

## **Oracle® Enterprise Repository**

eTrust SiteMinder セットアップおよびコンフィグレーション ガイド

10g リリース 3 (10.3)

2008 年 10 月

Copyright © 2007, 2008, Oracle. All rights reserved.

原著者 : Vimika Dinesh

協力者 : Scott Spieker, Jeff Schieli, Sharon Fay, Atturu Chandra Prasad Reddy

このプログラム(ソフトウェアおよびドキュメントを含む)には、オラクル社およびその関連会社に所有権のある情報が含まれています。このプログラムの使用または開示は、オラクル社およびその関連会社との契約に記された制約条件に従うものとします。著作権、特許権およびその他の知的財産権と工業所有権に関する法律により保護されています。独立して作成された他のソフトウェアとの互換性を得るために必要な場合、もしくは法律によって規定される場合を除き、このプログラムのリバース・エンジニアリング、逆アセンブル、逆コンパイル等は禁止されています。

このドキュメントの情報は、予告なしに変更される場合があります。オラクル社およびその関連会社は、このドキュメントに誤りが無いことの保証は致し兼ねます。これらのプログラムのライセンス契約で許諾されている場合を除き、プログラムを形式、手段(電子的または機械的)、目的に関係なく、複製または転用することはできません。

このプログラムが米国政府機関、もしくは米国政府機関に代わってこのプログラムをライセンスまたは使用する者に提供される場合は、次の注意が適用されます。

#### U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このプログラムは、核、航空産業、大量輸送、医療あるいはその他の危険が伴うアプリケーションへの用途を目的としておりません。このプログラムをかける目的で使用する場合、上述のアプリケーションを安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。万一かかるプログラムの使用に起因して損害が発生いたしましても、オラクル社およびその関連会社は一切責任を負いかねます。

Oracle, JD Edwards, PeopleSoft, Siebelは米国Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称は、他社の商標の可能性があります。

このプログラムは、第三者のWebサイトへリンクし、第三者のコンテンツ、製品、サービスへアクセスすることがあります。オラクル社およびその関連会社は第三者のWebサイトで提供されるコンテンツについては、一切の責任を負いかねます。当該コンテンツの利用は、お客様の責任になります。第三者の製品またはサービスを購入する場合は、第三者と直接の取引となります。オラクル社およびその関連会社は、第三者の製品およびサービスの品質、契約の履行(製品またはサービスの提供、保証義務を含む)に関しては責任を負いかねます。また、第三者との取引により損失や損害が発生いたしましても、オラクル社およびその関連会社は一切の責任を負いかねます。

## Oracle Enterprise Repository

# eTrust™ SiteMinder® セットアップおよびコンフィグレーション ガイド

## 目次

- **SiteMinder による認証で使用するための Oracle Enterprise Repository のコンフィグレーション**
  - SiteMinder による統合のシステム プロパティの有効化
  - アプリケーション プロパティ ファイルの変更
- **詳細オプション**
  - 新しいユーザのデフォルトのロールの作成と割り当て
  - 新しいユーザの作成と未承認のユーザの許可
  - 未承認のユーザと新しいユーザのログインの有効化
  - 新しいユーザの通知
  - 部門の同期
  - ロールの同期

## 概要

Oracle Enterprise Repository の **Advanced Container Authentication Login Module** は、(SSO システムによって値が設定されている可能性のある) HTTP リクエスト ヘッダによって渡されるユーザ資格の受け入れに使用されます。この機能を使用すると、eTrust Siteminder などのシングル サインオン システムとの統合が可能になります。

## SiteMinder による認証で使用するための Oracle Enterprise Repository のコンフィグレーション

以下のコンフィグレーション プロパティにアクセスするには、**Access Administrator** 権限が必要です。

**SSO SOAP ヘッダの拡張に関する注意事項** - この拡張により、AuthtokenCreate REX API メソッドに必要な SOAP ヘッダのユーザ情報を Advanced Container Login Module で受け入れることができます。ユーザ名は SOAP ヘッダ内で渡されます。この SOAP ヘッダの名前は、Oracle Enterprise Repository のシステム設定 `enterprise.container.auth.username` で識別され、`namespaceUri` は `www.oracle.com/oer` になります。SOAP ヘッダの値はユーザのユーザ名です。ユーザ名が SOAP ヘッダ内で渡されない場合は、Oracle Enterprise Repository のシステム設定 `enterprise.loginmodules.fallbackauthentication` が使用されます。`enterprise.loginmodules.fallbackauthentication` が `true` の場合、ユーザは、指定されたユーザ名とパスワードについてコンフィグレーション済みの `PluggableLoginModule` によって認証されます。

