CA Identity Manager™

Guía de administración

12.6.4

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 3: Tareas de administración 43

Capítulo 4: Usuarios 83

Capítulo 11: Sincronización 251

Capítulo 12: Flujo de trabajo (workflow) 267

Capítulo 1: Planificación de los roles

Para planificar los roles, decida qué tipo de roles necesita su negocio u organización, además de cómo delegará la gestión de usuarios y el acceso a las aplicaciones. Las características de cada rol se determinarán según estas decisiones.

Para utilizar los roles de forma eficaz, se deben tener en cuenta estos tipos de preguntas sobre las responsabilidades del administrador y las necesidades del usuario:

- ¿En qué departamentos y organizaciones hay usuarios que se deben gestionar?
- ¿Qué cuentas adicionales en puntos finales gestionados necesitarán los usuarios?
- ¿Qué usuarios deben ser administradores de otros usuarios?
- ¿Quién debe gestionar a los administradores?
- ¿Qué tareas de acceso y administración se necesitan en cada rol?
- ¿Quién debe crear los roles y las tareas?
- ¿Cómo se pueden utilizar los roles para delegar trabajos?

  La última pregunta se refiere a compartir el trabajo de gestión de usuarios y concesión de acceso a aplicaciones. Para obtener más información sobre el modelo de delegación, consulte la sección Administración delegada.

Según las respuestas a estas preguntas, se pueden decidir cuántos y qué tipo de roles se necesitan.

Esta sección contiene los siguientes temas:

Decisiones de roles

En la siguiente sección se incluye información de ayuda para tomar decisiones de roles fundamentadas.

Finalidad de los roles

Para utilizar los roles de forma eficaz, se deben tener en cuenta estos tipos de preguntas sobre las responsabilidades del administrador y las necesidades del usuario:

- ¿En qué departamentos y organizaciones hay usuarios que se deben gestionar?
- ¿Qué cuentas adicionales en puntos finales gestionados necesitarán los usuarios?
- ¿Qué usuarios deben ser administradores de otros usuarios?
- ¿Quién debe gestionar a los administradores?
- ¿Qué tareas de acceso y administración se necesitan en cada rol?
- ¿Quién debe crear los roles y las tareas?
- ¿Cómo se pueden utilizar los roles para delegar trabajos?

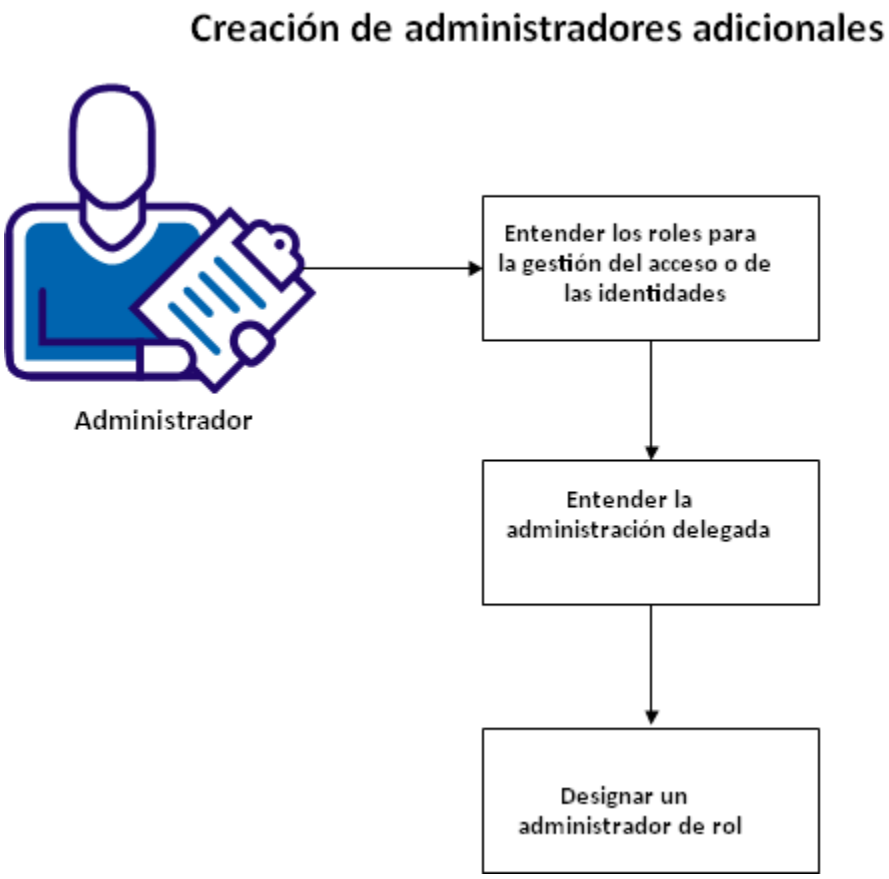
  La última pregunta se refiere a compartir el trabajo de gestión de usuarios y concesión de acceso a aplicaciones. Para obtener más información sobre el modelo de delegación, consulte la sección Administración delegada.

Según las respuestas a estas preguntas, se pueden decidir cuántos y qué tipo de roles se necesitan.

Creación de administradores adicionales

Se puede ser únicamente responsable de concesión de todos los roles a usuarios del sistema. Se puede compartir también el trabajo de concesión de roles de usuario designando administradores adicionales. A este método se le denomina *"administración delegada"*.

En el siguiente diagrama se muestra la información sobre los pasos que deben realizarse a la hora de crear y configurar usuarios.



En los siguientes temas se explica cómo crear administradores adicionales:

- Roles para Identity o Access Management (en la página 20)
- Administración delegada (en la página 20)
- Designación de administradores del rol (en la página 21)

Roles para Identity o Access Management

Para activar la gestión de identidades de usuarios y el acceso de estos a otras cuentas, CA CloudMinder proporciona dos tipos de roles. Con un rol de administrador, los usuarios pueden gestionar usuarios; por ejemplo, modificar la contraseña de un usuario o la pertenencia a grupos. Los roles de administrador pueden incluir también cualquier tarea que aparezca en la Consola de usuario. Con un rol de aprovisionamiento, los usuarios tienen acceso a otras aplicaciones de negocio; por ejemplo, un sistema de correo electrónico.

En la siguiente tabla se proporcionan más detalles sobre los roles:

Tipo de rol	Finalidad
Rol de administrador	Contiene tareas de administración que, al conceder ese rol, los usuarios pueden realizar en CA CloudMinder, como las tareas de gestión de usuarios.
Rol de aprovisionamiento	Contiene plantillas de cuenta que definen cuentas que existen en puntos finales gestionados, como un sistema de correo electrónico. Las plantillas de cuenta también definen cómo los atributos de usuario se asignan a dichas cuentas.
Rol de acceso	Los roles de acceso proporcionan una forma adicional de proporcionar autorizaciones en CA Identity Manager u otra aplicación. Por ejemplo, se pueden utilizar los roles de acceso para realizar las siguientes acciones: ■ Proporcionar acceso indirecto a un atributo de usuario ■ Crear expresiones complejas ■ Establecer un atributo de perfil que otra aplicación puede utilizar para determinar atribuciones

Administración delegada

La administración delegada es el uso de roles para compartir el trabajo de gestión de usuarios y concesión de acceso a aplicaciones.

Para cada rol del sistema, los usuarios pueden proporcionar servicio a una o varias de las siguientes funciones:

Función	Definición
Propietario del rol	Modifica el rol.
Administrador del rol	Asigna el rol a usuarios y otros administradores del rol.

Función	Definición
Miembro del rol	Utiliza el rol para realizar tareas de administración o acceso, o bien utilizar una cuenta de punto final.

Al dividir estas funciones entre usuarios, se puede compartir el trabajo de gestión de roles. Por ejemplo, se puede hacer que los administradores de niveles inferiores gestionen pertenencias a roles y que los administradores de niveles superiores modifiquen roles.

Se puede implementar la administración delegada de las siguientes formas:

- Designe directamente a un usuario como administrador de un rol determinado.
- Configure *reglas de administración* para un rol. Las reglas de administración definen qué usuarios pueden ser administradores de un rol. El sistema crea automáticamente administradores adicionales cuando los usuarios cumplen con los criterios que se especifican en las reglas.

  Nota: Solamente los administradores con privilegios para modificar roles pueden configurar reglas de administración para dichos roles. Normalmente, los administradores del sistema realizan esta actividad. Para configurar reglas de administración que deleguen automáticamente la administración de roles, consulte la sección titulada "Roles de administrador" en la sección de información de referencia de la ayuda en línea.

Designación de administradores del rol

Se puede designar un usuario como administrador de un rol. El administrador puede asignar a continuación el rol a otros usuarios.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario con tareas de gestión de usuarios con roles.
2. Seleccione Tareas, Roles y tareas.
3. Seleccione una de las tareas siguientes:
   - Roles de administrador, Modificar miembros/administradores del rol de administrador
   - Roles de aprovisionamiento, Modificar miembros/administradores del rol de aprovisionamiento
   - Roles de acceso, Modificar miembros/administradores del rol de acceso

Aparece una pantalla de búsqueda.

4. Seleccione el rol que intenta asignar al usuario.
5. Haga clic en la ficha Administradores.

   Se muestra una lista de administradores de rol actuales.

6. Haga clic en Agregar un usuario.

   Aparece una pantalla de búsqueda.

7. Busque el usuario que desea agregar como administrador y haga clic en Seleccionar.

   Se muestra una lista actualizada de administradores del rol.

8. Haga clic en Enviar.

   El usuario se convierte en administrador del rol. Con este paso se completa el proceso de delegar la administración de un rol de aprovisionamiento. El administrador puede asignar ahora el rol a otros usuarios, por lo que se concede acceso a las cuentas de puntos finales asociadas.

Pasos de delegación

Una vez que se decida cómo usar los roles según la sección Finalidad de los roles, la administración delegada se llevará cabo de la siguiente forma:

1. Los administradores crearán el rol con reglas para que un usuario sea propietario, administrador o miembro del rol.
2. Cuando se requiera realizar cambios en el rol, los propietarios de este lo modificarán.
3. Los administradores del rol pueden hacer lo siguiente:
   - Asignar más administradores del rol (opcional).
   - Asignar más miembros del rol (opcional).

   Algunos usuarios son ya administradores o miembros del rol en cumplimiento con las reglas definidas en dicho rol.
4. Los miembros del rol utilizan el rol para llevar a cabo lo siguiente:
   - Gestionar usuarios y otros objetos en el entorno de Identity Manager (miembros del rol de administrador).
   - Ejecutar funciones en aplicaciones de negocio (miembros del rol de acceso).
   - Utilizar las cuentas que se definen en las políticas del rol (miembros del rol de aprovisionamiento).

Ejemplo de delegación

Se puede crear un rol con reglas para que un usuario pueda ser miembro o administrador. A continuación, se puede asignar el rol para que otros usuarios (aquellos que ya no cumplen las reglas) se puedan convertir en miembros o administradores del rol.

Tenga en cuenta el siguiente ejemplo de administradores que gestionan los derechos de usuarios finales a las aplicaciones de negocio:

- Jeff es propietario del rol de contable; por tanto, cuando se requiere realizar cambios en el rol, Jeff lo modifica.
- David y Lisa son administradores de ese rol. Asignan usuarios regionales como miembros del rol.
- Otros usuarios son miembros del rol sin que ningún administrador les haya asignado dicho rol. En cambio, cumplen la regla para ser miembros del rol.

  Los miembros del rol utilizan el rol de contable para generar órdenes de compra y realizar otras tareas en aplicaciones financieras.

La sección Características de los roles ofrece detalles sobre reglas y otras características de los roles.

Características del rol

Cuando se crea un rol, se definen las características mostradas en la tabla siguiente:

Características	Definición
Perfil del rol	Características generales del rol.
Tareas	Tareas para un rol de administrador.
Plantillas de cuenta	Plantillas que definen cuentas en puntos finales gestionados para un rol de aprovisionamiento.
Reglas de miembros, Políticas de miembros	Una regla de miembros define las condiciones de que un usuario sea un miembro del rol de administrador o de acceso. Una política de miembros combina una regla de miembros con las reglas del ámbito. **Nota:** Los roles de aprovisionamiento no tienen reglas ni políticas de miembros. Para hacerle miembro a un usuario, se utiliza Modificar miembros/administradores del rol de aprovisionamiento.

Características	Definición
Reglas de administrador, Políticas de administración	■ Una regla de administrador define las condiciones para que un usuario sea un administrador de roles. ■ Una política de administración combina una regla de administrador con una regla de ámbito y privilegios de administrador para asignar el rol.
Reglas de propietarios	Condiciones para que un usuario sea un propietario del rol.
Reglas del ámbito	Límites en los cuales el rol puede gestionar objetos.
Agregar acciones, Eliminar acciones	Cambia a un perfil de usuario cuando se agrega o elimina un usuario como administrador o miembro de rol.

Perfil del rol

El perfil del rol indica el nombre y la descripción del rol, así como si este está activado. Si está activado, el rol estará disponible para usarse en cuanto se cree.

Tareas para los roles

En los roles de administrador se pueden elegir una o más tareas de administración (incluidas las tareas externas) de una o varias categorías.

Plantillas de cuenta

En cada rol de aprovisionamiento se incluyen plantillas de cuenta. Estas definen las cuentas que existen en los puntos finales gestionados. Por ejemplo, un punto final correspondiente a una cuenta de Exchange podría definir el tamaño del buzón de correo. Las plantillas de cuenta también definen cómo los atributos de usuario se asignan a las cuentas.

Se pueden elegir uno o varios puntos finales para cada tipo de punto final. El usuario al que se le asigna el rol recibe una cuenta en el punto final.

Reglas de miembros, administradores y propietarios

Cada rol incluye reglas sobre quiénes pueden ser miembros, administradores o propietarios de dicho rol. Por lo tanto, un usuario puede ser un miembro de un rol, de varios o de ninguno.

Las reglas de miembros, administradores y propietarios utilizan las condiciones de la siguiente tabla:

Condición de regla	Ejemplo	Sintaxis de regla
El usuario debe coincidir con un valor de atributo.	Usuarios en los que el título empieza por senior	donde <filtro-usuario>
El usuario debe coincidir con varios valores del atributo.	Usuarios donde título=gestor y localidad=este	donde <filtro-usuario>
El usuario debe pertenecer a las organizaciones mencionadas.	Usuarios en ventas de la organización e inferior	en <regla-organización>
El usuario debe pertenecer a organizaciones que cumplan la condición especificada por los atributos de la organización.	Usuarios en organizaciones donde Tipo de empresa=oro o platino	en organizaciones donde <filtro-organización>
El usuario debe pertenecer a organizaciones específicas y cumplir con atributos de usuario específicos.	Usuarios donde título=gestor y localidad=este y que están en el departamento de ventas o marketing de la organización	donde <filtro-usuario> y que están en <regla-organización>
El usuario debe pertenecer a un grupo específico.	Usuarios que son miembros del grupo 401K	que son miembros del grupo <grupo>
El usuario debe ser miembro de un rol.	Usuarios que son miembros del rol Help Desk	que son miembros de <regla-rol>
El usuario debe ser un administrador de un rol.	Usuarios que son administradores del rol Gestor de ventas	que son administradores de <regla-rol>
El usuario debe ser propietario de un rol.	Usuarios que son propietarios del rol Gestor de usuarios	que son propietarios de <regla-rol>
El usuario debe pertenecer a un grupo que cumpla con una condición especificada por los atributos del grupo.	Usuarios que son miembros de grupos donde propietario=CIO	que son miembros del grupo <filtro-grupo>

Condición de regla	Ejemplo	Sintaxis de regla
El usuario debe cumplir con una condición basada en una consulta LDAP.	(Utilice un directorio de LDAP en aquellos casos donde una consulta creada en la Consola de usuario de Identity Manager no es suficiente)	usuario devuelto por la consulta ldap_query

Algunas reglas pueden implicar la comparación de un valor con un atributo con varios valores. Para que se aplique la regla, ésta debe cumplir al menos uno de los valores de un atributo con varios valores. Por ejemplo, si la regla es Atributo A IGUAL A 1, y el valor del atributo A es 1, 2, 3 para el usuario X, entonces el usuario X cumple con los criterios.

Puede que el usuario que crea el rol no pueda modificarlo. Para poder modificar el rol, el usuario debe reunir las condiciones de las reglas de propietarios.

Nota: En implementaciones grandes, la evaluación de las reglas de miembros, administradores y propietarios puede tardar bastante tiempo. Para reducir el tiempo de evaluación de las reglas que incluyan atributos de usuario, se puede activar la opción de evaluación en memoria. Para obtener más información, consulte la *Guía de configuración*.

Reglas del ámbito

Se combinan las reglas de miembro y de administración con las reglas de ámbito. *Las reglas de ámbito* limitan los objetos en los cuales se puede utilizar el rol.

- Para un miembro del rol, las reglas de ámbito controlan qué objetos se pueden gestionar con el rol.
- Para un administrador de rol, las reglas de ámbito controlan qué usuarios se pueden convertir en miembros y administradores del rol.

El ámbito se aplica al objeto primario de la tarea. Por ejemplo, el usuario es el objeto primario de la tarea Crear usuario. Sin embargo, el ámbito no se aplica a los grupos para el usuario, porque el grupo es un objeto secundario.

Para la mayor parte de tipos de objeto, se pueden especificar los tipos de reglas de ámbito en la tabla siguiente.

Condición de regla	Ejemplo	Sintaxis de regla
Todos	Los miembros del rol pueden gestionar todos los objetos	Todos
El objeto debe coincidir con uno o varios valores del atributo.	Los usuarios cuyo **cargo** empieza por **sénior**	donde <filtro>

Cuando se selecciona la opción de filtro, CA Identity Manager muestra dos tipos de filtro:

<atributo> <comparador><valor>

Un atributo en el perfil del objeto debe coincidir con un valor específico.

<atributo-usuario> del administrador de <comparador> de <atributo>

Un atributo en el perfil del objeto debe coincidir con un atributo en el perfil del administrador. Por ejemplo: los usuarios donde el gestor = ID de usuario del administrador.

Las opciones adicionales que se describen en las tablas siguientes, están disponibles para los objetos de usuario, grupo y organización.

Nota: Las reglas de ámbito de usuario siguientes son ejemplos. Se pueden crear otras reglas para gestionar las diferentes relaciones entre el administrador y los usuarios que puede gestionar el administrador.

Condición de regla	Ejemplo	Sintaxis de regla
El usuario debe coincidir con un valor de atributo.	Los usuarios donde el miembro de ventas del grupo o el teléfono móvil no es igual a nulo	donde <filtro-usuario>
El usuario debe coincidir con varios valores del atributo.	Los usuarios donde cargo=gestor y localidad=EE.UU.	donde <filtro-usuario>
El usuario debe pertenecer a las organizaciones mencionadas.	Usuarios en la organización Australia o Nueva Zelanda **Nota:** La regla de ámbito de organización se aplica a las suborganizaciones de la organización que cumplen la regla. Por ejemplo, si la regla de la organización está "en Organización1", la regla de ámbito se aplica a Organización1.1 y a Organización1.2, pero no se aplica a Organización1.	en <regla-organización>
El usuario debe pertenecer a organizaciones que cumplan la condición especificada por los atributos de la organización.	Usuarios en organizaciones donde Tipo de empresa=oro o platino	en organizaciones donde <filtro-organización>
El usuario debe pertenecer a organizaciones específicas y cumplir con atributos de usuario específicos.	Los usuarios donde cargo=gestor y localidad=este y que están en el Departamento de Ventas o Marketing de la organización	donde <filtro-usuario> y que están en <regla-organización>

Condición de regla	Ejemplo	Sintaxis de regla
El atributo en el perfil del usuario debe coincidir con un atributo en el perfil del administrador.	Los usuarios donde gestor = ID de usuario del administrador	donde <atributo-usuario> del administrador de <comparador> de <atributo-usuario> **Nota:** No utilice el comparador Distinto de con un atributo de varios valores.
El usuario se encuentra en la misma organización que el administrador.	Los usuarios en la organización donde Jeff (el administrador) es un miembro	organización del administrador
El usuario se encuentra en una organización que está en el atributo del administrador.	Usuarios en ventas o marketing	organización que es un valor en <atributo-admin> del administrador

Nota: Las reglas siguientes de ámbito del grupo son solamente ejemplos. Se pueden crear otras reglas para gestionar las diferentes relaciones entre el administrador y los grupos que puede gestionar el administrador.

Condición de regla	Ejemplo	Sintaxis de regla
El grupo debe coincidir con un valor de atributo.	El nombre del grupo donde el nombre del grupo = 401K	donde <filtro-grupo>
Los grupos deben pertenecer a las organizaciones mencionadas.	Grupos en la contabilidad de organización e inferiores	en <regla-organización>
El grupo debe coincidir con un valor de atributo y pertenecer a organizaciones denominadas.	Grupos donde financian Tipo de negocio = finanzas y los que están en ventas de la organización e inferiores	en <filtro-grupo> y los que están en <regla-organización>
El grupo se deberá encontrar en un atributo del administrador.	Grupos en Descripción = Ingeniería	donde <atributo-grupo> del administrador de <comparador> de <atributo-usuario> **Nota:** No utilice el comparador Distinto de con un atributo de varios valores.

Nota: Las reglas siguientes de ámbito de la organización son solamente ejemplos. Se pueden crear otras reglas para gestionar las diferentes relaciones entre el administrador y las organizaciones que puede gestionar el administrador.

Condición de regla	Ejemplo	Sintaxis de regla
La organización debe coincidir con un valor de atributo.	organizaciones donde Nombre de organización=finanzas	en <filtro-organización>
La organización debe pertenecer a las organizaciones mencionadas.	organizaciones en finanzas e inferiores	en <regla-organización>
La organización debe coincidir con un valor de atributo y debe pertenecer a una organización denominada.	organizaciones en Nombre de organización=finanzas y están en finanzas e inferiores	donde <filtro-organización> y se encuentran en <filtro-organización>

Más información:

Directrices comunes sobre las reglas (en la página 29)

Directrices comunes sobre las reglas

Con independencia del tipo de regla que se cree, se debe comprender cómo Identity Manager procesa estas reglas.

Evaluación de los operadores

Al crear reglas para un rol, puede incluir los operadores >=, <=, < y >. Sin embargo, la base de datos relacional o el directorio LDAP evalúan estos operadores como cadenas. La mayoría de los almacenes de usuarios comparan las cadenas en orden ascendente. Por lo tanto, al comparar 500 con 1100, el almacén de usuarios puede determinar que 500 es mayor porque 5 es mayor que 1.

Se puede cambiar la forma en que se comparan las cadenas en el almacén de usuarios. Consulte la documentación del software de la base de datos relacional o el servicio del directorio LDAP.

Reglas que no distinguen mayúsculas de minúsculas

Cuando se crean roles de acceso o administrador, las reglas creadas se pueden evaluar de modo que, en función del almacén de usuarios, se distingan mayúsculas de minúsculas; o bien que no se efectúe esta distinción.

Sin embargo, al final de una operación de creación o modificación, las reglas se evalúan internamente de modo que se distingan mayúsculas de minúsculas antes de realizar cambios en el almacén de usuarios. Por ejemplo, si una regla tiene una condición en la que title=gestor, la regla coincidirá con el objeto del almacén de usuarios, con independencia de que el valor del cargo sea "gestor" o "Gestor".

Acciones Agregar y Eliminar

Se debe especificar una acción Agregar y Eliminar para que Identity Manager gestione correctamente la pertenencia a una función cuando un administrador concede o revoca la función.

- La acción Agregar debe hacer que el usuario cumpla los criterios de una de las reglas de miembros de la función. Por ejemplo, si en la regla de miembros correspondiente al rol de gestor de usuarios se indica que los miembros del rol tengan "User Manager" como valor del atributo de roles de administrador, la acción Agregar debe agregar "User Manage" al atributo de roles de administrador.
- La acción Eliminar debe modificar el perfil de un usuario para que ya no coincida con la regla de miembros al revocar dicha regla.

Cada rol puede disponer de dos *acciones Agregar* y dos *acciones Eliminar*.

Si los administradores pueden agregar y eliminar miembros del rol, defina acciones Agregar y Eliminar. Si no pueden, significa que los usuarios tienen asignados dicho rol en cumplimiento con la regla de miembros; por ejemplo, si pertenecen al grupo de administradores de roles. Por ejemplo:

- Un administrador puede asignar el rol A, por lo que se definirán acciones Agregar o Eliminar.
- El rol B contiene una regla en la que todos los miembros del grupo de finanzas tengan ese rol. No se puede asignar este rol, por lo que no tendrá acciones Agregar o Eliminar.

Al definir acciones Agregar y Eliminar, considere utilizar el atributo de rol de administrador, ya que Identity Manager puede utilizarlo con el fin de almacenar una lista de roles del usuario. Por ejemplo, se puede configurar una acción Agregar que agregue Empleado al atributo de rol de administrador de un usuario cuando dicho usuario se agregue como miembro del rol de empleado. Si un administrador asigna el rol de empleado a un gestor que ya tiene los roles de autoadministrador y gestor de usuarios, el atributo de rol de administrador del gestor contendrá los siguientes valores: Self Administrator, User Manager, Employee.

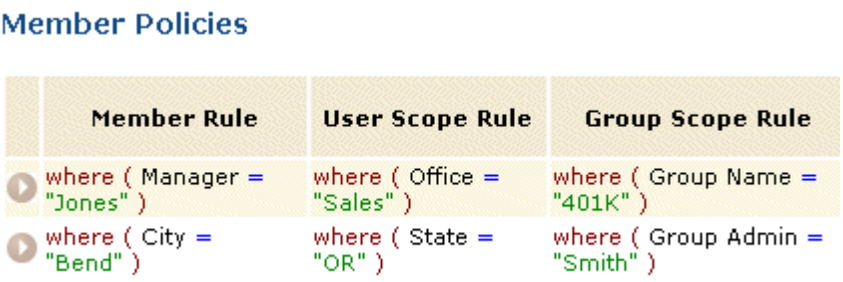
Para utilizar el atributo de rol de administrador, el atributo conocido %ADMIN_ROLE_CONSTRAINT% se deberá asignar a un atributo con varios valores en los perfiles de usuario. Para obtener más información, consulte la *Guía de configuración de CA Identity Manager*.

Importante: Al definir una acción Agregar, evite configurar una regla que haga referencia al rol que se esté definiendo. Por ejemplo, no defina la acción Agregar para incluir miembros en el rol A si ya es miembro del rol A. Esto producirá un error recursivo que hará que el servidor de políticas se reinicie.

Políticas de miembros

Una *política de miembros* indica que, si un usuario cumple la regla de miembros, dicho usuario tendrá definido el ámbito en esa política. En la siguiente ilustración se muestra un rol que tiene dos políticas de miembros.

- La primera política indica que si un miembro del rol tiene como gestor a Jones, ese miembro puede utilizar el rol para usuarios de la oficina de ventas y gestionarlos como miembros del grupo 401k.
- La segunda política indica que, si un miembro del rol está en la ciudad Bend, ese miembro del rol puede utilizar el rol para usuarios del estado de Oregón y gestionarlos como miembros de los grupos que tienen como administrador del grupo a Smith.

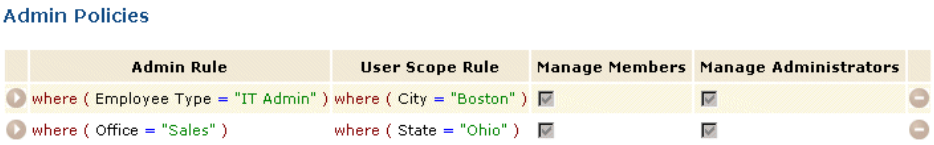


Políticas de administración

Una *política de administración* indica que, si un usuario cumple la regla de administración, dicho usuario tendrá definidos el ámbito del usuario y los privilegios de administrador en esa política. El ámbito del usuario define dónde se utiliza el rol. Los privilegios de administrador determinan si el administrador de rol puede gestionar miembros o administradores del rol.

En la siguiente ilustración se muestra un rol que tiene dos políticas de administración, que se definen de la siguiente forma:

- En la primera política, los administradores de TI pueden agregar y eliminar administradores y miembros del rol para usuarios de la ciudad de Boston.
- En la segunda política, los administradores del Departamento de Ventas pueden agregar y eliminar miembros del estado de Ohio.



Lista de comprobación de planificación de los roles

Antes de crear un rol, utilice esta lista de comprobación de características de los roles.

Característica de los roles	Detalles
Perfil del rol	Defina un nombre y una descripción para el rol. Establezca el estado como Activado.
Tareas	Incluya tareas de acceso o administración.
Plantillas de cuenta	Incluya plantillas de cuenta que definan cuentas que existan en los puntos finales (solamente roles de aprovisionamiento).
Políticas de miembros	En cada política de miembros, defina lo siguiente: ■ Reglas de miembros: quién puede utilizar el rol. ■ Reglas de ámbito: qué objetos puede gestionar un miembro del rol. ■ Acción Agregar: lo que le ocurre al perfil de un usuario que se convierte en miembro. ■ Acción Eliminar: lo que le ocurre al perfil de un usuario que se elimina como miembro.

Característica de los roles	Detalles
Políticas de administración	En cada política de administración, defina lo siguiente: ■ Reglas de administrador: quién puede gestionar los usuarios como miembros o administradores. ■ Reglas de ámbito: qué usuarios puede gestionar el administrador como miembros o administradores. ■ Acción Agregar: lo que le ocurre al perfil de un usuario que se convierte en administrador. ■ Acción Eliminar: lo que le ocurre al perfil de un usuario que se elimina como administrador.
Reglas de propietarios	Defina quién puede modificar el rol.

Capítulo 2: Roles de administrador

Esta sección contiene los siguientes temas:

Funciones y tareas de administración

Se pueden crear roles que contengan las tareas para la gestión de objetos en función de los distintos requisitos de cada negocio. Por ejemplo, se pueden crear varios roles con tareas para la gestión de usuarios y otros roles con tareas para la gestión de los roles que se creen.

También se pueden crear roles independientes con:

- Tareas para que los administradores gestionen usuarios.
- Tareas que gestionen a los administradores.
- Tareas para gestionar las funciones de administración.
- Tareas para gestionar las funciones de acceso.

Nota: También se pueden utilizar los roles del administrador predeterminados que se incluyen con CA Identity Manager. Estas funciones incluyen tareas agrupadas en categorías similares a la lista anterior.

Funciones de administración y entornos Identity Manager

Cuando se inicia sesión en un entorno Identity Manager, la cuenta de usuario posee una o más funciones de administración. Cada función de administración incluye tareas, como Crear usuario, que se utilizan en el entorno Identity Manager.

Por ejemplo, en el entorno *central* de Identity Manager, una función de administración, *Departamento de ayuda,* tiene tareas que permiten restablecer contraseñas. La función posee una regla de miembros que establece que el usuario debe ser un empleado del sector de las TI. Cuando dichos empleados inician sesión en el entorno *central* de Identity Manager, tienen la función de *Departamento de ayuda* y pueden restablecer las contraseñas de los usuarios en el entorno Identity Manager.

Roles de administrador y la Consola de usuario

El entorno de Identity Manager se visualiza a través de la Consola de usuario. Las funciones de administración asignadas determinan lo que muestra la consola. Puede verlo en la siguiente tabla:

Funciones asignadas	Formato de la Consola de usuario
Función de gestor del sistema	La lista de categorías de todos los objetos y las tareas de administración predeterminadas para gestionar tales objetos
Funciones para gestionar más de un tipo de objeto	La lista de categorías con un elemento por cada tipo de objeto que puede gestionar
Funciones para gestionar un tipo de objeto, por ejemplo Usuarios	Las tareas para dicho objeto (como Modificar usuario) *sin* una lista de categorías
Una función de aprobación	La pantalla Lista de trabajos Aparece si el administrador tiene tareas pendientes de aprobación (por ejemplo, los usuarios de autorregistro necesitan aprobación)

Si puede gestionar más de un objeto, aparecerá la lista de categorías y mostrará aquellos objetos que puede modificar (Usuarios y Grupos, por ejemplo), como las fichas situadas en la parte superior de la pantalla. Seleccione una ficha para ver las tareas de las funciones que tiene asignadas.

Nota: Si el explorador de Internet no admite hojas de estilo en cascada (CSS), la Consola de usuario utiliza un formato diferente. Para controlar el formato, consulte la *Guía de configuración*.

Creación de una función de administración

Puede crear una función de administración una vez que conozca los requisitos de dicha función. Estos requisitos afectan a todos los que utilicen dicha función, a los objetos que van a ser gestionados y al entorno que tendrán dichos objetos.

Comienzo de la creación de una función de administración

La función de administración se crea en la Consola de usuario.

Para crear un rol de administración

1. Inicie sesión en una cuenta de CA Identity Manager que tenga un rol con tareas para la creación de roles de administración.

   Por ejemplo, el primer usuario de un entorno tiene el rol de Gestor del sistema, el cual tiene la tarea Crear rol de administrador.

2. Seleccione Roles y tareas, Roles de administración y Crear rol de administrador.
3. Decida si se desea crear o copiar un rol.

   La ficha Perfil aparece cuando comienza a definir el rol de administrador.

4. Defina el Perfil del rol de administrador.

Definición del perfil de la función de administración

En la ficha Perfil, puede definir las características básicas de la función.

Para definir el perfil

1. Escriba un nombre y una descripción, y complete cualquier otro atributo personalizado que se haya definido para la función.

   Nota: Puede especificar atributos personalizados en la ficha Perfil que especifica información adicional acerca de los roles de administración. Esta información adicional se puede usar para simplificar la búsqueda de roles en entornos que incluyan un gran número de roles.

2. Seleccione Activado si está listo para dejar la función disponible para ser utilizada en cuanto la haya creado.
3. Seleccione las tareas de administración para la función (en la página 38).

Selección de las tareas de administración para la función

En la ficha Tareas, puede seleccionar las tareas de administración que se incluirán en la función. Puede incluir tareas de categorías diferentes o copiar tareas que se utilicen en otra función.

Para seleccionar las tareas de administración

1. Seleccione la categoría en el campo Filtrar por categoría.

   Para ver la lista de categorías de tarea disponibles, haga clic en el icono de flecha hacia abajo.

2. Seleccione la tarea para incluirla en el rol del campo Agregar tarea.

   CA Identity Manager agregará la tarea a la lista de tareas del rol.

3. Para agregar tareas adicionales, repita los pasos 1 y 2.

4. Para eliminar una tarea del rol, haga clic en el icono menos () de esa tarea.

5. Defina las políticas de miembros para una función de administración (en la página 39).

Definición de las políticas de miembros para una función de administración

En la ficha Miembros, puede crear políticas de miembros. Estas políticas determinan quién puede ser miembro de una función.

Para definir las políticas de miembros

1. Haga clic en Agregar para definir las políticas de miembros. Una política de miembros contiene las reglas siguientes:

   - Una regla de miembros que define los requisitos para que un usuario se convierta en miembro de la función.

     Nota: Los siguientes operadores tratan a los números como caracteres en las reglas de miembros:

     - Menor que (<)
     - Menor o igual que (<=)
     - Mayor que (>)
     - Mayor o igual que (=>)

     Por ejemplo, '10' irá después de '1' pero antes que '2'.

   - Reglas de ámbito que limitan los objetos primarios y secundarios disponibles para las tareas de la función.

     Por ejemplo, si la función contiene una tarea que modifica a los usuarios al asignarlos a grupos, la regla de ámbito de usuario limita los usuarios (objeto primario) que se pueden encontrar, y la regla de ámbito de grupo limita los grupos (objeto secundario) que se pueden asignar.

   Nota: Asegúrese de introducir una respuesta para una pregunta de ámbito como mínimo. Las reglas de ámbito limitan los objetos primarios y secundarios disponibles para las tareas en la función. Por ejemplo, si la función contiene una tarea que modifica a los usuarios al asignarlos a grupos, la regla de ámbito de usuario limita los usuarios (objeto primario) que se pueden encontrar, y la regla de ámbito de grupo limita los grupos (objeto secundario) que se pueden asignar.

2. Compruebe que la política de miembros aparece en la ficha Miembros.

   - Para editar una política, haga clic en el símbolo de flecha derecha que aparece a la izquierda.
   - Para eliminarla, haga clic en el icono con el signo menos.

3. En la ficha Miembros, active la casilla de verificación “Los administradores pueden agregar y eliminar miembros de esta función”, a menos que los usuarios sólo se puedan convertir en miembros si cumplen con una regla de miembros.

   Una vez que activa esta función, la pantalla se expande.

4. En el área expandida, defina la Acción Agregar/Eliminar para la agregación o eliminación de un usuario como miembro de la función.

   Importante: Cuando defina una acción Agregar, evite configurar una regla que haga referencia a la función que está definiendo. Por ejemplo, no defina una acción Agregar que convierta a un usuario en miembro de la Función A por su carácter de miembro de la misma función, ya que podría generar errores.

5. Defina las políticas de administración para una función de administración (en la página 40).

Definición de las políticas de administración para una función de administración

En la ficha Administradores, puede definir quién está autorizado a agregar o eliminar usuarios como miembros y administradores de la función.

Para definir las políticas de administración

1. Si desea que la opción Gestionar administradores se encuentre disponible, active la casilla de verificación “Los administradores pueden agregar y eliminar administradores de esta función”.

   Una vez que activa esta función, la pantalla se expande.

2. En el área expandida, defina la Acción Agregar/Eliminar para la agregación o eliminación de un usuario como administrador de la función.

3. Defina políticas de administración, que contengan reglas de administración y ámbito y al menos un privilegio de administrador (Gestionar miembros o Gestionar administradores).

   Nota: Puede agregar varias políticas de administración con reglas y privilegios diferentes para los administradores que cumplan con los criterios de la regla.

4. Para editar una política, haga clic en el símbolo de flecha que aparece a la izquierda. Para eliminarla, haga clic en el icono con el signo menos.

5. Defina las reglas de propietarios para una función de administración (en la página 41).

Definición de las reglas de propietarios para una función de administración

En la ficha Propietarios, puede definir las reglas sobre quién puede ser el propietario de una función, es decir, un usuario que puede modificar la función.

Para definir las reglas de propietarios

1. Defina las reglas de propietarios que determinan qué usuarios pueden modificar la función.
2. Haga clic en Enviar.

   Aparece un mensaje para indicar que se ha enviado la tarea. Es posible que se produzca un retraso momentáneo antes de que el usuario pueda utilizar la función.

Si ha seleccionado Activada al crear esta función, la función está disponible para su uso. Si un usuario reúne las condiciones de la regla de miembros, podrá iniciar sesión en el entorno Identity Manager y utilizar las tareas de la función.

Verificación de una función de administración

Para comprobar si se ha creado una función, seleccione Funciones de administración, Ver función de administración y, a continuación, seleccione el nombre de la función.

También puede elegir Sistema, Ver tareas enviadas para ver si se ha completado la tarea de creación de funciones.

Autorización a los usuarios para la autoasignación de funciones

Los usuarios se pueden asignar ciertos roles a ellos mismos. Por ejemplo, es posible que desee permitir a los usuarios que se registren para la función Gestor de la delegación a fin de que puedan delegar los elementos de trabajo de un usuario a otro.

Para controlar las funciones que los usuarios se pueden asignar a sí mismos, debe configurar los criterios en la tarea Autogestor de funciones.

Siga estos pasos:

1. Modifique la tarea Autogestor de funciones de esta manera:
   a. Seleccione Funciones y tareas, Modificar la tarea de administración, y busque la tarea Autogestor de funciones.
   b. Seleccione la ficha Fichas.

      CA Identity Manager muestra la lista de fichas que se aplican a la tarea.

c. Seleccione el icono de flecha derecha que se encuentra junto a la ficha Autogestor de funciones para editarla.

d. Rellene los campos siguientes:

Mostrar sólo aquellas funciones de administración que cumplan las siguientes reglas

Especifica los criterios que utilizará CA Identity Manager para determinar los roles que los usuarios podrán asignarse a ellos mismos.

Para agregar más reglas, haga clic en el icono más (+).

Usuario que se va a utilizar como administrador de la función de administración

Especifica el administrador para las funciones que los usuarios pueden asignarse a ellos mismos.

Las funciones que los usuarios pueden asignarse a sí mismos deben tener al usuario que haya seleccionado en este campo como administrador *y* deben reunir los criterios especificados en el campo Mostrar sólo aquellas funciones de administración que cumplan las siguientes reglas.

Pantalla Lista

Especifica las columnas y el formato de la lista de funciones que puede seleccionar un usuario para autoasignarse una función.

e. Haga clic en Aceptar y, a continuación, en Enviar.

2. Agregue la tarea Autogestor de funciones a una función y asigne dicha función a los usuarios que deban contar con esta capacidad.

Capítulo 3: Tareas de administración

Esta sección contiene los siguientes temas:

Planificación de las tareas de administración

Las funciones de administración constan de tareas de administración, las que representan capacidades específicas para la gestión de objetos. Por ejemplo, podría gestionar un objeto de usuario mediante las siguientes tareas de administración:

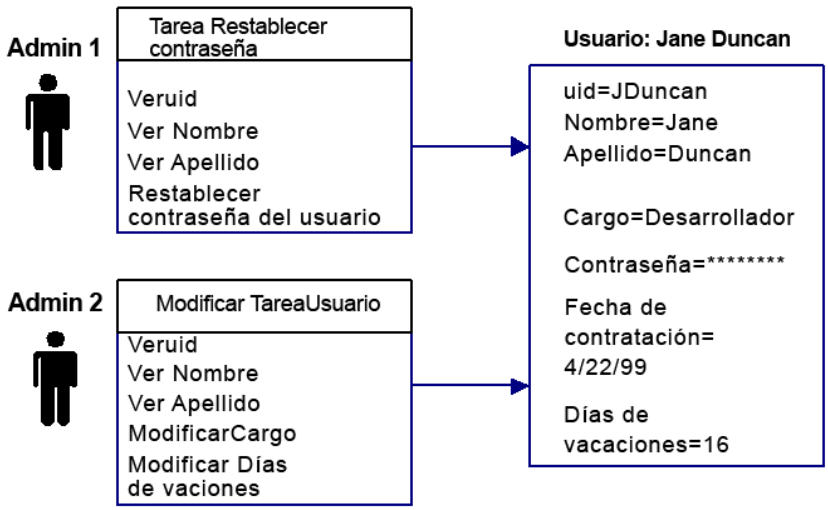
- Crear usuario
- Ver usuario
- Modificar usuario
- Restablecer contraseña del usuario

Cada tarea se crea o modifica para que cumpla exactamente con sus requisitos. A continuación, las tareas de administración adecuadas se combinan en funciones de administración, y estas funciones se asignan a los administradores. Gracias a ellas, los administradores tienen exactamente los privilegios necesarios para gestionar objetos.

Para planificar la creación de las tareas de administración, debe decidir qué objetos necesita gestionar (usuario, grupo, organización, función o tarea) y qué administradores utilizarán estas tareas. Por ejemplo:

- Para gestionar usuarios, los administradores del departamento de ayuda necesitan tareas que gestionen atributos de usuario, como el ID de usuario o el cargo.
- Para gestionar el acceso de los usuarios a las aplicaciones, otros administradores necesitan tareas que conviertan a los usuarios en miembros de las funciones de acceso.
- Para gestionar las funciones que utilizan los administradores del departamento de ayuda, los administradores de nivel superior necesitan tareas que gestionen las funciones de administración.

Puede crear tareas para un tipo de objeto (por ejemplo, usuarios) a fin de que distintos administradores gestionen atributos diferentes. Por ejemplo, en la ilustración siguiente se muestra un usuario gestionado por dos administradores.



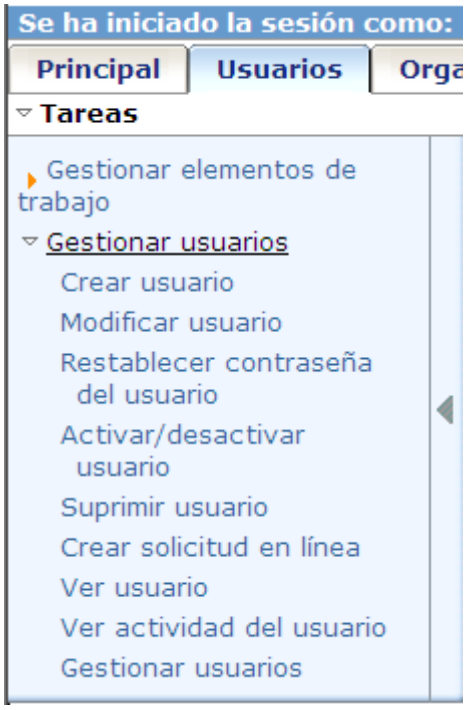
- Admin 1 tiene la tarea Restablecer contraseña del usuario. Este administrador puede ver el ID de usuario y el nombre del empleado o restablecer su contraseña.
- Admin 2 tiene la tarea Modificar usuario. Este administrador puede ver el ID de usuario y el nombre del empleado o modificar el cargo y los días de vacaciones.

Ejemplo de una tarea de administración

Cuando se crea una tarea de administración, se define el contenido y el diseño de las pantallas de la tarea. Esta definición incluye:

- El nombre de la tarea.
- La categoría donde aparece la tarea.
- Las fichas y los campos que se utilizarán en la tarea, y las propiedades de pantalla de los campos.
- Los campos que puede usar un administrador en una consulta de búsqueda y los campos que se muestran en los resultados de la búsqueda.

Para comprender los elementos de una tarea, parta de la tarea Modificar usuario. En este caso, Usuarios es la categoría, Gestionar usuarios es una subcategoría y Modificar usuario es la tarea. Los nombres de la categoría y de la tarea se crean en el momento de crear la tarea.



Al seleccionar Modificar usuario, aparecerá una pantalla de búsqueda. La *pantalla de búsqueda* muestra las opciones para buscar el objeto que se desea ver o modificar. Cada opción se denomina *filtro* y estos filtros constituyen un límite para los objetos hallados en la búsqueda.

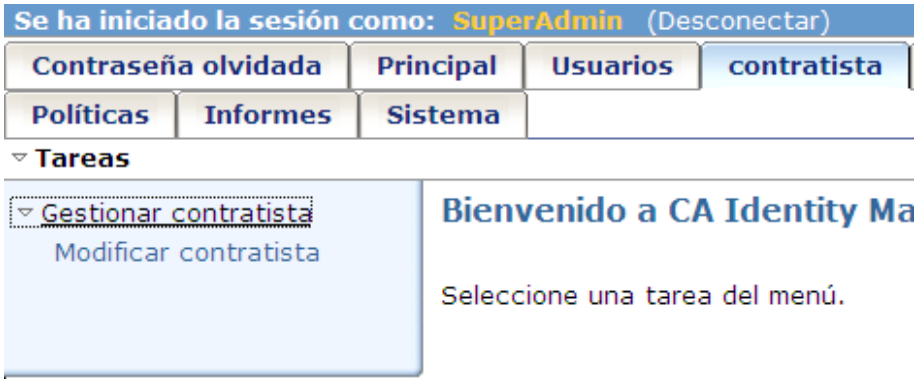
Una vez que haya completado la pantalla de búsqueda, aparece una pantalla con fichas. Por ejemplo, la siguiente ilustración muestra las fichas de la tarea Modificar usuario. La ficha Perfil es la primera en aparecer y muestra los atributos de usuario; las otras fichas muestran la función y los privilegios de grupo correspondientes al usuario.

Para las tareas que crea, debe decidir qué fichas incluir y determinar el orden y el contenido.

Por ejemplo, con la tarea Modificar usuario como plantilla, podría crear una tarea Modificar contratista, que incluya cambios en:

- Los campos de la ficha Perfil.
- Las fichas que se incluyen la tarea y su contenido.
- La categoría en la que aparece la tarea.

  Podría crear esta tarea en una categoría nueva: Contratista.



La tarea Modificar contratista incluye algunos de los campos de la ficha Perfil de la tarea Modificar usuario además de otros campos, como la fecha de inicio del contrato y la empresa del contratista. Para buscar un contratista, los administradores pueden buscar por nombre del contratista, empresa y fecha de inicio.

La nueva tarea también incluye una ficha Roles del contratista donde puede agregar roles para los contratistas.

Opciones de uso de las tareas de administración

Identity Manager permite utilizar las tareas de administración de dos formas:

- **Selección de la tarea**

  Se selecciona una categoría y una tarea y, a continuación, se busca el objeto al cual se aplica la tarea.

  Por ejemplo, para modificar un perfil de usuario, seleccione la categoría Usuarios y, a continuación, seleccione la tarea Modificar usuario. A continuación, se busca el usuario que desea modificar.

- **Selección del objeto**

  Para buscar un objeto, se usan las tareas "Gestionar", como Gestionar usuarios o Gestionar grupos. Una vez que se ha seleccionado el objeto, es posible visualizar una lista de las tareas que se pueden utilizar para gestionar dicho objeto. Este método se denomina *navegación objeto-tarea.*

  Por ejemplo, para modificar un usuario con este método, seleccione la categoría de usuario y, a continuación, seleccione la tarea Gestionar usuario. Busque y seleccione el usuario que desea gestionar. En los resultados de búsqueda, haga clic en un icono para ver una lista de las tareas que puede usar para gestionar el usuario seleccionado. En esa lista, puede seleccionar Modificar usuario o cualquier otra tarea adecuada.

  También puede configurar listas de tareas en tareas que no sean Gestionar. Por ejemplo, puede agregar una lista de tareas a una ficha Pertenencia a. En este caso, habrá una lista de tareas disponible para cada miembro que aparece en la ficha.

  Nota: En la lista de tareas de un objeto sólo aparecen las tareas que puede usar el administrador actual.

Tareas de administración predeterminadas

CA Identity Manager incluye un conjunto de tareas y roles de administración predeterminados que se agregan a CA Identity Manager mediante la importación de un archivo de definiciones de roles en la Consola de gestión. Si crea un entorno en la Consola de gestión y decide crear los roles predeterminados, CA Identity Manager importará un archivo de definiciones de roles de forma automática.

Nota: Para admitir algunas funciones, como la gestión de cuentas de determinados tipos de puntos finales, es posible que necesite importar archivos de definiciones de roles adicionales con el fin de crear los roles y las tareas que necesite.

En la mayoría de los casos, podrá utilizar las tareas predeterminadas, tal y como se instalaron. Sin embargo, es posible que necesite modificar la ficha Perfil en las tareas de usuario predeterminadas como, por ejemplo, Crear usuario, Modificar usuario y Ver usuario. La ficha Perfil incluye todos los campos que se han definido para el objeto de usuario en al archivo de configuración de directorios. Es posible que desee limitar el número de campos que aparecen en la ficha o cambiar las propiedades de visualización de campos.

Nota: Se recomienda crear una copia de una tarea predeterminada para modificarla en lugar de modificar la tarea predeterminada directamente.

Cómo crear una tarea de administración personalizada

Una *tarea de administración* es una función administrativa que un usuario puede realizar en Identity Manager. Entre los ejemplos de tareas de administración se incluye: Crear usuario, Modificar grupo y Ver pertenencia a función.

CA Identity Manager incluye tareas de administración predeterminadas que se pueden modificar para adaptarlas a las necesidad de su negocio.

Al crear una tarea de administración personalizada, debe llevar a cabo los siguientes pasos:

Nota: En la sección Requisitos de Active Directory (en la página 70) se incluyen más consideraciones en el caso de que CA Identity Manager esté gestionando un almacén de usuarios de Active Directory.

1. En la Consola de usuario de CA Identity Manager, seleccione Roles y tareas, Tareas de administración y Crear tarea de administración.

   CA Identity Manager solicita si desea crear una tarea nueva o crear una a partir de una tarea existente.

   Por ejemplo, seleccione la tarea Modificar usuario como base para la tarea nueva.

2. Seleccione Crear una copia de una tarea existente y busque la tarea que desee copiar.

   Nota: Se recomienda modificar la copia de una tarea predeterminada en lugar de modificar la tarea predeterminada directamente.

3. Al hacer clic en Aceptar, aparecerá una pantalla con las siguientes seis fichas:

Ficha	Finalidad	Consulte este tema
Perfil	Definir el perfil de la tarea que se está creando	Definición del perfil de la tarea (en la página 50)
búsqueda	Limitar el intervalo de objetos que gestiona la tarea	Definición del ámbito de la tarea (en la página 55)
Fichas	Elegir y diseñar las fichas de la tarea	Selección de fichas para la tarea (en la página 65)
Campos	Mostrar los campos utilizados en todas las fichas	Vista de campos de la tarea (en la página 69)
Eventos	Seleccionar un proceso de flujo de trabajo para cada evento si el entorno CA Identity Manager y la tarea utilizan un flujo de trabajo	Asignación de procesos de flujo de trabajo para eventos (en la página 69)

Ficha	Finalidad	Consulte este tema
Utilización de los roles	Muestra los roles que incluye la tarea que se está viendo o modificando.	Visualización de la utilización de los roles (en la página 69)

Nota: Para obtener más información sobre cómo crear tareas de administración personalizadas, consulte la *Guía de diseño de la Consola de usuario*.

Definición del perfil de la tarea

La ficha Perfil incluye la configuración general de la tarea.

Para definir el perfil de la tarea

1. Seleccione el tipo de objeto para la tarea, que se denomina objeto primario, y la acción que se debe realizar sobre él.
2. Rellene los campos necesarios y seleccione las casillas de verificación adecuadas que sean necesarias para la tarea.

   Nota: Si está creando una tarea que tenga una configuración de perfil semejante a la de una tarea ya existente, haga clic en Copiar el perfil de otra tarea. Esta opción rellena la información de configuración de perfil de la tarea que está creando utilizando la configuración de perfil de cualquier tarea existente que seleccione. A continuación, agregue un nombre y una descripción a la nueva tarea.
3. (Opcional) Asocie un identificador de tareas lógicas del negocio a la tarea.
4. Una vez que haya completado esta ficha, continúe con el paso siguiente, Definición del ámbito de la tarea (en la página 55).

Ficha Perfil de la tarea de administración

La ficha Perfil de la tarea de administración le permite definir la configuración general de una tarea de administración.

Esta ficha contiene los siguientes campos:

- **Nombre**

  Define el nombre de la tarea.
- **Etiqueta**

  Define el identificador único de la tarea. Se utiliza en direcciones URL, servicios Web o archivos de propiedades. La etiqueta puede contener caracteres ASCII (a-z, A-Z), números (0-9) o guiones bajos, y comenzar por una letra o un guión bajo.

- **Descripción**

  Especifica una nota opcional sobre el objetivo de la tarea.

- **Orden de las tareas**

  Especifica el orden en que se muestra la tarea. Si no se especifica ningún orden, las tareas se muestran en orden alfabético.

- **Categoría**

  Especifica una categoría para la tarea. Las categorías se muestran en forma de fichas en la parte superior de la pantalla.

- **Orden de categoría**

  Especifica el orden en el que aparece la ficha Categoría. Por ejemplo, si establece el orden de categoría como 3, la categoría que especifique aparecerá como la tercera ficha.

- **Categoría 2**

  Especifica la categoría de segundo nivel. Esta categoría aparece como un enlace debajo de la lista de fichas de categoría. La categoría de segundo nivel sólo aparece cuando se selecciona la ficha de la categoría de primer nivel. Por ejemplo, si ha creado una tarea con la categoría de primer nivel Empleado, y con la categoría de segundo nivel Gestión de empleados, esta última categoría sólo aparecerá después de haber seleccionado la ficha Empleado.

- **Orden de categoría 2**

  Especifica el orden en el que aparece la categoría de segundo nivel si existe más de una categoría de segundo nivel en una categoría primaria.

- **Categoría 3**

  Especifica la categoría de tercer nivel. Esta categoría aparece en el panel de navegación izquierdo. Las tareas se enumeran en la categoría de tercer nivel. Por ejemplo, en un entorno predeterminado, un usuario con la función de Gestor del sistema o de Gestor de usuarios podrá ver la categoría de tercer nivel Gestionar usuarios si selecciona la ficha Usuarios.

- **Orden de categoría 3**

  Especifica el orden en el que aparece la categoría de tercer nivel.

- **Objeto primario**

  Especifica el objeto sobre el que opera la tarea.

- **Acción**

  Especifica la operación que se realizará en el objeto.

- **Sincronización de usuarios**

  Especifica si la tarea sincroniza los usuarios con las políticas de identidad. Puede seleccionar una de las opciones siguientes:

  - **Desactivado** (predeterminado)

    Especifica que esta tarea no inicia la sincronización de usuarios.

  - **Al completar la tarea**

    Especifica que CA Identity Manager inicia el proceso de sincronización de usuarios después de que se hayan completado todos los eventos de una tarea. Este valor es la opción de sincronización predeterminada para las tareas Crear usuario, Modificar usuario y Suprimir usuario. La configuración predeterminada para el resto de tareas es Desactivado.

    Nota: Si selecciona la opción Al completar la tarea para una tarea que incluya varios eventos, CA Identity Manager no sincronizará los usuarios hasta que se completen todos los eventos de la tarea. Si uno o más de esos eventos requieren aprobación de flujo de trabajo, puede demorarse varios días. Para evitar que CA Identity Manager espere a aplicar políticas de identidad hasta que se terminen todos los eventos, seleccione la opción En cada evento.

  - **En cada evento**

    Especifica que CA Identity Manager inicia el proceso de sincronización de usuarios (en la página 481) cuando se completa cada evento de la tarea.

    En el caso de tareas con un evento principal y uno secundario para el mismo usuario, si configura la sincronización de usuarios en la opción En cada evento, es posible que se apliquen más políticas de identidad a un usuario que si se selecciona la opción Al completar la tarea.

- **Sincronización de cuentas**

  Sincroniza las cuentas que se hallan en el servidor de aprovisionamiento, si tiene la opción de aprovisionamiento activada.

  - **Desactivado** (predeterminado)

    Especifica que esta tarea no inicia la sincronización de cuentas.

  - **Al completar la tarea**

    Especifica que CA Identity Manager inicia el proceso de sincronización de cuenta después de que se hayan completado todos los eventos de una tarea.

- **En cada evento**

  Especifica que CA Identity ManagerCA Identity Manager inicia el proceso de sincronización de cuentas cuando se completa cada evento de la tarea.

  Nota: Para obtener el máximo rendimiento, seleccione Al completar la tarea. No obstante, si selecciona la opción Al completar la tarea para una tarea que incluya varios eventos, CA Identity Manager no sincronizará las cuentas hasta que se completen todos los eventos de la tarea. Si uno o más de esos eventos requieren aprobación de flujo de trabajo, puede demorarse varios días. Para evitar que CA Identity Manager espere a sincronizar las cuentas hasta que finalicen todos los eventos, seleccione la opción En cada evento.

- **Ocultar en menús**

  Evita que la tarea aparezca en los menús. Active este control si la tarea sólo la invoca una dirección URL u otra tarea.

- **Tarea pública**

  Hace que la tarea esté disponible para los usuarios que no han iniciado sesión en CA Identity Manager. Las tareas públicas predeterminadas son contraseña olvidada y autorregistro.

- **Activar auditoría**

  Registra información sobre la tarea en una base de datos de auditoría. La información de la auditoría se puede utilizar para generar informes. Consulte la *Guía de configuración*.

- **Activar Flujo de trabajo**

  Permite que los eventos de CA Identity Manager asociados con la tarea inicien los procesos de flujo de trabajo, si tiene instalado el motor de flujo de trabajo. Por ejemplo, los eventos asociados con la tarea Suprimir grupo pueden iniciar un proceso de flujo de trabajo que incluya un paso de aprobación.

- **Activar Servicios Web**

  Marca la tarea para indicar que ésta admite que se genere salida WSDL (Lenguaje de descripción de servicios Web) desde la Consola de gestión. Active este control si desea utilizar el envío de tareas remoto. Para obtener más información, consulte la *Guía de programación para Java.*

- **Proceso de flujo de trabajo**

  Permite la configuración del flujo de trabajo del nivel de tarea. Haga clic en el icono del lápiz para configurar el flujo de trabajo basado en política o no.

- **Prioridad de la tarea**

  Determina el orden en que CA Identity Manager ejecuta las tareas. Las tareas con prioridad Alta se ejecutan antes que las tareas con prioridad Media o Baja. La prioridad predeterminada de una tarea es Media.

  Nota: Puede utilizar la tarea Ver tareas enviadas para buscar tareas con una prioridad específica y luego mostrar su estado.

- **Identificadores de tareas lógicas del negocio**

  Asocia un identificador de tareas lógicas del negocio (en la página 74) con la tarea.

- **Botones de acción del flujo de trabajo**

  Agrega botones de acción personalizados a tareas de aprobación de flujo de trabajo.

- **Copiar el perfil de otra tarea**

  Copia los datos de la ficha Perfil de otra tarea.

  Por ejemplo, podría copiar la configuración de la ficha Perfil de la tarea Modificar usuario y luego agregarle un nombre y una descripción.

Propiedades de configuración de tareas

Las propiedades de configuración de tareas controlan las propiedades de visualización y determinados comportamientos de la tarea.

Ruta del icono de la tarea

Especifica la URL de un gráfico para utilizarlo como icono para esta tarea en las listas de tareas.

Vista previa del icono de la tarea

Muestra el icono de la tarea, tal como aparece en las listas de tareas.

Suprimir la navegación en las tareas

Cuando se selecciona, oculta la navegación superior y la lista de tareas una vez que el usuario selecciona una tarea. Esto impide a los usuarios que salgan de la tarea actual hasta que completen las acciones necesarias o cancelen la tarea.

Ventana de destino

Cuando se especifica un valor en este campo, CA Identity Manager abre esta tarea en una nueva ventana del explorador. Utilice este campo para abrir una nueva ventana del explorador para una tarea externa que redirige a los usuarios a otro sitio Web.

Puede especificar cualquier nombre para la ventana.

Nota: No utilice este campo para abrir tareas de administración de CA Identity Manager en una ventana del explorador independiente. CA Identity Manager no admite el uso de varios exploradores de Windows para una misma sesión de usuario de CA Identity Manager.

Definición del ámbito de la tarea

En la ficha Buscar puede definir el ámbito de la tarea. Este valor limita los objetos que están a disposición de la tarea. Por ejemplo, si el objeto de una tarea es usuarios, puede definir el ámbito a los usuarios que sean contratistas.

Nota: La ficha Buscar no aparece si la tarea no tiene un objeto primario, o bien si la acción es de automodificación, autovista o aprobación.

Puede configurar lo siguiente en la ficha Buscar:

Pantalla Buscar

La pantalla de búsqueda limita el ámbito de la tarea en función de filtros. Haga clic en Examinar para ver las opciones de pantalla de búsqueda disponibles.

Nota: Tal vez desee crear su propia pantalla de búsqueda (en la página 56). Para crear una versión modificada a partir de una pantalla de búsqueda existente, seleccione la pantalla y haga clic en Copiar. A continuación, podrá modificar la pantalla de búsqueda sin cambiar la definición de la pantalla de búsqueda original. Para crear una pantalla de búsqueda, haga clic en Nueva.

Opciones de búsqueda

Las opciones de búsqueda sólo aparecen cuando el objeto es una función o un grupo.

- La primera opción limita la búsqueda en función de los campos definidos en la pantalla de búsqueda. Dentro de estos límites, la búsqueda localiza todos los grupos o funciones en el ámbito del administrador.
- Otras opciones limitan la búsqueda como se indica.

Tenga en cuenta lo siguiente:

- De forma predeterminada, las pantallas de búsqueda de grupos admiten filtros. Esto significa que los administradores pueden especificar los criterios para limitar el ámbito de las búsquedas de grupo. Para eliminar la capacidad de usar filtros, cree una pantalla de búsqueda que no contenga ningún campo para incluir en una consulta de búsqueda.
- *No se admiten filtros*, es una opción que aparece en la ficha Buscar cuando el objeto es un rol. Indica que la tarea muestra los roles que cumplen los criterios en la opción seleccionada. Se omiten los campos de búsqueda que se configuran en la pantalla de búsqueda.

Los objetos modificados deben permanecer en el ámbito del administrador.

Cuando se selecciona esta casilla de verificación, CA Identity Manager muestra un error si los cambios en la tarea hacen que el administrador pierda ámbito sobre el objeto principal. Por ejemplo, un administrador puede utilizar Modificar usuario para cambiar el atributo de tipo de empleado de un usuario a Director. Este cambio puede establecer el usuario fuera del ámbito del administrador.

Configuración de la pantalla Buscar

Se configura una pantalla de búsqueda para limitar el ámbito de la tarea y controlar los campos donde los usuarios pueden realizar búsquedas. Las pantallas de búsqueda se aplican a dos tipos de objetos:

- Un *objeto primario*: el objeto que modificará o visualizará la tarea.
- Un *objeto secundario:* el objeto que está relacionado con el objeto primario.

  Por ejemplo, si incluye una ficha de grupo en una tarea Crear usuario, el usuario es el objeto primario y el grupo es el objeto secundario. La ficha Grupo requiere una pantalla de búsqueda para grupos.

  Nota: Después de configurar una pantalla de búsqueda, puede utilizarla para cualquier tarea de búsqueda de un objeto primario o secundario.

Filtros de búsqueda

Los filtros de búsqueda limitan los objetos que detecta la búsqueda. Por ejemplo, si el objeto es usuarios, puede limitar la búsqueda para que sólo se busquen contratistas. Se puede configurar un filtro para buscar usuarios con el tipo de empleado Contratista.

Es posible configurar los siguientes campos para las búsquedas:

Mostrar sólo aquellos objetos que cumplan las siguientes reglas

Define otros criterios que se combinan con el filtro definido por el usuario para restringir la búsqueda.

Tenga en cuenta lo siguiente cuando utilice este campo**:**

- Debido a limitaciones de las búsquedas de roles de aprovisionamiento, estos criterios sobrescriben los campos de filtro que tengan el mismo nombre introducido por el usuario.
- Los atributos que se utilizan al configurar este campo no se deben incluir como campos de búsqueda disponibles en la pantalla de búsqueda.

  Por ejemplo, si la pantalla de búsqueda se configura para que muestre sólo las funciones con el atributo Activado establecido en Sí, suprima el atributo Activado de la lista de atributos que pueden especificar los usuarios en los criterios de búsqueda.

  De lo contrario, se ignorarán los criterios introducidos por el usuario.

Filtro de búsqueda predeterminado

Define un filtro que aparece de forma predeterminada cuando un administrador usa la pantalla de búsqueda. Por ejemplo, si configura una pantalla de búsqueda para la tarea de modificación de contratista y sabe que los administradores, por lo general, buscan contratistas en función del nombre de la empresa, puede definir el filtro predeterminado Empresa contratista = *. Para anular el filtro predeterminado, los administradores pueden especificar criterios de búsqueda diferentes. Al establecer un filtro predeterminado se mejora el rendimiento ya que se limita la cantidad de resultados devueltos si un administrador no especifica un filtro antes de comenzar una búsqueda.

Seleccionar automáticamente todos los resultados de la búsqueda cuando se utilicen con tareas de varias selecciones

Especifica que todos los resultados de la búsqueda estén seleccionados de forma predeterminada. Si selecciona esta casilla, todos los objetos de la lista de resultados de la búsqueda aparecen con una casilla marcada al lado del nombre de objeto.

Buscar automáticamente

Especifica que se muestra un campo de búsqueda con los resultados de la búsqueda.

Establecer automáticamente el asunto de la tarea cuando sólo haya un único resultado de la búsqueda

Establece automáticamente el objeto primario de la tarea cuando sólo coincide un objeto con el filtro de búsqueda.

Por ejemplo, supongamos que esta opción está seleccionada para una pantalla de búsqueda de usuario que está asociada con la tarea Modificar usuario. Cuando un administrador abre la tarea de modificación de usuario e introduce un filtro de búsqueda que devuelve sólo un usuario, CA Identity Manager abre la tarea de modificación de usuario correspondiente a dicho usuario. No es necesario que el administrador seleccione el usuario para abrir la tarea Modificar usuario.

Nota: Para que este ajuste se aplique, también tiene que seleccionarse la opción Buscar automáticamente.

Guardar filtro de búsqueda

Especifica que el filtro de búsqueda de la tarea se guarda para el usuario en la sesión actual. La siguiente vez que un usuario busque en la tarea, se mostrará el filtro de búsqueda guardado.

Nota: CA Identity Manager guarda el filtro de búsqueda durante la sesión de usuario. Cuando el usuario cierra la sesión, el filtro de búsqueda se elimina.

Buscar en organización

Muestra un filtro de organización en la pantalla de búsqueda. Si se selecciona esta casilla de verificación, los administradores pueden especificar un filtro que limite las organizaciones en las cuales CA Identity Manager busca un objeto. Para especificar valores predeterminados para el filtro de búsqueda de la organización, especifique una pantalla de búsqueda en el campo Búsqueda de organizaciones.

