CA Identity Manager

Release Notes

r12.5 SP15

CA Technologies Product References

This document references the following CA products:

- CA IdentityMinder
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting
- CA GovernanceMinder

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 5: Known Issues 107

Chapter 1: New Features

This section contains the following topics:

r12.5 SP15

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP15:

CA Identity Manager User Store

- CA Directory r12.0 SP11

CA Identity Manager User Store and Runtime Store

- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1

Connector Xpress Database (JDBC)

- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1

Endpoints

- Microsoft Exchange Server Cluster (DAG) version 2010
- Microsoft SQL Server 2008 R2 SP2
- Microsoft SQL Server 2012 SP1
- CA Directory r12.0 SP11 as a JNDI endpoint

Additional Support

- Support of CA Identity Manager with CA SiteMinder SM r12 SP3 CR12, SM r12.5 CR1, SM r12.5 CR2, and SM r6.0 SP6 CR10
- Support of CA Identity Manager with CA GovernanceMinder (CA RCM) GM r12.5 SP8
- Mozilla Firefox 18.x support

Two Modes for Connecting to Exchange: Agentless and Agent

In previous releases, the Exchange connector required an agent on every Exchange endpoint.

Now, you can connect to Exchange 2007 and Exchange 2010 endpoints without using an agent. We recommend that you use agentless mode for new connections to these endpoints.

However, agentless mode does not work with Exchange 2003. To connect to Exchange 2003 endpoints, you must use the remote agent.

The following table lists the supported versions of Exchange for agentless and agent modes:

Endpoint Versions	Agentless	Agent
Exchange 2003	No	Yes
Exchange 2007	Yes	Yes
Exchange 2003 and Exchange 2007	No	Yes
Exchange 2010	Yes	Yes
Exchange 2007 and Exchange 2010	Yes	Yes

Support for Exchange Data Access Groups (DAG)

Exchange 2010 can use Data Access Groups (DAGs) to ensure high availability. You can connect to a DAG to ensure that the connection to the endpoint survives a failover.

Support for Automatic Mailbox Distribution in Exchange 2010

The connector can now handle automatic mailbox distribution.

When you create or move a mailbox, or mail-enable an existing user, the mailbox must be stored in a mailbox database. With Exchange Servers before Exchange 2010, you need to specify the mailbox database when you perform one of those operations. With Exchange Server 2010, you have the option of letting Exchange choose the database for you using automatic mailbox distribution.

Task Persistence DB Schema

Changes have been made to the existing SQL scripts that update the Task Persistence DB schema to use proper size for columns and the insert Runtime Status Detail stored procedure.

These changes will ensure that there are no longer any size discrepancies between the runtimeStatusDetail12 table and the corresponding archive_runtimeStatusDetail12 table for new or upgraded systems. This will eliminate failures for the Cleanup Submitted Tasks task.

Synchronization/Remove Account Template Values from Accounts

In this release, a new feature has been added in "Synchronization/Remove Account Template Values From Accounts" on the Responsibilities List attribute of Oracle Applications Account Template. Now you can use the feature to expire a Responsibility entry on Oracle Applications account.

The method of calculating the Responsibilities List to avoid some account out of sync problems has also been refined.

r12.5 SP14

New Certifications (see page 17)

SSL-Enabled JNDI User Store (see page 18)

Provisioning Manager Supports Searching Unmanaged Objects (see page 18)

Enhanced View Submitted Task Search (see page 18)

RACF Endpoint Connect - Group Association Ownership (see page 18)

Improved Localization Support for GINA/Credential Provider (see page 18)

Improved Error Messaging in GINA/Credential Provider (see page 19)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP14:

New Application Servers

The CA Identity Manager server can now be installed on the 64-bit of the JBoss Enterprise Application Platform 5.1.2

CA Identity Manager User Server Platform

- Red Hat Enterprise Linux 5.8
- Red Hat Enterprise Linux 6.3

Endpoints

- RACF 1.13
- Red Hat Enterprise Linux 5.8
- Red Hat Enterprise Linux 6.3
- CA Access Control r12.6 SP1
- Windows Server 2008 Core
- Lotus Notes 8.5.3 (64-bit) on AIX 6.1
- Oracle 11g R2 RAC as a JDBC endpoint

Additional Support

- Password Synchronization Agent support on Red Hat Enterprise Linux 6.3 (32-bit OS only)
- Credential Provider support on Windows Server 2008 R2 SP1
- Red Hat Enterprise Linux 5.8 support as a JCS platform
- Red Hat Enterprise Linux 6.3 support as a JCS platform
- Microsoft SQL JDBC Driver 4.0 with the CA Identity Manager Server, Connector Xpress (JDBC), and Java CS to manage MS SQL Server
- Support of CA Identity Manager with CA SiteMinder r6.0 SP5 CR31, r6.0 SP6 CR9, r12.0 SP3 CR10, and higher CRs
- Support of CA Identity Manager with CA GovernanceMinder (CA RCM) r12.5 SP7
- Support of CA SiteMinder r12.5 with CA Identity Manager versions r12.5 and r12.5 SP1 through r12.5 SP15

SSL-Enabled JNDI User Store

Peer certificate verification is now enforced. The feature requires that you add the user store SSL server certificate into the CA Identity Manager JRE default trusted keystore. The default trusted keystore is as follows:

```
JAVA_HOME\jre\lib\cacerts or jssecacerts
```

Provisioning Manager Supports Searching Unmanaged Objects

Provisioning Manager now supports searching for unmanaged objects. Unmanaged objects are configurable in Connector Xpress for DYN endpoints, and are represented as a value in a compound attribute that has a single-valued association. These objects were previously unsearchable.

Enhanced View Submitted Task Search

The View Submitted Task search screen on the Task ID is enhanced with the following options:

- *Allow searching on Task ID* checkbox is added to View Submitted Task tab configuration page
- *Task ID equals* field and a text box is added to the View Submitted Task initial search
- *Task ID* field is added for read-only display of Task ID

RACF Endpoint Connect-Group Association Ownership

A checkbox *Set Connect Group ownership* now appears on the endpoint tab for the RACF endpoint. When you select this option, the connect owner of the group associations is set to the group in the association rather than the CA Identity Manager administrative user ID.

Improved Localization Support for GINA/Credential Provider

The GINA/Credential Provider Secure Browser now supports localization on systems that are configured for a regional variation of a supported language. Specifically, the French (Canada) Windows locale (code page 3084) and Spanish (Spain) Windows locale (code page 3082) are now correctly displayed in French and Spanish respectively.

Improved Error Messaging in GINA/Credential Provider

The GINA/Credential Provider Secure Browser now informs the end user when the configured Self-Service Task URL is unreachable. The error message displayed when the network connection is unavailable or when the CA Identity Manager Server is unreachable is now customizable. This message is independent of the HTTP 404 Error message that was previously available in the Secure Browser.

r12.5 SP13

New Certifications (see page 20)

Enhanced Search Options for a Container Screen (see page 20)

Authorization Cache Size Tuning (see page 21)

ACF2 Support for Role and Compliance Manager (see page 21)

Improved Message on Program Exit (see page 21)

Protection from CSRF Attacks (see page 21)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP13:

Endpoints

- Red Hat Enterprise Linux 6.2 as an endpoint
- CA Access Control r12.6 as an endpoint
- HP-UX in a Shadow Mode as UNIX Remote Agent endpoint
- Microsoft Exchange Server 2010 SP2 as an endpoint
- PeopleSoft 8.52 as an endpoint

Additional Support

- Red Hat Enterprise Linux 6.2 support as a JCS platform
- Password Synchronization agent support on Active Directory 2008 R2 SP1 Core
- Password Synchronization agent support on Red Hat Enterprise Linux 6.2 (32-bit OS only)
- Password Synchronization agent support on Novell SuSE 11 SP1 (32-bit OS only)
- Additional interoperability support of CA Identity Manager with CA SiteMinder R12.5
- Additional interoperability support of CA Identity Manager with CA RCM r12.5 SP6

Enhanced Search Options for a Container Screen

The container search can be performed as a one level search or a full tree search against the endpoint. To support this enhancement, a search option is added to the Search for a Container screen under Create Explore and Correlate Definition task.

You can perform a search using *one* of the following options:

One Level

Performs a search at a container level against the endpoint.

Note: The One Level search improves the performance of all the non-hierarchical endpoints, for example, RSA endpoint.

Sub Tree

Performs a full tree search against the endpoint.

Note: To support this enhancement, the RSA container definitions are updated in both the Roledef metadata and JIAM JNDI object map. After you have upgraded CA Identity Manager, import the RSA-RoleDef.xml version 1.13 into the environment.

Authorization Cache Size Tuning

As of CA Identity Manager 12.5 SP13, you can tune the authorization cache size in a configuration file. This new feature includes a debug category that outputs the cache statistics to the application server log. The authorization cache stores information about the role membership, administration, and ownership privileges that a user requires to improve the performance. A separate cache is used for admin roles, access roles, and provisioning roles. You can configure the size of each role cache independently.

Note: For more information about Authorization Cache, see the *Implementation Guide*.

ACF2 Support for Role and Compliance Manager

The ACF2-ACFESAGE connector has been updated to allow the resource permissions to support CA Role and Compliance Manager. Resource rule lines split into separate connector objects for each specified service.

Improved Message on Program Exit

Provisioning Server returns the correct status for the POST_ADD_ACCOUNT Program Exit.

Protection from CSRF Attacks

CA Identity Manager is enhanced to improve the resistance to Cross-Site Request Forgery (CSRF) attacks. By default, the enhancement is disabled in CA Identity Manager.

To enable the enhancement:

1. Open the web.xml file located in the following location:

   application-server/iam_im.ear/user_console.war/WEB-INF
2. Find the <context-param> element with <param-name> csrf-prevention-on.
3. Set the <param-value> to true.
4. Restart the application server.

r12.5 SP12

New Certifications (see page 22)

Sample TEWS Code for .NET Framework 4 (see page 22)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP12:

Endpoints

- RSA SecureID 7.1 SP4
- ADAM/LDS 2008 R2 SP1 as a JNDI endpoint
- ADAM/LDS 2003 R2 SP2 as a JNDI endpoint
- CA Directory r12 SP8 as a JNDI endpoint

Additional Support

- SAP Netweaver 7.3 as a SAP R/3 endpoint
- Mozilla Firefox 9.x and 10.x support
- CA Identity Manager Server and Provisioning Directory on Red Hat Enterprise Linux 6.2
- Additional interoperability support of CA Identity Manager with CA SiteMinder 6.0 SP6 CR8, r12.0 SP3 CR9 and above

Sample TEWS Code for .NET Framework 4

The sample TEWS code that ships with the CA Identity Manager product has been updated for use with Microsoft's .NET Framework 4. The sample TEWS code now compiles and functions correctly with Visual Studio 2010.

r12.5 SP11

New Certifications (see page 23)

Enhanced ArcotID Self Service Tasks (see page 24)

New Configuration Item to Disable All Dialogs (see page 24)

French GINA and Credential Provider (see page 24)

Changes to Roles in Provisioning Manager Appear in the User Console (see page 25)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP11:

CA Identity Manager User Store

- Oracle OID 11g R1
- Novell eDirectory 8.8.6
- Microsoft ADAM (AD LDS) 2008 R2 SP1
- CA Directory r12.0 SP8

CA Identity Manager User Store and Runtime Store

- Oracle RAC 11g R2
- Microsoft SQL Server 2005 SP4
- Microsoft SQL Server 2008 SP2
- Microsoft SQL Server 2008 R2 SP1

Endpoints

- Novell eDirectory 8.8.6
- IBM i5/OS (also called OS/400) 7.1
- DB2 for iSeries on IBM i5/OS (also called OS/400) 7.1
- MySQL 5.5 as a JDBC endpoint
- Microsoft SQL 2005 SP4 as a Static and DYN JDBC endpoint
- Microsoft SQL 2008 R2 SP1 as a Static and DYN JDBC endpoint
- DB2 for z/OS 10.1 as a Static and DYN JDBC endpoint
- Lotus Notes 8.5.3
- CA Directory r12 SP8

Connector Xpress Endpoints

- Microsoft SQL Server 2008 SP2 as a Connector Xpress Database (JDBC) endpoint

Additional Support

- Mozilla Firefox 8.x support
- Password Synchronization Agent with IBM i5/OS (also called OS/400) 6.1 and 7.1
- Credential Provider with Windows 7 SP1 Professional Edition

Enhanced ArcotID Self-Service Tasks

The following new ArcotID self service tasks have been implemented in CA Identity Manager r12.5 SP11:

Create/Reset My ArcotID

Creates or resets an ArcotID. To create or reset an ArcotID, a user first uses this task to request an Activation code, which Arcot emails to the user at their Arcot account.

Once the user receives the code, they can enter it in CA Identity Manager to download the ArcotID from Arcot to their computer or smart phone.

Download My ArcotID

Allows you to download a new ArcotID, if you have an existing ArcotID. An activation code is sent to your email address for second factor authentication.

You can now execute tasks, such as Create/Reset My ArcotID and Download My Arcot ID, after login without multiple navigation steps.

Example:

http://*FQDNhostname*:*port*/iam/im/env/ca12/index.jsp?task.tag=CreateResetMy

http://*FQDNhostname*:*port* /iam/im/env/ca12/index.jsp?task.tag=DownloadMyArcotID

New Configuration Item to Disable All Dialogs

CA Identity Manager GINA and Credential Providers Secure Browser includes a new configuration item. Disable All Dialogs prevents Windows dialogs such as File, Open, Save, Print, and JavaScript errors from opening. The Secure Browser blocks access to these dialogs and secures the system from an attacker who may try to compromise the system.

Default Value: True

French GINA and Credential Provider

The GINA and Credential Provider user interfaces have been localized into French. The non-unicode system locale must be set to "French (France)" – code page 1036 – for the localization to be applied to the user interface.

Changes to Roles in Provisioning Manager Appear in the User Console

Previously changes to provisioning roles in Provisioning Manager did not affect what appears in the User Console. At this release, the changes made in Provisioning Manager are supported in the User Console. However, we recommend that you manage these roles through the User Console. Provisioning Manager features are being integrated into the User Console, the main user interface for CA Identity Manager.

r12.5 SP10

New Certifications (see page 26)

ACF2: Custom Attributes for Correlation (see page 27)

JCS: Bidirectional Relationship with Account and Group (see page 27)

Credential Provider Enhancements (see page 27)

History Editor Field Enhancement (see page 27)

Salesforce.com Connector Enhancements (see page 27)

Strong Synchronization Warning (see page 27)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP10:

CA Identity Manager User Store

- Red Hat Directory Server 8.2
- Oracle Directory Server EE 11g (11.1.1.5)

Connector Server

- Red Hat Enterprise Linux 5.7

CA Identity Manager Server and Provisioning Directory Platform

- Red Hat Enterprise Linux 5.7

Endpoints

- Red Hat Enterprise Linux 5.7 as a UNIX endpoint
- CA ACF2 r15
- CA Access Control 12.5 SP5
- CA DLP r14
- SAP R/3 4.6C and 4.7
- Oracle Database Server 11g R2 (static)
- Microsoft Active Directory 2008 R2 SP1
- Novell Suse 11 SP1 as a UNIX endpoint

Connector Xpress Endpoints

- Oracle OID 11g as a Connector Xpress LDAP (JNDI) endpoint
- Oracle Sun Java System Directory Server (iPlanet) 7 as a Connector Xpress LDAP (JNDI) endpoint
- Oracle Database server 11g R2 as a Connector Xpress Database (JDBC) endpoint

Additional support

- Mozilla Firefox 6.x support
- CA Technologies User Interface 7.0
- Password Synchronization agent support on Windows 2008 R2 Core
- Password Synchronization agent support on ACF2 r15
- Credential Provider on Windows 7 SP1 Professional Edition
- Additional interoperability support of CA Identity Manager with CA SiteMinder 6.0 SP6 CR7, r12.0 SP3 CR7 and above

ACF2: Custom Attributes for Correlation

This release includes the addition of 20 new attributes for the ACF2 connector, which you can map to endpoint attributes.

JCS: Bidirectional Relationship with Account and Group

The Java Connector Server (JCS) now supports a virtual persisted attribute. This attribute behaves identically to a normal virtual case, but the computed value is not discarded; it is persisted and mapped to the native attribute. Connector Xpress includes a new checkbox in the association editor to mark these associations and a new template exists to illustrate this capability.

Credential Provider Enhancements

The Credential Provider has been enhanced so that it can mimic the Microsoft password credential provider behavior. A new configuration parameter has been added for selecting the first credential as the default. For details on this enhancement, see the *Administration Guide*.

History Editor Field Enhancement

New lines being entered on the History Editor Field are visible in the History Display field.

Salesforce.com Connector Enhancements

Provisioning of users with portal licenses is added to the Salesforce.com connector.

Strong Synchronization Warning

Starting at this release, when you modify an account template to enable strong synchronization, a warning appears to confirm you enabled this feature. For more information on strong synchronization, see the *Administration Guide*.

r12.5 SP9

New Certifications (see page 28)

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP9:

CA Identity Manager Server Platform Support

- RedHat Enterprise Linux 6.x

Connectors

- RedHat Enterprise Linux 6.x

Provisioning Client Platform

- Windows 2008 R2 SP1

Endpoints

- CA Directory r12 SP7 as an LDAP endpoint
- RedHat Enterprise Linux 6.x as a UNIX endpoint
- EEM 8.4 SP4
- TSS r15
- Microsoft Windows 7 SP1

CA Identity Manager User Store

- CA Directory r12 SP7

Additional support

- Windows 7 SP1 as a Client platform
- RedHat Enterprise Linux 6.x for Provisioning Directory.
- RedHat Enterprise Linux 6.x as Java Connector Server platform.
- Password Synchronization agent support on RedHat Enterprise Linux 6.x.
- Password Synchronization agent support on TSS r15.
- Credential Provider on Windows 7 SP1.

r12.5 SP8

This section contains the following topics:

New Certifications

The following new platforms are certified with CA Identity Manager r12.5 SP8:

New Application Servers

The CA Identity Manager server can be installed on the 32-bit format of these application servers (in addition to the 64-bit format announced at r12.5 SP7):

- WebSphere 7
- JBoss 5.0 and 5.1

CA Identity Manager Server Platform

- Windows 2008 R2 SP1

Connectors

- CA Arcot WebFort 6.2 (new)
- PeopleSoft 8.5 Client Tools (updated)

Endpoints

- CA Directory r12 SP6 as an LDAP endpoint
- Windows 2008 R2 SP1
- RACF 1.12
- PeopleSoft 8.5 Client Tools

Provisioning Manager Platform

- Windows 2008 R2 SP1

New CA Identity Manager User Store Support

- CA Directory r12 SP6

Enhanced CA Identity Manager and CA RCM Integration

The following features are available with the enhanced integration between CA Identity Manager and CA RCM:

- You can import CA Identity Manager users as CA RCM users.
- You can customize the types of endpoint objects to import. If you only want a subset of a particular object type, you can also apply filters to the data that is imported.
- You can customize how attributes are mapped to what CA RCM fields.

