CA IdentityMinder™

Release Notes

12.6

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (Formerly called CA Role & Compliance Manager)

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 1: New Features

This section contains the following topics:

New Name and Appearance

In this release, CA Identity Manager has been renamed to CA IdentityMinder. All CA Security products are being renamed to follow the product family "Minder" name. This change makes it easier to identify CA Security products, and highlights the cohesiveness of CA security solutions.

Additionally, the default User Console has been updated to reflect new CA styles and colors.

Java Connector Server (Java CS or JCS) has been renamed to CA IAM Connector Server (CA IAM CS).

Simplified User Experience

This release includes the following user experience improvements:

- Updated self-service task screens

  The following screens are updated to improve usability:

  - Portal look and feel for the Login screen
  - Self registration/Creation of identity
  - Change My Password
  - Forgotten Password Reset
  - Forgotten User ID
- Certain admin tasks use Web 2.0 controls.

Provisioning Enhancements

CA IdentityMinder 12.6 includes the following new features and changes to improve provisioning.

Provisioning Server on Linux

The Provisioning Server can now be installed on Red Hat Linux as an alternative to Solaris.

Provisioning Manager Features in the User Console

Several features of the Provisioning Manager are now supported in the User Console:

- Synchronization of users, roles, endpoint accounts, and account templates

  The integration of endpoints and accounts in CA IdentityMinder can result in lost synchronization. For example, the provisioning roles that are assigned to a user can differ from the actual accounts that are possessed by that user. Synchronization tasks correct this problem.
- Correlation rules control the mapping of endpoint account attributes to user attributes in the User Console. For example, Access Control has an attribute called AccountName. You can create a rule to map it to FullName in the User Console.

Connector Enhancements

CA IdentityMinder 12.6 includes the following new features and changes to simplify building and deploying new connectors.

Hot Deployment – Install a New Connector without Restarting CA IAM CS

CA IAM Connector Server (CA IAM CS) is the new name for Java Connector Server (or Java CS or JCS).

CA IAM CS now supports *hot deployment*. Hot deployment is the process of adding, removing or updating a component without restarting CA IAM CS. You can now do the following tasks:

- Install, uninstall, or upgrade a connector *without* restarting CA IAM CS

  You can deploy a new or updated connector and install it without restarting CA IAM CS or logging in to its host. Contact CA Support for the latest connector versions.

- Deploy third-party libraries without restarting CA IAM CS

  Some connectors require libraries that we cannot ship with CA IAM CS. Previously, you would have to deploy these libraries and then restart CA IAM CS. Now, you can deploy these libraries while the connector server is running.

  CA IAM CS includes a core set of third-party libraries, and any connector can use any of these libraries. A connector can also include any other third-party library that it requires.

Note: Hot deployment does not work for C++ connectors.

Bundle Builder – New Tool for Creating Connectors

CA IAM CS requires that connectors be supplied as an Open Services Gateway initiative bundle. The OSGi framework is a module system and service platform for the Java programming language that implements a complete and dynamic component model. The SDK for the Connector Server now includes a Bundle Builder tool, which helps you wrap your connector in a bundle.

Logging for Connectors and CA IAM CS

You can now log in to CA IAM CS to see recent log messages for CA IAM CS and its connectors. You can still use log files to see all log messages.

Certificates for Connectors and CA IAM CS

You can now log in to CA IAM CS to view and manage certificates for CA IAM CS and its connectors.

Use Connector Xpress to Map Custom Attributes and Custom Capability Attributes

Use Connector Xpress to map custom attributes and custom capability attributes. Using the XML file <jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml to map attributes is no longer available.

CA IAM CS Is a Proxy for CCS

CA IdentityMinder now uses CA IAM CS as a proxy for C++ Connector Server (CCS). CA IdentityMinder no longer communicates with CCS directly.

Performance Enhancements

CA IdentityMinder 12.6 includes performance improvements in the following areas of the product.

Bulk Loader Performance Improvements

In this release, the performance of the bulk loader is improved. The improvements include the following changes:

- Higher submission rate of tasks through the parent Bulk Loader (Feeder) task; more tasks execute in parallel.
- Optimizations in database connection reuse; managed object attribute definition caching resulting in faster execution of each task from start to end.
- Improvements to some plug-ins and listeners to speed up processing of the events that are generated during task execution.

To improve performance further, we recommend that you make these change for the duration of the bulk load operation:

- Disable any unwanted Policy Xpress policies, Business Logic Task Handlers and synchronization flags at the task level.
- Run the Bulk Loader (Feeder) task as a dedicated user with the fewest possible admin roles and admin tasks in scope.