Guardar organización de la búsqueda

Especifica que se guardará la organización para la tarea si se ha establecido una organización para la búsqueda. La próxima vez que un usuario busque en la tarea, se mostrará la organización.

Búsqueda de organizaciones

Especifica la pantalla de búsqueda que utiliza CA Identity Manager para permitir a los administradores buscar una organización.

Ámbito de búsqueda predeterminada de organizaciones

Especifica el ámbito de búsqueda predeterminado de organizaciones que aparece cuando el administrador utiliza una pantalla de búsqueda. El ámbito de la búsqueda determina los niveles del árbol de organización que se incluyen en la búsqueda. Los administradores pueden sobrescribir el ámbito de búsqueda predeterminado de organizaciones mediante la especificación de criterios de búsqueda diferentes en la pantalla de búsqueda.

Por ejemplo, si configura una pantalla de búsqueda para una tarea Modificar contratista personalizada en un entorno que almacene información del contratista en varios niveles del árbol de la organización, puede configurar el ámbito de búsqueda predeterminado de organizaciones en E inferior.

Búsqueda de una única expresión

Define el tipo de filtro de búsqueda que aparecerá en la pantalla de búsqueda. Cuando selecciona esta casilla de verificación, los usuarios pueden especificar un solo filtro de búsqueda como <atributo><comparador><valor>. Si se anula la selección de esta casilla de verificación, los usuarios podrán especificar varios criterios de búsqueda. Por ejemplo, <atributo1><comparador><valor1> Y <atributo2><comparador> <valor2>. Los objetos que cumplen las condiciones de todos los filtros se devuelven en los resultados de búsqueda. En el ejemplo anterior, se devolverán como resultados los objetos que incluyan <valor1> y <valor2>.

Equivale sólo a la búsqueda

Prohíbe a los administradores utilizar operadores de búsqueda distintos a igual a.

Mostrar el número de resultados

Muestra el número de resultados de búsqueda coincidentes. Si se selecciona esta casilla de verificación, todas las búsquedas devolverán el mensaje: "Se han encontrado X resultados".

Agregar botón de tarea para <nombre tarea>

Agrega un enlace a otra tarea en la pantalla de búsqueda. El enlace se muestra como un botón.
Por lo general, este campo se utiliza para agregar una tarea Crear a una pantalla de búsqueda configurada para la navegación objeto-tarea.

Etiqueta opcional

Especifica una etiqueta para la tarea que se ha seleccionado en el campo anterior. Esta etiqueta aparece en el botón de la tarea.

Agregar botón de eliminación múltiple para <nombre tarea>

Agrega un enlace a una tarea. Este enlace permite a los administradores seleccionar varios objetos que suprimir. El enlace se muestra como un botón.
Por lo general, este campo aparece con navegación objeto-tarea.

Campos de búsqueda y resultados de búsqueda

En otra parte de la pantalla de búsqueda, se pueden seleccionar los campos que el administrador podrá utilizar en una consulta de búsqueda y los campos que aparecerán en los resultados de la búsqueda.

Seleccionar los campos en los que puede buscar el usuario

Seleccione los campos que un administrador puede utilizar para crear una consulta de búsqueda.

Para agregar más campos, selecciónelos en el cuadro de lista que verá bajo la tabla de campos de búsqueda.

Después de seleccionar los campos, puede cambiar el orden en que estos aparecen mediante los iconos de flecha hacia arriba y hacia abajo situados a la derecha del campo.

Nota: Si no especifica campos donde puede buscar el administrador, CA Identity Manager inicia la búsqueda automáticamente.

Seleccionar los campos que aparecen en los resultados de la búsqueda

Seleccione los campos que CA Identity Manager mostrará en los resultados de búsqueda. Puede seleccionar campos que no están disponibles en la consulta de búsqueda.

Para agregar más campos, selecciónelos en el cuadro de lista que verá bajo la tabla de campos de búsqueda.

Estilo

Cuando selecciona un campo para mostrar en los resultados de búsqueda, puede seleccionar una de las siguientes opciones de estilo:

- **Mostrar nombre booleano**

  Muestra el nombre del campo para todos los resultados que sean verdaderos. Por ejemplo, si introduce Activada como nombre del atributo que indica el estado de cuenta de un usuario, "Activada" aparecerá en los resultados de búsqueda de todas las cuentas de usuario activas.

- **Marca de verificación**

  Muestra el valor como una marca de verificación seleccionada en función del valor del atributo. Por ejemplo, si selecciona el estilo de marca de verificación para indicar el estado Activado/Desactivado de las cuentas de usuario, CA Identity Manager mostrará una marca de verificación seleccionada para todas las cuentas activas.

- **Cadena con varios valores**

  Muestra los valores en un atributo con varios valores en distintas líneas. Los valores se muestran alfabéticamente.

- **Cuadro de selección de sólo lectura**

  Muestra el valor como una casilla de verificación de sólo lectura.

- **STRING**

  Muestra el valor como una cadena de texto.

- **Tarea**

  Agrega una lista de tareas a un campo. Los usuarios hacen clic en un icono de flecha para ver una lista de las tareas que pueden realizar en el objeto asociado con el campo de búsqueda. Por ejemplo, si agrega una lista de tarea al campo Apellido en los resultados de búsqueda, los usuarios podrán hacer clic en el icono de flecha de ese campo para ver una lista de las tareas que puede realizar en el usuario seleccionado.

  Este ajuste también se puede emplear para hacer que un valor de atributo aparezca como vínculo de una tarea.

  Si selecciona el estilo Tarea, aparecerá un icono de flecha derecha junto a la columna Estilo. Haga clic en la flecha para abrir el cuadro de diálogo Propiedades del campo. Utilice este cuadro para configurar una lista de tareas.

- **Lista de tareas**

  Agrega tareas adicionales que los usuarios pueden realizar en objetos de las pantallas de búsqueda y lista. Por ejemplo, se puede configurar la pantalla de búsqueda en la tarea Modificar usuario para permitir a los usuarios realizar una tarea, como desactivar a un usuario, de la lista de usuarios devueltos por la búsqueda.

  Cuando selecciona esta opción, determina si los usuarios acceden a la tarea haciendo clic en un icono o en un vínculo de texto.

- **Menú de tareas**

  Agrega más tareas (similares al estilo de la lista de tareas) como elementos del menú emergente.

  Cuando selecciona esta opción, aparece un botón Acción al lado de cada objeto en una pantalla de búsqueda o lista. Los usuarios hacen clic en el botón Acción para consultar la lista de tareas que pueden realizar para ese objeto.

Nota: Para consultar las opciones de los estilos de la lista de tareas y el menú de tareas, seleccione (Separador) cuando agrega un campo a la tabla de resultados de la búsqueda. Para obtener más información sobre cómo agregar más tareas para registrar y enumerar pantallas, consulte la *Guía de diseño de la consola de usuario*.

Que se puede clasificar

Seleccione esta casilla de verificación para permitir a los administradores ordenar los resultados de búsqueda por campos.

Establecer el orden de clasificación predeterminado para los resultados de la búsqueda

Especifica el orden en que se mostrarán los resultados de la búsqueda. Los resultados de la búsqueda se ordenan inicialmente por el primer campo de la lista y luego por cada campo adicional en el orden en que aparecen. Seleccione la casilla de verificación Descendente para ordenar los resultados por orden descendente.

Seleccionar objetos con cambios en el campo *nombre de campo*

Especifica que se seleccionen los objetos en los que se ha modificado el campo especificado cuando el usuario haga clic en el botón Seleccionar.

Devolver *N* resultados por página

Seleccione la cantidad de resultados que se mostrarán por página. Cuando los resultados de la búsqueda superen el número especificado, CA Identity Manager mostrará un enlace a cada página de resultados.

Ayuda definida por el usuario en las pantallas Buscar

Si desea agregar texto personalizado a la pantalla de búsqueda, puede definir texto en el cuadro de texto HTML correspondiente. Puede agregar texto en las siguientes áreas:

- Comienzo o fin de la página
- Antes o después de la creación
- Antes o después de los resultados

Tipos de pantallas de búsqueda

Identity Manager incluye las siguientes pantallas de búsqueda preconfiguradas.

Pantalla de Buscar rol de acceso

La Pantalla Buscar rol de acceso permite configurar filtros de búsqueda para hallar roles de acceso que cumplan con determinados criterios.

Pantalla Buscar rol de acceso

La Pantalla Búsqueda de tareas de acceso permite configurar filtros de búsqueda para hallar tareas de acceso que cumplan con determinados criterios. Esta pantalla de búsqueda se usa para encontrar una tarea de acceso que se desee ver o modificar, o para agregar una tarea a una función de acceso.

Pantalla de Búsqueda de funciones de administración

La Pantalla Búsqueda de funciones de administración permite configurar filtros de búsqueda para hallar funciones de administración que cumplan con determinados criterios.

Pantalla de Búsqueda de tareas de administración

La Pantalla Búsqueda de tareas de administración permite configurar filtros de búsqueda para hallar tareas de administración que cumplan con determinados criterios. Esta pantalla de búsqueda se usa para encontrar una tarea de administración que se quiera ver o modificar, o para agregar una tarea a una función de administración.

Pantalla Buscar aprobaciones

La Pantalla Buscar aprobaciones permite configurar la visualización que aparece en la parte superior de una tarea de aprobación.

Pantalla de Búsqueda de Empezar certificación del usuario

La pantalla Búsqueda de Empezar certificación del usuario permite configurar filtros de búsqueda para hallar usuarios y establecer que necesitan certificación. El estado de certificación de los usuarios seleccionados se establecerá para indicar que *requieren certificación*.

Pantalla Certificar búsqueda de usuario

La Pantalla Certificar búsqueda de usuario permite configurar los filtros de búsqueda para hallar usuarios que requieren certificación.

Pantalla de búsqueda de Delegación

La Pantalla de búsqueda de Delegación permite configurar los filtros de búsqueda para hallar otros usuarios que se van a agregar como delegados. Un delegado es otro usuario a quien puede otorgar permiso temporal para ver y resolver elementos de su flujo de trabajo.

Pantalla Activar/desactivar la búsqueda de usuario

La Pantalla Activar/desactivar la búsqueda de usuario permite configurar los filtros de búsqueda para activar/desactivar usuarios que cumplan con determinados criterios.

Pantalla de Búsqueda del usuario EndCertification

La pantalla Búsqueda del usuario EndCertification permite configurar criterios de búsqueda para identificar usuarios cuyo ciclo de certificación debería estar completo.

Pantalla Búsqueda del Acuerdo de licencia del usuario final

La Pantalla Búsqueda del Acuerdo de licencia del usuario final permite configurar la tarea Autorregistro con una página que es específica de su aplicación basada en identidades.

Búsqueda Explorar y correlacionar

La Pantalla de búsqueda Explorar y correlacionar permite configurar filtros de búsqueda para explorar y correlacionar definiciones que cumplan con determinados criterios.

Búsqueda Carga de archivo de alimentador

La Pantalla búsqueda Carga de archivo de alimentador permite examinar el archivo de alimentador que se va a cargar. Los archivos de alimentador se utilizan para automatizar acciones repetitivas que se realizan en una gran cantidad de objetos gestionados.

Pantalla Buscar contraseña olvidada/Búsqueda del ID de usuario olvidado

La Pantalla Buscar contraseña olvidada permite configurar la tarea Contraseña olvidada para solicitar a los usuarios información que verifique su identidad.

Pantalla Buscar grupos

La Pantalla Buscar grupos permite configurar filtros de búsqueda para grupos, por ejemplo, grupos dentro de la organización financiera.

Pantalla de Búsqueda de conjuntos de políticas de identidad

La Pantalla de Búsqueda de conjuntos de políticas de identidad permite configurar criterios de búsqueda para hallar conjuntos de políticas de identidad que cumplan con determinados criterios.

Pantalla de Búsqueda de identificadores de atributos lógicos

La Pantalla de Búsqueda de identificadores de atributos lógicos permite configurar filtros de búsqueda para hallar identificadores de atributos lógicos. Esta pantalla de búsqueda se utiliza para hallar un identificador de atributos lógicos y ver o modificar su configuración.

Pantalla de búsqueda Gestionar informes

La Pantalla de búsqueda Gestionar informes permite configurar filtros de búsqueda para hallar un informe que desea ver o suprimir.

Pantalla de Búsqueda de usuarios sin certificar

La Pantalla de Búsqueda de usuarios sin certificar permite configurar filtros de búsqueda para hallar usuarios que no han sido certificados al finalizar el período de certificación.

Pantalla Buscar organizaciones

La pantalla Buscar organizaciones permite configurar filtros de búsqueda para limitar la selección de organizaciones a determinadas organizaciones secundarias.

Pantalla de Búsqueda de funciones de aprovisionamiento

La Pantalla de Búsqueda de funciones de aprovisionamiento permite configurar filtros de búsqueda para recuperar funciones de aprovisionamiento.

Pantalla de búsqueda de plantillas de cuenta

La pantalla de búsqueda de plantillas de cuenta permite configurar filtros de búsqueda para recuperar plantillas de cuenta.

Pantalla Búsqueda de políticas de contraseñas

La Pantalla Búsqueda de políticas de contraseñas permite configurar filtros de búsqueda para hallar políticas de contraseñas que cumplan con determinados criterios.

Pantalla Búsqueda de definición de instantánea

La Pantalla de Búsqueda predeterminada de definición de instantánea permite configurar filtros de búsqueda para hallar una definición de instantánea que desee ver, modificar o suprimir.

Pantalla estándar Buscar

La Pantalla estándar Buscar le permite configurar filtros para buscar objetos gestionados personalizados.

Pantalla Buscar usuarios

La pantalla de Búsqueda de usuarios le permite configurar filtros de búsqueda para hallar usuarios que cumplan con determinados criterios. Por ejemplo, puede buscar aquellos usuarios que sean contratistas.

Una vez que complete la ficha Buscar, elija las fichas para la tarea.

Selección de fichas para la tarea

En la ficha Fichas, asigne un nombre a las fichas y configúrelas. Cada una de ellas es un conjunto de campos que se incluyen en la tarea. Puede incluir fichas predeterminadas o crear nuevas. Por ejemplo, la tarea Modificar usuario incluye las siguientes fichas:

- Perfil
- Funciones de acceso
- Funciones de administración
- Grupos
- Delegar elementos de trabajo

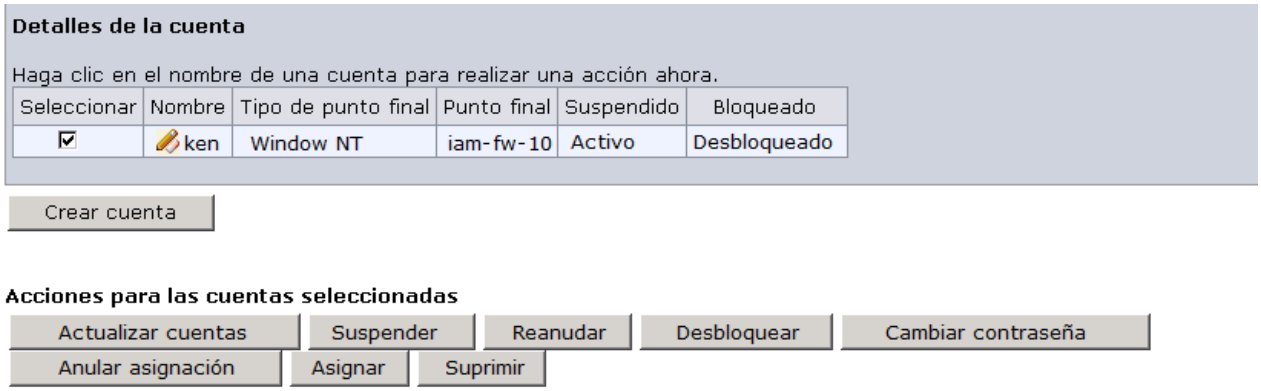
Para editar la definición de una ficha, haga clic en el icono Editar () situado junto al nombre de la ficha.

Más información:

Fichas Cuenta (en la página 66)
Ficha Programar (en la página 68)

Fichas Cuenta

La ficha Cuentas muestra las cuentas de los puntos finales gestionados para aquellos usuarios que tengan asignados roles de aprovisionamiento. Por lo general, esta ficha se agrega a las tareas que permiten ver o modificar un usuario.



Cuando se agrega una ficha Cuentas a la tarea Modificar usuario, los administradores pueden realizar otras acciones en las cuentas del usuario. Por ejemplo:

- Suspender o reanudar una cuenta.
- Desbloquear una cuenta que ha sido bloqueada automáticamente por acceso incorrecto o inapropiado. Por ejemplo, se puede bloquear una cuenta cuando el usuario supera la cantidad permitida de intentos de inicio de sesión fallidos establecida en una política de contraseñas de Identity Manager.
- Cambiar la contraseña de usuario de una o más cuentas
- Asignar o anular la asignación de cuentas a un usuario.

Para obtener detalles sobre otras opciones que se pueden proporcionar en la ficha Cuentas, consulte la ayuda de la Consola de usuario para la ficha Configurar Cuentas.

Requisito para el uso de la ficha Cuentas

Para utilizar la ficha Cuentas, debe configurar Identity Manager con compatibilidad para el aprovisionamiento. Además, el entorno Identity Manager deberá incluir un directorio de aprovisionamiento.

Nota: Para configurar la compatibilidad de aprovisionamiento en un entorno, consulte la *Guía de configuración*.

Campos de la ficha Cuentas

La ficha Cuentas muestra detalles sobre las cuentas que el usuario tiene en los sistemas de los puntos finales.

A continuación, detallamos algunos de los campos más importantes:

- Nombre: el nombre de inicio de sesión, nombre de correo electrónico u otro nombre de la cuenta.
- Tipo de punto final: el tipo de punto final (por ejemplo, un directorio de LDAP) que está asociado a la cuenta.
- Punto final: el punto final específico que está asociado a la cuenta.
- Suspendido: uno de tres estados.
  - Activo aparece si la cuenta está activada.
  - Suspendido aparece si la cuenta está desactivada.
  - Activación pendiente (manual) aparece si no se puede reanudar o suspender. Para reanudar o suspender la cuenta, inicie sesión en el sistema de punto final.
  - Si el estado no se puede recuperar porque no existe comunicación con el punto final, aparecerá como no disponible.
- Bloqueado: muestra si la cuenta está bloqueada. El bloqueo se produce cuando un usuario realiza varios intentos de inicio de sesión en la cuenta con una contraseña incorrecta. Si el estado no se puede recuperar porque no existe comunicación con el punto final, aparecerá como no disponible.

Otras funciones de la ficha Cuentas

Cuando la ficha Cuentas está incluida en una tarea que modifica a un usuario, los administradores que usan esa tarea pueden realizar funciones en las cuentas del usuario. Las funciones disponibles están determinadas por la configuración de la ficha.

Puede seleccionar las funciones que estarán disponibles mediante el uso de la Utilice la opción Modificar la tarea de administración en una tarea que contenga la ficha Cuentas. Puede editar la ficha Cuentas para determinar si funciones tales como Asignar cuenta y Anular asignación de cuenta estarán disponibles en la ficha.

Para obtener más información, consulte la ayuda en línea relativa a la ficha Configurar cuentas.

Ficha Programar

La programación le permite automatizar la ejecución de una tarea en una fecha futura. Si programa una tarea que está asociada a un flujo de trabajo, CA Identity Manager ejecutará todas las tareas según se defina en ese flujo de trabajo. El estado de las tareas programas se puede ver en la página Ver tareas enviadas.

En la página Ver tareas enviadas se puede cancelar una tarea programada que CA Identity Manager aún no haya ejecutado.

Nota: Si se cancela una tarea programada y se vuelve a enviar, la tarea se ejecutará inmediatamente, independientemente del tiempo de ejecución programado.

CA Identity Manager muestra el programador como una ficha especial. Para tener acceso al programador, debe configurar la tarea con la ficha Programar.

Cómo agregar la ficha Programar a una tarea de administración

CA Identity Manager le permite programar las tareas para que se ejecuten en una fecha y hora concretas. Para programar una tarea, debe agregar la ficha Programar a una tarea de administración.

Note: No puede agregar una ficha Programar a todas las tareas de administración de CA Identity Manager. Si no se puede programar la tarea, la ficha de programación no estará disponible en la pantalla Modificar tareas de administración.

Para agregar la ficha Programar a una tarea de administración

1. Seleccione Roles y tareas, Tareas de administración, Modificar tarea de administración.

   Aparece la página Seleccionar tarea de administración.

2. Seleccione Nombre o Categoría en el campo Buscar tareas de administración, introduzca la cadena que desee buscar y haga clic en Buscar.

   CA Identity Manager muestra las tareas de administración que cumplen con los criterios de búsqueda.

3. Seleccione una tarea de administración y, a continuación, haga clic en Seleccionar.

   CA Identity Manager muestra los detalles de tarea de la tarea de administración seleccionada.

4. Haga clic en Fichas.

   Se muestran las fichas que están configuradas para la tarea de administración seleccionada.

5. En el menú desplegable Qué fichas deben aparecer en esta tarea, seleccione Programar, y haga clic en  .

   La ficha Programar se agrega a la lista de fichas que aparecerán en la tarea de administración seleccionada.

6. Haga clic en Enviar.

   La ficha Programar se agrega a la tarea de administración seleccionada.

Vista de campos de la tarea

En la ficha Campos, puede ver los campos que se aplican a la tarea. Estos campos son los creados en las fichas de esta tarea. Para cambiar los campos usados, regrese a la ficha Fichas y seleccione la ficha que desea cambiar.

Una vez que complete la ficha, continúe con el paso siguiente: Asignación de procesos de flujo de trabajo para eventos (en la página 69).

Sin embargo, si el entorno Identity Manager no utiliza flujo de trabajo, puede hacer clic directamente en Enviar. Aparece un mensaje que indica si la tarea se ha completado correctamente. Si ha sido así, puede agregar la tarea a una función, de manera que los miembros de función puedan comenzar a usar la tarea.

Visualización de la utilización de los roles

En la ficha Utilización de los roles, puede ver los roles que incluyen la tarea que está viendo o modificando.

Los propietarios de roles pueden agregar y eliminar tareas de los roles.

Nota: Los roles de administración predeterminados proporcionan una lista de tareas en los roles de administración que se instalan con CA Identity Manager de manera predeterminada.

Asignación de procesos de flujo de trabajo para eventos

Si ha activado flujo de trabajo para el entorno Identity Manager, utilice la ficha Eventos para seleccionar un proceso de flujo de trabajo para todos los eventos que inicie la tarea. El proceso de flujo de trabajo que seleccione, anulará el proceso seleccionado de forma predeterminada en la consola de gestión de Identity Manager.

Para obtener más detalles sobre asignaciones de flujo de trabajo predeterminadas, consulte el capítulo de configuración avanzada de la *Guía de configuración*.

Para finalizar la creación de la tarea, haga clic en Enviar. Aparece un mensaje que indica si la tarea se ha completado correctamente. Si ha sido así, puede agregar la tarea a una función, de manera que los miembros de función puedan comenzar a usar la tarea.

Gestión de un almacén de usuarios de Active Directory

Si Active Directory es el almacén de usuarios, antes de crear tareas de administración, puede ser necesario configurar ciertas funciones de Active Directory.

El atributo sAMAccountName

El atributo sAMAccountName se aplica a usuarios y a grupos. Este atributo es obligatorio y se debe incluir en las pantallas de tarea utilizadas para crear usuarios y grupos.

Nota: Cuando cree usuarios, el valor del atributo sAMAccountName no puede superar los veinte caracteres. Esta limitación no se aplica a los grupos.

Puede escribir un identificador de atributos lógicos personalizado que genere automáticamente un sAMAccountName único al crear un usuario o un grupo. En este caso, puede incluir el atributo sAMAccountName como un campo oculto en las pantallas Crear usuario y Crear grupo.

Para obtener más información, consulte el capítulo Atributos lógicos de la *Guía de programación para Java*.

Tipo de grupo y ámbito

En Active Directory, hay dos tipos de grupos:

- Seguridad: aparece en Listas de control de acceso (ACL, la sigla en inglés), y es donde se definen los permisos para recursos y objetos.
- Distribución: se utiliza para agrupar objetos, como usuarios y grupos. Los grupos de distribución no se pueden utilizar para otorgar privilegios en Active Directory.

Cada tipo de grupo tiene un ámbito que determina lo siguiente:

- Ubicación de miembro: dónde pueden residir los posibles miembros
- Permisos: dónde se puede usar el grupo para privilegios de acceso (si se trata de un grupo de seguridad)
- Pertenencia del grupo a otros grupos: la ubicación de grupos a los que puede pertenecer el grupo

Cada tipo de grupo puede tener uno de los siguientes ámbitos:

Ámbito	Ubicación de miembro	Permisos	Pertenencia del grupo a otros grupos
Universal	Los miembros pueden ser grupos universales, globales y usuarios de cualquier dominio del bosque.	Se puede utilizar para otorgar acceso a cualquier dominio de un bosque.	Pueden ser miembros de local de dominio y grupos universales de cualquier dominio del bosque.
Global	Los miembros pueden ser grupos globales y usuarios ubicados en el mismo dominio que el grupo.	Se puede utilizar para otorgar acceso a cualquier dominio de un bosque.	Pueden ser miembros de grupos globales, local de dominio y universales en cualquier dominio del bosque.
Local de dominio	Los miembros pueden ser grupos universales, globales y usuarios de cualquier dominio del bosque. Los miembros también pueden ser grupos de local de dominio del mismo dominio.	Sólo se puede utilizar para otorgar acceso al dominio en el que reside el grupo.	Sólo puede ser miembro de otros grupos de local de dominio dentro del dominio.

Tipo de grupo y ámbito no son atributos obligatorios; sin embargo, si no se especifican, Active Directory creará un grupo de seguridad con ámbito global.

Para crear grupos de otro tipo, se puede crear un identificador de atributos lógicos personalizado. Consulte el capítulo sobre Atributos lógicos en la *Guía de programación para Java*.

Una vez que haya configurado estas funciones de Active Directory, siga con el próximo paso: Creación de una tarea administrativa.

Tareas externas para las funciones de la aplicación

Una tarea externa realiza los siguientes pasos:

- Permite al administrador realizar una función en otra aplicación que no sea CA Identity Manager desde la Consola de usuario.
- Opcionalmente, pasa la información a la aplicación para generar tareas específicas del usuario, grupo o de la organización.

Por ejemplo, una tarea externa puede transferir información acerca de una organización a una aplicación que genera órdenes de compra. El administrador que realiza la tarea puede ver los pedidos de compra abiertos de la organización desde la Consola de usuario.

Se pueden ver las tareas externas si se abre la aplicación en una nueva ventana del explorador o si las visualiza como fichas en una tarea de administración de CA Identity Manager.

Hay disponibles dos fichas para las tareas externas. Estas fichas se configuran de la misma manera; sin embargo, funcionan de forma distinta.

- La ficha Externo es una ficha visual, que significa que la tarea muestra el contenido de la dirección URL dentro de una ficha.
- Dirección URL externa es una ficha no visual, lo que significa que la tarea vuelve a dirigir a la dirección URL introducida.

Ficha Externa

Se puede agregar una ficha externa a cualquier tarea de creación, consulta o modificación para convertirla en una tarea externa. Por ejemplo, si se agrega una ficha Externa a una tarea Crear usuario, la ficha aparece en esa tarea.

Características de la ficha Externa:

- No se genera ningún evento para una tarea externa.
- Opcionalmente, se pueden utilizar objetos gestionados.

- En el campo Dirección URL externa, se puede especificar la dirección de una aplicación de estas formas:
  - Una dirección completa con el nombre de dominio totalmente cualificado, por ejemplo:

    http://servidor1.miempresa.org/informe/verInformeUsuario
  - Una ruta relativa, por ejemplo:

    /informe/verInformeUsuario

    Si especifica una ruta relativa, CA Identity Manager adjunta automáticamente el nombre de dominio totalmente cualificado del servidor en el que está instalado CA Identity Manager.
- Los atributos se configuran para que pasen a la aplicación en la ficha Perfil.
- El DN del administrador o el nombre de la tarea se pueden incluir en la dirección URL o excluir de ella.

Ficha Dirección URL externa

Se puede agregar una ficha Dirección URL externa a una tarea de visualización, como Ver usuario. Al utilizar la tarea Ver usuario, se le redirige al sitio web identificado mediante la dirección URL. No se muestra ninguna otra ficha.

Características de la ficha Dirección URL externa:

- La ficha Dirección URL externa debe ser la única ficha de la tarea. Si hay otras fichas asociadas a la misma tarea, la ficha Externa no redirigirá a los usuarios a la dirección URL especificada.
- La tarea puede generar eventos que se pueden auditar.
- En el campo Dirección URL externa, se puede especificar la dirección de una aplicación de estas formas:
  - Una dirección completa con el nombre de dominio totalmente cualificado, por ejemplo:

    http://servidor1.miempresa.org/informe/verInformeUsuario
  - Una ruta relativa, por ejemplo:

    /informe/verInformeUsuario

    Si especifica una ruta relativa, CA Identity Manager adjunta automáticamente el nombre de dominio totalmente cualificado del servidor en el que está instalado CA Identity Manager.

- Opcionalmente, se pueden utilizar objetos gestionados.
- Se pueden configurar atributos para pasarlos a la dirección URL.

  Especifique la dirección URL de la aplicación que desee iniciar e incluya los atributos que se deban transferir a la aplicación.
- El DN del administrador o el nombre de la tarea se pueden incluir en la dirección URL o excluir de ella.

Componentes avanzados de la tarea

Los componentes avanzados de la tarea permiten especificar el procesamiento personalizado para una tarea:

- Validación en el nivel de tareas: valida un valor de atributo con respecto a otros atributos de la tarea. Por ejemplo, se puede validar que el código de área en un número de teléfono proporcionado por el usuario sea adecuado para la ciudad y el estado del usuario.
- Los identificadores de tareas lógicas del negocio (en la página 74) realizan la lógica del negocio personalizada antes de enviar una tarea de CA Identity Manager para su procesamiento. Normalmente, la lógica del negocio personalizada valida los datos. Por ejemplo, un identificador de tareas lógicas del negocio puede comprobar el límite de pertenencia a un grupo antes de que CA Identity Manager agregue un nuevo miembro al grupo. Cuando se alcanza el límite de pertenencia a un grupo, el identificador de tareas lógicas del negocio mostrará un mensaje que informa al administrador de grupos de que no se ha podido agregar el miembro nuevo.

Creación de Identificadores de tareas lógicas del negocio

Un nombre de clase totalmente cualificado de identificador de tareas lógicas del negocio se define de la siguiente manera:

1. Cree o modifique una tarea de administración.
2. En la ficha Perfil de administrador, haga clic en Identificadores de tareas lógicas del negocio.

   Aparece la pantalla Identificadores de tareas lógicas del negocio. En esta pantalla se muestran los identificadores de tareas lógicas del negocio asignados a la tarea. Identity Manager ejecuta los identificadores en el orden en que aparecen en la lista.
3. Haga clic en Agregar.

   Aparece la pantalla Detalle del identificador de tareas lógicas del negocio.

Utilice la pantalla Detalle del identificador de tareas lógicas del negocio para definir la siguiente información para el identificador que va a asignar a la tarea:

Nombre

El nombre que va a asignar al identificador de tareas lógicas del negocio.

Descripción

Una descripción opcional del identificador de tareas lógicas del negocio.

Clase de Java

El nombre de clase del identificador totalmente cualificado, si el identificador de tareas lógicas del negocio se implementa en Java, por ejemplo:

com.miempresa.MiJavaBLTH

Identity Manager espera que el archivo de clase se ubique en el directorio raíz designado para archivos de clase de Java personalizados. Para obtener información sobre cómo implementar archivos de clase de Java, consulte la *Guía de programación para Java*.

Nombre de archivo de JavaScript

Especifique el nombre del archivo en este campo si el identificador de tareas lógicas del negocio se implementa en JavaScript, y el código JavaScript está contenido en un archivo. Por ejemplo, sería conveniente que detallase el JavaScript en un archivo si varias pantallas de tareas van a utilizar el identificador de tareas lógicas del negocio.

Identity Manager espera que el archivo se ubique en el directorio raíz designado para archivos de clase de JavaScript personalizados. Para obtener información sobre cómo implementar archivos JavaScript, consulte la *Guía de programación para Java*.

Si almacena el archivo en un subdirectorio de la raíz, incluya el nombre del subdirectorio al especificar el nombre del archivo JavaScript, por ejemplo:

JavaScriptSubDir\MiJavaScriptBLTH.js

La dirección de las barras inclinadas debe ser la adecuada para la plataforma en la que se implementa el archivo JavaScript.

JavaScript

Para implementar un identificador de tareas lógicas del negocio de JavaScript, puede escribir el código JavaScript completo en este campo en lugar de hacerlo en un archivo. Por ejemplo, si la secuencia de comandos es muy breve o si no se va a utilizar con otras pantallas de tareas, es conveniente que detalle el JavaScript en este campo.

Propiedad y valor

En las implementaciones de Java, estos campos son pares nombre/valor opcionales de datos. Se transmiten en el método init() del identificador de tareas lógicas del negocio para ser utilizados del modo en que lo necesite la lógica del negocio del identificador.

Para agregar una propiedad definida por el usuario, especifique un nombre y valor de propiedad y, a continuación, haga clic en Agregar.

Nota: Si agrega un identificador de tareas lógicas del negocio de Java, debe reiniciar el servidor de aplicaciones para cargar el identificador.

Eventos y tareas de administración

Las tareas de administración incluyen *eventos*, acciones que realiza CA Identity Manager para completar la tarea. Una tarea puede incluir varios eventos. Por ejemplo, la tarea Crear usuario puede incluir eventos que crean el perfil del usuario, agregan el usuario a un grupo y asignan funciones.

CA Identity Manager audita eventos, impone reglas del negocio específicas del cliente asociadas con eventos y, cuando los eventos se asignan a los procesos de flujo de trabajo, se requiere la aprobación de los eventos.

Si se generan varios eventos para una tarea y estos eventos están asignados a procesos del flujo de trabajo, todos los procesos de flujo de trabajo se deben finalizar antes de que CA Identity Manager pueda completar la tarea.

Eventos principales y secundarios

Generalmente, los eventos son independientes de otros eventos. No obstante, algunas tareas están asociadas con un evento primario y uno o más eventos secundarios:

- Un error en un evento primario tiene como resultado el rechazo automático de los eventos secundarios. Por ejemplo, si se produce un error en CreateUserEvent, no será necesario que AddToGroupEvent tenga lugar para el usuario. También tendrá como resultado la cancelación de la tarea asociada.
- Un error en un evento secundario no influye en el error o el éxito de otros eventos que se ejecuten para la tarea, ni en la ejecución de la tarea. Por ejemplo, en una tarea Crear usuario, se puede rechazar AddToGroupEvent, lo que significa que el nuevo usuario no se puede agregar a un grupo determinado. De todos modos, se podrá crear el usuario (CreateUserEvent) y se podrá asignar a roles de aprovisionamiento (AssignProvisioningRoleEvent), e incluso agregar a otros grupos.

Visualización de los eventos de una tarea

En la Consola de usuario de CA Identity Manager, puede ver los eventos asociados con una tarea.

Para ver los eventos de una tarea

1. Seleccione Roles y tareas, Ver tarea de administración en la Consola de usuario.
2. Busque y seleccione la tarea apropiada.
3. Seleccione la ficha Eventos.

   CA Identity Manager mostrará los eventos asociados con la tarea actual.

Eventos generados para perfiles no modificados

Los objetos de usuario, grupo y organización contienen un conjunto de atributos físicos que se almacenan en el directorio del usuario. Si un atributo físico de uno de estos objetos se modifica en una ficha de perfil, Identity Manager genera un evento Modificar... una vez que el usuario envía la tarea. Por ejemplo, si un atributo *Cargo* se modifica en una ficha Perfil de usuario, Identity Manager genera el evento ModifyUserEvent.

Si un objeto de usuario, grupo u organización se representa en una ficha de perfil pero no se ha modificado ningún atributo físico, cuando el usuario haga clic en Enviar, Identity Manager no generará ningún evento Modificar.... En su lugar, se generará el evento Ver... correspondiente, como se indica a continuación:

- Se generará ViewUserEvent en lugar de ModifyUserEvent.
- Se generará ViewGroupEvent en lugar de ModifyGroupEvent.
- Se generará ViewOrganizationEvent en lugar de ModifyOrganizationEvent.

Procesamiento de tareas de administración

El tiempo necesario para procesar una tarea depende de los pasos que ésta implique. Cuando se envía una tarea para el procesamiento, CA Identity Manager realiza los siguientes pasos:

1. CA Identity Manager valida los datos que se envían.

   Esto se denomina *fase sincrónica*.

2. Si la tarea requiere aprobación, CA Identity Manager envía la tarea al motor de flujo de trabajo.

   a. El motor de flujo de trabajo determina los aprobadores y coloca la tarea de aprobación en las listas de trabajo de los mismos.

   b. De forma opcional, CA Identity Manager enviará un correo electrónico para notificar a los aprobadores de la presencia del elemento de trabajo pendiente.

   c. Un aprobador reserva el elemento de trabajo (lo que elimina dicho elemento de las listas de trabajo de los demás) y lo aprueba o rechaza.

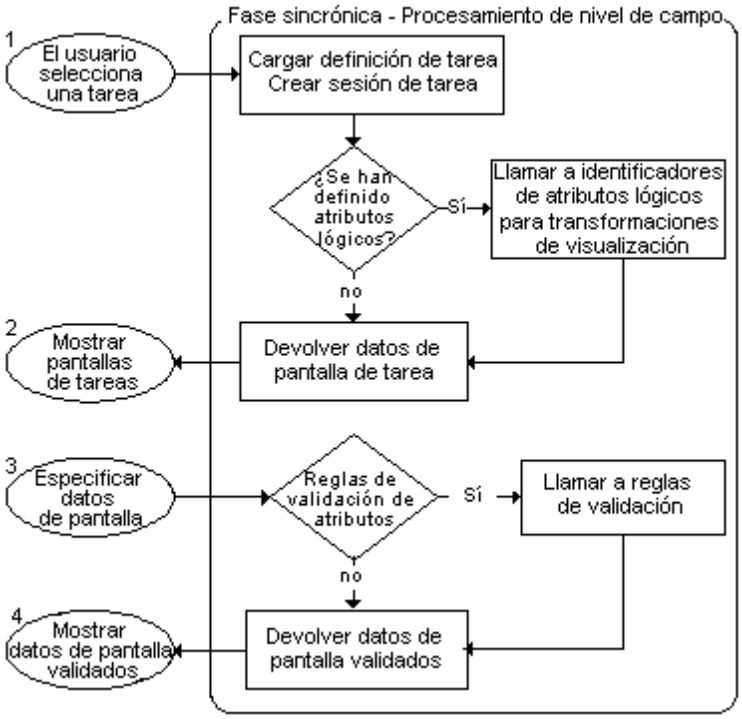
   d. De forma opcional, CA Identity Manager envía un correo electrónico donde se notifica a los usuarios involucrados sobre el estado de la tarea.

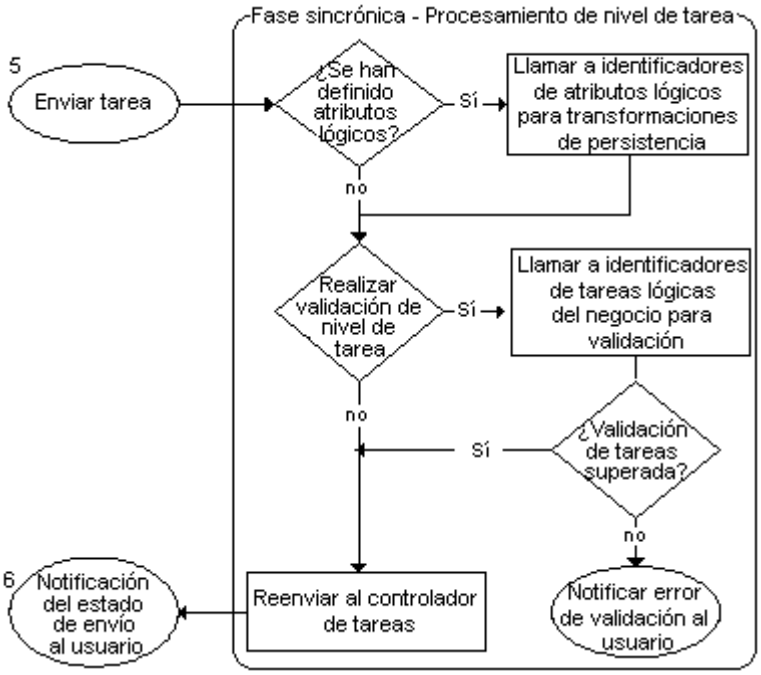
   Esto se denomina *fase asincrónica*.

3. CA Identity Manager lleva a cabo la tarea, siempre que esta no haya sido rechazada.

Procesamiento de fase sincrónica

Durante la fase sincrónica, Identity Manager puede transformar y validar los datos que los usuarios introducen en las pantallas de tareas y puede imponer lógica del negocio a esos datos antes de que la tarea se envíe para procesamiento. En el diagrama siguiente se proporciona una descripción de alto nivel de lo que ocurre durante esta fase.

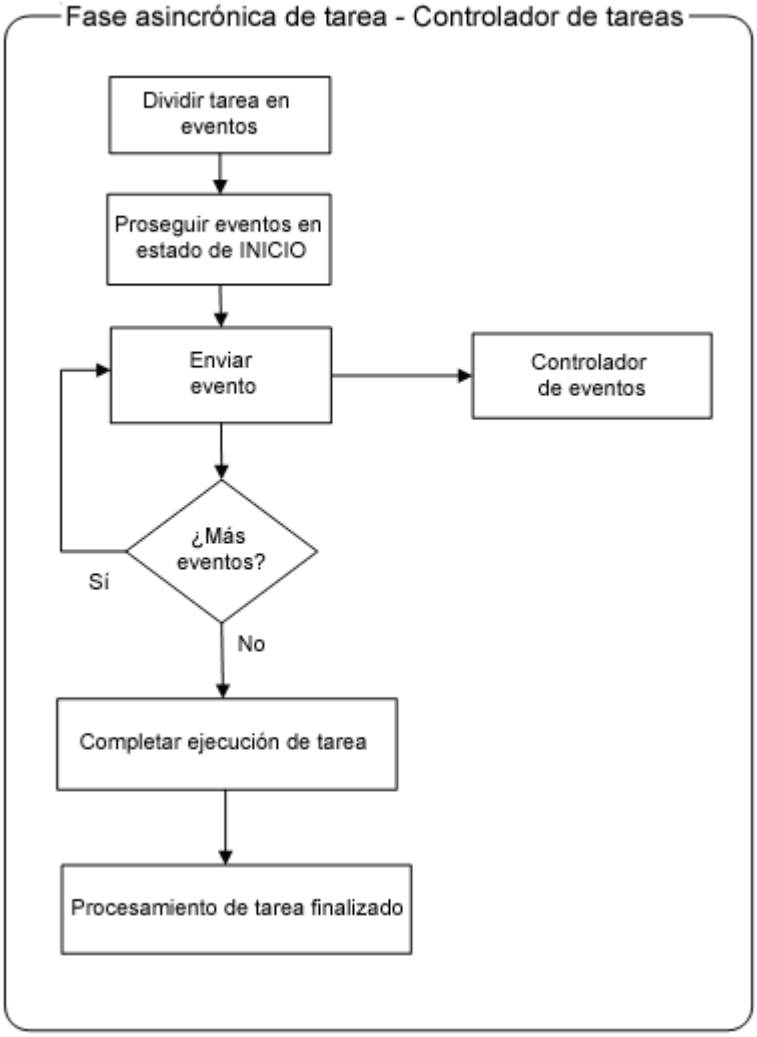




Procesamiento de fase asincrónica

Al finalizar la fase sincrónica, la tarea pasa a la fase asincrónica para ejecución. Durante esta fase, una tarea genera uno o más eventos. Estos eventos pueden ser definidos por el usuario, como crear un perfil de usuario o agregar un usuario a un grupo, o generados por el sistema, como escribir información en el registro de auditoría.

El controlador de tareas, un componente del servidor de Identity Manager, es responsable del ciclo de vida de una tarea y de sus eventos, tal y como se muestra en la siguiente ilustración:



En la mayoría de los eventos, el ciclo de vida, la ejecución y las acciones son independientes de cualquier otro evento. (La creación de tareas requiere que el evento de creación del objeto primario se ejecute antes de cualquier evento secundario.)

Por lo general, un evento realiza una transición por los siguientes estados:

- Inicio
- Pendiente
- Aprobado
- Ejecutar
- Completado
- Enviar

Nota: Identity Manager proporciona enlaces, denominados EventListeners, que "escuchan" un evento concreto o un grupo de eventos. Cuando se produce un evento, el agente de escucha de los eventos realiza una lógica del negocio personalizada apropiada para el evento y el estado actual del evento. Puede utilizar la API del agente de escucha para escribir agentes de escucha de eventos personalizados. Para obtener más información, consulte la *Programming Guide for Java*.

Imágenes para las tareas de administración

Se pueden crear imágenes con el fin de utilizarlas para las tareas de administración que se agreguen en la página principal.

Capítulo 4: Usuarios

Esta sección contiene los siguientes temas:

Creación de usuarios

Los perfiles de usuario permiten a los administradores gestionar la información de los usuarios; los privilegios, las aplicaciones y el acceso a los servicios; además de conceder la autogestión de los usuarios para sus propias cuentas y servicios. La creación de perfiles de usuario es una tarea común para un administrador del sistema.

Al crear y configurar un usuario, tenga en cuenta los siguientes elementos de la cuenta de usuario:

Tareas de autoservicio: los perfiles de usuario se configuran de forma predeterminada para conceder acceso al usuario a ciertas tareas de autoservicio, como cambiar su contraseña e información del perfil. El administrador del sistema con las tareas adecuadas puede modificar las tareas que se conceden a un usuario de forma predeterminada.

Grupos: los grupos simplifican gestión de roles. Por ejemplo, un administrador del sistema con las tareas adecuadas puede configurar varios roles para que el sistema asigne automáticamente a un usuario que se agrega como un miembro de un grupo.

Roles de administrador: los roles de administrador definen las tareas que un usuario puede realizar en la Consola de usuario. Por ejemplo, una tarea puede permitir a un usuario la modificación de información de una cuenta de usuario, como la dirección o el cargo. Otra tarea puede permitir a un usuario la administración de tareas, como por ejemplo, conceder a un usuario la pertenencia a un grupo. Cuando se asigna un rol de administrador a un usuario, el usuario puede realizar las tareas asociadas con el rol.

Cuentas de punto final y roles de aprovisionamiento: las cuentas que existen en otros sistemas se denominan Cuentas de punto final. Se pueden asignar cuentas en puntos finales a los usuarios de CA CloudMinder a través de los roles de aprovisionamiento. Por ejemplo, un usuario necesita una cuenta de Exchange para el correo electrónico, una cuenta de Oracle para el acceso a las bases de datos y una cuenta de Active Directory para utilizar un sistema de Windows. Cuando se asigna un rol de aprovisionamiento a un usuario, el usuario recibe las cuentas de punto final que determina el rol de aprovisionamiento.

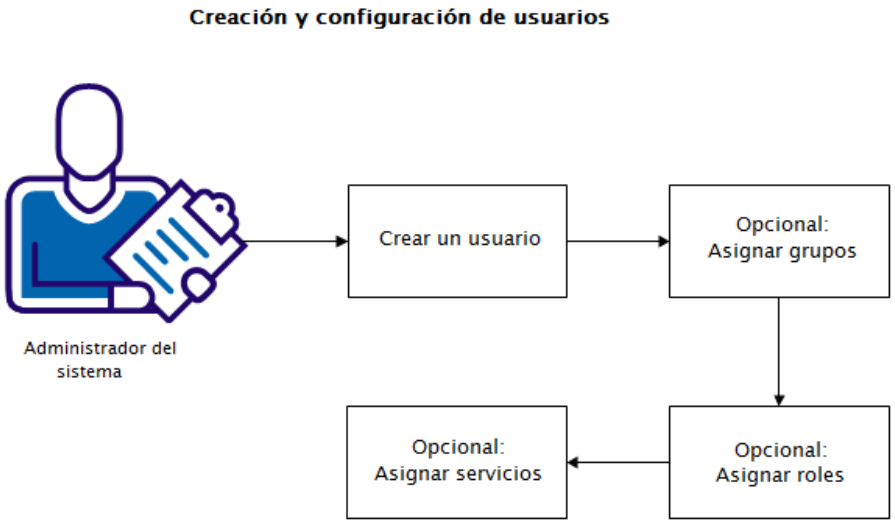
Roles de acceso: los roles de acceso proporcionan una forma adicional de proporcionar autorizaciones en CA Identity Manager u otra aplicación. Por ejemplo, se pueden utilizar los roles de acceso para realizar las siguientes tareas:

- Proporcionar acceso indirecto a un atributo de usuario
- Crear expresiones complejas
- Establecer un atributo en un perfil de usuario, que otra aplicación utiliza para determinar las autorizaciones

Servicios: Los servicios permiten combinar la elección de tareas de usuario, roles, grupos y atributos en un solo paquete. Se puede gestionar este paquete de privilegios como si fuera 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 e información agregada a los perfiles de cuentas de usuarios. Cuando se asigna un servicio a un usuario, el usuario recibe el conjunto entero de roles, tareas, grupos y atributos de la cuenta que determina el servicio.

Políticas de contraseñas: estas políticas gestionan las contraseñas de los usuarios mediante la aplicación de reglas y restricciones que controlan la caducidad, la composición y el uso de las contraseñas. Si un administrador del sistema crea políticas de contraseñas para el entorno, estas políticas se aplicarán automáticamente a los nuevos usuarios que coincidan con una o más reglas de políticas de contraseñas. Un administrador del sistema puede modificar las políticas de contraseñas con las tareas adecuadas.

El diagrama siguiente muestra la información sobre los pasos que deben realizarse a la hora de crear y configurar un usuario.



En los temas siguientes se explica la creación de usuarios en profundidad y de qué manera deben configurarse.

1. Creación de un usuario.
2. Asignación de grupos (si es necesario (en la página 86)).
3. Asignación de roles a un usuario (si es necesario).
4. Asignación de servicios (en la página 87). (si es necesario)

Creación del perfil de usuario

Utilice este procedimiento para crear un perfil de usuario. En función de cómo se configure la tarea Crear usuario, también se podrá utilizar esta tarea para definir elementos de perfil adicionales. Se puede agregar un usuario a un grupo o se puede convertir en miembro de un rol de administrador o de aprovisionamiento.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario con las tareas de gestión de usuarios.

   El rol Gestor de usuarios predeterminado concede las tareas adecuadas.

2. Seleccione Tareas, Usuarios, Gestionar usuarios, Crear usuario.

   Se abrirá la tarea Crear usuario.

3. Rellene los campos sobre la información de perfiles de usuarios, si es necesario.
4. Haga clic en Siguiente.
5. Rellene los campos en las otras fichas de la tarea, si es necesario.

   Por ejemplo, agregue el usuario a un grupo o asigne un rol de administrador, rol de aprovisionamiento o servicio al usuario, si se encuentran disponibles estas opciones.
6. Haga clic en Finalizar.

   Se crea el usuario.

Asignación de un grupo a un usuario

El usuario tiene la capacidad de convertir a otro usuario en miembro de un grupo.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario con las tareas de gestión de usuarios.
2. Seleccione Tareas, Grupos y Modificar miembros del grupo.

   Aparece una lista de los grupos que se pueden gestionar.
3. Seleccione un grupo y haga clic en Seleccionar.

   Aparece la lista de usuarios que se asignan al grupo.
4. Haga clic en Agregar usuario.
5. Busque un usuario al cual desee asignarle el grupo.

   Para mostrar una lista de todos los usuarios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.
6. Seleccione un usuario y haga clic en Seleccionar.

   Aparece una lista actualizada de los usuarios que se asignan al grupo.
7. Haga clic en Enviar.

   El usuario especificado se convierte en miembro del grupo.

Asignación de roles a un usuario

Se pueden asignar roles de aprovisionamiento a un usuario individual.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario con las tareas Modificar miembros/administradores del rol de aprovisionamiento.
2. Seleccione Roles y tareas.
3. Seleccione una de las tareas siguientes:
   - Roles de administrador, Modificar miembros/administradores del rol de administrador
   - Roles de aprovisionamiento, Modificar miembros/administradores del rol de aprovisionamiento
   - Roles de acceso, Modificar miembros/administradores del rol de acceso

   Aparece una pantalla de búsqueda.
4. Seleccione el rol que intenta asignar al usuario.

   Aparece la ficha Pertenencia a.
5. Haga clic en Agregar usuario.
6. Busque un usuario al cual desee asignarle el rol.

   Para mostrar una lista de todos los usuarios para los cuales tiene tareas administrativas, haga clic en Buscar sin modificar los criterios de búsqueda.
7. Seleccione un usuario y haga clic en Seleccionar.
8. Haga clic en Enviar.

   Los roles especificados se asignarán al usuario.

Asignación de un servicio a un usuario

Se puede asignar un servicio directamente a un usuario individual. Este usuario se convierte en *miembro* del servicio.

Siga estos pasos:

1. Vaya a Servicios, Solicitar y ver acceso.

   Aparece una lista de servicios que se pueden administrar.
2. Seleccione el servicio que desee asignar al usuario y haga clic en Seleccionar.

   Aparecerá una lista de usuarios asignados al servicio.
3. Haga clic en Solicitar acceso.
4. Busque un usuario al cual desee asignarle el servicio.

   Para mostrar una lista de todos los usuarios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

5. Seleccione un usuario y haga clic en Seleccionar.

   Aparecerá una lista actualizada de los usuarios asignados al servicio.

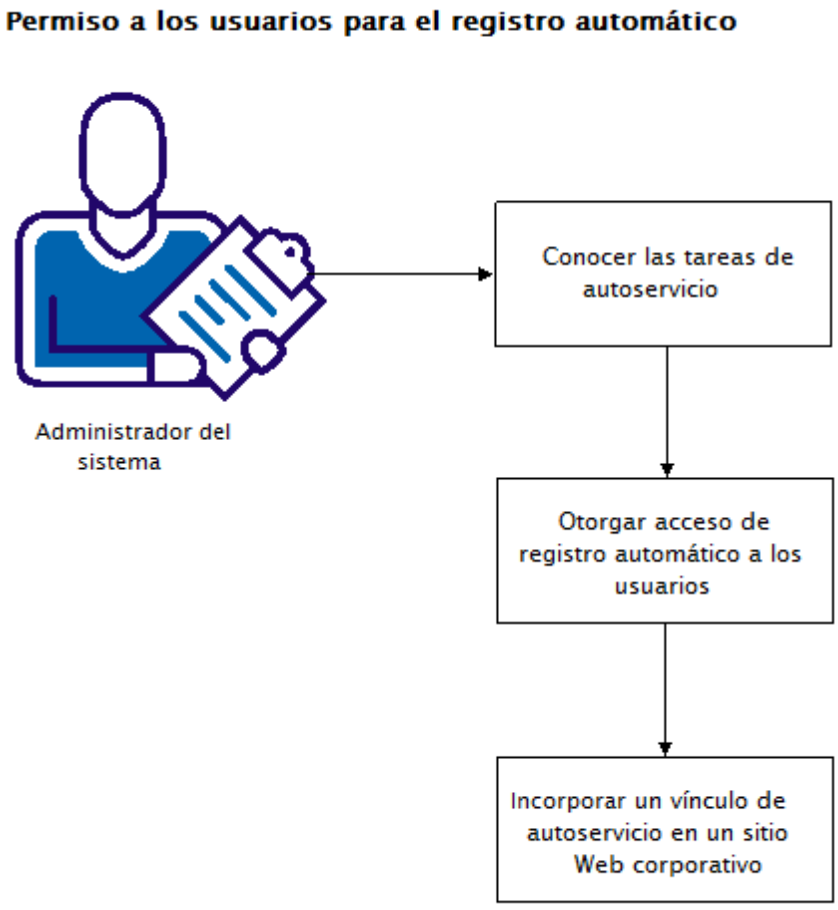
6. Haga clic en Guardar cambios.

   El usuario recibe el servicio especificado. El usuario recibe todas las aplicaciones, los roles, los grupos y los atributos incluidos en el servicio.

Permiso a los usuarios para el registro automático

Las tareas de autoservicio permiten a los usuarios gestionar su propio entorno. La tarea de registro automático permite a los usuarios crear su propio perfil y cuenta de usuario desde una Consola de usuario disponible públicamente. Por ejemplo, Bentley Cola permite a los empleados y clientes nuevos la creación de sus propios perfiles y cuentas de usuario a través de un vínculo incrustado en el sitio Web corporativo de Bentley Cola.

El diagrama siguiente muestra la información sobre los pasos que deben realizarse a la hora de permitir el registro automático a los usuarios.



En los temas siguientes se proporcionan detalles sobre cómo conceder acceso de registro automático a los usuarios.

1. Conocimiento de las tareas de autoservicio. (en la página 90)
2. Cómo otorgar acceso de registro automático a los usuarios (en la página 91).
3. Incrustación de un vínculo de autoservicio en un sitio Web corporativo (en la página 91).

Tareas de autoservicio

Las tareas de autoservicio son acciones que los usuarios pueden llevar a cabo, normalmente a través de la Consola de usuario, para gestionar sus propios perfiles. Las cuentas de usuario se configuran de forma predeterminada para conceder el acceso al usuario a ciertas tareas de autoservicio, como cambiar su contraseña e información del perfil. Un administrador del sistema con privilegios adecuados puede modificar que se concedan ciertas tareas de autoservicio a un usuario de forma predeterminada.

Estas tareas se dividen en dos tipos:

- Tareas públicas: tareas a las que los usuarios pueden acceder sin especificar credenciales de inicio de sesión. Ejemplos de tareas públicas son las tareas de autorregistro, contraseña olvidada e identificador de usuario olvidado.
- Tareas protegidas: tareas para las que los usuarios deben especificar credenciales válidas. Los ejemplos incluyen tareas para cambiar las contraseñas o la información del perfil.

La tabla siguiente enumera las tareas de autoservicio predeterminadas.

Tipo de tarea	Tareas
Tarea pública	■ Autorregistro: permite a los usuarios registrarse en un sitio Web corporativo. ■ Restablecimiento de la contraseña olvidada: permite a los usuarios restablecer una contraseña olvidada. ■ Contraseña olvidada: muestra una contraseña temporal que los usuarios pueden utilizar para iniciar sesión en CA Identity Manager. Cuando los usuarios inician sesión, se les solicita que introduzcan una nueva contraseña. ■ ID de usuario olvidado: recupera o restablece un identificador de usuario olvidado.
Tarea protegida	■ Solicitar y ver acceso: permite a los usuarios solicitar acceso y eliminar servicios. ■ Cambiar Mi contraseña: permite a los usuarios restablecer sus contraseñas. ■ Modificar Mi perfil: mantiene la información del perfil, como por ejemplo la dirección y el número de teléfono. ■ Modificar Mis grupos: permite a los usuarios suscribirse a grupos. ■ Ver Mis funciones: muestra las funciones del usuario. ■ Ver Mis tareas enviadas: muestra las tareas de CA Identity Manager que ha iniciado el usuario.

Acceso a las tareas de autoservicio

Una vez se han configurado las tareas de autoservicio para el entorno, se pueden agregar direcciones URL para las mismas a un sitio Web corporativo.

Las direcciones URL para las tareas de autoservicio tienen el siguiente formato:

https://*dominio*/iam/im/*alias_público*/ui7/index.jsp?task.tag=*etiqueta_tarea*

donde:

- *dominio* es el nombre de dominio completamente cualificado del servidor Web en el entorno donde está ejecutándose CA CloudMinder.
- *alias_público* es el alias público del entorno. El administrador del sistema define el alias público cuando se crea el entorno.
- *etiqueta_tarea* es el identificador único de la tarea.

  La etiqueta de la tarea Restablecimiento de la contraseña olvidada es ForgottenPasswordReset.

  https://*dominio*/iam/im/*alias_público*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  Para la tarea ID de usuario olvidado, la etiqueta de la tarea es ForgottenUserID:

  https://*dominio*/iam/im/*alias_público*/ui7/index.jsp?task.tag=ForgottenUserID

Incrustación de un vínculo de autoservicio en un sitio Web corporativo

Para permitir el acceso a una tarea de autoservicio pública desde un sitio Web corporativo, se puede agregar un vínculo a cualquier página Web. Cuando un usuario hace clic en el vínculo, se abre una pantalla de la tarea. Cuando el usuario finaliza la tarea, se le redirige a la Consola de usuario de forma predeterminada.

Para cambiar la página a la cual se redirigen los usuarios, se puede añadir task.RedirectURL a la dirección URL asociada con el vínculo como se muestra a continuación:

<A
href="http://*dominio*/iam/im/*alias_público*/ui7/index.jsp?task.tag=*etiqueta_tarea*&task.RedirectURL=http://*dominio*/*URL_redirigida*">*texto del vínculo*</A>

domain

El nombre de dominio totalmente cualificado del servidor web en el entorno donde está en ejecución CA Identity Manager.

public_alias

Una cadena única que se agrega a la dirección URL para obtener acceso a las tareas públicas.

Las tareas públicas son tareas de autoservicio, como las tareas de contraseña olvidada o registro automático. Los usuarios no necesitan iniciar sesión para acceder a las tareas públicas.

Nota: Para obtener más información acerca de los alias y las tareas públicas, consulte la *Guía de configuración*.

tasktag

El único identificador de la tarea. Para determinar la etiqueta de la tarea, utilice Modificar la tarea de administración para ver el perfil de la tarea.

redirect_URL

La dirección URL a la cual se dirigen los usuarios después de enviar la tarea.

Por ejemplo, se puede redirigir a los usuarios a la página Bienvenida después de realizar el registro automático.

link text

El texto en el cual hacen clic los usuarios para acceder a la URL de destino.

Por ejemplo, una compañía puede agregar un vínculo que permite a los usuarios restablecer una contraseña olvidada y que los dirige, a continuación, a la página Bienvenida.

El HTML siguiente representa un ejemplo de texto del vínculo:

<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/ welcome.html">Reset My Password</A>

Para que los usuarios vuelvan a la página en la cual han accedido a la tarea de autoservicio, se debe especificar RefererURL como el valor de la etiqueta task.RedirectURL como se muestra a continuación:

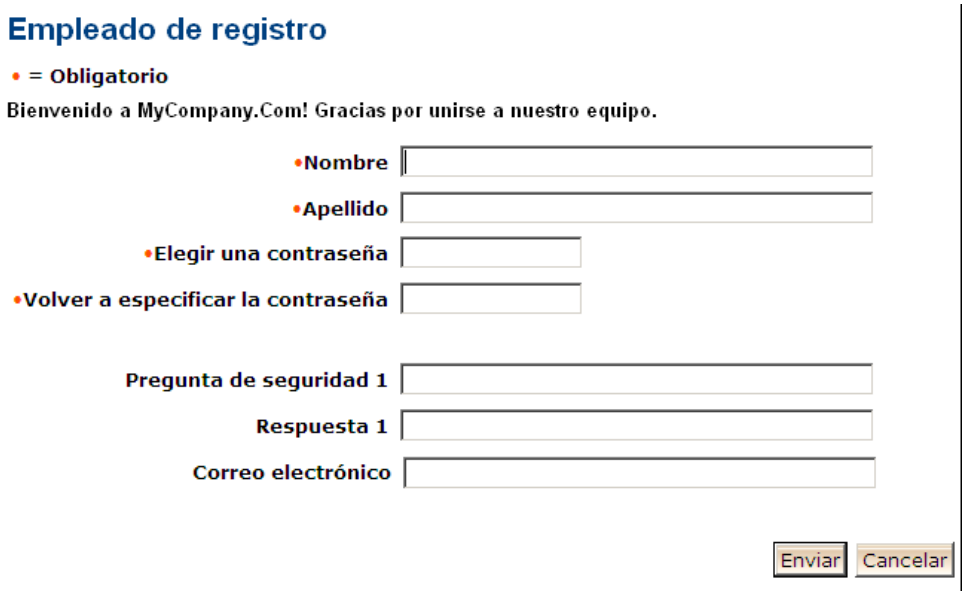
<A href="http://*dominio*/iam/im/*alias_público*/ui7/index.jsp?task.tag=*etiqueta_tarea*&task.RedirectURL=RefererURL</A>

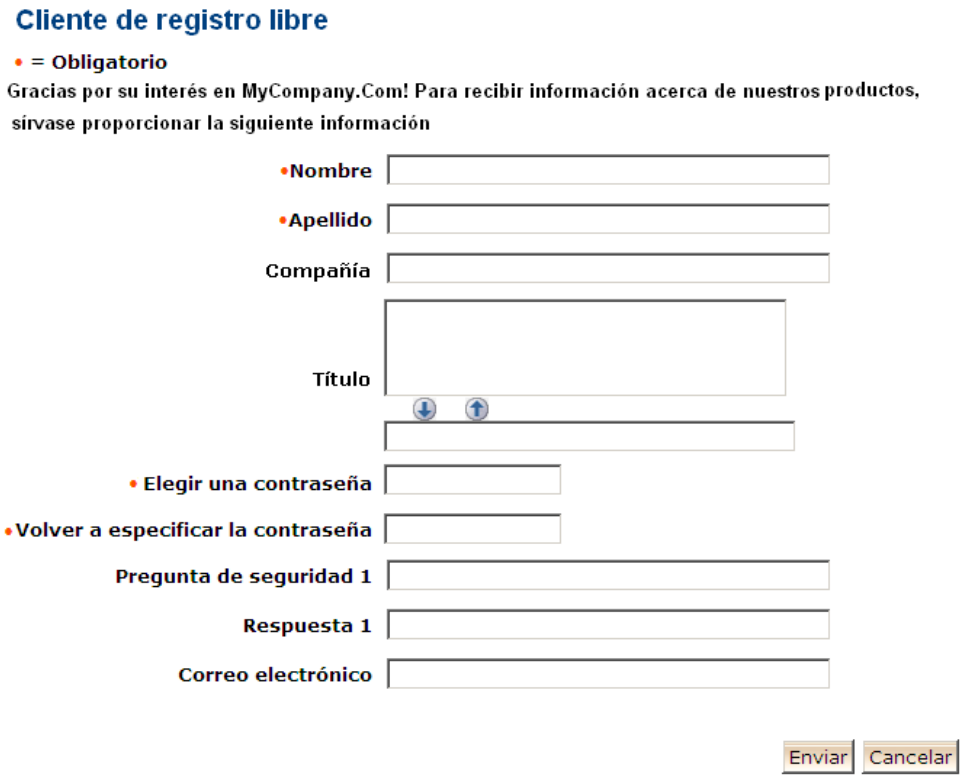
Configuración de varias tareas de autoservicio

Es posible crear varias tareas de autoservicio para diferentes tipos de usuarios. Por ejemplo, puede crear una tarea para registrar nuevos empleados y otra tarea para registrar clientes. Mediante diferentes tareas de autorregistro, se puede:

- Recopilar distintos tipos de información.
- Registrar usuarios en distintas organizaciones.
- Redirigir a los usuarios a páginas de cierre de sesión diferentes después de que se registren.
- Utilizar marcas diferentes.

Las siguientes figuras muestran la tarea de autorregistro para nuevos empleados y clientes, respectivamente.





Para configurar varias tareas de autoservicio del mismo tipo, especifique una etiqueta única al crear la tarea. El campo Etiqueta se ubica en la pantalla Configurar perfil de la tarea.

Al agregar el vínculo para que la tarea acceda a un sitio Web, se añade la etiqueta de la tarea y se crea una URL única.

Por ejemplo, se pueden crear dos tareas del siguiente modo:

Tarea	Etiqueta	URL
Registrar como un empleado nuevo	autorregistro_empleado	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_employee
Registrar como un cliente	autorregistro_cliente	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_customer

Restricción de acceso a la función de autogestor

De manera predeterminada, el rol de autogestor, que permite a los usuarios gestionar su información de perfil y ver sus funciones y tareas enviadas, se asigna a todos los usuarios.

Para asignar la función de autogestor a un subconjunto de usuarios, suprima la política de miembros existente y cree una nueva política de la manera descrita en Definición de políticas de miembros para una función de administración.

