CA Identity Manager™

Release Notes

12.6.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA Directory
- CA Identity Manager ™
- CA Identity Governance (formerly CA GovernanceMinder)
- 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.

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

12.6.4 9
- Changes to Existing Features 9
- New Certifications 10
- Top Secret V2 Connector Enhanced to Support Additional Objects/Attributes 11
- Mobile Application Password Change Enhancements 11
- Enhancements to the Bulk Load Client 11
- Mobile Application Support for Android OS 11
- Connector Xpress Support Customization of SCIM and Web Services Connector 11
- Policy XPress Supports SOAP and REST Web Services 11
- View My Work List task Search Screen 12

12.6.3 12
- New Certifications 13
- Unicast Support for JBoss 6.1 EAP 14
- New Events Generate Emails and Audit Data 14
- Support of ID Vault in Lotus Notes Domino 14
- HTTP Header Information Capture 15
- Service Object Enhancements 15

12.6.2 16
- New Certifications 17
- Mobile App Support 18
- Synchronization/Remove Account Template Values From Accounts 18
- Enhanced Configurations for the LND Connector 19
- Task Persistence Database Schema 19
- Support for Deactivating SAP Account Password 19
- Two Modes for Connecting to Exchange: Agentless and Agent 20
- Support for Exchange Data Access Groups (DAG) 20
- Support for Automatic Mailbox Distribution in Exchange 2010 20
- Connect to SQL Server When the Database is Offline 20
- Task to Create a Snapshot Definition for Reports 21

12.6.1 21
- New Certifications 21
- SSL-Enabled JNDI User Store 22
- Encrypted Password Support in Management Console Bootstrap Directory 22

12.6 22
- New Name and Appearance 23
- Simplified User Experience 23

Provisioning Enhancements 23
Connector Enhancements 24
Performance Enhancements 25
Policy Xpress Enhancements 26
Secure Management Console 27
Basic Access Requests 27
New Documentation for Config Xpress 29
Native CA Identity Manager Replacement for SiteMinder Advanced Password Services 30
Dynamic Keys for Encrypting Data 31
Active Directory Server Synchronization 31
Auditing Login and Logout Events 31
SHA-2 Support 32

Chapter 2: Installation Considerations 33

Enable Policy Xpress Support for Web Services SOAP and REST 33
Supported Platforms and Versions 34
Deprecated and Dropped Components 34
Co-installation of Unix Remote Agents with Additional CA Products 34
Passwords Not Encrypted 34
Oracle 11g R2 RAC as User Store and Object Store 35
Oracle 12c RDB as User Store and Object Store 35
AD LDS as a User Store 35
Non-ASCII Character Causes Installation Failure on Non-English Systems 35
Work Around Firewall on Windows 2008 SP2 36
Deploy JSP Pages for Administrator Actions 36
Linux: Provisioning Directory Installation 36
Linux: JDK Requirement for Installation 37
Linux 64-bit: SiteMinder Connectivity Errors 37
Improve Performance on WebSphere and AIX 38
Ignore WebSphere 7/Oracle Error 38

Chapter 3: Upgrade Considerations 39

System Manager Role Needs Admin Roles Scope After Upgrade from 12.6 39
Supported Upgrade Paths 40
New Scripts to Update the Task Persistence and Archive Schemas 40
New JCO Files for SAP R3 40
New Active Directory Role Definition File 40
Update to jboss.xml File 41
64-Bit Application Servers 41
Upgrade from r12 (CR6 or later) Fails on Some Clusters 42
Workflow Error after Upgrade from pre-r12.5 SP7 43

Environment Migration Error 43
Credential Provider Upgrade Error 44
Credential Provider Internal Error 44
No Search Screen with Explore and Correlate Task 44
Non-Fatal Error after Upgrading Provisioning Manager from r12 45
Rename ACF2, RACFand TSS Endpoints Before Upgrade 45
Run the SQL Upgrade Script 45

Chapter 4: Fixed Issues 47

12.6.4 47
12.6.3 50
12.6.2 52
12.6.1 53

Chapter 5: Documentation 57

Bookshelf 57
Known Issues 57
CA Identity Manager and CA Identity Governance Integration Release Notes 58

