CA Identity Manager

Release Notes

r12.5 SP6

CA Product References

This document references the following CA products:

- CA Identity Manager
- CA SiteMinder®
- CA Directory
- CA Enterprise Log Manager
- CA Role & Compliance Manager

Contact CA

Contact CA Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: New Features

This section contains the following topics:

r12.5 SP6

This section contains the following topics:

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP6:

- CA Directory r12 SP5, the Identity Manager User store and Connector Xpress JNDI endpoint
- AIX 6.1 as a supported platform for CA Identity Manager Server
- SiteMinder on AIX 6.1 (64 bit) installed with WAS 6.1 and JVM (64 bit) as a supported platform for the Identity Manager Server

TEWS – Retrieve Related Task Description Field

You can now use TEWS to retrieve the Related Task Description field.

This issue is only applicable to the TEWS API. In the CA Identity Manager User Console, in the System, View Submitted Tasks (VST) task, you can view all inbound tasks associated with a submitted task. For example, a "Create User" task can trigger account creation on an endpoint.

You can now view the the details of the account creation by accessing the associated inbound task on the Create User from View Submitted Tasks. The associated inbound task information was not previously available from the TEWS API. This enhancement allows the associated task information to be retrieved using TEWS.

r12.5 SP5

This section contains the following topics:

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP5:

- Oracle 11g R2 RAC as the Identity Manager user store
- Oracle Directory v7.0 as the Identity Manager user store
- SiteMinder r6.0 SP6 and SiteMinder r12.0 SP3 CR1

  SiteMinder r12.0 SP3 CR1 should be on a different system from the one with the Identity Manager Server
- All CA Identity Manager components run in 32-bit emulation mode on Windows 2008 R2

SAP User Management Engine (UME) Connector

You can now use the User Console to manage SAP User Management Engine (UME) endpoints. SAP UME is the user administration tool for SAP NetWeaver.

Default Snapshot Parameter XML Files

CA Identity Manager now includes a default snapshot parameter XML file for each default report. Each Identity Manager report uses a specific set of managed objects, and previously, the default XML files did not cover all the report use cases. Administrators were forced to use the ExportALL.xml file, which caused performance issues. Now each default snapshot parameter XML file is associated with an Identity Manager report, and can be selected at runtime to capture snapshot data.

Note: For more information about default snapshot parameter XML files, see the *Administration Guide*.

ExportALLTemplate.xml Available for Reporting Demonstrations

A new Snapshot Parameter XML file titled ExportALLTemplate.xml is available. This XML file is a subset of ExportAll.xml; it only exports a list of users, roles, endpoints, and accounts. Only use this XML file for the demonstration of reporting functionality.

Import this default XML file as you would a role definitions file, using the Management Console. This XML file is located in *im_EAR*\config\com\netegrity\config\imrexport\sample.

Note: Replace any text surrounded by "##" with meaningful values. For example, replace ##endpointname## with the valid endpoint name.

r12.5 SP4

This section contains the following topics:

ConfigXPress Environment Utility

ConfigXpress is a new sample utility that quickly analyzes an Identity Manager environment and reduces the amount of time required to understand the configuration of the environment. This new utility graphically displays the objects in the environment. It shows how each object is defined and its relationship to other objects in the environment. For example, it shows the number of tasks in a role, which could reveal a performance problem. The results appear within seconds at the click of a mouse.

This tool can be very useful for migrating the environments from test to production systems and comparing the differences between like objects. Using ConfigXpress, you can:

- Display the environment's current state
- Generate a PDF file that describes the Identity Management environment
- Compare environments and copy components from one environment to another
- Copy components to an external file for import later

The sample utility will be installed in the following directory:
`C:\\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\sample\support`

When you double click the ConfigXpress.air file, it downloads the Adobe Air runtime plug-in, which allows you to use the utility.

Web Services SDK Sample Connector

The Web Services SDK (SDKWS) is included in the Java JCS SDK. The SDKWS sample connector demonstrates how to implement a custom connector that communicates with a web service endpoint. A sample endpoint is provided as part of the SDKWS.

Password Management

The Logical Attribute Handler (LAH), ConfirmPasswordHandler, now correctly validates the old password. The validation of the old password is configurable, and is not enabled by default.

Configure Database ID and Application Owner Attributes in Oracle Applications Connector

You can now configure Database ID and Application Owner values. A new connector level attribute Application Database name has been added to the Oracle Applications Connector. In addition, you can now specify a value for the Applications User Name attribute.

Access Role and Task Support for SiteMinder Integrations

When CA Identity Manager integrates with CA SiteMinder, administrators can assign access roles that grant privileges in applications that are protected by SiteMinder. These access roles include access tasks, which represent a single action that a user can perform in a business application, such as generating a purchase order in a finance application.

For a new installation of CA Identity Manager, perform these steps for any environment for which you want to create access roles.

1. Access the Management Console.
2. Choose Advanced Settings, Miscellaneous.
3. Add EnableSMRBAC to the Property Field.
4. In the value field, enter: true.
5. Click Add.

Note: If you are upgrading environments with access roles, follow the procedures in the *Upgrade Guide*.

New Certifications

At this release, the following new platforms are certified:

- CA Directory r12 SP4 is supported as the Identity Manager user store
- CA Business Intelligence 3.2 is supported as the Business Objects Report Server

Localization for Custom HTML Fields

The CA Identity Manager localization model now includes the localization of custom HTML fields. Fields such as the style applied to search screen for Modify Admin Task/Modify User can now be localized by including localization tags; ${key=name}.

r12.5 SP3

This section contains the following topics:

CA DLP Connector Support

You can now use the CA Identity Manager User Console to manage CA DLP 12.5 endpoints.

Microsoft Exchange 2010 Support

You can now use the Identity Manager User Console to manage Microsoft Exchange 2010.

CA Identity Manager User Console Now Supports Exchange 2010

The Exchange 2007 remote agent now supports Exchange 2007 and Exchange 2010.

Change the CA Message Queuing Server service Run-As account to your Exchange Administrative Account after installing the remote agent.

As the Exchange 2010 server no longer supports support storage group, explicitly set the mail server field on all your mailbox enabled ADS account templates in the CA Identity Manager User Console. You can only set the mail server field in the CA Identity Manager User Console.

Note: For more information about Exchange 2010 support, see *Manage an Exchange 2010 Environment* in the *Connectors Guide*.

Exchange 2007 and Exchange 2010 in Mixed Environment Support

CA Identity Manager 12.5 SP3 supports Exchange 2007 and Exchange 2010 in mixed environments.

To enable support for Exchange 2007 and Exchange 2010 in mixed environments, select the Exchange 2010 Server with the Mailbox role that is configured as the Exchange Gateway server on the Active Directory Exchange General directory properties page. If you do not want to manage Exchange 2010, continue to manage your Exchange 2007 servers as before.

Note: The Exchange 2007 and Exchange 2010 remote agent must be installed on the Exchange Gateway server and any Exchange 2007 servers you want to create mailboxes on.

For more information about enabling and configuring Exchange 2007 and Exchange 2010 mixed environment support, see *Enable Exchange 2007 and Exchange 2010 Mixed Environment Support* and *Configure Exchange 2007 and Exchange 2010 Timeout Settings* in the *Connectors Guide.*

CA Directory r12.0 SP3 as a User Store

CA Directory r12.0 SP3 is supported as a CA Identity Manager user store.

Vista Credential Provider Customizable Tile Image

You can now customize bitmap images embedded in compiled DLL for Vista Credential Provider.

RSA 7.1 SP3 Support

You can now use the CA Identity Manager User Console to manage RSA 7.1 SP3 endpoints. The RSA Authentication Manager SecurID 7.1 Connector is not backward compatible with RSA 7.1 GA – SP2. We recommended that you:

- Upgrade your RSA installations to SP3 before deploying CA Identity Manager r12.5 SP3
- Upgrade the SDK files installed on the Java CS computer with RSA 7.1 Authentication Manager SP3 SDK files.

Note: For more information on upgrading the RSA SecurID 7.1 Connector, see *Upgrade the RSA SecurID Connector* in the *Connectors Guide*.

RSA 7.x ACE (SecurID) Connector Support for Distinction Between Hardware and Software Tokens

The RSA 7.x RSA ACE (SecurID) Connector now supports the distinction between hardware and software tokens.

SAPEmailWeakSyncConverter

The SAPEmailWeakSyncConverter converter has been added for SAP endpoints. The convertor prevents duplicate email entries being added to SAP accounts when you modify the email attribute and want to use weak synchronization on SAP account templates.

Note: For more information about enabling the converter, see Duplicate Email Entry when Modifying Email Attribute and Using Weak Synchronization *(see page 125)*.

User Management/SAP Connector Enhancement for Accumulated Provisioning Roles

The SAP connector now includes a cache of monitors. This cache prevents a race condition that occurred in previous CA Identity Manager versions when multi-valued attributes were set to forceModificationsMode=true.

r12.5 SP2

This section contains the following topics:

Google Apps Connector

You can now use the Identity Manager User Console to manage Google Apps endpoints.

Microsoft ADAM and LDS DYN JNDI Support

Microsoft ADAM (Active Directory Application Mode 2003) and LDS 2008 (Lightweight Directory Services) are now supported vendors for DYN JNDI.

Novell eDirectory 8.8.5 as a User Store

Novell eDirectory 8.8.5 is supported as an Identity Manager user store.

Authentication Checks to Inbound Requests Over HTTPS

To improve security, additional checks have been added to inbound requests when CA Identity Manager is configured with SSL.

UNIX Remote Agent Enhancement

Non-root users can now call the UNIX Remote Agent.

The enhancement allows the CAM service (the communications layer for C++ Connector Server to the UNIX Remote Agent binary) to run without the permissions of the root or super user. By having fewer permissions, the security of CAM service (which is always running listening for requests) is improved.

Global User changes to DYN Connector Accounts Performance Enhancement

Performance has been enhanced when propagating Global User changes to DYN connector accounts. The enhancement addresses a performance issue with accounts modified by a user.

Rather than using the attributes defined in the parser table, mapped attributes defined in the metadata are used for looping instead. That is, non-mapped attributes are ignored.

r12.5 SP1

This section contains the following topics:

Policy Xpress

Policy Xpress allows you to create complex business logic (policies) without the need to develop custom code. Policy Xpress tasks are located under the Policies tab and are associated with the Policy Xpress Manager role and the System Manager role, by default.

Previously, Policy Xpress was part of Option Pack 1. In this release, Policy Xpress has been incorporated into the core CA Identity Manager product and can be accessed under the Policies tab.

Also, note the following improvements to Policy Xpress that are available in this release:

- Policies are searched using scoping rules.
- Policies have Submitted Task and Reverse listeners.
- Creating, modifying, viewing, and deleting policies is captured in View Submitted Tasks as events. These events can be resubmitted in an error occurs. Also, you can configure workflow on these events.
- Policy Xpress audits all activity in View Submitted Tasks, including policies evaluated, actions performed, and failures.
- Several usability improvements made to plug-ins.
- Policies can validate data before task submission.
- Granular behavior control when a policy generates an error.

Note: For more information about Policy Xpress, see the *Administration Guide*.

Policy Xpress Plug-in Changes from Option Pack 1

CA Identity Manager r12.5 SP1 implements the following Policy Xpress plug-in changes:

Data Elements

- Has account attributes changed—Removed
- Endpoint objects—Removed
- Account values and Account values by identifier—Moved to the "Accounts" category
- Comparator, compare strings—Added a case sensitivity option
- Comparator, compare dates—Added a date format parameter
- Date—Added a date format parameter
- Time—Added a time format parameter

- List filter—Added a list size function
- Workflow—Can now return full names, user names, or email addresses

Actions

- Set account data and Set account data by identifier—Moved to the "Accounts" category
- Added a "move account" action

Reverse Synchronization for Endpoint Accounts

An endpoint system user can create, delete, or modify accounts on the endpoint. For example, a user may create or modify an account in the Active Directory domain using an external tool. CA Identity Manager must be aware of this potential security issue. Creating or modifying an account directly in the endpoint bypasses CA Identity Manager's approval processes and auditing.

Reverse synchronization helps ensure control of the endpoint accounts by identifying discrepancies between Identity Manager accounts and endpoint accounts. You create reverse synchronization policies to handle the change. Then, using Explore and Correlate to update CA Identity Manager, you trigger the execution of policies.

Previously, reverse synchronization was part of Option Pack 1. In this release, reverse synchronization is incorporated into the core CA Identity Manager product and can be accessed on the Endpoints tab in the User Console.

Note: For more details on reverse synchronization, see the Managed Endpoint Accounts chapter in the *Administration Guide*.

Bulk Tasks

Bulk Tasks (Scheduled Tasks in Option Pack 1) allow CA Identity Manager users to perform the following actions:

- Modify a User object, based on an attribute filter, such as department, city, termination date, and so on.
- Run a task on specific objects periodically, such as every Saturday.
- Make bulk user changes, such as modifying all users within a selected department.

This functionality differs from the scheduled task functionality in CA Identity Manager by providing a population filter. Unlike scheduled tasks, the population of objects affected by the bulk task is unknown when you configure the bulk task. Also, bulk tasks affect many objects, while scheduled tasks only affects one.

Note: For more information about Bulk Tasks, see the *Administration Guide*.

Email Notification Policies

Email notifications inform CA Identity Manager users of tasks and events in the system. For example, CA Identity Manager can send an email to approvers when an event or task requires an approval.

CA Identity Manager r12.5 SP1 provides two methods for creating email notifications:

- **Email Templates** (existing functionality)

  Administrators create email notifications using default templates installed with CA Identity Manager. To customize those templates, administrators use the Email Template API.

- **Email Notification Policies** (new functionality)

  CA Identity Manager r12.5 SP1 includes an additional method that allows business users to create, view, modify, and delete email notifications by using Email Management tasks in the User Console. These users do not need to know any code to configure email notifications.

  Administrators can define the content of an email, when it is sent, and who receives it. The content of the email can contain dynamic information, such as the current date or event information, which CA Identity Manager populates when the email is sent. For example, you can configure an email notification that is sent to an approver when a new user is created. The email can contain login information, date of hire, and manager.

  Email notification policies are Policy Xpress policies; however, you create and manage these email notification policies using a separate set of tasks in the User Console.

  Note: For more information about email notification policies, see the *Administration Guide*.

Preventative Identity Policies

A *preventative identity policy* is a type of identity policy that prevents users from receiving privileges that may result in a conflict of interest or fraud. These policies support a company's Segregation of Duties (SOD) requirements.

Preventative identity policies, which execute before a task is submitted, allow an administrator to check for policy violations before assigning privileges or changing profile attributes. If a violation exists, the administrator can clear the violation before submitting the task.

For example, a company can create a preventative identity policy that prohibits users who have the User Manager role from also having the User Approver role. If an administrator uses the Modify User task to give a User Manager the User Approver role, CA Identity Manager displays a message about the violation. The administrator can change the role assignments to clear the violation before submitting the task.

Preventative identity policies can also trigger a workflow process that requires approvals from designated approvers before CA Identity Manager executes the task.

Note: For more information about preventative identity policies, see the *Administration Guide*.

Workflow Enhancements

Several new enhancements were made to Workflow for this release and include the following:

- Global Event Level Policy-Based Workflow Mapping (see page 26)
- Task Level Policy-Based Workflow (see page 27)
- Escalation Approval Template (see page 28)
- Matching Attribute Resolver (see page 28)
- Highlighting Changed Attributes on Approval Screens (see page 30)
- Partial Attribute Level Approve/Reject (see page 30)
- Approval Policy Description (see page 30)
- Bulk Operations on Work Items (see page 31)

Global Event Level Policy-Based Workflow Mapping

An event can be mapped to a workflow process from the Management Console, or be associated with policy-based workflow approval policies in a specific task. The new Configure Global Policy-based Workflow for Events task, lets administrators set up policy-based workflow mapping for events at the environment level. Unlike setting up policy-based workflow for an event in an admin task, the configured policy-based workflow mappings are applied to all tasks that generate the event.

Task Level Policy-Based Workflow

Task Level policy-based workflow lets you associate a task with a workflow process based on the evaluation of a rule. This means that instead of a task always launching a workflow process, the workflow process runs and generates a work item only if a rule associated with the task is true.

For example, when creating a new group, you can define a rule that places the Create Group task under workflow control and creates a work item only if the new group is part of a designated parent organization. If the new group is not part of that organization, the workflow process does not execute and no work item is created.

If a task has multiple rules, all workflow process associated with the task need to be approved, for the task itself to be approved. Similarly, if one workflow process associated with the task is rejected, the task itself is rejected. Workflow rules can be assigned priority values to determine the order of rule evaluation and workflow execution.

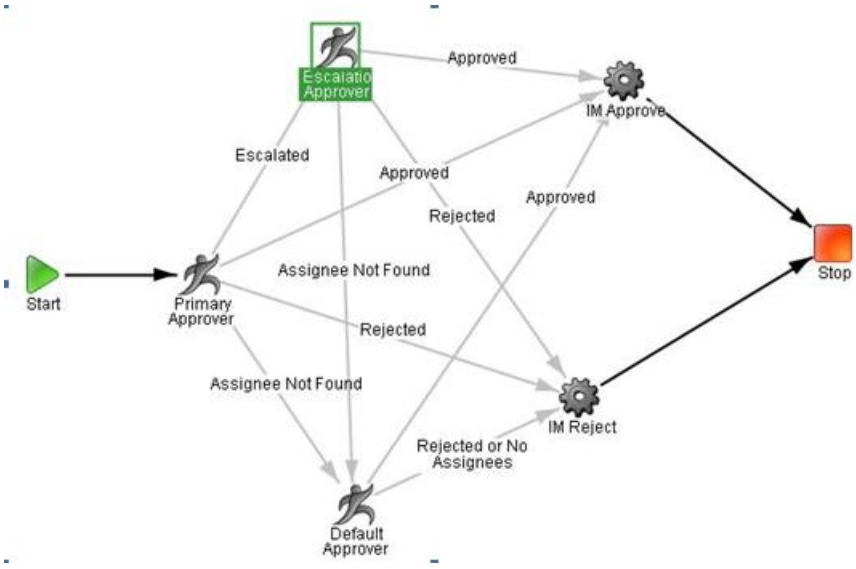
Only default CA Identity Manager workflow templates support workflow rules for task level policy-based workflow. You can also create custom workflow processes for use with workflow rules.

Note: For more information about policy-based workflow, see the Workflow chapter in the *Administration Guide.*

Escalation Approval Template

A new process template has been added that includes a timed transition approval node from the primary approver to the escalation approver. This user can approve or reject the request if the primary participant is not found.

Note: For more information on the Escalation Approval Template, see the Workflow chapter in the *Administration Guide*.



Matching Attribute Resolver

This resolver works on objects of type User only. A value from any object available is matched against a field on the user object. Use the following selection to set matching attribute rule constraints:

Approvers

Specifies the type of user to approve this task.

User or Object

Specifies the value that approvers will have in the attribute selected below.

Note: The value retrieved from the user or object should be an acceptable value for a search on user for the selected attribute.

- Object associated with the event—The event under workflow control.
- Initiator of this task—The user who initiated the admin task.

- Primary object of this task—The object being created/modified by the task.(Only available for task level event mapping.)
- Previous approver of this task—The previous approvers of this task.

Use or Object Attribute

Specifies the attribute that contains the value to use in the search for approvers.

Approver Search Attribute

Specifies the attribute that is used in the search to match the value identified above.

Note: When you set 'Approve Create User' task as a Match Attribute Resolver that works on Users, Participant Resolver, you must change the method signature for the imApprovers script on workpoint designer to point to the unique name for TwoStageProcessDefinition.

You must import the upgrade scripts for escalation approval process for previous approver information to be available (UpgradeWFScripts.zip). Import the scripts from the workflowScripts folder under the Administrative Tools in following default locations:

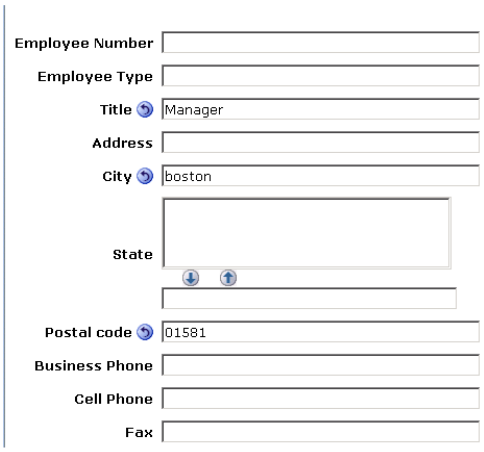
- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

When importing the WorkPoint scripts with the archiver tool on upgrade, the administrator should specify that this is an import into an existing database and override existing scripts.

Highlighting Changed Attributes on Approval Screens

In order for an approver to know what attributes have been modified or to undo the changes to those attributes if needed, an undo icon has been added to the approver profile screen that lets the approver know that this attribute has been changed.

The approver can see the original value for the editable attributes by clicking the undo button and can also change the value of the attribute to any other value.



Partial Attribute Level Approve/Reject

An approver can choose to partially approve or reject attribute changes on an approval profile screen . If an approver decides to reject the changes made to attributes visible on the approval screen the approver can click on the reject button and only those attributes will be reverted to their original value. In previous releases if an approver clicked on the reject button the entire event was rejected. Likewise if an approver clicks on the approve button only changes made to the attributes visible on the approval screen are approved.

Note: This is only applicable for event level policy based workflow for approval policies with an evaluation type of OnChange. For more information on this feature, see the Policy-Based Workflow section in the *Administration Guide*.