Capítulo 5: Gestión de contraseñas

Esta sección contiene los siguientes temas:

Gestión de contraseñas en Identity Manager

Identity Manager incluye varias funciones para gestionar las contraseñas de los usuarios:

- Políticas de contraseñas: estas políticas gestionan las contraseñas de los usuarios imponiendo reglas y restricciones que rigen el vencimiento, la composición y el uso de las contraseñas.
- Gestores de contraseñas: los administradores que tienen la función Gestor de contraseñas pueden restablecer una contraseña cuando el usuario llama al Departamento de ayuda.
- Gestión de las contraseñas de autoservicio: Identity Manager incluye varias tareas de autoservicio que permiten a los usuarios gestionar sus propias contraseñas. Estas tareas incluyen:
  - Autorregistro: los usuarios especifican una contraseña cuando se registran en un sitio Web corporativo.
  - Cambiar Mi contraseña: los usuarios pueden modificar sus contraseñas sin ayuda del personal de TI o del Departamento de ayuda.
  - Contraseña olvidada: los usuarios pueden restablecer o recuperar una contraseña olvidada después de que Identity Manager verifique su identidad.
  - Restablecer contraseña o desbloquear cuenta: los usuarios pueden restablecer o recuperar una contraseña olvidada o desbloquear una cuenta de Windows en el sistema en el que accedan a Identity Manager.
  - ID de usuario olvidado: los usuarios pueden recuperar un ID de usuario olvidado después de que Identity Manager verifique su identidad.

- Sincronización de contraseñas en cuentas de extremo: los cambios de las contraseñas se sincronizan en Identity Manager, el servidor de aprovisionamiento y en los sistemas de destino. Las nuevas contraseñas se verifican con respecto a las políticas de contraseñas de Identity Manager.

Descripción general de políticas de contraseñas

Una política de contraseñas es un conjunto de reglas y restricciones. Estas reglas especifican la creación y la caducidad de las contraseñas. La política de contraseñas se configura en un entorno de CA Identity Manager; sin embargo, la política se aplica al almacén de usuarios asociado con el entorno. Si un directorio de usuario está asociado con varios entornos, una política de contraseñas definida en un entorno también puede aplicarse en otros entornos.

En una política de contraseñas puede seleccionar las siguientes configuraciones:

Nota: Algunos de estos valores de configuración requieren asignaciones del directorio de usuarios para ciertos atributos. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

- Aplicación de contraseñas a un conjunto específico de usuarios
- Caducidad de la contraseña: permite definir los eventos que causan la caducidad de una contraseña, como por ejemplo el número de días transcurridos o el número de intentos de inicio de sesión erróneos. Cuando una contraseña vence, la cuenta del usuario se desactiva.
- Composición de las contraseñas: especifica los requisitos de contenido para contraseñas nuevas. Por ejemplo, puede seleccionar configuraciones que obliguen al usuario a crear contraseñas con un mínimo de ocho caracteres y que contengan un número y una letra.
- Expresiones regulares: proporciona una expresión que determina el formato de una contraseña válida. Se puede especificar si las contraseñas deben coincidir o no con este formato. Se pueden especificar también varias expresiones regulares.
- Restricciones en contraseñas: permite configurar límites para volver a utilizar la contraseña. Por ejemplo, los usuarios deben esperar 90 días antes de volver a utilizar la misma contraseña.
- Opciones avanzadas de contraseña: especifique las acciones que debe realizar CA Identity Manager, como escribir las contraseñas en minúsculas antes de procesarlas. También puede especificar la prioridad de la política de contraseñas si se aplican varias políticas de contraseñas.

Los usuarios de SiteMinder también pueden configurar políticas de contraseñas en la interfaz de usuario administrativo de SiteMinder. Estas políticas aparecen en la consola de usuario de CA Identity Manager.

Nota: Cuando CA Identity Manager se integra con SiteMinder, SiteMinder exige *todas* las políticas de contraseñas.

Creación de una política de contraseñas

Se pueden crear políticas de contraseñas mediante la Consola de usuario de CA Identity Manager.

Nota: La disponibilidad de algunas opciones de la política de contraseñas requiere la asignación de algunos atributos conocidos. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

Siga estos pasos:

1. En la Consola de usuario, seleccione una de las siguientes opciones:
   - Políticas, Gestionar políticas de contraseñas, Crear política de contraseñas.
   - Tareas, Políticas, Gestionar políticas de contraseñas, Crear política de contraseñas.
2. Introduzca un nombre único y una descripción opcional para la política de contraseñas.
3. Configure estas configuraciones de la política de contraseñas como mejore se adapten a su implementación:
   - Aplicación de una política de contraseñas a un conjunto de usuarios (en la página 100)
   - Configuración de la caducidad de la contraseña (en la página 102)
   - Configuración de la composición de contraseñas (en la página 106)
   - Especificación de expresiones regulares (en la página 107)
   - Configuración de restricciones de contraseña (en la página 109)
   - Configuración de opciones avanzadas de contraseña (en la página 113)

Activación de políticas de contraseñas adicionales

CA Identity Manager permite crear políticas de contraseñas básicas que gestionan las contraseñas de usuario exigiendo el vencimiento, la composición y el uso de las contraseñas. Se pueden definir también estas reglas de contraseña adicionales y estas restricciones:

- Caducidad de contraseña:
  - Hace un seguimiento de los inicios de sesión erróneos o correctos.
  - Autenticación del inicio de sesión.

- La contraseña caduca si no se cambia
- Inactividad de contraseña
- Contraseña incorrecta
- Varias expresiones regulares

- 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

Siga estos pasos:

1. Vaya a Directorios, <nombre del directorio>, Usuario en la Consola de gestión.
2. Verifique que se %PASSWORD DATA% y %ENABLED STATES% -> 'ESTADO' se asignan a atributos físicos.
3. Estos atributos se asignan de forma predeterminada en los archivos directory.xml de muestra. Si estos atributos no se encuentran asignados, consulte la *Guía de configuración de CA Identity Manager* para obtener información adicional.

Aplicación de una política de contraseñas a un conjunto de usuarios

Se pueden especificar reglas que determinan el conjunto de usuarios a los cuales se aplica una política de contraseñas. Esta posibilidad permite tener una política de contraseñas para empleados generales y una política más estricta para directores de alto nivel.

Siga estos pasos:

1. Cree o modifique una política de contraseñas en la Consola de usuario.
2. Seleccione el tipo de filtro que se va a configurar en el campo Filtro de directorios.

   Consulte la siguiente tabla para obtener una descripción de cada tipo de filtro.

   Nota: El tipo de almacén de usuarios al cual se aplica la política de contraseñas determina las opciones del cuadro de lista de Filtro de directorios. Algunos tipos de filtro no están disponibles para las bases de datos relacionales y los almacenes de usuarios de CA Directory cuando se integra CA Identity Manager con SiteMinder.
3. Especifique una condición seleccionando un atributo y un operador, e introduciendo un valor.
4. Para agregar condiciones adicionales, haga clic en el signo más.

La siguiente tabla describe las opciones para los tipos de filtro de directorios, y proporciona ejemplo de cada tipo de filtro. Los atributos en el lado izquierdo de "=" en los ejemplos siguientes son tal y como se indica en el área de definición del directorio de usuarios. Para las tareas de usuario del tipo Crear, las políticas de contraseñas con filtros de directorios configurados se aplican solamente cuando se cumplen las dos condiciones siguientes:

- CA Identity Manager no está integrado con SiteMinder.
- El tipo de filtro de directorio no es Usuario, Grupo, Filtro de grupo o Búsqueda de grupos.

Tipo de filtro	Utilice este filtro para...	Ejemplo
En una organización	Buscar y seleccionar una organización.	
En un grupo	Buscar y seleccionar un grupo.	
Un usuario	Buscar y seleccionar un único usuario.	
Filtro de usuario (No disponible para bases de datos relacionales cuando se integra con SiteMinder)	Especificar un filtro para los usuarios.	Tipo de empleado = Contratista Departamento=Seguridad
Expresión de búsqueda del usuario	Introducir una consulta de búsqueda para usuarios.	uid=jsmith (para LDAP) TBLUSERS.ID = jsmith (para bases de datos relacionales)
Filtro de grupo (No disponible para bases de datos relacionales cuando se integra con SiteMinder)	Especificar un filtro para grupos.	Autosuscripción = *
Expresión de búsqueda del grupo	Introducir una consulta de búsqueda para grupos.	cn=Sales (para LDAP) TBLGROUPS.NAME=GroupA (para bases de datos relacionales)
Filtro de organización (No disponible para bases de datos relacionales cuando se integra con SiteMinder)	Especificar un filtro para organizaciones.	Nombre de la organización = *Marketing

Tipo de filtro	Utilice este filtro para...	Ejemplo
Expresión de búsqueda de la organización	Introducir una consulta de búsqueda para organizaciones	ou=Boston (para LDAP) TBLORGANIZATIONS.NAME=Boston (para bases de datos relacionales)
búsqueda	Especificar una consulta que no esté incluida en las otras opciones para el tipo de filtro.	(&(uid=*sanz)(ou=Boston))

Configuración de la caducidad de la contraseña

Para ayudar a gestionar el acceso del usuario, se pueden definir eventos como varios intentos de inicio de sesión erróneos o la inactividad de la cuenta. Cuando se producen estos eventos, CA Identity Manager desactiva el responsable de la cuenta de usuario. Cuando se integra CA Identity Manager con SiteMinder, se puede especificar un redireccionamiento.

Nota: Estos valores de configuración requieren una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

Se pueden configurar los valores de configuración siguientes para la caducidad de la contraseña:

- Casilla de verificación Seguir los inicios de sesión erróneos/Seguir los inicios de sesión correctos
- Casilla de verificación Autenticar al producirse un error de seguimiento del inicio de sesión
- Configuración de La contraseña caduca si no se cambia
- Configuración de La contraseña caduca debido a la inactividad
- Configuración de Contraseña incorrecta

Casilla de verificación Seguir los inicios de sesión erróneos/Seguir los inicios de sesión correctos

Esta casilla de verificación activa y desactiva el seguimiento de intentos de inicio de sesión del usuario, incluyendo el tiempo del último intento de inicio de sesión. Si se activa esta casilla de verificación, CA Identity Manager escribe información de inicio de sesión en un atributo de datos de contraseña en el almacén de usuarios.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

Cuando la casilla de verificación Seguir los inicios de sesión erróneos está activada, la sección Contraseña incorrecta y la casilla de verificación Autenticar al producirse un error de seguimiento del inicio de sesión están activas. Cuando la casilla de verificación Seguir los inicios de sesión satisfactorios está activada, La contraseña caduca de la sección Inactividad y la casilla de verificación Autenticar al producirse un error de seguimiento del inicio de sesión están activas.

Si se tienen varias políticas de contraseñas, es necesario asegurarse de que todas las políticas de contraseñas aplicables desactivan los detalles de inicio de sesión. De lo contrario, una sola política que activa el seguimiento de los detalles de inicio de sesión puede causar que las políticas de contraseñas se comporten incorrectamente.

Casilla de verificación Autenticar al producirse un error de seguimiento del inicio de sesión

Al seleccionar esta casilla de verificación se activan los inicios de sesión cuando se produce un error en el seguimiento del usuario. De forma predeterminada esta casilla de verificación está desactivada. Cuando el seguimiento de inicio de sesión está desactivado, los usuarios no se pueden conectar.

Cuando se selecciona esta casilla de verificación, es necesario asegurarse de seleccionar también la casilla de verificación Seguir los inicios de sesión erróneos o Seguir los inicios de sesión satisfactorios.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

Configuración de La contraseña caduca si no se cambia

En los campos La contraseña caduca si no se cambia, se puede configurar el comportamiento de las contraseñas que han caducado. Opcionalmente se puede especificar cuánto tiempo antes se debe avisar a los usuarios de que su contraseña va a caducar.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

Puede configurar los siguientes campos:

Después de *<número>* días

Determina el número de días después de que caduque una contraseña que CA Identity Manager espera antes de desactivar el usuario o exigir un cambio de la contraseña.

Nota: CA Identity Manager no desactiva la cuenta de usuario hasta que el usuario intenta iniciar sesión después de que haya transcurrido el número especificado de días.

Desactivar usuario

Al seleccionar este botón de opción se desactiva el usuario cuando caduca la contraseña. Se pueden activar usuarios desactivados mediante:

- La tarea Activar/desactivar usuario en la Consola de usuario (los roles predeterminados Gestor del sistema, Gestor de organizaciones y Gestor de seguridad incluyen la tarea Activar/desactivar usuario).
- La interfaz de usuario administrativo de SiteMinder.

  Nota: Para obtener más información, consulte la guía *CA SiteMinder Policy Server Administration Guide*.

Forzar el cambio de contraseña

Al seleccionar este botón de opción se solicita un cambio de contraseña cuando el usuario intenta iniciar sesión de nuevo.

Emitir advertencias de caducidad durante *<número>* días

Introduzca el número de días previos antes de que se notifique a un usuario de que su contraseña va a caducar.

Configuración de La contraseña caduca debido a la inactividad

La configuración de La contraseña caduca debido a la inactividad permite especificar el tiempo entre los intentos de inicio de sesión del usuario. Una vez transcurrido este tiempo, una cuenta de usuario se considera inactiva. Se puede utilizar también esta sección para especificar una acción cuando un usuario cuya cuenta se considera inactiva tiene permisos para iniciar sesión.

Para configurar los valores de configuración de la sección La contraseña caduca debido a la inactividad, asegúrese de activar las casillas de verificación de los detalles de Seguir inicios de sesión.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

La sección La contraseña caduca debido a la inactividad contiene los valores de configuración siguientes:

- Después de *<número>* días: Determina el número de días de inactividad después de los cuales caduca una contraseña.
- Desactivar usuario: Desactiva el usuario cuando la contraseña caduca debido a la inactividad: la cuenta de usuario se desactiva. Los usuarios desactivados se deberán volver a activar mediante la tarea Activar/desactivar usuario.
- Forzar el cambio de contraseña: fuerza un cambio de la contraseña cuando una contraseña caduca debido a la inactividad. El usuario cambia la contraseña cuando intenta iniciar sesión de nuevo.

Configuración de Contraseña incorrecta

En la sección de configuración de Contraseña incorrecta se puede especificar cuántos inicios de sesión erróneos se permiten antes de desactivar la cuenta de usuario. Se puede especificar también cuánto tiempo debe durar la desactivación de la cuenta antes de que un usuario pueda intentar iniciar sesión de nuevo. Esta sección se aplica solamente cuando se ha seleccionado la casilla de verificación Seguir los inicios de sesión erróneos.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

La sección Contraseña incorrecta contiene los campos siguientes:

La cuenta se desactiva después de *<número>* contraseñas incorrectas sucesivas

Esta configuración determina el número de intentos erróneos consecutivos de inicio de sesión que puede realizar un usuario. La limitación del número de intentos fallidos protege contra programas que están diseñados para acceder a un recurso mediante el intento repetido de contraseñas hasta que se encuentra la correcta. Si un usuario no puede iniciar sesión correctamente después del número especificado de intentos, CA Identity Manager desactiva la cuenta. Sólo un administrador puede volver a activar la cuenta.

Después de *<número>* minutos

Esta configuración determina el tiempo total que un usuario espera antes de realizar otro intento de inicio de sesión o hasta que se vuelve a activar su cuenta. Si el usuario introduce otra contraseña incorrecta, CA Identity Manager desactiva la cuenta de nuevo. El usuario espera el tiempo especificado antes de intentarlo de nuevo.

Permitir un intento de inicio de sesión

Esta configuración especifica el número de minutos después de que un usuario introduzca una contraseña incorrecta antes de otro intento de inicio de sesión.

Reactivar cuenta

Esta configuración vuelve a activar una cuenta después del número especificado de minutos.

Configuración de la composición de contraseñas

Se pueden especificar reglas que determinen la composición de caracteres de nuevas contraseñas creadas. Asegúrese de tener en cuenta la longitud máxima de la contraseña al determinar los valores para los requisitos de carácter. Si el número total de caracteres supera la longitud máxima de contraseña, todas las contraseñas se rechazarán. Por ejemplo, si las letras y los dígitos están ambos establecidos en seis, todas las contraseñas contienen como mínimo 12 caracteres (6 letras y 6 dígitos). En este ejemplo, si una longitud máxima de la contraseña es de ocho caracteres, todas las contraseñas se rechazarán.

Los valores de configuración de la composición de contraseñas incluyen:

Longitud mínima de la contraseña

Especifica una longitud mínima para las contraseñas de usuario.

Longitud máxima de la contraseña

Especifica la longitud máxima para las contraseñas de usuario.

Núm. máximo de caracteres repetidos

Determina el número máximo de caracteres idénticos que pueden aparecer consecutivamente en una contraseña.

Por ejemplo, si este valor se establece como 3, “aaaa” no puede aparecer en ningún sitio de la contraseña. Sin embargo, “aaa” es aceptable dentro de una contraseña. Establezca este valor para asegurarse de que los usuarios no puedan introducir contraseñas de un solo carácter.

Letras mayúsculas

Especifica si se deben permitir caracteres alfabéticos en mayúscula y, en tal caso, el número mínimo que debe contener una contraseña.

Letras minúsculas

Especifica si se deben permitir caracteres alfabéticos en minúscula y, en tal caso, el número mínimo que debe contener una contraseña.

Letras

Especifica si se deben permitir letras y, en tal caso, el número mínimo que debe contener una contraseña.

Nota: La casilla de verificación Letras se selecciona automáticamente cuando se permiten letras en mayúscula o en minúscula.

Dígitos

Especifica si se deben permitir números y, en tal caso, el número mínimo que debe contener una contraseña.

Letras o dígitos

Especifica si se deben permitir letras y dígitos y, en tal caso, el número mínimo que debe contener una contraseña. Si esta configuración se establece conjuntamente con los dígitos, los caracteres pueden cumplir ambos requisitos. Por ejemplo, si esta configuración y los dígitos se establecen como 4, la contraseña “1234” es una contraseña válida.

Nota: La casilla de verificación Letras y dígitos se selecciona automáticamente cuando se permiten letras en mayúscula o en minúscula.

Puntuación

Especifica si se deben permitir signos de puntuación y, en tal caso, el número mínimo que debe contener una contraseña. Los signos de puntuación pueden ser puntos, comas, signos de exclamación, barras diagonales o guiones.

No se puede imprimir

Especifica si se deben permitir caracteres que no se pueden imprimir y, en tal caso, el número mínimo que debe contener una contraseña. Estos caracteres no son visibles en una pantalla.

Nota: Ciertos exploradores no son compatibles con caracteres no imprimibles.

No es alfanumérico

Especifica si se deben permitir caracteres no alfanuméricos como signos de puntuación y otros símbolos (“@” , “$” y “*”) y, en tal caso, el número mínimo que puede contener una contraseña. Se incluyen también caracteres no imprimibles. Un carácter no alfanumérico también cumple los requisitos de puntuación y de carácter no imprimible.

Especificación de expresiones regulares

Las expresiones regulares de contraseña permiten especificar patrones de texto de expresiones regulares para que la coincidencia de cadenas con cada contraseña sea válida. Esta prueba puede ser útil, por ejemplo, cuando sea necesario que el primer carácter sea un dígito y no lo sea el último carácter.

Se configuran varias expresiones para una sola política de contraseñas. Si se crean varias expresiones, las contraseñas aceptables coinciden con *todas* las expresiones especificadas.

Siga estos pasos:

1. Escriba una etiqueta descriptiva para la expresión (sin espacios en blanco) en el campo Nombre.
2. Escriba una expresión regular mediante la sintaxis descrita en la Sintaxis de expresiones regulares en el campo Debe coincidir.
3. Si la contraseña no coincide con la expresión regular, seleccione la casilla de verificación en la columna NO debe coincidir.

Nota: Se pueden especificar varias expresiones haciendo clic en el signo más (+) para agregar la expresión.

Ejemplo: La definición de expresión regular siguiente se puede utilizar para solicitar que todas las contraseñas empiecen con un letra mayúscula o minúscula: Name: MustStartAlpha

Expresión: [a-zA-Z].*

Sintaxis de expresiones regulares

Esta sección describe la sintaxis que se utiliza para elaborar expresiones regulares para la coincidencia de la contraseña. Esta sintaxis es consistente con la sintaxis de expresiones regulares que se admite en la concidencia de recursos al especificar dominios.

Caracteres	Resultados
\	Utilizado para citar un metacarácter (como "'*")
\\	Coincide con un carácter único "'\"
(A)	Subexpresiones de grupos (afecta al orden de la evaluación del patrón)
[abc]	Clase de carácter simple (cualquier carácter entre paréntesis coincide con el carácter de destino)
[a-zA-Z]	Clase de carácter con intervalos (cualquier intervalo de caracteres entre paréntesis coincide con el carácter de destino)
[^abc]	Clase de carácter negado
.	Coincide con cualquier carácter distinto a una nueva línea

Caracteres	Resultados
^	Coincide solamente al inicio de una línea
$	Coincide solamente al final de una línea
A*	Coincide con A 0 o más veces (expansivo)
A+	Coincide con A 1 o más veces (expansivo)
A?	Coincide con A 1 o 0 veces (expansivo)
A*?	Coincide con A 0 o más veces (no expansivo)
A+?	Coincide con A 1 o más veces (no expansivo)
A??	Coincide con A 0 o 1 vez (no expansivo)
AB	Coincide con A seguido por B
A|B	Coincide con A o con B
\1	Detectado previamente en la 1ª subexpresión puesta entre paréntesis
n	Detectado previamente en la subexpresión *n*th puesta entre paréntesis

Todos los operadores de cierre (+, *?) son expansivos de forma predeterminada, lo cual significa que coinciden con tantos elementos de la cadena como sea posible sin causar un error en la coincidencia total. Si se desea que un cierre sea no expansivo, ¿puede simplemente escribir después de éste un "?". Un cierre no expansivo coincidirá con el mínimo número de elementos de la cadena como sea posible al buscar coincidencias.

Configuración de restricciones de contraseña

Se pueden establecer restricciones en el uso de contraseñas. Las restricciones incluyen el tiempo que un usuario debe esperar antes de poder volver a utilizar una contraseña. También especifican que las contraseñas deben ser diferentes de las que se han seleccionado previamente. Mediante esta indicación, también se evita que los usuarios especifiquen palabras que pueden ser un riesgo para la seguridad o que contienen información personal.

Nota: Esta configuración requiere una configuración adicional. Consulte Activación de políticas de contraseñas adicionales (en la página 99).

La sección Restricción incluye los campos siguientes:

Número mínimo de días antes de la reutilización

Determina cuántos días debe esperar un usuario antes de reutilizar una contraseña.

Número mínimo de contraseñas antes de la reutilización

Determina cuántas contraseñas se deberán utilizar antes de que una contraseña se pueda reutilizar.

Nota: Si se especifica una longitud de hora y número para las contraseñas, los dos criterios se cumplirán antes de la reutilización de una contraseña. Por ejemplo, se puede configurar una política de contraseñas que requiera que los usuarios esperen 365 días y especifiquen12 contraseñas antes de la reutilización de una contraseña. Después de un año, si solamente se han utilizado seis contraseñas, se utilizarán otras seis antes de que el usuario pueda volver a utilizar la primera contraseña.

Porcentaje de diferencia con respecto a la contraseña anterior

Especifica el porcentaje de caracteres que debe contener una nueva contraseña. Se puede establecer el valor como 100. En este caso, la nueva contraseña no puede contener caracteres que ya aparecían en la contraseña anterior.

Ignorar secuencia cuando se comprueban diferencias

Ignora la posición de los caracteres en la contraseña al determinar el porcentaje.

Por ejemplo, con una contraseña inicial es BASEBALL12 y se selecciona la casilla de verificación Ignorar secuencia cuando se comprueban diferencias, 12BASEBALL no es aceptable. Cuando se desactiva la casilla de verificación, 12BASEBALL será una contraseña aceptable porque cada letra está en una posición diferente.

Para una mayor seguridad, active la casilla de verificación Ignorar secuencia cuando se comprueban diferencias.

Contraseñas	Porcentaje de diferencia	Ignorar secuencia	Aceptado
BASEBALL12 (antigua)	0	Seleccionado	Y
12BASEBALL		Deseleccionado	Y
BASEBALL12 (antigua)	100	Seleccionado	N
12BASEBALL		Deseleccionado	Y
BASEBALL12 (antigua)	0	Seleccionado	Y
12SOFTBALL		Deseleccionado	Y

Contraseñas	Porcentaje de diferencia	Ignorar secuencia	Aceptado
BASEBALL12 (antigua) 12SOFTBALL	90	Seleccionado Deseleccionado	N Y
BASEBALL12 (antigua) 12SOFTBALL	100	Seleccionado Deseleccionado	N N

Atributos del perfil

La configuración del campo Longitud coincidente impide que los usuarios utilicen información personal en las contraseñas. El campo Longitud coincidente determina la longitud mínima de secuencias que la política de contraseñas utiliza para comparar con los atributos en la entrada del directorio. Por ejemplo, si este valor se establece como cuatro, CA Identity Manager verifica que la contraseña no incluya los últimos cuatro caracteres de los atributos de perfil del usuario, por ejemplo, el apellido o el número de teléfono.

Diccionario

Especifica una lista de cadenas que no se pueden utilizar en contraseñas.

Nota: Después de la última línea de la entrada de diccionario se muestra un retorno de carro.

Los parámetros de Diccionario incluyen los elementos siguientes:

- Ruta: contiene la ruta completa y el nombre del archivo de diccionario.
- Longitud coincidente: controla la longitud de las cadenas que se comparan con valores del archivo de diccionario. La comparación ignora si las cadenas están en mayúsculas o minúsculas. El campo Longitud coincidente se puede dejar en blanco o establecerlo a cero. En estos casos, CA Identity Manager solamente rechaza contraseñas que coinciden exactamente con una cadena en el diccionario. Cuando la Longitud coincidente sea mayor que cero, CA Identity Manager rechaza entradas durante las condiciones siguientes:
  - La contraseña incluye una subcadena que empieza con la misma serie de caracteres que una entrada de diccionario.
  - El número de caracteres coincidentes consecutivos es mayor o igual al número especificado en el campo Longitud coincidente.

  Por ejemplo, tenga en cuenta el archivo de diccionario que contiene las siguientes entradas:
  - león
  - tigre
  - lobo

  Cuando el campo Longitud coincidente se establece a cuatro, se producen las acciones siguientes:

  "hombre lobo" se rechaza porque "lobo" coincide con la entrada Lobo en el archivo de diccionario.

  "tigresa" se rechaza porque "tigre" coincide con los primeros cinco caracteres de la entrada Tigre en el archivo de diccionario.

  "camaleón", se acepta puesto que "león" no incluye la primera letra de la entrada León en el archivo de diccionario.

Configuración de opciones avanzadas de contraseña

Las opciones avanzadas de la política de contraseñas permiten configurar el preprocesamiento de contraseñas enviadas antes de la validación y el almacenamiento. Se puede asignar también a la política una prioridad para permitir la evaluación predecible de varias políticas de contraseña que se aplican al mismo directorio de usuarios o espacio de nombres.

No forzar mayús./minús. | Forzar mayúsculas | Forzar minúsculas

Determina si las contraseñas se deben ser mayúsculas o minúsculas antes del procesamiento y almacenamiento. Elija una de las dos opciones haciendo clic en el botón Forzar mayúsculas o Forzar minúsculas. De lo contrario, asegúrese de dejar seleccionado el botón No forzar mayús./minús. (el cual es el predeterminado).

Importante: Asegúrese de que en cualquier caso en el que se fuerce la opción especificada, ésta sea consistente con los requisitos de composición relacionados con la opción definida.

Eliminar espacio en blanco inicial

Seleccione esta opción para eliminar el espacio blanco inicial de las contraseñas antes del procesamiento.

Eliminar espacio en blanco final

Seleccione esta opción para eliminar el espacio blanco final de las contraseñas antes del procesamiento.

Eliminar espacio en blanco incorporado

Seleccione esta opción para eliminar todos los espacios en blanco incrustados antes del procesamiento.

Nota: Algunas implementaciones del directorio de usuarios eliminan automáticamente el espacio en blanco inicial y final de los valores de atributo (en los cuales se almacenan las contraseñas de usuario) antes de almacenarlos. Los valores de configuración especificados en su política de contraseñas no tienen ningún efecto.

Prioridad de evaluación

Especifica la prioridad de evaluación para la política de contraseñas. El valor está en el intervalo de 0 (el valor predeterminado) a 999. Las políticas aplicables se evalúan en orden descendente (999 primero; 0 último).

Aplicar políticas de contraseñas de prioridad más baja

Determina si las políticas de contraseñas de prioridad más baja se aplican después de ésta.

Gestión de políticas de contraseñas

Los administradores que dispongan de los privilegios apropiados pueden gestionar las políticas de contraseñas utilizando las tareas Ver, Modificar, Crear y Suprimir política de contraseñas. De forma predeterminada, estas tareas aparecen en la categoría Políticas.

Cuando se accede a una de estas tareas, CA Identity Manager muestra la lista de políticas de contraseñas que se aplican al almacén de usuarios asociado con el entorno actual de CA Identity Manager. Si CA Identity Manager se integra con SiteMinder, la lista puede incluir políticas de contraseñas que se crean en la interfaz de usuario administrativo de SiteMinder mediante Servicios de contraseñas. Es posible gestionar las políticas de contraseñas que se creen en CA Identity Manager o SiteMinder.

Políticas de contraseñas y bases de datos relacionales

Si configura una política de contraseñas que se aplique a una base de datos relacional, debe utilizar el siguiente formato para configurar el atributo de datos de contraseña para el directorio de usuario de SiteMinder:

nombretabla.nombrecolumna

Para evitar problemas de sintaxis durante la ejecución, es recomendable que este campo se encuentre en la tabla principal.

Criterios de contraseña de CA Identity Manager e integración de Siteminder

Cuando CA Identity Manager se integra con SiteMinder y utiliza la capacidad de tratamiento de contraseñas de Siteminder, las políticas de contraseñas se obtienen del almacén de políticas de Siteminder. En este caso, elabore contraseñas que cumplan con los criterios de contraseña de Siteminder. Los caracteres de puntuación siguientes son los únicos que cumplen con los criterios de contraseña de Siteminder:

'*', '(', '\',',','@','"',':','#','_','-','!','&','?',')','(','{','}','*','.','/' "

Importante: CA Identity Manager no impone ninguna restricción al uso de caracteres de puntuación en las contraseñas. Sin embargo, si pretende utilizar la capacidad de contraseñas de Siteminder, es recomendable que elabore contraseñas que cumplan con las restricciones de Siteminder.

Restablecimiento de contraseñas o desbloqueo de la cuenta

En el caso de que los usuarios olviden su contraseña en sistemas Windows, se puede configurar Autoservicio para solicitar que el usuario cierre sesión desde la pantalla de Windows. Se puede utilizar esta función mediante la instalación del proveedor de credenciales para los sistemas Windows Vista y Windows 7.

Con esta función, el usuario inicia sesión en Autoservicio a través del explorador web Cube donde aparece una página de solicitud de cambio de la contraseña. Después de rellenar esta página, el usuario seleccionará Volver para volver a la pantalla Conexión de Windows.

Instalación del proveedor de credenciales

Siga estos pasos:

1. Localice la descarga de los componentes de aprovisionamiento de CA Identity Manager u otro medio de instalación.
2. Ejecute el instalador en el agente.

   Nota: Si está instalando el proveedor de credenciales en un sistema operativo de 64 bits, elija la versión de 64 bits de este software.
3. Siga las indicaciones del asistente para responder a las preguntas.
4. Si instaló el proveedor de credenciales en un sistema operativo de 64 bits, descargue Microsoft C++ 2008 SP1 Visual (64 bits).
5. Una vez que finaliza la instalación, Configure el proveedor de credenciales.

Configuración del proveedor de credenciales

Es posible utilizar una herramienta de configuración para configurar el sistema en el que haya instalado el proveedor de credenciales.

Para configurar el proveedor de credenciales

1. En el Explorador de Windows, vaya al directorio donde está instalado el proveedor de credenciales. Por ejemplo:

   C:\Archivos de programa\CA\Identity Manager\Credential Provider
2. Haga doble clic en el siguiente ejecutable:

   CAIMCredProvConfig.exe

3. Seleccione el primer proveedor de credenciales como opción predeterminada.

   Es posible que la pantalla de inicio de sesión no aplique esta configuración si hay un segundo proveedor de credenciales en uso como el proveedor de credenciales de contraseña de Microsoft. Si ambos proveedores intentan ser el proveedor predeterminado, la pantalla de inicio de sesión elige a un proveedor predeterminado.

4. Desactive el proveedor de credenciales predeterminado.

5. Rellene los campos de configuración del proveedor de credenciales como se indica a continuación:

   Link 1 URL (URL del vínculo 1)

   La dirección URL utilizada cuando un usuario hace clic en el vínculo ¿Olvidó la contraseña?. Este enlace debe ser una URL a una interfaz Web para el restablecimiento de contraseñas.

   A continuación, se proporciona un vínculo de muestra:

   `http://eastern.local:8080/iam/im/`*`entorno`*`/ca12/index.jsp?task.tag=forgottenpassword&facesViewId=/app/page/screen/fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%username%`

   Para esta dirección URL, la funcionalidad de autoregistro debe estar en funcionamiento en el entorno. Verifique también que la URL de autoservicio para el entorno de CA Identity Manager funciona en el sistema en el que va a instalar el proveedor de credenciales. %username% se reemplaza por el valor especificado en el campo de nombre de usuario del cuadro de diálogo Iniciar sesión.

   Link 2 **URL (URL del vínculo 2)**

   La dirección URL utilizada cuando un usuario hace clic en el vínculo Desbloquear cuenta. Este enlace debe ser una URL a una interfaz Web que permita al usuario desbloquear una cuenta. %username% se reemplaza por el valor especificado en el campo de nombre de usuario del cuadro de diálogo Iniciar sesión.

   Link3 URL (URL del vínculo 3)

   La dirección URL utilizada cuando un usuario hace clic en el vínculo Cuenta nueva. Este vínculo debe ser una URL a una interfaz Web que permita al usuario crear una cuenta. No se espera que la etiqueta %username% forme parte de la dirección URL.

Use custom title (Utilizar título personalizado)

Una cadena personalizada reemplaza la cadena Powered by (Proporcionado por...) que aparece en la barra del título o en el cuadro de diálogo Return (Volver) del proveedor de credenciales. La ubicación de la cadena se basa en el valor de configuración Section 508 Compliance (Cumplimiento de la sección 508).

Domain

El nombre del dominio de aprovisionamiento.

Section 508 Compliance (Cumplimiento de la sección 508) [Uso de Return (Devolver) en el menú)

Activa la función Devolver en un menú. Si no se marca, se usa el cuadro de diálogo Devolver.

Disable All Dialogs (Desactivar todos los cuadros de diálogo)

Impide que el explorador seguro genere nuevas ventanas de diálogo, tales como cuadros de diálogo emergentes, de error, de impresión o almacenamiento. El valor de configuración *Disable All Dialogs (Desactivar todos los cuadros de diálogo)* está activado para mejorar la seguridad del sistema, pero se puede desactivar para solucionar problemas.

6. Rellene los campos de configuración del explorador seguro de la siguiente manera:

   Lista de permitidos

   Direcciones URL que coinciden con un patrón de expresiones regulares y a las que siempre se permite el acceso.

   Lista de denegación

   Direcciones URL que coinciden con un patrón de expresiones regulares y a las que siempre se deniega el acceso.

7. (Opcional) Haga clic en Exportar para exportar la configuración a otro sistema.
8. Haga clic en Aceptar para guardar la configuración.
9. Reinicie el sistema.

Configuración del registro del proveedor de credenciales

Si decide no utilizar la herramienta de configuración del proveedor de credenciales, puede editar la configuración del registro de Windows en la siguiente clave:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]
```

link1_cmd

Este vínculo deberá ser la URL a la que se desplazará cuando un usuario haga clic en el vínculo 1.

link2_cmd

Este vínculo deberá ser la URL a la que se desplazará cuando un usuario haga clic en el vínculo 2. Por ejemplo, se puede agregar un enlace que conduzca a un sitio Web para desbloquear cuentas.

Si link2_cmd está en blanco, sólo aparecerá link1_cmd en la ventana del cuadro de diálogo de inicio de sesión.

link3_cmd

Este vínculo debe cargar una URL a una interfaz Web que permita al usuario crear una cuenta.

comp508

Activa la función Devolver en un menú. Si no se marca, se utiliza el diálogo Devolver.

domain

El nombre del dominio de aprovisionamiento.

langdir

La ubicación de las DLL de idioma localizadas.

disablepwdcp

La opción de desactivación del proveedor de credenciales de contraseña de Microsoft. Con 1, la opción está desactivada. Con 0, la opción está activada.

CredentialProviderInstallPath

La ruta del directorio completa en donde está instalado el proveedor de credenciales.

configdir

La ruta del directorio completa en donde está instalado el proveedor de credenciales.

selectdefaultcredential

Seleccione al primer proveedor de credenciales como la opción predeterminada. Seleccione Sí para activar el proveedor o bien No para desactivarlo.

Configuración del registro del explorador Cube

El componente de explorador seguro Cube tiene varios valores del registro que controlan su comportamiento. Estos valores de configuración se encuentran en la clave de registro siguiente:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]
```

Type

```
REG_SZ(String)
```

404

La ruta a un documento HTML estándar para mostrar si el equipo no se puede poner en contacto con CA Identity Manager durante el inicio.

default

La página predeterminada a la que navegar cuando no se incluye ninguna dirección URL en el comando Link1 o Link2.

allow

Activación explícita de la lista de control de acceso. Una expresión regular para direcciones URL coincidentes con patrones que siempre está activada. Para obtener más información, consulte Listas de control de acceso de Cube (en la página 120).

close

Cierra el explorador seguro y devuelve al usuario al cuadro de diálogo de olvido de la contraseña del proveedor de credenciales.

deny

Denegación explícita de la lista de control de acceso. Una expresión regular para direcciones URL coincidentes con patrones que siempre deniega el acceso. Para obtener más información, consulte Listas de control de acceso de Cube (en la página 120).

langdir

La ubicación de las DLL de idioma localizadas.

rejectinvalidcerts

Controla si el proveedor de credenciales acepta solamente certificados SSL válidos. Cuando se establece como No, esta opción permite el uso de certificados SSL caducados o no válidos.

Los valores válidos para esta clave son *yes* (sí) y *no*.

unreachable

Redirige a una dirección URL cuando Cube encuentra problemas de conectividad.

Valor de muestra: file:///C:\unreachable.html

usecustomtitle

Esto permite el título personalizado para el proveedor de credenciales.

customtitle

Este es un título que desea que aparezca en el proveedor de credenciales.

Listas de control de acceso a cubo

Las ACL de cubo son patrones de expresiones regulares que conceden o deniegan explícitamente el permiso para navegar a una URL seleccionada. Las ACL se evalúan en el siguiente orden:

1. Allow (el permiso se concede automáticamente en primer lugar)
2. Deny (las URL denegadas se comprueban en segundo lugar)

Ejemplos de listas de control de acceso

"allow"="(.pdf)"

Permite mostrar todos los documentos en formato PDF.

"deny"="(.doc|.xls)"

Deniega el acceso a los documentos de Microsoft Word y Excel.

Personalización del mensaje "Prowered by... (Con tecnología de...)"

Es posible que en el cuadro de diálogo Return (Volver) o en la opción del menú Return (Volver) del proveedor de credenciales aparezca el mensaje "Powered by... (Proporcionado por...)". Se puede editar o eliminar este mensaje.

Para personalizar el mensaje "Con tecnología de"

1. Descargue ResEdit, un editor de recurso freeware de http://www.resedit.net.
2. Inicie ResEdit.
3. Edite el archivo 1033.dll en la carpeta de idiomas.
4. Haga doble clic en la tabla de cadenas.
5. Elimine o modifique el recurso ID 135, la versión inglesa del recurso para este mensaje.

Restablecimiento de una contraseña para el inicio de sesión en Windows

Una vez instalado el proveedor de credenciales en un sistema Windows, aparece el vínculo ¿Contraseña olvidada? en el cuadro de diálogo estándar de inicio de sesión en Microsoft Windows. Mediante este vínculo, se puede restablecer directamente la contraseña o mostrar las pistas introducidas con anterioridad para recordarla.

Para restablecer una contraseña para el inicio de sesión en Windows

1. En el cuadro de diálogo Seguridad de Windows, haga clic en Iniciar sesión. Aparece el cuadro de diálogo Inicio de sesión de Windows.
2. Introduzca un nombre de usuario válido.
3. Haga clic en ¿Olvidó la contraseña?.

   Aparece la página CA Identity Manager Password Clue (Pista de la contraseña de CA Identity Manager).

   Si no recuerda la contraseña, vuelva al cuadro de diálogo de inicio de sesión para continuar. De lo contrario, realice el paso 4 para realizar la autenticación en Autoservicio de CA Identity Manager.
4. Escriba las respuestas a las preguntas de autenticación.

   Nota: Si no sabe o no recuerda las respuestas a todas las preguntas, haga clic en Solicitud para que un administrador pueda restablecer su contraseña.

   A continuación, se le solicitará que modifique la contraseña en la pantalla siguiente.

Instalación silenciosa del proveedor de credenciales

El proveedor de credenciales es compatible con el modo de instalación silenciosa. Es compatible con seis propiedades.

LINK1

Hace referencia a SOFTWARE\CA\CAIMCredentialProvider\link1_cmd en el registro.

LINK2

Hace referencia a SOFTWARE\CA\CAIMCredentialProvider\link2_cmd en el registro.

LINK3

Hace referencia a SOFTWARE\CA\CAIMCredentialProvider\link3_cmd en el registro.

DOMAIN

Hace referencia a SOFTWARE\CA\CAIMCredentialProvider\domain en el registro.

COMP508

Hace referencia a SOFTWARE\CA\CAIMCredentialProvider\comp508 en el registro.

USECUSTOMTITLE

Hace referencia a SOFTWARE\CA\Cube\usecustomtitle en el registro.

CUSTOMTITLE

hace referencia a SOFTWARE\CA\Cube\customtitle en el registro.

REJECTINVALIDCERTS

hace referencia a SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts en el registro.

UNREACHABLE

hace referencia a la ubicación de la página que no se encuentra.

La sintaxis para establecer el valor de estas propiedades es la siguiente:

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Archivos de programa\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\"LINK3=\"<url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"custom cp title\""
```

o

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Archivos de programa\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\" LINK3=\"<url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

o

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Archivos de programa\CA\Identity
Manager\Credential Provider\"
LINK1=\"<url>\" LINK2=\" <url>\" LINK3=\"<url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"file:///[INSTALLDIR]<file
name>\"CUBE_ALLOW=\"\"CUBE_DENY=\"\""
```

[INSTALLDIR]

Hace referencia al valor de la propiedad INSTALLDIR.

<url>

Especifica la dirección URL para desbloquear cuentas o recordar contraseñas.

<file name>

Define el nombre del archivo que no se encuentra.

CUBE_ALLOW

Se refiere a permitir la invocación de la dirección URL desde Cube.

CUBE_DENY

Se refiere a restringir la invocación de la dirección URL desde Cube.

Capítulo 6: Sincronización de contraseñas en puntos finales

Se puede instalar un agente de sincronización de contraseñas en determinados puntos finales compatibles con CA Identity Manager. El agente intercepta las solicitudes de cambio de contraseñas en el punto final y envía los cambios al servidor de aprovisionamiento.

Esta sección contiene los siguientes temas:

Sincronización de contraseña en Windows

CA Identity Manager puede interceptar el cambio de contraseña de una cuenta nativa de Windows y propagar la nueva contraseña a un usuario y todas las cuentas que pertenecen a dicho usuario.

Cuando el agente de sincronización de contraseñas detecta un intento de cambio de contraseña, el agente intercepta la solicitud y la envía al servidor de aprovisionamiento. A continuación, el servidor de aprovisionamiento propaga la contraseña nueva al usuario y a otras cuentas asociadas a ese usuario.

La sincronización de contraseña cuenta con los siguientes requisitos:

- El agente de sincronización de contraseñas de debe estar instalado en el sistema en el que se vayan a interceptar los cambios de contraseñas.
- El sistema se debe gestionar como un punto final adquirido.
- Se debe activar la casilla de verificación de que se ha instalado el agente de sincronización de contraseñas en la ficha Configuración de punto final.
- Las cuentas de los sistemas gestionados se deben explorar y correlacionar con los usuarios de CA Identity Manager.
- El entorno debe permitir cambios de contraseña que procedan de cuentas de puntos finales. Los administradores con acceso a la Consola de gestión activan esta función.

Importante: Tenga cuidado al formular reglas de contraseñas; una contraseña se aplique a todos los sistemas. Por ejemplo, si las contraseñas de Windows deben tener 12 caracteres, todos los sistemas que sólo admitan contraseñas de 10 caracteres rechazarán el cambio durante la sincronización.

El servidor de CA Identity Manager no tiene en cuenta las limitaciones de las contraseñas en el punto final. Al trabajar con cuentas de puntos finales, la política de contraseñas debe ser más estricta que la política de contraseñas de los puntos finales.

Instalación del agente de sincronización de contraseñas

El agente de sincronización de contraseñas se puede instalar en cualquier equipo Windows gestionado en el que inicien sesión los usuarios globales. El agente se ejecuta en segundo plano en estos equipos.

Ejecución del programa de instalación

Tenga en cuenta los siguientes requisitos:

- El servidor de aprovisionamiento debe gestionar el sistema en el que se está instalando el agente.
- Cree un usuario para que haga de administrador de los cambios de contraseña: el nombre sugerido es etapwsad. Este usuario debe tener el perfil PasswordAdministrator.
- Existen dos agentes de sincronización de contraseñas de Windows en el medio de instalación: uno para arquitecturas de 32 bits de Windows y otro para 64 bits. El agente de sincronización de contraseñas de 32 bits no es compatible con Windows de 64 bits. FIPS solamente es compatible con el agente de sincronización de contraseñas de 32 bits.

Siga estos pasos:

1. Busque el medio de instalación de CA Identity Manager.
2. Acceda a \Agent\PasswordSync o \Agent\PasswordSync-x64.
3. Ejecute el archivo setup.exe.
4. Responda a las preguntas del Asistente de configuración tal y como se indica a continuación:
   a. En el campo Nombre de host, introduzca el nombre del sistema del servidor de aprovisionamiento.

b. Cambie el puerto, tal y como se indica, si la instalación del servidor de aprovisionamiento utiliza un puerto no predeterminado.

   El puerto de LDAP recomendado que se utiliza para conectarse al servidor de aprovisionamiento es el 20390.

c. Haga clic en el botón de dominio Buscar para recuperar el dominio del servidor de aprovisionamiento.

d. Si la instalación del servidor de aprovisionamiento se configura para conmutación por error, siga las instrucciones que se muestran en pantalla para agregar una lista de servidores separados por comas.

e. Haga clic en Siguiente.

f. En el campo Administrador, escriba etapwsad como nombre de usuario global predeterminado para el agente de sincronización de contraseñas. Este usuario debe tener el perfil PasswordAdministrator. No existe de manera predeterminada.

g. En el campo Contraseña de administrador, escriba la contraseña del administrador.

h. Haga clic en Siguiente.

i. En la lista desplegable Tipo de punto final, seleccione Tipo de punto final en el host en el que va a instalar el agente.

j. En la lista desplegable Nombre de punto final, seleccione el nombre del punto final que se ha utilizado al crear el punto final en la Consola de usuario.

k. Haga clic en Configurar.

5. Haga clic en Finalizar cuando se solicite completar la instalación y reiniciar.

Actualización de puntos finales en la Consola de usuario

En la Consola de usuario, actualice el punto final para indicar que el agente se ha instalado.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Busque el punto final en el que se ha instalado el agente.
3. Haga clic en la ficha Configuración de punto final.
4. Active la casilla de verificación Agente de sincronización de contraseñas instalado.

Activación de entornos para la sincronización de contraseñas

Una vez que se instale el agente de sincronización de contraseñas, active el entorno para recibir los cambios de contraseña que se realicen en los puntos finales. Para esta tarea, un administrador tiene que acceder a la Consola de gestión y a CA Directory para activar el entorno con el fin de que se acepten estos cambios.

Siga estos pasos:

1. Para los nuevos usuarios, utilice la Consola de gestión de la siguiente forma:
   a. Seleccione el entorno.
   b. Haga clic en Configuración avanzada, Aprovisionamiento.
   c. Active la casilla de verificación Enable Password Changes from Endpoint Accounts (Activar cambios de contraseña de cuentas de puntos finales).
2. Para los usuarios existentes, establezca el atributo de eTPropagatePassword a 1 en CA Directory.

Configuración de servidores alternativos para el agente de sincronización de contraseñas

Para configurar un servidor alternativo para el agente de sincronización de contraseñas, se utiliza el asistente de configuración del agente de sincronización de contraseñas.

Para agregar un servidor alternativo para el agente de sincronización de contraseñas

1. Ejecute el archivo PwdSyncConfig.exe que se encuentra en *carpeta_sinc_contraseña*\bin.
2. Introduzca la siguiente información de configuración:

   Host

   Especifique el nombre de host del servidor de aprovisionamiento principal.

   De este modo, se rellenará el campo URL del servidor con el nombre de host que haya especificado.

   Puerto LDAP

   Especifique el número de puerto que utilizará el equipo para conectarse al servidor de aprovisionamiento.

   CA Identity Manager rellenará el campo URL del servidor con el host y el puerto que haya especificado.
3. Haga clic en el botón Buscar dominio para obtener la lista de dominios.
4. En el cuadro desplegable Dominio, seleccione el nombre del dominio y haga clic en Siguiente.

5. Agregue el nombre de host y el puerto de los servidores alternativos al campo URL del servidor con el siguiente formato:

   ldaps://*hostprincipal*:20390,ldaps://*hostalternativo1*:20390

6. Haga clic en Siguiente.
7. Complete los campos restantes del asistente de configuración.

Cómo funciona el agente de sincronización de contraseñas

El proceso de propagación comienza cuando los usuarios globales cambian su contraseña en un sistema Windows utilizando cualquier método. Una vez que se ha introducido la contraseña, ocurre lo siguiente:

1. El sistema operativo Windows realiza una comprobación para asegurarse de que la contraseña cumple la política de contraseñas. Si Windows no acepta la contraseña, se rechazará la solicitud de cambio y no se llevará a cabo ninguna acción más, incluida la sincronización.
2. El sistema Windows pasará la solicitud de cambio de contraseña al agente de sincronización de contraseñas de CA Identity Manager, que, si está configurado para comprobación de la calidad de las contraseñas, enviará la contraseña al servidor de aprovisionamiento para que realice una comprobación de la calidad de la contraseña. Si la contraseña no cumple las reglas de calidad de CA Identity Manager, la solicitud de cambio se rechazará y se mostrará un mensaje de error. La contraseña de Windows no se modificará, ni se producirá la sincronización.
3. El agente de sincronización de contraseñas enviará una contraseña que cumpla las reglas de calidad de Windows e CA Identity Manager al servidor de aprovisionamiento para propagación.
4. CA Identity Manager actualizará la contraseña de usuario global y propagará la nueva contraseña a todas las cuentas asociadas con el usuario global, o sólo a algunas.

Nota: Las políticas de contraseñas para Windows e CA Identity Manager deben ser idénticas o coherentes porque los mensajes de error que se muestran se basan en la política de contraseñas de Windows, aunque CA Identity Manager rechace la solicitud.

El parámetro de configuración password_update_timeout (eta_pwdsync.conf) especifica el tiempo (en segundos) que el PSA espera la confirmación de propagación-cambio-contraseña del servidor de CA Identity Manager. Si el PSA no recibe ninguna confirmación durante ese tiempo, continuará como si la propagación hubiera sido correcta y registrará una advertencia (eta_pwdsync.log) que indicará que no se ha podido verificar la propagación del cambio de contraseña. El valor mínimo del parámetro es cero (0), lo que significa que el PSA no esperará la confirmación. Para obtener más información, consulte eta_pwdsync.conf--Configuración del agente de sincronización de contraseñas en la ayuda del agente de aprovisionamiento.

Comprobación de la calidad de las contraseñas de nivel de cuentas

La comprobación de la calidad de las contraseñas se lleva a cabo cuando se crean o se modifican cuentas en los puntos finales gestionados o cuando se establecen contraseñas de usuario global. La comprobación de la calidad de las contraseñas en las cuentas se limita a comprobaciones basadas en los caracteres de la contraseña. Las comprobaciones de usuarios globales que se basan en el historial de cambios recientes (frecuencia de la actualización de la contraseña y frecuencia de la reutilización de la contraseña) no se llevan a cabo en las cuentas porque CA Identity Manager no intercepta todas todos los cambios de contraseña de las contraseñas de cuentas. Por ello, no dispone de un historial de cambio de contraseñas preciso con el que se puedan realizar estas comprobaciones.

La comprobación de las contraseñas de cuentas se controla mediante los siguientes parámetros de configuración de dominios:

- Tipo de punto final/Comprobar contraseñas de cuentas
- Tipo de punto final/Comprobar contraseñas de cuentas vacías

El valor de cada parámetro especifica el nivel de comprobación que se debe realizar para cada nivel de punto final gestionado. El punto final se puede especificar de las siguientes maneras:

```
ALL
-ALL
<NombreEspacionombres>
-<NombreEspacionombres>
<NombreEspacionombres>:<NombreDirectorio>
-<NombreEspacionombres>:<NombreDirectorio>
```

Los formatos que incluyen un signo menos (-) desactivan el parámetro. Los formatos sin este signo activan el parámetro. Los formatos [-]<NombreEspacionombres> controlan todos los puntos finales del tipo indicado, mientras que los formatos [-]<NombreEspacionombres>:<NombreDirectorio> controlan los puntos finales individuales. Los formatos [-]ALL controlan los puntos finales de todos los tipos. El valor predeterminado de ambos parámetros es -ALL.

Cada uno de estos parámetros se puede especificar varias veces. Si varios valores especifican el mismo punto final, se utilizará el último valor. Puede establecer reglas generales en primer lugar y, más adelante, reglas específicas que anulen la regla general.

El parámetro Comprobar contraseñas de cuentas ofrece una comprobación equivalente a la comprobación de la calidad de las contraseñas de usuario global. Si este parámetro está activado para un punto final, CA Identity Manager comprobará cualquier cambio solicitado para una cuenta existente, incluidos los intentos de establecer una contraseña vacía. Durante la creación de la cuenta, si no se proporciona ninguna contraseña, no se realizará la comprobación de la calidad de las contraseñas.

Comprobar contraseñas de cuentas vacías proporciona la comprobación adicional de las contraseñas vacías cuando se crean las cuentas. Si está activado el perfil de la contraseña y solicita una contraseña de un solo carácter como mínimo, una contraseña vacía producirá un error al crear la cuenta. Este parámetro es independiente de Comprobar contraseñas de cuentas porque en algunos tipos de puntos finales se admite la creación de una cuenta sin contraseña.

Nota: La comprobación de la calidad de las contraseñas de cuentas se omite para las contraseñas de cuentas sincronizadas si la contraseña proporcionada coincide con la contraseña de usuario global actual.

Cumplimiento de la calidad de las contraseñas

La opción Sincronización de contraseñas intercepta las solicitudes de cambio de contraseña en los sistema nativos (por ejemplo, Windows NT/ADS) y las envía al servidor de CA Identity Manager. El servidor sincroniza la contraseña de usuario global y las contraseñas de cuenta asociadas con el usuario global. Para cumplir el control de calidad de las contraseñas, se pueden utilizar tanto las reglas de calidad de las contraseñas de CA Identity Manager de un perfil de contraseña como las reglas de calidad de las contraseñas del sistema (Windows NT/ADS).

Configuración de sincronización de contraseñas

El agente de sincronización de contraseñas se configura al principio durante la instalación y se puede volver a configurar en cualquier momento mediante el asistente de configuración de sincronización de contraseñas. Se puede configurar mucho más. Por ejemplo, se puede cambiar la configuración de la calidad de la contraseña comprobando o modificando los tiempos de espera mediante el archivo eta_pwdsync.conf.

Este archivo se encuentra en la carpeta password_sync_folder\data\. Todas las claves de este archivo de configuración se establecen durante la instalación del agente de sincronización de contraseñas. Por lo tanto, cambie estas claves solamente si es necesario. Consulte el texto de este archivo para obtener más información.

Importante: Como precaución, cree una copia de seguridad del archivo de configuración antes de editarlo.

Sección de [Server]

Clave	Descripción	Predeterminado
host	Especifica el servidor de dominio que gestiona propagación de contraseñas.	Ninguno
puerto	Especifica el puerto de escucha de LDAP del servidor de aprovisionamiento.	20411

Clave	Descripción	Predeterminado
use_tls	Especifica si se utiliza TLS/SSL para establecer comunicaciones seguras entre el agente de sincronización de contraseñas y el servidor de aprovisionamiento.	Sí
admin_suffix	Especifica el sufijo del dominio del usuario administrativo que el agente de sincronización de contraseñas utiliza para iniciar sesión en CA Identity Manager.	Ninguno
admin	Especifica el nombre de cuenta del usuario administrativo que el agente de sincronización de contraseñas utiliza para conectarse a CA Identity Manager.	Ninguno
Contraseña	Especifica la contraseña para el nombre de cuenta que se especifica en la clave de administración.	Ninguno

Sección de [eTaDomain]

Clave	Descripción	Predeterminado
Dominio	Especifica el dominio de aprovisionamiento en el que se ha instalado el agente de sincronización de contraseñas.	Ninguno
etrust_suffix	Especifica el sufijo para todo el producto de CA Identity Manager.	Ninguno
domain_suffix	Especifica el sufijo del dominio para el dominio de aprovisionamiento.	Ninguno
endpoint type	Especifica el tipo de punto final en el que se ha instalado el agente de sincronización de contraseñas.	Ninguno
endpoint	Especifica el punto final en el que el agente de sincronización de contraseñas interceptará las contraseñas.	Ninguno
endpoint_dn	Especifica el nombre destacado del punto final.	Ninguno
container_dn	Especifica el nombre destacado del contenedor que incluye las cuentas cuyas contraseñas se van a cambiar.	Ninguno
acct_attribute_name	Especifica el nombre de atributo de la cuenta, por ejemplo, eTN16AccountName para Windows NT.	Depende del tipo de punto final

Clave	Descripción	Predeterminado
acct_object_class	Especifica el objectClass de las cuentas.	Depende del tipo de punto final

Sección de [PasswordProfile]

Clave	Descripción	Predeterminado
profile_enabled	Especifica si la función de comprobación de perfil de la contraseña se ha activado.	No
profile_dn	Especifica si el asistente de configuración de contraseñas genera un nombre destacado para el perfil de la contraseña.	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

Sección de [Timeout]

Clave	Descripción	Predeterminado
search_acct_dn	Especifica el valor de tiempo de espera al buscar el nombre destacado de la cuenta.	120 segundos
pwd_update	Especifica el valor de tiempo de espera al propagar contraseñas.	400 segundos
pwd_quality_check	Especifica el valor de tiempo de espera (en segundos) al realizar la comprobación de la calidad de las contraseñas.	1

Sección de [Logs]

Clave	Descripción	Predeterminado
log_file	Especifica el archivo de registro que contiene los mensajes registrados del agente de sincronización de contraseñas.	..\Archivos de programa\CA\Identity Manager Password Sync Agent
log_level	Especifica el nivel de registro. Los valores válidos son los siguientes: 1: archivo de Init 2: contraseña actualizada correctamente o con errores 3. depuración de la conexión 4: seguimiento	0: no registrar

Conmutación por error

Si el servidor de aprovisionamiento se ha apagado o cargado de forma incorrecta, el agente de sincronización de contraseñas puede producir una conmutación por error en otro servidor. La conmutación por error requiere que los diversos servidores de aprovisionamiento abastezcan al mismo dominio y que el agente utilice tales servidores.

En la sección que se configura el agente para utilizar servidores alternativos (en la página 128) se ofrecen las instrucciones de configuración.

Activación de mensajes de registro

Para saber por qué se ha rechazado una modificación de contraseña, puede ver los mensajes de registro enviados por el agente de sincronización de contraseñas. Todos los mensajes registrados se almacenan en el archivo eta_pwdsync.log. De manera predeterminada, este archivo se encuentra ubicado en la carpeta ..\Archivos de programa\CA\Agente de sincronización de contraseñas de CA Identity Manager.

El registro de PSA (en el archivo eta_pwdsync.log) tiene los siguientes mensajes:

- Mensajes de error que siempre se registran.
- Mensajes de diagnóstico (flujo del proceso, seguimiento), que se pueden activar o desactivar en función del valor del parámetro logging_enabled=yes|no del archivo eta_pwdsync.conf.

Para diagnosticar mejor los problemas, revise el archivo eta_pwdsync.log y el registro del servidor de aprovisionamiento del mismo período de tiempo.

El parámetro de configuración anterior log_level se ha desaprobado pero se ha mantenido para mantener la compatibilidad con versiones anteriores: log_level=0 se convierte en logging_enabled=no y log_level=anything también se convierte en logging_enabled=yes. Si hay parámetros antiguos y nuevos en el archivo de configuración, el ajuste explícito del parámetro logging_enabled=yes|no anulará el ajuste indirecto establecido a través del antiguo parámetro log_level=number.

Nota: La lista de conectores disponibles se incluyó en eta_pwdsync.log, pero el agente ya no proporciona esa información.

Verificación de la instalación

Una vez que haya finalizado la instalación del agente de sincronización de contraseñas, cambie una contraseña en el sistema Windows para verificar que también cambia la contraseña de usuario global asociada con la cuenta.

Sincronización de contraseñas en UNIX y Linux

CA Identity Manager puede interceptar el cambio de contraseña de una cuenta en un sistema UNIX o Linux, así como propagarlo en todas las otras cuentas asociadas al usuario global. El componente que se utiliza para autenticar contraseñas en sistemas de seguridad externos se denomina "módulo de autenticación conectable (PAM)". Con PAM, CA Identity Manager autentica contraseñas en sistemas de seguridad externos para que los usuarios globales puedan utilizar sus contraseñas de sistema existentes para iniciar sesión en CA Identity Manager.

Sincronización de contraseñas de UNIX

Se trata de un módulo de sincronización de contraseñas que detecta eventos de cambio de contraseña a través del marco de trabajo de PAM de UNIX. El módulo de sincronización de contraseñas de UNIX notifica al servidor de aprovisionamiento de un cambio de contraseña. El servidor de aprovisionamiento busca al usuario global asociado y propaga los cambios en otras cuentas relacionadas automáticamente.

Algunos de los sistemas operativos UNIX que son compatibles con el marco de trabajo de PAM son los siguientes:

- AIX v5.3 en la plataforma Power con PAM activado
- HP-UX v11.00 en una plataforma PA-RISC y en plataformas Itanium® 2
- Solaris v2.6 y posterior en plataformas Sparc e Intel
- Linux de 32 bits con glibc v2.2 y posterior en las plataformas s390 o i386 de Intel

  Nota: Para plataformas Linux, el binario test_sync debe estar en la RUTA de todos los usuarios, pero solamente los propietarios y usuarios raíz deben tener permisos de ejecución.

  Para agregar esta biblioteca a la ruta de todos los usuarios, incluya este comando en el archivo /etc/bashrc global:

  ```
  export PATH=$PATH:/etc/pam_CA_eta
  ```

Cómo funciona PAM de UNIX

El siguiente proceso describe las funciones de la característica PAM de UNIX:

1. La contraseña de un usuario de UNIX debe cambiarse por uno de los siguientes motivos:
   - Por decisión del usuario.
   - El usuario está obligado a cambiar la contraseña mediante la configuración del sistema o por intervención manual.
   - Un administrador cambia la contraseña del usuario.
2. La contraseña nueva se envía al servicio de contraseña del marco de trabajo de PAM.
3. El servicio de contraseña del marco de trabajo de PAM invoca la biblioteca de PAM para actualizar los archivos de seguridad de UNIX locales.
4. El servicio de contraseña del marco de PAM invoca el módulo de sincronización de contraseñas de UNIX (pam_CA_eta) para notificar al servidor de aprovisionamiento el cambio de contraseña.
5. El servidor de aprovisionamiento actualiza la contraseña del usuario global asociado y todas las cuentas asociadas a este.

Requisitos para utilizar la sincronización de contraseñas de UNIX

Los requisitos para utilizar la función de sincronización de contraseñas de UNIX son los siguientes:

- El agente de sincronización de contraseñas de UNIX se debe instalar en el sistema UNIX en el que desea detectar cambios de contraseña.
- Se tendrán que instalar CAM y el agente remoto de UNIX en el sistema UNIX en el que reside el agente de sincronización de contraseñas de UNIX.
- El sistema se debe gestionar como un punto final adquirido. Se debe activar la casilla de verificación Se ha instalado el agente de sincronización de contraseñas en las propiedades del punto final adquirido.
- Las cuentas de los sistemas gestionados se deben explorar y correlacionar con los usuarios globales.
- El entorno debe permitir cambios de contraseña que procedan de cuentas de puntos finales. Los administradores con acceso a la Consola de gestión activan esta función.

Instalación de la función de PAM de UNIX

Lleve a cabo el siguiente procedimiento para instalar PAM de UNIX.

Para instalar la función de PAM de UNIX

1. Seleccione el archivo de paquete que corresponde a la plataforma de UNIX:

Sistema operativo UNIX	Nombre de archivo del paquete
HP-UX v11 (PA-RISC)	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX (Itanium2)	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 (Power)	pam_CA_eta-1.1.AIX.tar.Z
Solaris (Sparc)	pam_CA_eta-1.1.Solaris.tar.Z
Solaris (Intel)	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux (x86)	pam_CA_eta-1.1.Linux.tar.gz
Linux (s390)	pam_CA_eta-1.1.LinuxS390.tar.gz

2. Transfiera el archivo de paquete que ha seleccionado a una carpeta temporal (/tmp) en el servidor de UNIX mediante FTP en modo binario, o bien con cualquier otra herramienta de transferencia de archivos que sea compatible con archivos binarios. Una sesión de transferencia de ejemplo podría mostrarse de la siguiente forma:

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. Inicie sesión como usuario raíz en el servidor de UNIX y extraiga el archivo de paquete:

   ```
   # cd /tmp
   # zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
   ```

   En Linux, utilice el comando:

   ```
   # tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
   ```

4. Copie la configuración y los archivos de TLS en la carpeta de configuración predeterminada:

   ```
   # cd pam_CA_eta-1.1
   # mv pam_CA_eta /etc
   ```

5. Copie el módulo de pam_CA_eta en la carpeta de bibliotecas de seguridad:

   En AIX, utilice el comando:

   ```
   # cp -p pam_CA_eta.o /usr/lib/security/
   ```

   En HP-UX, utilice el comando:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/
   ```

   En HP-UX Itanium2, utilice el comando:

   ```
   # cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
   ```

   En Linux i386 o s390, utilice el comando:

   ```
   # cp -p pam_CA_eta.so /lib/security/
   ```

   En Solaris (Sparc o Intel), utilice el comando:

   ```
   # cp -p pam_CA_eta.so /usr/lib/security/
   ```

6. (Opcional) Copie los programas de pruebas:

   ```
   # cp -p test_* /etc/pam_CA_eta
   # cp -p pam_test* (/usr)/lib/security/
   ```

Más información

Solución de problemas de sincronización de contraseñas de UNIX (en la página 145)

Actualización de puntos finales en la Consola de usuario

En la Consola de usuario, actualice el punto final para indicar que el agente se ha instalado.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Busque el punto final en el que se ha instalado el agente.
3. Haga clic en la ficha Configuración de punto final.
4. Active la casilla de verificación Agente de sincronización de contraseñas instalado.

Activación de entornos para la sincronización de contraseñas

Una vez que se instale el agente de sincronización de contraseñas, active el entorno para recibir los cambios de contraseña que se realicen en los puntos finales. Para esta tarea, un administrador tiene que acceder a la Consola de gestión y a CA Directory para activar el entorno con el fin de que se acepten estos cambios.

Siga estos pasos:

1. Para los nuevos usuarios, utilice la Consola de gestión de la siguiente forma:
   a. Seleccione el entorno.
   b. Haga clic en Configuración avanzada, Aprovisionamiento.
   c. Active la casilla de verificación Enable Password Changes from Endpoint Accounts (Activar cambios de contraseña de cuentas de puntos finales).
2. Para los usuarios existentes, establezca el atributo de eTPropagatePassword a 1 en CA Directory.

Configuración de la función de sincronización de contraseñas de UNIX

En la configuración de la función de sincronización de contraseñas de UNIX se utilizan parámetros de configuración en los siguientes archivos:

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

Importante: Dado que la contraseña de un usuario con privilegios de nivel alto se almacena en el archivo de configuración pam_CA_eta.conf, solamente se podrá leer ese archivo en la cuenta raíz. Tenga en cuenta que en las configuraciones del archivo en el archivo de paquete se incluyen las condiciones owner=raíz y mode=500, así como que el conmutador -p del comando cp las conserve durante la instalación.

Configuración del archivo pam_CA_eta.conf

Lleve a cabo el siguiente procedimiento para configurar el archivo pam_CA_eta.conf.

Para configurar el archivo pam_CA_eta.conf

1. Vaya a la carpeta /etc/pam_CA_eta.
2. Edite el archivo pam_CA_eta.conf. Este archivo de configuración contiene su propia documentación.

