# CA Identity Manager

## Release Notes

r12

# CA Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Security Command Center (SCC)
- CA Audit
- eTrust® Directory, also known as CA Directory

# Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

# Contents

# Chapter 1: Welcome

This document contains operating system support, installation considerations, known issues, and information about contacting CA Technical Support.

# Chapter 2: New Features

This section contains the following topics:



## Supported Platforms and Versions

In Identity Manager r12, there have been some additions made to supported application server versions, directories, and databases.

**Note**: For a complete list of supported platforms and versions, see the Identity Manager Support Matrix on the Identity Manager support site http://ca.com/support.

# Identity Manager Architecture

The Identity Manager r12 architecture includes the following changes from previous versions:

- **Embedded Provisioning Server and Provisioning Manager**

  The Provisioning Server is the server that manages additional accounts that are assigned to an Identity Manager user. When you assign a provisioning role to an Identity Manager user, the Provisioning Server creates accounts on endpoints that meet the requirements of the role. For example, if you assign a provisioning role that includes an Exchange account template, the Provisioning Server assigns an Exchange account to the user.

  The Provisioning Manager is the user interface for managing endpoint types, such as Exchange or Oracle, and endpoints, such as a specific system where Exchange is installed. This interface was formerly called eTrust Admin Manager. Other capabilities exist in Provisioning Manager, such as exploring and correlating accounts; however, that additional functionality is now duplicated in the Identity Manager User Console, where it is more easily accessed.

  Previous versions of Identity Manager required eTrust Admin for provisioning.

  **Note:** The Provisioning Server and Provisioning Manager are optional components.

- **Identity Manager Integration with SiteMinder**

  SiteMinder is no longer a prerequisite for installing Identity Manager. You can now optionally integrate with SiteMinder to provide advanced functionality, including SiteMinder authentication and advanced Password Policies.

  Previous versions of Identity Manager required SiteMinder for the following functionality:

  - Authentication
  - Storage of role and task information (in the policy store)
  - Connection to a user store
  - Password policies

  In Identity Manager, this functionality is provided natively.

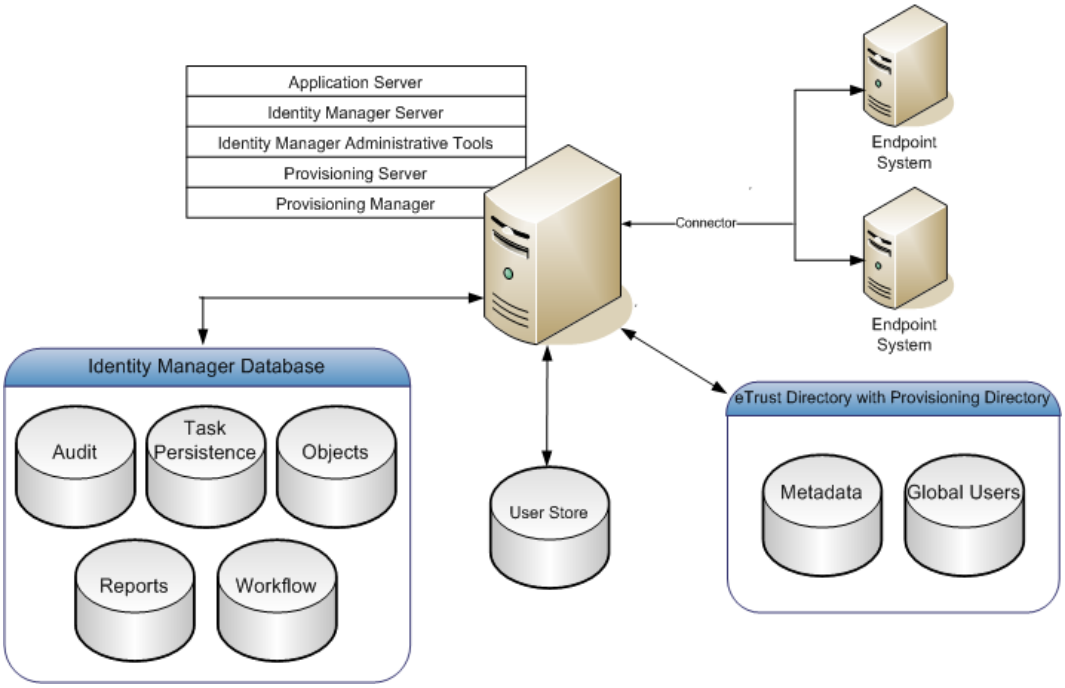
  **Note:** You can integrate with SiteMinder to provide advanced functionality, including SiteMinder authentication and advanced Password Policies.

- **Object Store**

  Identity Manager r12 now stores role and task information in a new object store. The object store is a relational database that is automatically configured by Identity Manager at runtime.

The following illustration depicts an Identity Manager implementation that includes provisioning.

**Note:** The Provisioning Directory, which stores information required to use provisioning and information about global users, must be installed in eTrust Directory, a prerequisite for installing Identity Manager with provisioning.




# Installer Improvements

All the components needed for Identity Manager server installation are now installed with one installer; this includes components for provisioning and extensions for a SiteMinder Policy Server.

The Identity Manager installer provides the Identity Manager Provisioning Server, Provisioning Directory, and Provisioning Manager. It also configures connections to the databases that store object data and data for workflow, task persistence, reporting, and auditing.

Changes made to the Identity Manager installation include the following:

- Identity Manager no longer requires SiteMinder for authentication.
- Task persistence is no longer optional and is enabled upon installation.
- A database schema is extended automatically for each database used by Identity Manager.
- The Administrative Tools are now installed in the following locations:
  - **Windows:** C:\Program Files\CA\IAM Suite\Identity Manager\tools
  - **UNIX:** *HOME*/CA/IAM_Suite/Identity_Manager/tools
- Post-installation scripts are no longer required.

# Reporting Enhancements

Identity Manager reports enable you to see the current state of an Identity Manager environment. You can use this information to ensure compliance with internal business policies or external regulations.

Identity Manager r12 includes the following enhancements for reports:

- **Integration with the IAM Report Server**

  Identity Manager r12 uses Business Objects Enterprise XI to design, manage, and view reports from the reporting database. Identity Manager provides a runtime version of Business Objects, so no separate license is required.

- **New admin tasks for exporting data to the Reporting Database**

  Identity Manager includes new default tasks, which allow you to export data from Identity Manager to the reporting database. Each time you export data to the reporting database, you create a *snapshot*, a representation of the current state of user-specified objects in an Identity Manager environment.

  Using the new default tasks, you can create snapshot definitions and capture a snapshot from which you can generate a report.

- **Additional Pre-defined Reports**

  Identity Manager includes the following pre-defined reports that you can use as installed or customize to suit your business needs:

  - **Endpoint Accounts**

    List of accounts by account name, owner and creation time for each endpoint, sorted by endpoint type.

  - **Non-Standard Accounts**

    List of the non-standard accounts such as orphan accounts and system accounts.

  - **Non-Standard Account Trends**

    Non-standard account trends by non-standard account type displayed as graphs.

  - **Orphan Accounts**

    List of accounts that are not associated with a user. Orphan accounts are listed by account name, owner and creation time for each endpoint and are sorted by endpoint type.

  - **Policies**

    List of policies, including policy conditions, and Action on Apply and Action on Remove actions.

  - **Role Administrators**

    List of role administrators.

  - **Role Members**

    List of role members.

  - **Role Owners**

    List of role owners.

  - **Roles**

    List of roles and their description.

  - **Snapshots**

    List of all available snapshots in the report database.

  - **Task Roles**

    List tasks by description, category and type. For each task, specify all associated roles.

  - **User Accounts**

    List of accounts by user. User accounts are listed by account name, account attributes and endpoint, sorted by endpoint type.

- **User Policy Sync Status**

  List of users, which includes policies that are currently allocated and policies that should be reallocated.

- **User Profile**

  List of users with all available information we have on it.

- **User Entitlements**

  List of users and their associated accounts, roles and groups.

# Connection Management

Connection Management is used to configure database server connection details in Identity Manager. When Identity Manager has to connect to a database server, it uses the Connection details to connect to the database server. Connection Management allows you to create multiple connections to different database servers under a Connection Type. For each Connection Type you can specify a default connection. You must configure a primary Connection Type for Identity Manager through the Management Console.

# Provisioning Enhancements

At this release, you can perform more actions in the Identity Manager user console. Some of these capabilities were available previously in eTrust Admin Manager. You can use the User Console to:

- Explore and correlate accounts on endpoints
- Correlate orphan and system accounts with an Identity Manager user
- Audit provisioning actions, such as assigning a provisioning role to a global user

In addition, this release includes:

- Connector Xpress, a graphical tool for building custom connectors
- Dynamic Connector (JNDI and JDBC) support for use with XML metadata that is generated from Connector Xpress
- Java Connector Server, a server that handles requests from Java connectors
- High availability features for the C++ Connector Server, formerly called the Super Agent.
- New Java Connectors for Kerberos to administer Kerberos principals and Kerberos password policies on Solaris servers.

- New Java Connectors for SAP (with CUA support)
- New Java connectors for Oracle, MS-SQL, and 0S/400, supplied with the Java Connector Server.

