

# CA Identity Manager™

## Notas de la versión 12.6.4



Esta documentación, que incluye sistemas incrustados de ayuda y materiales distribuidos por medios electrónicos (en adelante, referidos como la "Documentación") se proporciona con el único propósito de informar al usuario final, pudiendo CA proceder a su modificación o retirada en cualquier momento. Esta documentación es propiedad de CA. Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de CA.

No obstante lo anterior, si dispone de licencias de los productos informáticos a los que se hace referencia en la Documentación, Vd. puede imprimir, o procurar de alguna otra forma, un número razonable de copias de la Documentación, que serán exclusivamente para uso interno de Vd. y de sus empleados, y cuyo uso deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativas a los derechos de autor de CA.

Este derecho a realizar copias de la Documentación sólo tendrá validez durante el período en que la licencia aplicable para el software en cuestión esté en vigor. En caso de terminarse la licencia por cualquier razón, Vd. es el responsable de certificar por escrito a CA que todas las copias, totales o parciales, de la Documentación, han sido devueltas a CA o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, CA PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. CA NO RESPONDERÁ EN NINGÚN CASO, ANTE VD. NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTA DOCUMENTACIÓN INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

El uso de cualquier producto informático al que se haga referencia en la Documentación se regirá por el acuerdo de licencia aplicable. Los términos de este aviso no modifican, en modo alguno, dicho acuerdo de licencia.

CA es el fabricante de esta Documentación.

Esta Documentación presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

Copyright © 2014 CA. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, logotipos y marcas de servicios a los que se hace referencia en este documento pertenecen a sus respectivas empresas.

## Referencias a productos de CA Technologies

En este documento se hace referencia a los siguientes productos de CA Technologies:

- Gestión de identidades de CA CloudMinder™
- CA Directory
- CA Identity Manager™
- CA Identity Governance (anteriormente CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

## Información de contacto del servicio de Soporte técnico

Para obtener soporte técnico en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Soporte técnico en la dirección <http://www.ca.com/worldwide>.



# Contenido

---

## Capítulo 1: Nuevas funciones

9

12.6.4.....	9
Cambios en las funciones existentes.....	9
Nuevas certificaciones .....	10
Mejoras en el conector CA Top Secret V2 para la admisión de atributos y objetos adicionales .....	11
Mejoras en la funcionalidad de modificación de la contraseña para la aplicación móvil.....	11
Mejoras en el cliente de carga masiva .....	11
Compatibilidad de la aplicación móvil con el sistema operativo Android .....	11
Compatibilidad de Connector Xpress con la personalización de SCIM y del conector de servicios web.....	11
Compatibilidad de la política exprés con los servicios web SOAP y REST .....	12
Pantalla de búsqueda de la tarea Ver mi lista de trabajo .....	12
12.6.3.....	12
Nuevas certificaciones .....	13
Soporte de unidifusión para JBoss 6.1 EAP .....	14
Generación de nuevos correos electrónicos y datos de auditoría.....	14
Compatibilidad con el almacenamiento de ID en Lotus Notes Domino .....	14
Captura de información del encabezado HTTP.....	15
Mejoras del objeto de servicio.....	15
12.6.2.....	16
Nuevas certificaciones .....	17
Compatibilidad con aplicación para móviles.....	18
Synchronization/Remove Account Template Values From Accounts (Sincronización/eliminación de los valores de la plantilla de cuenta en Cuentas) .....	19
Configuración mejorada para el conector de LND.....	19
Esquema de la base de datos de persistencia de la tarea.....	19
Compatibilidad con la desactivación de la contraseña de cuentas de SAP.....	20
Dos modos para la conexión a Exchange: sin agente y con agente .....	20
Compatibilidad con los grupos de acceso de datos de Exchange (DAG).....	20
Compatibilidad con la distribución automática de buzones de correo en Exchange 2010 .....	21
Conexión a SQL Server cuando la base de datos esté sin conexión .....	21
Tarea para crear una definición de la instantánea para informes .....	21
12.6.1.....	21
Nuevas certificaciones .....	22
Almacén de usuarios de JNDI con SSL activado .....	22
Compatibilidad con las contraseñas cifradas en el directorio de arranque de la Consola de gestión.....	23
12.6.....	23
Aspecto y nombre nuevos.....	23

---

Experiencia del usuario simplificada .....	24
Mejoras del aprovisionamiento .....	24
Mejoras del conector .....	24
Mejoras del rendimiento .....	26
Mejoras de la política exprés .....	27
Seguridad de la Consola de gestión .....	28
Solicitudes de acceso básicas .....	28
Documentación nueva para Config Xpress .....	30
Reemplazo de CA Identity Manager nativa para SiteMinder Advanced Password Services.....	31
Claves dinámicas para cifrar datos.....	32
Sincronización del servidor de Active Directory.....	32
Auditoría de eventos de cierre de sesión e inicio de sesión .....	33
Soporte SHA-2.....	33

## **Capítulo 2: Consideraciones acerca de la instalación** **35**

Activación del soporte de la política exprés para los servicios web SOAP y REST .....	36
Versiones y plataformas compatibles .....	36
Componentes obsoletos y descartados .....	36
Coinstalación de agentes remotos de UNIX con los productos de CA adicionales .....	37
Contraseñas no cifradas .....	37
Oracle 11g R2 RAC como almacén de usuarios y almacén de objetos.....	37
Oracle 12c RDB como almacén de usuarios y almacén de objetos.....	38
ADAM 2008 como almacén de usuarios .....	38
Los caracteres no ASCII provocan errores de instalación en sistemas con idiomas distintos del inglés.....	38
Solución al problema del cortafuegos en Windows 2008 SP2 .....	38
Implemente las páginas de JSP para las acciones de administrador.....	39
Instalación del directorio de aprovisionamiento en Linux .....	39
Linux: requisito de JDK para la instalación .....	40
CA Identity Manager en Linux de 64 bits con errores de conectividad de SiteMinder .....	40
Mejora del rendimiento en WebSphere y AIX .....	41
Ignorar error de WebSphere 7 y Oracle .....	41

## **Capítulo 3: Actualizaciones** **43**

El rol Gestor del sistema necesita roles de administrador tras la actualización de 12.6 .....	43
Rutas de actualización compatibles .....	44
Scripts nuevos para actualizar la persistencia de la tarea y los esquemas del archivo de archivado .....	44
Archivos JCO nuevos para SAP R3 .....	44
Archivo de definición del rol de Active Directory nuevo.....	44
Actualización al archivo jboss.xml.....	45
Compatibilidad con los servidores de aplicaciones de 64 bits .....	45
Problema al actualizar un clúster de CA Identity Manager r12 CR6 o posterior.....	46

---

Error de flujo de trabajo después de la actualización desde una versión anterior a r12.5 SP7 .....	47
Error de migración de entorno.....	47
Error de actualización del proveedor de credenciales.....	48
Error interno del proveedor de credenciales de Vista .....	48
Ninguna pantalla de búsqueda con la tarea Explorar y correlacionar .....	48
Error no crítico tras actualizar el gestor de aprovisionamiento de r12.....	49
Cambiar de nombre los puntos finales de ACF2, RACF y TSS antes de la actualización.....	49
Ejecución del script de actualización de SQL.....	49

## **Capítulo 4: Problemas arreglados** **51**

12.6.4.....	51
12.6.3.....	54
12.6.2.....	56
12.6.1.....	58

## **Capítulo 5: Documentación** **61**

Biblioteca.....	62
Problemas conocidos .....	62
Notas de la versión de integración de CA Identity Manager y CA Identity Governance.....	63

## **Apéndice A: Funciones de accesibilidad** **65**

Cumplimiento con 508 .....	65
Mejoras del producto.....	65



# Capítulo 1: Nuevas funciones

---

Esta sección contiene los siguientes temas:

[12.6.4](#) (en la página 9)

[12.6.3](#) (en la página 12)

[12.6.2](#) (en la página 16)

[12.6.1](#) (en la página 21)

[12.6](#) (en la página 23)

## 12.6.4

### Cambios en las funciones existentes

#### Compatibilidad de CA Identity Manager con la nueva versión de CABI

Con esta versión, CA Identity Manager solamente es compatible con CA Business Intelligence (CABI) versión 3.3 SP1. El kit de instalación de CA Identity Manager proporciona los instaladores de CABI 3.3 y CABI 3.3 SP1. Se debe instalar CABI 3.3 y, a continuación, instalar CABI 3.3 SP1.

## Nuevas certificaciones

Las siguientes plataformas nuevas se han certificado con CA Identity Manager r12.6.4:

### **Puntos finales**

- CA ControlMinder r12.8 como punto final
- Microsoft Windows Active Directory 2012 R2 como punto final
- Oracle 12c Database como punto final
- Microsoft Lync Server 2010 y 2013 como punto final
- PeopleSoft Financials 9.2 como punto final
- System for Cross-domain Identity Management (SCIM) como punto final
- Lotus Notes Domino 9.x como punto final

### **Puntos finales de servicios web (Layer7)**

- Service Now
- Microsoft Azure
- Zendesk

### **Servidor de aplicaciones**

- JBoss 6.2.0 EAP

### **Almacén de usuarios de CA Identity Manager**

- Oracle 12c
- Microsoft Windows Active Directory 2012 R2

### **Almacén de objetos de CA Identity Manager**

- Oracle 12c

### **Proveedor de credenciales**

- Microsoft Windows 8
- Microsoft Windows 8.1

### **Compatibilidad adicional**

- Compatibilidad con el agente para la sincronización de contraseñas en Windows Active Directory 2012 R2
- Integración con CA SiteMinder r12.52 CR1, r12.52 SP1 y r12.51 CR3
- Compatibilidad con los exploradores Internet Explorer 11.x
- Compatibilidad con los exploradores Firefox 29.x

## Mejoras en el conector CA Top Secret V2 para la admisión de atributos y objetos adicionales

Se ha mejorado el conector CA Top Secret v2 para mostrar Recursos, Instalaciones, Segmentos y el resto de atributos en Mainframe.

## Mejoras en la funcionalidad de modificación de la contraseña para la aplicación móvil

Se han agregado niveles adicionales de seguridad en la aplicación móvil para el restablecimiento de la contraseña en los que se incluyen los flujos de número PIN y QnA. Para obtener más información, consulte la *Guía de administración*.

## Mejoras en el cliente de carga masiva

El cliente de carga masiva se ha mejorado para admitir la transformación de Kettle como un origen de datos y una acción secundaria, similar a su función en la interfaz de usuario de Tareas masivas.

## Compatibilidad de la aplicación móvil con el sistema operativo Android

La aplicación móvil ahora es compatible con dispositivos móviles que utilizan el sistema operativo Android.

## Compatibilidad de Connector Xpress con la personalización de SCIM y del conector de servicios web

Se ha mejorado Connector Xpress para que admita la personalización de SCIM y de los metadatos del conector de servicios web para

- Service Now
- Azure
- Zendesk

## Compatibilidad de la política exprés con los servicios web SOAP y REST

Se ha mejorado la política exprés para que sea compatible con los servicios web SOAP (mediante el método de autenticación básica) y REST (mediante el método de autenticación básica, autenticación proxy y métodos de autenticación OAuth), de modo que pueda integrarse con aplicaciones externas que proporcionen una interfaz de servicio web.

## Pantalla de búsqueda de la tarea Ver mi lista de trabajo

Se ha agregado una nueva pantalla de búsqueda a la tarea Ver mi lista de trabajo, que permite al usuario realizar búsquedas y filtrar los elementos de trabajo por el ID de usuario del asunto del flujo de trabajo o por el iniciador de la tarea.

