CA Identity Manager

リリース ノート

r12

本書及び関連するソフトウェア ヘルプ プログラム（以下「本書」と総称）は、ユーザへの情報提供のみを目的とし、CA はその内容を予告なく変更、撤回することがあります。

CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。本書は、CA または CA Inc. が権利を有する秘密情報でかつ財産的価値のある情報で、アメリカ合衆国及び日本国の著作権法並びに国際条約により保護されています。

上記にかかわらず、ライセンスを受けたユーザは、社内で使用する場合に限り本書の合理的な範囲内の部数のコピーを作成でき、またバックアップおよび災害復旧目的に限り合理的な範囲内で関連するソフトウェアのコピーを一部作成できます。ただし CA のすべての著作権表示およびその説明を各コピーに添付することを条件とします。

ユーザの認可を受け、プロダクトのライセンス条項を遵守する、従業員、法律顧問、および代理人のみがかかるコピーを利用することを許可されます。

本書のコピーを印刷し、関連するソフトウェアのコピーを作成する上記の権利は、プロダクトに適用されるライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、そのライセンスが終了した場合には、ユーザは CA に本書の全部または一部を複製したコピーを CA に返却したか、または破棄したことを文書で証明する責任を負います。

該当するライセンス契約書に記載されている場合を除き、準拠法により認められる限り、CA は本書を現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対する不侵害についての黙示の保証を含むいかなる保証もしません。また、本書の使用が直接または間接に起因し、逸失利益、業務の中断、営業権の喪失、情報の損失等いかなる損害が発生しても、CA はユーザまたは第三者に対し責任を負いません。CA がかかる損害について明示に通告されていた場合も同様とします。

本書及び本書に記載されたプロダクトは、該当するエンドユーザ ライセンス契約書に従い使用されるものです。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212, 52.227-14 及び 52.227-19(c)(1)及び(2)、及び、DFARS Section252.227-7014(b)(3)または、これらの後継の条項に規定される該当する制限に従うものとします。

本書に記載された全ての商標、商号、サービスマークおよびロゴは、それぞれの各社に帰属します。

Copyright © 2008 CA. All rights reserved.

CA 製品リファレンス

このドキュメントは、以下の CA 製品を参照しています。

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center（SCC）
- CA Audit
- eTrust® Directory（別名 CA Directory）

テクニカル サポートの連絡先

オンライン テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト(http://www.ca.com/jp/support/)を参照してください。

目次

第 1 章: ようこそ 9

第 2 章: 新機能 11

サポートされるプラットフォームおよびバージョン 11
Identity Manager のアーキテクチャ 12
インストーラの改善 13
レポートの拡張機能 14
接続の管理 16
プロビジョニングの拡張機能 16
DYN GUI 17
テクニカル プレビューとしてリリースされた Lotus Notes/Domino Connector 18
強化されたステータス レポート 18
サブミット済みタスクの表示の改善 18
ユーザ アクティビティの表示タスク 19
[ユーザ履歴]タブ 19
ワークフローの拡張機能 19
ワークフロー プロセス テンプレート 20
タスク レベルのワークフロー 20
ワークフロー アクション ボタン 20
オンライン リクエストおよび履歴 20
タスクのスケジューリング 21
ユーザ コンソールの拡張機能 21
カスタム ヘルプ 21
ネスト タスク 21
タブ コントローラ 22
タスク リスト 23
[プロファイル]タブの拡張機能 24
ロールのユーザ定義のカスタム属性 27
Bulk Loader 27
ユーザに基づいたデフォルトの組織検索 27
IPv6 サポート 28
FIPS 140-2 30

ローカライゼーション サポートの強化 30

第 3 章: 既存の機能の変更 31

非推奨のサーブレット フィルタ エージェント 31
管理コンソールの拡張機能 31
パスワード ポリシーの変更 32
非推奨の IMRExport ツール 32
z/OS コネクタのアーキテクチャの変更 33
サポートが終了した機能 33

第 4 章: システム要件 35

第 5 章: インストールに関する考慮事項 37

サポート マトリックスの場所 37
必要な Solaris のパッチ 38
SiteMinder の統合に必要な環境変数 38
ローカライズされた Identity Manager 環境のインストール 39
英語以外のシステムで ASCII 以外の文字を使用すると、インストールに失敗します 40
SiteMinder FIPS 140-2 専用モードに必要な設定の変更 40
JBoss: IPv6 サポートの設定 41
FIPS 140-2 の SPML サポート 41
z/OS コネクタのアーキテクチャの変更 42
eTrust Directory の場所 43
eTrust Directory をアンインストールする前に修正が必要です 43

第 6 章: 既知の問題 45

全般 45
- Identity Manager EAR が WebLogic では自動展開されません 45
- ワークフローおよび承認者としてのグループ メンバ 45
- 新しい Workpoint Properties を設定する必要がある可能性があります 46
- ロジカル アトリビュート ハンドラのコピーを作成できない 47
- ロール ポリシーのグループ フィルタの使用 47
- ロールおよびタスクの検索画面の設定 49
- Firefox ブラウザでの Identity Manager 環境の作成 49

アップグレード 49
- MS SQL および Oracle エンドポイントは、eTrust Admin 8.1 SP2 からのアップグレード後は使用できません 50

Solaris x86（Intel）プラットフォームで UNIX リモート エージェントを使用できない 50
Z/OS コネクタのアーキテクチャの変更 50
レポート 51
レポートの制限 51
Satisfy=All が XML ファイルで正しく機能しない 51
［マイ レポートの表示］タスクで Cookie を有効にする 52
ExportALL.xml および組織をサポートしていない環境 52
プロビジョニング 52
全般 53
コネクタ 58

第 7 章: ドキュメント 69

ブックシェルフ 70
オンライン ヘルプの拡張機能 71
eTrust の CA への商標変更 72
プロビジョニング用語の変更 72
Embedded IAM（EIAM）コネクタの新しい名前 72
プログラミング マニュアル 73

第 1 章: ようこそ

このドキュメントには、オペレーティング システムのサポート、製品のインストールに関する考慮事項、既知の問題、および CA テクニカル サポートへの問い合わせに関する情報が含まれています。

第 2 章: 新機能

このセクションは、以下のトピックから構成されます。

サポートされるプラットフォームおよびバージョン (11 ページ)
Identity Manager のアーキテクチャ (12 ページ)
インストーラの改善 (13 ページ)
レポートの拡張機能 (14 ページ)
接続の管理 (16 ページ)
プロビジョニングの拡張機能 (16 ページ)
テクニカル プレビューとしてリリースされた Lotus Notes/Domino Connector (18 ページ)
強化されたステータス レポート (18 ページ)
ワークフローの拡張機能 (19 ページ)
オンライン リクエストおよび履歴 (20 ページ)
タスクのスケジューリング (21 ページ)
ユーザ コンソールの拡張機能 (21 ページ)
ロールのユーザ定義のカスタム属性 (27 ページ)
Bulk Loader (27 ページ)
ユーザに基づいたデフォルトの組織検索 (27 ページ)
IPv6 サポート (28 ページ)
FIPS 140-2 (30 ページ)
ローカライゼーション サポートの強化 (30 ページ)

サポートされるプラットフォームおよびバージョン

Identity Manager r12 では、サポートされるアプリケーション サーバ バージョン、ディレクトリ、およびデータベースがいくつか追加されました。

注: サポートされているプラットフォームとバージョンの詳細については、Identity Manager サポート サイト http://ca.com/supportにある Identity Manager のサポート マトリックスを参照してください。

Identity Manager のアーキテクチャ

Identity Manager r12 のアーキテクチャには、以下の旧バージョンからの変更が含まれます。

- 組み込みプロビジョニング サーバおよびプロビジョニング マネージャ

  プロビジョニング サーバは、Identity Manager のユーザに割り当てられる追加アカウントを管理するサーバです。 Identity Manager のユーザにプロビジョニング ロールを割り当てると、プロビジョニング サーバはロールの要件を満たすアカウントをエンドポイントに作成します。 たとえば、Exchange アカウントのテンプレートを含むプロビジョニング ロールを割り当てる場合、プロビジョニング サーバは、Exchange アカウントをユーザに割り当てます。

  プロビジョニング マネージャは、Exchange または Oracle のようなエンドポイントタイプ、および Exchange がインストールされている特定システムのようなエンドポイントを管理するためのユーザ インターフェースです。 このインターフェースは、以前 eTrust Admin マネージャと呼ばれていました。 プロビジョニング マネージャには、アカウントの検索および関連付けなどのその他の機能があります。ただし、これらの追加機能は Identity Manager のユーザ コンソールに複製されており、簡単なアクセスが可能となっています。

  Identity Manager の旧バージョンでは、プロビジョニングに eTrust Admin を必要としました。

  注: プロビジョニング サーバおよびプロビジョニング マネージャは、オプション コンポーネントです。

- Identity Manager の SiteMinder との統合

  SiteMinder は、Identity Manager のインストールの前提条件ではなくなりました。オプションで SiteMinder と統合し、SiteMinder 認証および詳細なパスワード ポリシーを含む、高度な機能を提供できます。

  Identity Manager の旧バージョンでは、以下の機能に SiteMinder を必要としました。

  - 認証
  - ロール情報およびタスク情報の（ポリシー ストア内への）格納
  - ユーザ ストアへの接続
  - パスワード ポリシー

  Identity Manager では、この機能はネイティブで提供されます。

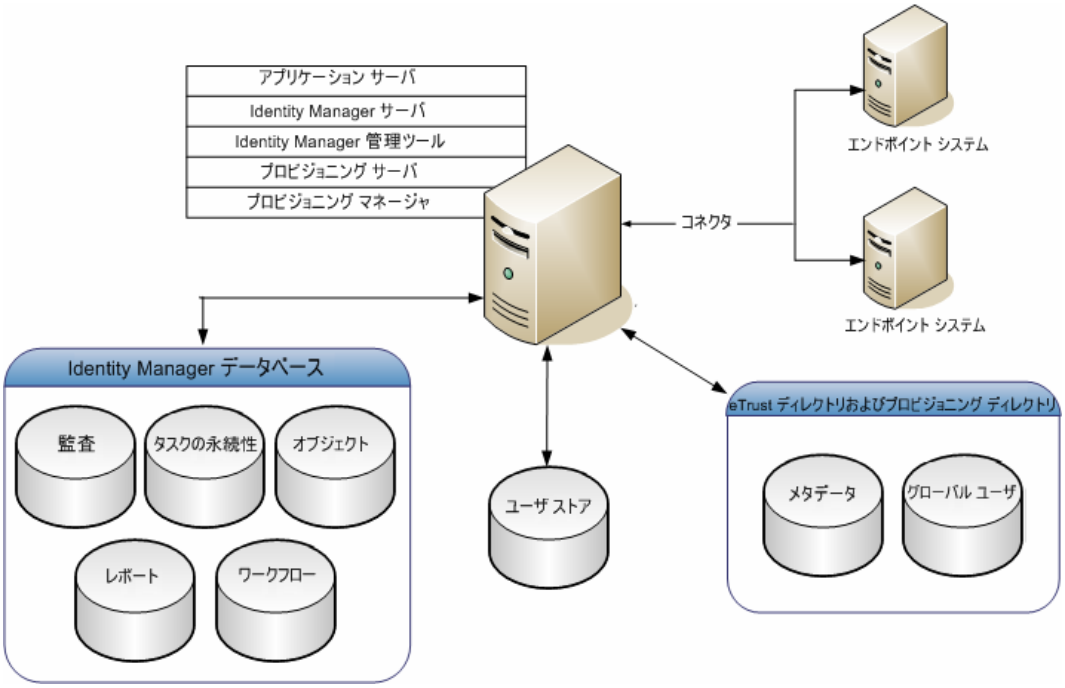
  注: SiteMinder と統合し、SiteMinder 認証および詳細なパスワード ポリシーを含む、高度な機能を提供できます。

- オブジェクト ストア

  Identity Manager r12 では、ロール情報およびタスク情報を新しいオブジェクト ストアに格納するようになりました。 オブジェクト ストアは、実行時に Identity Manager によって自動的に設定されるリレーショナル データベースです。

以下の図は、プロビジョニングを含む Identity Manager 実装を表しています。

注: プロビジョニング ディレクトリは、プロビジョニングを使用するのに必要な情報、およびグローバル ユーザについての情報を格納します。プロビジョニング付き Identity Manager のインストールの前提条件として、このディレクトリは、eTrust Directory にインストールしておく必要があります。



インストーラの改善

Identity Manager サーバのインストールに必要なすべてのコンポーネントは、1 つのインストーラでインストールされるようになりました。これには、プロビジョニング用コンポーネントおよび SiteMinder ポリシー サーバ用拡張が含まれます。

Identity Manager インストーラには、Identity Manager プロビジョニング サーバ、プロビジョニング ディレクトリ、およびプロビジョニング マネージャが用意されています。 さらに、オブジェクト データおよびワークフローのデータを格納するデータベースへの接続、タスクの永続性、レポート、および監査も設定します。

Identity Manager インストールには、以下の変更が含まれます。

- Identity Manager では、認証に SiteMinder は必要ありません。
- タスクの永続性はオプションではなくなり、インストール時に有効になります。
- データベース スキーマは、Identity Manager で使用される各データベース用に自動的に拡張されます。
- 管理ツールは、以下の場所にインストールされます。
  - Windows の場合： C:¥Program Files¥CA¥IAM Suite¥Identity Manager¥tools
  - UNIX の場合： HOME/CA/IAM_Suite/Identity_Manager/tools
- インストール後のスクリプトは必要ありません。