```
#
#   CA - CA Identity Manager
#
#   pam_CA_eta.conf
#
#   Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional
alternate server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
server
# value: a valid TCP/IP port number
# default: 20390
# port 20390


# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP
operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#              server is used.
#              Cloud based server is accessed by proxying the requests
#              through the on-premise CS, requiring use of remote-server
#              set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity
Manager server
# value: a numeric value
# default: 100
# size-limit 100


# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta


# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain    im


# keyword: user
# description: the CA Identity Manager Global User name used to bind to the
CA Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin


# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager
Global User
# value: the password of the above Global User
# default: no default
```

```
password SECRET


# keyword: directory-type
# description: the CA Identity Manager Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC


# keyword: endpoint-name
# description: the CA Identity Manager Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname"
command
#  (ie: getdomainname() system call) and "hostname" the result of the
"hostname"
#    command (ie: gethostname() system call)
# endpoint-name dirname


# keyword: tls-cacert-file
# description: the name of the CA Identity Manager CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem


# keyword: tls-cert-file
# description: the name of the CA Identity Manager client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem


# keyword: tls-key-file
# description: the name of the CA Identity Manager client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem


# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed


# keyword: use-status
```

```
# description: this module will exit with a non-zero status code in case of
failure.
# value: yes or no
# default: no
# use-status no


# keyword: verbose
# description: this module will display informational or error messages to
the user.
# value: yes or no
# default: yes
# verbose yes
```

Nota: Los parámetros de dominio, contraseña y servidor no tienen un valor predeterminado y deben actualizarse.

Configuración del archivo pam.conf

El archivo /etc/pam.conf es el archivo de configuración de PAM principal. Se debe editar el archivo para insertar una línea en la pila de servicio de contraseña. En algunos sistemas Linux, el archivo pam.conf se reemplaza por /etc/pam.d, por lo que se tendrá que editar el archivo /etc/pam.d/system-auth.

Para configurar el archivo pam.conf

1. Vaya al directorio /etc o /etc/pam.d si se está configurando el módulo de PAM en un sistema Linux adecuado.
2. Edite el archivo pam.conf para insertar una línea de sincronización de contraseñas en la pila de servicio de contraseña. Para configuraciones específicas de plataforma, consulte los siguientes ejemplos:

   passwd password required /usr/lib/security/pam_unix.so

   passwd password optional /usr/lib/security/pam_CA_eta.so

3. (Opcional) Se pueden agregar los siguientes parámetros opcionales en la línea de módulo pam_CA_eta:

   config=/path/file

   Indica la ubicación de un archivo de configuración alternativo.

   syslog

   Envía mensajes informativos y de error al servicio de syslog local.

   trace

   Genera un archivo de seguimiento para cada operación de actualización de contraseñas. Los archivos de seguimiento se denominan "/tmp/pam_CA_eta-trace.<nnnn>" donde "<nnnn>" es el número de PID del proceso de contraseña.

4. Implemente los siguientes cambios de configuración específicos de plataforma:

   Para sistemas AIX, agregue las siguientes líneas al final del archivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login   password  optional    /usr/lib/security/pam_CA_eta.so syslog
passwd  password  optional    /usr/lib/security/pam_CA_eta.so syslog
rlogin  password  optional    /usr/lib/security/pam_CA_eta.so syslog
su      password  optional    /usr/lib/security/pam_CA_eta.so syslog
telnet  password  optional    /usr/lib/security/pam_CA_eta.so syslog
sshd    password  optional    /usr/lib/security/pam_CA_eta.so syslog
OTHER   password  optional    /usr/lib/security/pam_CA_eta.so syslog
```

   Para sistemas HP-UX, agregue las siguientes líneas al final del archivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
```

   Para sistemas HP-UX Itanium2, agregue las siguientes líneas al final del archivo /etc/pam.conf:

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

```
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Para sistemas Sun Solaris, agregue la línea pam_CA_eta después de la línea pam_unix existente:

```
#

# Password management

#

other   password required       /usr/lib/security/pam_unix.so.1
other   password optional       /usr/lib/security/pam_CA_eta.so syslog
```

Para sistemas Linux, agregue la línea pam_CA_eta entre las líneas pam_cracklib y pam_unix existentes:

```
password    required     /lib/security/pam_cracklib.so retry=3 type=
password    optional     /lib/security/pam_CA_eta.so syslog
password    sufficient   /lib/security/pam_unix.so nullok use_authtok md5
shadow
password    required     /lib/security/pam_deny.so
```

5. Para sistemas AIX, edite el archivo /etc/security/login.cfg para establecer auth_type = PAM_AUTH. Se activa el marco de trabajo de PAM, que no está activado de forma predeterminada. Se trata de una configuración de período de ejecución, por lo que no se tendrá que reiniciar el sistema para que surta efecto.

Solución de problemas de sincronización de contraseñas de UNIX

Se pueden solucionar los problemas de la función de PAM de UNIX mediante syslog y mensajes de seguimiento, así como probando la configuración, la conexión de LDAP/TLS, la sincronización de contraseñas y el marco de trabajo de PAM.

Más información

Activación de mensajes de syslog (en la página 146)
Activación de mensajes de seguimiento (en la página 146)

Activación de mensajes de syslog

Agregue el parámetro de syslog a la línea pam_CA_eta en el archivo /etc/pam.conf para permitir que el módulo de pam_CA_eta genere mensajes informativos y de error. Cuando la opción de registro esté en uso, los administradores de UNIX verán mensajes de información en los archivos syslog cada vez que se cambie la contraseña de una cuenta de UNIX. Estos mensajes deben proporcionar la suficiente información para diagnosticar problemas fundamentales.

Se puede establecer esta opción de forma permanente en sistemas de producción, ya que no se requieren muchos más recursos que cuando se ejecuta en segundo plano.

Activación de mensajes de seguimiento

Si los mensajes de syslog no proporcionan la suficiente información, con el modo de seguimiento se pueden proporcionar más detalles. Para cada operación de actualización de contraseñas, el módulo de seguimiento genera un archivo denominado "/tmp/pam_CA_eta-trace.<nnnn>" (donde "<nnnn>" es el PID del proceso passwd) con una entrada para la mayoría de las llamadas de función que se utilizan en el módulo y de los datos que utilizan o devuelven dichas funciones.

Aunque los archivos de seguimiento solamente se puedan leer en la cuenta raíz, contendrán las contraseñas nuevas no cifradas. Por este motivo, este parámetro no se debe utilizar de forma permanente en un sistema de producción.

Prueba del archivo de configuración

Se puede utilizar la herramienta test_config, que se encuentra en el directorio /etc/pam_CA_eta, para verificar el archivo de configuración. En primer lugar, configure la estructura de carpetas del siguiente modo:

1. Mueva la carpeta pam_CA_eta a /etc.
2. Copie todo el contenido de pam_CA_eta-1.1 en /etc/pam_CA_eta.

Una entrada de línea de comando de ejemplo:

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

Una sesión de ejemplo:

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
El archivo de seguimiento es /tmp/test_config-trace.1274
```

Cuando se muestran los resultados del comando, se genera un archivo de seguimiento que contienen todos los detalles del análisis del archivo de configuración.

Visualización del servicio de CAM

Se puede realizar el procedimiento siguiente para descubrir quién ha iniciado el servicio.

Para ver el servicio de CAM

1. Inicie sesión en el equipo de UNIX como raíz mediante los clientes Telnet o SSH.
2. Emita el siguiente comando de UNIX:

   ```
   ps -ef | grep cam
   ```

   Se muestra una vista similar a la siguiente:

   ```
   root 13822        1 11 11:30:12 ?   0:00 cam
   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

Nota: Si el usuario raíz del sistema no inicia los servicios, se mostrarán como iniciados pero no podrá utilizarlos. CA Identity Manager emite un mensaje indicando que se ha denegado el permiso y que el usuario debe ser el usuario raíz.

Prueba de la conexión de LDAP/TLS

Se puede utilizar la herramienta test_ldap, que se encuentra en el directorio /etc/pam_CA_eta, para verificar la conexión al servidor de aprovisionamiento (mediante los parámetros del archivo de configuración). Una entrada de línea de comando de ejemplo:

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

Una sesión de ejemplo:

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
El archivo de seguimiento es /tmp/test_ldap-trace.1277
```

Cuando se muestra los resultados del comando, se genera un archivo de seguimiento que contienen todos los detalles del análisis del archivo de configuración y la conexión al servidor de aprovisionamiento.

Prueba de la sincronización de contraseñas

Se puede utilizar la herramienta test_sync, que se encuentra en la carpeta /etc/pam_CA_eta, para verificar que el servidor de aprovisionamiento propague de forma eficaz la actualización de contraseña de una cuenta local. Una entrada de línea de comando de ejemplo:

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

Una sesión de ejemplo:

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
Se inicia la sincronización de contraseñas de CA Identity Manager.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
La sincronización de contraseñas de CA Identity Manager se realiza correctamente.
/etc/pam_CA_eta/test_sync: succeeded
El archivo de seguimiento es /tmp/test_sync-trace.2244
```

Cuando se muestran los resultados del comando, se genera un archivo de seguimiento que contienen todos los detalles del análisis del archivo de configuración, la conexión al servidor de aprovisionamiento y la actualización de la cuenta.

Al utilizar el modo detallado (mediante el parámetro yes detallado predeterminado en el archivo de configuración), el comando proporciona mensajes de error potenciales e informativos sobre la propagación de contraseñas.

Prueba del marco de trabajo de PAM

Una biblioteca de prueba de PAM está disponible para verificar que el marco de trabajo de PAM detecte correctamente los cambios de contraseña.

Para probar el marco de trabajo de PAM

1. Copie el archivo pam_test en la carpeta /usr/lib/security(/hpux32).
2. Agregue una línea de clase de contraseña para la biblioteca de pam_test sin parámetros.

   A continuación, se muestra un ejemplo para Solaris:

   ```
   other password optional /usr/lib/security/pam_test
   ```
3. Emita un comando passwd en un usuario de prueba y, a continuación, busque la línea etiquetada pam_test[<pid>] en el archivo syslog.

   El resultado del comando muestra el nombre del archivo de seguimiento que se ha generado, por ejemplo:

   ```
   pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
   ```

Sincronización de contraseñas en OS400

El agente de sincronización de contraseñas permite que los cambios de contraseña, que se han realizado en el sistema de punto final OS/400, se propaguen a otras cuentas que se gestionan en CA Identity Manager. El agente de sincronización de contraseñas funciona de la siguiente forma:

1. Instala y ejecuta el agente en el sistema de punto final OS/400.

   Como parte de la instalación, el programa se registra en el sistema OS/400 para que, cuando los usuarios cambien sus contraseñas, el agente envíe los cambios de contraseña al servidor de aprovisionamiento.

2. El servidor de aprovisionamiento propaga el cambio de contraseña a las cuentas asociadas.

   El agente recibe los cambios de contraseña que se inician desde el comando Cambiar contraseña (CHGPWD) o la API Cambiar contraseña (QSYCHGPW).

3. El agente registra la operación correcta o errónea en un archivo de registro ubicado en PWDSYNCH/LOG.

El agente de sincronización de contraseñas es compatible con las siguientes plataformas:

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

Para instalar el agente de sincronización de contraseñas

1. Encuentre los medios de instalación del componente de aprovisionamiento.
2. Ejecute el instalador del agente de sincronización de contraseñas u OS/400 en \Agent.
3. Siga las instrucciones que se muestran en pantalla para completar la instalación.

   Nota: Las instrucciones de instalación del vínculo del software del agente de punto final se incluyen en las secciones siguientes.

Instalación del agente de sincronización de contraseñas de OS400

Se deben tener privilegios *ADDOBJ; además, se necesita lo siguiente para que el agente reciba notificaciones de cambio de contraseña:

- QPWDVLDPGM de valor de sistema se debe establecer en *REGFAC.
- El programa se debe registrar con el comando WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD)
- El entorno debe permitir cambios de contraseña que procedan de cuentas de puntos finales. Los administradores con acceso a la Consola de gestión activan esta función.

El agente se inicia solamente cuando se realiza un cambio de contraseña. Para cambiar la contraseña, emita el comando CHGPWD.

Nota: El usuario global se debe marcar para la sincronización de contraseñas.

En iSeries

1. Inicie sesión como usuario con privilegios *ALLOBJ y *SECADM (por ejemplo, QSECOFR).
2. Cree un usuario denominado "PWDSYNCH":

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Nota: Como medida de seguridad, el usuario se crea con la contraseña caducada.
3. Cree un archivo de guardado para almacenar el paquete de instalación en la biblioteca que seleccione (por ejemplo, MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. En el equipo de Windows con el archivo de guardado, utilice FTP para transferir el archivo de guardado a iSeries:

   ```
   ftp <hostname>
   binario
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. En iSeries, extraiga el programa del archivo de guardado:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Este comando extrae e instala el agente de sincronización en la biblioteca PWDSYNCH.
6. Verifique la instalación:

   ```
   DSPLIB PWDSYNCH
   ```

   Los siguientes objetos se deben mostrar:

Objeto	Tipo	Atributo
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Configure iSeries para utilizar PWDSYNCH como el programa de salida de validación de contraseña:

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```

8. En iSeries, especifique los parámetros de conexión para el servidor de conectores de CA IAM:

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

Instalación del agente de sincronización de contraseñas de OS400

Se deben tener privilegios *ADDOBJ; además, se necesita lo siguiente para que el agente reciba notificaciones de cambio de contraseña:

- QPWDVLDPGM de valor de sistema se debe establecer en *REGFAC.
- El programa se debe registrar con el comando WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD)
- El entorno debe permitir cambios de contraseña que procedan de cuentas de puntos finales. Los administradores con acceso a la Consola de gestión activan esta función.

El agente se inicia solamente cuando se realiza un cambio de contraseña. Para cambiar la contraseña, emita el comando CHGPWD.

Nota: El usuario global se debe marcar para la sincronización de contraseñas.

En iSeries

1. Inicie sesión como usuario con privilegios *ALLOBJ y *SECADM (por ejemplo, QSECOFR).
2. Cree un usuario denominado "PWDSYNCH":

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Nota: Como medida de seguridad, el usuario se crea con la contraseña caducada.

3. Cree un archivo de guardado para almacenar el paquete de instalación en la biblioteca que seleccione (por ejemplo, MYLIB):

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```

4. En el equipo de Windows con el archivo de guardado, utilice FTP para transferir el archivo de guardado a iSeries:

   ```
   ftp <hostname>
   binario
   cd MYLIB
   put PWDSYNCH.FILE
   ```

5. En iSeries, extraiga el programa del archivo de guardado:

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Este comando extrae e instala el agente de sincronización en la biblioteca PWDSYNCH.

6. Verifique la instalación:

   ```
   DSPLIB PWDSYNCH
   ```

   Los siguientes objetos se deben mostrar:

Objeto	Tipo	Atributo
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Configure iSeries para utilizar PWDSYNCH como el programa de salida de validación de contraseña:

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```

8. En iSeries, especifique los parámetros de conexión para el servidor de conectores de CA IAM (Servicios de la nube de CA IAM):

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

Actualización de puntos finales en la Consola de usuario

En la Consola de usuario, actualice el punto final para indicar que el agente se ha instalado.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Busque el punto final en el que se ha instalado el agente.
3. Haga clic en la ficha Configuración de punto final.
4. Active la casilla de verificación Agente de sincronización de contraseñas instalado.

Activación de entornos para la sincronización de contraseñas

Una vez que se instale el agente de sincronización de contraseñas, active el entorno para recibir los cambios de contraseña que se realicen en los puntos finales. Para esta tarea, un administrador tiene que acceder a la Consola de gestión y a CA Directory para activar el entorno con el fin de que se acepten estos cambios.

Siga estos pasos:

1. Para los nuevos usuarios, utilice la Consola de gestión de la siguiente forma:
   a. Seleccione el entorno.
   b. Haga clic en Configuración avanzada, Aprovisionamiento.
   c. Active la casilla de verificación Enable Password Changes from Endpoint Accounts (Activar cambios de contraseña de cuentas de puntos finales).
2. Para los usuarios existentes, establezca el atributo de eTPropagatePassword a 1 en CA Directory.

Configuración de SSL

Se utiliza SSL para cifrar la comunicación entre el agente de sincronización y el servidor de aprovisionamiento. Esto es importante para el agente de sincronización, ya que SSL envía contraseñas a través de la red. Se recomienda que siempre se utilice SSL.

El agente de sincronización debe confiar en el certificado del servidor de aprovisionamiento para conectarse con SSL. Por lo tanto, el certificado se debe instalar en el equipo de iSerie y configurarse para que el agente de sincronización confíe en el certificado. El gestor de certificados digitales, un componente opcional de OS/400, realiza estas tareas. Siga la documentación de OS/400 con respecto a la instalación y configuración del gestor de certificados digitales.

Instalación del certificado del servidor de aprovisionamiento

Se deben instalar los siguientes componentes de sistema operativo en el equipo de iSeries para utilizar SSL:

- Programa de licencia de proveedor de acceso criptográfico (5722 AC3)
- Gestor de certificados digitales (Opción 34 de OS/400)
- IBM HTTP Server para iSeries (5722-DG1)

En iSeries

1. Cargue el certificado del servidor de aprovisionamiento del equipo del servidor de aprovisionamiento en iSeries. El certificado se puede encontrar en la siguiente ruta:

   ```
   C:\Archivos de programa\CA\Identity Manager\Provisioning
   Server\Data\Tls\server\et2_cacert.pem
   ```

2. Inicie sesión en DCM.

   Utilice un explorador web para ir a http://<hostname>:2001. Cuando el sistema lo solicite, inicie sesión como QSECOFR y haga clic en el gestor de certificados digitales.

3. Haga clic la opción de selección de un almacén de certificados y seleccione el almacén de certificados *SYSTEM. Si este almacén no existe, cree un almacén llamado "*SYSTEM" y, a continuación, introduzca la contraseña del almacén de certificados.

4. Importe el certificado como certificado de autoridad de certificación mediante DCM.

   Haga clic en Gestionar certificados y, después, en Importar certificado. Seleccione la opción de la autoridad de certificación (CA) e introduzca el nombre de archivo del certificado de servidor de aprovisionamiento. (Aquí es donde se cargó el certificado en el paso 1). Introduzca la etiqueta Servidor de aprovisionamiento para el certificado.

5. Una vez que se haya importado el certificado de autoridad de certificación en el almacén de claves *SYSTEM de punto final, se debe asegurar de que el cliente de directorio de IBM QIBM_GLD_DIRSRV_CLIENT pueda acceder al almacén de claves *SYSTEM. De lo contrario, se produce un error de llamada de inicialización de SSL de PSA.

6. Configure la aplicación del cliente de servicios de directorio para que confíe en el certificado del servidor de aprovisionamiento. Para ello, abra la opción Gestionar aplicaciones, diríjase a Definir la lista de confianza de CA y seleccione al cliente de servicios de directorio.

   El certificado del servidor de aprovisionamiento debe mostrarse aquí si se importó correctamente en el paso 4.

   Haga clic en la opción De confianza para el certificado de servidor de aprovisionamiento: Después, haga clic en Aceptar.

7. Otorgue permiso de lectura PÚBLICO a los archivos de SSL y conceda acceso de lectura al almacén de certificados *SYSTEM:

   `(/QIBM/userdata/ICSS/Cert/Server/default.kdb)`

   Conceda permisos de lectura y ejecución en la carpeta principal.

   `(/QIBM/userdata/ICCS/Cert/Server)`

   Nota: La adopción de la autoridad de usuario PWDSYNCH no funciona en el sistema de archivos, por lo que se deben conceder permisos de acceso para todos los usuarios.

Desinstalación del agente de sincronización de contraseñas

Si se necesita desinstalar el agente de sincronización de contraseñas, siga este procedimiento.

En el punto de salida de validación de contraseña

1. Elimine PWDSYNCH:

   ```
   RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   ```

2. Suprima la biblioteca de agente de sincronización:

   ```
   DLTLIB PWDSYNCH
   ```

3. Suprima el usuario de PWDSYNCH:

   ```
   DLTUSRPRF PWDSYNCH
   ```

4. Elimine el certificado del servidor de aprovisionamiento siguiendo las instrucciones de SSL para iniciar sesión en DCM y trabaje con el almacén de certificados *SYSTEM:

   Haga clic en las opciones de gestionar certificados y suprimir certificado. A continuación seleccione la autoridad de certificación (CA).

   Seleccione el certificado Servidor de aprovisionamiento y haga clic en Suprimir.

Se debe establecer correctamente el parámetro de agente de contraseña de OS/400

El valor del parámetro "pwd_case_action" debe establecerse correctamente para que funcione. Entre los valores correctos se incluyen los siguientes:

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

Si pwd_case_action = [valor no válido], la contraseña se forzará a establecerse en mayúscula.

Nota: Al establecer el indicador pwd_case_action como pwd_to_uppercase o pwd_to_lowercase en el archivo de configuración OS400 PSA, la contraseña se podría no propagar de nuevo al usuario global si las contraseñas proporcionadas no cumplen con las configuraciones de la política de contraseñas en el servidor de aprovisionamiento. Por ejemplo, algunas políticas de contraseñas exigen que los valores de la contraseña contengan como mínimo 1 valor en mayúscula o en minúscula.

Nota: Anote el valor de sistema de QPWDLVL (nivel de contraseña) al configurar el agente de sincronización de contraseñas.

- Cuando QPWDLVL se establece en 0 (valor predeterminado) en el sistema AS400, se admiten contraseñas con una longitud de caracteres de 1 a 10 en mayúsculas.
- Cuando se establece QPWDLVL en 2 o 3, se permiten contraseñas de 1 a 128 caracteres con mezcla de mayúsculas y minúsculas.

De forma predeterminada, PSA propaga la contraseña sin cambios al servidor de aprovisionamiento. Sin embargo, con independencia del valor de QPWDLVL, se puede obligar a que PSA propague contraseñas con mayúsculas o minúsculas estableciendo "pwd_case_action" en "pwd_to_uppercase" o "pwd_to_lowercase" respectivamente.

Capítulo 7: Grupos

Se pueden crear varios tipos de grupos o una combinación de estos tipos:

- Grupo estático: una lista de usuarios que se agregan interactivamente
- Grupo dinámico: los usuarios pertenecen al grupo si cumplen una consulta LDAP (requiere un directorio LDAP como almacén de usuarios)

  Nota: El campo Consulta del grupo dinámico no se incluye en la tarea Crear grupo u otras tareas del grupo aunque este campo exista en directory.xml para un grupo. Para incluir el campo Consulta del grupo dinámico se debe editar la pantalla de perfil asociada.
- Grupo anidado: un grupo que contiene otros grupos (requiere un directorio LDAP como el almacén de usuarios)

Nota: Para ver los grupos estáticos, dinámicos y anidados a los que pertenece un usuario, utilice la ficha Grupos del objeto Usuario. La ficha aparece en las tareas Ver y Modificar usuario de forma predeterminada.

Esta sección contiene los siguientes temas:

Creación de un grupo estático

Puede asociar una colección de usuarios en un *grupo estático*. Para gestionar el grupo estático, agregue o suprima usuarios individuales de la lista de miembros. Para ver la lista de miembros de un grupo, use la ficha Pertenencia a, que se incluye en las tareas Ver y Modificar grupos de manera predeterminada.

Nota: La ficha Pertenencia a sólo muestra aquellos miembros que están agregados de forma explícita al grupo. No muestra los miembros que se agregan de manera dinámica.

Para crear un grupo estático:

1. En la Consola de usuario, seleccione Grupos, Crear grupo.
2. Decida si crear un grupo nuevo o una copia de un grupo, y haga clic en **Aceptar**.
3. En la ficha Perfil, introduzca un nombre de un grupo, una organización, una descripción y el nombre del administrador del grupo.

4. Haga clic en la ficha Pertenencia.
5. Haga clic en Agregar usuario.
6. Busque los usuarios que desea incluir.
7. Marque los usuarios y haga clic en Seleccionar.
8. Haga clic en Enviar.

Creación de un grupo dinámico

Puede crear un *grupo dinámico* al definir una consulta de filtro LDAP mediante la Consola de usuario para determinar dinámicamente la pertenencia a grupos en el tiempo de ejecución sin tener que buscar y agregar los usuarios por separado.

Por ejemplo, si desea generar un grupo que incluya todos los empleados de NeteAuto en Estados Unidos, puede definir un filtro de búsqueda de LDAP parecido al siguiente en el campo Consulta del grupo dinámico de la Consola de usuario:

ldap:///cn=Empleados,o=NeteAuto,c=US??sub

También podría modificar esta consulta para ubicar empleados fuera de los Estados Unidos.

Ejemplo de grupos estáticos, dinámicos y anidados (en la página 163) muestra el ejemplo de un grupo creado por grupos estáticos, dinámicos y anidados.

Para incluir el campo Consulta del grupo dinámico se debe editar la pantalla de perfil asociada. No se incluye de manera predeterminada en la tarea Crear grupo.

Nota: Para activar grupos dinámicos, los administradores del sistema configuran el soporte en el archivo de configuración del directorio (directory.xml):

- Agregue el elemento GroupTypes en la sección Comportamiento de los grupos del directorio tal y como se muestra a continuación:

  <GroupTypes type=*tipo*>

  tipo puede ser NESTED (en la página 161), DYNAMIC o ALL.

  GroupTypes distingue entre mayúsculas y minúsculas.
- Asigne el atributo conocido %DYNAMIC_GROUP_MEMBERSHIP% a un atributo físico que exista en el almacén de usuarios.

Para crear un grupo dinámico:

1. En la Consola de usuario, seleccione Grupos, Crear grupo.
2. Decida si crear un grupo nuevo o una copia de un grupo, y haga clic en **Aceptar**.

3. En la ficha Perfil, introduzca un nombre de un grupo, una organización, una descripción y el nombre del administrador del grupo.
4. En el campo Consulta del grupo dinámico, introduzca un filtro de búsqueda de LDAP como el del siguiente ejemplo:

   ldap:///cn=Empleados,o=NeteAuto,c=US??sub?
5. Haga clic en Enviar.

Nota: Sólo un administrador con la tarea Modificar grupo puede cambiar la pertenencia dinámica a un grupo.

Parámetros de la consulta del grupo dinámico

Puede utilizar los siguientes parámetros de consulta dinámica en la búsqueda:

ldap:///*<DN_base_búsqueda>*??*<ámbito_búsqueda>*?*<filtrobúsqueda>*

- *<DN_base_búsqueda>* es el punto en el que comienza la búsqueda en el directorio LDAP. Si no especifica el DN de base en la consulta, entonces la organización del grupo es el DN de base predeterminado.
- *<ámbito_búsqueda>* especifica el alcance de la búsqueda e incluye:
  - sub: devuelve entradas en el nivel del DN de base e inferior.
  - one: devuelve entradas un nivel por debajo del DN de base que especifique en la dirección URL. (predeterminado)
  - base: utiliza "one" y omite la base como opción de búsqueda

  Al usar one o base se obtienen únicamente los usuarios de la organización del nombre distintivo de la base.

  Con sub se obtienen todos los usuarios en la organización del nombre distintivo de la base y todas las suborganizaciones del árbol.

- *<filtrobúsqueda>* es el filtro que desea aplicar a las entradas incluidas en el ámbito de la búsqueda. Cuando introduzca un filtro de búsqueda, utilice la sintaxis de consulta LDAP estándar de esta forma:

  (<operador lógico ><comparación><comparación...>)

  - <operador lógico> es uno de los siguientes:

    Operador lógico O: |

    Operador lógico Y: &

    Operador lógico NO: !

  - <comparación> indica <atributo><operador><valor>

  Por ejemplo:

  (&(ciudad=boston)(estado=Massachusetts))

  El filtro de búsqueda predeterminado es (objectclass=*).

Al crear una consulta dinámica, tenga en cuenta lo siguiente:

- El prefijo "ldap" debe estar en minúscula, por ejemplo:

  ldap:///o=MiEmpresa??sub?(título=Gestor)

- No puede especificar el número de puerto o el nombre de host del servidor LDAP. Todas las búsquedas se producen dentro del directorio LDAP asociado con el entorno.

La tabla siguiente incluye consultas LDAP de muestra:

Descripción	**Consulta**
Todos los usuarios que son gestores.	ldap:///o=MiEmpresa??sub?(título=Gestor)
Todos los gestores de la sucursal oeste de Nueva York	ldap:///o=MiEmpresa??one?(&(título=Gestor) (roomNumber=NYOeste))
Todos los técnicos con teléfono móvil	ldap:///o=MiEmpresa??one? (&(tipoempleado=técnico) (móvil=*))
Todos los empleados cuyos números se encuentren entre 1000 y 2000	ldap:///o=MiEmpresa, (& (ou=empleado) (númeroempleado >=1000) (númeroempleado <=2000))
Todos los administradores del departamento de ayuda que han trabajado para la compañía durante más de seis meses	ldap:///o=MiEmpresa,(& (cn=adminayuda) (DOH => 2004/04/22) **Nota:** Esta consulta exige la creación de un atributo DOH para la fecha de contratación del usuario.

Nota: Las comparaciones > y < (mayor que y menor que) son lexicográficas, no aritméticas. Para obtener detalles sobre su uso, consulte la documentación correspondiente al servidor del directorio LDAP.

Creación de un grupo anidado

Si el almacén de usuarios es un directorio LDAP, puede agregar un grupo como miembro de otro grupo. Este grupo se denomina *grupo anidado*.

El grupo que contiene al grupo anidado se denomina *grupo principal*. Los miembros del grupo anidado se convierten en miembros del grupo principal. Sin embargo, los miembros del grupo principal no se convierten en miembros del grupo anidado.

Los grupos anidados son similares a las listas de distribución de correo electrónico, en las que una lista puede ser miembro de otra. Con los grupos anidados, puede agregar grupos y usuarios como miembros de un grupo. Al anidar un grupo en la lista de pertenencia de otro grupo, podría incluir los miembros de todos los grupos anidados.

Por ejemplo, si creara grupos independientes para las divisiones de fabricación, diseño, distribución y contabilidad de una empresa, para crear un grupo principal para toda la empresa debe anidar todos los grupos de divisiones independientes como miembros del grupo principal de la empresa. Como resultado, todos los cambios que realice en los grupos anidados de fabricación, diseño, distribución y contabilidad, se reflejarían automáticamente en el grupo anidado de toda la empresa. Un grupo anidado dentro de otro puede ser dinámico o puede contener otros grupos anidados.

La ilustración del Ejemplo de grupos estáticos, dinámicos y anidados (en la página 163) muestra un grupo principal creado por grupos estáticos, dinámicos y anidados.

Antes de crear un grupo anidado tenga en cuenta lo siguiente:

- Sólo un administrador con la tarea Modificar miembros del grupo puede agregar o modificar grupos anidados a partir de la lista de miembros estáticos del grupo en la Consola de usuario.
- Sólo los usuarios con los privilegios de administrador apropiados pueden modificar, agregar o eliminar miembros de un grupo.

  Por ejemplo, si los grupos anidados B y C crean al grupo principal A, el administrador del Grupo A sólo puede modificar los miembros de dicho grupo, y no los del grupo B y C. Los grupos B y C sólo pueden ser modificados por sus respectivos administradores.
- Para activar grupos anidados, los administradores del sistema configuran el soporte del grupo anidado en el archivo de configuración del directorio (directory.xml):
  - Agregue el elemento GroupTypes en la sección Comportamiento de los grupos del directorio tal y como se muestra a continuación:

    <GroupTypes type=*tipo*>

    tipo puede ser NESTED, DYNAMIC (en la página 158) o ALL.

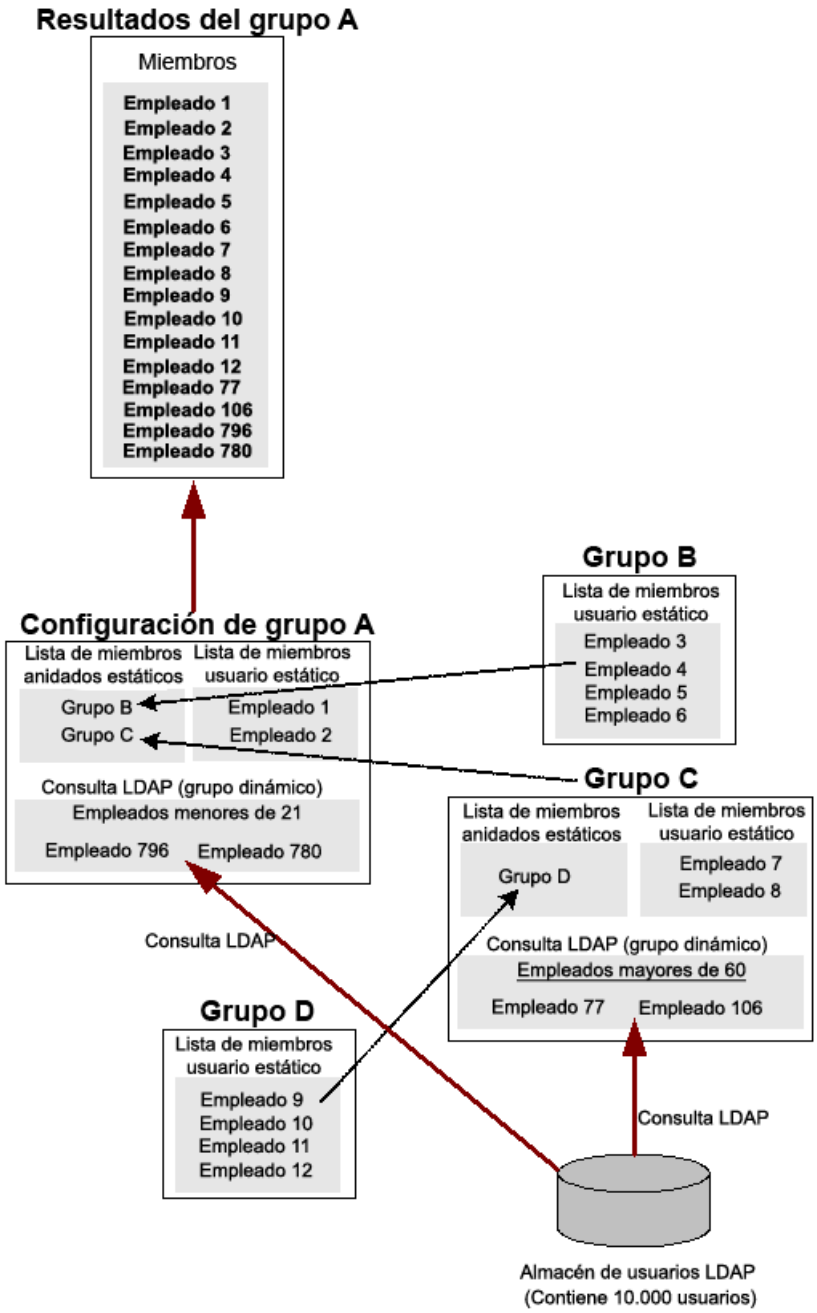
    GroupTypes distingue entre mayúsculas y minúsculas.
  - Asigne el atributo conocido %NESTED_GROUP_MEMBERSHIP% a un atributo físico que exista en el almacén de usuarios.

Para crear un grupo anidado:

1. En la Consola de usuario, seleccione Grupos, Crear grupo.
2. Decida si crear un grupo nuevo o una copia de un grupo, y haga clic en **Aceptar**.
3. En la ficha Perfil, introduzca un nombre de un grupo, una organización, una descripción y el nombre del administrador del grupo.
4. En la ficha Pertenencia a:
   a. Haga clic en Agregar grupo para agregar un grupo anidado al grupo.
   b. Busque un grupo existente.
   c. Coloque una marca junto al grupo y haga clic en Seleccionar.
   d. Haga clic en Enviar.

Ejemplo de grupos estáticos, dinámicos y anidados

Los grupos pueden ser complejos y constar de una combinación de grupos dinámicos, estáticos o anidados. En la ilustración siguiente, se muestra un ejemplo de un grupo principal creado por grupos estáticos, dinámicos y anidados.



En la ilustración anterior:

- El Grupo principal A contiene a los grupos anidados B y C, dos usuarios estáticos y una consulta LDAP dinámica que enumera a todos los empleados menores de 21 años.
- El Grupo B está formado por cuatro usuarios estáticos.
- El Grupo principal C contiene al Grupo anidado D, dos usuarios estáticos y una consulta LDAP dinámica que enumera a todos los empleados mayores de 60 años.
- El Grupo D contiene cuatro usuarios estáticos.
- La parte superior de la ilustración muestra a los miembros del Grupo A que resultan de los grupos anidados, las consultas dinámicas y las listas de miembro de usuarios estáticos de los grupos B, C y D.

Administradores de grupo

En la ficha Administradores de las tareas Crear o Modificar grupo, se pueden especificar usuarios y grupos como administradores de un grupo. Cuando se asigna un usuario como administrador de un grupo, asegúrese de que el administrador tenga el rol con el ámbito adecuado para gestionar el grupo. Por ejemplo:

1. Utilice Modificar grupo para asignar un usuario como administrador de un grupo.
2. Asigne a dicho usuario un rol de administrador con tareas de gestión de grupos como, por ejemplo, Modificar miembros del grupo o tareas de gestión de usuarios con una ficha Grupos.
3. Compruebe que el rol tenga el ámbito adecuado sobre el grupo.
    a. Utilice Ver rol de administrador en el rol asignado con las tareas de gestión de grupos.
    b. En la ficha Miembros, verifique que una política existe con lo siguiente:

        Una regla de miembros que cumpla el administrador del grupo.

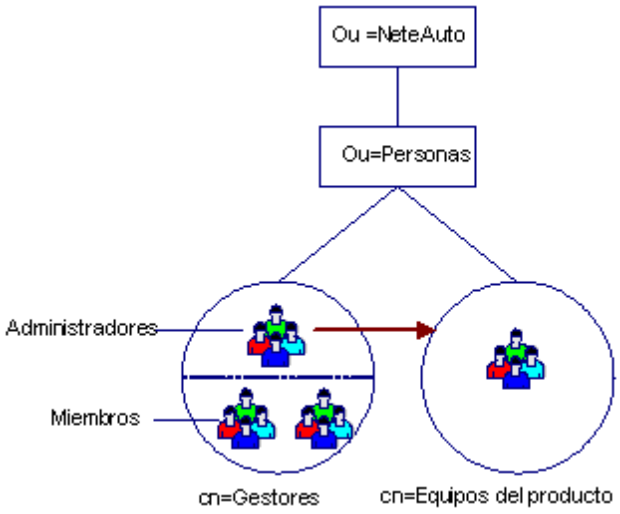
        Una regla de ámbito que incluya al grupo.

        Una regla de ámbito que incluya algunos usuarios que se deben agregar al grupo.

Nota: Para permitir que unos grupos sean administradores de otros grupos, los administradores del sistema configuran el soporte del administrador de grupos en el archivo de configuración del directorio (directory.xml):

- Establezca AdminGroupTypes type=ALL en la sección Comportamiento de grupos de administración del directorio. AdminGroupTypes distingue entre mayúsculas y minúsculas.
- Asigne el atributo conocido %GROUP_ADMIN_GROUP% a un atributo físico que exista en el almacén de usuarios.

Cuando se asigne un grupo como un administrador, solamente los administradores de ese grupo serán administradores del grupo que se está creando o modificando. Los miembros del grupo del administrador que se especifique no tendrán ningún privilegio para gestionar el grupo. La ilustración siguiente muestra un grupo como administrador de otro grupo.



En este ejemplo:

- El grupo Gestores es un administrador del grupo Equipos del producto.
- Los administradores del grupo Gestores pueden gestionar el grupo Equipos del producto. Los miembros del grupo Gestores no pueden.

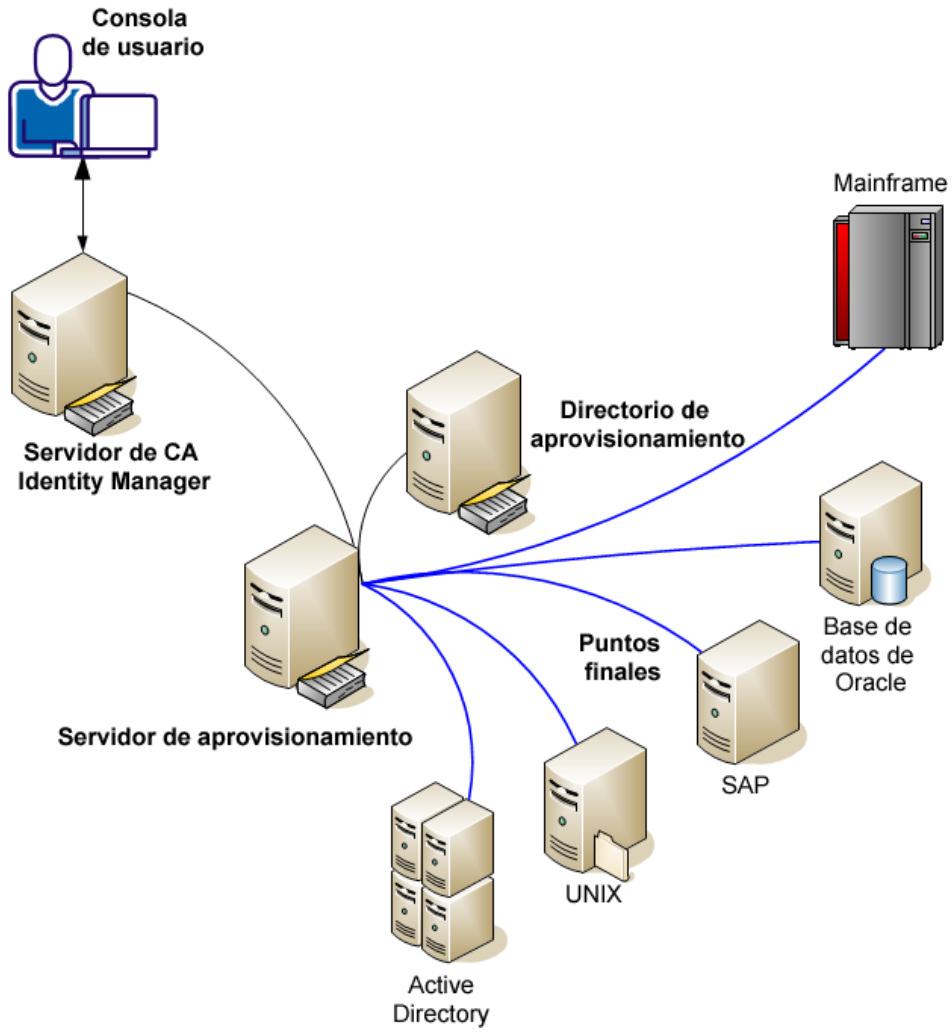
Capítulo 8: Cuentas de punto final gestionadas

En CA Identity Manager, se pueden gestionar las cuentas en sistemas de punto final si la instalación de CA Identity Manager tiene un servidor de aprovisionamiento. Se pueden gestionar las cuentas, como una cuenta de Exchange, Windows NT u Oracle y gestionar cuentas huérfanas y del sistema, que sean cuentas que no estén asociadas actualmente con CA Identity Manager.

Esta sección contiene los siguientes temas:

Integración de puntos finales gestionados

Con CA Identity Manager se pueden gestionar cuentas en varios sistemas desde una sola interfaz de usuario, la Consola de usuario. Las cuentas están en sistemas a los que se hace referencia como puntos finales gestionados, o sencillamente puntos finales. En el ejemplo siguiente se gestionan usuarios en cinco puntos finales.



Se pueden asignar cuentas con cualquier combinación de puntos finales a un usuario. Cuando se integra el punto final, CA Identity Manager asocia cada cuenta de punto final con un usuario en el directorio de aprovisionamiento.

Los procedimientos siguientes describen cómo integrar puntos finales de manera que las cuentas de punto final se puedan gestionar desde la Consola de usuario.

1. Importación del archivo de definición del rol (en la página 169)
2. Creación de reglas de correlación
3. Agregación del punto final al entorno
4. Creación de una definición de exploración y correlación
5. Exploración y correlación del punto final

Importación del archivo de definición del rol

Se importan las definiciones del rol desde un archivo que se aplica al nuevo punto final. Este procedimiento requiere acceso a la Consola de gestión.

Siga estos pasos:

1. En la Consola de gestión, haga clic en Entornos.
2. Seleccione el entorno en el que se está agregando el punto final.
3. Haga clic en Configuración de roles y tareas.
4. Haga clic en Importar.
5. Seleccione un punto final en Tipo de punto final.
6. Haga clic en Finalizar.

   El estado de la importación aparece en la ventana actual.
7. Haga clic en Continuar para salir.
8. Reinicie el entorno para que se apliquen los cambios.

Creación de reglas de correlación

Un administrador de hospedaje o un administrador con la tarea Configuración de atributos de correlación puede crear reglas que se utilizan cuando se examina un punto final. La tarea Ejecutar exploración y correlación utiliza estas reglas para la parte de correlación de la tarea.

Las reglas de correlación determinan cómo se asigna un atributo de cuenta de punto final a un atributo de usuario en la Consola de usuario. Por ejemplo, en el Control de acceso existe un atributo que se llama AccountName. Se puede crear una regla para asignarlo a FullName en la Consola de usuario. Si las reglas hacen que dos asignaciones se apliquen a un atributo de usuario, se utilizará el primer valor del parámetro.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Haga clic en Sistema, Configuración del aprovisionamiento, Configuración de atributos de correlación.
3. Haga clic en Agregar.
4. Defina una regla de correlación como se muestra a continuación:
   a. Seleccione una lista de atributos de usuario global.

      Este valor hace referencia al atributo de usuario clasificado en el directorio de aprovisionamiento.

   b. Active la casilla de verificación Establecer un atributo de cuenta específico.

   c. Seleccione un tipo de punto final.

   d. Seleccione un atributo de cuenta que se aplica al atributo de usuario global.

   e. Opcionalmente, complete los campos de subcadena.

      Si el campo Subcadena de está vacío, el procesamiento empieza al principio de la cadena. Si el campo Subcadena a está vacío, el procesamiento empieza al final de la cadena.
5. Haga clic en OK.
6. Haga clic en Enviar.

Nota: Cuando se cambia una regla de correlación, es necesario asegurarse de examinar el punto final aunque se haya examinado previamente.

Ejemplo de reglas de correlación

El ejemplo siguiente proporciona valores de configuración de muestra para un punto final de Active Directory.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

Las acciones siguientes se producen en cada cuenta previamente no correlacionada que se encuentra mientras se correlacionan las cuentas en un contenedor de Active Directory:

1. El servidor de aprovisionamiento compara el primer valor del parámetro (GlobalUserName) con el atributo de cuenta de punto final de Active Directory (NT_AccountID). El servidor intenta encontrar el usuario global único cuyo nombre coincide con el valor del atributo de NT_AccountID para esa cuenta. Si se encuentra una coincidencia única, el servidor de aprovisionamiento asocia la cuenta con el usuario global. Si se encuentra más de una coincidencia, el servidor de aprovisionamiento realiza el paso 5. Si no se encuentra ninguna coincidencia, el servidor de aprovisionamiento realiza el paso siguiente.
2. El servidor de aprovisionamiento tiene en cuenta el segundo valor del parámetro (FullName=LDAP Namespace:globalFullName). Como este valor es específico de otro tipo de punto final, se omitirá y el servidor de aprovisionamiento realizará el paso siguiente.
3. El servidor de aprovisionamiento tiene en cuenta el tercer valor del parámetro (FullName=ActiveDirectory:DisplayName). Como este valor es específico de Active Directory, se utilizará. El servidor intenta encontrar el usuario global único cuyo nombre completo coincide con el valor del atributo de DisplayName para esa cuenta. Si se encuentra una coincidencia única, el servidor de aprovisionamiento asocia la cuenta con el usuario global. Si se encuentra más de una coincidencia, el servidor de aprovisionamiento realiza el paso 5. Si no se encuentra ninguna coincidencia, el servidor de aprovisionamiento realiza el paso 4.
4. El servidor de aprovisionamiento tiene en cuenta el valor del parámetro final (CustomField01=ActiveDirectory:Telephone). Como este valor es específico de Active Directory, se utilizará. El servidor intenta encontrar el usuario global único cuyo atributo Campo personalizado #01 es igual al valor del atributo Teléfono para esa cuenta. El nombre que se ha dado al atributo de usuario global personalizado mediante las propiedades globales de la tarea del sistema no se muestra aquí. Si se encuentra una coincidencia única, el servidor de aprovisionamiento asocia la cuenta con el usuario global. Si se encuentra más de una coincidencia, el servidor de aprovisionamiento realiza el paso 5. Si no se encuentra ninguna coincidencia, el servidor de aprovisionamiento realiza el paso siguiente.
5. El servidor de aprovisionamiento asocia la cuenta con el objeto [usuario predeterminado]. Si el objeto [usuario predeterminado] no existe, el servidor lo crea.

Agregación del punto final al entorno

Agrega el punto final al entorno donde pretende gestionarlo. Cualquier administrador con la tarea Crear punto final puede realizar este procedimiento.

Siga estos pasos:

1. Seleccione Puntos finales, Gestionar puntos finales, Crear punto final.
2. Seleccione un tipo de punto final.
3. Complete las fichas para rellenar los campos.

   Los campos obligatorios comienzan por un círculo rojo.

   Nota: No utilice el símbolo # en el nombre de un punto final, ya que este carácter no se puede buscar.
4. Haga clic en Enviar.

Ahora ya se puede crear una tarea de Definición de exploración y correlación (en la página 172) de manera que se puedan gestionar sus cuentas.

Creación de una definición de exploración y correlación

Para agregar usuarios que existen en un punto final, se debe crear una definición de exploración y correlación para ese punto final. Cualquier administrador con la tarea Crear definición de exploración y correlación puede crear la definición.

Siga estos pasos:

1. En un entorno de CA Identity Manager, haga clic en Puntos finales, Definiciones de exploración y correlación y Crear definición de exploración y correlación.
2. Haga clic en Aceptar para iniciar una nueva definición.
3. Escriba el nombre de Explorar y correlacionar con una palabra significativa.
4. Haga clic en Seleccionar contenedor/punto final/método de exploración para elegir un punto final y los contenedores, si existen. Para un punto final grande, una búsqueda de contenedor puede tardar un rato; se puede utilizar el filtro de búsqueda para estrechar la búsqueda.
5. Seleccione un método de exploración para el contenedor. El proceso de exploración y correlación incluye los contenedores que elija y sus subcontenedores. En un contenedor de directorios, incluye todos los contenedores del árbol secundario.

6. Haga clic en las acciones de exploración/correlación que vaya a realizar:
   - **Explorar directorio para objetos gestionados**: busca objetos almacenados en el punto final, no en el directorio de aprovisionamiento.
   - **Correlacionar cuentas con usuarios**: correlaciona los objetos que se encontraron con la función de exploración con los usuarios del directorio de aprovisionamiento. Existen dos elecciones de correlación.
     - **Utilizar usuario existente**

       Utilice esta opción para aplicar una regla de correlación (en la página 169) que asigna cada cuenta a un usuario creado previamente.

       Si se encuentra el usuario, la cuenta se correlaciona con dicho usuario. Si se encuentran varios usuarios, la cuenta se correlaciona con el usuario predeterminado. Si no se encuentra ningún usuario, esta opción crea el usuario (si se conocen todos los atributos obligatorios) y correlaciona la cuenta con dicho usuario; de lo contrario, correlaciona la cuenta con el usuario predeterminado.
     - **Crear usuarios según la necesidad**

       Utilice esta opción al correlacionar cuentas en su punto final primario. Esta opción supone que las cuentas del punto final se denominan exactamente igual que los usuarios. El algoritmo de correlación coincidente queda sin utilizar con esta opción. En lugar de ello, cada cuenta se asocia al usuario con el mismo nombre. Si el usuario todavía no existe, se crea. No hay ninguna cuenta asociada al usuario predeterminado.
   - **Actualizar campos de usuario**: si existe una asignación entre los campos de los objetos y los campos de los usuarios, estos últimos se actualizan con los datos de los campos de los objetos.

     Se crean usuarios sin atributos opcionales como nombre completo, dirección y números de teléfono. Durante la adquisición inicial de un punto final, utilice esta opción para definir estos atributos de usuario mediante los valores de atributo de cuenta. Durante la exploración y correlación subsiguientes, utilice esta opción para actualizar los atributos de usuario a fin de aplicar los cambios hechos a los atributos de cuenta, quizás por herramientas distintas de CA Identity Manager.
7. Haga clic en Enviar.

Ahora un administrador con la tarea Ejecutar exploración y correlación (en la página 174) completa la integración del punto final.

Exploración y correlación del punto final

Administrador de hospedaje u otro administrador con la tarea Ejecutar exploración y correlación realiza este procedimiento. La fase de exploración de la tarea identifica las cuentas en el punto final. La fase de correlación asigna las cuentas a los usuarios de CA Identity Manager o crea las cuentas.

Siga estos pasos:

1. En un entorno de CA Identity Manager, haga clic en Puntos finales, Ejecutar exploración y correlación.
2. Seleccione Ejecutar ahora para ejecutar la exploración y la correlación inmediatamente o seleccione Programar nuevo trabajo (en la página 427) para ejecutar la exploración y correlación más adelante o según una programación repetitiva.

   Nota: Para realizar esta operación es necesario que el explorador cliente se encuentre en la misma zona horaria que el servidor. Por ejemplo, si en el cliente son las 22:00 del martes y en el servidor son las 07:00, la definición de exploración y correlación no funcionará.
3. Haga clic en una definición de exploración y correlación para ejecutarla.
4. Haga clic en Enviar.

   Las cuentas de usuario que existen en el punto final se crean o actualizan en CA Identity Manager en función de la definición de exploración y correlación que haya creado.
5. Verifique que la tarea se ha realizado correctamente de la siguiente manera:
   a. Seleccione Sistema, Ver tareas enviadas.
   b. Rellene el campo de nombre de la tarea como se indica a continuación: Ejecutar exploración y correlación
   c. Haga clic en Buscar.

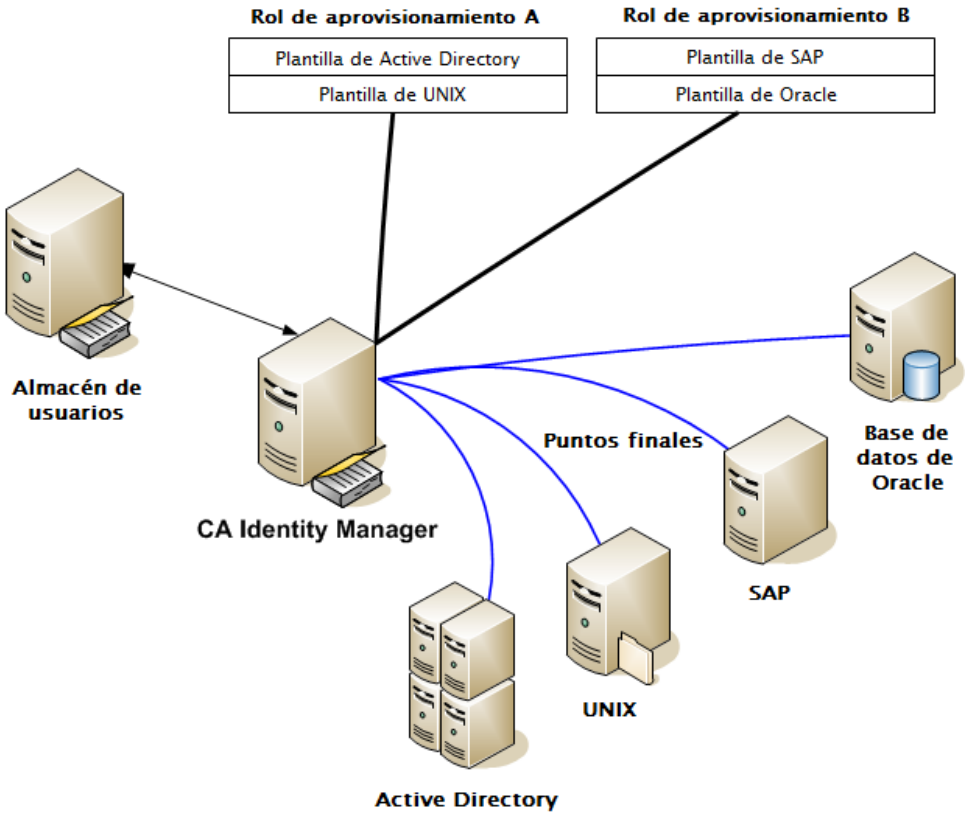
   Los resultados mostrarán si la tarea se ha realizado correctamente.

Nota: Se puede anular una tarea de exploración y correlación al consultar el estado de la tarea en Ver tareas enviadas (VST). Al anular una tarea se detiene el procesamiento de la misma, dejando la tarea en el estado que estaba cuando se anuló. Cualquier notificación generada se enviará para que todos los sistemas se mantengan sincronizados.

Sincronización de usuarios, cuentas y roles

La integración de varios puntos finales y cuentas en un solo sistema de gestión de usuarios puede dar lugar a una pérdida de sincronización. Los roles de aprovisionamiento o plantillas de cuenta que se asignan a un usuario pueden diferir de las cuentas reales que existen para ese usuario.

Por ejemplo, pongamos una situación con dos roles de aprovisionamiento, uno con Active Directory y plantillas de cuenta de UNIX y otro rol con SAP y plantillas de Oracle. El usuario john_smith tiene el rol de aprovisionamiento A, que contiene Active Directory y plantillas de cuenta de UNIX, pero ese usuario solamente tiene una cuenta de Active Directory. Posiblemente la plantilla de cuenta de UNIX se ha agregado al rol después de que se asignara al usuario. Por lo tanto, el administrador sincroniza el usuario con la definición del rol actual.



Las situaciones siguientes son otros motivos por los cuales los usuarios pierden sincronización con roles de aprovisionamiento o plantillas de cuenta:

- Los intentos anteriores de crear las cuentas necesarias han producido un error debido a problemas de hardware o software en su red, causando que falten algunas cuentas.
- Los roles de aprovisionamiento y las plantillas de cuenta cambian, creando así cuentas adicionales o que faltan.
- Las cuentas se han asignado a plantillas de cuenta después de que se crearan, de manera que las cuentas existen pero no están sincronizadas con sus plantillas de cuenta.
- La creación de una nueva cuenta se retrasa porque se ha especificado que la cuenta se creará más tarde.
- Se ha adquirido un nuevo punto final. Durante la exploración y la correlación, el servidor de aprovisionamiento no asignaba roles de aprovisionamiento a los usuarios automáticamente. Se debe actualizar el rol para indicarlo a los usuarios que requieran cuentas en el punto final. Cualquier cuenta que se haya correlacionado con un usuario se clasifica como cuenta adicional cuando se sincroniza el usuario.
- Se ha asignado una cuenta existente a un usuario copiando la cuenta al usuario.
- Se ha creado una cuenta para un usuario en lugar de asignar el usuario a un rol. Por ejemplo, se ha copiado un usuario a una plantilla de cuenta que no está en un rol de aprovisionamiento para ese usuario. La cuenta se ha clasificado como cuenta adicional o como cuenta con una plantilla de cuenta adicional. Si se copia el usuario en un punto final para crear una cuenta mediante la plantilla de cuenta predeterminada, esa cuenta podría ser una cuenta adicional.

Las secciones siguientes explican cómo realizar los tres tipos de sincronización:

1. Sincronización de usuarios con roles (en la página 177).
2. Sincronización de usuario con plantillas de cuenta (en la página 177).
3. Sincronización de cuenta de punto final con plantillas de cuenta (en la página 179).

Sincronización de usuario con roles

Esta tarea crea, actualiza o suprime cuentas para que cumplan con los roles de aprovisionamiento asignados a un usuario. Por ejemplo, los administradores utilizan herramientas nativas en un punto final para agregar o suprimir cuentas, pero no ha vuelto a explorar ese punto final para actualizar el directorio de aprovisionamiento. Por lo tanto, los usuarios tendrán cuentas adicionales o que faltan. Esta tarea también asegura que cada cuenta pertenece a las plantillas de cuenta correctas.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Tareas, Usuarios, Sincronización, Comprobar sincronización del rol.
3. Seleccione un usuario.

   Aparecerá una pantalla que muestra las cuentas esperadas, cuentas adicionales o cuentas que faltan.
4. Haga clic en Sincronizar para hacer que las cuentas coincidan con la plantilla de este rol.
   a. Se puede seleccionar una casilla de verificación para crear la cuenta en el punto final. Si más de una plantilla de cuenta para el usuario indica la misma cuenta, la cuenta se crea combinando todas las plantillas de cuenta relevantes.

      Esta cuenta se asigna a las plantillas de cuenta que no están actualmente sincronizadas con la cuenta.
   b. Se puede seleccionar una casilla de verificación para suprimir cuentas adicionales. Sin embargo, los usuarios pueden tener motivos legítimos para tener estas cuentas. En este caso, se debe dejar esta opción sin marcar.

      En ciertos puntos finales, la función de supresión de cuentas está desactivada; por lo tanto, la cuenta no se suprime.

Sincronización de usuario con plantillas de cuenta

Esta tarea sincroniza los atributos para las cuentas de punto final con las plantillas de cuenta asociadas para un usuario. Sin embargo, la sincronización completa depende de los siguientes factores:

- La sincronización completa de la cuenta se produce en dos situaciones. Una plantilla de cuenta utiliza la sincronización estricta (en la página 180) o dos o más plantillas de cuenta se han agregado a una cuenta.
- Si una plantilla de cuenta utiliza la sincronización débil (en la página 180), esta tarea inicia una sincronización de cuenta que implica solamente esta plantilla. Si la cuenta no estaba al principio sincronizada con otras plantillas de cuenta antes de esta actualización, es posible que no estuviera tampoco sincronizada después.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Tareas, Usuarios, Sincronización, Comprobar sincronización de plantilla de cuenta.
3. Seleccione un usuario.

   Aparecerá una pantalla que muestra las cuentas esperadas, cuentas adicionales o cuentas que faltan.
4. Haga clic en Sincronizar para hacer que las cuentas coincidan con la plantilla.

   a. Se puede seleccionar una casilla de verificación para crear la cuenta en el punto final. Si más de una plantilla de cuenta para el usuario indica la misma cuenta, la cuenta se crea combinando las plantillas de cuenta relevantes.

      Esta cuenta se asigna a las plantillas de cuenta que no están sincronizadas con la cuenta. La sincronización de cuentas no es necesaria en las nuevas cuentas creadas.

   b. Se puede seleccionar una casilla de verificación para suprimir cuentas adicionales. Sin embargo, los usuarios pueden tener motivos legítimos para tener estas cuentas. En este caso, se debe dejar esta opción sin marcar.

      En ciertos puntos finales, la función de supresión de cuentas está desactivada; por lo tanto, la cuenta no se suprime.

Atributos exclusivos para nuevas cuentas

En una plantilla de cuenta, algunos atributos sólo se aplican cuando se crea la cuenta. Por ejemplo, el atributo de contraseña es una expresión de regla que define la contraseña para las nuevas cuentas. Esta expresión de regla nunca actualiza la contraseña de una cuenta. Los cambios de la expresión de regla de contraseña sólo repercuten en las cuentas que se crean después de que se haya configurado la expresión de regla.

De igual manera, una expresión de regla de plantilla para un atributo de cuenta de sólo lectura sólo repercute en las cuentas que se crean después de que se haya configurado la expresión de regla. El cambio no repercute en las cuentas existentes.

Sincronización de cuentas de punto final con plantillas de cuenta

Esta tarea sincroniza una cuenta de punto final después de la modificación de una plantilla de cuenta asociada. Por ejemplo, quizás una cuenta de Active Directory no tiene ningún grupo, pero la plantilla de cuenta asociada está definida para incluir grupos.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Tareas, Puntos finales, Gestionar puntos finales, Comprobar sincronización de cuentas de puntos finales.
3. Seleccione un punto final.

   Se abrirá una pantalla que muestra las cuentas en ese punto final, las plantillas de cuenta asociadas y qué atributos no están sincronizados.
4. Haga clic en Sincronizar para hacer que los atributos de esas cuentas coincidan con lo definido en la plantilla de cuenta.

   Los cambios realizados en las plantillas de cuenta afectan a las cuentas existentes como se muestra a continuación:

   - Si se cambia el valor de un atributo de capacidad, se actualizará el atributo de cuenta correspondiente para que esté sincronizado con el valor de atributo de la plantilla de cuenta. Consulte la descripción de la sincronización débil y estricta.
   - El conector designa algunos atributos de cuenta como no actualizados por los cambios de la plantilla de cuenta. Los ejemplos incluyen ciertos atributos que el tipo de punto final solamente permite establecer durante la creación de cuenta y el atributo Contraseña.

Atributos actualizados

Al cambiar los atributos de capacidad de una plantilla de cuenta, el atributo correspondiente en las cuentas cambiará. Este cambio tiene un impacto en los atributos de la cuenta. El impacto se basa en los factores siguientes:

- Si la plantilla de cuenta se ha definido para usar la sincronización débil o fuerte.
- Si la cuenta pertenece a varias plantillas de cuenta.

Sincronización débil

La *sincronización débil* garantiza que los usuarios tengan los atributos de capacidad mínimos para sus cuentas. La sincronización débil es el valor predeterminado en la mayoría de los tipos de puntos finales. Si se actualiza una plantilla que utiliza la sincronización débil, CA Identity Manager actualiza los atributos de capacidad como se muestra a continuación:

- Si se actualiza un campo de número en una plantilla de cuenta, y el nuevo número es mayor que el número de la cuenta, CA Identity Manager cambiará el valor de la cuenta para que coincida con el nuevo número.
- Si no se seleccionó una casilla de verificación en una plantilla de cuenta y, posteriormente, la selecciona, CA Identity Manager actualizará la casilla de verificación en cualquier cuenta en la que la casilla de verificación no esté seleccionada.
- Si se modifica una lista en una plantilla de cuenta, CA Identity Manager actualizará todas las cuentas para incluir los valores de la nueva lista que no estuvieran incluidos en la lista de valores de la cuenta.

Si una cuenta pertenece a otras plantillas de cuenta (tanto si estas plantillas utilizan sincronización débil como estricta), CA Identity Manager sólo consultará la plantilla que se esté modificando. Esta acción es más eficaz que comprobar cada plantilla de cuenta. Dado que la sincronización débil sólo agrega capacidades a las cuentas, generalmente no es necesario consultar otras plantillas de cuenta.

Nota: Cuando se propagan desde una plantilla de cuenta de sincronización débil, los cambios que eliminarían o reducirían las capacidades, podrían dejar algunas cuentas no sincronizadas. Recuerde que con la sincronización débil, las capacidades no se eliminan ni se reducen nunca. Sin consultar otras plantillas de una cuenta, la propagación no tiene en cuenta si es suficiente la sincronización débil.

En esta situación, utilice Sincronizar usuario con plantillas de cuenta para sincronizar la cuenta con sus plantillas de cuenta.

Sincronización estricta

La sincronización estricta garantiza que las cuentas tengan los atributos de cuenta exactos que se especifican en la plantilla de cuenta.

Por ejemplo, supongamos que se agrega un grupo a una plantilla de cuenta de UNIX existente. Originalmente, la plantilla de cuenta hacía miembros de cuentas del grupo Personal. Ahora se desean hacer miembros de cuentas tanto a los grupos de personal como al del sistema. Todas las cuentas asociadas a la plantilla de cuenta se consideran que están sincronizadas cuando cada cuenta es miembro de los grupos de sistema y personal (y de ningún otro grupo). Cualquier cuenta que no esté en el grupo de personal se agregará a ambos grupos.

Otros factores que se deben tener en cuenta:

- Si la plantilla de cuenta utiliza la sincronización estricta, cualquier cuenta que pertenezca a grupos distintos de Personal y Sistema, se eliminará de esos grupos extra.
- Si la plantilla de cuenta utiliza la sincronización débil, las cuentas se agregan a los grupos Personal y Sistema. Cualquier cuenta que tenga definidos grupos adicionales, seguirá siendo un miembro de esos grupos.