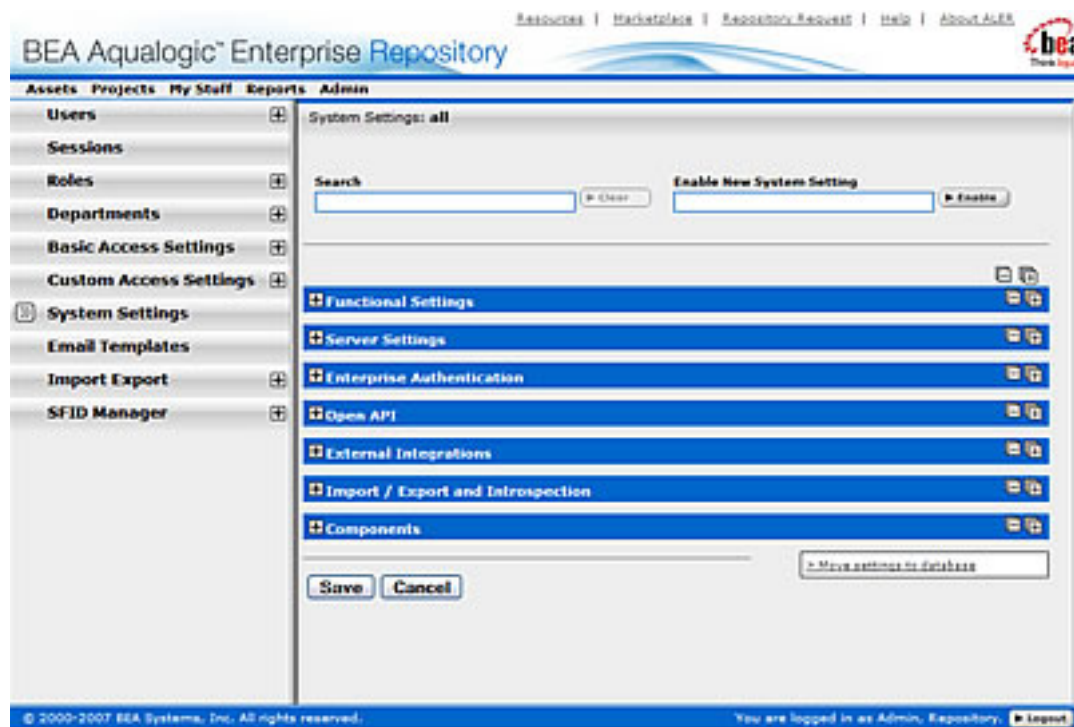
ログイン モジュールのプラグインは、データベース ログイン モジュール、LDAP ログイン モジュール、およびカスタム ログイン モジュールをコンフィグレーションするために設定されたコンフィグレーションです。コンテナ ログイン モジュールには、Container Managed Login Module または Advanced Container Login Module (SSO) のどちらかを指定することができます。これらは [System Settings] タブでコンフィグレーションできます。

**注意** : フォールバック認証は REX API でのみ使用できます。

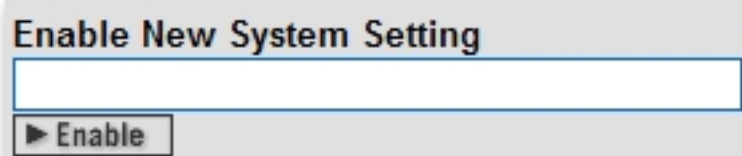
## SiteMinder による統合のシステム プロパティの有効化

この手順は Oracle Enterprise Repository の [Admin] 画面で行われます。

1. 左ペインの [System Settings] をクリックします。

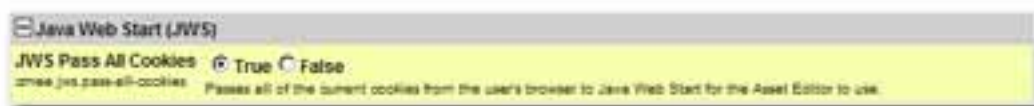


2. [Search] ボックスに「**enterprise.authentication.advancedcontainer.enabled**」と入力します。値を [True] に設定して [Save] をクリックします。
3. [Enable New System Setting] テキスト ボックスに「**cmee.jws.pass-all-cookies**」と入力します。



