

# CA IdentityMinder™

Release Notes  
r12.6.2



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 © 2013 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 CloudMinder™ Identity Management
- CA Directory
- CA IdentityMinder™
- CA GovernanceMinder (formerly CA Role & Compliance Manager)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

## 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](mailto: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	9
12.6.2.....	9
New Certifications.....	10
Mobile App Support.....	11
Synchronization/Remove Account Template Values From Accounts.....	11
New Configurable Settings for the LND Connector.....	12
Task Persistence Database Schema.....	12
Support for Deactivating SAP Account Password.....	12
Two Modes for Connecting to Exchange: Agentless and Agent.....	13
Support for Exchange Data Access Groups (DAG).....	13
Support for Automatic Mailbox Distribution in Exchange 2010.....	13
Connect to SQL Server When the Database is Offline.....	13
Task to Create a Snapshot Definition for Reports.....	14
12.6.1.....	14
New Certifications.....	14
SSL-Enabled JNDI User Store.....	15
Encrypted Password Support in Management Console Bootstrap Directory.....	15
12.6.....	15
New Name and Appearance.....	16
Simplified User Experience.....	16
Provisioning Enhancements.....	16
Connector Enhancements.....	17
Performance Enhancements.....	18
Policy Xpress Enhancements.....	20
Secure Management Console.....	20
Basic Access Requests.....	21
New Documentation for Config Xpress.....	23
Native CA IdentityMinder Replacement for SiteMinder Advanced Password Services.....	24
Dynamic Keys for Encrypting Data.....	25
Active Directory Server Synchronization.....	25
Auditing Login and Logout Events.....	25
SHA-2 Support.....	26
Chapter 2: Installation Considerations	27
Supported Platforms and Versions.....	27
Co-installation of Unix Remote Agents with Additional CA Products.....	28

---

Deprecated and Dropped Components .....	28
Passwords Not Encrypted .....	28
Oracle 11g R2 RAC as User Store and Object Store.....	28
AD LDS as a User Store .....	29
Non-ASCII Character Causes Installation Failure on Non-English Systems .....	29
Linux: JDK Requirement for Installation .....	29
Linux: Provisioning Directory Installation.....	30
Linux 64-bit: SiteMinder Connectivity Errors .....	30
Work Around Firewall on Windows 2008 SP2 .....	30
Deploy JSP Pages for Administrator Actions .....	31
Improve Performance on WebSphere and AIX .....	31
Ignore WebSphere 7/Oracle Error .....	32

## Chapter 3: Upgrade Considerations 33

Supported Upgrade Paths .....	33
New Scripts to Update the Task Persistence and Archive Schemas.....	33
New Active Directory Role Definition File .....	34
Update to jboss.xml File .....	34
64-Bit Application Servers .....	35
Upgrade from r12 (CR6 or later) Fails on Some Clusters .....	35
Workflow Error after Upgrade from pre-r12.5 SP7.....	36
Environment Migration Error .....	37
Credential Provider Upgrade Error .....	37
Credential Provider Internal Error.....	37
No Search Screen with Explore and Correlate Task .....	38
Non-Fatal Error after Upgrading Provisioning Manager from r12 .....	38
Rename ACF2, RACF and TSS Endpoints Before Upgrade .....	38
Run the SQL Upgrade Script .....	39

## Chapter 4: Known Issues 41

General.....	41
Connection Errors After CA IdentityMinder Server Upgrade.....	41
Warning Message When Running an OOTB Snapshot DDL Script .....	42
Non-Context Sensitive Help for Mobile App .....	43
Provisioning Directory Fails to Create through Management Console .....	43
AttributeLevelEncryption for User Passwords .....	44
Specifying LDAP DN When Using TEWS .....	45
setpasswd Fails on 64-bit Linux Systems.....	45
Password Policy Issue When Using a Combined User Store and Provisioning Directory.....	46
Cannot Connect to the CA IdentityMinder server when configuring the 64-bit Active Directory Password Synchronization Agent.....	47