Approval Policy Description

A new field called Policy Description has been added to the Approval Policy. This is an optional, non-searchable string description and appears on resulting work items.

Bulk Operations on Work Items

With this release of CA Identity Manager, the following bulk operations can be performed on selected work items:

- Approve
- Reject
- Reserve
- Release

In the User Console, the Configure Work List tab has been enhanced to include a new Supports bulk workflow operations check box. When this check box is enabled, the user can bulk approve, reject, release, and reserve work items that they own or work items from the delegators from the View My Work List screen. However, administrators can only perform bulk reserve or release of items on behalf of the existing user on the Manage User's Work Items screen.

Note: For more information about bulk operations on work items, see the *Administration Guide*.

Smart Provisioning Enhancements

The Suggested Roles functionality is now available for the Create User task, as well as the Modify User task (supported in CA Identity Manager r12.5).

When CA Identity Manager integrates with CA Role and Compliance Manager (CA RCM), the Suggested Roles functionality provides administrators with a list of provisioning roles that may be appropriate to assign to a user. The list of provisioning roles is determined by CA RCM, based on criteria entered by the administrator.

Suggested provisioning roles help ensure that users have the correct privileges, while maintaining a company's role model.

Note: For more information about Suggested Roles, see the *Administration Guide*.

Changing Languages in a CA Identity Manager User Session

CA Identity Manager r12.5 SP1 includes a new feature that allows users to change the language displayed in the login screen and the User Console when an Environment supports multiple languages.

Users can select the language they want to view from a Choose Language field in the login screen and in the User Console. The user does not need to log out of the Environment for changes in the display to take effect.

Note: For more information about changing languages, see the *User Console Design Guide*.

r12.5

This section contains the following topics:

CA Role & Compliance Manager Integration

CA Role & Compliance Manager (CA RCM) is an identity lifecycle management product that enables you to quickly and accurately develop, maintain, and analyze role models. CA RCM also provides centralized identity compliance policy controls and automates processes associated with meeting compliance and security demands. Using CA RCM, you can do the following:

- Validate that users have appropriate privileges
- Be sure that privileges are granted in accordance with security policies
- Monitor the effectiveness of identity management controls
- Understand what roles exist in your organization, and then establish a *role model* that fits your organization
- Analyze and maintain that role model as business evolves

CA Identity Manager integrates with CA RCM using the following:

- CA Identity Manager Connector

  The Connector for CA Identity Manager automatically synchronizes the role-based privilege data between CA Identity Manager and CA RCM. By using the connector, you can import data from CA Identity Manager to CA RCM or export data from CA RCM to CA Identity Manager.

  Note: For more information about the CA Identity Manager Connector, see the *CA RCM Connector for CA Identity Manager Guide*.

- Dynamic Notifications

  When CA Identity Manager integrates with CA RCM, you can leverage CA RCM capabilities to support day-to-day identity management operations. Any changes made in CA Identity Manager are updated immediately in CA RCM.

Smart Provisioning

Smart Provisioning is a collection of functionality that simplifies provisioning role assignment when CA Identity Manager integrates with CA RCM. This functionality includes:

- **Suggested Provisioning Roles**

  CA Identity Manager can provide administrators with a list of provisioning roles that may be appropriate to assign to a user. The list of provisioning roles is determined by CA RCM, based on criteria entered by the administrator.

  Suggested provisioning roles ensure that users have the correct privileges, while maintaining a company's role model.

- **Policy Validations**

  CA Identity Manager administrators can validate proposed changes against a role model in CA RCM before committing changes. Validating changes before they are committed helps companies maintain the role model that they have defined for their operations.

  Users can validate proposed changes to provisioning roles (assigning or removing them), and changes to user attributes.

  CA Identity Manager performs two types of policy validations:

  - **Compliance**

    Proposed changes are validated against the CA RCM role model to see if they violate explicit, predefined business policy rules in CA RCM.

  - **Pattern**

    Proposed changes are compared to the CA RCM role model to see if they cause the subject of the change to become "out of pattern." CA Identity Manager also makes sure that the changes do not significantly alter an established pattern in the role model.

  You can configure CA Identity Manager to perform these validations automatically when users perform certain tasks, or allow users to initiate the validation manually.

You can implement Smart Provisioning in an Identity Manager Environment once there is an established role model, based on Identity Manager data, in CA RCM.

Connector for Identity Manager - Supported Endpoints

In this release, the connector for Identity Manager supports the following endpoints. Some of these endpoints are supported using predefined endpoint handlers as in CA Identity Manager r12, while others use the customizable xml-based endpoint handler introduced in this release.

Endpoint	Support	Resources	Comments
Unix (ETC)	Customizable handler	UNIXETC Group	No known limitations
Windows (N16)	Customizable handler	NT Group	Update limitations
Oracle Database (ORA)		User Packages, User Role, User Procedure, and Admin Packages	Export is limited to specific endpoint rules.
OS400 (AS4)	Customizable handler	Profile Group and Member Group	Users must have a primary group to have regular groups. You must configure a primary group before you can add regular groups to a user. Similarly, remove all regular groups before removing a primary group.
Microsoft SQL	Customizable handler	DBAccess and Server Role	To remove a resource from an account template or a user, first remove the DB Access permission.
LDAP **Note:** LDAP is not a supported connector type in Provisioning	Customizable handler	Group	No known limitations

Endpoint	Support	Resources	Comments
SAP	Predefined handler	Authorization and Role	Authorization, with the exception of the Retrieval of User - Resource links operation. Role, with the exception of the following operations: ■ Retrieval of Account Template – Resource links ■ Retrieval of User – Resource links ■ Update of removed User - Resource links
DB2	Predefined handler	Index, Schema, Table, Tablespace, and View	User-Resource links are not imported
Active Directory (ADS)	Customizable handler	Active Directory Group	CA RCM account template handling must be based on an AD account policy or an AD contact policy. The connector can poll and update only one of these policy types. Account templates should reference only one endpoint. During data export, the connector does not accurately parse some change entries in the audit card. When you configure the connector, you must assign a DN field for each data type that is exported.

Connector for Identity Manager - Update Limitations

Successful update of endpoint data using the customizable endpoint handler requires thorough knowledge of the data structure, syntax, and rules of the target endpoint type. To avoid problems, you must consider the data structure dictated by the endpoint type when you configure the handler and define data mapping.

The following general issues apply when you use the customizable endpoint handler to send updates to CA Identity Manager:

- **Target endpoint restrictions** - Identity Manager allows configuration of password protection and other validation restriction on endpoints and endpoint types. These restrictions may cause creation of entities on Identity Manager to fail. CA RCM does not verify successful creation of new entities during update, and the CA RCM connector may not record these events in its log.
- **Account Templates** - The following limitations concern how CA RCM and Identity Manager handle resources, endpoints, and account templates:
  - Do not rename account templates in CA RCM. When you rename an account template, CA RCM attempts to update endpoints by deleting the existing template and creating a new template. This unintentionally modifies many template attributes.
  - Changes to an endpoint's resource are reflected in all endpoints of the same type. For example, if you delete the "admin privileges" resource from an account template, and send an update of that template to *a single*, *specific* Microsoft SQL Server endpoint - the "admin privileges" resource is removed from *every* Microsoft SQL Server endpoint that has that resource.
  - CA RCM does not verify whether an Identity Manager account template is available for a target endpoint or endpoint type. You must verify that the account template is available before you update endpoints of a given type.
  - The default account template (the Identity Manager account template referenced by CA RCM as a model for new account templates) is specified in a static configuration file. CA RCM does not verify this setting and does not detect if the default account template has been deleted or changed in Identity Manager.
- **Error Logging** - In some situations, errors during update are not recorded in the log file of the connector job.

CA Enterprise Log Manager Integration

CA Enterprise Log Manager uses the CA Common Event Grammar (CEG) to map events that originate in various systems in a standard format, and stores all events, even those which are not yet mapped, for review and analysis. Furthermore, CA Enterprise Log Manager provides users with a high-volume solution for managing and reporting on collected data, using configurable database queries and/or reports to search for various types of information and events.

CA Enterprise Log Manager provides better wider and deeper insight into un-managed systems and systems outside of CA Identity Manager's purview and control and also lets you investigate deeper into identities.

Integrating with CA Identity Manager lets you view CA Enterprise Log Manager identity centric reports and/or dynamic queries into CA Enterprise log Manager user Console using the Identity Manager User Console. From the User Console you can configure how existing CA Identity Manager/Enterprise Log Manager reports and/or queries are viewed and modified while you investigate deeper into a specific identity.

CA Enterprise Log Manager Reports

The following CA Enterprise Log Manager Reports are provided with CA Enterprise Log Manager role definitions by default:

Task	Invokes Report
System All Events by User	CA Identity Manager - System All Events filtered by user ID
Account Management by Host	Account Management by Host
Account Creations by Account	Account Creations by Account
Account Deletions by Account	Account Deletions by Account
Account Lockouts by Account	Account Lockouts by Account
Certification Process Activity by Host	CA Identity Manager - Process Activity by Host
Password Policy Modify Activity	CA Identity Manager - Policy Modify Activity

Identity Manager Directory Configuration Wizard

In this release, a new wizard is available that walks administrators through the process of creating an Identity Manager directory for their LDAP user store or Provisioning Server and helps reduce configuration errors. Before launching the wizard, you must first upload an Identity Manager LDAP directory configuration template. These templates are pre-configured with well-known and required attributes. After entering connection details for your LDAP user store or Provisioning Server, you can select LDAP attributes, map well-known attributes, and enter metadata for the attributes. When you are done mapping attributes, click Finish to create the directory.

Account Management Enhancements

In the User Console, you can now perform most account management tasks. For example, you can now:

- Explore the contents of an endpoint and correlate its accounts, or you can pick a subset of the endpoint to explore.
- Create and modify endpoints so that you can use them in account templates
- Create and modify account templates for all endpoints
- Manage individual accounts on an endpoint to unlock them, assign them to a new user, or perform several other tasks.

Also, you can now use the Management Console to define an endpoint type. You import a role definition file that contains the screens, tasks, and roles for that endpoint type. The endpoint types you can define include dynamic endpoint types that you create in Connector Xpress.

Previously, these features were available only in Provisioning Manager.

Endpoint Types that Require Provisioning Manager

You can now use the User Console to manage most endpoint types, however, the following endpoint types are only managed in Provisioning Manager:

- Entrust PKI
- CA SSO
- CA EEM
- Novell Netware
- Ingres
- NSK Safeguard

Install and Upgrade Enhancements

The following improvements have been made to the CA Identity Manager r12.5 installer:

- Install:
  - Pre-installation prerequisite checking
  - All connectors are now installed by default
- Upgrade:
  - New Upgrade Wizard with the following features:
    - Discovers CA Identity Manager components already installed
    - Provides version information of installed components
    - Specifies if the component is up to date or if an upgrade is available
    - Upgrade prerequisite checking
    - Provides direct launch of provisioning component installers
    - Verifies a successful upgrade with error checking
  - Automated CA Directory upgrade that moves from Ingres technology to DXGrid technology
  - Automated Identity Manager Directory and Environment migration
  - Automated task persistence migration
  - JDBC drivers added automatically
  - Automated WorkPoint workflow upgrade, with a choice of manual upgrade, if necessary
  - Automated data sources upgrade
  - Automated import of new feature and account screen role definition files

Automated Task Persistence Garbage Collection and Archiving

In this release, an administrator is able to schedule and modify jobs with specific parameters using the Cleanup Submitted Tasks task to clean up and archive task and event information in the task persistence database and also delete these recurring tasks as needed.

From the System Tab, you can launch a wizard by selecting Cleanup Submitted Tasks. From there, the wizard walks you through setting up and scheduling jobs and whether or not to archive the data. You can also choose to delete the recurring jobs when needed by selecting Delete Recurring Tasks from the System Tab.

By scheduling the tasks to clean up and archive task data, the potential for performance problems or system outages are greatly reduced. With the archive feature, you can back up the tasks to the archive database before deleting them from the runtime database. If you need to go back and view these deleted tasks, select the Search the archive check box on View Submitted Tasks to search and view a list of all tasks that have been deleted and archived.

Task Persistence Migration Tool

With this release, a new migration tool has been added for migrating the task persistence databases from r8.1 SP2 or r12 to r12.5. The command line tool is part of the Identity Manager Administrative Tools and is found in the following location:

admin_Tools/tools/tpmigration

The default location for a*dmin_tools* is:

- **Windows**: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager/tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Connector Xpress Enhancements

In Connector Xpress you can now do the following:

- Use multitable JDBC Connectors- values from multiple columns from a table, rather than from a single column, can populate a single attribute value.
- Use JDBC structural and auxiliary classes.
- Use a new flexible mapping process that includes a tree of class and attribute mappings has replaced the previous sequential wizard process. This lets you add and edit and remove attributes as required.
- Specify direct associations between any two classes of objects
- Specify indirect associations between objects. For example, where the association between the two objects is bidirectional and contained in a third entity such as a table, which holds the association links between the objects.
- Create method and script style operation bindings

- Bind operations to other object and class combinations
- Bind two or more opbindings to the same timing, that is the same operation for the same target object classes. For example, you can have two or more opbindings for the Before Add operation for the account object class.

Bulk Loader Allows Multiple Actions

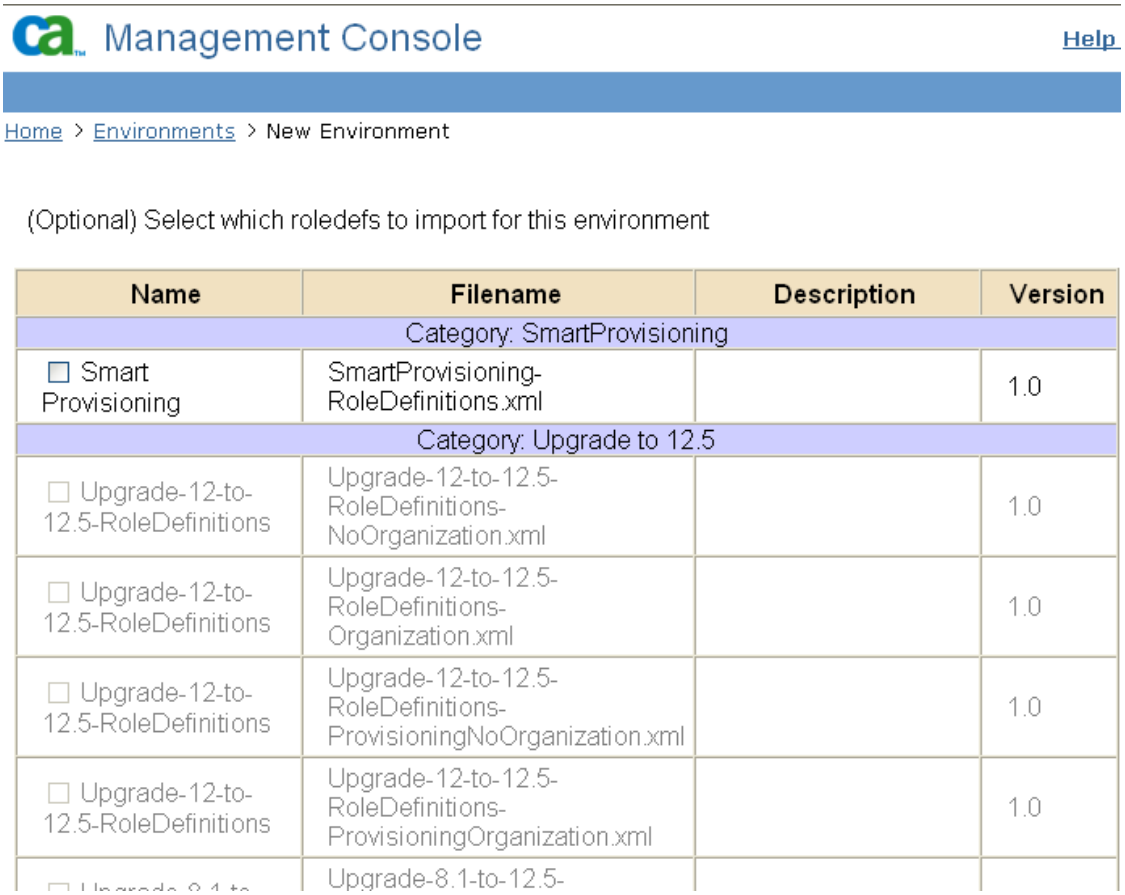
The Bulk Loader feature in CA Identity Manager now allows you to specify an alternate action mapping for objects that do not exist.

Previously, CA Identity Manager let you select an action to perform on a primary object. If that primary object did not exist and the action specified was Modify or Delete, an error was given. Also, if you specified a Create action on a primary object that already existed in CA Identity Manager, an error was given.

In CA Identity Manager r12.5, you can select a create (or self-create) alternate action to execute if the primary object does not exist.

Role and Task Import Enhancements

The Management Console now provides the ability to select one or more predefined Role Definitions files to import from a list of available files when you create or update an Identity Manager Environment. This significantly reduces the configuration steps for setting up an Environment.



The predefined Role Definitions files create roles and tasks for CA Identity Manager functionality, including:

- Smart Provisioning
- Enterprise Log Manager integration
- Account Management

Note: For more information about importing Role Definitions files, see the *Configuration Guide*.

Reporting Data Sources

In CA Identity Manager r12.5 you can specify a different data source for a report, other than the Snapshot Database. For example, if you want to access audit information, you can now provide the connection information for the audit database to a report and the report will pull its data from the audit database.

Also, specifying connection information for a data source (for reporting) has moved from the Management Console to the User Console, under System, JDBC Connection Management.

Note: For more information on reporting, see the *Administration Guide*.

New Default Reports

The following reports have been added to CA Identity Manager:

Report	Description	Source
Account Details	Displays a list of account templates with associated provisioning roles, endpoint types, endpoints, and accounts.	Snapshot database
Administration	Displays a list of administrators with their administrative entitlements.	Snapshot database
Audit-Assign/Revoke Provisioning Roles	Displays a list of provisioning role events.	Audit database
Audit-De-Provisioning	Displays a list of users and their accounts that were de-provisioned.	Audit database
Audit Details	Displays tasks and events with related status details.	Audit database
Audit-Pending Approval Tasks	Displays a list of pending approval tasks.	Audit database
Audit-Reset Password	Displays the list of users' passwords that have been reset for a given period of time.	Audit database
Endpoint Details	Displays a list of all endpoint types, endpoints, and the endpoint attributes.	Snapshot database

Workflow Enhancements

CA Identity Manager r12.5 includes the following enhancements to workflow functionality.

Support for WorkPoint 3.4.2

CA Identity Manager r12.5 supports Workpoint 3.4.2. Previously, CA Identity Manager r12 supported WorkPoint 3.3.2.

Policy-Based Workflow

Policy-based workflow allows you to associate an event with a workflow process based on the evaluation of a rule. This means that instead of an event always launching a workflow process, the workflow process runs and generates a work item only if a rule associated with the event is true.

For example, when creating a new group, you can define a rule that places the CreateGroupEvent under workflow control and creates a work item only if the new group is part of a designated parent organization. If the new group is not part of that organization, the workflow process does not execute and no work item is created.

If an event has multiple rules, then all workflow process associated with the event need to be approved in order for the event to be approved. Similarly, if one workflow process associated with the event is rejected, the event itself is rejected. Workflow rules can be assigned priority values to determine the order of rule evaluation and workflow execution.

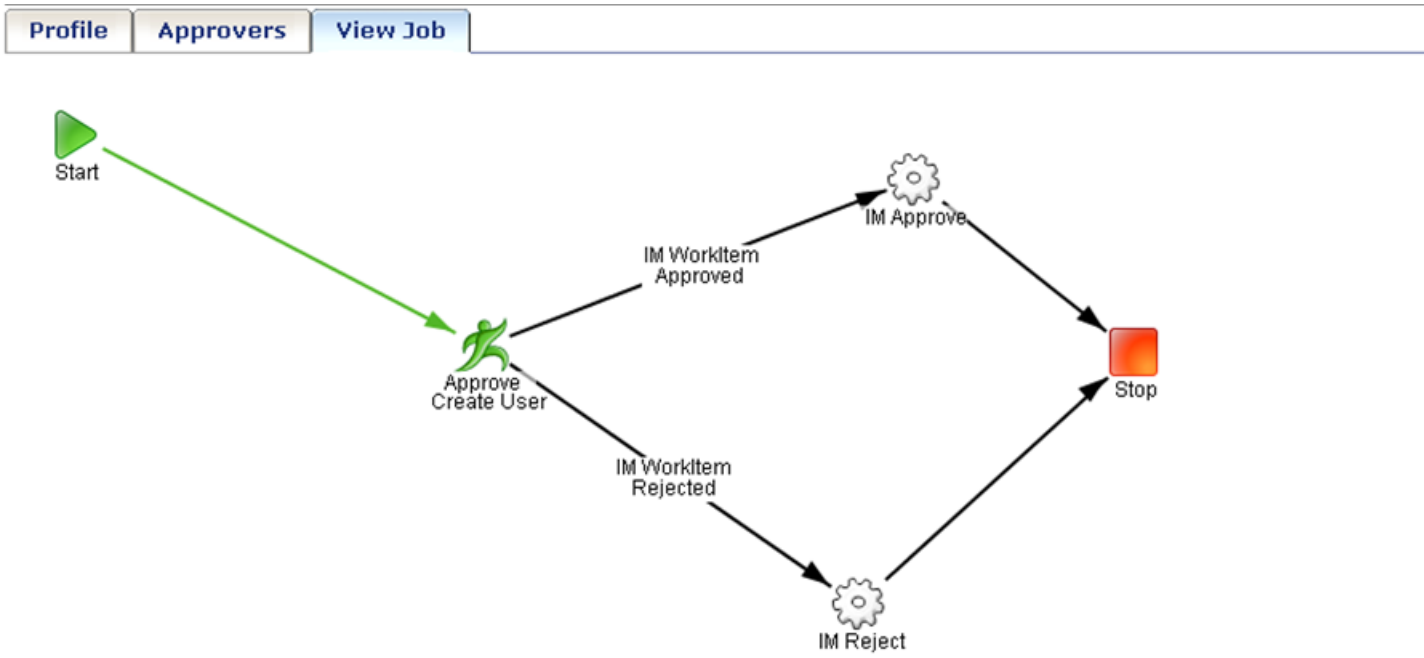
All default Identity Manager workflow templates and predefined processes support workflow rules. You can also create custom workflow processes for use with workflow rules.