Appendix A: Accessibility Features 59

508 Compliance 59
Product Enhancements 59

Chapter 1: New Features

This section contains the following topics:

12.6.4 (see page 9)
12.6.3 (see page 12)
12.6.2 (see page 16)
12.6.1 (see page 21)
12.6 (see page 22)

12.6.4

Changes to Existing Features

CA Identity Manager Supports New Version of CABI

With this release, the CA Identity Manager supports only CA Business Intelligence (CABI) version 3.3 SP1. The CA Identity Manager installation kit provides CABI 3.3 and CABI 3.3 SP1 installers. You must install CABI 3.3 and then install CABI 3.3 SP1.

New Certifications

The following new platforms are certified with CA Identity Manager r12.6.4:

Endpoints

- CA Control Minder r12.8 as an endpoint
- Microsoft Windows 2012 R2 Active Directory as an endpoint
- Oracle 12c Database as an endpoint
- Microsoft Lync Server 2010 and 2013 as an endpoint
- PeopleSoft Financials 9.2 as an endpoint
- System for Cross-domain Identity Management (SCIM) as an endpoint
- Lotus Notes Domino 9.x as an endpoint

Web Services (Layer7) Endpoints

- Service Now
- Microsoft Azure
- Zendesk

Application Server

- JBoss 6.2.0 EAP

CA Identity Manager User Store

- Oracle 12c
- Microsoft Windows 2012 R2 Active Directory

CA Identity Manager Object Store

- Oracle 12c

Credential Provider

- Microsoft Windows 8
- Microsoft Windows 8.1

Additional Support

- Password Synchronization agent support on Windows Active Directory 2012 R2
- Integration with CA SiteMinder r12.52 CR1, r12.52 SP1, and r12.51 CR3
- Browsers support for IE 11.x
- Browsers support for Firefox 29.x

Top Secret V2 Connector Enhanced to Support Additional Objects/Attributes

Top Secret V2 Connector has been enhanced to expose Resources, Facilities, Segments and all other attributes in the Mainframe.

Mobile Application Password Change Enhancements

The Mobile App has additional levels of security when resetting the Password that involves both the PIN and Q&A flow. For more information, refer to the *Administration Guide*.

Enhancements to the Bulk Load Client

The Bulk Load Client has been enhanced to support Kettle Transform as a data source and a secondary action, similar to what is in the Bulk Task user interface.

Mobile Application Support for Android OS

The mobile application now supports mobile devices that use the Android operating system.

Connector Xpress Support Customization of SCIM and Web Services Connector

The Connector Xpress is enhanced to support the customization of SCIM and Web Services Connector metadata for

- Service Now
- Azure
- Zendesk

Policy XPress Supports SOAP and REST Web Services

Policy XPress is enhanced to support Web Services SOAP (with basic authentication method) and REST (with basic authentication, proxy authentication, and OAuth authentication methods) such that it can be integrated with external applications that provide a web service interface.

View My Work List task Search Screen

A new search screen was added to the View My Work List task that allows you to search either by the user Id of the workflow subject, or by the initiator of the task to filter the workitems.

12.6.3

New Certifications (see page 13)

Unicast Support for JBoss 6.1 EAP (see page 14)

New Events Generate Emails and Audit Data (see page 14)

Support of ID Vault in Lotus Notes Domino (see page 14)

HTTP Header Information Capture (see page 15)

Service Object Enhancements (see page 15)

New Certifications

The following new platforms are certified with CA Identity Manager r12.6.3:

Endpoints

- Microsoft AD Exchange Server 2013 as an endpoint
- Salesforce v24 as an endpoint
- Solaris 11.1 as an endpoint
- SUSE 11 SP3 as an endpoint
- CA Directory r12.0 SP12 GA as a Connector Xpress JNDI endpoint
- CA ACF2 LDAP r15.1 as an endpoint
- CA RACF LDAP r15.1 as an endpoint
- CA TSS LDAP r15.1 as an endpoint

