

**Oracle® Enterprise Single Sign-On
Provisioning Gateway**
Oracle Identity Manager Connector ガイド
リリース 11.1.2
B72083-01

2012 年 7 月

Copyright © 1998, 2012, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、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。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことによる損害が発生しても、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 は Oracle Corporation およびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することができます。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

はじめに	4
対象読者	4
Provisioning Gateway OIMのコンポーネント	5
OIM Connector 11.1.2 のインストール	7
このコネクタを構成するファイルおよびディレクトリ	7
OIMConnector11.1.2.0.0.jarの構成	8
一般的なアプリケーション・サーバーのデプロイメント手順	9
OIM 9i Connectorへのアップグレード	12
コネクタ・ファイルおよびディレクトリ	12
OIM 9i Connectorの初期インストール	14
コネクタ・ファイルおよびディレクトリ	14
OIMConnector11.1.2.0.0.jarの構成	15
各種アプリケーション・サーバーのデプロイメント手順	16
SSO作業タスクの手動構成例	26
Provisioning Gateway定数の定義	26
既存プロセスのワークフローの構成	32
Passlogix Add Credentialプロセス・タスクの作成	35
Passlogix Change Passwordプロセス・タスクの作成	40
Passlogix Delete User Root Resourceプロセス・タスクの作成	44
iPlanetユーザー・プロセスのワークフローの構成	51
Passlogix Add Credentialプロセス・タスクの作成	51
Passlogix Change Passwordプロセス・タスクの作成	57
Passlogix Delete User Non-Root Resourceプロセス・タスクの作成	62
リコンシリエーション・プロセスのワークフローの構成	66
Reconciliation Add Credentialプロセス・タスクの作成	67
Reconciliation Passlogix Add Credentialプロセス・タスクの作成	72
サンプル・ワークフローの使用およびテスト	77
環境のデプロイメント	77
変数リスト	88
Passlogix Add Credentialsアダプタ	88
付録	90

はじめに

Oracle Enterprise Single Sign-On Provisioning Gateway (Provisioning Gateway)を使用すると、管理者は Oracle Enterprise Single Sign-On Logon Manager (Logon Manager)にユーザーの ID およびパスワードを自動的にプロビジョニングすることができます。分散エンタープライズ環境では、Provisioning Gateway からユーザーを SSO 対応アプリケーションにプロビジョニングする場合に、Oracle Identity Manager (OIM)を使用できます。ユーザーの資格証明を SSO 環境にプロビジョニングした後は、OIM によってユーザーのシングル・サインオンが可能になり、セキュリティが強化され、エンド・ユーザーはアプリケーション資格証明を把握、入力または思い出す必要がなくなります。

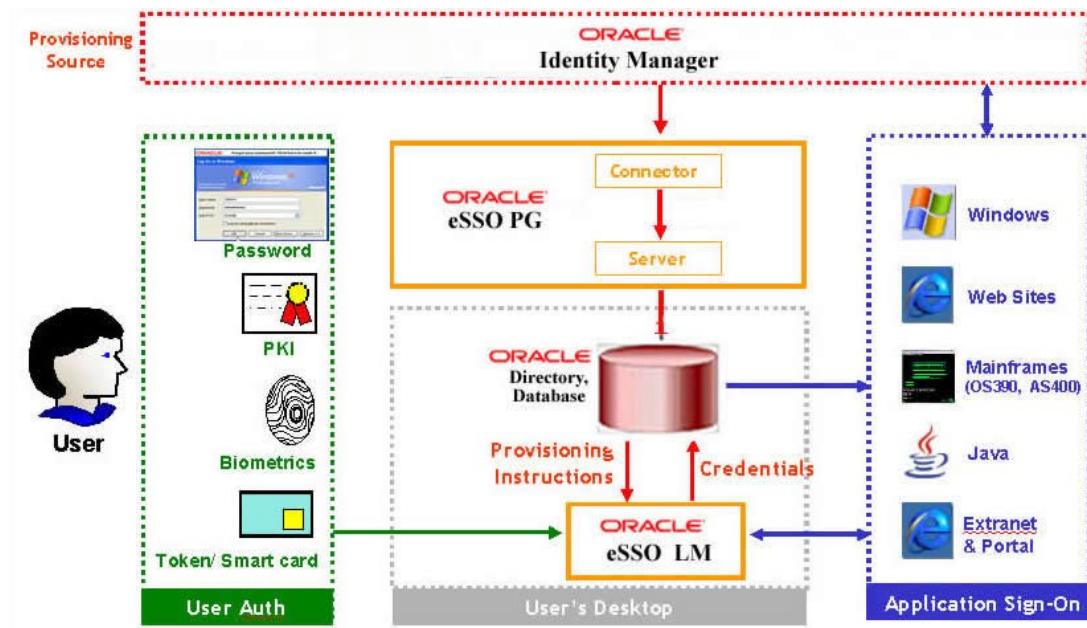
対象読者

このガイドでは、Provisioning Gateway OIM Connectorについて説明します。OIM Connector をデプロイする手順、および OIM Connector を使用して Provisioning Gateway のユーザー・プロビジョニングを管理する手順を示します。Provisioning Gateway の計画、実装およびデプロイメントを担当する経験豊富な管理者を対象としています。

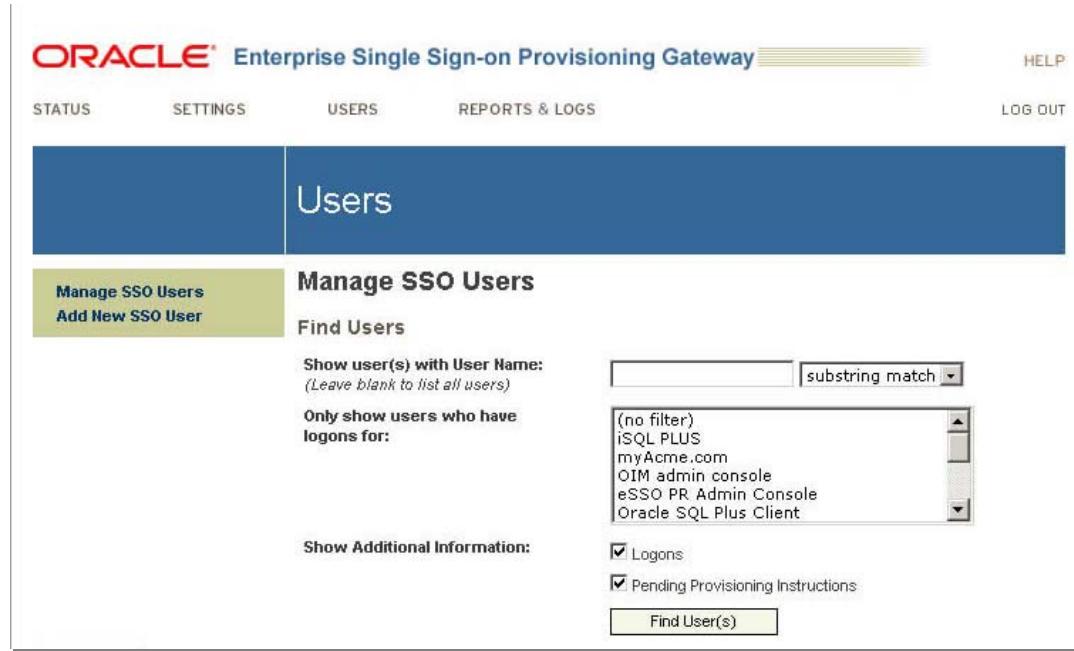
Provisioning Gateway OIM のコンポーネント

OIM と統合された Provisioning Gateway は、次のコンポーネントで構成されています。

- Provisioning Gateway Server: Web サービス・インターフェース経由でアカウント資格証明のプロビジョニング情報を受け入れ、LDAP やデータベースなどの SSO リポジトリ内のプロビジョニング情報をやり取りし、更新します。
- Provisioning Gateway Management Console: Provisioning Gateway Server と通信する Web ベースの管理グラフィカル・ユーザー・インターフェースを提供します。
- Oracle Identity Manager Connector: OIM と Provisioning Gateway Server 間の統合を提供します。このコネクタは Java ベースのクラス・ライブラリであり、製品ダウンロード中に使用可能になります。
- Provisioning Gateway CLI (コマンドライン・インターフェース) 管理ツール: Provisioning Gateway Server と通信します。



Provisioning Gateway には監査およびレポート機能が含まれており、管理者はユーザーおよびアプリケーションの使用状況に関する情報を得ることができます。たとえば、Provisioning Gateway Management Console を使用すると、管理者は Oracle Enterprise Single Sign-On Suite Administrative Console で特定のアプリケーションを構成しているすべてのユーザーを確認したり、特定ユーザー用の SSO 環境で構成されているすべてのアプリケーションを確認できます。Provisioning Gateway Server は OIM からプロビジョニング指示を受け取り、それに基づいて、Logon Manager Agent に対するアプリケーション構成の追加、削除および変更を更新します (Logon Manager Agent は、Provisioning Gateway Server と同じリポジトリと通信します)。



OIM Connector のデプロイでは、次の作業を行います。

- IIS サーバーで Provisioning Gateway Server をインストールし、設定する。
- OIM のデプロイメント管理ユーザー・インターフェースを使用して、Provisioning Gateway コネクタを OIM にインポートする。
- ルート・リソースおよび非ルート・リソース・オブジェクト用の OIM ワークフローを構成する。

このガイドでは、これらの構成を開始する手順を示します。

注意: ルート・リソース・オブジェクトは、Logon Manager がリポジトリへの接続に使用するアカウントを表します。ルート・リソース・オブジェクトは1つのみです。

非ルート・リソース・オブジェクトは、SSO テンプレートが存在するアカウントを表すリソース・オブジェクトです。

OIM Connector 11.1.2 のインストール

OIM Connector 11.1.2 は、Oracle Identity Manager (OIM)がコネクタ・コードと通信し、Provisioning Gatewayのユーザー・プロビジョニングを管理するためのインターフェースです。このコネクタは、[My Oracle Support](#)からダウンロードできます。

このコネクタを構成するファイルおよびディレクトリ

内容	目的	コメント
bin\ OIMConnector11.1.2.0.0.jar	OIM が Provisioning Gateway と通信するための jar ファイル。	この jar は、OIM サーバーの起動時に読み込まれます。
config\	コネクタの構成ファイル。	
lib\	OIMConnector11.1.2.0.0.jar を使用するための JAR ファイル。	thirdparty/endorsed ディレクトリ
docs\	各種システムの構成に関するユーザー・ガイドおよびテスト・ドキュメント。	
XML\Adapters.xml	Oracle コネクタのアダプタを含む XML ファイル。事前構成されたワークフローに手動でタスクを作成する場合に、このアダプタを使用できます。	Oracle 関連タスクを手動で作成
XML\VGOconstants.xml	VGO 定数リソースおよび VGO 定数 IT リソースを作成する XML ファイル。	Oracle 関連タスクを手動で作成する場合に使用します。
XML\Resourceobjects.xml	サンプル AD サーバーおよび iPlanet リソース。	サンプル・ワークフローに使用
XML\ITresources.xml	VGO 定数、iPlanet および Active Directory (AD) サーバーを含むサンプル IT リソース・ファイル。	サンプル・ワークフローに使用します。
XML\ lookups.xml	ワークフロー用の参照ファイル。	サンプル・ワークフローに使用
XML\ Lookup_iplanet_1.xml XML\ Lookup_iplanet_2.xml	iPlanet ワークフロー用のファイル。	サンプル・ワークフローに使用します。
XML\ReconAdapters.xml	インポートするリコンシリエーション・アダプタ。	各種ワークフローのリコンシリエーション

OIMConnector11.1.2.0.0.jarの構成

OIMConnector11.1.2.0.0.jar は、この製品に付属しています。このファイルを構成するには、次の手順を実行します。

1. OIMConnector11.1.2.0.0.jar の com\passlogix\integration\provision\conf\apiclientconf\ PMClientConfiguration.properties の下にある構成ファイルで、Vgo PM 接続変数の値を指定します。
Vgo PM のユーザー名およびパスワードは、OIM から渡されます。
2. PMClientConfiguration.properties ファイルの javaCLI.serviceurl 変数に、<http://<Hostname>/v-GO PM Service/UP.asmx> を構成します。
<Hostname>を、Provisioning Gateway が動作する IIS サーバーのホストに置き換えます。
3. javaCLI.serviceclient 変数に、プロビジョニング・サービス・クライアントの名前を構成します。たとえば、javaCLI.serviceclient=Provisioning Agent とします。
4. 変数 CLASSLOADER_PROPERTY_FILENAME を更新して、classloader.properties ファイルの場所を構成します。たとえば、CLASSLOADER_PROPERTY_FILENAME=<location>/classloader.properties とします。
<location>は、classloader.properties ファイルの絶対パスです。

一般的なアプリケーション・サーバーのデプロイメント手順

WebLogic

手順 1: インストール要件の確認

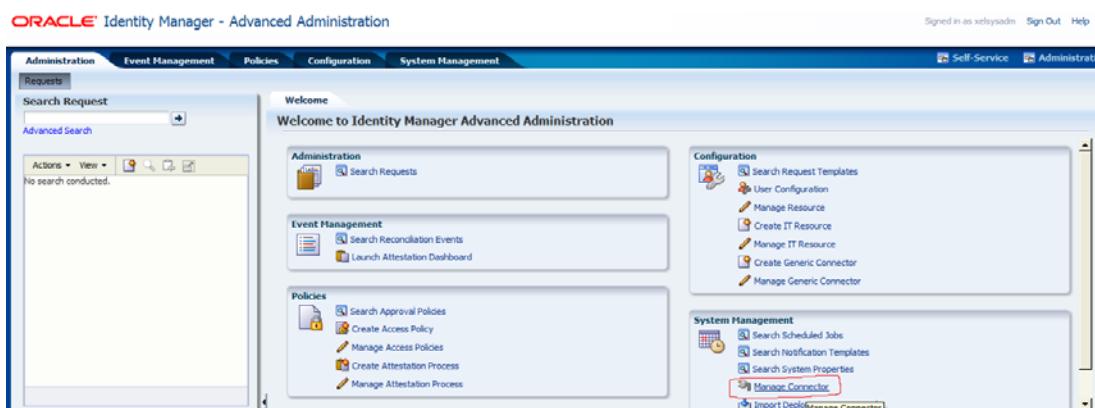
コンポーネント	要件
Oracle Identity Manager	OIM リリース 11.1.1.5 インストール、WebLogic Server
OIM インストールのホスト・プラットフォーム	Red Hat Linux バージョン 5.5

手順 2: Microsoft Active DirectoryおよびSun Java System Directory Server用のOIMサーバーの構成

1. OIM 内の Microsoft Active Directory Rev 4.4.0 および Sun Java System Directory Server Rev 4.1.0 用に Provisioning Gateway を構成して、Xellerate ユーザーをこれら 2 つのリソースにプロビジョニングできるようにします。パッケージには、テスト用の XML ファイルが含まれています。
2. 次のリンクを使用してアダプタをダウンロードします。
<http://www.oracle.com/technology/software/products/ias/htdocs/101202.html>

手順 3: OIMでのMicrosoft Active Directory Connectorのインストール

1. コネクタ・インストール・メディア・ディレクトリの内容を、ディレクトリ \$OIM_HOME/server/ConnectorDefaultDirectory にコピーします。
2. OIM Web コンソールにログオンします。「Welcome」ページで、「Advanced」をクリックします。
3. 「Advanced」ページで、「Manage Connector」を選択します。

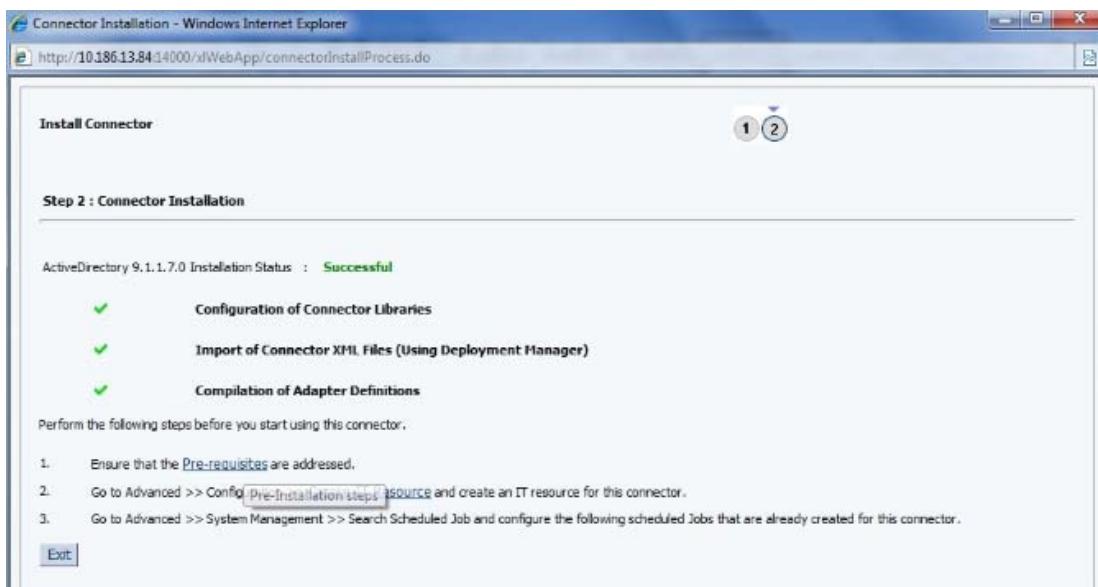


4. 「Connector Management」ページで、コネクタ名を入力または参照し、「Install」をクリックします。



5. 「Install Connector」ページで、ドロップダウン・リストから「ActiveDirectory 9.1.1.7.0」コネクタを選択し、「Continue」をクリックします。

6. インストールが完了すると、「Install Connector」ページの上部に「Active Directory Installation Status: Successful」というメッセージが表示されます。



7. 「Exit」をクリックします。

手順 4: OIMInterfaceコードおよびランタイム・ライブラリのコピー

1. OIMConnector11.1.2.0.0.jar を、OIM_HOME/server/JavaTasks にコピーします。
2. 次のバージョンのコネクタ・ランタイム・ライブラリを、OIM_HOME/server/ThirdParty にコピーします。

Jarの名前	Jarのバージョン
PMCLI.jar	-with 184 KB
axis.jar	1.2.1
bcprov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
jaxrpc.jar	-
opensaml-1.0.1.jar	1.0.1
Log4j-1.2.9.jar	1.2.9
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0

OIM 9i Connectorへのアップグレード

コネクタ・ファイルおよびディレクトリ

次の表に、OIM 9i Connector にアップグレードするファイルおよびディレクトリを示します。

内容	目的	コメント
XML\UpgradeInstall\Adapters.xml	既存のインストールからアップグレードする 注意: 新しいワークフローの構成には、この	Oracle 関連タスクを手動で作
docs\	各種システムの構成に関するユーザー・ガイド、およびテスト・ドキュメント。	

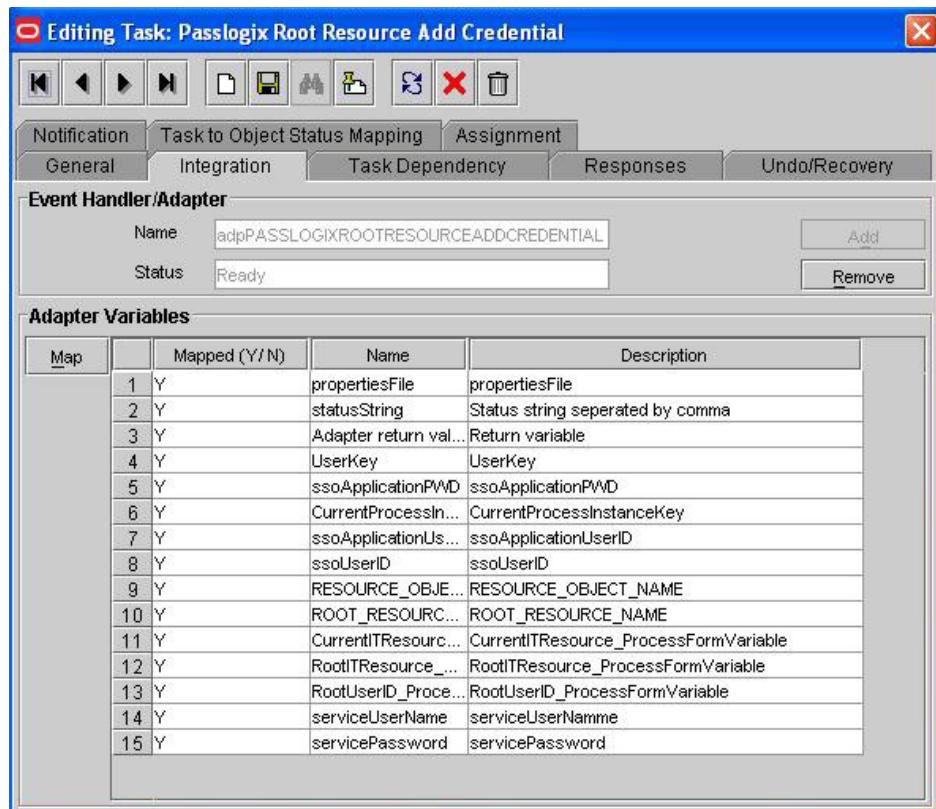
UpgradeInstall\Adapters.xml には、次のアダプタが変更され、含まれています。

- Passlogix Modify Password。
- Passlogix Reconciliation Add Credential。
- Passlogix Non Root Resource Add Credential。
- Passlogix Non Root Resource Delete Credential。
- Passlogix Root Resource Add Credential。

変数 vgoEnabledResources は、このリストのすべてのアダプタから削除されています。これらのアダプタは、リソースが VgoEnabled であるかどうかを指定しなくともワークフローで使用できます。

既存のインストールからアップグレードするには、UpgradeInstall\Adapters.xml を OIM にインポートします。以前のアダプタおよびそのワークフロー・マッピングは引き続き機能しますが、新しいワークフローの構成にはアップグレード済のアダプタを使用してください。

次の図は、Passlogix Root Resource Add Credential アダプタのマッピングです。Vgo Enabled Resources 変数のマッピングが、このアダプタから削除されている点に注目してください。



- ルート・リソースおよび非ルート・リソースに対して新しいワークフローを構成する手順については、「[既存プロセスのワークフローの構成](#)」を参照してください。
- アップグレード済のアダプタ内のマッピングについては、既存の VGO PM 定数リソースの値を使用してください。
- 「test.jar not found」(SF8617)エラーの解決方法については、「[付録](#)」を参照してください。

OIM 9i Connector の初期インストール

次の手順で、OIM 9i Connector の初期インストールについて説明します。

コネクタ・ファイルおよびディレクトリ

次の表に、OIM 9i Connector の初期インストールのファイルおよびディレクトリを示します。

内容	目的	コメント
bin\ OIMConnector11.1.2.0.0.jar	OIM が Provisioning Gateway と通信するための jar ファイル。	この jar を、OIM サーバー上の lib\endorsed\jars\rt に配置します。
config\	OIM コネクタの構成ファイル。	
lib\	OIM Connector 7.0.jar を使用するためのライブラリ。	thirdparty/endorsed ディレクトリ
docs\	各種システムの構成に関するユーザー・ガイド、およびテスト・ドキュメント。	
XML\ Adapters.xml	Oracle コネクタのアダプタを含む XML ファイル。	Oracle 関連タスクを手動で作成
XML\VGOconstants.xml	Provisioning Gateway 定数リソースおよび Provisioning Gateway 定数 IT リソースを作成する XML ファイル。	Oracle 関連タスクを手動で作成する場合に使用します。
XML\ Resourceobjects.xml	サンプル AD および iPlanet サーバーの事例。	サンプル・ワークフローに使用
XML\ ITresources.xml	Provisioning Gateway 定数、iPlanet および AD サーバーを含むサンプル IT リソース・ファイル。	サンプル・ワークフローに使用します。
XML\ lookups.xml	ワークフロー用の参照ファイル。	サンプル・ワークフローに使用
XML\ Lookup_iplanet_1.xml XML\ Lookup_iplanet_2.xml	iPlanet ワークフロー用のファイル。	サンプル・ワークフローに使用します。
XML\ReconAdapters.xml	インポートするリコンシリエーション・アダプタを含む XML ファイル。	各種ワークフローのリコンシリエーション

OIMConnector11.1.2.0.0.jarの構成

OIMConnector11.1.2.0.0.jar を構成するには、次の手順を実行します。

1. PMClientConfiguration.properties で、 Provisioning Gateway 接続変数の値を指定します。
2. PMClientConfiguration.properties ファイルの javaCLI.serviceurl 変数に、 `http://<Hostname>/v-GO PM Service/UP.asmx` を構成します。
3. `<Hostname>`を、 Provisioning Gateway アプリケーションが動作する IIS サーバーのホストに置き換えます。複数の URL をカンマで区切って入力できます。最初の試行に失敗すると、コネクタは各 URL をその入力順に使用して接続を試みます。このプロパティ・ファイルは、すべてのアダプタでパラメータとして使用されるため、 OIM サーバーが動作するマシンに存在する必要があります、その正確なパスがパラメータとして渡される必要があります。各アダプタの変数については、このドキュメントで説明されています。
4. javaCLI.serviceclient 変数に、 プロビジョニング・サービス・クライアントの名前を構成します。たとえば、 `javaCLI.serviceclient=Provisioning Agent` とします。
5. 変数 CLASSLOADER_PROPERTY_FILENAME を更新して、 classloader.properties ファイルの場所を構成します。たとえば、 `CLASSLOADER_PROPERTY_FILENAME=<location>/classloader.properties` とします (`<location>`は classloader.properties ファイルの絶対パスです)。

各種アプリケーション・サーバーのデプロイメント手順

WebLogic

手順 1: インストール要件の確認

コンポーネント	要件
Oracle Identity Manager	Oracle Identity Manager v 9i インストール、WebLogic Server 10.3、JDK 1.6.0_20 (JRE)
OIM インストールのホスト・プラットフォーム	Red Hat Linux バージョン 5.5

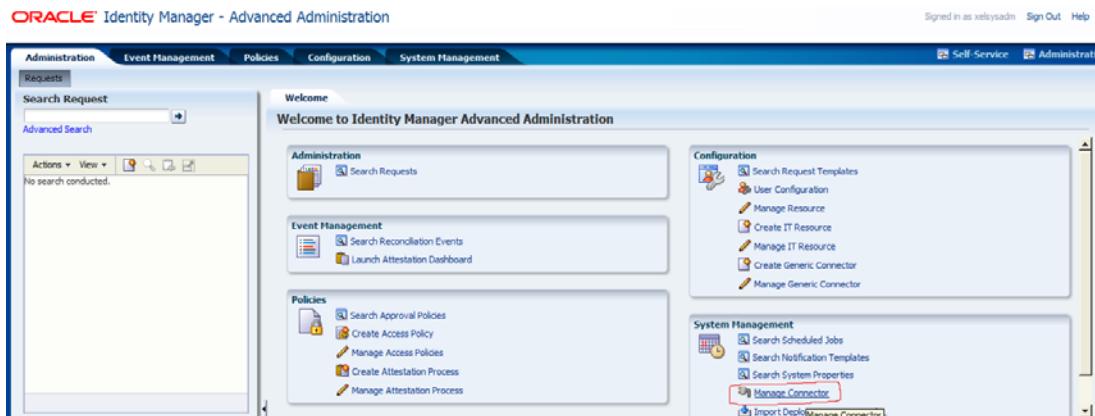
手順 2: Microsoft Active DirectoryおよびSun Java System Directory Server用のOIMサーバーの構成

1. OIM 内の Microsoft Active Directory Rev 4.4.0 および Sun Java System Directory Server Rev 4.1.0 用に Provisioning Gateway を構成して、Xellerate ユーザーをこれら 2 つのリソースにプロビジョニングできるようにします。パッケージには、テスト用の XML ファイルが含まれています。
2. 次のリンクを使用してアダプタをダウンロードします。

<http://www.oracle.com/technology/software/products/ias/htdocs/101202.html>

手順 3: OIMでのMicrosoft Active Directory Connectorのインストール

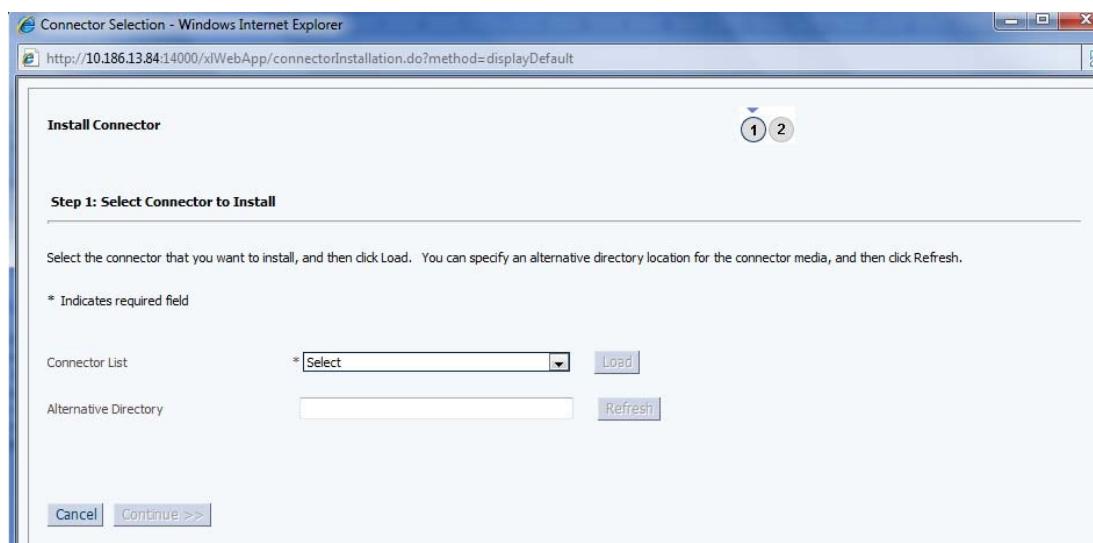
1. コネクタ・インストール・メディア・ディレクトリの内容を、ディレクトリ \$OIM_HOME/server/ConnectorDefaultDirectory にコピーします。
2. OIM Web コンソールにログオンします。「Welcome」ページで、「Advanced」をクリックします。
3. 「Advanced」ページで、「Manage Connector」を選択します。



4. 「Connector Management」ページで、「Install」をクリックします。



5. 「Install Connector」ページで、ドロップダウン・リストから AD コネクタを選択し、「Continue」をクリックします。



Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh.