Note: For more information about policy-based workflow, see the *Administration Guide*.

Workflow Job View

In this release you can now view a graphical representation of the runtime status of Workpoint jobs for task and event level Workflow in the User Console from the following:

- Approval tasks
- View Submitted Tasks



You can also view both template and legacy process definitions.

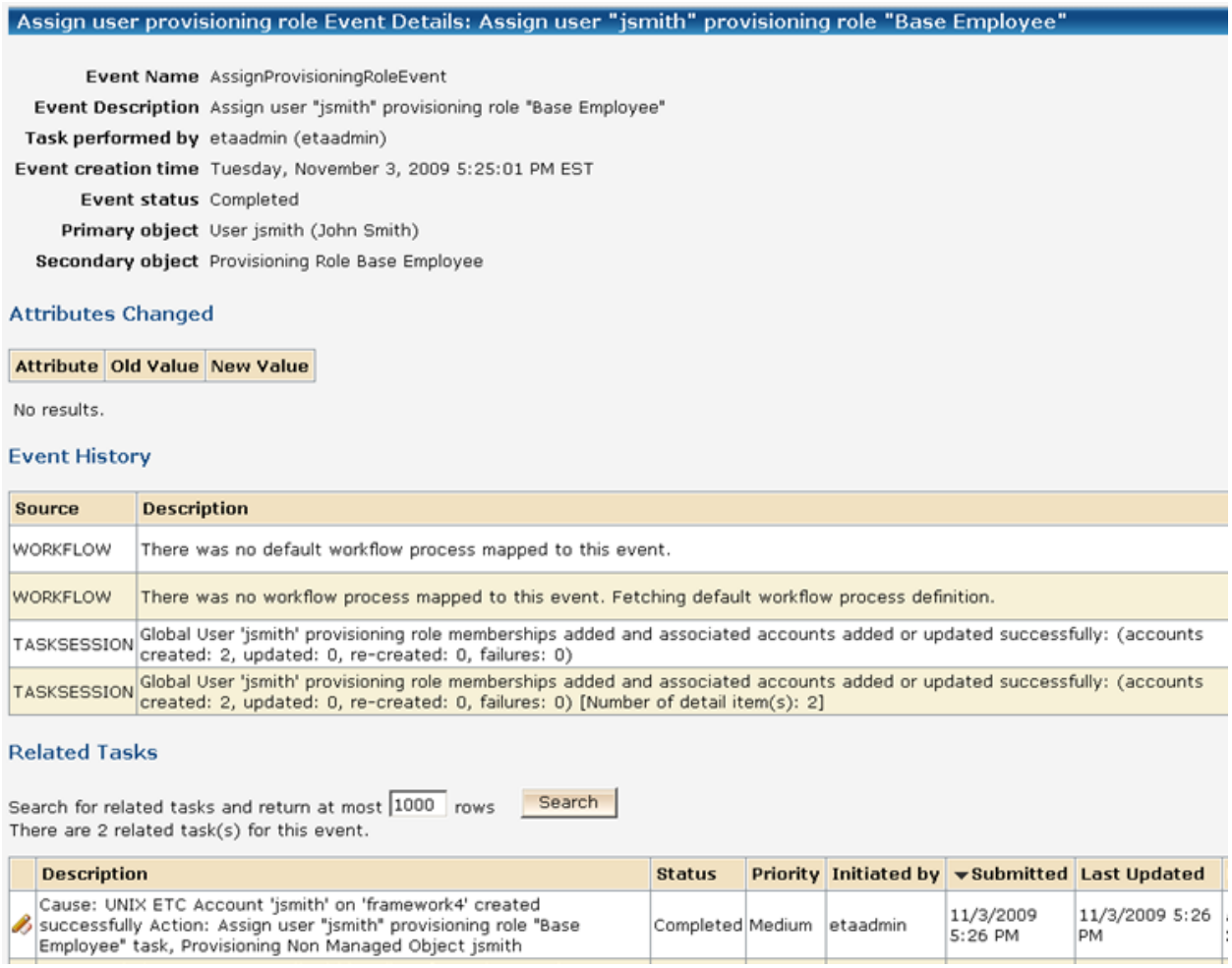
In new environments, approval tasks include the View Job tab by default. You can view the job images for events or tasks in the View Submitted Tasks created in this release only. You cannot view the job images for events created in earlier releases.

View Submitted Task Enhancements

The View Submitted Tasks tab now displays information about changes that occur on endpoints as a result of actions initiated from the Identity Manager User Console. For example, when an administrator assigns a provisioning role to a user in the User Console, the View Submitted Tasks tab displays information about which accounts were created successfully, and about any errors or failures that may have occurred.

This information appears in the Related Tasks section of the Event Details screen.

The following example shows the Event Details screen for an Assign User Provisioning Role event:



Note: For more information about the View Submitted Tasks tab, see the *Administration Guide*.

Profile Screen Enhancements

In CA Identity Manager r12.5, the Profile screen includes several new configuration settings to support new functionality. These new settings are described in the following sections.

Confirmation Fields

CA Identity Manager r12.5 now includes support for confirmation fields that you can use to verify that the values of two fields on a profile screen match. Examples of confirmation screens include Confirm Password and Confirm Email.

Note: For more information, see the *User Console Design Guide*.

Dynamic Field Display

CA Identity Manager can set certain field display properties based on the value of other fields in a profile screen. Using JavaScript, you can hide and show a field, or enable and disable a field. For example, you can use JavaScript to show an Agency field if the Employee Type is set to Temp. If the Employee Type is Full Time or Part Time, the Agency field is hidden.

Note: For information on using this feature, see the *User Console Design Guide*.

New Object Selector Field Style

CA Identity Manager r12.5 includes a new Object Selector style option for fields on a profile screen. This option displays a control that administrators can use to search for and select a managed object. This style is typically used in account management screens.

Note: For information on using this feature, see the *User Console Design Guide*.

Support for Microsoft Visual Studio 2008

CA Identity Manager fully supports Microsoft Visual Studio 2008 SP1. This means that all custom code written for previous releases of CA Identity Manager, which supported Microsoft Visual Studio 2003, must be recompiled using Visual Studio 2008 SP1. Custom code impacted may include the following:

- C++ custom connectors
- Provisioning manager plug-ins for Java custom connectors
- Common program exits

- Universal Provisioning Option (UPO) program exits
- Pluggable Authentication Module (PAM) DLLs
- Universal Feed Option program exits

Identity Policy Enhancements

You can create a member rule for a policy set, so that the policy set applies only to certain users. The rule is evaluated before evaluating identity policies in the set, which can save significant time. For example, if the member rule limits the identity policy evaluation to 10 percent of users, that rule would save 90 percent of the evaluation time.

Provisioning Role Owner Task

In the User Console, you can use a new task: Create Owner Policies for Provisioning Roles. You can select one or more provisioning roles and assign owner policies to control who can modify the roles. This task is an alternative to the Reset Provisioning Role Owners task, which can only be used on one role at a time.

Chapter 2: Changed Features

This section contains the following topics:

r12.5SP6

This section contains the following topics:

Configure GINA Clients to Accept Only Valid SSL Certificates

The GINA and Credential Provider have been enhanced. You can now configure the GINA and Credential Provider so that clients only accept valid SSL certificates. You can configure the GINA and Credential Provider so that the Yes button (accept certificate) is unavailable on the Security Warning dialog when an expired or invalid SSL certificate is imported.

This prevents clients accepting expired certificates, or non-genuine certificates from hosts attempting to impersonate a trusted CA Identity Manager server, greatly reducing the risk of man-in-the-middle attacks and the possibility of executing malicious code. This option also prevents the user from accessing the local filesystem through the Security Warning dialogs.

An option has been added to allow administrators to enable this setting during silent install.

To enable this option, set the REJECTINVALIDCERTS=Yes in the silent install options.

Note: This feature is not enabled by default.

r12.5 SP5

This section contains the following topics:

Short Name Attribute for Lotus Notes/Domino Can Be Multi-Valued

CA Identity Manager now allows the Short Name attribute in Lotus Notes to be multi-valued. However, you cannot use the User Console to work with multi-valued short names. For information about using multi-valued short names, please contact CA Support.

UNIX Remote Agent Works on Solaris Zones

The UNIX Remote Agent now supports installation on Solaris Zones where the /usr filesystem is inherited from the Global Zone. For deails on how to configure this functionality, see TechDoc 510246.

r12.5 SP4

This section contains the following topics:

Generate TEWS WSDL According to WS-I Compliance Standards

The TEWS WSDL can now be generated according to WS-I compliance standard.

Note: The existing samples and custom code do not compile successfully because they do not conform to WS-I standards.

To generate the TEWS WSDL to WS-I Compliance standards

1. In the CA Identity Manager Management Console, click Environments, env.name, Advanced Settings, Web Services.

   The Web Services page appears.

2. Select the Generate WSDL in WS-I form check box.

Note: A sample Java class file AccessUtil.WSI has been added to samples/WebServide/Axis. The file has been renamed so that it does not compile.

CA Identity Manager and Siteminder Integration Password Criteria

When CA Identity Manager is integrated with SiteMinder and uses Siteminder's password handling capability, password policies are obtained from the Siteminder Policy Store. In this case, construct passwords that meet Siteminder's password criteria. The following punctuation characters are the only punctuation characters that meet Siteminder's password criteria:

'*', '(', '\',',','@','"',':','#','_','-','!','&','?',')','(','{','}','*','.','/' “

Important: CA Identity Manager does not impose any restriction on the use of punctuation characters in passwords. However, if you intend to use Siteminder password capability, we recommended that you construct passwords that meet Siteminder's restrictions.

Admin Roles Now Enforce Scoping Rules for Provisioning Roles in Member and Admin Policies

Provisioning role scope is now implemented in provisioning role searches.

Administrators must specify provisioning role scope in member and admin policies for roles that include tasks for managing provisioning roles. For example, the Provisioning Role Manager role must include scope rules in member and admin policies to define which provisioning roles role members can manage.

If the scope rules are not specified, no provisioning roles are returned when administrators perform searches in tasks such as Modify Provisioning Role, or Modify Provisioning Role Membership.

Note: Administrators must define provisioning role scope in member and admin policies *only* when the tasks that manage provisioning roles are configured with the All Provisioning Roles search option on the Search tab for the task. For more information about search configuration settings, see the online help for the Search tab for a task.

Custom HTML on Admin Task Screens Support Localization

CA Identity Manager administrators can add text anywhere in a profile screen to provide additional information, such as online help text for a field, to users.

These fields can now be localized, so that they can display content in different languages.

To display custom HTML in a different language, specify a resource key with the following format in the custom HTML field:

${bundle=*ResourceBundle*:key=*keyID*}

ResourceBundle

Identifies the resource bundle that includes the text string mapping for the key ID.

keyID

Identifies the key ID that maps to the text string to display. The mapping must exist in a resource bundle.

For example, the HTML for a localized field should resemble the following:

```
<p>
${bundle=MyResourceBundle;key=MyResourceKey}
</p>
```

Note: For more information about specifying resource keys, see the chapter on CA Identity Manager Localization in the *User Console Design Guide*.

BIConfig Tool to Deploy Default Reports

BIConfig is a new utility that uses specific XML files to streamline the deployment of default reports within CA Identity Manager.

Note: For more information about the BIConfig utility, see the Report Server Installation chapter of the *Installation Guide*.

MySQL Supported for Report Database

To simplify the Report Server installation, CA Identity Manager now supports MySQL as a Report Database. If you have a previous installation of the Report Server with Oracle or Microsoft SQL, you can continue to use those databases. For a new installation of the Report Server, use the MySQL default database packaged with the installer.

r12.5 SP3

This section contains the following topics:

The Policy Xpress LDAP Plug-in Now Supports Secure Connections

When using the Policy Xpress LDAP plug-in, you can select the Secure Connection check box to communicate with an SSL-enabled directory server.

Enable Logging to Trace Domain Open and Close Events Initiated from the Provisioning Manager

Open and close events are user-initiated events that occur when the user opens or closes a Provisioning domain using the Provisioning Manager. Opening the domain establishes the first LDAP connection to the Provisioning Server. After, the Provisioning Manager can open additional LDAP connections. Closing the domain closes all open LDAP connections.

The Provisioning Manager logs domain open and close events at INFO level.

To enable open and close event logging, configure logging in the Provisioning Manager.

To enable open and close event logging

1. In the Provisioning Manager, click File, Preferences, Logging tab.

   The Logging tab appears.

2. Select the Enabled check box next to the logging destination you want.

Example: How open and close events are logged

Each Domain open event is logged in etaclient*.log as:

```
INFO IM Provisioning Manager - Domain opened (<working_domain>:<user>@<user_domain>)
```

Each Domain close event is logged in etaclient*.log as:

```
INFO IM Provisioning Manager - Domain closed (<working_domain>:<user>@<user_domain>)
```

Enable Logging of LDAP Unbind Operations

The Provisioning Server has been enhanced to log LDAP unbind operations in the etatrans*.log. An unbind operation does not necessarily mean that the domain is closed as the Provisioning Manager can open additional LDAP connections after the first connection has been established.

To enable Provisioning Server transaction logging

1. In the Provisioning Manager, click System, Domain Configuration, then expand Transaction Log.
2. Set Enable to true.

   Each unbind operation is logged as follows:

   ```
   Unbind    :E133:----:S: External Unbind (eTGlobalUserName=<user>) Requested by
   User <user>

   Unbind    :E133:----:P:     dn:
   eTGlobalUserName=<user>,eTGlobalUserContainerName=Global Users,eTNamesp

   Unbind    :E133:----:P:+    aceName=CommonObjects,dc=<dc>

   Unbind    :E133:----:F: SUCCESS: External Unbind (eTGlobalUserName=<user>)
   ```

Support for Ampersand in NIS Home Account Definitions on Remote NFS Servers

When accounts are created on an NIS endpoint and are configured to use a remote home directory mounted by NFS, the “Directory” name in the Remote server field now supports the ampersand character. This matches standard /etc/auto_home syntax. For example, the “Directory” field can contain “/export/home/&” to define the user home directory that is on the NFS server. The ampersand is replaced with the username when the directory is created, and the /etc/auto_home definition on the NIS server uses the ampersand syntax.

To create the remote directories so that they can be written to, join the NFS server to the NIS domain where you are provisioning the account. Joining the NFS server to the domain means that the created home directory on the NFIS server has permissions based on the uid of the NIS domain account, and that the new account is common across both servers.

UNIX Remote Agent Install on Solaris Sparse Zone is Now Supported

The UNIX Remote Agent has been enhanced to support installation on Solaris Zones where the /usr file system is inherited from the Global Zone.

Note: In previous versions of CA Identity Manager, only full root zones were supported.

Installing the UNIX Remote Agent on a zone with an inherited /usr file system creates a symbolic link in the /usr/bin directory of the Global Zone, named uxsautil. This link must point to the uxsautil binary installed with the Remote Agent. We recommend that you install the Agent in the Global Zone before installing in the non-Global Zone, using identical installation paths.

You can also create the Global Zone symbolic link manually. Verify that it points to the install location used in the non-Global Zone. For example, using the default install location, you would run the following commend:

```
ln -s /opt/CA/IdentityManager/ProvisioningUnixAgent/bin/uxsautil /usr/bin/uxsautil
```

If you use the UNIX Remote Agent in a sparse zone and run with the CAM service as a non-root user, manual configuration is required. As with the /usr/bin/uxsautil, which is inherited from the global zone, the file ownership permissions are also inherited. You must manually configure the permissions to match within the sparse zone, and then verify that the "cam" user and group match on both zones.

To configure the permissions to match within the sparse zone

1. In the global zone with the UNIX Remote Agent installed, find the User ID (uid) of the "cam" user, and the Group ID (gid) of the "cam" group.
2. In the sparse zone, add the user and group manually:

   ```
   - groupadd -g <gid> cam
   ```

   ```
   - useradd -u <uid> -g <gid> cam
   ```
3. Verify that the home directory of the "cam" user is a valid path. The user account is used during the Remote Agent installation process.
4. Install the UNIX Remote Agent with "CAM as a non-root user" enabled.

   Note: If the remote agent is uninstalled and the "cam" user and group have been created manually, delete the "cam" user and group manually. The Remote Agent can remove accounts it added, but cannot distinguish between manually created service accounts and a user account named "cam".

Enable Clear Password Fields on Reset User Password Task

You can now display clear password fields in the Password field in the Reset User Password task in the Identity Manager User Console instead of asterisks.

To enable clear password fields on Reset User Password task

1. Start the CA Identity Manager Management Console.
2. Select the environment you want to manage, then click Advanced Settings.

   The Advanced Settings page appears.
3. Click Business Logic Task Handlers, BlthPasswordServices.

   The Business Logic Handler Properties page appears.
4. Select the ClearPwdIfInvalid check box and enter true
5. Select the PwdConfirmAttrName checkbox and enter the following:
   `|passwordConfirm`
6. Verify that ConfirmPasswordHandler settings are as follows:
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfrmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   The Reset User Password task now displays clear password fields instead of asterisks.

r12.5 SP2

This section contains the following topics:

Salesforce.com Connector Account Deletion

You cannot use the Salesforce.com connector to delete a Salesforce.com user, as Salesforce.com does not support account deletion.

In CA Identity Manager 12.5 SP1, CA Identity Manager was configured to suspend the account on the Salesforce.com endpoint and place the account in a DeletePending state when any operation that attempted to delete a Salesforce.com account directly or indirectly occurred.

In CA Identity Manager 12.5 SP2, account deletion and suspension behavior has changed.

CA Identity Manager now simulates account deletion when any operation that attempts to delete a Salesforce.com account directly or indirectly occurs, for example, removing the role that created that account.

When the option *Account Options on Delete Accounts will be deleted from both the provisioning directory and the managed endpoint (not supported by Salesforce)* is selected on the Endpoint Settings tab in the User Console, the account is deactivated and placed in a group called CA ILM SFDC Connector Suspended on the Salesforce.com endpoint.

During an add operation, the Salesforce.com connector verifies that the account exists on the Salesforce.com endpoint and checks to see if the account is in the CA ILM SFDC Connector Suspended group.

If the account is in the CA ILM SFDC Connector Suspended group, CA Identity Manager removes the Suspended membership and modifies the account, instead of adding a new account.

During an explore and correlate, CA Identity Manager ignores all accounts in the CA ILM SFDC Connector Suspended group.

The Salesforce.com connector creates the CA ILM SFDC Connector Suspended group as required.

Note: For more information, about suspending and resuming a user account, see the *CA Identity Manager User Console online hel*p.

UNIX Remote Agent can be Installed on Solaris 10 Sparse Local Zones

The UNIX Remote Agent has been enhanced to support installation on Solaris Zones where the /usr filesystem is inherited from the Global Zone. Full root zones have been supported throughout r12.0 and r12.5's availability.

Installing the UNIX Remote Agent on a zone with an inherited /usr requires that a symbolic link is created in the Global Zone's /usr/bin directory, named "uxsautil." This link must point to the "uxsautil" binary installed with the Remote Agent, so we recommend that you install this agent in the Global Zone before the non-Global Zone, using identical installation paths.

You can also create the Global Zone symbolic link manually. Ensure that it points to the install location that will be used in the non-Global Zone. For example, using the default install location, you would enter:

```
ln -s /opt/CA/IdentityManager/ProvisioningUnixAgent/bin/uxsautil /usr/bin/uxsautil
```

If the UNIX Remote Agent is intended to be used in a sparse zone and run with the CAM service as a non root user, manual configuration is required. As the /usr/bin/uxsautil is inherited from the global zone, so are the file ownership permissions. These must be configured to match within the sparse zone. The "cam" user and group need to match on both zones.

1. In the global zone with the UNIX Remote Agent installed find the User Id (uid) of the "cam" user, and the Group Id (gid) of the "cam" group.
2. In the sparse zone, add the user and group manually:
   - `groupadd -g <gid> cam`
   - `useradd -u <uid> -g <gid> cam`

   Note: Ensure that the cam user's home directory is a valid path. The user account will be used during the Remote Agent installation process.

3. Install the UNIX Remote Agent with "CAM as a non root user" enabled.

As the "cam" user and group have been created manually, if the remote agent is uninstalled, they will also need to be deleted manually. The Remote Agent is written to remove accounts it added, but cannot distinguish manually created service accounts from a potential user.