## 12.6.3

[Nuevas certificaciones](#) (en la página 13)

[Soporte de unidifusión para JBoss 6.1 EAP](#) (en la página 14)

[Generación de nuevos correos electrónicos y datos de auditoría](#) (en la página 14)

[Compatibilidad con el almacenamiento de ID en Lotus Notes Domino](#) (en la página 14)

[Captura de información del encabezado HTTP](#) (en la página 15)

[Mejoras del objeto de servicio](#) (en la página 15)

---

## Nuevas certificaciones

Las siguientes plataformas nuevas están certificadas con CA Identity Manager r12.6.3:

### Puntos finales

- Microsoft AD Exchange Server 2013 como punto final
- Salesforce v24 como punto final
- Solaris 11.1 como punto final
- SUSE 11 SP3 como punto final
- CA Directory r12.0 SP12 GA como punto final de Connector Xpress JNDI
- CA ACF2 LDAP r15.1 como punto final
- CA RACF LDAP r15.1 como punto final
- CA TSS LDAP r15.1 como punto final

### Compatibilidad con los sistemas operativos del servidor

- Windows 2012 Essentials

### Sistema operativo del cliente del servidor

- Windows 2012 Essentials
- Windows 8

### Servidor de aplicación

- JBoss 6.1.1 EAP

### Almacén de usuarios de CA Identity Manager

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

### Compatibilidad adicional

- Compatibilidad con el agente para la sincronización de contraseñas en Active Directory 2012 Essentials
- Internet Explorer 10.x
- Google chrome 28.x
- Integración con CA SiteMinder r12.5 CR3, r12.51 CR1
- Compatibilidad de Unix sin agente con RHEL, SUSE, Solaris, AIX y HP-UX
- Compatibilidad de unidifusión y multidifusión con JBoss 6.1.0 EAP
- Compatibilidad de la CAM 1.14 con agentes remotos de esta versión

- Compatibilidad de AXIS2 1.6.2 con esta versión

## Soporte de unidifusión para JBoss 6.1 EAP

Para los clientes que instalan CA Identity Manager en JBoss 6.1 EAP, la unidifusión es un protocolo de mensajería alternativo a la multidifusión. Se recomienda probar ambos protocolos con el objetivo de determinar la mejor elección para la organización.

Para obtener más detalles sobre el uso de uno de los dos protocolos, consulte la versión JBoss de la *Guía de actualizaciones*.

## Generación de nuevos correos electrónicos y datos de auditoría

Se pueden permitir notificaciones de correo electrónico y datos de auditoría para dos eventos nuevos:

- `ForgottenPasswordAuditEventQnAInitiated`  
La tarea pública Contraseña olvidada genera este evento cuando un usuario ve la página de preguntas y respuestas durante un intento de restablecimiento de la contraseña.
- `ForgottenPasswordAuditEventQnALocked`  
La tarea pública Contraseña olvidada genera este evento cuando la página de preguntas y respuestas queda bloqueada después de varios intentos incorrectos al responder la pregunta de seguridad.

Configure las notificaciones de correo electrónico y de auditoría en la Consola de gestión.

**Nota:** Para obtener más información sobre cómo configurar notificaciones de correo electrónico, consulte la *Guía de administración*. Para obtener más información sobre cómo configurar la auditoría, consulte la *Guía de configuración*.

## Compatibilidad con el almacenamiento de ID en Lotus Notes Domino

La función de almacenamiento de ID de Lotus Notes Domino es ahora compatible con esta versión. Esta función permite recuperar y restablecer contraseñas, de forma nativa y segura, recuperar los ID perdidos y renombrar usuarios, entre otros.

---

## Captura de información del encabezado HTTP

Filtro de servlet nuevo: se ha agregado ClientExtractFilter en esta versión. Este filtro de servlet será un lugar central para extraer toda la información relacionada con el entorno de cliente web. Este filtro extrae información desde los encabezados HTTP. Actualmente solamente se extrae la dirección IP del cliente. Sin embargo, asegúrese de que esta información se extraiga solamente una vez para cualquier solicitud proporcionada.

Este filtro de servlet se ejecuta para cada solicitud como sugiere la dirección URL pattern:/\* del archivo web.xml.

La clase de utilidad WebClientInformation se ha agregado y actúa como marcador de posición para la información de cliente web extraída en el filtro. Esta clase solamente mantiene actualmente la dirección IP que, sin embargo, se podrá mejorar en el futuro.

A continuación, la clave coloca WebClientInformation en TaskSession como un atributo que identifica la clave WebClientInfo. De este modo, cualquier evento, tarea, interfaz de usuario o flujo de trabajo creado como resultado de solicitud dispondrá de la información de cliente donde se genera esta solicitud.

## Mejoras del objeto de servicio

Una opción de la casilla de verificación nueva Revocar servicios para los usuarios se utilizará para determinar si es necesario revocar el servicio antes de la supresión o si no se ha agregado en la tarea Suprimir usuario.

El soporte de filtrado de la tarea Solicitar y ver acceso se agrega de modo que el usuario obtendrá la sección de búsqueda para las opciones de búsqueda del administrador y del propietario.

La información específica de solicitud de servicio como la duración de solicitud de servicio y los datos del usuario se hacen visibles en el elemento de flujo de trabajo de aprobación Solicitud de servicio. Esta información se envía también en la notificación de correo electrónico cuando haya un flujo de trabajo de política global configurado en el evento AddServiceToUserEvent.

## 12.6.2

[Nuevas certificaciones](#) (en la página 17)

[Compatibilidad con aplicación para móviles](#) (en la página 18)

[Synchronization/Remove Account Template Values From Accounts](#)  
[\(Sincronización/eliminación de los valores de la plantilla de cuenta en Cuentas\)](#) (en la página 19)

[Configuración mejorada para el conector de LND](#) (en la página 19)

[Esquema de la base de datos de persistencia de la tarea](#) (en la página 19)

[Compatibilidad con la desactivación de la contraseña de cuentas de SAP](#) (en la página 20)

[Dos modos para la conexión a Exchange: sin agente y con agente](#) (en la página 20)

[Compatibilidad con los grupos de acceso de datos de Exchange \(DAG\)](#) (en la página 20)

[Compatibilidad con la distribución automática de buzones de correo en Exchange 2010](#)  
(en la página 21)

[Conexión a SQL Server cuando la base de datos esté sin conexión](#) (en la página 21)

[Tarea para crear una definición de la instantánea para informes](#) (en la página 21)

## Nuevas certificaciones

Las siguientes plataformas nuevas están certificadas con CA Identity Manager r12.6.2:

### Puntos finales

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

### Servidores de aplicaciones

- JBoss 6.1 EAP
- Servidor de aplicaciones WebSphere (WAS) 8.0
- Servidor de aplicaciones WebSphere (WAS) 8.5

### Almacén de usuarios de CA Identity Manager

- CA Directory r12.0 SP11 GA

### Almacén de usuarios de CA Identity Manager y almacén de objetos

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

**Nota:** JBoss no ha anunciado soporte para Microsoft SQL Server 2012.

### Compatibilidad adicional

- Java JDK 1.7.x
- Roles y roles del servidor definidos por el usuario de Microsoft SQL Server 2012 SP1
- Mozilla Firefox 18.x
- Servidor de informes de Business Objects XI 3.1 SP6 (CABI 3.3 SP1)
- Integración con CA SiteMinder r12.5 CR1, r12.5 CR2, r12.5.1, r12.0 SP3 CR12 y r6 SP6 CR10

- Integración con CA Identity Manager, CA Identity Governance r12.5 SP8 y CA Identity Governance r12.6 SP1
- Compatibilidad con aplicación para móviles
- Compatibilidad con el Diseñador de Workpoint versión 3.4.2.20080602-33
- Compatibilidad con Microsoft ADS/Exchange (modo sin agente), DAG y distribución automática de buzones de correo
- Compatibilidad con CA AuthMinder v7.1

## Compatibilidad con aplicación para móviles

La aplicación para móviles de CA Identity Manager permite aprovechar la infraestructura existente de CA Identity Manager para permitir que los usuarios completen las siguientes tareas en un dispositivo móvil, como iPhone o iPad:

- Restablecer una contraseña olvidada  
**Nota:** Cuando se permite a los usuarios de móviles que restablezcan una contraseña olvidada de su dispositivo, CA Identity Manager se basa en la seguridad del dispositivo, en lugar de en preguntas de seguridad. Se debe considerar la posibilidad de requerir más seguridad del dispositivo, como un código de acceso antes de activar la funcionalidad de restablecimiento de la contraseña.
- Cambiar una contraseña
- Responder a solicitudes de aprobación
- Ver detalles del gestor

Esta función permite que los usuarios aprueben solicitudes del flujo de trabajo para ver información acerca del gestor de un usuario.

**Nota:** CA Identity Manager 12.6.4 no es compatible con la versión 1.0 de la aplicación móvil. Descargue la última versión en Apple Store.

Para obtener más información sobre la aplicación para móviles, consulte la *Guía de administración*.

---

## Synchronization/Remove Account Template Values From Accounts (Sincronización/eliminación de los valores de la plantilla de cuenta en Cuentas)

Ahora se puede utilizar la función Synchronization/Remove Account Template Values From Accounts (Sincronización/eliminación de los valores de la plantilla de cuenta en Cuentas) en el atributo Responsibilities List (Lista de responsabilidades) de la plantilla de cuenta de Oracle Applications para que caduque una entrada de responsabilidad en la cuenta de Oracle Applications.

Adicionalmente, esta versión incluye mejoras en los cálculos de responsabilidad para impedir errores de sincronización.

Para obtener más información sobre la función, consulte Responsibilities List and Account Synchronization (Lista de responsabilidades y sincronización de cuentas) en la *Guía de conectores*.

## Configuración mejorada para el conector de LND

Para mejorar el rendimiento del Conector de LND durante las operaciones Explorar y Correlacionar, se ponen a disposición los siguientes valores de configuración configurables:

- readExpirationDateInSearch
- readOuFromPrimaryAddressBookOnly
- readAcctFromPrimaryAddressBookOnly
- enableUouDetection

**Nota:** Se pueden cambiar los valores de los atributos anteriores en el archivo siguiente:

CA\Identity Manager\Connector Server\conf\override\lnd\connector.xml

## Esquema de la base de datos de persistencia de la tarea

Esta versión incluye mejoras a los scripts de SQL que actualizan el esquema de la base de datos de persistencia de la tarea. Los scripts establecen el tamaño de columna correcto e insertan el procedimiento almacenado de detalles acerca del estado de tiempo de ejecución.

En esta actualización, no hay ninguna discrepancia de tamaño entre la tabla de runtimeStatusDetail12 y la tabla de archive\_runtimeStatusDetail12 correspondiente para los sistemas nuevos o actualizados. Esta actualización elimina los errores con la tarea Limpiar tareas enviadas.

## Compatibilidad con la desactivación de la contraseña de cuentas de SAP

En esta versión, el atributo Contraseña desactivada se encuentra disponible en la ficha Cuenta. Mediante este atributo, se puede crear una cuenta de SAP con una contraseña desactivada. Se puede desactivar también la contraseña de una cuenta de SAP existente. Para volverla a activar, restablezca la contraseña.

## Dos modos para la conexión a Exchange: sin agente y con agente

Con esta versión, se puede conectar a los puntos finales de Exchange 2007 y de Exchange 2010 sin utilizar ningún agente. Se recomienda utilizar el modo sin agente para las conexiones nuevas a estos puntos finales.

Sin embargo, el modo sin agente no funciona con Exchange 2003 y se debe realizar la conexión mediante el agente remoto.

La tabla siguiente muestra las versiones compatibles de Exchange para los modos con agente y sin agente:

Versiones de punto final	Agente	Sin agente
Exchange 2003	Sí	No
Exchange 2007	Sí	Sí
Exchange 2003 y Exchange 2007	Sí	No
Exchange 2010	Sí	Sí
Exchange 2007 y Exchange 2010	Sí	Sí

## Compatibilidad con los grupos de acceso de datos de Exchange (DAG)

En esta versión, Exchange 2010 podrá utilizar los grupos de acceso de datos de Exchange (DAG) para garantizar la alta disponibilidad. Se puede conectar a un DAG para garantizar que la conexión al punto final sobreviva a una conmutación por error.

## Compatibilidad con la distribución automática de buzones de correo en Exchange 2010

En esta versión, el conector de Active Directory (AD) Exchange podrá gestionar una distribución automática de buzones de correo en Exchange 2010.