Server Operating System

- Windows 2012 Essentials

Server Client Operating System

- Windows 2012 Essentials
- Windows 8

Application Server

- JBoss 6.1.1 EAP

CA Identity Manager User Store

- CA Directory r12.0 SP12 GA
- Microsoft Active Directory 2012 Essentials
- Microsoft ADAM 2012 Essentials

Additional Support

- Password Synchronization agent support on Active Directory 2012 Essentials
- Internet Explorer 10.x
- Google chrome 28.x
- Integration with CA SiteMinder r12.5 CR3, r12.51 CR1
- Unix Agentless support on RHEL, SUSE, Solaris, AIX and HPUX
- Support of Unicast and Multicast with JBoss 6.1.0 EAP
- Support of CAM 1.14 with Remote Agents of this release

- Support of AXIS2 1.6.2 with this release

Unicast Support for JBoss 6.1 EAP

For customers who install CA Identity Manager on JBoss 6.1 EAP, unicast is an alternative messaging protocol to multicast. We recommend testing both protocols to determine the best choice for your organization.

For details on using either protocol, see the JBoss version of the *Upgrade Guide*.

New Events Generate Emails and Audit Data

You can enable email notifications and audit data for two new events:

- ForgottenPasswordAuditEventQnAInitiated

  The Forgotten Password Public Task generates this event when a user sees the Question and Answer page during a password reset attempt.

- ForgottenPasswordAuditEventQnALocked

  The Forgotten Password Public Task generates this event when the Question and Answer page is locked due to unsuccessful attempts to answer security questions.

You configure email notifications and auditing from the Management Console.

Note: For information about how to configure email notifications, see the *Administration Guide*. For information about how to configuration auditing, see the *Configuration Guide*.

Support of ID Vault in Lotus Notes Domino

Lotus Notes Domino's ID Vault feature is now supported from this release. This feature allows you to natively and securely recover and reset passwords, recover lost IDs, rename users and so on.

HTTP Header Information Capture

New servlet filter : ClientExtractFilter has been added in this release. This servlet filter will be a central place to extract all the information related to the web client environment. This filter extract information from HTTP headers. Currently only client IP address is being extracted. We however ensure that this information is extracted only once, for any given request.

This servlet filter is executed for each request as suggested by URL pattern:/* in web.xml.

The WebClientInformation utility class has been added which acts as a placeholder for web client information extracted in filter. This class currently holds only IP address however may be enhanced in future.

Then this WebClientInformation is put into the TaskSession as an attribute identified by key: WebClientInfo. So any event, task , UI or workflow created as result of request will have client information where this request generated.

Service Object Enhancements

A new checkbox option "Revoke services for users" to determine if service needs to be revoked before deletion or not has been added in Delete User task.

“Request and View access” task filtering support is added such that the user will get search section for Admin and owner search options.

Service Request specific information like Service Request Duration, user data is made visible in the Service Request approval workflow item. This information is also sent in Email notification when there is global policy based workflow configured on event 'AddServiceToUserEvent'.

12.6.2

New Certifications (see page 17)

Mobile App Support (see page 18)

Synchronization/Remove Account Template Values From Accounts (see page 18)

Enhanced Configuration for the LND Connector (see page 19)

Task Persistence Database Schema (see page 19)

Support for Deactivating SAP Account Password (see page 19)

Two Modes for Connecting to Exchange: Agentless and Agent (see page 20)

Support for Exchange Data Access Groups (DAG) (see page 20)

Support for Automatic Mailbox Distribution in Exchange 2010 (see page 20)

Connect to SQL Server When the Database is Offline (see page 20)

Task to Create a Snapshot Definition for Reports (see page 21)

New Certifications

The following new platforms are certified with CA Identity Manager 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 Identity Manager User Store

- CA Directory r12.0 SP11 GA

CA Identity Manager 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 Identity Manager with CA Identity Governance r12.5 SP8 and CA Identity Governance 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 Identity Manager mobile app enables you to leverage your existing CA Identity Manager 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 Identity Manager 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 Identity Manager 12.6.4 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*.