UNIX Remote Agent can be Installed Silently

The IdentityManager.[Platform].sh script has been enhanced to allow silent installation in Identity Manager r12.5. You can use the following command to install the script:

```
sh IdentityManager.[platform].sh [-r file name] [-f file name]
```

-r:

Runs the installation dialogs and creates a response file with the values you entered. The product is not installed.

-f:

Installs the product. You can add a response file to customize unattended installation.

UNIX Remote Agent can be Called by Non-root Users

If the UNIX Remote Agent is enabled, use of CAM commands by the root user may change file ownership causing errors. For example, to authorize a Connector Server to have access to a UNIX endpoint, you would run this command:

```
cafthost -a <connector-server-hostname>
```

This command writes to cafthost.cfg in CAM's installation directory. If the root user issues the command, the file will be owned by the "root" user and group. However, when CAM is configured to run as a non root user, it will be owned by the "cam" user and group, and this account cannot read the file written with root's credentials.

Workaround

After running the "cafthost" command, run:

```
chown cam:cam cafthost.cfg
```

Following this, CAM (and CAFT which runs on top of CAM) should be restarted. As the superuser, run the following commands:

```
CAM_HOME=`cat /etc/catngcampath`; export CAM_HOME
$CAM_HOME/bin/caftclse
$CAM_HOME/bin/camclose
su - cam -c $CAM_HOME/bin/cam
su - cam -c $CAM_HOME/bin/caft
```

CAM is a common dependency of CA products, however this configuration has been tested only with the CA Identity Manager UNIX Provisioning Agent. If you have CA products that use CAM, check their support for this configuration with CA Support before installation.

This functionality can be enabled on new installations of the UNIX Remote Agent. Upgrade installations do not support changing of install time configuration parameters.

Oracle Applications Prerequisite

You must set the NLS_LANG as a system environment variable, with .UTF8 as the value.

Note: There must be a period (.) before UTF8 on the system where the Connector Server is installed.

Deprecated Components

The following components are deprecated in CA Identity Manager r12.5 SP2:

- Embedded Entitlement Manager (EEM) Connector

  Note: This connector was referred to as the Embedded IAM (EIAM) Option in CA Identity Manager r8.1 SP2 and earlier releases.

- Ingres Connector
- Novell Netware Connector
- NCR MP-RAS support in the UNIX Connector

Provisioning Server and Related Packages Enhancements

The Provisioning SDK and related packages have been enhanced to support the use of custom C++ connectors through the CA Identity Manager User Console.

Note: For more information, see the Tech Doc on: https://support.ca.com/irj/portal/anonymous/redirArticles?reqPage=search&searchID=TEC520582

r12.5 SP1

This section contains the following topics:

Additional Objects Included in Role Definitions File

The following additional objects are now imported and exported using the role definitions file:

- Policy Xpress policies
- Bulk Task definitions
- Email notification policies
- Reverse (New and Modify) Account policies

Localization Files are Now Deployed During Installation

In previous versions of CA Identity Manager, sample translated resource bundles, which you can use to display CA Identity Manager in a different language, were available in the Administrative Tools.

These translated resource bundles are now installed by default.

Note: For more information about creating localized versions of CA Identity Manager, see the *User Console Design Guide*.

Enhanced Work Item Delegation

In previous releases, you could specify the start time, but not the end time for delegations. Newly created delegations have their dates for delegation set to true, with the Default start time set to now.

At modification time, start and end dates can be changed. The default end time is one week from start date.

Alternately, you can do the same from the Delegate Work Items tab when Creating or Modifying a user.

Enhanced Dynamic Resolver

The Dynamic Resolver has been enhanced to add the previous approver to the supported object list. If the physical attribute that stores manager information is selected, the configuration routes an approval to a manager.

Adding a previous approver to the supported object list of the resolver lets the dynamic resolver be used with the escalation approval process. Because the modification is done solely for usage with the escalation approval process, there is no singling out of the person who actually did the approval. The entire population of Users, identified as approvers for the previous work item of the current job are inspected for requested information (manager UID, and so forth). All individuals identified by this inspection are the approvers for the current work item (escalation).

New Task Recurrence Model

A new, global recurrence model is available for the Execute Explore And Correlate task and the Capture Snapshot Data task. The new model functions as a wizard with the following two steps:

1. Recurrence—allows you to schedule the task or execute the task immediately.
2. The Task—allows you to specify task parameters.

Note: For more information about the new recurrence model, see the Recurrence Tab in the *Administration Guide*.

r12.5

This section contains the following topics:

Snapshot Database Performance Improvements

Significant performance improvements have been made when exporting data to the snapshot database.

To further improve performance, use a snapshot parameter XML file that targets specific data needs, such as targeting the Identity Manager objects used to generate a Report on endpoint accounts.

Snapshot Parameter XML File Enhancement

When exporting an endpoint object, you can now use the <exportattr> element along with the <objattr> element to define the account attributes to be exported with a particular endpoint type, as follows:

```
<exportattr objecttype="endpoint_type">
     <objattr name="description"/>
     <objattr name="fullName"/>
     <objattr name="lastLogin"/>
</exportattr>
```

Connection Management

Connection Management has been replaced with JDBC Connection Management in CA Identity Manager.

JDBC Connection Management allows you to specify alternate data sources for reporting within Identity Manager. It allows you to provide connection details to different databases and categorize them into connection types. Also, for each connection type you can specify a default connection.

Important! We recommend that you do *not* use the Identity Manager object store database as a data source for generating reports, due to performance reasons.

Environment Export Includes Additional Objects

The following Environment-specific managed objects are now exported with roles and tasks:

- Connections (including connection objects for CA RCM, CA Enterprise Log Manager, and reporting)
- Snapshot definitions
- Export and correlate definitions

If the export includes attributes that have a data classification of attributelevelencrypt or sensitive, CA Identity Manager encrypts those attributes in the exported file.

Fixes and Enhancements from CA Identity Manager Cumulative Releases (CRs)

CA Identity Manager r12.5 includes fixes and enhancements from CA Identity Manager r12 CRs 1 - 6.

Active Directory Connector Now Supports Win2003 R2 UNIX Attributes

The Windows 2003 R2 UNIX extensions in conjunction with CA Access Control UNIX Authentication Broker lets you use Active Directory to manage UNIX computers and accounts. CA Identity Manager provisions UNIX access by populating these attributes on Active Directory instead of provisioning each UNIX server. This highly simplifies the provisioning and identity management of UNIX environments.

Note: This functionality has been merged from CA Identity Manager r12 and is only available in the Provisioning Manager.

Endpoint Type Attribute Mapping Files have Moved

In CA Identity Manager r12, the attribute mapping file for extending Identity Manager to JIAM attributes was located in IdentityMinder.ear\custom\provisioning\im2jiammapping.

In CA Identity Manager r12.5, these attribute mapping files have been moved to their respective endpoint type jars. The JAR files are located in IdentityMinder.ear\user_console.war\WEB-INF\lib.

Default CleverPath Report Templates Are Removed

Default CleverPath Report Template support is being removed in CA Identity Manager r12.5. CA Identity Manager now supports Business Objects Report Server.

CA Identity Manager r12.5 includes a set of report templates to use with the Business Objects Report Server. For more information, see the chapter on Reporting in the *Administration Guide*.

Note: You can create custom report templates using Crystal Reports Developer, which you can purchase from Business Objects.

Deprecated Provisioning SDKs and Utilities

The following Provisioning Server SDKs and interfaces are deprecated in CA Identity Manager r12.5 SP1; however, they continue to function as documented.

To use the C++ Connector SDK and the JIAM SDK, download and install the CA Identity Manager Legacy Components package. It includes the *Programming Guide for Provisioning*, which describes these SDKs.

- **C++ Connector SDK**

  This SDK allows you to write custom static C++ Connectors. Existing C++ Connectors will continue to work with CA Identity Manager r12.5 SP6.

  Note: New connectors should be developed using the Java Connector SDK, which is described in the *Programming Guide for Java Connector Server*.

- **Java Identity and Access Management (JIAM) SDK**

  The JIAM SDK provided the following functionality in previous versions of CA Identity Manager:

  - Java interface to the Provisioning Server
  - An abstraction of Provisioning Server functionality to develop custom client applications
  - A single interface to supply multiple clients with access to Identity and Access Management functionality

  This API is being deprecated because it only provides access to a subset of CA Identity Manager functionality.

  This functionality is replaced by the following CA Identity Manager 12.5 functionality:

  - Admin tasks in the User Console

    You can use admin tasks to manipulate most of the objects that Identity Manager manages.

  - Task Execution Web Services (TEWS)

    The CA Identity Manager Task Execution Web Service (TEWS) is a web service interface that allows third-party client applications to submit remote tasks to CA Identity Manager for execution. This interface implements the open standards of WSDL and SOAP to provide remote access to CA Identity Manager.

  - Managed Object interfaces

    CA Identity Manager provides interfaces for managed objects, which are accessible through CA Identity Manager APIs.

  For more information about admin tasks, see the *Administration Guide*. For more information about TEWS and managed object interfaces, see the *Programming Guide for Java*.

- **etautil**

  You use the etautil batch utility to perform the same tasks as you do with the Provisioning Manager, but from a command line interface. It is described in the *Provisioning Reference Guide*.

  This functionality is replaced by the Task Execution Web Services (TEWS), which is described in the *Programming Guide for Java.*

- **Universal Provisioning Connector (UPC)**

  The UPC provides a mechanism for Identity Manager to invoke user-specified external programs when user provisioning requests are received. It uses program exits to send alerts regarding non-managed systems (non-managed mode) so that administrators can manually carry out the request and update the account request status. It also uses exits in a synchronous mode (managed mode) to provide a direct management interface to remote endpoint types.

iRecorder No Longer Supported

The iRecorder is no longer supported in CA Identity Manager r12.5. The iRecorder functionality has been replaced with CA Enterprise Log Manager.

Web Services Are Disabled For All Tasks in New Environments

Starting in CA Identity Manager 12.5, new tasks created by using the Choose Default Roles option during Environment creation, or created by importing optional role definition plug-ins have web services set to false by default. In previous CA Identity Manager releases, all tasks were enabled for web services by default.

After upgrading to CA Identity Manager 12.5, tasks in existing Environments, which were enabled for web services, continue to be enabled as they were in previous releases. If existing environments apply any of the upgrade role definition plug-ins, these new 12.5 tasks will have the web service flag set to false by default.

Chapter 3: Installation Considerations

This section contains the following topics:

Supported Platforms and Versions

At each release of CA Identity Manager, specific versions of application servers, directories, databases, and endpoints are supported.

Note: For a complete list of supported platforms and versions, see the CA Identity Manager support matrix on CA Support.

Installation on AIX 6.1

To use the true 64-bit capability of AIX 6.1, install the following:

- 64-bit application server, Websphere 6.1.0.25 (6.1 fix pack 25), or later
- 64-bit JVM/JRE
- 64-bit CA Identity Manager Siteminder Webagent API libraries

  Note: Only the 32-bit libraries are installed by default. The 64-bit libraries are not installed by default.

See the *Installation Guide* or *Upgrade Guide* for details.

AD LDS as a User Store

If you use AD LDS on Windows 2008 as the Identity Manager user store and you integrate CA Identity Manager with SiteMinder, SiteMinder r6.0 SP6/r6.x QMR6 is required.

Solaris Patches Required

Before installing provisioning software on Solaris 9 or 10, download and install the required patches.

To download the Sun Studio 10 patches for the Provisioning 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 Provisioning components

1. Go to the following URL:

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

Solaris minimum kernel parameters

When installing the Provisioning Server on Solaris, check /etc/system and verify the following minimum IPC kernel parameter values:

- set msgsys:msginfo_msgmni=32
- set semsys:seminfo_semmni=256
- set semsys:seminfo_semmns=512
- set semsys:seminfo_semmnu=256
- set semsys:seminfo_semume=128
- set semsys:seminfo_smmsl=128
- set shmsys:shminfo_shmmni=128
- set shmsys:shminfo_shmmin=4

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

During CA 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.

Workaround

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

Installing UNIX Remote Agent on 64-bit Red Hat Itanium

Installing UNIX remote agent on Red Hat/Itanium64 requires Red Hat IA-32 Execution Layer and various compatibility libraries. The CA-CCS RPM packages shipped with the Remote Agent are built with an older version of RPM. There are known issues resolving the compatibility library folder /emul/ia32-linux.

The IA-32 Execution Layer and required libraries are on the Supplementary CD that came with the OS. Verify that the libraries match the installed version of Redhat.

The following solution lets you work around an issue with RPM v4.2.3 or later. RPM v4.2.3 has a backward-compatibility problem with older RPM packages. The issue causes it to resolve the compatibility library folder /emul/ia32-linux as /emul/ia32-Linux incorrectly. That is, Linux is incorrectly capitalized.

The issue is a known RPM issue from v4.2.3.

The UNIX Remote Agent is a 32-bit package. If you use this component on 64-bit Red Hat/Itanium, then install the IA-32 Execution Layer and compatibility libraries. Install these components before installing the UNIX Remote Agent.

Note: For more information, see the Red Hat Knowledge Base at:

http://kbase.redhat.com/faq/docs/DOC-1626

To install UNIX Remote Agent on 64-bit Red Hat Itanium

1. Install the IA-32 Execution Layer.
2. Install the following compatibility libraries from the 32-bit Compatibility Layer Disc that matches your Red Hat installation:
   - -glibc
   - -bash
   - -libtermcap
   - If you are using RPM v4.2.3 or later, then do one of the following depending on your environment.
   - Create a symlink. For example, ln -s /emul/ia32-linux /emul/ia32-Linux
   - Add the following in /etc/rpm/macros:

     ```
     %_autorelocate_path      /emul/ia32-linux
     ```

     Note: For more information about this issue, see https://bugzilla.redhat.com/show_bug.cgi?id=137452

Provisioning Directory Installation on Linux

If you install the Provisioning Directory on a Linux system, the system automatically uses IPv6 addresses even if you intend to use IPv4 on this system. All DSAs appear to be running, but when you attempt to connect to the DSAs via Jxplorer or install the Provisioning Server, a connection refused error may appear.

To disable IPv6 on Linux

1. Before Provisioning Directory installation, follow the steps in the Red Hat Knowledge base article to Disable IPv6 on LINUX.
2. Make sure that /etc/hosts has no entry for this address:

   127.0.0.1 *hostname*

Identity Manager EAR does not Auto-Deploy with WebLogic

If you are using WebLogic 9 or 10 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.

Firewall Blocks Communication to Identity Manager Components in Windows 2008 SP2 Deployments

During installation in Windows 2008 SP2 deployments, communication to Identity Manager components, such as the Provisioning Server, Java Connector Server, and the C++ Connector Server, is blocked by the firewall.

Workaround

Add port exceptions or disable the Windows firewall to access distributed Identity Manager components in Windows 2008 SP2 deployments.

CA Identity Manager on Linux 64-bit with SiteMinder Connectivity Errors

The installer reports errors with CA Identity Manager on Linux 64 bit when "Connect to SiteMinder" is selected. The required agent configuration is not correct in SiteMinder

Important! Do the workaround steps before deploying any directory/environment.

Workaround

1. Remember the Agent name and password you provided during the installation. Alternately you can read the value for "AgentName" property from the following:

   `\IdentityMinder.ear\policyserver.rar\META-INF\ra.xml`

2. Open the SiteMinder WAM User Interface and create an agent with the Agent name. Verify that you select the "4.x agent" check box.

3. Start the application server and verify that you do not see policy server connectivity issues.

   You should see a line like the following without any exceptions:

   ```
   13:40:43,156 WARN  [default] * Startup Step 2 : Attempting to start
   PolicyServerService
   ```

IPv6 Support

CA Identity Manager supports IPv6 on the following operating systems:

- Solaris 9 or higher
- Windows XP SP2 or higher
- Windows 2003 SP2 or higher
- Windows 2008 or higher

Note: The Java Connector Server does not support IPv6 on Microsoft Windows platforms. No JDK is available to work with IPv6 as of release time for CA Identity Manager r12.5 SP6. If a JDK is released that works with IPv6, the CA Identity Manager support matrix will be updated on CA Support.

IPv6 JDK Requirements

The following JDKs are required to support IPv6:

Application Server	JDK Requirement
JBoss (standalone)	JDK 1.5
JBoss cluster using an IPv4/IPv6 stack	JDK 1.5
JBoss cluster	JDK 1.5 for Solaris *only*. Note: For Windows, no JDK is available to work with IPv6. If a JDK is released that works with IPv6, the CA Identity Manager support matrix will be updated on CA Support.
WebLogic	JDK 1.5
WebSphere	JDK 1.5 SR9 minimum

IPv6 Configuration Notes

Note the following before configuring an Identity Manager Environment that supports IPv6:

- For CA Identity Manager to support IPv6 addresses, all components in the CA Identity Manager implementation, including the operating system, JDK, directory servers, and databases must also support IPv6 addresses.
- If CA 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 CA Identity Manager using a JDBC connection, specify the hostname not the IP address.
- The 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 must be in IPv4 format.
- CA Identity Manager does not support IPv6 link local addresses.
- In an IPv4/6 environment, if you want to configure CA Directory DSAs to listen on multiple addresses, add the additional addresses to your DSA knowledge files. For more information, see the CA Directory documentation.

Provisioning Directory on Windows 2008 with Pure IPv6 Not Supported

Due to a Sun Java Systems limitation, installing the Provisioning Directory on a Windows 2008 server with the IPv6 networking service uninstalled is not supported.

To work around this issue, install the IPv6 service on the system and leave it disabled.

Chapter 4: Upgrade Considerations

This section contains the following topics:

Supported Upgrade Paths

The following is a list of products and versions that have a supported path for an upgrade to CA Identity Manager r12.5 SP6:

- CA Identity Manager r8.1 SP2
- CA Identity Manager r12
- CA Identity Manager r12 with Option Pack 1
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx

Note: Upgrades from ACE to r12.5 SP1 are *not* supported. Also, cross-platform upgrades (between UNIX and Windows) are not supported.

If you are upgrading CA Identity Manager in a clustered environment, use the Upgrade Guide. It is available in the CA Identity Manager r12.5 SP6 Bookshelf, which you can view or download from the CA Support Site.

CA Directory Upgrade License Patch

To upgrade CA Directory on a Windows system, you must apply a license patch for CA Directory before beginning the upgrade procedure.

If you do not apply the patch, the upgrade 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. CA Licensing.

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.

Note: You also need this patch if you plan to manually uninstall eTrust Directory r8.

CA Directory Upgrade Message Issue

When upgrading CA Directory, the installer may ask you to close cmd.exe, however cmd.exe is used by the upgrade. If you encounter this message, click Ignore and continue on with the upgrade.

Provisioning Server Communication may not Succeed

After the upgrade, communication with the Provisioning Server may not succeed. The Provisioning Server shared secret may need to be updated.

Workaround

1. Generate a new encrypted shared secret using the Password Tool.
2. Update the Provisioning Server shared secret in the systemWideProperties.properties file

   For example, for a WebLogic Admin Server in this location, the file is in this location:
   `<domain>\applications\ear\custom\identitymanager\systemWideProperties.properties`

   On each weblogic node, make this change in the systemWideProperties.properties in the EAR, which is in this location:
   `bea\weblogic92\common\nodemanager\servers\server_name\stage\IdentityMinder`

Hide from Exchange Address List Problem on Exchange 2007 Accounts

Symptom:

The Provisioning Server cannot set the Hide from Exchange Address List property on Exchange 2007 accounts.

Solution:

Upgrade the Exchange 2007 Remote Agent to the CR10 release when applying CA Identity Manager r12.5 SP6 to the core CA Identity Manager R12 components. For example, Server, Manager and Repository.

Upgrade from r12 (CR6 or later) Fails on Some Clusters

Symptom:

If you upgrade a cluster from CA Identity Manager r12 CR6 or later, the upgrade may fail due to some cluster properties in the installation file being cleared.

Solution:

Verify that the following properties are populated in the im-installer.properties file before the upgrade:

- WebSphere: Check if the cluster name is populated in DEFAULT_WAS_CLUSTER. If it is not, add it back manually.
- WebLogic: Check if the cluster name is populated in DEFAULT_BEA_CLUSTER. If it is not, add it back manually.

Note: This issue does not affect a JBoss cluster.

By default, the installation file is found in the following locations:

- Windows: C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- UNIX: /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Solaris: Websphere Cluster Issue after Upgrade from r12 CR12

Symptom:

When you upgrade from CA Identity Manager r12 CR 12 on a WebSphere 6.1.0.17 cluster running on Solaris, the installer does not copy the ims6AddWfEventsJMSQueue.jacl to the Deployment Manager profile.

Solution:

1. After you complete the upgrade, copy the ims6AddWfEventsJMSQueue.jacl file from the CA Identity Manager r12.5 SP6 Websphere-tools directory to the following location on the system where the Depolyment Manager is running:

   WAS_HOME/Application Server/profiles/*dm_profile*/bin

   The CA Identity Manager r12.5 SP6 Websphere-tools file is located in *WAS_HOME*/AppServer.

2. Run the following command against all cluster members except the primary cluster member:

   wsadmin -f ims6AddWfEventsJMSQueue.jacl *node server cluster*

Solaris: Upgrade of UNIX Remote Agent Fails

When upgrading a UNIX remote agent from CA Identity Manager r8.1.2 SP2 on the Solaris platform, the upgrade process fails.

Workaround

Uninstall the CA Identity Manager r8.1.2 SP2 remote agent on Solaris, then install the new remote agent.

Environment Migration Error

If you are upgrading from CA Identity Manager r8.1 SP2, or r12 CR1, CR2, or CR3, you may see the following error when importing your environments:

Attribute "accumulateroleeventsenabled" is not allowed to appear in element "Provisioning".