---

Workflow Participant Resolver Fails for EnableUserEventRoles .....	48
Duplicate name in View Submitted Tasks .....	48
Not Found Error When Creating a New Environment .....	48
Modifying Single Valued Compound Attributes in CA IdentityMinder .....	49
Limitations of Bulk loader in Relationship Attribute Level .....	50
Error Creating Provisioning-Enabled Environment using Tokenized Template .....	50
Oracle Applications Prerequisite.....	50
Oracle 11gR2 RAC User Store: Search is Case-Sensitive .....	50
CA IdentityMinder on JBoss does not Reconnect to Oracle.....	51
Skip to Main Content Fails in Mozilla Firefox.....	51
Concurrent Changes to a User Fails .....	51
Change to Policy Xpress Syntax.....	52
Update to SAP Help Topic .....	52
Enable the Fix for Oracle Bug 6376915 .....	53
Reporting.....	53
User Filter Search is Case Sensitive in the User Accounts and the Endpoint Accounts Custom	
Snapshots XML Files .....	53
Satisfy=All Not Working Properly in XML File .....	54
Issue While Using Multiple Filter With Endpoint Object.....	54
Snapshot is not Capturing Group Object Data .....	54
General Provisioning .....	54
Renaming Provisioning Roles not Supported.....	54
Solaris ECS Logging Above INFO Level Can Affect the Performance of the Provisioning Server.....	55
Already Exists Error When Adding an Endpoint .....	55
Correlation of a Microsoft SQL Endpoint Fails .....	55
CA SiteMinder Login Name Restriction for Global User Name .....	56
CA IAM CS and Connector Xpress.....	56
JNDI Account Management Screens – Creating Accounts with Multiple Structural objectclasses Fails.....	56
Endpoint Types.....	56
General.....	56
CA Access Control .....	60
CA Arcot .....	61
CA SSO Connector for Advanced Policy Server .....	61
DB2 and DB2 for z/OS .....	61
Google Apps .....	62
Microsoft Active Directory and Exchange .....	64
PeopleSoft.....	64
SAP .....	64
Siebel.....	65

---

Chapter 5: Fixed Issues	67
12.6.2.....	67
12.6.1.....	68
Chapter 6: Documentation	71
Bookshelf.....	71
CA IdentityMinder and CA RCM Integration Release Notes .....	71
Appendix A: Accessibility Features	73
508 Compliance.....	73
Product Enhancements .....	73

# Chapter 1: New Features

---

This section contains the following topics:

[12.6.2](#) (see page 9)

[12.6.1](#) (see page 14)

[12.6](#) (see page 15)

## 12.6.2

[New Certifications](#) (see page 10)

[Mobile App Support](#) (see page 11)

[Synchronization/Remove Account Template Values From Accounts](#) (see page 11)

[New Configurable Settings for the LND Connector](#) (see page 12)

[Task Persistence Database Schema](#) (see page 12)

[Support for Deactivating SAP Account Password](#) (see page 12)

[Two Modes for Connecting to Exchange: Agentless and Agent](#) (see page 13)

[Support for Exchange Data Access Groups \(DAG\)](#) (see page 13)

[Support for Automatic Mailbox Distribution in Exchange 2010](#) (see page 13)

[Connect to SQL Server When the Database is Offline](#) (see page 13)

[Task to Create a Snapshot Definition for Reports](#) (see page 14)

## New Certifications

The following new platforms are certified with CA IdentityMinder r12.6.2:

### Endpoints

- CA ControlMinder r12.6 SP2 as an endpoint
- CA ControlMinder r12.7 as an endpoint
- Windows Server 2012 as an NT endpoint
- Windows Server 2012 (ADAM) as a JNDI endpoint
- CA Directory r12.0 SP11 as a JNDI endpoint
- Windows Server 2012 Active Directory as an endpoint
- Java Mainframe Connector as an endpoint
- Microsoft AD Exchange Server 2010 SP3 as an endpoint
- Microsoft Office 365 as an endpoint
- SAPJCO V.3 as an endpoint

### Application Servers

- JBoss 6.1 EAP
- WebSphere Application Server (WAS) 8.0
- WebSphere Application Server (WAS) 8.5

### CA IdentityMinder User Store

- CA Directory r12.0 SP11 GA

### CA IdentityMinder User Store and Object Store

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

**Note:** JBoss has not announced support for Microsoft SQL Server 2012.

### Additional Support

- Java JDK 1.7.x
- Microsoft SQL Server 2012 SP1 user-defined roles and user-defined Server Roles
- Mozilla Firefox 18.x
- Business Objects Report Server XI 3.1 SP6 (CABI 3.3 SP1)
- Integration with CA SiteMinder r12.5 CR1, r12.5 CR2, r12.5.1, r12.0 SP3 CR12 and r6 SP6 CR10

- Integration with CA IdentityMinder with CA GovernanceMinder r12.5 SP8 and CA GovernanceMinder r12.6 SP1
- Mobile App support
- Support for Workpoint designer version 3.4.2.20080602-33
- Support for Microsoft ADS/Exchange Agentless mode, DAG, and Automatic Mailbox Distribution
- CA AuthMinder v7.1 support

## Mobile App Support

The CA IdentityMinder mobile app enables you to leverage your existing CA IdentityMinder infrastructure to allow users to complete the following tasks in a mobile device, such as an iPhone or iPad:

- Reset a forgotten password  
**Note:** When you enable mobile users to reset a forgotten password from their device, CA IdentityMinder relies on the device security, instead of security questions. Consider requiring more device security, such as a passcode before you enable password reset functionality.
- Change a password
- Respond to approval requests
- View manager details

This feature allows users who approve workflow requests to view information about a user's manager.

