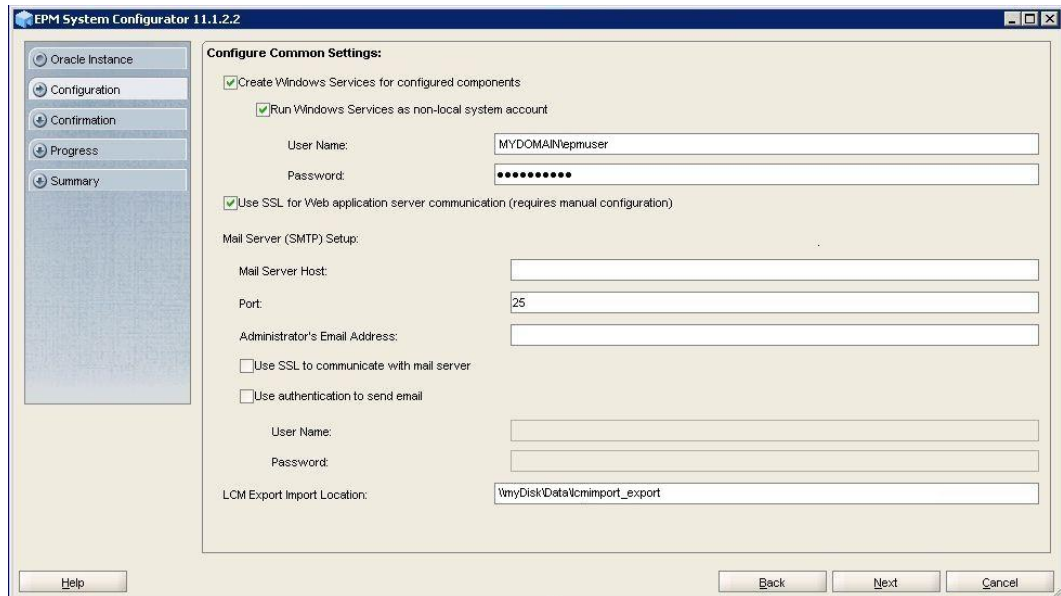
So konfigurieren Sie EPM System für SSL neu:

1. Starten Sie EPM System Configurator.
2. Führen Sie unter **Wählen Sie die EPM Oracle-Instanz, auf die die Konfiguration angewendet wird** die folgenden Schritte aus:
  - a. Geben Sie unter **EPM Oracle-Instanzname** den Instanznamen ein, den Sie bei der ursprünglichen Konfiguration der EPM System-Komponenten verwendet haben.
  - b. Klicken Sie auf **Weiter**.
3. Führen Sie im Fenster "Konfiguration" die folgenden Schritte aus:
  - a. Deaktivieren Sie **Alle deaktivieren**.
  - b. Blenden Sie die **Hyperion Foundation**-Konfigurationsaufgabe ein, und wählen Sie **Gemeinsame Einstellungen konfigurieren** aus.
  - c. Klicken Sie auf **Weiter**.

4. Führen Sie unter **Gemeinsame Einstellungen konfigurieren** die folgenden Schritte aus:

**Achtung:**

Bevor Sie die Einstellungen zur Verwendung von SSL für die Kommunikation mit dem E-Mail-Server auswählen, müssen Sie sicherstellen, dass der E-Mail-Server für SSL konfiguriert ist.



- a. Wählen Sie **SSL für Kommunikation mit Java-Webanwendungsserver verwenden (erfordert manuelle Konfiguration)** aus, um anzugeben, dass EPM System SSL für die Kommunikation verwenden soll.
  - b. **Optional:** Geben Sie Informationen für **Mailserver-Host** und **Port** ein. Um die SSL-Kommunikation zu unterstützen, müssen Sie den sicheren Port angeben, der vom SMTP-Mail-Server verwendet wird.
  - c. **Optional:** Um die SSL-Kommunikation mit dem SMTP-Mail-Server zu unterstützen, wählen Sie **SSL zur Kommunikation mit Mailserver verwenden** aus.
  - d. Wählen Sie in den verbleibenden Feldern Einstellungen aus, oder geben Sie Einstellungen ein.
  - e. Klicken Sie auf **Weiter**.
5. Klicken Sie in den nachfolgenden EPM System Configurator-Fenstern auf **Weiter**.
  6. Wenn der Deployment-Prozess abgeschlossen ist, wird das Fenster "Übersicht" angezeigt. Klicken Sie auf **Fertig stellen**.

## Optional: CA-Stammzertifikate für WebLogic Server installieren

Die Stammzertifikate der meisten bekannten Drittanbieter-CAs sind bereits im JVM-Keystore installiert. Führen Sie die Schritte in diesem Abschnitt aus, wenn Sie keine Zertifikate einer

bekannten Drittanbieter-CA verwenden (nicht empfohlen). Der Standardspeicherort des JVM-Keystores lautet `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`.



#### Hinweis:

Führen Sie diese Schritte auf allen Oracle Enterprise Performance Management System-Servern aus.

So installieren Sie CA-Stammzertifikate:

1. Kopieren Sie das CA-Stammzertifikat in ein lokales Verzeichnis auf dem Computer, auf dem Oracle WebLogic Server installiert ist.
2. Ändern Sie in einer Konsole das Verzeichnis in `MIDDLEWARE_HOME/jdk/jre/bin`.
3. Führen Sie einen `keytool`-Befehl wie den folgenden aus, um das CA-Stammzertifikat im JVM-Keystore zu installieren:

```
keytool -import -alias ALIAS -file CA_CERT_FILE -keystore KEYSTORE -storepass KEYSTORE_PASSWORD -trustcacerts
```

Beispiel: Sie können den folgenden Befehl verwenden, um das im aktuellen Verzeichnis gespeicherte Zertifikat `CAcert.crt` im JVM-Keystore mit `Blister` als Zertifikatalias im Keystore hinzuzufügen. Für Storepass wird der Wert `example_pwd` angenommen.

```
keytool -import -alias Blister -file CAcert.crt -keystore ../lib/security/cacerts -storepass example_pwd -trustcacerts
```



#### Hinweis:

Der obige Befehl und das entsprechende Beispiel verwenden Syntax zum Importieren von Zertifikaten mit `keytool`. Eine vollständige Liste der Importsyntax finden Sie in der `keytool`-Dokumentation.

## Zertifikat auf WebLogic Server installieren

Die Oracle WebLogic Server-Standardinstallation verwendet ein Demozertifikat, um SSL zu unterstützen. Oracle empfiehlt, ein Zertifikat eines bekannten Drittanbieters zu installieren, um die Sicherheit Ihrer Umgebung zu erhöhen.

Verwenden Sie auf jedem Hostcomputer von WebLogic Server ein Tool (z.B. `keytool`) zum Erstellen eines benutzerdefinierten Keystores, um das signierte Zertifikat für WebLogic Server- und Oracle Enterprise Performance Management System-Webkomponenten zu speichern.

So erstellen Sie benutzerdefinierte Keystores und importieren Zertifikate:

1. Ändern Sie in einer Konsole das Verzeichnis in `MIDDLEWARE_HOME/jdk/jre/bin`.

2. Führen Sie einen keytool-Befehl wie den folgenden aus, um den benutzerdefinierten Keystore (angegeben durch die Anweisung `-keystore` im Befehl) in einem vorhandenen Verzeichnis zu erstellen:

```
keytool -genkey -dname "cn=myserver, ou=EPM, o=myCompany, c=US" -alias  
epm_ssl -keypass password -keystore  
C:\oracle\Middleware\EPMSysstem11R1\ssl\keystore -storepass password -  
validity 365 -keyalg RSA
```

 **Hinweis:**

Der allgemeine Name (CN), den Sie festlegen, muss dem Servernamen entsprechen. Wenn Sie einen vollqualifizierten Domainnamen (FQDN) als CN verwenden, müssen Sie den FQDN beim Deployment von Webkomponenten verwenden.

3. Generieren Sie eine Zertifikatanforderung.

```
keytool -certreq -alias epm_ssl -file C:/certs/epmssl_csr -keypass  
password -storetype jks -keystore  
C:\oracle\Middleware\EPMSysstem11R1\ssl\keystore -storepass password
```

4. Fordern Sie ein signiertes Zertifikat für den WebLogic Server-Computer an.
5. Importieren Sie das signierte Zertifikat in den Keystore:

```
keytool -import -alias epm_ssl -file C:/certs/epmssl_cert -keypass  
password -keystore C:\Oracle\Middleware\EPMSysstem11R1\ssl\keystore -  
storepass password
```

## WebLogic Server konfigurieren

Nach dem Deployment von Oracle Enterprise Performance Management System-Webkomponenten müssen Sie sie für die SSL-Kommunikation konfigurieren.

So konfigurieren Sie die Webkomponenten für SSL:

1. Starten Sie Oracle WebLogic Server, indem Sie `MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/bin/startWebLogic.cmd` ausführen:
2. Starten Sie die WebLogic Server-Administrationskonsole, indem Sie die folgende URL aufrufen:

```
http://SERVER_NAME:Port/console
```

Beispiel: Um auf die WebLogic Server-Konsole zuzugreifen, die über den Standardport auf `myServer` bereitgestellt ist, verwenden Sie `http://myServer:7001/console`.

3. Geben Sie auf dem Begrüßungsbildschirm den Benutzernamen und das Kennwort des WebLogic Server-Administrators ein. Diese Zugangsdaten haben Sie in EPM System Configurator angegeben.
4. Klicken Sie im **Change Center** auf **Sperren und bearbeiten**.

5. Blenden Sie im linken Fenster der Konsole **Umgebung** ein, und wählen Sie **Server** aus.
6. Klicken Sie im Fenster "Zusammenfassung der Server" auf den Namen des Servers, für den Sie SSL aktivieren möchten.  
  
Beispiel: Um SSL für Oracle Hyperion Foundation Services-Komponenten zu aktivieren, verwenden Sie den Server `EPMServer0`.
7. Deaktivieren Sie **Listening-Port aktiviert**, um den HTTP-Listening-Port zu deaktivieren.
8. Stellen Sie sicher, dass **SSL-Listening-Port aktiviert** aktiviert ist.
9. Geben Sie unter **SSL-Listening-Port** den SSL-Listening-Port ein, den dieser Server auf Anforderungen abhören soll.
10. Wählen Sie **Keystores** aus, um die Registerkarte "Keystores" zu öffnen, und geben Sie den zu verwendenden Identity und Trust Keystore an.
11. Klicken Sie auf **Ändern**.
12. Wählen Sie eine Option aus:
  - **Benutzerdefinierte Identity und Trust**, wenn Sie kein Serverzertifikat einer bekannten Drittanbieter-CA verwenden
  - **Benutzerdefinierte Identity und Java-Standard-Trust**, wenn Sie ein Serverzertifikat einer bekannten Drittanbieter-CA verwenden
13. Klicken Sie auf **Speichern**.
14. Geben Sie unter **Benutzerdefinierter Identity Keystore** den Pfad des Keystores ein, in dem das signierte WebLogic Server-Zertifikat installiert ist.
15. Geben Sie unter **Benutzerdefinierter Identity Keystore-Typ** den Wert `jks` ein.
16. Geben Sie unter **Benutzerdefinierte Identity Keystore-Passphrase** und **Benutzerdefinierte Passphrase des Identity Keystores bestätigen** das Keystore-Kennwort ein.
17. Gehen Sie wie folgt vor, wenn Sie unter **Keystores** die Option **Benutzerdefinierte Identity und Trust** ausgewählt haben:
  - Geben Sie unter **Benutzerdefinierter Trust Keystore** den Pfad des benutzerdefinierten Keystores ein, in dem das Stammzertifikat der CA verfügbar ist, die Ihr Serverzertifikat signiert hat.
  - Geben Sie unter **Benutzerdefinierter Trust Keystore-Typ** den Wert `jks` ein.
  - Geben Sie unter **Benutzerdefinierte Trust Keystore-Passphrase** und **Benutzerdefinierte Passphrase des Trust Keystores bestätigen** das Keystore-Kennwort ein.
18. Klicken Sie auf **Speichern**.
19. Geben Sie SSL-Einstellungen an:
  - Wählen Sie **SSL** aus.
  - Geben Sie unter **Private Key-Alias** den Alias ein, den Sie beim Importieren des signierten WebLogic Server-Zertifikats angegeben haben.
  - Geben Sie unter **Private Key-Passphrase** und **Private Key-Passphrase bestätigen** das Kennwort ein, das zum Abrufen des Private Keys verwendet werden soll.



- Klicken Sie auf **Speichern**.

 **Hinweis:**

Wenn Sie SHA-2-Zertifikate verwenden, müssen Sie die Einstellung **JSSE SSL verwenden** für jeden verwalteten Server auswählen, der zur Unterstützung von EPM System verwendet wird. Diese Einstellung ist in der Registerkarte "Erweitert" auf der Seite "SSL" verfügbar. Sie müssen WebLogic Server neu starten, um diese Änderung zu aktivieren.

20. Aktivieren Sie die sichere Replikation für den Server:
  - a. Blenden Sie im linken Fenster der Konsole **Umgebung** ein, und klicken Sie auf **Cluster**.
  - b. Klicken Sie unter "Zusammenfassung der Cluster" auf den Namen des Servers, z.B. `Foundation Services`, für den die sichere Replikation aktiviert werden soll.  
  
Für den ausgewählten Server wird die Registerkarte "Konfiguration" im Fenster "Einstellungen" angezeigt.
  - c. Klicken Sie auf **Replikation**, um die Registerkarte "Replikation" zu öffnen.
  - d. Wählen Sie **Sichere Replikation aktiviert** aus. Sie müssen möglicherweise auf **Sperren und bearbeiten** klicken, um diese Option auswählen zu können.
  - e. Klicken Sie auf **Speichern**.
21. Führen Sie die Schritte 6 bis 20 für jeden verwalteten Server aus, der zu diesem Host gehört.
22. Aktivieren Sie die sichere Replikation, um einen Kanal für Replikationsaufrufe für das Cluster bereitzustellen.  
  
Ausführliche Informationen finden Sie im Oracle MetaLink-Dokument 1319381.1.
  - Blenden Sie in der Administrationskonsole **Umgebung** ein, und wählen Sie **Cluster** aus.
  - Wählen Sie **Replikation** aus.
  - Aktivieren Sie unter **Replikation** die Option **Sichere Replikation aktiviert**.
  - Klicken Sie auf **Speichern**.
23. Klicken Sie im **Change Center** auf **Änderungen aktivieren**.

## HFM-Serververbindung mit SSL-fähiger Oracle-Datenbank aktivieren

Die Netzwerkverbindung zwischen der HFM-Datenquelle und der Oracle-Datenbank kann mit SSL verschlüsselt werden. Damit dies funktioniert, muss das Oracle-Wallet wie in der [Oracle-Dokumentation](#) beschrieben konfiguriert sein. Der TNS-Listener muss auch so konfiguriert sein, dass er auf einen neuen Port für SSL-verschlüsselte Verbindungen horcht. Zum Schluss müssen die entsprechenden Zertifikate in den Keystore und Truststore auf den Servern geladen werden, die die HFM-Datenquelle hosten. Die Anweisungen unten stammen aus der [Dokumentation zur Oracle-Datenbank](#).

## Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie mit den nachfolgenden Schritten fortfahren:

- Ein funktionierender Datenbankserver.
- Stellen Sie sicher, dass keine lokalen Firewalls oder Netzwerkfirewalls die Kommunikation mit dem Server auf dem Port blockieren, auf dem der SSL-fähige TNS-Listener ausgeführt wird.

Im Beispiel unten wurde die Version Oracle 12c (12.1.0.2) verwendet, die auf MS Windows Server 2016 läuft. Diese Anweisungen funktionieren auch bei einer Linux-Installation, vorausgesetzt, die angegebenen Pfade für die Wallet-Dateien sind Linux-Dateisystempfade und die Umgebungsvariablensubstitutionen wurden ordnungsgemäß für die Shell geändert, die auf dem Datenbankserver verwendet wird. Die gleichen Anweisungen wurden erfolgreich in einer 19c-Entwicklung und für Supportinstanzen verwendet.

In den Beispielen in diesem Artikel werden selbstsignierte Zertifikate verwendet. Wenn Sie möchten, können Sie aber auch richtige Certificate Authority-Zertifikate verwenden. Informationen zu den genauen Schritten zum Installieren eines Zertifikats von einer Certificate Authority finden Sie in der [Dokumentation zur Oracle-Datenbank](#).

## Oracle-Datenbank konfigurieren

Befolgen Sie zum Konfigurieren der Oracle-Datenbank die nachfolgenden Schritte:

1. Erstellen Sie ein neues Wallet für die automatische Anmeldung auf dem Datenbankserver.

### Hinweis:

Diese Schritte müssen nur ausgeführt werden, wenn zuvor kein Oracle-Wallet erstellt wurde. Die folgenden Schritte müssen nicht ausgeführt werden, wenn das GUI-Tool des Oracle-Wallet auf dem Datenbankserver verwendet wird.

```
C:\> cd %ORACLE_HOME%
C:\oracledb\12.1.0\home> mkdir wallet
C:\oracledb\12.1.0\home> orapki wallet create -wallet wallet -pwd
password1 -auto_login
```

Sie können alle Meldungen ignorieren, in denen Sie aufgefordert werden, den Befehl `-auto_login_local` in der `orapki`-Befehlszeile zu verwenden. Wenn ein SSL-Authentifizierungsfehler auftritt, finden Sie Informationen zum Troubleshooting unter [Dokument-ID 2238096.1](#).

Prüfen Sie außerdem die Sicherheitsberechtigung der Datei `cwallet.sso` (im Wallet-Verzeichnis), und stellen Sie sicher, dass der Servicebenutzer des Oracle-Listeners Leseberechtigung für diese Datei hat. Ohne Leseberechtigung ist der SSL-Handshake später nicht erfolgreich. Dies tritt auf, wenn die Oracle-Datenbank mit dem vorgeschlagenen Oracle-Benutzer installiert wurde, der sich nicht

anmelden darf. Wenn die Oracle-Datenbank mit dem Oracle-Benutzer installiert wurde, muss der TNS-Listener als anderer Benutzer ausgeführt werden.

**2. Selbstsigniertes Zertifikat erstellen und in das Wallet laden**

```
C:\oracledb\12.1.0\home> orapki wallet add -wallet wallet -pwd password1 -
dn "CN={FQDN of db server}" -
keysize 1024 -self_signed -validity 3650
```

Das Kennwort `password1` im Beispiel oben muss mit dem in *Schritt 1* angegebenen Kennwort übereinstimmen.

**3. Neu erstelltes selbstsigniertes Zertifikat exportieren**

```
C:\oracledb\12.1.0\home> orapki wallet export -wallet wallet -pwd
password1 -dn "CN={FQDN of db server}"
-cert %COMPUTERNAME%-certificate.crt
```

**4. Kopieren Sie die exportierte Base64-Zertifikatsdatei auf die HFM-Server.**

**5. SQL\*NET und die TNS-Listener konfigurieren:**

**a.** Suchen Sie einen nicht verwendeten Port auf dem Datenbankserver. Im Beispiel unten wird der neue Listener auf Port 1522 erstellt. In der Regel wird für SSL-Verbindungen der Port 2484 verwendet. Sie können aber einen beliebigen verfügbaren Port verwenden. Sie müssen prüfen, ob der zu verwendende Port auf dem Datenbankserver verfügbar ist, bevor Sie fortfahren und die gewünschten Änderungen vornehmen.

**b.** Aktualisieren Sie `SQLNET.ORA`. Das `DIRECTORY`-Element der `WALLET_LOCATION`-Deklaration muss auf das oben in *Schritt 1* erstellte Wallet verweisen.

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS, NTS, BEQ)
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
WALLET_LOCATION=
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = C:\oracledb\12.1.0\home\wallet)
)
)
SSL_CLIENT_AUTHENTICATION = FALSE
```

**c.** Aktualisieren Sie `LISTENER.ORA`, um einen neuen Listener zu definieren. Verwenden Sie den oben in *Schritt 5a* angegebenen Port.

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\oracledb\12.1.0\home)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\oracledb\12.1.0\home\bin\oraclr12.dll")
)
)
SSL_CLIENT_AUTHENTICATION = FALSE
```

```

WALLET_LOCATION=
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = C:\oracledb\12.1.0\home\wallet)
)
)
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = myServer) (PORT = 1521))
)
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCPS) (HOST = myServer) (PORT = 1522))
)
(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
)
)
ADR_BASE_LISTENER = C:\oracledb

```

- d. Erstellen Sie in der Datei TNSNAMES.ORA einen neuen Eintrag für den neuen Port.**

```

ORCL_SSL =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCPS) (HOST = myServer) (PORT = 1522))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = myServer_service)
)
)

```

Sie müssen denselben Port angeben, der oben in *Schritt 5a* angegeben und in *Schritt 5c* verwendet wurde.

- e. Starten Sie den TNS-Listener neu.**

```

C:\oracledb\12.1.0\home>lsnrctl stop
C:\oracledb\12.1.0\home>lsnrctl start

```

- f. Prüfen Sie, ob der neue TNS-Listener funktioniert.**

```

C:\oracledb\12.1.0\home>ttnsping orcl_ssl
TNS Ping Utility for 64-bit Windows: Version 12.1.0.2.0 -
Production on 10-SEP-2019 15:43:22
Copyright (c) 1997, 2014, Oracle. All rights reserved.
Used parameter files:
C:\oracledb\12.1.0\home\network\admin\sqlnet.ora
Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)
(HOST = myServer)
(PORT = 1522)) (CONNECT_DATA = (SERVER = DEDICATED)

```

```
(SERVICE_NAME = myServer_service)))  
OK (130 msec)
```

## HFM-Server für die Verwendung von SSL-Datenbankverbindungen konfigurieren

### Zertifikate der Datenbank zum Truststore auf HFM-Servern hinzufügen

Die folgenden Schritte müssen auf jedem einzelnen EPM-Server ausgeführt werden, auf dem die HFM-Datenquelle ausgeführt wird. Die unten verwendete Umgebungsvariable `%MW_HOME%` steht für den Speicherort der Oracle Middleware-Installation. Diese Umgebungsvariable wird bei der EPM-Installation nicht standardmäßig erstellt. Sie wird hier verwendet, um das übergeordnete Verzeichnis der EPM-Installation anzuzeigen.

Der Speicherort der EPM-Installation wird durch die Umgebungsvariable `EMP_ORACLE_HOME` angegeben. Im Beispiel unten werden Keystore und Truststore in dasselbe Verzeichnis gestellt wie die EPM-Installation. Die Keystore- und Truststore-Dateien können sich an einer beliebigen Stelle des HFM-Serverdateisystems befinden.

1. Erstellen Sie ein neues Verzeichnis unter `%MW_HOME%`, in dem der Java-Keystore und der PKCS12-Truststore gespeichert werden.
  - a. `cd %MW_HOME%`
  - b. `mkdir certs`
2. Kopieren Sie die Java-Keystore-Datei "cacerts" aus dem JDK.
  - a. `cd %MW_HOME%\certs`
  - b. `copy %MW_HOME%\jdk1.8.0_181\jre\lib\security\cacerts testing_cacerts`  
Der JDK-Keystore muss kopiert und anstelle des JDK-Standard-Keystores verwendet werden, weil die in den Standard-Keystore eingefügten Schlüssel und Zertifikate verloren gehen, wenn das JDK upgegradet und das vorherige JDK gelöscht wird.
3. Kopieren Sie das Base64-Zertifikat nach `%MW_HOME%\certs`.
4. Importieren Sie das Zertifikat in die Java-Keystore-Datei `testing_cacerts`.
  - a. **Beispiel:** `keytool -importcert -file bur00cbb-certificate.crt -keystore testing_cacerts -alias "myserver"`
    - i. Sie müssen das Kennwort für den Keystore angeben.
    - ii. Sie müssen "myserver" durch die vollqualifizierte Domain des Datenbankservers ersetzen.
  - b. Wenn Sie gefragt werden, ob das Zertifikat vertrauenswürdig ist, geben Sie `j` an.
5. Erstellen Sie den Truststore im PKCS12-Format aus der Java-Keystore-Datei von JDK.  
Beispiel:

```
keytool -importkeystore -srckeystore testing_cacerts -srcstoretype JKS -  
deststoretype PKCS12 -destkeystore testing_cacerts.pfx
```

### HFM-JDBC-Verbindungen für die Verwendung von SSL aktualisieren

1. Konfigurieren Sie die JDBC-Verbindung für die HFM-Datenbank neu, um SSL zu verwenden.
  - a. Starten Sie das EPM-Konfigurationstool.

- i. Wählen Sie die Knoten **Datenbank konfigurieren** und **Auf Anwendungsserver bereitstellen** unter dem **Financial Management**-Knoten aus.
      - ii. Klicken Sie auf **Weiter**.
      - iii. Führen Sie jeden der folgenden Schritte für die HFM-JDBC-Verbindung aus.
        - i. Geben Sie den SSL-Port, den Servicenamen, den Benutzernamen und das Kennwort in den zugehörigen Spalten ein.
        - ii. Klicken Sie auf **(+)**, um die erweiterten Datenbankoptionen zu öffnen.
        - iii. Aktivieren Sie das Kontrollkästchen **Sichere Verbindungen verwenden**.
        - iv. Geben Sie den Speicherort des in *Schritt 2* erstellten Java-Keystores ein.
        - v. Klicken Sie auf **Anwenden**.
        - vi. Klicken Sie auf **(+)**, um die erweiterten Datenbankoptionen zu öffnen.
        - vii. Klicken Sie auf **JDBC-URL bearbeiten und geänderte Version verwenden**. Beachten Sie, dass an der angezeigten JDBC-URL keine Änderungen vorgenommen werden dürfen.
        - viii. Klicken Sie auf **Anwenden**.
        - ix. Klicken Sie auf **Weiter**.
    - b. Führen Sie die restlichen Schritte aus, um die HFM-Anwendung bereitzustellen, wie in der EPM-Dokumentation beschrieben.
  2. Öffnen Sie ein Befehlsfenster oder eine Shell, um die EPM-Registry so zu aktualisieren, dass SSL für die von der Datenquelle verwendete ODBC-Verbindung aktiviert werden kann.  
Führen Sie alle unten aufgeführten Befehle aus:

```
epmsys_registry.bat addproperty FINANCIAL_MANAGEMENT_PRODUCT/  
DATABASE_CONN/@ODBC_TRUSTSTORE "C:  
\Oracle\Middleware\certs\testing_cacerts.pfx"  
epmsys_registry.bat addencryptedproperty  
FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN  
/@ODBC_TRUSTSTOREPASSWORD <truststorepassword>  
epmsys_registry.bat addproperty FINANCIAL_MANAGEMENT_PRODUCT/  
DATABASE_CONN  
/@ODBC_VALIDATESERVERCERTIFICATE false
```

In den obigen Beispielen ist der Pfad `C:\Oracle\Middleware` der Wert von `%MW_HOME%` in den Schritten 1, 2 und 3.

Die Eigenschaft `FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_VALIDATESERVERCERTIFICATE` darf nur auf `"False"` gesetzt werden, wenn ein selbstsigniertes Zertifikat verwendet wird. Der Wert von `FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_TRUSTSTOREPASSWORD` muss das Kennwort des ursprünglichen, in *Schritt 2* kopierten Java-Keystores sein.

### Von HFM verwendete TNS-Namenseinträge aktualisieren

Bearbeiten Sie `TNSNAMES.ORA`, um einen neuen Eintrag zu erstellen, und benennen Sie den alten Eintrag um. Das folgende Beispiel zeigt eine aktualisierte `TNSNAMES.ORA`-Datei auf dem HFM-Server, bei der die erforderlichen Änderungen angewendet wurden. Grund für diese Änderungen ist, dass HFM den TNS-Namenseintrag `HFMTNS` sucht und verwendet. In diesem Eintrag müssen das Protokoll und der Port geändert werden, damit `XFMDataSource` ordnungsgemäß funktioniert.

```
HFMTNS_UNENC =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP) (HOST = myserver) (PORT = 1521))
)
(CONNECT_DATA =
(SERVICE_NAME = myserver_service)
(SERVER = DEDICATED)
)
)
HFMTNS =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS) (HOST = myserver) (PORT = 1522))
)
(CONNECT_DATA =
(SERVICE_NAME = myserver_service)
(SERVER = DEDICATED)
)
)
```

Der ursprüngliche `HFMTNS`-Eintrag wurde in `HFMTNS_UNENC` umbenannt. Der neue `HFMTNS`-Eintrag wurde erstellt, indem der Eintrag `HFMTNS_UNENC` kopiert und in `HFMTNS` umbenannt wurde. Anschließend wurde das Protokoll in `TCPS` aktualisiert und der Port in `1522` geändert. Der angegebene Port muss mit dem in der Datei `TNS LISTENER.ORA` angegebenen Port übereinstimmen.

## Verfahren für Oracle HTTP Server

### Wallets erstellen und Zertifikate für Oracle HTTP Server installieren

Ein Standard-Wallet wird automatisch mit Oracle HTTP Server installiert. Sie müssen ein echtes Wallet für jeden Oracle HTTP Server in Ihrem Deployment konfigurieren.

**Hinweis:** Ab Version 11.2.x ist der Oracle-Wallet-Manager nicht auf Oracle HTTP Server installiert. Der Oracle-Wallet-Manager wird nur installiert, wenn Sie Oracle Database Client installieren. Sie müssen den in Database Client verfügbaren Wallet-Manager verwenden, um das Wallet zu erstellen und das Zertifikat zu importieren. Wenn Sie Oracle HTTP Server für SSL konfigurieren, stellen Sie sicher, dass Sie immer auch den Oracle Database-Client (64-Bit) installieren, wenn Sie Ihre EPM System-Produkte installieren.

So erstellen und installieren Sie Oracle HTTP Server-Zertifikate:

1. Starten Sie Wallet Manager auf jedem Hostcomputer von Oracle HTTP Server.

Wählen Sie **Start, Alle Programme, Oracle-OHxxxxxx, Integrated Management Tools, Wallet Manager** aus.

xxxxxx ist die Oracle HTTP Server-Instanznummer.

2. Erstellen Sie ein neues, leeres Wallet.
  - a. Wählen Sie in Oracle Wallet Manager die Optionen **Wallet, Neu** aus.
  - b. Klicken Sie auf **Ja**, um ein Wallet-Standardverzeichnis zu erstellen, oder auf **Nein**, um die Wallet-Datei an einem Speicherort Ihrer Wahl zu erstellen.
  - c. Geben Sie im Fenster "Neues Wallet" unter **Wallet-Kennwort** und **Kennwort bestätigen** das gewünschte Kennwort ein.
  - d. Klicken Sie auf **OK**.
  - e. Klicken Sie im Bestätigungsdiaologfeld auf **Nein**.
3. **Optional:** Wenn Sie keine CA verwenden, die Oracle HTTP Server bekannt ist, importieren Sie das CA-Stammzertifikat in das Wallet.
  - a. Klicken Sie in Oracle Wallet Manager mit der rechten Maustaste auf **Vertrauenswürdige Zertifikate**, und wählen Sie **Vertrauenswürdiges Zertifikat importieren** aus.
  - b. Suchen Sie nach dem CA-Stammzertifikat, und wählen Sie es aus.
  - c. Wählen Sie **Öffnen** aus.
4. Erstellen Sie eine Zertifikatsanforderung.
  - a. Klicken Sie in Oracle Wallet Manager mit der rechten Maustaste auf **Zertifikat: [Leer]**, und wählen Sie **Zertifikatsanforderung hinzufügen** aus.
  - b. Geben Sie unter "Zertifikatsanforderung erstellen" die erforderlichen Informationen ein.

Geben Sie für den allgemeinen Namen den vollqualifizierten Serveralias ein, z.B. `epm.myCompany.com` oder `epminternal.myCompany.com`. Dieser Alias ist in der Datei `hosts` auf Ihrem System verfügbar.
  - c. Klicken Sie auf **OK**.
  - d. Klicken Sie im Bestätigungsdiaologfeld auf **OK**.
  - e. Klicken Sie mit der rechten Maustaste auf die erstellte Zertifikatsanforderung, und wählen Sie **Zertifikatsanforderung exportieren** aus.
  - f. Geben Sie einen Namen für die Zertifikatsanforderungsdatei an.
5. Fordern Sie mit den Zertifikatsanforderungsdateien signierte Zertifikate von der CA an.
6. Importieren Sie signierte Zertifikate.
  - a. Klicken Sie in Oracle Wallet Manager mit der rechten Maustaste auf die Zertifikatsanforderung, mit der das signierte Zertifikat angefordert wurde, und wählen Sie **Benutzerzertifikat importieren** aus.
  - b. Klicken Sie unter "Zertifikat importieren" auf **OK**, um das Zertifikat aus einer Datei zu importieren.
  - c. Wählen Sie unter "Zertifikat importieren" die Zertifikatsdatei aus, und klicken Sie auf **Öffnen**.



7. Speichern Sie das Wallet in einem geeigneten Verzeichnis, z.B. `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`.
8. Wählen Sie **Wallet, Automatische Anmeldung** aus, um die automatische Anmeldung zu aktivieren.

### Oracle Wallet mit ORAPKI (in Linux) einrichten

Führen Sie die folgenden Schritte aus, um Oracle Wallet mit der ORAPKI-Befehlszeile einzurichten:

1. Erstellen Sie einen Ordner für Ihr Wallet:

```
$ mkdir /MIDDLEWARE_HOME/oracle_common/wallet
```

2. Fügen Sie Ihrem Pfad den Speicherort des orapki-Utilitys hinzu:

```
$ export PATH=$PATH:$MIDDLEWARE_HOME/oracle_common/bin
```

3. Erstellen Sie ein Wallet für Ihr Zertifikat:

```
>$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet create -wallet  
[wallet_location] -auto_login
```

Mit diesem Befehl werden Sie aufgefordert, ein Wallet-Kennwort einzugeben und das Kennwort zu bestätigen, wenn in der Befehlszeile kein Kennwort angegeben wurde. Dadurch wird ein Wallet in dem für `-wallet` angegebenen Speicherort erstellt.

4. Generieren Sie einen Certificate Signing Request (CSR), und fügen Sie ihn Ihrem Wallet hinzu:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -dn 'CN=<CommonName>,OU=<OrganizationUnit>,  
O=<Company>, L=<Location>, ST=<State>, C=<Country>' -keysize 512|1024|  
2048|4096 -pwd [Wallet_Password]
```

5. Fügen Sie das Stamm- und das Zwischenzertifikat dem vertrauenswürdigen Keystore hinzu

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -trusted_cert -cert [certificate_location] [-pwd]
```

6. Verwenden Sie Ihre Zertifizierungsstelle, um den Certificate Signing Request (CSR) zu signieren. So exportieren Sie Zertifikatsanforderungen aus Oracle-Wallets:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet export -wallet  
[wallet_location] -dn 'CN=<CommonName>,OU=<OrganizationUnit>,  
O=<Company>, L=<Location>, ST=<State>, C=<Country>' -request  
[certificate_request_filename] [-pwd]
```

7. Importieren Sie den unterschriebenen Certificate Signing Request in Ihr Wallet:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -user_cert -cert [certificate_location] [-pwd]
```

8. So zeigen Sie die Inhalte von Wallets an:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet display -wallet  
[wallet_location] [-pwd]
```

### SSL-Aktivierung für Oracle HTTP Server

Nachdem Sie den Webserver auf jedem Hostcomputer von Oracle HTTP Server neu konfiguriert haben, aktualisieren die die Oracle HTTP Server-Konfigurationsdatei, indem Sie den Speicherort des Standard-Wallets durch den Speicherort des von Ihnen erstellten Wallets ersetzen.

So konfigurieren Sie Oracle HTTP Server für SSL:

1. Konfigurieren Sie den Webserver auf jedem Oracle HTTP Server-Hostcomputer in Ihrem Deployment neu.
2. Starten Sie EPM System Configurator für die Instanz.
3. Führen Sie im Fenster zur Auswahl der Konfigurationsaufgaben die folgenden Schritte aus, und klicken Sie anschließend auf **Weiter**.
  - a. Heben Sie die Auswahl von **Alle deaktivieren** aus.
  - b. Blenden Sie die Aufgabengruppe **Hyperion Foundation** ein, und wählen Sie **Webserver konfigurieren** aus.
4. Klicken Sie unter **Webserver konfigurieren** auf **Weiter**.
5. Klicken Sie unter **Bestätigung** auf **Weiter**.
6. Klicken Sie unter **Zusammenfassung** auf **Fertig stellen**.
7. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf` mit einem Texteditor.
8. Stellen Sie sicher, dass der von Ihnen verwendete SSL-Port unter OHS Listen port aufgeführt ist. Beispiel:  
  
Wenn Sie 19443 als SSL-Kommunikationsport verwenden, sollten Ihre Einträge wie folgt aussehen:  
  
Listen 19443
9. Setzen Sie den Wert des Parameters `SSLSessionCache` auf `none`.
10. Aktualisieren Sie die Konfigurationseinstellungen für jeden Oracle HTTP Server in Ihrem Deployment.
  - a. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig//ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf` mit einem Texteditor.
  - b. Suchen Sie die Anweisung `SSLWallet`, und ändern Sie den zugehörigen Wert so, dass er auf das Wallet verweist, in dem Sie das Zertifikat installiert haben. Wenn Sie das Wallet in `EPM_ORACLE_INSTANCEhttpConfig/ohs/`

config/OHS/ohs\_component/keystores/epmsystem erstellt haben, kann die Anweisung SSLWallet wie folgt aussehen:

```
SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/epmsystem"
```

- c. Speichern und schließen Sie die Datei `ssl.conf`.
- 11. Aktualisieren Sie die Datei `mod_wl_ohs.conf` auf jedem Oracle HTTP Server in Ihrem Deployment.
  - a. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf` mit einem Texteditor.
  - b. Stellen Sie sicher, dass die Anweisung `WLSSLWallet` auf das Oracle-Wallet verweist, in dem das SSL-Zertifikat gespeichert ist.

```
WLSSLWallet MIDDLEWARE_HOME/ohs/bin/wallets/myWallet
```

Beispiel: `C:/Oracle/Middleware/ohs/bin/wallets/myWallet`

- c. Setzen Sie den Wert der Anweisung `SecureProxy` auf `ON`.

```
SecureProxy ON
```

- d. Stellen Sie sicher, dass die `LocationMatch`-Definitionen für bereitgestellte Oracle Enterprise Performance Management System-Komponenten dem folgenden Oracle Hyperion Shared Services-Beispiel ähneln. Hier wird ein Oracle WebLogic Server-Cluster angenommen (auf `myserver1` und `myserver2` mit SSL-Port 28443):

```
<LocationMatch /interop/>
  SetHandler weblogic-handler
  pathTrim /
  WeblogicCluster myServer1:28443,myServer2:28443
  WLProxySSL ON
</LocationMatch>
```

- e. Speichern und schließen Sie die Datei `mod_wl_ohs.conf`.

## Auf WebLogic Server bereitgestellte EPM System-Webkomponenten konfigurieren

Nach dem Deployment von Oracle Enterprise Performance Management System-Webkomponenten müssen Sie sie für die SSL-Kommunikation konfigurieren.

So konfigurieren Sie die Webkomponenten für SSL:

1. Starten Sie Oracle WebLogic Server, indem Sie eine Datei unter `EPM_ORACLE_INSTANCE/domains/EPMSystem/bin/startWebLogic.cmd` starten:
2. Starten Sie die WebLogic Server-Administrationskonsole, indem Sie die folgende URL aufrufen:

```
http://SERVER_NAME:Port/console
```

Beispiel: Um auf die WebLogic Server-Konsole zuzugreifen, die über den Standardport auf `myServer` bereitgestellt ist, verwenden Sie `http://myServer:7001/console`.

3. Geben Sie auf dem Begrüßungsbildschirm den Benutzernamen und das Kennwort für den Zugriff auf `EPMSystem` ein. Der Benutzername und das Kennwort werden während der Konfiguration in EPM System Configurator angegeben.
4. Klicken Sie im **Change Center** auf **Sperren und bearbeiten**.
5. Blenden Sie im linken Fenster der Konsole **Umgebung** ein, und wählen Sie **Server** aus.
6. Klicken Sie im Fenster "Zusammenfassung der Server" auf den Namen des Servers, für den Sie SSL aktivieren möchten.

Beispiel: Wenn Sie alle Oracle Hyperion Foundation Services-Komponenten installiert haben, können Sie SSL für folgende Server aktivieren:

- `CalcManager`
  - `FoundationServices`
7. Deaktivieren Sie **Listening-Port aktiviert**, um den HTTP-Listening-Port zu deaktivieren.
  8. Stellen Sie sicher, dass **SSL-Listening-Port aktiviert** aktiviert ist.
  9. Geben Sie unter **SSL-Listening-Port** den SSL-Listening-Port für WebLogic Server ein.
  10. Geben Sie den zu verwendenden Identity und Trust Keystore an.
    - Wählen Sie **Keystores** aus, um die Registerkarte "Keystores" zu öffnen.
    - Wählen Sie unter **Keystores** eine Option aus:
      - a. Wählen Sie **Keystores** aus, um die Registerkarte "Keystores" zu öffnen.
      - b. Wählen Sie unter **Keystores** eine Option aus:
        - **Benutzerdefinierte Identity und Trust**, wenn Sie kein Serverzertifikat einer bekannten Drittanbieter-CA verwenden
        - **Benutzerdefinierte Identity und Java-Standard-Trust**, wenn Sie ein Serverzertifikat einer bekannten Drittanbieter-CA verwenden
      - c. Geben Sie unter **Benutzerdefinierter Identity Keystore** den Pfad des Keystores ein, in dem das signierte WebLogic Server-Zertifikat installiert ist.
      - d. Geben Sie unter **Benutzerdefinierter Identity Keystore-Typ** den Wert `jks` ein.
      - e. Geben Sie unter **Benutzerdefinierte Identity Keystore-Passphrase** und **Benutzerdefinierte Passphrase des Identity Keystores bestätigen** das Keystore-Kennwort ein.
      - f. Gehen Sie wie folgt vor, wenn Sie unter **Keystores** die Option **Benutzerdefinierte Identity und Trust** ausgewählt haben:
        - Geben Sie unter **Benutzerdefinierter Trust Keystore** den Pfad des benutzerdefinierten Keystores ein, in dem das Stammzertifikat der CA verfügbar ist, die Ihr Serverzertifikat signiert hat.
        - Geben Sie unter **Benutzerdefinierter Trust Keystore-Typ** den Wert `jks` ein.

- Geben Sie unter **Benutzerdefinierte Trust Keystore-Passphrase** und **Benutzerdefinierte Passphrase des Trust Keystores bestätigen** das Keystore-Kennwort ein.
- g.** Klicken Sie auf **Speichern**.
- 11.** Geben Sie SSL-Einstellungen an.
- Wählen Sie **SSL** aus.
  - Geben Sie unter **Private Key-Alias** den Alias ein, den Sie beim Importieren des signierten WebLogic Server-Zertifikats angegeben haben.
  - Geben Sie unter **Private Key-Passphrase** und **Private Key-Passphrase bestätigen** das Kennwort ein, das zum Abrufen des Private Keys verwendet werden soll.
  - **Nur Oracle Hyperion Provider Services-Webanwendung:** Wenn Sie Zertifikate mit Platzhaltern verwenden, um die Kommunikation zwischen WebLogic Server und anderen EPM System-Serverkomponenten zu verschlüsseln, müssen Sie die Hostnamenüberprüfung für die Provider Services-Webanwendung deaktivieren.
    - Wählen Sie **Erweitert** aus.
    - Wählen Sie unter **Hostnamenüberprüfung** die Option **Keine** aus.
  - Klicken Sie auf **Speichern**.
- 12.** Klicken Sie im **Change Center** auf **Änderungen aktivieren**.

## Domainkonfiguration aktualisieren

Bei diesem Prozess wird die Domainkonfiguration aktualisiert. Erstellen Sie ein vollständiges Backup Ihres Deployments, bevor Sie mit dieser Prozedur beginnen. Oracle empfiehlt, diese Prozedur in einem Test-Deployment zu testen, bevor Änderungen an einem Produktions-Deployment vorgenommen werden.

So aktualisieren Sie die Domainkonfiguration:

- 1.** Navigieren Sie zum Verzeichnis `MIDDLEWARE_HOME/oracle_common/bin`:  

```
cd MIDDLEWARE_HOME/oracle_common/bin
```
- 2.** Legen Sie `ORACLE_HOME`, `WL_HOME` und `JAVA_HOME` fest.  