Note: For more information about additional performance improvements, see the section on the bulk loader in the *Administration Guide*.

Improved Snapshot Export Performance

In this release, the process of exporting snapshot data for reports has been refactored to improve performance and usability. Using the Snapshot definition wizard, you can define or customize rules to load users, endpoints, admin roles, provisioning roles, groups, and organizations.

Using this feature, you can use a User Console task to select and export only the desired attributes for a particular snapshot instance. In previous releases, users had to edit an XML file manually.

Note: You can still use and customize the default XML files for capturing snapshots.

For more information about creating snapshot definitions, see the *Administration Guide*.

Secure Management Console

The Management Console enables administrators to create and manage CA IdentityMinder directories and environments.

The CA IdentityMinder installation now includes an option, which is selected by default, to secure the Management Console. During the installation, you create an account that can access the Management Console in a predefined directory.

After installation, you can add additional administrators who need access to the Management Console.

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

Policy Xpress Enhancements

This release contains the following enhancements to Policy Xpress:

- Attribute plug-ins for Managed Objects

  The following Managed Object Attribute plugins have been added to Policy Xpress:

  - Object Attribute—allows you to extract the value of any managed object attribute
  - Has the Object Attribute changed/Attribute of a Specific Object—same as 'Has the User attribute changed' and 'Attribute of a Specific User', but they work with any type of managed object
  - Set Object Attribute—allows you to modify the attribute of managed objects

- Trim Function

  The Trim function allows you to remove unwanted leading and trailing spaces from any data element or string.

- Support for More Action Rules

  Previously, when trying to add more than 60-70 action rules to a policy, Policy Xpress would not add the policy. In this case, no errors or exceptions were reported in the logs. Now, Policy Xpress policies can support up to 500 action rules.

- Policy Xpress Wiki

  The Policy Xpress documentation has been updated and now resides on a Wiki https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/wiki/-/wiki/Main/Policy+Xpress?&#p_36 in the CA Security Global User Community.

Basic Access Requests

CA IdentityMinder users can request access to services that they need to perform their job functions.

A *service* bundles together all the entitlements - tasks, roles, groups, and attributes - a user needs for a given business role. Services are available to the user through access request tasks in the CA IdentityMinder User Console. Access request tasks enable a user or administrator to request, assign, revoke and renew a service.

Services allow an administrator to combine user entitlements into a single package, which are managed as a set. For example, all new Sales employees need access to a defined set of tasks and accounts on specific endpoint systems. They also need specific information added to their user account profiles. An administrator creates a service named Sales Administration, containing all the required tasks, roles, groups, and profile attribute information for a new Sales employee. When an administrator assigns the Sales Administration service to a user, that user receives the entire set of roles, tasks, groups and account attributes that are defined by the service.

Another way users can access services is to request access themselves. In the User Console, each user has a list of services available for their request. This list is populated with services marked as "Self Subscribing" by an administrator with the appropriate privileges, typically during service creation. From the list of available services, users can request access to the services they need. When the user requests access to a service, the request is fulfilled automatically, and the associated entitlements are assigned to the user immediately. An administrator with the appropriate privileges can also configure service fulfillment to require workflow approval, or to generate email notifications.

Note: This initial release supports basic access request capabilities. Access request functionality enables end users to request entitlements (managed and un-managed by CA IdentityMinder), define approval flows, and use fulfillment flows.

This initial release does not provide support for advanced access request capabilities such as

- Bulk definition of access request services objects
- Integration with GovernanceMinder (formerly called Role and Compliance Manager)
- Granular filtering and searching

This initial release does not support the following capabilities:

- Bulk definition of services objects
- Granular filtering
- Searches
- Integration with other fulfillment mechanisms

For more information about services, see the *Administration Guide*.

New Documentation for Config Xpress

Config Xpress is a tool that is included with CA IdentityMinder. You can use this tool to analyze and work with the configurations of your CA IdentityMinder environments.

Config Xpress allows you to do these tasks:

- Move components between environments.

  The tool automatically detects any other required components, and prompts you move them too. This can save you a lot of work.
- Publish a report of the system components in a PDF file.
- Publish the XML configuration for a particular component.

For more information about importing configuration, see Manage Configuration with Config Xpress in the *Configuration Guide*.