* Indicates required field

Connector List * ActiveDirectory 9.1.1.7.0 Load

Alternative Directory Refresh

Connector History Details

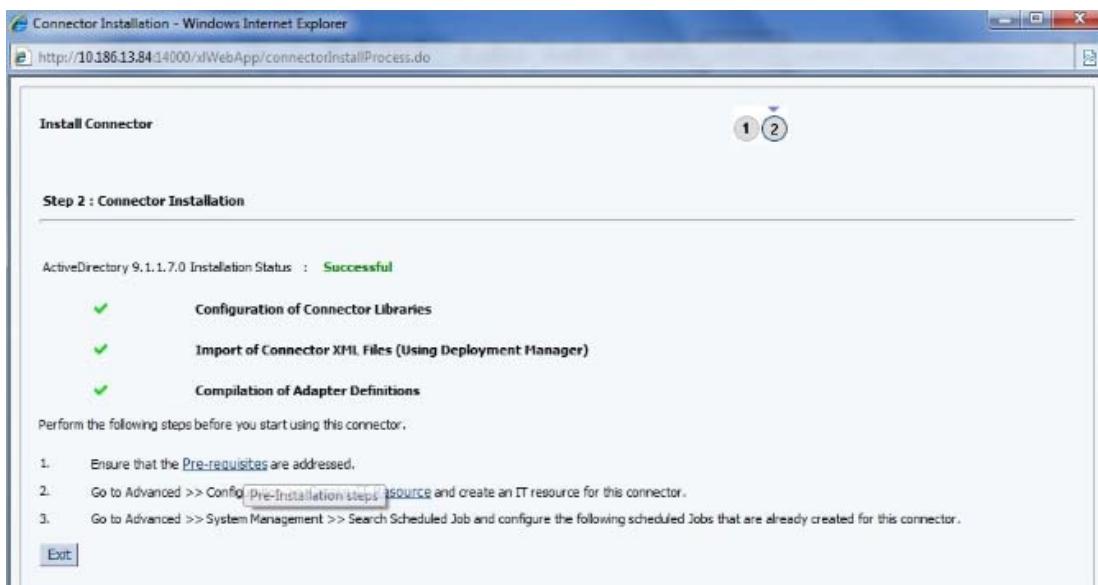
The ActiveDirectory 9.1.1.7.0 connector has no history of prior installations.

Connector Dependency Details

The ActiveDirectory 9.1.1.7.0 connector has no dependencies on other connectors.

Cancel Continue >>

インストールが完了すると、「Install Connector」ページの上部に「Active Directory Installation Status: Successful」というメッセージが表示されます。



6. 「Exit」をクリックします。

手順 4: OIMインターフェース・コードおよびランタイム・ライブラリのコピー

1. OIMConnector11.1.2.0.0.jar を、OIM_HOME/server/JavaTasks にコピーします。
2. 次のバージョンのコネクタ・ランタイム・ライブラリを、OIM_HOME/server/ThirdParty にコピーします。

Jarの名前	Jarのバージョン
PMCLI.jar	-with 184 KB
axis.jar	1.2.1
bcprov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
jaxrpc.jar	-
opensaml-1.0.1.jar	1.0.1
Log4j-1.2.9.jar	1.2.9
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0

3. BEA WebLogic 8.1 の JRE で、次のものを endorsed ディレクトリとして設定します。

Jarの名前	Jarのバージョン
dom.jar	Xerces-J_2_5_0
jaxp-api.jar	1.3
sax.jar	Xerces-J_2_5_0
xalan.jar	2.1.4
xercesImpl.jar	Xerces-J_2_5_0

4. WebLogic で、Kellerate 用の endorsed ライブラリをインストールします。

- a. WebLogic サーバーを停止します。
- b. WebLogic が lib ディレクトリで使用している JRE に endorsed フォルダを作成し、endorsed 表のライブラリをコピーします。(これは、特に JRE 1.4 で必要になります)。

JBoss

手順 1: インストール要件の確認

コンポーネント	要件
Oracle Identity Manager	Oracle リリース 9.0.1.1849.0 次の製品とともにインストールします。 JBoss-4.0.3SP1 および JDK 1.4.2
OIM インストールのホスト・プラットフォーム	Windows Server 2003

手順 2: Microsoft Active Directory および Sun Java System Directory Server 用の OIM サーバーの構成

1. OIM 内の Microsoft Active Directory Rev 4.4.0 および Sun Java System Directory Server Rev 4.1.0 用に Provisioning Gateway を構成して、Xellerate ユーザーをこれら 2 つのリソースにプロビジョニングできるようにします。パッケージには、テスト用の XML ファイルが含まれています。
2. 次のリンクを使用してアダプタをダウンロードします。
<http://www.oracle.com/technology/software/products/ias/htdocs/101202.html>
3. OIM インタフェース・コードおよびランタイム・ライブラリをコピーします。
 - a. OIMConnector11.1.2.0.0.jar を、xellerate_home\xellerate\JavaTasks にコピーします。
 - b. 次のバージョンのコネクタ・ランタイム・ライブラリを、xellerate_home\xellerate\ThirdParty にコピーします。

Jar の名前	Jar のバージョン
PMCLI.jar	-
axis.jar	1.2.1
bcpprov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
commons-logging-1.0.4.jar	1.0.4
jaxrpc.jar	-
log4j-1.2.9.jar	1.2.9
opensaml-1.0.1.jar	1.0.1
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0

次のものが *jboss-4.0.3SP1\lib\endorsed* にコピーされます。

Jarの名前	Jarのバージョン
dom.jar	Xerces-J_2_5_0
jaxp-api.jar	1.3
sax.jar	Xerces-J_2_5_0
xalan.jar	2.1.4
xercesImpl.jar	Xerces-J_2_5_0

手順 3: JBossでのXellerateのXMLライブラリのインストール

- JBoss サーバーを停止し、ライブラリを *jboss-4.0.3SP1\lib\endorsed* ディレクトリにコピーします。
- プロンプトが表示されたら古いライブラリを置き換え、JBoss サーバーを再起動します。
注意: OIM バージョン 9.1.0.1、JBoss バージョン 4.2.3.GA および JDK 1.6 については、*commons-logging-1.0.4.jar* 以外のすべての OIM サードパーティ jar を、JBoss の *run.bat* ファイルの *JBOSS_CLASSPATH* 変数に追加する必要があります。 *JBOSS_HOME/server/default/lib* ディレクトリに存在する *common-logging.jar* は、*JBOSS_CLASSPATH* に追加する必要があります。

サードパーティ jar を *JBOSS_CLASSPATH* に追加する例を、次に示します。

```
set OIM_THIRD_PARTY=OIM_HOME\ThirdParty set
OIM_THIRD_PARTY_JARS=%OIM_THIRD_PARTY%\PMCLI.jar;%OIM_THIRD_PARTY%\
```

```
PasslogixConnector.jar;%OIM_THIRD_PARTY%\Axis-1.2.1.jar;
```

```
%OIM_THIRD_PARTY%\bcprov-jdk13-128.jar;%OIM_THIRD_PARTY%
```

```
\commons-discovery-0.2.jar;
```

```
%OIM_THIRD_PARTY%\commons-logging-1.0.4.jar;
```

```
%OIM_THIRD_PARTY%\jaxrpc.jar;%OIM_THIRD_PARTY%\opensaml-1.0.4.jar;
```

```
%OIM_THIRD_PARTY%\wss4j.jar;%OIM_THIRD_PARTY%
```

```
\com.oracle.ws.orawsdl_1.2.0.0.jar;
```

```
%OIM_THIRD_PARTY%\xmlsec-1.3.0.jar;
```

```
if "%JBOSS_CLASSPATH%" == "" set RUN_CLASSPATH=%RUNJAR%;%OIM_THIRD_PARTY_JARS%
```

```
if "%RUN_CLASSPATH%" == "" set
```

```
RUN_CLASSPATH=%JBOSS_CLASSPATH%;%RUNJAR%;%OIM_THIRD_PARTY_JARS%
```

```
%
```

OIM_HOME は、OIM サーバーのインストール・ディレクトリです。

JBOSS_HOME は、JBoss のインストール・ディレクトリです。

OC4J

手順 1: インストール要件の確認

コンポーネント	要件
Oracle Identity Manager	OIM リリース 9.0.3 インストールおよび Oracle Containers for J2EE
OIM インストールのホスト・プラットフォーム	Windows Server 2003

手順 2: Microsoft Active DirectoryおよびSun Java System Directory Server用のOracle Identity Managerサーバーの構成

- Microsoft Active Directory Rev 4.4.0 および Sun Java System Directory Server Rev 4.1.0 用のプロジェクト・アダプタを OIM で構成し、Xellerate ユーザーをこれら 2 つのリソースにプロジェクト・マッピングできるようにします。手順 6 では、テスト用のパッケージにも XML が含まれています。
- 次のリンクを使用してアダプタをダウンロードします。
<http://www.oracle.com/technology/software/products/ias/htdocs/101202.html>

手順 3: OIMインターフェース・コードおよびランタイム・ライブラリのコピー

- OIMConnector11.1.2.0.0.jar を、xellerate_home\xellerate\JavaTasks の下にコピーします。
- 次のバージョンのコネクタ・ランタイム・ライブラリを、xellerate_home\xellerate\ThirdParty にコピーします。

Jarの名前	Jarのバージョン
PMCLI.jar	-
axis.jar	1.2.1
axis-ant-1.2.1.jar	1.2.1
bcprov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
jaxrpc.jar	-
opensaml-1.0.1.jar	1.0.1
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0

次のものが OC4J で共有ライブラリとして設定されます。

Jarの名前	Jarのバージョン
dom.jar	Xerces-J_2_5_0
jaxp-api.jar	1.3
sax.jar	Xerces-J_2_5_0
xalan.jar	2.1.4
xercesImpl.jar	Xerces-J_2_5_0

3. Oracle Process Manager から Oracle サーバーを停止します。
4. *(oc4j_home)\webservices\lib\commons-logging.jar* を削除します。

注意: これは、OIM Xellerate ロギング・ライブラリでのログ構成に関する問題を回避するために必要です。

5. OC4J で、Xellerate の共有ライブラリをインストールします。
 - a. ファイル`(oc4j_home)\j2ee\home\config\server.xml`を開きます。
 - b. `Oc4j_home` は、OC4J をインストール済のディレクトリを示します。
 - c. `passlogix` という名前の共有ライブラリのエントリを、前のエントリの直後に追加します。

共有ライブラリのエントリを次に示します。

```
<shared-library name="passlogix" version="1.1">
  1. <code-source path="xercesImpl.jar"/>
  <code-source path="xalan.jar"/>
  <code-source path="sax.jar"/>
  <code-source path="jaxp-api.jar"/>
  <code-source path="dom.jar"/>
</shared-library>
```

6. `server.xml` を保存します。これが、アプリケーションで使用される共有ライブラリです。
 - a. `passlogix` という名前のディレクトリを、`(oc4j_home)\j2ee\home\shared-lib` に作成します。
 - b. 1.1 という名前のディレクトリを作成します(この名前はライブラリのバージョンを定義します)。
 - c. 指定されたすべての jar を、このディレクトリに格納します。
 - d. ファイル`(oc4j_home)\j2ee\home\application-deployments\Xellerate\orion-application.xml`を開きます。

このファイルは、作成した共有ライブラリに Xellerate アプリケーションを割り当てます。

- e. 次のエントリを、ファイル末尾の`</orion-application>` タグの前に追加します。

```
<imported-shared-libraries>
  <import-shared-library name="passlogix" max-version="1.3"/>
</imported-shared-libraries>
```

- f. ファイルを保存します。

`max-version` は、Xellerate で使用する最上位のバージョンである必要があります。この場合は、1.1 より大きい必要があります。OC4J サーバーを起動します。

これまでの手順は、OC4J で OIMConnector11.1.2.0.0.jar を動作させるために必要です。以降の手順では、ワークフローXML ファイルを作成するか、OIM にインポートし、コネクタをテストする方法を示します。

WebSphere

手順 1: インストール要件の確認

コンポーネント	要件
Oracle Identity Manager	Oracle Identity Manager v. 9.0.1 インストールおよび WebSphere v. 5.1.1.5 Oracle9i v 9.2.0.1.0
OIM インストールのホスト・プラットフォーム	Windows Server 2003

手順 2: Microsoft Active Directory および Sun Java System Directory Server 用の OIM サーバーの構成

1. OIM 内の Microsoft Active Directory Rev 4.4.0 および Sun Java System Directory Server Rev 4.1.0 用に Provisioning Gateway を構成して、Xellerate ユーザーをこれら 2 つのリソースにプロビジョニングできるようにします。
2. 次のリンクを使用してアダプタをダウンロードします。
<http://www.oracle.com/technology/software/products/ias/htdocs/101202.html>

手順 3: OIM インタフェース・コードおよびランタイム・ライブラリのコピー

1. OIMConnector11.1.2.0.0.jar を、xellerate_home\xellerate\JavaTasks にコピーします。
2. 次のバージョンのコネクタ・ランタイム・ライブラリを、xellerate_home\xellerate\ThirdParty にコピーします。

Jar の名前	Jar のバージョン
PMCLI.jar	-
axis.jar	1.2.1
axis-ant-1.2.1.jar	1.2.1
bcpov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
commons-logging-1.0.4.jar	1.0.4
jaxrpc.jar	-
log4j-1.2.9.jar	1.2.9

Jarの名前	Jarのバージョン
opensaml-1.0.1.jar	1.0.1
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0

3. IBM WebSphere 5.1.1.5 の共有ライブラリの下にある次のバージョンのコネクタ・ランタイム・ライブラリを参照します。

Jarの名前	Jarのバージョン
dom.jar	Xerces-J_2_5_0
jaxp-api.jar	1.3
sax.jar	Xerces- J_2_5_0
xalan.jar	2.1.4
xercesImpl.jar	Xerces- J_2_5_0

4. WebSphere サーバーを再起動します。

SSO 作業タスクの手動構成例

AD ユーザーは、構成したワークフローでルート・リソース・オブジェクトとして機能します。ルート・リソースには、SSO リポジトリ・データが含まれます。このユーザーがルート・リソースに存在しないと、他のアプリケーション資格証明を Provisioning Gateway Server に登録することはできません。他の任意のリソース・オブジェクト(iPlanet など)または IT リソース(AD サーバー1、iPlanet ユーザーなど)は、非ルート・リソース・オブジェクトおよび非ルート IT リソースとしてそれぞれ分類されます。

Create User、Password Updated または Delete User タスクにすでに構成されている任意のルートまたは非ルート・リソース・オブジェクト・プロセス定義に対して、対応するタスク(Oracle Add Credential、Oracle Change Password または Oracle Delete User)をそれぞれのレスポンス・コードで追加し、マップします。Oracle に対して追加する新規タスクは、対応するワークフロー変数(プロセス・フォーム)に適切に構成されます。Oracle タスクは、事前構成されたワークフロー・タスクの完了に条件付きで基づきます。この項では、AD(ルート)および iPlanet(非ルート)リソースにすでに構成されているワークフローへの Oracle タスクの追加について説明します。

ルートおよび非ルート・リソース・オブジェクトのプロセス・タスクのアタプタは、異なる方法で構成されます。ルート・リソースのプロビジョニングについては、Provisioning Gateway Server に対して Add Credential、Change Password または Delete Credential メソッドがトリガーされる前にチェックが行われます。

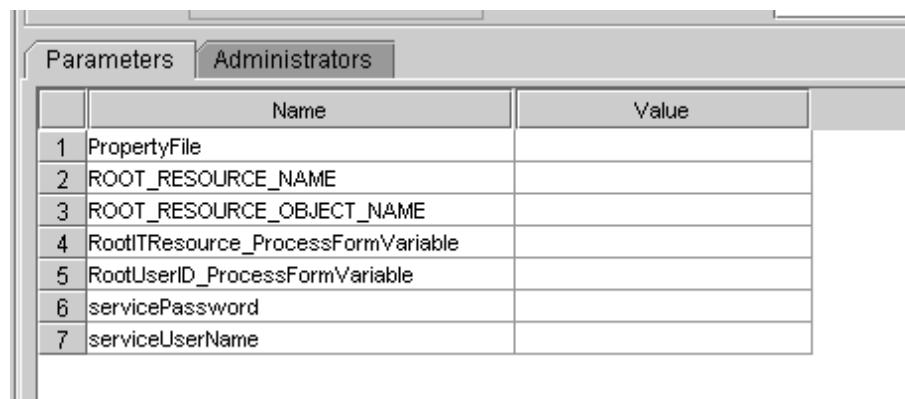
Provisioning Gateway定数の定義

Provisioning	フィールドの値	目的
1	ROOT_RESOURCE_NAME	これは、AD サーバーへの接続に使用される IT リソース名を示しています。この名前は、コネクタによって Provisioning Gateway Server に送信されます。つまり、Provisioning Gateway はこのフィールド値を含むテンプレート名を持つ必要があります。これは、Logon Manager のリポジトリにもなります。
2	ROOT_RESOURCE_OBJECT_NAME	AD サーバーのプロセス定義内に存在するリソース・オブジェクト名。
3	RootITResource_ProcessFormVariable	AD ユーザー・プロセス・フォーム上の変数
4	RootUserID_ProcessFormVariable	特定のユーザーの SSO ID として使用される UID フィールド。この値は、コネクタが資格証明手順を Provisioning Gateway に送信すると、SSO ID として使用されます。

Provisioning Gateway 定数リソース の作成	フィールドの値	目的
6	serviceUserName	Oracle Enterprise Single Sign-On Administrative
7	servicePassword	serviceUserName アカウントのパスワード。このフィールドは、バックエンド・データベースで暗号化されます。
8	Propertyfile	コネクタ・パックの初期化パラメータを持つ変数。サービス URL およびサービス・エージェント名の値を持ちます。複数の URL をカンマで区切って指定できます。これらは、OIM サーバーが動作するマシン上に存在するプロパティ・ファイルの正確なパスである必要があります。

- 「IT Resources Information」定義フォームを開き、次のパラメータで VGO PM 定数リソースを作成します。

リソース	値
ROOT_RESOURCE_NAME	
ROOT_RESOURCE_OBJECT_NAME	
RootITResource_ProcessFormVariable	
RootUserID_ProcessFormVariable	
serviceUserName	暗号化される
servicePassword	暗号化される
Propertyfile	



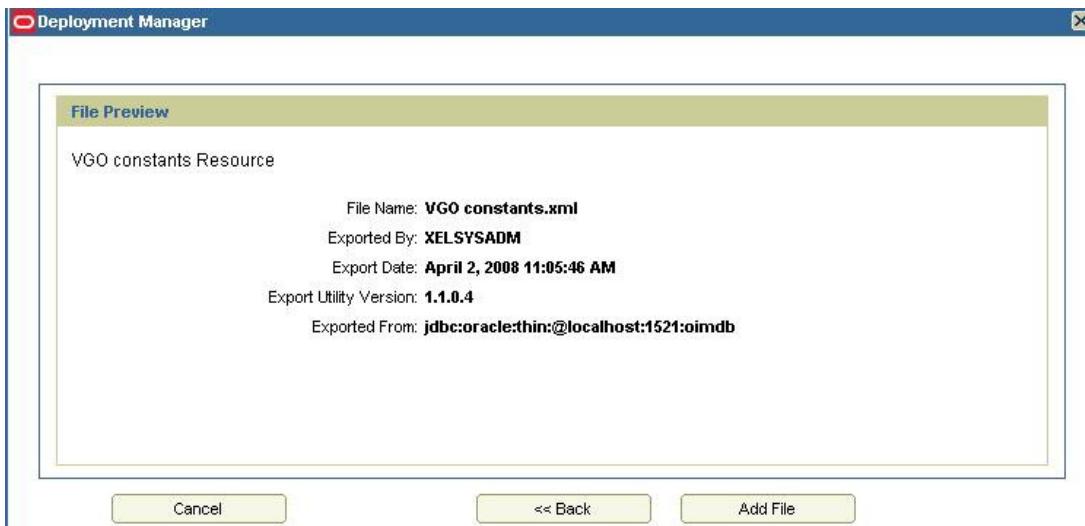
2. VGO PM 定数リソース・タイプの IT リソース VGO PM 定数を作成し、実装された実際のワークフローに依存する値を入力します。

次の表に、ワークフローの値の例を示します。

リソース	値
ROOT_RESOURCE_NAME	AD Server 2003
ROOT_RESOURCE_OBJECT_NAME	AD User
RootITResource_ProcessFormVariable	UD_ADUSER_AD
RootUserID_ProcessFormVariable	UD_ADUSER_UID
serviceUserName	Provisioning Gateway インストールのとおり
servicePassword	Provisioning Gateway インストールのとおり
プロパティ・ファイル	

次の手順を実行すると、パッケージで提供されている XML ファイルを使用して同じ結果を得ることができます。

1. Web インタフェースのインポート機能を使用して、*VGOconstants.xml* ファイルを OIM にインポートします。



2. このインスタンスはすでに存在するため、オプションで「Skip」をクリックして、新しいインスタンスを作成します。*VGOconstants* リソースが、OIM に追加されます。

「AD User」プロセス・フォームのProvisioning Gateway定数リソース型フィールドの定義

プロビジョニング中、Oracle コネクタは Provisioning Gateway の接続パラメータを必要とします。このプロセス・フォームを持つすべてのワークフローに対して、この手順を実行します。

この例では、AD プロセス・フォーム(ルート・リソース)および iPlanet (非ルート・リソース)を使用します。このフォームの可視性を構成できます。可視化して、Logon Manager の複数のインスタンスをデプロイするための参照を定義します。複数インスタンス構成の場合、IT リソース値は異なります。

1. 「AD User」プロセス・フォームを開きます。
2. 新しいバージョンの新規 AD ユーザー・フォームを作成します。
3. 新しいフィールド *VGOADConstants* を追加します。

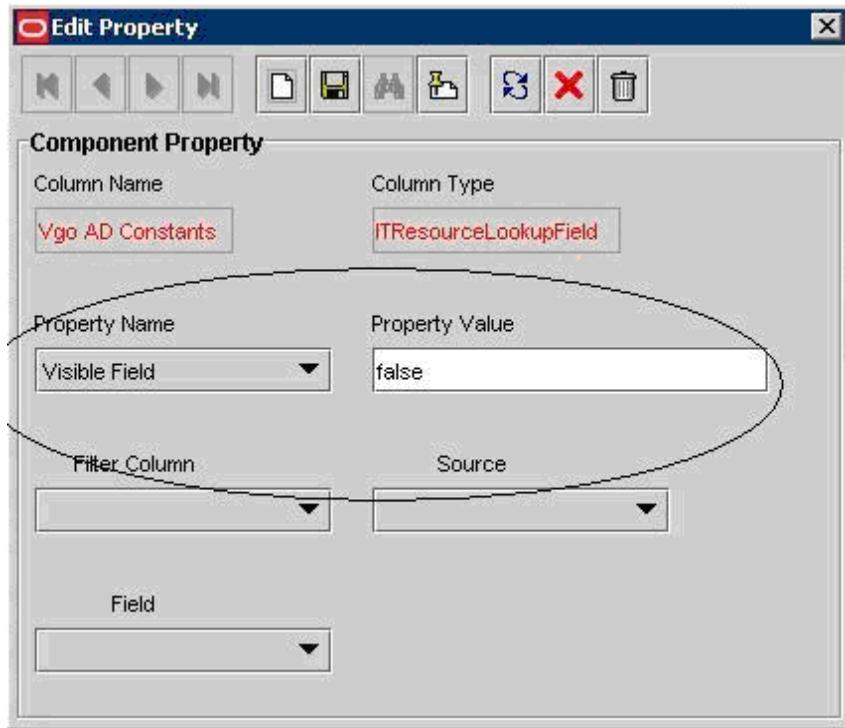
名前	変数型	長さ	フィールド・ラベル	フィールド型	デフォルト値
<i>VGOADConstants#</i>	Long		<i>VGOADConstants</i>	ITResourceLookUpField	<i>VGO PM 定数*</i>

*前に定義した IT リソース名 *VGO PM 定数*を入力します。

#*VGOADCONSTANTS* の前に *UD_ADUSER_*が付きます。

- a. 「Properties」タブで、*VGOADConstants* のプロパティを追加します。
- b. 「Add Property」ウインドウで、「Property Name」から「Type」項目を選択します。

4. 「Property Value」ボックスから「VGO PM Constant Resource」を選択します。
 - a. もう 1 つのプロパティを追加して、「Property Name」から「Visible Field」項目を選択します。「Property Value」ボックスに、false と入力します。
5. 新規 AD ユーザー・フォームをアクティブにします。