Workaround

Open the envsettings.xml file in the exported Env.zip, and update the accumulateroleeventsenabled to acumulateroleeventsenabled (remove the second 'c' in accumulate).

Environment Migration Fails if Connection to User Store Fails

Symptom:

During an environment migration when you are upgrading from CA Identity Manager r8.1 SP2, if the Identity Manager user store cannot be contacted, the environment is left in an incomplete state. For example, the base URL may be missing or the System Manager may not be set.

Solution:

1. Delete the affected environment.
2. Rename the file *Environment Name*EnvironmentMigrated.properties to *Environment Name*EnvironmentAutoMigrate.properties

   This file is located in *App Server Deploy Location*/IdentityMinder.ear/user_console.war/META-INF/
3. Restart the Application Server.

Credential Provider Upgrade Error

After you upgrade the CA Identity Manager r12 Credential Provider on a 32 bit Windows platform, the Disable Microsoft Password Credential Provider checkbox in the CAIMCredProvConfig application is unchecked.

Workaround

Open the CAIMCredProvConfig application and select the check box.

Vista Credential Provider Internal Error

Symptom:

When I upgrade Identity Manager Vista Credential Provider on 64-bit Windows platforms, I receive the error message *Internal Error 2324.2.*

Solution:

No action is required as the upgrade process has completed successfully.

No Search Screen with Explore and Correlate Task

If you upgraded from CA Identity Manager r12 *or* if you upgraded from CA Identity Manager r12.5 *and* migrated the Explore and Correlate task to the new recurrence model (see page 65), the Browse button in the Explore and Correlate task does not work correctly.

Workaround

Configure a search screen for the task so that the new Browse button brings up a search screen when clicked.

Reverse Synchronization Policies that Affect Suspension Attributes

If you create a reverse synchronization policy that detects a new account and suspends it, that suspension could be rejected by a related reverse synchronization policy. Consider the following example:

1. An administrator creates two policies:
   - A policy that detects new Windows account and suspends those accounts
   - A policy that detects changes to the N16SecurityFlag attribute in Windows accounts and rejects that change

     The N16SecurityFlag attribute concerns account suspension.
2. An endpoint user creates a Windows account using native tools on the endpoint.
3. The new account policy suspends the new account.
4. When explore and correlate runs again, it detects the account as modified.
5. The modify account policy detects the change to the N16SecurityFlag attribute and rejects that change. The account is no longer suspended.

This situation affects any endpoint type that handles account suspension. In this example, the modify account policy should detect changes in etSuspend not n16SecurityFlag. Therefore, since the change originates from etSuspend, the N16SecurityFlag is only changed on the endpoint and is not picked up as a changed attribute.

Post-Upgrade Steps: WorkPoint

If you upgraded from CA Identity Manager r8.1 SP2 or r12, the following WorkPoint files were renamed to *filename*.bak and a new version of the file was installed. Reapply any modifications you made to these files after the upgrade:

- From the Workpoint/bin directory: Archive.bat/.sh, Designer.bat/.sh, init.bat/.sh
- From the Workpoint/conf directory: workpoint-client.properties

Post-Upgrade Steps: DYN Endpoint Attributes

If you have an existing DYN namespace created in r8.1SP2 or r12, you must perform the following additional steps to enable account management from the Identity Manager User Console.

Remap any DYN endpoint attributes to the account screen using Connector Xpress, as follows:

1. After the upgrade, open the old DYN JDBC project in Connector Xpress.
2. Map the attributes to the account screen.
3. Redeploy the metadata.
4. Run the Role Definitions Generator.
5. Copy the respective file to the application server.
6. Restart CA Identity Manager.

Note: For more information about mapping endpoint attributes using Connector Xpress, see the *Connector Xpress Guide*.

Post-Upgrade Steps: z/OS Connectors

At CA Identity Manager r12, the z/OS connectors (CA ACF2, CA Top Secret and RACF) were re-architected for performance reasons to 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.

If you upgraded CA Identity Manager from before r12, do the following for each endpoint defined to your system:

1. Select CA ACF2, CA Top Secret, or RACF Endpoint from Object Type.
2. Click the search button. Right click 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.

Migrate Pending Tasks

If you migrated the pending tasks by using the upgrade program, no additional step is necessary. However, if you omitted that option, you should migrate your tasks.

1. Run the migration tool once use the -ALL option.

   This option excludes the pending tasks.

2. Run the migration tool again use the -pending option.

For details on using the migration tool, see the *Upgrade Guide*.

Unable to Create Exchange Mailboxes

Symptom:

I upgraded eTrust Admin 8.1 SP2 to CA Identity Manager r12.5 SP6 using the integrated installer. After the upgrade, the Exchange Gateway Server field on the Exchange General tab of the Active Directory endpoint does not display an Exchange Server and I cannot create exchange mailboxes. I changed the value of the DisableExchange2007 parameter, but this did not resolve the problem.

Solution:

The CA Identity Manager r12 integrated installer does not enable the Exchange 200x license setting by default. As a result, the ADS connector cannot explore ADS endpoint Exchange-specific attributes and mailboxes cannot be created.

To confirm that that the Exchange 200x license setting is missing, do the following:

1. Navigate to the folder *IMPS_home*\logs\ads\<ads endpoint>.log and search for the following:

   ```
   Exchange2000: License: F; EX2mdb: T; EX2servers: T
   ```

2. If the Licence value is ‘F’, the Exchange 200x license setting is missing and you cannot create Exchange mailboxes. The License value should be 'T'.

3. To resolve the issue, do either of the following:

   a. Re-install the CA Identity Manager Manager Provisioning Server using the individual IMPS installer. During the installation, select both the ADS connector and the Exchange 200x connector.

   b. Start regedit and navigate to the following registry key:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity
      Manager\Provisioning Server\Components\Server\
      ```

      Under the key, create a string registry with the value eTrust_E2K , then set the value to *yes*.

      Save the value, then restart the im_ccs and im_ps services.

      The Exchange 200x license setting is created in the registry.

4. Create a mailbox.

5. Navigate to the folder *IMPS_home*\logs\ads\<ads endpoint>.log and search for the following:

   ```
   Exchange2000: License: T; EX2mdb: T; EX2servers: T
   ```

   If the License value is a 'T', the license setting is now correct.

Note: If an Exchange Server was installed after the ADS endpoint was created, follow the instructions in the Tech Doc TEC446637, How to register a new or additional *Exchange Server in an existing Admin installation* to update the ADS endpoint so that it recognizes the Exchange Server.

Update Oracle Database with Garbage Collection Procedure

To add the Auditing Garbage Collection stored procedure to pre-SP5 Oracle audit databases, execute the ims_oracle_audit_upgradeto_r125_SP5.sql script against your Oracle Auditing database.

Non-Fatal Error after Upgrading Provisioning Manager from r12

Symptom:

After upgrading Provisioning Manager from CA Identity Manager r12 CRx, the installer displays the following message:

```
The installation wizard has finished upgrading CA Identity Manager but
non fatal errors or warnings occurred during the upgrade. For details
please see the installation log under C:\Program Files\CA\CA Identity
Manager.
Warning/Errors were reported related to the following components
```

The CA Identity Manager installation log contains the following entry:

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "The process cannot
access the file because it is being used by another process."
```

Solution:

The error occurs because the installer cannot create a directory that exists. However, the installation has completed successfully, and the Provisioning Manager is fully functional.

Chapter 5: Known Issues

This chapter lists the issues that are known to exist in CA Identity Manager r12.5 SP6. All Fixed Issues (see page 129) are in a separate chapter.

This section contains the following topics:

General

The following are general known issues in CA Identity Manager r12.5 SP6.

CA Identity Manager Does not Validate Home Page Field

The Global User supports a Home Page attribute (eTHomePage). If you configure CA Identity Manager with provisioning, and you configure CA Identity Manager to manage the Home Page attribute, administrators can specify a URL as a default home page when they use tasks such as Create User or Modify User.

If an administrator enters characters that are not supported for URLs in the Home Page field, CA Identity Manager cannot validate the field and displays an error message. In this case, synchronizion of the Home Page attribute to any target endpoint, if configured, fails.

Cannot Delete CA Identity Manager Environments using the CA Identity Manager Management Console

Symptom:

I am using CA Identity Manager r12.5 integrated with CA Siteminder r12.0 SP3 CR1. I tried to delete a CA Identity Manager environment using the CA Identity Manager Management Console, and the Siteminder Policy Server failed. As a result, the deletion of the CA Identity Manager environment failed and the CA Identity Manager environment was not deleted.

Solution:

To resolve, remove the CA Identity Manager environment manually and restart the Siteminder Policy Store.

In the Siteminder Policy Store, all the objects are stored as property collection, property section, property. For example, the property collection is the environment/directory. The property section contains all the object information such as screens, screen elements and such. The property is a collection of the attributes of those objects. Do the following to verify the data that you want to remove:

1. To determine the environment you need to remove, do the following:
   a. Find the propertycollection id from the imsenvironment6 table in the policy store.
   b. Note the values of the field names additionalpropertiesoid and domainoid for the environment you want to remove. For example:

      ```
      select domainoid, additionalpropertiesoid from imsenvironment6 where envname= <Environment name>
      ```

2. Using additionalpropertiesoid, go through the tables ‘smpropertycollection5. This contains the link to the property section table. For example:

   ```
   SELECT     propertycollectionoid, propertycollectionname, propertycollectiondesc

   FROM       smpropertycollection5

   WHERE     (propertycollectionoid = ‘<additionalpropertiesoid from step 2>’)
   ```

3. Get the records from the smpropertysection5 table. For example:

   ```
   SELECT     propertysectionoid, propertycollectionoid, propertysectionname, propertysectiondesc

   FROM         smpropertysection5

   WHERE     (propertycollectionoid = ‘<propertycollectionoid from step 3>’)
   ```

4. Use those ids to obtain the records from the smproperty5 table. For example:

   ```
   SELECT     propertyoid, propertysectionoid, propertyname, propertyvalue, propertyflags
   ```

```
FROM         smproperty5

WHERE  propertysectionoid in ( SELECT     propertysectionoid

FROM         smpropertysection5

WHERE     (propertycollectionoid in (SELECT     propertycollectionoid

FROM         smpropertycollection5

WHERE     (propertycollectionoid in (select additionalpropertiesoid from
imsenvironment6 where envname='<Environment name>'))

)))
```

5. To delete, reverse the process. That is, delete the entries in smproperty5, then smpropertysection5 and smpropertycollection5. For example:

```
delete from smproperty5 where propertysectionoid in (
SELECT     propertysectionoid

FROM         smpropertysection5

WHERE     (propertycollectionoid in (SELECT     propertycollectionoid

FROM         smpropertycollection5

WHERE     (propertycollectionoid in (select additionalpropertiesoid from
imsenvironment6 where envname = '<Environment name>'))

))

 )

delete from smpropertysection5 where propertycollectionoid in
(SELECT     propertycollectionoid

FROM         smpropertycollection5

WHERE     (propertycollectionoid in (select additionalpropertiesoid from
imsenvironment6 where envname= '<Environment name>'))

)

delete from smpropertycollection5 where propertycollectionoid in (select
additionalpropertiesoid from imsenvironment6 where envname= '<Environment
name>')
```

6. Remove the environment entry from the policy store table imsenvironment6:

```
delete from imsenvironment6 where envname = '<Environment name>'
```

7. Delete the domain information from smdomain4. Refer step 2 for the domainoid.
8. Restart CA Siteminder and CA Identity Manager.

Oracle 11gR2 RAC User Store: Search is Case-Sensitive

Symptom:

When Oracle 11gR2 RAC is the user store, searching for users, groups, or organizations sometimes provides no results although the objects exist.

Solution:

For this user store, the search is case sensitive. For example, searching for *smith* yields no results if the user was created as *Smith* in the database. Use the same case as was used when the object was created in the database.

"Out of Memory" Errors May Occur When Searching Large User Stores

When performing wildcard (*) searches on large user stores, the task can fail with a java.lang.OutOfMemoryError: Java heap space error. This issue occurs when many objects, such as users, are loaded into memory.

Workaround

Increase the heap settings in the application server startup script. Consider increasing the heap size to 1000 MB allocated with 1400 MB maximum.

Identity Manager Starts in Failed State When Databases Not Started

If the runtime databases required for CA Identity Manager are not started when you start the Identity Manager Server, CA Identity Manager attempts to initialize anyway and is left in a failed state.

Benign JSF RI Error on JBoss

When implementing JSF RI on JBoss, the following error appears in the application server log:

```
ERROR [org.apache.myfaces.shared_impl.config.MyfacesConfig] Both MyFaces and the RI are on your classpath. Please make sure to use only one of the two JSF-implementations.
```

This is a benign error and does not need to be fixed.

WorkPoint Designer Does not Open on JBoss 4.2.3

Symptom:

I installed CA Identity Manager on JBoss 4.2.3. When I try to open WorkPoint Designer, it fails to open.

Solution:

Before you open the WorkPoint Designer, complete the following steps:

1. In a text editor, edit one of the following files:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     *admin_tools/*Workpoint/bin/init.sh
2. Uncomment the following line in the section for JBoss 4.2.3 application servers:
   - **Windows:**

     `SET EJB_CLASSPATH=..\lib\jbossall-client.jar;..\lib`
   - **UNIX:**

     `EJB_CLASSPATH=../lib/jbossall-client.jar;../lib`

   Note: Be sure that all sections for other application servers are commented.
3. Copy the jbossall-client.jar from *jboss_home*\client\ to:

   admin_tools\Workpoint\lib
4. Copy the log4j.jar file from *jboss_home*/server/default/lib to *workpoint-installation-folder*/lib.

Bulk Loader Workflow Limitation

CA Identity Manager currently does not support event-level workflow processes for the Bulk Loader by default.

Workaround

You can enable task-level workflow for the Bulk Loader and use a generic Approve Task to achieve the same functionality.

Workflow Startup Issue on WebSphere on Linux Systems

If LANG is set to xxxUTF-8 on Linux systems, you may see a sun.io.MalformedInputException error during workflow startup. This happens on WebSphere on Linux.

For more information about the error, see the following and search for sun.io.MalformedInputException:

http://www.ibm.com/developerworks/java/jdk/linux/142/runtimeguide.lnx.en.html

Workaround:

Set the LANG variable to non-UTF8 (for example, en_US instead of en_US.UTF-8) before starting the application server, or set the variable in the users profile.

For example:

```
[root@linux bin]# echo $LANG
en_US.UTF-8
[root@linux bin]# LANG=en_US
[root@linux bin]# export LANG
[root@linux bin]# echo $LANG
en_US
[root@linux bin]# ./startServer.sh server1
```

Attributes Highlighted as Changed on Workflow Approval Screens

On an approval screen, additional attributes may appear highlighted as changed even if an administrator did not change them in the original task. This is because the screen can contain scripts that can change values of various attributes contained on the screen as a part of screen initialization or screen validation for a change of some other attribute.

Provisioning Role Name Changes are Not Dynamically Updated in CA RCM

If you rename a provisioning role in CA Identity Manager, that name change is not communicated to CA RCM through dynamic notification. This may impact the suggested roles functionality and compliance and policy validations.

Workaround

Use the Identity Manager Connector to import Identity Manager data into CA RCM.

Benign Error in the CA RCM Logs

When the CA RCM server receives a request from CA Identity Manager to create or modify a user or role, the following error is displayed in the CA RCM server log:

```
ERROR [Call] No returnType was specified to the Call object! You must call
setReturnType() if you have called addParameter().
```

This error is benign and can be safely ignored. The changes are successfully executed in CA RCM.

"Not Found" Error When Creating a New Environment in Certain Deployments

If CA Identity Manager integrates with CA SiteMinder 6.0.5 CR 31 or later, an "Error 404 - Not found" message maybe displayed when users try to browse to a new Environment URL.

This issue is due to a caching issue in the Policy Server.

Workaround

To resolve this issue, complete the following steps:

For Windows:

1. Add a keyword to the SiteMinder registry as follows:
   a. Navigate to \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\ObjectStore
   b. Add the "ServerCmdMsec" key with the following settings:
      - Type: DWORD
      - Value: 1
   c. Restart Policy Server
2. Restart the application server.
3. Close all browser instances. Then, use a new browser instance to access the Environment URL.

For Solaris:

1. Add a line to the <CA_HOME folder>/netegrity/siteminder/registry/sm.registry file ServerCmdMsec= 0x1 REG_DWORD
2. Restart the Policy Server.

3. Restart the application server.
4. Close all browser instances. Then, use a new browser instance to access the Environment URL.

Error Advising that Another Tab in the Environment Exists When Importing the Role Definition File into CA Identity Manager

Symptom:

I generated CA Identity Manager User Console account screens with Connector Xpress and when I imported the role definition file into CA Identity Manager, I got an error message advising me that another tab with the same name exists in the Identity Manager environment

Solution:

When association-type attributes are placed on the same tabs, the role definition generator tries to create two tabs with the same name. For example, when you place the association attributes member and memberof on the same tab.

We recommend that you place association-type attributes on separate tabs in Connector Xpress, before you import the role definition file into your CA Identity Manager environment.

Modifying Single Valued Compound Attributes in Identity Manager

If you modify a single valued compound attribute in CA Identity Manager for a dynamic endpoint, specify only a single value. If you specify multiple values, the existing value is cleared and the attribute is not given a value. The problem does not occur in the Provisioning Manager.

Reporting

The following issues are related to reporting in CA Identity Manager r12.5 SP6.

Error When Capturing Snapshot Data with ExportAll.xml

When using the ExportAll.xml snapshot definition to capture snapshot data, the process fails with the error "java.lang.OutOfMemoryError: Java heap space." This issue occurs when a large number of objects, such as users, are loaded into memory.

Workaround

Increase the heap settings in the application server startup script. Consider increasing the heap size to 1000 MB allocated, 1400 MB maximum.

Also, in the snapshot definition XML files, consider splitting the filter condition for the objects into multiple conditions. For example, instead of using the wildcard filter (*) to load all users, specify a multiple filters, such as "user id starts with 'a'", "user id starts with 'b'", and so on.

Capture Snapshot Data Task Shown as In Progress When Complete

When checking View Submitted Tasks, the Capture Snapshot Data task may be marked as "In progress", despite the task having completed. However, if you drill down to the detail section of the Capture Snapshot Data task, it correctly shows that the task is completed.

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).

Viewing a Report Redirects To the Infoview Login Page

When viewing a report in CA Identity Manager, you may be re-directed to the Business Objects Infoview login page.

Workaround

1. Be sure you are using the fully-qualified domain name of the CA Report Server (Business Objects).
2. Right-click on the Infoview login web page and select View Source.

3. Find the URL for the report.
4. Copy and paste the URL into a new browser window.
5. If you do not see the report, use an http trace tool to provide more information.
6. If you do see the report, try the following to fix the browser settings:
   - Accept 3rd party cookies.
   - Allow session cookies.
   - Remove High security settings.

Enable Third Part Cookies for View My Reports Task

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

Generating User Accounts Fails if More than 20,000 Records Exist

If over 20,000 records exist, generating a user accounts report fails.

Workaround

1. Open the Business Objects Central Management console.
2. Click Servers and select *servername*.pageserver.
3. Select Unlimited records for the entry Database Records To Read When Previewing Or Refreshing a Report.
4. Using Crystal Reports designer, open the user accounts report.
5. Using Database, Set Datasource Location, set the database location to your snapshot database.
6. Save this change.
7. Using Database, Datasource Expert, right click Command on the right side window.

   It shows the SQL syntax on the left-hand side and the Parameter List.
8. Enter the parameter name as you find it in the Parameters Fields in the report template.

9. Change the query in the left-hand side and add that parameter in the query.

   For example, if you have reportid parameter, the query will be:

   ```
   Select *  from endPointAttributes, endpointview, imreport6
   where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
   endPointAttributes.imr_reportid = endpointview.imr_reportid
    endpointview.imr_reportid = imreport6.imr_reportid and imreport6.imr_reportid
   = {?reportid}
   ```

10. Save the report.

For WebSphere, Non-Snapshot Reports Require the Date Picker

Non-Snapshot Reports use the current system date and time values for Start Date Time and End Date Time. However, these values do not work for WebSphere. An error appears when you click Schedule Reports.

Workaround

Select the Start and End Date Times using the Date Picker control.

General Provisioning

The following issues are general provisioning issues in CA Identity Manager r12.5 SP6.

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.

Workaround

Turn ECS logging off if you are experiencing poor Provisioning Server performance.

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 Provisioning 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.

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.

Workaround

Restart all connector servers that are configured to manage the endpoint.

Creating a Provisioning Role Linked to the Account Template Fails in CA Identity Manager

Symptom:

I deployed a JNDI project created with Connector Xpress prior to CA Identity Manager 12.5 to CA Identity Manager and executed an explore and correlate.

I created an account template and added two association attributes, for example, manager. When I created a provisioning role based on the account template, and assigned the provisioning role to the user, I got an error message advising me that the associated accounts creation or update failed.

Solution:

CA Identity Manager r12.5 SP6 does not support JNDI projects created with Connector Xpress prior to CA Identity Manager 12.5 using association-type attributes.

We recommend that you use the Provisioning Manager to create the account template.

Provisioning Server Chooses DNS Over Local Setting

The Provisioning Server installer prefers the DNS result for the Provisioning Directory host even if you configured the operating system to prefer the local host table over DNS.

SiteMinder Login Name Restriction for Global User Name

The following characters or character strings cannot be part of a global user name if that user needs to log into the SiteMinder Policy Server:

&
*
:
()

Workaround

Avoid using these characters in the global user name.

Some WebSphere Nodes May be Missing Objects

On a WebSphere cluster, changes to an environment may not appear on some nodes in the cluster. For example, after modifying a provisioning role, that change may not show up on another node in the WebSphere cluster.

Workaround

Move the Service Integration Bus out of the cluster and onto dedicated servers. See the WebSphere documentation on Connecting Applications on the Service Integration Bus.

Password Change on 64-Bit Linux does not Trigger the UNIX PAM Services

PAM is only supported on 32-bit Linux systems.

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. Use the CA Identity Manager self-service features instead of SAWI or DAWI.

Error Message when Setting Date, Time, or DateTime Attributes as Mulitvalued in Connector Xpress

Symptom:

When I map an inetOrgPerson Directory String attribute, for example otherHomePhone, and set it as multivalued, I receive the following error message when I try to create a new endpoint type:

Failed to create Endpoint Type: com.ca.commons.jndi.beans.JNDIBeanStoreException: Non-date value passed to ETADateHandler.

Solution:

Connector Xpress does not support multivalued Date or Date/time attributes.

Memberof List is empty when Assigning PosixAccounts to PosixGroups for Oracle Internet Directory

Symptom:

I created an Oracle Internet Directory endpoint project using Connector Xpress using the JNDI posix template. I acquired the endpoint, performed an explore and correlate, created the accounts and groups in CA Identity Manager, and assigned the accounts to groups. When I view the account properties and display the Memberof tab, the Memberof list is empty.

Solution:

Connector Xpress does not support PosixGroup membership of PosixAccounts for Oracle Internet Directory.

Java Connector Server

The following issues are related to the Java Connector Server in CA Identity Manager r12.5 SP6.

connector.xml Files Renamed During Upgrade

When upgrading the Java Connector Server from r8.1 SP2 to r12.5 SP6, all connector.xml files under JCS_HOME/conf/override/* will be renamed to connector.xml.orig.

If you use these connector.xml files, rename these files back to their original names after the upgrade.

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

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.

Workaround

Use the stop and start buttons instead of the restart buttons in the Windows Service Control Panel.

Reserved Characters Should not be Used in JNDI Account Names

When creating JNDI accounts, do not use reserved characters, including the backslash (/), in the account names. An error occurs when you try to delete them.

JNDI Account Management Screens – Creating Accounts with Multiple Structural objectclasses Fails

You cannot create accounts with multiple structural object classes.

Endpoint Types

The following issues are related to managing endpoint types in CA Identity Manager r12.5 SP6.

General

The following sections describe the known issues for the various connectors:

Endpoints with Retry Autolock must be Configured with a Generous Retry Limit

For endpoints that have "N" retry autolock" behavior, the account used to connect to the endpoint using Java CS should be configured to have a generous (or unlimited) "N" due to attempts to connect being used up quickly by the Java CS.

When the account is natively locked due to "N" being exceeded, it may be necessary to use native tools to unlock the account before the endpoint can be acquired again. This depends on the exact native "locked" behavior of the endpoint.

Account Templates are not Synchronized with Accounts on a Create or Modify Task in the User Console

Using the User Console, explicit account synchronization is not supported.

Workaround

Use Provisioning Manager to synchronize accounts with account templates.

Modifying Endpoint Directly Causes Failure when Importing Between Endpoint and Provisioning Server.

When the endpoint is modified directly (not using the Provisioning Server), a failure is returned on import because of inconsistent data between the endpoint and Provisioning Server. Two examples include:

- Someone removed tables from the MSSQL endpoint using native tools which resulted in some users getting resources that no longer exist.

  To resolve the failure, reexplore the endpoint using the Provisioning Server.

- Someone deleted some server roles on the endpoint, and those account templates that still had those server roles assigned received extra roles that do not exist on the endpoint any more.

  To resolve this failure, manually remove those "removed" server roles from the account templates.

ACF2, RACF, and CA Top Secret

The following sections describe the known issues for the Mainframe connectors:

CA LDAP Server for z/OS must have Appropriate Maintenance Applied before Using the RACF Connector or Using the Create/Delete Alias Processing in r12.0 and Beyond

If you are using any function of the RACF connector, or if you are using the create/delete alias processing in the ACF2 or TSS Connectors, contact support for the appropriate maintenance. When you contact support, make sure to specify which r12.5 release of CA Identity Manager is being used, as well as which version of CA LDAP Server for z/OS is being used. There are different fixes for CA LDAP Server r12 and CA LDAP Server r14 and we want to make sure the correct modules are given.

ACF2 and TSS Account Templates Created in the User Console Do Not Support User-Defined Fields

Support for ACF2 and TSS User-Defined fields is not available using the User Console. You can continue to manage these fields using the Provisioning Manager.

RACF Backend Code Does Not Allow Non-ASCII Characters Entered into Account Names

To resolve this issue, contact CA Support to request updated mainframe binaries.

Active Directory

The following sections describe the known issues for the Active Directory connector:

Incorrect Results During Sub-Tree Search with Active Directory 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 organization unit 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.

Workaround

Increase the search limit size.

Endpoint Descriptions for ADS2008 Endpoints are Displayed as Numbers

When viewing or modifying an ADS2008 endpoint using the User Console, the Domain Controller, Domain, and Forest field values on the ADS Server tab are displayed as numbers.

Required Fields when Office Communication Server Attribute Is Enabled is Set to True

If Office Communication Server attribute Is Enabled is set to true, the following three fields are required and should be set when using the ADS endpoint:

- Home Server
- SIP
- URI

Creating or Modifying an Account with an Exchange Mailbox Fails

Valid on Windows

Symptom:

When I attempt to create or modify an account with an Exchange mailbox in CA Identity Manager, the create or update call fails, and I get an error that says Failed to Execute CreateActiveDirectoryAccount. The error message concludes:

```
Processing data from remote server failed with the following error message: The user
"NT AUTHORITY\SYSTEM" isn't assigned to any management roles. For more information,
see the about_Remote_Troubleshooting Help topic.
```

Solution:

The service account running the Exchange Remote Agent needs appropriate permissions.

The help topic that the error message refers to is an Exchange help topic, and is not part of CA Identity Manager.

To manage the Exchange 2010 environment, give appropriate permissions to a service account for the Remote Agent, and restart the service.

Note: For more information about configuring Exchange 2010 account permissions, see Configuring the Exchange 20xx Remote Agent Component in the CA Identity Manager *Connectors Guide*.

Message Restrictions for Exchange Mailbox Enabled Accounts Are Ignored

Symptom:

When I specify the following restrictions for Exchange mailbox accounts, they are ignored:

- Accept Messages Only From
- Accept Messages from Everyone Except
- Full Access Permission
- Send As Permission

For example, I added Bob and Fred to the list of users that an Exchange mailbox holder can accept messages from. I searched for a list of users, and both Bob and Fred were in the list displayed by Identity Manager. Bob was added to the list of users that the Exchange mailbox holder can accept messages from, but Fred was not.

Solution:

When you search you for accounts you want to add to the Accept Messages Only From, Accept Messages from Everyone Except, Full Access Permission or Send-As Permissions lists, Identity Manager displays a list of all endpoint users regardless of whether they are Exchange enabled or not. However if you select a user or group that is not Exchange-enabled, Identity Manager ignores the request. In the example, Fred was ignored because they were not an Exchange-enabled user.

In addition, you can only add mail-enabled security groups to the Full Access Permission or Send-As Permissions lists.

CA DLP

The following sections describe the known issues for the CA DLP Connector.

Error Message – The Communications Mode of the Provisioning Server and Client Do Not Match. CMS Is In Standard mode. Client Is In Advanced mode.

Symptom:

When I create a CA DLP endpoint, I receive the following error message:

```
The Communications Mode of the Provisioning Server and Client Do Not Match. CMS Is In Standard mode. Client Is In Advanced mode.
```

Solution:

The Java CS and the CA DLP CMS (Central Management Server) must be in the same FIPS mode before the Java CS can use the CA DLP Connector to manage the CA DLP endpoint.

Note: For more information on configuring the Java CS and the CA DLP CMS (Central Management Server) so that they are the same FIPS 140 mode, see the topic *FIPS 140 Configuration in the Identity Manager Connectors Guide.*

CA DLP User is Placed in Root Group on CA DLP Endpoint

Symptom:

I created a CA DLP account template and used the default values for the group attribute: %UCOMP%/%UCOUNTRY%/%UDEPT%.

I created a user and assigned a provisioning role to user based on the template. When I viewed the CA DLP account of the user in CA Identity Manager, the group attribute was empty. On the CA DLP endpoint, the account was in the root group.

Solution:

When you created the global user, you did not specify a value for the Company, Country, or Department. As a result, the group attribute was set to / and the user was placed in the root group on the CA DLP endpoint.

This behaviour is expected when the Group attribute is set to /.

CA SSO Connector for Advanced Policy Server

The following sections describe the known issues for the CA SSO Connector for Advanced Policy Server:

PLS Account Search Returns Non-Existing Accounts when eTPLSCountry is Specified

When the eTPLSCountry attributed is included in the search request for PLS Accounts, the search response returns an entry even if an account with that name does not exist on the endpoint or provisioning repository.

PLS Connector Cannot Add More than 2000 Accounts to Applications

You cannot add more than 2000 PLS accounts to an application at one time. If you have more than 2000 PLS accounts to add, you must split the accounts into multiple operations.

DB2 and DB2 for z/OS

The following sections describe the known issues for the DB2 and DB2 for z/OS connectors:

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).

Workaround

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.

Authorities Granted Attribute in DB2 Account Template is a Capability Attribute

The Authorities Granted attribute in the DB2 account template in the Provisioning Manager is currently shown as an initial attribute but it is actually a capability attribute.

E2Kx

The following sections describe the known issues for the E2Kx connector:

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 multiple privileges exist in the mailbox rights list for the same object and normally happens when the managed exchange objects inherit rights from the parent object.

E2K7 Mailbox Out of Sync After Initial Creation

After creating an account template with Use Strong Sync checked, and synchronizing a global user with the account template, right-click global user and select Check Account Synchronization. The Mailbox Rights is out of sync.

Workaround

Select Exchange Advanced,Mailbox Rights, Add (usingSHIFT+ADD method), 'NT AUTHORITY\Authenticated Users', 'Read permissions' only.

Email Addresses are not Set on Email Enabled Groups

When creating a group and checking 'Create an exchange email address,' no email address is set for the group.

Workaround

Go to the Email Addresses Tab and apply the new email address there after the group is created.

An Error Message is Displayed when Trying to Modify an Account with an E27K Mailbox

An error message is displayed when you try to modify an account with an E27K mailbox. This error is benign and can be ignored.

Error Message is Insufficient when Trying to Create E2Kx Mailbox

An insufficient error message is displayed for characters within the INT field. This error, [-]?[\d]*, indicates that the required field must be a number.

Message Restrictions do not Allow 'Only From' and 'From Everyone Except' to be Selected Simultaneously in the Provisioning Manager

Exchange Server 2007 lets administrators select both 'Accept messages from only senders in the following list' and 'reject messages from senders in the following list'. The Provisioning Manager only allows one to be selected. This was the behaviour in Exchange 2003. If both are natively selected in Exchange 2007, this functionality is broken in the Provisioning Manager.

Google Apps

The following sections describe the known issues for the Google Apps Connector.

Google Apps—CAPTCHA Challenge

Symptom:

During authentication, I receive the following error message with a CAPTCHA challenge:

```
Authentication failed, CAPTCHA requires answering. Please use the following website to unlock JCS computer: https://www.google.com/a/yourdomain/UnlockCaptcha
```

Solution:

Do the following:

1. Log on to the computer where the Java CS is running.
2. Open a web browser.
3. Follow the link provided in the error message, and replace yourdomain.com with your Google Apps domain. For example:

   `https://www.google.com/a/`*`yourdomain.com`*`/UnlockCaptcha`
4. Answer the CAPTCHA question.

   The Google Apps server issues a new authentication token and trusts your computer.

Google Apps—Account and Endpoint Management is Not Supported in Provisioning Manager

The Provisioning Manager does not support the management of Google Apps objects. Use the CA Identity Manager User Console to manage Google Apps Connector objects.

Google Apps—Error Message When Creating Google Apps Accounts

Symptom:

When I create a Google Apps account, I receive the error message *Failed to Execute CreateGoogleAppsUser Google Apps account has been created, but some additional operation failed*

The account is created in CA Identity Manager and on the Google Apps endpoint, but it is not visible in the CA Identity Manager User Console because it is not associated with the global user.

Solution:

The error occurs when you try to create an account using the same nickname and username.

To fix the problem, do an explore and correlate on the Google Apps endpoint.

The account you created is associated with the global user in CA Identity Manager and is now visible.

Google Apps—Multiple Google Apps Endpoints on the Same Java CS

Google Apps Connector proxy settings are system-wide properties. If you create two or more Google Apps endpoints on the same Java CS, use the same proxy server, port, user name, and password for all the Google Apps endpoints on the same Java CS.

Google Apps—Error Message HTTP 403: Forbidden Received When Using NTLM Authentication

Symptom:

When I try to use NTLM authentication I receive the error *HTTP 403: Forbidden* from the proxy server and the Google Apps domain is not acquired.

Solution:

The error occurs because on a Windows computer, the Java CS is installed as a Windows Service and runs as Local System by default.

If Java CS is running on a Windows computer and NTLM is the strongest authentication scheme supported by the HTTP proxy, the Google Apps connector attempts to use NTLM authentication with the HTTP proxy.

If your HTTP proxy server uses NTLM authentication, configure the Java CS to run under a Windows domain account or a Windows local account.

To configure NTLM authentication

Do either of the following:

- Run Java CS with a Windows account that can be authenticated with the HTTP proxy server without providing a user name and password for proxy authentication when creating the endpoint.
- Run the Java CS with a Windows account that cannot be authenticated with the HTTP proxy server, and provide a HTTP user name and password that can be authenticated with the proxy when creating the endpoint.

Note: If you use a Windows domain user for HTTP proxy authentication, prefix the HTTP proxy user name with the Windows domain that the user is in. For example, DOMAIN\ProxyUserAccountName.

Lotus Notes/Domino

The following sections describe the known issues for the Lotus Notes/Domino connector:

LND Account Mail Files 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' check box is checked, 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.

Cannot Open Database on Remote System

Symptom:

To open a database on a remote system, that system must list the server where the agent is running as a trusted server.

Solution:

Run the explore and correlate on the LND endpoint to remove the eTLNDHomeServer attribute from the repository.

NDS

The following sections describe the known issues for the NDS connector

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.

Workaround

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.

OpenVMS

The following sections describe the known issues for the OpenVMS connector

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.

Workaround

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.

Workaround

Always reset the primary password when attempting to set a secondary password for the account.

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).

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.

Workaround

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.

Rights Attribute

The Rights attribute does not function in a reverse synchronization policy due to a connector issue. Avoid using this attribute in a reverse synchronization policy.

PKI

The following sections describe the known issues for the PKI connector

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 accounts with the same name appear as a duplicate to the PKI connector.

Email Notification Warning When Creating PKI Accounts

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

Workaround

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

PKI Connector does not Support Internationalization

Accounts with non-7bit-ASCII characters are not displayed in the Provisioning Manager correctly as the PKI Connector does not support internationalization.

RSA ACE (SecurID) Connector

The following sections describe the known issues for the RSA ACE (SecurID) Connector:

Install or Upgrade of RSA Remote Agent Fails Due to ECS Problem

Valid on Windows and Solaris

Symptom:

When I install or upgrade RSA remote agent, it sometimes fails due to an ECS problem.

Upgrade and fresh install of the remote agent fail with the message "Error applying transforms. Verify that the specified transform paths are valid."

The installation rolls back, and the agent does not get installed.

Solution:

1. Do the following:
   a. Reboot the machine before attempting to install ECS.
   b. Check for sufficient disk space.
   c. Make sure no other installation packages are running from another session.
   d. **(Windows)** Verify that no Windows automatic updates are running in the background.
2. If your ECS installation was corrupted before you started upgrading RSA Agent, do the following:
   a. **(Windows)** cd RemoteAgent\RSA\windows\

      CA Enterprise Common Services.exe

      The CA Enterprise Common Services Setup Maintenance program begins.

      Select Remove, and follow the prompts.

      (Solaris) Uninstall ECS:

      cd /opt/CA/eCS/scripts

      ./eCSuninstall.sh
   b. **(Solaris)** If the uninstall script fails, manually remove ECS:

      rm -rf /opt/CA/eCS

      rm -f /etc/.ecspath

      rm -f /opt/CA/SharedComponents/lib
   c. Locate ECS:

      (Windows) cd RemoteAgent\RSA\windows\

      (Solaris) cd RemoteAgent/RSA/solaris/ecs-installation
   d. Run ECS:

      (Windows) CA Enterprise Common Services.exe

      The CA Enterprise Common Services Setup Maintenance program begins.

      Select Repair, follow the prompts, and use default options.

      (Solaris) ./eCSinstall.sh /opt/CA/eCS

      ECS finishes.
3. Run the RSA Agent installer.

   Your local copy is upgraded.

RSA SecurId 7

The following sections describe the known issues for the RSA SecurId 7 connector:

Assigning a Provisioning Role to a Global User to Create an RSA Trusted User Account Fails

Valid on Windows and Solaris

Symptom:

When I assign a Provisioning Role to a global user to create an RSA trusted use in CA Identity Manager, the account creation fails.

Solution:

The account creation fails because the account template contains the default rule strings %P%, %UL% and %XD% that are not required for an RSA trusted user.

When you first create the template and delete the rule strings that are not required, the rule strings reappear when you assign the template.

When you create a template for an RSA trusted user, do the following.

1. Create the template using the default rule strings and click Submit.
2. Modify the account template, and delete the %P%, %XD% rule strings from the Password and Start Date fields on the Account tab.
3. Delete the rule string %UL% from the Start Date field on the User tab.
4. Submit the template.
5. Assign the provisioning role to the global user again.

Exploration of an RSA 7.1 Endpoint Fails

Symptom:

When I acquire an RSA 7.1 endpoint and select either a level 1 or level 2 exploration, the exploration fails with error messages similar to the following:

```
JCS: RSA7: Error searching RADIUS profiles in Incoming message header
or abbreviation processing failed nested exception is:
java.io.InvalidClassException:
com.rsa.authmgr.admin.radius.data.RadiusProfileListDTO; local class
incompatible: stream classdesc serialVersionUID = 20091214
```