Native CA IdentityMinder Replacement for SiteMinder Advanced Password Services

In addition to basic password policies, CA IdentityMinder provides the following additional password settings now decoupled from SiteMinder:

- Password expiration:
  - Track failed or successful logins - When enabled, tracking information for successful or failed login attempts is written to the password data attribute of the relevant user in the user store.
  - Authenticate on login tracking failure - If disabled, users are not able to log in when CA IdentityMinder cannot write tracking information to the user store.
  - Password expiration if not changed - Configures expiration behavior. If a password has not changed after a specified number of days, users are disabled or forced to change their password. Also allows expiration warnings to be sent for a specified number of days.
  - Password inactivity - Configures inactive user behavior. If the user has not made a successful login attempt after a specified number of days the user is disabled or forced to change their password.
  - Incorrect password - Configures the number of failed logins that are allowed before the user is disabled.
  - Multiple regular expressions - Specifies regular expressions that passwords must or must not match. CA IdentityMinder password policies support a single expression of each type.
- Password restrictions:
  - Minimum days before reuse
  - Minimum number of passwords before reuse
  - Percent different from last password
  - Ignore sequence when checking for differences - Ignore position of characters when calculating the percentage difference.

Note: This release does not support historical password data from a CA IdentityMinder deployment that uses CA SiteMinder password services (password history) to a deployment that includes only CA IdentityMinder r12.6 password services.

Dynamic Keys for Encrypting Data

In an environment, you can create dynamic keys that encrypt or decrypt data. If you suspect that a user gained unauthorized access to a key, you can change the password for the keystore. The keystore is the database that stores secret keys. Once you change this password, CA IdentityMinder re-encrypts the values of the keys.

The Secret Keys section of the *Administration Guide* provides details.

Active Directory Server Synchronization

CA IAM CS can be configured to let users with Active Directory Server (ADS), synchronize local identity information with cloud-based endpoint information. For example, you could set up your ADS to synchronize with a cloud-based SalesForce installation. Additions or changes to a synchronized local user group are then propagated to the SalesForce environment.

This feature requires CA IAM CS, a supported endpoint, and the appropriate connector.

Note the following about the Active Directory synchronization feature:

- This feature supports only Active Directory. Other LDAP directories are not supported for use with this feature in this release.
- This feature supports only cloud-based endpoints that have an existing connector. In this release, supported applications include Google Apps and SalesForce.

For more information about this feature, see the *Connectors Guide*.

Auditing Login and Logout Events

To improve monitoring of user access in CA IdentityMinder environment, you can configure CA IdentityMinder to audit the user login and logout events in an environment. You can view these logged events in the default Audit Details report.

Note: User login and logout events cannot be logged for CA SiteMinder.

You can configure these settings in the Audit Settings file. For more information about configuring login and logout events, see the Chapter "Auditing" in the *Configuration Guide*.

SHA-2 Support

SHA-2 SSL certificate hashing is a cryptographic algorithm developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). SHA2 certificates are more secure than all previous algorithms. In CA IdentityMinder, you can configure SHA-2 signed SSL certificates in place of certificates that are signed with the SHA-1 hash function.

Chapter 2: Installation Considerations

This section contains the following topics:

Supported Platforms and Versions

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

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

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 IdentityMinder Platform Support Roadmap on CA Support.

JDK Requirement for Linux Installations

CA IdentityMinder 12.6 requires Oracle JDK 1.6.

RedHat 6.x includes OpenJDK 1.6, which can cause the CA IdentityMinder installer to hang indefinitely. Be sure to use the required Sun JDK version, as specified in the CA IdentityMinder Support Matrix.

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 IdentityMinder with Oracle 11g R2 RAC.
- Create the database *tablespace* on the shared disk group while creating a tablespace.

AD LDS as a User Store

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

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

During CA IdentityMinder 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*

CA IdentityMinder EAR does not Auto-Deploy with WebLogic

If you are using WebLogic 9 or 10 in production mode, the CA IdentityMinder 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 IdentityMinder 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 IdentityMinder components in Windows 2008 SP2 deployments.

Deploy JSP Pages for Administrator Actions

The CA IdentityMinder 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.

Linux 64-bit: SiteMinder Connectivity Errors

Symptom:

The CA IdentityMinder 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

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

Chapter 3: Upgrade Considerations

This section contains the following topics:

Supported Upgrade Paths

The following is a list of products and versions that have a supported path for an upgrade to CA IdentityMinder 12.6:

- CA Identity Manager r12
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx

If you do not currently use one of these versions of CA Identity Manager, upgrade to one of these versions, then upgrade to CA IdentityMinder 12.6.