**Note:** CA IdentityMinder r12.6.2 does not support version 1.0 of the mobile app. Download the latest version from the Apple store.

For more information about the mobile app, see the *Administration Guide*.

## Synchronization/Remove Account Template Values From Accounts

You can now use the Synchronization/Remove Account Template Values From Accounts feature on the Responsibilities List attribute of Oracle Applications Account Template, to expire a responsibility entry on the Oracle Applications account.

Additionally, this release includes improvements to responsibility calculations to prevent "out of sync" errors.

For more information about the feature, see Responsibilities List and Account Synchronization in the *Connectors Guide*.

## New Configurable Settings for the LND Connector

To improve the performance of LND Connector during Explore and Correlate operations, the following configurable settings are now available:

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

**Note:** You can change the values of the above attributes in the following file:

`CA\Identity Manager\Connector Server\conf\override\lndconnector.xml`

## Task Persistence Database Schema

This release includes improvements to the SQL scripts that update the Task Persistence DB schema. The scripts set the correct column size and insert the Runtime Status Detail stored procedure.

In this update, there are no size discrepancies between the runtimeStatusDetail12 table and the corresponding archive\_runtimeStatusDetail12 table for new or upgraded systems. This update eliminates the failures with the Cleanup Submitted Tasks task.

## Support for Deactivating SAP Account Password

In this release, the Password Deactivated attribute is now available on the Account tab. Using this attribute, you can create an SAP account with a deactivated password. You can also deactivate the password of an existing SAP account. To reactivate, reset the password.

## Two Modes for Connecting to Exchange: Agentless and Agent

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

However, agentless mode does not work with Exchange 2003 and you must connect using the remote agent.

The following table lists the supported versions of Exchange for Agent and Agentless modes:

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

## Support for Exchange Data Access Groups (DAG)

In this release, Exchange 2010 can use Data Access Groups (DAGs) to ensure the 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

In this release, the Active Directory (AD) Exchange connector can handle an automatic mailbox distribution in Exchange 2010.

When you create or move a mailbox or mailenable an existing user, the mailbox must be stored in a mailbox database. Earlier Exchange Servers required you to specify the mailbox database for performing one of the above operations. Exchange Server 2010 selects the Exchange select the database using automatic mailbox distribution.

## Connect to SQL Server When the Database is Offline

You can now explore and correlate an SQL Server endpoint when its database is offline.

## Task to Create a Snapshot Definition for Reports

We now recommend that you use the Create Snapshot Definition task to create a snapshot for the data needed to build a report. The default snapshot XML parameter files are being phased out. For details, see the *Administration Guide*.

### 12.6.1

[New Certifications](#) (see page 14)

[SSL-Enabled JNDI User Store](#) (see page 15)

[Encrypted Password Support in Management Console Bootstrap Directory](#) (see page 15)

## New Certifications

The following new platforms are certified with CA IdentityMinder r12.6.1:

### Endpoints

- Microsoft SQL 2012 as a static and dynamic endpoint
- CA Directory r12 SP10 CR2 as a JNDI endpoint
- CA Embedded Entitlements Manager (EEM) - supported by Provisioning Manager

### CA IdentityMinder User Store

- CA Directory r12 SP10 CR2

### CA IdentityMinder User Store and Runtime Store

- Microsoft SQL Server 2012 SP1

### Additional Support

- Mozilla Firefox 14.x
- Business Objects Report Server XI 3.1 SP5 (CA Business Intelligence 3.3)  
This version matches the version supported by CA CA SiteMinder
- Support of the Report Server in a high availability configuration
- Support of CA IdentityMinder with CA GovernanceMinder (CA RCM) r12.6
- Support of CA IdentityMinder with CA SiteMinder r12.0 SP3 CR11

---

## 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 IdentityMinder JRE default trusted keystore. The keystore is the cacerts or jssecacerts file in this location:

```
JAVA_HOME\jre\lib\
```

Use the JDK's utility keytool to add the certificate.

## Encrypted Password Support in Management Console Bootstrap Directory

If you secure the Management Console using the bootstrap directory, called the AuthenticationDirectory, you can now encrypt the password for the Management Console administrator.