  These three connectors replace the sample options, which are no longer supported.
- Enhancements to Provisioning Manager that provides a generic UI for Dynamic JDBC and JNDI endpoint types created using Connector Xpress.

### DYN GUI

We have enhanced the DYN GUI in the Provisioning Manager to provide an enhanced set of features that allow you to manipulate arbitrary endpoint objects with a single Provisioning Manager plug-in.

For example, when you map a field in Connector Xpress, an item is placed in the metadata to represents that field. Whenever you examine any object in that connector, the DYN GUI uses the metadata to display the appropriate fields.

The changes in this release expand the capabilities of the DYN GUI with an enhanced set of features, make the future addition of new features simpler, and provide a better display for the user.

## Lotus Notes/Domino Connector Released as a Technical Preview

For the r12 release of Identity Manager, the java-based LND Connector is being released as a Technical Preview only.

This connector is **not** certified for production environments. The fully certified connector will be available in a CR release. Contact your CA Account Representative for details.

**Note:** Do not install the C++ LND Connector and the Java LND Connector in the same Identity Manager environment.

## Enhanced Status Reporting

Identity Manager r12 includes several features that allow you to view the status of Identity Manager tasks.

## View Submitted Task Improvements

Identity Manager r12 includes the View Submitted Task tab, which lets you view the status of a task, the dependency of a task on other tasks, events, and workflow.

In Identity Manager r12, the View Submitted Task tab includes the following enhancements:

- The View Submitted Task tab now displays more detail about tasks and their associated events.
- You can cancel pending tasks, and resubmit or reject failed tasks from the View Submitted Tasks tab.
- You can now configure the View Submitted Tasks tab.

## The View User Activity Task

User activity is a history of tasks that involve a specific user. Administrators can use the View User Activity task to track the following user information:

- Tasks performed on the user
- Tasks performed by the user
- Workflow approvals performed by the user

**To view user activity**

1. Click Users, Manage Users, View User Activity.

   The Select User screen appears.

2. Search for a user and click Select.

   The View User Activity screen appears.

   For more information on the user activity displayed, see the *User Console Online Help*.

## User History Tab

The User History tab allows you to view tasks that are related to a user. You can add this tab to a Modify or View User task.

**Note:** This tab is included in the default View User Activity task.

The task details that are displayed in this tab can also be viewed in the View Submitted Tasks tab.

# Workflow Enhancements

Identity Manager r12 includes enhancements to workflow functionality that simplify the workflow creation process and add new features. These enhancements are described in the following sections.

## Workflow Process Templates

Workflow process templates allow you to configure and manage workflow control, entirely from within the Identity Manager User Console. These generic process templates can be configured to control most Identity Manager tasks and events.

The new process templates enable both task-level and event-level workflow control, easier participant resolver configuration for approvers, and multi-step approval processes.

The list of approvers can also be determined dynamically at run-time, depending on attributes of the task or event being approved.

## Task-Level Workflow

You can associate workflow processes with both tasks and events. This means that participants can approve or reject an entire Identity Manager task, or a specific event within a task.

Task-level workflow allows participants to review all events before deciding to approve or reject a request. When a workflow process is associated with a specific event within a task, an approver cannot see the overall task context within which a request is made.

## Workflow Action Buttons

You can add new buttons to workflow approval tasks to supplement or replace the standard approve and reject buttons.  An example of this feature is demonstrated in the online request tasks.

# Online Requests and History

In the User Console, users can request changes to their own accounts, and administrators can request changes to user accounts. These tasks trigger a workflow process template that requires up to three approvers: a consultant to comment on the request, a business user to approve the request, and a technical expert to implement the request.

The online request tasks also incorporate a new history control which allows approvers to attach notes or comments to the task at different stages of completion.

# Task Scheduling

Scheduling lets you automate the execution of a task at a later date. If you schedule a task that is associated with a workflow process, Identity Manager executes all the tasks as defined in that process. The status of the scheduled tasks can be viewed in the View Submitted Tasks page.

A scheduled task that is not yet executed by Identity Manager can be rescheduled or cancelled through the View Submitted Tasks page.

Identity Manager provides the scheduler as a special tab. To access the scheduler, you must configure a task with the scheduler tab.

# User Console Enhancements

Identity Manager r12 includes multiple enhancements to add support for new features and simplify usability. These enhancements are outlined in the following sections.

## Custom Help

Identity Manager allows you to create your own custom help for tasks and tabs that you have customized in the User Console. To implement custom help, you can create a context-sensitive help system with custom HTML help files or Wiki pages and redirect help links within the Identity Manager User Console to access your custom help.

This feature also allows you to translate any of the default help (written in English) into another language.

## Nested Tasks

A nested task is an admin task that can be opened from the Profile tab of another task. Users of the first task open the nested task by clicking a link or button. For example, you can add a Delete User button to the Modify User task. If the user account is no longer valid, an administrator can click the Delete User button to remove the account without having to return to the navigation pane to select a new task.

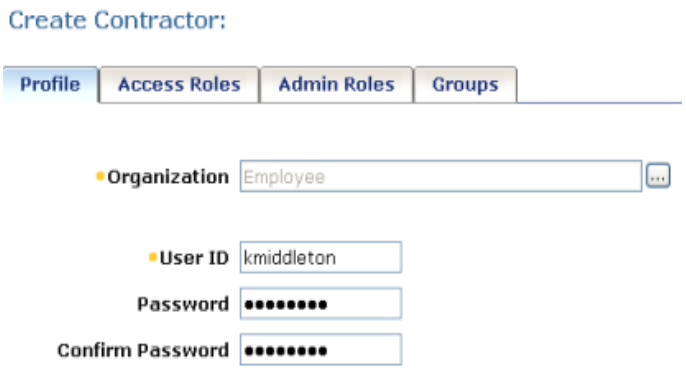
## Tab Controllers

A tab controller determines how the tabs in a task are displayed. You select one of the following tab controllers:

- **Standard Tab Controller**

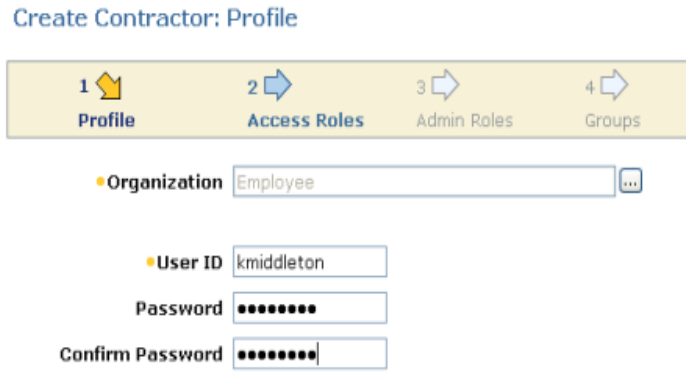
  Displays the tabs for the task as independent tabs. Users can use the tabs in the task in any order.

  This is the default tab controller.




- **Wizard Tab Controller**

  Displays the tabs in a task as a wizard. Administrators use each tab in order.



- **Sequence Tab Controller**

  Displays one tab, which is displayed as a single page, at a time. Users complete one tab and then click a custom button or link to move to the next tab.

  The sequence of tabs and the buttons and links that are displayed are determined programmatically by JavaScript that you write when you configure the sequence tab controller.

  In the custom JavaScript, you can specify the appearance and order of tabs based on user input. For example, if a user selects an option on the first tab, Identity Manager displays one page. If a user selects a different option, a different page is displayed.

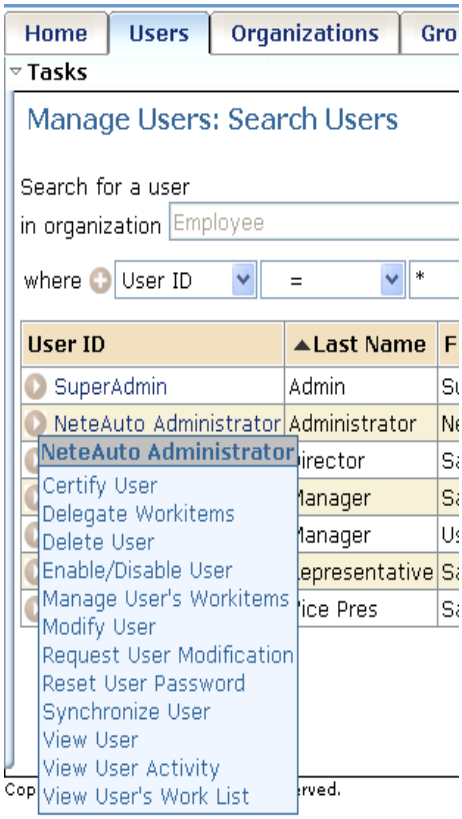

## Task Lists

Identity Manager r12 includes the following new default tasks that allow you to search for an object to manage:

- Manage Users
- Manage Groups
- Manage Organizations
- Manage Admin Roles
- Manage Admin Tasks
- Manage Access Roles
- Manage Access Tasks

Once you select the object, you can display a list of tasks that you can use to manage that object.

For example, to modify a user using this method, you select the Users category, then select the Manage User task. You search for and select the user that you want to manage. In the search results, click an icon to see a list of tasks that you can use to manage the selected user. From that list, you can select Modify User or any other appropriate task.