```
Connector Server Search failed: code 54
(LOOP_DETECT-NoSuchMethodError): failed on search operation:
eTDYNContainerName=SystemDomain,eTDYNDirectoryName=rsa71_sp4-test,
eTNamespaceName=RSA SecurID 7,dc=AUTO,dc=etasa:
com.rsa.authmgr.admin.tokenmgt.SearchTokensCommand.setFirstResult(
I)V (ldaps://qa852imr12-5a.ca.com:20411)
```

Solution:

To upgrade a CA Identity Manager r12 CR7 or older environment that manages RSA SecurId 7 DYN Endpoints, you need to update the IMPD installer if the original IMPD installer is older than R12 CR8 after the upgrade.

To update the update IMPD installer

1. Stop the CA Identity Manager Provisioning Server service.
2. Start JXplorer and connect to the router DSA of the Provisioning Store. The router DSA runs on the Identity Manager Provisioning server by default. Use the following parameters:

   Host

   IMPS computer

   Port

   20391

   Security Level

   User and Password

   User DN

   eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb
3. In JXplorer, navigate to the entry:

`eTConfigParamName=Managed Branches,eTConfigParamFolderName=JCS_<*>_TLS_20411,eTConfigParamFolderName=Connector Servers,eTConfigParamContainerName=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=CommonObjects,dc=<im dc name>,dc=etadb`

4. Change eTConfigParamValue=eTNamespaceName=RSA SecurId 7,dc=ADMR12 to eTConfigParamValue=eTNamespaceName=RSA SecurID 7,dc=ADMR12.

   That is, change the lower case *d* in the string RSA SecurId 7 to an uppercase *D.* For example, change RSA SecurId 7 to RSA SecurID 7.

5. In Jxplorer, navigate to the entry:

   `eTNamespaceName=RSA SecurId 7,dc=<im dc name>,dc=etadb`

   a. Right click the entry and rename it to the following:

      `eTNamespaceName=RSA SecurIdx 7,dc=<im dc name>,dc=etadb`

   b. Right click the entry you renamed in step a again and rename it to the following:

      `eTNamespaceName=RSA SecurID 7,dc=<im dc name>,dc=etadb`

6. Restart the CA Identity Manager Provisioning Server service.

Salesforce.com

The following sections describe the known issues for the Salesforce.com connector.

Salesforce.com—Accounts and Endpoint Management is not Supported in Provisioning Manager

The Provisioning Manager does not support the management of Salesforce.com objects. Use the CA Identity Manager User Console to manage Salesforce.com objects.

Salesforce.com—Assigning a Provisioning Role to a Suspended Account Does Not Automatically Resume the Account

Symptom:

When I assign a provisioning role to a suspended account in CA Identity Manager, the provisioning role gets reassigned, but it is not automatically resumed.

This error occurs if you suspended the account using the *Account will be Suspended option* on the endpoint Settings tab.

Solution:

CA Identity Manager does not support resuming a suspended account when you reassign a provisioning role to the account.

After you assign a role to a CA Identity Manager account for the Salesforce.com connector, do the following:

1. In CA Identity Manager, navigate to Modify User's Endpoint Accounts, and select the endpoint account you want to resume.
2. Click Resume.
3. When prompted to confirm that you want to resume the account, click Yes.

   The account is resumed.

Salesforce.com—Error Message when Creating Salesforce.com Accounts

Symptom:

When I create a Salesforce.com account, I receive the error message *Failed to Execute CreateSalesforceUser Salesforce.com User has been Created but Some Additional Operation Failed*.

I cannot see the account that I created in the CA Identity Manager User Console.

Solution:

The error can occur under the following conditions when you create the user account:

- The password you specified did not meet Salesforce.com minimum password complexity requirements. For example, you specified a password of less than eight characters in length.

  This occurs because Salesforce.com allows you to create an account without specifying a password.

  The account is created in CA Identity Manager, but it is not visible because it is not associated with the global user. The account appears in your Salesforce.com organization, but a password has not been set.

- You specified that the user was a member of a non-existent public group. This can occur if:

  - The group was deleted on the Salesforce.com endpoint but you have not performed an explore and correlate in CA Identity Manager.
  - The account template you used to create the user specifies non-existent groups.

  CA Identity Manager ignores all invalid group memberships.

Do one of the following:

- If you received an error message stating that the password you specified when you created the account did not meet the minimum password complexity requirements, set a password that meets the minimum password complexity requirements in the CA Identity Manager User Console.

  The user account you created is associated with the global user in CA Identity Manager and is now visible.

- If you received an error message stating that the user was a member of a non-existent public group, add the user to the correct groups.

Salesforce.com—Objects Displayed as Salesforce in CA Identity Manager User Console

Symptom:

In the CA Identity Manager User Console, I only see references to Salesforce objects, rather than Salesforce.com objects in drop-down lists.

Solution:

In the CA Identity Manager User Console, Salesforce.com objects are displayed using Salesforce as the descriptor, rather than Salesforce.com. For example, a Salesforce.com endpoint is displayed as Salesforce in drop-down lists.

The error is a display error, and does not affect the management of Salesforce.com endpoints.

SAP

The following sections describe the known issues for the SAP connector

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 child system.

Workaround

You can change the contractual license types for the children natively.

SAP Endpoint is not Pre-Populated from the SAPlogon.ini File

When the Provisioning Manager is running on Windows 2008, the endpoint details for SAP are not being pre-populated from the SAPlogon.ini file.

Note: This problem is specific to the Provisioning Manager running on Windows 2008 only.

Workaround

You must manually enter the contents of the SAPlogon.ini file into the Provisioning Manager.

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.

The Contractual User Type Attribute in the Account License Data Tab does not Work for all License Types

When a User type is selected from the available list, only some user types work. Some license types produce an error 'BAPI' function call error. The reason is some User types contain extra fields that are not recognized.

Duplicate Email Entry when Modifying Email Attribute and Using Weak Synchronization

Symptom:

I assigned a provisioning role to a user with a SAP account template with weak synchronization enabled and modified the email attribute. As a result, a duplicate email entry was added to the SAP account. One value contains the modifications, but the other value does not.

Example: Modifying the Email attribute on a SAP Account Template with Weak Synchronization Enabled

This example shows what happens when you modify the email attribute on SAP account template with weak synchronization enabled.

In this example, the account template has the following rule:

Email address	Default	Description	home
%AC%@company.com	true	Use during business hours	false

As a result, Bob Jones has the following email address:

```
bobjones@company.com,default,Used during business hours,not_home
```

If you change the description capability attribute and update the template, for example,

```
%AC%@company.com,default=yes,description=Use during EST business hours,home=no
```

Bobs account now has two email addresses, one with the modified attribute and one without:

```
bobjones@company.com,not_default,Used during business hours,not_home
bobjones@company.com,default,Used during EST business hours,not_home
```

Solution:

Weak synchronization only adds capabilities to accounts, and does not remove them, therefore this behaviour is expected when you use weak synchronization and modify the email attribute. If you want to continue to use weak synchronization when modifying the email attribute on SAP account templates, consider using the SAPEmailWeakSyncConverter. The converter prevents the addition of duplicate email entries to SAP accounts when you modify the email attribute and use weak synchronization.

The SAPEmailWeakSyncConverter is disabled by default. To enable the convertor, edit the SAP Connectors Connector.xml file.

Note: For more information about overriding a connector, see *Connector Configuration File* in the Java CS Implementation Guide.

To enable the SAPEmailWeakSyncConverter

1. Navigate to the following directory:
   jcs_home/conf/override/sap/
2. Open the SAMPLE.connector.xml file, and navigate to the converters section.
3. After the FLEXI_STR:SAPDate entry, add the following:

   ```
   <entry key="FLEXI_STR:SAPEmail">
   <bean class="com.ca.jcs.sap.converter.SAPEmailWeakSyncConverter"></bean>
   </entry>
   ```
4. Navigate to the validators section and add the following after the SAPDate validator entry:

   ```
   <entry key="FLEXI_STR:SAPEmail">
   <bean class="com.ca.jcs.sap.validator.SAPEmailAttributeValidator"></bean>
   </entry>
   ```
5. Rename the Sample.Conenctor.xml to connector.xml.
6. Restart the Java CS.

The convertor is enabled and duplicate email entries are not added to SAP accounts when you modify the email attribute SAP account templates and you use weak synchronization.

Siebel

The following sections describe the known issues for the Siebel connector

SBL Error when Creating Account on Multiple Endpoints

An account template that lists multiple endpoints can only list Siebel groups that exist on all endpoints.

UNIX ETC and UNIX NIS

The following sections describe the known issues for the UNIX ETC and UNIX NIS connectors:

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:

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

Workaround

You will need to locate a version 4 of ncurses for the operating system and install it.

Chapter 6: Fixed Issues

This section contains the following topics:

Fixed Issues in r12.5 SP6

CA Identity Manager r12.5 SP6 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 1 through 15.

Support Ticket	Problem Reported
19988097	Add support for JNDI opbindings on two types of metadata classes which are not currently supported. For example, those with ambiguous naming attributes and ambiguous connector-speak class mappings.
19961208	CA Identity Manager certificate expiration vulnerability in Windows GINA.
19961208-02	CA Identity Manager GINA DNS Poisoning vulnerability.
19934103	When a user has a set of roles assigned as part of the member policies (first set) and other roles that are relying on these first set of role memberships (second set), the second set of role information is not displayed in the Admin Roles tab of the user.
19908370	With %UE% in E-mail address template, changing the primary email address into a GU location does not put back this address as primary (SMTP: type) if this address is already in the list as not a primary one (smtp: type).
19904391-02	View my endpoint accounts has no editable default search screens.
19892860	Reset Role Owners does not working while Modify Provisioning Role -> Owners Tab is working.
19881252	Provisioning base operations, for example, Modify Provisioning Role, causes duplicate Operation ID's resulting in inaccurate task failures.

Support Ticket	Problem Reported
19876970-02	After upgrading IMPS to 12.5SP3, IM Web could no longer retrieve RACF account templates.
19869025	Switching language on CA Identity Manager user logon page does not work.
19865164	The Japanese string which is translated from AND in View Submitted Tasks task has the wrong meaning.
19858646	Failed to create an account on ACC endpoint when eTACCEnvironment=101 (+Native NT) and when the NT password policy does not allow creating accounts without password.
19817108	During account creation, CA Identity Manager encountered a null exception failure when user supplies an empty value on an attribute flagged as AttributeLevelEncrypt.
19809359	Custom attributes in AD endpoints fail when the attribute has a high ASCII character in the string value.
19805521	When a customer modifies the ExportAll snapshot to reflect only his ACF2 accounts, the snapshot completes correctly. However, some of the reports fail.
19780840	Cannot manage AD account UNIX attributes.
19780840-2	During UNIX group membership assignment on account, CA Identity Manager Web UI hits a performance problem when searching UNIX groups from a large number of OU's.
19774555	Install changes are required for SDK DYN UPO Script. There is a sample provided. However, the sample is missing a mapping.
19741924-4	TEWS cannot retrieve Related Task Description field.
19739519	SDK DYN UPO Script option does not work when accessed from the Manager.
19711396	When creating a CA Identity Manager Environment and importing the Upgrade-8.1-to-12.5SP1-RoleDefinitions XML file, duplicate Categories/Tabs are added to the CA Identity Manager User Console.
127245	Package.bat does not package the EAR without multiple modifications and deviations from the process documented in the bookshelf. Package.xml specfies the wrong name of the workflow temp rar file, the file name is specified as workflow_ear_rar. It should be workflow_temp_rar.
126929	The CA Identity Manager Create Provisioning Role task does not save the customfield value into the objectstore.

Fixed Issues in r12.5 SP5

CA Identity Manager r12.5 SP6 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 1 through 14.

Support Ticket	Problem Reported
19506580-01	Upon upgrading from CA Identity Manager 12.0 CR7 to CA Identity Manager r12.5 SP2, we found that workpoint workflow was failing. On examination, all of our workpoint workflow scripts were truncated to approximately 100 to 105 lines. The scripts were cut off in mid line and failed to operate properly.
18484199	Operators NOW and ONCE are translated, thus reports functionality doesn't work.
19139638-01	User's Access Roles tab performs very slowly after upgrade from r12 CR5 to CR10.
19450496-03	The policy is configured to send email to the LIST of WORKFLOW APPROVERS throws "PxValidationException: Plug-in is not used with the correct context"
19618541	Customer is not able to get CA Identity Manager to failover to SiteMinder. CA Identity Manager is using a built-in Site Minder agent to communicate to the policy server
19756917-1	FailOver not working with CA Identity Manager r12.5 SP3 and SiteMinder 12.0 SP2 CR1 (both on RedHat 5.5)
19474393;01	CA Identity Manager hangs on startup infinitely on * Startup Step 2 : Attempting to Start PolicyServerService
19661928-01	Attempting to import the Role Definitions for the category 'upgrade from 12.5 to 12.5SP' fails with error stating 'unable to locate file.
19710656-01	After upgrading to CA Identity Manager R12.5 SP3, customer lost the ability to specify rulestrings in RSA7 Templates to set Token assignments.
19685235-01	Connector XP: Direct Assocation with non-naming attribute.
19676068-01	When using CA Identity Manager to add and remove Provisioning Roles by the standard modify user task, the Add completes but the Remove fails with an Unable to allocate Operations object.
19621892	Importing policy express PXParameter's with white space as the parameter won't be preserved, even though the white space was there during the export.

Support Ticket	Problem Reported
19647218	An error message is displayed when trying to JDBC Oracle endpoint
19759654-01	In the modify user task > Groups tab > when clicking on "Add a group" button, you never get the expected search screen allowing you to filter the search request against groups.
19736733-02	CA Identity Manager re-using Op IDs which causes Provisioning Server problems. In this case, it involves using the Reset User Password task.
19799998-01	When selecting the link of forggoten password at the MSGina logon, a Security vulnerability has been identified in GINA.
19592759-01	JCS metadata created for conversion of an old r8 C++ Connector to an r12.5 Java Connector causes an error.
19754393-03	"Modify Group -> Membership" or "Modify Group Members" task fail with "exception:java.util.NoSuchElementException: Attribute member has no value"
19818241-01	Oracle Applications Connector is hard-coded to ID APPS.
19665364-01	Stored procedure GARBAGECOLLECTAUDITING12 for Oracle doesn't delete any rows from IMSAUDITTASKSESSION12
19613965-02	Certify Oracle (formerly Sun) Directory Server Enterprise Edition 7 as a User Store
115875	Unix Remote Agent Install Fails on Solaris 10 sparse local zone
122039	The migration tool is migrating only the task session objects. In case if you try to migrate the pending tasks it is not migrating the event objects entries in object12 table. This is causing the problem when you try to use View Submitted Tasks to view the event objects information.
128582	To open database (mail\s0000011.nsf) on remote machines the server where the agent is running has to be listed by remote machine as trusted server.
127294	Request to Create the snapshot export definition XMLs based on each OOTB report.

Fixed Issues in r12.5 SP4

CA Identity Manager r12.5 SP6 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 9-11.

Support Ticket	Problem Reported
19246058-02	Page two of the Policies Tab in the View Provisioning Role task is blank.
19380365-1	If notification fails for any reason, the Notification queue is blocked.
19393945	The Xpress policy “get” function for “Accounts” category and type returns accounts for all existing endpoints instead of selected endpoint type accounts.
19394400-1	You cannot enter the same for more than one custom attribute for access roles. This is doc issue for PROD00118276 below
19506576-01	When running CA Identity Manager R12.5 SP2, you are unable to select RSA SecureID 7 as an endpoint in the Provisioning Manager.
19515875-1	When browser language settings are set from English to Spanish, the Option Selector control in the Modify Admin Task for Create User has an incorrect label.
19537723-01	Updating the CA Identity Manager R12.5 SP2 agent does not read the correct token value in the file /etc/default/passwd for SUSE 10.2+
19538080;1	Unable to customize tabs in User Certification task because tab names are missing in when modifying or creating an Admin task. Trying to select tabs to include in the task results in Error: Tabs:[SendCertificationReminder] Name is required. Unable to customize tabs in User Certification task.
19600576-01	In a CA Identity Manager Siteminder integration, the error BLTHGenerateTemporaryPassword appears when the Execute Forgotten Password Task is executed.
19610949	Error message 3042 is not localized correctly. Resource Key appears rather than the localized attribute names.
19616645	Invoking a web service from policyxpress fails with the following exception in the server log: <java.rmi.RemoteException: Call invocation failed; nested exception is: java.io.IOException: Could not transmit message>
19620528-02	The CA Identity Manager User Console is unusable when a user's endpoint is unavailable.

Support Ticket	Problem Reported
19627490-1	The CCS terminates unexpectedly when allocating a provisioning role or an account template with a long email address.
19636205-1	TEWS security flaw
19657285-01	CA Identity Manager phishing vulnerability
19602608-01	The TEWS WSDL is now generated according to WS-I compliance standards.
19260275-01	Admin roles with scoping rules for Provisioning Roles can now be instantiated within the modify provisioning role members/administrators task .
19666650-01, 19586799-02	After upgrading to CA Identity Manager r12.5 SP3, Weblogic will not start.

Fixed Issues in r12.5 SP3

CA Identity Manager SP3 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 9-11.

Support Ticket	Problem Reported
18950014-01	Tile image in IM Vista Credential Provider is customizable.
19043290-02	CA Identity Manager Provisioning Manager logout information required in the Provisioning Server log.
19145596-01	Identity Policy evaluations lacks delta evaluation phase.
19159246-1	Trying to Add or Remove Roles or Policies from a user that has an Aux class causes an LDAP error 65, Object Class Violation.
19199844	Websphere custom 404 page can display the a stack trace that can contain the CA Identity Manager application's code's footprint, compromising system security.
19241289-02	Enhance ADS connector and Exchange remote agent to provide support for MS Exchange Server 2010 and also support a mixed 2007 and 2010 Exchange environment.
19257834-01/ 19257834-02	When sending email (using sendmail program exits, for example), need ability to configure to send with 8BITMIME or 7BITMIME encoding. The MailConnector class (part of core product) formats and sends an e-mail.

Support Ticket	Problem Reported
19260912-03	With directory mapping and protecting TEWS URLwith Siteminder, an error was thrown indicating that CA Identity Manager could not find the administrator in the directory.
19285874	When defining a wellknown "%GROUP_ADMIN_GROUP%" attribute for an CA Identity Manager environment with UserStore=ProvisioningStore, CA Identity Manager User Console does not display the Admin Group you added.
19309023:1	Adding members to a group with over 1000 users in Active Directory throws Failed to execute AddToGroupEvent. ERROR MESSAGE: NoSuchElementException:Attribute member has no value
19312573	Provide support for multivalued Owner attribute
19312793;02	Provide support for Unique LND Shortnames
19312829;02	Currently, the CA Identity Manager User Console generates a set of requests to modify a multi-value attribute (one request per one value). This causes problems in LND connector new features (for example, multi-value short name and owner attributes),
19312847-02	Add support for specifying additional header attributes in the CA Identity Manager email templates.
19312856;02	The current method of finding unused token to assign to a user has unacceptable performance.
19315466-01	An error message “"Failed to delete Endpoint Type "Inet Portal…” is received when trying to remove a DYN connector that has been incorrectly deployed using Connector Xpress.
19351567-01	The following message is received routinely in the CA Identity Manager log: 13:31:07,720 WARN [com.ca.iam.model.impl.IAMSessionImpl] Session com.ca.iam.model.impl.IAMSessionImpl@1a837c9 was not shut down properly.
19391958-01	When trying to reset a user password, the number of task persistence database connections increases exponentially. After some time, the maximum number of connections are increased and the application server crashes.
19409953-02	Assigning multiple SAP R/3 Roles to users does not apply all the Roles selected. Using the CA Identity Manager User Console to add 4 roles to an existing SAP user would often result in only one role being applied.
19420859;01	Existing RSA 7 Provisioning Connector supports an assignment of a next available (unassigned) token without the ability to distinguish between hardware and software tokens.

Support Ticket	Problem Reported
19442206	The Data Query section of Policy Xpress's does not have an option available to connect in a secure manner i.e. using SSL
19466106/19455231-02	In a sibling ADS environment, when the CCS tries to create a failover server list, the DsBindWithCred function crashes because the SAMID for the Enterprise Administrator is empty.
	Create a new CA DLP connector.
N/A	RSA token Explore gives the following error message: org.apache.directory.shared.ldap.exception.LdapSizeLimitExceededException: JCS: countLimit 500 exceeded error message
N/A	Certify Microsoft Exchange Connector and Remote Agent against Exchange 2010

Fixed Issues in r12.5 SP2

CA Identity Manager SP2 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 9-11.

Support Ticket	Problem Reported
18898396-01	Under some circumstances, SiteMinder transforms the header ca_im_notification into ca-im-notification. The second version was not supported.
18981757	Unable to view reports on German Localized Server.
18988910	Setting the eTHomepage value containing space clears the value. This was caused because of having a space in the attribute is an invalid URL.
19030877-02	If the customer is using JDK 1.5 and attempts to use the RDT tool to generate a JIAM extension jar for a custom connector it fails with following: errorNoClassDefFoundException thrown for javax.xml.stream.XMLStreamException.
19030877-05	Provisioning SDK needs to be addressed in order to get pttconvert.bat working.
19067356 19004912	The auditing database may eventually accumulate records that are no longer necessary. There needs to be a way to remove these records.
19103826	Included as part of CQ 113005

Support Ticket	Problem Reported
19122949-01	When a GU has no corp ID, changing the suspended status will cause the following error: ERROR: ETACallbackException:There is no task mapped to the provisioning event. 'POST_ADD_GLOBAL_USER' for the environment 'corp'
19125743-01	Aux OC not updated via Provisioning Role.
19135793-01	Setting the Answer field to be of Type="Password" and with Permissions="Read/Write Required" generates errors. Characters of the Answer field (from Security Q&A) shall be obfuscated This is field type "Password". However in the combination of setting the Answer field permissions to "Read/Write Required" throws errors.
19136165-01	In Connector Xpress, duplicating a Template does not set eTAccountContainer.
19137329:1 19137329	When the customer enters a token that contains a single quote, such as "can't" or "owner's", this character is not escaped property, and the token displays incorrectly.
19141667	Logical Attribute Handler lifecycle methods are not being called. This prevents access to properties defined for the LAH.
19154215	Imlanguage header variable set by Siteminder was ignored and default locale files were used if browser did not have any languages defined. If the browser did have any languages defined, it uses the smlanguage header variable.
19156852	LND account templates contain different values in Identity Manager and Provisioning Manager
19158692-01	When either the "Actions performed by user" or "Actions performed on user" tabs were clicked, an exception error was generated.
19161923	Customer would like failed attempt Counter to be updated each time the questions page is loaded rather than each time the FPR task is initiated.
19172631-01	After propagating password change through AD PSynch agent, users were able to log into Oracle with the new password but were prompted to change their password again. Password_date field was not being updated after password has been changed. This causes Oracle to prompt for a password change when user first logs into the system.
19175330-01	Supporting OID 4-way association attributes, including physical=>physical assocs.

Support Ticket	Problem Reported
19208273-01	When the customer upgraded their Provisioning Server from 8.1sp2 to r12.5, the upgrade failed. The customer enabled the password profile, but the global user password they put in the r12.5 installer did not match the password profile.
19218319	There is inconsistent behavior where CA Identity Manager sends a response with transaction ID – in some cases even when the event fails later, and in some cases an error is returned without a transaction ID. With this fix, a transaction ID is returned in all cases. If the task did not generate an error, the response consists of the response data and the transaction ID. If the task did generate an error, the response consists of the transaction ID and the IMSException message.
19233440-01	In Connector Xpress, cannot create an OID account on endpoint if executing through Role assignment and Account Template from Provisioning Manager.
19236949-01	Reporting: Validation errors when submitting report start/stop dates.
19237112	When attempting to acquire Lotus Notes target system, the JCS reported an error "Insufficient access to Domino Databases" and the acquisition fails.
19315032	In the Connector - RACF, wrong object class filter into one level search request when full name requested.
19380885-01	The XML payload in UPO Program Exit has an empty value for password although a non empty value was configured.
N/A	It is not possible for customers to use the RoleDefGenerator to generate account screens for their custom C++ connectors. It only works for DYN connectors and the standard static connectors.
N/A	If you are using WebLogic 9 or 10 in production mode, the Identity Manager EAR may not auto-deploy the first time you start the application server after an install or upgrade.

Fixed Issues in r12.5 SP1

CA Identity Manager SP1 includes the fixes in the following table. This release also includes fixes and enhancements from CA Identity Manager r12 CRs 9-11.

Support Ticket	Problem Reported
16978047	After upgrading from eTrust Admin 8.1 SP2 to Identity Manager r12.5, any Microsoft 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).
17145005	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.
18240718	Capture Snapshot task fails when 'imr_attrvalue' column is set to 20 characters in length.
18624436	When generating screens, tasks, and roles for an LDAP DYN endpoint type using the RoleDefGenerator, an exception occurs.
18664092	When installing the extensions for SiteMinder on a separate server, the user is prompted for the SiteMinder install directory only.
18726210	CA Identity Manager extensions to SiteMinder are not available on Linux.
18726850	After CA Identity Manager is deployed on a WebSphere cluster, the JDBC password is stored as plain text.
18745183	Samples for localization contain Localization and location2 folders, which is confusing.
18758373	While using Connector Xpress to build a connector for Oracle Internet Directory, errors appear during the mapping process
18751087	New tabs that were added to the AD connector are visible in the Provisioning Manager, but not in the User Console.
18942182	When the account synchronization is set to OnEveryEvent for the Enable/Disable User task or the Modify User task and the user's Enabled State is updated, the request sent to Provisioning Server is missing the eTSyncAccounts=1 so the new value is not synchronized with associated accounts.
N/A	If LANG is set to xxxUTF-8 on Linux systems, you may see a sun.io.MalformedInputException error during workflow startup. This happens on WebSphere on Linux.
N/A	When you click the Initiated by User tab in the View User Activity task for the first time, an error occurs.

Support Ticket	Problem Reported
N/A	If you attempt an automatic migration of your Directories and Environments during a CA Identity Manager upgrade, you may get a SiteMinder error. If you have changed the default SiteMinder port for authentication (44442), the installer incorrectly detects that SiteMinder is not running, and does not allow you to proceed.
N/A	If you change one of the specified Provisioning Servers, CA Identity Manager may send failover requests to the original Provisioning Server instead of the new Provisioning Server.
N/A	When installing CA Identity Manager, you must use a fully qualified URL.
N/A	After upgrading, mapping the DYN attributes, and redeploying the metadata into your DYN endpoint types, the first tab on the Endpoint screens generated using the RoleDef Generator tool is not displayed.
N/A	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

Chapter 7: Documentation

This section contains the following topics:

Bookshelf

The Bookshelf provides access to all CA 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 bookshelf ZIP file.

   Note: For best performance, when you install the bookshelf on a remote system, make the bookshelf accessible from a web server.
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, 7, or 8 or Mozilla Firefox 2 or 3. For links to PDF guides, Adobe Reader 7 or higher 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 CA 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 is now rebranded as CA Directory. Any mention of an eTrust product within the documentation is equivalent to the same product with the new CA brand.

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

Documentation Changes

The following changes have been made to the documentation set as of CA Identity Manager r12.5.

Installation Guides and High Availability Guide

The high-availability content for CA Identity Manager has been merged into the Installation Guides for each application server. There is no longer a separate guide to address high availability.

Upgrade Guide

A new guide in CA Identity Manager r12.5. All content related to an upgrade of CA Identity Manager has been separated out from the Installation Guides and placed in the Upgrade Guide.

User Console Design Guide

This new guide is intended for system administrators who initially configure an Identity Manager environment after installation.

This guide includes information about customizing tasks (including task navigation, and screen design), branding, and localization.

Programming Guide for Provisioning

This guide, which describes deprecated Provisioning APIs (see page 69), has been removed from the bookshelf. It is now available with the installation package for the APIs.

Appendix A: Third-Party Acknowledgements

This section contains the following topics:

Apache

Portions of this product include software developed by the Apache Software Foundation.

Apache Ant 1.6.5

Apache Axis 1.1

Apache Axis 1.2

Apache Axis 1.2.1

Apache Axis 1.4

Apache Axis2/Java 1.5

Apache Bean Scripting Framework 2.4.0

Apache Jakarta Commons BeanUtils 1.6.1 and 1.7

Apache Commons Cli 1.0

Apache Jakarta Commons Codec 1.3

Apache Jakarta Commons Collections 3.1

Apache Jakarta Commons DBCP 1.2.1

Apache Jakarta Commons Validator 1.2

Apache Commons Digester 1.7

Apache Commons Discovery 0.2

Apache Commons EL 1.0

Apache Commons File Upload 1.2

Apache Commons IO 1.3.1

Apache Commons Lang 2.1

Apache Commons Logging 1.0.4

Apache Commons Pool 1.3

Apache Derby 10.4.2

Apache ehcache 1.2.4

Apache Jakarta Taglibs 1.0.6

Apache Jakarta ORO 2.0.8

Apache Jakarta Slide 2.1

Apache Log4j 1.2.8

Apache HttpClient 3.0

Apache MyFaces 1.1.5

Apache JSTL Taglib 1.1

Apache POI 3.2

Apache Quartz 1.5.2

Apache Spring Framework 1.2.8

Apache StAX 1.2

Apache Struts 1.2.7 and 1.2.9

Apache Velocity 1.4

Apache Xalan-C 1.9.0

Apache Xalan-J 2.6.0

Apache xmltask 1.13

The Apache software is distributed in accordance with the following license agreement.

Apache License Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and (d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

ANTLR 2.7.5H#

Portions of this product include software developed by the ANTLR.org. The ANTLR software is distributed in accordance with the following license agreement.

ANTLR 2.7.5H# License

[The BSD License]

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of the author nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ASM 3

This product includes ASM v.3, which is distributed in accordance with the following license:

DOM4J

This product includes dom4j which is distributed in accordance with the following license agreement:

BSD Style License

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain copyright statements and notices.

Redistributions must also contain a copy of this document. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.

Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.

Due credit should be given to the DOM4J Project - http://www.dom4j.org THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HSQLDB 1.7.3

This product includes HSQLDB v.1.7.3, which is distributed in accordance with the following license:

For content, code, and products originally developed by Thomas Mueller and the Hypersonic SQL Group:

Copyright (c) 1995-2000 by the Hypersonic SQL Group.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Hypersonic SQL Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE HYPERSONIC SQL GROUP, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Hypersonic SQL Group.

For work added by the HSQL Development Group (a.k.a. hsqldb_lic.txt): Copyright (c) 2001-2005, The HSQL Development Group All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HSQLDB 1.8.0

This product includes HSQLDB v.1.8.0, which is distributed in accordance with the following license:

For content, code, and products originally developed by Thomas Mueller and the Hypersonic SQL Group:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Hypersonic SQL Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE HYPERSONIC SQL GROUP, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Hypersonic SQL Group.

For work added by the HSQL Development Group (a.k.a. hsqldb_lic.txt): Copyright (c) 2001-2005, The HSQL Development Group All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IBM DB2 Driver for JDBC and SQLJ

"CONTAINS Runtime Modules of IBM DB2 Driver for JDBC and SQLJ

(c) Copyright IBM Corporation 2006 All Rights Reserved"

Jaxen 1.3

Portions of this product include software developed by the Jaxen Project (http://www.jaxen.org/) and is distributed in accordance with the following license agreement.

/*

$Id: LICENSE.txt,v 1.3 2003/06/29 18:22:02 ssanders Exp $

Copyright 2003 (C) The Werken Company. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "jaxen" must not be used to endorse or promote products derived from this Software without prior written permission of The Werken Company. For written permission, please contact bob@werken.com.

4. Products derived from this Software may not be called "jaxen" nor may "jaxen" appear in their names without prior written permission of The Werken Company. "jaxen" is a registered trademark of The Werken Company.

5. Due credit should be given to The Werken Company. (http://jaxen.werken.com/).

THIS SOFTWARE IS PROVIDED BY THE WERKEN COMPANY AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WERKEN COMPANY OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*/

JDOM 1.11

This product includes software developed by the JDOM Project (http://www.jdom.org/). The JDOM software is distributed in accordance with the following license agreement.

$Id: LICENSE.txt,v 1.11 2004/02/06 09:32:57 jhunter Exp $

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact .

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management . In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin . For more information on the JDOM Project, please see .

JSON 1.0

Portions of this product include software developed by JSON.org. The JSON software is distributed in accordance with the following license agreement.

Copyright (c) 2002 JSON.org

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The Software shall be used for Good, not Evil.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jtopen 5.1.1

JTOpen is distributed by CA for use with the CA product without any Contribution or change, addition or modification to the Program. The source code for JTOpen may be found here http://prdownloads.sourceforge.net/jt400/jtopen_5_1_1_source.zip?download or here http://opensrcd.ca.com/ips/3279_1.

libcurl 7.15.0

Copyright - License

Curl and libcurl are true Open Source/Free Software and meet all definitions as such. It means that you are free to modify and redistribute all contents of the curl distributed archives. You may also freely use curl and libcurl in your commercial projects. Curl and libcurl are licensed under a MIT/X derivate license, see below. Curl and libcurl does not contain any GPL source. I don't agree with the "viral" aspects of GPL. Another reason it doesn't contain GPL source is that it would limit users of libcurl. There are other computer-related projects using the name curl as well. For details, check out our position on the curl name issue.

COPYRIGHT AND PERMISSION NOTICE Copyright (c) 1996 - 2004, Daniel Stenberg, .

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

MX4J 3.0.2

This product includes software developed by the MX4J project (http://mx4j.sourceforge.net)." The MX4J software is distributed in accordance with the following license agreement.

/* ==

* The MX4J License, Version 1.0

*

* Copyright (c) 2001-2004 by the MX4J contributors. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. The end-user documentation included with the redistribution,

* if any, must include the following acknowledgment:

* "This product includes software developed by the

* MX4J project (http://mx4j.sourceforge.net)."