64-Bit Application Servers

CA IdentityMinder 12.6 supports 64-bit application servers, which provide better performance than 32-bit application servers. The following 64-bit application server versions are supported:

- 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

If CA Identity Manager currently runs on 64-bit version of one of these application servers, you can upgrade to CA IdentityMinder 12.6 by following the procedure in the *Upgrade Guide.*

If CA Identity Manager currently runs on a lower version of the application server or a 32-bit version of the application server, you uninstall CA Identity Manager and the install CA IdentityMinder on the new application server. This process is called migration.

See the *Upgrade Guide* for full details on an upgrade and migration.

EEM Connector Not Supported in CA IdentityMinder 12.6

If your environment includes the EEM Connector, you should not upgrade to CA IdentityMinder 12.6.

Contact your account manager or CA Support for more information about EEM connector availability.

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

Symptom:

If you upgrade a cluster from CA IdentityMinder 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

Upgrade from r12.5 SP6 or Earlier on WebLogic

sy>

If you upgrade from r12.5 SP6 or earlier on the WebLogic application server, you see this error on workflow startup:

```
WARN  [ims.default] * Startup Step 25 : Attempting to start SchedulerService
ERROR [ims.bootstrap.Main] The IAM FW Startup was not successful
ERROR [ims.bootstrap.Main] org.quartz.SchedulerException: JobStore class
'org.quartz.impl.jdbcjobstore.JobStoreCMT' props could not be configured.
[See nested exception: java.lang.NoSuchMethodException: No setter for
property 'lockHandler.class']
```

Solution:

1. Stop WebLogic.
2. Go to the <IAM-EAR>/APP-INF/lib folder.
3. Remove the following files:
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Start the application server.
5. The workflow startup error no longer appears.

Environment Migration Error

Symptom:

If you are upgrading from CA IdentityMinder 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 IdentityMinder 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 IdentityMinder 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 IdentityMinder r12 *or* if you upgraded from CA IdentityMinder r12.5 *and* migrated the Explore and Correlate task to the new recurrence model, 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 IdentityMinder r12 CRx, the installer displays the following message:

The installation wizard has finished upgrading CA IdentityMinder 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 IdentityMinder 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.

Rename ACF2, RACFand TSS Endpoints Before Upgrade

Spaces in endpoint names are no longer supported. If you created endpoints with spaces in the name in a previous release, remove the spaces before upgrading to 12.6.

Chapter 4: Known Issues

This chapter lists the issues that are known to exist in CA IdentityMinder 12.6. All Fixed Issues are in a separate chapter.

This section contains the following topics:

General

The following are general known issues in CA IdentityMinder 12.6.

Specifying LDAP DN When Using TEWS

Symptom:

When using TEWS to call the task "CreateOracleServerAccountTemplate" you can get back the following error message:

Error Message: <code>500</code>

<description>Failed to execute CreateOracleServerAccountTemplate. ERROR

MESSAGE: com.ca.iam.model.IAMParseException: Not a valid IAM handle:

'UHGUSERS' ProcessStep::Unknown TabName: null ERRORLEVEL::Fatal</description>

The problem is that the DN TEWS is expecting is not what is in the Provisioning Directory.

This example did not work:

eTORADirectoryName=WSDLOracle4,eTNamespaceName=Oracle Server,dc=im,dc=eta

This example is the DN that did work:

EndPoint=WSDLOracle4,Namespace=Oracle Server,Domain=im,Server=Server

Solution:

To find the mapping make sure the application server log levels are set to verbose. Execute the Identity Manager tasks for which you need the data/paths. The paths will be in the log file. Searching on "<" and "insert into IM_" can be helpful for finding the paths as well as attribute values being passed by the tasks.

ArcotID Self-Service Tasks Do Not Secure CA Identity Manager

The Create/Reset My ArcotID and Download My ArcotID tasks are incompatible with an ArcotID credential being used to secure CA IdentityMinder. These tasks cannot use the two-factor authentication method.

Self-service tasks are normally protected by SiteMinder with the URLs invoked from within a calling application. However, SiteMinder can use only one authentication scheme. So if these tasks are protected by SiteMinder, using the CA IdentityMinder username/password authentication mechanism and the calling application authenticate uses an ArcotID for authentication, the tasks do not work.

Therefore, you cannot use the ArcotID credential to secure a CA IdentityMinder environment that is protected by SiteMinder.

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.