Cuando se crea o se mueve un usuario existente de un buzón de correo o mailenable, este se almacenará en una base de datos de buzón de correo. Los servidores Exchange anteriores requieren especificar la base de datos del buzón de correo para realizar una de las operaciones mencionadas. Exchange Server 2010 selecciona la base de datos de Exchange mediante una distribución automática de buzones de correo.

## Conexión a SQL Server cuando la base de datos esté sin conexión

Ahora se puede examinar y correlacionar un punto final de SQL Server cuando la base de datos esté sin conexión.

## Tarea para crear una definición de la instantánea para informes

Ahora se recomienda utilizar la tarea Crear definición de instantánea para crear una instantánea de los datos necesarios para generar un informe. Los archivos XML de parámetros de la instantánea predeterminados se eliminan gradualmente. Para obtener más información, consulte la *Guía de administración*.

## 12.6.1

[Nuevas certificaciones](#) (en la página 22)

[Almacén de usuarios de JNDI con SSL activado](#) (en la página 22)

[Compatibilidad con las contraseñas cifradas en el directorio de arranque de la Consola de gestión](#) (en la página 23)

## Nuevas certificaciones

Las siguientes plataformas nuevas están certificadas con CA Identity Manager r12.6.1:

### Puntos finales

- Microsoft SQL 2012 como punto final estático y dinámico
- CA Directory r12 SP10 CR2 como punto final de JNDI
- CA Embedded Entitlements Manager (EEM) compatible con el Gestor de aprovisionamiento

### Almacén de usuarios de CA Identity Manager

- CA Directory r12 SP10 CR2

### Almacén del tiempo de ejecución y almacén de usuarios de CA Identity Manager

- Microsoft SQL Server 2012 SP1

### Compatibilidad adicional

- Mozilla Firefox 14.x
- Servidor de informes de Business Objects XI 3.1 SP5 (CA Business Intelligence 3.3)  
Esta versión coincide con la versión compatible con CA SiteMinder.
- Compatibilidad del servidor de informes en una configuración de la disponibilidad alta
- Compatibilidad de CA Identity Manager con CA Identity Governance r12.6
- Compatibilidad de CA Identity Manager con CA SiteMinder r12.0 SP3 CR11

## Almacén de usuarios de JNDI con SSL activado

Ahora se impone la verificación del certificado del mismo nivel. La función requiere que se agregue el certificado de servidor SSL de almacén de usuarios en el almacén de claves de confianza predeterminado de JRE de CA Identity Manager. El almacén de claves es el archivo cacerts o jssecacerts en esta ubicación:

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

Utilice la herramienta clave de la utilidad JDK para agregar el certificado.

---

## Compatibilidad con las contraseñas cifradas en el directorio de arranque de la Consola de gestión

Si se asegura la Consola de gestión mediante el directorio de arranque denominado AuthenticationDirectory, se podrá cifrar ahora la contraseña para el administrador de la Consola de gestión.

### 12.6

[Aspecto y nombre nuevos](#) (en la página 23)

[Experiencia del usuario simplificada](#) (en la página 24)

[Mejoras del aprovisionamiento](#) (en la página 24)

[Mejoras del conector](#) (en la página 24)

[Mejoras del rendimiento](#) (en la página 26)

[Mejoras de la política exprés](#) (en la página 27)

[Seguridad de la Consola de gestión](#) (en la página 28)

[Solicitudes de acceso básicas](#) (en la página 28)

[Documentación nueva para Config Xpress](#) (en la página 30)

[Reemplazo de CA Identity Manager nativa para SiteMinder Advanced Password Services](#)  
(en la página 31)

[Claves dinámicas para cifrar datos](#) (en la página 32)

[Sincronización del servidor de Active Directory](#) (en la página 32)

[Auditoría de eventos de cierre de sesión e inicio de sesión de usuarios](#) (en la página 33)

[Soporte SHA-2](#) (en la página 33)

### Aspecto y nombre nuevos

Además, la consola de usuario predeterminada se ha actualizado para reflejar los nuevos estilos y colores de CA.

El servidor de conector de Java (Java CS o JCS) ha recibido el nuevo nombre de Servidor del conector de CA IAM (Servicios de la nube de CA IAM).

## Experiencia del usuario simplificada

Esta versión incluye las siguientes mejoras de experiencia del usuario:

- Pantallas de tarea de autoservicio actualizadas

Se han actualizado las siguientes pantallas para mejorar la usabilidad:

- Apariencia de portal de la pantalla de inicio de sesión
- Autorregistro/creación de una identidad
- Cambio de mi contraseña
- Restablecimiento de contraseña olvidada
- ID de usuario olvidado

- Ciertas tareas de administración utilizan controles de Web 2.0.

## Mejoras del aprovisionamiento

CA Identity Manager 12.6 incluye las siguientes funciones y cambios nuevos para mejorar el aprovisionamiento.

### Servidor de aprovisionamiento en Linux

El servidor de aprovisionamiento ahora se puede instalar en Red Hat Linux como alternativa a Solaris.

### Funciones del gestor de aprovisionamiento en la Consola de usuario

Varias funciones del gestor de aprovisionamiento ahora son compatibles con la Consola de usuario:

- Sincronización de usuarios, roles, cuentas de puntos finales y plantillas de cuenta  
La integración de puntos finales y cuentas en CA Identity Manager puede dar lugar a una pérdida de sincronización. Por ejemplo, los roles de aprovisionamiento que se asignan a un usuario pueden diferir de las cuentas reales que posee ese usuario. Las tareas de sincronización corrigen este problema.
- Las reglas de correlación controlan la asignación de atributos de cuentas de puntos finales a atributos de usuario en la Consola de usuario. Por ejemplo, Access Control tiene un atributo llamado AccountName. Se puede crear una regla para asignarlo a FullName en la Consola de usuario.

## Mejoras del conector

CA Identity Manager 12.6 incluye las siguientes funciones y cambios nuevos para facilitar la creación e implementación de conectores nuevos.

---

## Implementación en caliente: instalación de un conector nuevo sin reiniciar Servicios de la nube de CA IAM

El Servidor del conector de CA IAM (Servicios de la nube de CA IAM) es el nuevo nombre para el servidor de conector de Java (Java CS o JCS).

Servicios de la nube de CA IAM ahora es compatible con la *implementación en caliente*. La implementación en caliente es el proceso de agregar, eliminar o actualizar un componente sin reiniciar Servicios de la nube de CA IAM. Ahora se pueden llevar a cabo las siguientes tareas:

- Instalar, desinstalar o actualizar un conector *sin* reiniciar Servicios de la nube de CA IAM

Se puede implementar un conector nuevo o actualizado e instalarlo sin reiniciar Servicios de la nube de CA IAM o iniciar sesión en su host. Para obtener las últimas versiones del conector, es necesario ponerse en contacto con el [Soporte de CA](#).

- Implementar bibliotecas de terceros sin reiniciar Servicios de la nube de CA IAM

Algunos conectores requieren bibliotecas que no se pueden proporcionar con Servicios de la nube de CA IAM. Antes era necesario implementar estas bibliotecas y, a continuación, reiniciar Servicios de la nube de CA IAM. Ahora, se pueden implementar mientras el servidor de conectores se está ejecutando.

Servicios de la nube de CA IAM incluye una conjunto esencial de bibliotecas de terceros y cualquier conector puede utilizar cualquiera ellas. Un conector también puede incluir cualquier otra biblioteca de terceros que necesite.

**Nota:** La implementación en caliente no funciona con conectores de C++.

## Generador de paquetes: nueva herramienta para crear conectores

Servicios de la nube de CA IAM requiere que se proporcionen conectores como un paquete de iniciativa de puerta de enlace de servicios abiertos. El marco de trabajo de OSGi es un sistema de módulos y plataforma de servicios para el lenguaje de programación Java que implementa un modelo componentes completo y dinámico. El SDK para el servidor de conectores ahora incluye una herramienta de generación de paquetes, que ayuda a encapsular un conector en un paquete.

## Inicio de sesión para conectores y Servicios de la nube de CA IAM

Ahora se puede iniciar sesión en Servicios de la nube de CA IAM para ver mensajes de registro recientes para Servicios de la nube de CA IAM y sus conectores. Todavía se pueden utilizar archivos de registro para ver todos los mensajes de registro.

## Certificados para conectores y Servicios de la nube de CA IAM

Ahora se puede iniciar sesión en Servicios de la nube de CA IAM para ver y gestionar certificados para Servicios de la nube de CA IAM y sus conectores.

## Uso de Connector Xpress para asignar atributos personalizados y atributos de capacidad personalizados

Connector Xpress se utiliza para asignar atributos personalizados y atributos de capacidad personalizados. El uso del archivo <jcs-home>/conf/override/Ind/Ind\_custom\_metatdata.xml para asignar atributos ya no está disponible.

## Servicios de la nube de CA IAM como proxy para CCS

CA Identity Manager ahora utiliza Servicios de la nube de CA IAM como proxy para el servidor de conectores de C++ (CCS). CA Identity Manager ya no se comunica con CCS directamente.

## Mejoras del rendimiento

CA Identity Manager 12.6 incluye mejoras del rendimiento en las siguientes áreas del producto.

### Mejoras del rendimiento del cargador masivo

En esta versión, el rendimiento del cargador masivo ha mejorado. Las mejoras incluyen los cambios siguientes:

- Tasa de envío más alta de tareas mediante la tarea del cargador masivo principal (alimentador); se ejecutan más tareas de forma paralela.
- Optimizaciones en la reutilización de la conexión de la base de datos; el almacenamiento en la memoria caché de la definición de los atributos de objetos gestionados da lugar a una ejecución más rápida de cada tarea de principio a fin.
- Mejoras a algunos complementos y escuchas para acelerar el procesamiento de los eventos que se generan durante la ejecución de las tareas.

Para mejorar aún más el rendimiento, se recomienda llevar a cabo estos cambios durante la operación de la carga masiva:

- Desactivar todas las políticas de la política exprés, los identificadores de tareas lógicas del negocio y los indicadores de sincronización no deseados en el nivel de tarea.
- Ejecutar la tarea del cargador masivo (alimentador) como usuario especializado con la menor cantidad posible de roles de administrador y tareas de administración en el ámbito.

**Nota:** Para obtener más información sobre mejoras del rendimiento adicionales, consulte la sección sobre el cargador masivo en la *Guía de administración*.

## Rendimiento de las exportaciones de instantáneas mejorado

En esta versión, se ha refactorizado el proceso de exportación de datos de instantáneas para informes para mejorar el rendimiento y la usabilidad. Mediante el asistente Definición de la instantánea, se pueden definir o personalizar las reglas para cargar usuarios, puntos finales, roles de administrador, roles de aprovisionamiento, grupos y organizaciones.

Mediante esta función, se puede utilizar una tarea de la Consola de usuario para seleccionar y exportar solamente los atributos deseados para una instancia de instantánea concreta. En versiones anteriores, los usuarios tenían que editar un archivo XML manualmente.

**Nota:** Todavía se pueden utilizar y personalizar los archivos XML predeterminados para capturar instantáneas.

Para obtener más información sobre la creación de definiciones de instantáneas, consulte la *Guía de administración*.

## Mejoras de la política exprés

Esta versión contiene las siguientes mejoras de la política exprés:

- Complementos de atributos para objetos gestionados  
Los siguientes complementos de atributos de objetos gestionados se han agregado a la política exprés:
  - Atributo de objeto: permite extraer el valor de cualquier atributo del objeto gestionado.
  - El valor del atributo del objeto ha cambiado/Atributo de un objeto específico: igual que El valor del atributo del usuario ha cambiado y Atributo de un usuario específico, pero funcionan con cualquier tipo de objeto gestionado
  - Set Object Attribute (Establecer objeto de atributo): permite modificar el atributo de los objetos gestionados.
- Función Recorte  
La función Recorte permite eliminar los espacios iniciales y finales no deseados de cualquier elemento de datos o cadena.