「iPlanet User」プロセス・フォームのProvisioning Gateway定数リソース型フィールドの定義

1. 「iPlanet User」プロセス・フォームを開きます。
2. 新しいバージョンを作成し、New IPNT User という名前を付けます。

Object Permissions Properties Administrators Usage Pre-Populate Default Columns User Defined Fields									Child Table(s)	
Additional Columns										
Add		Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Pr	
	1	UD_IPNT_USR_VGOIPNTCONSTANTS	long		Vgo IPNT Constants	ITResourceLookupField	VGO PM Constants	14		
Delete	2	UD_IPNT_USR_USERID	String	50	User ID	TextField		1		
	3	UD_IPNT_USR_PASSWORD	String	15	Password	PasswordField		2		
	4	UD_IPNT_USR_TITLE	String	30	Title	ComboBox	Mr.	3		
	5	UD_IPNT_USR_FIRST_NAME	String	40	First Name	TextField		4		
	6	UD_IPNT_USR_MIDDLE_INITIAL	String	8	Middle Name	TextField		5		
	7	UD_IPNT_USR_LAST_NAME	String	40	Last Name	TextField		6		
	8	UD_IPNT_USR_ORGANIZATION	String	400	Organization DN	LookupField	ou=People	7		
	9	UD_IPNT_USR_DEPARTMENT	String	100	Department	LookupField	Department1	8		
	10	UD_IPNT_USR_LOCATION	String	100	Location	LookupField	Bangalore	9		
	11	UD_IPNT_USR_TELEPHONE	String	20	Telephone	TextField		10		
	12	UD_IPNT_USR_EMAIL	String	245	Email	TextField		11		
	13	UD_IPNT_USR_COMM_LANG	String	50	Communication Lang	ComboBox	English	12		
	14	UD_IPNT_USR_SERVER	long		Server	ITResourceLookupField	iPlanet User	13		

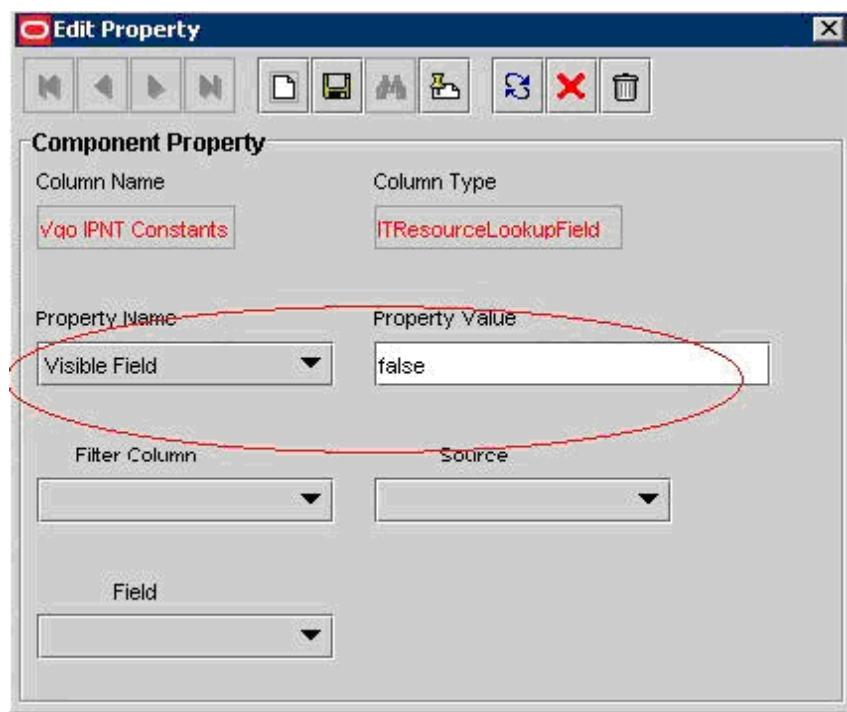
3. 新しいフィールド VGOIPNTConstants を追加します。実行時に、このフィールドは、VGOconstant 接続パラメータに対して事前入力済の VGO PM 定数データを提供します。

名前	変数型	長さ	フィールド・ラベル	フィールド型	デフォルト値
VGOIPNTConstants#	Long		VgoIPNTConstants	ITResourceLookUpField	VGO PM 定数*

*前に定義した IT リソース名 VGO PM 定数を入力します。

4. 「Properties」タブで、VGOIPNTConstants のプロパティを追加します。

- 「Add Property」ウィンドウの「Property Name」フィールドで、「Type」を選択します。「Property Value」として「VGO PM Constant Resource」を選択します。
- 別のプロパティを追加して、「Property Name」リストから「Visible Field」を選択します。「Property Value」ボックスに、**false**と入力します。



5. 新しい IPNT ユーザー・フォームをアクティブにします。

既存プロセスのワークフローの構成

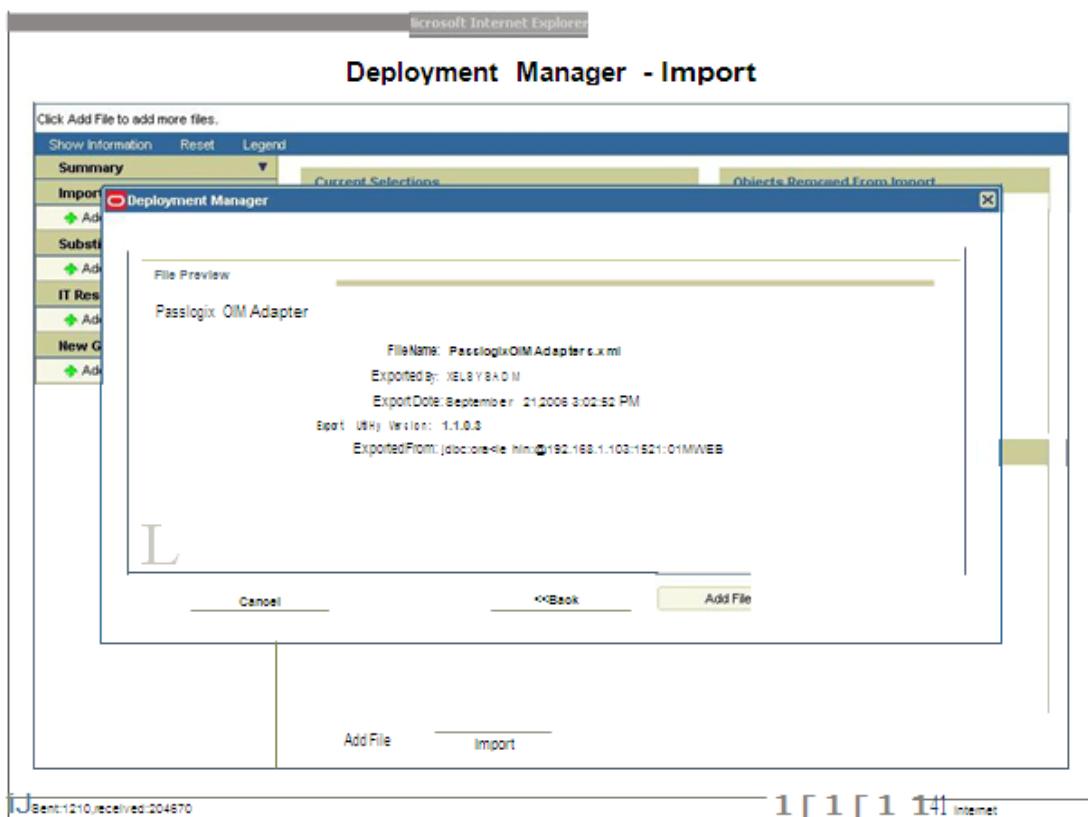
Oracle Adapterのインポート

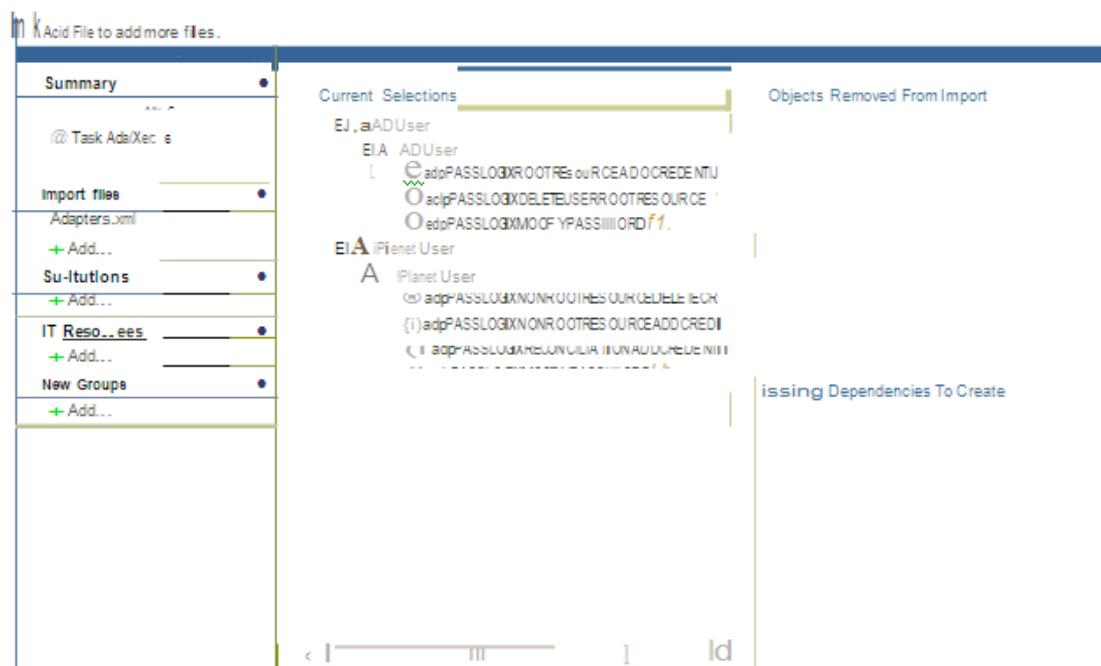
Adapters.xml ファイルには、任意の事前構成済ワークフローに使用できるアダプタが含まれています。このタスクは、必要なワークフロー(AD、iPlanet、ODB)のプロセス定義で作成できます。必要に応じて次のアダプタを追加します。

アダプタ名	目的
adpPASSLOGIXROOTRESOURCE ADD CREDENTIAL	<p>Logon Manager リポジトリに対して同じルート・リソースの資格証明を追加するために使用されるアダプタ。他のアプリケーションをユーザーに追加する前に、そのユーザーにルート・リソースをプロビジョニングする必要があります。</p> <p>次のように動作します。</p> <p>現在の AD がルート AD の場合、資格証明を直接追加します。</p> <p>実行時にそのユーザーにプロビジョニングされたリソースを確認します。</p> <p>プロビジョニングされたすべてのリソース・オブジェクトと、ワークフローのルート・リソースを対応付けます。</p> <p>ルート・リソースがプロビジョニングされると、ルート・リソースは Logon Manager に対して設定された UID を取得し、新しいアプリケーション資格証明を追加します。</p>
adpPASSLOGIXNONROOTRESOURCE ADD CREDENTIAL	<p>定義されたワークフローを持つリソースの資格証明を追加するために使用されるアダプタ。</p> <p>次のように動作します。</p> <p>ランタイム・ユーザーに対してプロビジョニングされたリソースを確認します。</p> <p>プロビジョニングされたすべてのリソース・オブジェクトをワークフローのルート・リソースと対応付け、存在する場合は続行し、存在しない場合は「Root resource not provisioned」というエラーをスローします。</p> <p>ルート・リソースがプロビジョニングされると、ルート・リソースは Logon Manager に対して設定された UID を取得し、新しいアプリケーション資格証明を追加します。</p>
adpPASSLOGIXDELETE USERROOTRESOURCE	ルート・リソースの資格証明を Oracle Provisioning Gateway Management Console から削除します。
adpPASSLOGIXNONROOTRESOURCE DELETE CREDENTIAL	非ルート・リソースの資格証明を Provisioning Gateway から削除します。

アダプタ名	目的
adpPASSLOGIXMODIFYPASSWORD	各種アプリケーションのパスワードを変更します。 次のように動作します。 ランタイム・ユーザーに対してプロビジョニングされたリソースを確認します。 そのユーザーにプロビジョニングされたすべてのリソース・オブジェクトをワークフローのルート・リソースと対応付け、存在する場合は続行し、存在しない場合は「Root resource not provisioned」というエラーをスローします。 資格証明の変更指示を Provisioning Gateway に送信します。
adpPASSLOGIXRECONCILIATION ADD CREDENTIAL	ユーザーに対してプロビジョニングされた新しいアプリケーションの資格証明を追加します。

1. *XmIAdapters.xml* をインポートします。Web インターフェースからデプロイメント・マネージャを使用します。
2. アダプタの名前がインポート・ウィンドウに表示されます。次の画面に表示されるすべてのアダプタをインポートします。インポートが完了すると、アダプタのリストがデザイン・コンソールの「Adapter Factory」表に表示されます。





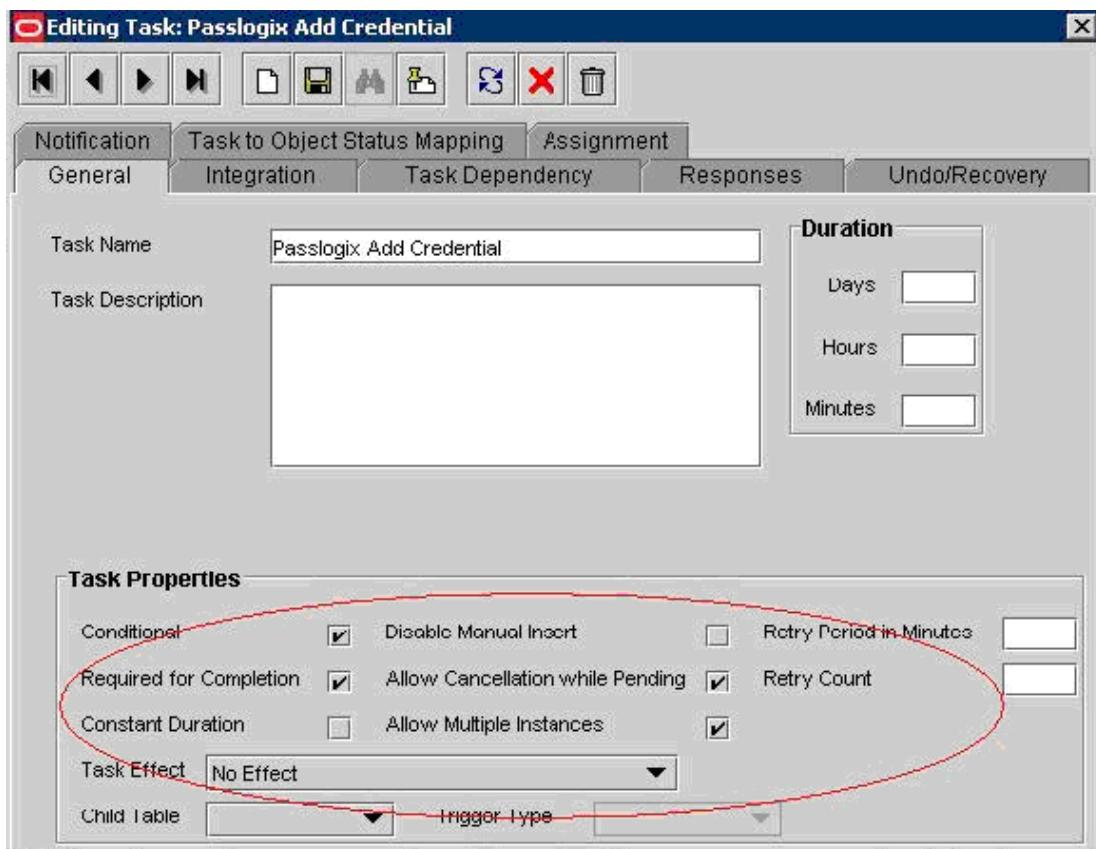
Passlogix Add Credential プロセス・タスクの作成

この項では、次の方について説明します。

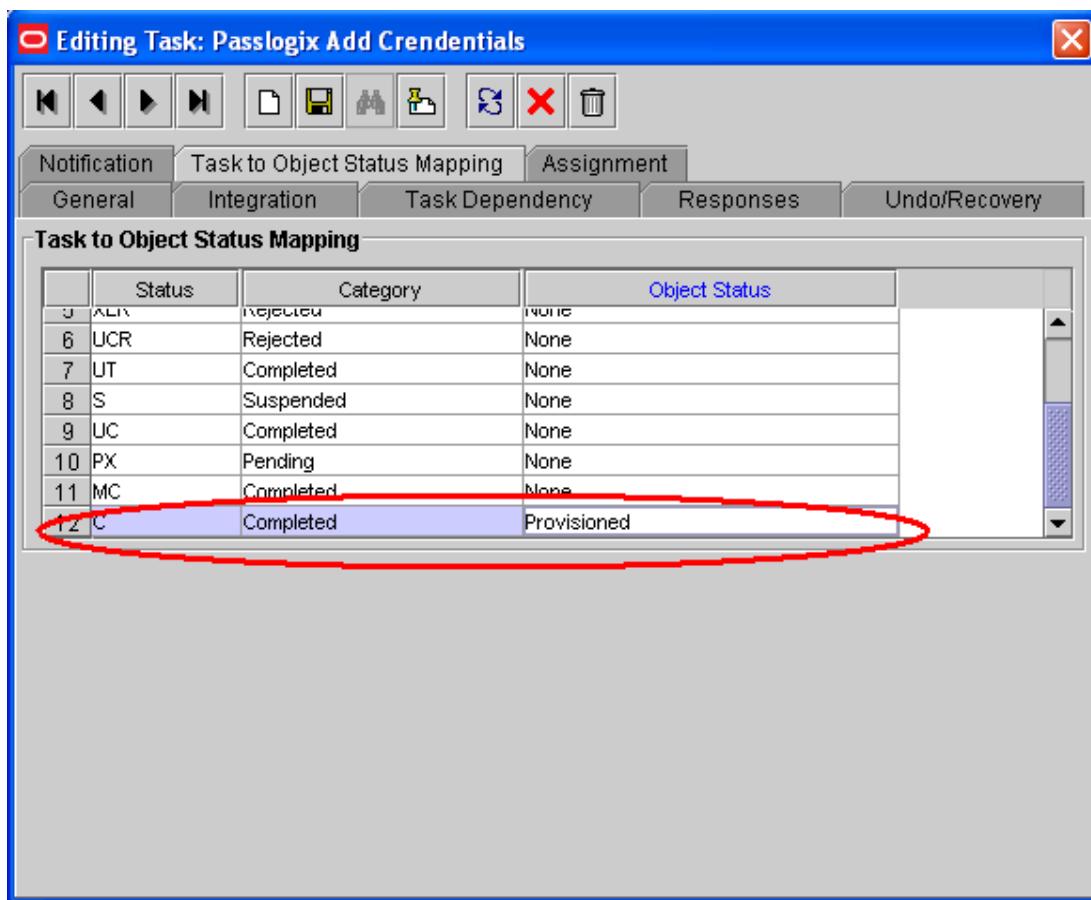
- Passlogix Add Credential プロセス・タスクを作成する。
- Passlogix Root Resource Add Credential アダプタをそれにアタッチする。
- アダプタ変数をマップする。

資格証明プロセス・タスクの追加

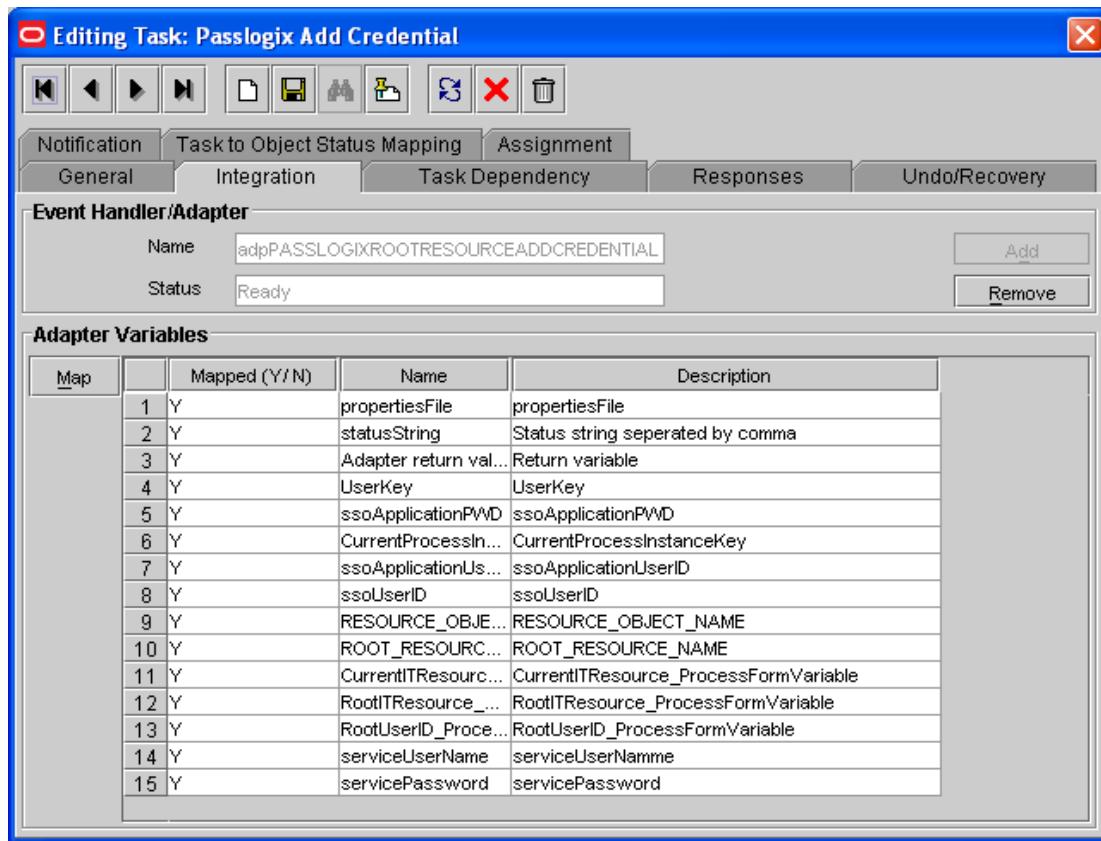
1. 作成、変更および削除などの基本的なユーザー操作に関してすでに構成されている「AD User」プロセス・フォームを開きます。この AD プロセスでは、Logon Manager と同じリポジトリを使用します。手動プロビジョニングの場合は、最初に AD でユーザーを作成し、次に Oracle Provisioning Gateway Management Console でユーザーを作成します。
2. **Passlogix Add Credential** タスクを追加します。
3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスが選択されていることを確認します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスとマップします。



5. 「Integration」タブで、**adpPasslogixRootResourceAddCredential**アダプタをこのタスクにアタッチし、変数を次の2つの画面に示すようにマップします。



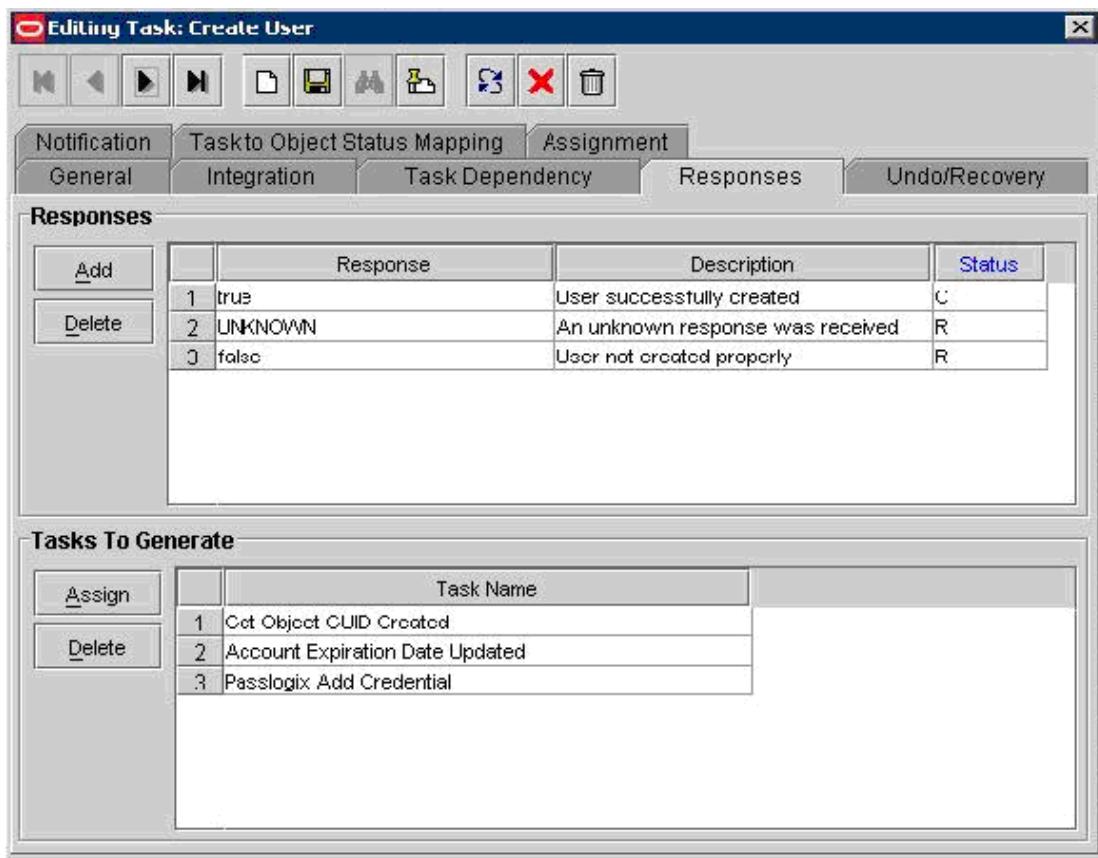
6. タスクの変数を、次の表に示すようにマップします。

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/ Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
User Key	long	User Definition	User Key	なし	
ssoUserID	String	Process Data	User Id	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcess InstanceKey	long	Process Data	Process Instance	なし	

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/ Literal Value	IT Asset Property
#CurrentITResource_Process FormVar	String	Literal	String	UD_ADUSER_AD	なし
Root_Resource_Name	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	Root_Resource_Name
Root_Resource_Object_Name	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	Root_Resource_Object_Name
RootITResource_ProcessFormVariable	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	RootITResource_ProcFormVar
RootUserID_ProcessFormVariable	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	RootUserID_ProcFormVar
serviceUserName	String	IT Resource	VGOADConst ants	VGO PM 定数リソース	serviceUser Name
servicePassword	String	IT Resource	VGOADConst ants	VGO PM 定数リソース	servicePassword
Propertyfile	String	Literal	String	PMClientConfigura tion. properties	
statusString		Literal		考慮するステータス値のカンマ区切りリスト (例: Provisioned, Disabled, Enabled)	

これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。

7. AD User の Create User プロセス・タスクの「Responses」タブで、true レスポンスを選択してハイライト表示します。次に、このタブの「Tasks to Generate」領域から、Passlogix Add Credential タスクを選択して割り当てます。これによって、AD ワークフローに対してユーザーが正常に作成された場合に Passlogix Add Credential が起動されるように構成されます。つまり、資格証明が Oracle コネクタに送信され、ユーザーは Provisioning Gateway レジストリに登録されます(同じ AD ルート・リソースです)。