## 12.6

[New Name and Appearance](#) (see page 16)

[Simplified User Experience](#) (see page 16)

[Provisioning Enhancements](#) (see page 16)

[Connector Enhancements](#) (see page 17)

[Performance Enhancements](#) (see page 18)

[Policy Xpress Enhancements](#) (see page 20)

[Secure Management Console](#) (see page 20)

[Basic Access Requests](#) (see page 21)

[New Documentation for Config Xpress](#) (see page 23)

[Native CA IdentityMinder Replacement for SiteMinder Advanced Password Services](#) (see page 24)

[Dynamic Keys for Encrypting Data](#) (see page 25)

[Active Directory Server Synchronization](#) (see page 25)

[Auditing User Login and Logout Events](#) (see page 25)

[SHA-2 Support](#) (see page 26)

## 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
- Deploy third-party libraries 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.

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*.

## 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 Value 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](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.

## 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*.

## 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* 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 Manage 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](#) (see page 27)
- [Co-installation of Unix Remote Agents with Additional CA Products](#) (see page 28)
- [Deprecated and Dropped Components](#) (see page 28)
- [Passwords Not Encrypted](#) (see page 28)
- [Oracle 11g R2 RAC as User Store and Object Store](#) (see page 28)
- [AD LDS as a User Store](#) (see page 29)
- [Non-ASCII Character Causes Installation Failure on Non-English Systems](#) (see page 29)
- [Linux: JDK Requirement for Installation](#) (see page 29)
- [Linux: Provisioning Directory Installation](#) (see page 30)
- [Linux 64-bit: SiteMinder Connectivity Errors](#) (see page 30)
- [Work Around Firewall on Windows 2008 SP2](#) (see page 30)
- [Deploy JSP Pages for Administrator Actions](#) (see page 31)
- [Improve Performance on WebSphere and AIX](#) (see page 31)
- [Ignore WebSphere 7/Oracle Error](#) (see page 32)

## 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](#).

## Co-installation of Unix Remote Agents with Additional CA Products

In this release, the UNIX Remote Agents (except for TRU64 platforms) are now installed such that the installed software tracks the dependent software components, such as CA ITCM.

If you want to upgrade the UNIX Remote Agent, the new tracking method does not update the reference counts of dependent software components. If you want to uninstall the product after this upgrade, use the following de-install file:

```
<install-dir>/scripts/uninstall-force.sh
```

**Note:** Ensure that the `uninstall-force.sh` is not used on hosts that have additional CA software installed. The products may depend on the 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 IdentityMinder Deprecation Policy](#) on CA Support.

## Passwords Not Encrypted

New installations do not encrypt user passwords by default. Also, when CA SiteMinder is integrated with CA IdentityMinder, you cannot enable password encryption by using `AttributeLevelEncrypt`. This attribute only works when CA SiteMinder is not installed.

This issue will be corrected at a future release.

## 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: JDK Requirement for Installation

CA IdentityMinder r12.6.2 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](#).

## 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: 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-INFra.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
```

## 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.

## 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](#) (see page 33)
- [New Scripts to Update the Task Persistence and Archive Schemas](#) (see page 33)
- [New Active Directory Role Definition File](#) (see page 34)
- [Update to jboss.xml File](#) (see page 34)
- [64-Bit Application Servers](#) (see page 35)
- [Upgrade from r12 \(CR6 or later\) Fails on Some Clusters](#) (see page 35)
- [Workflow Error after Upgrade from pre-r12.5 SP7](#) (see page 36)
- [Environment Migration Error](#) (see page 37)
- [Credential Provider Upgrade Error](#) (see page 37)
- [Credential Provider Internal Error](#) (see page 37)
- [No Search Screen with Explore and Correlate Task](#) (see page 38)
- [Non-Fatal Error after Upgrading Provisioning Manager from r12](#) (see page 38)
- [Rename ACF2, RACF and TSS Endpoints Before Upgrade](#) (see page 38)
- [Run the SQL Upgrade Script](#) (see page 39)

## Supported Upgrade Paths

You can upgrade to CA IdentityMinder r12.6.2 from the following versions:

- CA Identity Manager r12
- CA Identity Manager r12.5 or 12.5 SPx
- CA IdentityMinder r12.6 or 12.6 SPx

If you have a pre-r12 version of CA Identity Manager, first upgrade to r12, r12.5, or r12.5 SP1 to SP6. These versions include the `imsconfig` tool, which is required to upgrade a pre-r12 version. Then you can upgrade to CA IdentityMinder r12.6.2.

## New Scripts to Update the Task Persistence and Archive Schemas

This release includes new scripts to update the Task Persistence and Archive schemas. The update runs automatically when you start CA IdentityMinder first time after an upgrade. For more information about the new scripts, see the *Installation Guide*.

## New Active Directory Role Definition File

Be sure that you import the new role definition file for Active Directory into each environment. The current CA IdentityMinder environment may have an earlier release of the Active Directory Role definition file. So import the file to upgrade the role definitions to 1.08. For details about importing role definition files, follow the procedures in the *Upgrade Guide*.

## Update to jboss.xml File

During a JBoss restart or CA IdentityMinder initialization, many errors messages are logged to the CA IdentityMinder server.log file. These messages are related to events managed by JMX, but the receiving message bean is not yet initialized. To correct this problem, the following file now includes a depends clause:

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

The depends clause is included in this section:

```
<message-driven>  
<ejb-name>SubscriberMessageEJB</ejb-name>  
<destination-jndi-name>queue/iam/im/jms/queue/com.netegrity.ims.msg.queue  
</destination-jndi-name>  
<depends>jboss.web.deployment:war=/iam/im</depends>  
</message-driven>
```

Be sure to include this section in your jboss.xml file. The result is the receiving message bean is initialized before JMX starts to process the event queue.

## 64-Bit Application Servers

CA IdentityMinder r12.6.2 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, 5.1, and 6.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0, 8.0, 8.5

If CA Identity Manager currently runs on 64-bit version of one of these application servers, you can upgrade to CA IdentityMinder r12.6.2 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.

## 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

## Workflow Error after Upgrade from pre-r12.5 SP7

### Symptom:

If you upgrade from a pre-r12.5 SP7 system 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, RACF and 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.

## Run the SQL Upgrade Script

After the upgrade, the first time you start the CA IdentityMinder server, a script executes. It updates the Task Persistence table runtimeStatusDetail12 Description column size to 2000 characters.

If the script fails to run, follow these steps:

1. Do one of the following:
  - Microsoft SQL Server: Open the Query Analyzer tool and select the script you need.
  - Oracle: Open the SQL prompt for the script you need.
2. Select one of the following scripts:
  - Microsoft SQL Server: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\sqlserver\archive\_db\_sqlserver\_upgrade\_to126sp2.sql
  - Oracle on Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\db\taskpersistence\oracle9i\archive\_db\_oracle\_upgrade\_to126sp2.sql
  - Oracle on UNIX:  
/opt/CA/IdentityManager/IAM\_Suite/Identity\_Manager/tools/db/taskpersistence/oracle9i/archive\_db\_derby\_upgrade\_to126sp2.sql
3. Run the script file.
4. Verify that no errors appeared when you ran the script.



# Chapter 4: Known Issues

---

This chapter lists the issues that are known to exist in CA IdentityMinder r12.6.2. All Fixed Issues are in a separate chapter.

This section contains the following topics:

[General](#) (see page 41)

[Reporting](#) (see page 53)

[General Provisioning](#) (see page 54)

[CA IAM CS and Connector Xpress](#) (see page 56)

[Endpoint Types](#) (see page 56)

## General

The following are general known issues in CA IdentityMinder r12.6.2.

### Connection Errors After CA IdentityMinder Server Upgrade

**Symptom:**

Connect error when accessing CA RCM from CA IdentityMinder after upgrade of an existing installation.

**Solution:**

After CA IdentityMinder server upgrade more configuration is required.

**Follow these steps:**

1. In the CA IdentityMinder User Console, go to System, Web Services, Delete Web Services Configuration, Search.
2. Delete the IMRCM configuration.
3. Log in to the CA RCM web portal.
4. Go to Administration, Universes and select the universe configured to integrate with CA IdentityMinder.
5. Go to Connectivity tab and select the CA IdentityMinder connector.

Click Test and confirm that the connection is successful.

## Warning Message When Running an OOTB Snapshot DDL Script

### Symptom:

The following sql script produces an invalid index when run on a Microsoft SQL database:

IdentityManager/IAM\_Suite/IdentityManager/tools/imlexport/db/SqlServer/ims\_mssql\_report.sql

The script returns with the following warning message:

**Warning! The maximum key length is 900 bytes. The index 'imruser6\_index\_3' has maximum length of 1260 bytes. For some combination of large values, the insert/update operation will fail.**

### Solution:

#### Follow these steps:

1. Use the following code to create a stored procedure:

```
CREATE PROCEDURE sp_imruser6_index_3_exists
AS
BEGIN
DECLARE @MAX_LEN integer
DECLARE @sql_cmd nvarchar(255)
DECLARE @stmt nvarchar(255)
SET @MAX_LEN = (SELECT SUM(max_length)AS TotalIndexKeySize FROM
sys.columns WHERE name IN (N'imr_userdn', N'imr_reportid') AND object_id =
OBJECT_ID(N'imruser6'))
IF EXISTS (SELECT name FROM sysindexes WHERE name =
'imruser6_index_3') DROP INDEX imruser6_index_3 on imruser6
IF (@MAX_LEN > 900)
CREATE INDEX imruser6_index_3 ON imruser6 (imr_reportid)
INCLUDE(imr_userdn)
ELSE
CREATE INDEX imruser6_index_3 ON imruser6 (imr_reportid, imr_userdn)
END
GO
```

Stored procedure is now created.
2. Use the following command to run the stored procedure:

```
EXEC sp_imruser6_index_3_exists
```

After successfully executing the stored procedure, the column imr\_userdn under imruser6\_index\_3 becomes as included column.

## Non-Context Sensitive Help for Mobile App

**Symptom:**

When a user clicks the help icon while performing mobile app tasks, unrelated help displays.

**Solution:**

Browse for mobile app help in the table of contents or by searching the help.

## Provisioning Directory Fails to Create through Management Console

When creating a Provisioning Directory through Management Console, the Provisioning Server domain name field does not allow foreign language characters as the domain name. You may see the following error message:

“could not connect to the LDAP server machinename:20389 with userDN etGlobalUserName=admin,eTGlobalUserContainerName:GlobalUsers,eTNamespacename=CommonObjects,dc=foreignChars, dc=eta and specified password.”

## AttributeLevelEncryption for User Passwords

When you specify the AttributeLevelEncryption data classification for attributes in the directory configuration file (directory.xml), CA IdentityMinder encrypts the attribute value in the user store. In the User Console, the value appears in clear text.

The following attribute description shows the AttributeLevelEncryption data classification:

```
<ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title"
valuetype="String" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

In environments with the following configuration, enabling attribute level encryption for passwords prevents users from logging in:

- CA IdentityMinder integrates with CA SiteMinder, and
- The user store is a relational database

In this release, the AttributeLevelEncryption data classification is removed from the password attribute in the following directory configuration (directory.xml) files:

- DirectoryTemplates/RelationalDatabase.xml
- fwSampleRDB.xml
- Samples/NeteAutoRDB/NoOrganization.xml
- Samples/NeteAutoRDB/Organization.xml

These files are located in the *admin\_tools* directory.

**Note:** For more information on managing sensitive attributes, see the *Configuration Guide*.

## 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.

## 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>
    </entry>
  </map>
</property>
```

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.

## Skip to Main Content Fails in Mozilla Firefox

**Symptom:**

At the top of the User Console, you see a Skip to main content link. This link moves the main frame of the page to the top. However, this link fails in Mozilla Firefox.

**Solution:**

Use Microsoft Internet Explorer 8 or higher with JAWS to support this feature.

## Concurrent Changes to a User Fails

A modify user task fails in these situations:

- If you try to disable a user while modifying that user, the task fails.
- If you add the `forcePasswordChange` attribute to the User Profile screen while modifying a user, the task fails.

## Change to Policy Xpress Syntax

### Symptom:

Due to a change to Policy Xpress syntax, an error can occur. It occurs if the policy uses string parsing for the account identifier and the user has multiple accounts on a flat endpoint. Endpoints such as Oracle, OS400, and Microsoft SQL have accounts as a virtual container, which sit below the endpoint name. Starting at 12.6.1, the syntax of account identifier is as follows:

- For flat connectors, EndpointName: EndpointName:AccountName
- For hierarchical connectors, EndpointName:AccountContainerPath:AccountName

### Solution:

Locate Policy Xpress policies that use string parsing for the account identifier. Update those policies to conform to the new syntax.

## Update to SAP Help Topic

The help for the defaults tab related to SAP r3 accounts should have this definition for Decimal Notation.

- Specifies the different ways to represent decimal notations.
- You can choose from the following:
  - 1.234.567,89
  - 1,234,567.89
  - 1 234567,89

---

## 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 IdentityMinder 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 IdentityMinder and CA CloudMinder.
  - Measure the wait time for HW enqueue contention.

## Reporting

The following issues are related to reporting in CA IdentityMinder r12.6.2.

### 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 r12.6.2.

### 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.

## 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.

## 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 r12.6.2.

## General

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

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

This section applies to all of the TSS connectors.

Consider an endpoint that has 'N' retry autolock behavior. The account that is 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 is acquired again. This situation depends on the exact native "locked" behavior of the endpoint.

## Error in Endpoint Search Screens after Upgrading from CA Identity Manager r12.5 SP6 or Earlier

This section applies to all of the TSS connectors.

### **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 upgrading to r12.5 SP7 or later, an error can occur when you import role definitions files that include screens referring to the old object names.

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

**Solution:**

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

**The following case is an example of an Active Directory endpoint:**

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">
```

## 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.

This section applies to all of the TSS connectors.