レポートの拡張機能

Identity Manager レポートでは、Identity Manager 環境の現在の状態を確認できます。この情報を使って、内部のビジネス ポリシーや外部規制との準拠を確保できます。

Identity Manager r12 では、レポートの機能が拡張されました。

- IAM レポート サーバとの統合

  Identity Manager r12 は、Business Objects Enterprise XI を使用して、レポート データベースからレポートを設計、管理、および表示します。 Identity Manager は、Business Objects のランタイム版を提供するので、個別のライセンスは必要ありません。

- データをレポート データベースへエクスポートするための新しい管理タスク

  Identity Manager には、Identity Manager からデータをレポート データベースにエクスポートできる、新しいデフォルト タスクが用意されています。 データをレポート データベースにエクスポートするたびに、Identity Manager 環境にユーザ固有のオブジェクトの現在の状態を表示するスナップショットを作成します。

  新しいデフォルト タスクを使用すると、スナップショット定義を作成し、スナップショットを取得して、そこからレポートを生成できます。

- その他の定義済みレポート

  Identity Manager には、以下の定義済みレポートが用意されています。これらのレポートは、ビジネス ニーズに合うようにインストールまたはカスタマイズして使用できます。

  - エンドポイント アカウント

    エンドポイントごとのアカウント名、所有者、および作成日時を基準にするアカウントのリストであり、エンドポイント タイプ別に並べられます。

  - 非標準アカウント

    孤立アカウント、システム アカウントなどの非標準アカウントのリスト

  - 非標準アカウントの傾向

    グラフとして表示された非標準アカウント タイプ別の非標準アカウントの傾向

  - 孤立アカウント

    ユーザに関連付けられていないアカウントのリスト 孤立アカウントは、エンドポイントごとにアカウント名、所有者、および作成時日時を基準に示され、エンドポイント タイプ別に並べられます。

  - ポリシー

    ポリシー条件、ポリシー適用時のアクション、およびポリシー削除時のアクションを含む、ポリシーのリスト

  - ロール管理者

    ロール管理者のリスト

  - ロール メンバ

    ロール メンバのリスト

  - ロール所有者

    ロール所有者のリスト

  - ロール

    ロールおよびその説明のリスト

  - スナップショット

    レポート データベースで使用可能なすべてのスナップショットのリスト

  - タスク ロール

    説明、カテゴリ、およびタイプ別のタスクのリスト 各タスクに対して、関連付けられているすべてのロールを指定します。

- ユーザ アカウント

  ユーザ別のアカウントのリスト ユーザ アカウントは、アカウント名、アカウント属性、およびエンドポイントを基準に示され、エンドポイント タイプ別に並べられます。

- ユーザ ポリシー同期ステータス

  現在割り当てられているポリシーおよび再割り当てされる必要のあるポリシーを含むユーザのリスト

- ユーザのプロファイル

  ユーザおよびそのユーザに関する使用可能なすべての情報のリスト

- ユーザ権限

  ユーザ、およびそのユーザに関連付けられたアカウント、ロール、グループのリスト

接続の管理

[接続の管理]は、Identity Manager 内で、データベース サーバ接続の詳細設定に使用されます。 Identity Manager をデータベース サーバに接続する必要がある場合は、[接続]の詳細を使用してデータベース サーバに接続します。 [接続の管理]では、1 つの接続のタイプで異なるデータベース サーバへの複数の接続を作成できます。 各接続タイプに対してデフォルトの接続を指定できます。 管理コンソールを使用して Identity Manager のプライマリの接続タイプを設定する必要があります。

プロビジョニングの拡張機能

このリリースでは、Identity Manager のユーザ コンソールでより多くのアクションを実行できます。 これらの機能の中には、以前 eTrust Admin マネージャで使用可能であったものもあります。 ユーザ コンソールは、以下の目的で使用できます。

- エンドポイントのアカウントの検索および関連付け
- 孤立アカウントおよびシステム アカウントの Identity Manager のユーザとの関連付け
- グローバル ユーザへのプロビジョニング ロールの割り当てのような、プロビジョニング アクションの監査

さらに、このリリースに含まれるものは以下のとおりです。

- カスタム コネクタを作成するためのグラフィカル ツールである「Connector Xpress」

- Connector Xpress から生成された XML メタデータでの使用をサポートする動的コネクタ（JNDI および JDBC）
- Java コネクタからのリクエストを処理するサーバである Java コネクタ サーバ
- 以前 Super Agent と呼ばれていた C++ コネクタ サーバに対する高可用性を備えています。
- Solaris サーバの Kerberos プリンシパルおよび Kerberos パスワード ポリシーを管理する、Kerberos 用の新しい Java コネクタ
- SAP 用の新しい Java コネクタ（CUA サポート）
- Java コネクタ サーバで提供される、Oracle、Microsoft SQL、および OS/400 用の新しい Java コネクタ

  この 3 つのコネクタは、現在はサポートされていないサンプル オプションを置き換えます。
- Connector Xpress を使用して作成された、動的 JDBC および JNDI エンドポイント タイプに汎用 UI を提供するプロビジョニング マネージャに対する拡張機能

DYN GUI

プロビジョニング マネージャの DYN GUI を強化して、単一のプロビジョニング マネージャ プラグインで任意のエンドポイント オブジェクトを操作できる機能の拡張セットを提供します。

たとえば、Connector Xpress のフィールドをマップする場合、アイテムはそのフィールドを表すメタデータに配置されます。このコネクタのいずれかのオブジェクトを検査する場合は、DYN GUI では常に適切なフィールドを表示するメタデータが使用されます。

このリリースでの変更により、機能の拡張セットが追加され、DYN GUI の機能が拡張されています。そのため、今後追加される新しい機能はより簡単になり、ユーザに対する表示も見やすくなります。

テクニカル プレビューとしてリリースされた Lotus Notes/Domino Connector

r12 リリースの Identity Manager の場合、Java ベースの LND Connector はテクニカル プレビューとしてのみリリースされています。

このコネクタは、本稼働環境では検証されていません。 完全に検証済みのコネクタは CR リリースで提供される予定です。 詳細については、CA ジャパン ダイレクトまでお問い合わせください。

注: C++ LND Connectorと Java LND Connector を同じ Identity Manager 環境にインストールしないでください。

強化されたステータス レポート

Identity Manager r12 には、Identity Manager タスクのステータスを表示できる、いくつかの機能が含まれています。

サブミット済みタスクの表示の改善

Identity Manager r12 には、タスクのステータス、他のタスク、イベント、およびワークフロー上でのタスクの依存関係を表示する[サブミット済みタスクの表示]タブが用意されています。

Identity Manager r12 では、[サブミット済みタスクの表示]タブに、以下の拡張機能が追加されています。

- [サブミット済みタスクの表示]タブでは、タスクとそのタスクに関連するイベントについてより詳細に表示されるようになりました。
- [サブミット済みタスクの表示]タブから、保留中のタスクをキャンセル、および失敗したタスクを再度サブミットまたは拒否することができます。
- [サブミット済みタスクの表示]タブを設定できます。

ユーザ アクティビティの表示タスク

ユーザ アクティビティとは、ある特定のユーザに関するタスクの履歴です。 管理者は「ユーザ アクティビティの表示」タスクを使用して、以下のユーザ情報を追跡できます。

- ユーザに対して実行されるタスク
- ユーザによって実行されるタスク
- ユーザが実行するワークフローの承認

ユーザ アクティビティの表示方法

1. [ユーザ]-[ユーザ管理]-[ユーザ アクティビティの表示]をクリックします。

   [ユーザ選択]画面が表示されます。

2. ユーザを検索して[選択]をクリックします。

   [ユーザ アクティビティの表示]画面が表示されます。

   表示されたユーザ アクティビティの詳細については、ユーザ コンソールのオンライン ヘルプを参照してください。

[ユーザ履歴]タブ

[ユーザ履歴]タブでは、特定のユーザに関連するタスクを表示できます。 このタブを、[ユーザの変更]タスクまたは[ユーザの表示]タスクに追加できます。

注: このタブは、デフォルトの[ユーザ アクティビティの表示]タスクに含まれています。

このタブに表示されるタスク詳細は、[サブミット済みタスクの表示]タブでも表示できます。

ワークフローの拡張機能

Identity Manager r12 には、ワークフロー機能への拡張が含まれています。この拡張により、ワークフロー作成プロセスが簡略化され、新しい機能が追加されます。 以下のセクションでは、これらの拡張機能について説明します。

ワークフロー プロセス テンプレート

ワークフロー プロセス テンプレートでは、Identity Manager のユーザ コンソール内から全体のワークフロー制御を設定および管理できます。 この一般的なプロセス テンプレートを設定すると、ほとんどの Identity Manager のタスクとイベントを制御できます。

新しいプロセス テンプレートで、タスク レベルおよびイベント レベルでのワークフロー制御、承認者に対するより簡単な参加者リゾルバの設定、および複数手順の承認プロセスが可能になります。

承認されるタスクまたはイベントの属性によって、承認者のリストを実行時に動的に決定することも可能です。

タスク レベルのワークフロー

ワークフロー プロセスを、タスクおよびイベントの両方に関連付けることができます。 これは、参加者が Identity Manager のタスク全体、またはタスク内の特定のイベントのいずれかを承認または拒否できることを意味します。

タスク レベルのワークフローでは、承認者がリクエストの承認または拒否を決定する前にすべてのイベントを確認できます。 ワークフロー プロセスが特定のイベントに関連付けられている場合、承認者は、リクエストが行われたタスク全体の状況を確認できません。

ワークフロー アクション ボタン

新しいボタンをワークフロー承認タスクに追加して、標準の承認ボタンおよび拒否ボタンを補完または置換できます。 この機能の例としては、オンライン リクエスト タスクで示されるものが挙げられます。

オンライン リクエストおよび履歴

ユーザ コンソールでは、ユーザが自分のアカウントへの変更をリクエストし、管理者はユーザ アカウントへの変更をリクエストすることができます。 このタスクは、3 人までの承認者を必要とするワークフロー プロセス テンプレートをトリガします。承認者には、リクエストにコメントを作成するコンサルタント、リクエストを承認するビジネス ユーザ、リクエストを実装する技術者などが考えられます。

オンライン リクエスト タスクには、完了までのさまざまな段階で注意またはコメントをタスクに関連付けることができる、新しい履歴の制御も組み込まれています。

タスクのスケジューリング

スケジューリングで、今後の日付を指定してタスクの実行を自動化できます。 ワークフロー プロセスに関連付けられたタスクをスケジュールする場合は、Identity Manager はプロセスで定義されたタスクをすべて実行します。 スケジュール済みタスクのステータスは、[サブミット済みタスクの表示]ページに表示できます。

Identity Manager でまだ実行されていないスケジュール済みタスクは、[サブミット済みタスクの表示]ページでスケジュール変更またはキャンセルできます。

Identity Manager では、スケジューラが特殊なタブとして用意されています。 スケジューラにアクセスするには、スケジューラ タブでタスクを設定する必要があります。

ユーザ コンソールの拡張機能

Identity Manager r12 には、新しい機能のサポートを追加し、操作を簡単にするための複数の拡張機能が含まれています。 以下のセクションでは、これらの拡張機能について説明します。

カスタム ヘルプ

Identity Manager により、ユーザ コンソールでカスタマイズしたタスクおよびタブに、ユーザ独自のカスタム ヘルプを作成できます。 カスタム ヘルプを実装するために、カスタム HTML ヘルプ ファイルまたは Wiki ページ付き状況依存ヘルプ システムを作成して、Identity Manager ユーザ コンソール内のヘルプのリンクをリダイレクトして、カスタム ヘルプにアクセスできます。

この機能を利用すると、(英語で作成された)デフォルトのヘルプはいずれも他の言語に翻訳できます。

ネスト タスク

ネスト タスクは、別のタスクの[プロファイル]タブから開くことができる管理タスクです。 最初のタスクのユーザは、リンクまたはボタンをクリックしてネスト タスクを開きます。 たとえば、[ユーザの変更]タスクに[ユーザの削除]ボタンを追加できます。 ユーザ アカウントが有効ではなくなった場合、管理者は[ユーザの削除]ボタンをクリックしてアカウントを削除することができるため、ナビゲーション ペインに戻って新しいタスクを選択する必要がありません。

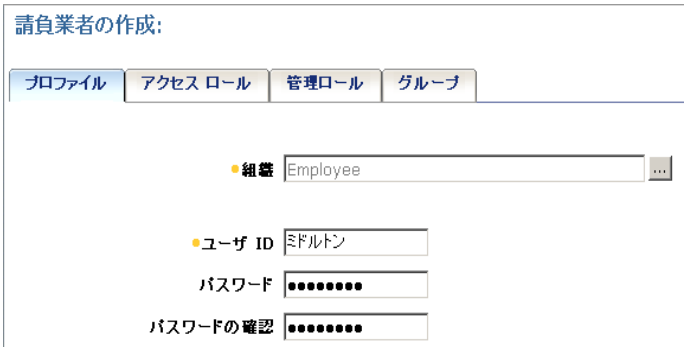
タブ コントローラ

タブ コントローラで、タスク内のタブの表示方法を指定します。 以下のタブ コントローラのいずれかを選択できます。

- 標準タブ コントローラ

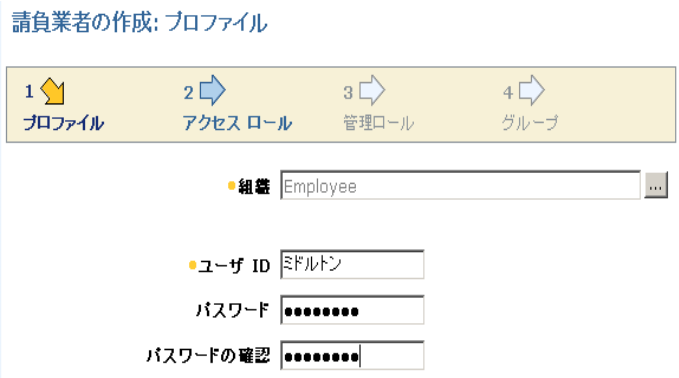
  タスク内のタブを個別のタブとして表示します。 ユーザは、タスク内のタブに任意の順序を指定できます。