- Compatibilidad con más reglas de acción

Antes, al intentar agregar más de 60 o 70 reglas de acción a una política, la política exprés no agregaba la política. En tal caso, no se comunicaba ningún error ni excepción en los registros. Ahora, las políticas de la política exprés pueden ser compatibles con hasta 500 reglas de acción.

- Wiki de la política exprés

La documentación de la política exprés se ha actualizado y ahora se encuentra en una [wiki](#) en la comunidad global de usuarios de CA Security.

## Seguridad de la Consola de gestión

La Consola de gestión permite a los administradores crear y gestionar entornos y directorios de CA Identity Manager.

La instalación de CA Identity Manager ahora incluye una opción, que se encuentra seleccionada de forma predeterminada, para asegurar la Consola de gestión. Durante la instalación, se crea una cuenta que puede acceder a la Consola de gestión en un directorio predefinido.

Después de la instalación, se pueden agregar administradores adicionales que necesiten acceder a la Consola de gestión.

**Nota:** Para obtener más información, consulte la *Guía de configuración*.

## Solicitudes de acceso básicas

Los usuarios de CA Identity Manager pueden solicitar acceso a los servicios que necesitan para realizar sus funciones de trabajo.

Un *servicio* agrupa todas las autorizaciones (tareas, roles, grupos y atributos) que un usuario necesita para un rol de negocio determinado. Los servicios están a disposición del usuario mediante las tareas de solicitud de acceso de la consola de usuario de CA Identity Manager. Las tareas de solicitud de acceso permiten que un usuario o administrador soliciten, asignen, revoquen y reanuden un servicio.

Los servicios permiten a un administrador combinar autorizaciones de usuario en un solo paquete, gestionándolas como un conjunto. Por ejemplo, todos los empleados nuevos de Ventas necesitan acceder a un conjunto definido de tareas y cuentas en los sistemas de punto final específicos. También necesitan de información específica agregada a los perfiles de cuenta de usuario. Un administrador crea un servicio denominado Administración de ventas que contiene todas las tareas, roles, grupos e información sobre los atributos de perfil necesarios para un empleado nuevo de Ventas. Cuando un administrador asigna el servicio Administración de ventas a un usuario, este usuario recibe todo el conjunto de roles, tareas, grupos y atributos de cuenta que define el servicio.

Los usuarios también pueden acceder a los servicios solicitando ellos mismos el acceso. En la Consola de usuario, cada usuario tiene una lista de servicios disponibles para la solicitud. Esta lista se rellena con servicios que un administrador ha marcado como Autosuscripción con los privilegios adecuados, normalmente durante la creación de un servicio. Desde la lista de servicios disponibles, los usuarios pueden solicitar acceso a los servicios que necesitan. Cuando el usuario solicita acceso a un servicio, la solicitud se rellena automáticamente y las autorizaciones asociadas se asignan inmediatamente al usuario. Un administrador con los privilegios adecuados también puede configurar el cumplimiento del servicio para requerir la aprobación del flujo de trabajo o generar notificaciones de correo electrónico.

**Nota:** Esta versión inicial es compatible con capacidades de solicitud de acceso básicas. La funcionalidad de solicitud de acceso permite a los usuarios finales solicitar autorizaciones (gestionadas y no gestionadas por CA Identity Manager), definir flujos de aprobación y utilizar flujos de cumplimiento.

Esta versión inicial no es compatible con capacidades de solicitud de acceso avanzadas como las siguientes:

- Definición masiva de objetos de servicios de solicitud de acceso
- Integración con CA Identity Governance (anteriormente denominado CA GovernanceMinder)
- Búsqueda y filtrado granular

Esta versión inicial no es compatible con las siguientes capacidades:

- Definición masiva de objetos de servicios
- Filtrado granular
- Búsquedas
- Integración con otros mecanismos de cumplimiento

Para obtener más información acerca de los servicios, consulte la *Guía de administración*.

## Documentación nueva para Config Xpress

Config Xpress es una herramienta que se incluye con CA Identity Manager. Se puede utilizar esta herramienta para analizar y trabajar con las configuraciones de los entornos de CA Identity Manager.

Config Xpress permite hacer las siguientes tareas:

- Mover componentes entre entornos.  
La herramienta detecta automáticamente cualquier otro componente obligatorio y solicita que también se muevan. Esto puede ahorrar mucho trabajo.
- Publicar un informe de los componentes del sistema en un archivo PDF.
- Publicar la configuración de XML para un componente concreto.

Para obtener más información sobre la importación de la configuración, consulte Gestión de la configuración en la *Guía de configuración*.

---

## Reemplazo de CA Identity Manager nativa para SiteMinder Advanced Password Services

Además de las políticas de contraseñas básicas, CA Identity Manager proporciona los siguientes valores de configuración de contraseñas adicionales ahora desacoplados de SiteMinder:

- Caducidad de contraseña:
  - Realizar un seguimiento de los inicios de sesión correctos o incorrectos: si está activado, la información de seguimiento de intentos de inicio de sesión correctos o incorrectos se escribe en el atributo de datos de la contraseña del usuario relevante en el almacén de usuarios.
  - Autenticar al producirse un error de seguimiento del inicio de sesión: si está desactivado, los usuarios no pueden iniciar sesión cuando CA Identity Manager no puede escribir información de seguimiento en el almacén de usuarios.
  - La contraseña caduca si no se cambia: configura el comportamiento de la caducidad. Si una contraseña no se ha cambiado después de un número especificado de días, los usuarios se desactivan o se les obliga a cambiar su contraseña. También permite el envío de advertencias de caducidad para un número especificado de días.
  - Inactividad de contraseña: configura el comportamiento de un usuario inactivo. Si el usuario no ha realizado un intento de inicio de sesión correcto después de un número especificado de días, se desactiva el usuario o se le obliga a cambiar la contraseña.
  - Contraseña incorrecta: configura el número de inicios de sesión incorrectos que se permiten antes de desactivar el usuario.
  - Varias expresiones regulares: especifica expresiones regulares con las que las contraseñas deben o no deben coincidir. Las políticas de contraseñas de CA Identity Manager son compatibles con una única expresión de cada tipo.
- Restricciones de la contraseña:
  - Número mínimo de días antes de la reutilización
  - Número mínimo de contraseñas antes de la reutilización
  - Porcentaje de diferencia con respecto a la contraseña anterior
  - Ignorar secuencia cuando se comprueban diferencias: ignorar la posición de los caracteres al calcular la diferencia del porcentaje.

**Nota:** Esta versión no es compatible con datos de la contraseña históricos de una implementación de CA Identity Manager que utilice servicios de contraseña de CA SiteMinder (historial de contraseñas) a una implementación que incluya solamente servicios de contraseña de CA Identity Manager r12.6.

## Claves dinámicas para cifrar datos

En un entorno, se pueden crear claves dinámicas que cifran o descifran datos. Si se sospecha que un usuario ha obtenido acceso no autorizado a una clave, se puede cambiar la contraseña del almacén de claves. El almacén de claves es la base de datos que almacena las claves secretas. Una vez modificada esta contraseña, CA Identity Manager vuelve a cifrar los valores de las claves.

En la sección Gestión de claves secretas de la *Guía de administración* se puede obtener más información.

## Sincronización del servidor de Active Directory

Se puede configurar Servicios de la nube de CA IAM para que permita que usuarios con el servidor Active Directory (ADS) sincronicen la información de identidad local con la información de punto final basada en la nube. Por ejemplo, se podría configurar ADS para sincronizarse con una instalación de Salesforce basada en la nube. Entonces, las adiciones o los cambios a un grupo de usuarios local sincronizado se propagarían al entorno de Salesforce.

Esta función requiere Servicios de la nube de CA IAM, un punto final compatible y el conector adecuado.

Se debe tener en cuenta lo siguiente sobre la función de sincronización de Active Directory:

- Esta función admite solamente Active Directory. No se pueden utilizar otros directorios LDAP con esta función en esta versión.
- Esta función es compatible solamente con puntos finales basados en la nube que dispongan de un conector existente. En esta versión, las aplicaciones compatibles incluyen Google Apps y Salesforce.

Para obtener más información sobre esta función, consulte *Connectors Guide*.

## Auditoría de eventos de cierre de sesión e inicio de sesión

Para mejorar el control del acceso de los usuarios en el entorno de CA Identity Manager, se puede configurar CA Identity Manager para que audite los eventos de inicio de sesión y de cierre de sesión de los usuarios en un entorno. Se pueden ver estos eventos registrados en el informe predeterminado Detalles de auditoría.

**Nota:** No se pueden registrar los eventos de inicio de sesión y de cierre de sesión de los usuarios para CA SiteMinder.

Se pueden configurar estos valores en el archivo Configuración de la auditoría. Para obtener más información sobre la configuración de los eventos de inicio de sesión y cierre de sesión, consulte el capítulo Auditoría en la *Guía de configuración*.

## Soporte SHA-2

El algoritmo de hash de certificado SSL de SHA-2 es un algoritmo criptográfico desarrollado por el Instituto nacional de normas y tecnología (NIST) y la Agencia de seguridad nacional (NSA). Los certificados de SHA-2 son más seguros que todos los algoritmos anteriores. En CA Identity Manager, se pueden configurar los certificados SSL firmados por SHA-2 en lugar de los certificados firmados con la función de hash SHA-1.



# Capítulo 2: Consideraciones acerca de la instalación

---

Esta sección contiene los siguientes temas:

- [Activación del soporte de la política exprés para los servicios web SOAP y REST](#) (en la página 36)
- [Versiones y plataformas compatibles](#) (en la página 36)
- [Componentes obsoletos y descartados](#) (en la página 36)
- [Coinstalación de agentes remotos de UNIX con los productos de CA adicionales](#) (en la página 37)
- [Contraseñas no cifradas](#) (en la página 37)
- [Oracle 11g R2 RAC como almacén de usuarios y almacén de objetos](#) (en la página 37)
- [Oracle 12c RDB como almacén de usuarios y almacén de objetos](#) (en la página 38)
- [ADAM 2008 como almacén de usuarios](#) (en la página 38)
- [Los caracteres no ASCII provocan errores de instalación en sistemas con idiomas distintos del inglés](#) (en la página 38)
- [Solución al problema del cortafuegos en Windows 2008 SP2](#) (en la página 38)
- [Implemente las páginas de JSP para las acciones de administrador](#) (en la página 39)
- [Instalación del directorio de aprovisionamiento en Linux](#) (en la página 39)
- [Linux: requisito de JDK para la instalación](#) (en la página 40)
- [CA Identity Manager en Linux de 64 bits con errores de conectividad de SiteMinder](#) (en la página 40)
- [Mejora del rendimiento en WebSphere y AIX](#) (en la página 41)
- [Ignorar error de WebSphere 7 y Oracle](#) (en la página 41)

## Activación del soporte de la política exprés para los servicios web SOAP y REST

Se ha mejorado la política exprés para que sea compatible con los servicios web SOAP (mediante el método de autenticación básica) y REST (mediante el método de autenticación básica, autenticación proxy y métodos de autenticación OAuth), de modo que pueda integrarse con aplicaciones externas que proporcionen una interfaz de servicio web. Para utilizar los servicios web de la política exprés (SOAP y REST) con la edición de la comunidad de JBoss 5.1, copie los siguientes jars en el directorio "\lib\endorsed" de edición de la comunidad de JBoss 5.1 desde el directorio cliente y vuelva a reiniciar el servidor de aplicaciones:

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

**Note:** No es necesario copiar estos archivos para las versiones de EAP.

## Versiones y plataformas compatibles

En CA Identity Manager r12.5 se han realizado algunos cambios en las versiones, directorios y bases de datos del servidor de aplicaciones compatibles.

**Nota:** Para obtener una lista completa de las plataformas y versiones compatibles, consulte el cuadro de compatibilidad de CA Identity Manager en [Soporte de CA](#).

## Componentes obsoletos y descartados

Ciertos componentes se están quedando obsoletos, lo que significa que no serán compatibles en versiones futuras. Otros componentes se han descartado, lo que quiere decir que ya no se proporcionan con el producto o que ya no se prueban con el producto. Estos componentes se muestran en [CA Identity Manager Deprecation Policy](#) en Soporte de CA.