8. 「Save」をクリックします。

Passlogix Change Passwordプロセス・タスクの作成

この項では、次の方針について説明します。

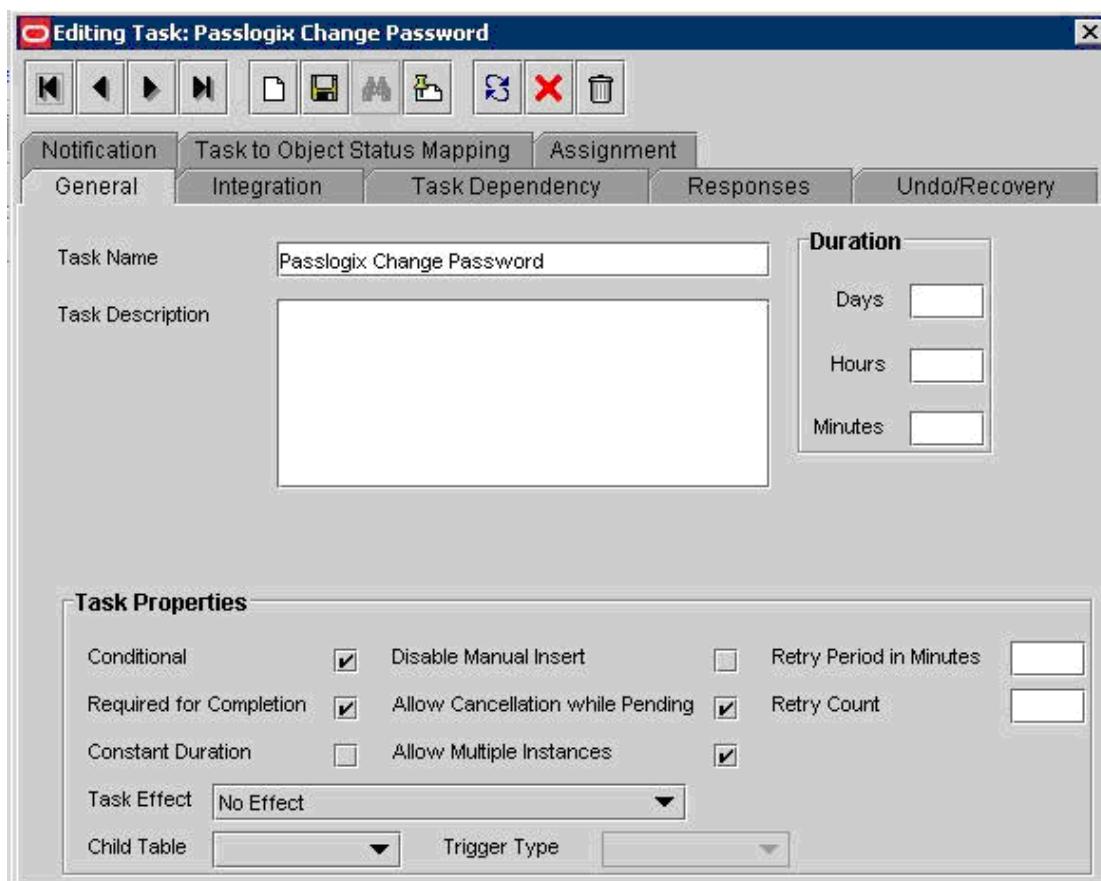
- Passlogix Change Password プロセス・タスクを作成する。
- Passlogix Modify Password アダプタをアタッチする。
- アダプタ変数をマップする。

Change Passwordプロセス・タスクの作成

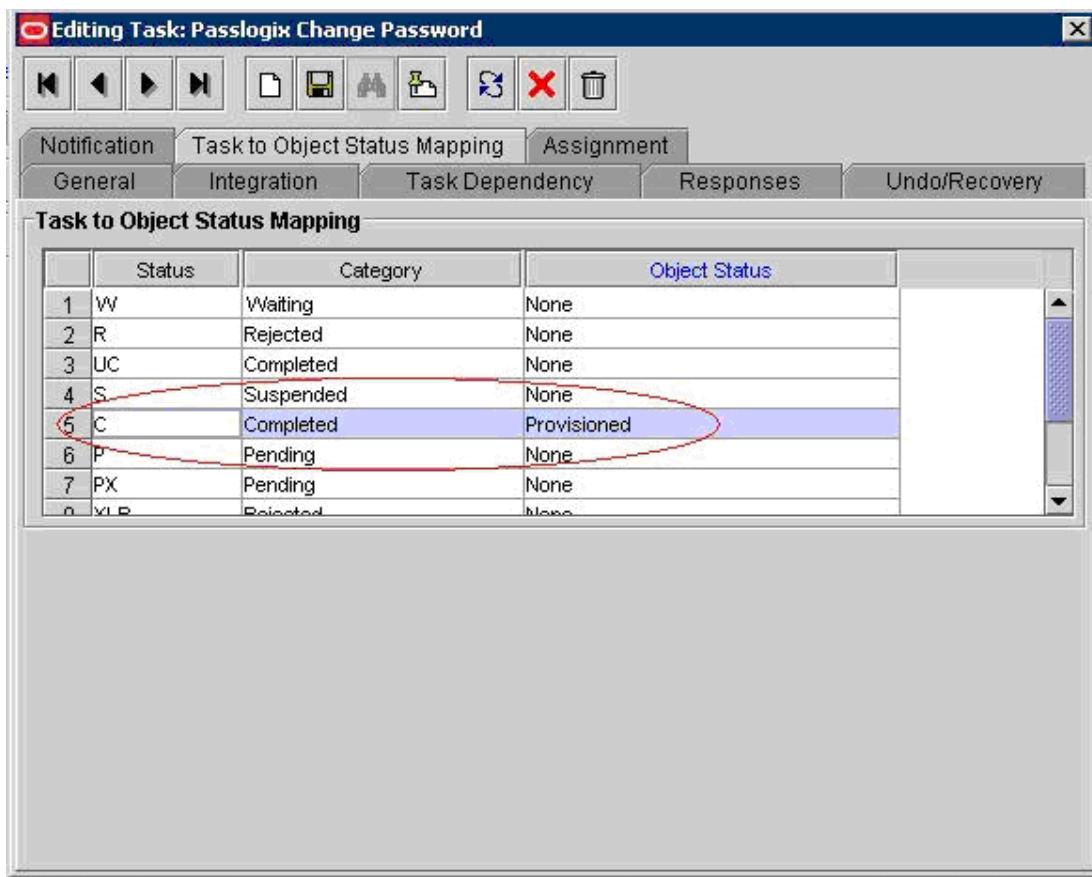
AD ユーザー・プロファイルのパスワードに変更があるたびに、このタスクがコールされます。このコールによって、Provisioning Gateway のパスワード変更の資格証明タスクに関連するタスクがトリガーされます。

Passlogix Change Password プロセス・タスクを追加するには、次の手順を実行します。

1. 「AD User」 プロセス定義を開きます。
2. AD ワークフローで、**Passlogix Change Password** タスクを追加します。
3. 「Required for Completion」、「Allow Cancellation while Pending」、「Conditional」 および「Allow Multiple Instances」 チェック・ボックスを選択します。「Task Effect」 コンボ・ボックスから「No Effect」 を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスとマップします。



5. 「Integration」 タブで、*adpPasslogixModifyPassword* アダプタをこのタスクにアタッチし、変数を次のようにマップします。

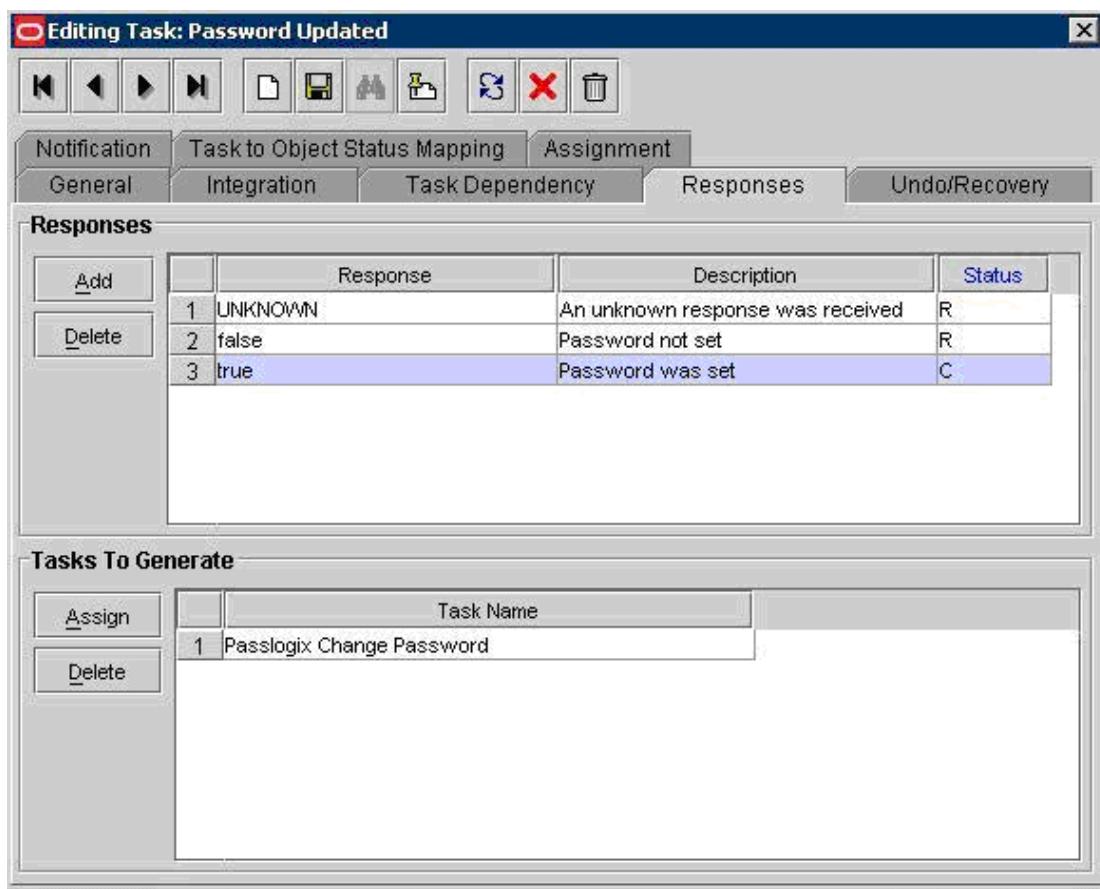
Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
User Key	long	User Definition	User Key	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcessInstanceKey	long	Process Data	Process Instance	なし	

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_ADUSER_A D	なし
Root_Resource_Name	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	Root_Resource_Name
Root_Resource_Object_Name	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	Root_Resource_Object_Name
RootITResource_ProcessFormVariable	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	RootITResource_ProcFormVar
RootUserID_ProcessFormVariable	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	RootUserID_ProcFormVar
serviceUserName	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	serviceUserName
servicePassword	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	servicePassword
Propertyfile	String	Literal	String	PMClientConfiguration.properties の正確なパス	
statusString	String	Literal	String	カンマ区切りのステータス値 (考慮するもの)。例: Provisioned, Disabled, Enabled	

これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。

6. 「AD User」プロセスの「Password Updated」プロセス・タスクの「Responses」タブで、true レスポンスを選択してハイライト表示します。次に、このタブの「Tasks to Generate」領域から、新しく作成した **Oracle Change Password** タスクを選択して割り当てます。

これによって、AD ワークフローに対するパスワード変更タスクごとに、Oracle Change Password タスクがコールされます。これは、パスワード変更タスクを含むどのワークフローについても同様です。



7. 「Save」をクリックします。

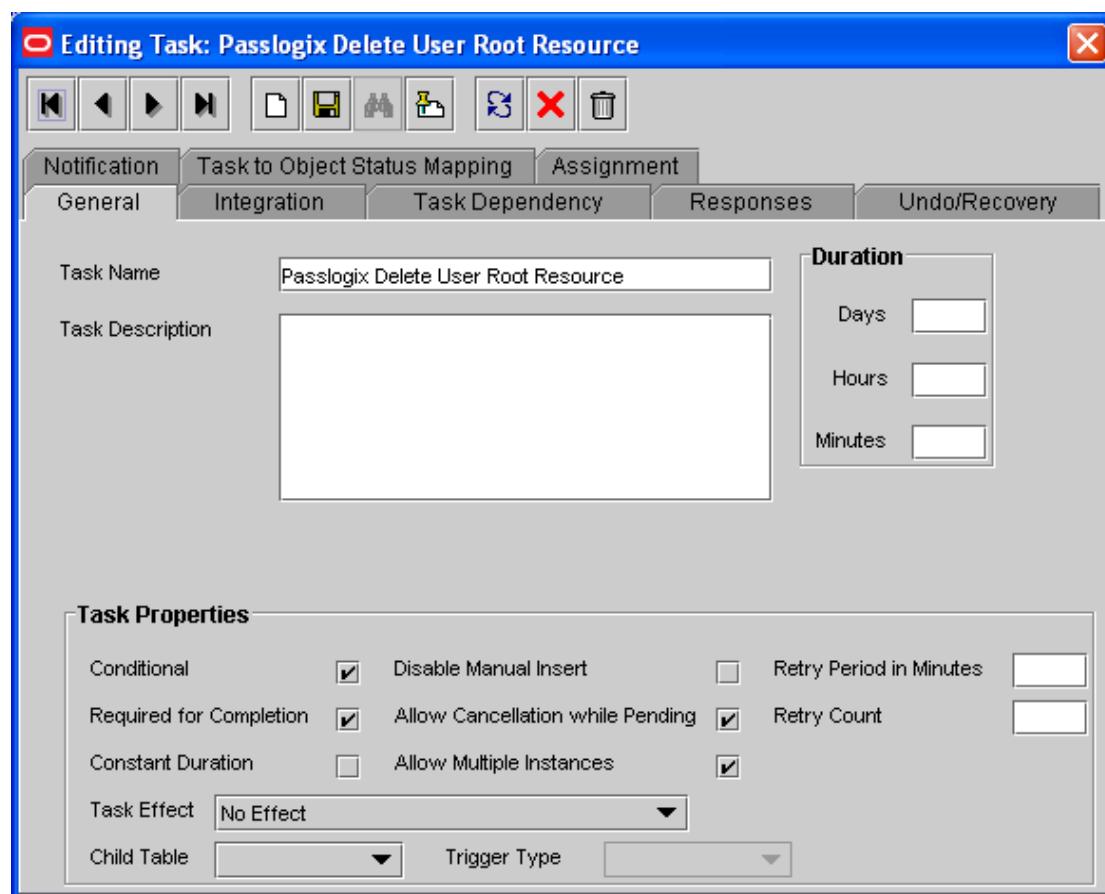
Passlogix Delete User Root Resourceプロセス・タスクの作成

この項では、次の方について説明します。

- Passlogix Delete User Root Resource プロセス・タスクを作成する。
- Passlogix Delete User Root Resource アダプタをアタッチする。
- アダプタ変数をマップする。

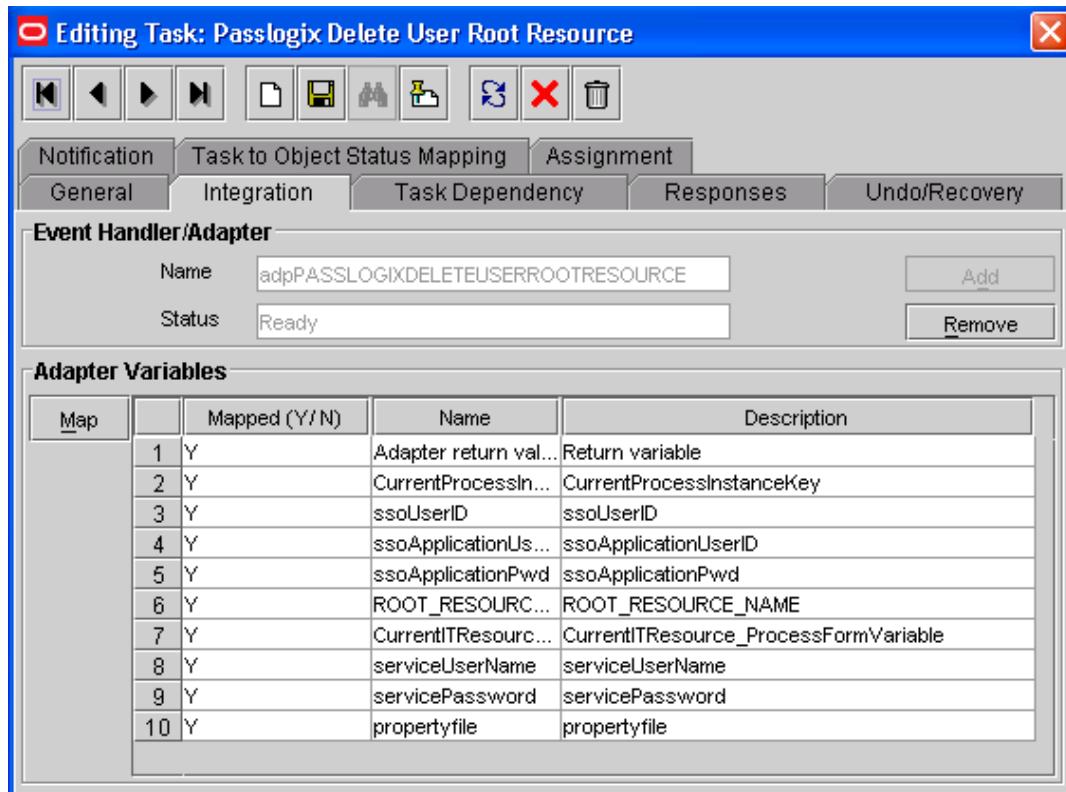
ユーザー・ルート・リソースの削除

1. 「AD User」プロセス・フォームを開きます。
2. **Passlogix Delete User Root Resource** タスクを追加します。



3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。

4. 「Integration」タブで、*adpPasslogixDeleteUserRootResource* アダプタをこのタスクにアタッチし、変数を次の画面に示すようにマップします。

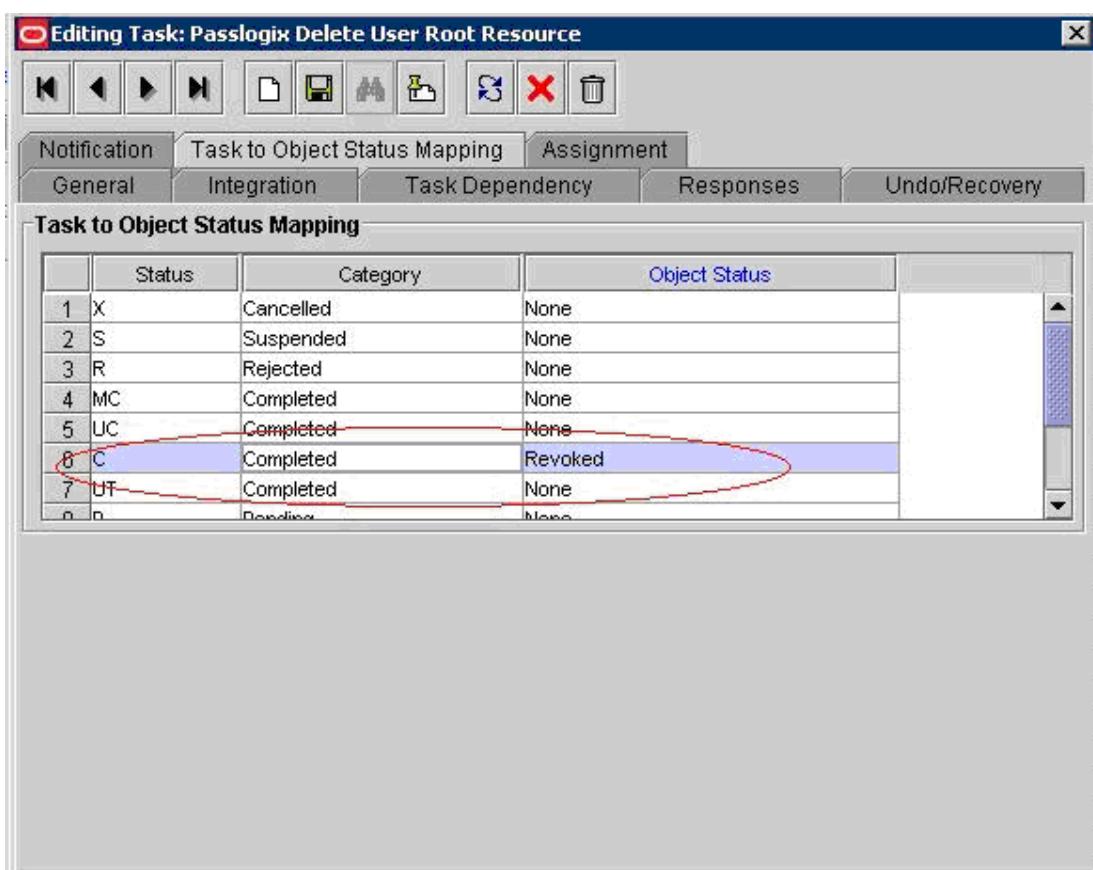


Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
ssoUserID	String	Process Data	User Id	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcess InstanceKey	long	Process Data	Process Instance	なし	
*Root_Resource_Name	String	IT Resources	VgoAD 定数	VGO PM 定数リソース	Root_Resource_Name

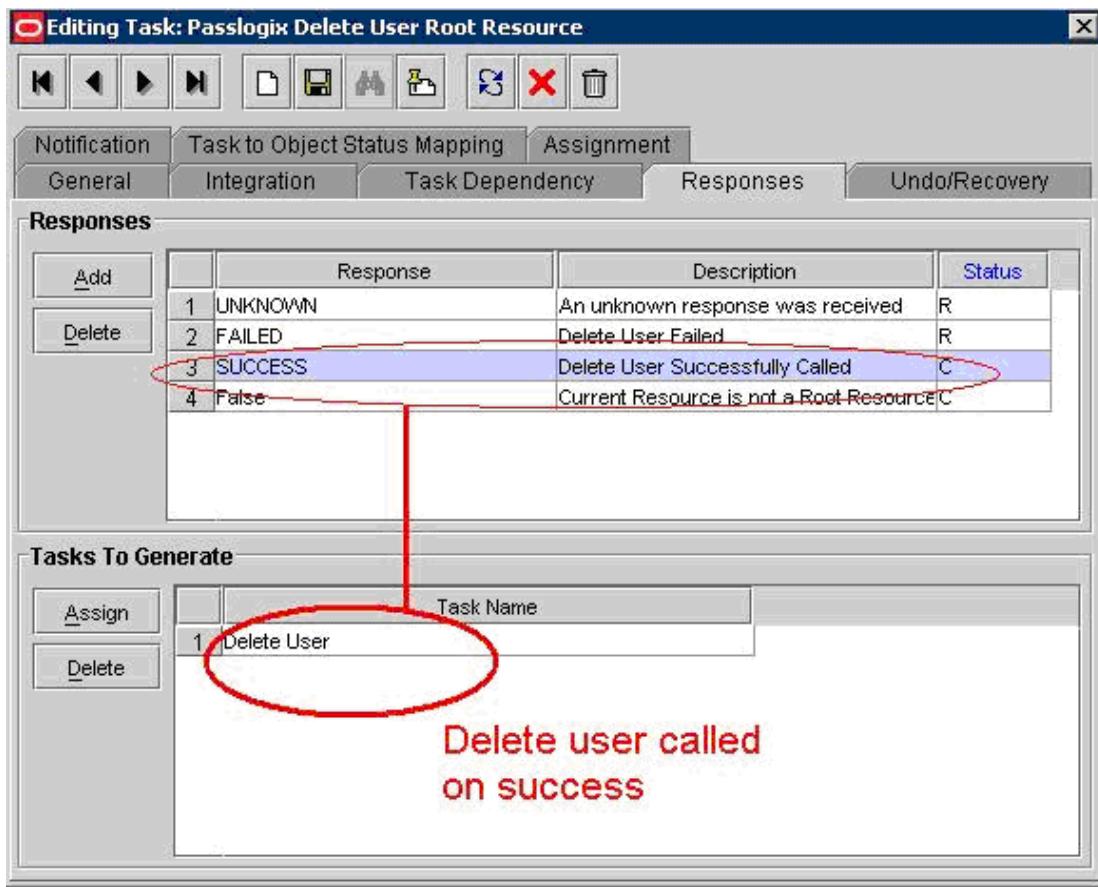
Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_ADUSER_AD	
serviceUserName	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	serviceUserName
servicePassword	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	Service Password
Propertyfile	String	Literal	String	正確なパス (PMClientConfiguration.properties)	

これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。

5. プロセス・タスク・ウィンドウの「Task to Object Status Mapping」タブで、「Completed (C)」プロセス・タスク・ステータスを「Revoked」リソース・オブジェクト・ステータスにマップします。



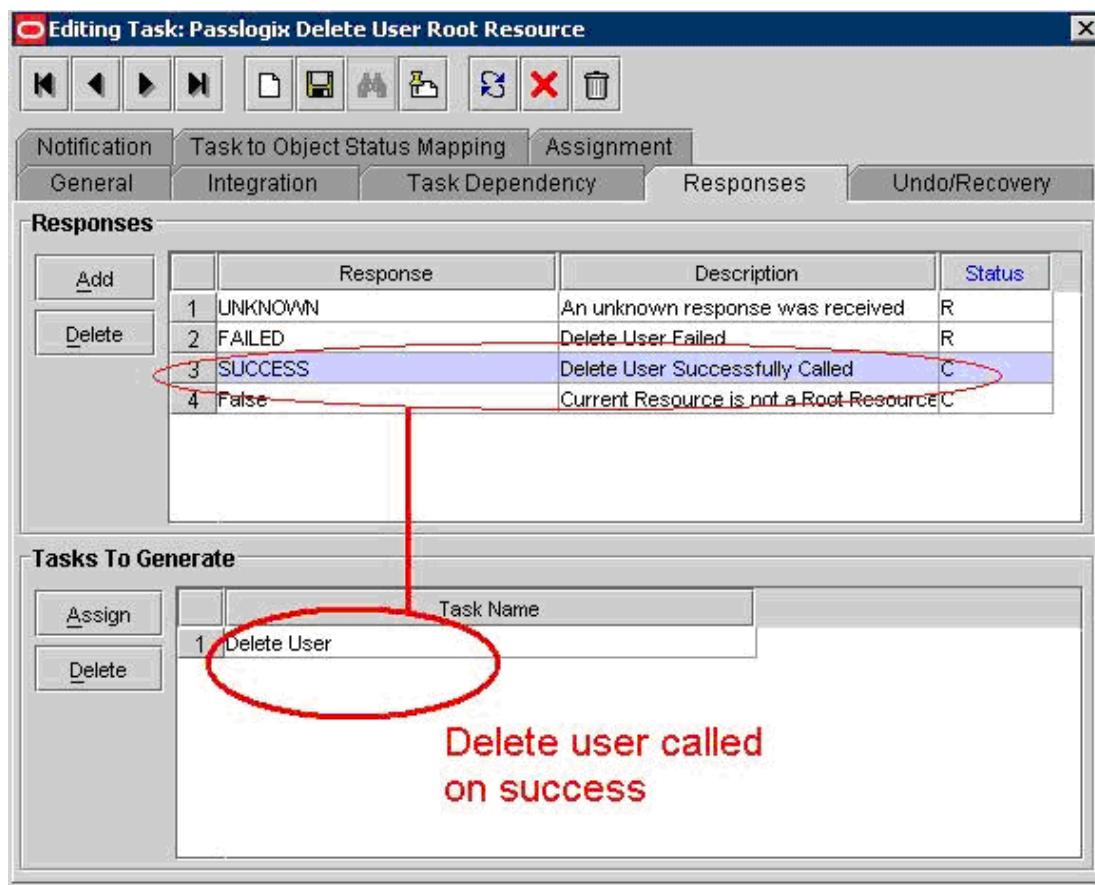
6. 「Create User Task」ウィンドウの「Recovery」タブで、「Delete User」を選択して削除します。Oracle Delete User Root Resource タスクを追加して割り当てます。