Password Policy Issue When Using a Combined User Store and Provisioning Directory

Symptom:

CA IdentityMinder does not apply certain password policies in deployments that use a combined user store and provisioning directory. This issue occurs with password policies that include the following rules and restrictions:

- Password expiration:
  - Track failed logins or successful logins.
  - Authenticate a login.
  - Password expiration if not changed
  - Password inactivity
  - Incorrect password
  - Multiple regular expressions
- Password restrictions:
  - Minimum days before reuse
  - Minimum number of passwords before reuse
  - Percent different from last password
  - Ignore sequence when checking for differences.

This issue occurs because %PASSWORD_DATA% is mapped to a binary attribute instead of a string attribute by default.

Solution:

In the Management Console, map %PASSWORD_DATA% to any eTCustomField attribute that is not mapped to another attribute. For example, eTCustomField99.

After you update the mapping, restart the environment.

Note: For more information about updating an existing CA IdentityMinder directory, see the *Configuration Guide*.

Cannot Connect to the CA IdentityMinder server when configuring the 64-bit Active Directory Password Synchronization Agent

Symptom:

When configuring the 64-bit Password Synchronization Agent (PSA), I am unable to connect to the CA IdentityMinder server to retrieve the list of available Active Directory endpoints.

Solution:

You can configure only the ciphers that the CA IAM CS uses. Add the three new SSL FIPS ciphers to the cipher suite that CA IAM CS uses.

Follow these steps:

1. Open the following configuration file in a text editor:

   cs_home\jcs\conf\server_osgi_shared.xml

2. Locate the defaultCipherSuite property in the file. The following example code in the file:

   ```
   <property name="defaultCipherSuite"><value>FIPS_TLS_PLUS_SSL_Ciphers</value></property>
   <property name="cipherSuites">
           <map>
             <entry key="FIPS_TLS_PLUS_SSL_Ciphers">
               <list>
                 <value>TLS_RSA_WITH_AES_128_CBC_SHA</value>
                 <value>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</value>
                 <value>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</value>
                </list>
   ```

   In this example, *FIPS_TLS_PLUS_SSL_Ciphers* is the default suite that corresponds to the list of ciphers under cipherSuites property.

3. Add the following entries to the list:

   ```
   <value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</value>
   ```

4. Click Save.

5. Restart the CA IAM CS service.

   The 64-bit active directory PSA now connects without an error.

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 IdentityMinder 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 IdentityMinder 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.

Modifying Single Valued Compound Attributes in CA IdentityMinder

If you modify a single valued compound attribute in CA IdentityMinder 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.

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 IdentityMinder 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 IdentityMinder on JBoss does not Reconnect to Oracle

Symptom:

When using JBoss 5.x with an Oracle Database datasource and upgrading CA IdentityMinder 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 IdentityMinder.

Reporting

The following issues are related to reporting in CA IdentityMinder 12.6.

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.

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).

Issue While Using Multiple Filter With Endpoint Object

Symptom:

When a snapshot definition is created with Endpoint object using Multiple Filter, none of the endpoint data is captured.

Solution:

In the Snapshot Policies Tab, in place of selecting multiple endpoint objects, specify '*' asterisk to select multiple endpoint objects.

Snapshot is not Capturing Group Object Data

Symptom:

When a snapshot definition is created with a Group object using "org-filter", none of the group data is captured.

Solution:

In the Snapshot Policies Tab, in place of selecting org-filter from the drop-down, select "(all)".

General Provisioning

The following issues are general provisioning issues in CA IdentityMinder 12.6.

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.

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.

Correlation of a Microsoft SQL Endpoint Fails

Symptom:

The correlation of a Microsoft SQL endpoint fails with the following message:
Object MS SQL Logins global users creation failed. Unable to determine object class from distinguished name.

This error occurs when all containers are selected for a Microsoft SQL endpoint, not just the container with accounts.

Solution:

1. Create an Explore and Correlate definition and search for a Microsoft SQL endpoint.
2. Search for all containers but select only the *endpoint-name* as a container.
3. Select explore and correlate attributes.
4. Execute the Explore and Correlate definition.

IM--SiteMinder Login Name Restriction for Global User Name

If a user is required to log in to the 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.

CA IAM CS and Connector Xpress

The following issues are related to CA IAM Connector Server (CA IAM CS) and Connector Xpress.

Note: In CA IdentityMinder 12.6, Java Connector Server (Java CS or JCS) has been renamed to CA IAM Connector Server (CA IAM CS).

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 IdentityMinder 12.6.