- An export from CA RCM now updates data in the CA Identity Manager object store, and *not* the Provisioning Server. This allows you to take advantage of the following CA Identity Manager features:
  - CA Identity Manager task model
  - CA Identity Manager transaction logging
  - CA Identity Manager policy triggers
- A new screen allows you to enable or disable Smart Provisioning functionality or edit global defaults for suggested roles and compliance checking across all tasks.
- Continuous updates verify that changes made in CA Identity Manager are queued up and passed to CA RCM. This feature allows CA RCM to make provisioning role suggestions and validate changes against compliance policies, based on current CA Identity Manager information, without waiting for another import from CA Identity Manager to update the CA RCM data.

These enhancements require CA RCM 12.5 SP4 and CA Identity Manager 12.5 SP8.

Out of Compliance Analytics on Resource-Based Rules

When integrated with CA RCM, CA Identity Manager displays Out of Compliance violations that are triggered as a result of resource-based business policy rules (BPRs) in CA RCM. For example, if a user is a member of the group Executive, the user cannot be a member of the group Non-Employee. If someone tries to assign both these groups to the user, an Out of Compliance violation occurs and is displayed in CA Identity Manager.

This feature requires CA RCM r12.5 SP4.

Arcot Connector

This release includes an Arcot connector. After you have set up a connection to a CA Arcot Webfort 6.2 endpoint, you can use CA Identity Manager to do the following tasks:

- Create, view, and modify CA WebFort Arcot users
- Generate, view, and modify OTP, ArcotID, and QnA credentials
- View and modify ArcotOTP

Note: For information about the Arcot connector, see the Download page for Endpoint Guides for CA Identity Manager.

New Detail for Violation Message Display

The user console has been enhanced to display detailed information when an event generates an OOC exception.

Option to Limit Explore and Correlate

In Provisioning Manager, Explore and Correlate/Explore now includes a Lower Memory Cache option. It provides an exploration behavior that avoids an Out of Memory problem when the Provisioning Server explores an account container with a very large number of accounts.

Peoplesoft Connector Peopletools 8.51 Support

The Peoplesoft connector now supports up to Peopletools 8.51.

Note: Peopletools and Peoplesoft client tools must be the same version for the connector to work.

Support for Polish Environments

CA Identity Manager installs translated versions of the User Console and online help in Polish. For more details on supported languages, see the *User Console Design Guide*.

r12.5 SP7

This section contains the following topics:

New Certifications

New Application Servers

The CA Identity Manager server can now be installed on these application servers that are available in 64-bit formats:

- WebSphere 7
- Weblogic 11
- JBoss 5.0 and 5.1

Upgrading the CA Identity Manager server is possible on these application servers:

- WebSphere 6.1
- WebLogic 10.3

  Note: Support for 32-bit formats is available only for upgrades to CA Identity Manager 12.5 SP7 on WebSphere 6.1 and WebLogic 10.3.

New connector support

- Lotus Notes with Domino Server running on RHEL 5.3 Server
- Lotus Notes with Domino Server running on AIX 6.1
- Kerberos connector support on Microsoft Windows

New endpoints supported

- AIX 6.1 and 7.0
- Linux 5.4
- CA Access Control r12.5 SP2, SP3, and SP4

New CA Identity Manager User Store Support

- ADS 2008 R2
- Microsoft ADAM (AD LDS) 2008 R2

Additional support

- Microsoft Exchange agent support with Microsoft Exchange 2010 SP1
- Windows 7 for Vista Credential Provider
- Internet Explorer 9.0 as a browser for the User Console and Management Console
- SiteMinder r12.0 SP3 CR2 for the CA Identity Manager Server
- CA Business Intelligence (BusinessObjects XI R3.2) on Windows and UNIX as the Business Objects Report Server

Nested Roles

You can include a provisioning role within another provisioning role. The included role is named a nested role.

For example, you could create an Employee provisioning role. The Employee role would provide accounts needed by all employees, such as email accounts. You include the Employee role in department-specific provisioning roles, such as a Finance role and a Sales role. The department provisioning roles would provide accounts related only to that department. This combination of roles provides the right accounts for each user.

Note: For more information about nested roles, see the *Administration Guide*.

Bulk Loader Notifications

You can select certification managers for the Bulk Loader task. When a Bulk Loader task completes, CA Identity Manager creates a Bulk Loader Notification for all certification managers configured for the task.

This notification then appears in the Home tab under Bulk Loader Notifications. Clicking the notification displays details for tasks initiated by the bulk load operation. Certification managers can then review and acknowledge the changes detailed in the notifications.

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

User Console Enhancements

The following enhancements are available in the User Console:

- Support for additional tasks in search results and list screens
- Sample User Console
- New task configuration properties
- Pagination in search results and list screens

Additional Tasks in Search and List Screens

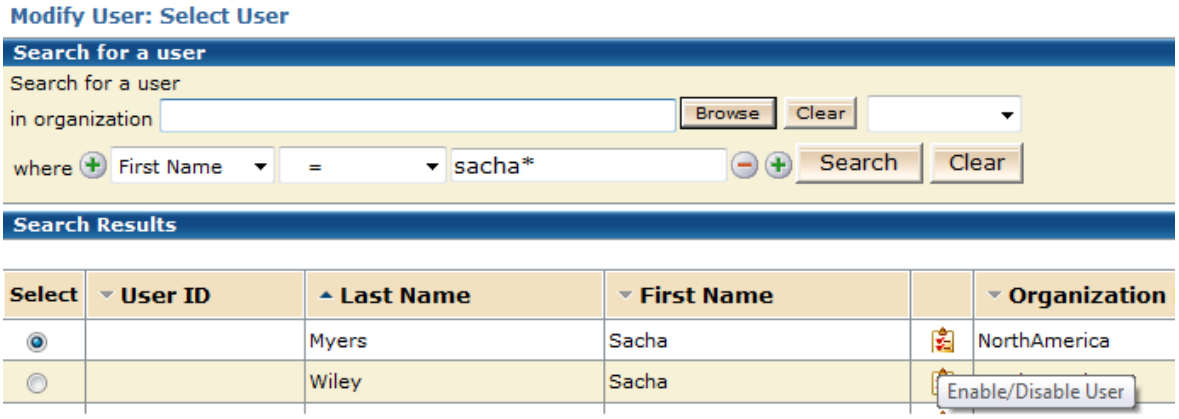
You can configure CA Identity Manager to add additional actions that users can perform in search and list screens. For example, you can configure the search screen in the Modify User task to enable users to perform a task, such as disabling a user, from the list of users returned by the search.

Adding tasks to search and list screens reduces the number of clicks required to complete a task, and simplifies the user console.

Tasks on search and list screens can be displayed using one of the following methods:

- Task links or icons

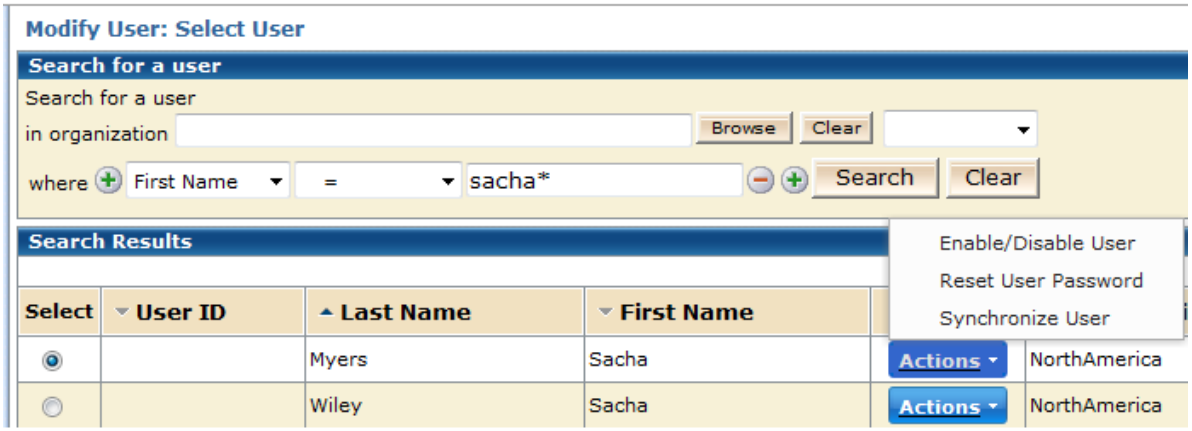
  Displays each task as a links or icon in the search results or list screens. Use this method to display a small number of tasks.



- Task Menus

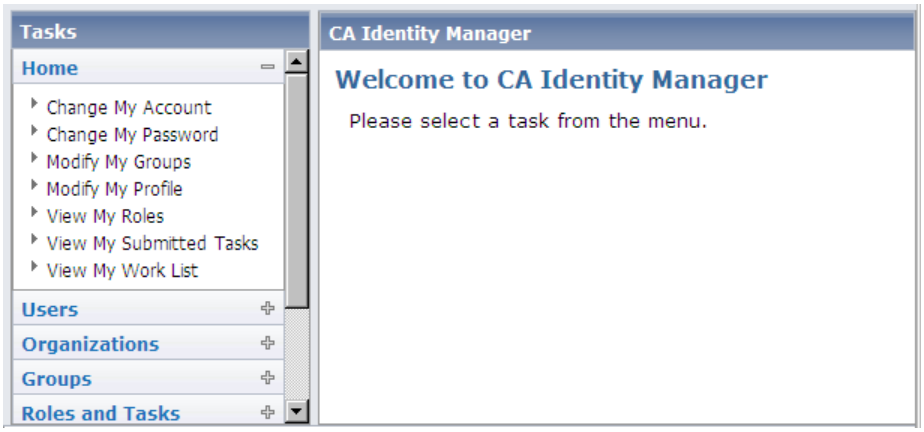
  Displays an Action button in each row in search results or list screens. Administrators click the Action button to see the list of tasks that they can perform for that user.

  Use this method if users are able to perform more than two or three tasks.



Sample UI7 Format for User Console

You can now use the User Console in a sample of the UI7 format, the new standard for applications developed by CA Technologies. The sample of the UI7 format features many usability improvements that reduce the number of required clicks. Also, the category task list remains visible by default while you perform tasks, but it can be hidden when needed. The sample format also uses Ext JS, which provides more options for using JavaScript.



You can evaluate this format by adding ui7 to the environment URL as follows:

http://*im_server*:*port*/iam/im/*environment*/ui7

To convert an environment to the sample UI7 format

1. Access the Management Console.
2. Select the environment.
3. Click Advanced Settings, Miscellaneous.
4. For Properties, enter: DefaultConsole.

   Be sure to avoid entering spaces before or after the property name.
5. For value, enter: ui7.
6. Click Add.
7. Click Restart Environment.

Task Configuration Properties

Task configuration properties control display properties and certain behaviors for the task. Using these properties, you can do the following:

- Specify an icon for a task

  This icon allows users to open additional tasks (see page 35) in search or list screens.

- Support for opening external tasks in a separate browser window

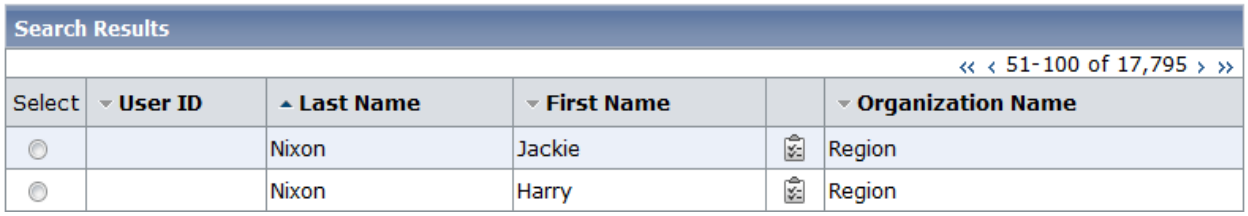
  CA Identity Manager can open a new browser window for an external task that redirects users to another web site.

- Hide task navigation

  You can hide the top-level navigation and task list once a user selects a task. This prevents users from navigating away from the current task until they complete required actions or cancel the task.

Pagination in Search Results and List Screens

CA Identity Manager now displays the number of the results currently being displayed, the total number of results, links to first and last page, and links to next and previous page.



Paging Support for Improved Search Performance

In previous versions of CA Identity Manager, large searches that returned many results caused the system to run out of memory in some cases. To help prevent memory issues, this version of CA Identity Manager includes paging support for the following objects:

- CA Identity Manager Directory

  You can configure the DirectorySearch element in the directory configuration file (directory.xml) that you use to create the CA Identity Manager Directory.

  By default, the value for maximum rows and page size is unlimited for existing directories. For new directories, the value for maximum rows is unlimited and the value for page size is 2000.

- Managed object definition

  To set maximum row limits and page sizes that apply to one type of object instead of an entire Directory, configure the managed object definition the directory.xml file that you use to create the CA Identity Manager Directory.

  Setting limits for a managed object type allows you to make adjustments based on business requirements. For example, most companies have more users than groups. Those companies can set limits for user object searches only.

Note: To use paging, the user store that CA Identity Manager manages must support paging. In some cases, the user store supports paging, but additional configuration is required. For more information, see the Configuration Guide.

Connector Xpress Enhancements

The following enhancements have been made to Connector Xpress:

- The Classes, Containers and Operation Bindings nodes are now top-level nodes.
- The Map Class and Attributes dialog has been renamed to the Map Class Dialog.
- An accounts screens node has been added to the mapping tree. The accounts screen editor has been moved from the Attributes Summary dialog to the Accounts screen dialog.
- The attribute mapping table has been moved to the Map Attributes dialog. In addition, mapping native attributes to provisioning attributes has been changed. That is, you now map provisioning attributes to native attributes, instead of native attributes to provisioning attributes.

- The Attributes Summary dialog has been renamed the Map Attributes dialog. All attribute mappings are now done on the Map Attributes dialog.
- The following new attributes have been added to the extended metadata:
  - Is Interesting to Compliance – allows you to mark an attribute as interesting to CA Role and Compliance Manager.
  - Connector Generator – Generator name which allows you to specify the value assigned to the property.
  - Is Connector Generated – allows you to specify that endpoint generates the value for property implicitly.
- Nodes in the mapping tree are no longer arbitrarily colored.

Improved Communication for Exchange 2007

When creating or modifying a mailbox, the ADS connector now sends information to the Exchange Remote Agent about which Active Directory to use. This communication allows the ADS connector and Exchange Server to have the same view of Active Directory. Therefore, all operations bypass the replication latency among the Active Directory servers.

r12.5 SP6

This section contains the following topics:

New Certifications (see page 39)

TEWS – Retrieve Related Task Description Field (see page 40)

New Certifications

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

- CA Directory r12 SP5, the CA 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 CA 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 CA Identity Manager user store
- Oracle Directory v7.0 as the CA 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 CA 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 CA 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 a CA 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 a CA 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.

Note: For more information, see the *Configuration Guide*. 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 CA Identity Manager user store.
- CA Business Intelligence 3.2 is supported on Windows and UNIX as the Business Objects Report Server.

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.

CA Directory r12.0 SP3 as a User Store

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

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 140)*.

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 CA 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 a CA 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 CA 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 50)
- Task Level Policy-Based Workflow (see page 51)
- Escalation Approval Template (see page 52)
- Matching Attribute Resolver (see page 52)
- Highlighting Changed Attributes on Approval Screens (see page 54)
- Partial Attribute Level Approve/Reject (see page 54)
- Approval Policy Description (see page 54)
- Bulk Operations on Work Items (see page 55)

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.

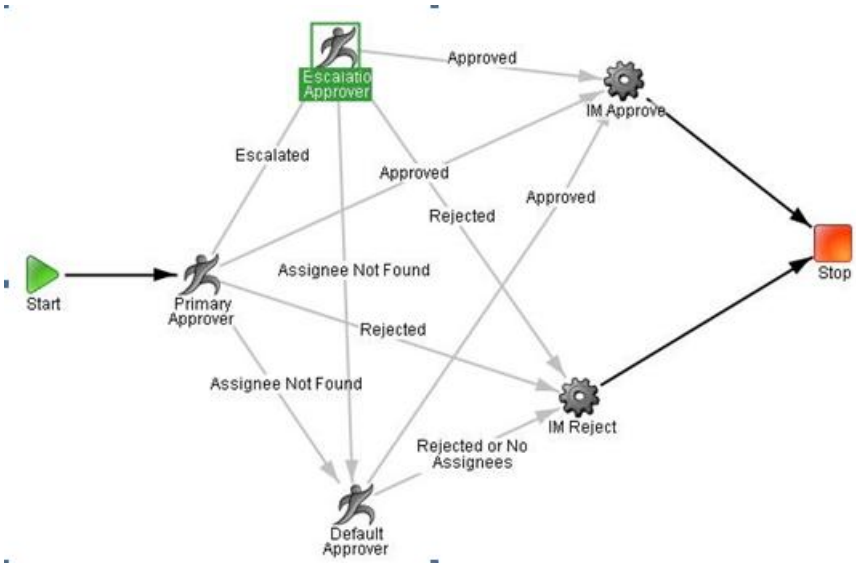
Only default CA Identity Manager workflow templates support workflow rules for task level policy-based workflow. You can also create custom workflow processes for use with workflow rules.