4. [Enable] をクリックします。

システム設定の [Server Settings] グループの [Java Web Start (JWS)] セクションに、[JWS Pass All Cookies] が表示されます。



5. プロパティが [True] に設定されていることを確認します。
6. [Save] をクリックします。
7. [System Settings] の [Search] テキスト ボックスに、「container login module」と入力します。

システム設定の [Enterprise Authentication] グループに [Container Login Module] セクションが開きます。

The screenshot shows a dialog box titled "Container Login Settings". It has four rows of settings:

- Container Login Module Class Name:** A text input field with the value "enterprise.loginmodules.containerloginmodule.classname" and a description "Class name of the container login module".
- Container Login Module Display Name:** A text input field with the value "enterprise.loginmodules.containerloginmodule.displayname" and a description "Display name of the container login module".
- Container Login Module:** A section with the value "enterprise.loginmodules.containerloginmodule.enabled" and a description "Enables the container login module". It has two radio buttons: "True" (which is selected) and "False".
- Container Login Module - Internal Checking:** A section with the value "enterprise.loginmodules.containerloginmodule.internalchecking" and a description "Enables internal checking for the container login module". It has two radio buttons: "True" (which is selected) and "False".

8. 次のプロパティを記載どおりに変更します。
  - [Container Login Module Class Name]
    - テキスト ボックスに  
「com.flashline.enterprise.authentication.server.loginmodule.AdvancedContainerLogin」と入力します。
  - [Container Login Module Display Name]
    - テキスト ボックスに「Advanced Container Login Module」と入力します。
  - [Container Login Module]
    - プロパティを [True] に設定します。
9. SSO ヘッダの値を次のように指定します (多くの場合、これらはポリシー サーバ内の応答と呼ばれます)。想定されるデータ型と指定できる値をヘッダ名の後に示します。想定される値の型は、ポリシー サーバによって提供される応答に適用します。
  - [Username Header Name]
    - このプロパティを、ユーザの UID 値を格納するヘッダの [Name] に設定します。
      - このヘッダには、ユーザのユーザ ID を格納する必要があります (必須)。
  - [Firstname Header Name]

- このプロパティを、ユーザの名前 (名) の値を格納するヘッダの [Name] に設定します。(英文字列)
  - このヘッダには、ユーザの適切な名前を格納する必要があります。
- [Middlename Header Name]
  - このプロパティを、ユーザの名前 (ミドル ネーム) の値を格納するヘッダの [Name] に設定します。(英文字列)
    - このヘッダには、ユーザのミドル ネームを格納する必要があります。
- [Lastname Header Name]
  - このプロパティを、ユーザの名前 (姓) の値を格納するヘッダの [Name] に設定します。(英文字列)
    - このヘッダには、ユーザの姓を格納する必要があります。
- [Status Header Name]
  - このプロパティを、ユーザのアクティブ状態の値を格納するヘッダの [Name] に設定します。
    - このヘッダには、OER 内のユーザの状態を指定する有効な整数値を格納する必要があります。有効な値については、次の一覧を参照してください **(必須)**。
      - 00 - アクティブ
      - 10 - 未承認
      - 20 - ロックアウト済み
      - 30 - 非アクティブ
- [Email Header Name]
  - このプロパティを、ユーザの電子メールの値を格納するヘッダの [Name] に設定します。
    - このヘッダには、ユーザの電子メール アドレスを格納する必要があります **(必須)**。
- [Phone Header Name]
  - このプロパティを、ユーザの電話番号の値を格納するヘッダの [Name] に設定します。
    - このヘッダには、ユーザの電話番号を格納する必要があります。
- [Roles Header Name]
  - このプロパティを、ユーザのロールの値を格納するヘッダの [Name] に設定します。
    - このヘッダには、ユーザのロールを格納する必要があります。
- [Department Header Name]
  - このプロパティを、ユーザの部門の値を格納するヘッダの [Name] に設定します。