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 CA IAM CS should be configured to have a generous (or unlimited) "N" due to attempts to connect being used up quickly by CA IAM 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

Removing Groups from an Access Control Account

Symptom:

When you remove a native group from a native user account that the Access Control Connector provisioned, the native groups are removed in a two-step process. The two-step process removes all existing group memberships and then adds back all required group memberships. This results in the correct group membership for the account, but can cause operational concerns for some customers.

Solution:

If you do not want to use the two-step process, you can use Connector XPress to create a C++ Connector Server (CCS) definition. The CCS definition can connect to the Provisioning Server directly, instead of routing through the CA IAM CS. This workaround results in one-step group modification for ACC accounts. However, you cannot use the User Console to manage ACC account group membership. To manage ACC account group membership, use the Provisioning Manager.

Note: For information about using Connector Xpress to create a C++ Connector Server definition, see How you Set a Managing Connector Server in the *Connector Xpress Guide*.

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.

CA SSO Connector for Advanced Policy Server

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

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*.

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—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 IdentityMinder and on the Google Apps endpoint, but it is not visible in the CA IdentityMinder 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 IdentityMinder 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 CA IAM CS, use the same proxy server, port, user name, and password for all the Google Apps endpoints on the same CA IAM 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, CA IAM CS is installed as a Windows Service and runs as Local System by default.

If CA IAM 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 CA IAM CS to run under a Windows domain account or a Windows local account.

To configure NTLM authentication

Do either of the following:

- Run CA IAM 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 CA IAM 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.

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 IdentityMinder 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.

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.

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.

Chapter 5: Documentation

This section contains the following topics:

Bookshelf

The Bookshelf provides access to all CA IdentityMinder 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.

CA IdentityMinder and CA RCM Integration Release Notes

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

Appendix A: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of CA IdentityMinder.

508 Compliance

CA IdentityMinder complies with Section 508 of the US Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG2.0) at the AA level. The Product Enhancements (see page 57) topic provides more details. You can also ask your account manager for a copy of CA Technology's Voluntary Product Accessibility Template (VPAT).

Product Enhancements

CA IdentityMinder offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse

Note: The following information applies to Windows-based and Macintosh-based applications. Java applications run on many host operating systems, some of which already have assistive technologies available to them. For these existing assistive technologies to provide access to programs written in JPL, they need a bridge between themselves in their native environments and the Java Accessibility support that is available from within the Java virtual machine (or Java VM). This bridge has one end in the Java VM and the other on the native platform, so it will be slightly different for each platform it bridges to. Sun is currently developing both the JPL and the Win32 sides of this bridge.

Display

To increase visibility on your computer display, you can adjust the following options:

Font style, color, and size of items

Lets you choose font color, size, and other visual combinations.

Screen resolution

Lets you change the pixel count to enlarge objects on the screen.

Cursor width and blink rate

Lets you make the cursor easier to find or minimize its blinking.

Icon size

Lets you make icons larger for visibility or smaller for increased screen space.

High contrast schemes

Lets you select color combinations that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

Volume

Lets you turn the computer sound up or down.

Text-to-Speech

Lets you hear command options and text read aloud.

Warnings

Lets you display visual warnings.

Notices

Gives you aural or visual cues when accessibility features are turned on or off.

Schemes

Lets you associate computer sounds with specific system events.

Captions

Lets you display captions for speech and sounds.

Note: If you are using a screen reader, we recommend that you install the latest version of the screen reader tool for better interpretation.

Keyboard

You can make the following keyboard adjustments:

Repeat Rate

Lets you set how quickly a character repeats when a key is struck.

Tones

Lets you hear tones when pressing certain keys.

Sticky Keys

Lets those who type with one hand or finger choose alternative keyboard layouts.

Skip Link

Lets you use the Skip to main content link for a quick navigation to the main content.

Mouse

You can use the following options to make your mouse faster and easier to use:

Click Speed

Lets you choose how fast to click the mouse button to make a selection.

Click Lock

Lets you highlight or drag without holding down the mouse button.

Reverse Action

Lets you reverse the functions controlled by the left and right mouse keys.

Blink Rate

Lets you choose how fast the cursor blinks or if it blinks at all.

Pointer Options

Let you do the following:

- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Choose the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Keyboard Shortcuts

The following table lists the keyboard shortcuts that CA IdentityMinder supports:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+K	Find Next
Ctrl+F	Find and Replace
Ctrl+V	Paste
Ctrl+S	Save
Ctrl+Shift+S	Save All
Ctrl+D	Delete Line
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End