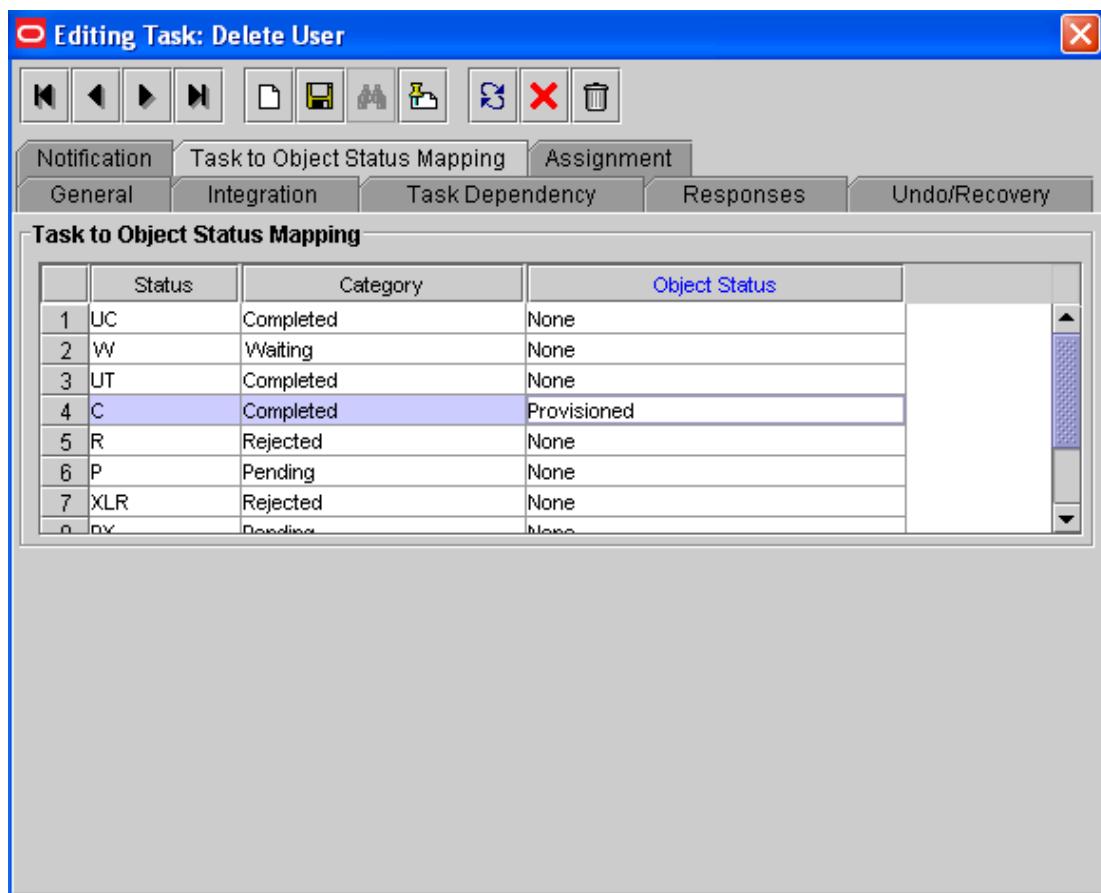
注意: ルート・リソースの場合、ユーザーはまず Provisioning Gateway から削除されてから、Active Directory から削除されるため、Revoke のコール時に Passlogix Delete User Root Resource プロセス・タスクがトリガーされる必要があります。Delete User は、成功時にコールする必要があります。

7. 「Passlogix Delete User Root Resource」タスク・ウィンドウの「Responses」タブで、レスポンス・コード **SUCCESS** を選択します。Delete User プロセス・タスクを追加して割り当てます。

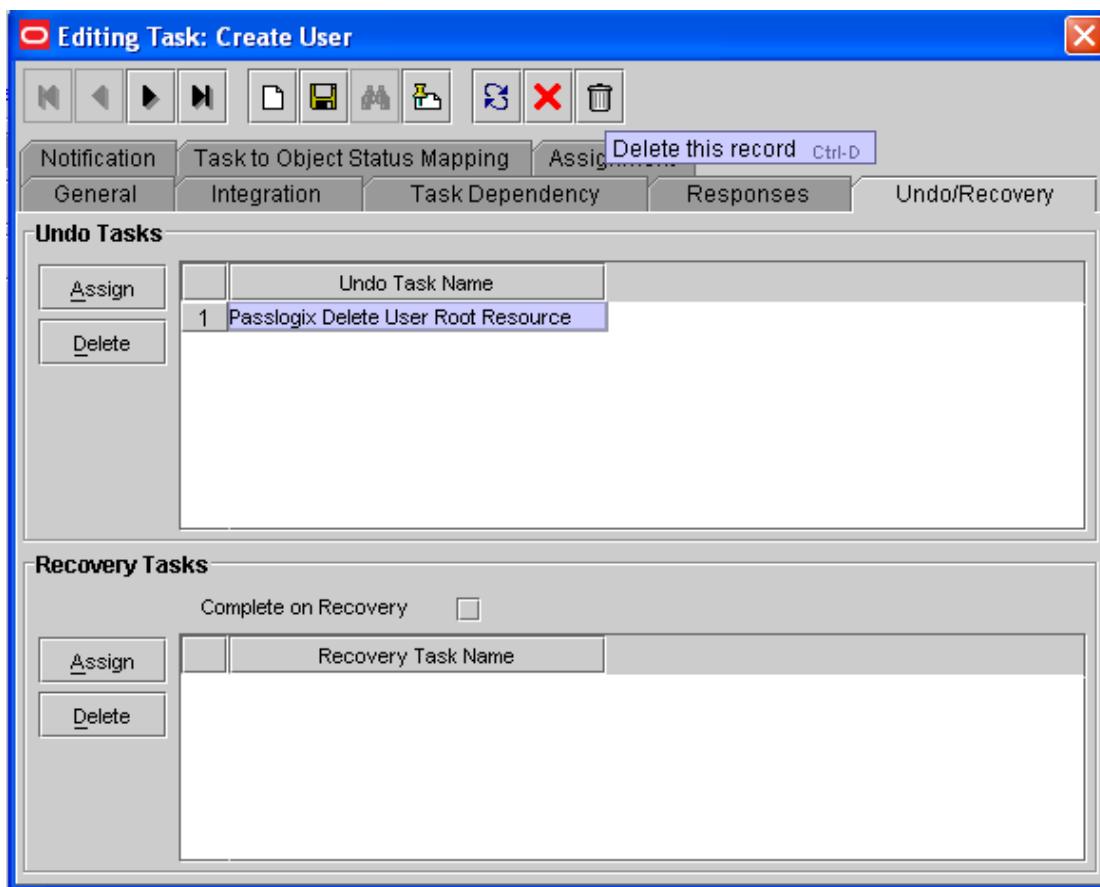
8. 「Passlogix Delete User Root Resource」タスク・ウィンドウの「Responses」タブで、レスポンス・コード **False** を選択します。Delete User プロセス・タスクを追加して割り当てます。



9. 「Delete User」プロセス・タスク・ウィンドウの「Task to Object Status Mapping」タブで、「Completed (C)」プロセス・タスク・ステータスのマッピングを「Revoked」から「Provisioned」リソース・オブジェクト・ステータスに変更します。



10. AD プロセス・ワークフローの Create User タスクで、リソース・オブジェクトが失効するときにトリガーされる「Undo/Recovery」タブに進みます。



11. 必要に応じてすべてのタスクを保存します。

iPlanet ユーザー・プロセスのワークフローの構成

この項では、非ルート・リソース・ワークフローのアダプタ構成について説明します。このプロセスでは、事前構成済ワークフロー内の主要タスク、特に Create User (プロビジョニング)、Delete User および Change Password タスクの識別を行います。これらのタスクは Oracle タスクをトリガーし、資格証明を Provisioning Gateway Management Console に送信します。

ワークフロー手順に対して **Create User** タスクを実行した後に、**Add Passlogix Credentials** タスクをコールします。**Delete User** タスクを実行した後に、**Delete Passlogix Credential** タスクをコールします。これは、対応するタスクの「Assign」タブで実行できます。

次に、iPlanet ワークフローに関する構成例を示します。ここでは、iPlanet ワークフローは非ルート・リソースです。したがって、iPlanet の資格証明は、Oracle Provisioning Gateway Management Console に送信可能です。現実の環境では、iPlanet のように多数の非ルート・リソース・ワークフローを持つことができます。

Passlogix Add Credential プロセス・タスクの作成

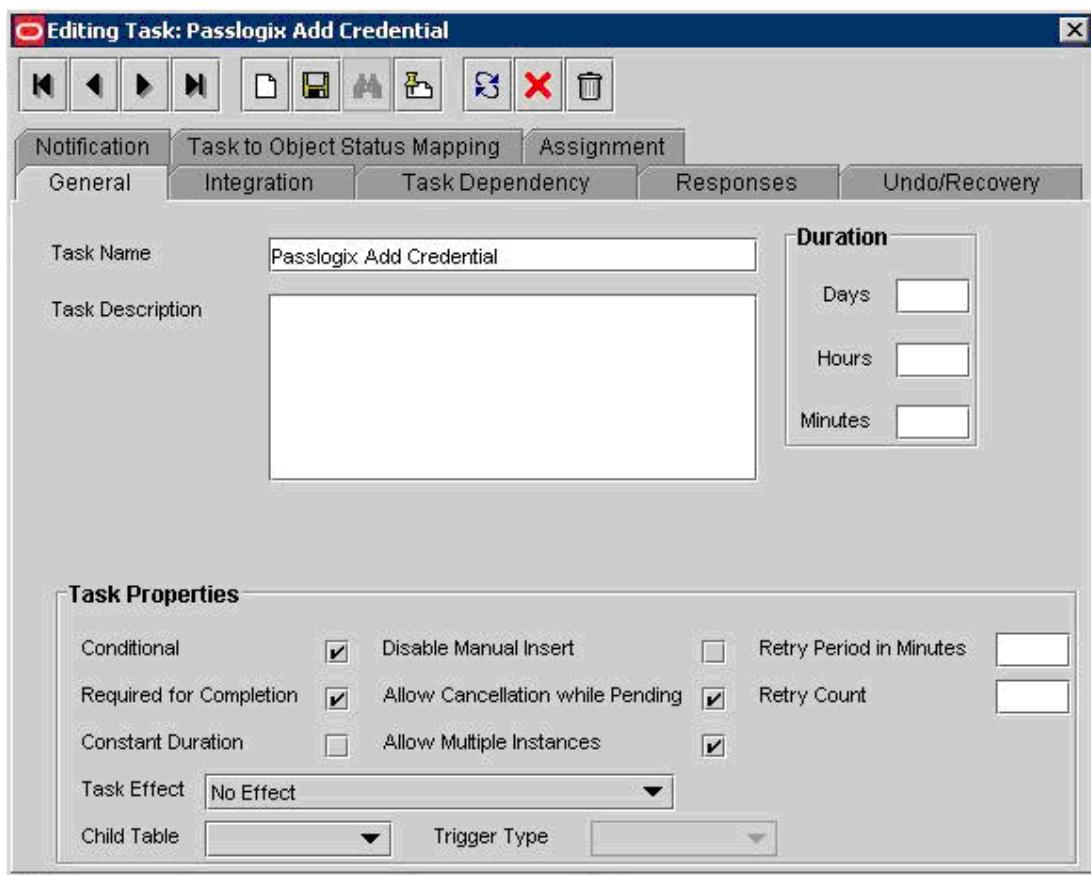
この項では、次の方法について説明します。

- Passlogix Add Credential プロセス・タスクを作成する。
- Passlogix Non Root Resource Add Credential アダプタをアタッチする。
- アダプタ変数をマップする。

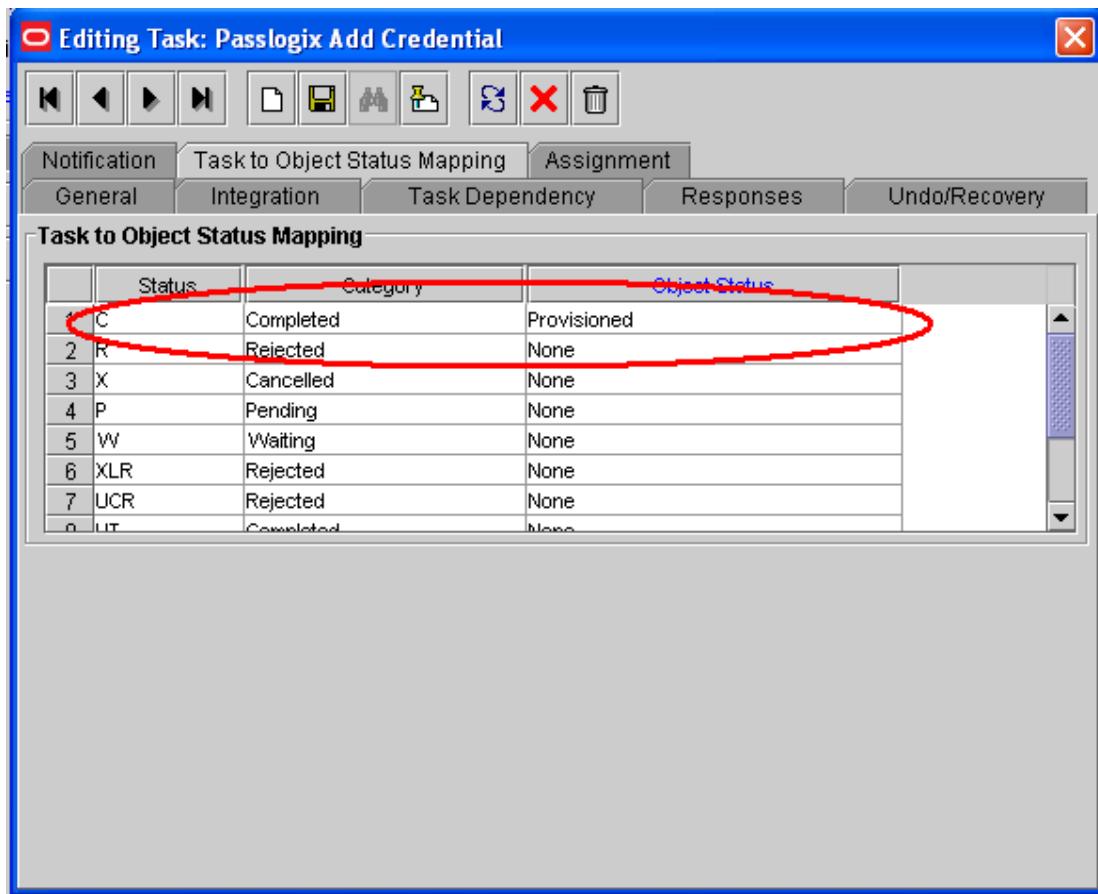
Add Credential タスクの作成

1. 「iPlanet User」プロセス・フォームを開きます。
2. **Passlogix Add Credential** タスクを追加します。

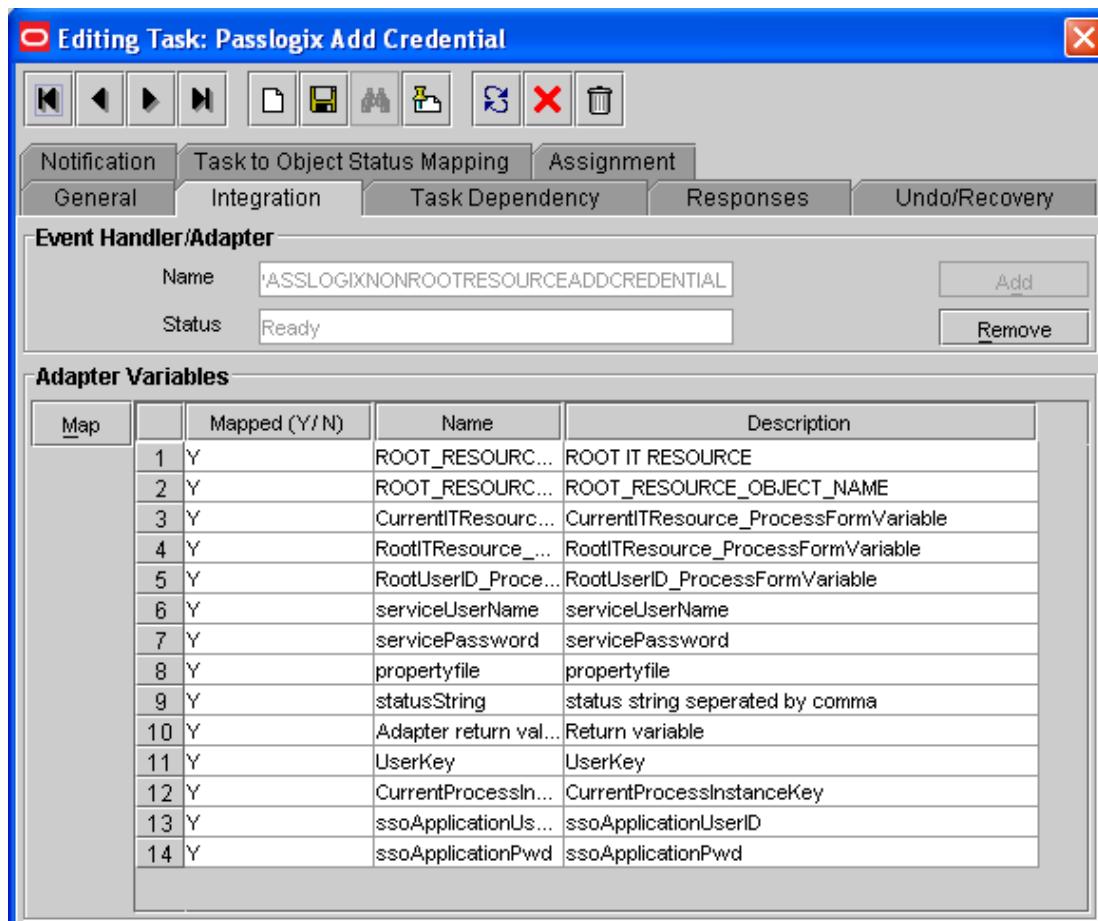
3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスにマップします。



5. 「Integration」タブで、*adpPasslogixNonRootResourceAddCredential* アダプタをこのタスクにアタッチし、その変数を次のようにマップします。

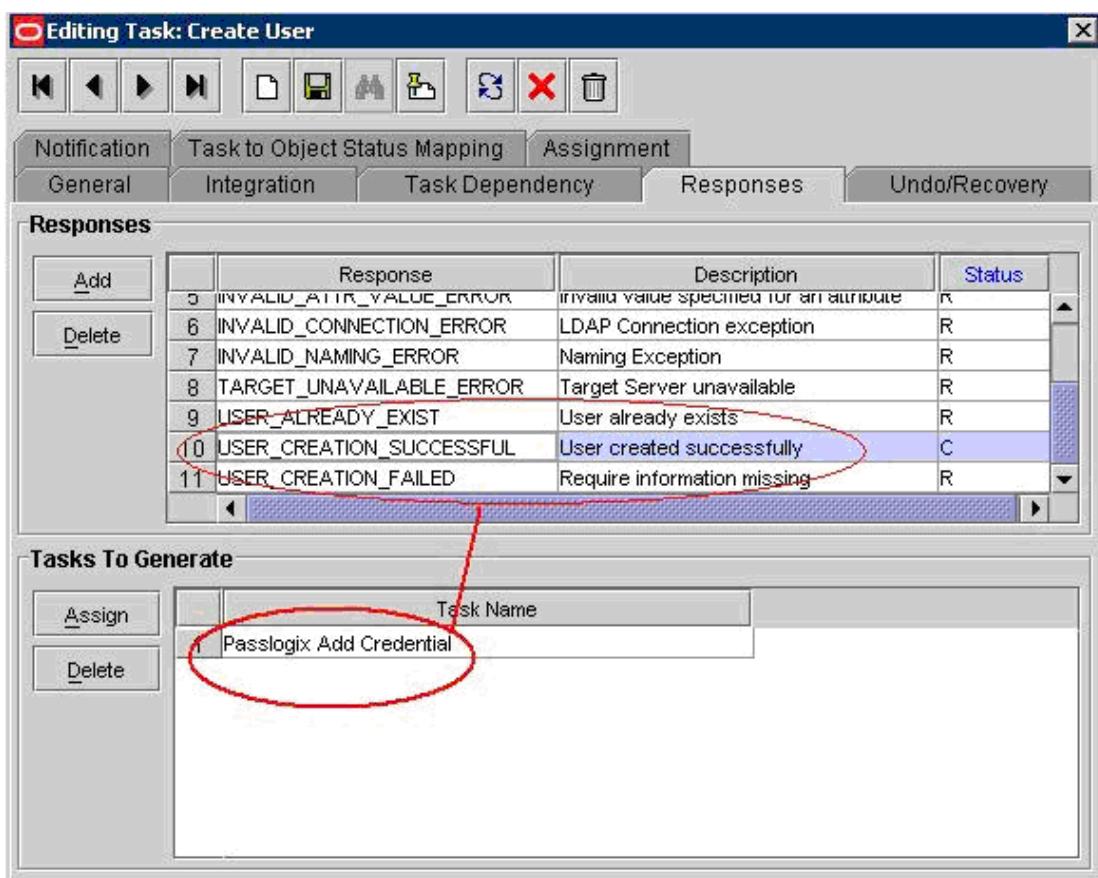


Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
User Key	long	User Definition	User Key	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcessInstanceKey	long	Process Data	Process Instance	なし	

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_IPNT_USR_SERVER	なし
Root_Resource_Name	String	IT Resources	VgoIPNTConstants	VGO PM 定数リソース	Root_Resource_Name
Root_Resource_Object_Name	String	IT Resources	VgoIPNTConstants	VGO PM 定数リソース	Root_Resource_Object_Name
RootITResource_ProcessFormVariable	String	IT Resources	VgoIPNTConstants	VGO PM 定数リソース	RootITResource_ProcFormVar
RootUserID_ProcFormVariable	String	IT Resources	VgoIPNTConstants	VGO PM 定数リソース	RootUserID_ProcFormVar
serviceUserName	String	IT Resource	VgoADConstants	VGO PM 定数リソース	serviceUserName
servicePassword	String	IT Resource	VgoADConstants	VGO PM 定数リソース	servicePassword
Propertyfile	String	Literal	String	PMClientConfiguration. properties の正確なパス	
statusString	String	Literal	String	考慮するステータス値のカンマ区切りリスト(例: Provisioned, Disabled, Enabled)	

CurrentITResource_ProcessFormVar: これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。このフィールドは、すべてのワークフローで異なります。これは、前述の iPlanet ワークフローのフィールド例として示されています。

6. iPlanet の Create User プロセス・タスクの「Responses」タブで、**User_Creation_Successful** レスポンスを選択してハイライト表示します。次に、このタブの「Tasks to Generate」領域から、**Oracle Add Credential** タスクを選択して割り当てます。



7. 「Save」をクリックします。

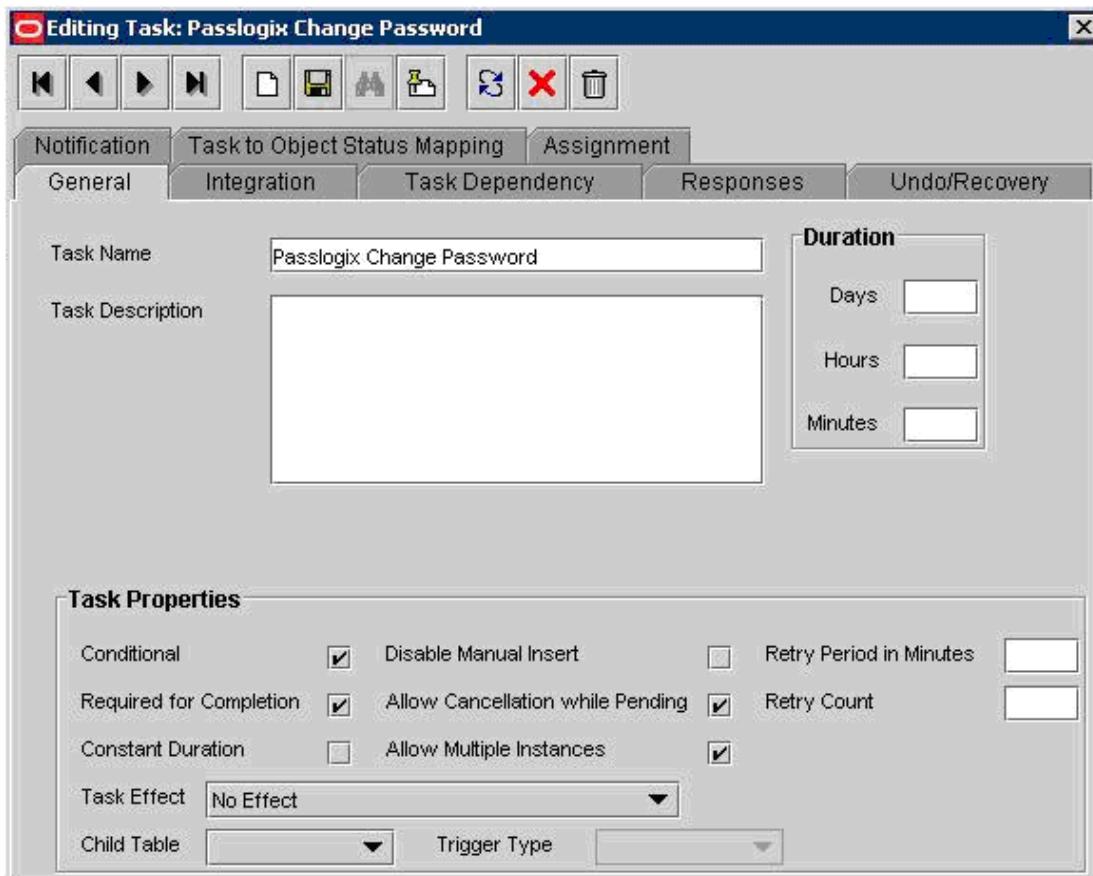
Passlogix Change Password プロセス・タスクの作成

この項では、次の方法について説明します。

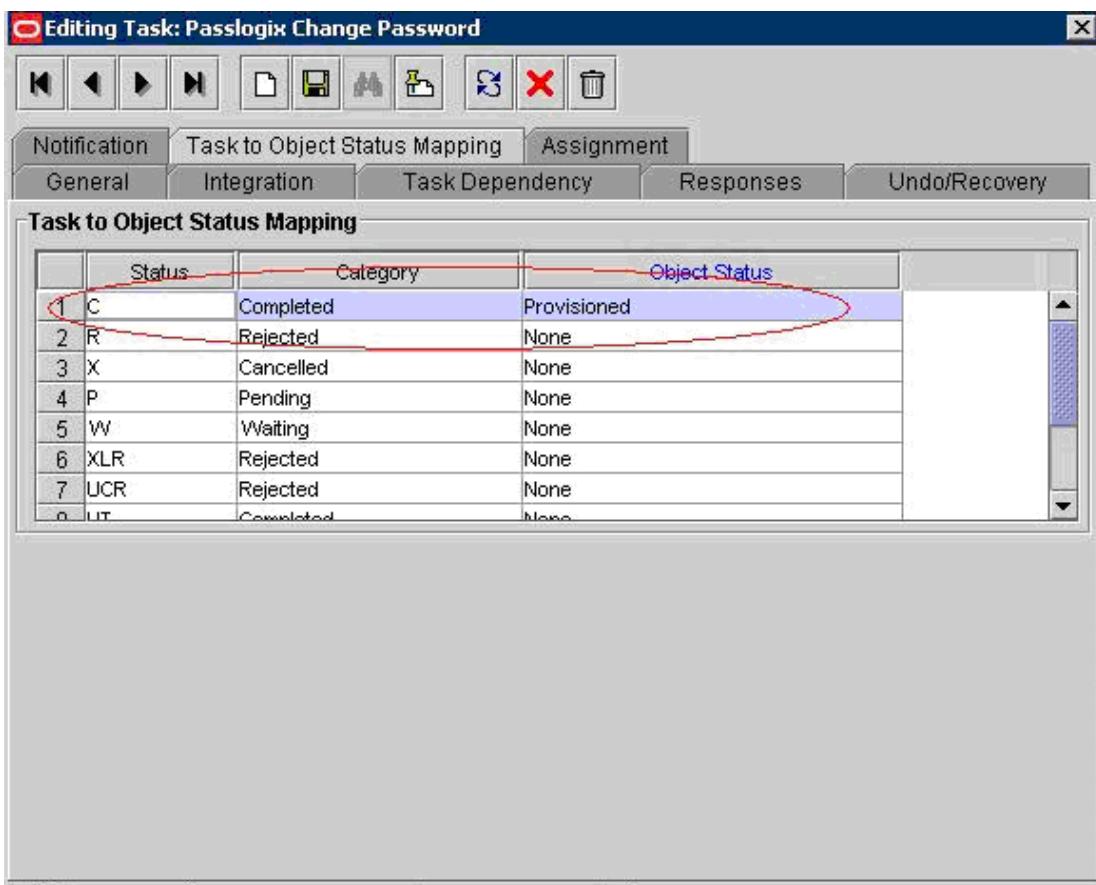
- Passlogix Change Password プロセス・タスクを作成する。
- Passlogix Modify Password アダプタをアタッチする。
- アダプタ変数をマップする。