You can also configure task lists in tasks other than Manage tasks. For example, you can add a task list to a Membership tab. In this case, a task list is available for each member that appears on the Membership tab.

## Profile Tab Enhancements

In Identity Manager r12, the Profile tab includes several new configuration settings to support new functionality. These new settings are described in the following sections.

## Task Categories

Task categories allow you to organize tasks to make them easier to locate and search for in the User Console.

You can specify three task categories:

- Category 1 is the top level category for tasks. These categories are displayed as tabs across the top of the User Console.
- Category 2 is a second level category. This category enables you group related tasks in a top-level category. If you do not specify a second level category, the default category is Tasks.
- Category 3 contains the tasks that administrators use. When administrators click the Category 3 name in the User Console, a list of tasks in that category is displayed.

Within each category, you can control the order in which the items in that category are displayed by specifying a category order. For example, in the following illustration, the Employee tab has a category order of 3.


**Note:** When a category contains multiple tasks, the category order that is specified in the profile for each task must be the same. If the category order is different, multiple instances of that category tab will appear. For example, the Employee category contains two tasks: Create Employee and Modify Employee. If the category order in the Create Employee task is 3 and the category order in the Modify Employee is 6, the Employee category appears as two tabs.

### Task Priority

In Identity Manager r12, you can now specify a task priority to ensure that Identity Manager executes the most time-sensitive tasks first.

You can set the task priority to High, Medium, or Low on the Profile tab for the task. The default priority is Medium.

**Note:** You can use the View Submitted Tasks task to search for tasks with a specific priority, and then display their status.

### Custom Data for Select Boxes

Identity Manager task screens include fields that allow users to select a value. These fields include the following:

- Check Box Multi-Select
- Dropdown
- Dropdown Combo
- Multi-Select
- Option Selector
- Option Selector Combo
- Radio Button Single-Select
- Single-Select

You can specify custom data that you want to use to populate select boxes in XML files. For example, you can use the Select Box Data XML files to populate options for a City or State drop down box on a Profile tab for the Create User task.

You can also use the Select Box Data XML file to configure a dependency between two fields in a task screen. For example, the options that are available in the City field may depend on the option a user chooses in the State field.

### Date Picker Control

The Identity Manager User Console now includes a Date Picker style that can be applied to fields on a Profile tab that collect and display dates.

When the Date Picker style is applied, a calendar icon appears next to a date field. Users click the calendar icon to display a calendar control where they can select the date they want.

### Binary and Picture Controls

You can now configure Identity Manager to display a picture on a profile or include a binary attribute. For example, you can configure a user profile screen to display a digital photograph of the user being managed, or attach a document to the profile screen.

**Note:** This is only supported for LDAP user stores.

## User-defined Custom Attributes for Roles

Identity Manager supports user-defined custom attributes that allow you to filter roles in your organization effectively. For example, in your corporate environment you may have the need to create more than a thousand roles. You might want to categorize these roles by business units or by geographical locations. If you want to search for roles that are specific to a particular geographical location, you can use the custom attributes to filter the roles in your organization.

You can use custom attributes in the Create, Modify, and View tasks for the following roles:

- Access Roles
- Admin Roles

You must perform the following steps to add custom attributes to admin tasks and search screens.

1. Add custom attributes to any of the admin tasks that are defined for roles.
2. Configure the search screens for roles with custom attributes.

## Bulk Loader

You can use the Bulk Loader tab in the User Console to upload feeder files that are used to manipulate large numbers of managed objects simultaneously. For example, you can create 1000 users in Identity Manager manually, or you can use the Bulk Loader. The advantage of the Bulk Loader method is that you can automate the process of manipulating a large number of managed objects using an information (feeder) file. The Bulk Loader task can also be mapped to a workflow process.

**Note:** CSV is the supported file format for the feeder, but you can create a custom feed for other file formats.

# Default Organization Search Based on User

To simplify the User Console, Identity Manager allows an administrator to configure a default organization for the Create User task based on the user trying to execute the task. When a user executes a Create User task, the organization will not be displayed on the Create User Profile tab, but will be set by default based on the user's organization.

**To configure a default organization based on a user**

1. In the Identity Manager User Console, go to Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Select the Create User task.
3. On the Tabs tab, click the right arrow icon next to Profile.
4. Click the ... (ellipses) button to display a list of screens to edit.
5. Select the Create User Profile screen and click Edit.
6. Search for Organization and click the right arrow icon to edit.

   **Note:** This field will not be present in an environment with no Organizations.
7. Set Style to Hidden.
8. In the Default JavaScript field, enter the following:

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

9. Click Apply.

# IPv6 Support

When configuring Identity Manager, you can enter both IPv4 and IPv6 addresses.

Identity Manager will support IPv6 on the following operating systems:

- Solaris 8 or higher
- Windows XP SP1 or higher
- Windows 2003 or higher

Each application server has specific JDK requirements:

- For a JBoss application server on a standalone system, Identity Manager supports IPv6 with JDK1.4.2_13 or 1.5 (on Solaris) or JDK1.5 (on Windows).
- For a JBoss cluster, no JDK is available to work with IPv6 as of release time for Identity Manager r12. If a JDK is released that works with IPv6, the platform support matrix will be updated.
- However, for a JBoss cluster that uses an IPv4/IPv6 stack, Identity Manager supports IPv6 with JDK1.4.2_13 or 1.5 (on Solaris) or JDK1.5 (on Windows).
- WebLogic and WebSphere application servers include JDK 1.5, which supports IPv6 addresses.

Note the following before configuring an environment that supports IPv6:

- For Identity Manager to support IPv6 addresses, all components in the Identity Manager implementation, including the operating system, JDK, directory servers, and databases must also support IPv6 addresses.
- If Identity Manager integrates with SiteMinder, the web server plug-in for the application server must also support IPv6.
- When you connect to SiteMinder or any database from Identity Manager using a JDBC connection, specify the hostname not the IP address.
- The IAM Report Server can be installed on a dual-stack host, which supports IPv4 and IPv6, but the communication to the server must be IPv4.

  When you configure a connection to the report server in the Management Console, the server name should be in IPV4 format.

# FIPS 140-2

Identity Manager r12 supports FIPS 140-2 in a new installation *only*. Also, Identity Manager comes with a Password Tool for providing a FIPS encryption key, which is located in the following directory:

C:\Program Files\CA\IAM Suite\Identity Manager\tools\PasswordTool

Note the following when enabling FIPS 140-2 for an Identity Manager environment:

- Once FIPS 140-2 support is enabled for an Identity Manager deployment, you cannot disable it. Similary, if you install Identity Manager without enabling FIPS 140-2 support, you cannot add support at a later time.
- If you want to enable FIPS 140-2 in an Identity Manager deployment that includes SiteMinder, the SiteMinder version must be r12.

# Enhanced Localization Support

The Identity Manager User Console and the User Console online help are available in the following languages:

- French
- Korean
- Japanese
- German
- Simplified Chinese
- Spanish
- Italian

**Note:** For information on using Identity Manager in one of these languages, see the *Configuration Guide*.

**More information:**

Installing Localized Identity Manager Environments (see page 39)

# Chapter 3: Changes to Existing Features

This section contains the following topics:



## Servlet Filter Agent Deprecated

The Servlet Filter Agent is deprecated in Identity Manager r12. We recommend the use of a Web Agent in place of a Servlet Filter Agent. If you have a Servlet Filter Agent already deployed in an *existing* Identity Manager environment, it will still work and will be supported.

## Management Console Enhancements

The Identity Manager Management Console includes the following new or changed screens:

- User Console page—Use this page to configure general settings for an Identity Manager User Console, including the icon and title, and the authentication class and logout page.

  **Note:** In Identity Manager, you configured the icon and title settings in the Themes page. The functionality on the Themes page has moved to the User Console page, and the Themes page has been removed.

- Environments page—You can now stop and start an Identity Manager environment from the Environments page. You do not have to restart the application server for environment changes to take effect.

- Provisioning page—This page no longer includes inbound synchronization configuration. To configure inbound synchronization, see the *Provisioning Guide*.

- Task Persistence page—Task persistence is now configured automatically during installation. You no longer need to enable task persistence manually. This page has been removed.

# Password Policy Changes

Since new Identity Manager r12 installations no longer require SiteMinder, there are some changes to the default Password Policy functionality. In deployments that do not integrate with SiteMinder, Identity Manager enables you to create basic password policies that manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage.

If you configure Identity Manager to integrate with SiteMinder, you can create advanced Password Policies that enable you to define the additional rules and restrictions:

- Directory filters
- Password expiration:
  - Track failed or successful logins
  - Authenticate on login
  - Password expiration if not changed
  - Password inactivity
  - Incorrect password
- Multiple regular expressions
- Password restrictions:
  - Minimum days before reuse
  - Minimum number of passwords before reuse
  - Percent different from last password
  - Ignore sequence when checking for difference
  - Profile attribute matching
  - Dictionary matching

# imrexport Tool Deprecated

The imrexport tool functionality has been integrated into the Identity Manager User Console. The Capture Snapshot Data task under the Reports tab now performs the functionality of the imrexport tool in Identity Manager r12.

# z/OS Connectors Architecture Change

The z/OS connectors (CA ACF2, CA Top Secret and RACF) have been re-architected for performance reasons to now use the CA LDAP Server for z/OS instead of the CA DSI Server on z/OS.