  これはデフォルトのタブ コントローラです。



- ウィザード タブ コントローラ

  タスク内のタブをウィザードとして表示します。 管理者は順番に各タブを使用します。

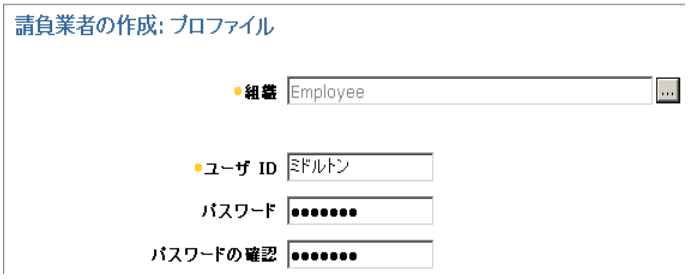


- シーケンス タブ コントローラ

  一度に 1 つのタブを 1 ページとして表示します。 1 つのタブの操作が終わって、カスタムのボタンまたはリンクをクリックすると、次のタブに移動します。

  タブの順序と、表示されるボタンとリンクは、シーケンス タブ コントローラの設定時に記述する JavaScript によって、プログラム的に決まります。

  カスタムの JavaScript で、ユーザ入力に基づいてタブの外観と順序を指定できます。 たとえば、最初のタブでオプションを選択すると、あるページが表示されるようにすることができます。 ユーザが別のオプションを選択すると、別のページが表示されます。



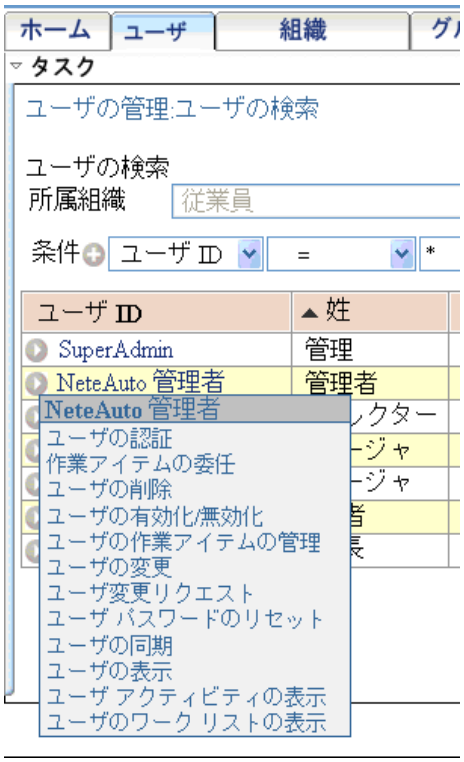
タスク リスト

Identity Manager r12 には、管理するオブジェクトを検索するための、以下の新しいデフォルト タスクが用意されています。

- ユーザの管理
- グループの管理
- 組織の管理
- 管理ロールの管理
- 管理タスクの管理
- アクセス ロールの管理
- アクセス タスクの管理

オブジェクトを選択すると、そのオブジェクトの管理に使用できるタスクの一覧を表示できます。

たとえば、この方法を使用してユーザを変更するには、[ユーザ]カテゴリを選択し、[ユーザの管理]タスクを選択します。 管理するユーザを検索して選択します。 検索結果の中からアイコンをクリックすると、選択したユーザの管理に使用できるタスクのリストが表示されます。 このリストから[ユーザの変更]や他の適切なタスクを選択できます。



また、管理タスク以外のタスクでも、タスク リストを設定できます。 たとえば、[メンバシップ]タブにタスク リストを追加することができます。 この場合、[メンバシップ]タブに表示されるメンバごとにタスク リストを使用できます。

[プロファイル]タブの拡張機能

Identity Manager r12 では、[プロファイル]タブに、新しい機能をサポートする新しい設定が含まれています。 以下のセクションでは、これらの新しい設定について説明します。

タスクのカテゴリ

タスクのカテゴリを使用してタスクを整理すると、User Console で簡単にタスクの場所を特定したり、検索することができるようになります。

以下の 3 つのタスク カテゴリを指定できます。

- カテゴリ 1 は、タスクの最上位のカテゴリです。 このカテゴリは、User Console の上部に並ぶタブとして表示されます。
- カテゴリ 2 は第 2 階層のカテゴリです。 このカテゴリを使用して、第 1 階層カテゴリの関連タスクをグループ化することができます。 第 2 階層カテゴリを指定しない場合、デフォルトのカテゴリは[タスク]です。
- カテゴリ 3 には、管理者が使用するタスクが含まれます。 管理者が User Console でカテゴリ 3 の名前をクリックすると、そのカテゴリのタスク リストが表示されます。

各カテゴリ内では、カテゴリ順を指定して、カテゴリ内のアイテムを表示する順序を制御できます。 たとえば、次の図では、[従業員]タブには 3 というカテゴリ順が指定されています。

注: カテゴリに複数のタスクが含まれる場合、各タスクのプロファイルに指定するカテゴリ順は同じにしてください。 カテゴリ順が異なると、そのカテゴリ タブは複数表示されます。 たとえば、[従業員]カテゴリに[従業員の作成]と[従業員の変更]という 2 つのタスクが含まれるとします。 [従業員の作成]タスクのカテゴリ順が 3 で、[従業員の変更]タスクのカテゴリ順が 6 の場合、[従業員]カテゴリは 2 つのタブに表示されます。

[Task Priority(タスク優先度)]

Identity Manager r12 では、タスク優先度を指定して、Identity Manager が最も緊急のタスクを確実に最初に実行できるようになりました。

タスクの[プロファイル]タブで、タスク優先度を高、中、または低に設定できます。 デフォルトの優先度は中です。

注: ステータスを表示するには、特定の優先度のタスクを検索してから[サブミット済みタスクの表示]を使用します。

セレクト ボックスのカスタム データ

Identity Manager タスク画面上のフィールドを使用して値を選択できます。 以下のフィールドが事前定義されています。

- チェック ボックスの複数選択
- ドロップダウン
- ドロップダウン コンボ
- 複数選択
- オプション セレクタ
- オプション セレクタ コンボ
- ラジオ ボタン 単一選択
- 単一選択

XML ファイルのセレクト ボックスに入力するカスタム データを指定できます。 たとえば、セレクト ボックス データ XML ファイルを使用して、「ユーザの作成」タスクの[プロファイル]タブにある市区町村または州ドロップダウン ボックスのオプションを入力できます。

また、セレクト ボックス データ XML ファイルを使用してタスク画面上の 2 つのフィールドの依存関係を設定することもできます。 たとえば、[市区町村]フィールドに入力可能なオプションを、[州]フィールドでユーザが選択したオプションに依存させることができます。

[Date Picker]コントロール

Identity Manager のユーザ コンソールに、[Date Picker]スタイルが追加されました。このスタイルは、日付を取得して表示する[プロファイル]タブのフィールドに適用できます。

[Date Picker]スタイルが適用されると、カレンダ アイコンが日付フィールドの横に表示されます。 ユーザがカレンダ アイコンをクリックすると、カレンダ コントロールが表示されます。このコントロールでは、目的の日付を選択できます。

バイナリおよび画像コントロール

Identity Manager を設定して、プロファイルに画像を表示したり、バイナリ属性を含めたりすることができます。 たとえば、ユーザ プロファイル画面を設定して、管理しているユーザのデジタル写真を表示したり、ドキュメントをプロファイル画面に関連付けたりできます。

注: この機能は、LDAP ユーザ ストアのみでサポートされます。

ロールのユーザ定義のカスタム属性

Identity Manager は、組織のロールを効率的にフィルタできるユーザ定義のカスタム属性に対応しています。 たとえば、企業環境では 1000 を超えるロールの作成が必要になることがあります。 場合によっては、これらのロールを業務部門別や地域別に分類できます。 特定の地域に固有のロールを検索する場合、カスタム属性を使用して、組織内のロールをフィルタすることができます。

以下のロールについては、タスクの作成、変更、および表示にカスタム属性を使用できます。

- アクセス ロール
- 管理ロール

管理タスクおよび検索画面にカスタム属性を追加するには、以下の手順を実行する必要があります。

1. ロールに定義されている任意の管理タスクにカスタム属性を追加します。
2. カスタム属性でロールの検索画面を設定します。

Bulk Loader

ユーザ コンソールの[Bulk Loader]タブを使用して、同時に多数の管理対象オブジェクトを操作するために使用するフィーダ ファイルをアップロードできます。 たとえば、1000 人のユーザを手動で Identity Manager に作成することも、Bulk Loader を使用して作成することもできます。 Bulk Loader 操作の利点は、多数の管理対象オブジェクトの操作の処理を 1 つの情報(フィーダ)ファイルを使用して自動化できることです。「Bulk Loader」タスクをワークフロー プロセスにマッピングすることもできます。

注: CSV は、フィーダでサポートされるファイル形式ですが、その他のファイル形式用にカスタム フィードを作成できます。

ユーザに基づいたデフォルトの組織検索

ユーザ コンソールを簡略化するため、Identity Manager では、タスクの実行を試みたユーザに基づいて、管理者が[ユーザの作成]タスクにデフォルトの組織を設定することができます。 ユーザが[ユーザの作成]タスクを実行した場合、組織は[ユーザ プロファイルの作成]タブに表示されませんが、ユーザの組織に基づいてデフォルトで設定されます。

ユーザに基づいてデフォルトの組織を設定するには、以下の手順に従います。

1. Identity Manager ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]に進みます。
2. [ユーザの作成]タスクを選択します。
3. [タブ]タブで、[プロファイル]の横にある右方向矢印アイコンをクリックします。
4. [...](省略記号)ボタンをクリックして、編集する画面のリストを表示します。
5. [ユーザ プロファイルの作成]画面を選択し、[編集]をクリックします。
6. 組織を検索して、編集する右方向矢印アイコンをクリックします。

   注: このフィールドは、組織のない環境では表示されません。
7. [スタイル]を[非表示]に設定します。
8. [デフォルトの JavaScript]フィールドに、以下のように入力します。

```
function defaultValue(blthContext)
{
return blthContext.getAdministrator().getOrg(null).getUniqueName();
}
```

9. [適用]をクリックします。

IPv6 サポート

Identity Manager を設定するときに、IPv4 と IPv6 の両方のアドレスを入力できます。

Identity Manager は以下のオペレーティング システムで IPv6 をサポートしています。

- Solaris 8 以上
- Windows XP SP1 以上
- Windows 2003 以上

アプリケーション サーバごとに固有の JDK 要件があります。

- スタンドアロン システムの JBoss アプリケーション サーバの場合、Identity Manager は JDK1.4.2_13 または 1.5（Solaris 上）または JDK1.5（Windows 上）で IPv6 をサポートします。
- JBoss クラスタの場合、Identity Manager r12 のリリース時点では IPv6 で動作する JDK は提供されていません。 IPv6 で動作する JDK がリリースされれば、プラットフォーム サポート マトリックスが更新されます。
- ただし、IPv4/IPv6 スタックを使用する JBoss クラスタの場合、Identity Manager は JDK1.4.2_13 または 1.5（Solaris 上）または JDK1.5（Windows 上）で IPv6 をサポートします。
- WebLogic および WebSphere アプリケーション サーバには IPv6 アドレスをサポートする JDK 1.5 が含まれています。

IPv6 をサポートする環境を設定する前に、以下の点に注意してください。

- Identity Manager で IPv6 アドレスをサポートするには、Identity Manager 実装のすべてのコンポーネント（オペレーティング システム、JDK、ディレクトリ サーバ、およびデータベースなど）も IPv6 アドレスをサポートしている必要があります。
- Identity Manager を SiteMinder と統合する場合、アプリケーション サーバの Web サーバ プラグインも IPv6 をサポートしている必要があります。
- Identity Manager から JDBC 接続を使用して、SiteMinder または任意のデータベースに接続するときに、IP アドレスではなく、ホスト名を指定します。
- デュアル スタック ホストに IPv4 と IPv6 をサポートする IAM レポート サーバをインストールできますが、このサーバへの通信は IPv4 である必要があります。

  管理コンソールでレポート サーバへの接続を設定する場合、サーバ名は IPV4 形式にする必要があります。

FIPS 140-2

Identity Manager r12 は新規インストールでのみ FIPS 140-2 をサポートします。 また、Identity Manager には FIPS 暗号化キーを提供するためのパスワード ツールが付属しています。このツールは次のディレクトリにあります。

```
C:¥Program Files¥CA¥IAM Suite¥Identity Manager¥tools¥PasswordTool
```