When the endpoint is modified directly (not using the Provisioning Server), a failure is returned when importing. This failure is 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. The 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.

## Restriction on the Endpoint Name for ACF2 ACFESAGE, RACF IRRDBU00, and TSSCFE connectors

### Symptom:

Attempting to create an endpoint with an endpoint name such as "user test", "user-test", and "\_usertest" on dumpfile connectors causes endpoint creation to fail with the message: 'Cannot create pool able connection factory'.

### Solution:

Space characters are no longer allowed in endpoint names for the ACF2 ACFESAGE, TSSCFE, or RACF IRRDBU00 connectors. The endpoint name for these connectors also has the following restrictions:

- Must be between 1 and 30 characters in length
- Starts with the alphanumeric characters
- Contains only alphanumeric and/or "\_" character only.

Before you upgrade to this version, delete the existing mainframe dumpfile endpoints which are not according to the given restrictions.

## CA Access Control

### Text for Calender Window Buttons are Shown in English

When creating an account template in the CA access control endpoint, the OK and CANCEL buttons in the calender window appear in English under the Login tab.

### 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*.

---

## CA Arcot

### Protecting ArcotID Tasks When CA SiteMinder Protects CA CloudMinder or CA IdentityMinder

If CA SiteMinder protects CA CloudMinder or CA IdentityMinder using a CA AuthMinder authentication scheme, the following tasks are disabled in CA CloudMinder or CA IdentityMinder:

- Create/Reset My ArcotID
- Download My ArcotID

This is because CA SiteMinder defines one authentication scheme for a protected resource. All CA IdentityMinder-protected tasks have the same URL, which is protected by one CA SiteMinder authentication scheme. This means that all CA CloudMinder or CA IdentityMinder tasks are covered by the same authentication scheme.

When ArcotID authentication protects the CA CloudMinder or CA IdentityMinder URL, users have to provide an ArcotID to access tasks. Users who access the tasks listed above do not have an ArcotID yet, so they cannot provide it to access the tasks.

When CA SiteMinder protects CA CloudMinder or CA IdentityMinder tasks, use an authentication scheme other than Arcot, such as Active Directory or LDAP, to prevent this issue.

**Note:** Create/Reset My ArcotID or Download My ArcotID are sensitive tasks. CA Technologies strongly recommends that you configure these tasks as protected tasks. If you configure these tasks as public tasks, users can access them without providing credentials. For more information about public tasks, see [Self-Service Tasks](#) in the User Console Design Guide.

## 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*.

## 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.

## Account search failure from Google Apps

**Symptom:**

Searching for a Google Apps account based on the first or last name fails.

**Solution:**

Updates to a user's first name or last name may take up to 30 minutes to be processed by Google Apps. Therefore, searching for the new name in CA IdentityMinder fails. Wait 30 minutes after a name change before using the new name in the search.

## Microsoft Active Directory and Exchange

The known issues for Active Directory and Exchange are now in the *Endpoint Guide for Active Directory and Exchange*. You can download this guide from [CA Support](#).

## 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: Fixed Issues

---

This section contains the following topics:

[12.6.2](#) (see page 67)

[12.6.1](#) (see page 68)

## 12.6.2

The following issues are fixed in CA IdentityMinder 12.6.2:

Support Ticket	Problem Reported
21198613/01	Password set by PX is not synchronized to global user and accounts.
21230281/01	Unable to import Logical Attribute Handlers in the Management Console.
21263275/01	Issues with Arcot Password policy.
21269108/02	Issues with installation of CA IdentityMinder r12.6 Password Synchronization agent.
21264877/01	Admin DN is getting appended to the External URL.
21275958/01	Null Pointer Exception while acquiring SAP endpoint.
21272983/01	Errors while reading CA Access Control endpoint with multiple Policy Model Databases (PMDBs) defined.
21173122/01	Imported rolesDef is not displayed.
21270763/01	Error occurs when a provision directory is created using wizard.
21280342/01	DoSynchUserRoles is not enabling the checkboxes for "add missing accounts" and "remove extra accounts" to the CA IdentityMinder Task Execution Web Service (TEWS) Web Services Description Language (WSDL).
21285651/01	'Synchronize Accounts with Account Template' task compatibility with TEWS.
21295778/01	"Error instantiating Policy Xpress plugin" error occurs when trying to create or modify any Policy Xpress policies.
21304316/01	Performance issue while adding groups to a user using create or modify user task.
21304316/02	Performance issue when adding groups to user, using Add Groups button on Modify User task.
21306987/01	NoClassDefFoundError error occurs when running highavailability.bat.
21307126/01	RSA Secure ID 7 - Cannot acquire endpoint due to issues with the script to create Open Service Gateway Initiative (OSGi) bundle.
21315277/04	C++ Connector Server crashes when searching for moved or renamed Active Directory (AD) user accounts.