Enhanced Configurations 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\lnd\connector.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 21)

SSL-Enabled JNDI User Store (see page 22)

Encrypted Password Support in Management Console Bootstrap Directory (see page 22)

New Certifications

The following new platforms are certified with CA Identity Manager 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 Identity Manager User Store

- CA Directory r12 SP10 CR2

CA Identity Manager 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 Identity Manager with CA Identity Governance r12.6
- Support of CA Identity Manager 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 Identity Manager 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 23)

Simplified User Experience (see page 23)

Provisioning Enhancements (see page 23)

Connector Enhancements (see page 24)

Performance Enhancements (see page 25)

Policy Xpress Enhancements (see page 26)

Secure Management Console (see page 27)

Basic Access Requests (see page 27)

New Documentation for Config Xpress (see page 29)

Native CA Identity Manager Replacement for SiteMinder Advanced Password Services (see page 30)

Dynamic Keys for Encrypting Data (see page 31)

Active Directory Server Synchronization (see page 31)

Auditing User Login and Logout Events (see page 31)

SHA-2 Support (see page 32)

New Name and Appearance

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 Identity Manager 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 Identity Manager 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 Identity Manager 12.6 includes the following new features and changes to simplify building and deploying new connectors.

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

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

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

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

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

- Deploy third-party libraries without restarting CA IAM CS

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

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

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

Bundle Builder – New Tool for Creating Connectors

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

Logging for Connectors and CA IAM CS

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

Certificates for Connectors and CA IAM CS

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

Use Connector Xpress to Map Custom Attributes and Custom Capability Attributes

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

CA IAM CS Is a Proxy for CCS

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

Performance Enhancements

CA Identity Manager 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 in the CA Security Global User Community.

Secure Management Console

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

The CA Identity Manager 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 Identity Manager 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 Identity Manager 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 Identity Manager), 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 CA Identity Governance (formerly called CA GovernanceMinder)
- 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 Identity Manager. You can use this tool to analyze and work with the configurations of your CA Identity Manager 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 Identity Manager Replacement for SiteMinder Advanced Password Services

In addition to basic password policies, CA Identity Manager 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 Identity Manager 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 Identity Manager 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 Identity Manager deployment that uses CA SiteMinder password services (password history) to a deployment that includes only CA Identity Manager 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 Identity Manager 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 Identity Manager environment, you can configure CA Identity Manager 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 Identity Manager, 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:

Enable Policy Xpress Support for Web Services SOAP and REST (see page 33)
Supported Platforms and Versions (see page 34)
Deprecated and Dropped Components (see page 34)
Co-installation of Unix Remote Agents with Additional CA Products (see page 34)
Passwords Not Encrypted (see page 34)
Oracle 11g R2 RAC as User Store and Object Store (see page 35)
Oracle 12c RDB as User Store and Object Store (see page 35)
AD LDS as a User Store (see page 35)
Non-ASCII Character Causes Installation Failure on Non-English Systems (see page 35)
Work Around Firewall on Windows 2008 SP2 (see page 36)
Deploy JSP Pages for Administrator Actions (see page 36)
Linux: Provisioning Directory Installation (see page 36)
Linux: JDK Requirement for Installation (see page 37)
Linux 64-bit: SiteMinder Connectivity Errors (see page 37)
Improve Performance on WebSphere and AIX (see page 38)
Ignore WebSphere 7/Oracle Error (see page 38)

Enable Policy Xpress Support for Web Services SOAP and REST

Policy XPress is enhanced to support Web Services SOAP (with basic authentication method) and REST (with basic authentication, proxy authentication, and OAuth authentication methods) such that it can be integrated with external applications that provide a web service interface. To use the Policy XPress web services (SOAP and REST) with JBoss 5.1 community edition, copy the following jars into your JBoss 5.1 community edition "\lib\endorsed" directory from the "client" directory, and then restart the application server:

- jbossws-native-jaxrpc.jar
- jbossws-native-jaxws.jar
- jbossws-native-jaxws-ext.jar
- jbossws-native-saaj.jar

Note: You do not need to consider copying these files for the EAP versions.

Supported Platforms and Versions

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

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

Deprecated and Dropped Components

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

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.

Passwords Not Encrypted

New installations do not encrypt user passwords by default. Also, when CA SiteMinder® is integrated with CA Identity Manager, 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 Identity Manager with Oracle 11g R2 RAC.
- Create the database *tablespace* on the shared disk group while creating a tablespace.