FIPS 140-2 を Identity Manager 環境用として有効にする場合は、以下の点に注意してください。

- 一度 FIPS 140-2 サポートを Identity Manager 展開のために有効にすると、無効にすることはできません。 同様に、FIPS 140-2 サポートを有効にしないで Identity Manager をインストールすると、後でサポートを追加することはできません。
- SiteMinder を含む Identity Manager の展開において FIPS 140-2 を有効にする場合、SiteMinder のバージョンは r12 である必要があります。

ローカライゼーション サポートの強化

Identity Manager ユーザ コンソールおよびユーザ コンソールのオンライン ヘルプは以下の言語で使用できます。

- フランス語
- 韓国語
- 日本語
- ドイツ語
- 中国語（簡体字）
- スペイン語
- イタリア語

注: これらの言語における Identity Manager の使用の詳細については、「Configuration Guide」を参照してください。

詳細情報:

ローカライズされた Identity Manager 環境のインストール（39 ページ）

第 3 章: 既存の機能の変更

このセクションは、以下のトピックから構成されます。

非推奨のサーブレット フィルタ エージェント (31 ページ)
管理コンソールの拡張機能 (31 ページ)
パスワード ポリシーの変更 (32 ページ)
非推奨の IMRExport ツール (32 ページ)
z/OS コネクタのアーキテクチャの変更 (33 ページ)
サポートが終了した機能 (33 ページ)

非推奨のサーブレット フィルタ エージェント

サーブレット フィルタ エージェントは、Identity Manager r12 で非推奨になりました。サーブレット フィルタ エージェントの代わりに、Web エージェントを使用することが推奨されます。 サーブレット フィルタ エージェントが 既存の Identity Manager 環境ですでに展開されている場合、引き続き動作し、サポートされます。

管理コンソールの拡張機能

Identity Manager 管理コンソールには、以下の新しい画面または変更された画面が含まれています。

- [ユーザ コンソール]ページ — このページでは、Identity Manager のユーザ コンソールの一般設定を行います。この設定には、アイコンおよびタイトル、認証クラスおよびログアウト ページが含まれます。

  注: Identity Manager では、[Themes]ページでアイコンおよびタイトルを設定していました。 [Themes]ページの機能は[ユーザ コンソール]ページに移動され、[Themes]ページは削除されました。

- [環境]ページ — [環境]ページから Identity Manager 環境を停止および開始できるようになりました。 環境の変更を反映するために、アプリケーション サーバを再起動する必要はありません。

- プロビジョニング ページ — このページに、インバウンド同期化設定は含まれなくなりました。 インバウンド同期化を設定するには、「プロビジョニング ガイド」を参照してください。

- [タスクの永続性]ページ — タスクの永続性は、インストール中に自動的に設定されるようになりました。 タスクの永続性を手動で有効にする必要はなくなりました。このページは削除されました。

パスワード ポリシーの変更

新しい Identity Manager r12 インストールでは、SiteMinder を必要としないので、デフォルトのパスワード ポリシー機能にいくつかの変更が加えられました。 SiteMinder と統合されていない実装では、Identity Manager では、ルールと制限を適用してパスワードの有効期限、構成、および使用方法を管理することで、ユーザ パスワードを管理する基本的なパスワード ポリシーを作成できます。

Identity Manager を SiteMinder と統合すると、以下のような追加ルールおよび制限を定義できる詳細なパスワード ポリシーを作成できます。

- ディレクトリ フィルタ
- パスワードの有効期限
  - ログインの失敗または成功の追跡
  - ログインの認証
  - 変更されない場合パスワードは失効
  - パスワードの未使用
  - パスワードが正しくありません。
- 複数の正規表現
- パスワードの制限
  - 再使用までの最短日数
  - 再使用までの最少パスワード数
  - 前のパスワードとの差異の割合(%)
  - 差異をチェックする場合に順番を無視
  - プロファイル属性のマッチング
  - 辞書のマッチング

非推奨の IMRExport ツール

IMRExport ツール機能は、Identity Manager ユーザ コンソールに統合されました。[レポート]タブの[スナップショット データのキャプチャ]タスクは、Identity Manager r12 で IMRExport ツールの機能を実行するようになりました。

z/OS コネクタのアーキテクチャの変更

z/OS コネクタ（CA ACF2、CA Top Secret および RACF）は、パフォーマンス上の理由から、z/OS 上の CA DSI サーバの代わりに z/OS 上の CA LDAP サーバを使用するようにアーキテクチャが変更されました。

CA LDAP サーバに関連するプロビジョニング サーバ設定ファイルのオプションが CA LDAP サーバをインストールするときに z/OS に入力され格納されるようになりました。また、メインフレーム LDAP サーバの接続情報は、プロビジョニング マネージャのエンドポイント タスク ビューから入力されるようになりました。

サポートが終了した機能

一部の eTrust Admin 機能は、Identity Manager r12 で使用できなくなりました。 以下の表に、Identity Manager r12 で使用する新機能を示します。

eTrust Admin 機能	Identity Manager 機能
Advanced Workflow	WorkPoint Workflow
Legacy Workflow	WorkPoint Workflow
自己管理 Web インターフェース（SAWI）	Identity Manager セルフサービス
委任管理 Web インターフェース（DAWI）	Identity Manager 委任管理
IA Manager	Identity Manager セルフサービス タスクおよび委任管理
eTrust Admin レポート etaReport	Identity Manager レポート
PeopleSoft フィード オプション	Bulk Loader
Universal フィード オプション	Bulk Loader
SAP オプション（C++ バージョン）	SAP コネクタ（Java バージョン）
MS SQL オプション（C++ バージョン）	MS SQL コネクタ（Java バージョン）
Oracle オプション（C++ バージョン）	Oracle コネクタ（Java バージョン）
OS/400 オプション	OS/400 コネクタ（Java バージョン）
CleverPath Portal オプション	変更なし

注： PeopleSoft フィード オプションおよび Universal フィード オプションの既存バージョン（eTrust Admin 8.1 SP2 で使用可能）では、Identity Manager r12 の使用を続けることができます。

第 4 章: システム要件

Identity Manager サーバをホストするシステムに必要な最小ハードウェア要件は、以下のとおりです。

- CPU: シングルまたはデュアルプロセッサ、Intel Pentium III（またはその互換）700～900 MHz、または Sparc Workstation 440 MHz
- メモリ: 2 GB
- 必要なディスク領域: 1 GB

注: 上記ハードウェア要件は、Identity Manager サーバをインストールするシステムにインストールされる必要のあるアプリケーション サーバの要件を考慮しています。

第 5 章: インストールに関する考慮事項

このセクションは、以下のトピックから構成されます。

サポート マトリックスの場所 (37 ページ)
必要な Solaris のパッチ (38 ページ)
SiteMinder の統合に必要な環境変数 (38 ページ)
ローカライズされた Identity Manager 環境のインストール (39 ページ)
英語以外のシステムで ASCII 以外の文字を使用すると、インストールに失敗します (40 ページ)
SiteMinder FIPS 140-2 専用モードに必要な設定の変更 (40 ページ)
JBoss: IPv6 サポートの設定 (41 ページ)
FIPS 140-2 の SPML サポート (41 ページ)
z/OS コネクタのアーキテクチャの変更 (42 ページ)
eTrust Directory の場所 (43 ページ)
eTrust Directory をアンインストールする前に修正が必要です (43 ページ)

サポート マトリックスの場所

サポートされているソフトウェア バージョンの詳細については、Identity Manager サポート マトリックスを参照してください。

サポート マトリックスへのアクセス方法

1. support.ca.com にログインします。
2. [Support By Product] または [Solution] をクリックします。
3. [Select a Product] または [Solution] ページの [Products] セクションで [CA Identity Manager] を選択します。

   [CA Identity Manager] ページが開きます。
4. [Recommend Readings] までスクロールします。
5. [CA Identity Manager Informational Documentation Index] をクリックします。

Identity Manager のサポートされているバージョンのプラットフォーム サポート マトリックスのページが表示されます。

必要な Solaris のパッチ

Solaris 9 または 10 にプロビジョニングをインストールする前に、パッチをダウンロードしてインストールしてください。

SDK 用 Sun Studio 10 パッチのダウンロード方法

1. 次の URL にアクセスします。
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. パッチ 117830 をダウンロードしてインストールします。

   注: Sun Studio 11 にはパッチは必要ありません。

すべてのコンポーネント用の Solaris 9 パッチのダウンロード方法

1. 次の URL にアクセスします。

   http://search.sun.com/search/onesearch/index.jsp
2. 9_recommended.zip をダウンロードしてインストールします。

SiteMinder の統合に必要な環境変数

Identity Manager を Solaris システムにインストールして、SiteMinder との統合を有効にすると、アプリケーション サーバのログに次のエラーが表示され、Identity Manager の起動に失敗する場合があります。

error "java: fatal: libetpki2.so: open failed: No such file or directory"

このエラーは、SiteMinder に必要な暗号化ライブラリをインストールする ETPKI インストールで CALIB 環境変数が正しく追加されない場合に発生します。

注: ETPKI は Identity Manager インストーラによって自動的にインストールされます。

回避方法

Identity Manager サーバを起動する前に、次のように CALIB 環境変数を追加します。

```
bash# export CALIB=/opt/CA/SharedComponents/ETPKI/lib
```

ローカライズされた Identity Manager 環境のインストール

Identity Manager には翻訳バージョンの Identity Manager ユーザ コンソールおよびユーザ コンソールのオンライン ヘルプも含まれています。 翻訳バージョンを使用するのに必要なファイルのほとんどは、次の場所にインストールされています。

im_admin_tools_dir¥samples¥Localization¥language

im_admin_tools_dir

Identity Manager 管理ツールのインストールされている場所です。

言語

使用する言語を表します。

注: インストール手順については、「Configuration Guide」を参照してください。

ただし、このほかにも翻訳バージョンの Identity Manager を使用するために必要なファイルがあります。

- リリース ノート
- オンライン ヘルプ ファイル

  注: im_admin_tools_dir¥samples¥Localization¥language で提供されているバージョンのオンライン ヘルプ ファイルは使用しないでください。

これらのファイルは、CA サポート サイトからダウンロード可能な CA Identity Manager r12 ローカライゼーション リソースに含まれています。

オンライン ヘルプ ファイルのインストール方法

1. CA Identity Manager r12 ローカライゼーション リソース ZIP ファイルをダウンロードします。
2. Identity Manager をホストするアプリケーション サーバからアクセスできるシステムにファイルを展開します。
3. 該当する言語の im_help_language.ZIP ファイルを IdentityMinder.ear¥user_console.war¥ にコピーします。

   IdentityMinder.ear

   アプリケーション サーバ上の Identity Manager アプリケーション (IdentityManager.ear)を展開した場所。

   注: オンライン ヘルプは、デフォルト バージョンのバックアップ コピーを作成してから、翻訳バージョンに置き換えるようにしてください。 デフォルトのオンライン ヘルプは、翻訳バージョンで上書きされてしまいます。

4. im_help.zip を user_console.war ディレクトリに展開します。
5. Identity Manager 環境を再起動します。

   翻訳バージョンのオンライン ヘルプを使用できるようになりました。

英語以外のシステムで ASCII 以外の文字を使用すると、インストールに失敗します

Identity Manager のインストール中に、インストーラにより一時ディレクトリにファイルが抽出されます。 一部のローカライズされたシステムでは、一時ディレクトリへのデフォルトパスに ASCII 以外の文字が含まれます。 たとえば、スペイン語 Windows システムの一時ディレクトリへのデフォルト パスは以下のとおりです。

C:¥Documents and Settings¥Administrador¥Configuración local¥Temp

ASCII 以外の文字を使用すると、インストーラにより空白の［Pre-Installation Summary］ページが表示され、インストールに失敗します。

インストールが失敗しないようにするには、以下の手順に従います。

ASCII 文字のみを含むフォルダを指すように環境変数 tmp を変更します。

SiteMinder FIPS 140-2 専用モードに必要な設定の変更

SiteMinder が FIPS 140-2 専用モードの場合、追加の設定手順が必要です。

Identity Manager を WebLogic または JBoss 上の FIPS 140-2 専用モードの SiteMinder で動作するように設定する方法

1. IdentityMinder.ear¥policyserver.rar¥META-INF¥ra.xml を開きます。
2. 次のエレメントを検索します。

```
<config-property>
<config-property-name>FIPSMode</config-property-name>
<config-property-type>java.lang.String</config-property-type>
<config-property-value>false</config-property-value>
</config-property>
```

3. <config-property-value> エレメントで false を true に変更します。
4. アプリケーション サーバを再起動します。

Identity Manager を WebSphere 上の FIPS 140-2 専用モードの SiteMinder で動作するように設定する方法

1. WebSphere 管理コンソールを開きます。
2. 次の場所に移動します。

   ［Enterprise Applications］ > ［IdentityMinder］ > ［Manage Modules］ > ［policyserver.rar］ > ［IdentityMinder.PolicyServerRA］ > ［J2C connection factories］ > ［PolicyServerConnection］ > ［Custom properties］
3. FIPSMode の値をクリックして、値を true に変更します。［OK］をクリックして、ページの上の［save］リンクをクリックします。

JBoss: IPv6 サポートの設定

IPv6 をサポートするシステム上に Identity Manager の JBoss バージョンをインストールする場合は、いくつかの設定が必要になります。

JBoss アプリケーション サーバに IPv6 を設定するには、以下の手順に従います。

1. 以下のディレクトリにある run_idm.sh ファイルを開きます。

   jboss_installation¥bin
2. JAVA_OPTS エントリの以下のいずれかのプロパティを変更します。
   - IPv6 のみの環境の場合は、以下のエントリをコメントアウトしてください。