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:

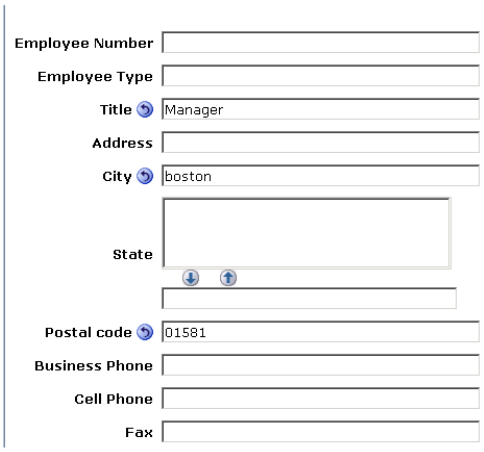
- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

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*.

r12.5

This section contains the following topics:

CA User Activity Reporting Integration

Beginning at CA Identity Manager r12.6, CA Enterprise Log Manager is called CA User Activity Reporting (CA UAR).

CA UAR 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 UAR 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 UAR 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 UAR identity centric reports and/or dynamic queries into CA UAR user Console using the CA Identity Manager User Console. From the User Console you can configure how existing CA Identity Manager/CA UAR 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

CA Identity Manager Directory Configuration Wizard

In this release, a new wizard is available that walks administrators through the process of creating a CA Identity Manager directory for their LDAP user store or Provisioning Server and helps reduce configuration errors. Before launching the wizard, you must first upload a CA 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 CA 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 r12 to r12.5 releases. The command line tool is part of the CA 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 a CA 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:

- Enterprise Log Manager integration
- Account Management

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

Report	Description	Source
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. For more information, see the EventState Element in the Auditing chapter of the *Configuration Guide*.	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.

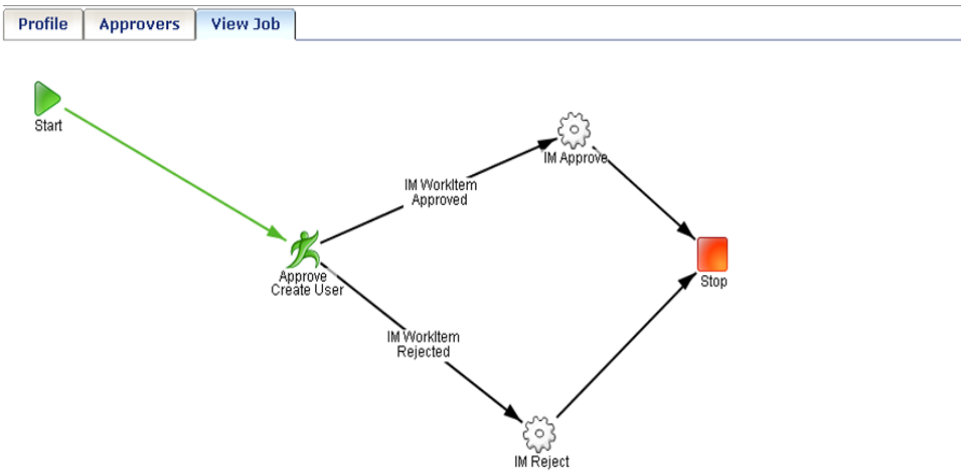
All default CA Identity Manager workflow templates and predefined processes support workflow rules. You can also create custom workflow processes for use with workflow rules.

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.

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.

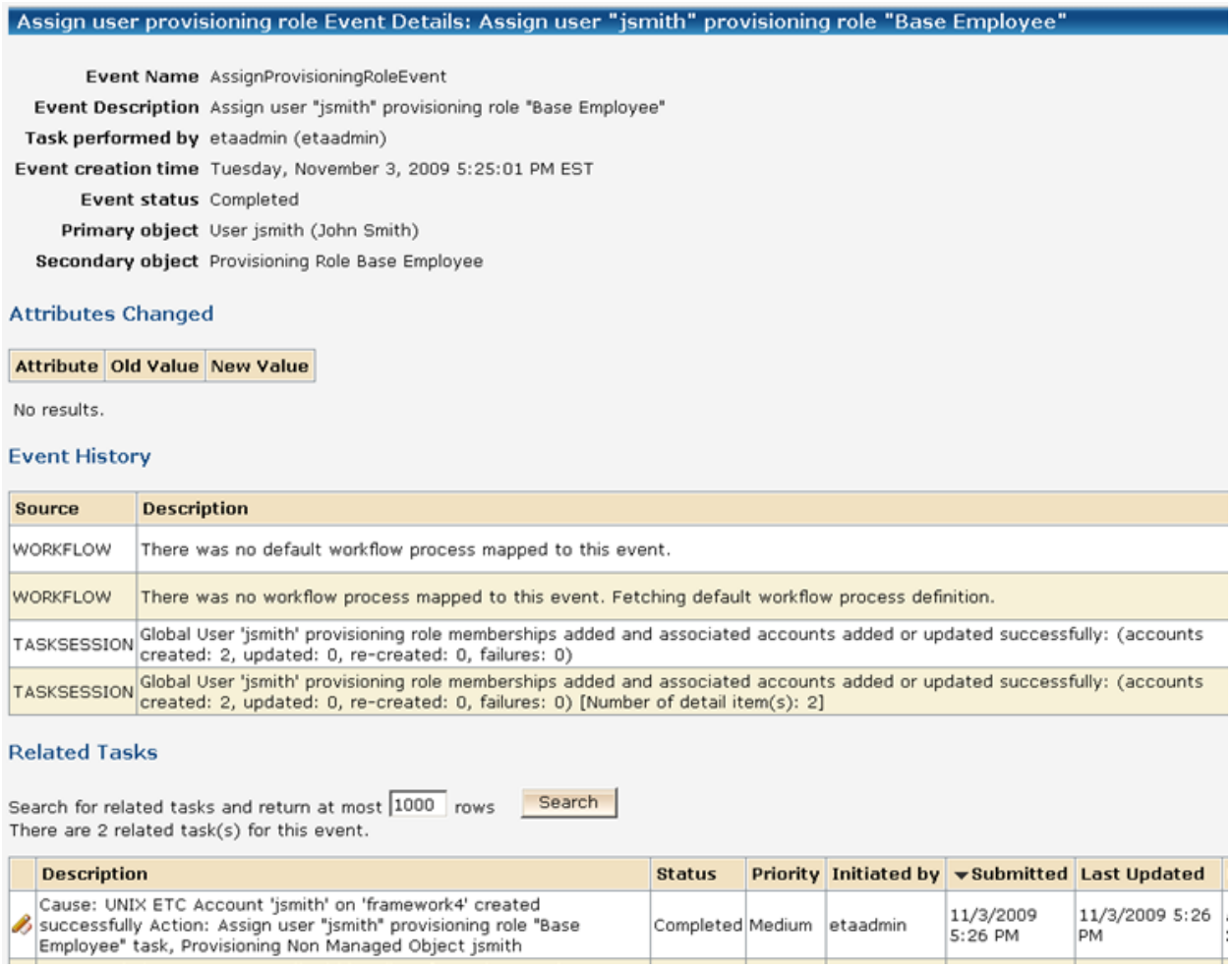
Note: For more information on reporting, see the *Administration Guide*.

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 CA 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:



Assign user provisioning role Event Details: Assign user "jsmith" provisioning role "Base Employee"

Event Name AssignProvisioningRoleEvent
Event Description Assign user "jsmith" provisioning role "Base Employee"
Task performed by etaadmin (etaadmin)
Event creation time Tuesday, November 3, 2009 5:25:01 PM EST
Event status Completed
Primary object User jsmith (John Smith)
Secondary object Provisioning Role Base Employee

Attributes Changed

Attribute	Old Value	New Value

No results.

Event History

Source	Description
WORKFLOW	There was no default workflow process mapped to this event.
WORKFLOW	There was no workflow process mapped to this event. Fetching default workflow process definition.
TASKSESSION	Global User 'jsmith' provisioning role memberships added and associated accounts added or updated successfully: (accounts created: 2, updated: 0, re-created: 0, failures: 0)
TASKSESSION	Global User 'jsmith' provisioning role memberships added and associated accounts added or updated successfully: (accounts created: 2, updated: 0, re-created: 0, failures: 0) [Number of detail item(s): 2]

Related Tasks

Search for related tasks and return at most 1000 rows Search
There are 2 related task(s) for this event.

Description	Status	Priority	Initiated by	Submitted	Last Updated
Cause: UNIX ETC Account 'jsmith' on 'framework4' created successfully Action: Assign user "jsmith" provisioning role "Base Employee" task, Provisioning Non Managed Object jsmith	Completed	Medium	etaadmin	11/3/2009 5:26 PM	11/3/2009 5:26 PM

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:

r12.5SP15

New Configurable Settings for the LND Connector

To improve the performance of LND Connector to Explore and Correlate, four new configurable settings are added for the LND Connector which are as follows:

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

Note: Changes to the values of the above attributes can be set in the following location:
`CA\Identity Manager\Connector Server\conf\override\lnd\connector.xml`

r12.5 SP13

SAP Role Description in the Search Screen

A Description column is added to the search results page. Use the description column to filter the search for SAP role and SAP profile objects in the Roles and Profiles tabs respectively.

Changes to Oracle Applications Account Templates

The following changes exist for Oracle Applications account templates:

- The Responsibility assignment has a "Valid from" date. This date had been changed from required to optional.
- If the "Valid from" date is empty when assigning a new responsibility to an Oracle Applications account, the current date is used.
- When checking account synchronization with an account template, CA Identity Manager checks if the "Valid from" date for responsibility assignment is empty in the template. If it is empty, synchronization does not report the account is not synchronized no matter what value the account has.
- When merging account templates, the following occurs:
  - An empty "Valid from" date for responsibility assignment results if one of the account templates being merged has an empty "Valid from" date for responsibility assignment.
  - An empty "Valid to" date for responsibility assignment results if one of the account templates being merged has an empty "Valid to" date for responsibility assignment.
- The "Effective From" and "Effective To" dates have changed from capability attributes to non-capability attributes.
- The "Effective From" date has changed from required to optional.
- If the "Effective From" date attribute is empty during account creation, this field uses the current date.
- During account modification, an empty "Effective From" date is ignored.

r12.5 SP11

Upgrade Minimizes the Chance of Undoing Customizations (see page 71)

Workflow Change for Reverse Synchronization (see page 71)

Upgrade Minimizes the Chance of Undoing Customizations

If you are upgrading from an r12.5 release, upgrading to this release has fewer chances to undo your customizations to role definition objects such as tasks, roles, and screens. For details, see the Post-Configuration chapter of the *Upgrade Guide*.

Workflow Change for Reverse Synchronization

When a reverse synchronization policy exists, the workflow should request approval from the manager of the CA Identity Manager user. However, when making a change to an endpoint account, the primary object of the workflow is the endpoint account, not the CA Identity Manager user who holds the account. To address this problem, workflow screens have a new checkbox to request approval based on the CA Identity Manager user.

The Dynamic Resolver and Match Attribute Resolver screens include a checkbox when you select an account object such as an Active Directory or Arcot account. The checkbox is labeled User Associated with this account. *S*electing this checkbo*x* updates the User or Object Attributes field and the resolver works with the attributes for the CA Identity Manager user not the endpoint account.

r12.5 SP10

Scoping for Tasks that Manage Admin and Access Roles (see page 72)

Arcot Connector Changes (see page 72)

Scoping for Tasks that Manage Admin and Access Roles

Role scoping is now implemented in tasks that manage admin and access roles. If you need this scoping feature in an environment, you add a new user-defined property and set scoping rules in the tasks.

Follow these steps:

1. In the Management Console, select the environment.
2. Click Advanced Settings, Miscellaneous.
3. Add the user-defined property EnableScope with the value AdminAccessRole.
4. Modify any role management task that needs this scoping.

   On the search tab, enable the All Admin/Access Roles search option.
5. Modify the role being managed to specify role scope in the member policies. For example, the AdminRole Manager role must include scope rules in member policies to define which admin roles can be managed by role members.

Arcot Connector Changes

In this release, the Arcot Connector has the following changes:

- Removal of Generate Arcot User ArcotID and Generate Arcot User QnA from the admin tasks
- Change of Role Definition Generator to support reading a custom admin role definition
- Addition of Generate My ArcotID, Download My ArcotID and Generate My Arcot QnA for self service tasks
- Addition of custom tab to support Download My ArcotID task

r12.5 SP9

Provisioning Role Names with Brackets (see page 72)

Provisioning Role Names with Brackets

When you use a View or Modify task, the Provisioning Roles tab now correctly displays any provisioning role name that contains a bracket character (either open '[' or close ']')

r12.5 SP8

This section contains the following topics:

Global Workflow Supports Additional Events

In previous versions of CA Identity Manager, only events generated by a tab could be associated with a workflow process.

You can now associate global policy-based and non policy-based workflow with events generated outside of tabs for a given task. CA Identity Manager generates these events using functionality, such as identity policies and Policy Xpress.

Suggest Role Audit Types Removed

The following audit types were removed from the suggest role feature of CA Identity Manager:

- Matched Privileges
- Almost Has

Out of Pattern Analytics Removed

Out of Pattern analytics were removed from the suggest role feature of CA Identity Manager.

Compliance Checks for Approval Tasks not Supported

Checking compliance when validating changes for an approval task is not supported in this release.

r12.5 SP7

This section contains the following topics:

Changes to User Console and Management Console URLs

In this release, the base URLs for the User Console and Management Console have changed, as described in the following table:

Component	New URL	Old URL
User Console	http://*hostname:port*/iam/im/*alias*	http://*hostname:port*/idm/*alias*
Management Console	http://*hostname:port*/iam/immanage	http://*hostname:port*/idmmanage

IdentityMinder.ear is now iam_im.ear

The IdentityMinder.ear file has been renamed for this release. The new name is iam_im.ear. This file is created by the installation or upgrade of this release.

New Date Picker Control

CA Identity Manager includes a new date picker control. You can add this control in lists and profile screens.

The complete list of Java date formats appears in the documentation for Java™ 2 Platform Std. Ed. v1.4.2 at the Oracle website (http://java.sun.com/j2se/1.4.2/docs). Search for SimpleDateFormat.

The date picker control supports a *subset* of the Java date formats. It *excludes* the following formats that are supported in the SimpleDateFormat:

Symbol	Meaning	Type	Example
G	Era	Text	"GG" -> "AD"
D	Day in year (1-365 or 1-364)	Number	"D" -> "65" "D" ->"065"
W	Week in month (1-5)	Number	"W" -> "3"
K	Hour (0-11 AM/PM)	Number	"K" -> "15" "KK"->"15"
S	Millisecond (0-999)	Number	"SSS" -> "007"

Note: The date picker tool supports only a 24 hour time format.

Scoped Searches for Provisioning Roles

CA Identity Manager now includes support for scoped searches for provisioning roles. Admin roles that include tasks that operate on provisioning roles must include a scope rule if the one of the following options is set on the Search tab for those tasks:

- All provisioning roles for which the user is an administrator
- All provisioning roles for which the user is an owner

If a scope rule is not defined for provisioning role objects, no roles are returned in the search results.

r12.5 SP6

This section contains the following topics:

Configure GINA Clients to Accept Only Valid SSL Certificates (see page 76)

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:

UNIX Remote Agent Works on Solaris Zones (see page 76)

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.

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.

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>)
   ```

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".

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 *User Console online help*.

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 CA 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.

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:

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 CA Identity Manager objects used to generate a Report on endpoint accounts.

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 CA 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 CA Identity Manager object store database as a data source for generating reports, due to performance reasons.

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 CA Identity Manager to including 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 iam_im.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 SP15.

  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 CA 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 CA 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.

Co-installation of Unix Remote Agents with Additional CA Products

In CA Identity Manager r12.5 SP15, the UNIX Remote Agents (with the exception of TRU64 platforms) are now installed so that the shared software components are tracked by the installer software. This allows co-installation with additional CA products such as CA ITCM.

However, when an earlier version of the UNIX Remote Agent is upgraded, for example, if you are upgrading from CA Identity Manager r12.5 SP9 to CA Identity Manager r12.5 SP15, the new tracking method will not update the reference counts of those packages which the agent is depending on. In such case, if you wish to uninstall the product after this upgrade, please use the de-install file: <install-dir>/scripts/uninstall-force.sh

Note: Make sure that the uninstall-force.sh is not used on hosts that have additional CA software installed. These products may depend on those same software packages which this script removes.

Deprecated and Dropped Components

Certain components are being deprecated, which means they will not be supported in future releases. Other components are dropped, meaning they are no longer shipped with the product or no longer tested with the product. These components are listed in the CA Identity Manager Deprecation Policy on CA Support.

Application Server Support

A prerequisite to installation of CA Identity Manager is to have support from your application server vendor or professional consultants. The vendor or consultants can provide answers to questions about installation and configuration of single node and cluster deployments.

32-bit and 64-Bit Application Servers

CA Identity Manager r12.5 SP15 supports the following 64-bit application server versions:

- JBoss 5.0 and 5.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0

CA Identity Manager r12.5 SP15 supports the following 32-bit application servers:

- JBoss 5.0 and 5.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 10.3
- IBM WebSphere 6.1 and 7.0

If you intend to remain on a 32-bit application server, you can upgrade to r12.5 SP15 by running the installer. To upgrade to r12.5 SP15 and move to a 64-bit application server, you first install the new application server. Then, you migrate data from the previous CA Identity Manager installation. See the *Upgrade Guide* for full details.

Note: Although we support installation of CA Identity Manager on 32-bit platforms, we strongly recommend a 64-bit platform. It has benefits for performance, operation, and future upgrades. The next major release of CA Identity Manager, r12.6, supports only 64-bit platforms.

Error/Warning Messages in the Deprecated Connectors

When using a deprecated connector such as the UPO Connector, the Accounts tab in CA Identity Manager fails to fetch all the UPO Connector accounts. The CA Identity Manager Server log displays the following error messages:

- ERROR [translator] The attribute cn in the corporate directory is required. A provisioning attribute should be mapped to it to ensure proper inbound synchronization.
- WARN [translator] Notification referenced endpoint type not supported in JIAM API: Option 'Universal Provisioning' is not supported because No metadata on namespace Universal Provisioning
- WARN [translator] Notification referenced endpoint type not supported in JIAM API: Option 'Universal Provisioning' is not supported because Failed to load

Note: The log errors occur with the deprecated connectors because the metadata for the endpoints is unavailable.

Oracle 11g R2 RAC as User Store and Object Store

When using Oracle 11g R2 RAC as a User store and a Runtime store, perform the following to use the Cluster capabilities of an Oracle database cluster:

- Use SCAN (Single Client Access Name) while you install CA Identity Manager with Oracle 11g R2 RAC.
- Create the database *tablespace* on the shared disk group while creating a tablespace.

Oracle 11g R2 RAC as a DYN (JDBC) Endpoint

To connect to an Oracle RAC service when creating a data source in Connector Xpress, select the Edit checkbox and type the JDBC URL. The URL form is as follows:

```
jdbc:oracle:thin:@(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = hostname1)(PORT = 1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = hostname2)(PORT = 1521))
(LOAD_BALANCE = yes)
(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = servicename))
)
```

AD LDS as a User Store

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

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.

Linux: Provisioning Directory Installation

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*

Linux 64-bit: UNIX Remote Agent Installation

Before you plan to install the CA Identity Manager UNIX Remote Agent on a Red Hat Linux 64-bit system, install the 32-bit packages using the following commands:

```
yum install glibc.i686
yum install libX11.i686
yum install libxcb.i686
yum install libXtst.i686
yum install libXau.i686
yum install libXi.i686
yum install libXext.i686
yum install libgcc.i686
yum install compat-libstdc++-33.i686
yum install ncurses-devel.i686
```

Note: The i686 suffix specifies that the library is 32-bit for the x86 processor. By default, the Only Native Packages filter option is selected under Add or Remove Software. You can also install the i686 architecture dependencies by clearing the Only Native Packages filter option under Add or Remove Software.

Linux 64-bit: SiteMinder Connectivity Errors

Symptom:

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

Solution:

Perform these steps *before* deploying any directory or environment.

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

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

2. Open the SiteMinder 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 no policy server connectivity issues appear. For example, look for a line such as following with no exceptions:

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

CA Identity Manager EAR does not Auto-Deploy with WebLogic

If you are using WebLogic 9 or 10 in production mode, the CA 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 iam_im.ear manually from the user_projects\applications folder.

Work Around Firewall on Windows 2008 SP2

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

To work around this problem, add port exceptions or disable the Windows firewall to access distributed CA Identity Manager components in Windows 2008 SP2 deployments.

Deploy JSP Pages for Administrator Actions

The CA Identity Manager Server includes sample JSP pages for performing the following actions:

- Ping the application server
- List deployed BLTHs
- List information about object types and managed object providers
- List plugin information
- Change logging levels

The JSP pages are installed in this location:

admin_tools\samples\admin

The folder contains a readme.txt file with instructions for using the JSP pages.

Note: You will see a 404 error if you use these JSP pages without following the instructions in the readme.txt file.

Improve Performance on WebSphere and AIX

For a WebSphere installation on AIX, you can achieve better performance in the User Console by setting the maximum heap size.

Follow these steps:

1. Locate the server.xml in the following location:
   `WAS_HOME/profiles/Profile/config/cells/Cell/nodes/Node/servers/Server`
2. Add maximumHeapSize="1000" to the jvmEntries element.

   You can use a higher value if necessary. For example, to set maximumHeapSize to 2 GB (2048 MB), you add it as shown in bold in the following excerpt from this file:

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments=""
debugMode="false"
debugArgs="-agentlib:jdwp=transport=dt_socket,server=y,suspend=
n,address=7777" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Ignore WebSphere 7/Oracle Error

When CA Identity Manager is installed using an Oracle runtime store and the WebSphere 7 default JRE, the following error appears in the CA Identity Manager logs.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server.

This error can be ignored.

SDK for C++ Connectors and JIAM

You can download a Software Development Kit (SDK) that supports legacy components. You use the Provisioning Server SDK to develop applications for managing C++ connectors. This kit also includes the JIAM SDK. JIAM is a Java interface to the Provisioning Server. To obtain this kit, go to CA support. In the CA Identity Manager r12.5 area, download the Legacy Components.

Chapter 4: Upgrade Considerations

This section contains the following topics:

Upgrade Active Directory Role Definition

The Active Directory Role definition file is upgraded to version 1.08.

Note: Ensure that you use the upgraded file. If the existing CA Identity Manager environment uses the earlier releases of the Active Directory Role definition file, reimport the file to upgrade to 1.08.

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 SP15:

- CA Identity Manager r12
- CA Identity Manager r12 with Option Pack 1
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SP 1 through SP6

  If you have a pre-r12 version of CA Identity Manager, first upgrade to one of the above versions, then upgrade to CA Identity Manager r12.5 SP15. The above versions of CA Identity Manager include the imsconfig tool, which is required to upgrade a pre-r12 version.
- CA Identity Manager r12.5 SP7 or higher

Note: Upgrades from ACE to r12.5 SP15 are *not* supported. Also, cross-platform upgrades (between UNIX and Windows) are not supported.

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 SP15 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 SP15 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 SP15 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*

Environment Migration Error

Symptom:

If you are upgrading from CA Identity Manager 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".

Solution:

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

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.

Credential Provider Internal Error

Symptom:

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

Solution:

No action is required. If no other errors were issued, the upgrade process 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 85), 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.

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 SP15. All Fixed Issues (see page 143) are in a separate chapter.

This section contains the following topics:

General

The following are general known issues in CA Identity Manager r12.5 SP15.

Enable the Fix for Oracle Bug 6376915

The Oracle bug 6376915 causes high water (HW) enqueue contention when the database is busy handling large objects (LOB) and the database is configured to use automatic segments space management (ASSM).

This bug causes performance and scalability problems with CA software, including CA Identity Manager and CA CloudMinder.

The fix for this problem introduces a mandatory event. Set this new event to make the ASSM architecture allocate LOB chunks more efficiently.

This bug was introduced in Oracle 10.2.0.3. It was fixed in both Oracle 10.2.0.4 and Oracle 11.1.0.7. However, the fix is not enabled by default.

The steps in this procedure assume that spfile is used for configuration.

Follow these steps:

1. Enter the following command:

   ```
   ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL
   1024' scope=spfile;
   ```

2. Restart the database.
3. To test the fix, use the following measures:
   - Use Bulk Loader to measure the task throughput in CA Identity Manager and CA CloudMinder.
   - Measure the wait time for HW enqueue contention.

Unable to Access CA Identity Manager User Console

Symptom:

After integrating CA SiteMinder r12.0 SP3 CR9 with CA Identity Manager using an IIS 7 SiteMinder Web Agent, I do not get a prompt for authentication or view the tabs when accessing the CA Identity Manager User Console.

Solution:

Reconfigure the IIS 7 agents from *Integrated* to *Classic* mode.

Important! The SiteMinder Agent must be higher than the application server plug-ins in the ISAPI Filters priority list.

setpasswd Fails on 64-bit Linux Systems

Symptom:

On Linux 64-bit and Solaris systems, setpasswd fails with this error:
`"/opt/CA/SharedComponents/csutils/bin/expect: error while loading shared libraries: libtcl8.4.so: cannot open shared object file: No such file or directory"`

Solution:

Set LD_LIBRARY_PATH to the following value:

/opt/CA/SharedComponents/csutils/lib/tcl8.4

setpasswd no longer generates this error.

Out of Memory Error in 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.

No warning when Group search limit is exceeded

When CA Directory r12.0 SP8 is the CA Identity Manager User Store, as distributed with CA Identity Manager r12.5 SP15, search results that include Group objects may be missing a warning. If the paging size (the pagesize attribute in the directory.xml) exceeds the CA Directory search limit (max-op-size configuration attribute), no warning appears. However, search results are valid. This issue will be addressed in a Service Pack release in the near future.

Workflow Participant Resolver Fails for EnableUserEventRoles

Symptom:

When you attempt to change workflow settings for the task, you may see this message:
`Cannot set "Primary object of this task" in the {0} Resolver Description section for the multi select task".`

Solution:

Go to the workflow page and change the approver to "Object associated with the event."

Duplicate name in View Submitted Tasks

Symptom:

In some heavy-load high availability environment, the CA Identity Manager server may send concurrent requests to the Provisioning Server and introduce race conditions in the Provisioning Server when handling parallel modification requests on same Global User.

Solution:

Change the following Provisioning Manager setting to No and restart the Provisioning Server.
`Identity Manager Server/Allow Concurrent Modification on Same Global User`

Note: If there is Program Exit accessing Global Users, leave this parameter set to Yes.

Not Found Error When Creating a New Environment

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 that Tab Already Exists when Importing a Role Definition File

Symptom:

I generated User Console account screens with Connector Xpress. When I imported the role definition file into an enviroment, I got an error message advising me that another tab with the same name exists.

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.

Modifying Single Valued Compound Attributes in CA 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.

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.

Limitations of Bulk loader in Relationship Attribute Level

Bulk loader cannot update the task operations on the user objects in the relationship attribute level.

- Relationship attributes that are not updated by Bulk Loader are Users Access roles, Users admin roles, Users Provisioning Roles, Users group membership, and Groups group.
- Relationship attributes that would get overwritten when you replace old attribute values with new attribute values from the bulk loader file are Groups Administrators, and Custom or default Multi-valued attribute.

Error Creating Provisioning-Enabled Environment using Tokenized Template

In this case, CA Identity Manager cannot assign the Provisioning Synchronization Manager role to the inbound administrator defined in the Environment creation wizard.

If the environment template has tokens or translated strings for the Provisioning Synchronization Manager role name, the search fails and a NoSuchObjectException is thrown.

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.

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.

CA Identity Manager on JBoss does not Reconnect to Oracle

Symptom:

When using JBoss 5.x with an Oracle Database datasource and upgrading CA Identity Manager from an r12.5 release, an application outage occurs if the database server is restarted. The outage is caused by JBoss replacing the property background-validation-minutes with background-validation-millis.

Solution:

To resolve this issue, perform the following steps:

1. Stop the application server.
2. Open the data source files located in */jboss folder/server/default [or server name in cluster]/deploy* and delete the following line:

   <background-validation-minutes> </background-validation-minutes>
3. Add the following line:

   <background-validation-millis>120000</background-validation-millis>

   Note: 120000 is the equivalent of 2 minutes previously specified by default for background-validation-minutes. Configure the value according to the business requirements.
4. Restart the application server.

Note: The issue does not affect a new installation of CA Identity Manager.

Reporting

The following issues are related to reporting in CA Identity Manager r12.5 SP15.

User Filter Search is Case Sensitive in the User Accounts and the Endpoint Accounts Custom Snapshots XML Files

Symptom:

When creating a filter on %USER_ID% in both the *useraccounts* export elements in *UserAccounts* and *Endpoint Accounts* custom snapshots xml file, the report does not display the results although the user exists.

Solution:

The filter search is case sensitive.

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.

Note: ExportAll.xml is moved from the Standard templates folder to the following file location::

```
C:\Program Files\CA\Identity Manager\IAM Suite\Identity
Manager\tools\samples\SnapshotExport
```

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).

General Provisioning

The following issues are general provisioning issues in CA Identity Manager r12.5 SP15.

Renaming Provisioning Roles not Supported

The renaming of provisioning roles after they are created is not supported.

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 CA 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, CA Identity Manager attempts to create a corresponding user in the CA Identity Manager user store. Errors occur and the Create User task fails in the CA 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 got an error message advising me that the associated accounts creation or update that failed after this procedure:

1. I deployed a JNDI project that was created with Connector Xpress in a version earlier than CA Identity Manager 12.5.
2. I then executed an explore and correlate task.
3. I created an account template and added two association attributes, for example, manager.
4. I created a provisioning role that is based on the account template, and assigned the provisioning role to the user.

Solution:

CA Identity Manager r12.5 SP15 does not support JNDI projects that were created with Connector Xpress in a version earlier than CA Identity Manager 12.5 using association-type attributes.

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

CA SiteMinder Login Name Restriction for Global User Name

If a user is required to log in to the CA SiteMinder Policy Server, the following characters or character strings cannot be part of a global user name:

&
*
:
()

Workaround

Avoid using these characters in the global user name.

Some WebSphere 6.1 Nodes May be Missing Objects

On a WebSphere 6.1 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 6.1 documentation on Connecting Applications on the Service Integration Bus.

Java Connector Server and Connector Xpress

The following issues are related to the Java Connector Server and Connector Xpress.

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.

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 SP15.

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 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.

Error in Endpoint Search Screens After Upgrading from 12.5 SP6 or Earlier

Symptom:

An error that resembles the following message occurs when you import endpoint role definitions files from r12.5 SP6 or earlier into r12.5 SP7 or later:

"Error in screen definition "Default Endpoint Type Primary Group Endpoint Capability Search" with tag "DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch" Error: The type "UNKNOWN" is not a valid object type."

In CA Identity Manager r12.5 SP7, certain objects were renamed. These objects are referenced in endpoint capability search screens. After you upgrade to r12.5 SP7 or later, an error can occur when you import role definitions files that include screens which reference the old object names.

This issue has been identified in Active Directory and CA Access Control endpoints.

Consider the following Active Directory endpoint example:

In CA Identity Manager r12.5 SP6, the Active Directory endpoint capability search screen name referenced the object ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP'.

The object name appears in the following screen definition:

```
<Screen name="Default Active Directory Primary Group Endpoint
Capability Search"
tag="DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

Object="ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP">
```

In CA Identity Manager r12.5 SP7, the object name was changed to 'ACTIVEDIRECTORY_ETADSGROUP'.

The new object name appears in the following screen definition:

```
<Screen name="Default Active Directory Group Endpoint Capability
Search"

tag="DefaultActiveDirectoryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

object="ACTIVEDIRECTORY_ETADSGROUP">
```

Solution:

Consider deleting screen definitions that reference the old object name before importing a role definitions file.

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

Symptom:

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

Solution:

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.

Access Control Connector

The following sections describe the known issues for the Access Control connector:

CA Access Control Connector Character Limitations

A limitation exists in the way the CA Access Control connector communicates with the CA Access Control endpoint. As a result, the CA Access Control connector cannot create or retrieve users and groups with the following characters in their names:

* ? " '

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 connector problem with CA LDAP r12

Symptom:

CA LDAP r12 does not correctly escape the comma character in RDN values. When the endpoint is explored, an error similar to the following exists in the etatrans log:

```
CA ACF2 Rule Key 'UNKNOWN'
```

This problem does not occur when CA LDAP r14 is installed on the enpdoint system.

Solution:

Install CA LDAP r14.

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 Remote Agent 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 CA 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, CA 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, CA 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.

No Such Attribute Error When Setting Is Master Attribute

Symptom:

I selected the Is Master attribute on the Live Communications Server tab in the CA Identity Manager User Console and received a No Such Attribute Error.

Solution:

The endpoint is using Office Communication Server. The attribute is not supported on endpoints using Office Communication Server. The attribute is only supported on endpoints using Live Communication Server.

CA Arcot Connector

The following sections describe the known issues for the CA Arcot connector:

Error When Adding Arcot Organization

Symptom:

I have an Arcot endpoint with one organization specified. I tried to remove the organization and add a new organization using the Modify Arcot Endpoint screen and received an error.

Solution:

To resolve, do the following:

1. On the Modify Arcot Endpoint screen, add the new organization to the Arcot Organizations field and click Submit.

   CA Identity Manager adds the organization to the Arcot endpoint.

2. On the Modify Arcot Endpoint screen, in Arcot Organizations field, remove the organization you do not want, then click Submit.

   CA Identity Manager removes the organization from the Arcot endpoint.

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 CA 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:

Unable to Save a Date Datatype due to Data Type Mismatch

Symptom:

When I set date type attribute on a DB2 endpoint (JDBC DB2 for IBM i), the following error is displayed:

```
Bad SQL Grammar: Data type mismatch. (YYYY-MM-DD)
```

Solution:

Edit the Connection URI on the endpoint page in Provisioning Manager and add *date format=iso*. The final URI appear as:*jdbc:as400://<host>:CA Portal/<db>;prompt=false;date format=iso;*. Note the spacing between *date* and *format*.

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 E2K7 Mailbox

An error message is displayed when you try to modify an account with an E2K7 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—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 Connector Server

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, 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 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 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:

Cannot View ACL Properties on LND Endpoint when Creating Mailbox Using Create Background Task

Symptom:

I created an LND mailbox by using the Create Background Task option on the Lotus Notes/Domino Connector Mail Tab. When I tried to view the ACL properties of the mailbox on the LND endpoint, I got the error message *You are not authorized to access that database.*

Solution:

You cannot view the properties of an ACL mailbox on an LND endpoint if you create a mailbox using the Create Background Task with the LND Connector.

If you create a mailbox using the Create Mailbox Now option, you can view the ACL properties of a mailbox on a LND endpoint.

Create LND Account Fails in Provisioning Manager When specifying that ID file is Stored on a Computer other than the LND Server

Symptom:

I tried to create an LND account and selected the User ID File Path check box on the User ID Tab and specified a UNC path to store the ID file for the user. The location I specified was on a computer other than the LND server.

The account creation failed with the error message *Failed to create archive document for user.*
On the LND endpoint, the account is created in notes.nsf. In the Archive DB on the endpoint, the path I entered in the User ID File Path' field is appended in the entry for the user, but the ID file is not attached.

Solution:

This issue occurs in the CA Identity Manager User Console and the Provisioning Manager. There is a limitation in the LND API for support of UNC file paths when specifying a location for the ID file other than the LND server.

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.

PeopleSoft

The following sections describe the known issues for the PeopleSoft connector.

Searches May Fail in Provisioning Manager

When you use the Provisioning Manager to search for a PeopleSoft endpoint with PeopleTools 8.49, the search for PPS Users for assignment to the "Alternate User ID", "Supervising User ID" and "Reassign Work To" fields does not return results in some cases.

There are two workarounds for this issue:

- Use the CA Identity Manager User Console to manage PeopleSoft endpoints (preferred)
- Enter the value in the Provisioning Manager fields without performing any searches. The value is still be subject to validation, such that if the entered value is not a PPS User, the assignment will fail upon clicking the “Apply” button.

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:

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 provisioning directory provisioning directory installer if the original provisioning directory installer is older than R12 CR8 after the upgrade.

To update the provisioning directory 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 CA 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.

RSA SSL Considerations

The RSA 7 connector uses RSA 7 SDK to communicate with RSA 7 endpoints. The RSA 7 SDK uses its own SSL implementation and key store. This changes the SSL behavior of JCS and causes other connectors to fail when SSL is used. For example, connection issues are found when running RSA7 connector with Google Apps connector when using SSL and a Proxy.

So, we recommend using the RSA 7 connector in its own JCS in such scenario.

Salesforce.com

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

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:

Installation of ETC Remote Agent on Linux 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 SP15

CA Identity Manager r12.5 SP15 includes the following fixed issues:

Support Ticket	Problem Reported
20509384/01 20509384/02	Policy Xpress Policies errors if multiple accounts on the same endpoint have the same name.
20589598/04	ADS user accounts don't display properly in Provisioning Manager.
20679358/01	Create XML directory fails with "postCreate" error message.
20820206/02	When changing the password in CA Identity Manager integrated with Siteminder, system prompts to add a white list of allowed URL redirects.
20842853/01	A warning message appears when using any task which has renamed search screens in Provisioning Roles Tab.
20865718/01	Provisioning server process hangs up on a rare condition because of large number of ETC endpoint accounts.
20924613/01	When assigning a group in the "memberof" tab of one account, it is changing the case of the container path in the group DN.

Support Ticket	Problem Reported
20932990/01	When searching for an endpoint, the description of Windows NT Endpoints is not found.
20940315/01	Error occurs when adding additional TSS Profiles to TSS Acid.
20940489/02	Error occurs when executing a workflow on reverse synchronization detection.
20991385/01	Deleting multiple users fails when using "Delete User" task.
20999896/03	Workflow worklist was not completely localized.
21009587/01	Explore of eDir causes Provisioning Server to crash when the memory usage exceeds 2GB limit.
21011911/01	CAFT crashes when trying to acquire a VMS endpoint.
21014908/01	Errors occur when an account template with resource links is modified and exported back to CA Identity Manager, resulting in unintended removal of Oracle Apps responsibilities.
21017231/01	"View My Submitted Tasks" is not working for users with a comma and/or a slash character in their %USER_ID%.
21021863/01	Error occurs when selecting a particular user in the Auditing Password Reset Report.
21024493/03	Poor performance AD Group removal in Policy Xpress.
21031482/01	Update calls via TEWS fails with an error if a target attribute contains one or more "|" (vertical bar) characters.
21034012/01	CA Identity Manager is not decoding the target URL correctly in Password Services process when SiteMinder is integrated.
21045899/01	A self- service account (e.g. RACF) password reset from CA Identity Manager user console is processed as an administrative change was not resetting the RACF password again (since it is pre-expired).
21049286/01	From Provisioning Manager, the "Change Endpoint's Account Templates" wizard does not retrieve any endpoints for a Dynamic Endpoint Type.
21050002/01	Connector Xpress errors occurred with normalizing data across multiple database (i.e., SQL and Oracle) maintain string values in different formats.
21057794/02	When uninstalling Unix Remote Agent, /etc/profile.CA.file is inaccurately deleted. This file is also used for other CA product such as ITCM.
21062873/02	Cleanup Submitted Task fails with an error message "String or binary data would be truncated".

Support Ticket	Problem Reported
21062881/01	Discrepancy in the runtimeStatusDetail12.descriptionParam column size between the Task Persistence and Archive databases (archive_runtimeStatusDetail12.descriptionParam): 1024 vs. 255.
21068903/01	If disc space is full and CA CloudMinder agent backs up the /etc/passwd, the password is initialized to a size of 0 (zero).
21069654/01	AXIS2 web services client errors occur with attempting to generate WSDL.
21070317/01	Synchronization of eTACFStoreACF2Rules is causing an inaccurate value to be written to ACF2.
21070932/01	The backslash character is not displayed in search results for group search screen.
21071316/01	Some Oracle roles are missing in Provisioning Manager.
21076345/01	Challenge questions and answers cannot be repeated unless they are in a different case.
21078275/01	Intermittent errors during SAP role assignments.
21085098/02	User accounts are disabled when a password change is processed.
21086705/01	Call ModifyUser(-Tab)/-ProvisioningRolesSearch method from CA Identity Manager Web Services (TEWS) works on Java but not in .NET (C#).
21092886/01	SDKWS template generated connector missing Endpoint Settings and Attribute Mapping tabs on endpoint in CA Identity Manager User Console.
21094823/01	Performance delays when running AD UserAccounts snapshot during report generation.
21100138/01	Resource removal from account template does not remove endpoint account.
21100138/02	Need to continue synchronization when individual account failures are encountered for specific Account Template resources.
21100138/03	Modify Endpoint Account Template Task does not trigger Account Synchronization when "Account Synchronization [on every event]" is enabled on the task.
21100138/04	CA Identity Manager does not support the SyncRemoveValues feature on eTFNDResponsibilityList attribute on FND account template.
21100411/01	Suspending SQL 2008 login accounts via "Modify Endpoint Accounts" task is not functioning properly.
21102376/01	Class Cast Exception occurring when utilizing TEWS.

Support Ticket	Problem Reported
21108497/01	CA Identity Manager TEWS response does not match exactly the generated WSDL.
21109376/02	Handling recursive Admin Role policy member rule created errors..
21118739/01	Localization support needed for TEWS.
21118746/01	Unable to run Policy Xpress located on Linux systems.
21121709/01	Errors occur during WSDL generation for .NET (C#) array references.
21125319/01	Resources are missing after completing RCM Import.
21125755/01	When saving a CA Identity Manager Report as a PDF, Japanese characters are not displayed properly.
21128259/01	Attribute level encryption was not working properly in all cases.
21129376/01	For the UNIX Remote Agent (Linux), the UID number was being changed when a user was added to a group.
21131191/01	During a TSS endpoint explore operation caused the deletion of all accounts from CA Identity Manager (when the TSS endpoint is manually updated outside of CA Identity Manager).
21131890/01	Several search filters are not handled properly by the TEWS filtering code.
21142156/01	Global ID for GLOBAL authentication in Oracle Account Template (eTORAExternalName) is too short for DN notation.
21143073/01	Forgot Password task is not initiated when Forgot Password link is used.
21143108/01	On workflow approval task with Read/Write Required fields, validation is not performed when task is rejected.
21152109/01	Slow performance during resolution of Admin Tasks via TEWS requests.
21152694/01	SAP Account Template Sync adding duplicate eTSAPAcctRole values.
21154505/01	CA LDAP errors during explore operation, causing the deletion of all RACF objects in CA Identity Manager.
21155926/01	Error when generating a report "Failed to retrieve data from the database".
21156189/01	Endpoint accounts not suspended when Password Reset task's failed attempt limit is exceeded.
21169574/01	Public Task does not use resource bundle.
21169862/01	Email in the ADS account does not match the primary address of the corresponding mailbox.

Support Ticket	Problem Reported
21171723/01	Error occurs when Orphan Accounts report is requested on customer's snapshot data.
21171874/03	Provisioning C++ Connector Server crashes when it attempts to free the MOTD buffer.
21172551/01	Active Directory groups are shown in search results when searched in Provisioning Manager and not in CA Identity Manager User Console.
21172898/01	The WSDL returned by TEWS is not valid after adding "View RACF Account" task.
21175775/01	When duplicating the AD account template from Provisioning Manager, errors displayed in "etatrans.log" log file and there is a delay observed in displaying account template configuration.
21176254/01	Archived tasks via TEWS are not available.
21176449/02	Very slow performance of application during bulk load operations.
21180850/01	Exploring the ECI group corporate LND Endpoint which contains a large number of objects (10,000 or more) is requiring excessive time.
21182100/02	SAP endpoint SNC Name is propagated as "0" rather than "" (blank value) when provisioning a global user using a role/template.
21182100/03	There is no support for the number format "1.234.567,89".
21191457/01	Bulkloader truncates right square bracket in records preview.
21191840/01	View submitted tasks showing tasks performed by users who no long exist in the organization.
21193349/01	Application server log shows errors when JMS DB does not respond to TP updates.
21196771/01	Fail to use the DYN schema to define cached account attributes.
21196867/01	Additional support is needed for search capability on ViewSubmittedTasks when accessed via TEWS. When selecting the ViewSubmitted Tasks by status using TEWS, status field always returns all tasks instead of the selected value.
21201799/01	Vulnerabilities detected in the use of TEWS6Servlet and ETACallBack servlets.
21201958/01	Inappropriate access granted to a workstation from the Forgotten Password GINA link.
21211349/01	Vulnerability: Stack trace showing internal code class names.
21214735/01	Performance degradation when adding a user to large ADS groups through the Policy Xpress.

Support Ticket	Problem Reported
21217449/01	Performance issue when "Explore endpoint for manage object" is run for a newly acquired Lotus Notes endpoint.
21221317/01	Policy Xpress error messages do not utilize localization.
21233631/01	Provisioning Role is removed when user is synchronized with Identity Policy even though the removal condition is not met.
21241009/01	Hiding the profile tab causes task not to save changes - Modify Email Task.
21244904/02	Required supporting more than 32 Characters on the global user attribute.
21246478/01	Modifying Bulk Load Execution details launch the actual task (out of schedule).
21255901/01	"eTTSSPolicy-Profiles: value #0 invalid per syntax" error message is displayed when attempting to modify TSS profile of an account.
21265595/01	Modifying the limit in LdapUtil.setDefensiveLimits(searchControls).

Fixed Issues in r12.5 SP14

CA Identity Manager r12.5 SP14 includes the following fixed issues:

Support Ticket	Problem Reported
20289041/01	The CA Identity Manager documentation on the permission for test_sync binary where the root user can only run is not updated.
20416951/01	The CA Identity Manager documentation on creating a CA Identity Manager Directory or Environment with CA SiteMinder integration is missing.
20469040/01	In the CA Identity Manager Provisioning Guide, information about Modes of Batch Request in the Sample SPML Requests is missing.
20474149/01	Unable to set the default values for a screen logical attribute when creating tasks.
20489955/01	The CA Identity Manager documentation on Manual EAR Deployment on the WebSphere Application Server is not updated.
20512235/01	The CA Identity Manager documentation about Synchronize Oracle Accounts with Account Template using the Provisioning Manager is not updated.

Support Ticket	Problem Reported
20576212/01	Provisioning Server terminates as the socket is closed due to excess select() errors.
20590108/02	Windows 2008 Core does not support as a CA Identity Manager Endpoint.
20619869/01	Access to the administrator user interface is granted even if the user account is locked out.
20638898/03	Unable to set a rule string in a template with an account integer field from a compound class.
20644079/01	When configuring CA Identity Manager with WebSphere Application Server 6.1, Out of Memory errors appear in the CA Identity Manager logs.
20657195/01	Error appears on the endpoint search screens after upgrading from 12.5 SP6 or earlier.
20666551/04	Config Xpress Screen does not show task associations in the Provisioning Manager.
20679358/01	The CA Identity Manager JDBC layer is unable to search for Universally Unique Identifier on an Oracle directory with a string UUID.
20686889/01	The *OPERATION* runtime context value for Connector Xpress JDBC Operation Binding is missing.
20696990/02	When generating accounts details report using default snapshot XML, the provisioning role members are not displayed though the members are available.
20742308/17 20935118/01 20910627/06	When capturing snapshot, case mismatch makes the snapshot process overlook the account information.
20743672/02	The maximum length of the eTDepartment attribute is increased to 100 characters.
20747494/02	Credential Provider does not support Windows Server 2008 R2 SP1.
20751640/01	When an environment is configured to provisioning users to several SQL Server 2005 Servers, arithmetic overflow error for data type smallint is displayed.
20762960/01	When you view a role member report that is requested from a capture snapshot based on the Provided RolememersReportSnapshot.xml file, an empty report is displayed.
20772901/01	Policy Xpress on the deleteuserevent fails to execute because the user with a Policy Xpress stamp is not updated.

Support Ticket	Problem Reported
20774505/02	CA Identity Manager waits for a minute to connect to the workflow server even though the workflow is disabled.
20775149/01	In the CA Identity Manager View Submitted Task, the Create User task is shown as audited instead of completed failing to submit the last operation text.
20780302/01	When executing the Modify My Endpoint Account task and View My Endpoint Account task for ACF2 accounts, com.ca.iam.model.IAMHandle cannot be cast to java.util.Collection error is displayed.
20781315/02	When using long names for the User ID, alignment issues appear in the Role Owners report.
20786300/01	When multiple users are added to the Provisioning role in a single task, the JBoss application server does not respond or crashes. To fix this issue, JBOSS_HOME\server\default\deploy\iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml run time configuration file has been modified.
20787858/01	Unable to set a password containing double quote on an ACC endpoint account.
20795369/02	When LDAP 389 port is blocked, the search results fail to fetch Primary Group Distinguished Name in the ADS connector.
20795391/01 20781187/01 20848077/01 20825437/01 20888111/01 20887387/01 20899097/01	Cleanup Submitted Tasks fails with specific tasks or categories with a primary key violation error message.
20795855/01	Inconsistencies are encountered when modifying the Unix account from the User Console and from the Provisioning Manager.
20797153/01	Creating LND accounts fails because the validation of mail template fails.
20797848/01	C++ Connector Server (CCS) crashes when trying to acquire a new Entrust PKI endpoint
20798785/01	CA Identity Manager documentation on the SiteMinder agent to an existing CA Identity Manager environment is not updated.

Support Ticket	Problem Reported
20801067/01	Delegates could see the pending work items duplicated in the login home page and in the Bulk Loader Notification.
20807004/01	Drop-down list on the user profile screen includes an additional row of concatenated values.
20807666/01	The dynamic connector attribute does not function when the attribute is changed to synchronized after initial deployment.
20808766/01 20955882/02	CA Identity Manager does not support LDAP connection pooling with SSL.
20813912/02	The Active Directory user store search result returns 1001 objects.
20815237/03	Some membership changes in the access roles that are associated with a user using User Console does not reflect on the Policy Server though Role-Based Access Control is enabled
20823538/01	Request for the change password of locked SAP Account fails to return the password.
20830672/01	Task name is not localized and displays ${bundle=resourceBundles string value.
20839018/01	When creating CA RACF User Permission using Provisioning Manager for the RACF endpoint through the Z-OS r14 LDAP server, LDAP error code 21 (invalid object class) is displayed.
20839375/01	eTADSaltSecurityIdentities attribute is marked as a capability attribute but the attribute is not marked in an ADS account template.
20843137/01	Modifying policy set task fails if a Policy Xpress has an email type that is configured to its event.
20843185/01	When executing SQL Query with a missing or invalid operator, ORA-00920: invalid relational operator error is thrown.
20843340/01	CA Identity Manager explore of ADS endpoint fails displaying unable to allocate operation object error.
20844997/01	Could not localize the attribute name in the identification screen upon a validation error.
20846653/01	The Workflow Admin Role resolver does not adhere to scoping rules.
20850506/01	Modify User task fails to complete even though the child tasks run successfully.
20851208/02	The ADS terminal services attribute get propagated with blank values to the endpoint.
20852034/04	Support for sqljdbc4.jar with the Connector Xpress (JDBC) to manage MS SQL Server has to be certified.

Support Ticket	Problem Reported
20856585/01	Unable to change the failover server and group values from User Console and Provisioning Manager after duplicating the active directory endpoint.
20861541/01	Endpoint failover status in both CA Identity Manager and Provisioning Manager displays incorrectly.
20866347/02	In French, the word *Return* in GINA or Credential Provider is not translated properly.
20867736/01	TEWS request to Execute Explore and Correlate task fails with an error against Cleanup Submitted Tasks.
20868664/01	When duplicating LDAP DYN group, a distorted window is displayed.
20868783/01	Unable to reset the new search in the search screen results.
20872100/01	If the group name is prefixed with ##, the Policy Xpress does not remove a group in MemberOf function.
20873691/01	Provisioning server installation fails when connecting to a remote provisioning directory with an error message Error out: Failed to locate provisioning directory domain.
20875436/01	When performing Set Account Data operation, java.lang.ClassCastException: com.netegrity.ims.events.IMTaskEvent incompatible with com.netegrity.imapi.UserEvent is displayed.
20877331/01	When resolving the roles based on group membership, LDAP connection spiking occurs.
20879473/01	Unable to display operation details from the remote Provisioning Manager GUI.
20882585/01	When removing SAP R3 role from an account through CA Identity Manager GUI, Error: java.lang.NullPointerException error message is displayed.
20883127/01	Connector Xpress Informix Datasource generates a JDBC URI invalid string.
20884389/01	When adding the password confirm field during the modify user task, the following error message is displayed: Password Validation Failed. Password must not contain only white characters error is displayed.
20884389/02	CA Identity Manager does not allow global user to login with the blank passwords.
20886184/01	In CA RCM, when removing the duplicate templates from a provisioning role, the user synchronization and account synchronization triggers all the users in the affected roles.

Support Ticket	Problem Reported
20887469/01	Though workflow is disabled, CA Identity Manager takes a minute to connect to the workflow server.
20888199/01	DN naming convention for the account templates for TEWS is not documented.
20888410/01	Unable to save the profile attributes in the order that user defines on a TSS template.
20892434/01	When a unique identifier is set to != %USER_ID%, the Bulk Loader is incorrectly evaluated.
20892603/01	Changing the view of User Console to horizontal skin makes the content on the screen unstable or jump.
20893717/01	Could not find a drop-down for the fields that have the type of enumeration or association. Unable to manage the role objects from CA Identity Manager because it is not the account type.
20896525/01	Some Chinese characters appear in the output device text that are generated from the SAP Account default property sheet.
20898024/01	When the account is locked in the DYN NDS eDirectory (JNDI) endpoint, it does not reflect in the Provisioning Manager.