## Coinstalación de agentes remotos de UNIX con los productos de CA adicionales

En esta versión, los agentes remotos de UNIX (excepto las plataformas de TRU64) se instalan ahora, de modo que el software instalado siga los componentes de software dependientes, como CA ITCM.

Si se desea actualizar el agente remoto de UNIX, el método de seguimiento nuevo no actualizará los números de referencia de los componentes de software dependientes. Si se desea desinstalar el producto después de esta actualización, utilice el archivo de desinstalación siguiente:

```
<directorio de instalación>/scripts/uninstall-force.sh
```

**Nota:** Garantice que el archivo `uninstall-force.sh` no se utilice en hosts que dispongan de software de CA adicional instalado. Los productos pueden depender de los mismos paquetes de software que elimina este script.

## Contraseñas no cifradas

Las instalaciones nuevas no cifran las contraseñas de usuario de forma predeterminada. Además, cuando se integra SiteMinder con CA Identity Manager, no se puede activar el cifrado de la contraseña mediante `AttributeLevelEncrypt`. Este atributo solamente funciona cuando SiteMinder no está instalado.

Esta incidencia se corregirá en una versión futura.

## Oracle 11g R2 RAC como almacén de usuarios y almacén de objetos

Al utilizar Oracle 11g R2 RAC como almacén de usuarios y almacén de tiempo de ejecución, se deben realizar las siguientes tareas para utilizar las capacidades del clúster de un clúster de base de datos de Oracle:

- Utilizar SCAN (Nombre de acceso del cliente único) mientras se instala CA Identity Manager con Oracle 11g R2 RAC.
- Crear el *espacio de tabla* de la base de datos en el grupo de disco compartido durante la creación de un espacio de tabla.

## Oracle 12c RDB como almacén de usuarios y almacén de objetos

Cuando se utiliza Oracle 12c RDB como almacén de usuarios y almacén de tiempo de ejecución, se debe utilizar solamente modo de base de datos sin contenedor. La opción RDBMS para Oracle 12c Container DB (multicliente) no se incluye en el producto para empresas.

## ADAM 2008 como almacén de usuarios

Si utiliza a ADAM 2008 como el almacén de usuarios de CA Identity Manager e integra CA Identity Manager con SiteMinder, será necesario SiteMinder r6.0 SP6/r6.x QMR6.

## Los caracteres no ASCII provocan errores de instalación en sistemas con idiomas distintos del inglés

Durante la instalación de CA Identity Manager, el instalador extrae archivos a un directorio temporal. En algunos sistemas localizados, la ruta predeterminada del directorio temporal contiene caracteres no ASCII. Por ejemplo, la ruta predeterminada del directorio temporal en un sistema Windows en español es la siguiente:

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

Los caracteres no ASCII harán que el instalador muestre una página de resumen previa a la instalación en blanco y, a continuación, se producirá un error de instalación.

### Solución

Cambie la variable de entorno temporal para que apunte a una carpeta que sólo contenga caracteres ASCII.

## Solución al problema del cortafuegos en Windows 2008 SP2

Durante la instalación en las implementaciones de Windows 2008 SP2, la comunicación con los componentes de CA Identity Manager, como por ejemplo el servidor de aprovisionamiento, el servidor de conector de Java y el servidor de conector de C++, la bloquea el cortafuegos.

Para solucionar este problema, agregue excepciones de puerto o desactive el cortafuegos de Windows para acceder a los componentes distribuidos de CA Identity Manager en las implementaciones de Windows 2008 SP2.

## Implemente las páginas de JSP para las acciones de administrador

El servidor de CA Identity Manager incluye páginas de JSP de muestra para realizar las acciones siguientes:

- Hacer ping al servidor de aplicaciones
- Mostrar los BLTH implementados
- Mostrar información acerca de los tipos de objeto y proveedores de objetos gestionados
- Mostrar la información de complementos
- Cambiar los niveles de registro

Las páginas de JSP se instalan en esta ubicación:

`admin_tools\samples\admin`

La carpeta contiene un archivo léame.txt con instrucciones para utilizar las páginas de JSP.

**Nota:** Aparecerá un error 404 si utiliza estas páginas de JSP sin seguir las instrucciones del archivo léame.txt.

## Instalación del directorio de aprovisionamiento en Linux

Si instala el directorio de aprovisionamiento en un sistema de Linux, el sistema automáticamente utiliza direcciones de IPv6 aunque pretenda utilizar IPv4 en este sistema. Todos los DSA parecen estar ejecutándose, pero cuando intenta conectarse a los DSA mediante Jxplorer o instalar el servidor de aprovisionamiento, puede que aparezca un error de conexión rechazada.

### Para desactivar IPv6 en Linux

1. Antes de la instalación del directorio de aprovisionamiento, siga los pasos del artículo de la base de conocimiento de Red Hat para [Desactivar IPv6 en LINUX](#).
2. Asegúrese de que `/etc/hosts` tiene ninguna entrada para esta dirección:  
`nombre de host 127.0.0.1`

## Linux: requisito de JDK para la instalación

CA Identity Manager 12.6.4 requiere Oracle JDK 1.6.

RedHat 6.x incluye OpenJDK 1.6, que puede hacer que el instalador de CA Identity Manager se cuelgue indefinidamente. Es necesario asegurarse de utilizar la versión de Sun JDK requerida, como se especificada en el [cuadro de compatibilidad](#) de CA Identity Manager.

## CA Identity Manager en Linux de 64 bits con errores de conectividad de SiteMinder

El instalador informa sobre errores con la CA Identity Manager en Linux de 64 bits cuando se selecciona "Conectarse a SiteMinder". La configuración del agente requerida no es correcta en SiteMinder

**Importante:** Realice los pasos de solución de problemas antes de implementar cualquier directorio/entorno.

### Solución

1. Recuerde el nombre del agente y contraseña proporcionados durante la instalación. Alternativamente puede leer el valor para la propiedad de "AgentName" de los siguientes elementos:

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

2. Abra la interfaz de usuario de SiteMinder WAM y cree un agente con el nombre de agente. Verifique que se selecciona la casilla de verificación "agente de 4.x".
3. Inicie el servidor de aplicaciones y verifique que no se produce ningún problema de conectividad con el servidor de políticas.

Debe consultar una línea como la siguiente sin ninguna excepción:

```
ADVERTENCIA 13:40:43,156 [valor predeterminado] * Paso 2 de inicio:  
intentando iniciar PolicyServerService
```

## Mejora del rendimiento en WebSphere y AIX

Para una instalación de WebSphere en AIX, se puede obtener un mejor rendimiento en la Consola de usuario si se establece el tamaño máximo de la memoria dinámica.

### Siga estos pasos:

1. Busque el archivo `server.xml` en la siguiente ubicación:  
`WAS_HOME/profiles/Profile/config/cells/Cell/nodes/Node/servers/Server`
2. Agregue `maximumHeapSize="1000"` al elemento `jvmEntries`.

Se puede utilizar un valor más alto si es necesario. Por ejemplo, para establecer `maximumHeapSize` en 2 GB (2048 MB), se agrega de la forma que se muestra en negrita en el siguiente extracto de este archivo:

```
<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=77
77" 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>
```

## Ignorar error de WebSphere 7 y Oracle

Cuando se instala CA Identity Manager mediante un almacén de tiempo de ejecución de Oracle y el JRE predeterminado WebSphere 7, aparece el error siguiente en los registros de CA Identity Manager.

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. (Oracle no admite el uso de la versión 10 de su controlador JDBC con la versión de Java Runtime Environment que utiliza el servidor de aplicaciones).

Este error se puede ignorar.



# Capítulo 3: Actualizaciones

---

En esta sección se describen los problemas de CA Identity Manager r12.5 SP1 relacionados con las actualizaciones.

Esta sección contiene los siguientes temas:

[El rol Gestor del sistema necesita roles de administrador tras la actualización de 12.6](#) (en la página 43)

[Rutas de actualización compatibles](#) (en la página 44)

[Scripts nuevos para actualizar la persistencia de la tarea y los esquemas del archivo de archivado](#) (en la página 44)

[Archivos JCO nuevos para SAP R3](#) (en la página 44)

[Archivo de definición del rol de Active Directory nuevo](#) (en la página 44)

[Actualización al archivo jboss.xml](#) (en la página 45)

[Compatibilidad con los servidores de aplicaciones de 64 bits](#) (en la página 45)

[Problema al actualizar un clúster de CA Identity Manager r12 CR6 o posterior](#) (en la página 46)

[Error de flujo de trabajo después de la actualización desde una versión anterior a r12.5 SP7](#) (en la página 47)

[Error de migración de entorno](#) (en la página 47)

[Error de actualización del proveedor de credenciales](#) (en la página 48)

[Error interno del proveedor de credenciales de Vista](#) (en la página 48)

[Ninguna pantalla de búsqueda con la tarea Explorar y correlacionar](#) (en la página 48)

[Error no crítico tras actualizar el gestor de aprovisionamiento de r12](#) (en la página 49)

[Cambiar de nombre los puntos finales de ACF2, RACF y TSS antes de la actualización](#) (en la página 49)

[Ejecución del script de actualización de SQL](#) (en la página 49)

## El rol Gestor del sistema necesita roles de administrador tras la actualización de 12.6

Cuando se actualiza desde la versión 12.6 (o posteriores) de CA Identity Manager, el rol Gestor del sistema debe ser proporcionado por un rol de administrador.

**Nota:** De no hacerse así, las búsquedas del rol Administrador pueden no devolver resultados.

Siga uno de los pasos siguientes:

- En la Consola de gestión, haga clic en Gestor del sistema y después seleccione el usuario.
- O bien puede agregar el Rol de administrador al rol Gestor del sistema mediante Modificar rol de administrador, Gestor del sistema.

## Rutas de actualización compatibles

Se puede actualizar a CA Identity Manager 12.6.4 desde las siguientes versiones:

- CA Identity Manager r12
- CA Identity Manager r12.5 o 12.5 SPx
- CA Identity Manager r12.6 o 12.6 SPx

Si se tiene una versión anterior a la r12 de CA Identity Manager, primero es necesario actualizar a r12, r12.5 o r12.5 SP1 a SP6. Estas versiones incluyen la herramienta de `imsconfig`, que se requiere para actualizar una versión anterior a la r12. A continuación, se puede actualizar a CA Identity Manager 12.6.4.

## Scripts nuevos para actualizar la persistencia de la tarea y los esquemas del archivo de archivado

Esta versión incluye scripts nuevos para actualizar la persistencia de la tarea y los esquemas del archivo de archivado. La actualización se ejecuta automáticamente cuando se inicia CA Identity Manager por primera vez después de una actualización. Para obtener más información acerca de los nuevos scripts, consulte la *Guía de instalación*.

## Archivos JCO nuevos para SAP R3

Si desea usar el conector nuevo para SAP R3, será necesario actualizar los archivos JCO. Consulte la guía de punto final para el conector SAP R3 para obtener más información.

## Archivo de definición del rol de Active Directory nuevo

Es necesario asegurarse de que se importa el archivo de definición del rol nuevo para Active Directory en cada entorno. Puede que el entorno de CA Identity Manager actual tenga una versión anterior del archivo de definición del rol de Active Directory. Así que, se debe importar el archivo para actualizar las definiciones del rol a 1.08. Para obtener más detalles sobre la importación de archivos de definición del rol, siga los procedimientos de la *Guía de actualización*.

## Actualización al archivo jboss.xml

Durante un reinicio de JBoss o inicialización de CA Identity Manager, se registran muchos mensajes de error en el archivo server.log de CA Identity Manager. Estos mensajes están relacionados con eventos que gestiona JMX, pero el bean de mensaje de recepción aún no está inicializado. Para corregir este problema, el siguiente archivo ahora incluye una cláusula de dependencia:

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

La cláusula de dependencia se incluye en esta sección:

```
<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>
```

Es necesario asegurarse de incluir esta sección en el archivo jboss.xml. Como resultado, el bean de mensaje de recepción se inicializa antes de que JMX empiece a procesar la cola de eventos.