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - IPv6/IPv4 の環境の場合は、以下のエントリをコメントアウトしてください。

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
3. ファイルを保存します。

FIPS 140-2 の SPML サポート

Identity Manager r12 では、SPML サーバは FIPS 140-2 に準拠しています。 SPML サービスは以下の環境に展開することをお勧めします。

- Apache Tomcat Server 4.1.36 または、より上位の 4.1.x バージョン
- JDK 1.5.11 または、より上位の JDK 1.5.x バージョン SSL モードで実行するには、Tomcat を有効にする必要がありますのでご注意ください。 詳細については、Apache の Tomcat 4 用管理者ガイド（http://jakarta.apache.org/tomcat/）の「SSL Configuration HOW-TO」を参照してください。

Apache Tomcat ではなく CA Tomcat を使用している場合、Identity Manager r12 で以下の SPML 用回避策が必要になります。

- CA Tomcat で JDK 1.4.xx を使用している場合、FIPS 140-2 を無効にする必要があります。 FIPS 140-2 サポートに必要な RSA Jsafe CryptoJ 4.0 ライブラリを JDK1.4 に最初のセキュリティ プロバイダとして設定することができないため、JDK 1.4 は CA Tomcat と互換性がありません。

  FIPS 140-2 サポートを無効にするには、Tomcat の起動中に JVM フラグ「-Dcom.ca.commons.security.fips=false」を渡します。

  - Tomcat をコマンドラインから実行している場合、JVM フラグの catalina.bat を含めることができます。 詳細については、このバッチ ファイルを参照してください。
  - Tomcat を Windows サービスとして実行している場合は、フラグを次のように渡します。

    a. レジストリ エディタを使用して、「HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥CA Tomcat 4.1.29 eTrustIAMWebServer¥Parameters」に進みます。

    b. 「JVM Option Number n」という文字列値を追加します。ここで「n」には前の JVM パラメータから続く数字が入ります。 値は、次のように指定します。

    Dcom.ca.commons.security.fips=false

    c. 新規追加のパラメータに配慮して、Edit DWORD 値「JVM Option Count」の値に 1 を加算してください。

- CA Tomcat で JDK 1.5 を使用している場合、非互換性の問題があります。 この問題を回避するには、次の手順に従います。

  a. %TOMCATHOME%¥common¥endorsed から 2 つの Xerces ライブラリ（xercesImpl.jar および xmlParserAPIs.jar）を手動で削除します。

  b. Tomcat を再起動します。

z/OS コネクタのアーキテクチャの変更

z/OS コネクタ（CA ACF2、CA Top Secret および RACF）は、パフォーマンス上の理由から、z/OS 上の CA DSI サーバの代わりに z/OS 上の CA LDAP サーバを使用するようにアーキテクチャが変更されました。

z/OS コネクタを設定する前に、z/OS r12 用の CA LDAP サーバをインストールする必要があります。このプログラムは、support.ca.com からダウンロードできます。

eTrust Directory の場所

プロビジョニング ディレクトリのスキーマは、eTrust Directory にインストールされています。 eTrust Directory は、Identity Manager インストール メディアからインストールできます。

eTrust Directory をアンインストールする前に修正が必要です

Windows システムから eTrust Directory をアンインストールする必要がある場合は、アンインストールの手順を開始する前に、パッチを適用する必要があります。

パッチを適用しないと、アンインストール手順によって、他の CA 製品に必要なライセンス ファイルが削除されてしまう可能性があります。

パッチは、CA Support サイトから ダウンロードできます。

パッチを検索する方法

1. support.ca.com にログインします。

   CA Support サイトが開きます。

2. ページの左側にあるリンクのリストで［Licensing］をクリックします。

3. ［License Package 1.8 is Now Available］をクリックします。

   License Package への変更の説明と、それをダウンロードするためのリンクが含まれたページが開きます。

4. 手順に従って、Windows パッチをダウンロードしてインストールします。

第 6 章: 既知の問題

このセクションは、以下のトピックから構成されます。

全般 (45 ページ)
アップグレード (49 ページ)
レポート (51 ページ)
プロビジョニング (52 ページ)

全般

Identity Manager r12 に関する全般的な既知の問題は以下のとおりです。

Identity Manager EAR が WebLogic では自動展開されません

本稼動モードで WebLogic 8 または 9 を使用している場合は、インストールまたはアップグレードを行った後、最初にアプリケーション サーバを起動したときに、Identity Manager EAR が自動展開されないことがあります。 このような場合は、user_projects¥applications フォルダから IdentityMinder.ear を手動で展開してください。

ワークフローおよび承認者としてのグループ メンバ

ワークフロー プロセスが特定のグループ メンバをその承認者とするように Workpoint Designer で設定されている場合は、ワークフロー アイテムはワークフロー コントロール下のイベントには作成されずに、テスト セッションが失敗する可能性があります。

解決方法としては、ワークフロー コントロール下にタスクを配置し、テンプレート メソッド (SingleStepApproval または TwoStageApprovalProcess テンプレートで) を使用してグループ メンバを承認者 (または参加者リゾルバ) として定義してください。

新しい Workpoint Properties を設定する必要がある可能性があります

Identity Manager には Workpoint の新しいバージョンが含まれています。 このバージョンでは、GeneralMonitor.properties および workpoint-server.properties で新しいプロパティを設定することができます。 これらの新しいプロパティはオプションで、必要な場合にのみ追加する必要があります。

新しいワークフロー プロパティは以下のとおりです。

- GeneralMonitor.properties ファイルでは
  - #JMX_HTML_ADAPTOR_PORT=9092

    このプロパティはデフォルトでコメントアウトされています。 プロパティが true に設定されている場合は、汎用 Sun JMX アダプタを使用する HTML ページが有効になります。このアダプタは、Workpoint Management Console アプリケーションとは別の、保護されていない Web ポートです。 このプロパティは、コメントアウトのままにしておくか、または false に設定し、代わりに Workpoint への JMX によるアクセスに Workpoint Management Console を使用することをお勧めします。
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    このプロパティは Workpoint 電子メール機能を使用するユーザにのみ適用されます。 このプロパティはメール モニタで処理されるエラーを制御します。 Identity Manager ユーザが Workpoint のメール機能を使用している場合は、このプロパティを適用できる可能性があります。

    注: JOB_ERROR_STATE_ON_MAIL_ERROR が設定されていない場合はデフォルトの true になります。 Workflow 電子メールを使用していて、ジョブステータスに影響を及ぼす電子メール エラーを表示させたくない場合は、false に設定することをお勧めします。
  - ENABLE_SCRIPT_TASK_GROUPING=false

    スクリプト モニタが同じジョブから実行しているすべての同時スクリプトを一緒にグループ化する必要がある場合は、このプロパティが制御します。 true の場合は、同じワーカー スレッドに特定のジョブのすべてのスクリプトを割り当てるように作用します。スクリプトは一度に 1 つずつ実行されます。 このプロパティは、オートメーションの非同期スクリプトを使用するジョブに複数のアクティビティがあり、同時にアクティブになる可能性がある場合に、並行例外の発生を防止するのに便利です。

    カスタマイズされたワークフロー スクリプトがあり、並行例外が発生する場合は、このプロパティを調べてください。

    追加の電子メール プロパティと関連するプロパティは、GeneralMonitor.properties ファイルに含まれています。

- workpoint-server.properties ファイルでは
  - server.automated.delay=500

    このプロパティは、サーバ自動ノードを制御して、これらのノードをキューに入れたデータベース トランザクションが継続されるまで、これらのノードがキューに入れられないようにします。 これは、タイミングの問題によるサーバ自動ノードのエラーを防ぎます。 このプロパティは、サーバの自動ノードが使用中である場合にお勧めします。

ロジカル アトリビュート ハンドラのコピーを作成できない

ユーザ コンソールでロジカル アトリビュート ハンドラのコピーを作成しようとすると、次のエラーが表示されます。

「オブジェクトが接続されていません。」

既存のロジカル アトリビュート ハンドラに基づかない、新しいロジカル アトリビュート ハンドラの作成が正しく機能しません。

ロール ポリシーのグループ フィルタの使用

Identity Manager でリレーショナル データベースに格納されたユーザを管理する場合、メンバ ポリシーおよび管理ポリシーのグループ フィルタが正常に動作しないことがあります。 たとえば、メンバ ポリシーで「グループのメンバで名前が A で始まるユーザ」などのようにフィルタを指定すると、Identity Manager では、このポリシーがグループの文字 A で始まるユーザではなく、すべてのユーザに不適切に適用されてしまうことがあります。

この問題を防ぐには、tblGroupMembers および tblGroupAdministrators の各テーブルのディレクトリ設定ファイル（directory.xml）にユーザ オブジェクトが定義されていることを確認してください。

directory.xml のユーザ オブジェクト定義は以下のようになります。

```
<ImsManagedObject name="User" description="My Users" objecttype="USER">
<!-- COMMENT Table -->
    <Table name="tblUsers" primary="true" />
    <Table name="tblUserAddress">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserRoles">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserDelegators">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserPasswordhints">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblUserIdentityPolicy">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblOrganizations">
    <Reference childcol="id" primarycol="org"/>
    </Table>

    <Table name="tblGroupMemebers">
    <Reference childcol="userid" primarycol="id"/>
    </Table>

    <Table name="tblGroupAdmins">
    <Reference childcol="userid" primarycol="id"/>
    </Table>
```

ディレクトリ設定ファイルを変更した後、管理コンソールを使用してこれをインポートします。

注: ディレクトリ設定ファイルの変更方法の詳細については、「Configuration Guide」を参照してください。

ロールおよびタスクの検索画面の設定

ロールまたはタスクの検索画面を設定するときに、「以下のルールに適合するオブジェクトのみ表示」オプションを使用して、検索で返されるロールおよびタスクを制限できます。 このオプションを設定するときに使用した属性は、検索画面の使用可能な検索フィールドとして追加しないでください。

たとえば、 検索画面を設定して、Enabled 属性が「Yes」に設定されているロールのみ表示する場合は、検索条件でユーザが指定できる属性のリストから Enabled 属性を削除します。

削除しない場合は、ユーザが入力した条件は無視されます。

Firefox ブラウザでの Identity Manager 環境の作成

Firefox ブラウザを通じて管理コンソールにアクセスする場合、Identity Manager 環境の作成が遅くなり、ハングしているように見える場合があります。 このような場合、環境の作成は継続されますが、ブラウザは更新されません。このため、いつ作成が完了するのかを確認することができません。

注: ブラウザ ウィンドウを閉じても、Identity Manager は環境の作成を続けます。

アップグレード

以下の問題は Identity Manager r12 のアップグレードに関連するものです。

MS SQL および Oracle エンドポイントは、eTrust Admin 8.1 SP2 からのアップグレード後は使用できません

eTrust Admin 8.1 SP2 から Identity Manager r12 にアップグレードした後は、プロビジョニング マネージャを使用して、アップグレードを行う前に取得したすべての MS SQL または Oracle エンドポイントを、データ ソース名（DSN）ではなく JDBC URL を使用するように手動で再設定する必要があります。 これは、MS SQL エンドポイントおよび Oracle エンドポイントを管理するために SuperAgent から JCS を使用するように切り替えるためです。

Oracle: Oracle エンドポイント プロパティ シートの詳細を変更します。

例

```
jdbc:oracle:thin:@oracle_server_host:1521:ORACLE
```

MS SQL: エンドポイントを右クリックし、［カスタム］ - ［Change Admin Password］を選択します。 この時点で、他のエンドポイントの詳細を表示しなくても、URL および接続のクレデンシャルを変更できます。

例

```
jdbc:sqlserver://serverHost:1433;instanceName=instance1
```

注: 移行手順および URL 構文の一覧については、「コネクタ ガイド」の第 4 章「データベース コネクタ」を参照してください。

Solaris x86 （Intel）プラットフォームで UNIX リモート エージェントを使用できない

Unix リモート エージェント パッケージでは、Solaris x86 （Intel）プラットフォームで UNIX リモート エージェントのインストールまたはアップグレードを実行するのに必要なファイルがありません。

Z/OS コネクタのアーキテクチャの変更

z/OS コネクタ（CA ACF2、CA Top Secret および RACF）は、パフォーマンス上の理由から、z/OS 上の CA DSI サーバの代わりに z/OS 上の CA LDAP サーバを使用するようにアーキテクチャが変更されました。

z/OS コネクタを設定する前に、z/OS r12 用の CA LDAP サーバをインストールする必要があります。このプログラムは、support.ca.com からダウンロードできます。

Identity Manager r12 にアップグレードしたら、システムに定義されている各エンドポイントで以下の操作を実行します。

[エンドポイント]タスク ビューで

1. [オブジェクト タイプ]から[CA ACF2]、[CA Top Secret]、または[RACF Endpoint]を選択します。
2. [検索]ボタンをクリックします。 [エンドポイント]を右クリックしてプロパティを選択します。 以下の情報を入力します。