Any provisioning server configuration file options that relate to the CA LDAP Server are now entered and stored on z/OS when the CA LDAP Server is installed. Also,mainframe LDAP Server connection information is now entered through the Provisioning Manager endpoint task view.

# Features No Longer Supported

Some eTrust Admin features are no longer available in Identity Manager r12. The following table lists the new features to use in Identity Manager r12.

| eTrust Admin Feature | Identity Manager Feature |
|---|---|
| Advanced Workflow | WorkPoint Workflow |
| Legacy Workflow | WorkPoint Workflow |
| Self Administration Web Interface (SAWI) | Identity Manager self-service |
| Delegated Administration Web Interface (DAWI) | Identity Manager delegated administration |
| IA Manager | Identity Manager self-service tasks and delegated administration |
| eTrust Admin Reporting<br>etaReport | Identity Manager reporting |
| PeopleSoft Feed Option | Bulk Loader |
| Universal Feed Option | Bulk Loader |
| SAP Option (C++ version) | SAP Connector (Java version) |
| MS SQL Option (C++ version) | MS SQL Connector (Java version) |
| Oracle Option (C++ version) | Oracle Connector (Java version) |
| OS/400 Option | OS/400 Connector (Java version) |
| CleverPath Portal Option | No replacement |

**Note:** Existing versions (available with eTrust Admin 8.1 SP2) of the PeopleSoft Feed Option and the Universal Feed Option will continue to work with Identity Manager r12.

# Chapter 4: System Requirements

The following minimum hardware is required for the system that will host the Identity Manager Server:

- CPU: Single or dual-processor, Intel Pentium III (or compatible) 700-900 MHz, or Sparc Workstation 440MHz
- Memory: 2 GB
- Available disk space: 1 GB

**Note:** These hardware requirements take into account the requirements of the application server that must be installed on the system where you install the Identity Manager Server.

# Chapter 5: Installation Considerations

This section contains the following topics:



## Support Matrix Location

For a complete list of supported software versions, see the Identity Manager support matrix.

**To locate the support matrix**

1. Log into support.ca.com.
2. Click Support By Product or Solution.
3. Select CA Identity Manager in the Products section under Select a Product or Solution page.

   The CA Identity Manager page opens.
4. Scroll to Recommend Readings.
5. Click CA Identity Manager Informational Documentation Index.

A page displays platform support matrices for supported versions of Identity Manager.

# Solaris Patches Required

Prior to installing provisioning on Solaris 9 or 10, download and install patches:

**To download the Sun Studio 10 patches for the SDK**

1. Go to the following URL:
   http://developers.sun.com/prodtech/cc/downloads/patches/ss10_patches.html
2. Download and install patch 117830.

   **Note**: Sun Studio 11 does not require patching.

**To download Solaris 9 patches for all components**

1. Go to the following URL:

   http://search.sun.com/search/onesearch/index.jsp
2. Download and install 9_recommended.zip

# Environment Variable Needed For SiteMinder Integration

When you install Identity Manager on a Solaris system and enable integration with SiteMinder, you may see the following error in the application server log, and Identity Manager may fail to start:

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

This failure occurs if the ETPKI installation, which installs an encryption library required by SiteMinder, does not add the CALIB environment variable correctly.

**Note:** The ETPKI is installed automatically by the Identity Manager Installer.

**Workaround**

Add the CALIB environment variable as follows before starting the Identity Manager Server:

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

# Installing Localized Identity Manager Environments

Identity Manager includes translated versions of the Identity Manager User Console and the User Console online help. Most of the files that are required to use a translated version are installed in the following location:

*im_admin_tools_dir*\samples\Localization*language*

***im_admin_tools_dir***

Specifies the installed location of the Identity Manager Administrative Tools.

***language***

Specifies the language that you want to use.

**Note:** For installation instructions, see the *Configuration Guide*.

However, there are additional files required to use a translated version of Identity Manager:

- Release Notes
- Online Help files

  **Note:** Do not use the version of the online help files that are available in *im_admin_tools_dir*\samples\Localization*language.*

These files are available in the CA Identity Manager r12 Localization Resources download, which is available on the CA support site.

**To install the online help files**

1. Download the CA Identity Manager r12 Localization Resources ZIP file.
2. Unzip the files on a system that is accessible from the application server that hosts Identity Manager.
3. Copy the im_help_*language*.ZIP file for the appropriate language to the *IdentityMinder.ear*\user_console.war\

   *IdentityMinder.ear*

   The deployed location of the Identity Manager application (IdentityManager.ear) on the application server.

   **Note:** Consider creating a backup copy of the default online help before replacing it with a translated version. The default online help is overwritten by the translated version.
4. Unzip the im_help.zip in the user_console.war directory.
5. Restart the Identity Manager environment.

   The translated version of the online help is available for use.

# Non-ASCII Character Causes Installation Failure on Non-English Systems

During Identity Manager installation, the installer extracts files to a Temp directory. On some localized systems, the default path to the Temp directory contains non-ascii characters. For example, the default path to the Temp directory on a Spanish Windows system is the following:

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

The non-ASCII characters cause the installer to display a blank Pre-Installation Summary page, and then cause the installation to fail.

**To prevent the installation from failing**

Change the tmp environment variable to point to a folder that contains only ASCII characters.

# Configuration Changes Required For SiteMinder FIPS 140-2 Only Mode

If SiteMinder is in FIPS 140-2 Only mode, an additional configuration step is required.