- このヘッダには、ユーザの部門を格納する必要があります。

## 10. SSO モジュールの動作を次のプロパティで更新します。

- [Use Container passed Departments]
  - ポリシー サーバの応答からユーザの部門を同期する場合は、この値を [True] に設定します。
- [Departments passed within single header]
  - 複数の部門名がポリシー サーバの応答として渡される場合は、この値を [True] に設定します。
- [Department Delimiter]
  - このプロパティの値を、1 つの部門ヘッダ内の複数の部門を区切る文字に設定します。このフィールドでは ¥u0020 (スペース) などの Unicode 表記を使用できます。
- [Use Container passed Roles]
  - ポリシー サーバの応答からユーザのロールを同期する場合は、この値を [True] に設定します (注意 : コンフィグレーションが適切であることを確認する前にこの値を [true] に設定すると、Oracle Enterprise Repository アプリケーションが使用できなくなる可能性があります)。
- [Roles passed within single header]
  - 複数のロール名がポリシー サーバの応答として渡される場合は、この値を [True] に設定します。
- [Role Delimiter]
  - このプロパティの値を、1 つのロール ヘッダ内の複数のロールを区切る文字に設定します。このフィールドでは ¥u0020 (スペース) などの Unicode 表記を使用できます。
- [Assign default roles to users]
  - Oracle Enterprise Repository 内の既存のユーザと新しいユーザのユーザアカウントに、「デフォルト」とマークされるすべてのロールが割り当てられる場合は、この値を [True] に設定します。
- [Auto create missing roles]
  - Oracle Enterprise Repository 内に現在は存在しないユーザのロール ヘッダ内に含まれるロールを Oracle Enterprise Repository で作成できるようにするには、この値を [True] に設定します。この機能により、ロールが作成され、そのロールにユーザが割り当てられます。ただし、作成されるロールにはパーミッションが割り当てられません。

- [Auto create missing departments]
  - 現在は存在しないユーザの部門ヘッダ内に含まれる部門を Oracle Enterprise Repository で作成できるようにするには、この値を [True] に設定します。この機能により、部門が作成され、その部門にユーザが割り当てられます。新しく作成される部門は、プロジェクトには割り当てられません。
- 11. [System Settings] の [Search] テキスト ボックスに、「cookie login module」と入力します。

システム設定の [Enterprise Authentication] グループに [Cookie Login Settings] セクションが開きます。
- 12. [Cookie Login Module] プロパティを [False] に設定します。
- 13. [System Settings] の [Search] テキスト ボックスに、「plug-in login」と入力します。

システム設定の [Enterprise Authentication] グループに [Plugin Login Settings] セクションが開きます。
- 14. [Plug-in Login Module] テキスト ボックスに「false」と入力します。
- 15. [Save] をクリックします。

## Oracle Enterprise Repository の SSO 統合および基本認証の使用

SiteMinder のインストールで**基本認証**を使用する場合は、Oracle Enterprise Repository **Asset Editor** を正しく機能させるために追加のプロパティ設定が必要になります。

1. 上記のプロセスを使用して、次のプロパティを有効にします。
  - `cmee.jws.suppress-authorization-header`
2. プロパティを [True] に設定します。
3. [Save] をクリックします。

## アプリケーション プロパティ ファイルの手動での変更

- **前提条件** : アプリケーション サーバを停止します。
  - プロパティ ファイルを変更すると、アプリケーション サーバで実行しているアプリケーションに影響を与える可能性があります。

1. WEB-INF/classes の containerauth.properties ファイルを編集します。

このファイルには、SiteMinder サーバに固有のヘッダ名のリストが格納されます。この情報は、SiteMinder が応答に使用する応答ヘッダを表し、組織の SiteMinder の管理者または設計者から入手する必要があります。

SiteMinder の応答で**電子メール** ヘッダに適した値が提供されない場合は、true のヘッダ値の代わりに空白の "" を使用できます。SiteMinder によって値が設定されていないその他のフィールドは null のままにしてください。

(アスタリスク (\*) は必須フィールドを示しています。)

- 適切な Oracle Enterprise Repository ユーザ情報にマップする必要のあるヘッダの変数をコンフィグレーションします。

(**注意** : 以下に示す値はあくまでも例であるため、お使いの SiteMinder システムで定義されている適切な SiteMinder 応答ヘッダ名で**置き換える**必要があります。)