   [Mainframe Server Information]セクションでは、以下の情報を入力します。

   - [IP Address/Machine Name]では、CA LDAP サーバが設定されて実行されている RACF 管理システムの IP アドレスを指定します。
   - [LDAP Port]では、z/OS 用の CA LDAP サーバのインストール中に指定したポート番号を指定します。 メインフレームの LDAP ポートが確認できない場合は、「Checking your CA LDAP Server for z/OS Configuration Information」のセクションを参照してください。
   - [LDAP Suffix]では、このエンドポイントに使用するサフィックスを指定します。 [Get Suffixes]ボタンをクリックすると、「Get Suffixes」ボタンをクリックしたときに、有効で使用可能なすべてのサフィックスがこのコンボ ボックスに自動的に入力されます。 [Mainframe IP Address/Machine Name]および[Mainframe LDAP Port]フィールドに有効な値が入力されたら、サフィックスを取得できます。

レポート

以下の問題は、Identity Manager r12 のレポートに関連するものです。

レポートの制限

1 つのレポート タスクに関する複数のスナップショットで同じ繰り返し時間を使用しないでください。

Satisfy=All が XML ファイルで正しく機能しない

スナップショット パラメータ XML ファイルでは、satisfy=all と satisfy=any はどちらも同じく satisfy=any (OR 演算子と同様)として機能してしまいます。

[マイ レポートの表示]タスクで Cookie を有効にする

Identity Manager で[マイ レポートの表示]タスクを使用してレポートを表示するには、ブラウザでサードパーティ セッションの Cookie を有効にします。

ExportALL.xml および組織をサポートしていない環境

組織オブジェクトと属性をエクスポートするスナップショット パラメータの XML ファイル(例: ExportAll.xml)を使用すると、環境が組織をサポートしていない場合は例外が発生します。 この問題を解決するには、ExportAll.xml ファイルの組織オブジェクトと属性をコメントアウトします。

プロビジョニング

以下の問題リストのプロビジョニング コンポーネントの略語は、次のように定義されます。

- ACC: CA アクセス制御コネクタ
- ADS: Active Directory サービス コネクタ
- DBZ: z/OS コネクタ用の DB2 Universal Database
- DYN: 動的コネクタ
- E2K: Exchange 2000 コネクタ
- EEM: Embedded Entitlements Manager コネクタ
- ETC: UNIX ETC
- FND: Oracle Application コネクタ
- INS: インストール
- KRB: Kerberos コネクタ
- LND: Lotus Notes/Domino コネクタ
- NDS: Novell Directory Services コネクタ
- N16: Windows NT リモート エージェント
- AS4: OS/400 コネクタ
- PKI: Entrust PKI コネクタ
- PLS: CA SSO for Advanced Policy Server コネクタ
- PSA: Password Sync Agent
- RSA: RSA SecurID コネクタ

- SAP：SAP コネクタ
- SBL：Siebel コネクタ
- UPO：Universal Provisioning コネクタ
- VMS：OpenVMS コネクタ
- z/OS：CA ACF2、CA Top Secret、RACF のコネクタ

全般

以下の問題は、Identity Manager r12 の全般的なプロビジョニングの問題です。

[ユーザ パスワードのリセット]タスクのアカウントの同期化

Identity Manager 環境のプロビジョニングを有効にするには、ProvisioningOnly-RoleDefinitions.xml という名前の設定ファイルをインポートします。このファイルでユーザ プロビジョニングのロールとタスクが作成されます。

このファイルでは、[ユーザ パスワードのリセット]タスクのデフォルトのアカウントの同期化設定はオフに設定されています（プロビジョニングを有効にする前は、同期化設定が[タスク完了時]に設定されています）。

[ユーザ パスワードのリセット]を使用して、アカウントの同期化をトリガするには、プロビジョニングを有効にするために ProvisioningOnly-RoleDefinitions.xml をインポートした後に、アカウントの同期化オプションを設定します。

ユーザ コンソールがエンドポイント タイプを検索および関連付けることができません

ユーザ コンソールの[検索]タスクと[関連付け]タスクには以下のエンドポイント タイプがありません。

- Kerberos
- UNIX NIS
- Entrust PKI
- Siebel
- Universal Database for z/OS
- カスタム開発されたエンドポイント タイプ

プロビジョニング マネージャを使用すると、これらのエンドポイント タイプを探索して関連付けることができます。 その後、ユーザ コンソールで、これらのエンドポイントの 1 つにアカウントを割り当てるなど、ルーチンのアカウント機能を実行することができます。

同一のタイム ゾーンでの作業の検索および関連付け

ユーザ コンソールでは[検索および関連付け]定義をスケジュールできます。 この操作ではクライアントブラウザがサーバと同じタイム ゾーンにあることが必要です。 たとえば、サーバ時間が火曜日の 7:00 AM のときにクライアント時間が 10:00 PM であれば、[検索および関連付け]定義は機能しません。

Solaris での Provisioning Server のコア ダンプ

Solaris 環境のプロビジョニング サーバでは、サービスのシャットダウン時にコア ファイルが生成されます。

このことにより影響を受ける機能はなく、問題ありません。

プロビジョニング ディレクトリ インストーラには正確な解決済みホスト名が必要です

プロビジョニング ディレクトリとプロビジョニング サーバを同じマシンにインストールする場合、インストーラでは正確に設定された名前解決のホスト名が必要です。 マシンがそのマシン名を目的の IP アドレスに解決できない場合は、プロビジョニング サーバのインストールに失敗したり、予期しない結果を招きます。 その場合は、以下の 2 つのシナリオが想定されます。

- FQDN とホスト名の名前解決の結果が異なる場合 (たとえば、IPv4/6 ネットワークで、DNS に IPv6 アドレスを登録し、ネットバイオスまたはホストファイルを介してホスト名に IPv4 アドレスがある場合)。 プロビジョニング ディレクトリを IPV6 でのみ待機するように設定してから、FQDN を使用してプロビジョニング サーバをインストールすると、 インストールは失敗します。これは、インストールの任意の段階で、インストール プログラムは FQDN ではなくホスト名を解決しようとするためです。 この解決方法としては、ホスト名とその IPv6 アドレスをホスト ファイルに追加すると、解決します。 しかし、これでもまだ不適切な設定であることに変わりはありません。
- DNS のないマシンまたはその他の名前参照を使用するマシンで、プロビジョニング ディレクトリとプロビジョニング サーバを IP アドレスを使用してインストールしようとすると、インストールは同じく失敗します。

  注: CA では、IP アドレスによるインストールはサポートしていません。

グローバル ユーザのパスワード変更の同期で行った特定のドメイン設定により、プロビジョニング サーバがクラッシュすることがあります

「Identity Manager Server/Use External Password Policies」ドメイン設定が「Yes」に設定されている場合は、複数のグローバル ユーザのパスワードを同時に変更できます。 その結果、パフォーマンスが低下し、プロビジョニング サーバがクラッシュすることがあります。

INFO レベルよりも上位のレベルで Solaris ECS のロギングを行うと、プロビジョニング サーバのパフォーマンスに影響します

INFO レベルよりも上位のレベルで ECS ロギングを有効にすると、応答を受け取る前にログが書き込まれるようになります。 このため、ログが書き込まれている間、リクエストは延期されます。 ECS ロギング機能を使用しているときにプロビジョニング サーバのパフォーマンスが低下している場合、回避策はこの機能を停止することです。

JIAM で不正なオブジェクト クラス名が指定されていると SPML の更新に失敗します

JIAM API でプロビジョニング サーバに送信されたリクエストに不正なオブジェクト クラス名が使用されると、プロビジョニング サーバはリクエストを拒否して「Internal consistency error in Provisioning Server」エラーが発生します。 たとえば、「eTSBLDirectory」オブジェクトの更新を実行するときは、「eTDirectory」という不正なオブジェクト クラスがプロビジョニング サーバに送信されます。 この問題は、SPML サービスを再起動することで解決できます。

グローバル ユーザ名の特殊文字

プロビジョニング マネージャでは、バック スラッシュ文字(¥)などの特殊文字を含むグローバル ユーザ名を作成できます。 ただし、Identity Manager サーバは特殊文字を含むユーザ名をサポートしていません。

プロビジョニング マネージャで特殊文字を含むグローバル ユーザを作成すると、Identity Manager は Identity Manager のユーザ ストアに対応するユーザを作成しようとします。 すると、エラーが発生して、Identity Manager のユーザ ストアで[ユーザの作成]タスクが失敗します。

プロビジョニング マネージャで特殊文字を含むグローバル ユーザを削除しようとするときにもエラーが発生します。

プロビジョニング マネージャに古い SAWI/DAWI 参照が含まれる

プロビジョニング マネージャには、現在サポートされていない SAWI および DAWI 機能のコントロールを含むダイアログも含まれています。 SAWI または DAWI ではなく、Identity Manager のセルフサービス機能を使用してください。

エンドポイントを追加したときにはすでにエラーが存在しています

エンドポイントを削除してからまったく同じ名前で追加すると、プロビジョニング サーバからその名前のエンドポイントはすでに存在すると主張する失敗が報告される場合があります。 これは、そのエンドポイントを管理するコネクタ サーバを複数設定した場合に発生する可能性があります。 この失敗は、エンドポイントを削除するときに、すべてのコネクタ サーバに削除が通知されるわけではないことが原因です。

この問題を解決するには、エンドポイントを管理するように設定されているすべてのコネクタ サーバを再起動してください。

Java コネクタ サーバ（Java CS）

以下の問題は、Identity Manager r12 の Java コネクタ サーバに関連するものです。

" / 文字シーケンスを使用して識別名を表示する場合に、Java コネクタの検索が失敗します

未解決の問題が 2 文字のシーケンス

"/ を処理する Java CS にあります。

これは、標準 JNDI API によって使用される複合名の処理に重要で、複数の技術にまたがる識別名を表します。

Java CS に渡されたその他の識別名の特殊文字の詳細については、

http://ietf.org

の LDAP RFC 2253 および javax.naming.ldap.LdapName の JavaDoc を参照してください。

Connector Xpress の Null ポインタ エラー

Endpoint Types を右クリックして［set Managing CS］を選択する、または複数のプロビジョニング サーバが存在する環境で Connector Xpress を使用して CS Config を直接編集することによって、コネクタ サーバのルーティング情報を変更しようとすると、Connector Xpress に null ポインタ エラーが表示される場合があります。 高度なコネクタ サーバ ルーティングを実行する必要がある場合は、csfconfig ツールを使用してください。

Windows サービスを使用した Java CS サービスの再起動が失敗する

Windows サービスを使用して Java CS サービスを再起動すると、サービスのシャットダウンを完了するまで Java CS サービスを開始できず、サービスの開始が失敗します。この問題が発生する場合は Windows の[サービス]設定パネルでの操作において、[再起動]ボタンではなく[停止]および[開始]ボタンを優先してください。

ストアド プロシージャを選択しない場合の誤ったエラー メッセージ

Connector Xpress ウィザードの[Map Table]画面の[Select Procedure]ドロップダウン リストからストアド プロシージャを選択しないで[Next]をクリックすると、次の誤ったエラーメッセージが表示されます。

Please specify a table to be mapped.

正しいメッセージは以下のとおりです。

Please specify a procedure to be mapped.

検索された DYN JNDI エンドポイントのコンテナがプロビジョニング マネージャに表示されません

新しく取得した DYN JNDI エンドポイントでコンテナの単一レベルの検索を行った後、検索件数に新しいレコードが追加されたことが表示されていても、[Provisioning Manager Content]パネルに新しく検索したコンテナが表示されないことがあります。 プロビジョニング マネージャを閉じて再び開くと、コンテナが表示されます。

DYN アカウントテンプレートの Suspended 属性が、プロビジョニング マネージャで太字で表示されます

プロビジョニング マネージャでは、DYN アカウント テンプレートの Account Suspension Status 属性が太字で表示されます。これは誤って機能属性として示されます。

DYN 機能属性のラベルがプロビジョニング マネージャで切り捨てられます

Connector Xpress で DYN JDBC または DYN JNDI のエンドポイント タイプを作成するときに指定した機能属性は、プロビジョニング マネージャに表示されるときに、ラベルが切り捨てられているか存在しないことがあります。 これは、Connector Xpress で displayName を指定するときに、ラベルの最後に「ラベル名 a」などの追加の文字を指定することで回避することができます。 これは、membership 機能属性の場合には発生しません。

また、以下のいずれかの方法で既存のメタデータを変更できます。

Connector Xpress の保存されたプロジェクトをロードした後

- ウィザードから実行します。
- メタデータ ツリーを展開して、［クラス］ -> ［eTDYNPolicy］ -> ［プロパティ］ -> ［機能属性］ -> ［メタデータ］までドリルダウンし、displayName の値を変更します。

いずれかの方法を選択して DYN エンドポイント タイプの既存のメタデータを変更した場合は、DYN エンドポイント タイプが新しいメタデータで更新されていることを確認してください。

コネクタ

以下の問題は、Identity Manager r12 のプロビジョニング コネクタに関連しています。

ADS コネクタによるサブツリー検索で正しい結果が返されません

多数のオブジェクトを持つ組織単位を複数個含むサブツリーに対してサブツリー検索を行うと、間違ってオブジェクトが返されないことがあります。 たとえば、検索の制限サイズが 500 に設定されており、各組織単位のオブジェクト数がその制限を超えている場合、結果は返ってきません。 検索フィルタで検索の制限サイズを 500 以下に絞り込んだ場合でも、検索では間違って結果は返ってきません。 この問題の回避策は、検索の制限サイズを大きくすることです。

ADS の期限の 2038 年以降への設定の回避

ADS アカウントの期限を 2038 年より後の日付に設定すると、プロビジョニング マネージャがクラッシュします。

EEM コネクタは、IE7 ではサポートされません。

IE7 がインストールされているマシンに、指定された EEM コネクタの C++ コネクタサーバ（CCS）がインストールされている場合、EEM コネクタはサポートされません。