**To configure Identity Manager to work with SiteMinder in FIPS 140-2 Only mode on WebLogic or JBoss**

1. Open *IdentityMinder.ear*\policyserver.rar\META-INF\ra.xml.
2. Locate the following element:

```
<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. Change false to true in the <config-property-value> element.
4. Restart the application server.

**To configure Identity Manager to work with SiteMinder in FIPS 140-2 Only mode on WebSphere**

1. Open the WebSphere administrative console.
2. Navigate to the following location:

   Enterprise Applications > IdentityMinder > Manage Modules > policyserver.rar > IdentityMinder.PolicyServerRA > J2C connection factories > PolicyServerConnection > Custom properties
3. Click on the value of FIPSMode and change the value to true. Click on OK and then "save" link at the top of the page.

# JBoss: Configuring IPv6 Support

If you install the JBoss version of Identity Manager on a system that supports IPv6, some configuration is required.

**To configure IPv6 on a JBoss application server**

1. Open the run_idm.sh file, which is located in:

   *jboss_installation*\bin
2. Modify *one* of the the following properties in the JAVA_OPTS entry:
   - For IPv6 only environments, uncomment the followng entry:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv6Addresses=true
   - For IPv6/IPv4 environments, uncomment the following entry:

     set IDM_OPTS=%IDM_OPTS% -Djava.net.preferIPv4Stack=true
3. Save the file.

# SPML Support for FIPS 140-2

For Identity Manager r12, the SPML server is FIPS 140-2 compliant. We recommend deploying the SPML service on:

- Apache Tomcat Server 4.1.36 or a higher version of 4.1
- JDK 1.5.11 or a higher version of JDK 1.5. Note that Tomcat must be enabled to run in SSL mode. For details, see the Apache's administrator guide for Tomcat 4, (http://jakarta.apache.org/tomcat/) section "SSL Configuration HOW-TO."

If you use CA Tomcat instead of Apache Tomcat, Identity Manager r12 requires these workarounds for SPML:

- If you are using JDK 1.4.xx with CA Tomcat, FIPS 140-2 must be disabled. JDK 1.4.xx is incompatible with CA Tomcat because the RSA Jsafe CryptoJ 4.0 library needed for FIPS 140-2 support cannot be placed as the first security provider in JDK1.4.

  To disable FIPS 140-2 support, pass the JVM flag "-Dcom.ca.commons.security.fips=false" during Tomcat start up.

  - If you are running Tomcat from the command line, you can include the JVM flag catalina.bat. More details exist in the batch file itself.
  - If you are running Tomcat as windows service, pass the flag as follows:

    a. Using the registry editor, navigate to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CA Tomcat 4.1.29 eTrustIAMWebServer\Parameters"

    b. Add a String Value called "JVM Option Number n" where 'n' is the number following on from the previous JVM parameter. For the value, specify:

    Dcom.ca.commons.security.fips=false

    c. Increase by one the value of Edit DWORD Value "JVM Option Count" to account for the newly added parameter.

- If you are using JDK 1.5 with CA Tomcat, an incompatibility problem exists. To work around this problem:

  a. Manually remove the two Xerces libraries (xercesImpl.jar and xmlParserAPIs.jar) from %TOMCATHOME%\common\endorsed.

  b. Restart Tomcat.

# Z/OS Connectors Architecture Change

The z/OS connectors (CA ACF2, CA Top Secret and RACF) have been re-architected for performance reasons to now use the CA LDAP Server for z/OS instead of the CA DSI Server on z/OS.

Before trying to configure any z/OS connector you must install the CA LDAP Server for z/OS r12 which can be downloaded from support.ca.com.

# Location of eTrust Directory

The Provisioning Directory schema is installed on eTrust Directory. You can install eTrust Directory from the Identity Manager installation media.

# Fix Required Before Uninstalling eTrust Directory

If you need to uninstall eTrust Directory from a Windows system, you must apply a patch before beginning the uninstall procedure.

If you do not apply the patch, the uninstall procedure may remove license files which are required by other CA products.

You can download the patch on the CA Support site.

**To locate the patch**

1. Log into the support.ca.com.

   The CA Support site opens.

2. Click Licensing in the list of links on the left side of the page.

3. Click License Package 1.8 is Now Available.

   A page opens that describes the changes to the License Package, and includes a link for downloading it.

4. Follow the instruction to download and install the Windows patch.

# Chapter 6: Known Issues

This section contains the following topics:



## General

The following are general known issues in Identity Manager r12.

### Identity Manager EAR does not Auto-Deploy with WebLogic

If you are using WebLogic 8 or 9 in production mode, the Identity Manager EAR may not auto-deploy the first time you start the application server after an install or upgrade. If this should occur, deploy the IdentityMinder.ear manually from the user_projects\applications folder.

### Workflows and Group Members as Approvers

If a workflow process is configured in Workpoint Designer to have a specific group's members as its approvers, a workflow item may not be created for the event under workflow control, and the task session may fail.

The solution is to place the task under workflow control using the template method (with the SingleStepApproval or TwoStageApprovalProcess template), and define group members as the approvers (or participant resolvers).

## New Workpoint Properties May Need to be Set

Identity Manager includes a new version of Workpoint. In this version, you can configure additional new properties in GeneralMonitor.properties and workpoint-server.properties. Please note that these new properties are optional and should be added only if necessary.

The new workflow properties are as follows:

- In the GeneralMonitor.properties file:
  - #JMX_HTML_ADAPTOR_PORT=9092

    This property has been commented out by default. The property, when set to true, enables an HTML page that uses the generic Sun JMX adaptor, which is an unsecured web port that is separate from the Workpoint Management Console application. We recommend that customers leave this property commented out or set to false, and instead use the Workpoint Management Console for JMX access to Workpoint.
  - JOB_ERROR_STATE_ON_MAIL_ERROR=false

    This property is only applicable to customers who are using the Workpoint email feature. This property controls error handling in the mail monitor. If Identity Manager customers are using the mail function of Workpoint, this property may be applicable.

    **Note:** JOB_ERROR_STATE_ON_MAIL_ERROR defaults to true if not set. You may want to set it to false if you are using Workflow email, but don't want email errors affecting the job status.
  - ENABLE_SCRIPT_TASK_GROUPING=false

    This property controls if the script monitor should group together all concurrent scripts executing from the same job. If true, this will have the effect of assigning all scripts for a particular job to the same worker thread, where they will be executed one at a time. This is useful to prevent concurrency exceptions when you have multiple activities in a job that use an asynchronous script for automation and may be active at the same time.

    If you have customized workflow scripts and experience concurrency exceptions, investigate this property.

    Additional email and related properties are contained in the GeneralMonitor.properties file.
- In the workpoint-server.properties file:
  - server.automated.delay=500

This property controls the server-automated nodes to ensure that these nodes are not serviced on the queue before the database transaction that queued them has a chance to persist. This will prevent server-automated nodes failure due to timing issues. This property is recommended when server automated nodes are in use.

## Cannot Create a Copy of a Logical Attribute Handler

When you attempt to create a copy of a logical attribute handler in the User Console, the following error appears:

"This object is not connected"

Creating a new logical attribute handler, which is not based on an existing logical attribute handler, works correctly.

## Using Group Filters in Role Policies

When Identity Manager manages a user store in a relational database, group filters in member and admin policies may not work correctly. For example, if you specify a filter, such as "Users who are members of groups whose name starts with A," in a member policy, Identity Manager may incorrectly apply the policy to all users, instead of users in groups that begin with the letter A.

To prevent this issue, make sure that the tables, tblGroupMembers and tblGroupAdministrators, are defined for the user object in the directory configuration file (directory.xml).

The user object definition in directory.xml should resemble the following:

```
<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>
```

After changing the directory configuration file, import it using the Management Console.

**Note:** For more information about modifying directory configuration files, see the *Configuration Guide*.

### Configuring Role and Task Search Screens

When you configure search screens for roles or tasks, you can limit the roles and tasks that are returned by the search by using the "Show only objects meeting the following rules" option. Attributes that are used when you configure this option should not be added as available search fields on the search screen.

For example, if you configure the search screen to display only roles where the Enabled attribute is set to Yes, remove the Enabled attribute from the list of attributes that users can specify in search criteria.

Otherwise, the user-entered criteria is ignored.

### Identity Manager Environment Creation in Firefox Browsers

If you access the Management Console through a Firefox browser, Identity Manager environment creation may be slow, and may appear to hang. In these cases, environment creation continues, but the browser does not refresh, which prevents you from seeing when the creation completes.

**Note:** If you close the browser window, Identity Manager continues to create the environment.

## Upgrades

The following issues are related to upgrades in Identity Manager r12.

## MS SQL and Oracle Endpoints Unavailable After Upgrade from eTrust Admin 8.1 SP2

After upgrading from eTrust Admin 8.1 SP2 to Identity Manager r12, any MS SQL or Oracle endpoints acquired before the upgrade require a manual reconfiguration using the Provisioning Manager, to use JDBC URLs instead of Data Source Names (DSNs). This is due to the switch from using the SuperAgent to Java CS for managing MS SQL and Oracle endpoints.

**Oracle:** Modify the details in the Oracle endpoint property sheet.

**Example:**

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

**MS SQL:** Right-click on the endpoint and select Custom, Change Admin Password. The URL and connection credentials can be changed at this point without needing to view the other endpoint details.

**Example:**

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

**Note:** Migration steps and a complete list of possible URL syntaxes can be found in Chapter 4: Database Connectors in the *Connectors Guide*.

## UNIX Remote Agent is Not Available for Solaris x86 (Intel) Platform

Unix Remote agent package is missing files that are required to perform the installation or upgrade of the UNIX remote agent on the Solaris x86 (Intel) platform.

## Z/OS Connectors Architecture Change

The z/OS connectors (CA ACF2, CA Top Secret and RACF) have been re-architected for performance reasons to now use the CA LDAP Server for z/OS instead of the CA DSI Server on z/OS.

Before trying to configure any z/OS connector you must install the CA LDAP Server for z/OS r12 which can be downloaded from support.ca.com.

Once you have upgraded to Identity Manager r12, do the following for each endpoint defined to your system:

**From the Endpoint task view**

1. Select CA ACF2, CA Top Secret, or RACF Endpoint from Object Type.
2. Click the search button. Right click on the Endpoint and select properties. Fill in the following information:

   **In the Mainframe Server Information section:**

   - **IP Address/Machine Name** specifies the IP address of the RACF managed system where the CA LDAP Server is configured and running.
   - **LDAP Port** specifies the port number that you specified during the CA LDAP Server for z/OS install. If you are not sure of the Mainframe LDAP Port, see the section "Checking your CA LDAP Server for z/OS Configuration Information".
   - **LDAP Suffix** specifies the suffix to use for this endpoint. This combo box is automatically populated with all valid and available suffixes when you click the "Get Suffixes" button. Suffixes can be retrieved once valid values have been provided for the Mainframe IP Address/Machine Name and Mainframe LDAP Port fields.

# Reporting

The following issues are related to reporting in Identity Manager r12.

## Reporting Limitation

Multiple snapshots associated with a single report task must not use the same recurrence time.

## Satisfy=All Not Working Properly in XML File

In a Snapshot Parameters XML file, satisfy=all and satisfy=any are both behaving as satisfy=any (similar to an OR operator).

## Enable Cookies for View My Reports Task

In order to view reports in Identity Manager using the View My Reports task, enable third party session cookies in the browser.

## ExportALL.xml and Environments with No Organization Support

When using a Snapshot Parameters XML file (for example: ExportAll.xml) that exports organization objects and attributes, an exception occurs when the environment has no support for organizations. To work around this issue, comment out the organization object and attributes in the ExportAll.xml file.

# Provisioning

Provisioning component abbreviations for the following issues list are defined as follows:

- ACC: CA Access Control Connector
- ADS: Active Directory Services Connector
- DBZ: DB2 Universal Database for z/OS Connector
- DYN: Dynamic Connector
- E2K: Exchange 2000 Connector
- EEM: Embedded Entitlements Manager Connector
- ETC: UNIX ETC
- FND: Oracle Applications Connector
- INS: Installation
- KRB: Kerberos Connector
- LND: Lotus Notes/Domino Connector
- NDS: Novell Directory Services Connector
- N16: Windows NT Remote Agent
- AS4: OS/400 Connector
- PKI: Entrust PKI Connector
- PLS: CA SSO for Advanced Policy Server Connector
- PSA: Password Sync Agent
- RSA: RSA SecurID Connector
- SAP: SAP Connector
- SBL: Siebel Connector
- UPO: Universal Provisioning Connector
- VMS: OpenVMS Connector
- z/OS: CA ACF2, CA Top Secret, RACF Connectors

## General

The following issues are general provisioning issues in Identity Manager r12.

### Account Synchronization for the Reset User Password Task

To enable provisioning for an Identity Manager environment, you import a configuration file, called ProvisioningOnly-RoleDefinitions.xml, that creates the roles and tasks for user provisioning.

In that file, the default account synchronization setting for the Reset User Password task is set to Off. (Before you enable provisioning, the synchronization setting is set to On Task Completion.)

To use the Reset User Password to trigger account synchronization, set the account synchronization option after you import ProvisioningOnly-RoleDefinitions.xml to enable provisioning.

### User Console Cannot Explore and Correlate Some Endpoint Types

The Explore and Correlate tasks in the User Console do not find the following endpoint types:

- Kerberos
- UNIX NIS
- Entrust PKI
- Siebel
- Universal Database for z/OS
- Custom developed endpoint types

To explore and correlate these endpoint types, you can use Provisioning Manager. Then, you can perform routine account functions in the User Console, such as assigning an account on one of these endpoints.

### Explore and Correlate Works in One Time Zone

In the User Console, you can schedule an Explore and Correlate definition. This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 PM on Tuesday when the server time is 7:00 AM, the Explore and Correlate definition will not work.

### Provisioning Server Core Dump on Solaris

The Provisioning Server on Solaris will produce a core file on shutdown of the service.

This does not affect any of the functionality and can be safely ignored.

### Provisioning Directory Installer Requires Correctly Resolved Hostname

The installer requires a hostname with a properly configured name resolution when installing the Provisioning Directory and Provisioning Server on the same machine. The Provisioning Server installation will fail or lead to unintended results if the machine cannot resolve its own machine name into the intended IP address. There are two possible scenarios:

- You have a different name resolve result for FQDN and hostname. (For example, in an IPv4/6 network, you register an IPv6 address in DNS, but have an IPv4 address for the hostname through net bios or host file). If you configure the Provisioning Directory to listen on IPV6 only, and then install the Provisioning Server using FQDN, the install will fail because the installation program is trying to resolve the host name rather than FQDN during certain stages in the installation. The workaround for this is to add the host name and its IPv6 address to the host file. However, this is still a mis-configuration.
- On a machine with no DNS or any other name lookup, if you try to install the Provisioning Directory and the Provisioning Server using an IP address, the install will fail for the same.

  **Note:** CA does not support installation by an IP address.

### Certain Domain Configurations Performed with Simultaneous Global User Password Changes can Cause the Provisioning Server to Crash

If "Identity Manager Server/Use External Password Policies" domain configuration is set to yes and you perform many simultaneous global user password changes. The result will be degraded performance, and eventually, the Provisioning Server  may crash..

### Solaris ECS Logging Above INFO Level Can Affect the Performance of the Provisioning Server

Enabling ECS logging above INFO level causes logs to be written before you receive a response. This causes your request to be delayed while the log is being written. If you are experiencing poor Provisioning Server performance when using ECS logging, the work around is to turn it off.

### SPML Updates Fail When JIAM Specifies Incorrect Objectclass Names

Sometimes the JIAM API may start to use incorrect, abridged object class names in requests sent to the Provisioning Server and the Provisioning Server will refuse the request and raise an "Internal consistency error in Provisioning Server" error.  For example, when performing an update of the "eTSBLDirectory" object, the incorrect object class "eTDirectory" is sent to the Provisioing Server. This problem can be resolved by restarting the SPML service.

### Special Characters in Global User Names

The Provisioning Manager allows you to create global user names that include special characters, such as the back slash character (\). However, the Identity Manager Server does not support user names with special characters.

When you create a global user in the Provisioning Manager with a special character, Identity Manager attempts to create a corresponding user in the Identity Manager user store. Errors occur and the Create User task fails in the Identity Manager user store.

Errors also occur if you try to delete a global user with special characters in the Provisioning Manager.

### Provisioning Manager Includes Obsolete SAWI/DAWI References

The Provisioning Manager includes dialogs that have controls for the SAWI and DAWI features, which are no longer supported. Please use the Identity Manager self-service features instead of SAWI or DAWI.

### Already Exists Error When Adding an Endpoint

If you delete and re-add an endpoint with exactly the same name, sometimes the Provisioning Server reports a failure claiming the endpoint of that name already exists. This can occur when you have configured multiple connector servers to manage that endpoint. The failure results from a problem during endpoint deletion, where not all connector servers are notified of the deletion.

To work around this problem, restart all connector servers that are configured to manage the endpoint.

## Java Connector Server (Java CS)

The following issues are related to the Java Connector Server in Identity Manager r12.

### Exploration of Java Connector Fails when using " / Character Sequence to Represent Distinguished Names

An unresolved issue exists in the Java CS dealing with the following two-character sequence:

"/

This is important to the handling of Composite Names used by the standard JNDI API to represent Distinguished Names that span multiple technologies.

For more information about other special characters in Distinguished Names passed to the Java CS, see LDAP RFC 2253 on:

http://ietf.org

and in the JavaDoc for javax.naming.ldap.LdapName

### Null Pointer Error in Connector Xpress

If you attempt to modify Connector Server routing information by either right clicking on an endpoint type and selecting set Managing CS, or directly editing CS Configs in environments with multiple Provisioning Servers using Connector Xpress, Connector Xpress may display a null pointer error. If you need to perform advanced connector server routing, use the csfconfig tool.

### Restarting Java CS Service Fails Using Windows Services

When restarting the Java CS service using Windows Services, it is possible to start the Java CS service before it has fully completed its shut down, causing the service to fail to start. If you encounter this problem, please use the stop and start buttons in preference to the restart buttons in the Windows Service Control Panel.

### Incorrect Error Message if you do not Select a Stored Procedure

If you do not select a stored procedure from the Select Procedure drop down list on the Map Table screens in the Connector Xpress Wizard and click Next, the following incorrect error message is displayed:

Please specify a table to be mapped.