## Compatibilidad con los servidores de aplicaciones de 64 bits

CA Identity Manager 12.6.4 es compatible con servidores de aplicaciones de 64 bits, que ofrecen un mejor rendimiento que los servidores de aplicaciones de 32 bits. Las siguientes versiones de servidores de aplicaciones de 64 bits son compatibles:

- JBoss 5.0, 5.1 y 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

Consulte la *Guía de actualización* para obtener más detalles acerca de la actualización en el servidor de aplicaciones.

## Problema al actualizar un clúster de CA Identity Manager r12 CR6 o posterior

Si actualiza un clúster de CA Identity Manager r12 CR6 o posterior a CA Identity Manager r12.5 SP1, puede producirse un error de actualización debido a algunas propiedades del clúster en el archivo de instalación que se va a borrar.

### Solución

Asegúrese de que las siguientes propiedades se encuentren en el archivo `im-installer.properties` antes de la actualización:

- WebSphere: compruebe si el nombre del clúster se ha incluido en `DEFAULT_WAS_CLUSTER`. Si no es así, vuelva a agregarlo manualmente.
- WebLogic: compruebe si el nombre del clúster se ha incluido en `DEFAULT_BEA_CLUSTER`. Si no es así, vuelva a agregarlo manualmente.

**Nota:** Este problema no afecta a los clústeres de JBoss.

De forma predeterminada, el archivo de instalación se encuentra en las siguientes ubicaciones:

- Windows: `C:\Archivos de programa\CA\CA Identity Manager\install_config_info\im-installer.properties`
- Unix: `/opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties`

## Error de flujo de trabajo después de la actualización desde una versión anterior a r12.5 SP7

### Síntoma:

Si se actualiza desde un sistema que contiene una versión anterior a r12.5 SP7 en el servidor de aplicaciones de WebLogic, aparecerá este error al iniciar el flujo de trabajo:

```
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']
```

### Solución:

1. Detenga WebLogic.
2. Vaya a la carpeta <IAM-EAR>/APP-INF/lib.
3. Elimine los siguientes archivos:
  - common-pool-1.3.jar
  - annotations.jar
  - eurekifyclient.jar
  - quartz-all-1.5.2.jar
4. Inicie el servidor de aplicaciones.
5. El error de inicio de flujo de trabajo ya no aparecerá.

## Error de migración de entorno

### Síntoma:

Si actualiza desde CA Identity Manager r12 CR1, CR2 o CR3, puede producirse el siguiente error al importar los entornos:

El atributo "accumulateroleeventsenabled" no puede aparecer en el elemento "Aprovisionamiento".

### Solución:

Abra el archivo envsettings.xml en el archivo Env.zip exportado y actualice accumulateroleeventsenabled a acumulateroleeventsenabled (elimine la segunda c de la palabra accumulate).

## Error de actualización del proveedor de credenciales

Tras actualizar el proveedor de credenciales de CA Identity Manager r12 en una plataforma de Windows de 32 bits, la casilla de verificación Desactivar el proveedor de credenciales de contraseña de Microsoft en la aplicación de CAIMCredProvConfig aparece deseleccionada.

### Solución

Abra la aplicación CAIMCredProvConfig y seleccione la casilla de verificación.

## Error interno del proveedor de credenciales de Vista

### Síntoma:

Cuando actualizo el proveedor de credenciales de Vista de CA Identity Manager en plataformas de Windows de 64 bits, recibo el mensaje de error *Error interno 2324.2*.

### Solución:

No se requiere ninguna acción dado que el proceso se ha completado con éxito.

## Ninguna pantalla de búsqueda con la tarea Explorar y correlacionar

Si ha actualizado desde CA Identity Manager r12 o desde CA Identity Manager r12.5 y ha migrado la tarea Explorar y Correlacionar al nuevo modelo de repetición, el botón Explorar de la tarea Explorar y Correlacionar no funcionará correctamente.

### Solución

Configure una pantalla de búsqueda para la tarea para que el nuevo botón Explorar abra una pantalla de búsqueda al hacer clic en éste.

## Error no crítico tras actualizar el gestor de aprovisionamiento de r12

### Síntoma:

Tras actualizar el gestor de aprovisionamiento de CA Identity Manager r12 CRx, el instalador muestra el siguiente mensaje:

El asistente de instalación ha terminado de actualizar CA Identity Manager pero no han tenido lugar errores críticos o advertencias durante la actualización. Para obtener más detalles, consulte el registro de instalación en C:\Archivos de programa\CA\CA Identity Manager.

Se ha informado de errores o advertencias relacionadas con los siguientes componentes

El registro de instalación de CA Identity Manager contiene la siguiente entrada:

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "El proceso no
puede obtener acceso al archivo porque está siendo utilizado en
otro proceso.")
```

### Solución:

El error ocurre porque el instalador no puede crear un directorio que ya existe. Sin embargo, la instalación se ha completado con éxito y el gestor de aprovisionamiento es completamente funcional.

## Cambiar de nombre los puntos finales de ACF2, RACF y TSS antes de la actualización

Ya no se admiten los espacios en los nombres de puntos finales. Si se han creado puntos finales con espacios en el nombre en una versión anterior, elimine los espacios antes de actualizar a 12.6.

## Ejecución del script de actualización de SQL

Después de la actualización, la primera vez que se inicia el servidor de CA Identity Manager, se ejecutará un script. Actualiza el tamaño de columna de la descripción de runtimeStatusDetail12 de la tabla de persistencia de la tarea a 2000 caracteres.

Si se produce un error al ejecutar el script, siga estos pasos:

1. Realice una de las siguientes acciones:
  - Microsoft SQL Server: abra la herramienta de analizador de consultas y seleccione el script que necesita.
  - Oracle: abra la solicitud de SQL para el script que necesita.
2. Seleccione uno de los scripts siguientes:
  - Microsoft SQL Server: <ruta de instalación>\tools\db\taskpersistence\sqlserver\archive\_db\_sqlserver\_upgrade\_to126sp2.sql
  - Oracle en Windows: <ruta de instalación>\tools\db\taskpersistence\oracle9i\archive\_db\_oracle\_upgrade\_to126sp2.sql
  - Oracle en UNIX: <ruta de instalación2>/tools/db/taskpersistence/oracle9i/archive\_db\_derby\_upgrade\_to126sp2.sql
3. Ejecute el archivo de script.
4. Verifique que no aparezca ningún error al ejecutar el script.

# Capítulo 4: Problemas arreglados

---

Esta sección contiene los siguientes temas:

[12.6.4](#) (en la página 51)

[12.6.3](#) (en la página 54)

[12.6.2](#) (en la página 56)

[12.6.1](#) (en la página 58)

## 12.6.4

En CA Identity Manager 12.6.4, se han corregido los problemas siguientes:

Ticket de soporte	Problema notificado
20957471/07	Problema corregido para CQ 170096 en IM 12.6 SP2
21517465/01	Alcance de rol de administrador en la pantalla de búsqueda.
21536689/01	Mantenimiento de una contraseña errónea durante la creación del directorio de IM
21539813/01	Error de actualización de las cuotas y del umbral para cuentas LND si establece Gestor como ACL de archivos de correo
21538682/01	En un IME con tókenes cuando el campo del seleccionador de fechas es erróneo, el mensaje de error muestra el ID de la clave en lugar del par clave-valor del conjunto de recursos
21521403/04	Cambio de categoría de Servicio a causa de la modificación de un objeto del servicio
21547136/01	En las cuentas de Oracle Applications, la fecha de inicio de un elemento de la lista de responsabilidades no se muestra en las cuentas nuevas del gestor de aprovisionamiento hasta que el punto final se explora de nuevo, en el caso de que la cuenta se haya creado mediante una plantilla sin fecha de inicio establecida.
21558292/01	Varios incumplimientos de 508
20957471/09	Las aprobaciones de sincronización inversa se generan para eliminar responsabilidades de una cuenta de Oracle Applications cuando se lleva a cabo una exploración después de crear nuevas cuentas a través de IM con las responsabilidades ya asignadas.
21551822/01	Resultados erróneos del seleccionador de objeto
21567422/01	Valor para la asignación de organización ausente en GM tras la importación desde IM
20957471/11	Comportamiento inesperado de Sincronización inversa de política de cuenta modificada para el servidor de Oracle
21576029/01	Error de visualización de la descripción de Windows NT en la Consola de usuario de IM
21559775/01	Error de importación de roles con caracteres XML no válidos (Unicode: 0x1f) generados por el seleccionador de objeto en la tarea de rol de acceso

---

21593378/01	Información incorrecta del gestor de notificaciones en vivo
21590547/01	IM 12.6 SP2: AD - errores de sincronización para cuentas de Active Directory a causa de un atributo UserPrincipalName en blanco
21588715/01	Cuando una regla de visualización se define en una pantalla de búsqueda de rol del administrador, el filtro de búsqueda deja de funcionar.
21590303/01	Durante la ejecución del nuevo cliente de carga masiva en IM r12.6 SP2, el cargador masivo abre todas sus tareas bajo el estado En curso y retiene JVM, con lo que el resto de tareas se mantienen a la espera en la cola
21594906/01	IM 12.6 SP1: error de aplicación del atributo en el nivel de auditoría AMBOS
21574514/02	IM 12.6 SP2: retención de la tarea en curso con PX activado en el flujo de trabajo del nivel de evento
21606642/02	Rendimiento lento de la tarea Modificar miembros del grupo cuando el grupo contiene 38 000 usuarios
21557047/01	Asignaciones de atributo incorrectas en el conector Office 365
12345678/01	Necesidad de nueva API del Agente web de SiteMinder en IM 12.6 SP4
21604197/01	Detención de la importación de definiciones en Rol de aprovisionamiento cuando el nombre contiene "\00"
21604199/01	Error de búsqueda de roles de aprovisionamiento en "\" en combinación con el carácter comodín "*"
21609415/01	Error del conector Google debido a una API desaprobadado
21626365/01	Error de script al intentar visualizar la página 2 de los detalles del Gestor de aprovisionamiento
21613942/01	Modificación del filtro de contenedor de cuenta
21419884/02	Tiempo excesivo para el filtrado de instantáneas
21592259/01	Error de ejecución inesperado de la funcionalidad de filtrado de contraseñas para la validación de contraseñas
21640856/01	Error de vencimiento de la responsabilidad, tras el rechazo de una aprobación generada por la sincronización inversa para la adición de una responsabilidad en una cuenta de Oracle Applications, aunque se muestra como rechazada en VST
21633958/01	Duplicación de roles de aprovisionamiento (PX)
21641737/01	Niveles de funcionalidad de Win2012 AD comunicados como Win2008R2
21643258/01	Error relacionado con una "solicitud de lectura" similar al error CQ176812
21575724/01	Error de visualización de miembros y administradores de un rol tras el reinicio de JBoss a causa de la regla de ámbito de usuarios en Políticas de administración de Roles de administrador.
21584724/01	Registro adicional para el conector SAP

---

21500603/01	Errores de integración de SiteMinder y CA Identity Manager
21639644/01	Exportación de la plantilla de cuenta de Oracle
21657577/01	Error durante la utilización de JavaScript en el conector personalizado CXP porque JCS ya no hace referencia a Apache CCPP
21636774/01	Obtención de responsabilidades con la fecha actual como fecha de finalización por parte de cuentas FND y devolución de un número mayor de filas ORA-06512 que las solicitadas en "APPS_APPLSYS3.FND_USER_PKG" por parte de ORA/01422: exact fetch.
21641383/01	Conservación de la tarea Activar/Desactivar usuario en el estado En curso si se configura el correo electrónico PolExpress
21646678/01	Error de la utilidad Ant al intentar agregar tókenes a los roles si se ha agregado la propiedad Título a las pantallas de búsqueda
21657600/01	Error de importación por parte de IM de los valores de los campos personalizados en Rol de aprovisionamiento
21687010/01	Error de inicio de algunos informes de ELM
21668810/01	Problemas con la supresión de usuarios asignados a grupos dinámicos
21699782/01	Limitación de la lista de elementos de trabajo. Este CQ cubre el trabajo necesario para la inclusión de elementos de la lista de trabajos en la página opcional de inicio de sesión o bienvenida.
21650405/01	Error de carga de flujos de trabajo basados en políticas por parte de la herramienta Config Xpress
21539813/01	Necesidad de modificaciones en la documentación para la resolución del defecto PROD00176400
21712883/01	IM 12.6 SP2: error de visualización de los atributos de fecha y hora de la cuenta de Active Directory en la zona horaria local en la Consola de usuario de IM
21669984/01	Posibilidad de uso de una tarea privada (no pública) convocada al alias público mediante TEWS cuando IM y SM están integrados
21711390/01	IM 12.6: vulnerabilidad de seguridad. La dirección URL para la solicitud de una página de imagen permite la definición de contentType por parte de un atacante, permitiendo la ejecución del código en el explorador de un usuario autenticado que visita la dirección URL.
21713498/01	Visualización del estado incorrecto Completado de una tarea aunque los eventos aún estén en curso
21699782/01	Adición de la búsqueda por iniciador e ID de usuario en la lista de trabajos del usuario
21704767/01	Error de ejecución de la muestra del EJE de Java para ModifyGroupMembership.java con 12.6 (cualquier Service Pack). Posible regresión para el funcionamiento con 12.5.

21651991/01	Adición de la opción de configuración para la supresión de notificaciones Modify_Account_Password de IMPS en IM
21730035/02	IM12.6 SP2: punto final de Active Directory. Error de actualización del aprovisionamiento a causa del valor de configuración del punto final El usuario debe cambiar la contraseña después de volver a configurar la contraseña en la ficha Configuración
21730581/01	Inconsistencia en el tipo de certificador entre el servidor de aprovisionamiento y punto final de LND
21746621/01	Error de exportación/correlación de cuentas en OU cuando el nombre contiene "&"
21764131/01	Error al intentar realizar una sincronización de cuentas con una plantilla de cuenta WEAK SYNC a causa del atributo único Office365 para Bloquear credenciales asignado a eTDYN-str-multi-c/023 en lugar de a un atributo DYN de valor único

## 12.6.3

Los problemas siguientes se han corregido en CA Identity Manager 12.6.3:

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21088049/02	La tarea Flujo de trabajo no responde en el estado "activo".
21227662/05	Una vez que un punto final de ACF2 se examina con el usuario que ha iniciado sesión, no se puede cambiar para usar el usuario de administrador del proxy.
21240169/01	Error StringIndexOutOfBoundsException al exportar el entorno de CA Identity Manager.
21298884/01	La asignación o eliminación de usuarios a/desde el servicio no se registra en el almacén de usuarios ni activa un error de PX en las cuentas.
21325322/03	Se produce un error en las suspensiones masivas al suspender todas las cuentas de LND o al agregar todas las cuentas al grupo de Denegar acceso (suspendido 0)
21329912/02	La sincronización de cuentas no funciona en CA Identity Manager 12.6.
21347968/01 21358148/01	El servidor de políticas se bloquea cuando un rol de acceso de CA Identity Manager se asigna a un usuario o se elimina de este.
21366658/01	La creación de usuarios mediante la tarea de cargador masivo devuelve una excepción de puntero al integrar CA SiteMinder.
21378657/01	El flujo de trabajo de escalación listo para utilizar se escala prematuramente si se define con la tarea Configurar una política global basada en flujo de trabajo para eventos.
21378803/01	El error La contraseña anterior no se puede volver a utilizar. aparece y producirá un error en la tarea.
21385464/01	Error NullPointerException cuando se configura la política de identidad configurada con la expresión MemberRule-Groups Where-Attribute.
21387236/01	La creación de un usuario a partir de una copia no copia el atributo de la organización.

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21389685/01	Vencimiento del tiempo de inicio de sesión cuando se integra con CA SiteMinder.
21393295/01	Ausencia del rol de aprovisionamiento de la lista de usuarios de CA Identity Manager de los roles de aprovisionamiento.
21395953/01	Envío de bucles de correo electrónico por la política exprés.
21417960/01 21417960/03	La modificación del rol de aprovisionamiento devuelve un puntero nulo.
21424762/02	Error del usuario prohibido.
21430655/01	Los eventos de flujo de trabajo de la política global se difieren al aprobador de escalación.
21430868/02	No se pueden eliminar las iniciales al renombrar las cuentas de LND.
21438148/03	La organización de LND de raíz no se examina y no se recupera ninguna cuenta.
21438256/01	El script de java de muestra no funciona con la tarea Autoregistro.
21438937/01	El carácter especial extraño acaba en la persistencia de la tarea Valor antiguo y en la auditoría.
21439600/01	Aparecerán ventanas en blanco para el cliente cuando inicien sesión mediante una contraseña de un usuario caducado.
21441213/01	La tarea de gestión importada del entorno de CA Identity Manager r12.5 devuelve el error de java.lang.ClassCastException.
21447986/01	Cuando una política exprés se activa y se registra al utilizar el idioma noruego, devuelve java.lang.IllegalArgumentException: llaves no coincidentes en el patrón.
21450831/01	Cuando se abre una plantilla nueva mediante Connector Xpress, no aparecerá el cuadro de diálogo de asignaciones de la operación.
21468616/01	Longitud del atributo de las iniciales
21470755/01	En la aplicación para móviles, la tarjeta del gestor de la tarjeta de contacto no funciona correctamente.
21470794/01	En la aplicación para móviles, todos los errores de restablecimiento de la contraseña se devuelven debido a los problemas complejos aunque se envíe la contraseña actual incorrecta.
21473825/01	En la aplicación para móviles de CA Identity Manager, se produce un error en el inicio de sesión después de restablecer una contraseña desde dentro de la aplicación móvil.
21475033/01	En la aplicación para móviles de CA Identity Manager, Restablecimiento de la contraseña olvidada se podrá utilizar solamente una vez.
21478278/01	No vuelve a aparecer ningún campo CAPTCHA en la pantalla de CA Identity Manager de nuevo cuando la fase de validación rechaza algunos otros campos.
21480621/01	La instalación de CA Identity Manager r12.6 SP2 en JBoss EAP 6 produce un error en la instalación del archivo iam_im_compile_jsp.* y de build.xml.

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21481343/01	No hay ninguna ranura activa disponible puesto que estas se bloquean indefinidamente.
21486937/01	Cuando el indicador Esperar se selecciona para una regla de acción en la política exprés para Ejecutar una función (no principal) como la categoría Código externo y el tipo Ejecutar código de JavaTipo. La política exprés generará el evento JavaActionWaitEvent y el estado quedará En curso.
21488801/01	La configuración de la política de contraseñas que requiere signos de puntuación resulta en una contraseña incorrecta.
21497995/01	Las operaciones masivas devuelven un error cuando se selecciona un (entre varios) elementos de la lista de trabajos de delegación.
21520525/01	<ETAHOME>\bin\ADSLDAPDiag.exe produce un error con el error Error 10054 reading data from server, al intentar realizar una conexión manual a un servidor Active Directory 2012.
21522674/01	Error en el restablecimiento de la conexión restablecía error en inicio del paso 5.
21535004/01	No se puede agregar el rol de SAP mediante TEWS.
21537907/01	ConfigXpress no funciona con la instalación de CA Identity Manager r12.6 SP2.
21539251/01	El error se produce al crear una copia o al modificar la tarea de administración Ver historial de acceso.
215544431/01	Error en la creación de la política de flujo de trabajo global.
21558358/01	El agente de Exchange sin agente está buscando CA CloudMinder/CAFT
21568224/01	ConfigXpress.air no funciona: devuelve el error en la instalación de CA Identity Manager r12.6 SP2.
21572374/01	En la aplicación para móviles de CA Identity Manager, la aprobación rápida no funcionará.
21585328/01	ConfigXpress.air produce un error al instalarse en CA Identity Manager r12.6 SP2.

## 12.6.2

Los problemas siguientes se han corregido en CA Identity Manager 12.6.2:

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21198613/01	La contraseña establecida por PX no se sincroniza en los usuarios globales y las cuentas.