Oracle 12c RDB as User Store and Object Store

When using Oracle 12c RDB as a User store and a Runtime store, use only non-Container DB mode. The Oracle 12c “Container” DB (multi-tenancy) RDBMS option is excluded for the enterprise product.

AD LDS as a User Store

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

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

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

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

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

Workaround

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

Work Around Firewall on Windows 2008 SP2

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

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

Deploy JSP Pages for Administrator Actions

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

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

The JSP pages are installed in this location:

admin_tools\samples\admin

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

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

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: JDK Requirement for Installation

CA Identity Manager 12.6.4 requires Oracle JDK 1.6.

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

Linux 64-bit: SiteMinder Connectivity Errors

Symptom:

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

Solution:

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

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

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

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

3. Start the application server and verify that no policy server connectivity issues appear. For example, look for a line such as following with no exceptions:

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

Improve Performance on WebSphere and AIX

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

Follow these steps:

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

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

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

Ignore WebSphere 7/Oracle Error

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

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

This error can be ignored.

Chapter 3: Upgrade Considerations

This section contains the following topics:

System Manager Role Needs Admin Roles Scope After Upgrade from 12.6 (see page 39)
Supported Upgrade Paths (see page 40)
New Scripts to Update the Task Persistence and Archive Schemas (see page 40)
New JCO Files for SAP R3 (see page 40)
New Active Directory Role Definition File (see page 40)
Update to jboss.xml File (see page 41)
64-Bit Application Servers (see page 41)
Upgrade from r12 (CR6 or later) Fails on Some Clusters (see page 42)
Workflow Error after Upgrade from pre-r12.5 SP7 (see page 43)
Environment Migration Error (see page 43)
Credential Provider Upgrade Error (see page 44)
Credential Provider Internal Error (see page 44)
No Search Screen with Explore and Correlate Task (see page 44)
Non-Fatal Error after Upgrading Provisioning Manager from r12 (see page 45)
Rename ACF2, RACFand TSS Endpoints Before Upgrade (see page 45)
Run the SQL Upgrade Script (see page 45)

System Manager Role Needs Admin Roles Scope After Upgrade from 12.6

When upgrading from CA Identity Manager version 12.6 or later, the System Manager role needs to be given the Admin Roles scope.

Note: If this is not done, then the Admin role searches may not return results.

Follow either of these steps:

- In the Management Console, click System Manager, and then choose the user.
- Alternatively, you can add the Admin Role scope to the System Manager role itself using Modify Admin Role, System Manager.

Supported Upgrade Paths

You can upgrade to CA Identity Manager 12.6.4 from the following versions:

- CA Identity Manager r12
- CA Identity Manager r12.5 or 12.5 SPx
- CA Identity Manager 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 Identity Manager 12.6.4.

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 Identity Manager first time after an upgrade. For more information about the new scripts, see the *Installation Guide*.

New JCO Files for SAP R3

If you plan to use the new connector for SAP R3, you need to update the JCO files. See the endpoint guide for the SAP R3 connector for more details.

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 Identity Manager 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 Identity Manager initialization, many errors messages are logged to the CA Identity Manager 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 Identity Manager 12.6.4 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

See the *Upgrade Guide* for full details on upgrading on your application server.

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

Symptom:

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

Solution:

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

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

Note: This issue does not affect a JBoss cluster.

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

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

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 Identity Manager r12 CR1, CR2, or CR3, you may see the following error when importing your environments:

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

Solution:

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

Credential Provider Upgrade Error

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

Workaround

Open the CAIMCredProvConfig application and select the check box.

Credential Provider Internal Error

Symptom:

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

Solution:

No action is required. If no other errors were issued, the upgrade process completed successfully.