The correct message is:

Please specify a procedure to be mapped.

### Explored Containers of DYN JNDI Endpoint are Missing in the Provisioning Manager

After performing a single level exploration of a container on newly acquired DYN JNDI endpoints, the Provisioning Manager Content panel may not show the newly explored container despite the exploration count showing the new record being added. Closing and reopening the Provisioning Manager will force the container to appear.

### DYN Account Template's Suspended Attributes are Bolded in the Provisioning Manager

The Provisioning Manager displays the Account Suspension Status attribute for DYN account templates as bolded which falsely indicates that this is a capability attribute.

### DYN Capability Attributes Labels May Be Truncated in the Provisioning Manager

Capability attributes specified when creating DYN JDBC or DYN JNDI endpoint types in Connector Xpress may have truncated or missing labels when displayed in the Provisioning Manager. This can be worked around by specifying an additional character at the end of the label, for example, "*LabelName a*" when specifying the displayName in Connector Xpress. This does not occur for membership capability attributes.

You can also modify the existing metadata by one of the following ways:

**After loading the saved project in Connector Xpress**

- Run through the Wizard
- Expand the metadata tree, drill down to the Classes -> eTDYNPolicy -> Properties -> Capability Attribute -> Metatadata, and modify the displayName value.

If you choose either of the methods to modify the existing metadata for a DYN endpoint type, ensure that your DYN endpoint type is updated with the new metadata.

## Connectors

The following issues are related to provisioning connectors in Identity Manager r12.

### Incorrect Results During Sub-Tree Search with ADS Connector

During a sub-tree search against a sub-tree containing multiple Organization Units with a large number of objects in each Organization Unit, the search could incorrectly return no objects. For example, with a search limit size set to 500 and the number of objects in each OU above that limit, no results will be returned. Even if the search filter narrows the search limit size to under 500, the search could still incorrectly return no objects. The work around for this problem is to increase the search limit size.

### Avoid Setting ADS Expiry Dates Past 2038

Setting an expiry date on an ADS account to a date later than 2038 will cause the Provisioning Manager to crash.

### EEM Connector is not Supported with IE7

The EEM connector is not supported if the C++ Connector Server (CCS) for the given EEM connector is installed on a machine with IE7 installed.

**Note:** In the Identity Manager r12 product documentation, Embedded Entitlements Manager (EEM) refers to the Embedded Identity and Access Manager (EIAM) Connector.

### Viewing EEM Account Templates with Provisioning Manager

The Provisioning Manager may become unresponsive when viewing EEM Account Templates.

The workaround is to close and restart the Provisioning Manager.

### Reopen Provisioning Manager to Acquire a new EEM Endpoint

Once a hostname has been set during an acquire, you must close and reopen the Provisioning Manager to acquire another endpoint. This is true even if the operation was cancelled.

### Unable to Select or Modify User Attributes on EEM Account Template

When creating account templates for an EEM endpoint, you must click the Application Properties tab after selecting the endpoint, and then click OK to finish the account template creation process.

### Acquiring DB2 z/OS Endpoint Crashes CCS

The DB2 UDB and DB2 z/OS connectors must not be routing requests to the same C++ Connector Server (CCS).

The work around is to install a second CCS on a separate machine so each of the DB2 UDB and DB2 z/OS connectors are hosted on their own C++ Connector Servers.

### Unattended Upgrade of ETC UNIX Remote Agent not Supported

Unattended upgrades of an ETC UNIX Remote Agent from eTrust Admin r8.1 SP2 to Identity Manager r12 are not supported. You must perform the upgrade in attended mode.

### ETC Remote Agent on a Linux OS Running on an S390 Fails

Attempting to install the ETC Remote Agent on a Linux operating system running on an S390 host fails with the error:

"linux098:/home/marty/LinuxS390 # ./IdentityManager.LinuxS390.sh lsm.exe: error while loading shared libraries: libncurses.so.4: cannot open shared object file: No such file or directory."

To work around this, you will need to locate a version 4 of ncurses for the operating system and install it.

### Executing Cafthost Command Causes an Error for HP-UX UNIX

You may see an error "Bus error (core dump)" when you execute the following command:

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

To add host(s), modify the "cafthost.cfg" configuration file manually using a text file editor within the "`cat /etc/catngcampath` directory, and add each host to a new line.

### Uninstallation of ETC Remote Agent Can Leave Orphan Files

When the ETC remote agent is upgraded from r8.1SP2 to r12, the several files can be left behind. If these files are not used by other installed packages, they can be removed:

- /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

### VMS modify Delete Account Rights Fails with SPML

You are unable to delete a value from the accountRights attribute on a VMS account using SPML. The SPML Client will return a success message, but the account will not be updated.

The work around is to use the Provisioning Manager to perform such modifications.

### Cannot Set a Secondary Password for OpenVMS Accounts

The OpenVMS remote agent utility 'vmsautil' does not enforce the semantics of the OpenVMS PRIMARY/SECONDARY password for user accounts. If you attempt to specify a secondary password when no primary password is set, the operation will fail with the "password is too short" error message.

The work around is to always reset the primary password when attempting to set a secondary password for the account.

### CAM/CAFT for OpenVMS is Missing One Instruction

The ETRUST_ADMIN_OPENVMS_INSTALLATION.TXT file is missing information on how to configure CAMCAFT.EXE on an OpenVMS system. The CAFTHOST Symbolic Name must be defined before installing CAM/CAFT. To define CAFTHOST, add the following command to your LOGIN.COM file:

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

Then log on to the OpenVMS system again.

### VMS Attribute eTVMSPWDLifeTime Shows as Out-of-Sync

The Password Lifetime (eTVMSPWDLifeTime) attribute is being shown as out-of-sync after the "Check Account Synchronization" operation if the account template attribute "Never expires" is set to true (checked).

### VMS Account Status is Incorrectly Reported by SPML as False

If a VMS account is suspended, the Provisioning Manager correctly reports the account status as "Active (Suspended in eTrust Admin)" however, SPML reports this as simply suspended is false

### Unable to Set VMS Password Flags

The eTVMSPwdFlags attribute is not being set correctly on an account add or modify operation if the request does not set a value for eTVMSAccessFlags also.

To work around this, an add or modify request should contain a value for eTVMSAccessFlags attribute as well as eTVMSPwdFlags attribute.

### VMS Migrate Password Attribute Shows as Out-of-Sync

Any VMS account or account template with the field MIGRATEPW set to true (checked), shows the eTVMSPwdFlags as out of sync after the "Check Account Synchronization" operation.

### VMS Account Suspension

Suspending an account at the account level using the Provisioning Manager successfully suspends the account, however it does not maintain "Suspended" in the properties page and changes back to "Active" when you apply the change. So you have an account that is suspended, but the properties page of the account has the attribute showing "Active" which means you can not actually make the account "Active" again.

There is no work around for this on an account itself. The only way to really work around this is to correlate the account to a global user and control the Accounts suspension through the global user's suspension

### VMS Usernames Can Not Contain Unescaped Unicode Characters

Attempting to create a VMS account with an incorrect name may crash the Provisioning Server which is installed on Solaris.

### NDS Connector Cannot Explore New Containers

The first explore tries to find and add containers after an NDS endpoint is acquired. If you add containers using NDS local tools and then try to re-explore the endpoint, the newly added containers nor their sub-entries will not appear in the tree.

You must remove the endpoint from the Provisioning Server and then re-acquire and explore it in order to view the new containers.

### NDS Connector Description is Single-Valued Field

In the NDS Connector, the account description is a single-value field, but in the NDS endpoint, the account description is a multi-valued field.

### Environment Variable Must be Deleted or Changed After Upgrade to Prevent Problems with UPO Connector Endpoint Type

During an upgrade of a remote SuperAgent to r12 C++ Connector Server, the ETAHOME environment variable may contain the incorrect installation path of the CCS and will cause problems with the UPO Connector endpoint type. You must manually delete the ETAHOME environment variable or change it to the correct installation path of the CCS after the upgrade before attempting to acquire or use the UPO endpoint.

### UPO Endpoint Acquisition does not Validate Domain Field

A UPO endpoint with an incorrectly specified value in the  domain attribute will be successfully acquired, however, the endpoint will raise "Connector Server Search failed: Insufficient access" errors during exploration.

This can be resolved by right-clicking on the endpoint in the Provisioning Manager and selecting Custom -> Update Credentials... and specifying the correct value for the domain.

### Required Kernel Parameter Check is not Performed Before Upgrading eTrust Common Services to Enterprise Common Services on Solaris

A required kernel parameter check is not performed on products that upgrade eTrust Common Services to Enterprise Common Services on Solaris (more likely to affect Solaris 9 than Solaris 10) . An installation is allowed to continue rather than being stopped with a warning if the kernel parameters are not sufficient. This affects:

- RSA Remote Agent on Solaris
- IMPS on Solaris
- IMPS SDK

To work around this problem:

Run

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

An informative message will be seen if the kernel does not meet requirements. If the kernel requirements are met, the installer will start

### Unable to Duplicate KRB Accounts

In the Provisioning Manager, attempting to duplicate a Kerberos account may result in an "eTKRBFullNameCorrelate not found in the attribute registry! (...) - Return Code: 111" error.  To work around this issue, add a new account rather than duplicating the account.

### Error when Specifying an Invalid REALM when Acquiring a KRB Endpoint

If you attempt to acquire a KRB endpoint and specify an invalid value for the REALM, a null pointer error message will result.

### z/OS Security Endpoint Crashes Solaris Provisioning Server

If the endpoint cannot connect to a CA LDAP Server for z/OS r12, the Provisioning Server will crash.

To work around this problem, make sure to configure the endpoint with valid connection information

### z/OS Synchronization Using the LDS Endpoint

The LDS synchronization agent is not included on the Identity Manager r12 product DVD. Contact support if you need this agent.

### E2K Error Message When Managing Mailbox Rights with Exchange 2007

Mailbox rights cannot be managed with Exchange 2007. You will receive a "CAFT Message: Access Denied - or command failed to execute" error message.

### E2K CAFT Error When Managing Mailbox Rights

"CAFT Message : Access denied - or command failed to execute" error message might be returned during management of mailbox rights even when your Exchange Remote Agent is configured correctly.

This can happen when mailbox rights list contains multiple privileges for the same object and normally happens when the managed exchange objects inherit rights from the parent object.

### E2K Multiple Primary Email Addresses Are Not Allowed

It is possible using the Provisioning Manager to add a new email address to an existing list of email addresses and set the new address to be the primary email address. However an existing primary email address is not demoted. By doing this an account can have multiple primary email addresses which native system does not allow. This can be avoided by first demoting the existing primary email address before adding the new primary email address

### Long PKI Path to INI File Can Reboot Provisioning Server

UNC paths over 77 characters will reboot the operating system. To work around this, avoid using long paths.

### PKI Accounts Appear as Duplicates

The PKI connector does not support Entrust PKI hierarchical endpoints and stores all accounts in a flat list. Because of this, a unique Entrust PKI account appears as a duplicate to the PKI connector.