注： Identity Manager r12 製品マニュアルでは、Embedded Entitlement Manager（EEM）とは、Embedded Identity and Access Manager（EIAM）コネクタを指します。

プロビジョニング サーバでの EEM アカウント テンプレートの表示

EEM アカウント テンプレートを表示すると、プロビジョニング マネージャが応答しなくなることがあります。

回避策は、プロビジョニング マネージャを終了して再起動することです。

新しい EEM エンドポイントを取得するには、プロビジョニング マネージャを再び開きます

エンドポイントの取得中にホスト名が設定されると、別のエンドポイントを取得するプロビジョニング マネージャを閉じて、再び開く必要があります。 これは、操作が取り消された場合でも同じです。

EEM アカウント テンプレートの User 属性を選択または変更できません

EEM エンドポイントのアカウント テンプレートを作成するときは、エンドポイントを選択した後に[アプリケーション プロパティ]タブをクリックし、[OK]をクリックしてアカウント テンプレートの作成プロセスを終了する必要があります。

DB2 z/OS エンドポイントを取得すると CCS がクラッシュします

DB2 UDB コネクタおよび DB2 z/OS コネクタを、同じ C++ コネクタ サーバ(CCS)に対する定期的なリクエストにしないでください。

回避策は、別のマシンに 2 番目の CCS をインストールして、DB2 UDB および DB2 z/OS の各コネクタが独自の C++ コネクタ サーバ上でホストされるようにします。

ETC UNIX リモート エージェントの無人アップグレードの非サポート

eTrust Admin r8.1 SP2 から Identity Manager r12 への ETC UNIX リモート エージェントの無人アップグレードは、サポートされません。 有人モードでアップグレードを実行する必要があります。

S390 で動作する Linux OS の ETC リモート エージェントが失敗します

S390 ホストで動作している Linux オペレーティング システムの ETC リモート エージェントをインストールしようとすると、次のエラーが表示されて失敗します。

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh lsm.exe: 共有ライブラリをロード中にエラーが発生しました: libncurses.so.4: 共有オブジェクト ファイルを開くことができません: そのようなファイルまたはディレクトリはありません。"

これを解決するには、オペレーティング システムで ncurses のバージョン 4 を検索してそれをインストールする必要があります。

Cafthost コマンドを実行すると HP-UX UNIX のエラーが発生します

以下のコマンドを実行すると、「Bus error (core dump)」というエラーが表示されることがあります。

```
cafthost -a <host_name>
```

ホストを追加するには、「cat /etc/catngcampath」ディレクトリ内でテキスト ファイル エディタを使用して、「cafthost.cfg」設定ファイルを手動で変更し、各ホストに新しい行を追加します。

ETC リモート エージェントをアンインストールすると孤立ファイルが残ります

ETC リモート エージェントを r8.1SP2 から r12 にアップグレードすると、いくつかのファイルはそのまま残されます。 これらのファイルが他のインストールされたパッケージで使用されていない場合、これらのファイルは削除されます。

- /usr/bin/uxsautil
- `cat /etc/catngdmopath.tng`/bin/uxsautil
- `cat /etc/catngdmopath.tng`/scripts/Config
- `cat /etc/catngdmopath.tng`/etc/ExitSetup.ini
- `cat /etc/catngdmopath.tng`/scripts/caftexec
- `cat /etc/catngdmopath.tng`/scripts/caftexec.cfg
- `cat /etc/catngdmopath.tng`/setup.gif

SPML を使用して、VMS のアカウント権限を削除することはできません

SPML を使用して VMS アカウントの accountRights 属性から値を削除することはできません。 SPML クライアントは成功したことを示すメッセージを返しますが、アカウントは更新されません。

回避策は、プロビジョニング マネージャを使用してこのような変更を行うことです。

OpenVMS アカウントのセカンダリ パスワードを設定できません

OpenVMS リモート エージェントの「vmsautil」ユーティリティでは、ユーザ アカウントの OpenVMS PRIMARY/SECONDARY パスワードの 意味は認識されません。 プライマリ パスワードが設定されていないときにセカンダリ パスワードを指定しようとすると、「パスワードが短かすぎます」というエラー メッセージが表示され、操作に失敗します。

回避策は、アカウントのセカンダリ パスワードを設定するときは、プライマリ パスワードを常に再設定することです。

OpenVMS の CAM/CAFT に指示がない

ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT ファイルに OpenVMS システムでの CAMCAFT.EXE の設定方法に関する情報が見つかりません。 CAM/CAFT をインストールする前に CAFTHOST シンボリック名を定義する必要があります。 CAFTHOST を定義するには、LOGIN.COM ファイルに次のコマンドを追加します。

```
CAFTHOST :==$CAPOLY$BIN:CAFTHOST.EXE
```

次に、OpenVMS システムに再びログオンします。

VMS 属性 eTVMSPWDLifeTime に同期がとれていないと表示されます

Password Lifetime（eTVMSPWDLifeTime）属性は、アカウント テンプレートの属性「Never expires」が「true」に設定されている場合（チェックが入っている場合）は、「アカウントの同期化チェック」操作を行った後、同期がとれていないと表示されます。

SPML により VMS アカウント ステータスが誤って False と報告されます

VMS アカウントが一時停止している場合、プロビジョニング マネージャではアカウント ステータスは「アクティブ（eTrust Admin では一時停止）」として正しく報告されますが、SPML では一時停止は間違っているとだけ報告されます。

VMS パスワード フラグを設定できません

リクエストにより TVMSAccessFlags の値が設定されない場合は、eTVMSPwdFlags 属性はアカウントの追加または変更操作で正しく設定されません。

これを回避するには、追加または変更リクエストに、eTVMSAccessFlags 属性と eTVMSPwdFlags 属性の値を含める必要があります。

VMS Migrate Password 属性に同期がとれていないと表示されます

「アカウントの同期化チェック」操作の後、MIGRATEPW フィールドが「true」に設定されている（チェックが入っている）フィールドにあるすべての VMS アカウントまたはアカウント テンプレートで、eTVMSPwdFlags は同期がとれていないと表示されます。

VMS アカウントの一時停止

プロビジョニング マネージャを使用してアカウント レベルでアカウントを一時停止するとアカウントは正常に一時停止されますが、プロパティ ページでは「一時停止」が保持されず、変更を適用すると「アクティブ」に戻ります。 そのため、一時停止になっているアカウントがあり、そのアカウントのプロパティ ページに「アクティブ」と表示される場合は、実際にそのアカウントをもう一度「アクティブ」に戻すことはできないことを意味しています。

アカウント自体でこれを回避する方法はありません。 これを実際に回避するための唯一の方法は、アカウントをグローバル ユーザに関連付け、そのグローバル ユーザを一時停止することでアカウントの一時停止を制御することです。

VMS ユーザ名にエスケープされていない Unicode 文字を含めることはできません

不正な名前で VMS アカウントを作成しようとすると、Solaris 環境にインストールされたプロビジョニング サーバがクラッシュすることがあります。

NDS コネクタで新しいコンテナを検索できません

NDS エンドポイントが取得された後の最初の検索で、コンテナの検索および追加が行われます。 NDS ローカル ツールを使用してコンテナを追加し、エンドポイントを再検索しようとすると、新しく追加されたコンテナもそのサブエントリもツリーには表示されません。

新しいコンテナを表示するためには、プロビジョニング サーバからエンドポイントを削除し、これを再取得して検索する必要があります。

単独値フィールドの NDS Connector の説明

NDS Connector では、アカウントの説明は単独値フィールドですが、NDS エンドポイントでは、アカウントの説明は複数値フィールドです。

UPO コネクタ エンドポイント タイプの問題を防ぐために、アップグレードを行った後は環境変数を削除または変更する必要があります

リモート SuperAgent to r12 C++ コネクタ サーバのアップグレード中に、ETAHOME 環境変数に CCS の誤ったインストール パスが含まれていることがあり、これが原因で、UPO コネクタのエンドポイント タイプの問題が発生します。 アップグレードした後で UPO エンドポイントを取得または使用する前に、ETAHOME 環境変数を手動で削除するか、CCS の正しいインストール パスに変更する必要があります。

UPO エンドポイントの取得でドメイン フィールドが検証されません

ドメイン属性に誤った値が指定されている UPO エンドポイントは正常に取得されますが、エンドポイントにより検索時に「Connector Server Search failed: Insufficient access」エラーが発生します。

これは、プロビジョニング マネージャのエンドポイントを右クリックして、[カスタム] -> [Update Credentials...]を選択し、ドメインに正しい値を指定することで解決できます。

Solaris の eTrust Common Services から Enterprise Common Services にアップグレードする前に必須 Kernel パラメータのチェックが実行されません

必須 kernel パラメータは、Solaris の eTrust Common Services から Enterprise Common Services（Solaris 10 よりも Solaris 9 に影響を及ぼしやすい）にアップグレードした製品では実行されません。 Kernel パラメータが十分でない場合、インストールで警告が表示されて停止されることなく続行されます。 これは以下に影響します。

- Solaris での RSA リモート エージェント
- Solaris での IMPS
- IMPS SDK

この問題を回避するには、次の手順に従います。

以下を実行します。

```
'<product installer dir>/solaris/ecs-installation/eCSinstall.sh'
```

カーネルが要件を満たしていない場合は、情報が含まれたメッセージが表示されます。カーネル要件が満たされている場合、インストールが開始されます。

KRB アカウントを複製できない

プロビジョニング マネージャで Kerberos アカウントを複製しようとすると、「eTKRBFullNameCorrelate not found in the attribute registry! (...) - Return Code: 111」というエラーが発生する場合があります。 この問題を回避するには、アカウントを複製するのではなく、新規アカウントを追加します。

KRB エンドポイントの取得時に無効な REALM を指定するとエラーが発生する

KRB エンドポイントを取得しようとして、REALM に無効な値を指定すると、null ポインタ エラー メッセージが表示されます。

z/OS Security エンドポイントにより Solaris プロビジョニング サーバがクラッシュします

エンドポイントが z/OS r12 用の CA LDAP サーバに接続できない場合は、プロビジョニング サーバがクラッシュします。

この問題を回避するには、有効な接続情報を使用してエンドポイントを設定してください。

LDS エンドポイントを使用した z/OS の同期

LDS 同期エージェントは Identity Manager r12 製品 DVD に含まれていません。 このエージェントが必要な場合は、テクニカル サポートにお問い合わせください。

Exchange 2007 でメールボックス権限を管理すると E2K エラー メッセージが表示されます

メールボックス権限は Exchange 2007 では管理できません。「CAFT Message: Access Denied - or command failed to execute」というエラー メッセージを受信します。

メールボックス権限を管理すると E2K CAFT エラーが発生します

Exchange リモート エージェントを正しく設定していても、メールボックス権限の管理中に「CAFT Message : Access denied - or command failed to execute」エラー メッセージが返されることがあります。

これは、メールボックス権限のリストに同じオブジェクトに対する複数の権限がある場合に発生します。また、通常は管理された Exchange オブジェクトが親オブジェクトから権限を継承するときに発生します。

E2K に複数の電子メール アドレス(メイン)を持つことは許可されていません

プロビジョニング マネージャを使用して新しい電子メール アドレスを既存の電子メール アドレスに追加し、電子メール アドレス(メイン)となる新しいアドレスを設定できます。 ただし、既存の電子メール アドレス(メイン)は格下げされます。 これを行うと、アカウントに複数の電子メール アドレス(メイン)を設定できますが、ネイティブ システムでは許可されていません。 これは、新しい電子メール アドレス(メイン)を追加する前に、最初に既存の電子メール アドレス(メイン)を格下げすることで回避できます。

INI ファイルまでの PKI パスが長いと、プロビジョニング サーバが再起動されることがあります

UNC パスが 77 文字を超えると、オペレーティング システムが再起動されます。 これを回避するには、長いパスを使用しないことです。

PKI アカウントが重複して表示されます

PKI コネクタは、Entrust PKI 階層エンドポイントをサポートしていないため、すべてのアカウントを階層なしのリストに保存しています。 このため、一意の Entrust PKI アカウントが PKI コネクタに対して重複して表示されます。

PKI グループ プロパティ シートが正しく表示されません

プロビジョニング サーバで PKI グループ プロパティ シートを開こうとすると、エラーメッセージ「Unable to display the requested property sheet」が表示されます。

PKI アカウントを作成すると電子メール通知の警告が発生します

プロキシ プロファイルを使用して PKI エンドポイントを取得し電子メール通知が 1 になると、「プロファイルの作成」オプションを指定しないで新しい PKI アカウントを作成することはできません。

この問題を回避するには、以下のいずれかの操作を実行します。

- プロキシ プロファイルを使用せずにエンドポイントを取得します。
- エンドポイントの取得時に電子メール通知を無効にし、エンドポイントに移動して手動で参照番号を確認します。

SAP 契約上のユーザ タイプの割り当て

契約上のユーザ タイプを[License Data]タブのユーザに割り当てる場合は、変更は主システムにのみ適用され、子システムには適用できません。

子の契約上のライセンス タイプを固有に変更することは可能です。

SAP 契約上のユーザ タイプ属性の必須フィールド

アカウントの[License Data]タブに指定できる契約上のユーザ タイプは、[LIC_TYPE]フィールド以外に必須フィールドを設定することはできません。 たとえば、契約上のユーザ タイプを使用するのに SAP R3 システム(SYSID)の名前を指定する必要がある場合は、割り当てに失敗して SAP R3 システムの名前の値が欠けているとのエラーが表示されます。