20899903/01	When UNIX account templates are created through CA RCM Auto-fix and Export options, the unique identifier settings does not display correctly in the Provisioning Manager. Though the correct setting is applied, User Console and Provisioning Manager show different settings when accounts are created with the template.
20901541/01	The auto-select option that is used for all search results to multi select the tasks does not automatically return the results.
20903103/01	Performance issues are observed when excessive search is performed when adding AD groups to AD accounts through Policy Xpress using JIAM.
20919274/01	Performance issue is observed when adding ADS groups through the Policy Xpress.
20921149/01	When the select box malfunctions, error messages are displayed.
20921328/01	The runtimestatus12 query takes long time to complete the task due to classic parameter data type mismatch error.
20923113/01	Unable to connect to Provisioning server through LDAPS, com.ca.commons.security.ssl.CustomSSLSocketFactory Failed to verify server error is displayed in WebSphere.
20925492/01	Validation script is not working properly when used on a multi text attribute.

Support Ticket	Problem Reported
20935494/01	Nested Group membership tab UI problem occurs when a %NESTED_GROUP_MEMBERSHIP% parameter is not used in the directory .XML file.
20935494/02	When a parent group is modified through a user interface, the nested group members are removed from the parent group.
20936162/01	The ACC connector can assign AD/NT groups, but cannot deassign the groups.
20940489/01	Cannot invoke reject event on Policy express reverse sync policy, an exception is received.
20950766/01	Error occurs when validating the response received from TEWS with WSDL to verify that the WSDL contract is not broken.
20957471/01	RCM exports take long time when updating the Active Directory membership.
20958734/01	When selecting All Computers option from ADS Account "Log on To" tab, the list of computer data does not appear.
20959045/01	The Return button label in GINA is displayed in English on a Spanish system.
20960887/01	When task-level auditing is disabled for Create User task, an exception com.netegrity.ims.statusDetail.RuntimeStatusDetailService.writeToAuditing is generated.
20964463/01	When searching for Unix-enabled ADS groups using one level search, no groups returned.
20967129/02	RACF Connect Group Ownership is set to the group instead of CA Identity Manager administrative user ID.
20971367/01	When trying to browse RACF endpoint with JXplorer or Softera LDAP browsers, LDP4901E Scope=one search for unknown attribute(SYSINFO) error occurs while expanding the endpoint node.
20972783/02	The error message is not customizable when the network connection is unavailable from the Credential Provider or GINA.
20973172/01	Dynamic Connector Informix, Connector Xpress failed to create an endpoint.
20973558/01	When CA Identity Manager is accessed in French, a warning message appears in English when the CA Directory dxserver DSA 'max-op-size' limits the search results.

Support Ticket	Problem Reported
20974541/01	The following issues are identified when the item in *View My Work List* supporting bulk workflow operations is selected. ■ Items are randomly processed when one or more items are selected (but not all) though Approved/Rejected/Reserved is applied. ■ Selected items differed while navigating within pages.
20977897/01	When the admin role member has admin attribute as a telephone number, the account template is not available for the user to modify.
20982569/01	When the "Section 508 Compliance" option is not selected while installing GINA or Credential Provider, the Return button does not function.
20989483/01	Problem with the configuration when using the SiteMinder setMaintainSession session.
20991858/01	Displaying as Unknown instead of the actual group name for a non-default built-in primary group set of the ADS account.
20996828/01	CA Identity Manager extensions installer crashes SiteMinder.
20999864/01	When items in *View My Work List* are selected, the selected and the approved items differ the list sorted by any column.
21000622/01	Peer certificate verification is disabled for a SSL-enabled JNDI user store.
21014140/01	Check Compliance button disappears when switching to wizard tab controller.
21020195/01	Due to a column type mismatch, SQL load process takes more time than expected to execute.
21021862/01	Audit data is missing when CA Identity Manager is upgraded from SP6 to SP12.
21024493/01 21024493/02	Performance is slow while setting the Active Directory attributes from Policy Xpress.
21025959/01	Policy Xpress samples are missing when inserting the samples to DB table.
21028697/02	Cannot add eTrustIAM application to SSO endpoint account.
21032229/01	Reset User Password task fails when the accounts exist in CA Identity Manager integrated with SiteMinder environment.
21033681/01	In the account tab, a geographical location name appears in the endpoint drop down for the Active Directory account.

Support Ticket	Problem Reported
21040471/01	Create User requests fail with imsapi.exception.UnpersistedObjectException in PWHelper.generateSiteMinderTemporaryPassword exception.
21068457/01	Global users lost their inclusion to the Active Directory account.

Fixed Issues in r12.5 SP13

CA Identity Manager r12.5 SP13 includes the following fixed issues:

Support Ticket	Problem Reported
20146045/01	The email template that notifies the administrator of a new password is not delivered.
20527773/01	When trying to set up explore and correlate definition into RSA endpoint, the system fails to respond.
20577033/03	When applying large number of account operations to the UNIX endpoints, the endpoint operations fail. The /etc/passwd file has no read permissions that interrupt the other applications to read the file.
20580467/01	When processing a task, the search order defined in the Default User Search screen is not evaluated.
20591776/02	Data is duplicated in a user entitlement report.
20603264/01	The GenerateTemporaryPassword integrated with CA SiteMinder generates password randomly even though the CA SiteMinder policies are disabled.
20603264/02	The random password generator does not execute the CA SiteMinder password policy directory filter.
20612995/01	CA Identity Manager Server encounters the *Cross-Site Request Forgery* (CSRF) attack.
20623541/01	The submitted tasks are set to the completed state in the CA Identity Manager View Submitted Tasks before all the events in the task are set as complete.
20625957/01	View User Activity task returns an invalid object name event_object12_5.
20635445/04	Performance of the provisioning roles deteriorates when upgrading to CA Identity Manager SP9 or later release.

Support Ticket	Problem Reported
20635873/01	In Modify User's Endpoint Accounts Screen, the drop-down of the Actions button takes time to display.
20636474/01	When upgrading from CA Identity Manager SP7 to a later version, the password policies redirect URL of the CA SiteMinder is incorrectly migrated.
20651404/01	Setting a strong password for the admin user causes bind failure for the user.
20653004/01	When performing a search on the Modify User's Endpoint Accounts task, the *Attribute name: %CONTAINER% not found in the attribute map provided* error is displayed.
20656452/01	When creating a new endpoint type for JavaBean property name, the *Required property missing* error message is displayed.
20663295/05	Shadow error is displayed when NIS is explored without correlate.
20663295/06	Adding an NIS account causes improper modes to the etc\passwd file.
20663295/08	NIS endpoint explore is slow because the uxsautil utility waits for a response from getgrgid().
20664198/01	The CA Identity Manager Password Services task causes security vulnerability.
20666551/02 20815928/01	Configuration Xpress does not update the CA Identity Manager environment directly.
20680041/02	The User Console does not display SAP role description.
20694223/01	When the language switching is enabled using any public tasks and the user attempts to switch a language, the user is redirected to the logout page.
20695093/01	When performing search to find the status of users, the *Enabled* logical attribute is not evaluated.
20697400/01	Entering * in the UserID field on the forgotten Password Reset Identify screen causes a CPU spike.
20702911/01	When the Modify User event fails, the system email notification event does not execute.
20703647/01	When querying the IM_ROLE_LD table in the Object Store database, the table does not exist in the CA Identity Manager DB scripts.

Support Ticket	Problem Reported
20706127/01	Provisioning Manager does not display a valid checkbox state for a Password Suspended TopSecret account.
20715769/02	HP-UX in Shadow Mode does not support as UNIX Remote Agent Endpoint.
20716831/01	CA RCM export to the CA Identity Manager fails when multi-byte characters exist in the RCM role names.
20726814/01	When creating or deleting the users in the access and admin roles, the add admin role to user and add users to group tasks remain *In Progress*.
20731581/01	Synchronizing the users after disabling the Identity Policies results in role removal and account deletion.
20742308/13	A single quote in the snapshot name prevents the snapshot association with the report task.
20748558/01	The MakeProvisioningRoleMember Change Action in IdentityPolicySet does not provision the endpoint with an account.
20750345/01	In Oracle Application, after CA RCM is exported to the CA Identity Manager, the start date is not set on the assigned responsibilities.
20750345/02	In Oracle applications, the account Effective Dates are modified after the CA RCM export to the CA Identity Manager.
20750345/03	After CA RCM export to the CA Identity Manager, user attributes for the new responsibility assignments appear to be created by the anonymous user.
20750345/03	When using the resume button from the User Console or resetting the Effective To date in the Provisioning Manager, the user access is not restored.
20753866/01	When the ValidateSMHeaders parameter is set to false, the user is not deleted and the attributes from the Change Password task are still available on the user profile.
20754518/01	When the user organization name is added to the search screen, the search breaks.
20757435/01	The ACF2-ACFESAGE connector does not support CA RCM.
20771607/01	The Hidden tasks are visible in the Neteauto skin.
20771903/01	Synchronizing the attributes to the user accounts takes time to complete.

Support Ticket	Problem Reported
20781649/01	The Accumulated Provisioning Role Event details are not clear in 12.x when compared with 8.x.
20782126/01	Generated WSDL in WS-I form attribute does not display WS-I compliant even though the attribute in the Management Console is selected.
20793623/01	The C++ Connector Server (CCS) intermittently crashes on the Provisioning Server.
20795375/01	When starting the CA Identity Manager environment, IM_TASK_LD queries are displayed.
20796935/01	POST_ADD_ACCOUNT Program Exit returns an incorrect status.
20797253/01	When using gidNumber attribute for ADS account, the status of the ADS user accounts in the User Console appear as Unavailable under the Suspended and Locked field.
20798698/01	Applying a role or policy server template for a user or an account fails with an invalid syntax 0x0015.
20799984/01	When user account is created using LND endpoint, the *Failed to read Group attributes* error is displayed.
20802272/01	When special characters for example, slash or back slash is used in the CA RCM role or account template name, the RCM fails to export to the CA Identity Manager.
20808066/01	The Endpoint Template Search returns no results or limited information.
20809565/01	The role scope constraint issue causes incorrect search query.
20816953/01	Searching for an Active Directory Generic Container object type using *starts with* clause does not return all the containers.
20817643/01	The Concurrent C++ Connector Server (CCS) initialization deletes the ADS endpoint.
20819711/01	The Select Box Data information is incorrect.
20825792/01	When Account Synchronization is set to On Every Event, the attributes are not synchronized.
20826616/02	The URL path is broken in the postXML.java file that is available in the samples directory.
20828332/01	When performing ADS operations, the C++ Connector Server (CCS) Service continues to stop.

Support Ticket	Problem Reported
20829628/01	When password policy composition is set to Minimum Length greater than 15 characters, the *Password validation failed: Cannot generate password* error is displayed in the public Forgotten Password task.
20833801/01	When trying to modify an Admin task, a null pointer error is displayed.
20845253/01	Lack of namespace in xmlns="http://tews6/wsdl" response.
20848946/01	If a user has UPO (C++) accounts, the Accounts tab in CA Identity Manager fails to fetch all the accounts.

Fixed Issues in r12.5 SP12

CA Identity Manager r12.5 SP12 includes the following fixed issues:

Support Ticket	Problem Reported
20519803/01	Warning message is not displayed when the user search results limit the number of results that are returned.
20575541/01	ID Policy of the type Reject is not triggered correctly.
20589598/01	Provisioning server hangs when the user accounts are modified in the Active Directory.
20590771/01	Access roles with membership policies are not stored in CA SiteMinder.
20591616/02	Certification of TEWS on .NET for WCF compliance.
20598237/02	LDAP Queries fail when RCM Role Import data from the Provisioning Server.
20600543/01	The scope for the admin task Modify Admin Role Members/Administrators membership tab is not evaluated properly.
20618795/01	Authorization cache that holds the user to roles mappings becomes large.
20636175/01	The caftkey command displays the encrypted not supported error.
20638046/01	The password reset task is not enforced when a new user is created.
20653691/01	Performance issues are raised when searching for orphan accounts in the Manage Orphan Accounts Task.

Support Ticket	Problem Reported
20657195/02	Explore and Correlate fails with the Error: An invalid XML character (Unicode: 0x1f) if the role definition XML file contains invalid characters.
20657874/01	When creating a user, the *object no longer in scope* error is displayed.
20663295/02	Explore and Correlate on NIS endpoint hangs if the group file contains special characters such as +:::.
20672752/01	When more than one user attribute is involved, the Bulk Task does not evaluate the result correctly.
20674645/01	Performance issues are raised with Modify User when encrypting the data properties.
20676855/01	The Preview Requested Actions button is aligned in a separate row rather than in the same row with all the other account management buttons.
20682668/01	Performance issues are raised when importing data from CA Identity Manager to RCM with the ACF2 endpoint.
20695812/01	The Netgroup file corrupts when Netgroups is modified for the UNIX endpoint.
20703164/01	Admin Role membership is not evaluated correctly.
20704002/01 20765210/01	When the Bulk Loader Task is performed, connection reset and connection closed errors occur in the JBoss log file.
20704126/01	Connector Xpress displays the read failed: Failed to find a Connector Server to handle error when you upgrade to the latest service pack.
20710243/01	Admin Role membership is not evaluated correctly.
20713491/01	Synchronization of Oracle Accounts with templates deletes the Oracle User roles.
20741439/01	Unable to remove more than one Netgroup memberships from the User using JNDI NIS endpoint.

Fixed Issues in r12.5 SP11

CA Identity Manager r12.5 SP11 includes the following fixed issues:

Support Ticket	Problem Reported
20146045/01	Temporary password is created randomly.

Support Ticket	Problem Reported
20357587/01	Null exception being thrown on provisioning page when None is selected as the provisioning server.
20376823/01	Approvers list is truncated where approvers or characters list is too long.
20388684/01	Changes made to the Provisioning Role from Provisioning Manager are not updated on the User Console.
20408188/01	Logging displays an incorrect rule evaluation.
20410837/02	Enhancement to the Reverse Sync Modified Account.
20429060/02	Credential Provider needs to be certified with Windows 7 SP1 Professional edition.
20444710/01	Admin role user scope does not work as expected.
20446773/01	CA Identity Manager re-encodes the SMAGENTNAME, causing problems on the redirect.
20448385/01 20541600/01	New values entered in the Dropdown combo (Drop down list and user defined input text) are lost.
20458009/02	After changing the global user password in the Provisioning Manager with the propagation against the TSS endpoint accounts, any Acid property sheet fails to display the data.
20478679/01	Progress BAR running under java program for Self-Service Tasks that run under Gina or Credential Provider does not work.
20479418/01	Connector Xpress Endpoint with Auxiliary object classes has tab encounters an issue problem in the Provisioning Manager.
20479480/01	Nested tasks do not work after the password is reset.
20485201/01	Synchronizing a SAP account with a SAP template including SAP roles containing SAP generated profiles can suppress the SAP generated profiles for the account.
20518025/01	Event Workflow to Certify User task does not trigger.
20525844/01	Object store schema tuning by adding REF_ID.
20554757/01	High Availability configuration diagram for failure between Provisioning Servers and Directories and Server is incorrect.
20558310/01	RSA account fails to provision users.
20558483/01	Discrepancy in attributes used for Oracle Systems Account between CA Identity Manager, Provisioning, and RCM.
20558483/02	RCM does not recognize eTORADefaultRole and ETORAUserRole.

Support Ticket	Problem Reported
20560790/01	User memberOf attribute is not cleaned when associated group is deleted.
20561553/01	TEWS interface errors with a soapenv client error: ConnectionWaitTimeoutException: Connection not available, Timed out waiting for 180029
20567711/01	Synchronizing an ADS/E2K account including SIP email addresses but no primary SIP email address with its template containing other addresses fails to fix proxyAddresses with ldap error 21.
20569763/01	Windows 64-bit Password Synchronization Agent fails with 5,000 password changes under a load.
20577033/01	When UNIX Remote Agent updates to the /etc/passwd file, the file may cause other applications to fail.
20578640/01	A warning message is displayed while using Nested Provisioning Roles roles even after the xml is imported.
20583233/02	Displays malformed eTSuspended attribute value InvalidAttributeValueException when setting suspended state and Account.modifyObject().
20588131/01	Bulk Loader client -b option fails with a (401) unauthorized error.
20588169/01	When using the /imcss skin, the category items on the left pane such as Users, Groups, Roles, and Tasks use the default icon.
20590364/01	The imsUninstall.jacl fails as JAAS entries are deprecated.
20590698/01	Correlate operation fails with a java.lang.ArrayIndexOutOfBoundsException or Create of ADS account with comma in the name.
20592337/01	Self-subscribed group with slash (/) in its name causes Modify My Groups to thrown as an exception.
20594929/01	eTRACRevokeDate inconsistent on valid date formats.
20597048/01	enabled attribute check box make change to unchecked by switching tabs in View Identity Policy task.
20602887/01	If a forgotten password public task with verification page limit set in forgotten password search screen is accessed in SP9, when entering a wrong answer in verify your identity screen, the OK button disappears.
20604012/01	LND Explore of Organization never completes.
20613137/03	GINA and Credential Provider user console should be localized into French.

Support Ticket	Problem Reported
20614378/01	Could not create or validate administrative groups error that may cause connection pool issues on JCS to LND and cause JCS to hang.
20615059/01	Task level email configuration is missing from the environment advanced setting export.
20615903/01	Delete User does not delete a user from a group at the LDAP Level.
20617610/01	CAUMSG_E_ERROR Message Argument Error.
20620426/01	Group unique member attribute is not cleaned when the associated user is deleted.
20655916/01	Control Characters (escaped comma) in ORG displays incorrectly.

Fixed Issues in r12.5 SP10

CA Identity Manager r12.5 SP10 includes the fixed issues in the following table:

Support Ticket	Problem Reported
19210595/02	Oracle Database 11g R2 as an endpoint: dynamic and static
19251022/01	Oracle Sun Java System Directory Server (iPlanet) 7.x as a JNDI endpoint
19574715/01	Password Synchronization Agent on Windows Server 2008 R2 Core
19980342/01	RedHat Directory Server 8.2 as a CA Identity Manager User Store.
20233987/01	Scoping of Administrators/Owners are inconsistent between Provisioning/Admin and Access Roles.
20238200/02	Enabled support for establishing bi-directional relationship between the account and the group.
20303148/01	Using operational bindings on a custom Xpress connector gives an error under explore/correlate
20334205/01	"InvocationTargetException:null" error message is displayed when trying to run Snapshot reports
20365872/01	Installation of Password Synchronization agent on 64 bit fails in silent mode.
20367589/01	When a temporary password in Forgotten Password is created by CA Identity Manager automatically, the new password does not match the password policy defined in the system.
20370989/02	Strong synchronization warning

Support Ticket	Problem Reported
20380926/01	After installing a Credential Provider on Windows 7 SP1 Enterprise x64 bit system, an icon is seen in the Other User tile icon.
20381233/01	When a snapshot report for Admin/Access roles with Custom Attributes is run, the data is not populated for Custom Attributes
20383927/02	Addition of 20 attributes to account class in ACF2 namespace which the customer can use to map endpoint attributes
20385503/01 20567030/01	setpasswd Fails On Linux due to missing EXPECT binary
20387740/01	On a UNIX endpoint, Explore and Corelated fails when /etc/group and /etc/passwd end with a blank line.
20388684/01	When a provisioning role is modified from the provisioning server, the modification is not updated on CA Identity Manager User console.
20389184/02	New lines being entered on the History Editor field should be visible in the History Display field.
20393681/02	The data for the delegators were being loaded, even though the delegators were turned off and OOTB workflow is timed out, when the workflow was trying to obtain the users.
20397807/01	"Show only objects meeting the following rules" criteria in search screen does not work.
20414709/01	Provisioning server (IMPS.EXE) is crashing under load in module libldap.dll.
20417827/01	Error on GetAccounts() with the DeleteUserEvent, DisableUserEvent, and EnableUserEvent in Policy Xpress.
20430145/01	Internet Explorer does not work with CA Identity Manager unless compatibility mode is turned on.
20433653/01	Custom filter is not working for self-subscribed groups.
20433685/01	Search screen ignores pre-configured filters.
20434236/01	Forgotten Password and Forgotten Password Reset tasks lose the ability to generate random questions and same verification questions are being loaded on the secondary verification screen.
20434574/02	No provision to select/set the Encryption Algorithm in Connector server connected via Connector Xpress.
20434744/01	On WAS 6.0 cluster, workflow goes to "Planned" state instead of Active and the work items are never assigned.

Support Ticket	Problem Reported
20435569/01	When creating new environment with using sample Japanese Role definition file in r12.5 SP7, "1: error" is shown in the CA Identity Manager Management Console.
20439386/01	"Accounts will enter Delete Pending State" option on the Endpoint Settings tab of a JNDI Connector Xpress endpoint is throwing a CONSTRAINT_VIOLATION when the associated provisioning role is deleted.