```
set ORACLE_HOME= /Oracle/Middleware
set WL_HOME= /Oracle/Middleware/wlserver
set JAVA_HOME= /Oracle/Middleware/jdk
```
- 3.** Aktivieren Sie in der WebLogic-Konsole den HTTP-Port für den Admin-Server.
- 4.** Verwenden Sie einen Befehl wie den folgenden, um einen Keystore zu erstellen:  

```
libovdconfig.bat -host HOSTNAME -port 7001 -userName USERNAME -domainPath %MWH%\user_projects\domains\EPMSystem -createKeystore
```

Ersetzen Sie in diesem Befehl `HOSTNAME` und `USERNAME` jeweils durch den Hostnamen des WebLogic-Servers und den Benutzernamen des Administrators. Stellen Sie sicher, dass in der Ausgabe die erfolgreiche Erstellung des OVD-Keystores gemeldet wird.

- 5.** Exportieren Sie das SSL-Zertifikat von AdminServer.

 **Note:**

Dieser Schritt gilt nur für das eingebettete LDAP (Standardauthentikator). Für andere LDAPs muss das Zertifikat mit den entsprechenden LDAP-spezifischen Befehlen exportiert werden. Das Zertifikatsdateiformat muss **Base 64 Encoded x.509** lauten.

- a. Greifen Sie über Internet Explorer auf die WebLogic-Administrationskonsole zu, indem Sie eine Verbindung zu `https://HOSTNAME:7002/console` herstellen.
  - b. Klicken Sie auf **Zertifikat anzeigen, Details**, und wählen Sie **Kopieren in Datei** aus, um das SSL-Zertifikat zu exportieren.
  - c. Speichern Sie das Zertifikat als Zertifikatsdatei vom Typ **Base 64 Encoded x.509** in einem lokalen Verzeichnis. Beispiel: `C:\certificate\slc17rby.cer`.
  - d. Verschieben Sie das Zertifikat auf den Server.
6. Verwenden Sie Keytool, um das in Schritt 4 erstellte Zertifikat in den Keystore zu importieren. Verwenden Sie Befehle wie die folgenden (es wird angenommen, dass sich `JAVA_HOME` und die ausführbare Keytool-Datei im Pfad befinden):

```
export PATH=$JAVA_HOME/bin:$PATH
```

```
keytool -importcert -keystore
DOMAIN_HOME\config\fmwconfig\ovd\default\keystores/adapters.jks -
storepass PASSWORD -alias wcp_ssl -file CERTIFICATE_PATH -noprompt.
```

**Beispiel:**

```
keytool -importcert -keystore %MWH%
\user_projects\domains\EPMSysystem\config\fmwconfig\ovd\default\keystore
s/adapters.jks -storepass examplePWD -alias wcp_ssl -file
C:\certificate\slc17rby.cer -noprompt
```

 **Note:**

- Das in diesem Befehl verwendete Kennwort muss dem Kennwort entsprechen, das beim Generieren des Keystores in Schritt 4 verwendet wurde.
- `CERTIFICATE_PATH` ist das Verzeichnis und der Name des Zertifikats.
- Alias kann ein beliebiger Alias Ihrer Wahl sein.

Bei einem erfolgreichen Import des Zertifikats wird in Keytool die Meldung `Certificate was added to keystore` (Zertifikat wurde Keystore hinzugefügt) angezeigt.

7. Aktivieren Sie in der WebLogic-Konsole zusätzlich zum HTTP-Port auch den SSL-Port für den Admin-Server.
8. Starten Sie den WebLogic-Admin-Server und Managed Server neu.

9. Melden Sie sich über eine sichere Verbindung bei Oracle Hyperion Enterprise Performance Management Workspace an, um sicherzustellen, dass alles funktioniert.

## Server und EPM System neu starten

Starten Sie alle Server im Deployment neu, und starten Sie dann Oracle Enterprise Performance Management System auf jedem Server.

## Deployments testen

Stellen Sie nach Abschluss des SSL-Deployments sicher, dass alles funktioniert.

So testen Sie Deployments:

1. Rufen Sie über einen Browser die sichere Oracle Hyperion Enterprise Performance Management Workspace-URL auf:

Wenn Sie `epm.myCompany.com` als Serveralias für die externe Kommunikation und 4443 als SSL-Port verwendet haben, lautet die EPM Workspace-URL:

```
https://epm.myCompany.com:4443/workspace/index.jsp
```

2. Geben Sie im Anmeldefenster einen Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Prüfen Sie, ob ein sicherer Zugriff auf die bereitgestellten Oracle Enterprise Performance Management System-Komponenten möglich ist.

## Externe Benutzerverzeichnisse mit SSL-Aktivierung konfigurieren

### Annahmen

- Für die externen Benutzerverzeichnisse, die Sie in Oracle Hyperion Shared Services Console konfigurieren möchten, ist SSL aktiviert.
- Wenn Sie kein Zertifikat einer bekannten Drittanbieter-CA verwendet haben, um SSL für das Benutzerverzeichnis zu aktivieren, verfügen Sie über eine Kopie des Stammzertifikats der CA, die das Serverzertifikat signiert hat.

### CA-Stammzertifikate importieren

Wenn Sie kein Zertifikat einer bekannten Drittanbieter-CA verwendet haben, um SSL für das Benutzerverzeichnis zu aktivieren, müssen Sie das Stammzertifikat der CA, die das Serverzertifikat signiert hat, in die folgenden Keystores importieren:

#### Hinweis:

Während des Anwendungs-Deployments fügt WebLogic die Anweisung - `Djavax.net.ssl.trustStore`, die auf `DemoTrust.jks` verweist, zur Datei `setDomainEnv.sh` oder `setDomainEnv.cmd` hinzu. Entfernen Sie - `Djavax.net.ssl.trustStore` aus der Datei `setDomainEnv.sh` oder `setDomainEnv.cmd`, wenn Sie das WebLogic-Standardzertifikat nicht verwenden.

Verwenden Sie ein Tool wie keytool, um das CA-Stammzertifikat zu importieren.

- Alle Oracle Enterprise Performance Management System-Server:  
**JVM-Keystore:** `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`
- Der Keystore, der von JVM auf dem Hostcomputer der einzelnen EPM System-Komponenten verwendet wird. Standardmäßig verwenden EPM System-Komponenten den folgenden Keystore:

`MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`

### Externe Benutzerverzeichnisse konfigurieren

Sie konfigurieren Benutzerverzeichnisse mit Shared Services Console. Bei der Konfiguration von Benutzerverzeichnissen müssen Sie die Option `SSL Enabled` (SSL aktiviert) auswählen. Damit wird die EPM System-Sicherheit angewiesen, das sichere Protokoll für die Kommunikation mit dem Benutzerverzeichnis zu verwenden. Sie können SSL für eine Verbindung zwischen der EPM System-Sicherheit und LDAP-fähigen Benutzerverzeichnissen aktivieren, wie z.B. Oracle Internet Directory und Microsoft Active Directory.

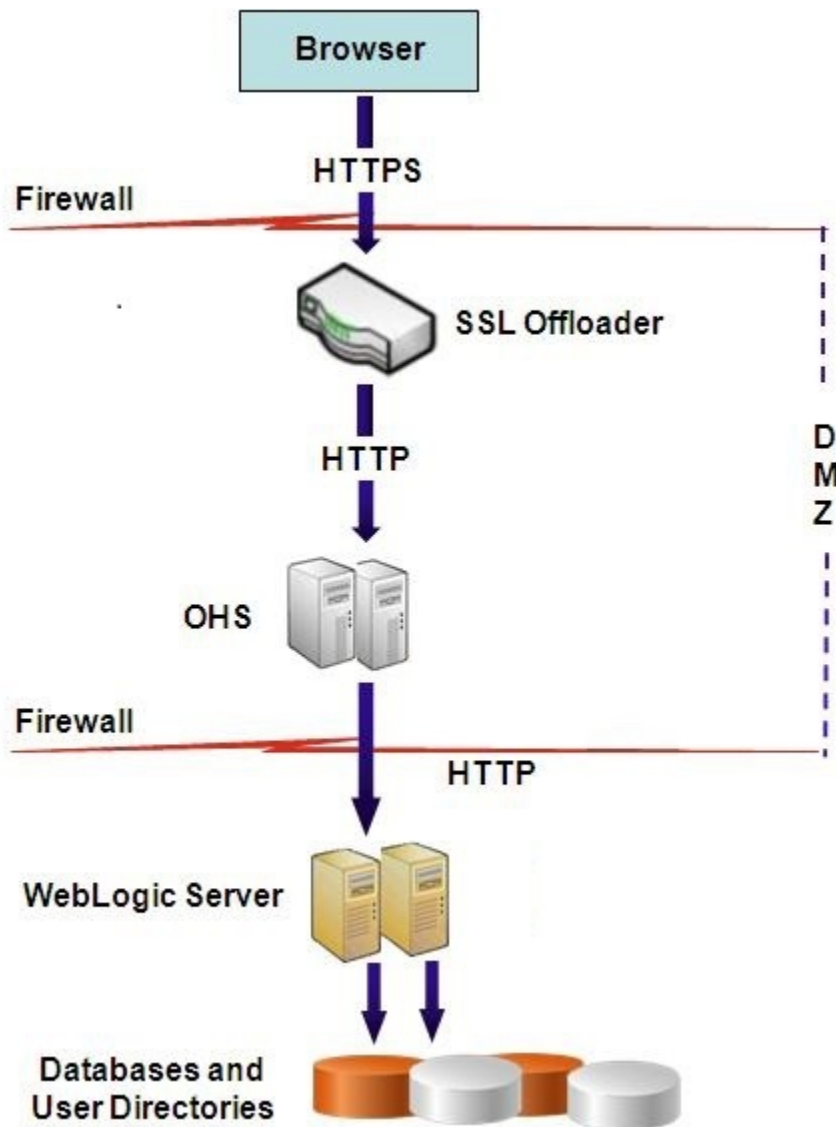
Informationen hierzu finden Sie unter "Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

## SSL auf dem Webserver beenden

### Deployment-Architektur

In diesem Szenario wird SSL verwendet, um den Kommunikationslink zwischen Oracle Enterprise Performance Management System-Clients (z.B. einem Browser) und Oracle HTTP Server zu sichern. Im Folgenden wird das Konzept veranschaulicht:





### Annahmen

Diese Konfiguration verwendet zwei Serveraliasnamen auf dem Webserver, z.B. `epm.myCompany.com` und `empinternal.myCompany.com`. Ein Serveralias dient zur externen Kommunikation zwischen dem Webserver und Browsern und der andere zur internen Kommunikation zwischen EPM System-Servern. Stellen Sie sicher, dass die Serveraliasnamen auf die IP-Adresse des Computers verweisen und über DNS aufgelöst werden können.

Ein signiertes Zertifikat zur Unterstützung der externen Kommunikation zwischen Browsern (z.B. über `epm.myCompany.com`) muss auf dem Webserver installiert sein (auf dem der virtuelle Host definiert ist, der die sichere externe Kommunikation unterstützt). Dieser virtuelle Host muss SSL beenden und HTTP-Anforderungen an Oracle HTTP Server weiterleiten.

Wenn SSL auf Oracle HTTP Server (OHS) oder auf dem Load Balancer beendet wird, müssen Sie wie folgt vorgehen:

- Legen Sie für jede logische Webanwendung den virtuellen Nicht-SSL-Host von Load Balancer oder Oracle HTTP Server fest (z.B. `empinternal.myCompany.com:80`, wobei

"80" der Nicht-SSL-Port ist). Öffnen Sie das Fenster "Konfiguration", und führen Sie die folgenden Schritte aus:

1. Blenden Sie die Konfigurationsaufgabe **Hyperion Foundation** ein.
  2. Wählen Sie **Logische Adresse für Webanwendungen konfigurieren** aus.
  3. Geben Sie *Hostname*, Nicht-SSL-Portnummer und SSL-Portnummer an.
- Legen Sie als externe URL den virtuellen SSL-Host von Load Balancer oder Oracle HTTP Server fest (z.B. `empexternal.myCompany.com:443`, wobei "443" der SSL-Port ist). Öffnen Sie das Fenster "Konfiguration", und führen Sie die folgenden Schritte aus:
    1. Blenden Sie die Konfigurationsaufgabe **Hyperion Foundation** ein.
    2. Wählen Sie **Gemeinsame Einstellungen konfigurieren** aus.
    3. Wählen Sie unter "Externe URL-Details" die Option **SSL-Offload aktivieren** aus.
    4. Geben Sie einen Wert für *Externer URL-Host* und *Externer URL-Port* an.

 **Hinweis:**

Wenn Sie **configtool** verwenden, um Webanwendungen erneut bereitzustellen oder den Webserver neu zu konfigurieren, werden die Einstellungen für die logische Webanwendung und für externe URLs ersetzt.

### EPM System konfigurieren

Das Standard-Deployment von EPM System-Komponenten unterstützt die SSL-Beendigung auf dem Webserver. Es ist keine weitere Aktion erforderlich.

Stellen Sie bei der Konfiguration von EPM System sicher, dass die logischen Webanwendungen auf den virtuellen Host (z.B. `empinternal.myCompany.com`) verweisen, der für die interne Kommunikation erstellt wurde. Anweisungen zum Installieren und Konfigurieren von EPM System finden Sie in den folgenden Informationsquellen:

- *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*
- *Oracle Enterprise Performance Management System - Installation: Beginnen Sie hier*

### Deployments testen

Prüfen Sie nach dem Abschluss des Deployment-Prozesses, ob alles funktioniert, indem Sie eine Verbindung über die sichere Oracle Hyperion Enterprise Performance Management Workspace-URL herstellen:

`https://virtual_host_external:SSL_PORT/workspace/index.jsp`

Beispiel: `https://epm.myCompany.com:443/workspace/index.jsp`, wobei 443 der SSL-Port ist.

## SSL für Essbase 11.1.2.4

### Übersicht

In diesem Abschnitt wird die Vorgehensweise beim Ersetzen der Standardzertifikate beschrieben, die zum Sichern der Kommunikation zwischen einer Oracle Essbase-Instanz und Komponenten wie MaxL, Oracle Essbase Administration Services-Server, Oracle Essbase Studio-Server, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management und Oracle Hyperion Shared Services Registry verwendet werden.

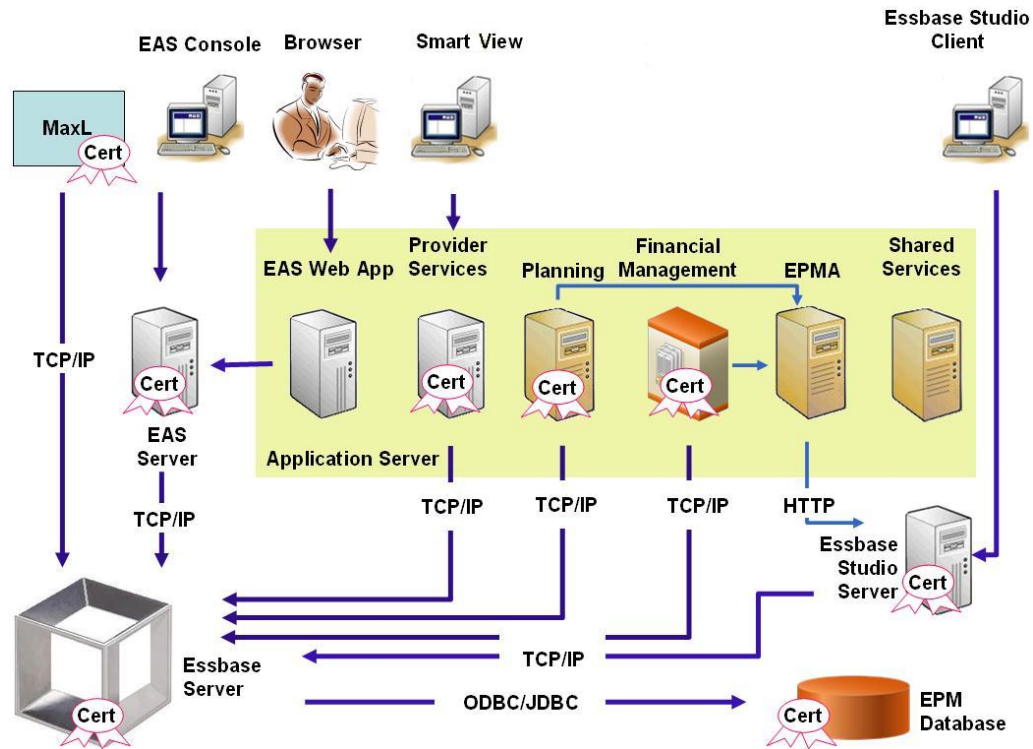
### Standard-Deployment

Essbase kann im SSL- und im Nicht-SSL-Modus bereitgestellt werden. Der Essbase-Agent hört einen unsicheren Port ab. Er kann auch für das Listening an einem sicheren Port konfiguriert werden. Alle Verbindungen, die auf den sicheren Port zugreifen, werden als SSL-Verbindungen behandelt. Wenn ein Client eine Verbindung zum Essbase-Agent über den Nicht-SSL-Port herstellt, wird die Verbindung als Nicht-SSL-Verbindung behandelt. Komponenten können gleichzeitig Nicht-SSL- und SSL-Verbindungen zu einem Essbase-Agent herstellen.

Sie können SSL sessionbasiert kontrollieren, indem Sie bei der Anmeldung das sichere Protokoll und den sicheren Port angeben. Informationen hierzu finden Sie unter [Sessionbasierte SSL-Verbindung herstellen](#).

Wenn SSL aktiviert ist, wird die gesamte Kommunikation in einer Essbase-Instanz verschlüsselt, um für Datensicherheit zu sorgen.

Standard-Deployments von Essbase-Komponenten im sicheren Modus verwenden selbstsignierte Zertifikate, um die SSL-Kommunikation zu aktivieren. Dies dient hauptsächlich zu Testzwecken. Oracle empfiehlt, Zertifikate von bekannten Drittanbieter-CAs zu verwenden, um SSL für Essbase in Produktionsumgebungen zu aktivieren.



Ein Oracle-Wallet speichert in der Regel das Zertifikat, mit dem die SSL-Kommunikation mit Clients aktiviert wird, die Essbase RTC verwenden. Ein Java-Keystore speichert das Zertifikat, mit dem die SSL-Kommunikation mit Komponenten aktiviert wird, die JAPI für die Kommunikation verwenden. Um die SSL-Kommunikation einzurichten, speichern Essbase-Clients und -Tools das Stammzertifikat der CA, die die Zertifikate des Essbase-Servers und -Agents signiert hat. Informationen hierzu finden Sie unter [Erforderliche Zertifikate und zugehörige Speicherorte](#).

### Erforderliche Zertifikate und zugehörige Speicherorte

Oracle empfiehlt, Zertifikate von bekannten Drittanbieter-CAs zu verwenden, um SSL für Essbase in einer Produktionsumgebung zu aktivieren. Sie können die selbstsignierten Standardzertifikate zu Testzwecken verwenden.

#### Hinweis:

Essbase unterstützt die Verwendung von Platzhalterzertifikaten, wodurch mehrere Subdomains mit einem SSL-Zertifikat gesichert werden können. Die Verwendung eines Platzhalterzertifikats ermöglicht Zeit- und Kosteneinsparungen bei der Verwaltung.

Platzhalterzertifikate können nicht verwendet werden, wenn die Hostnamenüberprüfung aktiviert ist.

Sie benötigen die folgenden Zertifikate:

- Ein CA-Stammzertifikat.  
Für Komponenten, die Essbase RTC verwenden, um eine Verbindung zu Essbase herzustellen, muss das CA-Stammzertifikat in einem Oracle-Wallet gespeichert

werden. Für Komponenten, die JAPI verwenden, um eine Verbindung herzustellen, muss das CA-Stammzertifikat in einem Java-Keystore gespeichert werden. Die erforderlichen Zertifikate und die jeweiligen Speicherorte sind in der folgenden Tabelle angegeben.

 **Hinweis:**

Sie müssen möglicherweise kein CA-Stammzertifikat installieren, wenn Sie Zertifikate einer bekannten Drittanbieter-CA verwenden, deren Stammzertifikat bereits im Oracle-Wallet installiert ist.

- Signiertes Zertifikat für Essbase-Server und Essbase-Agent.

**Tabelle 2-1 Erforderliche Zertifikate und zugehörige Speicherorte**

| Komponente <sup>1</sup>                                   | Keystore   | Zertifikat <sup>2</sup>   |
|---|--|---|
| MaxL  | Oracle-Wallet  | CA-Stammzertifikat  |
| Administration Services-Server                            | Oracle-Wallet  | CA-Stammzertifikat  |
| Provider Services   | Oracle-Wallet  | CA-Stammzertifikat  |
| Oracle Enterprise Performance Management System-Datenbank | Oracle-Wallet  | CA-Stammzertifikat  |
| Essbase Studio-Server                                     | Java-Keystore  | CA-Stammzertifikat  |
| Planning  | <ul style="list-style-type: none"> <li>• Oracle-Wallet</li> <li>• Java-Keystore</li> </ul> | CA-Stammzertifikat  |
| Financial Management                                      | Java-Keystore  | CA-Stammzertifikat  |
| Essbase (Server und Agent) <sup>3</sup>                   | <ul style="list-style-type: none"> <li>• Oracle-Wallet</li> <li>• Java-Keystore</li> </ul> | <ul style="list-style-type: none"> <li>• CA-Stammzertifikat</li> <li>• Signiertes Zertifikat für Essbase-Server und -Agent</li> </ul> |

Oracle Hyperion Shared Services-Repository

<sup>1</sup> Sie benötigen nur eine Keystore-Instanz, um mehrere Komponenten zu unterstützen, die ähnliche Keystores verwenden.

<sup>2</sup> Mehrere Komponenten können ein Stammzertifikat verwenden, das in einem Keystore installiert ist.

<sup>3</sup> Zertifikate müssen im Oracle-Standard-Wallet und im Java-Keystore installiert sein.

## Essbase-Komponenten installieren und bereitstellen

Der Konfigurationsprozess ermöglicht Ihnen die Auswahl eines sicheren Agent-Ports (Standard ist 6423), den Sie beim Konfigurieren von Oracle Essbase ändern können. Beim Deployment-Prozess werden standardmäßig die erforderlichen selbstsignierten Zertifikate installiert, um ein funktionales sicheres Deployment zum Testen zu erstellen.

EPM System Installer installiert ein Oracle-Wallet und ein selbstsigniertes Zertifikat unter *ARBOR\_PATH* auf dem Hostcomputer der Essbase-Instanz, wenn Oracle HTTP Server installiert ist. In Deployments mit einem einzelnen Host verwenden alle Essbase-Komponenten dieses Zertifikat gemeinsam.

## Vertrauenswürdige CA-Zertifikate von Drittanbietern für Essbase verwenden

### Zertifikatsanforderungen erstellen und Zertifikate erhalten

Erstellen Sie eine Zertifikatsanforderung, um ein Zertifikat für den Hostserver des Oracle Essbase-Servers und des Essbase-Agents zu erhalten. Eine Zertifikatsanforderung enthält verschlüsselte Informationen zu Ihrem Distinguished Name (DN). Sie leiten die Zertifikatsanforderung an eine Signing Authority weiter, um ein SSL-Zertifikat zu erhalten.

Sie verwenden ein Tool wie keytool oder Oracle Wallet Manager, um eine Zertifikatsanforderung zu erstellen. Ausführliche Informationen zum Erstellen einer Zertifikatsanforderung finden Sie in der Dokumentation zu dem von Ihnen verwendeten Tool.

Wenn Sie keytool verwenden, erstellen Sie eine Zertifikatsanforderung mit einem Befehl wie dem folgenden:

```
keytool -certreq -alias essbase_ssl -file C:/certs/essabase_server_csr -  
keypass password -storetype jks -keystore  
C:\oracle\Middleware\EPMSysstem11R1\Essbase_ssl\keystore -storepass  
password
```

### CA-Stammzertifikate erhalten und installieren

Das CA-Stammzertifikat prüft die Gültigkeit des Zertifikats, das verwendet wird, um SSL zu unterstützen. Es enthält den Public Key, mit dem der zum Signieren des Zertifikats verwendete Private Key abgeglichen wird, um das Zertifikat zu prüfen. Sie können das CA-Stammzertifikat von der Certificate Authority erhalten, die Ihre SSL-Zertifikate signiert hat.

Installieren Sie das Stammzertifikat der CA, die das Essbase-Serverzertifikat signiert hat, auf Clients, die eine Verbindung zum Essbase-Server oder -Agent herstellen. Stellen Sie sicher, dass das Stammzertifikat im Keystore des entsprechenden Clients installiert ist. Informationen hierzu finden Sie unter [Erforderliche Zertifikate und zugehörige Speicherorte](#).

#### Hinweis:

Mehrere Komponenten können ein CA-Stammzertifikat verwenden, das auf einem Serverrechner installiert ist.

### Oracle-Wallet

In [Erforderliche Zertifikate und zugehörige Speicherorte](#) finden Sie eine Liste der Komponenten, für die das CA-Stammzertifikat in einem Oracle-Wallet installiert sein muss. Sie können ein Wallet erstellen oder das Zertifikat im Demo-Wallet installieren, in dem das selbstsignierte Standardzertifikat installiert ist.

Ausführliche Anweisungen zum Erstellen von Wallets und zum Importieren von CA-Stammzertifikaten finden Sie in der Dokumentation zu Oracle Wallet Manager.

### Java-Keystore

In [Erforderliche Zertifikate und zugehörige Speicherorte](#) finden Sie eine Liste der Komponenten, für die das CA-Stammzertifikat in einem Java-Keystore installiert sein muss. Sie können das Zertifikat dem Keystore hinzufügen, in dem das selbstsignierte Standardzertifikat installiert ist, oder einen Keystore erstellen, um das Zertifikat zu speichern.



#### Hinweis:

Die CA-Stammzertifikate vieler bekannter Drittanbieter-CAs sind bereits im JVM-Keystore installiert.

Ausführliche Anweisungen finden Sie in der Dokumentation zu dem von Ihnen verwendeten Tool. Wenn Sie `keytool` verwenden, können Sie das Stammzertifikat mit einem Befehl wie dem folgenden importieren:

```
keytool -import -alias blister_CA -file c:/certs/CA.crt -keypass  
password -trustcacerts -keystore  
C:\Oracle\Middleware\EPMSysstem11R1\Essbase_ssl  
\keystore -storepass password
```

### Signierte Zertifikate installieren

Sie installieren die signierten SSL-Zertifikate auf dem Hostserver des Essbase-Servers und des Essbase-Agents. Für Komponenten, die Essbase RTC (C-APIs) verwenden, um eine Verbindung zum Essbase-Server oder -Agent herzustellen, muss das Zertifikat in einem Oracle-Wallet mit dem CA-Stammzertifikat gespeichert werden. Für Komponenten, die JAPI verwenden, um eine Verbindung zum Essbase-Server oder -Agent herzustellen, müssen das CA-Stammzertifikat und das signierte SSL-Zertifikat in einem Java-Keystore gespeichert werden. Ausführliche Anweisungen finden Sie in den folgenden Informationsquellen:

- Dokumentation zu Oracle Wallet Manager
- Dokumentation oder Onlinehilfe zu dem Tool, das Sie für den Import des Zertifikats verwenden, z.B. `keytool`

Wenn Sie `keytool` verwenden, können Sie das Zertifikat mit einem Befehl wie dem folgenden importieren:

```
keytool -import -alias essbase_ssl -file C:/certs/essbase_ssl.crt -keypass  
password -keystore  
C:\Oracle\Middleware\EPMSysstem11R1\Essbase_ssl\keystore -storepass password
```

### Registry-Werte für den Essbase-Server aktualisieren

#### Windows

1. Wechseln Sie über eine Befehlszeile zum Verzeichnis `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Führen Sie die folgenden Befehle aus, um die Windows-Registry zu aktualisieren:

```
epmsys_registry.bat updateproperty "#<Object ID>/@EnableSecureMode"
true
epmsys_registry.bat updateproperty "#<Object ID>/@EnableClearMode"
false
```

Stellen Sie sicher, dass <Object ID> durch die Komponenten-ID des Essbase-Servers ersetzt wird, die im Registry-Bericht verfügbar ist, der nach Abschluss des Konfigurationsprozesses für den Essbase-Server generiert wird.

## Linux

1. Wechseln Sie in einer Konsole zum Verzeichnis `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Führen Sie die folgenden Befehle aus, um die Registry zu aktualisieren:

```
epmsys_registry.sh updateproperty "#<Object ID>/@EnableSecureMode"
true
epmsys_registry.sh updateproperty "#<Object ID>/@EnableClearMode"
false
```

Stellen Sie sicher, dass <Object ID> durch die Komponenten-ID des Essbase-Servers ersetzt wird, die im Registry-Bericht verfügbar ist, der nach Abschluss des Konfigurationsprozesses für den Essbase-Server generiert wird.

## SSL-Einstellungen für Essbase aktualisieren

Sie können die SSL-Einstellungen für den Essbase-Server und die -Clients anpassen, indem Sie Werte für folgende Elemente in `essbase.cfg` angeben.

- Einstellung zum Aktivieren des sicheren Modus
- Einstellung zum Aktivieren des unsicheren Modus
- Bevorzugter Modus für die Kommunikation mit Clients (nur von Clients verwendet)
- Sicherer Port
- Cipher Suites
- Oracle-Wallet-Pfad

### Hinweis:

Stellen Sie sicher, dass Sie in der Datei `essbase.cfg` alle fehlenden erforderlichen Parameter hinzufügen, insbesondere `EnableSecureMode` und `AgentSecurePort`, und legen Sie die entsprechenden Werte fest.

So aktualisieren Sie die Datei `essbase.cfg`:

1. Kopieren Sie das Oracle-Wallet mit Zertifikaten für den Essbase-Server in das Verzeichnis `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/wallet`. Dies ist das einzige Verzeichnis für das Oracle-Wallet, das für den Essbase-Server zulässig ist.
2. Öffnen Sie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` mit einem Texteditor.



- Geben Sie Einstellungen nach Bedarf ein. Essbase-Standard Einstellungen sind impliziert. Wenn Sie das Standardverhalten ändern müssen, fügen Sie die Einstellungen für das benutzerdefinierte Verhalten in der Datei `essbase.cfg` hinzu. Beispiel: `EnableClearMode` wird standardmäßig erzwungen. Mit dieser Einstellung kann der Essbase-Server über unverschlüsselte Kanäle kommunizieren. Wenn der Essbase-Server nicht über unverschlüsselte Kanäle kommunizieren soll, geben Sie `EnableClearMode FALSE` in der Datei `essbase.cfg` an. Informationen hierzu finden Sie in der folgenden Tabelle.

**Tabelle 2-2 SSL-Einstellungen für Essbase**

| Einstellung                               | Beschreibung <sup>1</sup>  |
|---|--|
| <code>EnableClearMode</code> <sup>2</sup> | Aktiviert die unverschlüsselte Kommunikation zwischen Essbase-Anwendungen und dem Essbase-Agent. Wenn diese Eigenschaft auf <code>FALSE</code> gesetzt wird, verarbeitet Essbase keine Nicht-SSL-Anforderungen.<br><b>Standardwert:</b> <code>EnableClearMode TRUE</code><br><b>Beispiel:</b> <code>EnableClearMode FALSE</code>   |
| <code>EnableSecureMode</code>             | Aktiviert SSL-verschlüsselte Kommunikation zwischen Essbase-Clients und dem Essbase-Agent. Diese Eigenschaft muss auf <code>TRUE</code> gesetzt werden, damit SSL unterstützt wird.<br><b>Standardwert:</b> <code>FALSE</code><br><b>Beispiel:</b> <code>EnableSecureMode TRUE</code>  |
| <code>SSLCipherSuites</code>              | Eine Liste von Cipher Suites für die SSL-Kommunikation, nach Präferenz sortiert. Der Essbase-Agent verwendet eine dieser Cipher Suites für die SSL-Kommunikation. Wenn der Agent eine Cipher Suite auswählt, hat die erste Cipher Suite in der Liste die höchste Priorität.<br><b>Standardwert:</b> <code>SSL_RSA_WITH_RC4_128_MD5</code><br><b>Beispiel:</b> <code>SSLCipherSuites<br/>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code> |
| <code>APSRESOLVER</code>                  | URL von Oracle Hyperion Provider Services. Wenn Sie verschiedene Provider Services-Server verwenden, trennen Sie die einzelnen URLs durch ein Semikolon.<br><b>Beispiel:</b> <code>APSRESOLVER https://<br/>exampleAPShost1:PORT/aps;https://<br/>exampleAPShost2:PORT/aps</code>  |
| <code>AgentSecurePort</code>              | Der sichere Port, den der Agent abhört.<br><b>Standardwert:</b> <code>6423</code><br><b>Beispiel:</b> <code>AgentSecurePort 16001</code>   |
| <code>WalletPath</code>                   | Speicherort des Oracle-Wallets (maximal 1.024 Zeichen), in dem das CA-Stammzertifikat und das signierte Zertifikat gespeichert sind.<br><b>Standardwert:</b> <code>ARBORPATH/bin/wallet</code><br><b>Beispiel:</b> <code>WalletPath/usr/local/wallet</code>  |

**Tabelle 2-2 (Fortsetzung) SSL-Einstellungen für Essbase**

| Einstellung                      | Beschreibung <sup>1</sup>  |
|----------------------------------|--|
| ClientPreferredMode <sup>3</sup> | <p>Der Modus (sicher oder unsicher) für die Client-session. Wenn diese Eigenschaft auf "Sicher" gesetzt ist, wird der SSL-Modus für alle Sessions verwendet. Wenn diese Eigenschaft auf "Unsicher" gesetzt ist, hängt die Transportauswahl davon ab, ob die Clientanmeldeanforderung das sichere Transportschlüsselwort enthält. Informationen hierzu finden Sie unter <a href="#">Sessionbasierte SSL-Verbindung herstellen</a>.</p> <p><b>Standardwert:</b> CLEAR</p> <p><b>Beispiel:</b> ClientPreferredMode SECURE</p> |

<sup>1</sup> Der Standardwert wird erzwungen, wenn diese Eigenschaften nicht in `essbase.cfg` verfügbar sind.

<sup>2</sup> Essbase funktioniert nicht, wenn `EnableClearMode` und `EnableSecureMode` auf `FALSE` gesetzt sind.

<sup>3</sup> Clients verwenden diese Einstellung, um festzulegen, ob sie eine sichere oder unsichere Verbindung zu Essbase herstellen sollen.

- Speichern und schließen Sie die Datei `essbase.cfg`.

#### Verteilte Essbase-Knoten für SSL aktualisieren



#### Hinweis:

Dieser Abschnitt gilt nur für verteilte Deployments von Essbase

Stellen Sie sicher, dass das CA-Stammzertifikat im Wallet-Ordner (z.B. `WalletPath/usr/local/wallet`) enthalten ist und dass sich das signierte Zertifikat am erforderlichen Speicherort der einzelnen verteilten Knoten befindet.

- Kopieren Sie den Wallet-Ordner in die folgenden Speicherorte der einzelnen verteilten Knoten:
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
- Kopieren Sie den Wallet-Ordner in die folgenden Speicherorte der einzelnen verteilten Knoten, sofern vorhanden:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
- Kopieren Sie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` in die folgenden Speicherorte der einzelnen verteilten Knoten:
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`

4. Kopieren Sie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` in die folgenden Speicherorte der einzelnen verteilten Knoten, sofern vorhanden:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
5. Kopieren Sie den Wallet-Ordner in die Essbase-Clientinstallationsverzeichnisse der einzelnen verteilten Knoten:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient-32/bin`
6. Kopieren Sie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` in die folgenden Essbase-Clientinstallationsverzeichnisse der einzelnen verteilten Knoten:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient-32/bin`
7. Fügen Sie die folgenden Eigenschaften in der Datei `essbase.properties` hinzu:
  - `essbase.ssleverywhere=true`
  - `olap.server.ssl.alwaysSecure=true`
  - `APSRESOLVER=http[s]://host:httpsPort/aps`  
Ersetzen Sie diesen Wert unbedingt durch die entsprechende URL.

Sie müssen die Datei `essbase.properties` in den folgenden Speicherorten der einzelnen verteilten Knoten aktualisieren, sofern vorhanden:

  - `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.2.0/bin/essbase.properties`
  - `EPM_ORACLE_HOME/products/Essbase/aps/bin/essbase.properties`
  - `EPM_ORACLE_INSTANCE/aps/bin/essbase.properties`
8. Kopieren Sie `EPM_ORACLE_HOME/products/Essbase/aps/bin/essbase.properties` in das Verzeichnis `EPM_ORACLE_HOME/products/Essbase/eas` der einzelnen verteilten Knoten, sofern vorhanden.
9. **Nur für Oracle Hyperion Planning:** Fügen Sie die folgenden drei Eigenschaften in der Datei `essbase.properties` hinzu:
  - `essbase.ssleverywhere=true`
  - `olap.server.ssl.alwaysSecure=true`
  - `APSRESOLVER=APS_URL`  
Ersetzen Sie `APS_URL` durch die Provider Services-URL. Wenn Sie verschiedene Provider Services-Server verwenden, trennen Sie die einzelnen URLs durch ein Semikolon. Beispiel: `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

Sie müssen die Datei `essbase.properties` in den folgenden Speicherorten der einzelnen verteilten Knoten aktualisieren:

  - `EPM_ORACLE_HOME/products/Planning/config/essbase.properties`
  - `EPM_ORACLE_HOME/products/Planning/lib/essbase.properties`

10. **Nur für Oracle Hyperion Financial Reporting:** Fügen Sie die folgenden drei Eigenschaften in der Datei `EPM_ORACLE_HOME/products/financialreporting/bin/EssbaseJAPI/bin/essbase.properties` hinzu:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`

Ersetzen Sie `APS_URL` durch die Provider Services-URL. Wenn Sie verschiedene Provider Services-Server verwenden, trennen Sie die einzelnen URLs durch ein Semikolon. Beispiel: `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

 **Hinweis:**

In vollständigen SSL-Umgebungen ist es für Financial Reporting erforderlich, dass mit dem Essbase-Clusternamen eine Verbindung hergestellt wird. Es können keine Verbindungen hergestellt werden, wenn der Hostname zum Verbinden verwendet wird.

11. a. Legen Sie die Umgebungsvariablen fest:

- **Windows:** Erstellen Sie eine neue Systemvariable namens `API_DISABLE_PEER_VERIFICATION`, und setzen Sie ihren Wert auf 1.
- **Linux:** Fügen Sie die Direktive `API_DISABLE_PEER_VERIFICATION=1` in `setCustomParamsPlanning.sh` hinzu.

b. Fügen Sie die Direktive `API_DISABLE_PEER_VERIFICATION=1` in `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.bat` oder `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.sh` hinzu.

Legen Sie Umgebungsvariablen fest:

### SSL-Eigenschaften von JAPI-Clients anpassen

Verschiedene Standardeigenschaften sind für die auf JAPI basierenden Essbase-Komponenten vordefiniert. Die Standardeigenschaften können überschrieben werden, indem Eigenschaften in die Datei `essbase.properties` eingefügt werden.

 **Hinweis:**

Nur ein paar der in der folgenden Tabelle angegebenen SSL-Eigenschaften sind in der Datei `essbase.properties` externalisiert. Sie müssen die Eigenschaften hinzufügen, die nicht externalisiert sind.

So aktualisieren Sie SSL-Eigenschaften von JAPI-Clients:

1. Öffnen Sie `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.1.2.0/bin/essbase.properties` mit einem Texteditor.
2. Aktualisieren Sie Eigenschaften nach Bedarf. Eine Beschreibung der anpassbaren JAPI-Clienteigenschaften finden Sie in der folgenden Tabelle.

Wenn eine gewünschte Eigenschaft nicht in der Datei `essbase.properties` enthalten ist, fügen Sie sie hinzu.

**Tabelle 2-3 SSL-Standardeigenschaften für JAPI-Clients**

| Eigenschaft                                   | Beschreibung  |
|---|---|
| <code>olap.server.ssl.alwaysSecure</code>     | Legt den Modus fest, den Clients für alle Essbase-Instanzen verwenden sollen. Ändern Sie diesen Eigenschaftswert in <code>true</code> , um den SSL-Modus zu erzwingen.<br><b>Standardwert:</b> <code>false</code>   |
| <code>olap.server.ssl.securityHandler</code>  | Paketname für die Protokollverarbeitung. Sie können diesen Wert ändern, um einen anderen Handler anzugeben.<br><b>Standardwert:</b><br><code>java.protocol.handler.pkgs</code>  |
| <code>olap.server.ssl.securityProvider</code> | Oracle verwendet die Sun-SSL-Protokollimplementierung. Sie können diesen Wert ändern, um einen anderen Provider anzugeben.<br><b>Standardwert:</b><br><code>com.sun.net.ssl.internal.www.protocol</code>  |
| <code>olap.server.ssl.supportedCiphers</code> | Eine durch Komma getrennte Liste zusätzlicher Cipher, die für eine sichere Kommunikation aktiviert werden sollen. Sie dürfen nur Cipher angeben, die Essbase unterstützt.<br><b>Beispiel:</b><br><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code> |

**Tabelle 2-3 (Fortsetzung) SSL-Standard Eigenschaften für JAPI-Clients**

| Eigenschaft                       | Beschreibung   |
|-----------------------------------|--|
| olap.server.ssl.trustManagerClass | <p>Die TrustManager-Klasse zur Validierung des SSL-Zertifikats, indem die Signatur und das Ablaufdatum des Zertifikats geprüft werden.</p> <p>Standardmäßig ist diese Eigenschaft nicht festgelegt, um alle Verifizierungsprüfungen zu erzwingen.</p> <p>Wenn Verifizierungsprüfungen nicht erzwungen werden sollen, setzen Sie den Wert dieses Parameters auf <code>com.essbase.services.olap.security.EssDefaultTrustManager</code>. Hierbei handelt es sich um die TrustManager-Standardklasse, mit der alle Verifizierungsprüfungen erfolgreich ausgeführt werden können.</p> <p>Wenn Sie eine benutzerdefinierte TrustManager-Klasse implementieren möchten, geben Sie einen vollqualifizierten Klassennamen der TrustManager-Klasse an, mit der die Schnittstelle <code>javax.net.ssl.X509TrustManager</code> implementiert wird.</p> <p><b>Beispiel:</b><br/><code>com.essbase.services.olap.security.EssDefaultTrustManager</code></p> |

3. Speichern und schließen Sie die Datei `essbase.properties`.
4. Starten Sie alle Essbase-Komponenten neu.

## Sessionbasierte SSL-Verbindung herstellen

Oracle Essbase-Komponenten, wie z.B. MaxL, können SSL auf Sessionebene kontrollieren, indem eine Verbindung zum Essbase-Agent mit dem Transportschlüsselwort `secure` hergestellt wird. Beispiel: Sie können eine sichere Verbindung zwischen MaxL und dem Essbase-Agent herstellen, indem Sie einen der folgenden Befehle über eine MaxL-Konsole ausführen:

```
login admin example_password on hostA:PORT:secure
```

```
login admin example_password on hostA:secure
```

Die sessionbasierte Kontrolle hat Vorrang vor Konfigurationseinstellungen in der Datei `essbase.cfg`. Wenn kein Transportschlüsselwort angegeben ist, verwenden Essbase-Clients den für `ClientPreferredMode` festgelegten Wert, um zu bestimmen, ob eine sichere Verbindung mit Essbase initiiert werden soll. Wenn die Einstellung `ClientPreferredMode` nicht auf "secure" gesetzt ist, erfolgt die Kommunikation über einen nicht sicheren Kanal.

# SSL für Essbase 21c

## Übersicht

In diesem Abschnitt wird die Vorgehensweise beim Ersetzen der Standardzertifikate beschrieben, die zum Sichern der Kommunikation zwischen einer Oracle Essbase-Instanz und Komponenten wie MaxL, Oracle Essbase Administration Services-Server, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management und Oracle Hyperion Shared Services Registry verwendet werden.

### Hinweis:

In Essbase Administration Services (EAS) Lite wird der mit EPM Configurator konfigurierte SSL-Port des HTTP-Servers (z.B. 443) nicht verwendet. Die sichere URL in der Datei `easconsole.jnlp` wird standardmäßig auf den Nicht-SSL-Port (80) gesetzt.

**Workaround:** Ersetzen Sie den Nicht-SSL-Standardport in der sicheren URL, die in der Datei `easconsole.jnlp` angegeben ist, durch die aktualisierte sichere URL:

Standardmäßige sichere URL: `https://myserver:SECURE_PORT/easconsole/console.html`. Beispiel: `https://myserver:80/easconsole/console.html`

Aktualisierte sichere URL: `https://myserver:SECURE_PORT/easconsole/console.html`. Beispiel: `https://myserver:443/easconsole/console.html`

Weitere Informationen finden Sie im folgenden My Oracle Support-(MOS-)Artikel: [Dokument-ID 1926558.1 - SSL Port Not Included In easconsole.jnlp of the EAS Web Console](#).

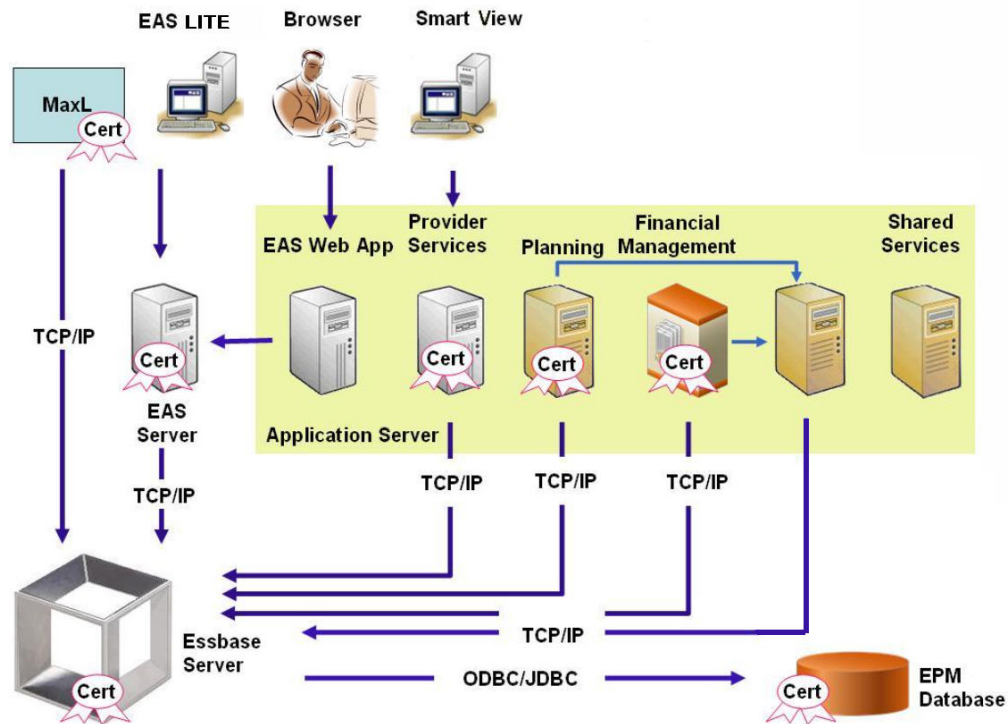
## Standard-Deployment

Essbase kann im SSL- und im Nicht-SSL-Modus bereitgestellt werden. Der Essbase-Agent hört einen unsicheren Port ab. Er kann auch für das Listening an einem sicheren Port konfiguriert werden. Alle Verbindungen, die auf den sicheren Port zugreifen, werden als SSL-Verbindungen behandelt. Wenn ein Client eine Verbindung zum Essbase-Agent über den Nicht-SSL-Port herstellt, wird die Verbindung als Nicht-SSL-Verbindung behandelt. Komponenten können gleichzeitig Nicht-SSL- und SSL-Verbindungen zu einem Essbase-Agent herstellen.

Sie können SSL sessionbasiert kontrollieren, indem Sie bei der Anmeldung das sichere Protokoll und den sicheren Port angeben. Informationen hierzu finden Sie unter [Sessionbasierte SSL-Verbindung herstellen](#).

Wenn SSL aktiviert ist, wird die gesamte Kommunikation in einer Essbase-Instanz verschlüsselt, um für Datensicherheit zu sorgen.

Standard-Deployments von Essbase-Komponenten im sicheren Modus verwenden selbstsignierte Zertifikate, um die SSL-Kommunikation zu aktivieren. Dies dient hauptsächlich zu Testzwecken. Oracle empfiehlt, Zertifikate von bekannten Drittanbieter-CAs zu verwenden, um SSL für Essbase in Produktionsumgebungen zu aktivieren.



Ein Oracle-Wallet speichert in der Regel das Zertifikat, mit dem die SSL-Kommunikation mit Clients aktiviert wird, die Essbase RTC verwenden. Ein Java-Keystore speichert das Zertifikat, mit dem die SSL-Kommunikation mit Komponenten aktiviert wird, die JAPI für die Kommunikation verwenden. Um die SSL-Kommunikation einzurichten, speichern Essbase-Clients und -Tools das Stammzertifikat der CA, die die Zertifikate des Essbase-Servers und -Agents signiert hat.

### Erforderliche Zertifikate und zugehörige Speicherorte

Oracle empfiehlt, Zertifikate von bekannten Drittanbieter-CAs zu verwenden, um SSL für Essbase in einer Produktionsumgebung zu aktivieren. Sie können die selbstsignierten Standardzertifikate zu Testzwecken verwenden.

#### Hinweis:

Essbase unterstützt die Verwendung von Platzhalterzertifikaten, wodurch mehrere Subdomains mit einem SSL-Zertifikat gesichert werden können. Die Verwendung eines Platzhalterzertifikats ermöglicht Zeit- und Kosteneinsparungen bei der Verwaltung.

Platzhalterzertifikate können nicht verwendet werden, wenn die Hostnamenüberprüfung aktiviert ist.

Sie benötigen die folgenden Zertifikate:

- Ein CA-Stammzertifikat.  
Für Komponenten, die Essbase RTC verwenden, um eine Verbindung zu Essbase herzustellen, muss das CA-Stammzertifikat in einem Oracle-Wallet gespeichert



werden. Für Komponenten, die JAPI verwenden, um eine Verbindung herzustellen, muss das CA-Stammzertifikat in einem Java-Keystore gespeichert werden. Die erforderlichen Zertifikate und die jeweiligen Speicherorte sind in der folgenden Tabelle angegeben.

 **Hinweis:**

Sie müssen möglicherweise kein CA-Stammzertifikat installieren, wenn Sie Zertifikate einer bekannten Drittanbieter-CA verwenden, deren Stammzertifikat bereits im Oracle-Wallet installiert ist.

- Signiertes Zertifikat für Essbase-Server und Essbase-Agent.

**Tabelle 2-4 Erforderliche Zertifikate und zugehörige Speicherorte**

| Komponente <sup>1</sup>                                   | Keystore   | Zertifikat <sup>2</sup>   |
|---|--|---|
| MaxL  | Oracle-Wallet  | CA-Stammzertifikat  |
| Administration Services-Server                            | Oracle-Wallet  | CA-Stammzertifikat  |
| Provider Services   | Oracle-Wallet  | CA-Stammzertifikat  |
| Oracle Enterprise Performance Management System-Datenbank | Oracle-Wallet  | CA-Stammzertifikat  |
| Planning  | <ul style="list-style-type: none"> <li>• Oracle-Wallet</li> <li>• Java-Keystore</li> </ul> | CA-Stammzertifikat  |
| Financial Management                                      | Java-Keystore  | CA-Stammzertifikat  |
| Essbase (Server und Agent) <sup>3</sup>                   | <ul style="list-style-type: none"> <li>• Oracle-Wallet</li> <li>• Java-Keystore</li> </ul> | <ul style="list-style-type: none"> <li>• CA-Stammzertifikat</li> <li>• Signiertes Zertifikat für Essbase-Server und -Agent</li> </ul> |
| Oracle Hyperion Shared Services-Repository                |  |   |

<sup>1</sup> Sie benötigen nur eine Keystore-Instanz, um mehrere Komponenten zu unterstützen, die ähnliche Keystores verwenden.

<sup>2</sup> Mehrere Komponenten können ein Stammzertifikat verwenden, das in einem Keystore installiert ist.

<sup>3</sup> Zertifikate müssen im Oracle-Standard-Wallet und im Java-Keystore installiert sein.

## Essbase-Komponenten installieren und bereitstellen

Der Konfigurationsprozess ermöglicht Ihnen die Auswahl eines sicheren Agent-Ports (Standard ist 6423), den Sie beim Konfigurieren von Oracle Essbase ändern können. Beim Deployment-Prozess werden standardmäßig die erforderlichen selbstsignierten Zertifikate installiert, um ein funktionales sicheres Deployment zum Testen zu erstellen.

EPM System Installer installiert ein Oracle-Wallet und ein selbstsigniertes Zertifikat unter `ARBOR_PATH` auf dem Hostcomputer der Essbase-Instanz, wenn Oracle HTTP Server installiert ist. In Deployments mit einem einzelnen Host verwenden alle Essbase-Komponenten dieses Zertifikat gemeinsam.

## Vertrauenswürdige CA-Zertifikate von Drittanbietern für Essbase verwenden

### Zertifikatsanforderungen erstellen und Zertifikate erhalten

Erstellen Sie eine Zertifikatsanforderung, um ein Zertifikat für den Hostserver des Oracle Essbase-Servers und des Essbase-Agents zu erhalten. Eine Zertifikatsanforderung enthält verschlüsselte Informationen zum allgemeinen Namen (CN=) Ihres Servers. Sie leiten die Zertifikatsanforderung an eine Signing Authority weiter, um ein SSL-Zertifikat zu erhalten.

Sie verwenden ein Tool wie keytool oder Oracle Wallet Manager, um eine Zertifikatsanforderung zu erstellen. Ausführliche Informationen zum Erstellen einer Zertifikatsanforderung finden Sie in der Dokumentation zu dem von Ihnen verwendeten Tool.

### Beispiele mit "keytool":

Erstellen Sie einen Java Keystore (JKS), und generieren Sie einen Private Key:

```
keytool.exe -genkey -dname "cn=myserver, ou=EPM, o=Oracle, c=US"  
-alias essbase_ssl -keypass password -keystore  
C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -storepass password  
-validity 365 -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -noprompt
```

Generieren Sie eine Zertifikatanforderung:

```
keytool -certreq -alias essbase_ssl -file  
C:\oracle\Middleware\EPMSysstem11R1\ssl\essbase_server.csr -keypass  
password  
-keystore C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -storepass  
password
```

Exportieren Sie Ihren Private Key (für diese Schritte benötigen Sie das openssl-Utility):

1. openssl.exe pkcs12 -in C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -passin pass:password -legacy -nocerts -out c:\Apache24\ssl\Apache24.key -passout pass:password
2. Signieren Sie die neu generierte Zertifikatsanforderung mit Ihrer CA (Certifying Authority), und fügen Sie sie in die folgende Datei ein:  
C:\oracle\Middleware\EPMSysstem11R1\ssl\essbase.cer.

### CA-Stammzertifikate erhalten und installieren

Das CA-Stammzertifikat prüft die Gültigkeit des Zertifikats, das verwendet wird, um SSL zu unterstützen. Es enthält den Public Key, mit dem der zum Signieren des Zertifikats verwendete Private Key abgeglichen wird, um das Zertifikat zu prüfen. Sie können das CA-Stammzertifikat von der Certificate Authority erhalten, die Ihre SSL-Zertifikate signiert hat.

Installieren Sie das Stammzertifikat der CA, die das Essbase-Serverzertifikat signiert hat, auf Clients, die eine Verbindung zum Essbase-Server oder -Agent herstellen.

Stellen Sie sicher, dass das Stammzertifikat im Keystore des entsprechenden Clients installiert ist. Informationen hierzu finden Sie unter [Erforderliche Zertifikate und zugehörige Speicherorte](#).



#### Hinweis:

Mehrere Komponenten können ein CA-Stammzertifikat verwenden, das auf einem Serverrechner installiert ist.

### CA-signierte Zertifikate installieren

Informationen zum Installieren von CA-signierten Zertifikaten finden Sie unter den folgenden Links:

- [WebLogic-TLS-Verbindung für Essbase einrichten](#)
- [TLS-Zertifikate aktualisieren](#)

Aktualisieren Sie die Datei `tls.properties` im folgenden Verzeichnis:

```
%EPM_HOME%\essbase\bin\tls_tools.properties:
certCA=c:\ssl\ca.crt;c:\ssl\intermediate.crt;c:\ssl\essbase.key;c:\
ssl\essbase.cer;
```

Dabei gilt:

```
C:\ssl\ca.crt - root CA certificate.
C:\ssl\intermediate.crt - intermediate CA certificate.
C:\ssl\essbase.key - your private key generated in the previous step.
C:\ssl\essbase.cer - your server's signed certificate issued by your CA.
```

Führen Sie die folgenden Befehle aus, um den Essbase-Server mit den neuen Zertifikaten zu aktualisieren:

```
set ORACLE_HOME=c:\OracleSSL
set EPM_HOME=%ORACLE_HOME%
set WL_HOME=%ORACLE_HOME%\wlserver
set JAVA_HOME=%ORACLE_HOME%\jdk
set DOMAIN_HOME=%ORACLE_HOME%\user_projects\domains\essbase_domain
%EPM_HOME%\essbase\bin\tls_tools.properties:
%ORACLE_HOME%\jdk\bin\java.exe -Xmx256m -jar %ORACLE_HOME%
\essbase\lib\tlsTools.jar %EPM_HOME%\essbase\bin\tls_tools.properties
```

### SSL-Einstellungen für Essbase aktualisieren

Sie können die SSL-Einstellungen für den Essbase-Server und die -Clients anpassen, indem Sie Werte für folgende Elemente in `essbase.cfg` angeben.

- Einstellung zum Aktivieren des sicheren Modus
- Einstellung zum Aktivieren des unsicheren Modus
- Bevorzugter Modus für die Kommunikation mit Clients (nur von Clients verwendet)

- Sicherer Port
- Cipher Suites
- Oracle-Wallet-Pfad



**Hinweis:**

Stellen Sie sicher, dass Sie in der Datei `essbase.cfg` alle fehlenden erforderlichen Parameter hinzufügen, insbesondere `EnableSecureMode` und `AgentSecurePort`, und legen Sie die entsprechenden Werte fest.

So aktualisieren Sie die Datei `essbase.cfg` im Verzeichnis:

`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase`

1. Geben Sie Einstellungen nach Bedarf ein. Essbase-Standard Einstellungen sind impliziert. Wenn Sie das Standardverhalten ändern müssen, fügen Sie die Einstellungen für das benutzerdefinierte Verhalten in der Datei `essbase.cfg` hinzu. Beispiel: `EnableClearMode` wird standardmäßig erzwungen. Mit dieser Einstellung kann der Essbase-Server über unverschlüsselte Kanäle kommunizieren. Wenn der Essbase-Server nicht über unverschlüsselte Kanäle kommunizieren soll, geben Sie `EnableClearMode FALSE` in der Datei `essbase.cfg` an. Informationen hierzu finden Sie in der folgenden Tabelle:

**Tabelle 2-5 SSL-Einstellungen für Essbase**

| Einstellung                               | Beschreibung <sup>1</sup>  |
|---|--|
| <code>EnableClearMode</code> <sup>2</sup> | Aktiviert die unverschlüsselte Kommunikation zwischen Essbase-Anwendungen und dem Essbase-Agent. Wenn diese Eigenschaft auf <code>FALSE</code> gesetzt wird, verarbeitet Essbase keine Nicht-SSL-Anforderungen.<br><b>Standardwert:</b> <code>EnableClearMode TRUE</code><br><b>Beispiel:</b> <code>EnableClearMode FALSE</code>   |
| <code>EnableSecureMode</code>             | Aktiviert SSL-verschlüsselte Kommunikation zwischen Essbase-Clients und dem Essbase-Agent. Diese Eigenschaft muss auf <code>TRUE</code> gesetzt werden, damit SSL unterstützt wird.<br><b>Standardwert:</b> <code>FALSE</code><br><b>Beispiel:</b> <code>EnableSecureMode TRUE</code>  |
| <code>SSLCipherSuites</code>              | Eine Liste von Cipher Suites für die SSL-Kommunikation, nach Präferenz sortiert. Der Essbase-Agent verwendet eine dieser Cipher Suites für die SSL-Kommunikation. Wenn der Agent eine Cipher Suite auswählt, hat die erste Cipher Suite in der Liste die höchste Priorität.<br><b>Standardwert:</b> <code>SSL_RSA_WITH_RC4_128_MD5</code><br><b>Beispiel:</b> <code>SSLCipherSuites<br/>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code> |

**Tabelle 2-5 (Fortsetzung) SSL-Einstellungen für Essbase**

| <b>Einstellung</b>               | <b>Beschreibung <sup>1</sup></b>  |
|----------------------------------|---|
| APRESOLVER                       | URL von Oracle Hyperion Provider Services. Wenn Sie verschiedene Provider Services-Server verwenden, trennen Sie die einzelnen URLs durch ein Semikolon.<br><b>Beispiel:</b> https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase  |
| AgentSecurePort                  | Der sichere Port, den der Agent abhört.<br><b>Standardwert:</b> 6423<br><b>Beispiel:</b> AgentSecurePort 16001  |
| WalletPath                       | Speicherort des Oracle-Wallets (maximal 1.024 Zeichen), in dem das CA-Stammzertifikat und das signierte Zertifikat gespeichert sind.<br><b>Standardwert:</b> ARBORPATH/bin/wallet<br><b>Beispiel:</b> WalletPath/usr/local/wallet   |
| ClientPreferredMode <sup>3</sup> | Der Modus (sicher oder unsicher) für die Client-session. Wenn diese Eigenschaft auf "Sicher" gesetzt ist, wird der SSL-Modus für alle Sessions verwendet.<br>Wenn diese Eigenschaft auf "Unsicher" gesetzt ist, hängt die Transportauswahl davon ab, ob die Clientanmeldeanforderung das sichere Transportschlüsselwort enthält. Informationen hierzu finden Sie unter <a href="#">Sessionbasierte SSL-Verbindung herstellen</a> .<br><b>Standardwert:</b> CLEAR<br><b>Beispiel:</b> ClientPreferredMode SECURE |

- <sup>1</sup> Der Standardwert wird erzwungen, wenn diese Eigenschaften nicht in `essbase.cfg` verfügbar sind.
- <sup>2</sup> Essbase funktioniert nicht, wenn `EnableClearMode` und `EnableSecureMode` auf `FALSE` gesetzt sind.
- <sup>3</sup> Clients verwenden diese Einstellung, um festzulegen, ob sie eine sichere oder unsichere Verbindung zu Essbase herstellen sollen.

2. Speichern und schließen Sie die Datei `essbase.cfg`.

### Verteilte Essbase-Knoten für SSL aktualisieren



#### Hinweis:

Dieser Abschnitt gilt nur für verteilte Deployments von Essbase

Stellen Sie sicher, dass das CA-Stammzertifikat im Wallet-Ordner (z.B. `WalletPath/usr/local/wallet`) enthalten ist und dass sich das signierte Zertifikat am erforderlichen Speicherort der einzelnen verteilten Knoten befindet.

1. Importieren Sie alle neuen CA-Zertifikate mit TLS-Tools.

Weitere Informationen finden Sie unter den folgenden Links:

- [WebLogic-TLS-Verbindung für Essbase einrichten](#)

- [TLS-Zertifikate aktualisieren](#)
2. Navigieren Sie zum Quellstandort: `ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase`, und ändern Sie die folgenden Eigenschaften in der Datei `essbase.properties`:
    - `essbase.ssleverywhere=true`
    - `olap.server.ssl.alwaysSecure=true`
    - `APSRESOLVER=APS_URL`  
Ersetzen Sie `APS_URL` durch die Provider Services-URL. Wenn Sie verschiedene Provider Services-Server verwenden, trennen Sie die einzelnen URLs durch ein Semikolon.  
  
`https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase.`
  3. Kopieren Sie die Ordner `Wallet` und `Walletssl` sowie die Dateien `essbase.cfg` und `essbase.properties` in die folgenden Zielpfade.

**Tabelle 2-6 Zielpfade**

| Zielpfade  | Walle<br>t | Walle<br>tssl | essb<br>ase.c<br>fg | essbas<br>e.<br>properti<br>es |
|--|------------|---------------|---------------------|--------------------------------|
| <code>EPM_ORACLE_HOME\common\EssbaseRTC-21C\11.1.2.0\bin</code>              | Ja         | Ja            | Ja                  | Ja                             |
| <code>EPM_ORACLE_HOME\common\EssbaseJavaAPI-21C\11.1.2.0\bin</code>          | Ja         | Ja            | Ja                  | Ja                             |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\aps</code>              | Ja         | Ja            | Ja                  | Ja                             |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase</code>          | Ja         | Ja            | Ja                  | Ja                             |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\template_files\essbase</code> | Ja         | Ja            | Ja                  | Ja                             |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\EssbaseServer\bin</code>      | Ja         | Ja            | Ja                  | Ja                             |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\aps\bin</code>                | Ja         | Ja            | Ja                  | Ja                             |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\ea<br/>s</code>               | Ja         | Ja            | Ja                  | Ja                             |
| <code>MIDDLEWARE_HOME\essbase\common\EssbaseJavaA<br/>PI\bin</code>          | Ja         | Ja            | Ja                  | Ja                             |

Tabelle 2-6 (Fortsetzung) Zielpfade

| Zielpfade   | Walle<br>t | Walle<br>tssl | essb<br>ase.c<br>fg | essbas<br>e.<br>properti<br>es |
|---|------------|---------------|---------------------|--------------------------------|
| <b>Nur für Oracle Hyperion Financial Reporting</b><br>EPM_ORACLE_HOME/products/<br>financialreporting/bin/EssbaseJAPI/bin/<br><b>Hinweis:</b> In vollständigen SSL-Umgebungen ist in<br>Financial Reporting der Essbase-Clusternamen zum<br>Herstellen einer Verbindung erforderlich. Es<br>können keine Verbindungen hergestellt werden,<br>wenn der Hostname zum Verbinden verwendet<br>wird. | Ja         | Ja            | Ja                  | Ja                             |
| <b>Nur für Oracle Hyperion Planning</b><br>EPM_ORACLE_HOME/products/Planning/config/<br>EPM_ORACLE_HOME/products/Planning/lib/  | Ja         | Ja            | Ja                  | Ja                             |

4. Legen Sie die Umgebungsvariablen fest:

- **Windows:** Erstellen Sie eine neue Systemvariable namens `API_DISABLE_PEER_VERIFICATION`, und setzen Sie ihren Wert auf 1.
- **Linux:** Fügen Sie die Direktive `API_DISABLE_PEER_VERIFICATION=1` in `setCustomParamsPlanning.sh` hinzu.

SSL-Eigenschaften von JAPI-Clients anpassen

Verschiedene Standardeigenschaften sind für die auf JAPI basierenden Essbase-Komponenten vordefiniert. Die Standardeigenschaften können überschrieben werden, indem Eigenschaften in die Datei `essbase.properties` eingefügt werden.



**Hinweis:**

Nur ein paar der in der folgenden Tabelle angegebenen SSL-Eigenschaften sind in der Datei `essbase.properties` externalisiert. Sie müssen die Eigenschaften hinzufügen, die nicht externalisiert sind.

So aktualisieren Sie SSL-Eigenschaften von JAPI-Clients:

1. Öffnen Sie `EPM_ORACLE_HOME/common/EssbaseJavaAPI-21C/11.2.0/bin/essbase.properties` in einem Texteditor.
2. Aktualisieren Sie Eigenschaften nach Bedarf. Eine Beschreibung der anpassbaren JAPI-Clienteigenschaften finden Sie in der folgenden Tabelle. Wenn eine gewünschte Eigenschaft nicht in der Datei `essbase.properties` enthalten ist, fügen Sie sie hinzu.

**Tabelle 2-7 SSL-Standardigenschaften für JAPI-Clients**

| Eigenschaft                                    | Beschreibung  |
|--|---|
| <code>olap.server.ssl.alwaysSecure</code>      | Legt den Modus fest, den Clients für alle Essbase-Instanzen verwenden sollen. Ändern Sie diesen Eigenschaftswert in <code>true</code> , um den SSL-Modus zu erzwingen.<br><b>Standardwert:</b> <code>false</code>   |
| <code>olap.server.ssl.securityHandler</code>   | Paketname für die Protokollverarbeitung. Sie können diesen Wert ändern, um einen anderen Handler anzugeben.<br><b>Standardwert:</b> <code>java.protocol.handler.pkgs</code>   |
| <code>olap.server.ssl.securityProvider</code>  | Oracle verwendet die Sun-SSL-Protokollimplementierung. Sie können diesen Wert ändern, um einen anderen Provider anzugeben.<br><b>Standardwert:</b> <code>com.sun.net.ssl.internal.www.protocol</code>   |
| <code>olap.server.ssl.supportedCiphers</code>  | Eine durch Komma getrennte Liste zusätzlicher Cipher, die für eine sichere Kommunikation aktiviert werden sollen. Sie dürfen nur Cipher angeben, die Essbase unterstützt.<br><b>Beispiel:</b><br><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>   |
| <code>olap.server.ssl.trustManagerClass</code> | Die TrustManager-Klasse zur Validierung des SSL-Zertifikats, indem die Signatur und das Ablaufdatum des Zertifikats geprüft werden. Standardmäßig ist diese Eigenschaft nicht festgelegt, um alle Verifizierungsprüfungen zu erzwingen. Wenn Verifizierungsprüfungen nicht erzwungen werden sollen, setzen Sie den Wert dieses Parameters auf <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> . Hierbei handelt es sich um die TrustManager-Standardklasse, mit der alle Verifizierungsprüfungen erfolgreich ausgeführt werden können.<br>Wenn Sie eine benutzerdefinierte TrustManager-Klasse implementieren möchten, geben Sie einen vollqualifizierten Klassennamen der TrustManager-Klasse an, mit der die Schnittstelle <code>javax.net.ssl.X509TrustManager</code> implementiert wird.<br><b>Beispiel:</b><br><code>com.essbase.services.olap.security.EssDefaultTrustManager</code> |

- Speichern und schließen Sie die Datei `essbase.properties`.
- Starten Sie alle Essbase-Komponenten neu.

## Sessionbasierte SSL-Verbindung herstellen

Oracle Essbase-Komponenten, wie z.B. MaxL, können SSL auf Sessionebene kontrollieren, indem eine Verbindung zum Essbase-Agent mit dem



Transportschlüsselwort `secure` hergestellt wird. Beispiel: Sie können eine sichere Verbindung zwischen MaxL und dem Essbase-Agent herstellen, indem Sie einen der folgenden Befehle über eine MaxL-Konsole ausführen:

```
login admin example_password on hostA:PORT:secure
```

```
login admin example_password on hostA:secure
```

Die sessionbasierte Kontrolle hat Vorrang vor Konfigurationseinstellungen in der Datei `essbase.cfg`. Wenn kein Transportschlüsselwort angegeben ist, verwenden Essbase-Clients den für `ClientPreferredMode` festgelegten Wert, um zu bestimmen, ob eine sichere Verbindung mit Essbase initiiert werden soll. Wenn die Einstellung `ClientPreferredMode` nicht auf "secure" gesetzt ist, erfolgt die Kommunikation über einen nicht sicheren Kanal.

# 3

## SSO mit Security Agents aktivieren

### Siehe auch:

- [Unterstützte SSO-Methoden](#)
- [Single Sign-On von Oracle Access Manager](#)
- [Single Sign-On für OracleAS](#)
- [EPM System-Produkte für SSO schützen](#)
- [Headerbasiertes SSO mit Identity Management-Produkten](#)
- [EPM System für headerbasiertes SSO mit Oracle Identity Cloud Services konfigurieren](#)
- [SSO für SiteMinder](#)
- [Single Sign-On für Kerberos](#)
- [EPM System für SSO konfigurieren](#)
- [Single Sign-On-Optionen für Smart View](#)

## Unterstützte SSO-Methoden

SSO erfordert, dass die Web Identity Management-Lösung den Anmeldenamen authentifizierter Benutzer an Oracle Enterprise Performance Management System-Produkte übergibt. Sie können die folgenden EPM System-Standardmethoden verwenden, um EPM System in kommerzielle und benutzerdefinierte webbasierte SSO-Lösungen zu integrieren.

- [HTTP-Header](#)
- [Benutzerdefinierte Anmeldeklasse](#)
- [HTTP-Autorisierungsheader](#)
- [Remote-Benutzer aus HTTP-Anforderung abrufen](#)
- [Headerbasierte Authentifizierung mit Identity Management-Produkten](#)

### ▲ **Achtung:**

Oracle empfiehlt als Sicherheitsmaßnahme, die Authentifizierung von Clientzertifikaten (wechselseitiger SSL) zwischen dem Webserver und dem Anwendungsserver zu implementieren, wenn Ihr Unternehmen Methoden verwendet, bei denen die Benutzeridentität zur Identitätspropagierung im Header enthalten ist.

### HTTP-Header

Wenn Sie Oracle Single Sign-On (OSSO), SiteMinder oder Oracle Access Manager als Web Identity Management-Lösung verwenden, wählt die EPM System-Sicherheit automatisch die

Option "Benutzerdefinierter HTTP-Header" aus, um den Anmeldenamen authentifizierter Benutzer an EPM System-Komponenten zu übergeben.

Der Anmeldeame eines EPM System-Produktbenutzers wird von `Login Attribute` festgelegt. Dieses Attribut wird bei der Konfiguration von Benutzerverzeichnissen in Oracle Hyperion Shared Services angegeben. Eine kurze Beschreibung zu `Login Attribute` finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

Der HTTP-Header muss den Wert des Attributs enthalten, das als `Anmeldeattribut` angegeben wurde. Beispiel: Wenn für `Login Attribute` der Wert `uid` angegeben ist, muss der HTTP-Header den Wert des Attributs `uid` enthalten.

Ausführliche Informationen zur Definition und Ausgabe von benutzerdefinierten HTTP-Headern finden Sie in der Dokumentation zu Ihrer Web Identity Management-Lösung.

Die EPM System-Sicherheit parst den HTTP-Header und validiert den enthaltenen Anmeldenamen anhand der in Shared Services konfigurierten Benutzerverzeichnisse.

### Benutzerdefinierte Anmeldeklasse

Wenn sich ein Benutzer anmeldet, authentifiziert die Web Identity Management-Lösung diesen Benutzer anhand eines Verzeichnisseservers. Sie kapselt die Zugangsdaten des authentifizierten Benutzers in einen SSO-Mechanismus, um SSO auch für Downstream-Systeme zu aktivieren. Verwendet die Web Identity Management-Lösung einen Mechanismus, der von EPM System-Produkten nicht unterstützt wird, oder ist der Wert von `Login Attribute` nicht im SSO-Mechanismus verfügbar, können Sie eine benutzerdefinierte Anmeldeklasse nutzen, um den Wert von `Login Attribute` abzuleiten und an EPM System-Produkte zu übergeben.

Bei Verwendung einer benutzerdefinierten Anmeldeklasse kann EPM System in Security Agents integriert werden, die eine auf X509-Zertifikaten basierende Authentifizierung verwenden. Wenn dieser Authentifizierungsmechanismus verwendet wird, müssen Shared Services-Standard-APIs implementiert werden, um die SSO-Schnittstelle zwischen EPM System-Komponenten und der Web Identity Management-Lösung zu definieren. Die benutzerdefinierte Anmeldeklasse muss den Wert des `Anmeldeattributs` an EPM System-Produkte übergeben. Eine kurze Beschreibung zu `Login Attribute` finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*. Einen Beispielcode und Implementierungsschritte finden Sie unter [Benutzerdefinierte Anmeldeklassen implementieren](#).

Um eine benutzerdefinierte Anmeldeklasse (Standardname `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`) verwenden zu können, muss eine Implementierung der Schnittstelle `com.hyperion.css.CSSSecurityAgentIF` im Classpath verfügbar sein. `CSSSecurityAgentIF` definiert die Methode zum Abrufen des Benutzernamens und des Kennworts (optional). Gibt die Schnittstelle ein Null-Kennwort zurück, sieht die Sicherheitsauthentifizierung den Anbieter als vertrauenswürdig an und verifiziert die Existenz des Benutzers für konfigurierte Anbieter. Unter Umständen wird von der Schnittstelle ein Wert für das Kennwort zurückgegeben, der nicht null ist. In diesem Fall versucht EPM System, die Anforderung unter Verwendung des von dieser Implementierung zurückgegebenen Benutzernamens und Kennworts zu authentifizieren.

CSSSecurityAgentIF umfasst zwei Methoden: `getUserName` und `getPassword`.

### **getUserName-Methode**

Diese Methode gibt den Benutzernamen für die Authentifizierung zurück.

```
java.lang.String getUserName(  
    javax.servlet.http.HttpServletRequest req,  
    javax.servlet.http.HttpServletResponse res)  
    throws java.lang.Exception
```

Der Parameter `req` identifiziert die HTTP-Anforderung, in der die Information enthalten ist, die zur Ermittlung des Benutzernamens benötigt wird. Der Parameter `res` wird nicht verwendet (ist aber für die Kompatibilität mit früheren Versionen bereits festgelegt).

### **getPassword-Methode**

Diese Methode gibt das Kennwort für die Authentifizierung in Klartext zurück. Der Kennwortabruf ist optional.

```
java.lang.String getPassword(  
    javax.servlet.http.HttpServletRequest req,  
    javax.servlet.http.HttpServletResponse res)  
    throws java.lang.Exception
```

Der Parameter `req` identifiziert die HTTP-Anforderung, in der die Information enthalten ist, die zur Ermittlung des Kennworts benötigt wird. Der Parameter `res` wird nicht verwendet (ist aber für die Kompatibilität mit früheren Versionen bereits festgelegt).

### **HTTP-Autorisierungsheader**

Die EPM System-Sicherheit unterstützt die Verwendung eines HTTP-Autorisierungsheaders, um den Wert von `Login Attribute` über Web Identity Management-Lösungen an EPM System-Produkte zu übergeben. EPM System-Produkte parsen den Autorisierungsheader, um den Anmeldenamen des Benutzers abzurufen.

### **Remote-Benutzer aus HTTP-Anforderung abrufen**

Die EPM System-Sicherheit unterstützt die Verwendung einer HTTP-Anforderung, um den Wert von `Login Attribute` über Web Identity Management-Lösungen an EPM System-Produkte zu übergeben. Verwenden Sie diese SSO-Methode, wenn die Web Identity Management-Lösung eine HTTP-Anforderung mit dem Wert von `Login Attribute` übergibt. Dieses Attribut wird mit der Funktion `setRemoteUser` festgelegt.

### **Headerbasierte Authentifizierung mit Identity Management-Produkten**

EPM System unterstützt beliebige Identity Management-Produkte, z.B. Oracle Identity Cloud Services, Microsoft Azure AD oder Okta, die die headerbasierte Authentifizierung unterstützen. Der konzeptionelle Workflow sieht wie folgt aus:

- Eine Gateway-Anwendung, die als Reverse-Proxy fungiert, schützt EPM System-Komponenten, indem nicht authentifizierter Netzwerkzugriff eingeschränkt wird.

- Die Gateway-Anwendung fängt HTTP(S)-Anforderungen an EPM System-Komponenten ab und stellt sicher, dass das Identity Management-Produkt Benutzer vor dem Weiterleiten der Anforderungen an EPM System-Komponenten authentifiziert.
- Die Gateway-Anwendung propagiert beim Weiterleiten der Anforderungen an EPM System-Komponenten die Identität des authentifizierten Benutzers an die EPM System-Komponente über HTTP-Headeranforderungen.

Damit dieses Authentifizierungsszenario unterstützt wird, muss EPM System so konfiguriert sein, dass es mit der über HTTP(S)-Anforderungen propagierten Identität des authentifizierten Benutzers arbeitet.

## Single Sign-On von Oracle Access Manager

Oracle Enterprise Performance Management System wird in Oracle Access Manager integriert, indem ein benutzerdefinierter HTTP-Header (Standardname `HYPLOGIN`) akzeptiert wird, der den Wert des Anmeldeattributs enthält. Das Anmeldeattribut wird festgelegt, wenn Sie ein externes Benutzerverzeichnis in Oracle Hyperion Shared Services konfigurieren. Eine kurze Beschreibung zu `Login Attribute` finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

Sie können einen beliebigen Headernamen verwenden, der EPM System den Wert des Anmeldeattributs bereitstellt. Sie verwenden den Headernamen bei der Konfiguration von Shared Services für SSO über Oracle Access Manager.

EPM System verwendet den Wert des Anmeldeattributs, um den Benutzer anhand eines konfigurierten Benutzerverzeichnisses zu authentifizieren (in diesem Fall das Benutzerverzeichnis, das Oracle Access Manager für die Benutzerauthentifizierung verwendet). Anschließend wird ein EPM-SSO-Token generiert, das SSO für EPM System aktiviert. Provisioning-Informationen des Benutzers werden in Native Directory geprüft, um den Benutzer für EPM System-Ressourcen zu autorisieren.

### Hinweis:

Die Oracle Essbase Administration Services-Konsole ist ein Thick Client und bietet keine SSO-Unterstützung über Oracle Access Manager.

Informationen zum Konfigurieren von Oracle Access Manager und zum Ausführen von Aufgaben, wie z.B. dem Einrichten von HTTP-Header und Policy-Domains, sind in der Dokumentation zu Oracle Access Manager verfügbar. In dieser Dokumentation wird angenommen, dass ein funktionsfähiges Oracle Access Manager-Deployment vorliegt, in dem Sie die folgenden Aufgaben ausgeführt haben:

- Die erforderlichen Policy-Domains für EPM System-Komponenten wurden eingerichtet.
- Ein HTTP-Header wurde erstellt, um den Wert des Anmeldeattributs an EPM System zu übergeben.

- Die unter [Zu schützende Ressourcen](#) aufgeführten EPM System-Ressourcen wurden geschützt. Anforderungen für den Zugriff auf geschützte Ressourcen werden von Oracle Access Manager überprüft.
- Für die unter [Ressourcen mit aufzuhebendem Schutz](#) aufgeführten EPM System-Ressourcen wurde der Schutz aufgehoben. Anforderungen für den Zugriff auf nicht geschützte Ressourcen werden von Oracle Access Manager nicht überprüft.

So konfigurieren Sie EPM System für SSO über Oracle Access Manager:

1. Fügen Sie das Benutzerverzeichnis, das Oracle Access Manager zur Benutzerauthentifizierung verwendet, als externes Benutzerverzeichnis in EPM System hinzu. Informationen hierzu finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

 **Hinweis:**

Stellen Sie sicher, dass das Kontrollkästchen **Vertrauenswürdig** im Fenster "Verbindungsinformationen" aktiviert ist, um anzugeben, dass das Benutzerverzeichnis eine vertrauenswürdige SSO-Quelle ist.

2. Konfigurieren Sie EPM System für SSO. Informationen hierzu finden Sie unter [EPM System für SSO konfigurieren](#).

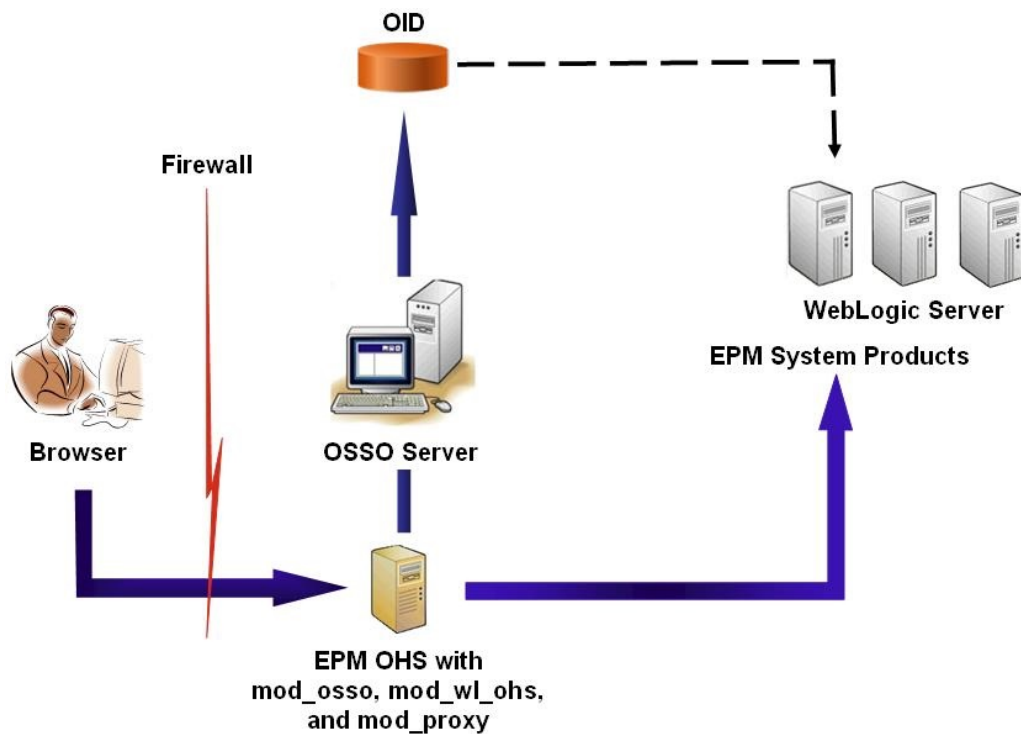
Wählen Sie Oracle Access Manager aus der Liste **SSO-Provider oder -Agent** aus. Wenn der HTTP-Header von Oracle Access Manager einen anderen Namen als `HYPLOGIN` verwendet, geben Sie den Namen des benutzerdefinierten Headers in das Textfeld neben der Liste **SSO-Mechanismus** ein.

3. Nur Oracle Data Relationship Management:
  - a. Konfigurieren Sie Data Relationship Management für die Shared Services-Authentifizierung.
  - b. Aktivieren Sie SSO in der Data Relationship Management-Konsole.  
Ausführliche Informationen finden Sie in der Dokumentation zu Data Relationship Management.

## Single Sign-On für OracleAS

Die OracleAS Single Sign-On-Lösung (OSSO) bietet SSO-Zugriff auf Webanwendungen, die Oracle Internet Directory (OID) als Benutzerverzeichnis verwenden. Benutzer melden sich mit einem in OID definierten Benutzernamen und Kennwort bei Oracle Enterprise Performance Management System-Produkten an.

### Prozessfluss



Der OSSO-Prozess:

1. Benutzer greifen über eine EPM System-URL, z.B. `http://OSSO_OHS_Server_NAME:OSSO_OHS_Server_PORT/interop/index.jsp`, auf eine EPM System-Komponente zu, die als geschützte OSSO-Anwendung definiert ist.
2. Da die URL durch OSSO geschützt ist, fängt `mod_osso` (auf Oracle HTTP Server bereitgestellt) die Anforderung ab. Oracle HTTP Server verwendet `mod_osso`, um zu prüfen, ob ein gültiges Cookie vorhanden ist. Wenn in der Anforderung kein gültiges Cookie verfügbar ist, werden Benutzer von Oracle HTTP Server an den OSSO-Server umgeleitet, der Benutzer nach Zugangsdaten fragt. Diese Zugangsdaten werden dann anhand von OID authentifiziert.
3. Der OSSO-Server erstellt `obSSOCookie` und gibt die Kontrolle an das Modul `mod_osso` auf dem Oracle HTTP Server zurück, der `obSSOCookie` im Browser festlegt. Außerdem wird die Anforderung über `mod_wl_ohs` (Oracle WebLogic Server) an die EPM System-Ressource umgeleitet. Bevor die Anforderung an eine EPM System-Ressource weitergeleitet wird, legt Oracle HTTP Server den Header `Proxy-Remote-User` fest, den die EPM System-Sicherheit zur Aktivierung von SSO verwendet.
4. Die EPM System-Komponente prüft, ob der Benutzer, dessen Identität von `Proxy-Remote-User` abgerufen wird, in OID vorhanden ist. Damit dieser Prozess funktioniert, muss das mit dem OSSO-Server konfigurierte OID als externes Benutzerverzeichnis in Oracle Hyperion Shared Services konfiguriert werden.

#### Voraussetzungen

1. Eine vollständig funktionsfähige Oracle Application Server-Infrastruktur.  
Um eine Oracle Application Server-Infrastruktur einzurichten, müssen Sie Oracle Identity Management Infrastructure 10.1.4 installieren und konfigurieren. Stellen Sie sicher, dass OSSO aktiviert ist. Die Installation von Oracle Identity

Management Infrastructure 10.1.4 umfasst die folgenden Komponenten zur Unterstützung von OSSO.

- Oracle 10g OSSO-Server.
- Ein OID, das der OSSO-Server zur Validierung von Zugangsdaten verwendet. Informationen hierzu finden Sie in den folgenden Dokumentationen:
  - *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
  - *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- Oracle HTTP Server als Frontend für den OSSO-Server. Diese Installation enthält `mod_osso`. Damit können Sie Partneranwendungen für OSSO definieren.

 **Hinweis:**

Die Oracle HTTP Server-Instanz ist Teil der OSSO-Infrastruktur. Sie wird nicht direkt zum Konfigurieren von OSSO für EPM System-Komponenten verwendet.

Stellen Sie während des Installationsprozesses sicher, dass `mod_osso` beim OSSO-Server als Partneranwendung registriert wird.

2. Ein vollständig funktionsfähiges EPM System-Deployment.  
Wenn Sie den Webserver für EPM System-Komponenten konfigurieren, konfiguriert EPM System Configurator `mod_wl_ohs.conf` auf Oracle HTTP Server, um Proxylanforderungen an WebLogic Server zu senden.

## Deployments testen

Stellen Sie nach Abschluss des SSL-Deployments sicher, dass alles funktioniert.

So testen Sie Deployments:

1. Rufen Sie über einen Browser die sichere Oracle Hyperion Enterprise Performance Management Workspace-URL auf:

Wenn Sie `epm.myCompany.com` als Serveralias für die externe Kommunikation und 4443 als SSL-Port verwendet haben, lautet die EPM Workspace-URL:

```
https://epm.myCompany.com:4443/workspace/index.jsp
```

2. Geben Sie im Anmeldefenster einen Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Prüfen Sie, ob ein sicherer Zugriff auf die bereitgestellten Oracle Enterprise Performance Management System-Komponenten möglich ist.

## OSSO für EPM System aktivieren

In diesem Abschnitt wird angenommen, dass Sie über eine vollständig konfigurierte OSSO-Infrastruktur verfügen. Informationen hierzu finden Sie in der Dokumentation *Oracle Application Server Administrator's Guide*.



## EPM System-Webserver als Partneranwendung registrieren

Sie verwenden das SSO-Registrierungstool von Oracle Identity Manager (`ssoreg.sh` oder `ssoreg.bat`), um den Oracle Enterprise Performance Management System-Webserver als Partneranwendung auf dem Oracle HTTP Server zu registrieren, der als Frontend für den OSSO-Server dient.

Führen Sie die folgenden Schritte auf dem Hostserver des Oracle HTTP Servers aus, der als Frontend für den OSSO-Server dient. Bei diesem Prozess wird die obfuskierte Datei `osso.conf` an einem Speicherort Ihrer Wahl generiert und gespeichert.

So registrieren Sie den EPM System-Webserver als Partneranwendung:

1. Öffnen Sie eine Konsole auf dem Hostserver des Oracle HTTP Servers, der als Frontend für den OSSO-Server dient, und navigieren Sie zum Verzeichnis `ORACLE_HOME/sso/bin` des Oracle HTTP Servers, z.B. `C:\OraHome_1\sso/bin` (Windows).
2. Führen Sie einen Befehl wie den folgenden mit der Option `-remote_midtier` aus:

```
ssoreg.bat -site_name epm.myCompany.com
-mod_osso_url http://epm.myCompany.com:19400
-config_mod_osso TRUE
-update_mode CREATE
-remote_midtier
-config_file C:\OraHome_1\myFiles\osso.conf
```

Im Folgenden werden die in diesem Befehl verwendeten Parameter erläutert. In dieser Beschreibung bezieht sich die Partneranwendung auf den Oracle HTTP Server, der als EPM System-Webserver verwendet wird.

- `-site_name` gibt die Website der Partneranwendung an, z.B. `epm.myCompany.com`.
- `-mod_osso_url` gibt die Partneranwendungs-URL im Format `PROTOCOL://HOST_NAME:PORT` an. Über diese URL akzeptiert der EPM System-Webserver eingehende Clientanforderungen, wie z.B. `http://epm.myCompany.com:19000`.
- `-config_mod_osso` gibt an, dass die Partneranwendung `mod_osso` verwendet. Sie müssen den Parameter `config_mod_osso` einschließen, um `osso.conf` zu generieren.
- `-update_mode` gibt den Aktualisierungsmodus an. Verwenden Sie den Standardparameter `CREATE`, um einen neuen Datensatz zu erstellen.
- `-remote_midtier` gibt an, dass sich die Partneranwendung `mod_osso` auf einer Remote-Middle-Tier befindet. Verwenden Sie diese Option, wenn sich die Partneranwendung in einem anderen `ORACLE_HOME`-Verzeichnis befindet als der OSSO-Server.
- `-virtualhost` gibt an, dass es sich bei der Partneranwendungs-URL um einen virtuellen Host handelt. Verwenden Sie diesen Parameter nur bei einem virtuellen Host.  
Wenn Sie eine Partneranwendungs-URL registrieren, die an einen virtuellen Host gebunden ist, müssen Sie den virtuellen Host in der Datei `httpd.conf` definieren. Informationen hierzu finden Sie unter [Optional: Virtuelle Hosts definieren](#).

- `-config_file` gibt den Pfad an, in dem die Datei `osso.conf` generiert werden soll.

### Optional: Virtuelle Hosts definieren

Wenn Sie bei der Registrierung der Partneranwendung die URL eines virtuellen Hosts verwendet haben, müssen Sie den virtuellen Host definieren, indem Sie die Datei `httpd.conf` auf dem Oracle HTTP Server aktualisieren, der als EPM System-Webserver verwendet wird.

So definieren Sie virtuelle Hosts:

1. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf` mit einem Texteditor.
2. Fügen Sie eine Definition wie die folgende hinzu. Bei dieser Definition wird angenommen, dass der Webserver auf dem virtuellen Server `epm.myCompany.com` am Port `epm.myCompany.com:19400` ausgeführt wird. Passen Sie die Einstellungen entsprechend Ihren jeweiligen Anforderungen an.

```
NameVirtualHost epm.myCompany.com:19400
Listen 19400
<VirtualHost epm.myCompany.com:19400>
DocumentRoot "C:/Oracle/Middleware/user_projects/epmsystem1/httpConfig/ohs
/config/OHS/ohs_component/private-docs"
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}
/${COMPONENT_NAME}/mod_osso.conf"
</VirtualHost>
```

### mod\_osso.conf erstellen

Erstellen Sie `mod_osso.conf` auf dem Oracle HTTP Server, der als Frontend für den EPM System-Webserver dient.

So erstellen Sie `mod_osso.conf`:

1. Verwenden Sie einen Texteditor, um eine Datei zu erstellen.
2. Kopieren Sie den folgenden Inhalt in die Datei, und ändern Sie sie für Ihre Umgebung.

```
LoadModule osso_module C:/Oracle/Middleware/ohs/ohs/modules/mod_osso.so
<IfModule mod_osso.c>
    OsoIpCheck off
    OsoIdleTimeout off
    OsoSecureCookies off
    OsoConfigFile C:/Oracle/Middleware/user_projects/epmsystem1/
httpConfig/
    ohs/config/OHS/ohs_component/osso/osso.conf
```

3. Fügen Sie in der Definition `<IfModule mod_osso.c` Speicherortdefinitionen wie die folgenden ein, um die einzelnen Ressourcen zu identifizieren, die mit OSSO geschützt werden sollen.

```
<Location /interop/>
    require valid user
    AuthType Oso
</Location>
</IfModule>
```

4. Speichern Sie die Datei unter `mod_osso.conf`.

#### Speicherort von `osso.conf` ändern

Bei der Registrierung des EPM System-Webserver als Partneranwendung (siehe [EPM System-Webserver als Partneranwendung registrieren](#)) wird die obfuskierte Datei `osso.conf` an dem von der Anweisung `-config_file` angegebenen Speicherort erstellt.

So ändern Sie den Speicherort von `osso.conf`:

1. Suchen Sie die Datei `osso.conf`, die bei der Registrierung des EPM System-Webserver als Partneranwendung erstellt wurde (siehe [EPM System-Webserver als Partneranwendung registrieren](#)).
2. Kopieren Sie `osso.conf` in das Verzeichnis (auf dem Oracle HTTP Server, der als Frontend für den OSSO-Server dient), das von der in der Datei `mod_osso.conf` definierten Eigenschaft `OssosConfigFile` angegeben ist (siehe [mod\\_osso.conf erstellen](#)).

#### EPM System für OSSO konfigurieren

Konfigurieren Sie das in der OSSO-Lösung integrierte Verzeichnis OID als externes Benutzerverzeichnis in EPM System, und aktivieren Sie anschließend SSO.

So konfigurieren Sie EPM System für OSSO:

1. Konfigurieren Sie das Verzeichnis OID der OSSO-Lösung als externes Benutzerverzeichnis. Informationen hierzu finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.
2. Aktivieren Sie SSO in EPM System. [EPM System für SSO konfigurieren](#)

#### Hinweis:

Um OSSO als Identity Management-Lösung zu konfigurieren, müssen Sie unter **SSO-Provider oder -Agent** die Option `Other` und unter **SSO-Mechanismus** die Option `Custom HTTP Header` auswählen und dann `Proxy-Remote-User` als Namen für den benutzerdefinierten HTTP-Header eingeben.

3. Weisen Sie mindestens einem OID-Benutzer die Rolle des Oracle Hyperion Shared Services-Administrators zu.
4. Starten Sie EPM System-Produkte sowie benutzerdefinierte Anwendungen neu, die Sicherheits-APIs von Shared Services verwenden.

#### Hinweis:

Stellen Sie sicher, dass das mit Shared Services konfigurierte Verzeichnis OID ausgeführt wird, bevor Sie EPM System-Produkte starten.

### Optional: Debugging-Meldungen auf dem OSSO-Server aktivieren

Um Debugging-Meldungen auf dem OSSO-Server zu erfassen, ändern Sie die Datei `policy.properties`. Debugging-Meldungen werden in die Datei `ORACLE_HOME/sso/log/ssoServer.log` geschrieben.

So erfassen Sie Debugging-Meldungen:

1. Öffnen Sie die Datei `ORACLE_HOME/sso/conf/policy.properties`, z.B. `C:\OraHome_1\sso\conf\policy.properties`, auf dem OSSO-Server mit einem Texteditor.
2. Setzen Sie den Wert der Eigenschaft `debugLevel` auf "DEBUG".

```
debugLevel = DEBUG
```

3. Speichern und schließen Sie die Datei `policy.properties`.

### Optional: Debugging-Meldungen für geschützte Ressourcen aktivieren

Um OSSO-Debugging-Meldungen für geschützte Ressourcen mit `mod_osso.conf` zu erfassen, ändern Sie die Datei `httpd.conf` auf dem EPM System-Webserver. Debugging-Meldungen werden in die Datei `EPM_ORACLE_INSTANCE/httpConfig/ohs/diagnostics/logs/OHS/ohs_component/ohs_component.log` geschrieben.

So erfassen Sie Debugging-Meldungen für geschützte Ressourcen:

1. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf` mit einem Texteditor.
2. Setzen Sie den Wert der Eigenschaft `OraLogSeverity` auf "TRACE".