Nota: Sincronice las cuentas con sus plantillas periódicamente para garantizar que estén sincronizadas con sus plantillas de cuenta.

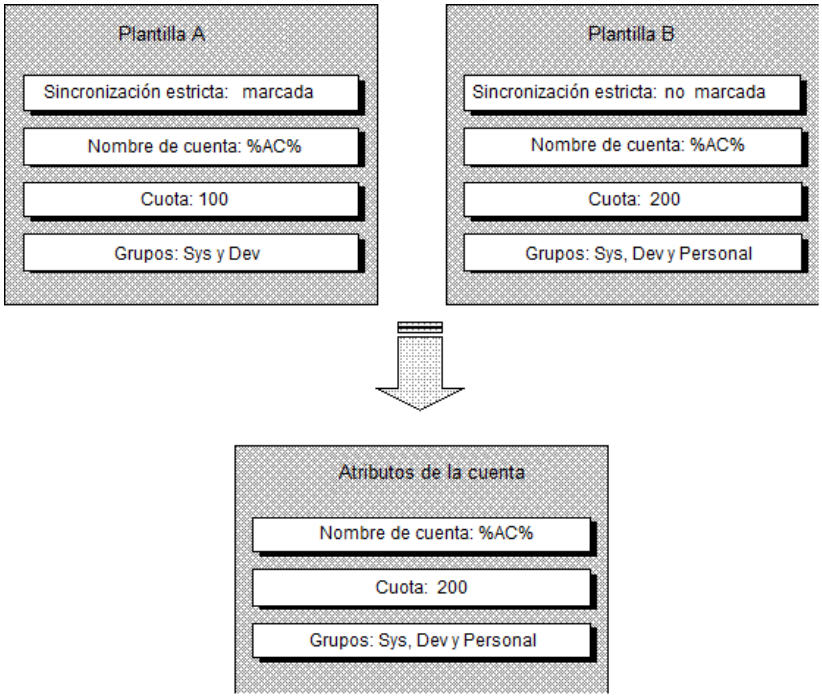
Cuentas con varias plantillas

La sincronización también depende de si la cuenta pertenece a más de una plantilla de cuenta. Si una cuenta tiene solamente una plantilla de cuenta y esa plantilla utiliza la sincronización estricta, cada atributo se actualiza para coincidir exactamente con lo que el valor del atributo de plantilla de cuenta evalúa. El resultado es el mismo que si el atributo fuera un atributo inicial.

Una cuenta puede pertenecer a varias plantillas de cuenta, como sería el caso si un usuario perteneciera a varios roles de aprovisionamiento, cada uno de los cuales indicando algún nivel de acceso en el mismo punto final gestionado. Cuando esto sucede, CA Identity Manager combina esas plantillas de cuenta en una plantilla de cuenta efectiva que indica el superconjunto de las capacidades de las plantillas de cuenta individuales. Se considera que esta plantilla de cuenta que utiliza la sincronización débil si todas sus plantillas de cuenta individuales son de sincronización débil o estricta o si alguna de las plantillas de cuenta individuales es estricta.

Nota: A menudo se utiliza solo la sincronización débil o solo la sincronización estricta para las plantillas de cuenta que controlan una cuenta, en función de si los roles de la compañía definen completamente los accesos que necesitan sus usuarios. Si sus usuarios no se ajustan en roles claros y se necesita la flexibilidad para conceder capacidades adicionales a las cuentas de sus usuarios, utilice la sincronización débil. Si se pueden definir roles para especificar exactamente los accesos que necesitan sus usuarios, utilice la sincronización estricta.

El ejemplo siguiente demuestra cómo se combinan varias plantillas de cuenta en una sola plantilla de cuenta efectiva. En este ejemplo, una plantilla de cuenta se marca para la sincronización débil y otra para la sincronización estricta. Por lo tanto, la plantilla de cuenta efectiva creada combinando las dos plantillas de cuenta se trata como una plantilla de cuenta de sincronización estricta. El atributo de cuota de entero adopta el valor mayor de las dos plantillas de cuenta y el atributo de grupos de varios valores adopta la unión de valores de las dos políticas.



Sincronización inversa con cuentas de punto final

Aunque es responsabilidad de CA Identity Manager crear, eliminar y modificar cuentas, no se puede impedir que un usuario de sistema de punto final realice estas operaciones por su cuenta. Esta situación puede producirse debido a razones de emergencia o maliciosas, como la acción de un pirata informático. La sincronización inversa garantiza el control de las cuentas que un usuario tiene en cada punto final al identificar discrepancias entre las cuentas de CA Identity Manager y las cuentas en los puntos finales.

Por ejemplo, si se creó una cuenta en el dominio de Active Directory mediante una herramienta externa, CA Identity Manager debe ser consciente de este problema potencial de seguridad. Además, omitir CA Identity Manager provoca una falta de procesos de aprobación e informes de auditoría.

Los tipos de discrepancias entre CA Identity Manager y los puntos finales gestionados son los siguientes:

- Una nueva cuenta detectada
- Un cambio en una cuenta existente

Puede tratar ambos casos definiendo las políticas para gestionar el cambio. A continuación y mediante el uso de Explorar y correlacionar para actualizar CA Identity Manager, inicia la ejecución de las políticas.

Funcionamiento de la sincronización inversa

La sincronización inversa con cuentas de punto final se produce de la siguiente manera:

1. Un administrador o usuario malicioso crea o modifica una cuenta en un punto final.
2. Cuando Explorar y correlacionar se ejecute en ese punto final, se detectará la cuenta nueva o modificada.
3. El servidor de aprovisionamiento envía una notificación al servidor de CA Identity Manager.
4. El servidor de CA Identity Manager busca una política de sincronización inversa que coincida con el cambio en el punto final.
5. Si se encuentra una política que coincida, se ejecuta. Si hay más de una política que se aplica a esta cuenta y esas políticas tienen el mismo ámbito, se ejecutará la política con la prioridad más elevada.
6. En función de la política, se produce una de las siguientes acciones:
   - En el caso de una nueva cuenta, la política acepta, suprime o suspende la cuenta o la envía para su aprobación.
   - En el caso de una cuenta modificada, la política acepta el valor, lo devuelve al último valor conocido o lo envía para la aprobación de flujo de trabajo.
7. Si se selecciona el flujo de trabajo, se genera un nuevo evento para el flujo de trabajo y se definen los aprobadores. A continuación, se produce una de las acciones siguientes:
   - Para una nueva cuenta, el aprobador puede aceptar, suprimir o suspender la cuenta, o bien asignarla a un usuario.
   - En el caso de una cuenta modificada, el proceso de flujo de trabajo es el mismo como si el valor se cambiara en la Consola de usuario, excepto por el hecho de que los valores rechazados se invirtieran en el punto final.

Asignación de atributos de punto final

Para utilizar la sincronización inversa en un atributo en una cuenta de punto final, primero asígnelo a un atributo visible en la Consola de usuario. Algunos atributos, como el nombre de cuenta y la contraseña, se asignan de forma predeterminada. Otros atributos no se asignan. Por ejemplo, la pertenencia al grupo de atributos de Active Directory no se asigna. Para algunos tipos de punto final, no se asigna ningún atributo.

Para comprobar si el atributo se puede asignar

1. En la Consola de usuario, haga clic en Puntos finales o en Tareas, Puntos finales.
2. Haga clic en Modificación inversa, Crear política de cuenta modificada de sincronización inversa.
3. Elija crear una política nueva o una copia de una política.
4. Haga clic en Tipo de punto final y elija un punto final como Active Directory.
5. Haga clic en Nombre del atributo para mostrar una lista de atributos que se pueden asignar.
6. Haga clic en Cancelar.

   Se cancela la política porque ahora solo se está utilizando para comprobar qué atributos se pueden asignar.

Importante: Se pueden gestionar ciertos atributos solamente mediante herramientas nativas en el punto final. Así, si un usuario del punto final modifica este tipo de atributo, se producirá un error en el evento inverso cuando la política de sincronización inversa se activa. Sin embargo, no se revocan los cambios realizados en otros atributos de ese evento inverso. Por lo tanto, se debe evitar asignar atributos que solo se pueden gestionar en el punto final.

Para asignar atributos de punto final para la sincronización inversa

1. Haga clic en Puntos finales, Modificar punto final.
2. Busque y seleccione un punto final que requiera la sincronización inversa.
3. Haga clic en la ficha Asignación de atributos.
4. Seleccione Utilizar valores personalizados.
5. Haga clic en Agregar para agregar un nuevo atributo personalizado.
6. Seleccione un atributo personalizado disponible. Por ejemplo, utilice CustomField 10 si no se está utilizando en el entorno.

7. Asigne el atributo personalizado al nombre de atributo de cuenta que desee gestionar.
8. Repita los pasos del 5 al 7 para agregar asignaciones entre todos los atributos de cuenta necesarios y el atributo personalizado seleccionado.

   Puede usar el mismo atributo personalizado (CustomField 10 en nuestro ejemplo) para todos los atributos que desee gestionar.
9. Haga clic en Enviar.

Para crear valores de línea de referencia para este punto final

Una vez que todos los valores para un punto final se hayan asignado, examine el punto final. Para esta operación, se desactiva la notificación entrante y se activa después de completar la exploración. La desactivación de la notificación elimina las notificaciones que no son necesarias. Por el contrario, cada cuenta que tiene valores en los nuevos atributos generará una notificación durante la operación de exploración.

1. En el Gestor de aprovisionamiento, desactive la notificación entrante de la siguiente manera:
   a. Haga clic en Sistema, Domain configuration (Configuración de dominio), CA Identity Manager Server, Enable Notification (Activar notificación).
   b. Seleccione No.
   c. Reinicie el servidor de aprovisionamiento para garantizar que los cambios surtan efecto.
2. En la Consola de usuario, haga clic en Puntos finales, Ejecutar Explorar y correlacionar.

   Elija una definición de exploración y correlación que no tenga la correlación seleccionada.

   Esta acción vuelve a completar los atributos del almacén de usuarios con los nuevos datos de atributos de punto final. Esta tarea puede tardar un poco si el punto final es de gran tamaño.
3. Vuelva a activar la notificación entrante en el Gestor de aprovisionamiento.
4. Reinicie el servidor de aprovisionamiento.

En la siguiente operación de exploración y correlación para ese punto final, se generan notificaciones de modificación de cuenta. Las notificaciones se generan si se produjo un cambio para un atributo que se asigna a un atributo de usuario global y se aplica una política a ese atributo.

Más información:

Capacidad y atributos iniciales (en la página 215)

Políticas para la sincronización inversa

Cuando se crea o se modifica una cuenta en un punto final, las políticas de sincronización inversa pueden realizar las acciones adecuadas como respuesta. Por ejemplo, el usuario crea algunas cuentas de Active Directory en varias OU en el dominio corporativo. Además, el usuario modifica algunas cuentas de Microsoft Exchange. Puede detectar las cuentas nuevas y modificadas y proporcionar las acciones adecuadas como respuesta mediante el uso de las políticas de cuenta de sincronización inversa.

Puede hacer lo siguiente usando la sincronización inversa:

- Configure una política para aceptar la cuenta, rechazarla o enviarla para que la apruebe el flujo de trabajo.
- Configure una política para aceptar un cambio en un atributo, devolverlo al atributo original o enviarlo para que lo apruebe el flujo de trabajo.
- Cuando se envía una cuenta para la aprobación de flujo de trabajo, el aprobador puede realizar una de las acciones siguientes:
  - Rechazarla (eliminarla/suspenderla del punto final o cambiar el valor para que coincida con el valor de almacenamiento de usuario de CA Identity Manager).
  - Aceptarla y actualizar el almacén de usuarios de CA Identity Manager para que coincida con la cuenta.
  - Asignarla a un usuario de la Consola de usuario (en el caso de la creación de usuario)

Creación de políticas para nuevas cuentas

Si desea definir un proceso para cuando se detecte una nueva cuenta en un punto final, creará una política de cuenta que se aplicará a nuevas cuentas. Se ejecutan nuevas políticas de cuenta cuando se detectan cuentas en el momento en que la opción Correlacionar se incluye en Explorar y correlacionar definición. Si se encontró una cuenta cuando sólo se ejecutaba la exploración, la política se ejecutará la próxima vez que la opción Correlacionar se incluya al explorar ese punto final.

Para crear una política para nuevas cuentas

1. En la Consola de usuario, haga clic en Puntos Finales o haga clic en Tareas, Puntos finales.
2. Nueva inversa, Crear política de sincronización inversa y de nueva cuenta.
3. Escriba un nombre y una descripción para la política.
4. Introduzca los parámetros siguientes:
   - Prioridad: la prioridad de la política. La política de prioridad más alta es la que tiene el número más bajo. Si las dos políticas tienen la misma prioridad y el mismo ámbito, se puede ejecutar cualquier política. Por tanto, asegúrese de definir distintos niveles de prioridad.
   - Tipo de punto final: todos los puntos finales o un tipo de punto final específico.
   - Punto final: el nombre del punto final específico. Si el tipo de punto final está definido en Todo, la única elección posible será todos los puntos finales.
   - Contenedor: el contenedor en el que reside la cuenta. Este campo sólo se aplica a puntos finales jerárquicos. Introduzca el contenedor como una lista de nodos que finalicen con el punto final. Por ejemplo, para una AD OU con la ruta "ou=secundario,ou=principal,ou=raíz,dc=dominio,dc=nombre" el formato "secundario,principal,raíz" es correcto.
   - Usuario correlacionado: controla cuándo ejecutar la política basada en si un usuario correlacionado se encuentra en el directorio de aprovisionamiento.

5. Seleccione una de las acciones siguientes:
   - Aceptar: no realiza ninguna acción en la cuenta. Esta opción debería ser útil si las dos políticas existen, una que rechaza todas las nuevas cuentas y una política de prioridad más alta que acepta cuentas creadas según una OU determinada. Por lo tanto, si se creó la cuenta en esa OU, se acepta. La prioridad de rechazo no se ejecuta ya que tiene una prioridad inferior.
   - Suprimir: elimina la cuenta del punto final.
   - Suspender: deja la cuenta en el punto final, pero la suspende.
   - Enviar para la aprobación: envía el cambio para la aprobación del flujo de trabajo.
6. Realice los pasos siguientes si define la acción en Enviar para la aprobación:
   a. Haga clic en el icono junto al proceso de flujo de trabajo.
   b. Elija un proceso de flujo de trabajo.
   c. Haga clic en OK.
7. Haga clic en Enviar.

Si asignó un proceso de flujo de trabajo a la política, necesita crear una tarea de aprobación (en la página 190).

Creación de políticas para cuentas modificadas

La sincronización inversa puede administrar cualquier atributo de cuenta en una cuenta de punto final siempre que se defina en la asignación de atributos (en la página 184).

Para definir un proceso para cuando se encuentre una discrepancia entre las cuentas de punto final existentes y sus valores conocidos en CA Identity Manager, se podrá crear una política de cuenta que se aplique a cuentas existentes. Si un atributo tiene varios valores, se puede agregar o eliminar más de un valor. En este caso, la política se aplica a cada valor independientemente o puede crear políticas distintas para valores diferentes.

Para crear una política para cuentas modificadas

1. En la Consola de usuario, haga clic en Puntos Finales o en Tareas, Puntos finales.
2. Haga clic en Modificación inversa, Crear política de cuenta modificada de sincronización inversa.
3. Escriba un nombre y una descripción para la política.
4. Introduzca los parámetros siguientes:
   - Prioridad: la prioridad de la política. La política de prioridad más alta es la que tiene el número más bajo. Si las dos políticas tienen la misma prioridad y el mismo ámbito, se puede ejecutar cualquier política. Por tanto, asegúrese de definir distintos niveles de prioridad.
   - Tipo de punto final: todos los puntos finales o un tipo de punto final específico.
   - Punto final: el nombre del punto final específico. Si el tipo de punto final está definido en Todo, la única elección posible será todos los puntos finales.
   - Contenedor: el contenedor en el que reside la cuenta. Este campo sólo se aplica a puntos finales jerárquicos. Introduzca el contenedor como una lista de nodos que finalicen con el punto final. Por ejemplo, para una AD OU con la ruta "ou=secundario,ou=principal,ou=raíz,dc=dominio,dc=nombre" el formato "secundario,principal,raíz" es correcto.
   - Atributo: el nombre físico.
   - Valor: una representación de cadena del valor, que puede incluir ***** (asterisco) como carácter comodín. El carácter comodín hace referencia a cualquier valor en el cambio.

5. Seleccione una de las acciones siguientes:
   - Aceptar: actualiza el valor de cuenta en el almacén de usuarios de CA Identity Manager para que coincida con el valor de la cuenta de punto final.
   - Rechazar: revierte el atributo para volver a incorporar el valor original sin afectar a otros cambios realizados en los atributos para la cuenta.
   - Enviar para la aprobación: envía el cambio para la aprobación del flujo de trabajo.
6. Realice los pasos siguientes si define la acción en Enviar para la aprobación:
   a. Haga clic en el icono junto al proceso de flujo de trabajo.
   b. Elija un proceso de flujo de trabajo.
   c. Haga clic en OK.
7. Haga clic en Enviar.

Si asignó un proceso de flujo de trabajo a la política, necesita crear una tarea de aprobación (en la página 190).

Creación de tareas de aprobación para la sincronización inversa

Va a crear tareas de aprobación inversa para políticas que tienen una acción de envío al flujo de trabajo. Tenga en cuenta las siguientes directrices a la hora de crear las tareas:

- En el caso de tareas que aprueben nuevas cuentas, tiene dos opciones.
  - Puede crear una pantalla de aprobación genérica para las cuentas. La pantalla de perfil para las tareas muestra sólo información general sobre la cuenta. La tarea Aprobación inversa de la nueva cuenta funciona de esta manera.
  - Si el aprobador tiene que ver los detalles de la nueva cuenta, esa pantalla debe ser específica del tipo de punto final. De esta forma, la tarea de aprobación con la pantalla debe usarse sólo para políticas que son específicas para ese tipo de punto final. La tarea debe incluir la ficha Aprobación inversa.
- Para las tareas que aprueban modificaciones de cuenta, la pantalla de aprobación debe ser específica de un tipo de punto final, de manera que el aprobador pueda ver los valores cambiados.

Las tareas de aprobación inversas son idénticas a las tareas de aprobación usadas para los cambios de cuentas. Si ya existe una tarea de aprobación para un tipo de punto final concreto, se puede usar esa tarea. En el caso de una nueva cuenta, se necesita una ficha de aprobación inversa adicional. Si no hay una tarea de aprobación existente para el tipo de punto final, use el siguiente procedimiento.

Para crear una tarea de aprobación para la sincronización inversa

1. En la Consola de usuario, haga clic en Tareas, Roles y tareas, o haga clic en Roles y tareas.
2. Haga clic en Tareas de administración, Crear tarea de administración.
3. Seleccione la tarea de modificación para el punto final.

   El nombre empezaría con "modify" e incluiría el nombre del tipo de punto final. Modificar la cuenta de Active Directory es un ejemplo.
4. Realice los cambios siguientes en la ficha Perfil:
   - Cambiar el nombre de la nueva tarea.
   - Cambiar la etiqueta de la tarea.
   - Cambiar la acción para aprobar el evento.
5. Realice los cambios siguientes en la ficha Fichas:
   a. Elimine todas las fichas de relación.
   b. Agregue la ficha Aprobación inversa si la tarea es aprobar las nuevas cuentas. Mueva esta ficha para que sea la primera.
   c. Copiar y editar las pantallas de aprobación en las fichas según corresponda.

      Nota: Se pueden producir problemas al utilizar algunas pantallas de cuenta en una tarea de aprobación. En este caso, modifique la pantalla de cuenta predeterminada para que la ficha funcione en la tarea.
6. Haga clic en Enviar.
7. Si la tarea es para las aprobaciones de nuevas cuentas, agregue la tarea a un rol al que el aprobador pertenecería. El rol define el ámbito de usuario, que se usa para buscar usuarios a los que se pueda asignar la nueva cuenta.

Ejecución de la sincronización inversa

La sincronización inversa se produce cuando usa la tarea Ejecutar Explorar y correlacionar. Gracias a ella, se actualiza el almacén de aprovisionamiento de CA Identity Manager con cuentas nuevas o modificadas en un punto final.

Para ejecutar la sincronización inversa

1. Cree una definición de exploración y correlación que incluya la opción Correlacionar. La correlación es necesaria para detectar nuevas cuentas.
2. Haga clic en Tareas, Puntos finales, Ejecutar Explorar y correlacionar.
3. Elija una definición que se aplica al punto final con las cuentas nuevas o cambiadas.

   Nota: Al correlacionar con el usuario existente, el usuario debe existir en el directorio de aprovisionamiento, por el contrario, el usuario se correlaciona con el usuario predeterminado en ese directorio. El almacén de usuarios de CA Identity Manager no se encuentra en el ámbito de la tarea Explorar y correlacionar.
4. Haga clic en Enviar.

Si la política no tiene proceso de flujo de trabajo, las cuentas ya se habrán procesado tal y como se definen en la política.

Nota: Si se rechazaron varios atributos en una cuenta detectada por la política de sincronización inversa, todas las acciones se colocarán en un evento. Sin embargo, si se produce un error en ese evento debido a un problema con uno de los atributos, no se actualizará ninguno.

Si el flujo de trabajo es parte de la política, las aprobaciones generadas por la sincronización inversa aparecen debajo de Flujo de trabajo, Ver Mi lista de trabajo para el aprobador.

Para las nuevas cuentas, el aprobador tiene las siguientes opciones:

- El aprobador puede optar entre suspender o suprimir la cuenta en el punto final seleccionando Eliminar o Suspender y después haciendo clic en Rechazar.
- De lo contrario, el aprobador podrá aceptar la nueva cuenta haciendo clic en Aprobar.

  Si un aprobador no selecciona un usuario en el campo Usuario correlacionado, la cuenta se asigna al usuario predeterminado. Si el campo Usuario correlacionado se completa en la tarea de aprobación, la cuenta se correlaciona con este usuario. El campo Usuario correlacionado contiene el usuario sugerido encontrado por el mecanismo de correlación si se puede encontrar un usuario.

Para las cuentas modificadas, el aprobador tiene las opciones siguientes:

- En cada cuenta, el aprobador verá los valores cambiados y los podrá aprobar o rechazar como si los cambios se iniciaran en las pantallas de gestión de cuentas.

- El aprobador verá cambios en los atributos de capacidad (por ejemplo, los grupos de Active Directory) como eventos de aprobación independientes.

Para comprobar si la sincronización inversa tuvo éxito.

1. Vaya a Sistema, Ver tareas enviadas.
2. Complete el campo del nombre de tarea de la siguiente manera: Actividad de aprovisionamiento.
3. Haga clic en Buscar.

Los resultados muestran si los eventos de sincronización inversa se han completado correctamente.

Ampliación de los atributos personalizados en los puntos finales

El servidor de aprovisionamiento puede gestionar atributos de punto final personalizados. Para permitir que CA Identity Manager lea los atributos de punto final personalizados asociados a los roles de aprovisionamiento, hay que llevar a cabo más pasos.

Para ampliar los atributos personalizados en los puntos finales

1. Genere metadatos a partir de la tabla del analizador si el conector se ha creado antes de CA Identity Manager r12.5.

   Consulte la *Guía de programación para el servidor de conectores Java*.
2. Utilice Connector Xpress del modo siguiente:
   a. Instale metadatos en el nodo de espacio de nombres.
   b. Genere un archivo JAR, un archivo de propiedad y un archivo de definición de rol mediante el generador de definiciones de roles.

      Para obtener más información, consulte la *Guía de Connector Xpress*.

3. Copie el archivo JAR en esta ubicación:
   - (Windows) *app server home*/iam_im.ear/user_console.war/WEB-INF/lib
   - (UNIX) *app server home*\iam_im.ear\user_console.war\WEB-INF\lib

     Nota: Para WebSphere, copie el archivo JAR en: WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*Cell_name*/applications/iam_im.ear/user_console.war/WEB-INF
4. Copie el archivo de propiedad en esta ubicación:
   - (Windows) *app server home*/iam_im.ear/custom/provisioning/resourceBundles
   - (UNIX) *app server home**i*am_im.ear\custom\provisioning\resourceBundles

     Nota: Para WebSphere, copie el archivo de propiedades en:

     WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*cell_name*/applications/iam_im.ear\custom\provisioning\resourceBundles
5. Repita los dos pasos anteriores para cada nodo si dispone de un clúster.
6. Reinicie el servidor de aplicaciones.
7. Importe el archivo de definición de rol según se indica a continuación:
   a. En la Consola de gestión, seleccione el entorno.
   b. Seleccione Configuración de tareas y roles
   c. Haga clic en Importar.
   d. Seleccione el tipo de punto final y haga clic en Finalizar.

Tareas de cuenta

En la Consola de usuario, puede crear, modificar, ver y suprimir cuentas de punto final asociadas con un usuario de Identity Manager. También puede asignar otras cuentas de punto de final que no estén asociadas con CA Identity Manager a un usuario.

Existen cuatro tipos de cuentas de punto final:

Aprovisionada

Cuentas que se crean cuando se asigna un rol de aprovisionamiento al usuario.

Excepción

Cuentas que se crean cuando se asigna al usuario una plantilla de cuenta.

Huérfana

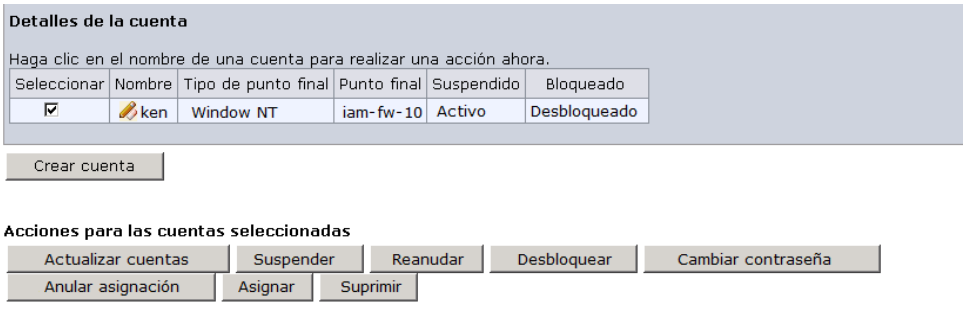
Cuentas que se crean en el sistema de punto final y no están asociadas con ningún usuario de CA Identity Manager.

Sistema

Cuentas que se crean en el sistema de punto final, no están asociadas con ningún usuario de CA Identity Manager y se utilizan para gestionar el sistema de punto final.

Visualización o modificación de cuentas de punto final

Tareas que permiten visualizar el perfil de un usuario, como Ver usuario o Modificar mi perfil, incluyen una ficha Cuentas que clasifica las cuentas de ese usuario en puntos finales.



Para cada cuenta, Identity Manager muestra información como el nombre de cuenta, el punto final donde existe la cuenta y el estado de la cuenta. Para modificar una tarea, existen opciones adicionales disponibles para cambiar la contraseña de un usuario y bloquear o suspender una cuenta.

En este ejemplo, la ficha Cuentas incluye un botón Búsqueda, que significa que la ficha está configurada con una pantalla de búsqueda. Se puede configurar esta ficha para utilizar una pantalla de lista, una pantalla de búsqueda, o ambos.

- Cuando se configuran las dos pantallas, la pantalla de búsqueda determina los campos en los resultados de la búsqueda.
- Si solamente se configura una pantalla de lista, determina los campos en los resultados de la búsqueda.
- Si no se ha configurado ninguna de las dos pantallas, la ficha de cuentas utiliza una visualización de lista estática, que significa que no se puede personalizar la ficha Cuentas para visualizar las columnas.

Para obtener detalles sobre otras opciones que se pueden proporcionar en la ficha Cuentas, consulte la ayuda de la Consola de usuario para la ficha Configurar cuentas.

Creación de una cuenta de aprovisionamiento

El método recomendado para crear una cuenta de punto final para un usuario de CA Identity Manager es asignar un rol de aprovisionamiento al usuario. El usuario recibe la cuenta con los atributos definidos en las plantillas para dicho rol. Cuando sea necesario, los cambios realizados en dicha plantilla de cuenta, como el tamaño del buzón para cuentas de Exchange, actualizan la cuenta de punto final.

Para crear una cuenta de aprovisionamiento

1. En la Consola de usuario, seleccione Gestionar usuarios, Modificar usuario.
2. Seleccione un usuario para modificarlo.
3. Haga clic en la ficha Roles de aprovisionamiento.
4. Haga clic en Agregar un rol de aprovisionamiento.
5. Seleccione un rol.
6. Haga clic en Enviar.

Creación de una cuenta de excepción

Puede crear una cuenta directamente en la ficha Cuentas cuando utilice la opción Modificar usuario en un usuario. Esta cuenta se denomina cuenta de excepción. No obstante, como no se incluye ningún rol de aprovisionamiento en esta cuenta, la sincronización de roles con usuarios no actualiza esta cuenta.

Para crear una cuenta de excepción

1. En la Consola de usuario, seleccione Usuarios, Modificar cuentas de punto final del usuario.
2. Seleccione un usuario para modificarlo.
3. Haga clic en Crear.
4. Seleccione un punto final.
5. Seleccione un contenedor si se requiere uno para este tipo de punto final.
6. Rellene los campos de cada ficha.
7. Haga clic en Enviar.

Asignación de cuentas huérfanas

En la Consola de usuario se pueden gestionar las cuentas huérfanas, que son aquellas que no están asociadas con un usuario de CA Identity Manager.

Para crear un usuario predeterminado para las cuentas huérfanas

Si el directorio de aprovisionamiento está separado del almacén de usuarios de CA Identity Manager, cree el usuario predeterminado del servidor de aprovisionamiento en el almacén de usuarios de CA Identity Manager. El usuario predeterminado se utiliza para las cuentas huérfanas.

1. En el Consola de usuario, haga clic en Usuarios.
2. Haga clic en Gestionar usuarios, Crear usuario.
3. Asigne un nombre al usuario, como se indica a continuación, incluidos los corchetes:
   `[usuario predeterminado]`

   Ahora puede asignar cuentas huérfanas a los usuarios.

Para asignar una cuenta huérfana

1. En el Consola de usuario, haga clic en Puntos finales.
2. Haga clic en Gestionar cuentas huérfanas.
3. Busque un usuario y selecciónelo.
4. Haga clic en un usuario para asignarlo a la cuenta huérfana.

Asignación de cuentas de sistema

En la Consola de usuario se pueden gestionar cuentas del sistema, que son cuentas de punto final que se utilizan para gestionar el sistema de punto final.

Para asignar una cuenta de sistema a un usuario, cree una tarea de administración basada en la tarea Gestionar cuentas del sistema. La tarea nueva tiene un usuario de CA Identity Manager específico que se aplica a un punto final específico. Puede crear una tarea para cada tipo de punto final.

Para configurar una tarea y asignarla a cuentas de sistema

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Crear tarea de admin.
2. Base la tarea nueva en la opción Gestionar cuentas del sistema.

   Por ejemplo, puede crear una tarea llamada *Gestionar cuentas del sistema Oracle* para asignar cuentas de sistema en un tipo de punto final de Oracle.
3. En la ficha Examinar, haga clic en el botón Examinar para editar la pantalla de búsqueda. En dicha pantalla, incluya un filtro de búsqueda para un usuario para asignarlo a esta cuenta de sistema.
4. Envíe la tarea.
5. Incluya esta tarea en un rol.
6. Asigne el rol a un usuario que vaya a asignar cuentas de sistema de un punto final a un usuario.

   El usuario con este rol puede ejecutar la tarea nueva para asignar usuarios del sistema a un usuario de CA Identity Manager.

Pantalla de tarea Mover cuenta

Use esta pantalla de tarea para mover cuentas de un contenedor de un punto final a otro. Los campos de esta pantalla se muestran a continuación:

Mover detalles de la cuenta

Especifica la cuenta, el contenedor principal, el contenedor de destino, el punto final y el tipo de punto final que desee mover.

Botón Seleccionar contenedor

Haga clic en este botón para buscar contenedores de cuenta disponibles que pertenezcan al punto final.

Supresión de una cuenta de punto final

Se puede suprimir una cuenta de punto final de dos maneras:

1. Mediante la tarea de Modificar usuario de la ficha Roles de aprovisionamiento, elimine el rol que creó dicha cuenta.
2. Utilice la tarea Modificar cuentas de punto final del usuario para suprimir la cuenta.

Para eliminar una cuenta mediante la tarea Modificar cuentas de punto final del usuario

1. En la Consola de usuario, seleccione Usuarios, Modificar cuentas de punto final del usuario.
2. Seleccione un usuario para modificarlo.
3. Busque cuentas basadas en un tipo de punto final.
4. Seleccione una cuenta.
5. Haga clic en el botón Suprimir.

Las cuentas eliminadas se vuelven a crear al emplear el gestor de aprovisionamiento del modo siguiente:

- La sincronización del usuario con los roles permite volver a crear cuentas de aprovisionamiento, cuentas creadas cuando un usuario tiene un rol de aprovisionamiento.
- La sincronización de cuentas con plantillas de cuentas vuelve a crear cuentas de excepción (si la cuenta dispone de una plantilla de cuenta) y de aprovisionamiento.

Modificación de la contraseña de una cuenta de punto final

Puede cambiar la contraseña de una cuenta de punto final sin conocer la contraseña actual.

Para modificar la contraseña de una cuenta de punto final

1. En la Consola de usuario, seleccione Usuarios, Modificar cuentas de punto final del usuario.
2. Seleccione un usuario para modificarlo.
3. Busque cuentas basadas en un tipo de punto final.
4. Seleccione una o varias cuentas.
5. Haga clic en el botón Cambiar contraseña.
6. Introduzca una contraseña nueva.

   Las políticas de contraseñas de CA Identity Manager validan la contraseña nueva.
7. Haga clic en Enviar.

Realización de acciones en varias cuentas

Puede llevar a cabo varias acciones diferentes en una o más cuentas. Por ejemplo, puede reanudar una cuenta que se había suspendido, desbloquear una cuenta cuando un usuario haya introducido una contraseña incorrecta, así como asignar o desasignar una cuenta a un usuario. Las acciones se aplican a todas las cuentas seleccionadas y el procedimiento es el mismo.

Para realizar tareas en varias cuentas

1. En la Consola de usuario, seleccione Usuarios, Modificar cuentas de punto final del usuario.
2. Seleccione un usuario para modificarlo.
3. Busque cuentas basadas en un tipo de punto final.
4. Seleccione una o varias cuentas.
5. Haga clic en uno de los botones de Acciones para las cuentas seleccionadas.
6. Responda al cuadro de diálogo que aparece y haga clic en Enviar.

Operaciones de cuenta avanzadas

En el gestor de aprovisionamiento, se pueden realizar un número de operaciones adicionales en las cuentas:

- Asociar una cuenta con usuarios globales diferentes
- Explorar cuentas automáticamente
- Suprimir cuentas
- Utilizar Pendiente de suprimir
- Volver a crear cuentas suprimidas

Cambiar el usuario global en una cuenta

A continuación, se muestran ejemplos de momentos en los que se desearía asociar una cuenta a un usuario global diferente:

- Tiene dos usuarios globales con el mismo nombre y CA Identity Manager correlaciona la cuenta con la persona incorrecta.
- CA Identity Manager ha correlacionado una cuenta con el objeto de [usuario predeterminado] y se desea asociarlo con otro objeto de usuario global.
- Se ha creado una cuenta mediante Nuevo y ahora se desea asociarla a un usuario global.

Para asociar una cuenta a un usuario global diferente en el gestor de aprovisionamiento, arrastre y suelte la cuenta en el usuario global correcto.

Cómo funciona la exploración automática

CA Identity Manager no avisa de la agregación o supresión de cuentas u otros objetos mediante herramientas nativas en el punto final hasta que este se explora. En el proceso de exploración se avisa de que se han producido agregaciones y supresiones (y, en algunos casos, modificaciones). Además, se aplican dichos cambios a la representación de CA Identity Manager del objeto en el directorio de aprovisionamiento.

Sin embargo, si se utiliza el gestor de aprovisionamiento para intentar crear un objeto con el mismo nombre antes de llevar a cabo esta exploración, CA Identity Manager avisa de que ya existe un objeto con ese nombre e informa sobre este error. A continuación, CA Identity Manager explora ese objeto, por lo que crea una representación de él en el directorio de aprovisionamiento. Puede empezar a trabajar inmediatamente con ese objeto. La exploración automática de un único objeto tiene lugar cada vez que una operación Agregar, Mover o Cambiar nombre genera un error existente desde el punto final cuando el objeto no existe en el directorio de aprovisionamiento.

Se puede combinar la exploración automática con el parámetro de configuración del dominio de correlación automática/sincronización que se describe en la *Guía de referencia de aprovisionamiento*. Cuando estas características funcionan juntas, primero se procesa un intento de crear una cuenta a partir de una plantilla de cuenta como intento de crear una nueva cuenta. A continuación, en el procesamiento se utilizan los siguientes pasos:

- Avisa de la existencia de una cuenta sin explorar.
- Explora esa cuenta automáticamente.
- Correlaciona la cuenta automáticamente con el usuario global.
- Agrega una plantilla de cuenta a la cuenta como si se tratase de una cuenta existente correlacionada con este usuario global.

Supresión de cuentas

Si primero se debe suprimir una cuenta, puede utilizar los siguientes métodos en el gestor de aprovisionamiento:

- Haga clic con el botón secundario del ratón en la cuenta y seleccione Suprimir.
- Haga clic con el botón secundario del ratón en un usuario global y seleccione Delete User and Accounts (Suprimir usuario y cuentas).
- Ejecute el asistente Suprimir cuentas.
- Sincronice usuarios globales con roles de aprovisionamiento y especifique que desea suprimir cuentas adicionales.

Cuando se elimina un usuario global de un rol de aprovisionamiento, el gestor de aprovisionamiento proporciona las siguientes opciones para la supresión de cuentas:

- Si decide suprimir estas cuentas, CA Identity Manager elimina las cuentas del directorio de aprovisionamiento.
- Si decide no suprimir las cuentas, se puede utilizar la opción Sincronizar usuario con roles y Suprimir Cuenta.

Cuando se elimina un usuario global de un rol de aprovisionamiento antes de suprimir cuentas, se pueden enumerar las cuentas del usuario global. Haga clic con el botón secundario del ratón en el usuario global y seleccione List Accounts (Enumerar cuentas).

- El listado de cuentas muestra los roles de aprovisionamiento a los que pertenece cada cuenta. Si una cuenta pertenece a un rol de aprovisionamiento, se suprime al eliminar un usuario de ese rol y se acepta la acción de sincronización de usuarios con objeto de suprimir las cuentas.
- Si una cuenta no pertenece a ningún rol de aprovisionamiento, se trata de una cuenta adicional y se informa de ello mediante la opción Check User Synchronization (Comprobar sincronización de usuarios). La cuenta se suprime si se selecciona el elemento de menú Synchronize the User with Roles (Sincronizar el usuario con roles) en el usuario global.

Uso de Pendiente de suprimir

CA Identity Manager se puede configurar en cada uno de los puntos finales; por tanto, las cuentas de un punto final no se suprimirán si los administradores inician las acciones Suprimir o Sincronizar que suprimirían normalmente dichas cuentas. En cambio, las cuentas se pondrán en el estado Pendiente de suprimir en CA Identity Manager y en el estado Suspendido en el punto final gestionado.

Las cuentas con el estado Pendiente de suprimir se pueden identificar en el gestor de aprovisionamiento de la ficha Estadísticas de las propiedades de cuenta. En una cuenta suspendida se incluirá la razón Pendiente de suprimir y una marca de tiempo al introducir dicho estado. El almacenamiento del estado Pendiente de suprimir y la marca de tiempo Suspendido permiten la escritura de una utilidad que identifica estas cuentas con el estado Pendiente de suprimir y las suprime más adelante del servidor de aprovisionamiento y el punto final gestionado.

Cómo volver a crear cuentas suprimidas

Si se suprime una cuenta en un punto final gestionado mediante una herramienta distinta de CA Identity Manager, la función de comprobación de la sincronización de cuentas informa de que falta la cuenta, ya que existe en el directorio de aprovisionamiento pero no en el punto final gestionado. Cuando esto sucede, vuelva a crear la cuenta en el punto final mediante la emisión de la característica Sincronizar cuenta con plantillas de cuenta, que vuelve a crear la cuenta mediante las plantillas de cuenta asociadas a la cuenta.

Si las cuentas se vuelven a crear, CA Identity Manager las registra como creadas de nuevo. Estas cuentas se pueden identificar de forma independiente desde cuentas que se hayan actualizado, ya que los administradores deben ser estar al tanto de que los atributos distintos de los de capacidad (por ejemplo, contraseñas) se hayan establecido en los valores de plantillas de cuenta originales.

Capítulo 9: Funciones de aprovisionamiento

Esta sección contiene los siguientes temas:

Roles de aprovisionamiento y plantillas de cuenta

Para simplificar la gestión de cuentas, las cuentas se crean y se mantienen mediante el uso de plantillas de cuenta, que se emplean en los roles de aprovisionamiento. Un rol de aprovisionamiento contiene una o más plantillas de cuenta. Al aplicar ese rol a un usuario, éste recibe las cuentas definidas mediante las plantillas.

Estas plantillas sirven de base para las cuentas en un tipo de punto final específico. Proporcionan el mismo tipo de capacidades que las políticas de aprovisionamiento de eTrust Admin.

Mediante el uso de plantillas de cuenta, puede hacer lo siguiente:

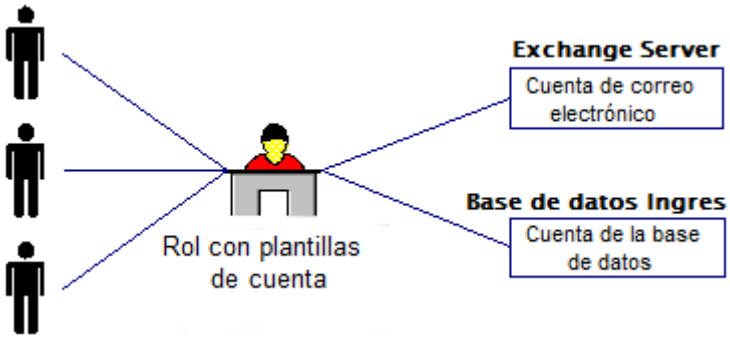
- Controlar los atributos de cuenta que tienen los usuarios de CA Identity Manager en un punto final cuando se crean sus cuentas.
- Definir atributos mediante el uso de cadenas de reglas o valores.
- Combinar atributos de cuenta de diferentes roles de aprovisionamiento, de manera que los usuarios sólo tengan una cuenta en un punto final concreto, con todos los atributos de cuenta necesarios.
- Crear o actualizar atributos de cuenta a medida que los usuarios globales cambian los roles de aprovisionamiento.
- Sincronizar los atributos de cuenta de manera que los usuarios globales sólo tengan los atributos que necesiten.
- Realizar consultas para ver las cuentas que se crearán, actualizarán o suprimirán durante una operación de sincronización.
- Determinar los atributos de cuenta que se pueden sincronizar con roles de aprovisionamiento y aquellos que no se pueden sincronizar.

Creación de roles para la asignación de cuentas

En la mayor parte de las organizaciones, los administradores dedican bastante tiempoo a proporcionar a los usuarios cuentas de inicio de sesión para los distintos sistemas y aplicaciones. Para simplificar esta actividad repetitiva, se pueden crear roles de aprovisionamiento, que son roles que contienen plantillas de cuenta. Las plantillas definen los atributos que existen en un tipo de cuenta. Por ejemplo, una plantilla de cuenta para una cuenta de Exchange define atributos como el tamaño del buzón de correo. Las plantillas de cuenta también definen cómo los atributos de usuario se asignan a las cuentas.

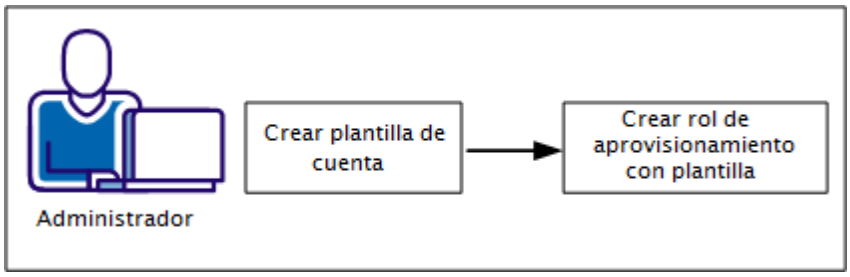
Pongamos el ejemplo en el que todos los empleados de la empresa Forward, Inc. necesitan acceder a una base de datos y correo electrónico. El administrador desea evitar la creación de una cuenta de base de datos y correo electrónico para cada empleado. Por tanto, el administrador crea un rol de aprovisionamiento para esa compañía. El rol contiene una plantilla de cuenta para un servidor Microsoft Exchange para proporcionar cuentas de correo electrónico, y una plantilla para una base de datos de Oracle. En este ejemplo, el servidor de Exchange y la base de datos de Oracle se llaman puntos finales, que son el sistema o la aplicación donde existen las cuentas.

Nota: Forward, Inc. es un nombre de compañía ficticio que se utiliza estrictamente para finalidades informativas y no hace referencia a ninguna compañía existente.



Una vez creados los roles, los administradores del negocio como gestores o personal de soporte pueden asignar esos roles a usuarios para darles las cuentas en puntos finales. Cuando los usuarios reciban el rol, podrán conectarse al punto final.

La creación de un rol de aprovisionamiento que incluye una plantilla de cuenta es un proceso de dos pasos tal y como se muestra a continuación:



Las secciones siguientes explican cómo crear un rol que se puede utilizar para asignar cuentas:

1. Creación de una plantilla de cuenta. (en la página 208)
2. Creación de un rol de aprovisionamiento (en la página 209)

Creación de una plantilla de cuenta.

Para simplificar la gestión de cuentas, las cuentas se crean y se mantienen mediante el uso de plantillas de cuenta, que se emplean en los roles de aprovisionamiento. Un rol de aprovisionamiento contiene una o más plantillas de cuenta. Al aplicar ese rol a un usuario, éste recibe las cuentas definidas mediante las plantillas.

Estas plantillas sirven de base para las cuentas en un tipo de punto final específico.

Mediante el uso de plantillas de cuenta, puede hacer lo siguiente:

- Controlar los atributos de cuenta que tienen los usuarios en un punto final al crear las cuentas.
- Definir atributos mediante el uso de cadenas de reglas o valores.
- Combinar atributos de cuenta de diferentes roles de aprovisionamiento, de manera que los usuarios sólo tengan una cuenta en un punto final concreto, con todos los atributos de cuenta necesarios.
- Crear o actualizar atributos de cuenta a medida que los usuarios globales cambian los roles de aprovisionamiento.

En el servidor de CA Identity Manager está instalada una plantilla de cuenta predeterminada para cada tipo de punto final. En un rol de aprovisionamiento, puede usar la plantilla de cuenta predeterminada, o bien puede crear sus propias plantillas de cuenta para los puntos finales que haya configurado.

Para crear una plantilla de cuenta

1. Vaya a Puntos Finales, que se puede encontrar bajo Tareas, y haga clic en Plantillas de cuenta, Crear plantilla de cuenta.
2. Seleccione un tipo de punto final para la plantilla.
3. Defina Nombre del punto final con el nombre del sistema del punto final o del host local, si procede.
4. Seleccione el punto final que vaya a utilizar en la ficha Puntos finales.
5. Complete los campos de las fichas o utilice los valores predeterminados.

   Cada tipo de punto final tiene un conjunto de fichas distinto. Haga clic en Ayuda para obtener las definiciones de los campos.
6. Haga clic en Enviar.

Nota: Si se especifican varios puntos finales al buscar objetos de punto final en la Plantilla de cuenta, se devuelve el subconjunto común (intersección) de los objetos relacionados. Un ejemplo es un grupo de Active Directory que existe en cada uno de los puntos finales seleccionados que están asociados a la Plantilla de cuenta. Cuando los resultados de la búsqueda muestran atributos distintos del nombre del objeto, se muestran los valores de atributo de los objetos asociados al primer punto final. Un ejemplo es el atributo de descripción para el objeto de idioma en un conector de PeopleSoft.

Creación de un rol de aprovisionamiento

El rol de aprovisionamiento se creará en cuanto decida los requisitos del rol:

- Qué usuarios necesitan otras cuentas
- Qué cuentas se asocian con el rol
- Quiénes son los miembros, administradores y propietarios del rol

Para crear un rol de aprovisionamiento

1. En la Consola de usuario, vaya a Roles y tareas, Roles de aprovisionamiento, Crear rol de aprovisionamiento.

   Para obtener detalles de cada ficha, haga clic en el enlace Ayuda de la pantalla.

2. Complete la ficha Perfil. Sólo es obligatorio el campo Nombre.

   Nota: Puede especificar atributos personalizados en la ficha Perfil que especifica información adicional acerca de los roles de aprovisionamiento. Esta información adicional se puede usar para simplificar la búsqueda de roles en entornos que incluyan un gran número de roles.

3. Complete la ficha Plantillas de cuenta.

   a. Haga clic en un tipo de punto final, como, por ejemplo, ActiveDirectory.

   b. Haga clic en una plantilla de cuenta.

      Las plantillas que se pueden seleccionar se basan en el tipo de punto final.

   c. Agregue las plantillas de cuenta que sean necesarias para los diferentes tipos de extremo.

4. Complete la ficha Roles de aprovisionamiento si desea anidar roles de aprovisionamiento en esta ficha.

   Este paso requiere que haya activado los roles anidados (en la página 214) para este entorno.

5. Complete la ficha Administradores agregando reglas de administración que controlen quién gestiona los miembros y administradores del rol.

6. Complete la ficha Propietarios agregando reglas de propietarios que controlen quién puede modificar este rol.

7. Haga clic en Enviar.
8. Para verificar que se ha creado el rol, haga clic en Roles de aprovisionamiento y, a continuación, Ver rol de aprovisionamiento.

Tareas de rol y plantilla

En la Consola de usuario, puede crear y gestionar roles de aprovisionamiento mediante la selección de Roles y tareas, así como la selección de una tarea de Roles de aprovisionamiento. Existen tareas para las operaciones estándar como, por ejemplo, convertir a un usuario en miembro de un rol, y modificar o suprimir un rol.

Antes de crear un rol de aprovisionamiento, necesita una plantilla de cuenta en la que incluir ese rol o un rol de aprovisionamiento que desee importar. Puede importar roles que se hayan creado en el Gestor de aprovisionamiento o eTrust Admin. No obstante, CA Identity Manager no admite roles anidados que se hayan creado en eTrust Admin.

Importación de una función de aprovisionamiento

Aunque gestione los roles de aprovisionamiento en la Consola de usuario, es posible que algunos roles de aprovisionamiento se hayan creado en el gestor de aprovisionamiento o en una aplicación externa. En el caso de estos roles de aprovisionamiento, se puede restablecer el propietario del rol para que sea un administrador de CA Identity Manager, de manera que se pueda gestionar en la Consola de usuario.

Para importar una función de aprovisionamiento

1. Inicie sesión en la Consola de usuario como un usuario con el rol de gestor del sistema. Haga clic en Tareas, Roles y tareas.
2. Haga clic en Roles de aprovisionamiento, Restablecer propietarios del rol de aprovisionamiento y seleccione un rol de aprovisionamiento creado en el gestor de aprovisionamiento.
3. Complete la ficha Propietarios agregando reglas de propietarios que controlen quién puede modificar este rol.
4. Haga clic en Enviar.

Ahora la función se puede modificar, asignar o visualizar mediante las tareas de la categoría de Funciones de aprovisionamiento.

Asignación de nuevos propietarios a roles de aprovisionamiento

Puede seleccionar uno o más roles de aprovisionamiento y asignar políticas de propietario para controlar quién puede modificar los roles.

Para asignar nuevos propietarios a roles de aprovisionamiento

1. Inicie sesión en la Consola de usuario como un usuario con el rol de gestor del sistema.
2. Haga clic en Tareas, Roles o haga clic en Roles y tareas.
3. Haga clic en Roles de aprovisionamiento, Crear políticas de propietarios para roles de aprovisionamiento.
4. Seleccione uno o varios roles de aprovisionamiento.
5. Complete la ficha Propietarios agregando reglas de propietarios que controlen quién puede modificar este rol.
6. Haga clic en Enviar.

Los usuarios que cumplen con las políticas de propietario nuevas pueden modificar los roles de aprovisionamiento seleccionados.

Contraseñas para las cuentas creadas por roles de aprovisionamiento

Cuando a un usuario se le asigna un rol de aprovisionamiento, durante la creación de la cuenta para ese usuario se produce un error si la contraseña del usuario de CA Identity Manager no cumple los requisitos de la contraseña del punto final. Esta situación incluye la creación de un usuario nuevo con una contraseña provisional.

Por lo tanto, establezca la política de contraseñas para que coincida o para que sea más estricta que los requisitos de la contraseña de punto final. Se puede establecer la política de contraseñas mediante la política de contraseñas de CA Identity Manager o el perfil de la contraseñas de aprovisionamiento. Si se utilizan los dos métodos, las políticas deberán coincidir.

Orden de procesamiento de eventos del rol de aprovisionamiento

Entre las tareas de CA Identity Manager se incluyen *eventos*, acciones que realiza CA Identity Manager para finalizar una tarea y que determinan la pertenencia al rol de aprovisionamiento. Por ejemplo, la tarea Modificar usuario incluye AssignProvisioningRoleEvent y RevokeProvisioningRoleEvent. La asignación o la revocación de un rol de aprovisionamiento puede agregar o eliminar una cuenta en un punto final. En algunos casos, el punto final puede necesitar que todas las acciones de Agregar tengan lugar antes de las acciones Eliminar.

Para que el proceso de CA Identity Manager agregue las acciones en primer lugar, active el valor Accumulation of Provisioning Role Membership Events (Activar la acumulación de eventos de pertenencia del rol de aprovisionamiento) en la Consola de gestión. Cuando se activa este valor, CA Identity Manager acumula todas las acciones Agregar y Eliminar en un solo evento, denominado AccumulatedProvisioningRolesEvent. Por ejemplo, si la tarea Modificar usuario asigna un usuario a tres roles de aprovisionamiento y elimina ese usuario de otros dos roles de aprovisionamiento, se generará AccumulatedProvisioningRolesEvent que contiene cinco acciones: 3 acciones Agregar y 2 acciones Eliminar.

Cuando se ejecute este evento, todas las acciones Agregar se combinarán en una sola operación y se enviarán al servidor de aprovisionamiento con el fin de procesarlas. Una vez que haya finalizado el procesamiento de las acciones de agregar, CA Identity Manager combinará las acciones de eliminar en una sola operación y enviará dicha operación al servidor de aprovisionamiento.

La activación de esta configuración repercute en las siguientes funciones de CA Identity Manager:

- **Ficha Roles de aprovisionamiento en Tareas de usuario**

  Cuando un administrador agrega o elimina un usuario de un rol de aprovisionamiento mediante el uso de la ficha Roles de aprovisionamiento, CA Identity Manager acumula estas acciones en un solo evento.

- **Políticas de identidad**

  Todos los eventos de pertenencia al rol de aprovisionamiento (AssignProvisioningRoleEvent o RevokeProvisioningRoleEvent) que se generan como resultado de una evaluación de Identity Policy se acumulan en un único AccumulatedProvisioningRolesEvent. CA Identity Manager ejecuta este evento como cualquier otro evento secundario. Por ejemplo, piense en un conjunto de políticas de identidad que incluya dos políticas: La Política A revoca la pertenencia en el Rol de aprovisionamiento A y la Política B convierte a los usuarios en miembros del Rol de aprovisionamiento B. Si CA Identity Manager determina que un usuario ya no cumple la Política A, pero ahora cumple la Política B, se generará un evento AccumulatedProvisioningRolesEvent con dos acciones (una para la acción Eliminar y otra para la acción Agregar). La acción Agregar se ejecutará en primer lugar y, a continuación, se ejecutará la acción Eliminar.

- **Ver tareas enviadas**

  Para ver el estado de AccumulatedProvisioningRolesEvent, así como el estado de cada una de las acciones individuales, utilice la tarea Ver tareas enviadas, en la que verá los detalles del evento.

  Si se produce un error en una acción individual, el estado del evento será de error, y la tarea pasará al estado de error.

- **Flujo de trabajo**

  Puede asociar un proceso de flujo de trabajo con AccumulatedProvisioningRolesEvent. En este caso, un aprobador puede aprobar o rechazar el evento completo y, de este modo, aprobar o rechazar todos los eventos individuales.

  Se necesita configuración adicional para activar el flujo de trabajo de los eventos individuales en AccumulatedProvisioningRolesEvent.

- **Auditoría**

  CA Identity Manager audita la información acerca de AccumulatedProvisioningRolesEvent y de cada evento individual.

Activación de la acumulación de eventos de pertenencia del rol de aprovisionamiento

CA Identity Manager proporciona un parámetro de configuración en la Consola de gestión que permite la combinación de todas las acciones Agregar y Eliminar para un evento de pertenencia del rol de aprovisionamiento en una sola operación. Una vez que se han combinado, CA Identity Manager procesa las acciones Agregar en una sola operación antes de procesar las acciones Eliminar.

Esta configuración hace posible una secuencia de eventos necesaria para algunos tipos de puntos finales.

Nota: Esta función está desactivada de forma predeterminada.

Para activar la acumulación de eventos de pertenencia del rol de aprovisionamiento

1. Acceda a la Consola de gestión de Identity Manager.
2. Haga clic en Entornos.
3. Seleccione el entorno que desee configurar.
4. Abra Configuración avanzada, Aprovisionamiento.
5. Seleccione la casilla de verificación Activar la acumulación de eventos de pertenencia del rol de aprovisionamiento.
6. Reinicie el servidor de aplicaciones.

Activación de roles anidados en un entorno

Se puede incluir un rol de aprovisionamiento dentro de otro rol de aprovisionamiento. El rol incluido se denomina rol anidado.

Por ejemplo, se podría crear un rol de aprovisionamiento de empleado. El rol de empleado proporcionaría cuentas requeridas por todos los empleados, como cuentas de correo electrónico. El rol de empleado se incluye dentro de los roles de aprovisionamiento específicos de departamentos, tales como el rol de contabilidad y el rol de ventas. Los roles de aprovisionamiento de departamento proporcionarían cuentas relacionadas únicamente con ese departamento. Esta combinación de roles proporciona las cuentas correctas para cada usuario.

Para permitir roles anidados en un entorno

1. En la Consola de gestión, seleccione el entorno.
2. Haga clic en Configuración de roles y tareas, Importar.
3. Seleccione Soporte de roles de aprovisionamiento anidado.
4. Haga clic en Finalizar.
5. Reinicie el entorno.

Incluya un rol en un rol de aprovisionamiento

Para incluir un rol en un rol de aprovisionamiento

1. Vaya a Roles y tareas, Roles de aprovisionamiento, Modificar roles de aprovisionamiento.
2. Complete la ficha Roles de aprovisionamiento al hacer clic en Agregar un rol y seleccionar un rol de aprovisionamiento.

   Por motivos de rendimiento, se recomienda limitar la anidación de roles a tres niveles. Por ejemplo, en el rol de aprovisionamiento actual (el rol de primer nivel) incluye otro rol (el rol de segundo nivel), que puede contener un rol de tercer nivel. Se recomienda que el rol de tercer nivel no contenga ningún rol.
3. Complete la política de propietarios modificando la regla de propietarios.

   El ámbito debe ser igual que el alcance del rol que agregó o más amplio.
4. Haga clic en Enviar.

Atributos de las plantillas de cuenta

Los atributos de las plantillas de cuenta determinan cómo se definen los atributos en la cuenta.

Capacidad y atributos iniciales

Las plantillas de cuenta incluyen dos tipos de atributos:

- *Atributos de capacidad* que representan información de la cuenta como, por ejemplo, tamaño de almacenamiento, cantidad, límites de frecuencia o miembros del grupo. El Gestor de aprovisionamiento muestra en negrita los atributos de capacidad en todas las pantallas de plantillas de cuenta para simplificar la identificación de los atributos de capacidad.
- *Atributos iniciales* que representan toda la información que se configura inicialmente para una cuenta como, por ejemplo, nombre de cuenta, contraseña y estado de la cuenta, así como información personal, como el nombre, la dirección y los números de teléfono.

Las cuentas se consideran sincronizadas con sus plantillas de cuenta cuando todos los atributos de capacidad están sincronizados. Estos atributos son diferentes en cada tipo de punto final como, por ejemplo, miembros del grupo, privilegios, cuotas, restricciones de inicio de sesión, que controlan lo que hace el usuario cuando inicia sesión en la cuenta.

La sincronización no actualiza otros atributos de cuenta. Se inicializan desde las plantillas de cuenta durante la creación de una cuenta y también se pueden actualizar durante las funciones de propagación. El servidor de aprovisionamiento proporciona dos funciones de propagación (una actualización inmediata de las cuentas en el momento del cambio de la plantilla de cuenta y una actualización de las cuentas en el momento del cambio de los atributos de usuario global).

Búsqueda de la capacidad y atributos iniciales

Para descubrir qué atributos se definen como capacidades y cuáles son iniciales, es necesario generar el archivo eTACapability.txt. Introduzca el comando siguiente desde un símbolo del sistema de Windows:

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

Especifica C:\Program Files\CA\Identity Manager\Provisioning Server\bin

Una versión del archivo se genera para todos los conectores que se han instalado.

Cadenas de reglas en plantillas de cuenta

Cuando se crea una plantilla de cuenta, se utilizan cadenas de reglas para definir el formato de muchos atributos de cuenta. Las cadenas de reglas son variables para el valor real. Las cadenas de reglas son útiles cuando se desea generar atributos que cambian de una cuenta a otra. Cuando se evalúan las reglas, CA Identity Manager sustituye las cadenas de reglas introducidas en las plantillas de cuenta por los datos especificados en el objeto de usuario.

Nota: La evaluación de las reglas no se realiza en las cuentas creadas durante una exploración ni en las cuentas creadas sin roles de aprovisionamiento.

En la tabla siguiente aparecen las cadenas de reglas de CA Identity Manager:

Cadena de regla	Descripción
%AC%	Nombre de la cuenta
%D%	Fecha actual con el formato *dd/mm/aaaa* (la fecha es una valor calculado y no está relacionada con la información del usuario global*).* Esta cadena de regla es equivalente a una de las siguientes: %$$DATE()% %$$DATE%
%EXCHAB%	Buzón oculto de la libreta de direcciones de intercambio
%EXCHS%	Nombre del servidor de inicio del buzón
%EXCMS%	Nombre del almacén del buzón de correo
%GENUID%	Identificador numérico de usuario de UNIX/POSIX Esta variable de regla es la misma que %UID%, siempre que se haya configurado el valor UID del usuario global. Sin embargo, si el usuario global no tiene un valor de UID asignado, y la generación de UID está activada (Propiedades globales en Tarea del sistema), se producirán varias acciones. El siguiente valor de UID disponible se adjudica, se asigna al usuario global y se utiliza como el valor de esta variable de regla.
%P%	Contraseña
%U%	Nombre de usuario global
%UA%	Dirección completa (generada a partir de la calle, la ciudad, el estado y el código postal)
%UB%	Edificio
%UC%	Ciudad
%UCOMP%	Nombre de la compañía
%UCOUNTRY%	País

Cadena de regla	Descripción
%UCU*xx*% o %UCU*xxx*%	El campo personalizado (*xx* o *xxx* representa el ID de campo de dos o tres dígitos, de acuerdo con lo especificado en la ficha Campos personalizados por el usuario del marco de tareas del sistema)
%UD%	Descripción
%UDEPT%	Departamento
%UE%	Dirección de correo electrónico
%UEP%	Dirección de correo electrónico principal
%UES%	Direcciones de correo electrónico secundarias
%UF%	Nombre
%UFAX%	Número de fax
%UHP%	Página de inicio
%UI%	Iniciales
%UID%	Identificador numérico de usuario de UNIX/POSIX
%UL%	Apellidos
%ULOC%	Ubicación
%UMI%	Inicial del segundo nombre
%UMN%	Segundo nombre
%UMP%	Número de teléfono móvil
%UN%	Nombre completo
%UO%	Nombre de la oficina
%UP%	Número de teléfono
%UPAGE%	Número de buscapersonas
%UPC%	Código postal
%UPE%	Extensión del número de teléfono
%US%	estado
%USA%	Dirección postal
%UT%	Cargo

Cadena de regla	Descripción
%XD%	Genera la marca de hora en formato XML dateTimeValue, un formato de cadena de longitud fija. En un atributo dateValue o timeValue, puede escribir una expresión de subcadena (:desplazamiento,longitud) para extraer la fecha o partes de la hora de dateTimeValue. Por ejemplo, %XD:1,10% genera AAAA-MM-DD; y %XD:12,8% genera HH:MM:SS.

Valores de los atributos

Para usar un valor específico y constante para un atributo de cuenta, escriba el valor en el campo de la plantilla de la cuenta en lugar de hacerlo en una cadena de regla. Por ejemplo, puede escribir valores para especificar límites de frecuencia o volumen de cantidad.

Si el valor del atributo constante debe contener más de un signo de porcentaje, escriba dos signos de porcentaje (%%) cada vez. CA Identity Manager los convertirá en un signo de porcentaje (%) cuando cree el valor del atributo de cuenta. Si el valor de la plantilla de cuenta contiene sólo un signo de porcentaje, CA Identity Manager no generará un error. La regla establece que si desea un valor literal del 25%, deberá especificar 25%%. Sin embargo, como un caso especial, se aceptará 25%.

Expresiones de reglas avanzadas

Para proporcionar mayor flexibilidad que una sencilla sustitución de atributos de usuario global, puede introducir expresiones de reglas avanzadas, entre las que se incluyen las siguientes:

- Subcadenas de expresiones de reglas que utilizan desplazamiento y longitud.
- Combinaciones de cadenas de reglas y valores.
- Expresiones de reglas para configurar varios valores para atributos de cuenta con varios valores.
- Variables de reglas para otros atributos de usuario global.
- Invocación de funciones integradas.
- Invocación de funciones de cierre de programa escritas por el cliente.

Combinación de cadenas de reglas y valores

Puede combinar cadenas de reglas y valores constantes en un valor de atributo de la plantilla de cuenta. Por ejemplo, si no hubiera ninguna cadena de reglas %UI%, podría obtener el mismo efecto mediante la concatenación de varias expresiones de regla, como se muestra a continuación:

```
%UF:,1%%UMI:,1%%UL:,1%
```

La cadena de regla %UA% es equivalente a lo siguiente:

```
%USA%, %UC%, %US%, %UPC%
```

También puede combinar una cadena de reglas con un valor constante para crear un atributo de punto final principal de UNIX, como se muestra a continuación:

```
/u/home/%AC%
```

Subcadenas de reglas

A continuación, se indica la sintaxis para crear un valor de subcadena de una variable de regla:

```
%var[:offset,length]%
```

var

Representa el nombre de la variable de regla predefinida, tal y como se describió en la tabla incluida anteriormente.

offset

(Opcional) Define el desplazamiento inicial del sufijo de sufijo de subcadena. El número 1 representa el primer carácter.

length

(Opcional) Define el desplazamiento final del sufijo de sufijo de subcadena. Un valor de longitud de asterisco (*) indica el final del valor.

Por ejemplo, para definir un atributo de cuenta para los cuatro primeros caracteres del atributo Edificio del usuario global, utilice lo siguiente para definir la variable:

```
%UB:1,4%
```

Si el atributo Edificio está vacío o tiene menos de cuatro caracteres, el valor del atributo de cuenta resultante tendrá menos de cuatro caracteres.

Expresiones de reglas con varios valores

La mayoría de las expresiones de reglas tienen un solo valor. Comienzan a partir de un valor de atributo de usuario (posiblemente vacío) y tienen como resultado un valor de atributo de cuenta (también posiblemente vacío). Sin embargo, a veces preferirá considerar un atributo de usuario vacío como 0 valores. En ocasiones, preferirá generar varios valores para rellenar un valor de atributo de cuenta con varios valores.

La sintaxis siguiente le permite trabajar con cero o más valores que puede contener un atributo de usuario:

%**var*%

El asterisco (*) del indicador de varios valores opcional que aparece inmediatamente después del primer signo de porcentaje % en una expresión de regla indica que el resultado de esta expresión de regla debería ser 0, 1 o más de 1 en función de la cantidad de valores que contenga el atributo de usuario al que se haga referencia.