PLS コネクタへのリクエスト中に C++ コネクタ サーバがクラッシュすることがあります

PLS コネクタへのリクエスト中に CCS がクラッシュした場合、ポリシー サーバのインストールを調査する必要があります。これは、そのことが原因である可能性があるためです。Access Control サービスが常に再起動されるため、ポリシー サーバへのリクエストに大幅な速度低下の兆候が見られます。

SBL アカウントの一時停止

SBL アカウントまたは SBL アカウント テンプレートを変更し、アカウントを使用して変更を同期する場合、他の変更と一緒に eTSuspended を設定しないでください。これは、他の属性の変更が無視されるためです。

これを回避するには、変更を eTSuspended 変更を含むリクエストと他の属性の値に対する変更を含むリクエストの 2 つのリクエストに分割してください。

JIAM RSA のアカウントの同期化チェックのレポートに誤りがある

RSA アカウントで JIAM を使用してアカウントの同期化チェック操作を実行する場合、エンドポイントにアカウントがないと、コネクタ サーバが成功の通知と「Account missing from endpoint」というメッセージを返す代わりに、誤って「Connector Server Read failed: Sd_GetSerialByLogin Error Invalid user」というエラー メッセージを返します。 プロビジョニング マネージャからのアカウントの同期が正しく機能していることを確認してください。

OS/400 ユーザから複数のグループを削除するとプロビジョニング サーバが応答しなくなります

一度の操作でユーザから複数のグループ（「#」で始まる 1 つ以上のグループ）を削除すると、プロビジョニング サーバが応答しなくなることがあります。

これを回避するには、一度に 1 つのグループを削除してください。

OS/400 アカウントでプライマリ グループを削除できません

OS/400 グループのメンバシップは、グループ メンバであるアカウントを変更するか、グループのメンバシップを変更することで変更できます。 グループのメンバシップを変更する場合、グループのメンバシップがプライマリ グループのメンバシップである場合はアカウントを削除できません。

これを回避するには、アカウントを変更してからプライマリ グループのメンバシップを削除してください。

FND コネクタの応答リストに「開始日」および「終了日」の両方の日付を含める必要があります

FND コネクタの応答リストには「開始日」および「終了日」の両方の日付が含まれている必要があります。そうでない場合は、応答リストが不安定になり元に戻すことができなくなります。

この問題を回避するには、FND アカウントまたはアカウントテンプレートの作成および変更中に、（たとえば、「開始日」および「終了日」の日付を空白にする代わりに過去または未来の日付を使用して）、応答リストで常に「開始日」および「終了日」の日付を指定する必要があります。

VISTA の Host to Caft 定義が動作しません

N16 リモート エージェントを VISTA または VISTA SP1 エンドポイントにインストールしており、[すべてのプログラム] -> [CA] - > [Identity Manager] -> [Host to Caft Definition]から管理サーバを追加し、VISTA マシンをエンドポイントとして取得しようとしている場合は、「アクセスが拒否されました」というエラー メッセージが表示されます。

これを回避するには、コマンド プロンプトを開き、以下のコマンドを発行してエンドポイントを取得します。

```
cafthost -a <hostname/IP>
```

LND アカウントのカスタム ID の場所および組織単位の証明書 ID に対しては絶対パスを使用します

アカウントのカスタム ID の場所および組織単位の証明書 ID にアクセスするときに UNC パスを使用しても、相対パスにある共有フォルダが常に動作するとは限りません。絶対パス(ドライブ文字を含む)を使用することをお勧めします。

SPML の LND 検索要求で検索結果が返ってきません

SPML または SPML サーバを介して検索要求を実行する場合、lastName および homeServer 以外の属性を使用するときは、検索結果が返ってきません。

SPML で作成された LND アカウントとグローバル ユーザを関連付けることができません

プロビジョニング マネージャでは、現在、SPML を介して作成されたアカウントとグローバル ユーザを関連付けることはできません。

LND アカウント名に日本語文字を使用しないでください

アカウント名に日本語文字が含まれているアカウントは、現在、ID パスワードを変更することはできません。 アカウント ID のファイルで英文字を使用すれば、この問題は解決します。

「User Unique OU」を使用して LND アカウントを作成できません

「User Unique OU」を使用してアカウントを作成することはできません。 このようにして作成されたアカウントは、プロビジョニング マネージャで検索したりアクセスしたりすることができません。

LND Account Short Name 属性には 85 文字以上の日本語文字を含めることができません

Account Short Name 属性に 85 文字以上の日本語文字を使用すると、Domino サーバがクラッシュすることが確認されています。 この問題は、Account Name にも日本語文字が含まれている場合にのみ発生します。

Display LND アカウントのグループ メンバシップに日本語文字が含まれていると、プロビジョニング マネージャに表示されません

プロビジョニング マネージャでは、組織および組織単位で作成されたアカウントは、[親グループ]タブのグループ メンバシップには表示されません。

LND JCS コネクタから日本語文字を含む LND アカウントおよび認証者 ID にアクセスできません

LND JCS コネクタから、日本語文字を含むアカウントおよび認証者 ID にはアクセスできません。 これらの ID ファイルにアクセスするために必要なすべての機能は、このバージョンでは失敗することが確認されています。

LND オブジェクト DN パスに日本語文字があるとディレクトリの検索時に問題が発生します

オブジェクト DN パスに特定の日本語文字があると、ディレクトリの検索時にプロビジョニング サーバがハングされることが確認されています。 たとえば、0x80fd、0x4e88、および 0x5642 の Unicode を持つ日本語文字などが含まれます。

LND コネクタでは、検索された LND アカウントの階層の名前の変更や移動を行うことができません

このバージョンの LND コネクタでは、検索された LND アカウントの階層の名前の変更や移動を行うことはできません。 これらの操作を行うと、属性フィールドは無効になります。

これらの操作に対する回避策はありません。

カスタム アクションを使用して LND アカウントとそのメール ファイルを削除することができません

カスタム アクションを使用して LND アカウントとそのメール ファイルを削除する操作は失敗します。

プロビジョニング マネージャではエラー メッセージも生成されませんが、エンドポイントを検査すると、アカウントとメールファイルがまだそこにあることが表示されます。 これに対するプロビジョニング マネージャを使用した回避策はありません。

LND アカウントのメールが登録中に作成されません

プロビジョニング マネージャの LND アカウント作成ウィンドウの[プロファイル]タブページには、「Create Replicas」と呼ばれるチェック ボックスがあります。

クラスタ化された環境にある Domino エンドポイントを管理するときに、「Create Replicas」チェックボックスがオンになっている場合は、アカウントの複製とメール ファイルをクラスタ化環境でも作成する必要があります。 複製のメール ファイルの作成は、このリリースでの登録中には処理されません。

第 7 章: ドキュメント

Identity Manager r12 ガイドのファイル名は、以下のとおりです。

マニュアル名	ファイル名
リリース ノート	im_release_enu.pdf
実装ガイド	im_impl_enu.pdf
WebLogic のインストール ガイド	im_install_weblogic_enu.pdf
WebSphere のインストール ガイド	im_install_websphere_enu.pdf
JBoss のインストール ガイド	im_install_jboss_enu.pdf
「Configuration Guide」	im_config_enu.pdf
高可用性ガイド	im_high_avail_enu.pdf
管理ガイド	im_admin_enu.pdf
Programming Guide for Java	im_dev_enu.pdf
Programming Guide for Provisioning	im_dev_provisioning_enu.pdf
プロビジョニング ガイド	im_provisioning_enu.pdf
コネクタ ガイド	im_connectors_enu.pdf
コネクタ Xpress ガイド	im_connector_xpress_enu.pdf
Java コネクタ サーバ実装ガイド	im_jcs_impl_enu.pdf
Programming Guide for Java Connector Server	im_jcsProg_Enu.pdf
iRecorder 統合ガイド	audit_im_irec_ref_enu.pdf
用語集	im_glossary.pdf
マニュアル選択メニュー	im_bookshelf_enu.zip

Identity Manager r12 ガイドは、以下の場所からダウンロードできます。

- CA Support サイト

PDF ファイルを表示するには、Adobe Reader 7 以上を使用する必要があります。まだコンピュータにインストールされていない場合は、Adobe の Web サイトからダウンロードして、インストールしてください。

注: 最高の性能を発揮できるように、「マニュアル選択メニュー」をリモート システムにインストールする場合は、Web サーバからマニュアル選択メニューにアクセスできるようにしてください。

このセクションは、以下のトピックから構成されます。

ブックシェルフ (70 ページ)
オンライン ヘルプの拡張機能 (71 ページ)
eTrust の CA への商標変更 (72 ページ)
プロビジョニング用語の変更 (72 ページ)
Embedded IAM (EIAM) コネクタの新しい名前 (72 ページ)
プログラミング マニュアル (73 ページ)

ブックシェルフ

ブックシェルフでは、単一インターフェースから、すべての Identity Manager ドキュメントにアクセスできます。 ブックシェルフには、以下が含まれています。

- HTML 形式での全ガイドのコンテンツの拡張リスト
- ランク付けされた検索結果およびコンテンツ内で強調表示された検索語付きの全ガイドにわたる全文検索
- 上位レベルのトピックへ導くパンくずリスト
- 全ガイド内のトピックへの単一 HTML インデックス
- ガイドの印刷用 PDF 版へのリンク

ブックシェルフを使用するには、以下の手順に従います。

1. ブックシェルフを CA サポート サイトからダウンロードします。
2. ZIP ファイルの中身を展開します。
3. ブックシェルフは、以下のとおり表示されます。
   - ブックシェルフが、ローカル システム上にあり、Internet Explorer を使用している場合は、Bookshelf.hta ファイルを開きます。
   - ブックシェルフが、リモート システム上にあるか、または Mozilla Firefox を使用している場合は、Bookshelf.html ファイルを開きます。

     注: 最高の性能を発揮できるように、ブックシェルフをリモート システムにインストールする場合は、Web サーバからブックシェルフにアクセスできるようにしてください。

ブックシェルフは、Internet Explorer 6 または 7、もしくは Mozilla Firefox 2 を必要とします。 PDF ガイドを利用するには、Adobe Reader 7 または 8 が必要です。 Adobe Reader は、www.adobe.com でダウンロードできます。

注: r12 および r6.0 SP5 の CA SiteMinder ブックシェルフは、CA サポート サイトで公開されています。これは、Identity Manager で使われているものと同じブックシェルフ形式を使用しています。

オンライン ヘルプの拡張機能

ユーザ コンソール オンライン ヘルプおよび管理コンソール オンライン ヘルプの両方に、以下の機能があります。

パンくずリスト

ヘルプ階層のどこにいるかをわかりやすいナビゲーションで示します。 これらの機能は、ヘルプ ページの上部にあります。

検索の強調表示

結果ページで結果のコンテンツを黄色の強調表示で識別します。

ナビゲーション ボタン

ナビゲーションをスムーズにするため、前矢印ボタンおよび次矢印ボタンを表示しています。 これらの機能は、パンくずリストの下のヘルプ ページの上部にあります。

eTrust の CA への商標変更

いくつかの CA セキュリティ製品の商標は、現在「eTrust」から「CA」に移行されています。 この移行中、ドキュメント内では、eTrust 製品および CA 製品の両方への参照が含まれます。 たとえば、eTrust Directory は、次のリリースでは、CA Directory に商標変更されます。ドキュメント内での eTrust 製品のいずれの説明も、新しい CA 商標を持つ同一製品の説明に相当します。

プロビジョニング用語の変更

既存の eTrust Admin の顧客には、特定の用語が変更されて、eTrust Admin が CA Identity Manager の一部になって、表示される場合があります。 以下の表は、この変更を示しています。

eTrust Admin 用語	Identity Manager における新しい用語
eTrust 管理サーバ	プロビジョニング サーバ
eTrust Admin マネージャ	一般マネージャ
ディレクトリ	エンドポイント、エンドポイント
名前空間	エンドポイントのタイプ
ポリシーまたはポリシー フォルダ	アカウント テンプレート
ロール	プロビジョニング ロール
分散 SuperAgent フレームワーク	コネクタ サーバ フレームワーク
SuperAgent	C++ コネクタ サーバ
オプション	コネクタ
管理ディレクトリまたは管理リポジトリ	プロビジョニング ディレクトリ
Identity Manager の企業ディレクトリ	Identity Manager のユーザ ストア
企業ユーザ	インバウンド管理者

Embedded IAM（EIAM）コネクタの新しい名前

注: CA Identity Manager r12 製品マニュアルでは、Embedded Entitlement Manager（EEM）とは、Embedded Identity and Access Manager（EIAM）コネクタを指します。

プログラミング マニュアル

Identity Manager r12 ドキュメント セットには、2 冊のプログラミング ガイドが含まれています。

Programming Guide for Java

以前は「Identity Manager Developer's Guide」というタイトルが付けられていたこのマニュアルは、Identity Manager の Java API の使用についての情報を提供します。HTML バージョンは、Javadoc ページに統合され、相互参照の関連情報に必要なハイパーリンクを含みます。

Programming Guide for Provisioning

以前は「eTrust Admin SDK 開発者ガイド」というタイトルが付けられていたこのマニュアルは、Identity Manager プロビジョニング サーバ SDK についてのプログラミング情報を提供します。 開発者は、C++ でのプログラミングについての知識が必要です。