```
OraLogSeverity TRACE:32
```

3. Speichern und schließen Sie die Datei `httpd.conf`.

## EPM System-Produkte für SSO schützen

Sie müssen Oracle Enterprise Performance Management System-Ressourcen schützen, damit SSO-Anforderungen von Benutzern an den Security Agent (OAM, OSSO oder SiteMinder) umgeleitet werden.

Oracle HTTP Server leitet Benutzer mit `mod_osso` an den OSSO-Server weiter. Benutzer werden nur dann weitergeleitet, wenn die angeforderten URLs für den Schutz in `mod_osso` konfiguriert sind. Informationen hierzu finden Sie unter [Sicherheit verwalten](#) in der Dokumentation *Oracle HTTP Server Administrator's Guide*.

Informationen zum Ressourcenschutz für SiteMinder SSO entnehmen Sie der SiteMinder-Dokumentation.

### Nur OAM: Hinzufügen von Standardheadern zu Antworten verhindern

OAM fügt geschützten URLs standardmäßig zwei Header hinzu: `Pragma: no-cache` und `Cache-Control: no-cache`. Da diese Header mit ähnlichen Cachingrichtlinien in Konflikt stehen, die von EPM System und Webanwendungen hinzugefügt wurden, cachen Browser

möglicherweise nicht den Inhalt der geschützten URLs, was zu einer langsameren Performance führt.

Ausführliche Informationen zum Verhindern, dass diese OAM-Header Antworten hinzugefügt werden, finden Sie im Abschnitt zum Optimieren von OAM-Agents im Abschnitt [Oracle Access Management-Performanceoptimierung](#) der Dokumentation *Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

### Zu schützende Ressourcen

In der folgenden Tabelle sind die Kontexte aufgelistet, die geschützt werden müssen. Syntax zum Schützen einer Ressource (z.B. mit `interop`) für OSSO:

```
<Location /interop>
Require valid-user
AuthType Basic
order deny,allow
deny from all
allow from myServer.myCompany.com
satisfy any
</Location>
```

Der Parameter `allow from` gibt die Server an, mit denen der Kontextschutz umgangen werden kann.

Für Oracle Hyperion Enterprise Performance Management Workspace und Oracle Hyperion Financial Reporting müssen Sie nur die Parameter festlegen, die im folgenden Beispiel angegeben sind:

```
<Location /workspace>
Require valid-user
AuthType Basic
</Location>
```

**Tabelle 3-1 EPM System - Zu schützende Ressourcen**

| EPM System-Produkt                     | Zu schützender Kontext   |
|--|--|
| Oracle Hyperion Shared Services        | <ul style="list-style-type: none"> <li>/interop</li> <li>/interop/.../*</li> </ul>                   |
| EPM Workspace                          | <ul style="list-style-type: none"> <li>/workspace</li> <li>/workspace/.../*</li> </ul>               |
| Financial Reporting                    | <ul style="list-style-type: none"> <li>/hr</li> <li>/hr/.../*</li> </ul>                             |
| Oracle Hyperion Planning               | <ul style="list-style-type: none"> <li>/HyperionPlanning</li> <li>/HyperionPlanning/.../*</li> </ul> |
| Oracle Integrated Operational Planning | <ul style="list-style-type: none"> <li>/interlace</li> <li>/interlace/.../*</li> </ul>               |

**Tabelle 3-1 (Fortsetzung) EPM System - Zu schützende Ressourcen**

| <b>EPM System-Produkt</b>   | <b>Zu schützender Kontext</b>   |
|---|---|
| Oracle Hyperion Financial Management                                  | <ul style="list-style-type: none"> <li>• /hfmadf</li> <li>• /hfmadfe/.../*</li> <li>• /hfmoofficeprovider</li> <li>• /hfmoofficeprovider/.../*</li> <li>• /hfmsmartviewprovider</li> <li>• /hfmsmartviewprovider/.../*</li> </ul> |
| Oracle Hyperion Financial Reporting Web Studio                        | /frdesigner/**  |
| Oracle Data Relationship Management                                   | <ul style="list-style-type: none"> <li>• /drm-web-client</li> <li>• /drm-web-client/.../*</li> </ul>  |
| Oracle Essbase Administration Services                                | <ul style="list-style-type: none"> <li>• /hbrlauncher</li> <li>• /hbrlauncher/.../*</li> </ul>  |
| Oracle Hyperion Financial Data Quality Management                     | <ul style="list-style-type: none"> <li>• /HyperionFDM</li> <li>• /HyperionFDM/.../*</li> </ul>  |
| Oracle Hyperion Calculation Manager                                   | <ul style="list-style-type: none"> <li>• /calcmgr</li> <li>• /calcmgr/.../*</li> </ul>  |
| Oracle Hyperion Provider Services                                     | <ul style="list-style-type: none"> <li>• /aps</li> <li>• /aps/.../*</li> </ul>  |
| Oracle Hyperion Profitability and Cost Management                     | <ul style="list-style-type: none"> <li>• /profitability</li> <li>• /profitability/.../*</li> </ul>  |
| Account Reconciliation Manager  | <ul style="list-style-type: none"> <li>• /arm</li> <li>• /arm/.../*</li> </ul>  |
| Oracle Hyperion Financial Close Management                            | <ul style="list-style-type: none"> <li>• /fcc</li> <li>• /fcc/.../*</li> </ul>  |
| Oracle Hyperion Financial Data Quality Management, Enterprise Edition | <ul style="list-style-type: none"> <li>• /aif</li> <li>• /aif/.../*</li> </ul>  |
| Oracle Hyperion Tax Governance Tax Operations                         | /tss<br>/taxop  |
| Oracle Hyperion Tax Provision Supplemental Data Manager               | /taxprov<br><ul style="list-style-type: none"> <li>• /sdm*</li> <li>• /sdm/**</li> <li>• /sdm/./**</li> <li>• /SDM-Datamodel-context-root/**</li> </ul>   |
| Oracle Essbase  | <ul style="list-style-type: none"> <li>• /essbase/.../*</li> <li>• /essbase/**</li> <li>• /essbase*</li> </ul>  |

**Ressourcen mit aufzuhebendem Schutz**

In der folgenden Tabelle sind die Kontexte aufgelistet, deren Schutz aufgehoben werden muss. Die Syntax zum Aufheben des Schutzes einer Ressource (mit /interop/framework(.\*) als Beispiel) für OSSO lautet:

```
<LocationMatch /interop/framework(.*)>
  Require valid-user
  AuthType Basic
```

```

allow from all
satisfy any
</LocationMatch>

```

**Tabelle 3-2 EPM System - Ressourcen mit aufgehobenem Schutz**

| EPM System-Produkt | Kontexte mit aufzuhebendem Schutz  |
|--------------------|--|
| Shared Services    | <ul style="list-style-type: none"> <li>• /interop/framework</li> <li>• /interop/framework*</li> <li>• /interop/framework.*</li> <li>• /interop/framework/.../*</li> <li>• /interop/Audit</li> <li>• /interop/Audit*</li> <li>• /interop/Audit.*</li> <li>• /interop/Audit/.../*</li> <li>• /interop/taskflow</li> <li>• /interop/taskflow*</li> <li>• /interop/taskflow/.../*</li> <li>• /interop/WorkflowEngine</li> <li>• /interop/WorkflowEngine/*</li> <li>• /interop/WorkflowEngine/.../*</li> <li>• /interop/TaskReceiver</li> <li>• /framework/lcm/HSSMigration</li> </ul>  |
| EPM Workspace      | <ul style="list-style-type: none"> <li>• /epmstatic/.../*</li> <li>• /workspace/bpmstatic/.../*</li> <li>• /workspace/static/.../*</li> <li>• /workspace/cache/.../*</li> </ul>  |
| Planning           | <ul style="list-style-type: none"> <li>• /HyperionPlanning/Smartview</li> <li>• /HyperionPlanning/faces/PlanningCentral</li> <li>• /HyperionPlanning/servlet/<br/>HspDataTransfer</li> <li>• /HyperionPlanning/servlet/HspLCMServlet</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet/.../*</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet/**</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet*</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet/.../*</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet/**</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet*</li> </ul> |

**Tabelle 3-2 (Fortsetzung) EPM System - Ressourcen mit aufgehobenem Schutz**

| EPM System-Produkt                                  | Kontexte mit aufzuhebendem Schutz  |
|---|--|
| Financial Reporting                                 | <ul style="list-style-type: none"> <li>• /hr/common/HRLogon.jsp</li> <li>• /hr/services</li> <li>• /hr/services/*</li> <li>• /hr/services/.../*</li> <li>• /hr/modules/com/hyperion/reporting/web/reportViewer/HRStaticReport.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/repository/HRObjectListXML.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/reportViewer/HRHtmlReport.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookTOCFns.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookPdf.jsp</li> </ul> |
| Data Relationship Management<br>Calculation Manager | /drm-migration-client <ul style="list-style-type: none"> <li>• /calcmgr/importexport.postExport.do</li> <li>• /calcmgr/common.performAction.do</li> <li>• /calcmgr/lcm.performAction.do*</li> <li>• /calcmgr/lcm.performAction.do/*</li> </ul>   |
| Administration Services                             | <ul style="list-style-type: none"> <li>• /eas</li> <li>• /easconsole</li> <li>• /easdocs</li> </ul>  |
| Financial Management                                | <ul style="list-style-type: none"> <li>• /hfm/EIE/EIEListener.asp</li> <li>• /hfmapplicationsservice</li> <li>• /oracle-epm-fm-webservices</li> <li>• /hfmlcmsservice</li> </ul>   |
| Financial Close Management                          | <ul style="list-style-type: none"> <li>• /FCC-DataModel-context-root</li> <li>• /oracle-epm-erpi-webservices/*</li> <li>• /ARM-DataModel-context-root</li> <li>• /oracle-epm-erpi-webservices/**</li> <li>• /arm/batch/armbatchexecutionservlet</li> <li>• /ARM-DataModel-context-root</li> </ul>  |



**Tabelle 3-2 (Fortsetzung) EPM System - Ressourcen mit aufgehobenem Schutz**

| EPM System-Produkt                | Kontexte mit aufzuhebendem Schutz   |
|-----------------------------------|---|
| Integrated Operational Planning   | <ul style="list-style-type: none"> <li>• /interlace/services/</li> <li>• /interlace/services/*</li> <li>• /interlace/services.*</li> <li>• /interlace/services/.../*</li> <li>• /interlace/anteros</li> <li>• /interlace/anteros/*</li> <li>• /interlace/anteros.*</li> <li>• /interlace/anteros/.../*</li> <li>• /interlace/interlace</li> <li>• /interlace/interlace/*</li> <li>• /interlace/interlace.*</li> <li>• /interlace/interlace/.../*</li> <li>• /interlace/WebHelp</li> <li>• /interlace/WebHelp/*</li> <li>• /interlace/WebHelp.*</li> <li>• /interlace/WebHelp/.../*</li> <li>• /interlace/html</li> <li>• /interlace/html/*</li> <li>• /interlace/html.*</li> <li>• /interlace/html/.../*</li> <li>• /interlace/email-book</li> <li>• /interlace/email-book/*</li> <li>• /interlace/email-book.*</li> <li>• /interlace/email-book/.../*</li> </ul> |
| Profitability and Cost Management | <ul style="list-style-type: none"> <li>• /profitability/cesagent</li> <li>• /profitability/lcm</li> <li>• /profitability/control</li> <li>• /profitability/ApplicationListener</li> <li>• /profitability/HPMApplicationListener</li> </ul>  |
| Oracle Essbase                    | <ul style="list-style-type: none"> <li>• /essbase/agent/.../*</li> <li>• /essbase/jet/logout.html</li> <li>• /essbase/jet/.\.(js   css   gif   jpe?g   png)\$</li> </ul>  |
| FDMEE                             | <ul style="list-style-type: none"> <li>• /aif/services/FDMRuleService</li> <li>• /aif/services/RuleService</li> <li>• /aif/LCMServlet</li> </ul>  |

## Headerbasiertes SSO mit Identity Management-Produkten

### Voraussetzungen

- Ein vollständig konfiguriertes Oracle Enterprise Performance Management System-Produkt. Der Verzeichnisserver des Identity Management-Produkts muss in EPM System als Benutzerverzeichnis zur Autorisierung von Benutzern konfiguriert sein.
- Ein vollständig konfiguriertes Identity Management-Produkt (Microsoft Azure AD, Okta usw.), das die headerbasierte Authentifizierung unterstützt.

Die folgenden generischen Prozesse sind an der Konfiguration von EPM System für headerbasiertes SSO mit einem kompatiblen Identity Management-Produkt beteiligt. Da die konkreten Schritte vom verwendeten Produkt abhängig sind, finden Sie die ausführliche Vorgehensweise in der Dokumentation zu Ihrem Identity Management-Produkt.

Ausführliche Schritte zum Konfigurieren der headerbasierten Authentifizierung mit Oracle Identity Cloud Services finden Sie unter [EPM System für headerbasiertes SSO mit Oracle Identity Cloud Services konfigurieren](#).

1. Registrieren Sie EPM System als Enterprise-Anwendung im Identity Management-Produkt. Mit diesem Schritt kann der Identity Management-Administrator die Authentifizierung in der Enterprise-Anwendung einschließlich unterstützter Funktionen, wie Multifaktor-Authentifizierung, konfigurieren.  
Verwenden Sie den vollständig qualifizierten Domainnamen (FQDN) des Gateways ergänzt mit `workspace/index.jsp` (Beispiel: `https://gateway.server.example.com:443/workspace/index.jsp`) als Enterprise-Anwendungs-URL für EPM System.

Konfigurieren Sie die Enterprise-Anwendung von EPM System, um einen HTTP-Header zu propagieren.

Sie können jeden nicht reservierten Headernamen als Namen für den HTTP-Header verwenden. Bei dem Wert des Headers muss es sich um die Eigenschaft handeln, die EPM System-Benutzer eindeutig identifiziert.

2. Installieren, konfigurieren und registrieren Sie ein Anwendungs-Gateway, um sicherzustellen, dass die Enterprise-Anwendung nur authentifizierte Anforderungen an EPM System weiterleitet.  
Verwenden Sie die folgenden Konfigurationseinstellungen:
  - FQDN des Gateway-Servers (Beispiel: `gateway.server.example.com:443`) als Zugriffspunkt.
  - FQDN von EPM System (Beispiel: `epm.server.example.com:443`) als Ressource, an die authentifizierte HTTP(S)-Anforderungen weitergeleitet werden sollen.
3. Aktivieren Sie SSO in EPM System, um HTTP(S)-Header vom Anwendungs-Gateway zu berücksichtigen. Ausführliche Informationen finden Sie unter [Sicherheitsoptionen festlegen](#).  
So aktivieren Sie SSO:
  - a. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
  - b. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
  - c. Klicken Sie auf **Sicherheitsoptionen**.
  - d. Führen Sie im Abschnitt **SSO-Konfiguration** die folgenden Schritte aus:
    - i. Aktivieren Sie das Kontrollkästchen **SSO aktivieren**.
    - ii. Wählen Sie in der Dropdown-Liste für den SSO-Provider oder Security Agent die Option **Sonstige** aus.
    - iii. Wählen Sie in der Dropdown-Liste **SSO-Mechanismus** die Option **Benutzerdefinierter HTTP-Header** aus, und geben Sie den Namen des Headers an, den der Sicherheitsagent an EPM System übergibt.
  - e. Klicken Sie auf **OK**.

4. Aktualisieren Sie die Einstellung "Abmelde-URL bereitstellen" in Oracle Hyperion Enterprise Performance Management Workspace in die Einstellung auf der Webseite, die Benutzern bei der Abmeldung von EPM System angezeigt werden soll.  
So aktualisieren Sie die Einstellung "Abmelde-URL bereitstellen" in EPM Workspace:
  - a. Greifen Sie als Systemadministrator auf EPM Workspace zu. Informationen hierzu finden Sie unter [Auf EPM Workspace zugreifen](#).
  - b. Wählen Sie **Navigieren, Workspace-Einstellungen, Servereinstellungen** aus.
  - c. Ändern Sie unter **Workspace Server-Einstellungen** unter **Abmelde-URL bereitstellen** die URL der Webseite, die Benutzern bei der Abmeldung von EPM System angezeigt werden soll.
  - d. Klicken Sie auf **OK**.
5. Starten Sie Oracle Hyperion Foundation Services und alle verwalteten Server von EPM System neu.

## EPM System für headerbasiertes SSO mit Oracle Identity Cloud Services konfigurieren

In diesem Szenario authentifiziert Oracle Identity Cloud Services Oracle Enterprise Performance Management System-Benutzer und propagiert die erforderlichen HTTP-Header, um SSO zu aktivieren.

In diesem Abschnitt werden die Schritte zum Einrichten und Konfigurieren von EPM System zur Unterstützung von SSO mit Oracle Identity Cloud Services erläutert. Sie können diese Schritte ableiten, um die headerbasierte Authentifizierung von EPM System mit einem beliebigen Identity Management-System (z.B. Azure AD) oder einem Infrastructure-as-a-Service-(IaaS)-Provider zu unterstützen, der die headerbasierte Authentifizierung unterstützt.

Der konzeptionelle Workflow sieht wie folgt aus:

- Eine Gateway-Anwendung, die als Reverse-Proxy fungiert, schützt EPM System-Komponenten, indem nicht authentifizierter Netzwerkzugriff eingeschränkt wird.
- Die Gateway-Anwendung fängt HTTP(S)-Anforderungen an EPM System-Komponenten ab und stellt sicher, dass das Identity Management-Produkt Benutzer vor dem Weiterleiten der Anforderungen an EPM System-Komponenten authentifiziert.
- Die Gateway-Anwendung propagiert beim Weiterleiten der Anforderungen an EPM System-Komponenten die Identität des authentifizierten Benutzers an die EPM System-Komponente über HTTP-Headeranforderungen.

### Voraussetzungen und Beispiel-URLs

So richten Sie headerbasiertes SSO mit Oracle Identity Cloud Services ein:

- Ein vollständig konfiguriertes Oracle Enterprise Performance Management System-Produkt.

- Ein Host oder Container mit einem vollständig konfigurierten Oracle App-Gateway, der als Reverse-Proxy zum Schutz von EPM System fungiert, indem nicht autorisierter Zugriff eingeschränkt wird.  
Das Oracle App-Gateway muss so konfiguriert sein, dass HTTP-Anforderungen für EPM System -Komponenten abgefangen werden. Außerdem muss sichergestellt werden, dass Benutzer von Oracle Identity Cloud Services authentifiziert werden, bevor Anforderungen an EPM System weitergeleitet werden. Das Oracle App-Gateway muss beim Weiterleiten der Anforderungen an EPM System-Komponenten die Identität des authentifizierten Benutzers über HTTP-Headeranforderungen propagieren.
- Domainadministratorzugriff auf Oracle Identity Cloud Services.

In dieser Beschreibung werden die folgenden Beispiel-URLs verwendet:

- Basis-URL des vollständig qualifizierten Domainnames (FQDN) des Oracle Identity Cloud Services-Servers (Identitätsprovider):  
`https://identity.server.example.com:443/`
- FQDN des Oracle App-Gateway-Servers (der die Gateway-Anwendung hostet):  
`https://gateway.server.example.com:443/`
- Enterprise-Anwendungs-URL für EPM System. Hierbei handelt es sich um die FQDN des Oracle App-Gateway-Servers ergänzt mit `workspace/index.jsp`:  
`https://gateway.server.example.com:443/workspace/index.jsp`



#### Note:

Oracle Identity Cloud Services und Oracle App-Gateway sind mit HTTPS-Unterstützung konfiguriert. Die Unterstützung von HTTPS für EPM System ist optional. Diese Beschreibung geht davon aus, dass EPM System mit HTTPS-Unterstützung konfiguriert wurde.

## Headerbasierte Authentifizierung für EPM System aktivieren

Das Aktivieren der headerbasierten Authentifizierung für Oracle Enterprise Performance Management System umfasst die folgenden Schritte:

- [EPM System-Anwendung und -Gateway zu Oracle Identity Cloud Services hinzufügen](#)
- [App-Gateway konfigurieren](#)
- [Benutzerverzeichnisse für Autorisierung konfigurieren](#)
- [SSO in EPM System aktivieren](#)
- [EPM Workspace-Einstellungen aktualisieren](#)

## Anwendung und Gateway von EPM System zu Oracle Identity Cloud Services hinzufügen

Um die headerbasierte Authentifizierung einzurichten, müssen Sie Oracle Enterprise Performance Management System als Enterprise-Anwendung erstellen.

## EPM System als Enterprise-Anwendung in Oracle Cloud Identity Console hinzufügen

So fügen Sie EPM System als Enterprise-Anwendung hinzu:

1. Greifen Sie als Domainadministrator auf Oracle Cloud Identity Console zu.
  - a. Navigieren Sie in einem Browser zu <https://www.oracle.com/cloud/sign-in.html>.
  - b. Geben Sie Ihren Oracle Fusion Cloud EPM-Accountnamen ein.
  - c. Geben Sie auf der Oracle Fusion Cloud EPM-Accountanmeldeseite Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf **Anmelden**.
  - d. Klicken Sie im **Slide-in-Menü** auf **Benutzer** und anschließend auf die Option für die primäre Identität.
  - e. Klicken Sie auf die Option für die Identity-Konsole.
2. Fügen Sie EPM System als Enterprise-Anwendung hinzu.
  - a. Klicken Sie im Slide-in-Menü auf **Anwendungen**.
  - b. Klicken Sie auf **Hinzufügen, Enterprise-Anwendung**.

The screenshot shows the Oracle Identity Cloud Service console interface. On the left is a dark sidebar with navigation options: Dashboard, Users, Groups, Applications (highlighted), Oracle Cloud Services, Jobs, Reports, Settings, and Security. The main content area is titled 'Add Enterprise Application' and features a progress bar with three steps: 1. Details (active), 2. OAuth Configuration, and 3. SSO Configuration. Below the progress bar, the 'Details' section contains several input fields: 'Name' (EPM System), 'Description' (On-Premises EPM 11.2), 'Application Icon' (with an upload button), 'Application URL' (r.example.com:443/workspace/index.jsp), 'Custom Login URL', 'Custom Logout URL', 'Custom Error URL', and 'Linking callback URL'. Below these fields is a 'Tags' section with an 'Add Tag' button and a note: 'Add tags to your applications to organize and identify them. A tag consists of a key-value pair.' At the bottom, the 'Settings' section has three checkboxes: 'Display in My Apps' (checked), 'User can request access' (unchecked), and 'User must be granted the app' (unchecked). The top right of the console shows 'License Type :: Foundation' and 'Cookie Preferences'.

3. Fügen Sie Anwendungsdetails hinzu:
  - a. Geben Sie unter **Name** einen eindeutigen Namen ein, um die Enterprise-Anwendung von EPM System zu identifizieren.
  - b. Geben Sie optional eine Beschreibung ein.

- c. Laden Sie optional ein Anwendungssymbol für EPM System hoch. Klicken Sie auf **Hochladen**, um das Symbol auszuwählen und hochzuladen.
  - d. Geben Sie unter **Anwendungs-URL** die Start-URL ein, an die das Gateway die Benutzer weiterleiten soll. Bei dieser URL handelt es sich um die FQDN des Oracle App-Gateways ergänzt mit `workspace/index.jsp`. Bei dieser Ergänzung handelt es sich um den EPM System-Anwendungskontext.
  - e. Wählen Sie unter **Einstellungen** die Option **Unter "Meine Apps anzeigen"** aus, um die EPM System-Enterprise-Anwendung in der Registerkarte **SSO-Konfiguration** auf der Seite **Meine Apps** in Oracle Cloud Identity Console anzuzeigen.
  - f. Klicken Sie auf **Weiter**.
4. Geben Sie SSO-Konfigurationsdetails an.
    - a. Klicken Sie auf **SSO-Konfiguration**.
    - b. Fügen Sie eine Ressource für die Enterprise-Anwendung hinzu. Blenden Sie unter **SSO-Konfiguration** die Option **Ressourcen** ein.
      - i. Klicken Sie auf **Hinzufügen**.

The screenshot shows a dialog box titled "Add Resource" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Resource Name:** A text input field containing "EPM".
- Resource URL:** A text input field containing "/.\*".
- URL Query String:** An empty text input field.
- Regex:** A checkbox that is checked.
- Description:** An empty text area with a small icon in the bottom right corner.
- OK:** A blue button in the bottom right corner.

- ii. Geben Sie einen eindeutigen Ressourcennamen an.
  - iii. Geben Sie unter **Ressourcen-URL** den Wert `/.*` ein.
  - iv. Aktivieren Sie das Kontrollkästchen **Regulärer Ausdruck**.
  - v. Klicken Sie auf **OK**.
  - vi. Blenden Sie unter **SSO-Konfiguration** die Option **Ressourcen** ein.
- c. Fügen Sie eine Authentifizierungs-Policy hinzu. Blenden Sie unter **SSO-Konfiguration** die Option **Authentifizierungs-Policy** ein.
    - i. Aktivieren Sie die Kontrollkästchen **CORS zulassen** und **Sichere Cookies erforderlich**.
    - ii. Klicken Sie auf **Hinzufügen** unter **Verwaltete Ressourcen**, und definieren Sie **Formular oder Zugriffstoken** als Authentifizierungsmethode für die SSO-Ressource.

| Name     | Value      |
|----------|------------|
| HYPLOGIN | Work Email |

- iii. Wählen Sie unter **Ressource** die SSO-Ressource aus, die Sie im vorherigen Schritt hinzugefügt haben.
  - iv. Blenden Sie **Header** ein.
  - v. Geben Sie den Namen des HTTP-Headers ein, der in EPM System propagiert wird.  
Der Headername für die Standardauthentifizierung lautet HYPLOGIN. Sie können einen beliebigen Namen verwenden.
  - vi. Wählen Sie unter **Wert** die Eigenschaft aus, die EPM System-Benutzer eindeutig identifiziert.  
Der Wert dieses Feldes muss mit der Benutzeridentität in EPM System übereinstimmen. Beispiel: Wenn es sich bei der Benutzeridentität in EPM System um die E-Mail-ID handelt, wählen Sie den Wert für die geschäftliche E-Mail-Adresse aus.
  - vii. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Fertigstellen**, um die Enterprise-Anwendung zu erstellen.
  6. Klicken Sie auf **Aktivieren**, um die Anwendung zu aktivieren.
  7. Registrieren Sie das App-Gateway, und richten Sie den Host und die Anwendung für EPM System ein.
    - a. Klicken Sie im **Slide-in-Menü** auf **Sicherheit, App-Gateways**.
    - b. Klicken Sie auf **Hinzufügen**.
    - c. Geben Sie unter **Details** einen eindeutigen Namen für das Gateway sowie eine optionale Beschreibung ein.
    - d. Klicken Sie auf **Weiter**, um das Fenster "Hosts" zu öffnen.
    - e. Fügen Sie einen App-Gateway-Host für EPM System hinzu.
      - i. Klicken Sie im Fenster "Hosts" auf **Hinzufügen**.

The screenshot shows a configuration window titled "Add Host" with the following fields and values:

- Host Identifier:** EPMAppGateway
- Host:** gateway.server.example.com
- Port:** 443
- SSL Enabled:**
- Additional Properties:**

```
ssl_certificate /usr/local/gateway.server.example.com.crt;
ssl_certificate_key /usr/local/gateway.server.example.com.key;
ssl_password_file /usr/local/gateway.server.example.com.password.txt;
```

A green "Save" button is visible in the bottom right corner.

- ii. Geben Sie unter **Host-ID** den Wert `EPMAppGateway` ein.
- iii. Geben Sie unter **Host** den vollständig qualifizierten Domainnamen des Computers ein, der den App-Gateway-Server hostet, z.B. `gateway.server.example.com`.
- iv. Geben Sie unter **Port** den Port ein, auf dem der App-Gateway-Server auf HTTPS-Anforderungen antwortet.
- v. Aktivieren Sie das Kontrollkästchen **SSL-fähig**.
- vi. Geben Sie unter **Zusätzliche Eigenschaften** Folgendes ein:
  - Standort des SSL-Zertifikats
  - Schlüssel für das SSL-Zertifikat
  - SSL-Kennwortdatei (sofern benötigt)

Ausführliche Informationen finden Sie unter [App-Gateways registrieren](#) im Abschnitt "App-Gateways einrichten" in der Dokumentation *Oracle Identity Cloud Service verwalten*.
- vii. Klicken Sie auf **Speichern**.
- viii. Klicken Sie auf **Weiter**, um das Fenster "Anwendungen" zu öffnen.
- f. Fügen Sie dem App-Gateway die Enterprise-Anwendung von EPM System hinzu.
  - i. Klicken Sie unter **Anwendungen** auf **Hinzufügen**.
  - ii. Wählen Sie unter **Anwendung** die Enterprise-Anwendung von EPM System aus, die Sie Oracle Cloud Identity Console zuvor hinzugefügt haben.



Assign an App to gate

\* Application EPM System

\* Select a Host EPMAAppGateway

Policy default

\* Resource Prefix /

\* Origin Server https://epm.server.example.com:443

Additional Properties

```
ssl_certificate /usr/local/epm.server.example.com.crt;  
ssl_certificate_key /usr/local/epm.server.example.com.key;  
ssl_password_file /usr/local/epm.server.example.com.password.txt;
```

Save

- iii. Wählen Sie unter **Host auswählen** den Wert `EPMAAppGateway` aus (dies ist der EPM System-Host, den Sie dem App-Gateway hinzugefügt haben).
  - iv. Geben Sie unter **Ressourcenpräfix** den Wert `/` ein, um alle Anforderungen an den EPM System-Host weiterzuleiten.
  - v. Geben Sie im Bereich für den Ursprungsserver den vollständig qualifizierten Domainnamen des Computers ein, der Oracle Hyperion Enterprise Performance Management Workspace hostet. Geben Sie außerdem die Portnummer ein, die EPM Workspace verwendet.
  - vi. Klicken Sie auf **Speichern**.
8. Notieren Sie sich die Client-ID und das Client Secret des App-Gateways. Sie benötigen diese Werte zum Einrichten des App-Gateways.
- a. Klicken Sie im **Slide-in-Menü** auf **Sicherheit, App-Gateways**.
  - b. Klicken Sie auf den Namen des Gateways, das Sie für die Enterprise-Anwendung von EPM System hinzugefügt haben.
  - c. Kopieren Sie die Client-ID (eine alphanumerische Zeichenfolge) in einen Texteditor.
  - d. Klicken Sie auf **Secret anzeigen**, um den Code für das Client Secret anzuzeigen.
  - e. Kopieren Sie das Client Secret (eine alphanumerische Zeichenfolge) in einen Texteditor.
  - f. Speichern Sie die Textdatei.

 **Note:**

Der App-Gateway-Server muss nach jeder Aktualisierung der Konfiguration von Oracle Identity Cloud Services neu gestartet werden. Informationen zum Starten und Stoppen des App-Gateway-Servers finden Sie unter [App-Gateway starten und stoppen](#).

## App-Gateway konfigurieren

Ausführliche Informationen finden Sie unter [App-Gateways einrichten](#) in der Dokumentation *Oracle Identity Cloud Service verwalten*.

Sie benötigen die Werte für die Client-ID und das Client Secret, die Sie im vorherigen Abschnitt notiert haben, um den App-Gateway-Server zu konfigurieren.

## Benutzerverzeichnisse für Autorisierung konfigurieren

Einige Identity Management-Produkte, z.B. Oracle Identity Cloud Services und Microsoft Azure, können nicht direkt als Benutzerverzeichnisse in Oracle Enterprise Performance Management System konfiguriert werden. Sie können solche Produkte mit Oracle Unified Directory oder Oracle Virtual Directory konfigurieren und Letzteres dann als Benutzerverzeichnis in EPM System konfigurieren. Ausführliche Schritte zum Konfigurieren von Benutzerverzeichnissen finden Sie unter [Benutzerverzeichnisse konfigurieren](#).

## SSO in EPM System aktivieren

Konfigurieren Sie Sicherheitsoptionen in Oracle Enterprise Performance Management System, um SSO zu aktivieren. Detaillierte Anweisungen finden Sie unter [Sicherheitsoptionen festlegen](#).

So aktivieren Sie SSO:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Klicken Sie auf **Sicherheitsoptionen**.
4. Führen Sie im Abschnitt **SSO-Konfiguration** die folgenden Schritte aus:
  - a. Aktivieren Sie das Kontrollkästchen **SSO aktivieren**.
  - b. Wählen Sie in der Dropdown-Liste für den SSO-Provider oder Security Agent die Option **Sonstige** aus.
  - c. Wählen Sie in der Dropdown-Liste **SSO-Mechanismus** die Option **Benutzerdefinierter HTTP-Header** aus, und geben Sie den Namen des Headers an, den der Sicherheitsagent an EPM System übergibt (`HYPLOGIN` oder der benutzerdefinierte Name, den Sie beim Hinzufügen von Ressourcen für die Enterprise-Anwendung in Oracle Cloud Identity Console angegeben haben).
5. Klicken Sie auf **OK**.

### Note:

Nach einer Änderung der SSO-Konfiguration starten Sie unbedingt alle EPM System-Services neu.

## EPM Workspace-Einstellungen aktualisieren

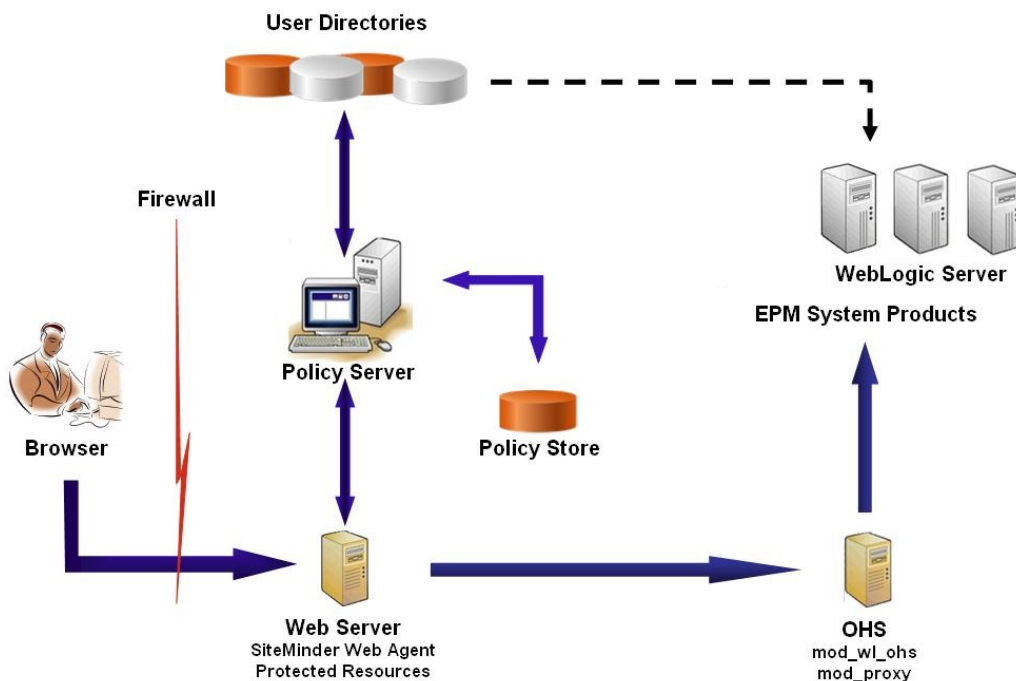
1. Greifen Sie als Systemadministrator auf Oracle Hyperion Enterprise Performance Management Workspace zu. Informationen hierzu finden Sie unter [Auf EPM Workspace zugreifen](#).
2. Wählen Sie **Navigieren, Workspace-Einstellungen, Servereinstellungen** aus.
3. Ändern Sie unter **Workspace Server-Einstellungen** den Wert unter **Abmelde-URL bereitstellen** in die URL der Webseite, die Benutzern bei der Abmeldung von Oracle Enterprise Performance Management System angezeigt werden soll.
4. Klicken Sie auf **OK**.
5. Starten Sie Oracle Hyperion Foundation Services und alle EPM System-Komponenten neu.

## SSO für SiteMinder

SiteMinder ist eine Weblösung. Desktopanwendungen und ihre Add-ins (beispielsweise Microsoft Excel und Report Designer) können Authentifizierung durch SiteMinder nicht verwenden. Oracle Smart View for Office kann jedoch die SiteMinder-Authentifizierung verwenden.

### Prozessfluss

In der folgenden Abbildung finden Sie eine Übersicht über SiteMinder-fähiges SSO:



SiteMinder-SSO-Prozess:

1. Benutzer versuchen, auf eine mit SiteMinder geschützte Oracle Enterprise Performance Management System-Ressource zuzugreifen. Sie verwenden eine

URL, um eine Verbindung zu dem Webserver herzustellen, der als Frontend für den SiteMinder-Policy-Server dient, wie z.B. `http://`

`WebAgent_Web_Server_Name:WebAgent_Web_ServerPort/interop/index.jsp.`

2. Der Webserver leitet Benutzer an den Policy-Server um, der die Benutzer nach Zugangsdaten fragt. Nachdem die Zugangsdaten anhand der konfigurierten Benutzerverzeichnisse geprüft wurden, übergibt der Policy-Server die Zugangsdaten an den Webserver, der den SiteMinder-Web-Agent hostet.
3. Der Webserver, der den SiteMinder-Web-Agent hostet, leitet die Anforderung an den Oracle HTTP Server um, der als Frontend für EPM System dient. Oracle HTTP Server leitet Benutzer an die angeforderte Anwendung um, die auf Oracle WebLogic Server bereitgestellt ist.
4. Die EPM System-Komponente prüft Provisioning-Informationen und zeigt Inhalt an. Damit dieser Prozess funktioniert, müssen die Benutzerverzeichnisse, die SiteMinder zur Benutzerauthentifizierung verwendet, als externe Benutzerverzeichnisse in EPM System konfiguriert sein. Diese Verzeichnisse müssen als vertrauenswürdig konfiguriert sein.

### Besondere Hinweise

SiteMinder ist eine Weblösung. Desktopanwendungen und ihre Add-ins (beispielsweise Microsoft Excel und Report Designer) können Authentifizierung durch SiteMinder nicht verwenden. Smart View kann jedoch die SiteMinder-Authentifizierung verwenden.

### Voraussetzungen

1. Eine vollständig funktionsfähige SiteMinder-Installation mit den folgenden Komponenten:
  - SiteMinder-Policy-Server, auf dem Policies und Agent-Objekte definiert sind
  - SiteMinder-Web-Agent, der auf dem Webserver installiert ist, der als Frontend für den SiteMinder-Policy-Server dient
2. Ein vollständig funktionsfähiges EPM System-Deployment.  
Beim Konfigurieren des Webserver für EPM System-Komponenten konfiguriert EPM System Configurator den Wert `mod_wl_ohs.conf`, um Proxyanforderungen an den WebLogic Server zu senden.

### SiteMinder-Web-Agent aktivieren

Der Web-Agent ist auf einem Webserver installiert, der Abfragen für EPM System-Ressourcen abfängt. Wenn nicht authentifizierte Benutzer versuchen, auf geschützte EPM System-Ressourcen zuzugreifen, wird der Web-Agent gezwungen, die Benutzer nach SSO-Zugangsdaten zu fragen. Wenn der Benutzer authentifiziert wird, fügt der Policy-Server den Anmeldenamen dieses Benutzers im Header hinzu. Danach wird die HTTP-Anforderung an den EPM System-Webserver übergeben, der die Anforderungen umleitet. EPM System-Komponenten extrahieren die Zugangsdaten von authentifizierten Benutzern aus Headern.

SiteMinder unterstützt SSO in allen EPM System-Produkten, die auf heterogenen Webserverplattformen laufen. Wenn EPM System-Produkte verschiedene Webserver verwenden, müssen Sie sicherstellen, dass das SiteMinder-Cookie unter Webservern der gleichen Domain weitergegeben werden kann. Hierzu geben Sie die entsprechende EPM System-Anwendungsdomain als Wert für die Eigenschaft `Cookiedomain` in der Datei `WebAgent.conf` der einzelnen Webserver an.

Informationen hierzu finden Sie im Abschnitt zum Konfigurieren von Web-Agents in der Dokumentation *Netegrity SiteMinder Agent Guide*.

 **Hinweis:**

Da Oracle Hyperion Shared Services die Basisauthentifizierung verwendet, um den zugehörigen Inhalt zu schützen, muss der Webserver, der Anforderungen an Shared Services abfängt, die Basisauthentifizierung aktivieren, um SSO mit SiteMinder zu unterstützen.

Sie konfigurieren den Web-Agent, indem Sie den Konfigurationsassistenten für den SiteMinder-Web-Agent ausführen (über `WEBAGENT_HOME/install_config_info/nete-wa-config`, z.B. `C:\netegrity\webagent\install_config_info\nete-wa-config.exe` unter Windows). Der Konfigurationsprozess erstellt die Datei `WebAgent.conf` für den SiteMinder-Webserver.

So aktivieren Sie den SiteMinder-Web-Agent:

1. Öffnen Sie `WebAgent.conf` mit einem Texteditor. Der Speicherort dieser Datei hängt von dem verwendeten Webserver ab.
2. Setzen Sie den Wert der Eigenschaft `enableWebAgent` auf `Yes`.  
`enableWebAgent="YES"`
3. Speichern und schließen Sie die Konfigurationsdatei des Web-Agents.

### Beispiel 3-1 SiteMinder-Policy-Server konfigurieren

Ein SiteMinder-Administrator muss den Policy-Server so konfigurieren, dass SSO für EPM System-Produkte aktiviert ist.

Der Konfigurationsprozess umfasst die folgenden Schritte:

- Erstellen Sie einen SiteMinder-Web-Agent, und fügen Sie geeignete Konfigurationsobjekte für den SiteMinder-Webserver hinzu.
- Erstellen Sie eine Realm für jede EPM System-Ressource, die geschützt werden soll, und fügen Sie der Realm den Web-Agent hinzu. Informationen hierzu finden Sie unter [Zu schützende Ressourcen](#).
- Erstellen Sie in der Realm, die für geschützte EPM System-Ressourcen erstellt wurde, Realms für nicht geschützte Ressourcen. Informationen hierzu finden Sie unter [Ressourcen mit aufzuhebendem Schutz](#).
- Erstellen Sie eine HTTP-Headerreferenz. Der Header muss EPM System-Anwendungen den Wert von `Login Attribute` bereitstellen. Eine kurze Beschreibung zu `Login Attribute` finden Sie unter "OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.
- Erstellen Sie Regeln in den Realms mit den Web-Agent-Aktionen "Get", "Post" und "Put".
- Erstellen Sie ein Antwortattribut mit dem Wert  
`hyplogin=<%userattr="SM_USERLOGINNAME"%>`.
- Erstellen Sie eine Policy, weisen Sie Zugriff auf das Benutzerverzeichnis zu, und fügen Sie der Liste "Aktuelle Elemente" Regeln hinzu, die Sie für EPM System erstellt haben.

- Legen Sie Antworten für die Regeln fest, die Sie für EPM System-Komponenten erstellt haben.

### Beispiel 3-2 SiteMinder-Webserver zum Weiterleiten von Anforderungen an den EPM System-Webserver konfigurieren

Konfigurieren Sie den Webserver, der den SiteMinder-Weg-Agent hostet, sodass Anforderungen von authentifizierten Benutzern (die den Header enthalten, mit dem der Benutzer identifiziert wird) an den EPM System-Webserver weitergeleitet werden.

Verwenden Sie für Webserver, die auf Apache basieren, Anweisungen wie die folgende, um authentifizierte Anforderungen weiterzuleiten:

```
ProxyPass / http://EPM_WEB_SERVER:EPM_WEB_SERVER_PORT/
ProxyPassReverse / http://EPM_WEB_SERVER:EPM_WEB_SERVER_PORT/
ProxyPreserveHost On
#If SiteMinder Web Server is using HTTPS but EPM Web Server is using HTTP
RequestHeader set WL-Proxy-SSL true
```

Ersetzen Sie in dieser Anweisung `EPM_WEB_SERVER` und `EPM_WEB_SERVER_PORT` durch die tatsächlichen Werte für Ihre Umgebung.

### Beispiel 3-3 SiteMinder in EPM System aktivieren

Die Integration von SiteMinder erfordert, dass Sie die SiteMinder-Authentifizierung für EPM System-Produkte aktivieren. Informationen hierzu finden Sie unter [EPM System für SSO konfigurieren](#).

## Kerberos-Single Sign-On

### Übersicht

Oracle Enterprise Performance Management System-Produkte unterstützen Kerberos-SSO, wenn der Anwendungsserver, der Host der EPM System-Produkte ist, für die Kerberos-Authentifizierung eingerichtet ist.

Kerberos ist ein vertrauenswürdiger Authentifizierungsservice, in dem jeder Kerberos-Client den Identitäten anderer Kerberos-Clients vertraut (Benutzer, Netzwerkservices usw.).

Wenn ein Benutzer auf ein EPM System-Produkt zugreift, passiert Folgendes:

1. Der Benutzer meldet sich über einen Windows-Computer bei einer Windows-Domain an, die auch eine Kerberos-Realm ist.
2. Der Benutzer versucht sich mittels eines Browsers, der zur Verwendung von Integrated Windows Authentication konfiguriert wurde, am EPM System-Produkt anzumelden, das auf dem Anwendungsserver läuft.
3. Der Anwendungsserver (Negotiate Identity Asserter) fängt die Anforderung ab und ruft das SPNEGO-Token (Simple and Protected Generic Security Services API (GSSAPI) Negotiation Mechanism) mit dem Kerberos-Ticket aus dem Autorisierungs-Header des Browsers ab.
4. Der Asserter validiert die Identität des Benutzers aus dem Token anhand des zugehörigen Identitätsspeichers, um Informationen zu dem Benutzer an das EPM System-Produkt zu übergeben. Das EPM System-Produkt validiert den Benutzernamen anhand von Active Directory. Das EPM System-Produkt gibt ein SSO-Token aus, das SSO in allen EPM System-Produkten unterstützt.

## Einschränkungen in der Unterstützung

Kerberos SSO wird von allen EPM System-Produkten unterstützt, mit folgenden Ausnahmen:

- Kerberos-SSO wird für andere Thick-Clients als Oracle Smart View for Office nicht unterstützt.
- Smart View unterstützt die Kerberos-Integration nur für Oracle Essbase-, Oracle Hyperion Planning- und Oracle Hyperion Financial Management-Provider.

## Annahmen

In diesem Dokument, das Kerberos-Konfigurationsschritte auf Anwendungsebene enthält, werden Kenntnisse über die Kerberos-Konfiguration auf Systemebene vorausgesetzt. Stellen Sie sicher, dass die Voraussetzungen für diese Aufgaben erfüllt sind, bevor Sie mit diesen Schritten beginnen.

In diesem Dokument wird angenommen, dass Sie in einer voll funktionsfähigen Kerberos-fähigen Netzwerkumgebung arbeiten, in der Windows-Clientcomputer für die Kerberos-Authentifizierung konfiguriert sind.

- Active Directory des Unternehmens ist für die Kerberos-Authentifizierung konfiguriert. Informationen hierzu finden Sie in der [Microsoft Windows Server-Dokumentation](#).
- Browser, die für den Zugriff auf EPM System-Produkte verwendet werden, sind für die Aushandlung mit Kerberos-Tickets konfiguriert.
- Zeitsynchronisierung mit maximal fünfminütigen Abweichungen zwischen KDC und Clientcomputern. Informationen hierzu finden Sie im Abschnitt zu Authentifizierungsfehlern aufgrund von nicht synchronisierten Uhren unter [http://technet.microsoft.com/en-us/library/cc780011\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780011(WS.10).aspx).

## Kerberos-SSO mit WebLogic Server

Kerberos-SSO für Oracle WebLogic Server verwendet den Negotiate Identity Asserter zum Aushandeln und Decodieren von SPNEGO-Token, um SSO mit Microsoft-Clients zu ermöglichen. WebLogic Server decodiert SPNEGO-Token, um ein Kerberos-Ticket zu erhalten. Das Ticket wird validiert und einem WebLogic Server-Benutzer zugewiesen. Sie können den Active Directory-Authentikator von WebLogic Server mit dem Negotiate Identity Asserter verwenden, um Active Directory als Benutzerverzeichnis für WebLogic Server-Benutzer zu konfigurieren.

Wenn der Browser Zugriff auf ein EPM System-Produkt fordert, gibt KDC ein Kerberos-Ticket an den Browser aus. So wird ein SPNEGO-Token mit den unterstützten GSS-Tokentypen erstellt. Der Negotiate Identity Asserter decodiert das SPNEGO-Token und verwendet GSSAPIs, um den Sicherheitskontext zu akzeptieren. Die Identität des Benutzers, der die Anforderung ausgelöst hat, wird einem Benutzernamen zugewiesen und an WebLogic Server zurückgegeben. Zusätzlich bestimmt WebLogic Server die Gruppen, denen der Benutzer angehört. Dann wird das EPM System-Produkt dem Benutzer zur Verfügung gestellt.

 **Hinweis:**

Benutzer müssen einen Browser verwenden, der SPNEGO unterstützt (z.B. Internet Explorer oder Firefox), um auf die EPM System-Produkte zugreifen zu können, die auf WebLogic Server ausgeführt werden.

Unter Verwendung der Benutzer-ID aus dem Authentifizierungsprozess sucht der Autorisierungsprozess des EPM Systems nach Zugriffsberechtigungsdaten. Der Zugriff auf das EPM System-Produkt wird basierend auf Provisioning-Daten eingeschränkt.

### WebLogic Server-Verfahren zur Unterstützung der Kerberos-Authentifizierung

Ein Administrator muss die folgenden Aufgaben ausführen, um die Kerberos-Authentifizierung zu unterstützen:

- WebLogic-Domain für EPM System erstellen. Informationen hierzu finden Sie unter [WebLogic-Domain für EPM System erstellen](#).
- Authentifizierungsprovider erstellen. Informationen hierzu finden Sie unter [LDAP-Authentifizierungsprovider in WebLogic Server erstellen](#).
- Negotiate Identity Asserter erstellen. Informationen hierzu finden Sie unter [Negotiate Identity Asserter erstellen](#).
- Kerberos-Identifizierung erstellen. Informationen hierzu finden Sie unter [Kerberos-Identifizierung für WebLogic Server erstellen](#).
- JVM-Optionen für Kerberos aktualisieren. Informationen hierzu finden Sie unter [JVM-Optionen für Kerberos aktualisieren](#).
- Autorisierungs-Policys konfigurieren. Informationen hierzu finden Sie unter [Autorisierungs-Policys konfigurieren](#).
- SSODiag bereitstellen und verwenden, um zu überprüfen, ob WebLogic Server für die Unterstützung von Kerberos-SSO für EPM System bereit ist. Informationen hierzu finden Sie unter [SSODiag zum Testen der Kerberos-Umgebung verwenden](#).

### WebLogic-Domain für EPM System erstellen

EPM System-Komponenten werden in der Regel in der WebLogic-Domain `EPMSystem` bereitgestellt (der Standardspeicherort ist `MIDDLEWARE_HOME/user_projects/domains/EPMSystem`).

So konfigurieren Sie die WebLogic-Domain für EPM System für die Kerberos-Authentifizierung:

1. Installieren Sie EPM System-Komponenten.
2. Stellen Sie nur Oracle Hyperion Foundation Services bereit.  
Beim Foundation Services-Deployment wird die WebLogic-Standarddomain für EPM System erstellt.
3. Melden Sie sich bei Oracle Hyperion Shared Services Console an, um zu überprüfen, ob das Foundation Services-Deployment erfolgreich war. Informationen hierzu finden Sie unter [Shared Services Console starten](#).



## LDAP-Authentifizierungsprovider in WebLogic Server erstellen

Ein WebLogic Server-Administrator erstellt den LDAP-Authentifizierungsprovider, der Benutzer- und Gruppeninformationen auf einem externen LDAP-Server speichert. LDAP v2- oder v3-konforme LDAP-Server arbeiten mit WebLogic Server. Informationen hierzu finden Sie in den folgenden Referenzen:

- [LDAP-Authentifizierungsprovider konfigurieren](#) in der Dokumentation *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
- [Authentifizierungs- und Identity Assertion-Provider konfigurieren](#) in der Onlinehilfe *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

## Negotiate Identity Asserter erstellen

Der Negotiate Identity Assertion-Provider aktiviert SSO mit Microsoft-Clients. Er decodiert SPNEGO-Token, um Kerberos-Token abzurufen, validiert die Kerberos-Token und ordnet die Token WebLogic-Benutzern zu. Der Negotiate Identity Assertion-Provider, eine Implementierung von Security Service Provider Interface (SSPI) gemäß WebLogic-Sicherheits-Framework, stellt die notwendige Logik bereit, um einen Client basierend auf dem SPNEGO-Token des Clients zu authentifizieren.

- [Negotiate Identity Assertion-Provider konfigurieren](#) in der Dokumentation *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
- [Authentifizierungs- und Identity Assertion-Provider konfigurieren](#) in der Onlinehilfe *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

Setzen Sie beim Erstellen des Negotiate Identity Assertion-Providers das Kennzeichen für die JAAS-Steuerung für alle Authentikatoren auf `SUFFICIENT`. Informationen hierzu finden Sie im Abschnitt zum Festlegen des Kennzeichens für die JAAS-Steuerung in der Onlinehilfe [Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help](#).

## Kerberos-Identifizierung für WebLogic Server erstellen

Erstellen Sie auf dem Active Directory-Domaincontrollercomputer Benutzerobjekte für den WebLogic Server und für den EPM System-Webserver, und ordnen Sie sie den Service Principal Names (SPNs) für Ihren WebLogic Server und Ihren Webserver in der Kerberos-Realm zu. Clients können einen Service ohne SPN nicht finden. Sie speichern SPNs in keytab-Dateien, die in die WebLogic Server-Domain kopiert und beim Anmeldeprozess verwendet werden.

Ausführliche Informationen finden Sie unter [Identifizierung für WebLogic Server erstellen](#) in der Dokumentation *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

So erstellen Sie die Kerberos-Identifizierung für WebLogic Server:

1. Erstellen Sie auf dem Active Directory-Domaincontrollercomputer einen Benutzeraccount, z.B. `epmHost`, für den Hostcomputer der WebLogic Server-Domain.

 **Hinweis:**

Erstellen Sie die Identifizierung als Benutzerobjekt und nicht als Computer. Verwenden Sie den einfachen Namen des Computers, z.B. `epmHost`, wenn der Hostname `epmHost.example.com` lautet.

Notieren Sie das Kennwort, das Sie beim Erstellen des Benutzerobjekts verwenden. Sie benötigen das Kennwort zum Erstellen von SPNs.

Wählen Sie keine Kennwortoptionen aus, vor allem nicht die Option `User must change password at next logon`.

2. Ändern Sie das Benutzerobjekt so, dass es mit dem Kerberos-Protokoll konform ist. Der Account muss eine Kerberos-Vorauthentifizierung erfordern.
  - Wählen Sie in der Registerkarte **Account** eine zu verwendende Verschlüsselung aus.
  - Stellen Sie sicher, dass keine andere Accountoption (insbesondere `Do not require Kerberos pre-authentication`) ausgewählt ist.
  - Da beim Festlegen des Verschlüsselungstyp das Objektkennwort möglicherweise beschädigt wurde, setzen Sie das Kennwort auf das Kennwort zurück, das Sie beim Erstellen des Objekts festgelegt haben.
3. Öffnen Sie auf dem Hostcomputer des Active Directory-Domaincontrollers ein Fenster mit einem Befehls-Prompt, und navigieren Sie zu dem Verzeichnis, in dem Active Directory-Supporttools installiert sind.
4. Erstellen und konfigurieren Sie die erforderlichen SPNs.
  - a. Verwenden Sie einen Befehl wie den folgenden, um zu überprüfen, ob die SPNs dem Benutzerobjekt (`epmHost`) zugeordnet sind, das Sie in Schritt 1 dieses Verfahrens erstellt haben.