La mayoría de los valores de atributo son de un solo valor, de manera que sólo pueden contener 0 o 1 valores. Sin embargo, los atributos personalizados (CustomField01 a CustomField99) son atributos con varios valores, de manera que una variable de regla que haga referencia a estos atributos puede contener 0, 1 o más de un valor.

Si un atributo de usuario tiene más de un valor pero no incluye el asterisco (*) en la expresión de regla, el resultado de la evaluación de la regla será el del primer valor. No obstante, en la mayoría de los casos los valores de atributo no se ordenan oficialmente y, como resultado, es posible que no se pueda prever el valor que CA Identity Manager considerará en primer lugar.

Si un atributo de usuario tiene más de un valor e incluye el asterisco (*) en la expresión de regla, se generarán varios valores para el atributo de cuenta. No defina este tipo de expresión de regla con varios valores en una plantilla de cuenta si el atributo de cuenta que se está estableciendo a partir de ese atributo de plantilla de cuenta no es un atributo con varios valores.

Puede definir un atributo de cuenta extendido en el tipo de punto final de ADS para que sea un atributo con varios valores, y utilizar esta sintaxis de expresión de regla con varios valores para definir ese atributo. Por ejemplo, piense en un entorno que defina un atributo de cuenta extendido de ADS denominado patentes y en el atributo de usuario personalizado número tres también denominado patentes.

Una plantilla de cuenta de ADS podría definir la cadena de regla %*UCU03% para el atributo de patentes. A continuación, podría cambiar un atributo de patentes del usuario agregando uno o más valores. Cuando aplique los cambios al usuario, seleccione la opción de actualización de las cuentas del usuario. Esta opción consulta la plantilla de cuenta, busca la variable de regla %*UCU03% y sabe cómo copiar todas las patentes del usuario en el atributo de patentes de la cuenta.

De igual forma, durante la creación de la cuenta, se evalúan las cadenas de regla. Además, durante el cambio de la plantilla de cuenta, si se ha modificado la cadena de regla, podrá recalcular la regla para todas las cuentas asociadas con la plantilla de cuenta.

La sintaxis %**var*% también es significativa para las variables *var* que hacen referencia a atributos de usuario con un solo valor. Esto sólo se aplica cuando existe concatenación y si los atributos a los que se hace referencia no están establecidos en los usuarios.

El asterisco (*) del indicador de varios valores opcional indica que la regla que contiene una variable de regla %**var*% evalúa como sin valor si el atributo de usuario no tiene ningún valor. Esto es diferente de la expresión de regla con un solo valor %*var*%, que siempre evalúa como un solo valor, aunque se trate de una cadena vacía.

Para comprender la diferente, tenga en cuenta las cadenas de regla siguientes:

```
(310)%UP%
 (310)%*UP%
```

Ambas reglas se utilizan para añadir el código de área 310 al número de teléfono. No obstante, son diferentes porque si los usuarios no tienen ningún valor para su número de teléfono, la primera regla evaluará el valor de cuenta de (310). La segunda cadena de regla no genera ningún valor y deja el atributo de cuenta como no establecido.

Por otro lado, considere las cadenas de regla siguientes que se utilizan para añadir la extensión telefónica al número de teléfono:

```
%UP% %UPE%
%UP% %*UPE%
```

Si una persona tiene un número de teléfono pero no tiene ninguna extensión, la primera cadena de regla generará un valor que incluirá el número de teléfono para cada usuario sin ninguna extensión. La segunda cadena de regla no generará ningún valor. En este caso, utilice la primera regla con %UPE%.

Reglas de atributos de usuario global explícitas

Cada usuario tiene muchos más atributos de los que están incluidos en la tabla de reglas anterior. Probablemente, no necesitará crear expresiones de reglas que hagan referencia a estos atributos. Sin embargo, si fuera necesario, puede utilizar la siguiente sintaxis para hacer referencia a un atributo de usuario específico:

```
%#ldap-attribute%
```

Por ejemplo, si debe determinar el valor del campo Suspendido del usuario, puede determinar el nombre del atributo LDAP correspondiente para este campo (que es eTSuspended) y crear la expresión de regla que evalúe a 0 o 1, como eTSuspended:

```
%#eTSuspended%
```

Por ejemplo, también puede obtener los roles de aprovisionamiento del usuario con la siguiente expresión de regla:

```
%*#eTRoleDN%
```

Estos roles de aprovisionamiento son valores de nombre destacado completo de LDAP. Es probable que en combinación con la función integrada RDNVALUE (consulte la tabla siguiente), los valores sean un poco más útiles. Tenga el cuenta el asterisco (*) de indicador de valor múltiple para obtener todos los roles de aprovisionamiento asignados del usuario como varios valores.

La sintaxis de la subcadena también se puede aplicar a estas expresiones de regla, de manera que puede utilizar %#eTTelephone:6,*% con el mismo significado que %UP:6,*. Cada una pide a CA Identity Manager que elimine los cinco primeros caracteres del campo de teléfono del usuario.

Funciones de reglas integradas

Las funciones de reglas integradas se pueden utilizar en las expresiones de reglas para realizar varias transformaciones en los valores. El formato general de la invocación de una función de regla integrada es la siguiente:

```
%[*]$$función(arg[,…])[:desplazamiento,longitud]%
```

donde el asterisco (*) de indicador de valor múltiple y las especificaciones de subcadena de desplazamiento y longitud son nuevamente opcionales.

Las funciones integradas reconocidas son las siguientes:

Función de regla integrada	Descripción
ALLOF	Combina todos los parámetros en un valor con varios valores. Se conserva el orden y se eliminan los duplicados. Por ejemplo, si los atributos de usuario se establecen de acuerdo con lo siguiente: eTCustomField01: { A, B } eTCustomField02: { A, C } La regla: %*ALLOF(%*UCU01%,%*UCU02%)% evaluará los tres valores { A, B, C }.
DATE	Evalúa la fecha actual en formato *dd/mm/aaaa*. La expresión de regla %D% es equivalente a una de las siguientes: %$$DATE()% %$$DATE%
FIRSTOF	Devuelve el primer valor de cualquiera de los parámetros. Se utiliza para insertar un valor predeterminado si no se ha establecido ningún atributo: %$$FIRSTOF(%UCU01%,'unknown')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% Si no se establece ninguno de estos valores, el resultado será ningún valor. Para introducir una cadena constante en un argumento, escríbala entre comillas simples.
INDEX	Devuelve un valor de un atributo con varios valores. Index 1 es el primer valor. Si el índice es mayor que el número de valores, el resultado será el valor no establecido (vacío). Estas reglas son equivalentes a las siguientes: %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%

Función de regla integrada	Descripción
NOTEMPTY	Devuelve un solo valor de su único argumento pero notifica un error si no se establece este atributo. Ejemplo 1: Se produce un error en la creación o la actualización si el usuario no tiene asignado un atributo UID: %$$NOTEMPTY(%UID%)% Ejemplo 2: Se utiliza el nombre, a menos que no se haya establecido, en cuyo caso se utilizará el apellido. Si no se ha establecido ninguno, se producirá un error en la creación o la actualización. %$$NOTEMPTY(%$$FIRSTOF(%UF% %UL%)%)%
PRIMARYEMAIL	Devuelve la dirección de correo electrónico principal de varias direcciones de correo electrónico. La expresión %UE% es equivalente a lo siguiente: %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	Trata el valor de atributo como un nombre destacado de LDAP y extrae el nombre común del objeto del DN: %*$$RDNVALUE(%#eTRoleDN%)% Devuelve los nombres comunes de todos los roles de aprovisionamiento asignados. Si el usuario pertenece a dos roles de aprovisionamiento con el mismo nombre común, el nombre de ese rol se lista una vez.
TOLOWER	Convierte el texto en mayúsculas en texto en minúsculas: %$$TOLOWER(%AC%)%
TOUPPER	Convierte el texto en minúsculas en texto en mayúsculas: %$$TOUPPER(%U%)%

Función de regla integrada	Descripción
TRIM	Elimina los caracteres en blanco iniciales o finales de un valor de atributo. Por ejemplo, “%UF %UL%” suele crear un valor con el nombre y el apellido separados por un carácter en blanco. Sin embargo, si el usuario tuviera el atributo de nombre vacío, esta regla generaría un valor que terminaría con un carácter en blanco final. No obstante, al utilizar “%$$TRIM(%UF% %UL%)% se asegura de que no exista ningún carácter inicial ni final en blanco en el valor del atributo de cuenta aunque no se haya establecido el nombre o el apellido.

Rendimiento de roles de aprovisionamiento

Al emplear CA Identity Manager con un servidor de aprovisionamiento, existen determinadas mejoras de rendimiento de aprovisionamiento que debería tener en cuenta.

Caché de objetos JIAM

Identity Manager se comunica con el servidor de aprovisionamiento mediante el uso de la API de Java IAM (JIAM). Para mejorar el rendimiento de la comunicación, la caché se configura para los objetos recuperados del servidor de aprovisionamiento.

Activación de la caché de JIAM

Para activar la caché de JIAM

1. Acceda a la configuración del entorno a través de la Consola de gestión. Haga clic en Configuración avanzada, Varios.
2. Configure la propiedad definida por el usuario para la caché de JIAM.
   - **Propiedad**: JIAMCache
   - **Valor**: true
3. Haga clic en Agregar.
4. Haga clic en Guardar.

   Se guardará la propiedad definida por el usuario.

Definición de TTL (tiempo de vida) de caché de JIAM

La caché de JIAM almacena información durante un período de tiempo específico antes de que caduquen los datos. Este período de tiempo se conoce como tiempo de vida (TTL). El valor (en segundos) de TTL de caché de JIAM se establece para definir el tiempo que los datos permanecen en la memoria caché.

Para obtener el máximo beneficio de los datos almacenados localmente en la caché, se equilibra el aumento de rendimiento con la obtención de datos puntuales. Se recomienda un valor mínimo de TTL de un día y un valor máximo de siete días. Para conocer los valores de tiempo de vida que se deben utilizar, consulte la tabla siguiente:

Vigencia deseada	Configuración de TTL (segundos)
24 horas (1 día)	86.400
72 horas (3 días)	259.200
120 horas (5 días)	432.000
168 horas (7 días)	604.800

Para definir la TTL de la caché de JIAM

1. Acceda a la configuración del entorno a través de la Consola de gestión. Haga clic en Configuración avanzada, Varios.
2. Configure la propiedad definida por el usuario para la TTL de la caché de JIAM.
   - **Propiedad**: JIAMCacheTTL.
   - **Valor**: número de segundos que los datos permanecen en la caché de JIAM.

     Valor predeterminado: 300
3. Haga clic en Agregar.
4. Haga clic en Guardar.

   Se guardará la propiedad definida por el usuario.

Agrupación de sesiones

Para mejorar el rendimiento, Identity Manager puede asignar previamente un número de sesiones para que se agrupen cuando se utilicen para comunicarse con el servidor de aprovisionamiento.

Para obtener más información sobre la agrupación de sesiones, consulte la *Ayuda en línea de la Consola de gestión.*

Tareas de aprovisionamiento para entornos existentes

Si importa definiciones de roles personalizados y desea activar el aprovisionamiento en un entorno, *también* debe importar las definiciones de los roles de sólo aprovisionamiento de la Consola de gestión. Estas definiciones de roles se encuentran en la carpeta siguiente:

`iam_im.ear\management_console.war\WEB-INF\Template\environment`

Nota: Para obtener más información sobre la importación de definiciones de roles, consulte la *Guía de configuración*.

Capítulo 10: Servicios gestionados (Solicitudes de acceso básicas)

Esta sección contiene los siguientes temas:

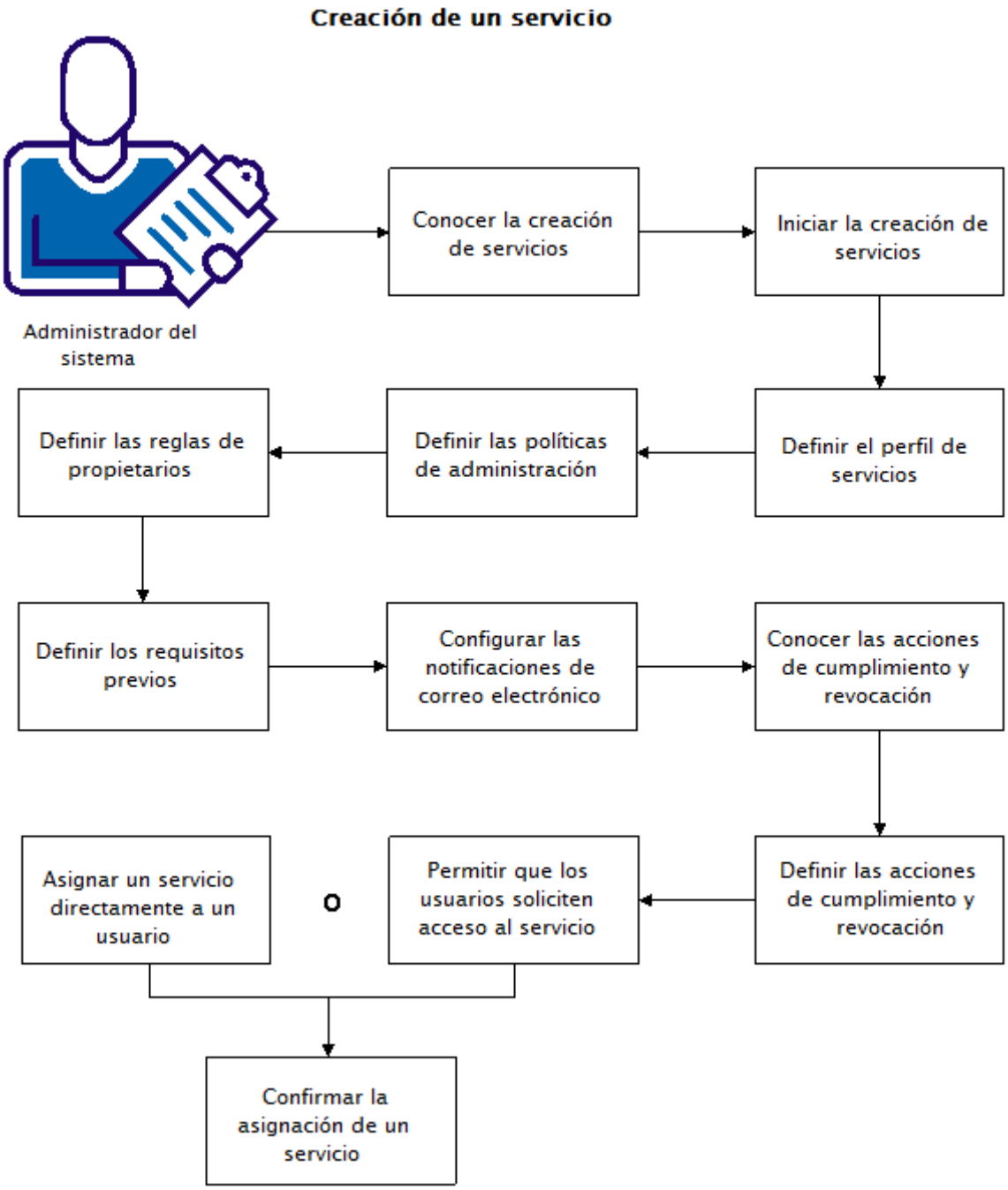
Creación de un servicio

Los servicios simplifican la gestión de las autorizaciones Un servicio agrupa todas las autorizaciones (tareas, roles, grupos y atributos) que un usuario necesita para un rol de negocio determinado. El usuario tendrá los servicios a disposición mediante las tareas de solicitud de acceso en la Consola de usuario de CA CloudMinder. 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.

El diagrama siguiente muestra la información sobre los pasos que deben realizarse a la hora de crear un servicio.


Creación de un servicio
Administrador del sistema
Conocer la creación de servicios
Iniciar la creación de servicios
Definir el perfil de servicios
Definir las políticas de administración
Definir las reglas de propietarios
Definir los requisitos previos
Configurar las notificaciones de correo electrónico
Conocer las acciones de cumplimiento y revocación
Definir las acciones de cumplimiento y revocación
Permitir que los usuarios soliciten acceso al servicio
O
Asignar un servicio directamente a un usuario
Confirmar la asignación de un servicio

En los temas siguientes se explica cómo crear un servicio y ponerlo a disposición de los usuarios:

1. Conocimiento de la creación de servicios.
2. Inicio de la creación de servicios (en la página 233).
3. Definición del perfil de servicios.
4. Definición de las políticas de administración para el servicio (en la página 235).
5. Definición de las reglas de propietarios para el servicio (en la página 236).
6. Definición de los requisitos previos para el servicio (en la página 236).
7. Configuración de las notificaciones de correo electrónico para la renovación del servicio. (en la página 237)
8. Conocimiento de las acciones de cumplimiento y revocación (en la página 238).
9. Definición de las acciones de cumplimiento y revocación para el servicio. (en la página 238)
10. Permisión a los usuarios para solicitar acceso a servicios.

    En la Consola de usuario, cuando el usuario hace clic en Mi acceso y, a continuación, en Solicitar y ver acceso, el usuario tendrá a su disposición una lista de servicios para la solicitud. Los servicios que aparecen en esta lista son los que ha marcado un administrador como Autosuscripción con los privilegios adecuados, normalmente durante la creación de un servicio.
11. Asignación de un servicio directamente a un usuario (en la página 87).
12. Confirmación de la asignación de un servicio.

Conocimiento de la creación de servicios

Antes de la creación de un servicio, tenga en cuenta las autorizaciones y la información previa necesarias para la creación y cumplimiento del servicio.

Tenga en cuenta las preguntas siguientes:

1. ¿Qué necesidad empresarial aborda este servicio? Por ejemplo, se puede crear un servicio que pone una cuenta de Salesforce.com a disposición de todos los empleados nuevos.
2. ¿Necesitan los miembros del servicio roles de administrador? En este caso, cree o identifique los roles de administrador.
3. ¿Deben recibir los miembros del servicio acceso a uno o más puntos finales? En este caso, cree o identifique los puntos finales.
4. Si los miembros del servicio necesitan acceder a los puntos finales, cree o identifique los roles de aprovisionamiento y las plantillas de cuenta asociadas.

5. ¿Necesitan los miembros del servicio ser miembros de grupos? En este caso, cree o identifique los puntos finales.
6. ¿Es necesario consultar o modificar ciertos atributos de usuario cuando un usuario se convierte en miembro del servicio? Por ejemplo, cuando un usuario recibe el servicio Salesforce.com, ¿se debe confirmar si el atributo de departamento para el usuario se establece como Ventas? En este caso, cree o identifique los atributos de usuario.

Una vez se han creado o identificado los requisitos previos, podrá empezar con la creación de servicios (en la página 233).

Inicio de la creación de servicios

El usuario crea un servicio desde la Consola de usuario.

Siga estos pasos:

1. Inicie sesión en una cuenta que dispone de privilegios de gestión de servicios.

   Por ejemplo, el primer usuario de un entorno tiene el rol de gestor del sistema y tiene la tarea Crear servicio.
2. En el menú de navegación, seleccione Servicios, que se pueden enumerar bajo Tareas.
3. Haga clic en Gestionar servicios, Crear servicio.
4. Definición del perfil de servicios.

Definición del perfil de servicios

En la ficha Perfil, se pueden definir las características básicas del servicio.

Siga estos pasos:

1. Introduzca un nombre y una etiqueta. Una etiqueta es un identificador único del servicio.

   Nota: Las etiquetas pueden contener solamente caracteres alfanuméricos y no pueden empezar con un número. Una vez se ha creado, el nombre de etiqueta no se puede cambiar ni reutilizar, aunque un servicio se suprima más tarde.
2. Seleccione Activado si desea poner el servicio a disposición de los usuarios para su uso después de crearlo.
3. Seleccione Autosuscripción si desea que aparezca este servicio en la lista de servicios disponibles para que los usuarios lo soliciten. Cuando se activa Autosuscripción, los usuarios podrán solicitar acceso a este servicio a través de la Consola de usuario.

4. (Opcional) Agregue una o varias categorías. Escriba un nombre de categoría y haga clic en la flecha hacia arriba para agregarla al servicio.

   Las categorías agregan información adicional a un servicio. Esta información adicional se puede usar para simplificar la búsqueda de servicios en entornos que incluyan un gran número de servicios.

5. Especifique una hora en la pantalla de datos del usuario del periodo de ejecución del servicio si desea recopilar más datos sobre el usuario en el momento en que un usuario solicita el servicio.

   Utilice una pantalla de datos del usuario del periodo de ejecución del servicio para garantizar que el sistema dispone de todos los datos del usuario necesarios para cumplir el servicio. Por ejemplo, se requiere una dirección de correo electrónico válida para cumplir un servicio que crea una cuenta en Google Apps. Si una dirección de correo electrónico de un usuario no existe en el almacén de usuarios de CA CloudMinder, el usuario deberá proporcionarlo al solicitar el servicio.

   a. Haga clic en Examinar.

      Aparece una lista de las pantallas de perfil disponibles. Estas pantallas normalmente se utilizan para recopilar datos del usuario.

   b. Seleccione una pantalla de perfil que contenga los datos del usuario que desee recopilar. Seleccione una de las siguientes opciones:

      - Haga clic en Seleccionar para recopilar todos los datos del usuario que contiene la pantalla.

      O

      - Haga clic en Copiar para personalizar los datos del usuario que desee recopilar. Especifique un nombre y etiqueta única para la nueva pantalla. Agregue, edite o elimine elementos de datos del usuario y haga clic en Aceptar.

      O

      - Haga clic en Editar para cambiar los datos del usuario que presenta la pantalla. Agregue, edite o elimine elementos de datos del usuario y haga clic en Aceptar.

      Importante: Si se edita una pantalla de datos del usuario, los cambios se aplicarán en todos los sitios de la Consola de usuario en la que se utilice la pantalla. Tenga en cuenta que se puede copiar y personalizar la pantalla del perfil.

   c. Haga clic en Seleccionar.

      Los elementos de datos del usuario seleccionados se recopilan en el momento en que el usuario solicita el servicio.

      Nota: Si los datos necesarios se encuentran en el sistema cuando un usuario solicita el servicio, los datos se rellenan previamente en la pantalla de perfil.

6. Definición de las políticas de administración para el servicio (en la página 235).

Definición de las políticas de administración para el servicio

En la ficha Administradores, el usuario define quién puede agregar o eliminar usuarios como miembros y administradores de este servicio. Las políticas de administración contienen reglas del ámbito de administración y un privilegio de administrador como mínimo (Gestionar miembros o Gestionar administradores).

Las reglas de administrador definen quién puede administrar este servicio. Las reglas del ámbito limitan qué usuarios pueden convertirse en administradores. Por ejemplo, una regla de administrador puede permitir a todos los miembros del grupo de Ventas a que administren un servicio. Una regla de ámbito puede limitar solamente a los usuarios del grupo de Ventas en Boston, MA.

Siga estos pasos:

1. En la ficha Administradores, haga clic en Agregar.

   Aparecerá la pantalla Política de administración.

2. Defina una regla de administrador para la cual los usuarios puedan administrar este servicio. Por ejemplo, se pueden especificar los usuarios miembros del grupo de Ventas o que tienen el atributo de perfil de cargo específico de Director de Ventas.

   Haga clic en la flecha de la izquierda para editar una parte que se ha especificado previamente de una regla.

3. Defina una regla de ámbito para limitar qué usuarios pueden administrar este servicio. Por ejemplo, si se especifican usuarios miembros del grupo de Ventas en la regla de administrador, se puede limitar el ámbito de la regla solamente a los usuarios cuya ciudad sea Boston, MA.

   Nota: Se pueden agregar varias políticas de administración con reglas y privilegios diferentes para cada servicio.

4. Si desea que los administradores agreguen o eliminen miembros de este servicio, haga clic en Puede gestionar miembros de este servicio.

5. Haga clic en Aceptar.

6. Para continuar editando una política, haga clic en el icono Editar. Para eliminar una política, haga clic en el icono con el signo menos.

7. Definición de las reglas de propietarios para el servicio. (en la página 236)

Definición de las reglas de propietarios para el servicio

En la ficha Propietarios, se pueden definir las reglas sobre quién puede ser propietario del servicio. Un propietario es un usuario que puede modificar el servicio.

Siga estos pasos:

1. En la ficha Propietarios, haga clic en Agregar.

   Aparece la pantalla Regla de propietarios.

2. Defina una regla de propietarios para la cual los usuarios puedan administrar este servicio. Por ejemplo, se pueden especificar los usuarios miembros del grupo de Ventas o que tienen el atributo de perfil de cargo específico de Director de Ventas.

   Haga clic en la flecha de la izquierda para editar una parte que se ha especificado previamente de una regla.

3. Haga clic en Aceptar.

4. Definición de los requisitos previos para el servicio. (en la página 236)

Definición de los requisitos previos para el servicio

En la ficha Requisitos previos, defina los servicios de los que los usuarios deben disponer antes de solicitar este servicio. Un servicio solamente aparece en la lista de servicios disponibles para un usuario dado si este usuario es miembro de todos los servicios previos.

Si se establece una duración para un servicio previo, esta duración se aplicará al servicio que se está definiendo. Por ejemplo, el Servicio A es un requisito previo para el Servicio B. El Servicio A tiene una duración de una semana. El Servicio B también caduca en una semana.

Siga estos pasos:

1. En la ficha Requisitos previos, haga clic en Agregar servicio.

   Aparece una pantalla de búsqueda.

2. Busque un servicio que desee designar como requisito previo para este servicio.

   Para mostrar una lista de todos los servicios para los cuales dispone de privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

3. Seleccione un servicio y haga clic en Seleccionar.

   Aparece una lista actualizada de requisitos previos para este servicio.

Configuración de las notificaciones de correo electrónico para la renovación del servicio

Algunos servicios caducan después de un cierto período.

En la ficha Correo electrónico, se puede configurar una notificación de correo electrónico que recuerda a los miembros de servicio que deben renovar su pertenencia antes de que caduque. Los miembros pueden utilizar la tarea Renovar servicio para renovar su acceso.

CA CloudMinder proporciona una plantilla de correo electrónico predeterminada que incluye contenido dinámico. Este contenido se rellena automáticamente cuando se envía el correo electrónico. El contenido dinámico, que aparece entre llaves ({ }) en el editor de la notificación de correo electrónico, agrega al correo electrónico un nombre de usuario específico, un nombre de servicio y una fecha de caducidad.

En el editor se puede modificar el contenido de la notificación de correo electrónico. Por ejemplo, se puede modificar el contenido o texto del asunto, cambiar el tipo de letra o eliminar el contenido dinámico.

Tenga en cuenta los elementos siguientes al configurar las notificaciones de correo electrónico:

- Si incluye contenido dinámico en la notificación de correo electrónico, no modifique el texto entre llaves ({ }).
- Si el servicio tiene un servicio previo que caduca, las notificaciones de correo electrónico se enviarán solamente para el servicio previo, incluso cuando se configuran notificaciones de correo electrónico para los dos servicios.

Siga estos pasos:

1. En la ficha Correo electrónico, seleccione la casilla de verificación Notificación de correo electrónico para los usuarios antes de que caduque un servicio para activar las notificaciones.
2. (Opcional) Personalice la notificación de correo electrónico mediante los controles en el editor.

   El editor de la notificación de correo electrónico admite HTML. Se puede agregar contenido de HTML al contenido de la notificación de correo electrónico haciendo clic en el botón Toggle HTML Source (botón de alternancia del código fuente de HTML) (<>) en la barra de herramientas.
3. Conocimiento de las acciones de cumplimiento y revocación. (en la página 238)

Conocimiento de las acciones de cumplimiento y revocación

En la ficha Acciones, defina las autorizaciones y la información (tareas, roles, grupos, y atributos) que deben agregarse, modificarse o eliminarse cuando un servicio se asigna o se revoca. Introduzca sencillamente que las acciones de servicio definen las acciones que realiza un servicio.

CA CloudMinder utiliza una política exprés para definir las circunstancias bajo las cuales ocurren las acciones de cumplimiento y revocación. CA CloudMinder configura esta política previamente de modo que cuando un usuario solicite un servicio existan las condiciones y los datos apropiados. El servicio se cumple o se revoca automáticamente.

Un administrador debe definir las acciones que toma el sistema para cumplir o revocar un servicio. Por ejemplo, al crear un servicio, un administrador puede especificar que los miembros de servicio reciban el rol de administrador Director de ventas, el rol de aprovisionamiento Salesforce.com y el grupo Ventas. Asimismo, el administrador puede especificar que estas autorizaciones se eliminen al revocar el servicio.

Definición de las acciones de cumplimiento y revocación para el servicio

En la ficha Acciones, defina las autorizaciones y la información que el sistema agrega, modifica o elimina cuando se asigna o se elimina el servicio de un usuario.

Siga estos pasos:

1. Haga clic en la ficha Acciones.

   Aparece la pantalla de las acciones de cumplimiento y revocación.

2. Haga clic en los botones Gestionar acciones de cumplimiento o Gestionar acciones de revocación.

   Se muestra la pantalla Crear política exprés.

   Los siguientes campos se han predefinido con el fin de crear una regla de acción:

   Nombre

   Proporciona un nombre descriptivo para la regla de acción. Este nombre debe ser único.

   Descripción

   Define el significado de una regla de acción.

   Prioridad

   Define qué regla de acción se ejecuta, en caso de que haya varias que coincidan. Este campo resulta útil para definir las acciones predeterminadas. Por ejemplo, si tiene varias reglas, una para cada nombre de departamento, es posible configurar una predeterminada agregando una regla adicional sin condiciones, pero con una prioridad más baja (como 10 si las demás son de 5). Si no coincide ninguna regla de departamento, se utiliza la predeterminada.

3. Especifique los criterios para cumplir las condiciones de la regla de acción.
4. Haga clic en Agregar acción cuando el botón Coincidente se encuentre debajo de Agregar acciones.

   Aparece la pantalla Agregar acción cuando coincida. En esta pantalla, defina las acciones que realiza el sistema cuando se cumpla la regla.
5. Introduzca un nombre descriptivo que defina la finalidad de la acción.

   Por ejemplo, introduzca Agregar el rol de administrador del Director de ventas."
6. Seleccione la categoría de acción que desee que realice el sistema.

   Por ejemplo, para agregar un rol, seleccione la categoría Roles.
7. Seleccione el tipo de acción que desee que realice el sistema.

   Por ejemplo, para agregar o eliminar un rol de administrador, seleccione el tipo Configurar rol de admin.
8. Seleccione la función que desee que realice el sistema.

   Por ejemplo, para agregar un rol de administrador, seleccione la función Agregar.

   Nota: Cuando se selecciona una función, aparece una descripción de la función. Esta descripción ayuda a determinar si la función seleccionada da lugar al comportamiento del sistema que desea.
9. Defina la acción específica que desee que realice el sistema.

   Por ejemplo, para agregar un rol de administrador denominado Director de ventas, introduzca el nombre de rol o haga clic en el botón Examinar y seleccione Director de ventas de la lista de roles de administrador disponibles.
10. Haga clic en Aceptar.

    Repita este procedimiento hasta agregar todas las acciones deseadas para el servicio.
11. Haga clic en Aceptar.

    El sistema asocia las acciones de cumplimiento y revocación designadas con el servicio. Cuando un usuario recibe el servicio, las autorizaciones asociadas y la información se agrega, modifica o elimina.
12. Ahora se puede asignar un servicio a un usuario (en la página 87).

Asignación de un servicio a un usuario

Se puede asignar un servicio directamente a un usuario individual. Este usuario se convierte en *miembro* del servicio.

Siga estos pasos:

1. Vaya a Servicios, Solicitar y ver acceso.

   Aparece una lista de servicios que se pueden administrar.

2. Seleccione el servicio que desee asignar al usuario y haga clic en Seleccionar.

   Aparecerá una lista de usuarios asignados al servicio.

3. Haga clic en Solicitar acceso.

4. Busque un usuario al cual desee asignarle el servicio.

   Para mostrar una lista de todos los usuarios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

5. Seleccione un usuario y haga clic en Seleccionar.

   Aparecerá una lista actualizada de los usuarios asignados al servicio.

6. Haga clic en Guardar cambios.

   El usuario recibe el servicio especificado. El usuario recibe todas las aplicaciones, los roles, los grupos y los atributos incluidos en el servicio.

Confirmación de la asignación de un servicio

Una vez que ha asignado un servicio a un usuario, confirme que todas las tareas asociadas con el servicio se han completado correctamente.

Siga estos pasos:

1. Vaya a Servicios, Ver historial de solicitud de acceso al servicio

   Aparece una pantalla de búsqueda.

2. Busque el servicio que se ha asignado a un usuario.

   Para mostrar una lista de todos los servicios para los cuales dispone de privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

   Aparece una lista de servicios que se pueden administrar.

3. Seleccione el servicio que se ha asignado y haga clic en Seleccionar.

   Aparecerá un historial de acciones asociado con el servicio.

4. Haga clic en Cambiado por última vez para ver primero las acciones más recientes.
5. Confirme que el usuario en cuestión ha recibido el servicio correctamente.
6. Haga clic en Cerrar.

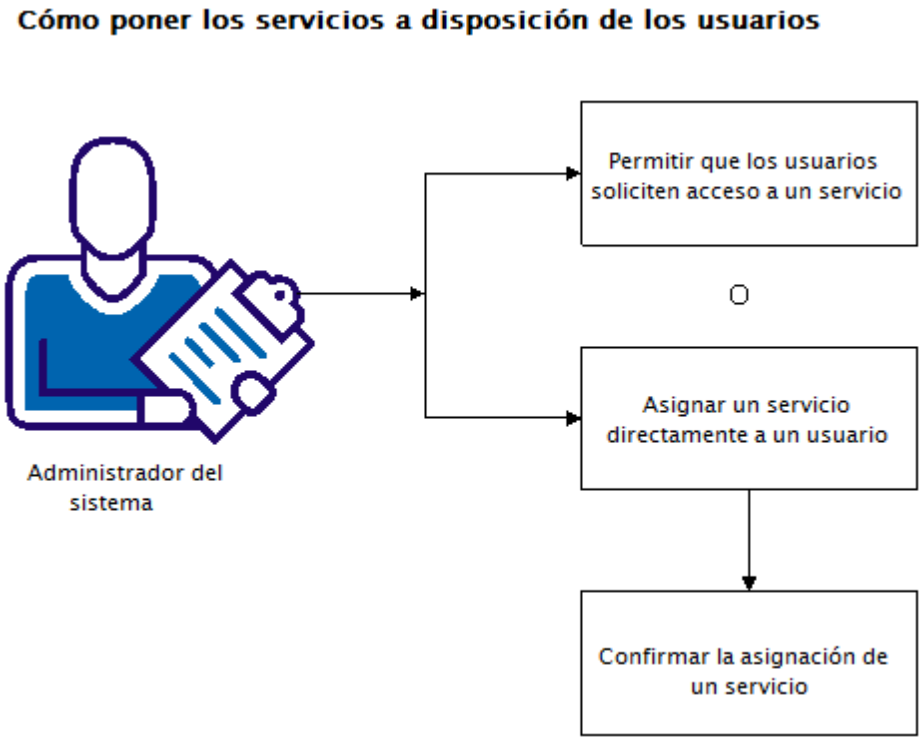
Cómo poner los servicios a disposición de los usuarios

Los servicios simplifican la gestión de las autorizaciones Un servicio agrupa todas las autorizaciones que necesita un usuario para un rol de negocio determinado. El usuario tendrá los servicios a disposición mediante las tareas de solicitud de acceso en la Consola de usuario. Las tareas de solicitud de acceso permiten que un usuario o administrador soliciten, asignen, revoquen y reanuden un servicio mediante la interfaz de usuario.

Los servicios permiten a un administrador del sistema combinar actividades de usuario e información - tareas, roles, grupos y atributos - en un solo paquete, que se gestionan como un conjunto. Por ejemplo, todos los empleados nuevos del departamento de ventas requieren acceso a un conjunto definido de tareas, cuentas en sistemas de punto final específicos e información agregada a los perfiles de cuentas de usuarios. Un administrador del sistema 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 las solicitudes de usuario acceden a un servicio, la solicitud se completa automáticamente. Las tareas asociadas, los roles, los grupos y los atributos se asignan al usuario inmediatamente. Un administrador de CA CloudMinder con los privilegios adecuados puede configurar también el cumplimiento del servicio para que requiera una aprobación del flujo de trabajo, o para generar notificaciones de correo electrónico.

El diagrama siguiente muestra la información y los pasos que hay que realizar para poner los servicios a disposición de los usuarios.



Se pueden poner los servicios a disposición de los usuarios mediante los métodos siguientes:

1. Permitir que los usuarios soliciten acceso ellos mismos.

   En la Consola de usuario de CA CloudMinder, cuando el usuario hace clic en Mi acceso y, a continuación, en Solicitar y ver acceso, el usuario tendrá a su disposición una lista de servicios para la solicitud. Los servicios que aparecen en esta lista son los que ha marcado un administrador de CA CloudMinder como Autosuscripción con los privilegios adecuados, normalmente durante la creación de un servicio.

   Cuando el usuario solicita acceso, el sistema asigna el servicio al usuario. El usuario recibe todas las aplicaciones, los roles, los grupos y los atributos asociados con el servicio. Si el servicio incluye un rol de inicio para una aplicación, aparece un icono y un vínculo a la aplicación en la página principal de la Consola de usuario.

2. Asignación de un servicio directamente a un usuario (en la página 87).
3. Si se asigna un servicio directamente a un usuario, es necesaria la Confirmación de la asignación de un servicio (en la página 243).

Asignación de un servicio a un usuario

Se puede asignar un servicio directamente a un usuario individual. Este usuario se convierte en *miembro* del servicio.

Siga estos pasos:

1. Vaya a Servicios, Solicitar y ver acceso.

   Aparece una lista de servicios que se pueden administrar.

2. Seleccione el servicio que desee asignar al usuario y haga clic en Seleccionar.

   Aparecerá una lista de usuarios asignados al servicio.

3. Haga clic en Solicitar acceso.

4. Busque un usuario al cual desee asignarle el servicio.

   Para mostrar una lista de todos los usuarios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

5. Seleccione un usuario y haga clic en Seleccionar.

   Aparecerá una lista actualizada de los usuarios asignados al servicio.

6. Haga clic en Guardar cambios.

   El usuario recibe el servicio especificado. El usuario recibe todas las aplicaciones, los roles, los grupos y los atributos incluidos en el servicio.

Confirmación de la asignación de un servicio

Una vez que ha asignado un servicio a un usuario, confirme que todas las tareas asociadas con el servicio se han completado correctamente.

Siga estos pasos:

1. Vaya a Servicios, Ver historial de solicitud de acceso al servicio

   Aparece una pantalla de búsqueda.

2. Busque el servicio que se ha asignado a un usuario.

   Para mostrar una lista de todos los servicios para los cuales dispone de privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

   Aparece una lista de servicios que se pueden administrar.

3. Seleccione el servicio que se ha asignado y haga clic en Seleccionar.

   Aparecerá un historial de acciones asociado con el servicio.

4. Haga clic en Cambiado por última vez para ver primero las acciones más recientes.
5. Confirme que el usuario en cuestión ha recibido el servicio correctamente.
6. Haga clic en Cerrar.

Modificación de un servicio

Como administrador del sistema, se puede modificar un servicio creado previamente. Por ejemplo, se pueden cambiar las autorizaciones que el servicio concede a los miembros del servicio agregando un rol al servicio. Se pueden ajustar también las reglas del administrador y de propietarios para el servicio, requisitos previos del servicio y otros detalles administrativos.

Si CA CloudMinder ha completado un servicio para un usuario determinado, cualquier cambio realizado en el servicio no se propagará a ese usuario. Si decide modificar un servicio, los usuarios que recibieron el servicio antes de que lo cambiara tienen las autorizaciones originales. Los usuarios que reciben el servicio después de que lo cambie tienen las autorizaciones que concede el servicio modificado. Por ejemplo, imagine la siguiente situación:

Como administrador del sistema, se crea un servicio de Director de ventas que concede el rol Director de ventas y el grupo de Ventas a miembros del servicio. Los usuarios solicitan que el servicio Director de ventas y CA CloudMinder completen el servicio concediendo el rol y el grupo adecuados a los usuarios. Se decide modificar el servicio Director de ventas para incluir el rol Gestor de empleados. Los miembros existentes del servicio no reciben el rol Gestor de empleados. Solamente los miembros nuevos del servicio Director de ventas reciben el rol Gestor de empleados, además del rol Director de ventas y el grupo de Ventas.

Por ello se debe tener en cuenta la modificación de un servicio solamente si el servicio no tiene ningún miembro. Es decir, se debe modificar un servicio solamente cuando ningún usuario ha solicitado y recibido el servicio, y ningún administrador ha asignado el servicio a un usuario.

Se puede modificar información administrativa, reglas del administrador y de propietarios, requisitos previos del servicio y autorizaciones - tareas, roles, grupos y atributos - para el servicio.

Siga estos pasos:

1. Inicie sesión en una cuenta de CA CloudMinder que tiene privilegios de gestión de servicios.

   Por ejemplo, el primer usuario de un entorno tiene el rol Gestor del sistema, el cual tiene la tarea Modificar servicio.

2. En el menú de navegación, seleccione Tareas, Servicios.
3. Haga clic en Gestionar servicios y después en Modificar servicio.

   Aparece una pantalla de búsqueda.
4. Busque el servicio que desea modificar.

   Para mostrar una lista de todos los servicios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.
5. Seleccione un servicio y haga clic en Seleccionar.

   Aparecerá un mensaje de confirmación.
6. Haga clic en Sí.
7. Haga clic en Enviar.

   CA CloudMinder aplica sus cambios en el servicio.

Adición de una búsqueda a Solicitar y ver acceso

La tarea Solicitar y ver acceso muestra una lista de servicios; sin embargo, no existe ningún campo para buscar más servicios. Para agregar un campo de búsqueda:

1. Seleccione Funciones y tareas, Tareas de administración, Modificar tarea de administración.
2. Busque Solicitar y ver acceso.
3. Seleccione la tarea en la categoría Servicio.
4. Haga clic en Fichas.
5. Debajo de la ficha, haga clic en el icono de edición situado a la izquierda de Gestionar acceso.
6. Haga clic en Examinar en la línea Pantalla de lista.
7. Configure la opción que se aplica para agregar la búsqueda correcta.
8. Seleccione la pantalla necesaria y haga clic en el botón Editar para editar la pantalla.
9. En Configuración de la pantalla Lista estándar, vaya a la sección "Seleccionar los campos en los que puede buscar el usuario:".
10. Seleccione los campos de búsqueda y configure los nombres de los campos de búsqueda.
11. Haga clic en Aceptar para guardar los cambios.

La información sobre la solicitud de servicio, como la Duración de la solicitud de servicio y Datos del usuario, aparece en el elemento del flujo de trabajo de aprobación de la solicitud de servicio. También, esta información se envía por correo electrónico si se asigna el flujo de trabajo basado en políticas AddServiceToUserEvent a la tarea Solicitar y ver acceso.

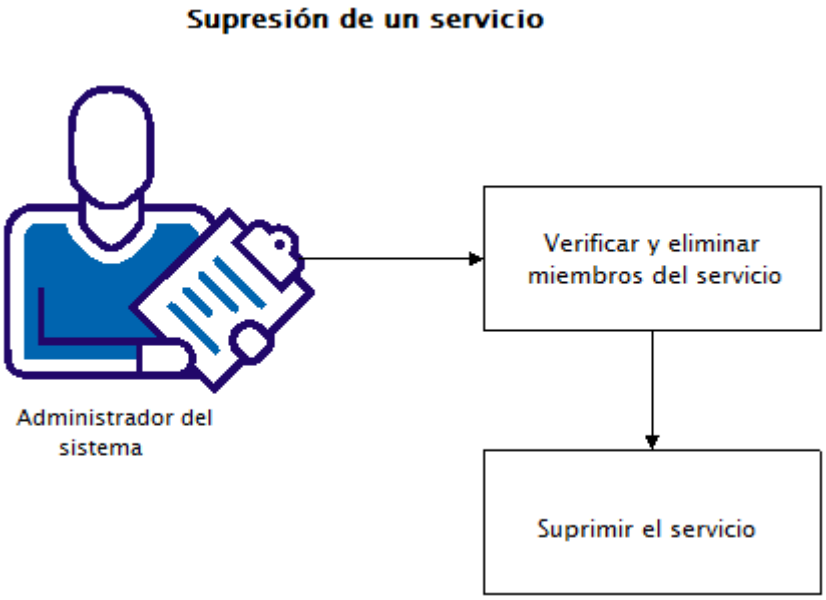
Supresión de un servicio

Como administrador del sistema, se puede suprimir un servicio. Un servicio suprimido se elimina totalmente del sistema.

Si se asignan usuarios a un servicio, no se puede suprimir el servicio. Antes de suprimir un servicio se deben comprobar primero y eliminar todos los usuarios asignados, o los *miembros*.

Nota: De la misma manera, si un usuario es miembro de un servicio, no se puede suprimir el usuario. Se debe eliminar primero el usuario como miembro del servicio y, a continuación, suprimir el usuario.

El diagrama siguiente muestra la información y los pasos que deben realizarse para suprimir un servicio.



Los temas siguientes explican cómo suprimir un servicio:

1. Verificación y eliminación de miembros del servicio (en la página 248)
2. Supresión del servicio (en la página 248)

Verificación y eliminación de miembros del servicio

Antes de suprimir un servicio se deben comprobar primero y eliminar los miembros existentes.

Siga estos pasos:

1. Inicie sesión en una cuenta de CA CloudMinder que tiene privilegios de gestión de servicios.

   Por ejemplo, el primer usuario de un entorno tiene el rol Gestor del sistema, el cual tiene la tarea Modificar servicio.

2. Seleccione Tareas, Servicios, Solicitar y ver acceso.

   Aparece una lista de servicios que se pueden administrar.

3. Seleccione el servicio que desee suprimir y haga clic en Seleccionar.

   Aparecerá una lista de usuarios asignados al servicio.

4. Si el servicio tiene miembros, desactive las casillas de verificación situadas junto a los usuarios.

5. Haga clic en Guardar cambios.

   Aparecerá un mensaje de confirmación.

6. Haga clic en Sí.

   CA CloudMinder elimina los miembros del servicio.

Supresión de un servicio

Se puede suprimir un servicio que no tiene ningún miembro del servicio.

Para suprimir un servicio

1. Inicie sesión en CA CloudMinder con una cuenta que dispone de privilegios de gestión de servicios.

   Por ejemplo, el primer usuario de un entorno tiene el rol Gestor del sistema, el cual tiene la tarea Suprimir servicio.

2. Vaya a Servicios situado en el panel izquierdo o seleccionando Tareas.

3. Haga clic en Gestionar servicios, Suprimir servicio.

   Aparece una pantalla de búsqueda.

4. Busque el servicio que desee suprimir.

   Para mostrar una lista de todos los servicios para los cuales tiene privilegios administrativos, haga clic en Buscar sin modificar los criterios de búsqueda.

5. Seleccione un servicio y haga clic en Seleccionar.

   Aparecerá un mensaje de confirmación.

6. Haga clic en Sí.

   El servicio se ha suprimido.

Renovación del acceso a un servicio

Algunos servicios caducan después de un cierto período de tiempo. Los administradores pueden renovar un servicio para los usuarios para evitar una interrupción en su acceso.

Se puede renovar un servicio mediante uno de los métodos siguientes:

- Seleccionando el servicio y, a continuación, seleccionando el acceso del usuario para renovar
- Seleccionando el usuario y, a continuación, seleccionando el servicio para renovar

Nota: En función de cómo se configura un entorno, los usuarios finales pueden renovar también su acceso mediante la tarea Renovar acceso.

El procedimiento siguiente describe cómo renovar el acceso seleccionando primero el servicio. Si desea seleccionar primero el usuario, utilice la tarea Solicitudes de acceso del usuario, Gestionar solicitudes de renovación de usuarios en la categoría Usuarios.

Siga estos pasos:

1. Haga clic en Servicios, Renovar acceso en la Consola de usuario.
2. Busque y seleccione el servicio que desea renovar.

   La Consola de usuario muestra una lista de usuarios que tienen actualmente acceso al servicio seleccionado y caduca la fecha de su acceso.

3. Seleccione la duración de la renovación en la columna Solicitud de acceso y después haga clic en Aceptar.

   Las opciones en el campo Duración se determinan cuando se crea el servicio.

4. Haga clic en Guardar cambios.

Se puede consultar el estado de la renovación del servicio utilizando Ver búsqueda del historial de solicitud de acceso en la Consola de usuario.

Capítulo 11: Sincronización

Esta sección contiene los siguientes temas:

Sincronización de usuarios entre servidores

Configure la sincronización en Identity Manager para asegurarse de que los datos de los usuarios del directorio corporativo y directorio de aprovisionamiento coinciden. Para identificar cambios en cualquier directorio, configure la sincronización de entrada y salida.

Sincronización de entrada

La *sincronización de entrada* mantiene a los usuarios de CA Identity Manager actualizados con los cambios que se produzcan en el directorio de aprovisionamiento. En los cambios del directorio de aprovisionamiento se incluyen los que se realicen mediante sistemas con conectores al servidor de aprovisionamiento. La sincronización utiliza las asignaciones definidas en la pantalla Provisioning (Aprovisionamiento) de la Consola de gestión.

Conmutación por error para la sincronización de entrada

La conmutación por error en una dirección URL del servidor de Identity Manager se produce solamente si no se está ejecutando el servidor de aplicaciones que ha denominado una dirección URL. Si el servidor de aplicaciones está ejecutando y acepta la notificación pero, a continuación, se produce un error de configuración como entorno desconocido o entorno no iniciado, estos errores bloquearán la entrega de notificaciones. Estos problemas se deberán resolver antes de que las notificaciones de entrada funcionen correctamente.

Sincronización de salida

La sincronización de salida implica el uso de Identity Manager para crear y actualizar usuarios en el directorio de aprovisionamiento.

Creación de usuarios globales desde Identity Manager

La creación de usuarios en el directorio de aprovisionamiento solamente se produce para el aprovisionamiento de eventos relacionados, como la asignación de un rol de aprovisionamiento a un usuario. No se crea ningún usuario en el directorio de aprovisionamiento al utilizar una tarea de administración para crear usuarios a menos que esa tarea asigne un rol o incluya una política de identidad que asigne el rol.

Cuando la creación de usuarios en Identity Manager activa la creación de usuarios en el directorio de aprovisionamiento, Identity Manager envía un correo electrónico con una contraseña temporal a la dirección de correo electrónico del nuevo usuario, ya que se define en el directorio de aprovisionamiento. Los usuarios pueden iniciar sesión en la Consola de usuario con esa contraseña; sin embargo, luego tendrán que cambiarla. Como resultado, la contraseña se sincroniza entre el almacén de usuarios y directorio de aprovisionamiento.

Si el usuario no tiene ninguna dirección de correo electrónico, el usuario no podrá acceder a la Consola de usuario hasta que se cambie la contraseña en el almacén de usuarios, o bien que un administrador de CA Identity Manager cambie la contraseña del usuario en el gestor de aprovisionamiento.

Note: Para enviar por correo electrónico una contraseña temporal, deben activarse las notificaciones de correo electrónico y CreateProvisioningUserNotificationEvent debe configurarse para las notificaciones de correo electrónico. (Consulte la *Guía de configuración*).

Actualización de usuarios globales mediante Identity Manager

La actualización de usuarios en el directorio de aprovisionamiento se produce al utilizar una tarea de administración que modifica usuarios. Si no existe ningún usuario global, no se realizará la sincronización.

Las asignaciones de salida unen los eventos de usuario de Identity Manager con los eventos de salida que afectan al directorio de aprovisionamiento.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

Si un usuario existe en el directorio de aprovisionamiento pero no en Identity Manager, se puede crear dicho usuario en la Consola de usuario. Si se han asignado atributos para la tarea de creación y los usuarios tienen el mismo ID de usuario, los atributos para el aprovisionamiento de usuarios se actualizan en el directorio de aprovisionamiento. Ahora se puede gestionar ese usuario desde Identity Manager.

Nota: Si un evento actualiza atributos de usuario y se desea que los valores se sincronicen en CA Identity Manager, después se tendrán que asignar los eventos en el evento de salida: POST_MODIFY_GLOBAL_USER.

Supresión de usuarios globales mediante Identity Manager

De forma predeterminada, se configura la sincronización de salida para el evento Suprimir usuario. Cuando se suprime un usuario en Identity Manager, el usuario se suprime también en el directorio de aprovisionamiento y todas las cuentas de puntos finales.

Si CA Identity Manager no puede suprimir la cuenta de un usuario en un punto final gestionado, suprimirá el usuario del resto de las cuentas, pero no suprimirá el usuario del directorio de aprovisionamiento.

Por ejemplo, suponga que el usuario A tiene una cuenta de UNIX y una cuenta de Exchange, que se gestionan en el servidor de aprovisionamiento. Cuando el usuario A se suprime en Identity Manager, el servidor de aprovisionamiento intenta suprimir las cuentas del usuario. Si el servidor de aprovisionamiento no puede suprimir la cuenta de Exchange debido a un error de comunicación, suprimirá la cuenta de UNIX del usuario A, pero no suprimirá el usuario del directorio de aprovisionamiento. Sin embargo, el usuario A no se restaura en el almacén de usuarios.

Activación de la sincronización de contraseñas

El servidor de aprovisionamiento permite sincronizar contraseñas entre usuarios de Identity Manager y cuentas de usuario de puntos finales asociadas. Se requieren dos configuraciones para activar los cambios iniciados de puntos finales:

- Se deberán configurar puntos finales para capturar cambios iniciados de puntos finales y enviarlos al servidor de aprovisionamiento.

  Nota: Para obtener más información sobre cómo configurar puntos finales para la sincronización de contraseñas, consulte la *Guía de administración de CA Identity Manager*.

- El atributo de activación del agente de sincronización de contraseñas se debe activar para el usuario global.

Para activar la sincronización de contraseñas

1. En la Consola de gestión, seleccione Advanced Settings (Configuración avanzada), Provisioning (Aprovisionamiento).
2. Active Enable Password Changes from Endpoint Accounts (Activar cambios de contraseña de cuentas de puntos finales).
3. Haga clic en Save.
4. Reinicie el servidor de aplicaciones.

Sincronización de usuarios en tareas de creación o modificación de usuarios

En la ficha de perfil de una tarea que crea o modifica usuarios, los controles de sincronización garantizan que los cambios que se realicen en Identity Manager también se hagan en el usuario global. Si se crean tareas de administración que crean o modifican usuarios y tiene políticas de identidad, establezca los controles de sincronización de la siguiente forma:

- Establezca Sincronización de usuarios en Al completar la tarea.
- Establezca Sincronización de cuentas en Al completar la tarea.

Nota: Para obtener el máximo rendimiento, seleccione Al completar la tarea. No obstante, si selecciona la opción Al completar la tarea para una tarea que incluya varios eventos, Identity Manager no realizará la sincronización hasta que finalicen todos los eventos de la tarea. Si uno o más de esos eventos requieren aprobación de flujo de trabajo, puede demorarse varios días. Para evitar que Identity Manager espere a aplicar las políticas de identidad o sincronizar las cuentas hasta que se completen todos los eventos, seleccione la opción En cada evento.

Si se agregan atributos a tareas de administración que gestionan usuarios, se tendrán que actualizar las asignaciones de atributo en la pantalla Provisioning (Aprovisionamiento) de la Consola de gestión. Para cada atributo de usuario en Identity Manager, existe un atributo de aprovisionamiento predeterminado.

User Attribute	Provisioning Attribute
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%

Tareas de sincronización

Puede realizar los siguientes tipos de sincronización:

Sincronización de usuarios

Garantiza que cada usuario tenga las cuentas necesarias en los puntos finales gestionados adecuados y que cada cuenta se asigne a las plantillas de cuenta pertinentes, tal y como se describen en los roles de aprovisionamiento del usuario.

Sincronización de cuentas

Garantiza que los valores de atributo de capacidad de las cuentas sean los adecuados, tal y como se indica en las plantillas de cuenta asignadas de la cuenta. La sincronización de cuentas puede ser estricta o débil. La sincronización débil garantiza que los atributos de capacidad de cuentas tengan, como mínimo, la capacidad mínima que se requieren en sus plantillas de cuenta. La sincronización estricta garantiza que los atributos de capacidad de cuenta tengan la capacidad exacta que se requieren en sus plantillas de cuenta. La sincronización de cuentas es estricta si la cuenta pertenece a, como mínimo, una plantilla de cuenta cuya casilla de verificación Sincronización estricta esté activada.

Ninguna casilla de verificación Sincronización estricta correspondiente domina la sincronización de usuarios; sin embargo, existe un concepto similar. Cuando se emite el elemento de menú Sincronizar usuario con roles a usuarios, se muestran dos opciones de sincronización:

- Agregue cuentas que falten y asignaciones de plantillas de cuenta.
- Suprima cuentas adicionales y asignaciones de plantillas de cuenta.
- Al activar solamente la casilla de verificación Agregar, que es similar a la sincronización de cuentas débil, desea que los usuarios globales tengan, como mínimo, todas las cuentas que se requieren en los roles de aprovisionamiento asignados; sin embargo, permite que los usuarios tengan cuentas adicionales que no se indican en los roles de aprovisionamiento actuales.

Active las casillas de verificación Agregar y Suprimir, que son similares a la sincronización de cuentas estricta, para que los roles de aprovisionamiento definan exactamente qué cuentas deben tener los usuarios. Algunas cuentas adicionales se suprimen.

Seleccione la sincronización de cuentas estricta o débil, o bien la sincronización de usuarios estricta o débil según la precisión con la que se hayan definido los roles de aprovisionamiento. Si sus usuarios no se ajustan a los roles de aprovisionamiento claramente definidos en los que el acceso a la cuenta depende de estos roles, utilice la sincronización estricta.

Nota: Algunos tipos de puntos finales establecen la sincronización estricta como predeterminada. Para obtener más información, consulte *Connectors Guide*.

La sincronización de usuarios y la sincronización de cuentas son tareas independientes que se deben realizar de forma individual. Normalmente, primero se realiza la sincronización de usuarios para garantizar que todas las cuentas necesarias se creen; a continuación, se realiza la sincronización de cuentas con objeto de que el servidor de aprovisionamiento asigne o cambie los valores de los atributos de cuenta.

El servidor de aprovisionamiento proporciona dos conjuntos de opciones del menú de sincronización para objetos:

- Las opciones del menú de comprobación de la sincronización verifican la sincronización y devuelven una lista de cuentas que no cumplen con los roles de aprovisionamiento o las plantillas de cuenta.
- Las opciones del menú de sincronización sincronizan los usuarios globales con sus roles de aprovisionamiento, o bien las cuentas con sus plantillas de cuenta.

Si se ejecutan primero las funciones de comprobación de la sincronización, el servidor de aprovisionamiento indicará qué correcciones llevarán a cabo estas. Si las funciones de comprobación de la sincronización no encuentran ningún problema, estas no se ejecutarán.

Por qué los usuarios se desincronizan

A continuación, se muestran los motivos por los que los usuarios se desincronizan con sus roles de aprovisionamiento o las plantillas de cuenta:

- Los intentos anteriores de crear las cuentas necesarias han producido un error debido a problemas de hardware o software en la red, lo que provoca que falten cuentas.
- Los roles de aprovisionamiento y las plantillas de cuenta pueden haberse modificado, lo que provoca que se creen cuentas adicionales o que falten.
- Las cuentas se han asignado a plantillas de cuenta después de que se crearan, de manera que las cuentas existen pero no están sincronizadas con sus plantillas de cuenta.
- La creación de una nueva cuenta se retrasa porque se ha especificado que la cuenta se creará más tarde.
- Se ha adquirido un nuevo punto final. Durante la exploración y correlación, el servidor de aprovisionamiento no asigna roles de aprovisionamiento a los usuarios automáticamente, por lo que se debe actualizar el rol para indicar qué usuarios deben tener cuentas en el nuevo punto final. Cualquier cuenta que se haya correlacionado con un usuario se clasifica como cuenta adicional cuando se sincroniza el usuario.
- Se ha asignado una cuenta existente a un usuario copiando la cuenta en el usuario, lo que realiza una correlación manual y crea una cuenta adicional.
- Se ha creado una cuenta para un usuario en lugar de asignar el usuario a un rol. Por ejemplo, si se copia un usuario en una plantilla de cuenta que no está en ninguno de los roles de aprovisionamiento del usuario, la cuenta se muestra como cuenta adicional o como cuenta con una plantilla de cuenta adicional. Si se copia el usuario en un punto final para crear una cuenta mediante la plantilla de cuenta predeterminada del punto final, esa cuenta podría ser una cuenta adicional.

Sincronización de usuarios

Con la sincronización de usuarios se crean, actualizan o suprimen cuentas para que cumplan con los roles de aprovisionamiento asignados a un usuario. Por tanto, si los administradores agregan o suprimen cuentas en puntos finales gestionados mediante herramientas nativas y no han vuelto a realizar una exploración reciente del punto final para actualizar el directorio de aprovisionamiento, es posible que en la sincronización de usuarios no se avisen de problemas cuando un usuario pueda tener cuentas adicionales o que falten.

Usuario con roles de sincronización

Se puede comprobar la sincronización de usuarios para mostrar las cuentas adicionales o las plantillas de cuenta y cuentas que faltan. Cuando se solicita sincronizar usuarios con roles, el servidor de aprovisionamiento garantiza que el usuario tenga todas las cuentas que se requieren en los roles de aprovisionamiento de la persona; además, garantiza que cada cuenta pertenezca a las plantillas de cuenta correctas.

- Con esta tarea se puede activar una casilla de verificación para crear la cuenta en el punto final. Si hay más de una plantilla de cuenta en los roles de aprovisionamiento del usuario que indique la misma cuenta, la cuenta se creará combinando todas las plantillas de cuenta relevantes.
- Durante la sincronización de usuarios con roles, se podrán suprimir las cuentas adicionales. Puede determinar si los usuarios tienen motivos para tener cuentas distintas de las que se requieren en los roles de aprovisionamiento. Si ese es el caso, no se debe seleccionar esta opción de supresión.

  Si una cuenta que se suprime se encuentra en un punto final gestionado para el que se han desactivado supresiones de cuentas, la cuenta no se suprimirá.

Creación de cuentas

Dado que los roles de aprovisionamiento contienen plantillas de cuenta y estas se asocian a puntos finales, los usuarios deben tener cuentas en cada punto final con los atributos de cuenta correctos.

Con esta tarea se puede activar una casilla de verificación para crear la cuenta en el punto final. Si hay más de una plantilla de cuenta en los roles de aprovisionamiento del usuario que indique la misma cuenta, la cuenta se creará combinando todas las plantillas de cuenta relevantes.

Esta cuenta se asigna a las plantillas de cuenta que no están actualmente sincronizadas con la cuenta. La sincronización de cuentas no es necesaria en las nuevas cuentas creadas.

Supresión de cuentas

Durante la sincronización de usuarios con roles, se podrán suprimir las cuentas adicionales. Puede determinar si los usuarios tienen motivos para tener cuentas distintas de las que se requieren en los roles de aprovisionamiento. Si ese es el caso, no se debe seleccionar esta opción de supresión.

Si una cuenta que se suprime se encuentra en un punto final gestionado para el que se han desactivado supresiones de cuentas, la cuenta no se suprimirá.

Adición de plantillas de cuenta a cuentas

Si falta una cuenta en una o varias asignaciones de plantillas de cuenta, los usuarios con la sincronización de plantillas de cuenta asignarán una cuenta existente a dichas plantillas de cuenta. Cuando una cuenta se asigna a una o varias plantillas de cuenta nuevas, se ejecuta automáticamente la sincronización de cuentas con el fin de actualizar los atributos de capacidad de la cuenta en las capacidades que se especifican en las plantillas de cuenta.

Después de actualizar las cuentas de usuario con la sincronización de plantillas de cuenta, puede que la cuenta no esté sincronizada con las plantillas de cuenta. Si una de las plantillas de cuenta agregadas era una plantilla de cuenta de sincronización estricta, o bien si se agregan dos o varias plantillas de cuenta a una cuenta, los usuarios con la sincronización de roles iniciarán una sincronización de cuentas completa en la cuenta. Sin embargo, si solamente se agrega una plantilla de cuenta de sincronización débil, la sincronización de usuarios con la sincronización de plantillas de cuenta iniciará una sincronización de cuentas que afectará solamente a esta plantilla de cuenta. Si la cuenta no estaba al principio sincronizada con otras plantillas de cuenta antes de esta actualización, es posible que no estuviera tampoco sincronizada después.

Eliminación de plantillas de cuenta de cuentas

También se puede utilizar la sincronización de usuarios con roles para eliminar las plantillas de cuenta adicionales de una cuenta. Esta acción solamente se realizará si se selecciona la opción de supresión. Cuando la sincronización de usuarios determina que se debe actualizar una cuenta para eliminar una o varias plantillas de cuenta adicionales, se ejecuta automáticamente la sincronización de cuentas en la cuenta con el fin de sincronizar sus atributos de capacidad con las plantillas de cuenta restantes de la cuenta.

Esta sincronización de cuentas, que se ejecuta al eliminar plantillas de cuenta de una cuenta, utilizará la sincronización estricta si alguna de las plantillas de cuenta restantes se marcan para sincronización estricta, así como para sincronización débil si todas las plantillas de cuenta restantes se marcan para sincronización débil.

Si la sincronización débil o estricta que se utiliza repercute en si las capacidades de la cuenta, que se concedieron cuando se asignó una plantilla de cuenta a una cuenta, se eliminarán cuando se suprima más adelante esa plantilla de cuenta. Con la sincronización estricta, las capacidades que se concedan mediante plantillas de cuenta (como pertenencia a grupos o cuotas más altas) se eliminarán (pertenencia a grupos eliminada o cuotas más bajas) si ninguna de las plantillas de cuenta restantes de la cuenta indican esa capacidad. Sin embargo, con la sincronización débil, normalmente no se realizan cambios en la cuenta debido a que el servidor de aprovisionamiento no distingue entre capacidades adicionales a petición y capacidades que se conceden a través de plantillas de cuenta.

La excepción a esta regla es con determinados atributos de capacidad con varios valores que se designan como atributos de SyncRemoveValues. Un atributo con varios valores simples, que representa una recolección de valores asignados a la cuenta (es decir, una lista de pertenencias a grupos), normalmente se mostrará como atributo de SyncRemoveValues. Para estos atributos, la acción de sincronización débil, que se ejecuta a la vez que se elimina una plantilla de cuenta de una cuenta, eliminará los valores que se indican en la plantilla de cuenta que se va a eliminar; siempre y cuando ese valor no se indique en una de las plantillas de cuenta restantes.

Por ejemplo, si se crean plantillas de cuenta donde cada una de ellas asigne una pertenencia a grupos única a su cuenta, el objetivo de esta función de SyncRemoveValues es que, cuando se cambien los roles de aprovisionamiento de un usuario global para no volver a solicitar una plantilla de cuenta concreta, la cuenta se actualizará para que no vuelva a pertenecer al grupo que se indica en la plantilla de cuenta. Se debe tener cuenta que no es exactamente igual a la sincronización estricta, ya que se conservan las pertenencias a grupos que se proporcionan en cuentas que no son las que se indican en las plantillas de cuenta.

Para todos los atributos con un único valor y determinados valores con diversos valores que no se han asignado como atributos de SyncRemoveValues, la acción de sincronización débil a la vez que la de supresión de una plantilla de cuenta de una cuenta será la misma que una de sincronización débil; nunca se eliminarán las capacidades.

Si se desea que la sincronización débil no elimine nunca las capacidades, desactive la función de SyncRemoveValues estableciendo los valores de plantillas de cuenta de sincronización/eliminación de parámetros de configuración de dominios de Cuentas a No.

Sincronización de plantillas de cuenta

Los cambios realizados en las plantillas de cuenta afectan a las cuentas existentes como se muestra a continuación:

- Si cambia el valor de un atributo de capacidad, se actualizará el atributo de cuenta correspondiente (si procede) para que esté sincronizado con el valor de atributo de la plantilla de cuenta. Consulte la descripción de la sincronización débil y estricta.
- El conector designa algunos atributos de cuenta como no actualizados por los cambios de la plantilla de cuenta. Los ejemplos son ciertos atributos que el tipo de punto final solamente permite establecer durante la creación de cuenta y el atributo Contraseña.

Atributos actualizados

Al cambiar los atributos de capacidad de una plantilla de cuenta, el atributo correspondiente en las cuentas cambiará. Este cambio tiene un impacto en los atributos de la cuenta. El impacto se basa en los factores siguientes:

- Si la plantilla de cuenta se ha definido para usar la sincronización débil o fuerte.
- Si la cuenta pertenece a varias plantillas de cuenta.