21230281/01	No se pueden importar identificadores de atributos lógicos en la Consola de gestión.
21263275/01	Incidencias con la política de contraseñas de Arcot.
21269108/02	Incidencias con la instalación del agente para la sincronización de contraseñas de CA Identity Manager r12.6.

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21264877/01	El nombre distintivo del administrador se añade a la dirección URL externa.
21275958/01	Excepción de puntero nulo al adquirir el punto final de SAP.
21272983/01	Errores al leer el punto final de CA Access Control con bases de datos de varios modelos de políticas (PMDB) definidas.
21173122/01	Las definiciones de rol importadas no aparecen.
21270763/01	El error se produce cuando un directorio de aprovisionamiento se crea mediante el asistente.
21280342/01	DoSynchUserRoles no permite las casillas de verificación para Agregar cuentas que faltan ni Eliminar cuentas adicionales al servicio web de ejecución de tareas (TEWS) de CA Identity Manager para el lenguaje de descripción de servicios web (WSDL).
21285651/01	Compatibilidad de la tarea Sincronizar cuentas con plantilla de cuenta con TEWS.
21295778/01	El error al crea instancias del complemento de política exprés se produce cuando se intenta crear o modificar algunas políticas exprés.
21304316/01	Problema de rendimiento al agregar grupos a un usuario mediante la tarea de creación o modificación de usuarios.
21304316/02	Problema de rendimiento al agregar los grupos a un usuario, mediante el botón Agregar grupos en la tarea Modificar usuario.
21306987/01	El error NoClassDefFoundError se produce al ejecutar highavailability.bat.
21307126/01	RSA Secure ID 7: no puede adquirir un punto final debido a los problemas con el script para crear un grupo OSGi (iniciativa de puerta de enlace de servicios abiertos)
21315277/04	El servidor de conectores C++ se bloquea al buscar cuentas de usuario de Active Directory movidas o renombradas.
21319140/01	Los datos del archivo dir.xml de SQL importado se escriben en mayúscula.
21322022/01	Las conexiones de CA Identity Manager son más lentas después de un período de tiempo.
21325322/01	Cierre de la sesión debido a error de comunicación en LND al modificar cuentas.
21331632/01	El mensaje de advertencia al revocar el servicio no incluye el parámetro de nombre de usuario.
21335464/01	Error de script del gestor de aprovisionamiento al visualizar una operación que comprende varias páginas.
21351855/01	CA Identity Manager produce un error al crear un entorno cuando no se ha seleccionado ningún aprovisionamiento y solo se ha seleccionado el rol del gestor del sistema.
21361599/01	El error siguiente aparece cuando se utiliza la tarea Modificar usuario:
21383034/01	Error de la tarea crítico: Se ha producido un error al ejecutar SynchronizeAttributesWithAccountEvent: ERRORMESSAGE: For input string

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21393461/01	Excepción al actualizar el atributo Activar/desactivar usuario o cualquier otro atributo de usuario.

## 12.6.1

Las incidencias siguientes están corregidas en CA Identity Manager 12.6.1:

<b>Ticket de soporte</b>	<b>Problema notificado</b>
20576709/02	Es necesaria la compatibilidad con el uso compartido del servidor de informes de Business Objects tanto para CA Identity Manager como para SiteMinder.
20576725/02	Es necesaria la compatibilidad con el servidor de informes de Business Objects en una configuración de disponibilidad alta.
20583665/02	Es necesaria la compatibilidad con el servidor de informes de Business Objects XI 3.1 SP5 (CABI 3.3).
20774861/02	No se pueden incluir datos de Objeto Secundario en la política exprés.
20777137/02	Mejora en el flujo de trabajo basado en la política para obtener los objetos secundarios (objetos de usuario) que se necesitan para los objetos primarios.
20888199/01	Convención de denominación de nombre destacado para las plantillas de cuenta para TEWS no documentada.
21073146/01	"Sincronizar cuentas con plantilla de cuenta" no sincroniza.
21086870/01	El instalador de JCS independiente no solicita clave de FIPS, lo que provoca problemas relacionados con el cifrado.
21108813/01	CA Identity Manager 12.6 no proporciona las definiciones del rol esperadas.
21111634/01	No se crean registros de punto final de JCS.
21131768/01	Incidencia de atributo de flujo de trabajo de política global (las definiciones del evento no tienen el tipo de objeto secundario).
21135604/01	Se produce un error NullPointerException en la tarea Ver identificador de atributos lógicos.
21136454/01	La vulnerabilidad de seguridad de inyección de código SQL se ha corregido en esta versión.
21136456/01	Vulnerabilidad de seguridad
21136499/01	Seleccionar datos de cuadro no funciona con una pantalla de perfil adjunta a un servicio en CA Identity Manager 12.6.
21137701/01	Se recibe una excepción "PxEnvironmentException" se recibe cuando la política exprés llama al código externo de Java

<b>Ticket de soporte</b>	<b>Problema notificado</b>
21140501-1	Compatibilidad con implementaciones en la nube (gestión de clientes).
21146621/01	Validación del atributo global en directory.xml
21156269/01	Diferencias entre los esquemas de la base de datos generados por el instalador y los scripts de base de datos individuales en la carpeta de herramientas.
21156269/01	Se necesitan más scripts para la creación manual de bases de datos.
21162602/01	La correlación personalizada para TSS no funciona con Unix.
21170706/01	Los resultados de Ver tareas enviadas se ordenan de forma incorrecta cuando los la configuración regional se establece como danés-
21175201/01	La sincronización de cuentas iniciada por la notificación de entrada no se produce cuando los roles de aprovisionamiento se asignan mediante políticas de la política exprés.
21181592/01	No se puede cargar CA Identity Manager r12.6 con un error de ruta de clase no válida.
21183366/01	Se utiliza un nombre del usuario incorrecto con los orígenes de datos.
21187385/01	Bloqueos de CA Identity Manager intermitentes.
21188814/01	El servidor de políticas de SiteMinder r12 SP3 CR11 se bloquea al acceder a la política de CA Identity Manager.
21190699/01	No se puede obtener información del objeto secundario de la política exprés en ninguna política basada en una tarea o un evento. Además, se devuelve información del valor del atributo original incluso cuando la política exprés se desencadena después de la finalización de una tarea.
21190873/01	Incidencia de cumplimiento 508: la sugerencia de las casillas de verificación no tiene sentido.
21193837/01	Creación y supresión de objetos gestionados
21194712-1	La política exprés con iterador se interrumpe cuando Flujo de trabajo rechaza una asignación de rol de acceso activado.
21200396/01	Incidencia de cumplimiento 508: problemas con el vínculo Saltar directamente al contenido principal.
21200412/01	Incidencia de cumplimiento 508: el software de asistencia para usuarios discapacitados no lee correctamente los mensajes de error y advertencia.
21213029-1	Las variables de servicios de contraseña almacenadas en la memoria caché de JSession no se borran (al cerrar sesión) y las solicitudes subsiguientes se redirigen a la página pws.fcc.



# Capítulo 5: Documentación

---

A continuación se especifican los nombres de archivo de las guías de CA Identity Manager:

Nombre de la guía	Nombre del archivo
Notas de la versión	im_release_enu.pdf
Guía de implementación	im_impl_enu.pdf
Guía de instalación para WebLogic	im_install_weblogic_enu.pdf
Guía de instalación para WebSphere	im_install_websphere_enu.pdf
Guía de instalación para JBoss	im_install_jboss_enu.pdf
Guía de actualizaciones	im_upgrade_enu.pdf
Guía de configuración	im_config_enu.pdf
Guía de administración	im_admin_enu.pdf
Guía de diseño de la Consola de usuario	im_uc_design_enu.pdf
Guía de programación para Java	im_dev_enu.pdf
Guía de referencia de aprovisionamiento	im_provisioning_reference_enu.pdf
Guía de conectores	im_connectors_enu.pdf
Guía de Connector Xpress	im_connector_xpress_enu.pdf
Guía de implementación del servidor de conector de Java	im_jcs_impl_enu.pdf
Guía de programación para el servidor de conector de Java	im_jcsProg_Enu.pdf
Glosario	im_glossary.pdf
Biblioteca	im_bookshelf_enu.zip

Esta sección contiene los siguientes temas:

[Biblioteca](#) (en la página 62)

[Problemas conocidos](#) (en la página 62)

[Notas de la versión de integración de CA Identity Manager y CA Identity Governance.](#)  
(en la página 63)

## Biblioteca

La biblioteca permite acceder a toda la documentación de CA Identity Manager desde una única interfaz. Incluye la siguiente información:

- Lista ampliable de contenidos para todas las guías en formato HTML.
- Búsqueda de texto completo en todas las guías con los resultados de la búsqueda clasificados y los términos de la búsqueda resaltados en el contenido.
- Rutas de navegación que enlazan con temas de nivel más alto.
- Un único índice HTML para los temas de todas las guías.
- Vínculos a las versiones en PDF de las guías para imprimirlas.

### Para usar la biblioteca

1. Descargue la biblioteca desde el [sitio de soporte de CA](#).
2. Extraiga el contenido del archivo ZIP de la biblioteca.

**Nota:** Para obtener el mejor rendimiento, al instalar la biblioteca en un sistema remoto, haga que se pueda acceder a ella desde un servidor Web.

3. Visualice la biblioteca de esta forma:

- Si la biblioteca se encuentra en el sistema local y utiliza Internet Explorer, abra el archivo Bookshelf.hta.
- Si la biblioteca se encuentra en un sistema remoto o utiliza Mozilla Firefox, abra el archivo Bookshelf.html.

**Nota:** Para obtener el mejor rendimiento, al instalar la biblioteca en un sistema remoto haga que se pueda acceder a ella desde un servidor Web.

La biblioteca requiere Internet Explorer 7 o 8, o Mozilla Firefox 2 o 3. Para los enlaces a las guías en PDF, se necesita Adobe Reader 7 o superior. Adobe Reader se puede descargar en [www.adobe.com](http://www.adobe.com).

## Problemas conocidos

Todos los problemas conocidos relacionados con CA Identity Manager se encuentran en el sitio de [Soporte de CA](#).

## Notas de la versión de integración de CA Identity Manager y CA Identity Governance.

Todas las notas de la versión relacionadas con la integración entre CA Identity Manager y CA Identity Governance se encuentran en *CA Identity Governance Release Notes*. Se puede acceder a la biblioteca de CA Identity Governance desde [Soporte de CA](#).



# Apéndice A: Funciones de accesibilidad

---

CA Technologies se compromete a garantizar que todos los clientes, independientemente de su capacidad, puedan emplear correctamente los productos y la documentación compatible para llevar a cabo las tareas de negocio vitales. Esta sección explica las funciones de accesibilidad que forman parte de CA Identity Manager.

## Cumplimiento con 508

CA Identity Manager cumple con la Sección 508 de la Ley de rehabilitación de EE. UU. y las Directrices de accesibilidad de contenido web (WCAG2.0) de nivel AA. El tema [Product Enhancements](#) (en la página 65) proporciona más detalles. También se puede solicitar al gestor de cuentas una copia de CA Technology's Voluntary Product Accessibility Template (VPAT).

## Mejoras del producto

*CA Identity Manager* ofrece mejoras de accesibilidad en las áreas siguientes:

- Pantalla
- Sonido
- Teclado
- Ratón

**Nota:** La siguiente información hace referencia a aplicaciones basadas en Windows y Macintosh. Las aplicaciones Java se ejecutan en muchos sistemas operativos de host, algunos de los cuales ya tienen tecnologías de asistencia disponibles. Para que estas tecnologías de asistencia existentes proporcionen acceso a programas escritos en JPL, necesitan un puente entre ellos en sus entornos nativos y Java Accessibility, que está disponible en la máquina virtual de Java (Java VM). Este puente tiene un extremo en Java VM y el otro en la plataforma nativa, así será algo diferente según la plataforma para la que sirva de puente. Sun está desarrollando actualmente los extremos de JPL y Win32 de este puente.

## **Pantalla**

Para aumentar la visibilidad en la pantalla de su equipo, se pueden ajustar las siguientes opciones:

### **Estilo de fuente, color y tamaño de los elementos**

Permite elegir el color de la fuente, el tamaño y otras combinaciones visuales.

### **Resolución de la pantalla**

Permite cambiar el número de píxeles para ampliar los objetos en la pantalla.

### **Ancho del cursor y frecuencia de intermitencia**

Hace que sea más fácil encontrar el cursor o minimizar su intermitencia.

### **Tamaño de los iconos**

Permite ampliar los iconos para mejorar la visibilidad o disminuirlos obtener más para espacio de pantalla.

### **Esquemas de alto contraste**

Permite seleccionar combinaciones de color que son más fáciles de ver.

## **Sonido**

El sonido se utiliza como alternativa a la visualización o para que los sonidos del equipo sean más fáciles de oír o distinguir ajustando las siguientes opciones:

### **Volumen**

Permite aumentar o disminuir el sonido del equipo.

### **Texto a voz**

Permite oír opciones de comandos y texto en voz alta.

### **Advertencias**

Permite mostrar advertencias visuales.

### **Avisos**

Proporciona indicaciones visuales o auditivas cuando se activan o desactivan las funciones de accesibilidad.

### **Esquemas**

Permite asociar sonidos del equipo con eventos del sistema específicos.

### **Leyendas**

Permite mostrar leyendas para voz y sonidos.

**Nota:** Si se está usando un lector de pantalla, se recomienda la instalación de la última versión de la herramienta de lector de pantalla para obtener una mejor interpretación.

## Teclado

Se pueden hacer los siguientes ajustes de teclado:

### Frecuencia de repetición

Permite configurar la velocidad de repetición de un carácter cuando se presiona una tecla.

### Tonos

Permite oír tonos al pulsar para ciertas teclas.

### Teclas permanentes

Permite elegir distribuciones del teclado alternativas a las personas que escriban con una mano o un dedo.

### Vínculo de salto

Permite utilizar el vínculo Saltar directamente al contenido principal para una navegación rápida al contenido principal.

## Ratón

Se pueden utilizar las opciones siguientes para hacer más rápido y fácil el uso del ratón:

### Velocidad de clic

Permite elegir la velocidad de clic del botón del ratón para realizar una selección.

### Bloqueo de clic

Permite destacar o arrastrar sin mantener pulsado el botón del ratón.

### Acción inversa

Permite invertir las funciones que controlan los botones principal y secundario del ratón.

### Frecuencia de intermitencia

Permite elegir la velocidad de parpadeo del cursor o si parpadea.

### Opciones del puntero

Permite hacer lo siguiente:

- Ocultar el puntero mientras se escribe
- Mostrar la ubicación del puntero
- Establecer la velocidad con la que el puntero se mueve en la pantalla
- Elegir el tamaño y color del puntero para obtener mayor visibilidad
- Mover el puntero a una ubicación predeterminada en un cuadro de diálogo

### Excepciones de Mozilla Firefox

Se recomienda que los usuarios de teclado y de JAWS utilicen Internet Explorer 8 por las siguientes razones:

- En Firefox, los cuadros de diálogo no reciben foco de entrada/salida.
- En Firefox, el lector de pantalla no siempre lee primero el vínculo Salta directamente al contenido principal.

### Accesos directos del teclado

En la tabla siguiente se muestran los accesos directos que admite CA Identity Manager:

Teclado	Descripción
Ctrl + X	Cortar
Ctrl + C	Copiar
Ctrl + K	Buscar siguiente
Ctrl + F	Buscar y reemplazar
Ctrl + V	Pegar
Ctrl + S	Guardar
Ctrl + Mayús + S	Guardar todo
Ctrl + D	Suprimir línea
Ctrl + Tecla de flecha derecha	Palabra siguiente
Ctrl + Tecla de flecha abajo	Desplazarse hacia abajo en la línea
Fin	Final de línea