- `enterprise.container.auth.username = <UID>*`
- `enterprise.container.auth.firstname = <FIRST_NAME>`
- `enterprise.container.auth.middlename = <MIDDLE_NAME>`
- `enterprise.container.auth.lastname = <LAST_NAME>`
- `enterprise.container.auth.status = <STATUS>`
- `enterprise.container.auth.email = <MAIL>*`
- `enterprise.container.auth.phone = <PHONE>`
- `enterprise.container.auth.roles = <ROLES>`
- `enterprise.container.auth.depts = <DEPARTMENTS>`
- `enterprise.container.auth.enable-synch-roles = true`
- `enterprise.container.auth.roles-single-header = true`
- `enterprise.container.auth.roles-delimiter = ¥u0020`
- `enterprise.container.auth.enable-synch-depts = true`
- `enterprise.container.auth.depts-single-header = true`
- `enterprise.container.auth.depts-delimiter = ¥u0020`

**注意** : 上記の最後の 6 つのプロパティは、ロールまたは部門の同期が有効な場合に利用されます。1 つのヘッダには複数のロールまたは部門が指定されます。このような追加のプロパティは、ブール パラメータ `enable-synch-roles` および `enable-synchdepts` に指定されている値に応じて無効にしたり、無視したりすることができます。

この例の区切り記号フィールドでは、Unicode のスペース文字を使用しています。ただし、その他の区切り文字については Unicode は不要です。

2. 大部分の SiteMinder Web エージェント アプリケーションは、アプリケーション サーバとは別の HTTP サーバに対してデプロイされます。このシナリオでは、AJP タイプのコネクタ (Apache HTTP Server 用の `mod_jk/mod_jk2`、IBM HTTP Server 用の `mod_was_ap20_http` など) が HTTP サーバをアプリケーション サーバにリンクします。通常、パフォーマンスまたはリソース プール上の理由で、HTTP サーバは個別のマシンで実行されます。このシナリオでは、以下に示すように `cmee.properties` ファイルを変更して、アプリケーションの新しい名前を反映する必要があります。

○ WEB-INF/classes の `cmee.properties` ファイルを編集します。

- 元のコンフィグレーション (Coyote を使用する Tomcat)
  - `cmee.server.paths.image=http¥://tomcat.example.com¥:8080/flashline-web/images`
  - `cmee.server.paths.jsp=http¥://tomcat.example.com¥:8080/flashline`
  - `cmee.server.paths.servlet=http¥://tomcat.example.com¥:8080/flashline`
  - `cmee.server.paths.jnlp-tool=http¥://tomcat.example.com¥:8080/flashline-web/webstart`
  - `cmee.server.paths.resource=http¥://tomcat.example.com¥:8080/flashline-web`
  - `cmee.enterprisetab.homepage=http¥://tomcat.example.com¥:8080/flashline/custom/home.jsp`
  - `cmee.assettab.asset-detail-page=http¥://tomcat.example.com¥:8080/flashline/cmee/index.jsp`
- 新しいコンフィグレーション (mod\_jk2 による Apache HTTP と Tomcat の連携)
  - `cmee.server.paths.image=http¥://apache.example.com/flashlineweb/images`
  - `cmee.server.paths.jsp=http¥://apache.example.com/flashline`
  - `cmee.server.paths.servlet=http¥://apache.example.com/flashline`
  - `cmee.server.paths.jnlp-tool=http¥://apache.example.com/flashline-web/webstart`
  - `cmee.server.paths.resource=http¥://apache.example.com/flashline-web`
  - `cmee.enterprisetab.homepage=http¥://apache.example.com/flashline/custom/home.jsp`
  - `cmee.assettab.asset-detail-page=http¥://apache.example.com/flashline/cmee/index.jsp`
- この例でリポジトリに接続するための新しい URL は次のとおりです。