No Search Screen with Explore and Correlate Task

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

Workaround

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

Non-Fatal Error after Upgrading Provisioning Manager from r12

Symptom:

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

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

The CA Identity Manager installation log contains the following entry:

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

Solution:

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

Rename ACF2, RACFand TSS Endpoints Before Upgrade

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

Run the SQL Upgrade Script

After the upgrade, the first time you start the CA Identity Manager 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: Fixed Issues

This section contains the following topics:

12.6.4 (see page 47)
12.6.3 (see page 50)
12.6.2 (see page 52)
12.6.1 (see page 53)

12.6.4

The following issues are fixed in CA Identity Manager12.6.4:

Support Ticket	Problem Reported
20957471/07	Need fix delivered for CQ 170096 on IM 12.6 SP2
21517465/01	Admin role scoping in the search screen.
21536689/01	IM Directory creation keeps bad password
21539813/01	Failed to update quotas and threshold for LND accounts if Mail File ACL set to Manager
21538682/01	In a "tokenized" IME when a date picker field is in error then the returned error message shows the Key ID instead of the pair value from the resource bundle.
21521403/04	Modify of a Service object causes the category to change from Service
21547136/01	On Oracle Applications accounts, the From date on a responsibilityList item is not visible on new accounts in Provisioning Manager until the endpoint is re-explored, if the account is created using a template without any From date set.
21558292/01	MULTIPLE 508 NON-COMPLIANCES
20957471/09	Reverse Sync approvals are generated to remove responsibilities from an Oracle Apps account when an explore is peformed after new accounts were created via IM with responsibilities already assigned.
21551822/01	erroneous object selector results
21567422/01	value for Organization mapping missing in GM after import from IM
20957471/11	Reverse Sync Modified Account policies are not behaving as expected for Oracle Server
21576029/01	Description for Windows NT endpoint does not get displayed in IM user console

21559775/01	Roles import fails with invalid XML character (Unicode: 0x1f) generated by object selector in access role task
21593378/01	Live notification's manager information incorrect
21590547/01	IM 12.6 SP2: AD- A Blank UserPrincipalName attribute causes out of sync errors for AD accounts
21588715/01	When a Showing Rule is defined into an Admin Role Search screen then the search filter does no more work.
21590303/01	Running new bulk loader client in IM r12.6 SP2, the bulk loader opens all of its tasks as in progress and hogs the JVM leaving other requests stuck in queue.
21594906/01	IM 12.6 SP1 - Audit level BOTH on the attribute not taking effect
21574514/02	IM 12.6 SP2:Tassk stuck in progres with PX triggered on event level workflow
21606642/02	slow performances with "Modify Group Members" task when group contains 38K users
21557047/01	Incorrect attribute mappings in Office 365 connector ?
12345678/01	Need new SM Web Agent API on IM 12.6 SP4.
21604197/01	Role Def Import stops on Prov Role with name containing "\00"
21604199/01	Fail to search Prov Roles on "\" in combination with wildcard "*".
21609415/01	Google connector error due to deprecated (?) API
21626365/01	Script Error trying to view page 2 of Provisioning Manager op details
21613942/01	Modify Account Container Filter
21419884/02	ridiculously filtered snapshot takes excessive time to complete
21592259/01	Password filter not working as expected for password validation
21640856/01	When an approval generated by reverse sync for adding a responsibility to an Oracle Apps account is rejected, the responsibility is not expired even though it shows in VST as having been revoked.
21633958/01	DUPLICATE PROV ROLES(PX)
21641737/01	Win2012 ADS functionality levels reported as Win2008R2
21643258/01	Same as CQ176812 but this one is related to "read order"
21575724/01	User scoping rule on Admin policies of Admin roles results in members/administrators of a role not being visible after a restart of JBoss
21584724/01	Additional logging for the SAP connector
21500603/01	CA Identity Manager and SiteMinder integration fails

21639644/01	Oracle Account Template Export
21657577/01	JCS no longer referencing the Apache CCPP causing failures when JavaScript is used in custom CXP connector.
21636774/01	FND Accounts getting Responsibilities End Dated to Current Date and ORA/01422: exact fetch returns more than requested number of rows ORA-06512: at "APPS_APPLSYS3.FND_USER_PKG"
21641383/01	Task "Enable/Disable User" getting stucked "In Progress" if PolXpress email is configured.
21646678/01	Ant utility fails trying to tokenize roles if property 'Title' is added to search screens.