20441092/01	When the ADS endpoint has large number of objects in the Users container, searching for containers for explore and correlate from CA Identity Manager User Console is taking a long time.
20441092/02	eTDYNContainer naming attribute being mapped as isMultivalued=true, which was against the current expectations of Provisioning Server/JIAM.
20444074/01	Under heavy TEWS load CA Identity Manager response time drastically increases.
20441738/01	CA Identity Manager contains PHP scripts that are easily accessible via public tasks or after authentication which leads to security vulnerability.
20448421/01	When the Reset account password task is submitted, it is failing with the error "'selfChange' is not a property of SAP R3.Account".
20448458/01	When the column has a string NULL (with no quotes) and the deletion sequence string is also NULL (with no quotes), the bulk loader was replacing it with the object value as null.
20453659/02	A search result returned is not in the expected format
20461346/01	While executing View User task via TEWS, the following error is displayed in TaskSessionCache. "java.util.ConcurrentModificationException"
20469342/01	ACF template has Phone number required, when it does not appear that it should be.
20476237/01	Creating an Exchange mailbox inconsistently fails with an unknown error in the Exchange Remote Agent logs.
20481749/01	CCS crash after turning on AD connector logging and searching for a user.
20483159/01	SSO Next Password is being updated when it should not be.
20485607/01	When creating users, adding many groups causes submit to take a long time

Support Ticket	Problem Reported
20500202/01	Modify Group task attempts to change %MEMBER_OF% user's attribute resulting in constraint violation.
20501148/01	When running etautil select command with redirection to text file, ETA_I_1336, ETAUTIL command complete message is recorded in the middle of the list.
20501964/01	When using the SPML to modify a Global User custom field, the request received by the Provisioning Server includes not only the update for the changed custom field but also includes updates for all custom fields to update them with their existing values.
20506692/01	"eTSQLLogin::eTSuspended" attribute looks at the only one attribute dealing with SQL Login status but it does not map to SQL Login locked out status. It only act on DB Access (Grant/Deny).
20520061/01	CA Identity Manager CCS Server is Crashing Frequently
20527964/01	With a Verification page attempt limit value in Forgotten Password Search Screen, when entering a wrong answer then the OK button disappears.
20532092/01	The locked status of the endpoint account is unavailable even the endpoint is accessible.
20537311/01	New attribute Alias (eTSAPUserAlias) has been added into SAP connector metadata and a new control was added to Provisioning Manager plug-in
20551917/01	MySQL JBDC connector missing membership data
20560002/01	CA Identity Manager Vulnerable to Cross Site Scripting (XSS) attacks
20569763/01	Password synchronization agent on a Domain Controller fails to connect
Not available	Acquiring ETC Endpoint on Solaris 10 x86 (32 bit) with IPV6 enabled Fails
Not available	Provisioning of users with portal licenses has been added to Salesforce.com connector

Fixed Issues in r12.5 SP9

CA Identity Manager r12.5 SP9 includes the fixed issues in the following table.

Support Ticket	Problem Reported
20125638/01	When a CA Identity Manager realm in SiteMinder uses auth/az directory mapping, then user cannot login to CA Identity Manager. A naming exception is thrown when a DN from the authentication directory is searched for in the authorization directory.
20153693/01	View User task locks the scroll bar of a <select></select> control when viewed by Internet Explorer. Additionally, a user cannot establish which items are selected and which are not.
20140866/02	When CA Identity Manager fails over to a secondary policy server and load is generated on the CA Identity Manager extensions, Siteminder hangs.
20078491/02	Date format is not localized in the Out Of Office Assistant date picker field when editing the start date or end date of a delegated user.
19805521/05	The total audit data generated is around 1.67 million records. This could be an issue as the Business obect server is running out of memory.
20308001/01	Bulk load performance - Need to close connection related objects to facilitate efficient connection management.
20326288/02	Executing call Store Procedure using Policy Xpress does not work for Oracle. The current Policy Xpress is unable to handle this because the Oracle SP requires that you explicitly set the output parameter into the call in Java.
20372531/01	Add a new configuration to Psync file to trace openldap messages which can be written to the same psync log file to aid debugging.
20395928/01	When running an explore correlate we found that certain character combinations result in error
20351942/01	Policy Xpress failed to set a value at Oracle database. The Policy Xpress is unable to handle the task created by the page which contains a list of users. e.g. Disable user.
20371208/01	Customer has observed that on a Corp=Prov environment, global user -> account propagation does not happen on custom fields beyond eTCustomField10. Fields eTCustomField01 to eTCustomFields10 were being propagated as expected. L1 has also determined that this problem did not occur on a Corp!=Prov environment

Support Ticket	Problem Reported
20382777/01	Provisioning related events not being generated to the Audit DB when "Accumulation of Provisioning Role Membership Events" is enabled
20389722/01	KRB account template does not allow colons on the user id field.
20318294/01	Nskutil crashes im_ccs. When trying to do anything against a tandem machine, you will get Unable to connect to Connector Server:
20319593/01	A customer added an additional field on the forgotten password task screen. If the validation on the additional field failed the customer was still presented with an option to submit or cancel the task. The customer asked that the Submit/Okay button be hidden so as not to give the impression the task can be completed successfully.
20200261/01	Provisioning Manager error "Encountered an improper argument" trying to right-click on a DYN endpoint (JNDI/JDBC)
20385320/01	The Provisioning Manager installer failed to install the CA Enterprise Common Service because the temp folder contains a space character.
20395199/01	When submitting a TEWS request from WS-I generated WSDL, CA Identity Manager throws an exception trying to find the task TEWS is trying to execute. This is as a result of WS-I no longer using just the TaskContext section, but a [taskName]TaskContext. This is causing CA Identity Manager, which will ignore the TaskContext tag to not ignore the [taskName]TaskContext tag and try to use this as the task name, which fail on lookup of the task.
20409006/01	Due to localized task names Bulk Loader client could not find the mapped task names to perform the load.
20431265/01	A problem with editing the "Modify My Group" task causes the task to no longer show any groups after it has been edited.
20395199/02	When Generating the WSDL CA Identity Manager does not generate the SOAP binding correctly when WSI compliance is turned on
20263873/01	Customer has requested for custom validation on MOBILE & PHONE ATTR'S specified in directory.xml as part of bulk loader.
20297801/01	Dropdown Combo style does not default to the dropdown list of items.
20301423/01	When the Forgotten Password public task is shown an error is logged by the app server.
20300619/01	CONXP JNDI DYN connector does not allow you to create new accounts when primary key is defined with IDENTITY property.

Support Ticket	Problem Reported
20323570/01	CA service reported that the ConfigXpress couldn't connect to immanage (the r12.5 sp7 management console) and hangs on large zip import.
20283299/01	Enabling Forgotten Password LAH for Tracking Questions using a counter causes Q&A to appear decrypted.
20345483/01	The encryption key for Forgotten password LAH is masked under the environment, System ->Logical Attribute Handler -> Forgotten password Handler. However using the management console --> Advance settings --> Logical Attribute Handler --> Forgotten password Handler, you can view this clear text.
20349975/01	The Forgotten Password LAH has the option for an encryption key to be set. When this is set, the question/answer pairs subsequently set by users will be encrypted and should not be readable from the Password Hint field. However, the decrypted values are be added once it is used (thru Forgotten Password task). This causes the question/answer pairs to become readable from the Password Hint field.
20254561/01	CA Identity Manager server loses directory connection to the Provisioning Server.
20345692/01	Java error when hit Submit button at "View My Submitted Tasks"
20248448/01	JCS LND connector memory leak causes failure to acquire endpoint
20316004/03	Password changes to DYN endpoint do not update the passwordExpirationTime attribute. This causes Novell and PRISM to see the password as being expired and users are prompted to change their passwords again
20016653/01	When the incorrect current value is assigned to the old attribute in the AuditFilter.setOldAttributeValue() method. This error causes a null pointer exception to be thrown.
20366901/01	msExchHomeServerName attribute is missing error on ADS Account Sync (mail-enabled ads account)
20374491/01	User tabbed tasks are not shown in IMCSS skins for user with Self Manager role.
20366901/02	When a user that has Mail-Enabled, that user tries to modify the mailbox and receives the following error: “The operation couldn't be performed because object 'server/Users/user' couldn't be found on 'DC'.”

Support Ticket	Problem Reported
20309463/01	Square brackets in provisioning role names are not correctly handled. When using the View or Modify user task the Provisioning Roles tab will not display any provisioning role that has a name containing a bracket character (either open '[' or close ']').
20323570/02	Customer tried to export the Directory XML, comment out the User managed object default container and re-import the XML. This resulted in a corruption of the XML
20357587/01	Customer is unable to detach an environment from a provisioning server. Customer is able to go to management console -> advanced settings -> provisioning page. On that page, if they select "None" from the selected provisioning server, this results in a Null exception being thrown on the screen when they hit Save.
20436202/01	When a screen field attribute in an admin task is "Multi-Text" style and "Read Only" Permission with n Size then this Admin task does not display more than the n lines since the scroll bar is not available.

Fixed Issues in r12.5 SP8

CA Identity Manager r12.5 SP8 includes the fixes issues in the following table.

Support Ticket	Problem Reported
16885325	The Provisioning Manager LND account creation window contains a check box called 'Create Replicas' on the Profile tab page. When administering a Domino endpoint in a clustered environment, when this 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.
1980552/4	When user accounts snapshot is filtered based on user accounts object for %USER_ID% equals to "a*", it doesn't limit collected data simply to the corporate / global user id's who "start with a" and their accounts.
19821141/1	While Importing CA Identity Manager Roles from a previous working environment a crash is encountered in smobjimport resulting in an incomplete migration and role entries presented in OID value instead of plain text in the Siteminder FSS UI.
19888244/2	Dynamic Groups in Corp=Prov do not work as expected.
19890864/8 19953802/6	When attempting to leverage filtering , we're unable to filter the user accounts snapshot

Support Ticket	Problem Reported
19896525	People Soft 8.5 Client tools are now supported with CA Identity Manager 12.5 SP8
19940810/2	When managing a Linux endpoint, attempts to add or delete a provisioning role from a global user may cause the CAFT process to be terminated.
19953802/6	When attempting to leverage filtering, customer is unable to utilize the user accounts snapshot filter.
19978492/1	When importing IME.zip file using migration tool, an error message is encountered.
20013459/2	When using trim on an attribute coming from a custom JNDI connector, it causes error if the value on the endpoint is entirely whitespace.
20034691	Deleting CA Identity Manager environments and directories corrupts the SiteMinder policy store.
20036944	Cam/Caft 1.13 Build 10 Patch 3 has been packaged into the Unix Remote Agent
20043079	When "System Properties"->"Generate UID" is enabled, but "Auto Generate" is NOT, and you have an account template using the %GENUID% rulestring (referred to as on-demand UID generation), applying that template to a global user causes an internal consistency error.
20063601	Mandatory fields on verification screen are not mandatory when using TEWS.
20067502/3 20067502/5	Update of an existing Directory xml with DataClassification of AttributeLevelEncrypt is ignored.
20085318/2	Attempting to change an ACF UDF attribute from 'Y' to a negative value, CA Identity Manager causes an invalid value error on ACF2.
20088479	When the TASK_NAME field for imsaudittasksession12 was being written, a database error was thrown because the size of the data exceeded the column size of the task_name field, which was 255.
20090052	When attempting to leverage filtering, we're unable to filter the user accounts snapshot.
20111177	Multiple TEWS requests are prolonging the average time it takes to process any request by a factor of 5 - 10.
20111767	When running TEWS on CA Identity Manager environment with SQL Server DB, Audit Deadlock was being encountered.
20128436	If the user installs the Provisioning Server without selecting all the Java connectors, JCS installation will fail with "Error publishing metadata".

Support Ticket	Problem Reported
20128922	User's pending work item list is not updated when we open the workitem one by one and do approve/reject/review operation on it
20140866/2	When IdentityManager fails over to a secondary policy server and load is generated on the CA Identity Manager extensions, Siteminder hangs
20141979	AuthenticationModule samples has been requested by the customer.
20142967 20142967-02	The CAM has been upgraded to 1.13 in the UNIX remote agent for the following platforms: Solaris, Linux, AIX, TRU64, HPUX, Solaris Intel
20144370	The Reset User Password task removes the users password if no password is introduced and no password policy applies to the user.
20158596	For Multi Valued attributes on SQL Server User Store: both OR and AND operators don't work.
20161021	Unable to get PSync silent install to run on W2K8 SP2 32 bit
20162822	Not Equal expression under password policy does not work as expected.
20193974	When using SQL as a user store, Identity Policy is evaluated incorrectly
20196607	In an Exchange 2010 environment, if an account has been associated with a mobile phone, then IM will be unable to delete the account.
20197678	In a multi-master AD setup, there are possibilities of replication collision occurring which causes Inbound notification clogging.
20198020	The customer has created a PolicyXpress policy to update the user accounts associated with a user when the user is being deleted. The policy fails to update the accounts when the user was deleted. However a similar policy set to update the accounts when the user is modified worked correctly.
20199681	ForgottenPasswordReset in TEWS doesn't allow a second attempt when the new password violates password policy
20199681/2	TEWS Pwd reset does not return ImsException on invalid password attempt
20211820	Provisioning Manager does not display auxiliary class tabs in account property sheet for a JNDI DYN endpoint.
20219061	The Batch file used to generate the javadoc for framework or ims is missing key java interfaces inside package
20220302	Browsing ACF2 endpoint in JXplorer results in Invalid objectclass etACFSystemInfo error.
20222329	Change PSync's default logging location does not work

Support Ticket	Problem Reported
20227974	Deleting a Directory and/or environment, when integrated with SM, leaves a corrupt Policy Store
20228504	The 2 utilities that ship with the UNIX password sync agent, test_ldap and test_sync, are not able to run on Redhat Linux 5. They fail with the following error: [root@tanen01-rh5 pam_CA_eta]# ./test_ldap
20230069	When modifying a custom attribute on a GU that would result in updates to the RACF Group memberships on the associated account, the ProvServer is not properly determining the end value.
20230215	After upgrading to SP6 the OpBindings defined in the JCS(JNDI) project stopped executing if multiple structural classes are mapped.
20230661	When adding task tag to a search screen all task tags are returned regardless of what is put into the search.
20230695	There is not an option to filter Task data(Data Element) as task tag name in policy express
20263873	Customer wanted to have a custom validation on MOBILE & PHONE ATTR'S specified in directory.xml as part of bulk loader. Currently the bulk loader only warns managed object not complaint with validation in log as warning in modify operation only.
20275003	Cannot clear the AD attribute for account expiry via IM UI in Modify Active Directory Account Task.
20277743	Explore of 500,000 LDAP users crashes im_ps process, out of memory
20284601	Provisioning attempts to remove RACF default group when account should only be set as "pending delete" on delete account operation.
20300175	In some cases, the result of an exploration of an Unix end-point may not be consistent
20304925	Can't view accounts if they are members of groups who's name contains a '$'.
20322892	AD account rename from Policy Xpress policy is not working
20328318	Error when using a compound class with a ConnXP (JDBC). In IM the error seen is "A JIAM operation failed" and in the Proisioning Manager the error seen is "Unexpected error generating compound attribute"
20364624	User Console does not add XML tags when setting PPS Roles

Fixed Issues in r12.5 SP7

CA Identity Manager r12.5 SP7 includes the fixes issues in the following table.

Support Ticket	Problem Reported
19774952/3	CA Identity Manager is unable to redirect the login to another landing page other than default when NOT integrated with SiteMinder.
19953802/3	Snapshot Time missing in parameter (User accounts Report, view my report task).
19947459/2	During mailbox provisioning, the Exchange 2007 remote agent intermittently reports 'Not a mailbox user error' when setting 'HiddenFromAddressListsEnabled' on the newly created mailbox.
20066423/2	When specifying backup Domain Controllers for an ADS endpoint not having a NEWLINE after the final entry in the config file causes the last character of the final server name to be truncated. Causing the look up to fail if the other servers are unavailable.
19618443	When trying install SunOS remote agent in Solaris 10 this error appears: SMX000007 Script or command "scripts/camscript.sh" failed with exit code 41
19659198	Task Resubmit does not function properly. When a provisioning role is added to a user but the endpoint is unavailable, the operation fails which is expected. It is possible to resubmit the failed task through the view submitted task interface once the endpoint is available again. However when the role addition task is resubmitted the account is not correctly added to the user.
19861329	When the user tries to remove all the Password Hint Questions and Answers, CA Identity Manager makes no changes but show a warning message: Task submitted. No changes have been made.
19869065	If a task belongs to the "self" action (such as self create or self modify), then the tab which contains the task is duplicated in the menu bar.
19871270	When acquiring an Active Directory endpoint with an extra UPN suffix through either Provisioning Manager or the User Console, the customer encounters an issue where all the dot (".") characters in the UPN become commas (",").

Support Ticket	Problem Reported
19872463	After enabling Manage Members for the Account Templates tab within the Create UNIX - etc Account task, the Account Template search page displays a ClassCastException.
19913803	TEWS load causes the server to run out of memory and refuses to accept login requests until it is re-started.
19947459	Provisioning directory high availability environment timing issue caused by the load-share in the knowledge file.
19948858	Createdatabase.sh is missing although it is described in IM R12.5 installation guide Run the Script for Workflow topic.
19965422	The customer added the OOTB Accounts into the Tab of the Forgotten Password Task and enabled the "Load Status.
19965638	The account does not have a mailbox but when they doing User Synchronization, the ADS connector tries to access the mailbox rights attribute which actually does not exist on a Recipient account. This result in an error
19974677	When the modify user task check box for 'Must Remain In Scope' is selected, the following message appears if an attempt is made to modify the object resulting in the object becoming out-of-scope to the Admin. "Object xyz is no longer in scope. Cannot submit task"
19974816	CA Identity Manager skin displays the Title field bigger and different from all other attributes.
19982376	No ADS group is retrieved from Provisioning Manager Active Directory Account Template.
19993152	In a clustered setup, the generated ETACALLBACK URI (for inbound synchronization) uses the local hostname and not the hostname defined for the base URI of the environment causes problem with Inbound synchronization from the Provisioning Server where it goes to the individual application servers directly and not to the load balancer.
20005197	Boolean field in custom report not passing value from CA Identity Manager to Crystal server. When you have a parameter value "true" or "false" the report value always takes "true" as that parameter value.
20007478	Apparently the eTADSpayload attribute must be padded by leading zeros, but this is not the case when correlated with the ADS account.
20009373	When a Policy Xpress Action rules triggers on DisableUserEvent, the 'Error finding Account' message is displayed on the screen and in the logs.

Support Ticket	Problem Reported
20009422	The CA Identity Manager Server cannot connect to a user store hosted by CA Directory running in FIPS mode.
20013050	Workflow participant resolver does not work correctly for EnableUserEvent when the user sets up the approval, the validation error displays "Cannot set Primary object of this task" in the {0} Resolver Description section for the multi-select task."
20017466	Customer reported that when updating an RSA account using global user, template propagation, the default shell value on the account is set to the account First Name.
20017629	When a report runs, we see the instance run-time stamp plus status in the reports server, History tab. The failed ones get status Failed, and the completed ones get Success. However, when we run the report directly from the Reports Server, using the same data source values, the report completes successfully.
20045418	There is a problem when using client SQL Server Database with respect to the audit tables, specifically the data in the table imsAuditObjectAttributes12. It does not display special characters properly. This causes the Audit reports to fail.
20050469	When a user sets the "End Date" of the "Out of Office Assistant" in the "Edit Delegation Details" page, the page prints an error message which says [Delegate Work Items] Start date in the past.
20050886	Duplicate name exists reported when customer doing a load test when adding some users, then removing some users, and then recreated the users.