Support Ticket	Problem Reported
21319140/01	The imported SQL based dir.xml data is in upper case.
21322022/01	CA IdentityMinder Logins are slower over a period of time.
21325322/01	"Session closed due to communications failure" on LND when modifying accounts.
21331632/01	Warning message when revoking service does not include the user name parameter.
21335464/01	Provisioning manager script error when viewing an operation that spans multiple pages.
21351855/01	CA IdentityMinder fails to create environment when no provisioning and system manager role only chosen.
21361599/01	The following error appears when Modify User task is used:
21383034/01	Task failed Fatal: Failed to execute SynchronizeAttributesWithAccountEvent: ERRORMESSAGE: For input string
21393461/01	Exception while updating Enable/Disable user or any other user attribute.

## 12.6.1

The following issues are fixed in CA IdentityMinder 12.6.1:

Support Ticket	Problem Reported
20576709/02	Need to support sharing of common Business Objects Report Server for both CA IdentityMinder and SiteMinder
20576725/02	Need to support Business Objects Report Server in a high availability Configuration
20583665/02	Need to support Business Objects Report Server XI 3.1 SP5 (CABI 3.3)
20774861/02	Unable to include Secondary Object data in Policy Xpress
20777137/02	Enhancement is made to the policy based workflow to get the secondary objects (user objects) which are needed for the primary objects
20888199/01	DN naming convention for account templates for TEWS not documented
21073146/01	"Synchronize accounts with account template" does not synchronize
21086870/01	Standalone JCS installer does not prompt for FIPS key, causing encryption related problems
21108813/01	CA IdentityMinder 12.6 does not provide the expected role definitions
21111634/01	JCS endpoint logs are not created

---

**Support Ticket Problem Reported**

21131768/01	Global Policy Workflow attribute issue (Event definitions were missing secondary object type)
21135604/01	View Logical Attribute Handlers task fails with a NullPointerException
21136454/01	SQL Injection security vulnerability has been fixed in this release
21136456/01	Security vulnerability
21136499/01	Select Box Data is not working with a Profile screen that is attached to a Service in CA IdentityMinder 12.6
21137701/01	An exception "PxEnvironmentException" is received when Policy Xpress policy calls external Java code
21140501-1	Support for cloud deployments (tenant management)
21146621/01	Global Attribute Validation in directory.xml
21156269/01	Differences between the DB schemas generated by the installer and the individual database scripts in the tools folder
21156269/01	More scripts needed for manual database creation
21162602/01	Custom correlation for TSS does not work on Unix
21170706/01	View Submitted Task results are incorrectly sorted when regional settings are set to Danish
21175201/01	Account synchronization initiated by inbound notification does not occur when Provisioning Roles are assigned using Policy Xpress policies
21181592/01	Failed to load CA IdentityMinder r12.6 with an error of the invalid class-path
21183366/01	Wrong username used with datasources
21187385/01	CA IdentityMinder crashes intermittently
21188814/01	CA SiteMinder r12 SP3 CR11 policy server crashes while accessing CA IdentityMinder policy
21190699/01	Unable to get secondary object information from Policy Xpress on either event or task based policies. Also original attribute value info is returned even when Policy Xpress fires after task completion.
21190873/01	508 compliance issue - Tool Tip of checkboxes are not meaningful.
21193837/01	Create&delete Managed Objects
21194712-1	Policy Xpress with iterator breaks when a triggered access role assignment is rejected by Workflow

---

**Support Ticket Problem Reported**

---

21200396/01	508 Compliance Issue: "Skip to main content" link problems
21200412/01	508 Compliance Issue: Warning and Error messages are not read properly by assisting software to disabled users.
21213029-1	The password services variables stored in the JSession cache are not cleared (on logout) and subsequent requests get redirected to the pws.fcc page

---

# Chapter 6: Documentation

---

This section contains the following topics:

[Bookshelf](#) (see page 71)

[CA IdentityMinder and CA RCM Integration Release Notes](#) (see page 71)

## 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](http://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 73) 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

### Mozilla Firefox Exceptions

We recommend that keyboard users and JAWS users use Internet Explorer 8 for the following reasons:

- In Firefox, dialogs do not receive the in/out focus.
- In Firefox, the skip to main content link is not always read first by screen reader.

### 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