21657600/01	IM failed to import the custom fields values on Provisioning Role
21687010/01	Unable to launch some ELM reports.
21668810/01	Problem with deleting users assigned to dynamic groups.
21699782/01	WORK ITEM LIST - LIMITATION. This CQ covers the work needed to make inclusion of worklist items on logon/welcome page optional.
21650405/01	Config Xpress tool not loading policy based workflows
21539813/01	Documentation changes needed for resolution of defect PROD00176400.
21712883/01	IM 12.6 SP2 - Active Direcotry account attributes for date/time are not showing up in local timezone in the IM User Console
21669984/01	Can use a private (not public) task called on the public alias using TEWS when IDM and SM are integrated.
21711390/01	IM 12.6 - Security vulnerability- The URL to request an image page allows contentType to be defined by an attacker, allowing code execution in the browser of an authenticated user who visits the URL
21713498/01	Task status shows complete while events still show in progress
21699782/01	Add initiator and userid search on User's worklist
21704767/01	Java AXIS sample for ModifyGroupMembership.java isn't working with 12.6 (any service pack) - Possible regression used to work with 12.5
21651991/01	Add configuration option to suppress IMPS Modify_Account_Password notifications to IM
21730035/02	IM12.6 SP2: AD endpoint:Setting 'User must change password after password reset flag' on Configuration tab of endpoint does not update provisioning

21730581/01	Inconsistence in Certifier Type between Provisioning Server and LND endpoint
21746621/01	Unable to Explore/Correlate accounts under OU with name containing "&"
21764131/01	The Office365 single attribute for Block Credential is mapped to eTDYN-str-multi-c/023 instead of to a single-valued DYN attribute which causes errors when trying to do an account sync with a WEAK SYNC Account Template.

12.6.3

The following issues are fixed in CA Identity Manager 12.6.3:

Support Ticket	Problem Reported
21088049/02	Workflow job is not responding in "active" state.
21227662/05	Once an ACF2 endpoint is explored with the logged in user, you cannot change to use the proxy admin user.
21240169/01	StringIndexOutOfBoundsException when exporting CA Identity Manager environment.
21298884/01	Assign/Remove Service To/From User not writing to UserStore or Triggering PX to accounts.
21325322/03	Bulk suspensions fail to suspend all LND accounts or add all accounts to the Deny Access Group (Suspended 0)
21329912/02	Account synchronization is not working in CA Identity Manager 12.6.
21347968/01 21358148/01	Policy server crashed when CA Identity Manager access role assigned/removedto/ from a user.
21366658/01	Creating user through bulk loader task is returning null pointer exception when CA SiteMinder is integrated.
21378657/01	OOTB Escalation Workflow prematurely escalates if defined using the "COnfigure Global Policy Based Workflow for Events" task.
21378803/01	Error "Previous password cannot be reused." occurs and fails the task.
21385464/01	NullPointerException when identity policy configured with MemberRule-Groups Where-Attribute Expression.
21387236/01	Create user from Copy is not copying the organization attribute.
21389685/01	Login time exceeds when integrated with CA SiteMinder.
21393295/01	Provisioning role missing from CA Identity Manager user's list of provisioning roles.
21395953/01	Policy Xpress sends e-mail loops.