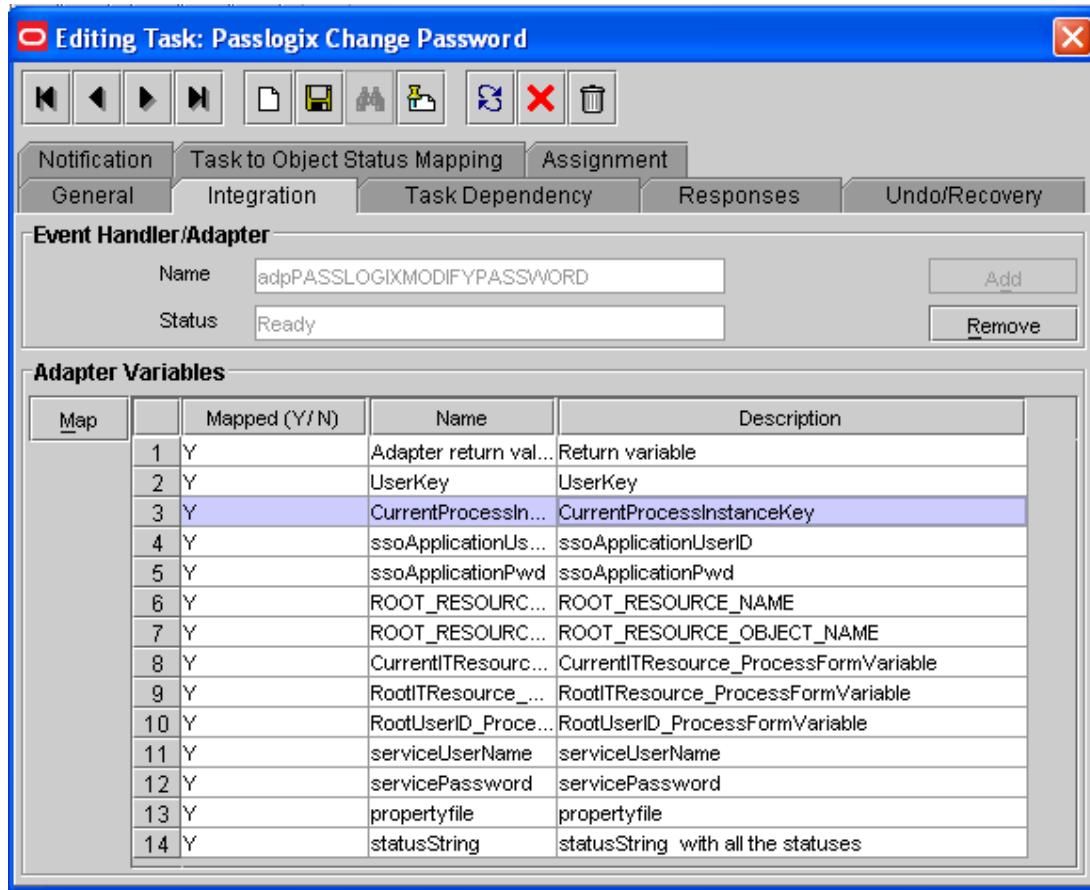
Change Password タスクの作成

1. 「iPlanet User」プロセス・フォームを開きます。Change Password タスクは、すでに iPlanet ワークフローに存在します。Passlogix Change Password タスクを作成し、それを iPlanet Change Password タスクが正常に完了したものに割り当てます。
2. **Passlogix Change Password** タスクを追加します。(これは iPlanet ワークフロー用です)。
3. 「Required for Completion」、「Allow Cancellation while Pending」、「Conditional」および「Allow Multiple Instances」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスにマップします。



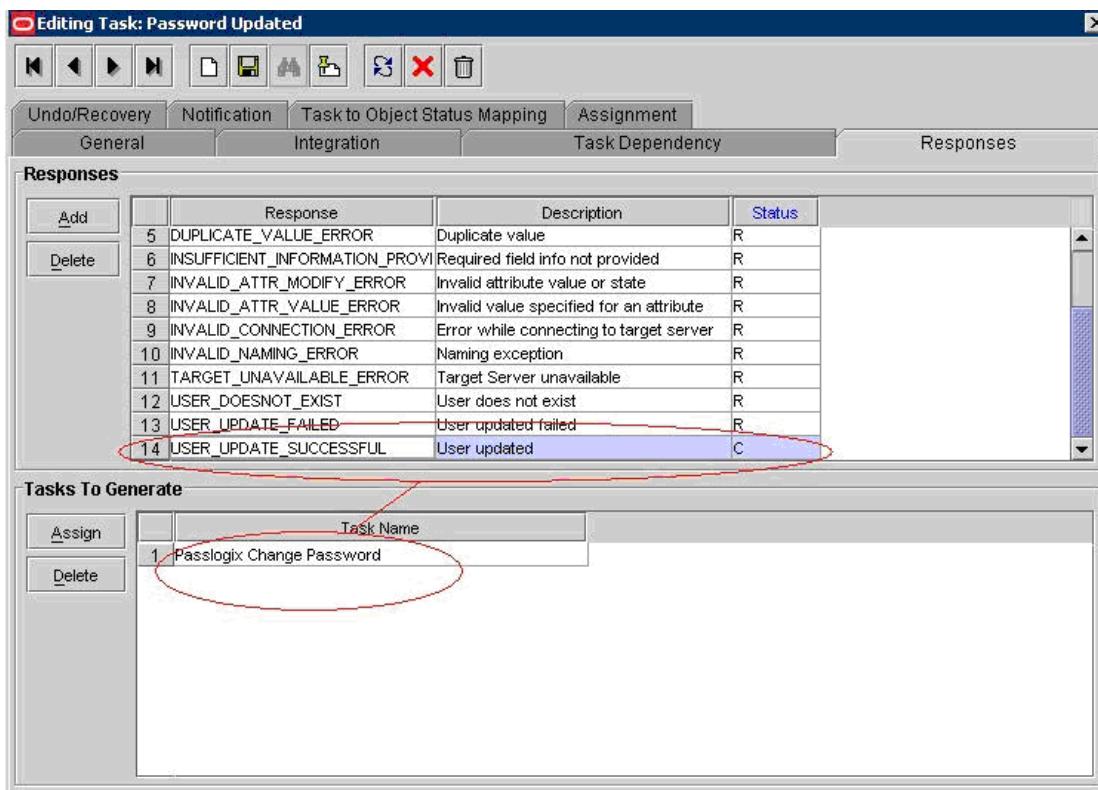


5. 「Integration」タブで、*adpPasslogixModifyPassword* アダプタをこのタスクにアタッチし、その変数を次のようにマップします。

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
User Key	long	User Definition	User Key	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcess InstanceKey	long	Process Data	Process Instance	なし	
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_IPNT_USR_SERVER	なし

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Root_Resource_Name	String	IT Resources	VgoIPNT 定数	VGO PM 定数リソース	Root_Resource_Name
Root_Resource_Object_Name	String	IT Resources	VgoIPNT 定数	VGO PM 定数リソース	Root_Resource_Object_Name
RootITResource_ProcessFormVariable	String	IT Resources	VgoIPNT 定数	VGO PM 定数リソース	RootITResource_ProcFormVar
RootUserID_ProcessFormVariable	String	IT Resources	VgoIPNT 定数	VGO PM 定数リソース	RootUserID_ProcFormVar
serviceUserName	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	serviceUserName
servicePassword	String	IT Resource	VgoAD 定数	VGO PM 定数リソース	servicePassword
Propertyfile	String	Literal	String	PMClientConfiguration. properties の正確なパス	
statusString	String	Literal	String	考慮するステータス値のカンマ区切りリスト(例: Provisioned, Disabled, Enabled)	

これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。



6. 「iPlanet User Password Updated」プロセス・タスクの「Responses」タブで、**User_Update_Successful** レスポンスを選択してハイライト表示します。次に、このタブの「Tasks to Generate」領域から、**Passlogix Change Password** タスクを選択して割り当て、親(この場合は iPlanet)ワークフローに対するすべてのパスワード変更タスク・リクエストに関してこのタスクをトリガーするようにワークフローに指示します。これは、任意の非ルート・ワークフローを対象にできます。
7. すべてのタスクを保存します。

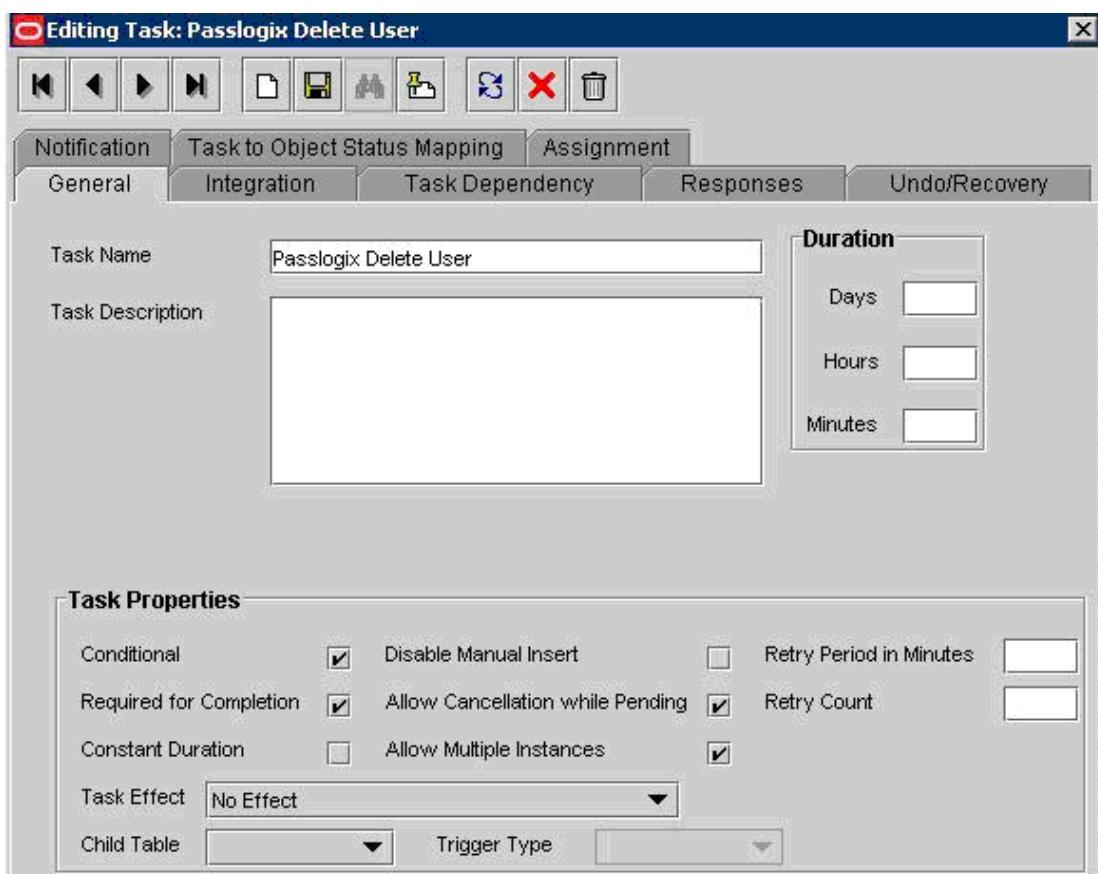
Passlogix Delete User Non-Root Resourceプロセス・タスクの作成

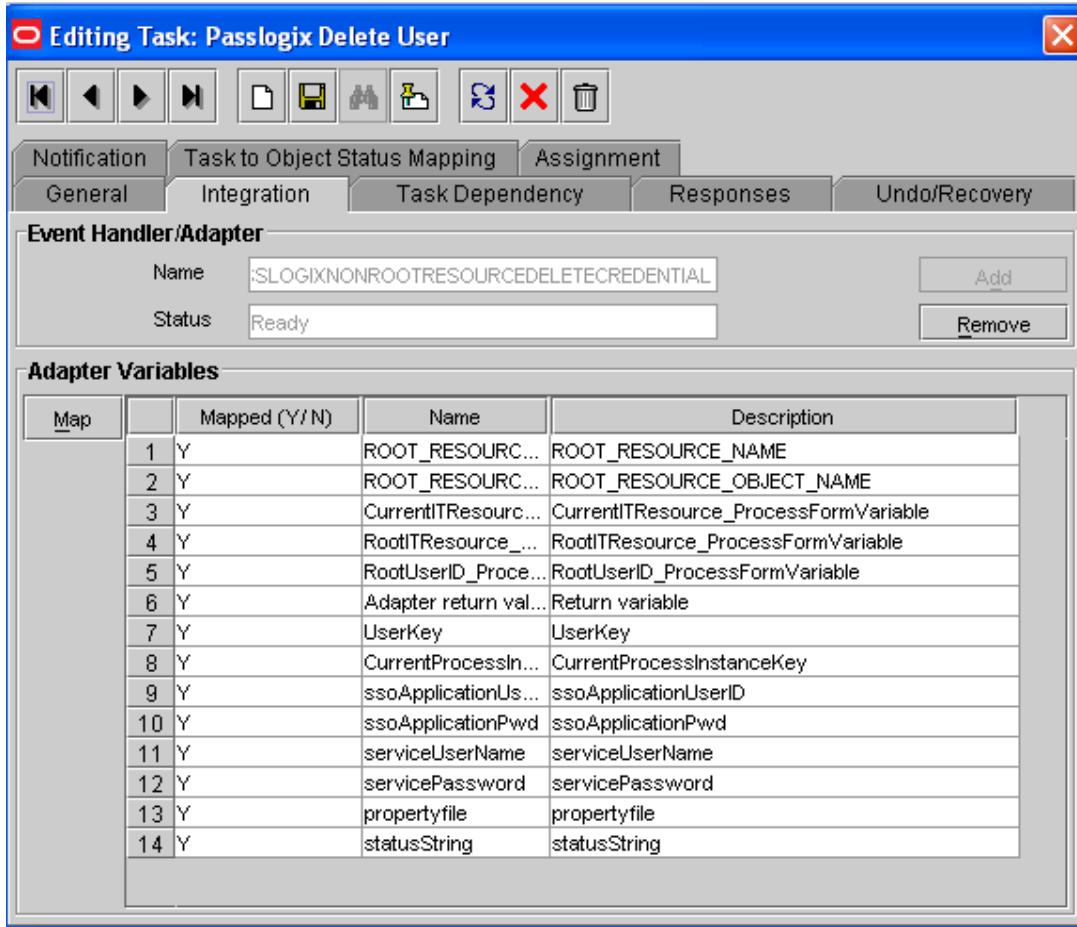
この項では、次の方について説明します。

- Passlogix Delete User Non Root Resource プロセス・タスクを作成する。
- Passlogix Non Root Resource Delete Credential アダプタをアタッチする。
- アダプタ変数をマップする。

Delete User Non-Root Resourceタスクの作成

1. 「iPlanet User」プロセス・フォームを開きます。
2. **Passlogix Delete User Non Root Resource**タスクを追加します。すべてのアダプタと、そのルートおよび非ルート・リソースに対する機能の詳細は、[「既存プロセスのワークフローの構成」](#)を参照してください。
3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。
4. 「Creating New Task」ウィンドウの「Task to Object Status Mapping」タブで、「Completed (C)」プロセス・タスク・ステータスを「Provisioned」リソース・オブジェクト・ステータスとマップします。





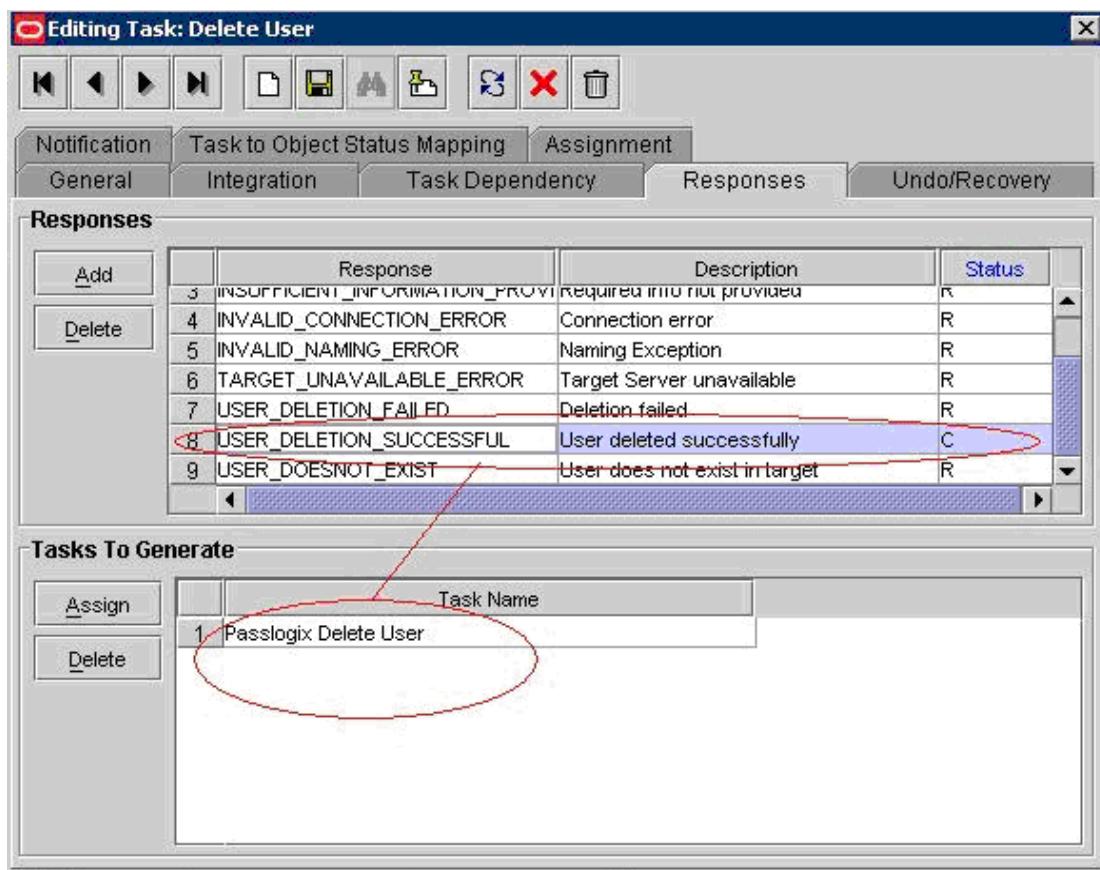
5. 「Integration」タブで、*adpPasslogixNonRootResourceDeleteCredential* アダプタをこのタスクにアタッチし、その変数を次のようにマップします。

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Adapter return value	Object	Response Code	なし	なし	
User Key	long	User Definition	User Key	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Process Data	Password	なし	
CurrentProcess InstanceKey	long	Process Data	Process Instance	なし	
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_IPNT_USR_SERVER	なし

Variable Name	Data Type	Map To	Qualifier	IT Asset Type/Literal Value	IT Asset Property
Root_Resource_Name	String	IT Resources	VgoIPNT 定数	VGO PM 定数リソース	Root_Resource_Name
Root_Resource_Object_Name	String	IT Resources	VgoIPNT 定数	VGO PM 定数 リソース	Root_Resource_Object_Name
RootITResource_ProcessFormVariable	String	IT Resources	VgoIPNT 定数	VGO PM 定数 リソース	RootITResource_ProcFormVar
RootUserID_ProcessFormVariable	String	IT Resources	VgoIPNT 定数	VGO PM 定数 リソース	RootUserID_ProcFormVar
serviceUserName	String	IT Resource	VgoAD 定数	VGO PM 定数 リソース	Service UserName
servicePassword	String	IT Resource	VgoAD 定数	VGO PM 定数 リソース	Service Password
Propertyfile	String	Literal	String	PMClientConfiguration. properties の正確な パス	
statusString	String	Literal	String	考慮するステータス値のカンマ区切りリスト(例: Provisioned, Disabled, Enabled)	

これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。

6. iPlanet の Delete User プロセス・タスクの「Responses」タブで、**User_Deletion_Successful** レスポンスを選択してハイライト表示します。次に、このタブの「Tasks to Generate」領域から、**Passlogix Delete User Non Root Resource** タスクを選択して割り当てます。



7. 「Save」をクリックします。

リコンシリエーション・プロセスのワークフローの構成

リコンシリエーションが事前構成済ワークフロー(ルートまたは非ルート・リソース)で常に機能することを前提としています。OIM の「Process」ワークフローには常に Reconciliation Insert Received タスクが存在しますが、これは新しいワークフロー(「Process」タイプ)の作成時に提供されます。

	Task	Default Assignee	Event Handler/Adapter	Conditional	Required for Completion	
Add	1 Reconciliation Add Credential		adpRECONCILIATIONPASSLOGIXADD CREDENTIAL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	2 Passlogix Add Credential		adpPASSLOGIXADD CREDITENTI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	3 Passlogix Change Password		adpPASSLOGIXCHANGEPASS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	4 Passlogix Delete User		adpPASSLOGIXDELETEUSERN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	5 Reconciliation Insert Received			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	6 Reconciliation Update Received			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	7 Reconciliation Delete Received			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	8 Service Account Alert			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	9 Service Account Moved			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	10 Service Account Changed			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	11 System Validation			<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	12 Create User		adpPLANETCREATEUSER	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	13 Delete User		adpPLANETDELETEUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	14 Change Email		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	15 Email Updated		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	16 Change First Name		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	17 First Name Updated		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	18 Change Last Name		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	19 Last Name Updated		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	20 Change Middle Name		adpPLANETMODIFYUSER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

このタスクは、リコンシリエーション・イベントが任意のワークフローで受信されるとトリガーされます。Reconciliation Add Credential タスクと同じワークフローに追加し、それに *adpPasslogixReconciliationAddCredential* アダプタを統合します。発生するリコンシリエーション・イベントごとに、Add Passlogix Credential タスクをトリガーし、新しい資格証明を Provisioning Gateway Server に送信します。

以降の項では、iPlanet および AD サーバーのリコンシリエーションの例を示し、Reconciliation Add Passlogix タスクの追加方法について説明します。

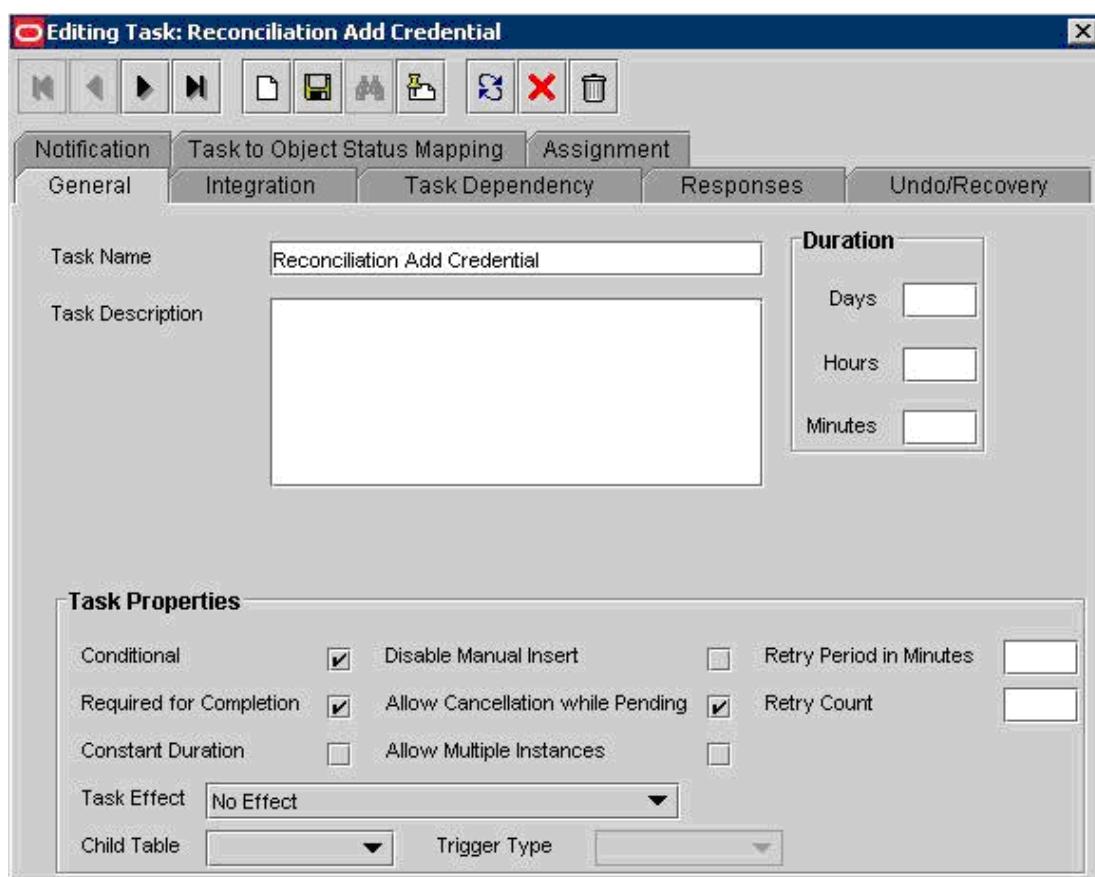
Reconciliation Add Credential プロセス・タスクの作成