**`http://apache.example.com/flashline/index.jsp`**

3. Oracle Enterprise Repository アプリケーションを再起動します。

# SiteMinder の詳細オプション

以下に示すオプションでは、デフォルトのロール、新しいユーザの作成と通知、部門の同期、およびロールの同期を支援する機能を追加します。

## 新しいユーザのデフォルトのロールの作成と割り当て

### 拡張 RBAC を使用する場合：

1. Oracle Enterprise Repository メニュー バーの [Admin] をクリックします。
2. [Admin] 画面で、[Roles] をクリックします。
3. [Create New] をクリックします。
4. 名前フィールドに「**Browse\_Only**」と入力します。
  - [Automatically assign to new users] をチェックします。
  - このプロファイルに該当する既存のユーザをすべて追加します。
5. [Save] をクリックします。
6. [1: Create/Submit] ロールをクリックします。
7. [Edit] をクリックします。
  - [Automatically assign to new users] のチェックをはずします。
8. [Save] をクリックします。
9. [User] ロールをクリックします。
10. [Edit] をクリックします。
  - [Automatically assign to new users] のチェックを外します。(Oracle Enterprise Repository に付属する [User] は、デフォルトのロールであり、新しいユーザに自動的に割り当てられます)。
11. [Save] をクリックします。
12. [Custom Access Settings] をクリックします。
13. [Create New] をクリックします。
14. 名前フィールドに「**Browse\_Only**」と入力します。
  - [Automatically assign to all new assets] をチェックします。
  - ロールのリストで Browse\_Only を探します。
  - [View] をチェックします。
15. [Save] をクリックします。
16. [OK] をクリックしてすべてのアセットに適用します。

## 基本アクセス設定を使用する場合：

1. Oracle Enterprise Repository メニュー バーの [Admin] をクリックします。
2. [Admin] 画面で、[Roles] をクリックします。
3. [Create New] をクリックします。
4. 名前フィールドに「**Browse\_Only**」と入力します。
  - [Automatically assign to new users] をチェックします。
  - このプロファイルに該当する既存のユーザをすべて追加します。
5. [User] ロールをクリックします。
6. [Edit] をクリックします。
  - [Automatically assign to new users] のチェックを外します。(Oracle Enterprise Repository に付属する [User] は、デフォルトのロールであり、新しいユーザに自動的に割り当てられます)。
7. [Save] をクリックします。

## 新しいユーザの作成と未承認のユーザの許可

Oracle Enterprise Repository SiteMinder による認証統合では、新しいユーザの認証が成功すると、Oracle Enterprise Repository データベース内に新しいユーザが自動的に作成されます。新しいユーザに与えられるアクセス権とパーミッションは、前の節で説明したように、デフォルトの**新しいユーザのロール**のコンフィグレーションによって決定されます。アクセス管理者による承認時に、アクセス設定の異なる他のロールに新しいユーザが割り当てられる場合があります。ただし、ロールの同期が有効な状態で SiteMinder による統合がコンフィグレーションされている場合、ユーザには SiteMinder の応答ヘッダが提供するロールが割り当てられます。

## 未承認のユーザと新しいユーザのログインの有効化

このオプションを有効にすると、Oracle Enterprise Repository の未承認のユーザと新しいユーザは、SiteMinder による認証後にアプリケーションにアクセスできます。無効にすると、新しいユーザまたは未承認のユーザは Oracle Enterprise Repository にアクセスできません。この機能は、アプリケーションにアクセスする前に手動の承認プロセスが必要な場合に特に役立ちます。

- [Enable Unapproved User Login] = **true** (ファイル : enterprise.properties)
  - enterprise.security.unapproveduser.allowlogin=true

## 新しいユーザの通知

このプロパティを有効にすると、Oracle Enterprise Repository に新しいユーザ アカウントが SiteMinder 経由で追加された場合に、アクセス管理者に電子メール通知が送信されます。

- [Enable New User Notification] = **true** (ファイル : cmee.properties)
  - cmee.new.unapproved.users.notify=true

## 部門の同期

このプロパティを有効にすると、SiteMinder の応答ヘッダの値から部門名が同期されます。

- [Enable Department Syncing] = **true** (ファイル : *containerauth.properties*)
  - enterprise.container.auth.enable-synch-depts - 既知の部門がユーザと同期される場合は true に設定します。それ以外の場合は false に設定します。
- [Enable Department Creation] = **true** (ファイル : *containerauth.properties*)\*
  - enterprise.container.auth.auto-create-missing-depts - ログイン時にユーザの部門が自動的に作成される場合は true に設定します。それ以外の場合は false に設定します。