```
setspn -L epmHost
```

- b. Verwenden Sie einen Befehl wie den folgenden, um den SPN für WebLogic Server in Active Directory Domain Services (AD DS) zu konfigurieren und eine keytab-Datei mit dem Shared Secret-Schlüssel zu generieren.

```
ktpass -princ HTTP/epmHost.example.com@EXAMPLE.COM -pass password -  
mapuser epmHost -out c:\epmHost.keytab
```

5. Erstellen Sie eine keytab-Datei auf dem Hostcomputer von WebLogic Server.
  - a. Öffnen Sie eine Eingabeaufforderung.
  - b. Navigieren Sie zu `MIDDLEWARE_HOME/jdk/bin`.
  - c. Führen Sie einen Befehl wie den folgenden aus:

```
ktab -k keytab_filename -a epmHost@example.com
```

- d. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Kennwort ein, das Sie beim Erstellen des Benutzers in Schritt 1 dieses Verfahrens festgelegt haben.

6. Kopieren Sie die keytab-Datei in das Startverzeichnis in der WebLogic-Domain, z.B. in C:\Oracle\Middleware\user\_projects\domains\EPMSystem.
7. Stellen Sie sicher, dass die Kerberos-Authentifizierung richtig funktioniert.

```
kinit -k -t keytab-file account-name
```

In diesem Befehl gibt `account-name` den Kerberos-Principal an, z.B. `HTTP/epmHost.example.com@EXAMPLE.COM`. Die Ausgabe dieses Befehls muss der folgenden ähneln:

```
New ticket is stored in cache file C:\Documents and
Settings\Username\krb5cc_MachineB
```

### JVM-Optionen für Kerberos aktualisieren

Informationen hierzu finden Sie unter [Startargumente für Kerberos-Authentifizierung mit WebLogic Server verwenden](#) und [JAAS-Anmeldedatei erstellen](#) in der Dokumentation *Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.1)*.

Wenn EPM System Managed Server als Windows-Services ausgeführt werden, aktualisieren Sie die Windows-Registry, um die JVM-Startoptionen festzulegen.

So aktualisieren Sie JVM-Startoptionen in der Windows-Registry:

1. Öffnen Sie den Windows-Registry-Editor.
2. Wählen Sie **Arbeitsplatz, HKEY\_LOCAL\_MACHINE, Software, Hyperion Solutions, FoundationServices0, HyS9EPMServer\_epmsystem1** aus.
3. Erstellen Sie die folgenden Zeichenfolgenwerte:

 **Hinweis:**

Die in der folgenden Tabelle aufgelisteten Namen sind Beispiele.

**Tabelle 3-3 JVM-Startoptionen für Kerberos-Authentifizierung**

| Name        | Typ    | Daten   |
|-------------|--------|---|
| JVMOption44 | REG_SZ | -Djava.security.krb5.realm= <i>Active Directory Realm Name</i>                              |
| JVMOption45 | REG_SZ | -Djava.security.krb5.kdc= <i>Active Directory host name or IP address</i>                   |
| JVMOption46 | REG_SZ | -<br>Djava.security.auth.login.config= <i>location of Kerberos login configuration file</i> |
| JVMOption47 | REG_SZ | -<br>Djavax.security.auth.useSubjectCredsOnly=<br>false                                     |

4. Aktualisieren Sie den Wert von JVMOptionCount DWord, damit die hinzugefügten JVMOptions wiedergegeben werden (4 zum aktuellen Dezimalwert hinzufügen).

### Autorisierungs-Policys konfigurieren

Informationen zum Konfigurieren von Autorisierungs-Policys für Active Directory-Benutzer, die auf EPM System zugreifen, finden Sie unter [Optionen zum Sichern von Webanwendungen und EJB-Ressourcen](#) in der Dokumentation *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

Beispiele für Policy-Konfigurationsschritte finden Sie unter [Policys für SSODiag erstellen](#).

### SSODiag zum Testen der Kerberos-Umgebung verwenden

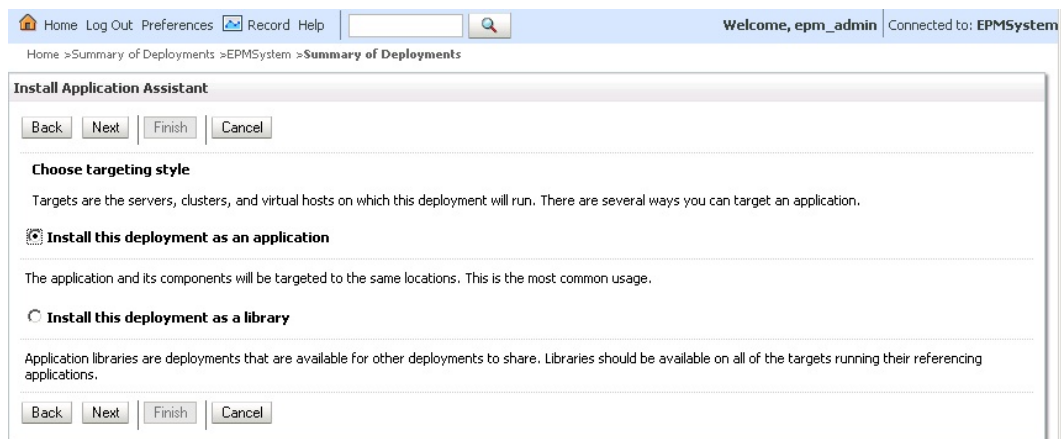
SSODiag ist eine Diagnosewebanwendung, mit der getestet wird, ob WebLogic Server in Ihrer Kerberos-Umgebung für die Unterstützung von EPM System bereit ist.

### SSODiag bereitstellen

Verwenden Sie zum Bereitstellen von SSODiag die Administratorzugangsdaten für WebLogic Server (Standardbenutzername ist `epm_admin`), die Sie beim Bereitstellen von Foundation Services angegeben haben.

So können Sie SSODiag bereitstellen und konfigurieren:

1. Melden Sie sich bei der WebLogic Server-Administrationskonsole für die EPM System-Domain an.
2. Wählen Sie im Change Center die Option **Sperren und bearbeiten** aus.
3. Klicken Sie unter **EPMSystem** in **Domainstruktur** auf **Deployments**.
4. Klicken Sie unter **Zusammenfassung der Deployments** auf **Installieren**.
5. Wählen Sie unter **Pfad** `EPM_ORACLE_HOME/products/Foundation/AppServer/InstallableApps/common/SSODiag.war` aus.
6. Klicken Sie auf **Weiter**.
7. Stellen Sie sicher, dass unter **Zielfestlegung wählen** die Option **Dieses Deployment als Anwendung installieren** ausgewählt ist, und klicken Sie auf **Weiter**.



8. Wählen Sie unter **Deployment-Ziele wählen** Folgendes aus, und klicken Sie auf **Weiter**.
  - **EPMServer**

- **Alle Server im Cluster**

Home Log Out Preferences Record Help Welcome, epm\_admin Connected to: EPMSystem

Home > Summary of Deployments > EPMSystem > Summary of Deployments

**Install Application Assistant**

Back Next Finish Cancel

**Select deployment targets**

Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

**Available targets for SSODiag**

| Servers                              |
|--------------------------------------|
| <input type="checkbox"/> AdminServer |

| Clusters  |
|---|
| <input checked="" type="checkbox"/> EPMServer               |
| <input checked="" type="radio"/> All servers in the cluster |
| <input type="radio"/> Part of the cluster                   |

Back Next Finish Cancel

9. Wählen Sie unter **Optionale Einstellungen** das Sicherheitsmodell **Benutzerdefinierte Rollen und Policys: Verwenden Sie nur Rollen und Policys, die in der Administrationskonsole definiert sind** aus.

Home Log Out Preferences Record Help Welcome, epm\_admin Connected to: EPMSystem

Home > Summary of Deployments > EPMSystem > Summary of Deployments

**Install Application Assistant**

Back Next Finish Cancel

**Optional Settings**

You can modify these settings or accept the defaults

**General**

What do you want to name this deployment?

Name:

**Security**

What security model do you want to use with this application?

DD Only: Use only roles and policies that are defined in the deployment descriptors.

Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.

Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.

Advanced: Use a custom model that you have configured on the realm's configuration page.

10. Klicken Sie auf **Weiter**.
11. Wählen Sie im Prüfenster die Option **Nein, die Konfiguration wird später geprüft** aus.
12. Klicken Sie auf **Fertig stellen**.
13. Wählen Sie im Change Center die Option **Änderungen aktivieren** aus.

### Oracle HTTP Server für SSODiag konfigurieren

Aktualisieren Sie `mod_wl_ohs.conf`, um Oracle HTTP Server so zu konfigurieren, dass SSODiag-URL-Anforderungen an WebLogic Server weitergeleitet werden.

So konfigurieren Sie die URL-Weiterleitung in Oracle HTTP Server:

1. Öffnen Sie `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf` mit einem Texteditor.
2. Fügen Sie die Definition `LocationMatch` für `SSODiag` hinzu:

```
<LocationMatch /SSODiag/>
    SetHandler weblogic-handler
    WeblogicCluster myServer:28080
</LocationMatch>
```

Im vorherigen Beispiel gibt `myServer` den Foundation Services-Hostcomputer und `28080` den Port an, den Oracle Hyperion Shared Services auf Anforderungen abhört.

3. Speichern und schließen Sie die Datei `mod_wl_ohs.conf`.
4. Starten Sie Oracle HTTP Server neu.

### Polycys für SSODiag erstellen

Erstellen Sie eine Policy in der WebLogic Server-Administrationskonsole, um die folgende SSODiag-URL zu schützen.

```
http://OHS_HOST_NAME:PORT/SSODiag/krbssodiag
```

In diesem Beispiel gibt `OHS_HOST_NAME` den Namen des Hostservers von Oracle HTTP Server und `PORT` den Port an, den Oracle HTTP Server auf Anforderungen abhört.

So erstellen Sie Polycys, um SSODiag zu schützen:

1. Wählen Sie im Change Center in der WebLogic Server-Administrationskonsole für die EPM System-Domain die Option **Sperren und bearbeiten** aus.
2. Wählen Sie **Deployments, SSODiag, Sicherheit, URLPatterns, Polycys** aus.
3. Erstellen Sie die folgenden URL-Muster:
  - /
  - /index.jsp
4. Ändern Sie jedes von Ihnen erstellte URL-Muster:
  - a. Klicken Sie in der Liste der URL-Muster unter **URL-Muster der Standalone-Webanwendung** auf das von Ihnen erstellte Muster (`/`), um es zu öffnen.
  - b. Wählen Sie **Bedingungen hinzufügen** aus.
  - c. Wählen Sie unter **Prädikatliste** die Option **Benutzer** aus.
  - d. Klicken Sie auf **Weiter**.
  - e. Geben Sie unter **Benutzerargumentname** den Active Directory-Benutzer ein, z.B. `krbuser1`, dessen Account für den Zugriff auf einen für die Kerberos-Authentifizierung konfigurierten Clientdesktop verwendet wird, und wählen Sie **Hinzufügen** aus. Bei `krbuser1` handelt es sich um einen Active Directory- oder Windows-Desktopbenutzer.
  - f. Klicken Sie auf **Fertig stellen**.
5. Klicken Sie auf **Speichern**.

## SSODiag zum Testen der WebLogic Server-Konfiguration für die Kerberos-Authentifizierung verwenden

Wenn die WebLogic Server-Konfiguration für die Kerberos-Authentifizierung richtig funktioniert, wird auf der Seite *Oracle Hyperion Kerberos SSO diagnostic Utility V 1.0* folgende Meldung angezeigt:

```
Retrieving Kerberos User principal name... Success.  
Kerberos principal name retrieved... SOME_USER_NAME
```

### **Achtung:**

Konfigurieren Sie keine EPM System-Komponenten für die Kerberos-Authentifizierung, wenn SSODiag den Kerberos-Principal-Namen nicht abrufen kann.

So testen Sie WebLogic Server-Konfigurationen für die Kerberos-Authentifizierung:

1. Starten Sie Foundation Services und Oracle HTTP Server.
2. Starten Sie über die WebLogic Server-Administrationskonsole die SSODiag-Webanwendung, um alle Anforderungen zu bedienen.
3. Melden Sie sich mit gültigen Active Directory-Zugangsdaten bei einem Clientcomputer an, der für die Kerberos-Authentifizierung konfiguriert ist.
4. Stellen Sie über einen Browser eine Verbindung zu der folgenden SSODiag-URL her:

```
http://OHS_HOST_NAME:PORT/SSODiag/krbssodiag
```

In diesem Beispiel gibt *OHS\_HOST\_NAME* den Namen des Hostservers von Oracle HTTP Server und *PORT* den Port an, den Oracle HTTP Server auf Anforderungen abhört.

Wenn die Kerberos-Authentifizierung richtig funktioniert, zeigt SSODiag die folgenden Informationen an:

```
Retrieving Kerberos User principal name... Success.  
Kerberos principal name retrieved... SOME_USER_NAME
```

Wenn die Kerberos-Authentifizierung nicht richtig funktioniert, zeigt SSODiag die folgenden Informationen an:

```
Retrieving Kerberos User principal name... failed.
```

## Sicherheitsmodelle ändern

Das Standardsicherheitsmodell für Webanwendungen, die durch die Sicherheits-Realm geschützt sind, lautet *DDonly*. Sie müssen das Sicherheitsmodell in *CustomRolesAndPolicies* ändern.

So ändern Sie Sicherheitsmodelle:

1. Öffnen Sie `MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/config/config.xml` mit einem Texteditor.
2. Suchen Sie das folgende Element im Anwendungs-Deployment-Deskriptor für die einzelnen Foundation Services-Komponenten:

```
<security-dd-model>DDOnly</security-dd-model>
```

3. Gehen Sie wie folgt vor, um das Sicherheitsmodell für die einzelnen Komponenten zu ändern:

```
<security-dd-model>CustomRolesAndPolicies</security-dd-model>
```

4. Speichern und schließen Sie die Datei `config.xml`.

### EPM System-Sicherheitskonfiguration aktualisieren

Ändern Sie die EPM System-Sicherheitskonfiguration, um Kerberos-SSO zu aktivieren.

So konfigurieren Sie EPM System für die Kerberos-Authentifizierung:

1. Melden Sie sich als Administrator bei Shared Services Console an.
2. Fügen Sie die Active Directory-Domain, die für die Kerberos-Authentifizierung konfiguriert ist, als externes Benutzerverzeichnis in Shared Services hinzu. Informationen hierzu finden Sie im Abschnitt zum Konfigurieren von OID, Active Directory und sonstigen LDAP-basierten Benutzerverzeichnissen in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.
3. Aktivieren Sie SSO. Informationen hierzu finden Sie unter [OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren](#). Wählen Sie unter **Sicherheitsoptionen** die Einstellungen in der folgenden Tabelle aus, um Kerberos SSO zu aktivieren.

**Tabelle 3-4 Einstellungen zum Aktivieren von Kerberos-SSO**

| Feld                     | Erforderliche Einstellung                    |
|--------------------------|--|
| SSO aktivieren           | Ausgewählt                                   |
| SSO-Provider oder -Agent | Sonstige                                     |
| SSO-Mechanismus          | Remote-Benutzer aus HTTP-Anforderung abrufen |

4. Starten Sie Foundation Services neu.

### Kerberos-SSO testen

Melden Sie sich bei Foundation Services an, um zu überprüfen, ob Kerberos-SSO richtig funktioniert.

So testen Sie Kerberos-SSO:

1. Stellen Sie sicher, dass Foundation Services und Oracle HTTP Server ausgeführt werden.
2. Melden Sie sich mit gültigen Active Directory-Zugangsdaten bei einem Clientcomputer an, der für die Kerberos-Authentifizierung konfiguriert ist.



3. Stellen Sie über einen Browser eine Verbindung zur Foundation Services-URL her.

### EPM System-Komponenten konfigurieren

Konfigurieren Sie mit EPM System Configurator sonstige EPM System-Komponenten, und stellen Sie diese in der WebLogic-Domain bereit, in der Foundation Services bereitgestellt ist.

### EPM System Managed Server für die Kerberos-Authentifizierung konfigurieren

In Microsoft Windows-Umgebungen werden EPM System Managed Server als Windows-Services ausgeführt. Sie müssen die JVM-Startoptionen für jeden WebLogic Managed Server ändern. Im Folgenden finden Sie eine umfassende Liste von Managed Servern im nicht komprimierten Deployment-Modus:

- AnalyticProviderServices0
- CalcMgr0
- ErpIntegrator0
- EssbaseAdminServer0
- FinancialReporting0
- HFMWeb0
- FoundationServices0
- HpsAlerter0
- HpsWebReports0
- Planning0
- Profitability0

Wenn EPM System-Webanwendungen im komprimierten Deployment-Modus bereitgestellt werden, müssen Sie die JVM-Startoptionen nur von Managed Server `EPMSystem0` aktualisieren. Wenn Sie über mehrere komprimierte Managed Server verfügen, müssen Sie die JVM-Startoptionen für alle Managed Server aktualisieren.

Informationen hierzu finden Sie unter [Startargumente für Kerberos-Authentifizierung mit WebLogic Server verwenden](#) in der Dokumentation *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

#### Hinweis:

Im Folgenden wird beschrieben, wie die JVM-Startoptionen für den FoundationServices Managed Server festgelegt werden. Sie müssen diese Aufgabe für jeden WebLogic Managed Server im Deployment ausführen.

Eine ausführliche Beschreibung der Schritte zum Konfigurieren von JVM-Optionen in WebLogic Server-Startskripten finden Sie unter [JVM-Optionen für Kerberos aktualisieren](#).

So konfigurieren Sie JVM-Optionen in WebLogic Server-Startskripten:

## Autorisierungs-Policys konfigurieren

Konfigurieren Sie Autorisierungs-Policys für Active Directory-Benutzer, die auf andere EPM System-Komponenten als Foundation Services zugreifen. Informationen zum Konfigurieren von Sicherheits-Policys über die WebLogic-Administrationskonsole finden Sie unter [Autorisierungs-Policys konfigurieren](#).

## Standardsicherheitsmodell von EPM System-Komponenten ändern

Sie bearbeiten die EPM System-Konfigurationsdatei, um das Standardsicherheitsmodell zu ändern. Bei nicht komprimierten EPM System-Deployments müssen Sie das Standardsicherheitsmodell jeder EPM System-Webanwendung ändern, die in der Datei `config.xml` erfasst ist. Im Folgenden finden Sie eine Liste der EPM System-Webanwendungen:

- AIF
- APS
- CALC
- EAS
- FINANCIALREPORTING
- PLANNING
- PROFITABILITY
- SHARED SERVICES
- WORKSPACE

So ändern Sie Sicherheitsmodelle:

1. Öffnen Sie `MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/config/config.xml` mit einem Texteditor.
2. Setzen Sie in der Definition "app-deployment" der einzelnen EPM System-Komponenten den Wert von `<security-dd-model>` auf `CustomRolesAndPolicies`, wie im folgenden Beispiel gezeigt:

```
<app-deployment>
  <name>SHARED SERVICES#11.1.2.0</name>
  <target>EPMServer</target>
  <module-type>ear</module-type>
  <source-path>C:\Oracle\Middleware\EPMSysstem11R1/products/Foundation/
AppServer/InstallableApps/common/interop.ear</source-path>
  <security-dd-model>CustomRolesAndPolicies</security-dd-model>
  <staging-mode>nostage</staging-mode>
</app-deployment>
```

3. Speichern und schließen Sie die Datei `config.xml`.
4. Starten Sie WebLogic Server neu.

## URL-Schutz-Policys für EPM System-Komponenten erstellen

Erstellen Sie eine URL-Schutz-Policy in der WebLogic Server-Administrationskonsole, um die einzelnen EPM System-Komponenten-URLs zu schützen. Ausführliche Informationen finden Sie unter [Optionen zum Sichern von Webanwendungen und EJB-Ressourcen](#) in der

Dokumentation *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

So erstellen Sie URL-Schutz-Policys:

1. Klicken Sie im Change Center in der WebLogic Server-Administrationskonsole für die EPM System-Domain auf **Sperren und bearbeiten**.
2. Klicken Sie auf **Deployments**.
3. Blenden Sie eine EPM System-Unternehmensanwendung (z.B. `PLANNING`) in Ihrem Deployment ein, und klicken Sie auf die entsprechende Webanwendung (z.B. `HyperionPlanning`). Eine Liste der EPM System-Komponenten finden Sie unter [Standardsicherheitsmodell von EPM System-Komponenten ändern](#).

 **Hinweis:**

Einige Unternehmensanwendungen, wie z.B. Oracle Essbase Administration Services, umfassen mehrere Webanwendungen, für die URL-Muster definiert werden müssen.

4. Erstellen Sie für die Webanwendung eine Policy für URL-Muster.
  - AIF
  - APS
  - CALC
  - EAS
  - FINANCIALREPORTING
  - PLANNING
  - PROFITABILITY
  - SHARED SERVICES
  - WORKSPACE
- a. Klicken Sie auf **Sicherheit, Policys, Neu**.
- b. Geben Sie unter **URL-Muster** die geschützten und ungeschützten URLs für die EPM System-Produkte ein. Weitere Details finden Sie unter [EPM System-Ressourcen schützen und den Schutz aufheben](#).
- c. Klicken Sie auf **OK**.
- d. Klicken Sie auf das erstellte URL-Muster.
- e. Klicken Sie auf **Bedingungen hinzufügen**.
- f. Wählen Sie unter **Prädikatliste** eine Policy-Bedingung aus, und klicken Sie auf **Weiter**.  
Oracle empfiehlt die Verwendung der Bedingung `Group`, mit der diese Sicherheits-Policy allen Elementen einer bestimmten Gruppe gewährt wird.
- g. Geben Sie die Argumente für das ausgewählte Prädikat an. Beispiel: Wenn Sie im vorherigen Schritt `Group` ausgewählt haben, müssen Sie die folgenden Schritte ausführen:
- h. Geben Sie unter **Gruppenargumentname** den Namen der Gruppe ein, der die Benutzer angehören, die Zugriff auf die Webanwendung erhalten sollen.

Der von Ihnen eingegebene Name muss exakt mit einem Active Directory-Gruppennamen übereinstimmen.

- Klicken Sie auf **Hinzufügen**.
  - Wiederholen Sie die vorherigen Schritte, um weitere Gruppen hinzuzufügen.
- i. Klicken Sie auf **Fertig stellen**.  
WebLogic Server zeigt eine Fehlermeldung an, wenn die Gruppe in Active Directory nicht gefunden werden kann. Sie müssen diesen Fehler beheben, bevor Sie fortfahren.
  - j. Klicken Sie auf **Speichern**.
5. Wiederholen Sie die Schritte 3 und 4 dieses Verfahrens für die anderen EPM System-Komponenten in Ihrem Deployment.
  6. Klicken Sie im Change Center auf **Konfiguration freigeben**.
  7. Starten Sie WebLogic Server neu.

### Clientzertifikatbasierte Authentifizierung in Webanwendungen aktivieren

Fügen Sie die Definition `login-config` in die Konfigurationsdatei der folgenden Anwendungsarchive unter `EPM_ORACLE_HOME/products/` ein.

- `Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear`
- `FinancialDataQuality/AppServer/InstallableApps/aif.ear`
- `financialreporting/InstallableApps/HReports.ear`
- `Profitability/AppServer/InstallableApps/common/profitability.ear`

So aktivieren Sie die clientzertifikatbasierte Authentifizierung:

1. Stoppen Sie EPM System-Komponenten und -Prozesse.
2. Blenden Sie mit 7-Zip ein im Enterprise Archive enthaltenes Webarchiv ein. Beispiel:  
`EPM_ORACLE_HOME/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear/eas.war`.
3. Navigieren Sie zu `WEB-INF`.
4. Ändern Sie `web.xml`, indem Sie die folgende Definition für `login_config` direkt vor dem Element `</webapp>` hinzufügen:

```
<login-config>
  <auth-method>CLIENT-CERT</auth-method>
</login-config>
```

5. Speichern Sie die Datei `web.xml`.
6. Klicken Sie auf **Ja**, wenn Sie von 7-Zip gefragt werden, ob Sie das Archiv aktualisieren möchten.

### EPM System-Sicherheitskonfiguration aktualisieren

Konfigurieren Sie die EPM System-Sicherheit, um SSO zu berücksichtigen. Weitere Informationen finden Sie unter [EPM System für SSO konfigurieren](#).

## EPM System für SSO konfigurieren

Oracle Enterprise Performance Management System-Produkte müssen so konfiguriert werden, dass ein Security Agent für SSO unterstützt wird. Die in Oracle Hyperion Shared Services angegebene Konfiguration legt Folgendes für alle EPM System-Produkte fest:

- Ob SSO über einen Security Agent akzeptiert wird
- Mit welcher Authentifizierungsmethode SSO akzeptiert wird

In einer Umgebung, in der SSO aktiviert ist, parst das EPM System-Produkt, auf das der Benutzer als erstes zugegriffen hat, den SSO-Mechanismus, um die darin enthaltene, authentifizierte Benutzer-ID abzurufen. Das EPM System-Produkt gleicht die Benutzer-ID mit den in Shared Services konfigurierten Benutzerverzeichnissen ab, um zu ermitteln, ob es sich um einen gültigen EPM System-Benutzer handelt. Danach gibt es ein Token aus, mit dem SSO für alle EPM System-Produkte aktiviert wird.

Die in Shared Services hinterlegte Konfiguration aktiviert SSO und legt die für alle EPM System-Produkte geltende Authentifizierungsmethode fest, mit der SSO Annahmen ausführt.

So aktivieren Sie SSO in einer Web Identity Management-Lösung:

1. Starten Sie Oracle Hyperion Shared Services Console als Shared Services-Administrator. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Stellen Sie sicher, dass die Benutzerverzeichnisse, die von der Web Identity Management-Lösung verwendet werden, in Shared Services als externe Benutzerverzeichnisse konfiguriert wurden.

Beispiel: Um Kerberos-SSO zu aktivieren, müssen Sie Active Directory für die Kerberos-Authentifizierung als externes Benutzerverzeichnis konfigurieren.

Anweisungen finden Sie unter Benutzerverzeichnisse konfigurieren.

4. Wählen Sie **Sicherheitsoptionen** aus.
5. Wählen Sie **Erweiterte Optionen anzeigen** aus.
6. Führen Sie im Fenster "Definierte Benutzerverzeichnisse" im Bereich für die **SSO-Konfiguration** die folgenden Schritte aus:
  - a. Wählen Sie **SSO aktivieren** aus.
  - b. Wählen Sie unter **SSO-Provider oder -Agent** eine Web Identity Management-Lösung aus. Wenn Sie SSO mit Kerberos konfigurieren möchten, wählen Sie **Sonstige** aus.

Der empfohlene SSO-Mechanismus wird automatisch ausgewählt. Informationen hierzu finden Sie in der folgenden Tabelle. Weitere Informationen finden Sie unter [Unterstützte SSO-Methoden](#).

 **Hinweis:**

Wenn Sie nicht mit dem empfohlenen SSO-Mechanismus arbeiten, müssen Sie unter **SSO-Provider oder -Agent** die Option `Sonstige` auswählen. Beispiel: Wenn Sie einen anderen Mechanismus als HTTP-Header für SiteMinder verwenden möchten, wählen Sie unter **SSO-Provider oder -Agent** die Option `Sonstige` aus. Wählen Sie anschließend unter **SSO-Mechanismus** den gewünschten SSO-Mechanismus aus.

**Tabelle 3-5 Empfohlene SSO-Mechanismen für Web Identity Management-Lösungen**

| Web Identity Management-Lösung | Empfohlener SSO-Mechanismus       |
|--------------------------------|-----------------------------------|
| Oracle Access Manager          | Custom HTTP Header <sup>1</sup>   |
| OSSO                           | Custom HTTP Header                |
| SiteMinder                     | Custom HTTP Header                |
| Kerberos                       | Get Remote User from HTTP Request |

<sup>1</sup> Der standardmäßige Name für den HTTP-Header lautet `HYPLOGIN`. Wenn Sie einen benutzerdefinierten HTTP-Header verwenden, ersetzen Sie diese Bezeichnung.

7. Klicken Sie auf **OK**.

## Single Sign-On-Optionen für Smart View

Obwohl Oracle Smart View for Office ein Thick Client und kein Browser ist, wird die Verbindung zu Serverkomponenten über HTTP hergestellt. Aus Systemperspektive entspricht das Verhalten eher einem Browser. Smart View unterstützt alle webbasierten Standardintegrationsmethoden, die von Browserschnittstellen unterstützt werden. Es gibt jedoch einige Einschränkungen:

- Wenn Smart View über eine vorhandene Browsersession gestartet wird, die mit einer Oracle Enterprise Performance Management System-Komponente verbunden ist, müssen sich Benutzer erneut bei Smart View anmelden, da das Cookie aus der vorhandenen Session nicht gemeinsam verwendet wird.
- Wenn Sie anstelle des Oracle Access Manager-Standardanmeldeformulars ein Anmeldeformular verwenden, das auf benutzerdefinierter HTML basiert, müssen Sie sicherstellen, dass die Quelle des benutzerdefinierten Formulars die Zeichenfolge `loginform` enthält. Dies ist erforderlich, damit die Integration von Smart View in Oracle Access Manager funktioniert.

# 4

## Benutzerverzeichnisse konfigurieren

### Siehe auch:

- [Benutzerverzeichnisse und EPM System-Sicherheit](#)
- [Vorgänge bezüglich der Benutzerverzeichniskonfiguration](#)
- [Oracle Identity Manager und EPM System](#)
- [Informationen zu Active Directory](#)
- [OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren](#)
- [Relationale Datenbanken als Benutzerverzeichnisse konfigurieren](#)
- [Benutzerverzeichnisverbindungen testen](#)
- [Einstellungen der Benutzerverzeichnisse ändern](#)
- [Benutzerverzeichniskonfigurationen löschen](#)
- [Suchreihenfolge des Benutzerverzeichnisses verwalten](#)
- [Sicherheitsoptionen festlegen](#)
- [Verschlüsselungsschlüssel erneut generieren](#)
- [Sonderzeichen verwenden](#)

## Benutzerverzeichnisse und EPM System-Sicherheit

Oracle Enterprise Performance Management System-Produkte werden von vielen Benutzer- und Identitätsmanagementsystemen unterstützt. Diese werden auch als Benutzerverzeichnisse bezeichnet. Hierzu gehören LDAP-fähige Benutzerverzeichnisse wie Sun Java System Directory Server (früher SunONE Directory Server) und Active Directory. Darüber hinaus unterstützt EPM System relationale Datenbanken als externe Benutzerverzeichnisse.

EPM System-Produkte verwenden beim Provisioning in der Regel Native Directory und externe Benutzerverzeichnisse. Eine Liste der unterstützten Benutzerverzeichnisse finden Sie in unter [Oracle Enterprise Performance Management System Certification Matrix](#).

EPM System-Produkte erfordern einen Benutzerverzeichnis-Account für jeden Benutzer, der auf diese Produkte zugreift. Diese Benutzer können Gruppen zugewiesen werden, um das Zuweisen von Zugriffsberechtigungen zu vereinfachen. Benutzern und Gruppen können die EPM System-Rollen und Objekt-ACLs zugewiesen werden. Aufgrund des Verwaltungsaufwands rät Oracle davon ab, einzelnen Benutzern Zugriffsberechtigungen zuzuweisen. Benutzer und Gruppen aus allen konfigurierten Benutzerverzeichnissen werden in Oracle Hyperion Shared Services Console angezeigt.

Standardmäßig konfiguriert EPM System Configurator das Shared Services-Repository für die Unterstützung von EPM System-Produkten als Native Directory. Verzeichnismanager führen den Zugriff auf Native Directory sowie dessen Verwaltung über Shared Services Console aus.

## Vorgänge bezüglich der Benutzerverzeichniskonfiguration

Um SSO und die Autorisierung zu unterstützen, müssen Systemadministratoren externe Benutzerverzeichnisse konfigurieren. Mit Oracle Hyperion Shared Services Console können Systemadministratoren verschiedene Aufgaben für die Konfiguration und die Verwaltung von Benutzerverzeichnissen ausführen. In diesen Abschnitten finden Sie die entsprechenden Anweisungen:

- Benutzerverzeichnisse konfigurieren:
  - [OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren](#)
  - [Relationale Datenbanken als Benutzerverzeichnisse konfigurieren](#)
- [Benutzerverzeichnisverbindungen testen](#)
- [Einstellungen der Benutzerverzeichnisse ändern](#)
- [Benutzerverzeichniskonfigurationen löschen](#)
- [Suchreihenfolge des Benutzerverzeichnisses verwalten](#)
- [Sicherheitsoptionen festlegen](#)

## Oracle Identity Manager und EPM System

Oracle Identity Manager ist eine Lösung für die Rollen- und Benutzeradministration, die Prozesse wie das Hinzufügen, Aktualisieren und Löschen von Benutzer-Accounts und Berechtigungen auf Attributebene unternehmensressourcenübergreifend automatisiert. Oracle Identity Manager ist als eigenständiges Produkt oder als Teil der Oracle Identity and Access Management Suite Plus verfügbar.

Oracle Enterprise Performance Management System kann anhand von Unternehmensrollen, die LDAP-Gruppen sind, in Oracle Identity Manager integriert werden. Rollen von EPM System-Komponenten können Unternehmensrollen zugewiesen werden. Benutzer oder Gruppen, die Oracle Identity Manager-Unternehmensrollen hinzugefügt werden, erhalten automatisch zugeordnete EPM System-Rollen.

Beispiel: Angenommen, Sie haben eine Oracle Hyperion Planning-Anwendung mit dem Namen *Budgetplanung*. Um diese Anwendung zu unterstützen, können Sie drei Unternehmensrollen - "Interaktiver Benutzer Budgetplanung", "Endbenutzer Budgetplanung" und "Admin Budgetplanung" - in Oracle Identity Manager erstellen. Stellen Sie bei der Zuweisung von EPM System-Rollen sicher, dass die Provisioning-Manager die Unternehmensrollen aus Oracle Identity Manager mit den erforderlichen Rollen aus *Budgetplanung* und anderen EPM System-Komponenten, einschließlich Shared Services, zuweisen. Alle den Unternehmensrollen in Oracle Identity Manager zugewiesenen Benutzer und Gruppen erhalten die EPM System-Rollen. Informationen zum Bereitstellen und Verwalten von Oracle Identity Manager finden Sie in der Dokumentation zu Oracle Identity Manager.

Um Oracle Identity Manager in EPM System zu integrieren, müssen die Administratoren folgende Schritte durchführen:

- Stellen Sie sicher, dass Elemente (Benutzer und Gruppen) von Oracle Identity Manager-Unternehmensrollen, die für das Provisioning in EPM System verwendet



werden sollen, in einem LDAP-fähigen Benutzerverzeichnis, z.B. OID oder Active Directory, definiert sind.

- Konfigurieren Sie das LDAP-fähige Benutzerverzeichnis, in dem Elemente der Unternehmensrollen definiert sind, als externes Benutzerverzeichnis in EPM System. Informationen hierzu finden Sie unter [OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren](#).

## Informationen zu Active Directory

In diesem Abschnitt werden Microsoft Active Directory-Konzepte erklärt, die in diesem Dokument verwendet werden.

### DNS-Suche und Hostnamensuche

Systemadministratoren können Active Directory so konfigurieren, dass Oracle Hyperion Shared Services eine Suche nach statischen Hostnamen oder eine DNS-Suche durchführen kann, um Active Directory zu identifizieren. Die Suche nach statischen Hostnamen unterstützt kein Failover für Active Directory.

Die Verwendung der DNS-Suche sichert die Hochverfügbarkeit von Active Directory in Szenarios, in denen Active Directory auf mehreren Domaincontrollern konfiguriert ist, um Hochverfügbarkeit sicherzustellen. Wenn Shared Services für das Ausführen einer DNS-Suche konfiguriert ist, wird der DNS-Server aufgefordert, registrierte Domaincontroller zu identifizieren. Anschließend wird eine Verbindung zum Domaincontroller mit der höchsten Gewichtung hergestellt. Wenn bei dem Domaincontroller, der mit Shared Services verbunden ist, ein Fehler auftritt, schaltet Shared Services dynamisch auf den nächsten verfügbaren Domaincontroller mit der größten Gewichtung um.



#### Hinweis:

Die DNS-Suche kann nur konfiguriert werden, wenn ein redundantes Active Directory-Setup verfügbar ist, das ein Failover unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

### Globaler Katalog

Ein globaler Katalog ist ein Domaincontroller, der eine Kopie aller Active Directory-Objekte in einer Gesamtstruktur speichert. Er speichert eine vollständige Kopie aller Objekte im Verzeichnis für seine Hostdomain und eine Teilkopie aller Objekte für alle anderen Domains im Forest. Diese werden in typischen Benutzersuchoperationen verwendet. Weitere Informationen zum Einrichten eines globalen Katalogs finden Sie in der Microsoft-Dokumentation.

Wenn Ihr Unternehmen einen globalen Katalog nutzt, verwenden Sie eine der folgenden Methoden zur Konfiguration von Active Directory:

- Konfigurieren des Servers des globalen Katalogs als externes Benutzerverzeichnis (empfohlen).
- Konfigurieren jeder Active Directory-Domain als separates externes Benutzerverzeichnis.

Das Konfigurieren des globalen Katalogs anstelle einzelner Active Directory-Domains ermöglicht Oracle Enterprise Performance Management System-Produkten, auf lokale und universelle Gruppen innerhalb der Gesamtstruktur zuzugreifen.

## OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren

Systemadministratoren verwenden die Verfahren in diesem Abschnitt, um LDAP-basierte Unternehmensbenutzerverzeichnisse wie OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server oder ein LDAP-basiertes Benutzerverzeichnis, das nicht im Konfigurationsfenster aufgeführt wird, zu konfigurieren.

So konfigurieren Sie OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.  
Die Registerkarte "Providerkonfiguration" wird geöffnet. In diesem Fenster werden alle konfigurierten Benutzerverzeichnisse aufgeführt, einschließlich Native Directory.
3. Klicken Sie auf **Neu**.
4. Wählen Sie unter **Verzeichnistyp** eine Option aus:
  - **Lightweight Directory Access Protocol (LDAP)**, um ein anderes LDAP-basiertes Verzeichnis als Active Directory zu konfigurieren. Wählen Sie diese Option zum Konfigurieren von Oracle Virtual Directory aus.
  - **Microsoft Active Directory (MSAD)**, um Active Directory zu konfigurieren.  
**Nur Active Directory und Active Directory Application Mode (ADAM):**  
Wenn Sie ein benutzerdefiniertes ID-Attribut für Active Directory oder ADAM verwenden möchten (d.h. ein anderes Attribut als `ObjectGUID`, z.B. `sAMAccountName`), wählen Sie **Lightweight Directory Access Protocol (LDAP)** aus, und konfigurieren Sie es mit dem Verzeichnistyp `Other`.
5. Klicken Sie auf **Weiter**.

The screenshot shows the Oracle Enterprise Performance Management System configuration interface. The main window is titled "Configure User Directories" and is divided into three sections: "1. MSAD Connection Information", "2. MSAD User Configuration", and "3. MSAD Group Configuration". The "Server Information" section is currently active and contains the following fields:

- Directory Server: Microsoft
- Name:
- Host Name:  (Radio buttons for DNS Lookup and Host Name are present, with Host Name selected)
- Port: 389
- SSL Enabled:
- Base DN:  (Fetch DN button is next to it)
- ID Attribute: objectguid
- Maximum Size: 0
- Trusted:
- Anonymous Bind:
- User DN:  (Append Base DN checkbox is next to it)
- Password:


Below the "Server Information" section, there is a "Show Advanced Options" checkbox which is checked. This section contains three sub-sections:

- LDAP Options**
  - Referrals: ignore
  - Dereference Aliases: Always
  - Connection Read Timeout: 60 sec
- Connection Pooling**
  - Max Connections: 100
  - Timeout: 300000 ms
  - Evict Interval: 120 mins
  - Allowed Idle Connection Time: 120 mins
  - Grow Connections:
- Custom Module**
  - Enable Custom Authentication Module:



At the bottom of the window, there are buttons for "Help", "Back", "Next", "Finish", and "Cancel".

6. Geben Sie die geforderten Parameter ein.

**Tabelle 4-1 Fenster "Verbindungsinformationen"**

| Label             | Beschreibung   |
|-------------------|--|
| Verzeichnisserver | <p>Wählen Sie ein Benutzerverzeichnis aus. Der Wert von <b>ID-Attribut</b> wird für das ausgewählte Produkt in das empfohlene, konstante, eindeutige ID-Attribut geändert. Diese Eigenschaft wird automatisch ausgewählt, wenn Sie Active Directory in Schritt 4 auswählen.</p> <p>Wählen Sie in folgenden Szenarios die Option <i>Sonstige</i> aus:</p> <ul style="list-style-type: none"> <li>• Wenn Sie ein Benutzerverzeichnis konfigurieren, das nicht aufgeführt ist, z.B. Oracle Virtual Directory</li> <li>• Wenn Sie ein aufgeführtes LDAP-fähiges Benutzerverzeichnis konfigurieren (z.B. OID), aber ein benutzerdefiniertes ID-Attribut verwenden möchten</li> <li>• Wenn Sie Active Directory oder ADAM konfigurieren und ein benutzerdefiniertes ID-Attribut verwenden möchten</li> </ul> |
|                   | <p> <b>Hinweis:</b></p> <p>Da Oracle Virtual Directory eine virtualisierte Abstraktion von LDAP-Verzeichnissen und RDMBS-Daten-Repositorys in einer Verzeichnisansicht bietet, erkennt Oracle Enterprise Performance Management System es als einzelnes externes Benutzerverzeichnis an, ungeachtet der Anzahl und Art der Benutzerverzeichnisse, die Oracle Virtual Directory unterstützt.</p>   |
| Name              | <p><b>Beispiel:</b> Oracle Internet Directory</p> <p>Ein beschreibender Name für das Benutzerverzeichnis. Wenn mehrere Benutzerverzeichnisse konfiguriert sind, kann hiermit ein bestimmtes identifiziert werden. Der Name darf keine Sonderzeichen außer Leerzeichen und Unterstrichen enthalten.</p> <p><b>Beispiel:</b> Corporate_OID</p>   |

**Tabelle 4-1 (Fortsetzung) Fenster "Verbindungsinformationen"**

| Label     | Beschreibung   |
|-----------|--|
| DNS-Suche | <p><b>Nur Active Directory:</b> Wählen Sie diese Option aus, um die DNS-Suche zu aktivieren. Informationen hierzu finden Sie unter <a href="#">DNS-Suche und Hostnamensuche</a>. Oracle empfiehlt, die DNS-Suche als die Verbindungsmethode zu Active Directory in Produktionsumgebungen zu konfigurieren, um Verbindungsfehler zu vermeiden.</p> <div data-bbox="667 506 1377 688" style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Hinweis:</b></p> <p>Wenn Sie einen globalen Katalog konfigurieren, wählen Sie diese Option nicht aus.</p> </div> <p>Wenn Sie diese Option auswählen, werden die folgenden Felder angezeigt:</p> <ul style="list-style-type: none"> <li>• <b>Domain:</b> Der Domainname einer Active Directory-Gesamtstruktur.<br/> <b>Beispiele:</b> <code>example.com</code> oder <code>us.example.com</code></li> <li>• <b>AD-Site:</b> Sitename von Active Directory. In der Regel ist dies der relative Distinguished Name (DN) des Siteobjekts, das im Konfigurationscontainer von Active Directory gespeichert ist. Normalerweise bezeichnet AD-Site einen geographischen Standort wie eine Stadt, ein(en) Bundesland/-staat, eine Region oder ein Land.<br/> <b>Beispiele:</b> <code>Santa Clara</code> oder <code>US_West_region</code></li> <li>• <b>DNS-Server:</b> DNS-Name des Servers, der die DNS-Serversuche nach Domain-Controllern unterstützt.</li> </ul> |
| Hostname  | <p><b>Nur Active Directory:</b> Wählen Sie diese Option aus, um die statische Hostnamensuche zu aktivieren. Informationen hierzu finden Sie unter <a href="#">DNS-Suche und Hostnamensuche</a>.</p> <div data-bbox="667 1291 1377 1474" style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Hinweis:</b></p> <p>Wählen Sie diese Option aus, wenn Sie einen globalen Katalog für Active Directory konfigurieren.</p> </div>   |

**Tabelle 4-1 (Fortsetzung) Fenster "Verbindungsinformationen"**




| Label         | Beschreibung   |
|---------------|--|
| Hostname      | <p>DNS-Name des Benutzerverzeichnisseservers. Verwenden Sie den vollqualifizierten Domainnamen, wenn das Benutzerverzeichnis dazu verwendet werden soll, SSO von SiteMinder zu unterstützen. Oracle empfiehlt die Verwendung des Hostnamens, um eine Active Directory-Verbindung ausschließlich für Testzwecke herzustellen.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"><p> <b>Hinweis:</b></p><p>Wenn Sie einen globalen Katalog für Active Directory konfigurieren, geben Sie den Namen des Servers an, der als Host für den globalen Katalog dient. Informationen hierzu finden Sie unter <a href="#">Globaler Katalog</a>.</p></div> <p><b>Beispiel:</b> MyServer</p> |
| Port          | <p>Die Port-Nummer, mit der das Benutzerverzeichnis ausgeführt wird.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"><p> <b>Hinweis:</b></p><p>Wenn Sie einen globalen Katalog für Active Directory konfigurieren, geben Sie den Port an, der vom Server für den globalen Katalog verwendet wird (der Standardwert ist 3268). Informationen hierzu finden Sie unter <a href="#">Globaler Katalog</a>.</p></div> <p><b>Beispiel:</b> 389</p>   |
| SSL aktiviert | <p>Das Kontrollkästchen, mit dem eine sichere Kommunikation für dieses Benutzerverzeichnis ermöglicht wird. Das Benutzerverzeichnis muss für eine sichere Kommunikation konfiguriert sein.</p>   |

Tabelle 4-1 (Fortsetzung) Fenster "Verbindungsinformationen"

| Label          | Beschreibung   |
|----------------|--|
| Basis-DN       | <p>Distinguished Name (DN) des Knotens, mit dem die Suche nach Benutzern und Gruppen beginnen sollte. Sie können verfügbare Basis-DNs auch mit der Schaltfläche <b>DNs abrufen</b> auflisten und dann den entsprechenden Basis-DN aus der Liste auswählen.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> <b>Hinweis:</b></p> <p>Wenn Sie einen globalen Katalog konfigurieren, geben Sie den Basis-DN der Gesamtstruktur an.</p> </div> <p>Informationen zu den Einschränkungen bei der Verwendung von Sonderzeichen finden Sie unter <a href="#">Sonderzeichen verwenden</a>.</p> <p>Oracle empfiehlt Ihnen, den niedrigsten DN auszuwählen, der alle Benutzer und Gruppen der EPM System-Produkte umfasst.</p> <p><b>Beispiel:</b> dc=example,dc=com</p>                       |
| ID-Attribut    | <p>Dieser Attributwert kann nur geändert werden, wenn <i>Sonstige</i> unter <b>Verzeichnistyp</b> ausgewählt wurde. Dieses Attribut muss ein gemeinsames Attribut sein, das in Benutzer- und Gruppenobjekten auf dem Verzeichnisserver vorhanden ist.</p> <p>Der empfohlene Wert für dieses Attribut wird automatisch für OID (orclguid), SunONE (nsuniqueid), IBM Directory Server (Ibm-entryUuid), Novell eDirectory (GUID) und Active Directory (ObjectGUID) festgelegt.</p> <p><b>Beispiel:</b> orclguid</p> <p>Wenn Sie den ID-Attributwert manuell festlegen, nachdem Sie <i>Sonstige</i> unter <b>Verzeichnisserver</b> ausgewählt haben, muss dieser zum Beispiel zum Konfigurieren eines Oracle Virtual Directory:</p> <ul style="list-style-type: none"> <li>• Auf ein eindeutiges Attribut verweisen</li> <li>• Vom Speicherort unabhängig sein</li> <li>• Unverändert bleiben</li> </ul> |
| Maximale Größe | <p>Die maximale Anzahl an Ergebnissen, die von einer Suche zurückgegeben werden. Ist dieser Wert höher als der von den Einstellungen des Benutzerverzeichnisses unterstützte Wert, überschreibt das Benutzerverzeichnis diesen Wert.</p> <p>Lassen Sie dieses Feld für andere Benutzerverzeichnisse als Active Directory leer, damit alle Benutzer und Gruppen abgerufen werden, die den Suchkriterien entsprechen.</p> <p>Setzen Sie diesen Wert für Active Directory auf 0, damit alle Benutzer und Gruppen abgerufen werden, die den Suchkriterien entsprechen.</p> <p>Wenn Sie Oracle Hyperion Shared Services im Modus "Delegierte Administration" konfigurieren, setzen Sie diesen Wert auf "0".</p>   |

**Tabelle 4-1 (Fortsetzung) Fenster "Verbindungsinformationen"**

| Label   | Beschreibung   |
|---|--|
| Vertrauenswürdig  | Dieses Kontrollkästchen gibt an, dass es sich bei diesem Provider um eine vertrauenswürdige SSO-Quelle handelt. SSO-Tokens aus vertrauenswürdigen Quellen enthalten nicht das Benutzerkennwort.  |
| Anonymer Bind   | Das Kontrollkästchen gibt an, dass von Shared Services für die Suche nach Benutzern und Gruppen ein anonymes Binding zum Benutzerverzeichnis hergestellt werden kann. Diese Funktion kann nur verwendet werden, wenn das Benutzerverzeichnis anonyme Binds zulässt. Ist diese Option nicht ausgewählt, müssen Sie im Benutzer-DN ein Account mit ausreichender Zugriffsberechtigung angeben, um das Benutzerverzeichnis nach den dort hinterlegten Informationen durchsuchen zu können. Oracle empfiehlt, dass Sie keinen anonymen Bind verwenden.   |
| <div style="display: flex; align-items: center;"> <p><b>Hinweis:</b></p> </div> <p style="margin-left: 40px;">Anonymer Bind wird für OID nicht unterstützt.</p> |  |
| Benutzer-DN   | <p>Diese Option ist deaktiviert, wenn <b>Anonymer Bind</b> ausgewählt wurde.</p> <p>Distinguished Name (DN) des Benutzers, der von Shared Services zum Binding mit dem Benutzerverzeichnis herangezogen werden soll. Dieser Benutzer muss über Suchberechtigungen für das RDN-Attribut innerhalb des DNS verfügen. <b>Beispiel:</b> Im DN <code>cn=John Doe, ou=people, dc=myCompany, dc=com</code> muss dem Binding-Benutzer die Suchberechtigung für das <code>cn</code>-Attribut zugewiesen sein. Sonderzeichen im Benutzer-DN müssen mit Escape-Zeichen angegeben werden. Informationen zu Einschränkungen finden Sie unter <a href="#">Sonderzeichen verwenden</a>.</p> <p><b>Beispiel:</b> <code>cn=admin, dc=myCompany, dc=com</code></p> |
| Basis-DN anhängen   | <p>Mit diesem Kontrollkästchen kann der Basis-DN an den Benutzer-DN angehängt werden. Hängen Sie den Basis-DN nicht an, wenn Sie ein Verzeichnismanager-Account als Benutzer-DN verwenden.</p> <p>Dieses Kontrollkästchen ist deaktiviert, wenn die Option "Anonymer Bind" ausgewählt wurde.</p>   |
| Kennwort  | <p>Benutzer-DN-Kennwort</p> <p>Dieses Feld ist deaktiviert, wenn die Option "Anonymer Bind" ausgewählt wurde.</p> <p><b>Beispiel:</b> <code>UserDNpassword</code></p>  |
| Erweiterte Optionen anzeigen  | Mit diesem Kontrollkästchen zeigen Sie die erweiterten Optionen an.  |
| Bezüge  | <p><b>Nur Active Directory:</b></p> <p>Wurde Active Directory so konfiguriert, dass es Bezügen folgt, wählen Sie <code>follow</code> aus, damit den LDAP-Bezügen automatisch gefolgt wird. Wenn Sie keine Bezüge verwenden möchten, wählen Sie <code>Ignorieren</code> aus.</p>  |



Tabelle 4-1 (Fortsetzung) Fenster "Verbindungsinformationen"

| Label  | Beschreibung   |
|--|--|
| Aliasnamen dereferenzieren                             | Wählen Sie die Methode aus, die von der Shared Services-Suche verwendet werden soll, um Aliasnamen im Benutzerverzeichnis zu dereferenzieren, damit die Suche das Objekt abrufen kann, auf das der DN des Alias zeigt. Wählen Sie eine der folgenden Optionen aus: <ul style="list-style-type: none"> <li>• <b>Immer:</b> Aliasnamen immer dereferenzieren</li> <li>• <b>Nie:</b> Aliasnamen nie dereferenzieren</li> <li>• <b>Suche:</b> Aliasnamen nur während der Namensauflösung dereferenzieren</li> <li>• <b>Suchen:</b> Aliasnamen nur nach der Namensauflösung dereferenzieren</li> </ul>  |
| Timeout beim Lesen der Verbindung                      | Intervall (in Sekunden), nach dem der LDAP-Provider den LDAP-Leseversuch abbricht, falls keine Antwort erfolgt.<br><b>Standardwert:</b> 60 Sekunden  |
| Max. Verbindungen                                      | Maximale Anzahl der Verbindungen im Verbindungspool. Der Standardwert für LDAP-basierte Verzeichnisse, einschließlich Active Directory, lautet "100".<br><b>Standardwert:</b> 100  |
| Timeout  | Timeout für eine Verbindung mit dem Pool. Nach dieser Periode gibt das System eine Ausnahme aus.<br><b>Standardwert:</b> 300.000 Millisekunden (5 Minuten)   |
| Evict-Intervall  | <b>Optional:</b> Zeitintervall, nach dessen Verstreichen der Eviction-Prozess zum Löschen des Pools ausgeführt wird. Bei diesem Entfernungsprozess werden inaktive Verbindungen gelöscht, bei denen die Zulässige Zeit für inaktive Verbindung überschritten wurde.<br><b>Standardwert:</b> 120 Minuten  |
| Zulässige Zeit für inaktive Verbindung                 | <b>Optional:</b> Zeitspanne, nach welcher der Entfernungsprozess die inaktiven Verbindungen aus dem Pool entfernt.<br><b>Standardwert:</b> 120 Minuten   |
| Verbindungen erhöhen                                   | Diese Option gibt an, ob der Verbindungspool die unter <code>Max. Verbindungen</code> angegebene Anzahl übersteigen darf. Standardmäßig ist diese Option aktiviert. Wenn Sie das Anwachsen des Verbindungspools nicht zulassen, gibt das System einen Fehler zurück, wenn eine Verbindung nicht innerhalb der unter <code>Timeout</code> festgelegten Zeit verfügbar ist.  |
| Benutzerdefiniertes Authentifizierungsmodul aktivieren | Mit diesem Kontrollkästchen aktivieren Sie die Verwendung des benutzerdefinierten Authentifizierungsmoduls zur Authentifizierung von Benutzern, die in diesem Benutzerverzeichnis definiert sind. Sie müssen auch den vollqualifizierten Java-Klassennamen des Authentifizierungsmoduls im Fenster "Sicherheitsoptionen" angeben. Informationen hierzu finden Sie unter <a href="#">Sicherheitsoptionen festlegen</a> .<br>Die Authentifizierung über das benutzerdefinierte Authentifizierungsmodul ist transparent für Thin und Thick Clients und erfordert keine Änderungen an der Clientbereitstellung. Informationen hierzu finden Sie unter "Benutzerdefinierte Authentifizierungsmodule verwenden" in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i> . |

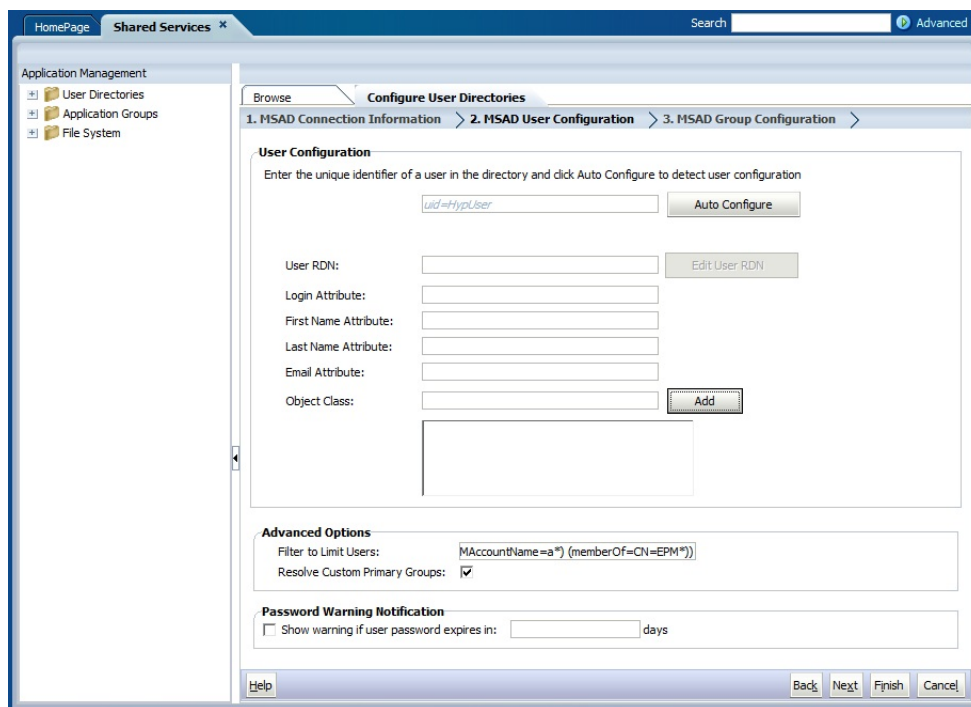
7. Klicken Sie auf **Weiter**.

Shared Services verwendet die in diesem Fenster definierten Eigenschaften, um einen Benutzer-URL zu erstellen. Dieser wiederum legt den Knoten fest, mit dem die Suche nach Benutzern beginnt. Die Verwendung dieser URLs beschleunigt die Suche.

**Achtung:**

Der Benutzer-URL darf nicht auf einen Aliasnamen verweisen. Die Sicherheit in EPM System setzt voraus, dass die Benutzer-URL auf einen tatsächlichen Benutzer verweist.

Oracle empfiehlt, in diesem Fenster den Bereich "Automatische Konfiguration" zum Abrufen der geforderten Daten zu nutzen.



**Hinweis:**

Eine Liste mit Sonderzeichen, die Sie bei der Benutzerkonfiguration verwenden können, finden Sie unter [Sonderzeichen verwenden](#).

8. Geben Sie unter **Automatische Konfiguration** eine eindeutige Benutzer-ID im Format `attribute=identifizier` ein. Beispiel: `uid=jdoe`.

Die Attribute von Benutzern werden im Bereich der Benutzerkonfiguration angezeigt.

Bei der Konfiguration von OID lässt sich der Benutzerfilter nicht automatisch konfigurieren, da die Root-DSE von OID keine Einträge im Attribut für

Benennungskontexte enthält. Informationen hierzu finden Sie unter [Benennungskontexte verwalten](#) in der Dokumentation *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

 **Hinweis:**

Sie können die benötigten Benutzerattribute manuell in die Textfelder der Benutzerkonfiguration eingeben.

**Tabelle 4-2 Fenster "Benutzerkonfiguration"**

| Label           | Beschreibung <sup>1</sup>   |
|-----------------|---|
| Benutzer-RDN    | Der relative DN des Benutzers. Jede Komponente eines DN wird als RDN bezeichnet und steht für einen Zweig in der Verzeichnisstruktur. Der RDN eines Benutzers ist in der Regel die Entsprechung von <code>uid</code> oder <code>cn</code> .<br>Informationen zu Einschränkungen finden Sie unter <a href="#">Sonderzeichen verwenden</a> .<br><b>Beispiel:</b> <code>ou=People</code>   |
| Anmeldeattribut | Ein eindeutiges Attribut (dies kann ein benutzerdefiniertes Attribut sein) speichert den Anmeldenamen des Benutzers. Benutzer verwenden den Wert dieses Attributs als Benutzernamen, wenn sie sich bei EPM System-Produkten anmelden.<br>Benutzer-IDs (Wert von Anmeldeattribut) müssen für alle Benutzerverzeichnisse eindeutig sein. Beispiel: Sie können <code>uid</code> bzw. <code>sAMAccountName</code> als Anmeldeattribut für Ihre SunONE- bzw. Ihre Active Directory-Konfiguration verwenden. Die Werte dieser Attribute müssen für alle Benutzerverzeichnisse, einschließlich Native Directory, eindeutig sein. |

 **Hinweis:**

Bei Benutzer-IDs muss die Groß- und Kleinschreibung nicht beachtet werden.

 **Hinweis:**

Wenn Sie OID als externes Benutzerverzeichnis für EPM System-Produkte konfigurieren, die in einer Kerberos-Umgebung auf Oracle Application Server bereitgestellt werden, müssen Sie diese Eigenschaft auf `userPrincipalName` setzen.

**Standardwert**

- **Active Directory:** `cn`
- **LDAP-Verzeichnisse außer Active Directory:** `uid`

**Tabelle 4-2 (Fortsetzung) Fenster "Benutzerkonfiguration"**

| Label              | Beschreibung <sup>1</sup>  |
|--------------------|--|
| Vornamensattribut  | Dieses Attribut speichert den Vornamen des Benutzers.<br><b>Standardwert:</b> givenName  |
| Nachnamensattribut | Dieses Attribut speichert den Nachnamen des Benutzers.<br><b>Standardwert:</b> sn  |
| E-Mail-Attribut    | <b>Optional:</b> Dieses Attribut speichert die E-Mail-Adresse des Benutzers.<br><b>Standardwert:</b> mail  |
| Objektklasse       | Objektklassen des Benutzers (die erforderlichen und optionalen Attribute, die dem Benutzer zugeordnet sind). Shared Services verwendet die in diesem Fenster aufgeführten Objektklassen im Suchfilter. So kann Shared Services alle Benutzer ermitteln, die eine Zugriffsberechtigung erhalten sollen. |

 **Hinweis:**

Wenn Sie den Benutzerverzeichnistyp `Other` verwenden, um Active Directory oder ADAM zu konfigurieren, und ein benutzerdefiniertes ID-Attribut verwenden möchten, müssen Sie diesen Wert auf `user` setzen.

Bei Bedarf können Sie Objektklassen manuell hinzufügen. Um eine Objektklasse hinzuzufügen, geben Sie den Namen der Objektklasse in das Feld **Objektklasse** ein und klicken auf **Hinzufügen**.

Um Objektklassen zu löschen, wählen Sie die Objektklasse aus und klicken auf **Entfernen**.

**Standardwert**

- **Active Directory:** user
- **LDAP-Verzeichnisse außer Active Directory:** person, organizationalPerson, inetorgperson

Filter zur Einschränkung der Benutzer

Diese LDAP-Abfrage ruft nur die Benutzer ab, denen EPM System-Produktrollen zugewiesen werden sollen. Beispiel: Die LDAP-Abfrage `(uid=Hyp*)` ruft nur Benutzer ab, deren Namen mit `Hyp` beginnen.

Im Fenster "Benutzerkonfiguration" wird der Benutzer-RDN validiert, außerdem wird bei Bedarf die Verwendung eines Benutzerfilters empfohlen.

Mit dem Benutzerfilter wird die Anzahl der Benutzer eingegrenzt, die von einer Abfrage zurückgegeben werden. Dies ist besonders sinnvoll, wenn der vom Benutzer-RDN ermittelte Knoten viele Benutzer umfasst, für die keine Zugriffsberechtigung erforderlich ist. Benutzerfilter können auch so eingesetzt werden, dass Benutzer, für die keine Zugriffsberechtigung erforderlich ist, ausgeschlossen werden. Dadurch wird die Leistung verbessert.

**Tabelle 4-2 (Fortsetzung) Fenster "Benutzerkonfiguration"**

| Label   | Beschreibung <sup>1</sup>   |
|---|---|
| Benutzersuchattribut für RDN mit mehreren Attributen  | <p><b>Nur LDAP-aktivierte Benutzerverzeichnisse außer Active Directory:</b> Legen Sie diesen Wert nur fest, wenn Ihr Verzeichnisserver zum Verwenden eines RDN mit mehreren Attributen konfiguriert ist. Der von Ihnen festgelegte Wert muss der eines der RDN-Attribute sein. Der Wert des Attributs, den Sie angeben, muss eindeutig sein, und das Attribut muss suchbar sein.</p> <p>Beispiel: Ein SunONE-Verzeichnisserver ist zum Kombinieren der Attribute "cn" (cn=John Doe) und "uid" (uid=jDoe12345) konfiguriert, um einen RDN mit mehreren Attributen ähnlich dem folgenden zu erstellen:</p> <pre>cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com</pre> <p>In diesem Fall können Sie <code>cn</code> oder <code>uid</code> verwenden, wenn diese Attribute die folgenden Bedingungen erfüllen:</p> <ul style="list-style-type: none"> <li>• Das Attribut ist von dem Benutzer suchbar, der im Feld "Benutzer-DN" in der Registerkarte "Verbindungsinformationen" angegeben wurde.</li> <li>• Sie müssen für das Attribut einen eindeutigen Wert im Benutzerverzeichnis festlegen.</li> </ul> |
| Lösen Sie benutzerdefinierte Primärgruppen auf.       | <p><b>Nur Active Directory:</b> Mit diesem Kontrollkästchen wird angegeben, ob Primärgruppen von Benutzern zur Festlegung effektiver Rollen bestimmt werden sollen. Dieses Kontrollkästchen ist standardmäßig ausgewählt. Oracle empfiehlt, diese Einstellung nicht zu ändern.</p>  |
| Warnung anzeigen bei Ablauf des Benutzerkennworts in: | <p><b>Nur Active Directory:</b> Mit diesem Kontrollkästchen wird festgelegt, ob eine Warnmeldung angezeigt werden soll, wenn das Active Directory-Benutzerkennwort innerhalb der angegebenen Anzahl von Tagen abläuft.</p>  |

<sup>1</sup> EPM System-Sicherheit kann Standardwerte für Felder verwenden, für die ein Konfigurationswert optional ist. Wenn Sie in diese Felder keine Werte eingeben, werden während der Laufzeit Standardwerte verwendet.

**9. Klicken Sie auf Weiter.**

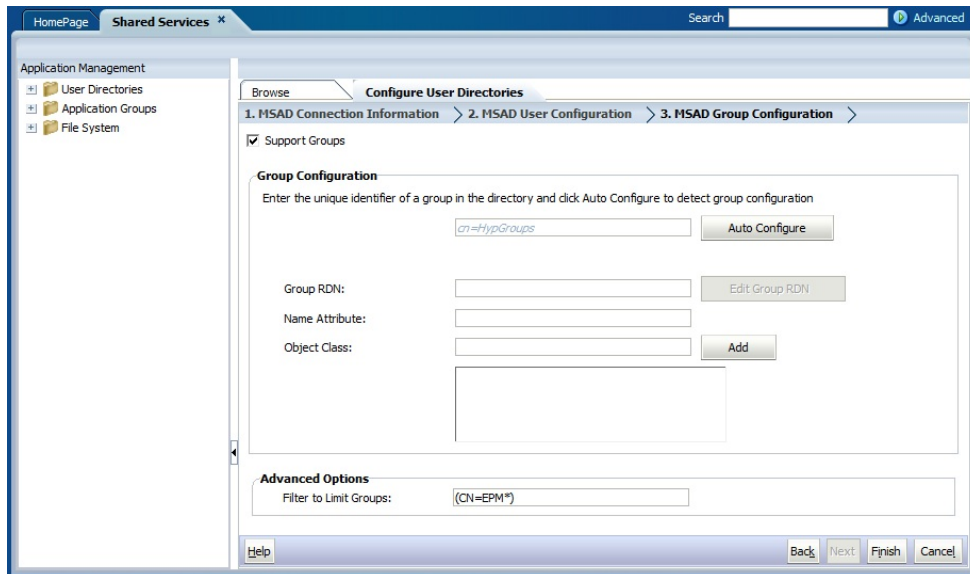
Das Fenster "Gruppenkonfiguration" wird angezeigt. Shared Services verwendet die in diesem Fenster definierten Eigenschaften, um einen Gruppen-URL zu erstellen. Dieser wiederum legt den Knoten fest, mit dem die Suche nach Gruppen beginnt. Die Verwendung dieses URLs beschleunigt die Suche.

**▲ Achtung:**

Der Gruppen-URL darf nicht auf einen Aliasnamen verweisen. Die EPM System-Sicherheit erfordert, dass der Gruppen-URL auf eine tatsächliche Gruppe verweist. Wenn Sie ein Novell eDirectory konfigurieren, das Gruppenaliasnamen und Gruppen-Accounts verwendet, müssen diese im Gruppen-URL verfügbar sein.

 **Hinweis:**

Die Dateneingabe in das Fenster für die Gruppenkonfiguration ist optional. Wenn Sie die Einstellungen für den Gruppen-URL nicht vornehmen, sucht Shared Services innerhalb des Basis-DN nach Gruppen. Dies kann sich nachteilig auf die Leistung auswirken, besonders, wenn das Benutzerverzeichnis viele Gruppen enthält.



10. Deaktivieren Sie die Option **Gruppen unterstützen**, wenn Ihre Organisation nicht vorhat, eine Zugriffsberechtigung für Gruppen zu erteilen, oder wenn die Benutzer im Benutzerverzeichnis nicht in Gruppen kategorisiert werden. Wenn Sie diese Option deaktivieren, werden die Felder dieses Fensters deaktiviert.

Wenn Gruppen unterstützt werden, empfiehlt Oracle, die Funktion zur automatischen Konfiguration zum Abrufen der benötigten Daten zu verwenden.

Wenn Sie OID als Benutzerverzeichnis konfigurieren, können Sie die Funktion zur automatischen Konfiguration nicht nutzen, da die Root-DSE von OID keine Einträge im Attribut für Benennungskontexte enthält. Informationen hierzu finden Sie unter [Benennungskontexte verwalten](#) in der Dokumentation *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

11. Geben Sie im Textfeld **Automatische Konfiguration** eine eindeutige Gruppen-ID ein, und klicken Sie auf **Los**.

Die Gruppen-ID muss im Format `attribute=identifizier` angegeben werden.  
Beispiel: `cn=western_region`.

Die Attribute von Gruppen werden im Bereich der Gruppenkonfiguration angezeigt.

 **Hinweis:**

Sie können die benötigten Gruppenattribute in die Textfelder der Gruppenkonfiguration eingeben.

 **Achtung:**

Wenn die Gruppen-URL nicht für Benutzerverzeichnisse festgelegt wurde, die das Zeichen / (Schrägstrich) oder \ (umgekehrter Schrägstrich) im Knotennamen enthalten, ist die Suche nach Benutzern und Gruppen nicht erfolgreich. Beispiel: Benutzer oder Gruppen können nicht aufgelistet werden, wenn keine Gruppen-URL für ein Benutzerverzeichnis angegeben wurde, in dem Benutzer und Gruppen in einem Knoten wie `OU=child\ou,OU=parent/ou` oder `OU=child/ou,OU=parent \ ou` vorhanden sind.

**Tabelle 4-3 Fenster "Gruppenkonfiguration"**

| Label       | Beschreibung <sup>1</sup>   |
|-------------|---|
| Gruppen-RDN | <p>Der relative DN der Gruppe. Dieser Wert ist der relative Pfad für den Basis-DN und wird als Gruppen-URL verwendet. Geben Sie einen Gruppen-RDN an, der den niedrigsten Benutzerverzeichnisknoten identifiziert, in dem alle Gruppen verfügbar sind, die eine Zugriffsberechtigung erhalten sollen.</p> <p>Wenn Sie eine primäre Active Directory-Gruppe für das Provisioning verwenden, müssen Sie sicherstellen, dass die primäre Gruppe den Gruppen-RDN aufweist. Shared Services ruft die primäre Gruppe nicht ab, wenn sie sich außerhalb des gültigen Bereichs für die Gruppen-URL befindet.</p> <p>Der Gruppen-RDN wirkt sich erheblich auf die Leistung bei Anmeldung und Suche aus. Da es sich um den Startpunkt aller Gruppensuchen handelt, müssen Sie den niedrigsten Knoten ermitteln, in dem alle Gruppen für EPM System-Produkte verfügbar sind. Zur Gewährleistung der optimalen Leistung sollte die Anzahl der Gruppen im Gruppen-RDN nicht über 10.000 steigen. Falls mehrere Gruppen vorhanden sind, verwenden Sie einen Gruppenfilter, um nur die Gruppen abzurufen, denen Sie Zugriffsberechtigungen erteilen möchten.</p> |


 **Hinweis:**

Shared Services zeigt eine Warnung an, wenn die Anzahl der verfügbaren Gruppen im Gruppen-URL höher als 10.000 ist.

Informationen zu Einschränkungen finden Sie unter [Sonderzeichen verwenden](#).

**Beispiel:** `ou=Groups`

**Tabelle 4-3 (Fortsetzung) Fenster "Gruppenkonfiguration"**

| Label                                | Beschreibung <sup>1</sup>  |
|--------------------------------------|--|
| Namensattribut                       | <p>Dieses Attribut speichert den Gruppennamen.</p> <p><b>Standardwert</b></p> <ul style="list-style-type: none"> <li>• <b>LDAP-Verzeichnisse einschließlich Active Directory:</b> <code>cn</code></li> <li>• <b>Native Directory:</b> <code>cssDisplayNameDefault</code></li> </ul>  |
| Objektklasse                         | <p>Objektklassen der Gruppe. Shared Services verwendet die in diesem Fenster aufgeführten Objektklassen im Suchfilter. So kann Shared Services alle Gruppen ermitteln, die einem Benutzer zugeordnet sind.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Hinweis:</b></p> <p>Wenn Sie den Benutzerverzeichnistyp <code>Other</code> verwenden, um Active Directory oder ADAM zu konfigurieren, und ein benutzerdefiniertes ID-Attribut verwenden möchten, müssen Sie diesen Wert auf <code>group?member</code> setzen.</p> </div> <p>Bei Bedarf können Sie Objektklassen manuell hinzufügen. Um eine Objektklasse hinzuzufügen, geben Sie den Namen der Objektklasse in das Textfeld "Objektklasse" ein, und klicken Sie auf <b>Hinzufügen</b>.</p> <p>Um Objektklassen zu löschen, wählen Sie die Objektklasse aus, und klicken Sie auf <b>Entfernen</b>.</p> <p><b>Standardwert</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory:</b> <code>group?member</code></li> <li>• <b>LDAP-Verzeichnisse außer Active Directory:</b> <code>groupofuniquenames?uniquemember, groupOfNames?member</code></li> <li>• <b>Native Directory:</b> <code>groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive</code></li> </ul> |
| Filter zur Einschränkung der Gruppen | <p>Diese LDAP-Abfrage ruft nur die Gruppen ab, denen EPM System-Produktrollen zugewiesen werden sollen. Beispiel: Die LDAP-Abfrage <code>( (cn=Hyp*)(cn=Admin*))</code> ruft nur Gruppen ab, deren Namen mit <code>Hyp</code> oder <code>Admin</code> beginnen.</p> <p>Mit dem Gruppenfilter wird die Anzahl der Gruppen eingegrenzt, die von einer Abfrage zurückgegeben wird. Dies ist besonders sinnvoll, wenn der vom Gruppen-RDN ermittelte Knoten viele Gruppen umfasst, für die keine Zugriffsberechtigung erforderlich ist. Die Filter können auch so eingesetzt werden, dass solche Gruppen ausgeschlossen werden, deren Zugriffsberechtigung nicht nötig ist. Dadurch wird eine Leistungsverbesserung erzielt.</p> <p>Wenn Sie die primäre Active Directory-Gruppe für das Provisioning verwenden, müssen Sie sicherstellen, dass alle Gruppenfilter, die Sie festlegen, die im gültigen Bereich der Gruppen-URL enthaltene primäre Gruppe abrufen können. Beispiel: Der Filter <code>( (cn=Hyp*)(cn=Domain Users))</code> ruft Gruppen ab, deren Name mit <code>Hyp</code> beginnt und deren primäre Gruppe den Namen <code>Domain Users</code> hat.</p>  |



<sup>1</sup> EPM System-Sicherheit kann Standardwerte für Felder verwenden, für die ein Konfigurationswert optional ist. Wenn Sie in diese Felder keine Werte eingeben, werden während der Laufzeit Standardwerte verwendet.

**12. Klicken Sie auf **Fertig stellen**.**

Shared Services speichert die Konfiguration und zeigt wieder das Fenster "Definierte Benutzerverzeichnisse" an. Hier wird nun das von Ihnen konfigurierte Benutzerverzeichnis aufgeführt.

**13. Testen Sie die Konfiguration.** Informationen hierzu finden Sie unter [Benutzerverzeichnisverbindungen testen](#).

**14. Ändern Sie die Suchreihenfolge, falls erforderlich.** Ausführliche Informationen finden Sie unter [Suchreihenfolge des Benutzerverzeichnisses verwalten](#).

**15. Legen Sie die Sicherheitsoptionen fest, falls erforderlich.** Ausführliche Informationen finden Sie unter [Sicherheitsoptionen festlegen](#).

**16. Starten Sie Oracle Hyperion Foundation Services und andere EPM System-Komponenten erneut.**

## Relationale Datenbanken als Benutzerverzeichnisse konfigurieren

Benutzer- und Gruppeninformationen aus den Systemtabellen der relationalen Datenbanken von Oracle, SQL Server und IBM DB2 können verwendet werden, um die Zuweisung von Berechtigungen zu unterstützen. Wenn Gruppeninformationen nicht aus dem Systemschema der Datenbank abgeleitet werden können, unterstützt Oracle Hyperion Shared Services das Provisioning für Gruppen von diesem Datenbankprovider nicht. Beispiel: Shared Services kann keine Gruppeninformationen aus alten IBM DB2-Versionen extrahieren, da die Datenbank Gruppen verwendet, die im Betriebssystem definiert sind. Provisioning-Manager können jedoch diese Benutzer Gruppen in Native Directory hinzufügen und diesen Gruppen Zugriffsberechtigungen zuweisen. Informationen zu unterstützten Plattformen finden Sie unter *Oracle Enterprise Performance Management System Certification Matrix* auf der Seite [Oracle Fusion Middleware Supported System Configurations](#) des Oracle Technology Network (OTN).



**Hinweis:**

Wenn Sie eine DB2-Datenbank verwenden, muss der Benutzername mindestens acht Zeichen enthalten. Benutzernamen dürfen höchstens 256 Zeichen (Oracle- und SQL-Serverdatenbanken) bzw. 1000 Zeichen (DB2) enthalten.

Konfigurieren Sie Shared Services so, dass es sich als Datenbankadministrator mit der Datenbank verbindet, beispielsweise als Oracle `SYSTEM`- Benutzer, um eine Liste aller Benutzer und Gruppen zu erhalten.

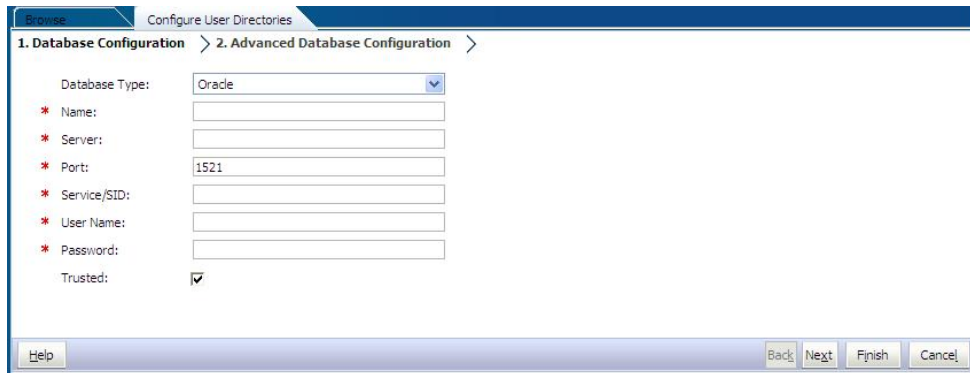


**Hinweis:**

Shared Services weist nur aktiven Datenbankbenutzern Zugriffsberechtigungen zu. Inaktive und gesperrte Datenbankbenutzer-Accounts werden ignoriert.

So konfigurieren Sie Datenbankprovider:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Klicken Sie auf **Neu**.
4. Wählen Sie im Fenster **Verzeichnistyp** die Option **Relationale Datenbank (Oracle, DB2, SQL Server)** aus.
5. Klicken Sie auf **Weiter**.



6. Geben Sie die Konfigurationsparameter in der Registerkarte "Datenbankkonfiguration" ein.

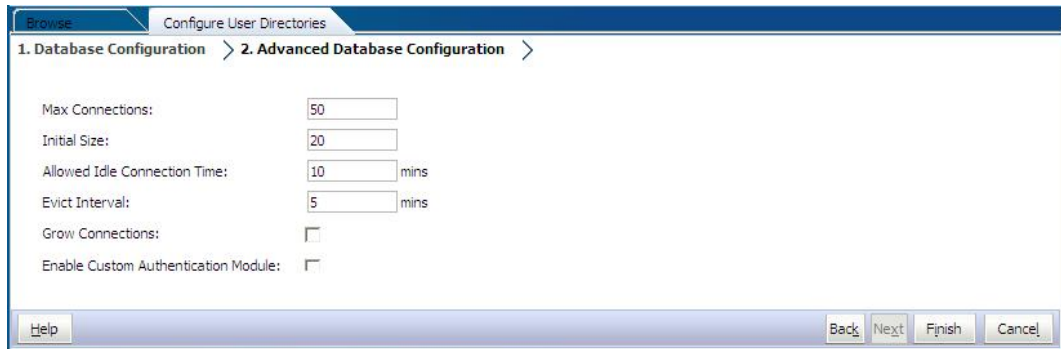
**Tabelle 4-4 Registerkarte "Datenbankkonfiguration"**

| Label                              | Beschreibung   |
|------------------------------------|--|
| Datenbanktyp                       | Der relationale Datenbankprovider. Shared Services unterstützt nur Oracle und SQL Server als Datenbankprovider.<br><b>Beispiel:</b> Oracle |
| Name                               | Ein eindeutiger Konfigurationsname für den Datenbankprovider<br><b>Beispiel:</b> Oracle_DB_FINANCE   |
| Server                             | Der DNS-Name des Computers, auf dem der Datenbankserver ausgeführt wird<br><b>Beispiel:</b> myserver                                       |
| Port                               | Die Port-Nummer des Datenbankservers<br><b>Beispiel:</b> 1521  |
| Service/SID (nur Oracle)           | Der Systembezeichner (Standard ist orcl)<br><b>Beispiel:</b> orcl  |
| Datenbank (nur SQL Server und DB2) | Die Datenbank, zu der Shared Services eine Verbindung herstellen soll<br><b>Beispiel:</b> master   |

**Tabelle 4-4 (Fortsetzung) Registerkarte "Datenbankkonfiguration"**

| Label            | Beschreibung   |
|------------------|--|
| Benutzername     | Der Benutzername, den Shared Services für den Zugriff auf die Datenbank verwenden sollte. Diese Datenbank muss Zugriffsberechtigungen auf Datenbank-Systemtabellen haben. Oracle empfiehlt, den Account <code>system</code> für Oracle-Datenbanken und den Benutzernamen des Datenbankadministrators für SQL Server-Datenbanken zu verwenden.<br><b>Beispiel:</b> SYSTEM |
| Kennwort         | Das Kennwort des Benutzers, festgelegt in <b>Benutzername</b><br><b>Beispiel:</b> system_password  |
| Vertrauenswürdig | Kontrollkästchen, mit dem festgelegt wird, dass der Provider eine vertrauenswürdige SSO-Quelle ist. SSO-Tokens aus vertrauenswürdigen Quellen enthalten nicht das Benutzerkennwort.  |

7. **Optional:** Klicken Sie auf **Weiter**, um den Verbindungspool zu konfigurieren. Die Registerkarte "Erweiterte Datenbankkonfiguration" wird geöffnet.



8. In der Registerkarte "Erweiterte Datenbankkonfiguration" geben Sie die Verbindungspool-Parameter ein.

**Tabelle 4-5 Registerkarte "Erweiterte Datenbankkonfiguration"**

| Label                                     | Beschreibung   |
|---|--|
| Max. Verbindungen<br>Ausgangsgröße        | Maximale Verbindungen im Pool. Der Standardwert ist 50.<br>Verfügbare Verbindungen, wenn der Pool initialisiert wird. Der Standardwert ist 20.   |
| Zulässige Zeit für inaktive<br>Verbindung | <b>Optional:</b> Zeitspanne, nach welcher der Entfernungsprozess die inaktiven Verbindungen aus dem Pool entfernt. Der Standardwert ist 10 Minuten.  |
| Evict-Intervall                           | <b>Optional:</b> Das Intervall für das Ausführen des Entfernungsprozesses, um den Pool zu bereinigen. Bei der Entfernung werden die inaktiven Verbindungen gelöscht, bei denen der Wert im Feld Zulässige Zeit für inaktive Verbindung überschritten wurde. Der Standardwert ist fünf Minuten. |

**Tabelle 4-5 (Fortsetzung) Registerkarte "Erweiterte Datenbankkonfiguration"**

| Label  | Beschreibung   |
|--|--|
| Verbindungen erhöhen                                   | Gibt an, ob der Verbindungspool über die unter <i>Max.</i> Verbindungen angegebene Zahl hinaus wachsen kann. Standardmäßig ist diese Option nicht aktiviert, sodass der Pool nicht anwachsen kann. Wenn Sie das Anwachsen des Verbindungspools nicht zulassen, gibt das System einen Fehler zurück, wenn eine Verbindung nicht innerhalb der unter <i>Timeout</i> festgelegten Zeit verfügbar ist.   |
| Benutzerdefiniertes Authentifizierungsmodul aktivieren | Mit diesem Kontrollkästchen aktivieren Sie die Verwendung des benutzerdefinierten Authentifizierungsmoduls zur Authentifizierung von Benutzern, die in diesem Benutzerverzeichnis definiert sind. Sie müssen auch den vollqualifizierten Java-Klassennamen des Authentifizierungsmoduls im Fenster "Sicherheitsoptionen" angeben. Informationen hierzu finden Sie unter <a href="#">Sicherheitsoptionen festlegen</a> .<br>Die Authentifizierung des benutzerdefinierten Authentifizierungsmoduls ist sowohl für Thin Clients als auch für Thick Clients transparent. Informationen hierzu finden Sie unter "Benutzerdefinierte Authentifizierungsmodule verwenden" in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i> . |

9. Klicken Sie auf **Fertig stellen**.
10. Klicken Sie auf **OK**, um zum Fenster "Definierte Benutzerverzeichnisse" zurückzukehren.
11. Testen Sie die Datenbank-Providerkonfiguration. Informationen hierzu finden Sie unter [Benutzerverzeichnisverbindungen testen](#).
12. Ändern Sie die Suchreihenfolge, falls erforderlich. Ausführliche Informationen finden Sie unter [Suchreihenfolge des Benutzerverzeichnisses verwalten](#).
13. Geben Sie Sicherheitseinstellungen an, wenn erforderlich. Informationen hierzu finden Sie unter [Sicherheitsoptionen festlegen](#).
14. Starten Sie Oracle Hyperion Foundation Services und weitere Oracle Enterprise Performance Management System-Komponenten erneut.

## Benutzerverzeichnisverbindungen testen

Testen Sie nach dem Konfigurieren eines Benutzerverzeichnisses die Verbindung, um sicherzustellen, dass Oracle Hyperion Shared Services mit den aktuellen Einstellungen eine Verbindung mit dem Benutzerverzeichnis herstellen kann.

So testen Sie eine Benutzerverzeichnisverbindung:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie in der Liste der Benutzerverzeichnisse die Konfiguration eines externen Benutzerverzeichnisses aus, die getestet werden soll.
4. Klicken Sie auf **Testen, OK**.

## Einstellungen der Benutzerverzeichnisse ändern

Administratoren können beliebige Parameter einer Benutzerverzeichniskonfiguration außer dem Namen ändern. Oracle empfiehlt, die Konfigurationsdaten von Benutzerverzeichnissen, die zur Zuweisung von Zugriffsberechtigungen verwendet wurden, nicht zu ändern.

### **Achtung:**

Durch Änderung von Einstellungen in der Benutzerverzeichniskonfiguration, z.B. ID-Attribut, werden die Zugriffsberechtigungsdaten unwirksam. Gehen Sie extrem vorsichtig vor, wenn Sie die Einstellungen eines Benutzerverzeichnisses mit Zugriffsberechtigungszuweisungen ändern.

So ändern Sie eine Benutzerverzeichnisverbindung:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie ein zu bearbeitendes Benutzerverzeichnis aus.
4. Klicken Sie auf **Bearbeiten**.
5. Ändern Sie die Konfigurationseinstellungen.

### **Hinweis:**

Sie können den Konfigurationsnamen nicht ändern. Wenn Sie die Konfiguration eines LDAP-Benutzerverzeichnisses ändern, können Sie einen anderen Verzeichnisserver oder *Sonstige* (für benutzerdefinierte LDAP-Verzeichnisse) aus der Verzeichnisserverliste auswählen. Native Directory-Parameter können nicht bearbeitet werden.

Erklärungen zu den Parametern, die Sie ändern können, finden Sie in folgenden Tabellen:

- Active Directory und andere LDAP-basierte Benutzerverzeichnisse finden Sie in den Tabellen in [OID, Active Directory und andere LDAP-basierte Benutzerverzeichnisse konfigurieren](#).
  - Datenbanken: Siehe Tabelle in [Relationale Datenbanken als Benutzerverzeichnisse konfigurieren](#).
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

## Benutzerverzeichniskonfigurationen löschen

Systemadministratoren können eine Konfiguration eines externen Benutzerverzeichnisses jederzeit löschen. Beim Löschen einer Konfiguration werden alle

Zugriffsberechtigungsinformationen für die Benutzer und Gruppen aus dem Verzeichnis unwirksam. Das Verzeichnis wird aus der Suchreihenfolge entfernt.

 **Tipp:**

Wenn Sie kein konfiguriertes Benutzerverzeichnis verwenden möchten, das zur Zuweisung von Zugriffsberechtigungen verwendet wurde, entfernen Sie es aus der Suchreihenfolge, sodass es nicht nach Benutzern und Gruppen durchsucht wird. Diese Aktion erhält die Integrität der Zugriffsberechtigungsinformationen und ermöglicht Ihnen, das Benutzerverzeichnis später noch zu verwenden.

So löschen Sie eine Benutzerverzeichniskonfiguration:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie ein Verzeichnis aus.
4. Klicken Sie auf **Löschen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie erneut auf **OK**.
7. Starten Sie Oracle Hyperion Foundation Services und weitere Oracle Enterprise Performance Management System-Komponenten erneut.

## Suchreihenfolge des Benutzerverzeichnisses verwalten

Wenn ein Systemadministrator ein externes Benutzerverzeichnis konfiguriert, fügt Oracle Hyperion Shared Services das Benutzerverzeichnis der Suchsequenz automatisch hinzu und weist dem Benutzerverzeichnis die nächste verfügbare Suchsequenz vor der Native Directory-Suchsequenz zu. Die Suchreihenfolge wird für die Durchläufe in den konfigurierten Benutzerverzeichnissen verwendet, wenn Oracle Enterprise Performance Management System nach Benutzern und Gruppen sucht.

Systemadministratoren können Benutzerverzeichnisse aus der Suchreihenfolge entfernen. In diesem Fall weist Shared Services die Suchreihenfolge der verbleibenden Verzeichnisse automatisch neu zu. Benutzerverzeichnisse, die nicht in der Suchreihenfolge enthalten sind, werden nicht zur Unterstützung von Authentifizierung und Zuweisung von Zugriffsberechtigungen verwendet.

 **Hinweis:**

Shared Services beendet die Suche nach dem Benutzer bzw. nach der Gruppe, wenn der angegebene Account gefunden wurde. Oracle empfiehlt, das Unternehmensverzeichnis, in dem die meisten EPM System-Benutzer enthalten sind, bei der Suchreihenfolge an erster Stelle anzugeben.

Standardmäßig ist Native Directory in der Suchreihenfolge als letztes Verzeichnis festgelegt. Administratoren können die folgenden Aufgaben ausführen, um die Suchreihenfolge zu verwalten:

- [Benutzerverzeichnis der Suchreihenfolge hinzufügen](#)
- [Suchreihenfolge ändern](#)
- [Zuweisung einer Suchreihenfolge entfernen](#)

### Benutzerverzeichnis der Suchreihenfolge hinzufügen

Ein neu konfiguriertes Benutzerverzeichnis wird der Suchreihenfolge automatisch hinzugefügt. Wenn Sie ein Verzeichnis aus der Suchreihenfolge entfernen, können Sie es am Ende der Suchreihenfolge hinzufügen.

So fügen Sie der Suchreihenfolge ein Benutzerverzeichnis hinzu:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie ein deaktiviertes Benutzerverzeichnis aus, das der Suchreihenfolge hinzugefügt werden soll.
4. Klicken Sie auf **Einschließen**.  
Diese Schaltfläche ist nur verfügbar, wenn Sie ein Benutzerverzeichnis ausgewählt haben, das nicht in der Suchreihenfolge enthalten ist.
5. Klicken Sie auf **OK**, um zum Fenster "Definierte Benutzerverzeichnisse" zurückzukehren.
6. Starten Sie Oracle Hyperion Foundation Services und andere EPM System-Komponenten erneut.

### Zuweisung einer Suchreihenfolge entfernen

Wenn Sie ein Benutzerverzeichnis aus der Suchreihenfolge entfernen, wird die Verzeichniskonfiguration dadurch nicht ungültig. Das Benutzerverzeichnis wird aus der Liste der Verzeichnisse entfernt, die beim Authentifizieren der Benutzer durchsucht werden. Ein Verzeichnis, das nicht in der Suchreihenfolge enthalten ist, wird auf den Status *Deaktiviert* gesetzt. Wenn ein Administrator ein Benutzerverzeichnis aus der Suchreihenfolge entfernt, wird die Suchfolge, die den anderen Benutzerverzeichnissen zugewiesen ist, automatisch aktualisiert.



#### Hinweis:

Native Directory kann nicht aus der Suchreihenfolge entfernt werden.

So entfernen Sie ein Benutzerverzeichnis aus der Suchreihenfolge:

1. Greifen Sie als Systemadministrator auf Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie ein Verzeichnis aus, das aus der Suchreihenfolge entfernt werden soll.
4. Klicken Sie auf **Ausschließen**.

5. Klicken Sie auf **OK**.
6. Klicken Sie im Fenster "Ergebnis Verzeichniskonfiguration" auf **OK**.
7. Starten Sie Foundation Services und andere EPM System-Komponenten erneut.

### Suchreihenfolge ändern

Die Standardsuchreihenfolge, die den einzelnen Benutzerverzeichnissen zugewiesen ist, basiert auf der Reihenfolge, in der das Verzeichnis konfiguriert wurde. Standardmäßig ist Native Directory in der Suchreihenfolge als letztes Verzeichnis festgelegt.

So ändern Sie die Suchreihenfolge:

1. Greifen Sie als Systemadministrator auf Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie ein Verzeichnis aus, dessen Suchreihenfolge Sie ändern möchten.
4. Klicken Sie auf **Nach oben** oder **Nach unten**.
5. Klicken Sie auf **OK**.
6. Starten Sie Foundation Services, andere EPM System-Komponenten sowie benutzerdefinierte Anwendungen, die die Sicherheits-APIs von Shared Services verwenden, erneut.

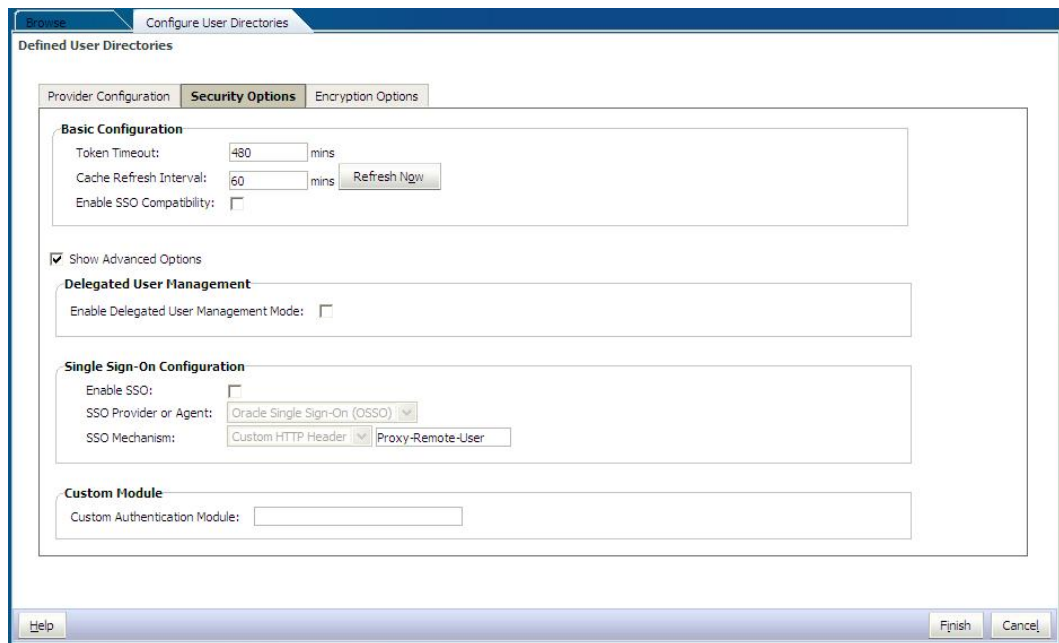