Sincronización débil

La *sincronización débil* garantiza que los usuarios tengan los atributos de capacidad mínimos para sus cuentas. La sincronización débil es el valor predeterminado en la mayoría de los tipos de puntos finales. Si se actualiza una plantilla que utiliza la sincronización débil, CA Identity Manager actualiza los atributos de capacidad como se muestra a continuación:

- Si se actualiza un campo de número en una plantilla de cuenta, y el nuevo número es mayor que el número de la cuenta, CA Identity Manager cambiará el valor de la cuenta para que coincida con el nuevo número.
- Si no se seleccionó una casilla de verificación en una plantilla de cuenta y, posteriormente, la selecciona, CA Identity Manager actualizará la casilla de verificación en cualquier cuenta en la que la casilla de verificación no esté seleccionada.
- Si se modifica una lista en una plantilla de cuenta, CA Identity Manager actualizará todas las cuentas para incluir los valores de la nueva lista que no estuvieran incluidos en la lista de valores de la cuenta.

Si una cuenta pertenece a otras plantillas de cuenta (tanto si estas plantillas utilizan sincronización débil como estricta), CA Identity Manager sólo consultará la plantilla que se esté modificando. Esta acción es más eficaz que comprobar cada plantilla de cuenta. Dado que la sincronización débil sólo agrega capacidades a las cuentas, generalmente no es necesario consultar otras plantillas de cuenta.

Nota: Cuando se propagan desde una plantilla de cuenta de sincronización débil, los cambios que eliminarían o reducirían las capacidades, podrían dejar algunas cuentas no sincronizadas. Recuerde que con la sincronización débil, las capacidades no se eliminan ni se reducen nunca. Sin consultar otras plantillas de una cuenta, la propagación no tiene en cuenta si es suficiente la sincronización débil.

En esta situación, utilice Sincronizar usuario con plantillas de cuenta para sincronizar la cuenta con sus plantillas de cuenta.

Sincronización estricta

La sincronización estricta garantiza que las cuentas tengan los atributos de cuenta exactos que se especifican en la plantilla de cuenta.

Por ejemplo, supongamos que se agrega un grupo a una plantilla de cuenta de UNIX existente. Originalmente, la plantilla de cuenta hacía miembros de cuentas del grupo Personal. Ahora se desean hacer miembros de cuentas tanto a los grupos de personal como al del sistema. Todas las cuentas asociadas a la plantilla de cuenta se consideran que están sincronizadas cuando cada cuenta es miembro de los grupos de sistema y personal (y de ningún otro grupo). Cualquier cuenta que no esté en el grupo de personal se agregará a ambos grupos.

Otros factores que se deben tener en cuenta:

- Si la plantilla de cuenta utiliza la sincronización estricta, cualquier cuenta que pertenezca a grupos distintos de Personal y Sistema, se eliminará de esos grupos extra.
- Si la plantilla de cuenta utiliza la sincronización débil, las cuentas se agregan a los grupos Personal y Sistema. Cualquier cuenta que tenga definidos grupos adicionales, seguirá siendo un miembro de esos grupos.

Nota: Sincronice las cuentas con sus plantillas periódicamente para garantizar que estén sincronizadas con sus plantillas de cuenta.

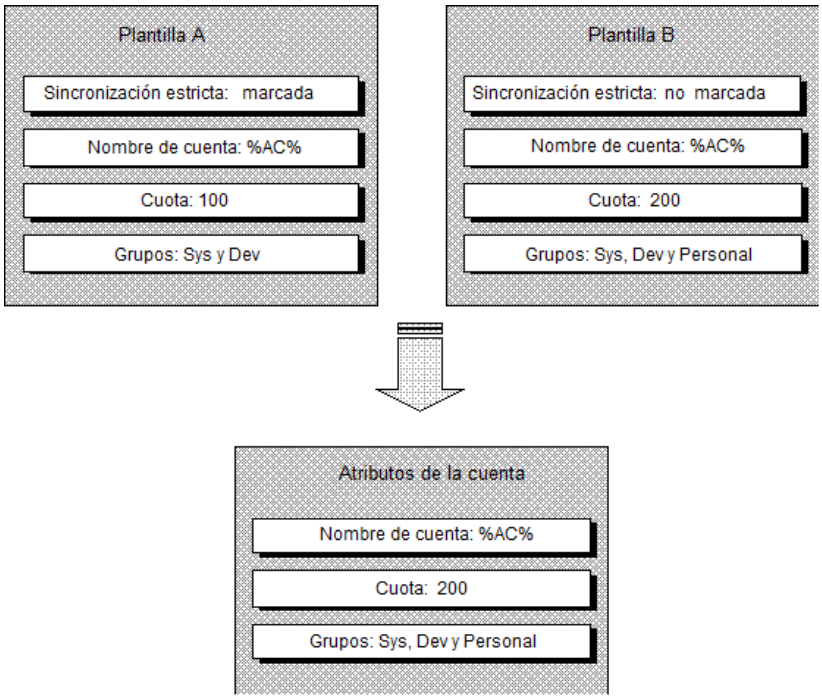
Cuentas con varias plantillas

La sincronización también depende de si la cuenta pertenece a más de una plantilla de cuenta. Si una cuenta tiene solamente una plantilla de cuenta y esa plantilla utiliza la sincronización estricta, cada atributo se actualiza para coincidir exactamente con lo que el valor del atributo de plantilla de cuenta evalúa. El resultado es el mismo que si el atributo fuera un atributo inicial.

Una cuenta puede pertenecer a varias plantillas de cuenta, como sería el caso si un usuario perteneciera a varios roles de aprovisionamiento, cada uno de los cuales indicando algún nivel de acceso en el mismo punto final gestionado. Cuando esto sucede, CA Identity Manager combina esas plantillas de cuenta en una plantilla de cuenta efectiva que indica el superconjunto de las capacidades de las plantillas de cuenta individuales. Se considera que esta plantilla de cuenta que utiliza la sincronización débil si todas sus plantillas de cuenta individuales son de sincronización débil o estricta o si alguna de las plantillas de cuenta individuales es estricta.

Nota: A menudo se utiliza solo la sincronización débil o solo la sincronización estricta para las plantillas de cuenta que controlan una cuenta, en función de si los roles de la compañía definen completamente los accesos que necesitan sus usuarios. Si sus usuarios no se ajustan en roles claros y se necesita la flexibilidad para conceder capacidades adicionales a las cuentas de sus usuarios, utilice la sincronización débil. Si se pueden definir roles para especificar exactamente los accesos que necesitan sus usuarios, utilice la sincronización estricta.

El ejemplo siguiente demuestra cómo se combinan varias plantillas de cuenta en una sola plantilla de cuenta efectiva. En este ejemplo, una plantilla de cuenta se marca para la sincronización débil y otra para la sincronización estricta. Por lo tanto, la plantilla de cuenta efectiva creada combinando las dos plantillas de cuenta se trata como una plantilla de cuenta de sincronización estricta. El atributo de cuota de entero adopta el valor mayor de las dos plantillas de cuenta y el atributo de grupos de varios valores adopta la unión de valores de las dos políticas.



Atributos exclusivos para nuevas cuentas

En una plantilla de cuenta, algunos atributos sólo se aplican cuando se crea la cuenta. Por ejemplo, el atributo de contraseña es una expresión de regla que define la contraseña para las nuevas cuentas. Esta expresión de regla nunca actualiza la contraseña de una cuenta. Los cambios de la expresión de regla de contraseña sólo repercuten en las cuentas que se crean después de que se haya configurado la expresión de regla.

De igual manera, una expresión de regla de plantilla para un atributo de cuenta de sólo lectura sólo repercute en las cuentas que se crean después de que se haya configurado la expresión de regla. El cambio no repercute en las cuentas existentes.

Sincronización de cuentas

La sincronización de cuentas actualiza los atributos de capacidad para garantizar que la cuenta tenga las capacidades que se especifican en las plantillas de cuenta. Esta sincronización no afecta a los atributos iniciales de la cuenta.

Para sincronizar cambios de atributos de capacidad en una plantilla de cuenta con sus cuentas, utilice una de las opciones del menú de sincronización que se explican en esta sección.

Comprobación de la sincronización de cuentas

Se puede comprobar la sincronización de cuentas para puntos finales y usuarios. Esta acción devuelve una lista de cuentas que no cumplen con las plantillas de cuenta. En la siguiente tabla se describe lo que sucede cuando se comprueba la sincronización de cuentas en cada objeto:

Objeto	Sincroniza
Punto final	Los atributos de cuenta para cada cuenta de un punto final. Se garantiza el cumplimiento con las plantillas de cuenta asociadas.
Usuario global	Atributos de cuenta para cada una de las cuentas de un usuario. Se garantiza el cumplimiento con las plantillas de cuenta asociadas.

Sincronización de cuentas

Se puede realizar la sincronización de cuentas en puntos finales, usuarios y plantillas de cuenta. En la tabla siguiente se muestra cómo repercute cada sincronización de cuentas en los objetos:

Objeto	Sincroniza
Punto final	Cada cuenta de un punto final con sus plantillas de cuenta asociadas.
Usuario global	Cada cuenta de un usuario global con cada plantilla de cuenta asociada.

Capítulo 12: Flujo de trabajo (workflow)

Esta sección contiene los siguientes temas:

Descripción general de flujo de trabajo

La función de flujo de trabajo de CA Identity Manager permite que una tarea de CA Identity Manager sea controlada por un proceso de flujo de trabajo. Un *proceso de flujo de trabajo* consiste en uno o más pasos que se deben realizar antes de que CA Identity Manager pueda finalizar una tarea que se encuentra bajo el control del flujo de trabajo. Una *tarea* es una instancia del tiempo de ejecución de un proceso del flujo de trabajo.

Diseñador de Workpoint es software de Workpoint LLC, una filial de Planet Group, Inc., que está integrado en CA Identity Manager. Diseñador de Workpoint le permite gestionar los procesos del flujo de trabajo y las tareas del flujo de trabajo.

Un proceso de flujo de trabajo consiste en uno o más pasos, denominados *actividades*, que se deben realizar para llevar a cabo una tarea del negocio, como por ejemplo crear o modificar la cuenta de usuario de un empleado. Normalmente, un proceso de flujo de trabajo incluye una o más actividades manuales que necesitan que un usuario autorizado, o participante, apruebe o rechace la tarea.

Un *participante* es una persona autorizada para realizar una actividad de flujo de trabajo. En CA Identity Manager, los participantes también se denominan *aprobadores*, ya que deben aprobar o rechazar la tarea bajo el control del flujo de trabajo. Un *resolvedor de participantes* es una función o un conjunto de criterios para determinar quiénes son los participantes.

Las actividades manuales individuales de un flujo de trabajo se denominan *elementos de trabajo* en CA Identity Manager.

Una *lista de trabajo* es una lista generada por el flujo de trabajo de tareas aprobadas, o *elementos de trabajo*, que aparecen en la Consola de usuario del participante autorizado para aprobar la tarea.

Diagrama de proceso de Workpoint

En general, las tareas de CA Identity Manager activan eventos de CA Identity Manager. Por ejemplo, para crear un usuario, un administrador selecciona la tarea Crear usuario. Cuando se inicia esta tarea, se activa el evento CreateUserEvent.

El siguiente diagrama es un ejemplo de un proceso de flujo de trabajo sencillo (el proceso predefinido CreateUserApproveProcess) tal y como aparece en el Diseñador de Workpoint. Este proceso se invoca mediante CreateUserEvent si la tarea Crear usuario se encuentra bajo el control del flujo de trabajo.

El proceso incluye una actividad manual, Aprobar Crear usuario, que se corresponde con una tarea de aprobación del flujo de trabajo de CA Identity Manager del mismo nombre. El participante debe aprobar o rechazar la tarea de aprobación, normalmente haciendo clic sobre un botón en la Consola de usuario, antes de que la tarea bajo el control del flujo de trabajo pueda ejecutarse hasta completarse.

Flujo de trabajo y notificación por correo electrónico

Al iniciar una tarea, CA Identity Manager envía la tarea para procesarla y muestra un mensaje de confirmación similar a este:

```
Confirmación: tarea completada.
```

Sin embargo, si la tarea está bajo el control del flujo de trabajo y necesita aprobación, el mensaje será similar al siguiente:

```
Alerta: tarea pendiente.
```

Además de los mensajes en pantalla, CA Identity Manager puede generar automáticamente notificaciones de correo electrónico cuando:

- Un evento o tarea que necesita aprobación o rechazo de un aprobador del flujo de trabajo está pendiente.
- Un aprobador aprueba un evento o tarea.
- Un aprobador rechaza un evento o tarea.
- Finaliza un evento o tarea.

Más información:

Notificaciones de correo electrónico (en la página 369)

Documentación de Workpoint

Para obtener información general sobre los conceptos del flujo de trabajo e instrucciones sobre los procesos, actividades y tareas del flujo de trabajo en el Diseñador de Workpoint, consulte la documentación de Workpoint. Para ello, abra la siguiente página HTML:

admin_tools\WorkPoint\docs\designer\default.htm

admin_tools

Define el directorio de instalación de las herramientas administrativas de CA Identity Manager. El directorio de instalación predeterminado es el siguiente:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Nota: Workpoint es un producto de terceros instalado con CA Identity Manager. CA Identity Manager es compatible con un subconjunto de funciones de WorkPoint. Por ejemplo, CA Identity Manager no es compatible con la WpConsole. Sin embargo, la documentación de WorkPoint describe todas las funciones del producto. Partes de la documentación de Workpoint no se aplican a los usuarios de CA Identity Manager.

Métodos de control del flujo de trabajo

CA Identity Manager proporciona dos métodos para establecer tareas bajo el control del flujo de trabajo:

Método con plantilla

CA Identity Manager incluye plantillas de proceso del flujo de trabajo que se pueden utilizar para establecer las tareas bajo el control del flujo de trabajo. El *método con plantilla* permite utilizar estas plantillas para configurar y gestionar completamente el flujo de trabajo desde la Consola de usuario. Estas plantillas de proceso genéricas, introducidas en CA Identity Manager r12, se pueden configurar para controlar la mayoría de las tareas y los eventos de CA Identity Manager.

El método con plantilla activa nuevas funciones, como por ejemplo:

- El control del flujo de trabajo tanto a nivel de tarea como a nivel de evento.
- Configuración simplificada del resolvedor de participantes para aprobadores del flujo de trabajo.
- Delegación de elementos de trabajo, que incluye escenarios "fuera de la oficina" en los que se permite que un usuario delegue en otro la aprobación de elementos de trabajo.
- Reasignación de elementos de trabajo, que permite reasignar una tarea en ejecución a otro usuario para aprobarla.

Método de Workpoint

CA Identity Manager también incluye un conjunto de procesos de flujo de trabajo predefinidos con asignaciones de eventos predeterminadas que corresponden a tareas específicas de CA Identity Manager. El *método de Workpoint* necesita que estos procesos se configuren y se personalicen desde el Diseñador de Workpoint. Estos procesos predefinidos son compatibles con versiones anteriores a CA Identity Manager r12.

El método de Workpoint también activa nuevas funciones, como por ejemplo:

- El control del flujo de trabajo tanto a nivel de tarea como a nivel de evento.
- Delegación de elementos de trabajo, que incluye escenarios "fuera de la oficina" en los que se permite que un usuario delegue en otro la aprobación de elementos de trabajo.
- Reasignación de elementos de trabajo, que permite reasignar una tarea en ejecución a otro usuario para aprobarla.

Nota: Para mayor flexibilidad y facilidad de uso, CA recomienda que use el método con plantilla siempre que sea posible.

Más información:

Uso del control del flujo de trabajo: método con plantilla (en la página 270)

Uso del control del flujo de trabajo: método con plantilla

Presente a partir de CA Identity Manager r12, el método con plantilla permite configurar plantillas de proceso de flujo de trabajo en la Consola de usuario, sin que sea necesario abrir el Diseñador de Workpoint.

Las ventajas del método con plantilla son:

- Las plantillas de proceso de varias etapas pueden aplicarse a la mayoría de necesidades del flujo de trabajo sin que sea necesario personalizarlas en Diseñador de Workpoint.
- Las plantillas admiten el control del flujo de trabajo tanto a nivel de tarea como a nivel de evento.
- La misma plantilla de proceso del flujo de trabajo se puede configurar para utilizarse con muchas tareas diferentes mientras que el propio diseño del proceso se mantiene inalterado.
- Los resolvedores de participantes se pueden especificar fácilmente en la consola de usuario.
- La delegación de elementos de trabajo se puede realizar en la Consola de usuario.

Requisito previo: Activar flujo de trabajo

Debe tener activado el flujo de trabajo antes de poder utilizarlo para controlar las tareas de CA Identity Manager. El flujo de trabajo se encuentra desactivado de forma predeterminada.

Siga estos pasos:

1. En la Consola de gestión, seleccione un entorno.
2. Vaya a Configuración avanzada, Flujo de trabajo.
3. Seleccione la casilla de verificación Activado y haga clic en Guardar.

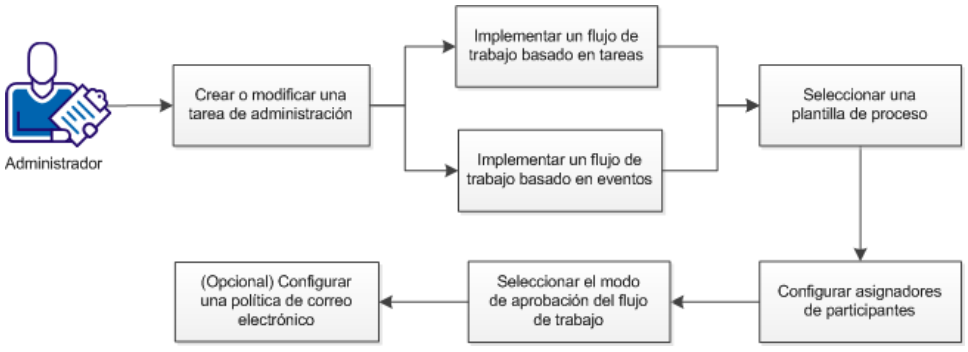
   Nota: Las asignaciones de eventos de esta pantalla sólo se aplican si utiliza el método de Workpoint para configurar el flujo de trabajo. Si utiliza el método de la plantilla (recomendado), no asigne eventos a procesos mediante esta Consola de gestión.
4. Reinicie el servidor de aplicaciones.
5. (Opcional) Configure las herramientas administrativas de Workpoint (en la página 292).

Más información:

Asignación de un proceso a un evento de manera global (en la página 299)
Métodos de control del flujo de trabajo (en la página 269)

Colocación de las tareas de administración bajo el control del flujo de trabajo: método con plantilla

Como administrador, puede colocar tareas de administración bajo el control del flujo de trabajo mediante el método con plantilla.



Siga estos pasos:

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración, Modificar (o Crear) tareas de administración.
2. Busque la tarea que desee establecer bajo el control del flujo de trabajo y haga clic en Seleccionar.
3. Realice *una* de las siguientes acciones:
   - Implemente un flujo de trabajo a nivel de tarea: (en la página 273) para ello, haga clic en el botón de edición Proceso de flujo de trabajo en la ficha Perfil.
   - Implemente un flujo de trabajo a nivel de evento: (en la página 276) para ello, seleccione uno o varios eventos en la ficha Eventos.
4. Seleccione una plantilla de proceso (en la página 279).
5. Configure los resolvedores de participantes (en la página 283).
6. Seleccione un modo de aprobación del flujo de trabajo.
7. (Opcional) Defina una política de correo electrónico para el proceso de flujo de trabajo (en la página 288).

   Nota: Si se selecciona el proceso EscalationApproval, se mostrará un campo llamado Tiempo de espera de la aprobación (min). Este campo se especifica en minutos y no puede estar vacío. De forma predeterminada, el tiempo está establecido en 60 minutos.

Después de configurar un control del flujo de trabajo, un usuario con el rol adecuado realiza la tarea de administración. Por su parte, el participante del flujo de trabajo designado aprueba o rechaza la tarea o el evento.

Flujo de trabajo basado en evento o tarea

CA Identity Manager permite asociar procesos de flujo de trabajo con tareas o eventos. Esto significa que los participantes pueden aprobar o rechazar una tarea completa de CA Identity Manager o un evento específico de una tarea.

Por ejemplo, algunas tareas de CA Identity Manager generan varios eventos, y es posible que un aprobador necesite revisar todos los eventos antes de decidir si aprueba o rechaza una solicitud. Esto es posible bajo el flujo de trabajo a nivel de tarea. Cuando un proceso de flujo de trabajo se asocia con un evento determinado de una tarea, un aprobador no puede ver el contexto global de la tarea dentro del que se realiza una solicitud.

Flujo de trabajo a nivel de tarea

El flujo de trabajo a nivel de tarea permite a los aprobadores revisar todos los eventos antes de decidir si aprueban o rechazan una solicitud. El flujo de trabajo a nivel de tarea se produce antes de que se procese cualquier actividad de tarea. No se ejecutarán eventos ni tareas anidadas antes de que comience la tarea del proceso de flujo de trabajo.

Si se rechaza el flujo de trabajo a nivel de tarea, no se ejecuta ninguna parte de la tarea.

Nota: Una tarea que se configura para controlar el flujo de trabajo a nivel de la tarea también se puede configurar para controlar simultáneamente el flujo de trabajo a nivel del evento. El flujo de trabajo simultáneo a nivel de evento se puede aplicar globalmente o para una tarea específica.

Más información

Flujo de trabajo a nivel de evento (en la página 276)
Proceso global para la asignación de eventos (en la página 297)

Atributo de proceso a nivel de tarea

Los procesos de flujo de trabajo que son compatibles con el flujo de trabajo a nivel de tarea tienen todos un atributo especial que se define en el diseñador de WorkPoint. Este atributo de datos del usuario a nivel de proceso, llamado TASK_LEVEL, está configurado como verdadero de forma predeterminada en las plantillas de proceso siguientes:

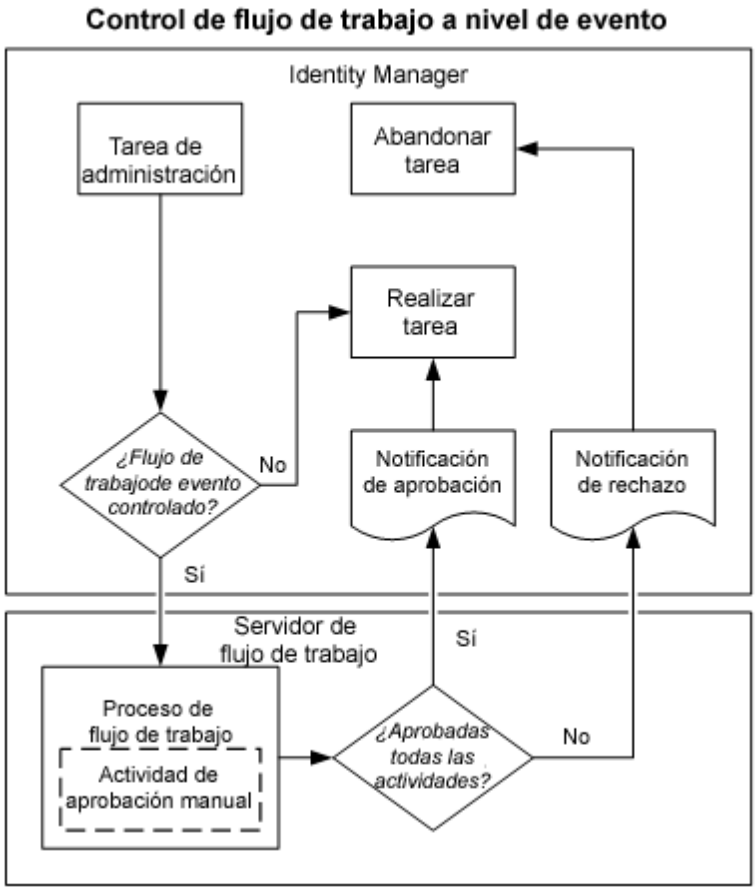
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

Cuando se selecciona una tarea de administración para el flujo de trabajo a nivel de tarea, solamente están disponibles estas plantillas de proceso.

Nota: Aunque TASK_LEVEL esté establecido como verdadero, las plantillas de proceso se pueden utilizar para el flujo de trabajo a nivel de evento. No cambie el valor del atributo TASK_LEVEL.

Diagrama de control a nivel de tarea

El siguiente diagrama ilustra la interacción entre CA Identity Manager y el servidor de flujo de trabajo cuando se inicia un proceso de flujo de trabajo típico a nivel de tarea:



Más información:

Diagrama de control a nivel de evento (en la página 277)

Configuración del flujo de trabajo a nivel de tarea

El flujo de trabajo a nivel de tarea se produce antes de que se procese cualquier actividad de tarea. No se ejecutarán eventos ni tareas anidadas antes de que comience la tarea del proceso de flujo de trabajo.

Para configurar el flujo de trabajo en el nivel de tarea

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración, Modificar (o Crear) tareas de administración.

   Aparecerá la pantalla Seleccionar tarea de administración.

2. Busque la tarea que desee establecer bajo el control del flujo de trabajo, y haga clic en Seleccionar.

   Aparecerá la pantalla Modificar (o Crear) tarea de administración.

3. En la ficha Perfil, compruebe que esté seleccionado Activar Flujo de trabajo.

4. En la ficha Perfil, haga clic en el botón Proceso del flujo de trabajo.

   Aparecerá la ficha Configuración del flujo de trabajo a nivel de tarea.

5. Seleccione una de las siguientes plantillas de proceso de la lista de procesos del flujo de trabajo:

   - SingleStepApproval
   - TwoStageApprovalProcess

   La ficha Configuración del flujo de trabajo a nivel de tarea se expandirá.

6. Configure los resolvedores de participantes según necesite la plantilla de proceso.

   Las solicitudes de participantes se agregarán al proceso.

7. Haga clic en Aceptar.

   CA Identity Manager guardará la configuración del flujo de trabajo del nivel de tarea.

8. Haga clic en Enviar.

   CA Identity Manager procesa la modificación de la tarea.

Flujo de trabajo a nivel de evento

Un evento se puede asignar a un proceso de flujo de trabajo. Cuando se activa un evento asignado a un proceso de flujo de trabajo, el proceso de flujo de trabajo se inicia. La tarea que activó el evento se coloca en un estado pendiente y se considera bajo control del flujo de trabajo.

Un proceso de flujo de trabajo puede requerir que un participante apruebe o rechace un evento o una tarea para que el proceso pueda finalizar. Una tarea que necesite que un participante apruebe manualmente el flujo de trabajo tardará más tiempo en finalizar que una tarea que no se encuentre bajo el control del flujo de trabajo.

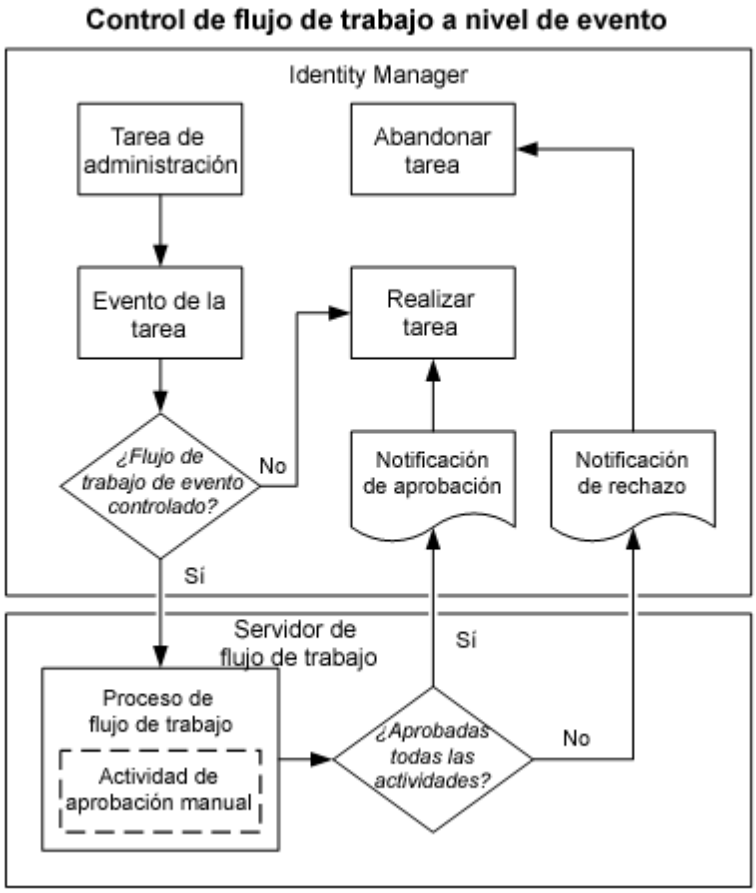
Cuando se hayan realizado todas las actividades de un proceso de flujo de trabajo, el evento asignado al proceso de flujo de trabajo quedará liberado del control del flujo de trabajo. Cuando todos los eventos activados por una tarea determinada quedan liberados del control del flujo de trabajo, la tarea controlada por flujo de trabajo está terminada.

Mientras la tarea se encuentra bajo el control del flujo de trabajo, el contenido de las pantallas de tarea se guarda en la base de datos de persistencia de tareas. El estado de la tarea del flujo de trabajo (datos correspondientes al flujo de trabajo) se almacena en la base de datos de Workpoint.

Nota: La ficha Eventos muestra los eventos que se generan mediante cada ficha de una tarea. Después de agregar una nueva ficha a una tarea, deberá enviar y, a continuación, abrir de nuevo la tarea mediante el uso de Modificar la tarea de administración, antes de que se muestren nuevos eventos en la ficha Eventos.

Diagrama de control a nivel de evento

El siguiente diagrama ilustra la interacción entre CA Identity Manager y el servidor de flujo de trabajo cuando se inicia un proceso de flujo de trabajo típico a nivel de evento:



Más información:

Diagrama de control a nivel de tarea (en la página 274)

Configuración del flujo de trabajo a nivel de evento

El flujo de trabajo a nivel de evento comienza cuando se activa un evento que está asignado a un proceso del flujo de trabajo. La tarea que activó el evento se establece en estado pendiente hasta que el participante apruebe o rechace la tarea.

Para configurar el flujo de trabajo en el nivel de evento

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración, Modificar (o Crear) tareas de administración.

   Aparecerá la pantalla Seleccionar tarea de administración.

2. Busque la tarea que desee establecer bajo el control del flujo de trabajo, y haga clic en Seleccionar.

   Aparecerá la pantalla Modificar (o Crear) tarea de administración.

3. En la ficha Perfil, compruebe que esté seleccionado Activar Flujo de trabajo.

4. En la ficha Eventos, seleccione un evento para asignar a una plantilla de proceso.

   Aparecerá la pantalla de asignación del flujo de trabajo.

5. Seleccione una de las siguientes plantillas de proceso de la lista de procesos del flujo de trabajo:

   - SingleStepApproval
   - TwoStageApprovalProcess

   La pantalla de asignación del flujo de trabajo se expandirá.

6. Configure los resolvedores de participantes según necesite la plantilla de proceso.

   Las solicitudes de participantes se agregarán al proceso.

7. Haga clic en Aceptar.

   CA Identity Manager guardará la configuración del flujo de trabajo del nivel de evento.

8. Repita los pasos 3 - 6 para cada evento que desee establecer bajo el control del flujo de trabajo.

9. Haga clic en Enviar.

   CA Identity Manager procesa la modificación de la tarea.

Nota: La lista de procesos del flujo de trabajo incluye procesos para utilizarse con el método de la plantilla y con el método de WorkPoint:

- Cuando se selecciona un proceso con el método con plantilla (SingleStepApproval o TwoStageApprovalProcess), la página se expandirá para permitir la configuración del resolvedor de participantes.
- Cuando se selecciona un proceso con el método de WorkPoint, la página no se expandirá. Los resolvedores de participantes se configuran en el Diseñador del punto de trabajo.

Tipos de plantillas de proceso

Las plantillas de proceso de flujo de trabajo tienen las siguientes características:

- Definida en el Diseñador de Workpoint.
- Tiene actividades manuales que corresponden a tareas de aprobación de CA Identity Manager.
- Incluye atributos especiales que contienen información para identificar a los participantes (también llamados "aprobadores").

Las plantillas de proceso de flujo de trabajo no incluyen información para seleccionar participantes específicos. Esto lo realiza CA Identity Manager después de que un usuario configure un flujo de trabajo y sus resolvedores de participantes. Esta información se asigna a un evento para el control del flujo de trabajo a nivel de evento, y a una tarea para el control del flujo de trabajo a nivel de tarea.

Al utilizar el método con plantilla, toda la configuración del flujo de trabajo y los participantes se realiza en la Consola de usuario.

Existen tres plantillas de proceso que se pueden utilizar con el método de plantilla:

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

Funcionamiento de una plantilla de proceso

Una plantilla de proceso del flujo de trabajo contiene varios lugares en los que solicita listas de participantes. Cuando la plantilla se asigna a un evento o una tarea de CA Identity Manager, se deben configurar los resolvedores de participantes para estas listas.

En tiempo de ejecución, tal como se muestra en la siguiente figura, CA Identity Manager proporciona las listas de participantes para el proceso del flujo de trabajo basándose en la información configurada.

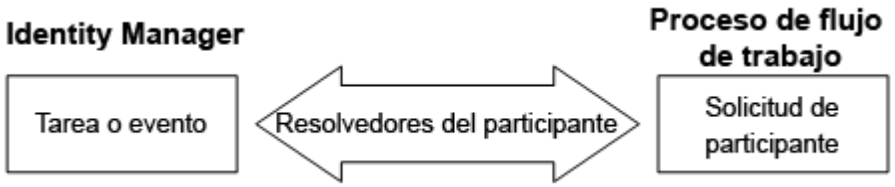


Diagrama de la plantilla de etapa única

El siguiente diagrama ilustra la plantilla de proceso SingleStageApproval tal y como aparece en el Diseñador de Workpoint. La plantilla de proceso incluye dos actividades manuales:

- Un nodo de aprobación para el participante principal. Si este usuario aprueba o rechaza la solicitud, el proceso se ejecuta hasta finalizar.
- Un nodo de aprobación para un participante predeterminado. Este usuario puede aprobar o rechazar la tarea si el participante principal no se encuentra o no responde.

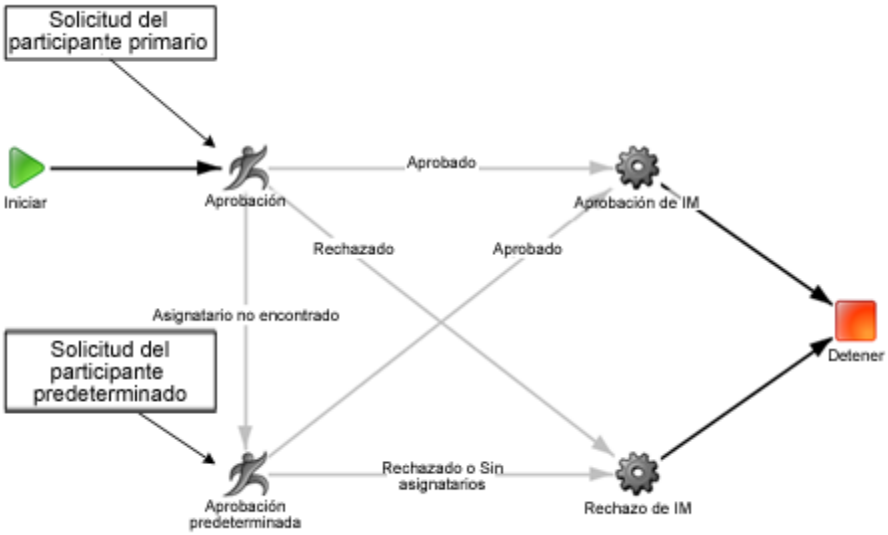


Diagrama de la plantilla de dos etapas

El siguiente diagrama ilustra la plantilla de proceso TwoStageApproval tal y como aparece en el Diseñador del punto de trabajo. La plantilla de proceso TwoStageApproval incluye tres actividades manuales:

- Un nodo de aprobación para el participante empresarial. Si este usuario aprueba o rechaza la solicitud, el proceso continúa con el aprobador técnico.

- Un nodo de aprobación para el participante técnico. Si este usuario aprueba o rechaza la solicitud, el proceso se ejecuta hasta finalizar.
- Un nodo de aprobación para un participante predeterminado. Este usuario puede aprobar o rechazar la tarea si el participante empresarial o el participante técnico no se encuentran o no responden.

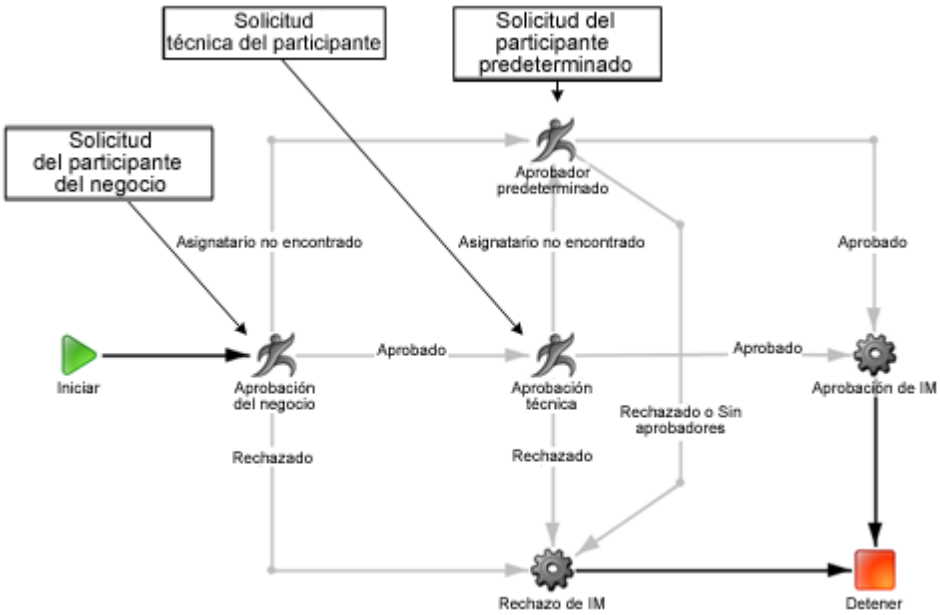
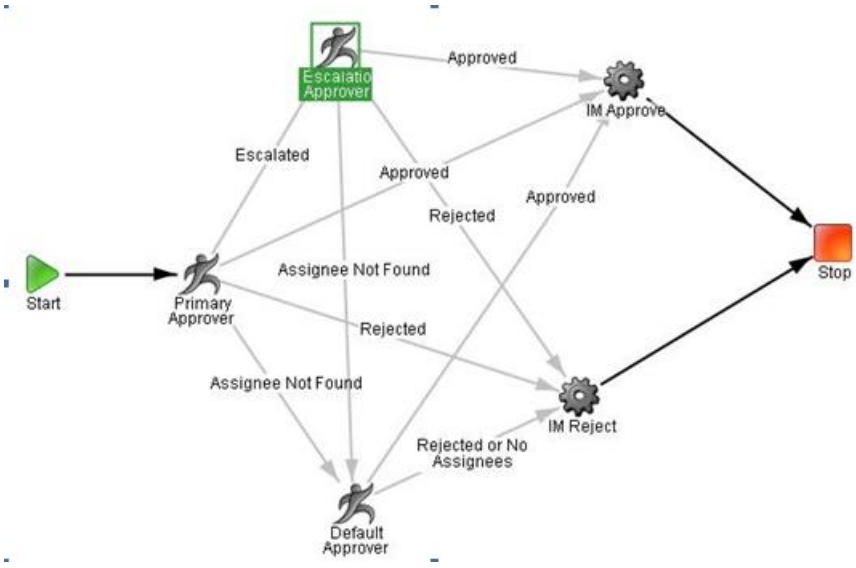


Diagrama de plantilla de aprobación de escalación

El siguiente diagrama ilustra la plantilla de proceso EscalationApproval tal y como aparece en el Diseñador de Workpoint. La plantilla de proceso incluye las siguientes actividades manuales:

- Un nodo de aprobación para el participante principal. Si este usuario aprueba o rechaza la solicitud, el proceso se ejecuta hasta finalizar.
- Un nodo de aprobación para un participante predeterminado. Este usuario puede aprobar o rechazar la solicitud si no se encuentra el participante primario.

- Nodo de aprobación de la transición con tiempo controlado desde el aprobador primario al aprobador de escalación. Este usuario puede aprobar o rechazar la solicitud si se encuentra el participante principal pero no responde en el período de tiempo de espera configurado.



Nota: Para agregar la opción de tiempo de espera a un proceso existente, agregue el campo de datos del usuario PARTICIPANT_TIMEOUT al nodo de actividad y agregue Transición "escalada" al nodo en el que se debe escalar el elemento de trabajo.

Uso de la plantilla de aprobación de escalación

Para usar la plantilla de aprobación de escalación, debe importar manualmente el siguiente archivo zip cuando se actualiza de r12.5 a r12.5 SP1:

Workflow 12.5 to 12.5 SP1 upgrade.zip

El archivo zip está situado en la carpeta workflowScripts, debajo de las herramientas administrativas.

. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- Windows: <rutainstalación>\tools
- UNIX: <rutainstalación2>/tools

Tipos de resolvedores del participante

Para el método de la plantilla, existen siete tipos de resolvedores de participantes:

Miembros de la función de la tarea de aprobación

Especifica los participantes que son miembros de roles que conceden acceso a la tarea de aprobación.

Lista de usuarios

Especifica que los participantes son una lista de usuarios específica.

Miembros del grupo

Especifica que los participantes son miembros de una lista de grupos específica.

Miembros del rol de administrador

Especifica que los participantes son miembros de una lista de roles de administración específica.

Miembros de la tarea de administración

Especifica que los participantes son miembros de roles de administración asociados con una lista específica de tareas de administración.

Resolvedor dinámico

Especifica que los participantes se seleccionan dinámicamente dependiendo de la tarea o el evento que se vaya a aprobar.

Resolvedor nulo

Se resuelve como una lista nula sin usuarios.

Personalizado

Especifica que los participantes están determinados por una resolución de participantes personalizada.

Business Owner Resolver (Resolvedor del propietario del negocio)

Especifica la lista de participantes configurados en la Regla del catálogo como Propietarios del negocio de una entidad.

Admin Owner Resolver (Resolvedor del propietario administrador)

Especifica la lista de participantes configurados en la Regla del catálogo como Propietarios administradores de una entidad.

Manager Resolver (Resolvedor del gestor)

Especifica el participante que se establece como Gestor del objeto de usuario.

Miembros de la función de la tarea de aprobación

Este resolvedor asigna la actividad a todos los miembros de todos los roles de CA Identity Manager que conceden acceso a la tarea de aprobación. Este resolvedor no necesita ninguna configuración adicional.

Lista de usuarios

Este resolvedor asigna el elemento de trabajo a una lista especificada de usuarios.

No se aplica la definición del ámbito. Cualquiera que tenga acceso a la pantalla de configuración del flujo de trabajo puede agregar a otro usuario a la lista o eliminarlo de ella.

Este resolvedor tiene las reglas de validación siguientes:

- Se deberá proporcionar, como mínimo, un nombre de usuario.
- Los nombres de usuario deben pertenecer a usuarios existentes.

Miembros del grupo

Este resolvedor asigna el elemento de trabajo a todos los miembros de todos los grupos especificados en la lista de grupos.

La evaluación de quiénes son los miembros del grupo se realiza en el momento en el que se crea el elemento de trabajo, no al especificar el resolvedor del participante.

No se aplica la definición del ámbito. Cualquiera que tenga acceso a la pantalla de configuración del flujo de trabajo puede agregar a un grupo a la lista o eliminarlo de ella.

Este resolvedor tiene las reglas de validación siguientes:

- Se debe especificar, como mínimo, un grupo.
- Los nombres de grupo deben pertenecer a grupos existentes.

Miembros del rol de administrador

Este resolvedor asigna el elemento de trabajo a todos los miembros de los roles de administrador especificados en la lista de roles de administrador.

La evaluación de quiénes son los miembros del rol se realiza en el momento en el que se crea el elemento de trabajo, no en el momento en el que se especifica el asignador del participante.

No se aplica la definición del ámbito. Cualquiera que tenga acceso a la pantalla de configuración del flujo de trabajo puede agregar cualquier rol o eliminarlo de la lista.

Este resolvedor tiene las reglas de validación siguientes:

- Se debe especificar como mínimo un rol de administrador.
- Los nombres del rol de administrador deben ser los mismos que los roles de administrador ya existentes.

Miembros de la tarea de administración

Este resolvedor asigna el elemento de trabajo a todos los miembros de todos los roles de administración asociados a las tareas de administración especificadas en la lista de tareas de administración.

No se aplica la definición del ámbito. Cualquiera que tenga acceso a la pantalla de configuración del flujo de trabajo puede agregar una tarea a la lista o eliminarla de ella.

La evaluación de quiénes son los miembros del rol y qué roles están presentes en la tarea se realiza en el momento en el que se crea el elemento de trabajo, no al especificar el resolvedor del participante.

Este resolvedor tiene las reglas de validación siguientes:

- Hay que especificar como mínimo una tarea de administrador.
- Los nombres de las tareas de administrador deben ser los mismos que los de las tareas de administrador ya existentes.

Resolvedor dinámico

Este resolvedor devuelve una lista de usuarios según una regla dinámica resuelta en el tiempo de ejecución. Utilice la siguiente selección para establecer restricciones de regla dinámicas:

Aprobadores

Especifica el tipo de usuario que aprueba esta tarea.

Nota: Sólo muestra aquellos objetos que pueden contener usuarios (o aprobadores).

Usuario u objeto

Especifica el usuario o el objeto en el que se pueden encontrar los aprobadores.

- Objeto asociado con el evento: el evento bajo control del flujo de trabajo.
- Iniciador de esta tarea: el usuario que inició la tarea de administración.
- Objeto primario de esta tarea: el objeto que la tarea creó/modificó.
- Anterior aprobador de esta tarea: los aprobadores anteriores de esta tarea.

Usuario asociado con esta cuenta

Actualiza el campo de los atributos del objeto o el usuario para que se enumeren los atributos del usuario de CA Identity Manager en lugar de los atributos de las cuentas de punto final. El resolvedor elimina los atributos a nivel del usuario de CA Identity Manager. Esta casilla de verificación se aplica cuando se selecciona un objeto de cuenta de punto final, por ejemplo, una cuenta de Active Directory.

Atributo

Especifica el atributo que contiene los aprobadores.

Nota: La lista de atributos se ordena alfabéticamente y contiene una lista de nombres para mostrar únicos. Los atributos extendidos se excluyen de la lista.

Tipo de objeto del evento

Especifica el tipo de objeto del evento.

Nota: Sólo aparece si se selecciona "Objeto asociado con el evento".

Nota: El Resolvedor dinámico con Crear grupo requiere que el objeto exista previamente. La información sobre los administradores o la pertenencia al grupo se puede utilizar con resolvedores de atributos dinámicos o de coincidencia para los grupos existentes solamente.

Se ha mejorado el resolvedor dinámico para agregar el aprobador anterior a la lista de objetos admitidos. Si se selecciona el atributo físico que aloja la información del gestor, la configuración enruta una aprobación a un gestor.

Para configurar el resolvedor de aprobación de gestores:

- Defina los aprobadores en Usuarios.
- Seleccione "Anterior aprobador de esta tarea" en la lista desplegable Usuario u Objeto.
- Defina el atributo en un atributo físico que contenga información del gestor.

Resolvedor del atributo coincidente

Este resolvedor funciona en objetos de tipo de sólo usuario. El valor de cualquier objeto disponible coincide con un campo en el objeto de usuario. Utilice la siguiente selección para establecer restricciones de regla de atributos coincidentes:

Aprobadores

Especifica el tipo de usuario que aprueba esta tarea.

Usuario u objeto

Especifica el valor que tendrán los aprobadores en el atributo seleccionado debajo.

Nota: El valor recuperado del usuario u objeto debería ser un valor aceptable para una búsqueda en el usuario del atributo seleccionado.

- Objeto asociado con el evento: el evento bajo control del flujo de trabajo.
- Iniciador de esta tarea: el usuario que inició la tarea de administración.
- Objeto primario de esta tarea: el objeto que la tarea crea/modifica (sólo disponible para la asignación de eventos en el nivel de tarea).
- Anterior aprobador de esta tarea: los aprobadores anteriores de esta tarea.

Usuario asociado con esta cuenta

Actualiza el campo de los atributos del objeto o el usuario para que se enumeren los atributos del usuario de CA Identity Manager en lugar de los atributos de las cuentas de punto final. El resolvedor elimina los atributos a nivel del usuario de CA Identity Manager. Esta casilla de verificación se aplica cuando se selecciona un objeto de cuenta de punto final, por ejemplo, una cuenta de Active Directory.

Atributo de usuario u objeto

Especifica el atributo que contiene el valor que se usa en la búsqueda de aprobadores.

Atributo de búsqueda del aprobador

Especifica el atributo que se usa en la búsqueda para que coincida con el valor identificado anteriormente.

Nota: Al configurar la tarea 'Aprobar creación de usuario' como un resolvedor del atributo coincidente que funciona en Usuarios, Resolvedor de participante, hay que cambiar la firma de método para el script de imApprovers sobre el diseñador de Workpoint para que apunte al nombre único para TwoStageProcessDefinition.

Resolvedor nulo

El resolvedor nulo no devuelve ningún usuario. En función de cómo esté diseñado el proceso de flujo de trabajo, esto puede causar que el proceso omita por completo la aprobación. El resolvedor nulo no requiere ninguna configuración más.

Resolvedor del participante personalizado

El resolvedor de participantes personalizados es un objeto Java que determina los participantes de la actividad de flujo de trabajo y devuelve una lista a CA Identity Manager. Éste, a su vez, transmite la lista al motor de flujo de trabajo. Por lo general, sólo deberá escribir un resolvedor del participante personalizado si las políticas estándar no ofrecen la lista de participantes que requiere una actividad.

Nota: El resolvedor del participante personalizado se crea mediante la API del Resolvedor del participante. Para obtener más información, consulte la *Guía de programación para Java.*

Definición de una política de correo electrónico para un proceso de flujo de trabajo

Puede especificar una política de correo electrónico para cada paso del proceso de flujo de trabajo. En función de la política de correo electrónico definida, se enviará un correo electrónico cuando un proceso alcance el paso o actividad correspondientes. Para las notificaciones de correo electrónico relacionadas con un proceso de flujo de trabajo, se puede seleccionar solamente el tipo *Cuándo enviar* del *Correo electrónico del flujo de trabajo pendiente*.

Nota: Para obtener más información sobre las políticas de correo electrónico, consulte la sección Cómo crear políticas de notificación de correo electrónico.

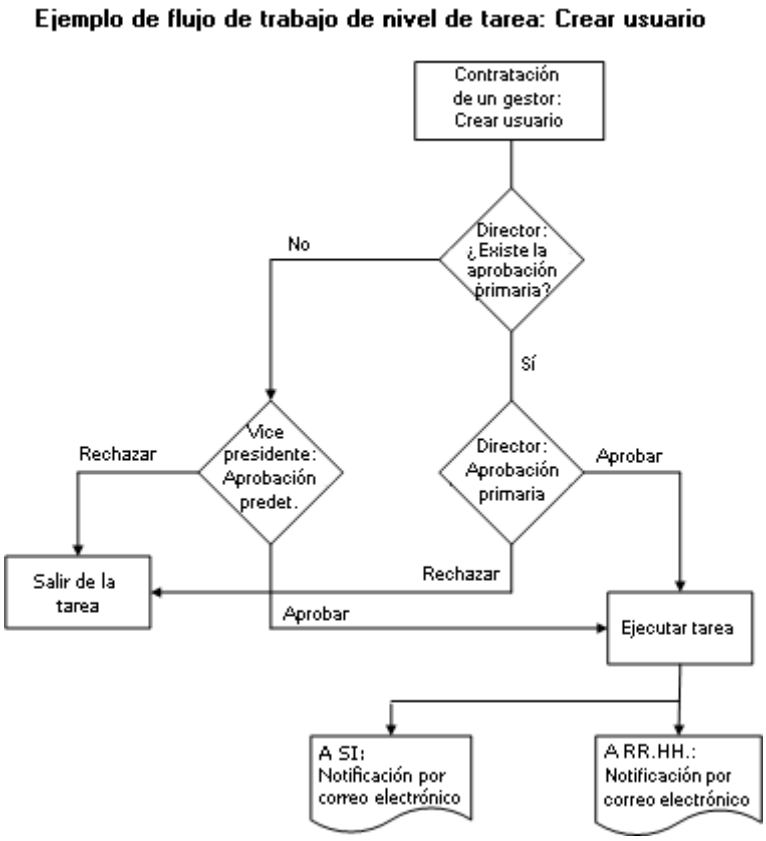
Ejemplo de flujo de trabajo: Crear usuario

El administrador de CA Identity Manager de una empresa necesita definir un flujo de trabajo y funciones de usuario para manejar el siguiente escenario:

- El gerente de ventas de la empresa contrata un representante de ventas nuevo. El gerente de ventas debe poder crear un usuario de CA Identity Manager para la nueva contratación.
- Para agilizar el proceso de contratación, los participantes desean ejecutar sólo un elemento de trabajo para aprobar (o rechazar) la tarea.
- El director de ventas será el aprobador primario de todas las nuevas contrataciones. Si el director de ventas no puede realizar esta tarea por algún motivo, el vicepresidente de ventas será el aprobador predeterminado.
- Si se aprueba la nueva contratación, CA Identity Manager deberá enviar las notificaciones de usuario nuevo por correo electrónico a los departamentos de Recursos humanos (RR.HH) y de Servicios informáticos.

Creación de un diagrama de control de usuario

El diagrama siguiente ilustra el flujo lógico para el escenario de creación de usuario:



Ejemplo de implementación de flujo de trabajo

Para implementar este escenario de ejemplo, el administrador debe realizar las siguientes tareas:

- Asegurarse de que el iniciador de la tarea sea miembro del rol de administración requerido:

  El gerente de ventas debe ser miembro de la función Gestor de usuarios. Esta función otorga al gerente de ventas la autoridad necesaria para iniciar la tarea de administración Crear usuario para la nueva contratación del representante de ventas.

- Activar el flujo de trabajo de la tarea para la tarea de administración Crear usuario.

  El flujo de trabajo de tarea garantiza que sólo se genere un elemento de trabajo para completar la tarea Crear usuario. Puesto que existen varios eventos individuales asociados a la tarea Crear usuario, el flujo de trabajo de eventos generará varios elementos de trabajo y su configuración también será más difícil.

- Configurar los resolvedores del participante.

  El número de resolvedores del participante posible está determinado por la plantilla de proceso de flujo de trabajo seleccionada. La plantilla SingleStageApproval incluye al aprobador primario y predeterminado, mientras que otras plantillas admiten más opciones.

  Puesto que este escenario requiere sólo dos aprobadores individuales, el resolvedor de participante Lista de usuarios ofrece la solución más sencilla. Este resolvedor permite seleccionar los distintos aprobadores por nombre, en lugar de seleccionar entre varios usuarios por función o por grupo.

- Configurar notificación por correo electrónico.

  La Consola de gestión permite la notificación vía correo electrónico para tareas y eventos específicos. Para este escenario, se activa el correo electrónico de la tarea y se envían notificaciones por esta vía cuando se complete la tarea Crear usuario.

  Se requiere una plantilla de correo electrónico para enviar mensajes a los departamentos de Recursos humanos y de Servicios informáticos con el asunto y texto de mensaje apropiados.

Más información

Notificaciones de correo electrónico (en la página 369)
Colocación de las tareas de administración bajo el control del flujo de trabajo: método con plantilla (en la página 271)
Configuración del flujo de trabajo a nivel de tarea (en la página 275)

Cómo usar el método de Workpoint

El método de Workpoint se aplica a versiones de CA Identity Manager anteriores a la r12. Existen catorce procesos de flujo de trabajo de Workpoint predefinidos. Estos procesos están asignados de forma predeterminada a eventos específicos de CA Identity Manager. Debe usar el Diseñador de Workpoint para configurar resolvedores del participante y modificar, como desee, los procesos de flujo de trabajo.

El método de Workpoint también requiere el uso de la Consola de gestión para asignar un proceso de flujo de trabajo a un evento de aprobación y colocar la tarea correspondiente bajo el control del flujo de trabajo en un nivel global dentro del entorno.

En esta sección, se detallan los pasos avanzados necesarios para colocar tareas de administración bajo el control del flujo de trabajo mediante el método de Workpoint.

Nota: Para mayor flexibilidad y facilidad de uso, CA recomienda que use el método con plantilla siempre que sea posible.

Para usar el método de Workpoint

1. Configure las herramientas administrativas de Workpoint. (en la página 292)
2. En la Consola de gestión:
   a. Asegúrese de que el flujo de trabajo esté activado para su entorno; para ello, seleccione la casilla de verificación Activado en Configuración avanzada, Flujo de Trabajo.

      Nota: Las asignaciones de eventos de esta pantalla sólo se aplican si utiliza el método de Workpoint para configurar el flujo de trabajo. Si utiliza el método de la plantilla (recomendado), no asigne eventos a procesos mediante esta Consola de gestión.

   b. (Opcional) Para asignar eventos globales, asocie uno o más eventos al proceso de flujo de trabajo predefinido apropiado.

   c. Si fuera necesario, reinicie el entorno CA Identity Manager.
3. En la Consola de usuario:
   a. Para la asignación de eventos específicos de tarea, asocie uno o más eventos al proceso de flujo de trabajo predefinido apropiado. (opcional)
4. En el Diseñador de Workpoint
   a. Asocie una tarea de aprobación a un proceso de flujo de trabajo (opcional).

   b. Configure los resolvedores del participante con un proceso de flujo de trabajo (opcional).
5. En la Consola de usuario:
   a. Una vez configurado el control de flujo de trabajo, el usuario con la función adecuada realiza la tarea de administración.

   b. El participante del flujo de trabajo designado aprueba o rechaza el evento.

Más información:

Asignación de procesos a eventos (en la página 298)
Asociación de una actividad de flujo de trabajo con una tarea de aprobación (en la página 303)
Resolvedores del participante: Método de Workpoint (en la página 304)

Configuración de herramientas administrativas de Workpoint

Diseñador de Workpoint es software de Workpoint LLC, una filial de Planet Group, Inc., que está integrado en CA Identity Manager. Diseñador de Workpoint le permite gestionar los procesos del flujo de trabajo y las tareas del flujo de trabajo. Entre las herramientas administrativas de Workpoint se incluyen Diseñador de Workpoint y Archivo de Workpoint. Para configurar las herramientas administrativas de Workpoint, instale las herramientas administrativas de CA Identity Manager. Si no las ha instalado, puede ejecutar el instalador y seleccionar la opción Herramientas administrativas de CA Identity Manager.

Nota: Para usar las herramientas administrativas para flujo de trabajo, se debe instalar un JDK compatible en el sistema en el que estén instaladas las herramientas administrativas. Para obtener una lista completa de las plataformas y las versiones compatibles, consulte el cuadro de compatibilidad de CA Identity Manager en el sitio de soporte de CA Identity Manager.

Las herramientas de cliente de flujo de trabajo se encuentran en el directorio WorkPoint de las herramientas administrativas de CA Identity Manager. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Las herramientas de este directorio permiten hacer lo siguiente:

- Crear el esquema de base de datos de flujo de trabajo
- Cargar los scripts de flujo de trabajo predeterminados
- Diseñar y controlar los procesos y las tareas del flujo de trabajo

Configuración de las herramientas administrativas de Workpoint en JBoss

Para configurar las herramientas administrativas de Workpoint en JBoss, edite los archivos init.bat/sh y workpoint-client.properties.

Edición de init.bat/init.sh

Para editar init.bat/init.sh

1. En un editor de texto, edite uno de los siguientes archivos:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     admin_tools/Workpoint/bin/init.sh
2. Anule los comentarios de la línea EJB_CLASSPATH en la sección de JBoss del archivo.

   Nota: Asegúrese de que se eliminen todas las secciones de otros servidores de aplicaciones.
3. Copie el archivo jbossall-client.jar de *inicio_jboss*\client\ a:

   admin_tools\Workpoint\lib

Edición de workpoint-client.properties

Edite el archivo workpoint-client.properties basado en el tipo de servidor de aplicaciones que haya seleccionado durante la instalación de CA Identity Manager.

Para configurar el archivo workpoint-client.properties

1. Abra *admin_tools*\Workpoint\conf\ workpoint-client.properties en un editor de texto.

   admin_tools es una ubicación en la que se están instaladas las herramientas administrativas. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:
   - **Windows:** <rutainstalación>\tools
   - **UNIX:** <rutainstalación2>/tools
2. Localice la sección titulada JBOSS SETTINGS.
3. Elimine todos los valores de propiedades de esa sección.

   Por ejemplo:

   ```
   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming
   ```

   Nota: Es posible que necesite editar el valor de propiedad java.naming.provider.url. Por ejemplo, sustituya localhost por jnp://*nombre_servidor o puerto*:*ip*. Asegúrese de utilizar el número de puerto jnp 1099.
4. Guarde el archivo.

Configuración de las herramientas administrativas de Workpoint en WebLogic

Para configurar las herramientas administrativas de Workpoint en WebLogic, edite los archivos init.bat/sh y workpoint-client.properties.

Edición de init.bat/init.sh

Para editar init.bat/init.sh

1. En un editor de texto, edite uno de los siguientes archivos:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     admin_tools/Workpoint/bin/init.sh
2. Anule los comentarios de EJB_CLASSPATH en la sección de WebLogic del archivo:

   Nota: Asegúrese de que se eliminen todas las secciones de otros servidores de aplicaciones.
3. Copie el archivo wlclient.jar de *inicio_weblogic*\server\lib en la siguiente ubicación:

   admin_tools\Workpoint\lib\

Edición de workpoint-client.properties

Edite el archivo workpoint-client.properties basado en el tipo de servidor de aplicaciones que haya seleccionado durante la instalación de CA Identity Manager.

Para configurar el archivo workpoint-client.properties

1. Abra *admin_tools*\Workpoint\conf\ workpoint-client.properties en un editor de texto.
2. Localice la sección de Weblogic del archivo.
3. Anule los comentarios de todos los valores de propiedades de esa sección.
4. Guarde el archivo.

   Nota: La propiedad java.naming.provider.url debe señalar al nombre de dominio completo y al número de puerto de WebLogic del sistema en el que instaló el servidor de CA Identity Manager.

Configuración de las herramientas administrativas de Workpoint en WebSphere

Para configurar las herramientas administrativas de Workpoint en WebSphere, edite los archivos init.bat/sh y workpoint-client.properties.

Edición de init.bat/init.sh

Para editar init.bat/init.sh

1. En un editor de texto, edite uno de los siguientes archivos:
   - **Windows:**

     admin_tools\Workpoint\bin\init.bat
   - **UNIX:**

     admin_tools/Workpoint/bin/init.sh
2. Anule los comentarios de la sección de WebSphere de IBM.

   Nota: No comente la entrada WP_CLASSPATH de la sección COMMON WP_CLASSPATH.
3. Asegúrese de que se comentan todas las secciones para otros servidores de aplicaciones.
4. Si es necesario, sustituya los valores de JAVA_HOME y WAS_HOME por las rutas apropiadas para su entorno.

Edición de workpoint-client.properties

Edite el archivo workpoint-client.properties basado en el tipo de servidor de aplicaciones que haya seleccionado durante la instalación de CA Identity Manager.

Para configurar el archivo workpoint-client.properties

1. Abra *admin_tools*\Workpoint\conf\ workpoint-client.properties en un editor de texto.

   admin_tools es una ubicación en la que se están instaladas las herramientas administrativas. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:
   - **Windows**: <rutainstalación>\tools
   - **UNIX**: <rutainstalación2>/tools
2. Localice la sección titulada IBM WEBSPHERE SETTINGS.
3. Elimine todos los valores de propiedades de esa sección.

   Por ejemplo:
   `java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory`
   `java.naming.provider.url=iiop://localhost:`*`puerto_bootstrap`*

   Nota: El número de puerto bootstrap debe coincidir con el número de puerto especificado en la Consola de administración de WebSphere. Para localizar el número de puerto correcto, vaya a Servidor, Puntos finales, Dirección de servidor Bootstrap.

4. Actualice el puerto DIRECCIÓN_BOOTSTRAP para el perfil de WebSphere del modo siguiente:
   a. En la Consola de administración de WebSphere, desplácese a Servidores de aplicaciones, nombre_servidor, Comunicaciones.
   b. Expanda los puertos.
   c. Edite el archivo workpoint-client.properties en iam_im.ear/config.
   d. Cambie el puerto predeterminado 2809 de la sección WebSphere por el puerto del perfil para la DIRECCIÓN_BOOTSTRAP.
5. Guarde el archivo.

Inicio de Diseñador de Workpoint.

Para iniciar Diseñador de Workpoint, ejecute el siguiente archivo:

- **Windows:** *admin_tools*\WorkPoint\bin\Designer.bat
- **UNIX:** *admin_tools*/WorkPoint/bin/Designer.sh

donde *admin_tools* es el directorio de instalación de las herramientas administrativas de CA Identity Manager. Las herramientas administrativas se encuentran en las siguientes ubicaciones predeterminadas:

- **Windows**: <rutainstalación>\tools
- **UNIX**: <rutainstalación2>/tools

Nota: Debe configurar los componentes del flujo de trabajo instalados antes de poder ejecutar el Diseñador de Workpoint. Para obtener instrucciones, consulte la sección "Configuración de herramientas administrativas de Workpoint" para su servidor de aplicaciones.

Más información:

Configuración de las herramientas administrativas de Workpoint en JBoss (en la página 292)
Configuración de las herramientas administrativas de Workpoint en WebLogic (en la página 294)
Configuración de las herramientas administrativas de Workpoint en WebSphere (en la página 294)

Procesos de Workpoint

CA Identity Manager incluye una serie de procesos de flujo de trabajo que están predefinidos en el Diseñador de workpoint. Puede usar los procesos predefinidos con las asignaciones de evento predeterminadas respectivas, asignar los procesos de flujo de trabajo a otros eventos, modificar los procesos de flujo de trabajo mediante la adición o eliminación de actividades y crear nuevos procesos de flujo de trabajo.

Proceso global para la asignación de eventos

La asignación de procesos de flujo de trabajo a un evento en un nivel global puede estar basada en política o no.

Para obtener más información sobre cómo asignar un evento a un proceso de flujo de trabajo mediante un flujo de trabajo basado en políticas, consulte Asignación de flujo de trabajo basado en políticas en el nivel de evento global.

Esta tabla muestra el proceso de flujo de trabajo global predeterminado y las asignaciones de eventos, especificadas en la Consola de gestión.

Importante: Se trata de asignaciones globales. El proceso de flujo de trabajo asignado se ejecuta cada vez que alguna tarea del entorno genera el evento correspondiente.

Proceso de flujo de trabajo	Evento asignado
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Nota: Los procesos de flujo de trabajo marcados con un asterisco (*) no se asignan a eventos de forma predeterminada.

Más información:

Asignación de un proceso a un evento de manera global (en la página 299)
Asignación de un proceso a un evento en una tarea específica (en la página 300)

Asignación de procesos a eventos

Puede crear y modificar procesos de flujo de trabajo en el Diseñador de Workpoint. Al crear un proceso de flujo de trabajo para CA Identity Manager, lo hace planteándose una tarea concreta de CA Identity Manager. La ejecución de esta tarea está controlada por el proceso de flujo de trabajo.

Además de crear el proceso de flujo de trabajo, también debe hacer lo siguiente:

- Identificar el evento que genera la tarea de CA Identity Manager, que se describe en Tareas de administración y eventos. Puede crear un proceso de flujo de trabajo para cualquier tarea de CA Identity Manager que genera un evento.
- Asignar el proceso de flujo de trabajo a un evento mediante uno de los siguientes métodos:
  - Asignar un proceso de flujo de trabajo a un evento de manera global.

    Con esta asignación global, el proceso de flujo de trabajo se produce cada vez que se genera el evento en el entorno, independientemente de la tarea que le dio origen.
  - Asignar un proceso de flujo de trabajo a un evento generado por una tarea específica.

    Con esta asignación específica por tarea, el proceso de flujo de trabajo sólo se produce cuando la tarea especificada genera el evento.