```
* Alternately, this acknowledgment may appear in the software itself,
* if and wherever such third-party acknowledgments normally appear.
*
* 4. The name "MX4J" must not be used to endorse or promote
* products derived from this software without prior written
* permission.
* For written permission, please contact biorn_steedom@users.sourceforge.net
*
* 5. Products derived from this software may not be called "MX4J",
* nor may "MX4J" appear in their name, without prior written
* permission of Simone Bordet.
*
* THIS SOFTWARE IS PROVIDED ``AS IS|&"&| AND ANY EXPRESSED OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED. IN NO EVENT SHALL THE MX4J CONTRIBUTORS
* BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* ====================================================================
```

*

* This software consists of voluntary contributions made by many

* individuals on behalf of the MX4J project. For more information on

* MX4J, please see

* http://mx4j.sourceforge.net.

*/

Oracle JDBC Driver 10g Release 2

This Product is distributed with Oracle JDBC Driver 10G Release 2 (10.2.0.1.0)from Oracle USA, Inc. (?Oracle?) The following additional terms and conditions apply to your use of the Oracle software product ("Oracle Product"):

(1) you may only use the Oracle Product to run the CA Product; (2) to the extent permitted by applicable law, Oracle disclaims liability for any damages, whether direct, indirect, incidental, or consequential, arising from your use of the Oracle Product; (3) at the termination of this Agreement, you must discontinue use and destroy or return to CA all copies of the Product; (4) Oracle is not obligated to provide technical support, phone support, or updates to the Oracle Product hereunder; (5) CA reserves the right to audit your use of the Oracle Product and report such use to Oracle or to assign this right to audit your use of the Oracle Product to Oracle; (6) Oracle shall be a third party beneficiary of this Agreement.

Rhino 1.5R5

Rhino 1.5R5

Rhino is distributed by CA for use with this CA product in unmodified, object code form in accordance with the Netscape Public License 1.0. Source code for Rhino may be obtained from its authors at http://www.mozilla.org/rhino/download.html. Any provisions in the CA license agreement that differ from the NPL are offered by CA alone and not by any other party.

NETSCAPE PUBLIC LICENSE

Version 1.0

---

1. Definitions.

1.1. ``Contributor|&"&| means each entity that creates or contributes to the creation of Modifications.

1.2. ``Contributor Version|&"&| means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. ``Covered Code|&"&| means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. ``Electronic Distribution Mechanism|&"&| means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. ``Executable|&"&| means Covered Code in any form other than Source Code.

1.6. ``Initial Developer|&"&| means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. ``Larger Work|&"&| means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. ``License|&"&| means this document.

1.9. ``Modifications|&"&| means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is: A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications. B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. ``Original Code|&"&| means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.11. ``Source Code|&"&| means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or a list of source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. ``You|&"&| means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, ``You|&"&| includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, ``control|&"&| means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of fifty percent (50%) or more of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims: (a) to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, or as part of a Larger Work; and (b) under patents now or hereafter owned or controlled by Initial Developer, to make, have made, use and sell (``Utilize|&"&|) the Original Code (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to Utilize the Original Code (or portions thereof) and not to any greater extent that may be necessary to Utilize further Modifications or combinations.

2.2. Contributor Grant. Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code or as part of a Larger Work; and

(b) under patents now or hereafter owned or controlled by Contributor, to Utilize the Contributor Version (or portions thereof), but solely to the extent that any such patent is reasonably necessary to enable You to Utilize the Contributor Version (or portions thereof), and not to any greater extent that may be necessary to Utilize further Modifications or combinations.

3. Distribution Obligations.

3.1. Application of License. The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code. Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications. You must cause all Covered Code to which you contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims. If You have knowledge that a party claims an intellectual property right in particular functionality or code (or its utilization under this License), you must include a text file with the source code distribution titled ``LEGAL|&"&| which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If you obtain such knowledge after You make Your Modification available as described in Section 3.2, You shall promptly modify the LEGAL file in all copies You make available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Your Modification is an application programming interface and You own or control patents which are reasonably necessary to implement that API, you must also include this information in the LEGAL file.

3.5. Required Notices. You must duplicate the notice in Exhibit A in each file of the Source Code, and this License in any documentation for the Source Code, where You describe recipients' rights relating to Covered Code. If You created one or more Modification(s), You may add your name as a Contributor to the notice described in Exhibit A. If it is not possible to put such notice in a particular Source Code file due to its structure, then you must include such notice in a location (such as a relevant directory file) where a user would be likely to look for such a notice. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions. You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works. You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation. If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute or regulation then You must:

(a) comply with the terms of this License to the maximum extent possible; and

(b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License. This License applies to code to which the Initial Developer has attached the notice in Exhibit A, and to related Covered Code.

6. Versions of the License.

6.1. New Versions. Netscape Communications Corporation (``Netscape|&"&|) may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions. Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works. If you create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), you must (a) rename Your license so that the phrases ``Mozilla|&"&|, ``MOZILLAPL|&"&|, ``MOZPL|&"&|, ``Netscape|&"&|, ``NPL|&"&| or any confusingly similar phrase do not appear anywhere in your license and (b) otherwise make it clear that your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY. COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN ``AS IS|&"&| BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

9. LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THAT EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS. The Covered Code is a ``commercial item,|&"&| as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of ``commercial computer software|&"&| and ``commercial computer software documentation,|&"&| as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS. This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in, the United States of America: (a) unless otherwise agreed in writing, all disputes relating to this License (excepting any dispute relating to intellectual property rights) shall be subject to final and binding arbitration, with the losing party paying all costs of arbitration; (b) any arbitration relating to this Agreement shall be held in Santa Clara County, California, under the auspices of JAMS/EndDispute; and (c) any litigation relating to this Agreement shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS. Except in cases where another Contributor has failed to comply with Section 3.4, You are responsible for damages arising, directly or indirectly, out of Your utilization of rights under this License, based on the number of copies of Covered Code you made available, the revenues you received from utilizing such rights, and other relevant factors. You agree to work with affected parties to distribute responsibility on an equitable basis.

AMENDMENTS

Additional Terms applicable to the Netscape Public License.

I. Effect. These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator client code and to all Covered Code under this License.

II. ``Netscape's Branded Code|&"&| means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo. This License does not grant any rights to use the trademark ``Netscape|&"&|, the ``Netscape N and horizon|&"&| logo or the Netscape lighthouse logo, even if such marks are included in the Original Code.

IV. Inability to Comply Due to Contractual Obligation. Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code. To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if such code would otherwise be considered ``Modifications|&"&| under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products. Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing. Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

VI. Arbitration and Litigation. Notwithstanding the limitations of Section 11 above, the provisions regarding arbitration and litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A.

``The contents of this file are subject to the Netscape Public License Version 1.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/NPL/ Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are

Copyright (C) 1998 Netscape Communications Corporation. All Rights Reserved.

Contributor(s): _____.|&"&|

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. This is due to time constraints encountered in simultaneously finalizing the License and in preparing the Original Code for release. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Rhino 1.7R1

Rhino 1.7R1

Rhino is distributed by CA for use with this CA product in unmodified, object code form in accordance with the Mozilla Public License 1.1. Source code for Rhino may be obtained from its authors at http://www.mozilla.org/rhino/download.html. Any provisions in the CA license agreement that differ from the MPL are offered by CA alone and not by any other party.

MOZILLA PUBLIC LICENSE

Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit

A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or

trademark) Licensable by Initial Developer to use, reproduce,

modify, display, perform, sublicense and distribute the Original

Code (or portions thereof) with or without Modifications, and/or

as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have

made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly

infringes any patent, then any and all rights granted by such

Participant to You under Sections 2.1 and/or 2.2 of this License

shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken minto account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

SAAJ 1.2

SAAJ v.1.2

For the above software the following terms and conditions shall apply:

This product contains certain files (the CDDL Files) which are governed by the Common Development and Distribution License, Version 1.0. The source code for the CDDL Files may be found here: http://opensrcd.ca.com.

SAXPath

This product includes SAXPath 1.0 distributed in accordance with the following terms:

/*--

$Id: LICENSE,v 1.1 2002/04/26 17:43:56 jstrachan Exp $

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "SAXPath" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@saxpath.org.
4. Products derived from this software may not be called "SAXPath", nor may "SAXPath" appear in their name, without prior written permission from the SAXPath Project Management (pm@saxpath.org).

   In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following:

   > "This product includes software developed by the SAXPath Project (http://www.saxpath.org/)."

   Alternatively, the acknowledgment may be graphical using the logos available at http://www.saxpath.org/

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE SAXPath AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the SAXPath Project and was originally created by bob mcwhirter and James Strachan . For more information on the SAXPath Project, please see .

*/

SpiderMonkey 1.5

This product includes SpiderMonkey 1.5. The source code version of SpiderMonkey 1.5 is licensed under the Mozilla Public License, Version 1.1 and is available at http://www.mozilla.org/js/spidermonkey/.

Sun JDK 1.6.0

This Product is distributed with Sun JDK 1.6.0 (JAVA SE DEVELOPMENT KIT (JDK), VERSION 6) (Sun JDK). The Sun JDK is distributed in accordance with the Sun Microsystems, Inc. (Sun) Binary Code License Agreement set forth below. As noted in Section G of the Supplemental License Terms of this license, Sun has provided additional copyright notices and license terms that may be applicable to portions of the Sun JDK in the THIRDPARTYLICENSEREADME.txt file that accompanies the Sun JDK.

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE DEVELOPMENT KIT (JDK), VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java Platform, Standard Edition (Java SE) on Java-enabled general purpose desktop computers and servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM SE Development Kit 6; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

H. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

I. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

ADDITIONAL TERMS AND CONDITIONS FOR THE USE OF

Sun JDK 1.6

(JAVA 2 PLATFORM STANDARD EDITION RUNTIME ENVIRONMENT 6.0)

Licensee agrees that the following terms (in addition to the applicable provisions above) shall apply with respect to any open source code provided by Sun Microsystems, Inc. contained within the Product. Notwithstanding anything contained in the CA End User License Agreement, solely with respect to such open source, these terms are not superseded by any written agreement between CA and Licensee:

"Software" means Java' 2 Platform Standard Edition Version 1.6_X and any user manuals, programming guides and other documentation provided to Licensee.

Title to Software and all associated intellectual property rights is retained by Sun Microsystems, Inc. ('Sun') and/or its licensors. Licensee acknowledges that Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this agreement.

The Software is provided "AS IS". As to any claim made by Licensee against Sun respecting Software, Licensee's exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software by Licensee to Sun which Licensee acknowledges is $0.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. The foregoing limitations shall not affect any warranties provided in any other applicable agreement between Licensee and CA.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid for Software by Licensee to Sun which Licensee acknowledges is $0. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

Licensee acknowledges that Licensee's use of the Software will terminate immediately without notice if Licensee fails to comply with any provision of this agreement. Licensee acknowledges that Sun may terminate this agreement immediately should the Software become, or in Sun's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, Licensee must destroy all copies of Software.

Licensee acknowledges and agrees as between Licensee and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and Licensee agrees to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use Licensee makes of the Sun Marks inures to Sun's benefit.

Notwithstanding anything to the contrary contained in any agreement between Licensee and CA, any action related to this agreement in which Sun is a party will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

Licensee acknowledges that additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

Windows Registry API Native Interface 3.13

Placed into the public domain on April 2, 2001

Authored by Timothy Gerard Endres

time@gjt.org

http://www.trustice.com/

This work has been placed into the public domain.

You may use this work in any way and for any purpose you wish.

THIS SOFTWARE IS PROVIDED AS-IS WITHOUT WARRANTY OF ANY KIND,

NOT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY. THE AUTHOR

OF THIS SOFTWARE, ASSUMES _NO_ RESPONSIBILITY FOR ANY

CONSEQUENCE RESULTING FROM THE USE, MODIFICATION, OR

REDISTRIBUTION OF THIS SOFTWARE.

Xinha .96 Beta 2