Support Ticket	Problem Reported
21417960/01 21417960/03	Modify provisioning role returns null pointer.
21424762/02	Forbidden user error.
21430655/01	Global Policy based workflow events defers to escalation approver.
21430868/02	Unable to remove the middle initial when renaming LND accounts.
21438148/03	The root LND organization is not explored and no accounts are retrieved.
21438256/01	Sample java script does not work with Self Registration task.
21438937/01	Odd special character ends up in task persistence "Old Value" and in auditing.
21439600/01	Customer finds blank windows when they login using password expired user.
21441213/01	Management task imported from CA Identity Manager r12.5 environment returns java.lang.ClassCastException error.
21447986/01	When a Policy Xpress policy is triggered and logged in using Norwegian language, it returns java.lang.IllegalArgumentException: Unmatched braces in the pattern.
21450831/01	When opening a new template using Connector Xpress, it is not showing the Operation Bindings dialog.
21468616/01	Middle initial attribute length.
21470755/01	In Mobile Application, contact card's manager card is not functioning properly.
21470794/01	In Mobile Application, all password reset errors report back as complexity issues even if you submit the incorrect current password.
21473825/01	In CA Identity Manager Mobile application, login fails after resetting a password from inside the mobile application.
21475033/01	In CA Identity Manager Mobile application, Forgotten Password Reset can only be used once.
21478278/01	A CAPTCHA field in CA Identity Manager screen is not displayed again when validation phase rejects some other fields.
21480621/01	Installing CA Identity Manager r12.6 SP2 on JBoss EAP 6 fails to install the iam_im_compile_jsp.* and the build.xml.
21481343/01	No active slots available as they are blocked indefinitely.
21486937/01	When "Wait" flag is checked for an action rule in Policy Xpress to "Execute a function" (not main) as "External Code" category and "Execute Java Code" Type; The JavaActionWaitEvent is generated by Policy Xpress and status remains "In progress".
21488801/01	Configuring password policy which require punctuation character results in incorrect password.

Support Ticket	Problem Reported
21497995/01	Bulk operations returns an error when selecting one (out of multiple) delegation worklist items.
21520525/01	<ETAHOME>\bin\ADSLDAPDiag.exe fails with "Error 10054 reading data from server", when attempting manual connection to an Active Directory server 2012.
21522674/01	Connection reset error at startup step 5.
21535004/01	Unable to add SAP role using TEWS.
21537907/01	ConfigXpress is not working in the CA Identity Manager r12.6 SP2 installation.
21539251/01	Error occurs when creating a copy or modifying the Admin Task "View Access History".
215544431/01	Global Workflow policy creation fails.
21558358/01	Agentless exchange agent is looking for CA CloudMinder/CAFT
21568224/01	ConfigXpress.air is not working- returns an error on CA Identity Manager r12.6 SP2 installation.
21572374/01	In CA Identity Manager mobile application, quick approval is not working.
21585328/01	ConfigXpress.air fails to install on CA Identity Manager r12.6 SP2.

12.6.2

The following issues are fixed in CA Identity Manager 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 Identity Manager 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.

Support Ticket	Problem Reported
21280342/01	DoSynchUserRoles is not enabling the checkboxes for "add missing accounts" and "remove extra accounts" to the CA Identity Manager 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.
21319140/01	The imported SQL based dir.xml data is in upper case.
21322022/01	CA Identity Manager 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 Identity Manager fails to create environment when no provisioning and system manager role only chosen.
21361599/01 21383034/01	The following error appears when Modify User task is used: 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 Identity Manager 12.6.1:

Support Ticket	Problem Reported
20576709/02	Need to support sharing of common Business Objects Report Server for both CA Identity Manager and SiteMinder

Support Ticket	Problem Reported
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 Identity Manager 12.6 does not provide the expected role definitions
21111634/01	JCS endpoint logs are not created
21131768/01	Global Policy Workflow attribute issue (Event definitions were missing secondary object type)
21135604/01	View Logical Attribute Handlers task fails with a NullPointer Error
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 Identity Manager 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

Support Ticket	Problem Reported
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 Identity Manager r12.6 with an error of the invalid class-path
21183366/01	Wrong username used with datasources
21187385/01	CA Identity Manager crashes intermittently
21188814/01	CA SiteMinder® r12 SP3 CR11 policy server crashes while accessing CA Identity Manager 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
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 5: Documentation

This section contains the following topics:

Bookshelf (see page 57)
Known Issues (see page 57)
CA Identity Manager and CA Identity Governance Integration Release Notes (see page 58)

Bookshelf

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

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

To use the Bookshelf

1. Download the bookshelf from the CA Support Site.
2. Extract the contents of the bookshelf ZIP file.

   Note: For best performance, when you install the bookshelf on a remote system, make the bookshelf accessible from a web server.
3. Open the Bookshelf.html file.

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

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

Known Issues

All known issues related to CA Identity Manager are found on the CA support site.

CA Identity Manager and CA Identity Governance Integration Release Notes

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

508 Compliance

CA Identity Manager 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 59) 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 Identity Manager 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 Identity Manager 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