この項では、次の方法について説明します。

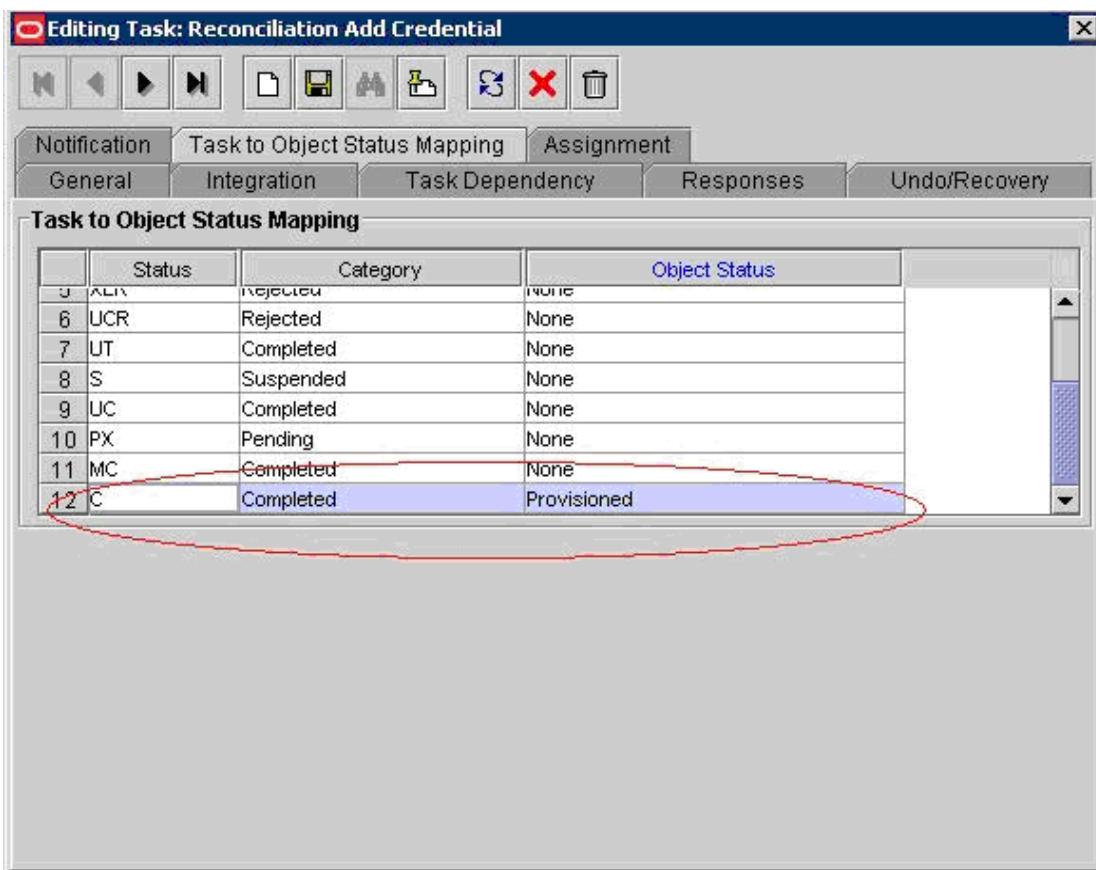
- Reconciliation Add Credential プロセス・タスクを作成する。
- Passlogix Reconciliation Add Credential アダプタをアタッチする。
- アダプタ変数をマップする。

Reconciliation Add Credential タスクの作成

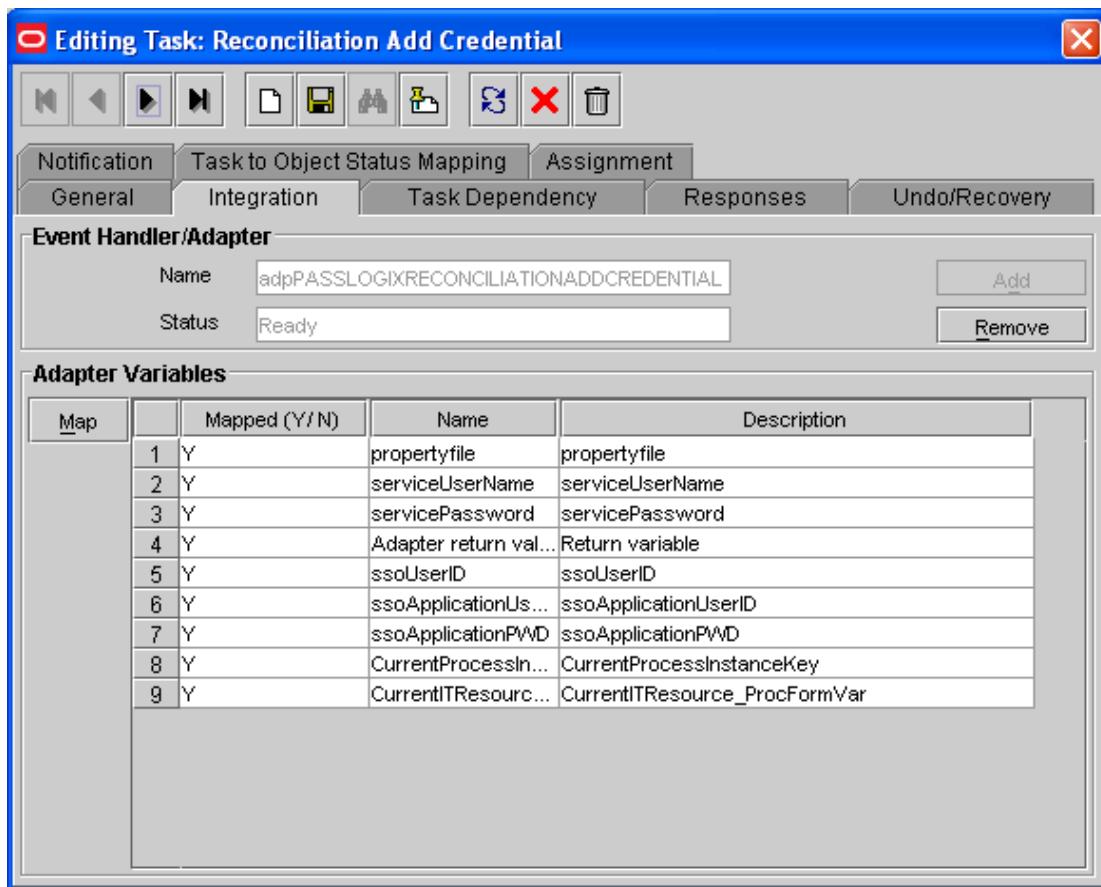
1. 「iPlanet User」プロセス・フォームを開きます。
2. **Reconciliation Add Credential** タスクを追加します。
3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから、「No Effect」を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスにマップします。



5. 「Integration」タブで、*adpPasslogixReconciliationAddCredential*アダプタをこのタスクにアタッチし、変数を次の画面および表に示すようにマップします。

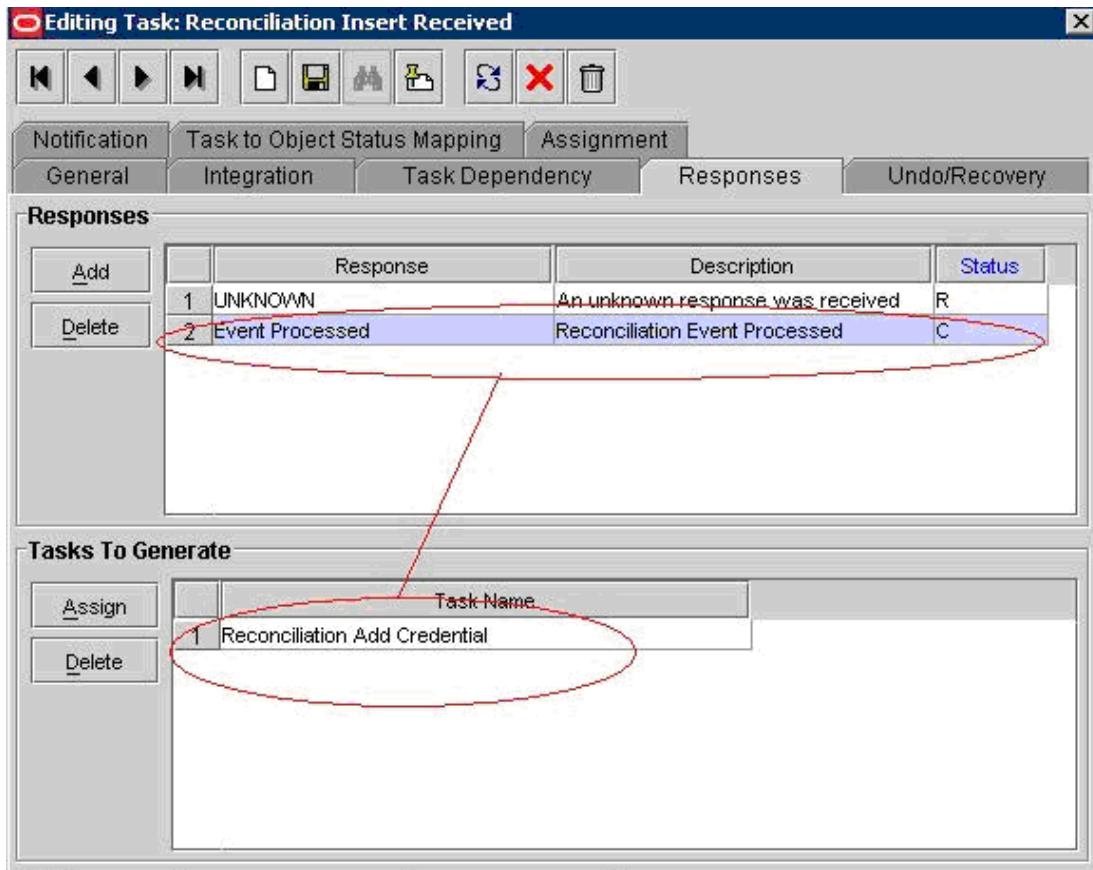


Variable Name	Data Type	Map To	Qualifier	Literal Value/IT Resource Type	IT Resource Property
Adapter return value	Object	Response Code	なし	なし	
ssoUserID	String	Process Data	User Id	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Literal	String	ダミー	なし
CurrentProcessInstanceKey	long	Process Data	Process Instance	なし	

Variable Name	Data Type	Map To	Qualifier	Literal Value/IT Resource Type	IT Resource Property
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_IPNT_USR_SERVER	
serviceUserName	String	Literal	String	Vgo インストールのとおり	なし
servicePassword	String	Literal	String	Vgo インストールのとおり	Service Password
Propertyfile	String	Literal	String	正確なパス	Propertyfile

このアダプタの動作の詳細は、[「リコンシリエーション・プロセスのワークフローの構成」](#)を参照してください。

6. iPlanet ユーザーの Reconciliation Insert Received プロセス・タスクの「Responses」タブで、「Event Processed」レスポンスを選択します。次に、このタブの「Tasks to Generate」領域から、Reconciliation Oracle Add Credential タスクを選択して割り当てます。これは、新しいユーザーがリコンシリエーション・プロセスでプロビジョニングされた場合に、資格証明を Oracle コードに送信するようにワークフロー・ログックに指示するため、重要です。



7. タスクを保存します。

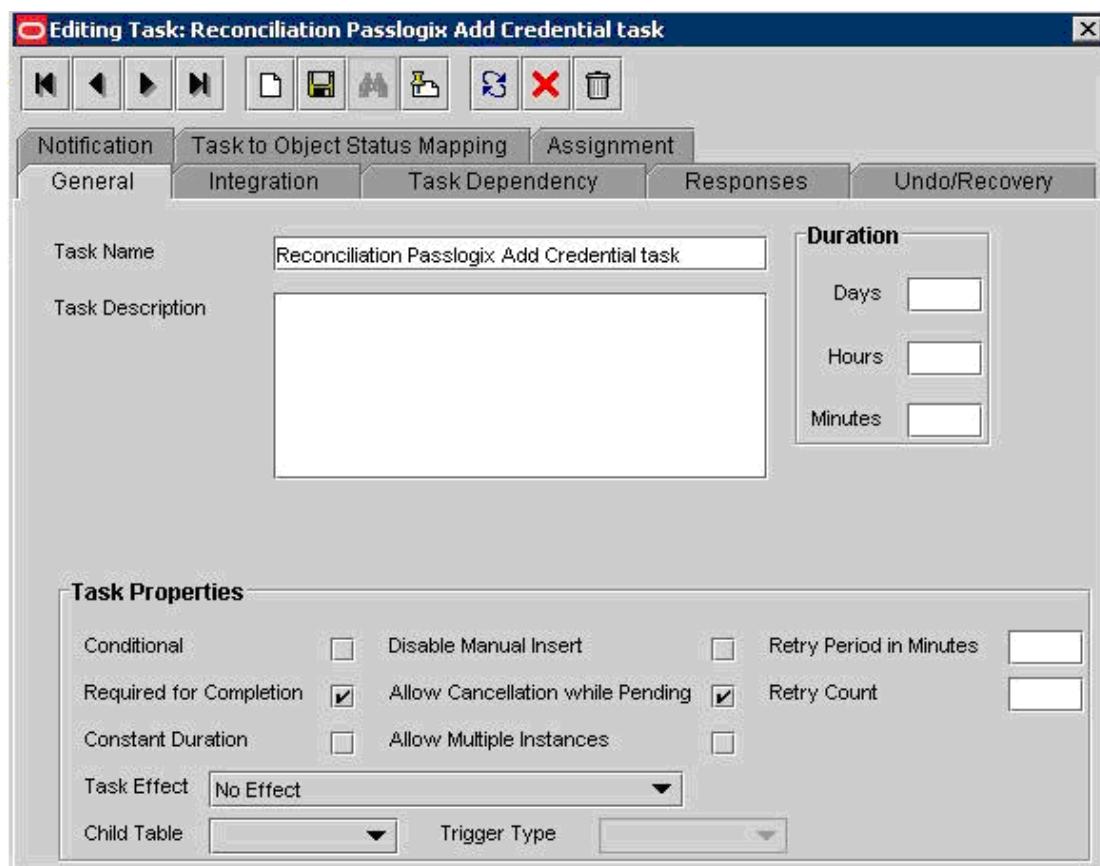
Reconciliation Passlogix Add Credential プロセス・タスクの作成

この項では、次の方法について説明します。

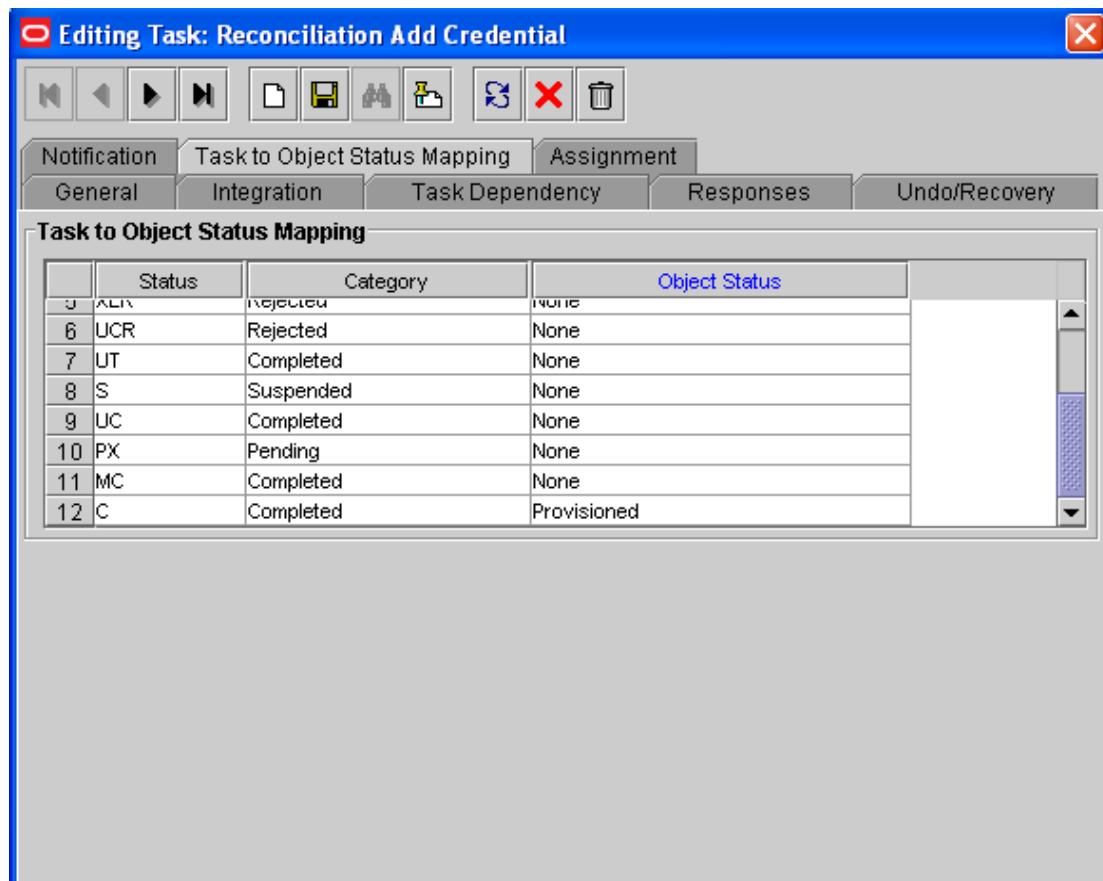
- Reconciliation Passlogix Add Credential プロセス・タスクを作成する。
- Passlogix Reconciliation Add Credential アダプタをアタッチする。
- アダプタ変数をマップする。

Reconciliation Add Credential タスクの作成

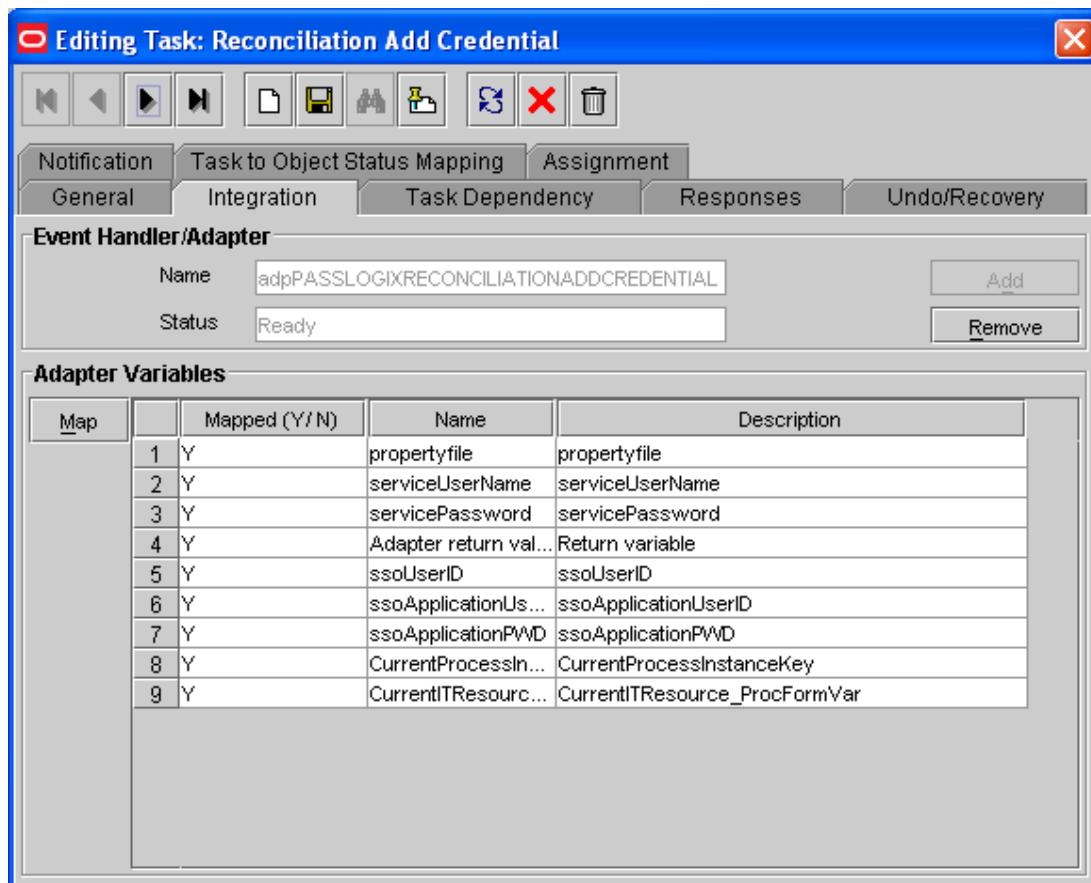
1. 「AD User」プロセス・フォームを開きます。
2. **Reconciliation Passlogix Add Credential** タスクを追加します。
3. 「Required for Completion」、「Allow Cancellation while Pending」および「Conditional」チェック・ボックスを選択します。「Task Effect」コンボ・ボックスから「No Effect」を選択します。



4. 「Creating New Task」 ウィンドウの「Task to Object Status Mapping」 タブで、「Completed (C)」 プロセス・タスク・ステータスを「Provisioned」 リソース・オブジェクト・ステータスにマップします。



5. 「Integration」タブで、*adpPasslogixReconciliationAddCredential* アダプタをこのタスクにアタッチし、変数を次のようにマップします。

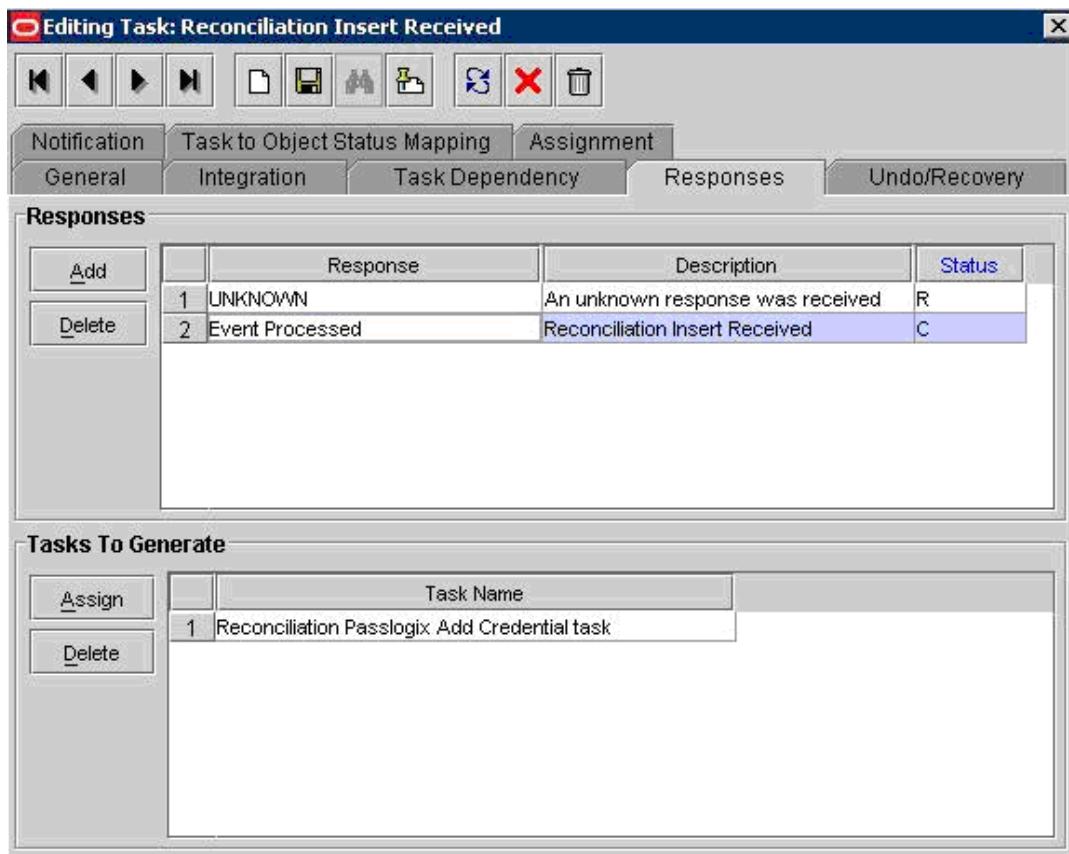


これは、「Resource Object」フォームの「IT Resource」フィールドの列名です。

Variable Name	Data Type	Map To	Qualifier	Literal Value/ IT Resource Type	IT Resource Property
Adapter return value	Object	Response Code	なし	なし	
ssoUserID	String	Process Data	User Id	なし	
ssoApplicationUserID	String	Process Data	User Id	なし	
ssoApplicationPWD	String	Literal	String	ダミー	なし
CurrentProcessInstanceId	long	Process Data	Process Instance	なし	

Variable Name	Data Type	Map To	Qualifier	Literal Value/ IT Resource Type	IT Resource Property
#CurrentITResource_ProcessFormVar	String	Literal	String	UD_ADUSER_AD	
serviceUserName	String	Literal	String	Vgo インストールのとおり	なし
servicePassword	String	Literal	String	Vgo インストールのとおり	なし
Propertyfile	String	Literal	String	PMClientConfiguration.properties の正確なパス	

6. 「AD User」のReconciliation Insert Received プロセス・タスクの「Responses」タブで、「Event Processed」レスポンスをハイライト表示して選択します。次に、このタブの「Tasks to Generate」領域から、**Reconciliation Passlogix Add Credentials** を選択して割り当てます。



7. 閉じる前にタスクを保存します。

前提

- この例では、新しいアプリケーション(新しいアカウント)がアイデンティティにプロビジョニングされています。Provisioning Gateway のリソース・フィールド(デフォルト値を持つプロセス・フォーム・フィールド)の値を、OIM リコンシリエーション・エンジンによって処理されるリコンシリエーション・ハッシュマップに入力するのは、リコンシリエーション・デザイナの役割です。これは、特定のアプリケーション・ワークフローに関して 1 人のユーザーに割り当てることができる Provisioning Gateway Server がシステムに複数ある場合に該当します。リコンシリエーション・コードからこの値が見つからない場合、Reconciliation Add Credential タスクは失敗します。このフィールドが重要な場合は、このフィールドをリソース・オブジェクト・レベルで必須フィールドにする必要があることを、常に前提としています。その場合は、Reconciliation Insert が受信されて、このフォームにビジネス・ルールに基づいて値を入力し、Reconciliation Passlogix Add Credential をコールした後に実行される、別の「Process」タスクが存在することもあります。この選択は、ビジネス・ロジックによって異なります。
- serviceUsername および Servicepassword は、IT リソース VGO 定数にマップされます。これら 2 つのフィールドはバックエンド・データベースで暗号化され、セキュリティで保護されます。複数の SSO サーバーを使用する場合、Provisioning Gateway Server を VGOADConstants タイプの IT リソースとして構成可能であり、実行時にそのフィールドに対してマッピングを実行できます。デフォルトでは、マッピングに使用できる VGOADConstants インスタンスは 1 つだけです。

サンプル・ワークフローの使用およびテスト

この項では、XML ファイル(提供されたパッケージの *Resourceobjects.xml*、*ITresources.xml*、*lookups.xml*)をサンプル・ワークフローとして使用するテスト環境のデプロイメントについて説明します。