### 部門の同期に関する注意事項

SiteMinder による統合では、新しい部門は**作成されません**。SiteMinder の応答ヘッダの値に指定されている名前と同じ名前を持つ、Oracle Enterprise Repository 内の既存の部門とユーザがリンクされるだけです。

SiteMinder サーバは、名前が同じでユーザが割り当てられている部門ごとに値が異なる複数のヘッダ、またはユーザが割り当てられているすべての部門を格納する 1 つのヘッダを渡すようにコンフィグレーションできます。

- コンフィグレーション 1 - 名前が同じで、それぞれ値が異なる複数のヘッダ :  
enterprise.container.auth.enable-synch-depts= **true**  
enterprise.container.auth.depts-single-header= **false**  
enterprise.container.auth.depts-delimiter= ""  
enterprise.container.auth.depts= **DEPT\_HEADER\_NAME**

```
DEPT_HEADER_NAME=DEPTA  
DEPT_HEADER_NAME=DEPTB  
DEPT_HEADER_NAME=DEPTC
```

and NOT

```
DEPT_HEADER_NAME=DEPTA DEPTB DEPTC ...
```

- コンフィグレーション 2 - 区切り記号で区切られた複数の値を持つ 1 つのヘッダ :

```
enterprise.container.auth.enable-synch-depts= true
enterprise.container.auth.depts-single-header= true
enterprise.container.auth.depts-delimiter= "^"
enterprise.container.auth.depts= DEPT_HEADER_NAME
```

```
DEPT_HEADER_NAME=DEPTA^DEPTB^DEPTC^ ...
```

and NOT

```
DEPT_HEADER_NAME=DEPTA
DEPT_HEADER_NAME=DEPTB
DEPT_HEADER_NAME=DEPTC
```

## ロールの同期

このプロパティを有効にすると、SiteMinder の応答ヘッダの値からロール名が同期されます。

- [Enable Role Syncing] = **true** (ファイル : containerauth.properties)
  - enterprise.container.auth.auto-create-missing-roles - 既知のロールが自動作成される場合は true に設定します。それ以外の場合は false に設定します。

### ロールの同期に関する注意事項

SiteMinder による統合では、新しいロールを**作成できません**。この統合では、SiteMinder の応答ヘッダの値に指定されている名前と同じ名前を持つ、Oracle Enterprise Repository 内の既存のロールとユーザがリンクされます。既存のロールへのリンクに加えて、Oracle Enterprise Repository 内には存在しないヘッダの値にあるロールも作成されます。この方法で作成されるロールには、デフォルトではアクセス権が割り当てられません。

- [Enable Missing Role Creation] = **true** (ファイル : containerauth.properties)
  - *enterprise.container.auth.auto-create-missing-roles* = **true**

SiteMinder サーバは、ユーザが割り当てられているロールごとに 1 つのヘッダの値を渡すようにコンフィグレーションできます。

- コンフィグレーション 1 - 名前が同じで、それぞれ値が異なる複数のヘッダ :

```
enterprise.container.auth.enable-synch-roles= true
enterprise.container.auth.roles-single-header= false
enterprise.container.auth.roles-delimiter= ""
enterprise.container.auth.roles= ROLE_HEADER_NAME
```

```
ROLE_HEADER_NAME=ROLEA  
ROLE_HEADER_NAME=ROLEB  
ROLE_HEADER_NAME=ROLEC
```

and NOT

```
DEPT_HEADER_NAME=ROLEA ROLEB ROLEC ...
```

- コンフィグレーション 2 - 区切り記号で区切られた複数の値を持つ  
1 つのヘッダ :

```
enterprise.container.auth.enable-synch-roles= true  
enterprise.container.auth.roles-single-header= true  
enterprise.container.auth.roles-delimiter= "^"  
enterprise.container.auth.roles= ROLE_HEADER_NAME
```

```
DEPT_HEADER_NAME=ROLEA^ROLEB^ROLEC^ ...
```

and NOT

```
ROLE_HEADER_NAME=ROLEA  
ROLE_HEADER_NAME=ROLEB  
ROLE_HEADER_NAME=ROLEC
```

## デバッグのロギングの有効化

デバッグのロギングを有効にするには、log4j.properties ファイルに次の行を追加します。  
log4j.category.com.flashline.enterprise.authentication.client.LoginContext=debug, cmeeLog