20052434	If the user profile has a multi-valued field, and in a Modify User event there were updates to more than one of the values in the multi-valued field, then the Audit Details Report would show under 'Old Value' and 'New Value' only the old and new of one of the values.
20053259	Audit Details and Audit-Reset Password Reports fail.
20056353	Issue with how CA Identity Manager renders the dynamic elements for accessID and facility ID. It is not rendering the elements correctly.
20062793	Policy-based workflow misbehaves when the Corporate and the Provisioning Directory are the same directory, and the Approval Rule is based on "Primary Object of the Event".

Support Ticket	Problem Reported
20071186	AS400 JCS connector calls the native program QSYCHGPW.PGM to perform password change operation. This program is subject to the native system password rules (min length, history, etc.). A password change originating from CA Identity Manager is always considered an administrative password change and should not be subjected to user password history check. This is causing constant failure because the administrator uses a standard password for password reset.
20092989	Group membership rule fails when AD is the Corporate store.
20097639	While attempting to deploy a customized environment role definition file, encountered an error "Error: The type "UNKNOWN" is not a valid object type".
20114826	Modified search screen for admin roles ignores name filter. The new Admin Task does not start automatically by skipping the search screen and editing the specific mentioned Admin Role name.
N\A	Issues occur when you configure the filter on the Search Screen. For example, the default Search Screen filter may search for an admin role based upon the name beginning with Ad. An error prevents the search screen from processing the default filter, thus returning inaccurate search results.
N\A	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.
N\A	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.
N\A	On WebSphere on Linux, if LANG is set to xxxUTF-8 on Linux systems, you may see a sun.io.MalformedInputException error during workflow startup.

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.
19961208/2	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).
19904391/2	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.
19876970/2	After upgrading Provisioning Server 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.

Support Ticket	Problem Reported
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 specifies 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 custom field value into the objectstore.

Fixed Issues in r12.5 SP5

CA Identity Manager r12.5 SP5 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	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	User's Access Roles tab performs very slowly after upgrade from r12 CR5 to CR10.
19450496/3	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	FailOver not working with CA Identity Manager r12.5 SP3 and SiteMinder 12.0 SP2 CR1 (both on RedHat 5.5)
19474393	CA Identity Manager hangs on startup infinitely on * Startup Step 2 : Attempting to Start PolicyServerService
19661928	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	After upgrading to CA Identity Manager R12.5 SP3, customer lost the ability to specify rulestrings in RSA7 Templates to set Token assignments.
19685235	Connector XP: Direct Assocation with non-naming attribute.
19676068	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.
19647218	An error message is displayed when trying to JDBC Oracle endpoint

Support Ticket	Problem Reported
19759654	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.
19736733/2	CA Identity Manager re-using Op IDs which causes Provisioning Server problems. In this case, it involves using the Reset User Password task.
19799998	When selecting the link of forgotten password at the MSGina logon, a Security vulnerability has been identified in GINA.
19592759	JCS metadata created for conversion of an old r8 C++ Connector to an r12.5 Java Connector causes an error.
19754393/3	"Modify Group -> Membership" or "Modify Group Members" task fail with "exception:java.util.NoSuchElementException: Attribute member has no value"
19818241	Oracle Applications Connector is hard-coded to ID APPS.
19665364	Stored procedure GARBAGECOLLECTAUDITING12 for Oracle doesn't delete any rows from IMSAUDITTASKSESSION12
19613965/2	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 SP4 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
19246058/2	Page two of the Policies Tab in the View Provisioning Role task is blank.
19380365	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	You cannot enter the same for more than one custom attribute for access roles. This is doc issue for PROD00118276 below
19506576	When running CA Identity Manager R12.5 SP2, you are unable to select RSA SecureID 7 as an endpoint in the Provisioning Manager.
19515875	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	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	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	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>
19620528/2	The CA Identity Manager User Console is unusable when a user's endpoint is unavailable.

Support Ticket	Problem Reported
19627490	The CCS terminates unexpectedly when allocating a provisioning role or an account template with a long email address.
19636205	TEWS security flaw
19657285	CA Identity Manager phishing vulnerability
19602608	The TEWS WSDL is now generated according to WS-I compliance standards.
19260275	Admin roles with scoping rules for Provisioning Roles can now be instantiated within the modify provisioning role members/administrators task .
19666650 19586799/2	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	Tile image in IM Vista Credential Provider is customizable.
19043290/2	Provisioning Manager logout information required in the Provisioning Server log.
19145596	Identity Policy evaluations lacks delta evaluation phase.
19159246	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.
19241289/2	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 19257834/2	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
19260912/3	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 a CA Identity Manager environment with UserStore=ProvisioningStore, CA Identity Manager User Console does not display the Admin Group you added.
19309023	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
19312793/2	Provide support for Unique LND Shortnames
19312829/2	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),
19312847/2	Add support for specifying additional header attributes in the CA Identity Manager email templates.
19312856/2	The current method of finding unused token to assign to a user has unacceptable performance.
19315466	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	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	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.
19409953/2	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	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 19455231/2	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	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.
19030877/2	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.
19030877/5	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	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	Aux OC not updated via Provisioning Role.
19135793	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	In Connector Xpress, duplicating a Template does not set eTAccountContainer.
19137329 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 CA Identity Manager and Provisioning Manager
19158692	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	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	Supporting OID 4-way association attributes, including physical=>physical assocs.
19208273	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.

Support Ticket	Problem Reported
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	In Connector Xpress, cannot create an OID account on endpoint if executing through Role assignment and Account Template from Provisioning Manager.
19236949	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	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 CA 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 CA 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).

Support Ticket	Problem Reported
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.
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.

Support Ticket	Problem Reported
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. Open the Bookshelf.html file.

   Note: If you access the bookshelf from a local drive and are using Microsoft Internet Explorer, a warning appears about active content. To work around this problem, install the bookshelf on a remote system or use a different browser.

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

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.

Documentation Changes

The following changes have been made to the documentation set for CA Identity Manager:

Upgrade Guides

For CA Identity Manager r12.5 SP7 and higher, one guide exists for each application server and includes all information necessary for an upgrade of CA Identity Manager.

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.

User Console Design Guide

This new guide is intended for system administrators who initially configure a CA 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 88), has been removed from the bookshelf. It is now available with the installation package for the APIs.

CA Identity Manager and CA RCM Integration Release Notes

All release notes related to the integration between CA Identity Manager and CA RCM are located in the *CA RCM Release Notes*. You can access the CA RCM bookshelf from CA Support.

Connector Xpress On-Line Help

The Connector Xpress on-line help contains two redundant topics, Map Class and Attributes Dialog (JNDI) and Map Class and Attributes Dialog (JDBC). These topics have been replaced by the Map Class Dialog (JNDI) and the Map Class Dialog (JDBC) topics.

Appendix A: CA Identity Manager Third-Party Acknowledgements

This section contains the following topics:

AIX JRE 1.4.2

Acknowledgment:
&||&CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

This product includes portions of the the Aleksey XML Security Library v.1.2.9 distributed in accordance with the following: xmlsec, xmlsec-openssl, xmlsec-gnutls libraries.

Aleksey XML Security Library 1.2.9

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 ALEKSEY SANIN 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 Aleksey Sanin shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Apache

Portions of this product include software developed by the Apache Software Foundation.

Apache Ant 1.7

Apache Axiom 1.2.8

Apache Axis 1.1

Apache Axis 1.2

Apache Axis 1.2.1

Apache Axis 1.4

Apache Axis 1.4.1

Apache Axis2 1.4.1

Apache Axis2/Java 1.5

Apache Bean Scripting Framework 2.4.0

Apache Commons Cli 1.0

Apache Commons Cli 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, 2.5

Apache Commons Logging 1.0.4

Apache Commons Pool 1.3, 1.5.5

Apache Commons Validator 1.2

Apache ds 1.5

Google Collections 1.0

Google Data APIs Client Library

Apache HttpClient 3.1

Apache HTTP Web Server 2.0.54

Apache HTTP Web Server 2.2.3

Apache Jakarta Commons BeanUtils 1.6.1 and 1.7

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 Jakarta Taglibs 1.0.6

Apache Jakarta ORO 2.0.8

Apache Jakarta Slide 2.1

Apache JAX-RPC 1.1

Apache Jetty 6.1.26, 7.2.2

Apache Log4j 1.2.8

Apache Log4j 1.2.15, 1.2.16

Apache log4net 1.2.10

Apache log4cxx 0.10.0

Apache MyFaces 1.1.5, 1.2.6

Apache JSTL Taglib 1.1

Apache ORO 2.07, 2.08

Apache POI 3.2

Apache Quartz 1.7.3

Apache Rampart 1.3, 1.4

Apache Spring Framework 1.2.8

Apache StAX 1.2

stax-api 1.0.1

Apache Struts 1.2.7 and 1.2.9

Apache Tomahawk 1.1.8

Apache Velocity 1.4 and 1.6.2

Apache Xalan-C 1.9.0 and 1.10

Apache Xalan-J 2.6.0

Apache Xerces-C 2.5.0 and 2.6.2

Apache xmltask 1.13

ehcache 2.0.0

ehcache-core 1.2.4

ehcache-core 1.3.0

jmeter 2.3

wss4j 1.5.1

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:

boost

Boost 1.32

Boost 1.34.1

Boost 1.42

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

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, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BSAFE Crypto-C

BSAFE Crypto-C 6.2.1.8

You may not remove, alter or destroy any proprietary, trademark or copyright markings or notices placed upon or contained within the RSA Software, User Manuals or any related materials or documentation. You will insert and maintain within every CA product and any related materials or documentation a copyright notice in your name.

You agree to insert and maintain within the CA Products and marketing materials, the RSA Seal depicted in the Logo Usage Guide. You shall ensure display of the RSA Seal within any CA Product such that users are exposed to the RSA Seal during normal operation of such CA product as follows. The Seal must be in the startup splash screen and within any security-related dialog windows visible in the normal operation of the product. You must include the RSA Seal within related marketing materials including but not limited to printed and electronic data sheets, direct mail, user documentation, product packaging and advertisements for the Licensed Product.

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 1.8.0

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.

Ganymed SSH-2 for Java

This product includes Ganymed SSH-2 for Java, which is distributed in accordance with the following terms:

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.

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"

Java Architecture for XML Binding (JAXB) 2.0

Java Architecture for XML Binding (JAXB) 2.0

This product contains portions of the "Java Architecture for XML Binding" (JAXB) 2.0 (the "JAXB Component"), which was obtained under the Common Development and Distribution License v1.0 (CDDL) and other open source licenses, and is licensed to you in unmodified, binary code form under the CA license agreement. Any provisions in the CA license agreement that differ from the CDDL are offered by CA alone and not by any other party. The third party licensors of this component provide it 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, and disclaim liability for any claim or loss, including, without limitation, direct, indirect, special, punitive, exemplary or consequential damages. The source code for the JAXB Component may be found here: http://opensrcd.ca.com/ips/2584_6 or here https://jaxb.dev.java.net/.

JAX-RS v1.1.1

JAX-RS v1.1.1 is distributed by CA for use with this CA product in unmodified, object code form, under the CA license agreement. Any provisions in the CA license agreement that differ from the CDDL are offered by CA alone and not by any other party. The third party licensors of this component provide it 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, and disclaim liability for any claim or loss, including, without limitation, direct, indirect, special, punitive, exemplary or consequential damages. CA makes the source code for JAX-RS v1.1.1 available at http://opensrcd.ca.com/ips/04890_6/ under the terms of the CDDL v.1.0. license:

Open Source Initiative OSI - Common Development and Distribution License (CDDL)

[OSI Approved License]

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)

Version 1.0

1. Definitions.

   1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.

   1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

   1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

   1.4. Executable means the Covered Software in any form other than Source Code.

   1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.

   1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

   1.7. License means this document.

   1.8. 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 the Source Code and Executable form of any of the following:

A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

B. Any new file that contains any part of the Original Software or previous Modification; or

C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. 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.

1.12. Source Code means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. 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. License Grants.

2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(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 Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party 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 Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and 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 Software 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 distributes or otherwise makes the Modifications available to a third party.

(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) 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 (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. 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 that 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.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of 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 form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form 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 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.

3.6. Larger Works.

You may create a Larger Work by combining Covered Software 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 Software.

4. Versions of the License.

4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE 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 SOFTWARE 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 SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE 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 SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. 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. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initia Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. 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 SOFTWARE, 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 LOST PROFITS, 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 PARTYS 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.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) 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 Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. 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 the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, 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. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. 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.

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 7.20.1

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.

*

* 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.

Oracle JDBC Driver 11g Release 2

This Product is distributed with Oracle 11G JDBC Driver release 2 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 1.7R1

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.

slf4j 1.5.8

This product includes SLF4J 1.5.8 software and SLF4J-API 1.5.8 distributed in accordance with the following terms:

SLF4J source code and binaries are distributed under the MIT license. Copyright (c) 2004-2008 QOS.ch All rights reserved.

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 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.

These terms are identical to those of the MIT License, also called the X License or the X11 License, which is a simple, permissive non-copyleft free software license. It is deemed compatible with virtually all types of licenses, commercial or otherwise. In particular, the Free Software Foundation has declared it compatible with GNU GPL. It is also known to be approved by the Apache Software Foundation as compatible with Apache Software License.

Sun JRE

Sun Microsystems, Inc.

Binary Code License Agreement

READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

1. LICENSE TO USE. Sun grants you a non-exclusive and non-transferable license for the internal use only of the accompanying software and documentation and any error corrections provided by Sun (collectively "Software"), by the number of users and the class of computer hardware for which the corresponding fee has been paid.
2. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. Licensee acknowledges 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.
3. 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.
4. 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.

5. 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.
6. 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. Upon Termination, you must destroy all copies of Software.
7. 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.
8. 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).
9. 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.
10. 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.
11. 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.

==========

JAVATM 2 RUNTIME ENVIRONMENT (J2RE),

STANDARD EDITION,

VERSION 1.4.1_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms ("Supplemental Terms") add to or modify the terms of the Binary Code License Agreement (collectively, the "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.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (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 binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers ("Programs").

2. License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) 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 (unless otherwise specified in the applicable README file), (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. (vi) include the following statement as part of product documentation (whether hard copy or electronic), as a part of a copyright page or proprietary rights notice page, in an "About" box or in any other form reasonably designed to make the statement visible to users of the Software: "This product includes code licensed from RSA Security, Inc.", and (vii) include the statement, "Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/".

3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license 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 (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (v) 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, (vi) include the following statement as part of product documentation (whether hard copy or electronic), as a part of a copyright page or proprietary rights notice page, in an "About" box or in any other form reasonably designed to make the statement visible to users of the Software: "This product includes code licensed from RSA Security, Inc.", and (vii) include the statement, "Some portions licensed from IBM are available at http://oss.software.ibm.com/icu4j/".

4. Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional 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.

5. Notice of Automatic Software Updates from Sun. You acknowledge that the Software may automatically download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

6. Notice of Automatic Downloads. You acknowledge that, by your use of the Software and/or by requesting services that require use of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. 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 OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
7. 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.
8. Source Code. Software may contain source code that 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.
9. 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.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#133025/Form ID#011801)

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/

Xinha .96 Beta 2