環境のデプロイメント

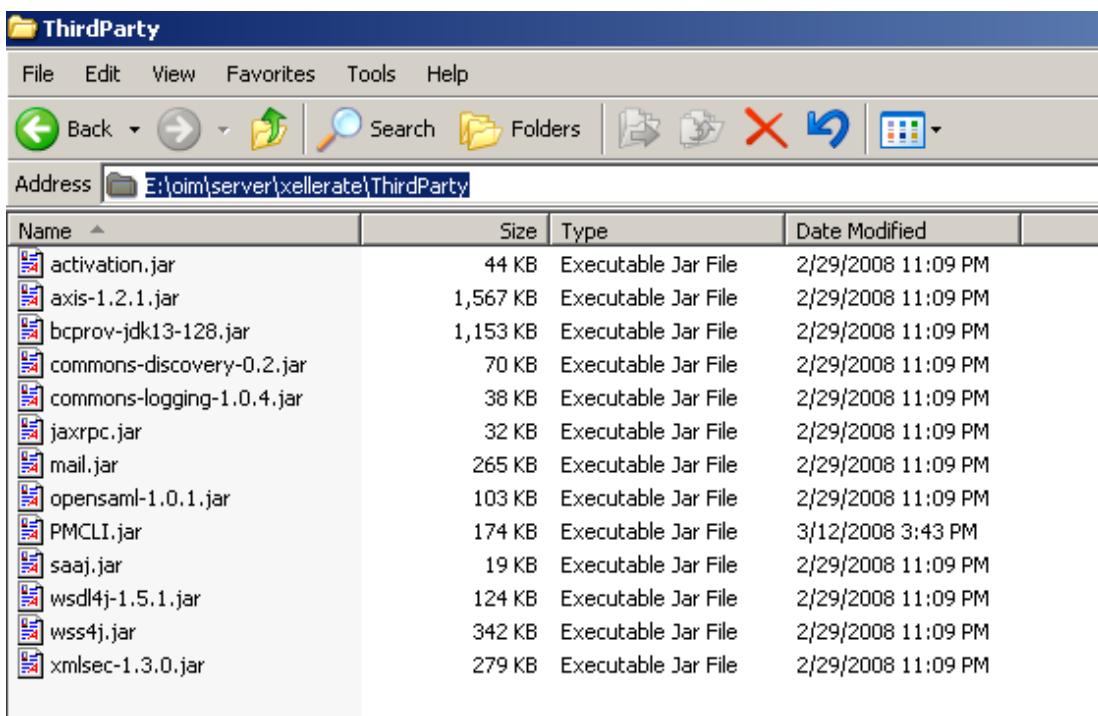
- JBoss 4.0.3 SP1(アプリケーション・サーバーとして)
- OIM 9.1.0.1849.0
- Java version j2sdk1.4.2_15

インストール手順については、[JBossのインストールに関する項](#)を参照してください。

ライブラリ

- <*oim\server\xellerate\ThirdParty*>ディレクトリのパッケージから次の jar をコピーします。

Jarの名前	Jarのバージョン
PMCLI.jar	174KB
axis.jar	1.2.1
bcpprov-jdk13-128.jar	1.28.0
commons-discovery-0.2.jar	0.2
commons-logging-1.0.4.jar	1.0.4
jaxrpc.jar	-
opensaml-1.0.1.jar	1.0.1
com.oracle.ws.orawsdl_1.2.0.0.jar	1.2
wss4j.jar	-
xmlsec-1.3.0.jar	1.3.0



ここでテストする java バージョンは、j2sdk1.4.2_15 です。

2. 次の表に示すファイルを <jboss-4.0.3SP1_home>\lib\endorsed にコピーします。これらのファイルは、パッケージで提供されます。
古いバージョンを置き換える必要がある場合があります。その場合は、ISO パス (ISO\Libraries\JavaCLI\1.4\endorsed) にあるファイルと置き換えます。
3. 次の jar を置き換えるか、配置します。

Jarの名前	Jarのバージョン
dom.jar	Xerces-J_2_5_0
jaxp-api.jar	1.3
sax.jar	Xerces-J_2_5_0
xalan.jar	2.1.4
xercesImpl.jar	Xerces-J_2_5_0

Oracleコネクタのデプロイ

1. *OIMConnector11.1.2.0.0.jar* のプロパティ・ファイルを変更して、適切な環境のサービス URL を設定します。
2. jar を再作成します。パッケージから OIMConnector11.1.2.0.0.jar をコピーし、*<oim_server_home>\xellerate\JavaTasks* ディレクトリに格納します。このパッケージにはサンプル AD サーバー・ワークフローが含まれているため、すぐに使用できる AD コネクタ・パックが必要になりますが、このパッケージには含まれていません。
3. AD のテストに使用するコネクタは *xliActiveDirectory.jar* で、ディレクトリ・サーバー・フォルダの OIM コネクタ・パックに含まれています。

XMLファイルのインポート

1. XML(*Resourceobjects.xml*)をインポートします。(これはサンプル・ワークフローです)。XML ファイル内のすべてを選択します。次の 4 つの画面に示す手順を実行します。



DeploymentManager - Import

Substitutions

Provide the substitutions for the users/groups (Optional).

Type	Current Name	Value
UD_ADUSRC	Current Uname	UewUame
UDJPNT_GRP	version 9	
Version	InitialVersion	
UD_ADUSER Version	Version 12	
User	KELSYSADM	
User Group	SYSTEM ADMINISTRATORS	
UDJPNT_USR Version	Version 2	
User Group	OPERATORS	
UD_IPNT_ROL Version	InitialVersion	
All		

Select next

DeploymentManager

Provide IT Resource Instance Data.

OPM Constants Resource	VGO PM Constants	
VGO PM Constants	Parameter Name Parameter Value	
<<New Instance>>	ROOT_RESOURCE_NAME	<input type="text"/>
LDAP Server	RootITResource_ProcessFormVariable	<input type="text"/>
iPlanet User	RootUserID_ProcessFormVariable	<input type="text"/>
<<New Instance>>	servicePassword	<input type="text"/>
Remote Manager	VGoEnabled_Resources	<input type="text"/>
<<New Instance>>	ROOT_RESOURCE_OBJECT_NAME	<input type="text"/>
ADServer	serviceUserName	<input type="text"/>
<<New Instance>>		

Select next

Deployment Manager

Provide IT Resource Instance Data.

OPM Constant Resource VGO PM Constants <<New Instance>> LDAP Server iPlanet User <<New Instance>> Remote Manager <<New Instance>> ADServer <<New Instance>>	Provide the name of the IT resource instance to be created. Instance Name: <input type="text"/> Parameter Name Parameter Value ROOT_RESOURCE_NAME RootITResource_ProcessFormVariable servicePassword RootUserID_ProcessFormVariable VGoEnabled_Resources ROOT_RESOURCE_OBJECT_NAME serviceUserName
--	---

Skip this new instance for all the other It Resources

Deployment Manager

Provide IT Resource Instance Data.

AD Server > AD Server 2003 AD Server One << New Instance>> VGO PM Constant Resource VGO PM Constants << New Instance>> LDAP Server iPlanet User << New Instance>>	AD Server 2003 Parameter Name Parameter Value Server Address ADGroup LookUp Definition Use SSL Last Modified Time Stamp Admin FQDN AtMap Group AtMap ADUser Admin Login Root Context Admin Password
--	--

Creating a new instance is optional
If required create or skip the new instance option

AD Server 2003 またはAD Server Oneの値の入力

これは、リポジトリ用に Oracle に接続されているリソースです。これらは値の例です。

IT Resources Information		
Name	AD Server 2003	
Type	AD Server	Remote Manager
<input checked="" type="radio"/> Parameters <input type="radio"/> Administrators		
	Name	Value
1	ADGroup LookUp Definition	Lookup.ADReconciliation.GroupLookup
2	Admin FQDN	administrator@plogix.com
3	Admin Login	plogix\administrator
4	Admin Password	*****
5	AtMap ADUser	AtMap.AD
6	AtMap Group	AtMap.ADGroup
7	Last Modified Time Stamp	0
8	Last Modified Time Stamp Group	0
9	Root Context	dc=plogix,dc=com
10	SSL Port Number	636
11	Server Address	192.168.1.224
12	Use SSL	true

ADに対するSSLの有効化

資格証明は AD サーバーから、OIM JVM(JBoss が確実にユーザーを正常に作成するために使用)にインポートする必要があります。

SSL の構成の項のアクティブ・ディレクトリの OIM コネクタ・ガイドに示されているように、標準的な手順に従って、AD 資格証明を特定システムの AD からインポートします。

コマンド・プロンプトのコマンド例を次に示します。

```
keytool -import -alias passcert -file ActiveDir.cer -keystore
C:\j2sdk1.4.2_15\jre\lib\security -storepass changeit
```

資格証明をインポートした後に、マシンを再起動して JVM が新しい資格証明を持つようにします。次に、OIM サーバーを再起動します。

VGO定数リソースへの値の追加

ルート・リソースを次のように構成します。

ROOT_RESOURCE_NAME	AD Server 2003
ROOT_RESOURCE_OBJECT_NAME	AD User
RootITResource_ProcessFormVariable	UD_ADUSER_AD
RootUserID_ProcessFormVariable	UD_ADUSER_UID

ROOT_RESOURCE_NAME	AD Server 2003
serviceUserName	Vgo インストールのとおり
servicePassword	Vgo インストールのとおり

新しいADユーザーの作成のテスト・ケース

- 新しいOIMユーザーを作成します。
- それに、ADサーバー・リソース・オブジェクトを追加します。値が事前に入力された状態で、プロセス・フォームが表示されます。

Provision Resource to User
You are provisioning to pass102 pass102 [PASS102].

1 2 3 4 5 6

Step 5: Provide Process Data

AD User Form

Prepopulate

* Indicates required field

AD Server	*	<input type="text"/>	<input type="button" value="Clear"/>
User ID	*	<input type="text" value="PASS102"/>	
Password	*	<input type="text"/>	
First Name		<input type="text" value="pass102"/>	
Middle Name		<input type="text"/>	
Last Name		<input type="text" value="pass102"/>	
Full Name		<input type="text" value="pass102pass102"/>	
User must change password at next logon	<input type="checkbox"/>		
Password never expires	<input checked="" type="checkbox"/>		
Account Expiration Date	<input type="text"/>	<input type="button" value="Calendar"/>	<input type="button" value="Clear"/>
Organization Name	<input type="text"/>	<input type="button" value="Clear"/>	

Buttons:

- AD Server Lookupを選択し、AD Server 2003を選択します(「AD Server 2003またはAD Server Oneの値の入力」でのITリソースの値が入力されています)
 - パスワードには厳密なポリシーがあります。厳密なポリシーに準拠したパスワードを使用するようしてください。準拠していない場合はAdd User Creationが失敗します。
 - 「AD Server 2003」が Provisioning Gateway 側にテンプレートとして存在することを確認してください。存在しない場合、Oracleコードが失敗します。
 - このタスクの完了時に、ユーザーが ADサーバーに作成されます。このユーザーは検証可能で、資格証明は Oracleに追加されます。

User Name	Logons	Instructions
+ ADUSER3	-	<input checked="" type="checkbox"/> ADD "AD Server 2003"
+ batman3	-	
+ gagag	-	<input checked="" type="checkbox"/> DELETE "AD Server 2003"
+ jack1 jack1	-	<input checked="" type="checkbox"/> ADD "Tomcat" <input checked="" type="checkbox"/> DELETE "Tomcat" <input checked="" type="checkbox"/> DELETE "Tomcat"
+ jack4	-	<input checked="" type="checkbox"/> ADD "AD Server 2003"
+ OIMTEST2234	-	<input checked="" type="checkbox"/> ADD "AD Server 2003"
+ OIMUSER1hdfs	-	<input checked="" type="checkbox"/> ADD "AD Server 2003"
+ PASS102	-	<input checked="" type="checkbox"/> ADD "AD Server 2003"

サーバー・ログが Add User Creation および Add Oracle Credentials をトリガーします。太字のテキストは、プロセスのチェックポイントを示しています。

最初にADユーザーが作成される

```

08/03/07 18:26:29 Running CONCATFIRSTANDMIDDLE
08/03/07 18:26:29 Target Class =
com.thortech.xl.util.adapters.tcUtilStringOperations
08/03/07 18:26:29 Running CONCATLAST
08/03/07 18:26:29 Target Class =
com.thortech.xl.util.adapters.tcUtilStringOperations
08/03/07 18:26:53 Running Get Attribute Map
08/03/07 18:26:53 Running Get Path
08/03/07 18:26:53 Running Create User
08/03/07 18:26:54 object created: cn=TESTM1023
08/03/07 18:26:56 Running Get Path
08/03/07 18:26:56 Running GETRDN

08/03/07 18:26:56 Target Class =
com.thortech.xl.util.adapters.tcUtilStringOperations
08/03/07 18:26:56 Running Get User ObjectGUID
08/03/07 18:27:00 Running GETADPROCESSFORMDATA
08/03/07 18:27:00 Running GETADITRESOURCEKEY
08/03/07 18:27:00 Running MAPCRITERIAFORADITRESOURCE
08/03/07 18:27:00 Target Class =
com.thortech.xl.util.adapters.tcUtilHashTableOperations
08/03/07 18:27:00 Running GETADITRESOURCEINSTANCES
08/03/07 18:27:01 Running GETADITRESOURCENAME

```

次にOracle用の資格証明が追加される

```

08/03/07 18:27:01 Running ADDPASSLOGIXCREDENTIAL1
08/03/07 18:27:01 Target Class =
com.passlogix.integration.provision.OIM.OIMInterface
08/03/07 18:27:01 Command Invoker class is
com.passlogix.integration.provision.client.apicommand.APICommandInvoker

```

```
08/03/07 18:27:01 Trying to start reading the component classes
08/03/07 18:27:01 Read the component class name as
com.passlogix.integration.provision.client.apicommand.APICommandAddCredCommand
08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandAddCredCommand
08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandAddCredCommand
08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandAddCredCommand
08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
AddCredCommand
08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandAddCredCommand
08/03/07 18:27:01 Read the component for 1 as
com.passlogix.integration.provision.client.apicommand.APICommandCancel
08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandCancel
08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandCancel
08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandCancel
08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
Cancel
08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandCancel
08/03/07 18:27:01 Read the component for 2 as
com.passlogix.integration.provision.client.apicommand.APICommandDelCredCommand
08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandDelCredCommand
08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandDelCredCommand
08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandDelCredCommand
08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
DelCredCommand
08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandDelCredCommand
08/03/07 18:27:01 Read the component for 3 as
com.passlogix.integration.provision.client.apicommand.APICommandDelUserCommand
08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandDelUserCommand
```

```
08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandDelUserCommand

08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandDelUserCommand

08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
DelUserCommand

08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandDelUserCommand

08/03/07 18:27:01 Read the component for 4 as
com.passlogix.integration.provision.client.apicommand.APICommandModCredCommand

08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandModCredCommand

08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandModCredCommand

08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandModCredCommand

08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
ModCredCommand

08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandModCredCommand

08/03/07 18:27:01 Read the component for 5 as
com.passlogix.integration.provision.client.apicommand.APICommandStatus

08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandStatus

08/03/07 18:27:01 Initializing APICommand
com.passlogix.integration.provision.client.apicommand.APICommandStatus

08/03/07 18:27:01 Set up APICommand
com.passlogix.integration.provision.client.apicommand.APICommandStatus

08/03/07 18:27:01 Starting
APICommandcom.passlogix.integration.provision.client.apicommand.APICommand
Status

08/03/07 18:27:01 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandStatus

08/03/07 18:27:01 Read the component for 6 as
com.passlogix.integration.provision.client.apicommand.APICommandInvoker

08/03/07 18:27:01 Created an instance of
com.passlogix.integration.provision.client.apicommand.APICommandInvoker

08/03/07 18:27:01 Initialized the
com.passlogix.integration.provision.client.apicommand.APICommandInvoker
```

日付がコマンドとしてOracle APIに渡される

```
08/03/07 18:27:01 Initializing APICommandInvoker with params service
URL : http://192.168.1.224:82/v-GO%20PM%20Service/UP.asmx,service User Name :
plogix\administrator,service user password : <*****>,service client name :
<Provisioning Agent>,<null>
08/03/07 18:27:04 Initialized APICommandInvoker
08/03/07 18:27:04 Setting up
com.passlogix.integration.provision.client.apicommand.APICommandInvoker
08/03/07 18:27:04 Starting the
com.passlogix.integration.provision.client.apicommand.APICommandInvoker
08/03/07 18:27:04 Completed the setup of
com.passlogix.integration.provision.client.apicommand.APICommandInvoker
08/03/07 18:27:04 Command Invoker located as
com.passlogix.integration.provision.client.apicommand.APICommandInvoker
08/03/07 18:27:04 Read the component for 7 as null
08/03/07 18:27:04 The initialization of the Provisioning Manager Client was
successful.
08/03/07 18:27:04 Invoking the command add_credential with parameters
{sso_password=Sena@120, sso_application=AD Server 2003, sso_userid=TESTM1023,
sso_app_userid=TESTM1023}
08/03/07 18:27:04 Invoking APICommandInvoker.
08/03/07 18:27:04 Invoking command add_credential
08/03/07 18:27:04 Populating arguments for command add_credential
08/03/07 18:27:04 Returning 'operation' for command add_credential
08/03/07 18:27:04 No Execution time provided.Default Execution Time set to 'NOW'.
08/03/07 18:27:04 Sending command Instruction to Web Service
08/03/07 18:27:11 Successfully sent command Instruction to Web Service
```

成功を示す文字列がProvisioning Gateway側から戻される

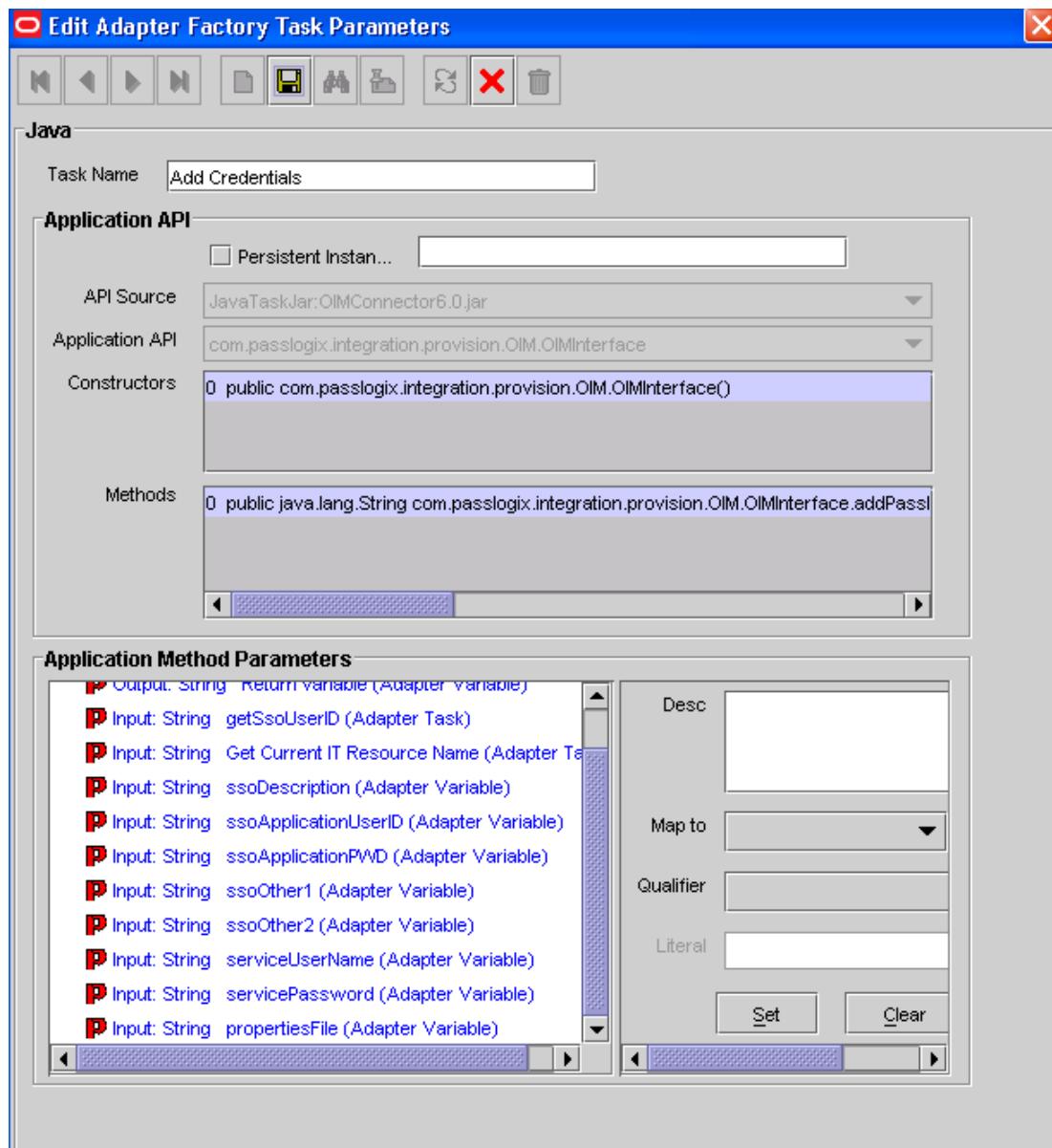
```
08/03/07 18:27:11 Invoked the command add_credential with return 0edc100c-
bba3-4cf2-a74d-335e8fcbabbd
08/03/07 18:27:11 addPasslogixCredential Method Success
```

変数リスト

この項では、Oracle コネクタに渡される様々なアダプタおよび変数について説明します。

Passlogix Add Credentials アダプタ

次の画面は、Passlogix Add Credentials に対するアダプタのマッピングを示しています。同じ変数が渡されるコネクタ内のすべてのメソッドで、同じメソッド・シグネチャが使用されます。



変数とその説明を次に示します。これらの変数は、Provisioning Gateway と通信するためにコネクタに渡されます。

名前	変数の説明 (OIM)	Oracle側	コメント
ssoUserID	Oracle リポジトリ内の新しいユーザーのユーザーID。		同じユーザーIDが、Oracle が中央リポジトリとして使用している Active Directory に存在する必要があります。Identity Manager は、このユーザーをそれぞれのリポジトリに最初にプロビジョニングし、その後 Oracle への資格証明の追加を試行するようにする必要があります。
ssoDescription	使用する SSO の名前。		
ssoApplicationUserID	既存のアプリケーション・テンプレート用の新しいユーザーID。		
ssoOther1	テンプレート用の他の必須フィールド。		
ssoOther2	テンプレート用の他の必須フィールド。		
ssoApplicationPWD	新しいアプリケーション・テンプレート用の新しいパスワード。		
serviceUserName	サービス・ユーザー名は、Provisioning Gateway クライアントへの管理ログインに使用されます。		
servicePassword	サービス・パスワードは、Provisioning Gateway クライアントへの管理ログインに使用されます。		
propertyfile	PMClientConfiguration.properties ファイルのパス取得用の変数。		

付録

adpPasslogixChangePassword アダプタからアダプタ・タスクを削除するには、次の手順を実行します。

1. OIM デザイン・コンソールを開きます。
2. 「Development Tools」 → 「Adapters Factory」に移動します。
3. Passlogix Change Password アダプタを開き、「printdata」および「printset」タスクを図 1 に示すように削除します。

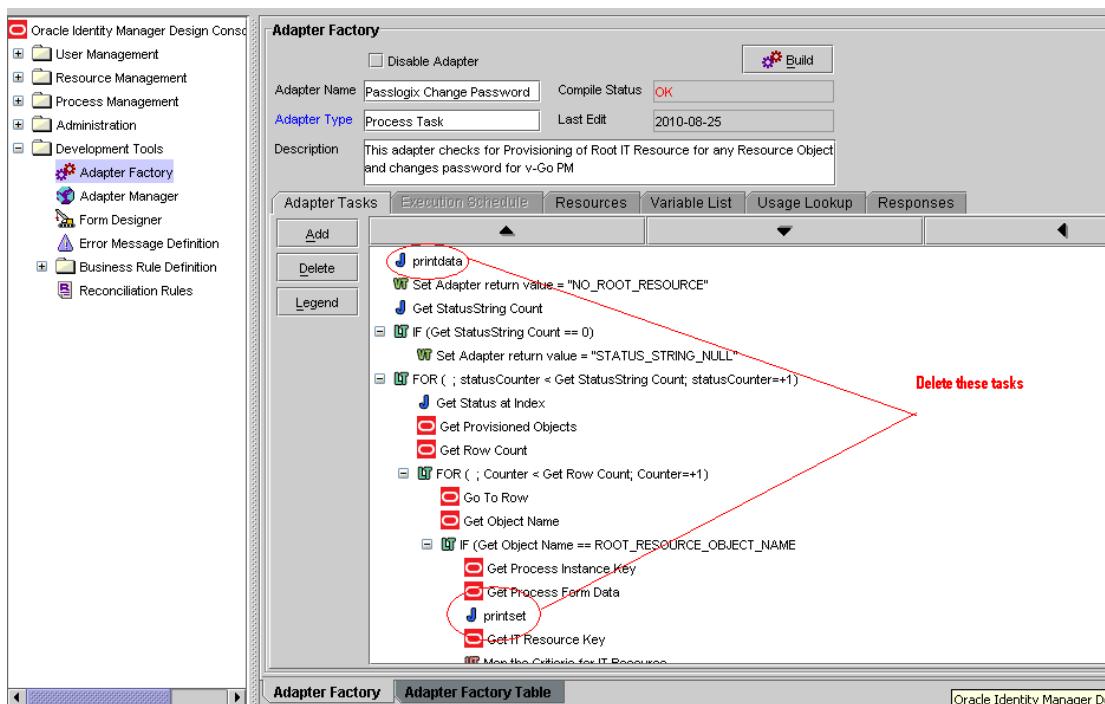


図 1

4. 図 2 に示すように、「Build」ボタンを使用してアダプタを再コンパイルします。

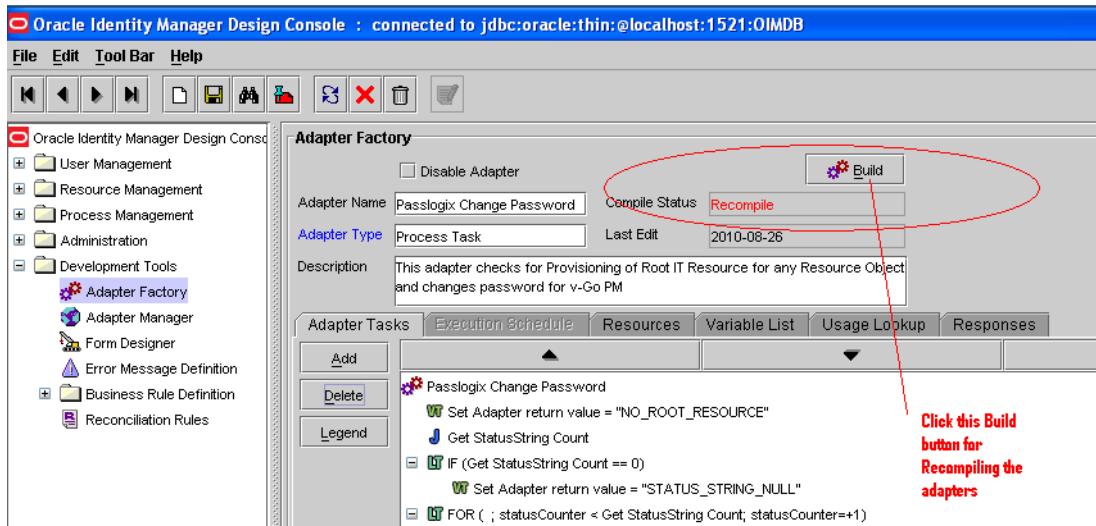


図 2