## Sicherheitsoptionen festlegen

Die Sicherheitsoptionen umfassen die globalen Parameter, die für alle Benutzerverzeichnisse in der Suchreihenfolge gelten.

So legen Sie Sicherheitsoptionen fest:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie **Sicherheitsoptionen** aus.
4. Legen Sie unter **Sicherheitsoptionen** die globalen Parameter fest.





**Tabelle 4-6 Sicherheitsoptionen für Benutzerverzeichnisse**

| Parameter                           | Beschreibung  |
|-------------------------------------|---|
| Token timeout                       | Zeit (in Minuten), nach der das SSO-Token abläuft, das von Oracle Enterprise Performance Management System-Produkten oder von der Webidentitätsmanagement-Lösung ausgestellt wurde. Benutzer müssen sich nach dieser Periode neu anmelden. Der Token timeout wird basierend auf der Systemuhr des Servers festgelegt. Der Standardwert ist 480 Minuten.   |
| Aktualisierungsintervall des Caches | Intervall (in Minuten) für die Aktualisierung des Oracle Hyperion Shared Services-Caches von Gruppen für Benutzerbeziehungsdaten. Der Standardwert ist 60 Minuten. Shared Services cacht Informationen zu neuen externen Benutzerverzeichnisgruppen und neuen Benutzern, die erst nach der nächsten Cache-Aktualisierung zu vorhandenen Gruppen hinzugefügt werden. Benutzer, denen Zugriffsberechtigungen durch eine neu erstellte externe Benutzerverzeichnisgruppe zugewiesen wurden, erhalten die Zugriffsberechtigung auf Ihre Rollen nicht, bis der Cache aktualisiert ist. |


 **Hinweis:**

Ein Token timeout ist etwas anderes als ein Session timeout.

**Tabelle 4-6 (Fortsetzung) Sicherheitsoptionen für Benutzerverzeichnisse**

| Parameter   | Beschreibung   |
|---|--|
| Jetzt aktualisieren                               | Klicken Sie auf diese Schaltfläche, um die Aktualisierung des Shared Services-Caches, der Gruppen für Benutzerbeziehungsdaten enthält, manuell zu initiieren. Sie möchten möglicherweise eine Cache-Aktualisierung initiieren, nachdem Sie neue Gruppen in externen Benutzerverzeichnissen erstellt haben sowie Zugriffsberechtigungen für diese zugewiesen haben oder nachdem Sie neue Benutzer vorhandenen Gruppen hinzugefügt haben. Der Cache wird erst aktualisiert, nachdem Shared Services einen Aufruf ausführt, der die Daten im Cache verwendet.   |
| SSO-Kompatibilität aktivieren                     | Wählen Sie diese Option aus, wenn Ihre Bereitstellung in Oracle Business Intelligence Enterprise Edition Release 11.1.1.5 oder eine frühere Version integriert ist.  |
| Modus "Delegiertes Benutzermanagement" aktivieren | Option, mit der Sie das delegierte Benutzermanagement von EPM System-Produkten aktivieren können, um das verteilte Management von Zugriffsberechtigungsaktivitäten zu unterstützen. Informationen hierzu finden Sie im Abschnitt zum delegierten Benutzermanagement in der <i>Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit</i> .   |
| SSO aktivieren                                    | Option, mit der Sie die SSO-Unterstützung für Security Agents wie Oracle Access Manager aktivieren   |
| SSO-Provider oder -Agent                          | Wählen Sie die Webidentitätsmanagement-Lösung aus, über die EPM System-Produkte SSO akzeptieren sollen. Wählen Sie <b>Sonstige</b> aus, wenn Ihre Webidentitätsmanagement-Lösung nicht aufgeführt ist (z.B. Kerberos).<br>Der bevorzugte SSO-Mechanismus und -Name werden automatisch ausgewählt, wenn Sie den SSO-Provider auswählen. Sie können den Namen des SSO-Mechanismus (des HTTP-Headers oder der benutzerdefinierten Anmeldeklasse) ändern, falls erforderlich.<br>Wenn Sie <i>Sonstige</i> als SSO-Provider oder -Agent wählen, müssen Sie sicherstellen, dass dieser SSO-Provider oder -Agent ein mit dem EPM System-kompatibles SSO-Verfahren unterstützt. Informationen hierzu finden Sie unter "Unterstützte SSO-Methoden" in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i> . |

**Tabelle 4-6 (Fortsetzung) Sicherheitsoptionen für Benutzerverzeichnisse**

| Parameter       | Beschreibung  |
|-----------------|---|
| SSO-Mechanismus | <p>Die Methode, mit der die gewählte Webidentitäts-Managementlösung die Anmeldenamen der Benutzer für EPM System-Produkte bereitstellt. Eine Beschreibung der zulässigen SSO-Methoden finden Sie im Abschnitt zu unterstützten SSO-Methoden in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i>.</p> <ul style="list-style-type: none"> <li>Benutzerdefinierter HTTP-Header: Legen Sie den Namen des Headers fest, den der Sicherheitsagent an EPM System übergibt.</li> <li>Benutzerdefinierte Anmeldekasse: Geben Sie die benutzerdefinierte Java-Klasse an, die HTTP-Anforderungen für die Authentifizierung verarbeitet. Informationen hierzu finden Sie unter "Benutzerdefinierte Anmeldekasse" in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i>.</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> <b>Hinweis:</b></p> <p>Benutzerdefinierte Anmeldekasse ist nicht identisch mit der benutzerdefinierten Authentifizierung.</p> </div> <ul style="list-style-type: none"> <li>HTTP-Autorisierungs-Header: Dies ist der HTTP-Standardmechanismus.</li> <li>Remote-Benutzer aus HTTP-Anforderung abrufen: Wählen Sie diese Option aus, wenn der Security Agent den Remote-Benutzer in der HTTP-Anforderung ausfüllt.</li> </ul> |

**Tabelle 4-6 (Fortsetzung) Sicherheitsoptionen für Benutzerverzeichnisse**

| Parameter                                   | Beschreibung   |
|---|--|
| Benutzerdefiniertes Authentifizierungsmodul | <p>Der vollqualifizierte Java-Klassenname des benutzerdefinierten Authentifizierungsmoduls (z.B. <code>com.mycompany.epm.CustomAuthenticationImpl</code>), das zum Authentifizieren von Benutzern in allen Benutzerverzeichnissen verwendet werden soll, für die das benutzerdefinierte Authentifizierungsmodul ausgewählt wurde.</p> <p>Das Authentifizierungsmodul wird für ein Benutzerverzeichnis nur verwendet, wenn bei der Verzeichniskonfiguration die Verwendung aktiviert wurde (Standard).</p> <p>Oracle Hyperion Foundation Services erfordert, dass die JAR-Datei für die benutzerdefinierte Authentifizierung den Namen <code>CustomAuth.jar</code> hat. <code>CustomAuth.jar</code> muss im Verzeichnis <code>MIDDLEWARE_HOME\user_projects\domains\WEBLOGIC_DOMAIN\lib</code> verfügbar sein. Dieses lautet in der Regel <code>C:\Oracle\Middleware\user_projects\domains\EPMSys\lib</code>.</p> <p>Die Datei <code>CustomAuth.jar</code> muss in allen Clientinstallationen im Verzeichnis <code>EPM_ORACLE_HOME/common/jlib/11.1.2.0</code> vorhanden sein. Dieses lautet in der Regel <code>C:\Oracle\Middleware\EPMSys11R1\common\jlib\11.1.2.0</code>.</p> <p>In der JAR-Datei können Sie eine beliebige Paketstruktur und einen beliebigen Klassennamen verwenden. Informationen hierzu finden Sie unter "Benutzerdefinierte Authentifizierungsmodule verwenden" in der Dokumentation <i>Oracle Enterprise Performance Management System - Sicherheitskonfiguration</i>.</p> |

5. Klicken Sie auf **OK**.
6. Starten Sie Foundation Services und andere EPM System-Komponenten erneut.

## Verschlüsselungsschlüssel erneut generieren

Oracle Enterprise Performance Management System verwendet die folgenden Sicherheitsschlüssel:

- Verschlüsselungsschlüssel für Single Sign-On-Token, mit dem SSO-Token für EPM System verschlüsselt und entschlüsselt werden. Dieser Schlüssel ist in der Oracle Hyperion Shared Services-Registry gespeichert
- Schlüssel für vertrauenswürdige Services, mit dem EPM System-Komponenten die Authentizität des Service prüfen, der ein SSO-Token anfordert
- Verschlüsselungsschlüssel für die Providerkonfiguration, mit dem das Kennwort (Kennwort für Benutzer-DN für LDAP-fähige Benutzerverzeichnisse) verschlüsselt wird, das die EPM System-Sicherheit für das Binding an ein konfiguriertes externes Benutzerverzeichnis verwendet. Dieses Kennwort wird beim Konfigurieren eines externen Benutzerverzeichnisses festgelegt.

Ändern Sie diese Schlüssel periodisch, um die EPM System-Sicherheit zu erhöhen. Oracle Hyperion Shared Services und das Sicherheitssystem von EPM System verwenden die AES-Verschlüsselung mit 128-Bit-Schlüsselstärke.

**▲ Achtung:**

Von Oracle Hyperion Financial Management und Oracle Hyperion Profitability and Cost Management verwendete Taskflows werden ungültig, wenn Sie den Single Sign-On-Verschlüsselungsschlüssel neu generieren. Nach der Neugenerierung des Schlüssels müssen Sie die Taskflows öffnen und speichern, damit sie neu validiert werden.

So generieren Sie Single Sign-On-Verschlüsselungsschlüssel, Schlüssel für die Providerkonfiguration oder Schlüssel für vertrauenswürdige Services neu:

1. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu. Informationen hierzu finden Sie unter [Shared Services Console starten](#).
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie **Verschlüsselungsoptionen** aus.
4. Wählen Sie unter **Verschlüsselungsoptionen** den Schlüssel aus, der neu generiert werden soll.

**Tabelle 4-7 Verschlüsselungsoptionen für EPM System**

| Option               | Beschreibung  |
|----------------------|---|
| Single Sign-On-Token | <p>Wählen Sie diese Option aus, wenn der Verschlüsselungsschlüssel, mit dem SSO-Token für EPM System verschlüsselt und entschlüsselt werden, neu generiert werden soll.</p> <p>Klicken Sie auf eine der folgenden Schaltflächen, wenn unter <b>Sicherheitsoptionen</b> die Option <b>SSO-Kompatibilität aktivieren</b> ausgewählt ist:</p> <ul style="list-style-type: none"> <li>• <b>Neuen Schlüssel erstellen</b>, um einen neuen Verschlüsselungsschlüssel für SSO-Token zu erstellen</li> <li>• <b>Auf Standardwert zurücksetzen</b>, um den Standardverschlüsselungsschlüssel für SSO-Token wiederherzustellen</li> </ul> |
| Trusted Services Key | <p>Wählen Sie diese Option aus, um den Schlüssel für vertrauenswürdige Authentifizierung neu zu generieren, mit dem EPM System-Komponenten die Authentizität des Service prüfen, der ein SSO-Token anfordert.</p>   |

**✎ Hinweis:**

Wenn Sie den Standardverschlüsselungsschlüssel übernehmen, müssen Sie die vorhandene Keystore-Datei (`EPM_ORACLE_HOME/common/CSS/ssHandlerTK`) auf allen EPM System-Hostcomputern löschen.

**Tabelle 4-7 (Fortsetzung) Verschlüsselungsoptionen für EPM System**

| Option                          | Beschreibung   |
|---------------------------------|--|
| Providerkonfigurationsschlüssel | Wählen Sie diese Option aus, um den Schlüssel neu zu generieren, mit dem das Kennwort (Kennwort für Benutzer-DN für LDAP-fähige Benutzerverzeichnisse) verschlüsselt wird, das die EPM System-Sicherheit für das Binding an ein konfiguriertes externes Benutzerverzeichnis verwendet. Dieses Kennwort wird beim Konfigurieren eines externen Benutzerverzeichnisses festgelegt. |

5. Klicken Sie auf **OK**.
6. Haben Sie sich entschieden, einen neuen SSO-Verschlüsselungsschlüssel zu erstellen, dann führen Sie diesen Schritt aus.
  - a. Klicken Sie auf **Herunterladen**.
  - b. Klicken Sie auf **OK**, um `ssHandlerTK` (Keystore-Datei, die den neuen SSO-Verschlüsselungsschlüssel unterstützt) in einem Ordner auf dem Hostserver von Oracle Hyperion Foundation Services zu speichern.
  - c. Kopieren Sie `ssHandlerTK` auf alle EPM System-Hostcomputer in `EPM_ORACLE_HOME/common/CSS`.
7. Starten Sie Foundation Services und andere EPM System-Komponenten erneut.

## Sonderzeichen verwenden

Active Directory und andere LDAP-basierte Benutzerverzeichnisse erlauben Sonderzeichen in Entitys, z.B. in DNs, Benutzernamen, Rollen und Gruppennamen. Damit Oracle Hyperion Shared Services diese Zeichen interpretieren kann, ist ggf. eine spezielle Einstellung erforderlich.

Grundsätzlich müssen Sie Escape-Zeichen verwenden, wenn Sie Sonderzeichen in den Einstellungen von Benutzerverzeichnissen angeben, z.B. im Basis-DN und in Benutzer- und Gruppen-URLs. In der folgenden Tabelle sind die Sonderzeichen aufgelistet, die in Benutzernamen, Gruppennamen, Benutzer-URLs, Gruppen-URLs sowie im OU-Wert des Benutzer-DN verwendet werden können.

**Tabelle 4-8 Unterstützte Sonderzeichen**

| Zeichen | Name oder Bedeutung         | Zeichen | Name oder Bedeutung      |
|---------|-----------------------------|---------|--------------------------|
| (       | Klammer links               | \$      | Dollarzeichen            |
| )       | Klammer rechts              | +       | Pluszeichen              |
| "       | Doppeltes Anführungszeichen | &       | Et-Zeichen               |
| '       | Einfaches Anführungszeichen | \       | Umgekehrter Schrägstrich |
| ,       | Komma                       | ^       | Caret-Zeichen            |
| =       | Gleichheitszeichen          | ;       | Semikolon                |
| <       | Kleiner als-Zeichen         | #       | Nummernzeichen           |
| >       | Größer als-Zeichen          | @       | At-Zeichen               |

 **Hinweis:**

Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten, die im Basis-DN enthalten sind.

- Als Wert des Attributs "Anmeldebenutzer" sind Sonderzeichen nicht zulässig.
- Das Sternchen (\*) wird in Benutzernamen, Gruppennamen, Benutzer- und Gruppen-URLs und im OU-Namen des Benutzer-DN nicht unterstützt.
- Attributwerte, die eine Kombination aus Sonderzeichen enthalten, werden nicht unterstützt.
- Das Et-Zeichen (&) kann ohne Escape-Zeichen verwendet werden. In den Active Directory-Einstellungen muss & als `&amp;` angegeben werden.
- Benutzer- und Gruppennamen können nicht gleichzeitig einen umgekehrten Schrägstrich (\) und einen Schrägstrich (/) enthalten. Namen wie `test/\user` und `new\test/user` werden z.B. nicht unterstützt.

**Tabelle 4-9 Zeichen, die keine Escape-Zeichen erfordern**

| Zeichen | Name oder Bedeutung | Zeichen | Name oder Bedeutung         |
|---------|---------------------|---------|-----------------------------|
| (       | Klammer links       | '       | Einfaches Anführungszeichen |
| )       | Klammer rechts      | ^       | Caret-Zeichen               |
| \$      | Dollarzeichen       | @       | At-Zeichen                  |
| &       | Et-Zeichen          |         |                             |

 **Hinweis:**

& muss als `&amp;` angegeben werden.

Diese Zeichen müssen mit Escape-Zeichen versehen werden, wenn Sie sie in Benutzerverzeichniseinstellungen verwenden (Benutzernamen, Gruppennamen, Benutzer-URLs, Gruppen-URLs und Benutzer-DN).

**Tabelle 4-10 Escape-Zeichen für Sonderzeichen in den Konfigurationseinstellungen von Benutzerverzeichnissen**

| Sonderzeichen          | Escape-Zeichen               | Beispieleinstellung     | Beispiel mit Escape      |
|------------------------|------------------------------|-------------------------|--------------------------|
| Komma (,)              | Umgekehrter Schrägstrich (\) | <code>ou=test,ou</code> | <code>ou=test\,ou</code> |
| Pluszeichen (+)        | Umgekehrter Schrägstrich (\) | <code>ou=test+ou</code> | <code>ou=test\+ou</code> |
| Gleichheitszeichen (=) | Umgekehrter Schrägstrich (\) | <code>ou=test=ou</code> | <code>ou=test\=ou</code> |
| Nummernzeichen (#)     | Umgekehrter Schrägstrich (\) | <code>ou=test#ou</code> | <code>ou=test\#ou</code> |

**Tabelle 4-10 (Fortsetzung) Escape-Zeichen für Sonderzeichen in den Konfigurationseinstellungen von Benutzerverzeichnissen**

| Sonderzeichen                | Escape-Zeichen                      | Beispieleinstellung | Beispiel mit Escape |
|------------------------------|-------------------------------------|---------------------|---------------------|
| Semikolon (;)                | Umgekehrter Schrägstrich (\)        | ou=test;ou          | ou=test\;ou         |
| Kleiner als-Zeichen (<)      | Umgekehrter Schrägstrich (\)        | ou=test<ou          | ou=test\<>ou        |
| Größer als-Zeichen (>)       | Umgekehrter Schrägstrich (\)        | ou=test>ou          | ou=test\>ou         |
| Anführungszeichen (")        | Zwei umgekehrte Schrägstriche (\\)  | ou=test"ou          | ou=test\\"ou        |
| Umgekehrter Schrägstrich (\) | Drei umgekehrte Schrägstriche (\\\) | ou=test\ou          | ou=test\\\ou        |

 **Hinweis:**

- In Benutzer-DNs muss das doppelte Anführungszeichen (") als Escape-Zeichen mit einem umgekehrten Schrägstrich versehen werden. Beispiel: ou=test"ou muss als ou=test\"ou angegeben werden.
- In Benutzer-DNs muss der umgekehrte Schrägstrich (\) als Escape-Zeichen mit einem umgekehrten Schrägstrich versehen werden. Beispiel: ou=test\ou muss als ou=test\\ou angegeben werden.

 **Achtung:**

Wenn keine Benutzer-URL angegeben wurde, dürfen Benutzer, die in der RDN-Root erstellt werden, nicht das Zeichen / (Schrägstrich) oder \ (umgekehrter Schrägstrich) enthalten. Diese Zeichen dürfen auch nicht in den Namen von Gruppen verwendet werden, die in der RDN-Root erstellt werden, falls keine Gruppen-URL angegeben wurde. Beispiel: Gruppennamen wie OU=child\ou, OU=parent/ou oder OU=child/ou, OU=parent\ou werden nicht unterstützt. Dies gilt nicht, wenn Sie in der Konfiguration des Benutzerverzeichnisses als ID Attribute ein eindeutiges Attribut verwenden.

**Sonderzeichen in Native Directory**

In Native Directory werden Sonderzeichen in Benutzer- und Gruppennamen unterstützt.

**Tabelle 4-11 Unterstützte Sonderzeichen: Native Directory**

| Zeichen | Name oder Bedeutung | Zeichen | Name oder Bedeutung |
|---------|---------------------|---------|---------------------|
| @       | At-Zeichen          | ,       | Komma               |



**Tabelle 4-11 (Fortsetzung) Unterstützte Sonderzeichen: Native Directory**

| <b>Zeichen</b> | <b>Name oder Bedeutung</b>     | <b>Zeichen</b> | <b>Name oder Bedeutung</b> |
|----------------|--------------------------------|----------------|----------------------------|
| #              | Nummernzeichen                 | =              | Gleichheitszeichen         |
| \$             | Dollarzeichen                  | +              | Pluszeichen                |
| ^              | Caret-Zeichen                  | ;              | Semikolon                  |
| (              | Klammer links                  | !              | Ausrufezeichen             |
| )              | Klammer rechts                 | %              | Prozentzeichen             |
| '              | Einfaches<br>Anführungszeichen |                |                            |

# 5

## Benutzerdefinierte Authentifizierungsmodule verwenden

### Siehe auch:

- [Übersicht](#)
- [Beispiele für Anwendungsfälle und Einschränkungen](#)
- [Voraussetzungen](#)
- [Überlegungen zu Design und Codierung](#)
- [Benutzerdefinierte Authentifizierungsmodule bereitstellen](#)

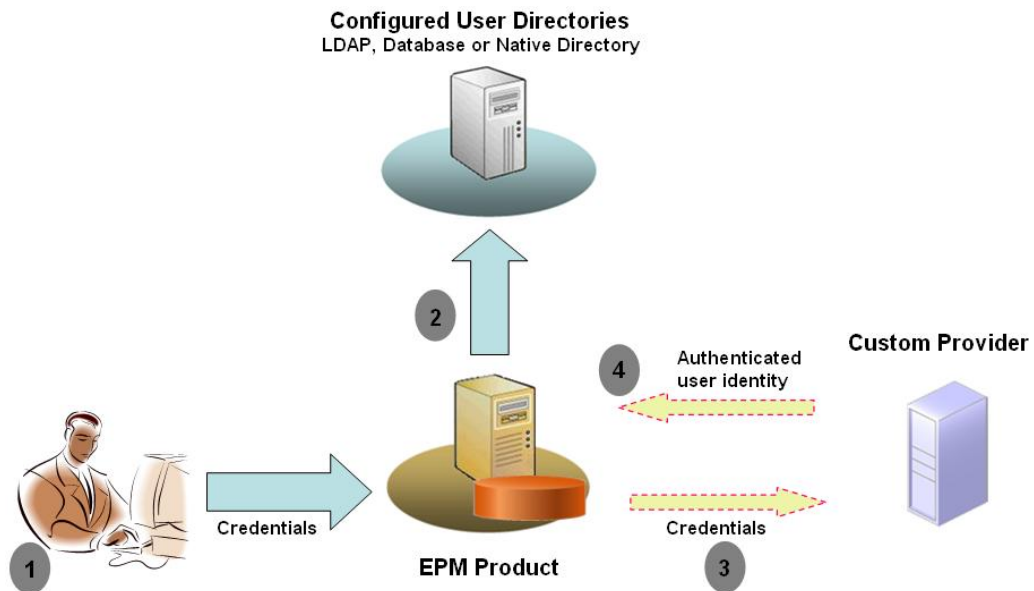
### Übersicht

Ein benutzerdefiniertes Authentifizierungsmodul ist ein Java-Modul, das Kunden entwickeln und implementieren, um Oracle Enterprise Performance Management System-Benutzer zu authentifizieren. EPM System-Produkte verwenden in der Regel ein Anmeldefenster, um den Benutzernamen und das Kennwort für die Benutzerauthentifizierung zu erfassen. Anstelle der EPM System-Authentifizierung können Sie ein benutzerdefiniertes Authentifizierungsmodul verwenden, um Benutzer zu authentifizieren und authentifizierte Benutzerzugangsdaten zur weiteren Verarbeitung an EPM System zu übergeben. Bei der Implementierung eines benutzerdefinierten Authentifizierungsmoduls werden EPM System-Produkte nicht geändert.

Sie können ein benutzerdefiniertes Authentifizierungsmodul sowohl mit Thick Clients (z.B. Oracle Smart View for Office und Oracle Essbase Studio) als auch mit Thin Clients (z.B. Oracle Hyperion Enterprise Performance Management Workspace) verwenden.

Das benutzerdefinierte Authentifizierungsmodul verwendet die Informationen, die ein Benutzer zur Anmeldung bei einem EPM System-Produkt eingibt. Wenn das benutzerdefinierte Authentifizierungsmodul für ein Benutzerverzeichnis aktiviert ist, werden Benutzer über dieses Modul authentifiziert. Bei erfolgreicher Benutzerauthentifizierung gibt das benutzerdefinierte Authentifizierungsmodul den Benutzernamen an EPM System zurück.

Die folgende Abbildung zeigt ein Beispielszenario für die benutzerdefinierte Authentifizierung:



Beispiel: Sie können die RSA SecurID-Infrastruktur als benutzerdefinierten Provider verwenden, um eine transparente, strenge Authentifizierung für EPM System sicherzustellen. Übersicht:

1. Der Benutzer gibt Zugangsdaten (normalerweise Benutzername und Kennwort) ein, um auf ein EPM System-Produkt zuzugreifen. Mit diesen Zugangsdaten muss der Benutzer bei dem vom benutzerdefinierten Authentifizierungsmodul verwendeten Provider eindeutig identifiziert werden. Beispiel: Wenn Sie eine RSA SecurID-Infrastruktur zur Authentifizierung von Benutzern verwenden, gibt der Benutzer eine RSA-Benutzer-ID und -PIN ein (und nicht eine Benutzer-ID und ein Kennwort für EPM System).
2. Anhand der Suchreihenfolge (siehe [Suchreihenfolge](#)) durchläuft EPM System die konfigurierten Benutzerverzeichnisse, um den Benutzer zu suchen.
  - Wenn das aktuelle Benutzerverzeichnis nicht für die benutzerdefinierte Authentifizierung konfiguriert ist, versucht EPM System, den Benutzer über die EPM System-Authentifizierung zu suchen und zu authentifizieren.
  - Wenn das Benutzerverzeichnis für die benutzerdefinierte Authentifizierung konfiguriert ist, delegiert EPM System den Authentifizierungsprozess an das benutzerdefinierte Modul.
3. Wenn EPM System die Authentifizierung an das benutzerdefinierte Modul delegiert, akzeptiert das benutzerdefinierte Authentifizierungsmodul die Zugangsdaten und verwendet eigene Logik, um die Benutzerauthentifizierung anhand eines benutzerdefinierten Providers durchzuführen, z.B. einer RSA SecurID-Infrastruktur.
4. Wenn das benutzerdefinierte Authentifizierungsmodul den Benutzer anhand des zugehörigen Providers authentifiziert, gibt es den Benutzernamen an EPM System oder eine Java-Ausnahme zurück.

Der vom benutzerdefinierten Authentifizierungsmodul zurückgegebene Benutzername muss mit einem Benutzernamen in einem Benutzerverzeichnis identisch sein, das für die benutzerdefinierte Authentifizierung aktiviert ist.

- Wenn das benutzerdefinierte Authentifizierungsmodul einen Benutzernamen zurückgibt, sucht EPM System den Benutzer in einem Benutzerverzeichnis,

das für die benutzerdefinierte Authentifizierung aktiviert ist. In dieser Phase durchsucht EPM System keine Benutzerverzeichnisse, die nicht für die benutzerdefinierte Authentifizierung konfiguriert sind.

- Wenn das benutzerdefinierte Authentifizierungsmodul eine Ausnahme auslöst oder keinen Benutzer zurückgibt, setzt EPM System die Suche nach dem Benutzer in den verbleibenden Benutzerverzeichnissen der Suchreihenfolge fort, die nicht für die benutzerdefinierte Authentifizierung aktiviert sind. Wenn kein Benutzer gefunden wird, der den Zugangsdaten entspricht, zeigt EPM System einen Fehler an.

## Beispiele für Anwendungsfälle und Einschränkungen

Szenarios zur Implementierung der benutzerdefinierten Authentifizierung umfassen Folgendes:

- Unterstützung für Einmalkennwörter hinzufügen
- Authentifizierung anhand von [Resource Access Control Facility \(RACF\)](#) durchführen
- LDAP-fähigen Benutzerverzeichnissen ein SASL-(Simple Authentication and Security Layer-)Binding anstelle von einfachen LDAP-Bindings hinzufügen

Eine Authentifizierung mit einer geheimen Kennwortantwort funktioniert möglicherweise nicht richtig, wenn Sie ein benutzerdefiniertes Authentifizierungsmodul implementieren. Benutzerdefinierte Meldungen, die vom benutzerdefinierten Authentifizierungsmodul ausgegeben werden, werden nicht an die Clients propagiert. Da Clients, wie z.B. Oracle Hyperion Enterprise Performance Management Workspace, die Fehlermeldung überschreiben und eine allgemeine Meldung anzeigen, sind die folgenden Szenarios nicht gültig:

- Zwei aufeinanderfolgende RSA SecurID-PINs
- Kennwortvariante mit geheimen Kennwortfragen, wie z.B. die Eingabe des ersten, letzten und dritten Zeichens des Kennworts

## Voraussetzungen

- Ein vollständig getestetes Java-Archiv namens `CustomAuth.jar`, das Bibliotheken des benutzerdefinierten Authentifizierungsmoduls enthält. `CustomAuth.jar` muss die öffentliche Schnittstelle `CSSCustomAuthenticationIF` implementieren, die im Paket `com.hyperion.css` als Teil der Oracle Hyperion Shared Services-Standard-APIs definiert ist. Informationen hierzu finden Sie unter [http://download.oracle.com/docs/cd/E12825\\_01/epm.111/epm\\_security\\_api\\_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html](http://download.oracle.com/docs/cd/E12825_01/epm.111/epm_security_api_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html).
- Zugriff auf Shared Services als Shared Services-Administrator.

## Überlegungen zu Design und Codierung

### Suchreihenfolge

Zusätzlich zu Native Directory können mehrere Benutzerverzeichnisse in Oracle Hyperion Shared Services konfiguriert werden. Allen konfigurierten Benutzerverzeichnissen wird eine Standardposition in der Suchreihenfolge zugewiesen. Sie können die Suchreihenfolge in Oracle Hyperion Shared Services Console ändern. Mit Ausnahme von Native Directory können Sie konfigurierte Benutzerverzeichnisse aus der Suchreihenfolge entfernen. Oracle

Enterprise Performance Management System verwendet keine Benutzerverzeichnisse, die nicht in der Suchreihenfolge enthalten sind. Informationen hierzu finden Sie in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

Die Suchreihenfolge bestimmt, in welcher Reihenfolge EPM System die Benutzerverzeichnisse durchläuft, um Benutzer zu authentifizieren. Wenn der Benutzer in einem Benutzerverzeichnis authentifiziert ist, stoppt EPM System die Suche und gibt den Benutzer zurück. EPM System verweigert die Authentifizierung und gibt einen Fehler zurück, wenn der Benutzer anhand der Benutzerverzeichnisse in der Suchreihenfolge nicht authentifiziert werden kann.

### Auswirkung von benutzerdefinierter Authentifizierung auf Suchreihenfolge

Die benutzerdefinierte Authentifizierung hat Auswirkungen darauf, wie die EPM System-Sicherheit die Suchreihenfolge interpretiert.

Wenn das benutzerdefinierte Authentifizierungsmodul einen Benutzernamen zurückgibt, sucht EPM System den Benutzer nur in einem Benutzerverzeichnis, das für die benutzerdefinierte Authentifizierung aktiviert ist. In dieser Phase ignoriert EPM System Benutzerverzeichnisse, die nicht für die benutzerdefinierte Authentifizierung konfiguriert sind.

### Erläuterungen zum Ablauf der benutzerdefinierten Authentifizierung

Die folgenden Anwendungsfallszenarios werden verwendet, um den Ablauf der benutzerdefinierten Authentifizierung zu erkunden:

- [Anwendungsfallszenario 1](#)
- [Anwendungsfallszenario 2](#)
- [Anwendungsfallszenario 3](#)

### Anwendungsfallszenario 1

In der folgenden Tabelle werden die EPM System-Benutzerverzeichniskonfiguration und die Suchreihenfolge aus diesem Szenario beschrieben. In diesem Szenario wird angenommen, dass das benutzerdefinierte Authentifizierungsmodul eine RSA-Infrastruktur zur Authentifizierung von Benutzern verwendet.

**Tabelle 5-1 Setup für Szenario 1**

| Typ und Name des Benutzerverzeichnisses | Suchreihenfolge | Benutzerdefinierte Authentifizierung | Beispiele für Benutzernamen                             | Kennwort <sup>1</sup> |
|---|-----------------|--------------------------------------|---|-----------------------|
| Native Directory                        | 1               | Deaktiviert                          | test_user_1<br>test_user_2<br>test_user_3               | password              |
| LDAP-fähig SunONE_West                  | 2               | Deaktiviert                          | test_ldap1<br>test_ldap_2<br>test_user_3<br>test_ldap_4 | ldappassword          |

**Tabelle 5-1 (Fortsetzung) Setup für Szenario 1**

| Typ und Name des Benutzerverzeichnis | Suchreihenfolge | Benutzerdefinierte Authentifizierung | Beispiele für Benutzernamen              | Kennwort <sup>1</sup>   |
|--------------------------------------|-----------------|--------------------------------------|--|---|
| LDAP-fähig<br>SunONE_East            | 3               | Aktiviert                            | test_ldap1<br>test_ldap_2<br>test_user_3 | ldappassword<br>auf SunONE und<br>RSA PIN im<br>benutzerdefinierten Modul |

<sup>1</sup> Der Einfachheit halber wird angenommen, dass alle Benutzer dasselbe Kennwort für das Benutzerverzeichnis verwenden.

Um den Authentifizierungsprozess zu starten, gibt ein Benutzer einen Benutzernamen und ein Kennwort im Anmeldefenster eines EPM System-Produkts ein. In diesem Szenario führt das benutzerdefinierte Authentifizierungsmodul die folgenden Aktionen aus:

- Akzeptiert einen Benutzernamen und eine RSA-PIN als Benutzerzugangsdaten
- Gibt einen Benutzernamen im Format *username@providername*, z.B. *test\_ldap\_2@SunONE\_East*, an die EPM System-Sicherheit zurück

**Tabelle 5-2 Benutzerinteraktion und Ergebnisse**

| Benutzername und Kennwort    | Authentifizierungsergebnis  | Anmeldebenutzerverzeichnis                   |
|------------------------------|---|--|
| test_user_1/password         | Erfolgreich   | Native Directory                             |
| test_user_3/password         | Erfolgreich   | Native Directory                             |
| test_user_3/<br>ldappassword | Erfolgreich   | SunONE_West (Suchreihenfolge 2) <sup>1</sup> |
| test_user_3/RSA PIN          | Erfolgreich   | SunONE_East (Suchreihenfolge 3) <sup>2</sup> |
| test_ldap_2/<br>ldappassword | Erfolgreich   | SunONE_West (Suchreihenfolge 2)              |
| test_ldap_4/RSA PIN          | Fehler<br>EPM System zeigt einen<br>Authentifizierungsfehler an. <sup>3</sup> |  |

<sup>1</sup> Die benutzerdefinierte Authentifizierung kann diesen Benutzer nicht authentifizieren, da der Benutzer EPM System-Zugangsdaten eingegeben hat. EPM System kann diesen Benutzer nur in einem Benutzerverzeichnis identifizieren, das nicht für die benutzerdefinierte Authentifizierung aktiviert ist. Der Benutzer ist nicht in Native Directory (Suchreihenfolgenummer 1) enthalten, wurde jedoch in SunONE West (Suchreihenfolgenummer 2) gefunden.

<sup>2</sup> EPM System kann diesen Benutzer weder in Native Directory (Suchreihenfolgenummer 1) noch in SunONE West (Suchreihenfolgenummer 2) finden. Das benutzerdefinierte Authentifizierungsmodul validiert den Benutzer anhand des RSA-Servers und gibt *test\_user\_3@SunONE\_EAST* an EPM System zurück. EPM System sucht den Benutzer in SunONE East (Suchreihenfolgenummer 3), einem Benutzerverzeichnis, für das die benutzerdefinierte Authentifizierung aktiviert ist.

<sup>3</sup> Oracle empfiehlt, alle Benutzer, die vom benutzerdefinierten Modul authentifiziert wurden, in einem Benutzerverzeichnis zu speichern, für das die benutzerdefinierte Authentifizierung aktiviert ist und das in der Suchreihenfolge vorhanden ist. Die Anmeldung ist nicht erfolgreich, wenn der vom benutzerdefinierten Authentifizierungsmodul zurückgegebene Benutzername nicht in einem Benutzerverzeichnis aus der Suchreihenfolge vorhanden ist, für das die benutzerdefinierte Authentifizierung aktiviert ist.

## Anwendungsfallszenario 2

In der folgenden Tabelle werden die EPM System-Benutzerverzeichnis-Konfiguration und die Suchreihenfolge aus diesem Szenario beschrieben. In diesem Szenario wird angenommen, dass das benutzerdefinierte Authentifizierungsmodul eine RSA-Infrastruktur zur Authentifizierung von Benutzern verwendet.

In diesem Szenario führt das benutzerdefinierte Authentifizierungsmodul die folgenden Aktionen aus:

- Akzeptiert einen Benutzernamen und eine RSA-PIN als Benutzerzugangsdaten
- Gibt einen Benutzernamen, z.B. `test_ldap_2`, an die EPM System-Sicherheit zurück

**Tabelle 5-3 Beispielsuchreihenfolge**

| Benutzerverzeichnis     | Suchreihenfolge | Benutzerdefinierte Authentifizierung | Beispiele für Benutzernamen               | Kennwort <sup>1</sup>  |
|-------------------------|-----------------|--------------------------------------|---|--|
| Native Directory        | 1               | Deaktiviert                          | test_user_1<br>test_user_2<br>test_user_3 | password   |
| LDAP-fähig, z.B. SunONE | 2               | Aktiviert                            | test_ldap1<br>test_ldap2<br>test_user_3   | ldappassword auf SunONE und RSA PIN im benutzerdefinierten Modul |

<sup>1</sup> Der Einfachheit halber wird angenommen, dass alle Benutzer dasselbe Kennwort für das Benutzerverzeichnis verwenden.

Um den Authentifizierungsprozess zu starten, gibt ein Benutzer einen Benutzernamen und ein Kennwort im Anmeldefenster eines EPM System-Produkts ein.

**Tabelle 5-4 Benutzerinteraktion und Ergebnisse**

| Benutzername und Kennwort | Ergebnis der Anmeldung | Anmeldebenutzerverzeichnis |
|---------------------------|------------------------|----------------------------|
| test_user_1/password      | Erfolgreich            | Native Directory           |
| test_user_3/password      | Erfolgreich            | Native Directory           |
| test_user_3/ldappassword  | Fehler                 | SunONE <sup>1</sup>        |
| test_user_3/RSA PIN       | Erfolgreich            | SunONE <sup>2</sup>        |

<sup>1</sup> Benutzerauthentifizierung anhand von Native Directory ist nicht erfolgreich, da das Kennwort nicht übereinstimmt. Die Benutzerauthentifizierung mit dem benutzerdefinierten Authentifizierungsmodul ist nicht erfolgreich, da das verwendete Kennwort keine gültige RSA-PIN ist. EPM System versucht nicht, diesen Benutzer in SunONE (Suchreihenfolge 2) zu authentifizieren, da die benutzerdefinierten Authentifizierungseinstellungen die EPM System-Authentifizierung in diesem Verzeichnis überschreiben.

<sup>2</sup> Benutzerauthentifizierung anhand von Native Directory ist nicht erfolgreich, da das Kennwort nicht übereinstimmt. Das benutzerdefinierte Authentifizierungsmodul authentifiziert den Benutzer und gibt den Benutzernamen `test_user_3` an EPM System zurück.

### Anwendungsfallszenario 3

In der folgenden Tabelle werden die EPM System-Benutzerverzeichnis-Konfiguration und die Suchreihenfolge aus diesem Szenario beschrieben. In diesem Szenario wird angenommen, dass das benutzerdefinierte Authentifizierungsmodul eine RSA-Infrastruktur zur Authentifizierung von Benutzern verwendet.

Aus Gründen der Klarheit in solchen Szenarios empfiehlt Oracle, dass Ihr benutzerdefiniertes Authentifizierungsmodul den Benutzernamen im Format `username@providername` zurückgibt, z.B. `test_ldap_4@SunONE`.

**Tabelle 5-5 Beispielsuchreihenfolge**

| Benutzerverzeichnis     | Suchreihenfolge | Benutzerdefinierte Authentifizierung | Beispiele für Benutzernamen               | Kennwort <sup>1</sup>  |
|-------------------------|-----------------|--------------------------------------|---|--|
| Native Directory        | 1               | Aktiviert                            | test_user_1<br>test_user_2<br>test_user_3 | RSA_PIN  |
| LDAP-fähig, z.B. MSAD   | 2               | Deaktiviert                          | test_ldap1<br>test_ldap4<br>test_user_3   | ldappassword   |
| LDAP-fähig, z.B. SunONE | 3               | Aktiviert                            | test_ldap1<br>test_ldap4<br>test_user_3   | ldappassword auf SunONE und RSA PIN im benutzerdefinierten Modul |

<sup>1</sup> Der Einfachheit halber wird angenommen, dass alle Benutzer dasselbe Kennwort für das Benutzerverzeichnis verwenden.

Um den Authentifizierungsprozess zu starten, gibt ein Benutzer einen Benutzernamen und ein Kennwort im Anmeldefenster eines EPM System-Produkts ein.

**Tabelle 5-6 Benutzerinteraktion und Ergebnisse**

| Benutzername und Kennwort | Authentifizierungsergebnis | Anmeldebenutzerverzeichnis |
|---------------------------|----------------------------|----------------------------|
| test_user_1/password      | Erfolgreich                | Native Directory           |
| test_user_3/RSA_PIN       | Erfolgreich                | Native Directory           |
| test_user_3/ldappassword  | Erfolgreich                | MSAD (Suchreihenfolge 2)   |
| test_ldap_4/ldappassword  | Erfolgreich                | MSAD (Suchreihenfolge 2)   |
| test_ldap_4/RSA PIN       | Erfolgreich                | SunONE (Suchreihenfolge 3) |

### Benutzerverzeichnisse und benutzerdefiniertes Authentifizierungsmodul

Um das benutzerdefinierte Authentifizierungsmodul zu verwenden, können einzelne Benutzerverzeichnisse mit Informationen zu EPM System-Benutzern und -Gruppen so



konfiguriert werden, dass die Authentifizierung an das benutzerdefinierte Modul delegiert wird.

EPM System-Benutzer, die mit einem benutzerdefinierten Modul authentifiziert werden, müssen in einem der Benutzerverzeichnisse aus der Suchreihenfolge vorhanden sein (siehe [Suchreihenfolge](#)). Das Benutzerverzeichnis muss außerdem so konfiguriert sein, dass die Authentifizierung an das benutzerdefinierte Modul delegiert wird.

Die Identität des Benutzers im benutzerdefinierten Provider (z.B. 1357642 in der RSA SecurID-Infrastruktur) unterscheidet sich möglicherweise vom Benutzernamen in dem Benutzerverzeichnis (z.B. jDoe in Oracle Internet Directory), das in Shared Services konfiguriert wurde. Nach der Benutzerauthentifizierung muss das benutzerdefinierte Authentifizierungsmodul den Benutzernamen jDoe an EPM System zurückgeben.

 **Hinweis:**

Als Best Practice empfiehlt Oracle, für die in EPM System konfigurierten Benutzerverzeichnisse denselben Benutzernamen zu verwenden wie im Benutzerverzeichnis, das vom benutzerdefinierten Authentifizierungsmodul verwendet wird.

#### Java-Schnittstelle `CSSCustomAuthenticationIF`

Das benutzerdefinierte Authentifizierungsmodul muss die Java-Schnittstelle `CSSCustomAuthenticationIF` verwenden, damit es in das EPM System-Sicherheits-Framework integriert werden kann. Bei erfolgreicher benutzerdefinierter Authentifizierung muss es eine Zeichenfolge mit einem Benutzernamen und bei nicht erfolgreicher Authentifizierung eine Fehlermeldung zurückgeben. Damit der Authentifizierungsprozess abgeschlossen werden kann, muss der vom benutzerdefinierten Authentifizierungsmodul zurückgegebene Benutzername in einem der Benutzerverzeichnisse aus der Shared Services-Suchreihenfolge vorhanden sein. Das EPM System-Sicherheits-Framework unterstützt das Format `username@providerName`.

 **Hinweis:**

Stellen Sie sicher, dass der vom benutzerdefinierten Authentifizierungsmodul zurückgegebene Benutzername kein \* (Sternchen) enthält, da das EPM System-Sicherheits-Framework bei der Suche nach Benutzern das Sternchen als Platzhalterzeichen interpretiert.

Informationen zur Signatur der Schnittstelle `CSSCustomAuthenticationIF` finden Sie unter [Beispielcode 1](#).

Ihr benutzerdefiniertes Authentifizierungsmodul (kann eine Klassendatei sein) muss in der Datei `CustomAuth.jar` enthalten sein. Die Paketstruktur ist unwichtig.

Ausführliche Informationen zur Schnittstelle `CSSCustomAuthenticationIF` finden Sie in der [Sicherheits-API-Dokumentation](#).

Die Methode `authenticate` von `CSSCustomAuthenticationIF` unterstützt die benutzerdefinierte Authentifizierung. Als Eingabeparameter akzeptiert die Methode `authenticate` Zugangsdaten (Benutzername und Kennwort), die der Benutzer für den Zugriff auf EPM System eingegeben hat. Diese Methode gibt eine Zeichenfolge (Benutzername) zurück, wenn die benutzerdefinierte Authentifizierung erfolgreich ist. Bei nicht erfolgreicher Authentifizierung gibt sie `java.lang.Exception` aus. Der von der Methode zurückgegebene Benutzername muss einen Benutzer in einem der Benutzerverzeichnisse aus der Shared Services-Suchreihenfolge eindeutig identifizieren. Das EPM System-Sicherheits-Framework unterstützt das Format `username@providerName`.

#### Hinweis:

Verwenden Sie den Klassenkonstruktor, um Ressourcen zu initialisieren, wie z.B. einen JDBC-Verbindungspool. Dadurch wird die Performance verbessert, da Ressourcen nicht für jede Authentifizierung geladen werden.

## Benutzerdefinierte Authentifizierungsmodule bereitstellen

Für ein Oracle Enterprise Performance Management System-Deployment wird nur ein benutzerdefiniertes Modul unterstützt. Sie können die benutzerdefinierte Authentifizierung für ein oder mehrere Benutzerverzeichnisse in der Suchreihenfolge aktivieren.

Das benutzerdefinierte Authentifizierungsmodul muss die öffentliche Schnittstelle `CSSCustomAuthenticationIF` implementieren, die im Paket `com.hyperion.css` definiert ist. In diesem Dokument wird angenommen, dass Sie über ein benutzerdefiniertes Modul mit vollständiger Funktionalität verfügen und dass das Modul die Logik zum Authentifizieren von Benutzern anhand eines Benutzerproviders Ihrer Wahl definiert. Nachdem Sie ein benutzerdefiniertes Authentifizierungsmodul entwickelt und getestet haben, müssen Sie es in der EPM System-Umgebung implementieren.

### Übersicht über die Schritte

Ihr benutzerdefinierter Authentifizierungscode darf nicht `log4j` für das Fehlerlogging verwenden. Wenn der Code aus einem früheren Release `log4j` verwendet, müssen Sie es aus dem Code entfernen, bevor Sie den Code für dieses Release verwenden.

Führen Sie die folgenden Schritte aus, um das benutzerdefinierte Authentifizierungsmodul zu implementieren:

- Stoppen Sie EPM System-Produkte, einschließlich Oracle Hyperion Shared Services, sowie alle Systeme, die Shared Services-APIs verwenden.
- Kopieren Sie das Java-Archiv `CustomAuth.jar` des benutzerdefinierten Authentifizierungsmoduls in das Deployment:
  - **WebLogic:** Kopieren Sie `CustomAuth.jar` in das Verzeichnis `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`. Dieses lautet in der Regel `C:/Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

Bei einem Upgrade von Release 11.1.2.0 oder 11.1.2.1, das eine Implementierung des benutzerdefinierten Authentifizierungsmoduls enthielt, verschieben Sie `CustomAuth.jar` von `EPM_ORACLE_HOME/common/jlib/11.1.2.0` in `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Alle Client-Deployments:** Kopieren Sie `CustomAuth.jar` in alle EPM System-Client-Deployments am folgenden Speicherort:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, in der Regel `Oracle/Middleware/common/jlib/11.1.2.0`. Stellen Sie sicher, dass die Datei `CustomAuth.jar` immer im Verzeichnis `EPM_ORACLE_HOME/common/jlib/11.1.2.0` gespeichert wird.

Damit alle Server und Clients die benutzerdefinierte Authentifizierung verwenden können, muss die Datei `CustomAuth.jar` an den folgenden beiden Speicherorten vorhanden sein:

- \* `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`
- \* `EPM_ORACLE_HOME/common/jlib/11.1.2.0`

- Aktualisieren Sie Einstellungen für das Benutzerverzeichnis in Shared Services. Informationen hierzu finden Sie unter [Einstellungen in Shared Services aktualisieren](#).
- Starten Sie Shared Services, und dann sonstige EPM System-Produkte.
- Testen Sie Ihre Implementierung. Informationen hierzu finden Sie unter [Deployments testen](#).

### Einstellungen in Shared Services aktualisieren

Standardmäßig ist die benutzerdefinierte Authentifizierung für alle Benutzerverzeichnisse deaktiviert. Sie können das Standardverhalten überschreiben, um die benutzerdefinierte Authentifizierung für bestimmte externe Benutzerverzeichnisse oder für Native Directory zu aktivieren.

### Benutzerverzeichniskonfigurationen aktualisieren

Sie müssen die Konfiguration des Benutzerverzeichnisses aktualisieren, für das die benutzerdefinierte Authentifizierung aktiviert werden muss.

So aktualisieren Sie die Benutzerverzeichniskonfiguration:

1. Starten Sie Oracle Hyperion Foundation Services.
2. Greifen Sie als Systemadministrator auf Oracle Hyperion Shared Services Console zu.
3. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
4. Wählen Sie im Fenster "Definierte Benutzerverzeichnisse" das Benutzerverzeichnis aus, für das Sie die Einstellung für die benutzerdefinierte Authentifizierung ändern möchten.

#### Hinweis:

In EPM System werden nur die in der Suchreihenfolge enthaltenen Benutzerverzeichnisse verwendet.

5. Klicken Sie auf **Bearbeiten**.
6. Wählen Sie **Erweiterte Optionen anzeigen** aus.

7. Wählen Sie unter **Benutzerdefiniertes Modul** die Option **Authentifizierungsmodul** aus, um das benutzerdefinierte Modul für das aktuelle Benutzerverzeichnis zu aktivieren.
8. Klicken Sie auf **Fertig stellen**.
9. Wiederholen Sie diese Prozedur, um die Konfiguration sonstiger Benutzerverzeichnisse in der Suchreihenfolge zu aktualisieren.

### Sicherheitsoptionen aktualisieren

Stellen Sie sicher, dass `CustomAuth.jar` unter `EPM_ORACLE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib` verfügbar ist, bevor Sie mit dem folgenden Verfahren beginnen.

So aktualisieren Sie Sicherheitsoptionen:

1. Greifen Sie als Systemadministrator auf Shared Services Console zu.
2. Wählen Sie **Administration, Benutzerverzeichnisse konfigurieren** aus.
3. Wählen Sie **Sicherheitsoptionen** aus.
4. Wählen Sie **Erweiterte Optionen anzeigen** aus.
5. Geben Sie unter **Authentifizierungsmodul** den vollqualifizierten Klassennamen des benutzerdefinierten Authentifizierungsmoduls ein, das zum Authentifizieren von Benutzern in allen Benutzerverzeichnissen verwendet werden soll, für die das benutzerdefinierte Authentifizierungsmodul ausgewählt wurde. Beispiel:  
`com.mycompany.epm.CustomAuthenticationImpl`.
6. Klicken Sie auf **OK**.

### Deployments testen

Wenn Native Directory nicht für die benutzerdefinierte Authentifizierung konfiguriert ist, verwenden Sie keine Native Directory-Benutzer zum Testen der benutzerdefinierten Authentifizierung.

#### Hinweis:

Sie sind dafür zuständig, Probleme beim benutzerdefinierten Authentifizierungsmodul zu identifizieren und zu beheben. Oracle geht davon aus, dass Ihr benutzerdefiniertes Modul fehlerfrei funktioniert, um einen Benutzer aus dem vom benutzerdefinierten Modul verwendeten Benutzerverzeichnis einem Benutzer in einem benutzerdefinierten Benutzerverzeichnis zuzuordnen, für das die benutzerdefinierte Authentifizierung aktiviert ist und das in der EPM System-Suchreihenfolge verfügbar ist.

Um Ihr Deployment zu testen, melden Sie sich bei EPM System an. Verwenden Sie hierzu Ihre Benutzerzugangsdaten aus dem Benutzerverzeichnis, wie z.B. einer RSA SecurID-Infrastruktur, die vom benutzerdefinierten Modul verwendet wird. Diese Zugangsdaten können sich von den Zugangsdaten für EPM System unterscheiden.

Ihre Implementierung gilt als erfolgreich, wenn Sie auf die Ressourcen der EPM System-Produkte zugreifen können. Ein Fehler, der angibt, dass der Benutzer nicht gefunden wurde, ist nicht immer ein Indikator dafür, dass eine Implementierung nicht erfolgreich war. Prüfen Sie in solchen Fällen, ob die eingegebenen Zugangsdaten im benutzerdefinierten

Benutzerspeicher vorhanden sind und ob ein übereinstimmender Benutzer in einem der Benutzerverzeichnisse aus der EPM System-Suchreihenfolge vorhanden ist, für das die benutzerdefinierte Authentifizierung aktiviert ist.

So testen Sie die benutzerdefinierte Authentifizierung:

1. Stellen Sie sicher, dass EPM System-Produkte ausgeführt werden.
2. Greifen Sie auf eine EPM System-Komponente zu, wie z.B. Oracle Hyperion Enterprise Performance Management Workspace.
3. Melden Sie sich als ein Benutzer an, der in einem Benutzerverzeichnis mit aktivierter benutzerdefinierter Authentifizierung definiert ist.
  - a. Geben Sie unter **Benutzername** Ihre Benutzer-ID ein, wie z.B. eine RSA-Benutzer-ID.
  - b. Geben Sie unter **Kennwort** ein Kennwort ein, wie z.B. eine RSA-PIN.
  - c. Klicken Sie auf **Anmelden**.
4. Prüfen Sie, ob Sie auf die EPM System-Produktressourcen zugreifen können.

# 6

## Richtlinien zum Sichern von EPM System

### Siehe auch:

- [SSL implementieren](#)
- [Administrator Kennwort ändern](#)
- [Verschlüsselungsschlüssel erneut generieren](#)
- [Datenbankkennwörter ändern](#)
- [Cookies schützen](#)
- [SSO-Tokentimeout reduzieren](#)
- [Sicherheitsberichte prüfen](#)
- [Authentifizierungssystem für starke Authentifizierung anpassen](#)
- [Debugging-Utilities für EPM Workspace deaktivieren](#)
- [Standardfehlerseiten des Webservers ändern](#)
- [Unterstützung für Software von Drittanbietern](#)

### SSL implementieren

SSL nutzt ein kryptographisches System zur Verschlüsselung von Daten. SSL erstellt eine geschützte Verbindung zwischen einem Client und einem Server, mit der Daten sicher übertragen werden.

Um Ihre Oracle Enterprise Performance Management System-Umgebung zu sichern, müssen Sie alle Kommunikationskanäle Ihrer Webanwendungen und Benutzerverzeichnisverbindungen mit SSL sichern. Informationen hierzu finden Sie unter [SSL-Aktivierung für EPM System-Komponenten](#).

Schützen Sie außerdem alle Agent-Ports mit einer Firewall, wie z.B. den Port 6861, bei dem es sich um den Oracle Hyperion Reporting and Analysis-Agent-Port handelt. Endbenutzer benötigen keinen Zugriff auf EPM System-Agent-Ports.

### Administrator Kennwort ändern

Der Standardaccount des Native Directory-Administrators gewährt Zugriff auf alle Oracle Hyperion Shared Services-Funktionen. Dieses Kennwort wird festgelegt, wenn Sie Oracle Hyperion Foundation Services bereitstellen. Sie müssen das Kennwort dieses Accounts regelmäßig ändern.

Bearbeiten Sie das *Admin*-Benutzer-Account, um das Kennwort zu ändern. Informationen hierzu finden Sie unter "Benutzeraccounts ändern" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

## Verschlüsselungsschlüssel erneut generieren

Verwenden Sie Oracle Hyperion Shared Services Console, um folgende Elemente in regelmäßigen Abständen neu zu generieren:

- Single Sign-On-Token

### **Achtung:**

Von Oracle Hyperion Financial Management und Oracle Hyperion Profitability and Cost Management verwendete Taskflows werden ungültig, wenn Sie einen neuen Keystore generieren. Nach der Neugenerierung des Schlüsselspeichers öffnen und speichern Sie die Taskflows, damit diese wieder Gültigkeit haben.

- Schlüssel für vertrauenswürdige Services
- Schlüssel für Providerkonfiguration

Informationen hierzu finden Sie unter [Verschlüsselungsschlüssel erneut generieren](#).

### **Hinweis:**

Oracle Hyperion Shared Services und das Sicherheitssystem von Oracle Enterprise Performance Management System verwenden die AES-Verschlüsselung mit 128-Bit-Schlüsselstärke.

## Datenbankkennwörter ändern

Ändern Sie in regelmäßigen Abständen das Kennwort für alle Oracle Enterprise Performance Management System-Produktdatenbanken. Das Verfahren zum Ändern des Datenbankkennworts in der Oracle Hyperion Shared Services-Registry wird in diesem Abschnitt beschrieben.

Eine ausführliche Beschreibung der Schritte zum Ändern des Kennworts einer EPM System-Produktdatenbank finden Sie in der *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*.

So ändern Sie Datenbankkennwörter von EPM System-Produkten im Shared Services-Registry:

1. Ändern Sie über die Datenbank-Administrationskonsole das Kennwort des Benutzers, dessen Account zum Konfigurieren der EPM System-Datenbank verwendet wurde.
2. Stoppen Sie die EPM System-Produkte (Webanwendungen, Services und Prozesse).
3. Konfigurieren Sie mit Hilfe von EPM System Configurator die Datenbank neu, und verwenden Sie hierzu eines der folgenden Verfahren.

**Nur Oracle Hyperion Shared Services:**

 **Hinweis:**

In verteilten Umgebungen, in denen sich EPM System-Produkte auf anderen Computern befinden als Shared Services, müssen Sie dieses Verfahren auf allen Servern durchführen.

- a. Wählen Sie aus den Aufgaben "Foundation" in EPM System Configurator die Option **Datenbank konfigurieren** aus.
- b. Wählen Sie auf der Seite "Konfiguration von Shared Services und Registry-Datenbank" die Option **Verbindung zu einer zuvor konfigurierten Shared Services-Datenbank herstellen**.
- c. Geben Sie das neue Kennwort des Benutzers an, dessen Account zum Konfigurieren der Shared Services-Datenbank verwendet wurde. Lassen Sie alle anderen Einstellungen unverändert.
- d. Fahren Sie mit der Konfiguration fort, und klicken Sie auf **Fertig stellen**, wenn Sie fertig sind.

**EPM System-Produkte, die sich von Shared Services unterscheiden:** **Hinweis:**

Führen Sie diese Schritte für die EPM System-Produkte aus, die ausschließlich auf dem aktuellen Server bereitgestellt sind.

Ausführliche Anweisungen hierzu finden Sie in der *Oracle Enterprise Performance Management System - Installations- und Konfigurationsdokumentation*.

4. Starten Sie EPM System-Produkte und -Services.

## Cookies schützen

Die Oracle Enterprise Performance Management System-Webanwendung hat ein Cookie festgelegt, um die Session zu verfolgen. Beim Festlegen des Cookies, besonders bei einem Session-Cookie, kann der Server ein Sicherheits-Flag setzen. Dadurch wird der Browser gezwungen, den Cookie über einen sicheren Kanal zu senden. So wird das Risiko eines Session-Hijackings reduziert.

 **Hinweis:**

Sichern Sie Cookies nur, wenn EPM System-Produkte in einer Umgebung bereitgestellt werden, für die SSL aktiviert ist.

Ändern Sie den Sessiondeskriptor für Oracle WebLogic Server, um WebLogic Server-Cookies zu sichern. Legen Sie den Wert des `cookieSecure`-Attributs im `session-param`-Element auf `true` fest. Informationen hierzu finden Sie im Abschnitt zum Sichern von



Webanwendungen in der Dokumentation [Oracle Fusion Middleware Programming Security for Oracle WebLogic Server 11g](#).

## SSO-Tokentimeout reduzieren

Der Standardtimeout für das SSO-Token ist 480 Minuten. Reduzieren Sie den SSO-Tokentimeout beispielsweise auf 60 Minuten, um die Wiederverwendung des Tokens nach der Bereitstellung zu verringern. Informationen hierzu finden Sie im Abschnitt zum Festlegen von Sicherheitsoptionen in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

## Sicherheitsberichte prüfen

Der Sicherheitsbericht enthält Audit-Informationen, die sich auf Sicherheitsaufgaben beziehen, für die Auditing konfiguriert wurde. Erstellen und prüfen Sie diesen Bericht regelmäßig über Oracle Hyperion Shared Services Console, vor allem um nicht erfolgreiche Anmeldeversuche in Oracle Enterprise Performance Management System-Produkten und Provisioning-Änderungen zu identifizieren. Wählen Sie **Detaillierte Ansicht** als Berichterstellungsoption aus, um die Berichtsdaten basierend auf geänderten Attributen und den neuen Attributen zu gruppieren. Informationen hierzu finden Sie unter "Berichte generieren" in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

## Authentifizierungssystem für starke Authentifizierung anpassen

Mit einem benutzerdefinierten Authentifizierungsmodul können Sie EPM System eine starke Authentifizierung hinzufügen. Beispiel: Sie können die RSA SecurID-Zwei-Faktor-Authentifizierung im Modus für nicht geheime Kennwortantworten verwenden. Das benutzerdefinierte Authentifizierungsmodul ist für Thin Clients und Thick Clients transparent und erfordert keine clientseitigen Deployment-Änderungen. Informationen hierzu finden Sie unter [Benutzerdefinierte Authentifizierungsmodule verwenden](#).

## EPM Workspace-Debugging-Utilitys deaktivieren

- Zu Fehlerbehebungszwecken wird Oracle Hyperion Enterprise Performance Management Workspace mit JavaScript-Dateien ausgeliefert, die nicht mit einem JavaScript-Cruncher bearbeitet wurden. Aus Sicherheitsgründen müssen Sie diese JavaScript-Dateien aus der Produktionsumgebung entfernen:
  - Erstellen Sie eine Backupkopie des Verzeichnisses `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.
  - Löschen Sie die `.js`-Dateien aus den einzelnen Unterverzeichnissen von `EPM_ORACLE_HOME/common/epmstatic/wspace/js`, mit Ausnahme der Datei `DIRECTORY_NAME.js`.

Jedes Unterverzeichnis enthält eine `.js`-Datei, die den Namen des Verzeichnisses beinhaltet. Beispiel: `EPM_ORACLE_HOME/common/epmstatic/wspace/js/com/hyperion/bpm/web/common` enthält `Common.js`. Entfernen Sie alle `.js`-Dateien mit Ausnahme derjenigen, die den Namen des Verzeichnisses enthält, in diesem Fall die Datei `Common.js`.

- EPM Workspace bietet einige Debugging-Utilities und Testanwendungen, die verfügbar sind, wenn EPM Workspace im Debugging-Modus bereitgestellt wird. Aus Sicherheitsgründen müssen Administratoren das clientseitige Debugging in EPM Workspace deaktivieren.

So deaktivieren Sie den Debugging-Modus:

1. Melden Sie sich bei EPM Workspace als Administrator an.
2. Wählen Sie **Navigieren, Verwalten, Workspace-Servereinstellungen** aus.
3. Wählen Sie in den Workspace-Servereinstellungen unter **ClientDebugEnabled** die Option **Nein** aus.
4. Klicken Sie auf **OK**.

## Standardfehlerseiten des Webservers ändern

Wenn Anwendungsserver für die Annahme von Anforderungen nicht zur Verfügung stehen, gibt das Webserver-Plug-in für den Backend-Anwendungsserver (z.B. Oracle HTTP Server-Plug-in für Oracle WebLogic Server) eine Standardfehlerseite mit Informationen zum Plug-in-Build zurück. Webserver zeigen ihre Standardfehlerseite auch bei anderen Gelegenheiten an. Angreifer können diese Informationen verwenden, um bekannte Schwachstellen öffentlicher Websites zu auszunutzen.

Passen Sie die Fehlerseiten (des Webanwendungsserver-Plug-ins und des Webservers) so an, dass sie keine Informationen zu Produktionssystemkomponenten enthalten, z.B. Serverversion, Servertyp, Build-Datum des Plug-ins und Plug-in-Typ. Weitere Informationen finden Sie in der Herstellerdokumentation zum Anwendungsserver und zum Webserver.

## Unterstützung für Software von Drittanbietern

Oracle bestätigt und unterstützt die Zusicherung der Rückwärtskompatibilität von Drittanbietern. Demzufolge können bei zugesicherter Rückwärtskompatibilität des Anbieters auch nachfolgende Wartungsreleases und Service Packs verwendet werden. Im Falle einer auftretenden Inkompatibilität wird Oracle eine Patch-Version spezifizieren, mit der das Produkt bereitgestellt werden kann (und die inkompatible Version aus der unterstützten Matrix entfernen), oder eine Wartungsversion bzw. Servicekorrektur für das Oracle-Produkt bereitstellen.

**Serverseitige Aktualisierungen:** Unterstützung für Upgrades auf serverseitige Komponenten von Drittanbietern wird über die "Subsequent Maintenance Release Policy" gesteuert. In der Regel unterstützt Oracle Upgrades von serverseitigen Drittanbieterkomponenten auf das nächste Wartungsrelease für das Service Pack des aktuell unterstützten Release. Upgrades für das nächste Major Release werden nicht unterstützt.

**Clientseitige Updates:** Oracle unterstützt automatische Updates für Clientkomponenten, einschließlich Updates auf das nächste Major Release von Drittanbieter-Clientkomponenten. Beispiel: Sie können für die JRE-Version des Browsers ein Update auf die aktuell unterstützte JRE-Version durchführen.

# A

## Beispielcodes für benutzerdefinierte Authentifizierung

### Beispielcode 1

#### Hinweis:

Ihr benutzerdefinierter Authentifizierungscode darf nicht log4j für das Fehlerlogging verwenden. Wenn der Code für die benutzerdefinierte Authentifizierung aus einem früheren Release log4j verwendet hat, müssen Sie log4j aus dem Code entfernen, bevor Sie es für dieses Release verwenden.

Das folgende Code-Snippet ist eine leere Implementierung des benutzerdefinierten Moduls:

```
package com.hyperion.css.custom;

import java.util.Map;
import com.hyperion.css.CSSCustomAuthenticationIF;

public class CustomAuthenticationImpl implements CSSCustomAuthenticationIF {
    public String authenticate(Map context,String userName,
        String password) throws Exception{
        try{
            //Custom code to find and authenticate the user goes here.
            //The code should do the following:
            //if authentication succeeds:
                //set authenticationSuccessFlag = true
                //return authenticatedUserName
            // if authentication fails:
                //log an authentication failure
                //throw authentication exception
        }
        catch (Exception e){
            //Custom code to handle authentication exception goes here
            //Create a new exception, set the root cause
            //Set any custom error message
            //Return the exception to the caller
        }
        return authenticatedUserName;
    }
}
```

Eingabeparameter:

- **Kontext:** Eine Zuordnung, die ein Schlüssel/Wert-Paar der Gebietsschemainformationen enthält.
- **Benutzername:** Ein Bezeichner zur eindeutigen Identifizierung des Benutzers in dem Benutzerverzeichnis, in dem das benutzerdefinierte Modul den Benutzer authentifiziert. Der Benutzer gibt den Wert dieses Parameters ein, wenn er sich bei einer Oracle Enterprise Performance Management System-Komponente anmeldet.
- **Kennwort:** Das Kennwort für den Benutzer in dem Benutzerverzeichnis, in dem das benutzerdefinierte Modul den Benutzer authentifiziert. Der Benutzer gibt den Wert dieses Parameters ein, wenn er sich bei einer EPM System-Komponente anmeldet.

## Beispielcode 2

Der folgende Beispielcode zeigt die benutzerdefinierte Authentifizierung von Benutzern mit einem Benutzernamen und einem Kennwort aus einer Flat File. Sie müssen Benutzer- und Kennwortlisten im Klassenkonstruktor initialisieren, damit die benutzerdefinierte Authentifizierung funktioniert.

```
package com.hyperion.css.security;

import java.util.Map;
import java.util.HashMap;
import com.hyperion.css.CSSCustomAuthenticationIF;
import java.io.*;

public class CSSCustomAuthenticationImpl implements
CSSCustomAuthenticationIF{
    static final String DATA_FILE = "datafile.txt";

    /**
     * authenticate method includes the core implementation of the
     * Custom Authentication Mechanism. If custom authentication is
     * enabled for the provider, authentication operations
     * are delegated to this method. Upon successful authentication,
     * this method returns a valid user name, using which EPM System
     * retrieves the user from a custom authentication enabled provider.
     * User name can be returned in the format username@providerName,
     * where providerName indicates the name of the underlying provider
     * where the user is available. authenticate method can use other
     * private methods to access various core components of the
     * custom authentication module.

     * @param context
     * @param userName
     * @param password
     * @return
     * @throws Exception
     */
    Map users = null;
```

```
public CSSCustomAuthenticationImpl(){
    users = new HashMap();
    InputStream is = null;
    BufferedReader br = null;
    String line;
    String[] userDetails = null;
    String userKey = null;
    try{
        is = CSSCustomAuthenticationImpl.class.getResourceAsStream(DATA_FILE);
        br = new BufferedReader(new InputStreamReader(is));
        while(null != (line = br.readLine())){
            userDetails = line.split(":");
            if(userDetails != null && userDetails.length==3){
                userKey = userDetails[0]+ ":" + userDetails[1];
                users.put(userKey, userDetails[2]);
            }
        }
    }
    catch(Exception e){
        // log a message
    }
    finally{
        try{
            if(br != null) br.close();
            if(is != null) is.close();
        }
        catch(IOException ioe){
            ioe.printStackTrace();
        }
    }
}

/* Use this authenticate method snippet to return username from a flat file
*/

public String authenticate(Map context, String userName, String password)
throws Exception{
    //userName : user input for the userName
    //password : user input for password
    //context : Map, can be used to additional information required by
    //          the custom authentication module.

    String authenticatedUserKey = userName + ":" + password;

    if(users.get(authenticatedUserKey)!=null)
        return (String)users.get(authenticatedUserKey);
    else throw new Exception("Invalid User Credentials");
}

/* Refer to this authenticate method snippet to return username in
   username@providername format */

public String authenticate(Map context, String userName, String password)
throws Exception{
```

```
//userName : user input for userName
//password : user input for password
//context : Map can be used to additional information required by
//          the custom authentication module.

//Your code should uniquely identify the user in a custom provider
and in a configured
//user directory in Shared Services. EPM Security expects you to
append the provider
//name to the user name. Provider name must be identical to the name
of a custom
//authentication-enabled user directory specified in Shared Services.

//If invalid arguments, return null or throw exception with
appropriate message
//set authenticationSuccessFlag = false

String authenticatedUserKey = userName + ":" + password;
if(users.get(authenticatedUserKey)!=null)
    String userNameStr = (new StringBuffer())
        .append((String)users.get(authenticatedUserKey))
        .append("@").append(PROVIDER_NAME).toString();
    return userNameStr;
else throw new Exception("Invalid User Credentials");
}
```

## Datendatei für Beispielcode 2

Stellen Sie sicher, dass die Datendatei den Namen `datafile.txt` aufweist (dies ist der im Beispielcode verwendete Name) und dass sie in dem von Ihnen erstellten Java-Archiv enthalten ist.

Fügen Sie der Flat File, die als benutzerdefiniertes Benutzerverzeichnis verwendet wird, den folgenden Inhalt hinzu, um das mit Beispielcode 2 implementierte benutzerdefinierte Authentifizierungsmodul zu unterstützen (siehe [Beispielcode 2](#)).

```
xyz:password:admin
test1:password:test1@LDAP1
test1:password:test1
test1@LDAP1:password:test1@LDAP1
test1@1:password:test1
user1:Password2:user1@SunONE1
user1_1:Password2:user1
user3:Password3:user3
DS_User1:Password123:DS_User1@MSAD1
DS_User1:Password123:DS_User1
DS_User1@1:Password123:DS_User1
```

Fügen Sie der Flat File, die als benutzerdefiniertes Benutzerverzeichnis verwendet wird, den folgenden Inhalt hinzu, wenn der Benutzername im Format *username@providername* zurückgegeben werden soll:

```
xyz:password:admin
test1:password:test1
test1@1:password:test1
user1_1:Password2:user1
user3:Password3:user3
DS1_1G100U_User61_1:Password123:DS1_1G100U_User61
DS1_1G100U_User61_1@1:Password123:DS1_1G100U_User61
TUser:password:TUser
```

# B

## Benutzerdefinierte Anmeldeklassen implementieren

Oracle Enterprise Performance Management System stellt `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` bereit, um die Benutzeridentität (DN) aus x509-Zertifikaten zu extrahieren.

Wenn Sie die Benutzeridentität im Zertifikat aus einem anderen Attribut als "DN" ableiten müssen, müssen Sie eine benutzerdefinierte Anmeldeklasse wie `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` entwickeln und implementieren, wie in diesem Anhang beschrieben.

### Beispielcodes für benutzerdefinierte Anmeldeklassen

Dieser Beispielcode zeigt die Implementierung der Standardklasse `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`. Sie müssen die Methode `parseCertificate(String sCertificate)` dieser Implementierung in der Regel so anpassen, dass der Benutzername aus einem anderen Zertifikatsattribut als DN abgeleitet wird:

```
package com.hyperion.css.sso.agent;

import java.io.ByteArrayInputStream;
import java.io.UnsupportedEncodingException;
import java.security.Principal;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import com.hyperion.css.CSSSecurityAgentIF;
import com.hyperion.css.common.configuration.*;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * X509CertificateAuthImpl implements the CSSSecurityAgentIF interface It
 * accepts
 * the X509 certificate of the authenticated user from the Web Server via a
 * header, parses the certificate, extracts the DN of the User and
 * authenticates the user.
 */
public class X509CertificateSecurityAgentImpl implements CSSSecurityAgentIF
{
    static final String IDENTITY_ATTR = "CN";
    String g_userDN = null;
    String g_userName = null;
    String hostAddress = null;
    /**
```



```

    * Returns the User name (login name) of the authenticated user,
    * for example demouser. See CSS API documentation for more
information
    */
    public String getUsername(HttpServletRequest req,
        HttpServletResponse res)
        throws Exception
    {
        hostAddress = req.getServerName();
        String certStr = getCertificate(req);

        String sCert = prepareCertificate(certStr);

        /* Authenticate with a CN */
        parseCertificate(sCert);

        /* Authenticate if the Login Attribute is a DN */
        if (g_userName == null)
        {
            throw new Exception("User name not found");
        }
        return g_userName;
    }

    /**
    * Passing null since this is a trusted Security agent
authentication
    * See Security API documentation for more information on
CSSSecurityAgentIF
    */
    public String getPassword(HttpServletRequest req,
        HttpServletResponse res)
        throws Exception
    {
        return null;
    }

    /**
    * Get the Certificate sent by the Web Server in the HYPLOGIN
header.
    * If you pass a different header name from the Web server, change
the
    * name in the method.
    */
    private String getCertificate(HttpServletRequest request)
    {
        String cStr = (String)request
            .getHeader(CSSConfigurationDefaults.HTTP_HEADER_HYPLOGI
N);
        return cStr;
    }

    /**
    * The certificate sent by the Web server is a String.
    * Put a "\n" in place of whitespace so that the X509Certificate

```

```

    * java API can parse the certificate.
    */
private String prepareCertificate(String gString)
{
    String str1 = null;
    String str2 = null;

    str1 = gString.replace("-----BEGIN CERTIFICATE-----", "");
    str2 = str1.replace("-----END CERTIFICATE-----", "");
    String certStrWithNL = "-----BEGIN CERTIFICATE-----"
        + str2.replace(" ", "\n") + "-----END CERTIFICATE-----";
    return certStrWithNL;
}

/**
 * Parse the certificate
 * 1. Create X509Certificate using the certificateFactory
 * 2. Get the Principal object from the certificate
 * 3. Set the g_userDN to a certificate attribute value (DN in this
sample)
 * 4. Parse the attribute (DN in this sample) to get a unique username
 */
private void parseCertificate(String sCertificate) throws Exception
{
    X509Certificate cert = null;
    String userID = null;
    try
    {
        X509Certificate clientCert = (X509Certificate)CertificateFactory
            .getInstance("X.509")
            .generateCertificate(
                new
                ByteArrayInputStream(sCertificate
                    .getBytes("UTF-8")));

        if (clientCert != null)
        {
            Principal princDN = clientCert.getSubjectDN();
            String dnStr = princDN.getName();
            g_userDN = dnStr;
            int idx = dnStr.indexOf(",");
            userID = dnStr.substring(3, idx);
            g_userName = userID;
        }
    }
    catch (CertificateException ce)
    {
        throw ce;
    }
    catch (UnsupportedEncodingException uee)
    {
        throw uee;
    }
}

```

```
    } //end of getUsernameFromCert  
} // end of class
```

## Benutzerdefinierte Anmeldeklassen bereitstellen

Führen Sie die folgenden Schritte aus, um die benutzerdefinierte Anmeldekasse zu implementieren:

1. Erstellen und testen Sie die benutzerdefinierte Anmeldekasse. Stellen Sie sicher, dass Ihr Code keine Referenzen auf `log4j` enthält. Informationen hierzu finden Sie unter [Beispielcodes für benutzerdefinierte Anmeldeklassen](#).

Sie können einen beliebigen Namen für Ihre benutzerdefinierte Klasse verwenden.

2. Fügen Sie die benutzerdefinierte Anmeldekasse in die Datei `CustomAuth.jar` ein.
3. Kopieren Sie die Datei `CustomAuth.jar` in das Deployment:

- **WebLogic:** Kopieren Sie `CustomAuth.jar` in das Verzeichnis `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`. Dieses lautet in der Regel `Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

### Hinweis:

Bei einem Upgrade von Release 11.1.2.0 oder 11.1.2.1, das eine Implementierung der benutzerdefinierten Anmeldekasse enthielt, verschieben Sie `CustomAuth.jar` von `EPM_ORACLE_HOME/common/jlib/11.1.2.0` in `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Client-Deployments:** Kopieren Sie `CustomAuth.jar` in alle Client-Deployments von Oracle Enterprise Performance Management System am folgenden Speicherort:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, in der Regel `Oracle/Middleware/common/jlib/11.1.2.0`

Oracle empfiehlt, die Clientzertifikatauthentifizierung zu aktivieren, wenn Sie eine benutzerdefinierte Anmeldekasse verwenden.

# C

## Benutzer und Gruppen benutzerverzeichnisübergreifend migrieren

### Übersicht

Viele Szenarios können dazu führen, dass die Benutzer- und Gruppenidentitäten bereitgestellter Oracle Enterprise Performance Management System-Benutzer veralten. Ein Zugriff auf EPM System-Komponenten ist nicht möglich, wenn die verfügbaren Provisioning-Informationen veraltet sind. Folgende Szenarios können dazu führen, dass Provisioning-Daten veralten:

- Deaktivierung eines Benutzerverzeichnisses: Unternehmen können ein Benutzerverzeichnis deaktivieren, nachdem Benutzer in ein anderes Verzeichnis verschoben wurden.
- Versionsupgrade: Ein Upgrade der Benutzerverzeichnisversion kann Änderungen bei den Anforderungen für Hostcomputernamen oder Betriebssystemumgebungen beinhalten.
- Anbieteränderung: Unternehmen können ein Benutzerverzeichnis durch ein Benutzerverzeichnis eines anderen Anbieters ersetzen. Beispiel: Ein Unternehmen kann Oracle Internet Directory durch SunONE Directory Server ersetzen.



#### Hinweis:

- In diesem Anhang wird das Benutzerverzeichnis, das Sie einstellen, als *Quellbenutzerverzeichnis* bezeichnet. Das Benutzerverzeichnis, in das die Benutzeraccounts verschoben wurden, wird als *Zielbenutzerverzeichnis* bezeichnet.
- Diese Migrationsprozedur unterstützt nicht die Migration von Benutzeraccounts aus einem Quellbenutzerverzeichnis in ein Zielbenutzerverzeichnis, sondern nur deren Zuordnung in EPM-Anwendungen. Benutzer müssen im Zielbenutzerverzeichnis manuell erstellt werden. Dieser Prozess gilt für Benutzer in jedem Quellbenutzerverzeichnis, einschließlich Native Directory.

Wenn ein mit Hyperion Shared Services konfiguriertes Quellbenutzerverzeichnis andere Gruppen als Native Directory-Gruppen enthält, sollten diese Gruppen auch im Zielbenutzerverzeichnis erstellt werden.

### Voraussetzungen

- Oracle Enterprise Performance Management System-Benutzer und -Gruppen, deren Provisioning-Daten benutzerverzeichnisübergreifend migriert werden, müssen im Zielbenutzerverzeichnis verfügbar sein.

Gruppenbeziehungen, die im Quellbenutzerverzeichnis vorhanden sind, müssen im Zielbenutzerverzeichnis beibehalten werden.

- Die Benutzernamen von EPM System-Benutzern müssen in allen Quell- und Zielbenutzerverzeichnissen identisch sein.

## Migrationsverfahren

### Native Directory-Daten exportieren

Führen Sie in der Quellumgebung folgende Schritte aus:

Mit Oracle Hyperion Enterprise Performance Management System Lifecycle Management können Sie nur die folgenden Shared Services-Artefakte aus Native Directory exportieren:

- Native Directory-Gruppen
- Zugewiesene Rollen
- Delegationslisten

Lifecycle Management erstellt mehrere Exportdateien, in der Regel im Verzeichnis `EPM_ORACLE_INSTANCE/import_export/USER_NAME/EXPORT_DIR/resource/` Native Directory. Dabei gibt `USER_NAME` die Identität des Benutzers an, der den Export durchgeführt hat, z.B. `admin`, und `EXPORT_DIR` ist der Name des Exportverzeichnisses. In der Regel werden folgende Dateien erstellt:

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`
- `Assigned Roles/PROD_NAME.csv` für jede bereitgestellte Anwendung, wobei `PROD_NAME` der Name einer Oracle Enterprise Performance Management System-Komponente ist, z.B. `Shared Services`.

#### Hinweis:

- Ausführliche Anweisungen zum Exportieren von Daten mit Lifecycle Management finden Sie in der Dokumentation *Oracle Enterprise Performance Management System - Lifecycle Management*.
- Stellen Sie sicher, dass die Datei `Users.csv` nicht exportiert wird.

Stellen Sie nach dem Artefaktexport sicher, dass im Migrationsstatusbericht für den letzten Exportvorgang der Status `Completed` angezeigt wird.

So exportieren Sie Native Directory-Daten:

1. Wählen Sie im Ansichtsbereich von Oracle Hyperion Shared Services Console in der Anwendungsgruppe **Foundation** die Anwendung **Shared Services** aus.
2. Wählen Sie für die Migration nur die erforderlichen Artefakte aus der folgenden Liste aus:

- Native Directory-Gruppen
  - Zugewiesene Rollen
  - Delegationslisten
3. Klicken Sie auf **Exportieren**.
  4. Geben Sie einen Namen für das Exportarchiv ein. Der Standardname lautet `admin DATE`, z.B. `admin 13-03-18`.
  5. Klicken Sie auf **Exportieren**.

### Native Directory-Daten importieren

Führen Sie in der Zielumgebung folgende Schritte aus:

1. Erstellen Sie Folgendes manuell:
  - a. Benutzer im externen Zielbenutzerverzeichnis, analog zum Quellbenutzerverzeichnis.
  - b. Gruppen im externen Zielbenutzerverzeichnis, analog zum Quellbenutzerverzeichnis, mit Ausnahme der Native Directory-Gruppen.
2. Konfigurieren Sie das Zielbenutzerverzeichnis.

Fügen Sie das Zielbenutzerverzeichnis als externes Benutzerverzeichnis in EPM System hinzu, wenn Sie die Benutzeraccounts aus dem Quellbenutzerverzeichnis in ein anderes Benutzerverzeichnis verschoben haben. Beispiel: Wenn Sie die Benutzeraccounts von Oracle Internet Directory in SunONE Directory Server verschoben haben, müssen Sie SunONE Directory Server als externes Benutzerverzeichnis hinzufügen. Informationen hierzu finden Sie in Kapitel 3 zum Konfigurieren von Benutzerverzeichnissen in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

 **Hinweis:**

Stellen Sie sicher, dass das Zielbenutzerverzeichnis Benutzeraccounts und Gruppen für alle EPM System-Benutzer enthält, deren Daten aus dem Quellbenutzerverzeichnis migriert werden.

Wenn Sie die Benutzer in ein Benutzerverzeichnis verschoben haben, das bereits als externes Benutzerverzeichnis definiert ist, stellen Sie sicher, dass die Benutzerverzeichnisse für Oracle Hyperion Shared Services sichtbar sind. Hierzu können Sie nach Benutzern aus Shared Services Console suchen. Informationen hierzu finden Sie im Abschnitt zum Suchen nach Benutzern, Gruppen, Rollen und Delegationslisten in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

Stellen Sie beim Konfigurieren des Zielbenutzerverzeichnisses als externes Benutzerverzeichnis sicher, dass die Eigenschaft "Anmeldeattribut" auf das Attribut verweist, dessen Wert ursprünglich als Benutzername im Quellbenutzerverzeichnis verwendet wurde. Informationen hierzu finden Sie unter [Voraussetzungen](#).

3. Verschieben Sie das Zielbenutzerverzeichnis an den Anfang der Suchreihenfolge.

 **Hinweis:**

Wenn der Name des Zielbenutzerverzeichnisses mit dem Namen des Quellverzeichnisses identisch ist, müssen Sie das Quellbenutzerverzeichnis aus der EPM System-Konfiguration löschen.

Shared Services weist einem neu hinzugefügten Benutzerverzeichnis eine niedrigere Priorität in der Suchreihenfolge zu als vorhandenen Verzeichnissen. Ändern Sie die Suchreihenfolge, damit das Zielbenutzerverzeichnis eine höhere Priorität in der Suchreihenfolge hat als das Quellbenutzerverzeichnis. Anhand dieser Reihenfolge kann Shared Services Benutzer im Zielbenutzerverzeichnis ermitteln, bevor die Quelle durchsucht wird. Informationen hierzu finden Sie im Abschnitt zum Verwalten der Suchreihenfolge für Benutzerverzeichnisse in der *Oracle Enterprise Performance Management - Administrationsdokumentation für Benutzersicherheit*.

4. Starten Sie Oracle Hyperion Foundation Services und andere EPM System-Komponenten neu, um die vorgenommenen Änderungen zu erzwingen.
5. Importieren Sie die Native Directory-Daten (die aus der Quellumgebung exportiert wurden):  
Führen Sie Lifecycle Management mit der Option `create/update` aus, um die zuvor aus Native Directory exportierten Daten (unten aufgelistet) zu importieren.
  - `Groups.csv`
  - `Assigned Roles.csv`
  - `Delegated Lists.csv`

 **Hinweis:**

- Ausführliche Anweisungen zum Importieren von Daten mit Lifecycle Management finden Sie in der Dokumentation *Oracle Enterprise Performance Management System - Lifecycle Management*.
- Stellen Sie sicher, dass die Datei `Users.csv` nicht importiert wird.

Stellen Sie nach dem Datenimport sicher, dass im Migrationsstatusbericht für den letzten Importvorgang der Status `Completed` angezeigt wird.

So importieren Sie Native Directory-Daten:

- a. Blenden Sie im Ansichtsbereich von Shared Services Console **Dateisystem** ein.
- b. Wählen Sie den Speicherort der Importdateien im Dateisystem aus.
- c. Wählen Sie den Typ der Artefakte aus, für die Sie Provisioning-Informationen importieren möchten.
- d. Klicken Sie auf **Importieren**.
- e. Klicken Sie auf **OK**.

## Produktspezifische Updates

### ▲ **Achtung:**

Oracle empfiehlt, ein Backup der Benutzer- und Gruppendaten in dem von der Oracle Enterprise Performance Management System-Komponente verwendeten Repository zu erstellen, bevor produktspezifische Aktualisierungen gestartet werden. Nach der Aktualisierung von Informationen im lokalen Produkt-Repository können Sie die alten Benutzer- und Gruppendaten im lokalen Produkt-Repository nur über Backups wiederherstellen.

### **Planning**

Oracle Hyperion Planning speichert Informationen zu berechtigten Benutzern und Gruppen im Planning-Repository. Wenn Benutzer und Gruppen benutzerverzeichnisübergreifend migriert wurden und dadurch eine Benutzeridentität in Native Directory geändert wurde, müssen Sie die Informationen im Planning-Repository mit den Informationen in Native Directory synchronisieren. Klicken Sie hierzu auf die Schaltfläche zum Migrieren von Benutzern und Gruppen. Diese Schaltfläche ist in Planning verfügbar, wenn Zugriff auf Eingabeformulare, Elemente und Aufgabenlisten zugewiesen wird.

### **Financial Management**

Oracle Hyperion Financial Management erfasst Informationen zu Benutzern und Gruppen, die über Zugriffsberechtigungen für Objekte in einem lokalen Financial Management-Repository verfügen. Wenn Benutzer und Gruppen benutzerverzeichnisübergreifend migriert und dadurch Benutzer- und Gruppeninformationen in Native Directory geändert wurden, müssen Sie die Informationen im Financial Management-Repository mit den Informationen in Native Directory synchronisieren.