### PKI Groups Property Sheet Does Not Display Correctly

When trying to open a PKI group property sheet in the Provisioning Manager, the error message "Unable to display the requested property sheet" is displayed.

### Email Notification Warning When Creating PKI Accounts

If you acquire a PKI endpoint using a proxy profile and email notification is turned one, you cannot create a new PKI account without specifying "create profile" option.

To work around this, do one of the following:

- Acquire the endpoint without the Proxy profile.
- Turn off the email notifications when acquiring the endpoint and go to the endpoint to check the reference number manually

### Assigning SAP Contractual User Types

When assigning a contractual user type to a user on the License Data tab, the change can only be applied to the Master system, not any of the child systems.

It is possible to change the contractual license types for the children natively.

### Mandatory Fields in the SAP Contractual User Type Attribute

The Contractual User Type that can be specified on the account's License Data tab cannot have mandatory fields other than the LIC_TYPE field. For example, if you have to specify the name of a SAP R3 System (SYSID) to use a Contractual User Type, the assignment will fail and you will get an error saying that there is a missing value for the Name of the SAP R3 System.

### C++ Connector Server Can Crash During a Request to the PLS Connector

If you find that your CCS has crashed during a request to a PLS connector, you should investigate your Policy Server installation as it could be the cause of the problem. The symptom you will see in your requests to the Policy Server will slow down significantly due to the constant restarting of the Access Control Service.

### SBL Account Suspension

When Modifying a SBL Account or SBL Account Template and synchronizing the changes with an account, do not set eTSuspended along with other modifications as that will cause other attribute modifications to be ignored.

To work around this, split the changes into two separate requests, one containing eTSuspended modifications and the other containing the changes to the values of any other attributes.

### JIAM RSA Check Account Sync Reports Incorrectly

When performing a Check Account Sync operation on an RSA account using JIAM, if the account is missing from the endpoint, the Connector Server wrongly returns a failure with the error message "Connector Server Read failed: Sd_GetSerialByLogin Error Invalid user", instead of returning success and the message "Account missing from endpoint". Check that Account Sync from the Provisioning Manager works correctly.

### Removing Multiple Groups from OS/400 User Stalls the Provisioning Manager

Removing multiple groups from a user, in a single operation where one or more of the groups starts with "#", can lead the Provisioning Manager to become unresponsive.

To work around this, remove one group at a time.

### OS/400 Account Cannot Have Primary Group Removed

The OS/400 group membership can be changed by either modifying the account that is a group member or by modifying the group's membership. When modifying a group's membership, accounts cannot be removed if their group membership is a primary group membership.

To work around this, modify the account and remove the primary group membership.

### FND Connector Must Contain Both a "From" and "To" Date in a Responsibility List

The FND connector must contain both a "From" and "To" Date in a responsibility list, otherwise the responsibility list becomes unstable and un-recoverable.

To work around this, you must always specify a "From" and "To" Date in a responsibility list, either during the FND account or account template creation or modification, (for example, using dates far in the past or future instead of blank "From" and "To" Dates).

### Host to Caft Definition on VISTA does not Work

If you have installed the N16 Remote Agent on a VISTA or VISTA SP1 endpoint, and try to add the managing Server through All Programs -> CA - > Identity Manager -> Host to Caft Definition, and then try to acquire that VISTA machine as an endpoint, you will get an 'Access Denied" error message.

To work around this, open a command prompt and issue the following command to acquire the endpoint.

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

### Use Absolute Paths to Access LND Account Custom ID Locations and Organizational Unit Certificate IDs

Using UNC paths when accessing Account Custom ID locations and Organizational Unit certificate IDs does not always work with shared folders in a relative path. The use of absolute path (including drive letter) is recommended.

### LND Search Request in SPML Does not Return Results

Performing a Search Request in SPML or through SPML Server for an Account, does not return a result when using attributes beside lastName and homeServer

### Correlating LND Accounts and Global Users Created through SPML Does Not Work

In the Provisioning Manager, correlating Accounts and Global Users created through SPML does not currently work.

### Avoid using Japanese Characters in LND Account Names

Changing ID Password does not currently work with Accounts containing Japanese characters in the Account Name. Using English characters in the Account ID file solves this issue.

### LND Accounts Cannot be Created with "User Unique OU"

Accounts cannot be created with 'User Unique OU'. The resulting account will not be searchable or accessible in Provisioning Manager.

### LND Account Short Name Attribute Can Contain No More Than 85 Japanese Characters

Using more than 85 Japanese characters in the Account Short Name attribute has been known to cause the Domino Server to crash. This problem only occurs when the Account Name also contains Japanese characters.

### Provisioning Manager does not Display LND Account's Group Memberships if they Contain Japanese Characters

In the Provisioning Manager, accounts created in Organization and Organizational Units containing Japanese characters do not show their Group Membership(s) in the Member Of tab.

### LND Account and Certifier IDs Containing Japanese Characters Cannot be Accessed by the LND JCS Connector

Account and Certifier IDs containing Japanese characters cannot be accessed by the LND JCS connector. All functions needing to access these ID files are known to fail in this version.

### Japanese Characters in LND Object DN Paths Can Cause Problems During Directory Exploration

Some Japanese characters in object DN paths are known to cause Provisioning Server to hang during Directory Exploration. Examples include, Japanese characters with Unicode 0x80fd, 0x4e88, and 0x5642.

### LND Connector Cannot Perform Rename or Move in Hierarchy on Explored LND Accounts

This version of the LND connector cannot perform the custom actions Rename or Move in Hierarchy on explored LND accounts. The attribute fields are disabled for these actions.

There is no work around for these actions.

### LND Account and its Mail File Cannot be Deleted Using the Custom Action

Deleting an account and the account's mail file using the 'custom' action fails.

No error message is generated by the Provisioning Manager, but an inspection of the endpoint shows that the account is still there and so is its mail file. There is no work around using the Provisioning Manager for this.

### LND Account Mail Fails are not Being Created During Registration

The Provisioning Manager LND account creation window contains a check box called 'Create Replicas' on the Profile tab page.

When administering a Domino endpoint that is in a clustered environment, when the 'Create Replicas' checkbox is ticked, replicas of the account should be created in the cluster environment, along with its associated mail file. The creation of replica mail files is not being handled during registration in this release.

# Chapter 7: Documentation

The file names for the Identity Manager r12 guides are as follows:

| Guide Name | File Name |
|---|---|
| Release Notes | im_release_enu.pdf |
| Implementation Guide | im_impl_enu.pdf |
| Installation Guide for WebLogic | im_install_weblogic_enu.pdf |
| Installation Guide for WebSphere | im_install_websphere_enu.pdf |
| Installation Guide for JBoss | im_install_jboss_enu.pdf |
| Configuration Guide | im_config_enu.pdf |
| High Availability Guide | im_high_avail_enu.pdf |
| Administration Guide | im_admin_enu.pdf |
| Programming Guide for Java | im_dev_enu.pdf |
| Programming Guide for Provisioning | im_dev_provisioning_enu.pdf |
| Provisioning Guide | im_provisioning_enu.pdf |
| Connectors Guide | im_connectors_enu.pdf |
| Connector Xpress Guide | im_connector_xpress_enu.pdf |
| Java Connector Server Implementation Guide | im_jcs_impl_enu.pdf |
| Programming Guide for Java Connector Server | im_jcsProg_Enu.pdf |
| iRecorder Integration Guide | audit_im_irec_ref_enu.pdf |
| Glossary | im_glossary.pdf |
| Bookshelf | im_bookshelf_enu.zip |

The Identity Manager r12 guides are available for download at the following location:

- CA Support site

To view PDF files, you must download and install the Adobe Reader 7 or higher from the Adobe web site if it is not already installed on your computer.

**Note**: For best performance, when you install the bookshelf on a remote system, make the bookshelf accessible from a web server.

This section contains the following topics:



# Bookshelf

The Bookshelf provides access to all Identity Manager documentation from a single interface. It includes the following:

- Expandable list of contents for all guides in HTML format
- Full text search across all guides with ranked search results and search terms highlighted in the content
- Breadcrumbs that link you to higher level topics
- Single HTML index to topics in all guides
- Links to PDF versions of guides for printing

**To use the Bookshelf**

1. Download the bookshelf from the CA Support Site.
2. Extract the contents of the ZIP file.
3. View the bookshelf as follows:
   - If the bookshelf is on the local system and you are using Internet Explorer, open the Bookshelf.hta file.
   - If the bookshelf is on a remote system or if you are using Mozilla Firefox, open the Bookshelf.html file.

     **Note:** For best performance, when you install the bookshelf on a remote system, make the bookshelf accessible from a web server.

The Bookshelf requires Internet Explorer 6 or 7 or Mozilla Firefox 2. For links to PDF guides, Adobe Reader 7 or 8 is required. You can download Adobe Reader at www.adobe.com.

**Note**: The CA SiteMinder Bookshelf has been published for r12 and r6.0 SP5 at the CA Support site using the same bookshelf format used by Identity Manager.

# Online Help Enhancements

Both the User Console online help and the Management Console online help now have the following features:

**Breadcrumbs**

Indicate where you are in the help hierarchy for easier navigation. They are located at the top of the help page.

**Search Highlighting**

Identifies the context of your search in the resulting pages with a yellow highlight.

**Navigation Buttons**

Displays previous and next arrow buttons for easier navigation. They are located at the top of the help page, under the breadcrumbs.

# eTrust Rebranding to CA

The branding of some CA security products is currently in transition from "eTrust" to "CA". During this transition, you may see references to both eTrust products and CA products in the documentation. For example, eTrust Directory will be rebranded as CA Directory in its next release. Any mention of an eTrust product within the documentation is equivalent to the same product with the new CA brand.

# Provisioning Terminology Changes

Existing eTrust Admin customers may notice certain terms have changed now that eTrust Admin is part of CA Identity Manager. The following table shows these changes.

| eTrust Admin Term | New Term in Identity Manager |
|---|---|
| eTrust Admin Server | Provisioning Server |
| eTrust Admin Manager | Provisioning Manager |
| Directory | Endpoint, Endpoints |
| Namespace | Endpoint Type |
| Policy or Provisioning Policy | Account Template |
| Roles | Provisioning Roles |
| Distributed SuperAgent Framework | Connector Server Framework |
| SuperAgent | C++ Connector Server |
| Option | Connector |
| Administrative Directory or Administrative Repository | Provisioning Directory |
| Identity Manager Corporate Directory | Identity Manager User Store |
| Corporate User | Inbound Administrator |

# New Name for Embedded IAM (EIAM) Connector

In the CA Identity Manager r12 product documentation, Embedded Entitlements Manager (EEM) refers to the Embedded Identity and Access Manager (EIAM) Connector.

# Programming Documentation

There are two programming guides included in the Identity Manager r12 document set.

**Programming Guide for Java**

Formerly titled the Identity Manager Developer's Guide, this guide provides information about using the Identity Manager Java APIs. The HTML version is integrated with Javadoc pages, and includes hyperlinks where necessary to cross-reference relevant information.

**Programming Guide for Provisioning**

Formerly titled the eTrust Admin SDK Developer's Guide, this guide provides programming information about the Identity Manager Provisioning Server SDK. Developers must have knowledge about programming with C++.