  Nota: Si asigna un evento a un proceso de flujo de trabajo tanto global como específico de una tarea, prevalece el proceso de flujo de trabajo asociado a la tarea específica.
- Especificar un resolvedor del participante para la actividad de flujo de trabajo en el proceso de flujo de trabajo.
- Asociar una actividad de flujo de trabajo a una tarea de aprobación.

Más información:

Asignación de un proceso a un evento de manera global (en la página 299)
Asignación de un proceso a un evento en una tarea específica (en la página 300)
Actividades de flujo de trabajo (en la página 302)
Resolvedores del participante: Método de Workpoint (en la página 304)

Asignación de un proceso a un evento de manera global

Se asigna un proceso de flujo de trabajo a un evento de manera global de manera que el proceso se ejecute cuando alguna tarea del entorno genere el evento.

Para asignar un proceso de flujo de trabajo a un evento de manera global

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   `http://hostname/iam/immanage`

   nombre de host

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager. Por ejemplo, miservidor.miempresa.com:puerto.

2. Haga clic en Entornos y seleccione el nombre del entorno de CA Identity Manager apropiado.
3. Haga clic en Configuración avanzada y, a continuación, en Flujo de trabajo.
4. Para asignar un evento a un proceso de flujo de trabajo realice los siguientes pasos:
   a. Seleccione un evento del cuadro de lista Evento.
   b. Seleccione un proceso de flujo de trabajo del cuadro de lista Proceso de aprobación.
   c. Haga clic en Agregar.
5. Cuando finalice la asignación de eventos a procesos de flujo de trabajo, haga clic en Guardar.
6. Reinicie el entorno de CA Identity Manager para que se apliquen los cambios.

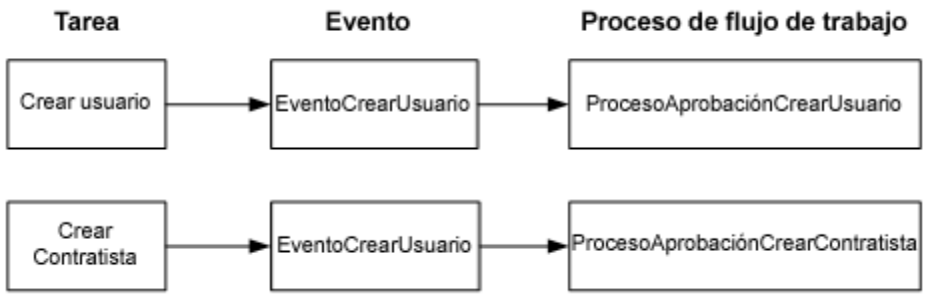
Más información:

Proceso global para la asignación de eventos (en la página 297)

Asignación de un proceso a un evento en una tarea específica

Puede asignar un proceso de flujo de trabajo a un evento que genere una determinada tarea. En este caso, el proceso de flujo de trabajo sólo se produce cuando la tarea especificada genera el evento asignado.

La asignación específica de tarea ofrece control variable sobre los procesos de flujo de trabajo que se pueden ejecutar para el mismo evento. Por ejemplo, el siguiente diagrama muestra dos tareas diferentes que generan el mismo evento, pero que activan dos procesos de flujo de trabajo distintos:



En este diagrama, cada tarea usa un proceso de flujo de trabajo distinto.

Crear usuario

Especifica la tarea de administración predeterminada que activa CreateUserEvent, que está asignada a CreateUserApproveProcess, un proceso de flujo de trabajo predeterminado.

Crear contratista

Especifica una tarea personalizada basada en Crear usuario. En este caso, CreateUserEvent se asigna a CreateContractorApproveProcess, un proceso de flujo de trabajo personalizado creado para aprobar cuentas de contratistas nuevos.

Para asignar procesos de flujo de trabajo a un evento en una tarea existente

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Modificar la tarea de administración.
2. Busque una tarea de administrador.
3. Seleccione una tarea (por ejemplo, la tarea Modificar usuario o Crear usuario) y haga clic en Seleccionar.
4. En la ficha Eventos, seleccione un proceso de flujo de trabajo para el evento en la tarea.

   Nota: Se debe activar el flujo de trabajo para que los nombres del evento y el menú desplegable del proceso de flujo de trabajo aparezcan en esta ficha.
5. Mediante el menú desplegable Proceso del flujo de trabajo, asigne un proceso al nombre de evento y haga clic en Aceptar.

6. Haga clic en Enviar.
7. Abra la Consola de gestión y reinicie el entorno de CA Identity Manager para que se apliquen los cambios.

Para asignar un proceso de flujo de trabajo a un evento en una tarea nueva

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Crear tarea de administración.

   Nota: Asegúrese de seleccionar una tarea de aprobación de flujo de trabajo existente (como Aprobar Crear grupo o Aprobar crear usuario) como la plantilla para la nueva tarea de aprobación.
2. En la ficha Perfil, introduzca la información en los campos apropiados.
3. En la ficha Eventos, seleccione un proceso de flujo de trabajo para el evento en la tarea.

   Nota: Se debe activar el flujo de trabajo para que los nombres del evento y el menú desplegable del proceso de flujo de trabajo aparezcan en esta ficha.
4. Mediante el menú desplegable Proceso del flujo de trabajo, asigne un proceso al nombre de evento y haga clic en Aceptar.
5. Haga clic en Enviar.
6. Abra la Consola de gestión y reinicie el entorno de CA Identity Manager para que se apliquen los cambios.

Nota: La lista de procesos del flujo de trabajo incluye procesos para utilizarse con el método de la plantilla y con el método de WorkPoint:

- Cuando se selecciona un proceso con el método con plantilla (SingleStepApproval o TwoStageApprovalProcess), la página se expandirá para permitir la configuración del resolvedor de participantes.
- Cuando se selecciona un proceso con el método de WorkPoint, la página no se expandirá. Los resolvedores de participantes se configuran en el Diseñador del punto de trabajo.

Más información:

Proceso global para la asignación de eventos (en la página 297)

Actividades de flujo de trabajo

CA Identity Manager incluye una serie de actividades de flujo de trabajo que están predefinidas en el Diseñador de Workpoint. Estas actividades se asignan a los procesos de flujo de trabajo predefinidos.

Los procesos de trabajo predefinidos son procesos de paso único, es decir, cada proceso contiene una sola actividad predefinida.

Cada actividad predefinida corresponde a una tarea de aprobación de flujo de trabajo con el mismo nombre predefinido en CA Identity Manager. Puede usar las actividades predefinidas en otros procesos de flujo de trabajo, y puede crear actividades nuevas.

Puede usar los procesos de flujo de trabajo predefinidos sin modificarlos o bien agregarles más actividades. Para obtener información sobre cómo agregar una actividad a un proceso, consulte la documentación de Workpoint.

Procesos, tareas y actividades

La siguiente tabla detalla las actividades de flujo de trabajo predefinidas y el proceso de flujo de trabajo que cada actividad tiene asignado de forma predeterminada.

Nota: Las actividades de flujo de trabajo predefinidas y las tareas de aprobación correspondientes tienen el mismo nombre.

Proceso del flujo de trabajo	Tarea/actividad de flujo de trabajo
CertifyRoleApprovalProcess**	Aprobar Certificar función
Proceso de consulta*	
CreateGroupApproveProcess	Aprobar Crear grupo
CreateOrganizationApproveProcess	Aprobar Crear organización
CreateUserApproveProcess	Aprobar Crear usuario
DeleteGroupApproveProcess	Aprobar Eliminar grupo
DeleteOrganizationApproveProcess	Aprobar Eliminar organización
DeleteUserApproveProcess	Aprobar Eliminar usuario
ModifyAccessRoleMembershipApproveProcess	Aprobar Modificar la pertenencia a la función de acceso
ModifyAdminRoleMembershipApproveProcess	Aprobar Modificar la pertenencia a la función de administración
ModifyGroupMembershipApproveProcess	Aprobar Modificar la pertenencia al grupo

Proceso del flujo de trabajo	Tarea/actividad de flujo de trabajo
ModifyIdentityPolicySetApproveProcess	Aprobar Modificar conjunto de políticas de identidad
ModifyOrganizationApproveProcess	Aprobar Modificar la organización
ModifyUserApproveProcess	Aprobar Modificar usuario
SelfRegistrationApproveProcess	Aprobar autoregistro
SingleStepApproval*	
TwoStageApprovalProcess*	

Nota: Los procesos de flujo de trabajo marcados con un asterisco (*) deberán usarse con el método con plantilla. Están configurados en la Consola de usuario y, en consecuencia, no cuentan con tareas ni actividades asociadas de forma predeterminada. CertifyRoleApprovalProcess (**) es un proceso de ejemplo que muestra un resolvedor del participante personalizado.

Asociación de una actividad de flujo de trabajo con una tarea de aprobación

Para asociar una actividad de flujo de con a una tarea de aprobación de flujo de trabajo, deberá definir un par nombre/valor en el Diseñador de Workpoint.

Nota: Si no se define un par nombre/valor para una actividad de flujo de trabajo, CA Identity Manager utilizará de forma predeterminada una tarea cuyo nombre coincida con el de la tarea de aprobación.

Para asociar una actividad de flujo de trabajo con una tarea de aprobación

1. Inicie el Diseñador de Workpoint.
2. Haga clic en Archivo, Abrir, Proceso.
3. Seleccione un proceso del flujo de trabajo y haga clic en Abrir.
4. Haga clic con el botón secundario del ratón en el nodo de actividad del proceso y seleccione Propiedades.
5. Seleccione Texto en el menú desplegable Tipo.
6. En la ficha Datos del usuario, introduzca lo siguiente:
   - **Nombre:** TASK_TAG.
   - **Valor:** nombre de etiqueta de tarea de aprobación.
7. Haga clic en Agregar.
8. Haga clic en Aceptar para guardar los cambios.

Cree tareas de aprobación para puntos finales

Se pueden crear tareas de aprobación para pantallas de gestión de cuentas. Para las tareas que aprueban modificaciones de cuenta, la pantalla de aprobación debe ser específica de un tipo de punto final, de manera que el aprobador pueda ver los valores cambiados. Para crear una tarea de aprobación para una tarea Crear o modificar tarea, siga este procedimiento:

Para crear una tarea de aprobación para un punto final

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Crear tarea de admin.
2. Seleccione "Crear una copia de una tarea de administración" que se utiliza para gestionar cuentas en el punto final.

   El nombre empezará con "crear" e indicará el nombre del tipo de punto final. Crear cuenta de Active Directory es un ejemplo.
3. Realice los siguientes cambios en la ficha Perfil.
4. Cambiar el nombre de la nueva tarea.
   - Cambiar la etiqueta de la tarea.
   - Cambiar la acción para aprobar el evento.
5. Realice los cambios siguientes en la ficha Fichas:
   a. Eliminar todas las fichas de relación.
   b. Copiar y editar las pantallas de aprobación en las fichas según corresponda.

      Nota: Puede encontrar problemas al utilizar las pantallas de cuenta en una tarea de aprobación y puede ser necesario realizar cambios a la pantalla de cuenta predeterminada para que funcionen en una tarea de aprobación.
6. Haga clic en Enviar.

Resolvedores del participante: Método de Workpoint

Para especificar los participantes con el método de Workpoint, defina las siguientes propiedades de actividad en el Diseñador de Workpoint:

- El nombre de la secuencia de comandos predefinida de CA Identity Manager que permite la comunicación entre CA Identity Manager y el servidor de flujo de trabajo. La secuencia de comandos emite una solicitud a CA Identity Manager para localizar participantes de actividad y, a continuación, envía esa lista al servidor de flujo de trabajo.
- Referencias a uno o más resolvedores del participante.

Tipos de resolvedores del participante

En lugar de introducir una lista específica de participantes en las propiedades de actividad del flujo de trabajo, se hace referencia a los participantes con un nombre arbitrario que se asigna a un *resolvedor de participante*.

Para el modelo de proceso predefinido, existen cuatro tipos de resolvedores del participante:

Resolvedor de participante por función

Especifica que los participantes son miembros de un rol determinado.

Resolvedor del participante por grupo

Especifica que los participantes son miembros de un grupo determinado.

Resolvedor del participante personalizado

Especifica que los participantes están determinados por una resolución de participantes personalizada.

Resolvedor del participante por filtro

Especifica que los participantes se eligen a través de un filtro de búsqueda.

Resolvedores del participante por función

Con los resolvedores del participante por tipo de rol, CA Identity Manager recupera todos los miembros de esa función y los devuelve como participantes.

Si no se especifica un tipo de resolvedor en el parámetro UserData del cuadro de diálogo Actividad, se utiliza el resolvedor por tipo de función de manera predeterminada.

Si no especifica ningún resolvedor de participantes en la ficha Datos de usuario del cuadro de diálogo de propiedades de actividad de Workpoint, CA Identity Manager buscará, de forma predeterminada, todas las funciones disponibles y que contengan esta tarea de aprobación. A continuación, devolverá los miembros de dicha función como participantes.

Para configurar resolvedores de participantes por función

1. Inicie el Diseñador de Workpoint.
2. Haga clic en Archivo, Abrir, Proceso.
3. Seleccione un proceso del flujo de trabajo y haga clic en Abrir.
4. Haga clic con el botón secundario del ratón en el nodo de actividad del proceso y seleccione Propiedades.
5. Seleccione Texto en el menú desplegable Tipo.

6. En la ficha Datos del usuario, introduzca lo siguiente:
   - **Nombre:** APPROVER_ROLE_NAME
   - **Valor:** el nombre de una función de CA Identity Manager (por ejemplo, Gestor de seguridad)
7. Haga clic en Agregar.

   Nota: No es necesario que esta función contenga tareas de aprobación.
8. Seleccione Texto en el menú desplegable Tipo.
9. En la ficha Datos de usuario, introduzca el par nombre/valor siguiente (opcional):

   Nombre: APPROVERS_REQUIRED

   Valor: YES.
10. Haga clic en Agregar.

    Nota: La configuración de aprobación predeterminada es APPROVERS_REQUIRED=NO. En este caso, una actividad se aprueba de forma automática si no se encuentra ningún participante.

    Si APPROVERS_REQUIRED=YES e CA Identity Manager no encuentra ningún participante, la actividad no se completará correctamente.
11. Haga clic en Aceptar para guardar los cambios.

Resolvedores del participante por grupo

Con los resolvedores del participante por tipo de grupo, CA Identity Manager recupera todos los miembros de ese grupo y los devuelve como participantes.

Para configurar resolvedores del participante por grupo

1. Inicie el Diseñador de Workpoint.
2. Haga clic en Archivo, Abrir, Proceso.
3. Seleccione un proceso del flujo de trabajo y haga clic en Abrir.
4. Haga clic con el botón secundario del ratón en el nodo de actividad del proceso y seleccione Propiedades.
5. Seleccione Texto en el menú desplegable Tipo.
6. En la ficha Datos del usuario, introduzca lo siguiente:
   - **Nombre:** APPROVER_GROUP_UNIQUENAME
   - **Valor**: el nombre de un grupo de CA Identity Manager
7. Haga clic en Agregar.
8. Seleccione Texto en el menú desplegable Tipo.

9. En la ficha Datos de usuario, introduzca el par nombre/valor siguiente (opcional):
   - **Nombre:** APPROVERS_REQUIRED
   - **Valor:** YES.
10. Haga clic en Agregar.

    Nota: La configuración de aprobación predeterminada es APPROVERS_REQUIRED=NO. En este caso, una actividad se aprueba de forma automática si no se encuentra ningún participante.

    Si APPROVERS_REQUIRED=YES e CA Identity Manager no encuentra ningún participante, la actividad no se completará correctamente.
11. Haga clic en Aceptar para guardar los cambios.

Resolvedores del participante personalizados

El resolvedor de participantes personalizados es un objeto Java que determina los participantes de la actividad de flujo de trabajo y devuelve una lista a CA Identity Manager. Éste, a su vez, transmite la lista al motor de flujo de trabajo. Por lo general, sólo deberá escribir un resolvedor del participante personalizado si las políticas estándar no ofrecen la lista de participantes que requiere una actividad.

Nota: El resolvedor del participante personalizado se crea mediante la API Resolvedor del participante. Para obtener más información, consulte la *Guía de programación para Java.*

Para configurar un resolvedor del participante personalizado

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   `http://hostname/iam/immanage`

   nombre de host

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager. Por ejemplo, miservidor.miempresa.com:puerto.
2. Haga clic en Entornos y seleccione el nombre del entorno de CA Identity Manager apropiado.
3. Haga clic en Configuración avanzada, Resolvedor de participantes de flujo de trabajo.

4. En la pantalla Resolvedor del participante de flujo de trabajo, haga clic en Nuevo e introduzca:

   Nombre

   Especifica el nombre del resolvedor de participantes, por ejemplo, APPROVER_CUSTOMRESOLVER_NAME

   Descripción

   Especifica una descripción del resolvedor de participantes personalizado.

   Clase

   Especifica el nombre de clase Java, por ejemplo, com.netegrity.samples.GroupFinder

5. Haga clic en Guardar.
6. Inicie el Diseñador de Workpoint.
7. Haga clic en Archivo, Abrir, Proceso.
8. Seleccione un proceso del flujo de trabajo y haga clic en Abrir.
9. Haga clic con el botón secundario del ratón en el nodo de actividad del proceso y seleccione Propiedades.
10. Seleccione Texto en el menú desplegable Tipo.
11. En la ficha Datos del usuario, introduzca lo siguiente:

    Nombre

    Especifica el nombre del resolvedor de participantes personalizado. Debe coincidir con el nombre que se haya introducido en la pantalla de resolvedor de participantes de tipo personalizado de la Consola de gestión de CA Identity Manager, por ejemplo:

    APPROVER_CUSTOMRESOLVER_NAME

    Valor

    Especifica un nombre único para el resolvedor personalizado, por ejemplo, GroupFinder.

12. Haga clic en Agregar.

    Nota: La configuración de aprobación predeterminada es APPROVERS_REQUIRED=NO. En este caso, una actividad se aprueba de forma automática si no se encuentra ningún participante.

    Si APPROVERS_REQUIRED=YES e CA Identity Manager no encuentra ningún participante, la actividad no se completará correctamente.

13. Haga clic en Aceptar para guardar los cambios.

Resolvedores del participante por filtro

Un resolvedor de participantes por filtro permite que CA Identity Manager busque usuarios o grupos que coincidan con los criterios de filtro. Debe especificar un filtro de búsqueda en el Diseñador de Workpoint, e CA Identity Manager devolverá los aprobadores que coincidan con la actividad de flujo de trabajo pertinente.

Deberá crear un resolvedor del participante por filtro en la ficha Datos de usuario del cuadro de diálogo de propiedades de la actividad del Workpoint.

Sintaxis del filtro de resolvedores del participante

A continuación, se indican los tres atributos necesarios que se combinan para realizar un filtro de búsqueda:

- Atributo del aprobador (por ejemplo, cargo)
- Operación del atributo del aprobador (por ejemplo igual a)
- Valor del atributo del aprobador (por ejemplo gestor)

Los atributos de filtro de búsqueda requeridos se combinan en el siguiente orden:

atributo operación valor

Por ejemplo:

cargo igual a gestor o *departamento que contiene plantilla*

Atributos de filtro requeridos del resolvedor del participante

Los siguientes atributos de filtro del resolvedor de participante son *obligatorios*:

Nota: En cada filtro, n representa un número entero positivo que indica el número de filtro de búsqueda. El valor predeterminado es 1.

APPROVER_FILTER_n_ATTRIBUTE

Especifica el atributo del aprobador. Por ejemplo, Cargo, Departamento, ID de usuario. (Las cadenas de nombre del atributo del aprobador deben coincidir con las cadenas de nombre del atributo del usuario de CA Identity Manager).

APPROVER_FILTER_n_OP

Especifica la operación asociada al atributo del aprobador. Por ejemplo, igual a, no igual a, o contiene. (Las palabras clave de operación no distinguen entre mayúscula y minúscula).

Éstas son entradas válidas para este filtro:

- EQUALS
- STARTSWITH

- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

Especifica el valor asociado al aprobador. Por ejemplo, gestor, plantilla, ingeniería.

Atributos de filtro opcionales del resolvedor del participante

Los siguientes atributos de filtro del resolvedor de participante son *opcionales*.

APPROVER_OBJECTTYPE

USER o GROUP (no distingue entre mayúscula y minúscula)

El valor predeterminado es USER.

APPROVER_ORG_UNIQUENAME

Un nombre exclusivo para una organización del aprobador. (Las cadenas de nombre de organización deben coincidir con las cadenas de nombre de organización de Identity Manager).

El predeterminado es root (raíz).

APPROVER_ORG_AND_LOWER

La organización o las organizaciones secundarias del aprobador:

- 0 significa buscar en la organización del aprobador.
- 1 significa buscar en todas las organizaciones secundarias de la organización del aprobador.

El valor predeterminado es 1.

APPROVER_FILTER_NO

El número de filtros de búsqueda que está usando. Si tiene dos filtros, entonces este número debería ser 2.

El valor predeterminado es 1.

Nota: Este filtro es obligatorio si el número de filtros es mayor que uno.

APPROVER_FILTER_n_CONJ_TYPE

Puede combinar filtros de búsqueda con tipos de conjunción OR o AND.

Nota: Los filtros separados por la conjunción OR tienen prioridad con respecto a aquellos separados por AND.

Por ejemplo, puede especificar el tipo de conjunción AND si está buscando "cargo igual a gestor" Y "departamento igual a desarrollo".

Nota: n representa un número entero positivo mayor que 1, que indica el número de filtros de búsqueda.

Agregación de un filtro de resolvedor del participante

Para agregar filtros de resolvedor de participante

1. Inicie el Diseñador de Workpoint.
2. Haga clic en Archivo, Abrir, Proceso.
3. Seleccione un proceso del flujo de trabajo y haga clic en Abrir.
4. Haga clic con el botón secundario del ratón en el nodo de actividad del proceso y seleccione Propiedades.
5. Seleccione Texto en el menú desplegable Tipo.
6. En la ficha Datos del usuario, introduzca lo siguiente:
   - **Nombre:** APPROVER_FILTER_1_ATTRIBUTE
   - **Valor:** un identificador de función único (por ejemplo, cargo).
7. Haga clic en Agregar.
8. Repita los pasos 6 y 7 para cada atributo del filtro de búsqueda.

   Nota: La configuración de aprobación predeterminada es APPROVERS_REQUIRED=NO. En este caso, una actividad se aprueba de forma automática si no se encuentra ningún participante.

   Si APPROVERS_REQUIRED=YES e CA Identity Manager no encuentra ningún participante, la actividad no se completará correctamente.
9. Haga clic en Aceptar para guardar los cambios.

Ejemplo: resolvedor de participante de filtro

El almacén de usuarios de la siguiente tabla contiene cuatro usuarios: María, Sara, Juan y David, con atributos de ID de usuario, cargo y departamento.

Usuario	ID	Título	Departamento
María	admin1	adminsis	administración

Usuario	ID	Título	Departamento
Sara	test1	adminsis	desarrollo
John	admin2	gestor	desarrollo
David	admin3	adminsis	contabilidad

CA Identity Manager aplica los tres filtros definidos en la tabla siguiente con respecto al almacén de usuarios mencionado:

Nombre	Valor
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	igual a
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	departamento
APPROVER_FILTER_2_OP	igual a
APPROVER_FILTER_2_VALUE	administración
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	cargo
APPROVER_FILTER_3_OP	igual a
APPROVER_FILTER_3_VALUE	adminsis

CA Identity Manager aplica los filtros en el siguiente orden:

1. Evalúa el segundo y el tercer filtro conectado por la conjunción OR:

   "departamento igual a administración" OR "cargo igual a adminsis"

   Se excluye a Juan y devuelve a María, Sara y David.

2. Evalúa el primer y el segundo filtro conectado con la conjunción AND (donde * representa un carácter comodín.

   "uid igual a admin*" AND "departamento igual a administración"

   Se excluye a Sara, y devuelve María y David.

Los últimos usuarios que devuelve del almacén son María y David.

Orden de prioridad del resolvedor del participante

Si no especifica ningún resolvedor del participante, de forma predeterminada, Identity Manager identifica todas las funciones que contengan la tarea de aprobación y devolverá a esos miembros de función como participantes.

Si especifica más de un resolvedor del participante, Identity Manager los evalúa con este orden de prioridad:

1. Personalizado
2. Función
3. Filtro
4. Grupo

Identity Manager identifica y aplica el primer resolvedor en este orden de prioridad y omite cualquier otro resolvedor subsiguiente.

Sólo deberá tener un resolvedor por vez. Además, asegúrese de que el resolvedor esté configurado debidamente para que Identity Manager pueda identificar participantes correctamente.

Especificación de la secuencia de comandos de recursos de flujo de trabajo

Identity Manager se entrega con una secuencia de comandos, llamada IM Approvers (aprobadores de IM), que transmite información entre Identity Manager y el servidor de flujo de trabajo.

Cuando se requiere una lista de participantes para una actividad de flujo de trabajo, la secuencia de comandos transmite a Identity Manager el nombre de la actividad, el identificador del participante provisto en la ficha Datos de usuario del cuadro de diálogo de propiedades de la actividad del Diseñador del punto de trabajo, y cualquier otra información suministrada en dicha ficha. Identity Manager busca los participantes y vuelve a transmitir la lista a la secuencia de comandos. La secuencia de comandos, a su vez, transmite la lista al servidor de flujo de trabajo.

Cuando tiene una nueva definición de proceso del flujo de trabajo y la actividad de proceso del flujo de trabajo es una tarea de aprobación de Identity Manager, se debe especificar la secuencia de comando IM Approvers en la ficha Recursos del cuadro de diálogo de propiedades de la actividad del Diseñador del punto de trabajo.

Para especificar la secuencia de comandos IM Approvers en el Diseñador del punto de trabajo

1. En la ficha Recursos, haga clic en Seleccionar.
2. En el cuadro de diálogo de selección de recursos, seleccione Regla en la lista desplegable. Con esta acción se muestran las reglas (secuencias de comando) que puede asociar con la actividad.

3. Seleccione el nombre de secuencia de comandos IM Approvers (aprobadores de IM) y haga clic en Agregar.
4. Haga clic en Aceptar y, a continuación en Aplicar en el cuadro de diálogo de propiedades de la actividad.

Nota: No modifique la secuencia de comandos IM Approvers.

Especificación de participantes para tareas Certificar usuario

Las tareas Certificar usuario generan el evento CertifyRoleEvent. Este evento puede estar sujeto a aprobación de flujo de trabajo a través del proceso predefinido CertifyRoleApproveProcess.

Identity Manager también incluye el resolvedor del participante predefinido CertifyRoleParticipantResolver, que aparece en el entorno de forma predeterminada. Los participantes de actividades en un CertifyRoleApprovalProcess se especifican a través de CertifyRoleParticipantResolver.

Para proporcionar la información de configuración de participantes

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   `http://hostname/iam/immanage`

   nombre de host

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager. Por ejemplo, miservidor.miempresa.com:puerto.
2. Haga clic en Entornos y seleccione el nombre del entorno de CA Identity Manager apropiado.
3. Haga clic en Configuración avanzada y, a continuación, en Opciones varias.
4. Defina los pares nombre/valor que especifican los aprobadores para cada función que se debe certificar:
   - En el campo Propiedad, use el formato: *tipo-función.nombre-función*

     tipo-función debe ser una de estas funciones: admin, acceso, aprovisionamiento.

     nombre-función es el nombre de cualquier función existente.

     El nombre de función y el tipo de función debe estar separados por un punto (.).
   - En el campo Valor, especifique las ID de los aprobadores y sepárelas con punto y coma (;).

En este ejemplo, la certificación de usuario se puede aprobar para las siguientes funciones y a cargo de los siguientes participantes:

- jsmith01 y ajones19 pueden aprobar la certificación para la función de Gestor de usuarios
- plewis12 es el único aprobador para la función de Gestor del sistema
- rtrevor8 y pkitt3 pueden aprobar la certificación para Mi función de acceso

Propiedad	Valor
admin.Gestor de usuarios	jsmith01;ajones19
admin.Gestor del sistema	plewis12
acceso.Mi función de acceso	rtrevor8;pkitt3

Nota: Cualquier función no especificada no tendrá aprobadores para un CertifyRoleEvent.

Procesos del Diseñador del punto de trabajo

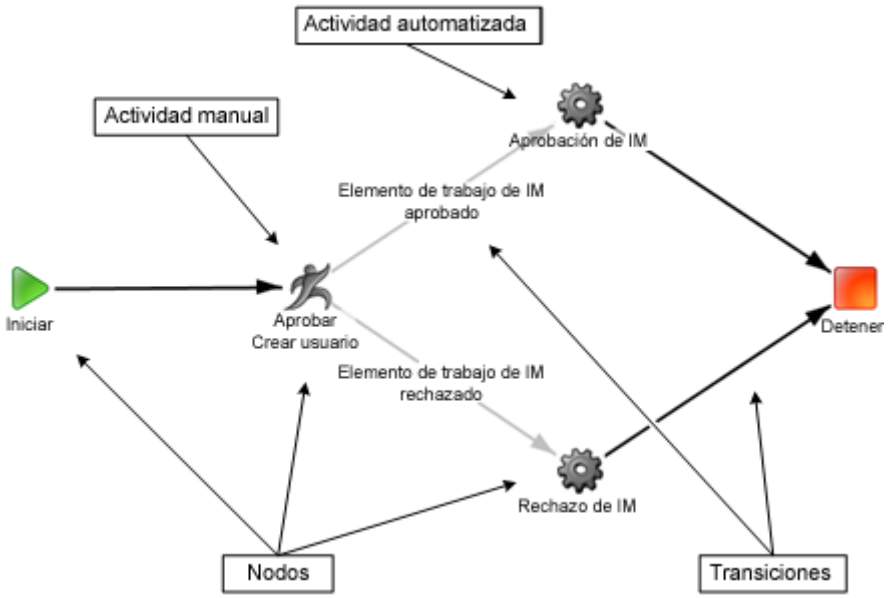
En el Diseñador del punto de trabajo puede personalizar los procesos y las actividades de flujo de trabajo predeterminadas que se entregan con Identity Manager. También puede crear nuevas.

Este documento presenta información de flujo de trabajo de WorkPoint que es específica para Identity Manager. Si desea obtener información completa, consulte la documentación del Diseñador del punto de trabajo.

Nota: A la hora de crear un proceso de flujo de trabajo, puede hacerlo creando una copia de un proceso de Identity Manager ya existente. A continuación, modifique el proceso nuevo para ajustarlo a sus necesidades. Un proceso de flujo de trabajo creado de este modo incluye elementos y nodos específicos de Identity Manager predeterminados como secuencias de comandos de transición y actividades automatizadas.

Diagrama de proceso de Workpoint

El diagrama siguiente muestra un proceso de flujo de trabajo típico con un conjunto mínimo de componentes para un proceso que controla una tarea de Identity Manager. El diagrama ilustra el proceso predefinido CreateUserApproveProcess, que controla la ejecución de una tarea Crear usuario.



Componentes del proceso de WorkPoint

El proceso de flujo de trabajo contiene los siguientes nodos y transiciones:

Iniciar

Cada proceso de flujo de trabajo comienza con este nodo.

Detener

Cada proceso de flujo de trabajo termina con este nodo.

Actividad manual

Una actividad manual exige que un participante apruebe o rechace una tarea de Identity Manager. Además, debe tener el mismo nombre que una tarea de aprobación de flujo de trabajo de Identity Manager.

Un proceso de flujo de trabajo que controla una tarea de Identity Manager debe incluir como mínimo una actividad manual que requiera aprobación.

Actividad automatizada

Una actividad automatizada tiene asignadas una de estas dos secuencias de comandos:

- Notify IM Approve: (Notificar aprobación a IM) informa a Identity Manager que ejecute la tarea respectiva bajo el control del flujo de trabajo.
- Notify IM Reject: (Notificar rechazo a IM) informa a Identity Manager que cancele la ejecución de la tarea de Identity Manager.

En general, la secuencia de comandos Notificar aprobación a IM se activa si se aprueban todas las actividades manuales, y la secuencia de comando Notificar rechazo a IM se activa si se rechaza cualquier actividad manual.

Transición incondicional

Una transición incondicional es una ruta desde un nodo del proceso del flujo de trabajo a otro, y no está asociada con una secuencia de comandos condicional.

Transición condicional

Una transición condicional representa una ruta alternativa desde un nodo del proceso del flujo de trabajo a otro, y está asociada con una secuencia de comandos condicional.

Una secuencia de comandos condicional determina si la transición se produce mediante la evaluación del resultado de la actividad asociada. Si la secuencia de comandos devuelve verdadero, se realiza la transición y el proceso avanza al próximo nodo indicado.

Es posible que dos o más secuencias de comandos de condición sean verdaderas. Esto permite realizar una actividad en paralelo, puesto que cada secuencia de comandos está asociada con una transición distinta.

Nota: Puede usar secuencias de comandos personalizadas en transiciones condicionales. Para obtener instrucciones, consulte la *Guía de programación para Java.*

Propiedades de las actividades manuales

En la tabla siguiente se detallan configuraciones de propiedades específicas de Identity Manager. Estas configuraciones se definen en fichas específicas del cuadro de diálogo de propiedades de la actividad del Diseñador del Workpoint.

Ficha Propiedad	Descripción de la propiedad
Recursos	Aprobadores de IM: especificado en la lista Incluir. Esta secuencia de comandos transmite información entre Identity Manager y el servidor de flujo de trabajo.

Ficha Propiedad	Descripción de la propiedad
Agentes	Nobody Auto Complete: (Autocompletar Nadie) especificado en la lista asíncrona y asociado con el estado disponible. Esta secuencia de comandos determina si una actividad deberá considerarse como aprobada si no existen participantes de la actividad.
Datos de usuario	Define los pares nombre/valor que usa Identity Manager para recuperar los participantes de la actividad. Como alternativa, también puede definir datos que se transmitirán a un resolvedor del participante personalizado.

Propiedades de la transición condicional

Las siguientes secuencias de comandos predeterminadas aparecen en la ficha Condición del cuadro de diálogo Propiedades de la transición:

Elemento de trabajo de IM aprobado

Arroja verdadero, si la actividad asociada es aprobada. El proceso de flujo de trabajo avanza al próximo nodo que indica la transición.

Elemento de trabajo de IM rechazado

Arroja verdadero, si se rechaza la actividad asociada. El proceso de flujo de trabajo avanza al próximo nodo que indica la transición.

Tareas e instancias de procesos

Un *proceso de flujo de trabajo* define los pasos que se deben cumplir a fin de que Identity Manager pueda completar una determinada tarea. Una *tarea* es una instancia del tiempo de ejecución de un proceso del flujo de trabajo.

Por ejemplo, el proceso del flujo de trabajo predeterminado CreateUserApproveProcess define los pasos que deben darse para que un usuario nuevo sea aprobado. Cuando se crea verdaderamente un usuario nuevo en Identity Manager y la tarea se envía para aprobación, se crea una instancia de tarea de CreateUserApproveProcess en el Diseñador del punto de trabajo.

Se puede abrir, ver y modificar tareas en el Diseñador del punto de trabajo mediante una interfaz que es muy similar a la que se usa para editar procesos del flujo de trabajo.

Puede haber varias tareas basadas en el mismo proceso simultáneamente.

Filtrado de tareas

El Diseñador del punto de trabajo incluye filtros que le permiten buscar tareas en función de distintos criterios. Por ejemplo, puede buscar tareas que:

- Se basen en uno o más procesos de flujo de trabajo seleccionados.
- Tengan una referencia de tarea definida por el usuario o una ID de tarea única.
- Se encuentren en un determinado estado(como activo, completo o suspendido).
- Han sido creadas o iniciadas dentro de un intervalo de fechas especificado.

Nota: Para obtener instrucciones e información de referencia sobre filtros de tareas, consulte la documentación del Diseñador del punto de trabajo.

Estado de la tarea y propiedades

Cuando abre una tarea, se muestra el diagrama de flujo de trabajo respectivo. Los nodos y las transiciones de la actividad de flujo de trabajo se muestran en color para indicar si se han ejecutado o no.

Puede ver, y en algunos casos, modificar:

- Propiedades de una tarea, incluida información de participantes y del historial de tareas.
- El estado de una tarea abierta, por ejemplo, si se ha completado.
- Propiedades de nodos y de transiciones individuales de una tarea.

Propiedades de actividades y de elementos de trabajo.

Puede ver y, en algunos casos, modificar propiedades de actividades de tareas y de procesos, entre ellas:

- Información de estado de actividad
- Información de aprobación de actividad
- Información de tarea de aprobación (denominada *elemento de trabajo* en el Diseñador del punto de trabajo), por ejemplo:
  - Si ningún participante ha reservado el elemento de trabajo (lo que elimina el elemento de las listas de otros aprobadores), el estado será Disponible, y no se muestra la ID de usuario de ningún participante.
  - Si un participante ha reservado el elemento de trabajo, pero todavía no lo ha completado, el estado será Abierto, y se mostrará la ID de usuario del participante y la hora de reserva.
  - Si el elemento de trabajo ya se ha completado, el estado será Completo. Se muestra la ID de usuario del participante que ha aprobado o rechazado la tarea según el control de flujo de trabajo, junto con la hora de finalización.

Las propiedades específicas del elemento de trabajo son:

- El nombre y el estado actual del elemento de trabajo.
- Información del historial de estado, incluidas las ID de usuario de los participantes responsables de determinados estados.
- Información de participantes del elemento de trabajo autorizados.

Nota: Para obtener información sobre propiedades de elemento de trabajo, tarea y actividad, consulte la documentación del Diseñador del punto de trabajo.

Realización de actividades de flujo de trabajo

En un proceso de flujo de trabajo, una actividad manual es realizada por una persona designada como participante de la actividad. Los participantes apruebas o rechazan un evento asociado con una tarea de aprobación. Esta actividad la realizan en Identity Manager.

Cuando se ejecuta una actividad asociada a una tarea de aprobación de Identity Manager, tienen lugar las siguientes operaciones:

1. Identity Manager notifica a los participantes.
2. Un participante aprueba o rechaza la tarea.
3. El servidor de flujo de trabajo completa la actividad.

Búsqueda y notificación de participantes

Cuando comienza una actividad de flujo de trabajo asociada con una tarea de aprobación de Identity Manager, el servidor de flujo de trabajo transmite la información sobre los participantes de la actividad a Identity Manager. Esta información se define en las propiedades de la actividad. Identity Manager utiliza esta información para recuperar participantes de la actividad y advertirles de que hay una tarea de aprobación pendiente.

Después de identificar a los participantes, Identity Manager agrega un nuevo elemento de trabajo (la tarea de aprobación) a la lista de trabajo de cada participante. De manera alternativa, Identity Manager también envía una notificación por correo electrónico sobre el nuevo elemento de trabajo a cada participante.

Nota: Si la propiedad de actividad APPROVERS_REQUIRED se establece en falso y no se halla ningún participante, la tarea se considera aprobada de manera predeterminada.

Nota: Un círculo en la columna de estado indica que la tarea de aprobación está disponible para que la reclame cualquier participante. Una marca de verificación indica que el propietario de la lista de trabajo ha aceptado la tarea de aprobación, pero que todavía no la ha completado.

Aceptación y realización de la tarea de aprobación

Una vez que se hallan los participantes, la actividad no se puede completar hasta que uno de ellos acepte la tarea de aprobación y la apruebe o la rechace bajo el control del flujo de trabajo.

Para aceptar una tarea de aprobación, el participante debe hacer clic en el nombre del elemento de trabajo en la consola de actividad del flujo de trabajo y, a continuación, hacer clic en Reservar elemento. (La acción de reservar un elemento lo elimina de la lista de trabajo de otros aprobadores).

Una vez que el participante acepta una tarea de aprobación, se compromete a tomar la decisión de aprobación o rechazo de la tarea bajo el control del flujo de trabajo. Y, puesto que no es posible que varios participantes acepten la misma tarea de aprobación, esta tarea se elimina de las listas de trabajo de otros participantes.

Una vez que un participante acepta una tarea de aprobación, aparece una pantalla de aprobación en la que el participante puede tomar una de las siguientes acciones:

- Aprobar o rechazar la tarea bajo el control del flujo de trabajo inmediatamente.
- Liberar la tarea de aprobación para que quede disponible para otros participantes.
- Cerrar el cuadro de diálogo y completar la tarea más adelante. Para volver a abrir el cuadro de diálogo Aprobar Crear usuario que se muestra arriba, el participante debe hacer clic en el nombre de la tarea de aprobación en la lista de trabajo.

Además, en la pantalla de aprobación, el participante puede actualizar uno o varios campos modificables, si los hubiera. Puede hacer que los campos de esta pantalla se puedan editar al momento en que crea la tarea.

Una vez que el participante aprueba o rechaza la tarea bajo el control del flujo de trabajo, se completa la actividad y el proceso de flujo de trabajo puede continuar por la ruta determinada según el resultado de la actividad, como se describe en la sección siguiente.

El servidor de flujo de trabajo completa la actividad

En la ventana del Diseñador, aparece una actividad manual con dos o varias transiciones condicionales iniciadas en ella.

Cada transición condicional se asocia con una secuencia de comandos. Cuando un participante completa la actividad, las secuencias de comandos evalúan el resultado. El resultado de estas evaluaciones determina la dirección del flujo del proceso.

La siguiente ilustración muestra la actividad Aprobar Crear usuario en el Diseñador y la tarea de aprobación pertinente con el mismo nombre en Identity Manager.

Cuando el participante de la actividad (o aprobador) hace clic en el botón Aprobar o Rechazar de Identity Manager:

1. Finaliza la actividad Aprobar Crear usuario en la instancia de tarea del proceso. Las secuencias de comandos asociadas con las transiciones condicionales evalúan el resultado de la actividad.
2. La instancia de la tarea continúa, dependiendo de qué transición condicional dé verdadero en su evaluación:
   - Si se aprueba la actividad, la secuencia de comandos de elemento de trabajo de IM aprobado arroja verdadero. El flujo de trabajo lleva la transición Elemento de trabajo de IM aprobado al siguiente nodo. Esta actividad automatizada, Aprobación de IM, notifica a Identity Manager para que ejecute la tarea Crear usuario.
   - Si se rechaza la actividad, la secuencia de comandos Elemento de trabajo de IM rechazado arroja verdadero. El flujo de trabajo lleva la transición Elemento de trabajo de IM rechazado al siguiente nodo. Esta actividad automatizada, Rechazo de IM, notifica a Identity Manager para que cancele la tarea Crear usuario.

Vista de los trabajos de Workpoint

Puede ver el estado de tiempo de ejecución de los trabajos de Workpoint en la Consola de usuario, desde las siguientes ubicaciones:

- Tareas de aprobación
- Ver tareas enviadas

En los nuevos entornos, todas las tareas de aprobación incluyen la ficha Ver trabajo de forma predeterminada. Sólo aquellos eventos creados en esta versión admiten la visualización de imágenes de trabajos de todas las definiciones de procesos ejecutadas para ese evento o tarea en Ver tareas enviadas. Los eventos creados en versiones anteriores no admiten la función Vista de trabajo de flujo de trabajo.

Cómo agregar la ficha Ver trabajo a las fichas de aprobación existentes

En las tareas de aprobación, debe agregar la nueva ficha Ver trabajo para todas las tareas existentes, con el fin de ver la imagen del trabajo para ese elemento de trabajo.

Nota: Los nuevos entornos contienen esta ficha para las tareas de aprobación.

Para agregar la ficha Ver trabajo a una tarea existente

1. En la categoría Tareas y roles de administración, ejecute ModifyAdminTask mediante la selección de Tarea de administración, Modificar la tarea de administración.
2. Haga clic en Buscar y seleccione una tarea de aprobación (por ejemplo, Aprobar Crear usuario) y, a continuación, haga clic en Seleccionar.

   Aparecerá el cuadro de diálogo Modificar la tarea de administración: Aprobar Crear usuario.
3. Haga clic en la ficha Fichas y, en el menú desplegable, seleccione Ver trabajo (JobView) y haga clic en Enviar.

   La ficha Ver trabajo se agregará a la tarea de aprobación.

   Repita este proceso con todas las tareas de aprobación existentes.

Configuración de la ficha Ver trabajo

Configure esta ficha con lo siguiente:

Nombre

Un nombre que asigna a la ficha.

Etiqueta

Un identificador de la ficha que es único dentro de esta tarea. Debe comenzar con una letra o guión bajo, y contener sólo letras, números o guiones bajos. La etiqueta se utiliza principalmente para configurar valores de datos a través de documentos XML o parámetros de HTTP.

Ocultar ficha

Impide que se vea la ficha en la tarea. Esta opción es útil para aplicaciones que necesitan ocultar la ficha, pero que aún conservan el acceso a los atributos que contiene.

Vista de trabajo

En esta ficha se muestra la imagen del trabajo del elemento de trabajo especificado.

Visualización de la ficha Ver trabajo en una tarea de aprobación

Para ver la ficha Ver trabajo en una tarea de aprobación, siga este procedimiento.

Para ver la ficha Ver trabajo

1. En el cuadro de diálogo Lista de trabajo, seleccione la tarea de aprobación que desee ver.
2. Haga clic en la ficha Ver trabajo para ver el estado de la tarea en tiempo de ejecución.

   Desde aquí, puede aprobar, rechazar, reservar o cerrar la ficha.

También puede hacer clic en la ficha Principal y en Ver mi lista de trabajo para acceder al cuadro de diálogo Lista de trabajo.

Visualización de un trabajo de flujo de trabajo para el flujo de trabajo a nivel de evento

Para ver un trabajo de flujo de trabajo para Flujo de trabajo a nivel de evento en Ver tareas enviadas, siga este procedimiento.

Para ver un trabajo de flujo de trabajo

1. En la ficha Sistemas, seleccione Ver tareas enviadas, especifique sus criterios de búsqueda y seleccione Buscar.
2. Seleccione el evento y haga clic en el lápiz para ver los detalles del evento.
3. En Vista de los trabajos del flujo de trabajo de eventos, seleccione el proceso y haga clic en el lápiz para ver la imagen del trabajo de este evento.

Visualización de un trabajo de flujo de trabajo para el flujo de trabajo de nivel de tarea

Para ver un trabajo de flujo de trabajo para el flujo de trabajo de nivel de tarea en Ver tareas enviadas, siga este procedimiento.

Para ver un trabajo de flujo de trabajo

1. En la ficha Sistemas, seleccione Ver tareas enviadas, especifique sus criterios de búsqueda y seleccione Buscar.
2. Seleccione la tarea y haga clic en el lápiz para ver los detalles de la tarea.

En Vista de trabajo de flujo de trabajo de tarea, seleccione el proceso y haga clic en el lápiz para ver la imagen del trabajo de estas tareas.

Flujo de trabajo basado en políticas

El flujo de trabajo basado en políticas permite colocar un evento o una tarea de administración debajo del control de flujo de trabajo de acuerdo con la evaluación de una regla. Esto significa que, en lugar de que un evento o una tarea de administración siempre lance un proceso de flujo de trabajo, el proceso de flujo de trabajo ejecuta y genera un elemento de trabajo sólo si una regla asociada con el evento o la tarea de administración es verdadera.

Una *regla de aprobación* es una condición que determina si un proceso de flujo de trabajo se inicia o no. Si se inicia, el proceso de flujo de trabajo coloca el evento o la tarea de administración bajo el control del flujo de trabajo agregando un elemento de trabajo a una lista de trabajo del aprobador.

Una *política de aprobación* es la combinación de la regla de aprobación, el tipo de evaluación de regla, orden de política, descripción de política, y el proceso de flujo de trabajo.

Por ejemplo, al crear un nuevo grupo, puede definir una política de aprobación que coloque CreateGroupEvent bajo el control del flujo de trabajo y sólo cree un elemento de trabajo si el nuevo grupo forma parte de una organización principal designada. Si el nuevo grupo no forma parte de esa organización, no se ejecutará el proceso de flujo de trabajo, ni se creará ningún elemento de trabajo.

Si un evento tiene varias reglas, se tendrán que aprobar todos los procesos de flujo de trabajo asociados al evento para que el evento se pueda aprobar. Al igual que ocurre para las tareas de administración, puede definir una política de aprobación que coloca CreateGroupTask debajo del control de flujo de trabajo y crea un elemento de trabajo si el nombre del nuevo grupo comienza con "Ventas". Si el nombre del grupo nuevo no comienza con Ventas, el proceso de flujo de trabajo no se ejecuta y no se crea ningún elemento de trabajo.

Puede crear una regla de política que se evalúe siempre, o sólo cuando cambie un atributo específico de un objeto gestionado, por ejemplo, cuando cambie el valor del salario de un empleado.

Nota: En versiones anteriores del flujo de trabajo basado en la política, si algún aprobador modificaba los atributos, estos se enviaban a la reaprobación. Con la aprobación y el rechazo de nivel del atributos, solamente se aprueban cambios en cualquier etapa una vez. El elemento de trabajo nunca se envía a la reaprobación aunque el atributo contenido en la regla se modifique. Una vez que un aprobador aprueba un cambio, no verán el elemento de trabajo otra vez hasta que un cambio nuevo se envíe o la tarea se reenvíe.

Más información:

Flujo de trabajo a nivel de evento (en la página 276)
Flujo de trabajo a nivel de tarea (en la página 273)
Orden de la política (en la página 330)
Evaluación de reglas (en la página 328)

Procesos de flujo de trabajo predeterminados

Todas las plantillas de flujo de trabajo predeterminadas y los procesos de flujo de trabajo predefinidos admiten las siguientes reglas de flujo de trabajo:

- **Plantillas de proceso**: permiten configurar aprobadores (o resolvedores del participante) en la Consola de usuario.
- **Proceso de flujo de trabajo predefinidos**: requieren que configure resolvedores del participante en el Diseñador de Workpoint.

También puede crear procesos de flujo de trabajo personalizados para utilizarlos con las reglas de flujo de trabajo.

Más información:

Procesos de Workpoint (en la página 297)

Objetos de reglas

Los administradores de CA Identity Manager pueden crear políticas de aprobación para un evento o tarea de administración basados en los objetos siguientes. A continuación se recogen los objetos para eventos si se aplican a un evento dado y están presentes durante la ejecución de eventos:

- **Iniciador de la tarea**: el administrador de CA Identity Manager que ejecuta la tarea.
- **Objeto primario del evento**: el objeto primario asociado con el evento.
- **Objeto secundario del evento**: el objeto secundario asociado con el evento con relación al objeto primario.

A continuación se describen los objetos para tareas de administración:

- **Objeto primario de la tarea**: el objeto primario asociado con la tarea.
- **Iniciador de la tarea**: el administrador de Identity Manager que ejecuta la tarea.
- **Infracciones de la política de identidad**: En el caso de las infracciones de la política de identidad, las reglas se basan en el nombre de la política de identidad que provocó la infracción, por ejemplo, nombre de política ES IGUAL A política de título. El mensaje de infracción aparece en la ficha Detalles de la tarea en la pantalla de aprobación, que es la misma que Detalles de la tarea, Ver tareas enviadas. El mensaje de infracción de SOD aparece debajo del nuevo encabezamiento de sección denominado "infracción de la política de identidad". Los aprobadores pueden ver estos mensajes y decidir aprobar o rechazar la tarea.

Evaluación de reglas

Las reglas de políticas se pueden evaluar para un evento de las dos maneras que se indican a continuación:

- Siempre

  Se invocan las políticas con tipo de evaluación de Siempre si la política evalúa en verdadero sin tener en cuenta si los atributos incluidos en la política se cambian o no. En la pantalla de aprobación para un elemento de trabajo que se generó como resultado de un tipo de evaluación de política especificado en Siempre, un aprobador puede cambiar los atributos editables en la pantalla de aprobación.

  Nota: Si el aprobador hace clic en el botón Rechazar, el evento se rechaza como ocurrió anteriormente.

- Sólo si cambia un atributo especificado en la condición de aprobación.

  Sólo se invoca una política con tipo de evaluación OnChange si la política se evalúa como Verdadera y ninguno de los atributos incluidos en la política cambia. En la pantalla de aprobación para un elemento de trabajo que se generó como resultado de una política con tipo de evaluación definido en Onchange, el aprobador sólo podrá cambiar el valor de aquellos atributos contenidos en la política, si dichos atributos tienen permiso de lectura y escritura para esa pantalla de aprobación. El resto de atributos que existen en la pantalla de aprobación sólo tienen permisos de sólo lectura.

  Nota: Si el aprobador hace clic en el botón Rechazar, sólo se rechazarán los cambios realizados a los atributos incluidos en la política de aprobación y se evaluará la siguiente política de aprobación en orden.

  Esta opción se aplica sólo al objeto primario del evento o de la tarea.

Por ejemplo, considere las siguientes políticas, todas ellas para ModifyUserEvent en la tarea de administración Modificar usuario:

Política	Regla	Evaluación
Política 1	Usuario donde (ID de usuario = Smith01)	Siempre
Política 2	Usuario donde (Título = Gestor)	Cuando cambia el atributo Título
Política 3	Usuario donde (Salario >= 80.000)	Cuando cambia el atributo Salario

La política 1 se evalúa cada vez que el administrador ejecuta la tarea Modificar usuario para el usuario Smith01, independientemente del atributo que cambie.

La política 2 se evalúa cuando el administrador ejecuta la tarea Modificar usuario para cambiar el atributo Título de cualquier objeto de usuario. La política 2 es verdadera si el título cambia a Director.

La política 3 se evalúa cuando el administrador ejecuta la tarea Modificar usuario para cambiar el atributo Salario de cualquier objeto de usuario. La política 3 es verdadera si el salario cambia a 80.000 o más.

En este ejemplo, si un administrador usa la tarea Modificar usuario para cambiar el atributo Título a Gestor para el usuario Smith01, tanto la política 1 como la política 2 evalúan si es verdadero y se inician sus procesos de flujo de trabajo respectivos. En este caso, se aplica el orden de prioridades estándar.

La evaluación de reglas condicional permite que un aprobador de un elemento de trabajo cambie un atributo que afecta a otro elemento de trabajo del mismo evento mientras este evento sigue pendiente. Sólo será posible para políticas de aprobación que tienen el tipo de evaluación definido en Siempre. En el ejemplo anterior, si un administrador cambia un atributo del usuario Smith01, la política 1 será verdadera y generará un elemento de trabajo. Mientras se aprueba el elemento de trabajo generado por la política 1, ese aprobador puede cambiar, en la misma pantalla de aprobación, el atributo Salario de Smith01. En este caso, el nuevo valor de salario de Smith01 determinará si la política 3 generará o no un elemento de trabajo para la misma instancia de ModifyUserEvent. Si el aprobador cambia el salario a 90.000, la política 3 generará un nuevo elemento de trabajo que se deberá aprobar antes de que se apruebe el evento. Se aplicará el orden de prioridades estándar.

Más información:

Orden de la política (en la página 330)
Objetos de reglas (en la página 327)

Ejemplo de evaluación de reglas

Considere las siguientes políticas, todas ellas para ModifyUserEvent en la tarea de administración Modificar usuario:

Política	Regla	Evaluación
Política 1	Usuario donde (ID de usuario = Smith01)	Siempre
Política 2	Usuario donde (Título = Gestor)	Cuando cambia el atributo Título
Política 3	Usuario donde (Salario >= 80.000)	Cuando cambia el atributo Salario

La política 1 se evalúa cada vez que el administrador ejecuta la tarea Modificar usuario para el usuario Smith01, independientemente del atributo que cambie.

La política 2 se evalúa cuando el administrador ejecuta la tarea Modificar usuario para cambiar el atributo Título de cualquier objeto de usuario. La política 2 es verdadera si el título cambia a Director.

La política 3 se evalúa cuando el administrador ejecuta la tarea Modificar usuario para cambiar el atributo Salario de cualquier objeto de usuario. La política 3 es verdadera si el salario cambia a 80.000 o más.

En este ejemplo, si un administrador usa la tarea Modificar usuario para cambiar el atributo Título a Gestor para el usuario Smith01, tanto la política 1 como la política 2 evalúan si es verdadero y se inician sus procesos de flujo de trabajo respectivos. En este caso, se aplica el orden de prioridades estándar.

La evaluación de reglas condicional permite que un aprobador de un elemento de trabajo cambie un atributo que afecta a otro elemento de trabajo del mismo evento mientras este evento sigue pendiente. Sólo será posible para políticas de aprobación que tienen el tipo de evaluación definido en Siempre. En el ejemplo anterior, si un administrador cambia un atributo del usuario Smith01, la política 1 será verdadera y generará un elemento de trabajo. Mientras se aprueba el elemento de trabajo generado por la política 1, ese aprobador puede cambiar, en la misma pantalla de aprobación, el atributo Salario de Smith01. En este caso, el nuevo valor de salario de Smith01 determinará si la política 3 generará o no un elemento de trabajo para la misma instancia de ModifyUserEvent. Si el aprobador cambia el salario a 90.000, la política 3 generará un nuevo elemento de trabajo que se deberá aprobar antes de que se apruebe el evento. Se aplicará el orden de prioridades estándar.

Orden de la política

Todas las políticas de aprobación contienen un campo Orden de la política en el que un valor entero positivo, ordenado de menor a mayor, especifica la prioridad. La prioridad de cada política determina lo siguiente:

- El orden en el que se evalúan las reglas de aprobación.
- En la reglas que son verdaderas, el orden en el que se inician los procesos de flujo de trabajo.

Una política con un valor entero inferior tiene una prioridad superior y su regla se evalúa antes que la de una política con un valor entero superior. En todas las políticas para un evento o tarea de administración que sean verdaderas, la política con mayor prioridad iniciará en primer lugar su proceso de flujo de trabajo.

Ejemplo de orden de la política

En este sencillo ejemplo se muestra cómo funciona el orden de la política. En este ejemplo, se supone que las reglas de políticas se evalúan siempre.

Si un evento tiene varias políticas que se evalúan siempre, para que el evento se apruebe es necesario que se aprueben todas las políticas. Sin embargo, si una política asociada con el evento, que tiene un tipo de evaluación de política establecido en SIEMPRE, se rechaza, se rechazará el evento propiamente dicho.

Nota: Si la política asociada con el evento tiene un tipo de evaluación definido en Onchange, sólo se rechazarán los cambios asociados con los atributos contenidos en dicha política. No se rechaza el evento propiamente dicho y se evaluará la siguiente política.

En este ejemplo, política 1, política 2 y política 3 tienen un tipo de evaluación de política definido en SIEMPRE. La política 1 se evalúa como falsa, el proceso de flujo de trabajo, denominado "proceso 1", no se ejecuta y no se genera ningún elemento de trabajo para el usuario 1. El control del evento pasa inmediatamente a la política 2. Las políticas 2 y 3 se evalúan como verdaderas. Debido a su prioridad superior, el flujo de trabajo proceso 2 se ejecuta en primer lugar y genera un elemento de trabajo para el usuario 2.

Si el usuario 2 aprueba el elemento de trabajo, se ejecuta el flujo de trabajo Proceso 3 y genera un elemento de trabajo para el usuario 3, quien deberá aprobar el elemento de trabajo para que se apruebe el evento. Estas acciones se muestran en la tabla siguiente:

Prioridad	Política	Resultado	Flujo de trabajo	Aprobador	Acción
1	Política 1	Falso	Proceso 1	Usuario 1	—
2	Política 2	Verdadero	Proceso 2	Usuario 2	Aprobado
3	Política 3	Verdadero	Proceso 3	Usuario 3	Aprobado

Sin embargo, si el usuario 2 rechaza el elemento de trabajo, se rechazará el evento y no generará ningún elemento de trabajo para el usuario 3, tal y como se muestra en la tabla siguiente:

Prioridad	Política	Resultado	Flujo de trabajo	Aprobador	Acción
1	Política 1	Falso	Proceso 1	Usuario 1	—
2	Política 2	Verdadero	Proceso 2	Usuario 2	Rechazado

Prioridad	Política	Resultado	Flujo de trabajo	Aprobador	Acción
3	Política 3	Verdadero	Proceso 3	Usuario 3	—

A continuación, la política 1, la política 2 y la política 3 tienen un tipo de evaluación de política definido en ONCHANGE. Si el usuario 2 rechaza el elemento de trabajo, sólo se rechazarán los cambios asociados con los atributos contenidos en la política 2. A continuación se evaluará la política 3 y el proceso 3 de flujo de trabajo ejecuta y genera un elemento de trabajo para el usuario 3. Si el usuario 3 rechaza el elemento de trabajo, se rechaza el evento ya que se rechazaron todos los cambios a este evento. Si el usuario 3 aprueba el elemento de trabajo, se aprueba el evento y se mantienen los cambios de atributo incluidos en la política 3.

Prioridad	Política	Resultado	Flujo de trabajo	Aprobador	Acción
1	Política 1	Falso	Proceso 1	Usuario 1	—
2	Política 2	Verdadero	Proceso 2	Usuario 2	Rechazado
3	Política 3	Verdadero	Proceso 3	Usuario 3	Aprobado

Descripción de política

Se ha agregado un atributo de descripción de cadena opcional y que no puede buscarse al objeto gestionado de la política de aprobación y aparece en los elementos de trabajo resultantes.

Número máximo de caracteres compatibles: 255 caracteres

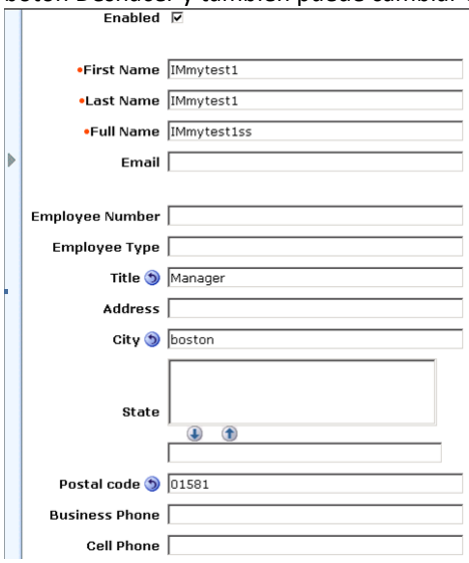
Puede introducir información sobre el paquete/clave en el siguiente formato para la descripción:

```
$ (bundle=<nombre completo de los paquetes de recursos> : key=<clave>)
```

Cómo resaltar los atributos cambiados en las pantallas de aprobación

Para que un aprobador sepa qué atributos se han modificado o para deshacer los cambios en ellos si fuera necesario, se ha agregado un icono de deshacer a la pantalla del perfil del aprobador que permita saber a éste que este atributo se ha modificado.

El aprobador puede ver el valor original para los atributos editables haciendo clic en el botón Deshacer y también puede cambiar el valor del atributo a cualquier otro valor.



Políticas de aprobación y atributos con varios valores

Anteriormente, si se configuraba una regla para un atributo con varios valores, no había una forma de indicar que deseaba que se aplicase esta regla sólo en valores recién agregados o eliminados para atributos con varios valores. Esta acción se consigue al consultar el tipo de evaluación de política para una regla basada en un atributo con varios valores. Si el tipo de evaluación de regla es Onchange, sólo se aplicará esta regla a los valores recién agregados o eliminados (no a todos) del atributo con varios valores. Si la regla debe basarse en todos los valores del atributo con varios valores independientemente de que estuvieran recién agregados o eliminados, el tipo de evaluación para esa regla debe ser Siempre.

Los cambios realizados a los atributos con varios valores se resaltan en la pantalla del perfil con un icono Deshacer. Si una regla se evaluó como verdadera debido a que se agregó o quitó un nuevo valor en un atributo con varios valores, el aprobador encargado de aprobar este cambio verá TODOS los valores contenidos en el atributo con varios valores. Al hacer clic en el icono de deshacer se devuelve el valor para ese atributo a su valor original. Si un aprobador desea ver los valores eliminados, hacer clic en el icono Deshacer mostrará el conjunto original de valores. Hacer clic en el icono para rehacer muestra el nuevo conjunto de valores que permite al aprobador diferenciar cuáles fueron los valores eliminados y cuáles los agregados. Hacer clic en el botón para aprobar aprueba todos los cambios en este atributo con varios valores. Hacer clic en el botón para rechazar rechaza todos los cambios en este atributo con varios valores. Todas las reglas posteriores que pertenezcan a este atributo con varios valores no se evaluarán a menos que haya una delta de valores para este atributo con varios valores.

Nota: Para las reglas basadas en los atributos con varios valores, los valores contenidos en el atributo con varios valores son los valores reales y no los de visualización. Por ejemplo, el valor de visualización para el estado MA es Massachusetts. Cuando se crea una política de aprobación que se basa en el atributo de estado, la regla debería parecerse a estado=MA.

Considere las siguientes políticas de ejemplo, todas ellas para ModifyUserEvent en la tarea de administración Modificar usuario:

Política	Regla	Evaluación
Política 1	Usuario donde (Estado = MA)	OnChange
Política 2	Usuario donde (Estado = DC)	Siempre

La política 1 se evalúa cada vez que un administrador invoca la tarea ModifyUser para cambiar el atributo de estado y se evalúa como verdadera si el valor MA se agrega o se quita del atributo de estado.

La política 2 se evalúa cada vez que el administrador invoca la tarea Modificar usuario para un usuario cuyo estado contenga el valor DC.

Atributos marcados como cambiados en las pantallas de aprobación del flujo de trabajo

En una pantalla de aprobación, los atributos adicionales pueden parecer marcados como cambiados aunque un administrador no los cambiara en la tarea original. Esto es porque la pantalla puede contener scripts que pueden cambiar los valores de diversos atributos contenidos en la pantalla como parte de la inicialización de la pantalla o validación de la pantalla para cambiar algún otro atributo.

Ejemplos de políticas

En los siguientes ejemplos de casos empresariales se demuestra cómo se pueden aplicar las políticas de aprobación de flujo de trabajo para un evento:

Ejemplo 1:

Caso: un administrador modifica la cuenta de una base de datos relacional perteneciente a un empleado.

Tarea de administración: ModifyMSSQLAccount

Evento: ModifyMSSQLAccountEvent

Regla de aprobación: usuario donde (Título = RDBAcctManager)

Proceso de flujo de trabajo: ModAcctApproval (proceso de flujo de trabajo personalizado)

Objeto: Iniciador de la tarea

Evaluación: Evaluar siempre la regla

Ejemplo 2:

Caso: un administrador modifica el salario de un empleado para que refleje un nuevo aumento.

Tarea de administración: Modificar usuario

Evento: ModifyUserEvent

Regla de aprobación: usuario donde (Salario >= 100000)

Proceso de flujo de trabajo: SalaryChangeApproval (proceso de flujo de trabajo personalizado)

Objeto: objeto primario del evento (usuario)

Evaluación: evaluar sólo cuando cambie el atributo Salario

Ejemplo 3:

Caso: un administrador agrega un usuario al grupo Contratistas cuando el título del usuario cambia a Contratista. Este ejemplo se puede dividir en las dos políticas de aprobación siguientes:

Política 1:

Tarea de administración: Modificar usuario

Evento: ModifyUserEvent

Regla de aprobación: usuario donde (Título = Contratista)

Proceso de flujo de trabajo: SingleStepApproval (plantilla de proceso predeterminada)

Objeto: objeto primario del evento (usuario)

Evaluación: evaluar sólo cuando cambie el atributo Título

Política 2:

Tarea de administración: Modificar grupo (o Modificar miembros del grupo)

Evento: AddToGroup

Regla de aprobación: grupo donde (Nombre de grupo = Contratistas)

Proceso de flujo de trabajo: SingleStepApproval (plantilla de proceso predeterminada)

Objeto: Objeto secundario del evento (grupo)

Evaluación: Evaluar siempre la regla

En los siguientes ejemplos de casos se demuestra cómo se pueden aplicar las políticas de aprobación de flujo de trabajo para una tarea:

Ejemplo 1:

Caso: un administrador modifica la cuenta de Active Directory perteneciente a un empleado.

Tarea de administración: ModifyActiveDirectoryAccount

Objeto: Iniciador de la tarea

Regla de aprobación: usuario donde (Título = ActiveDirectoryManager)

Proceso de flujo de trabajo: aprobación en un único paso

Evaluación: Evaluar siempre la regla

Ejemplo 2:

Caso: un administrador modifica un usuario cuyo código de empleado es HighSecurity.

Tarea de administración: Modificar usuario

Objeto: Objeto primario de la tarea

Regla de aprobación: usuario donde (númeroempleado = HighSecurity)

Proceso de flujo de trabajo: aprobación en un único paso

Evaluación: Evaluar siempre la regla

Ejemplo 3:

Caso: un administrador modifica un usuario para asignar los roles de administrador CheckApprover y CheckSigner.

Tarea de administración: Modificar usuario

Objeto: Infracción de la política de identidad

Regla de aprobación: IdentityPolicy donde (Nombre = CheckRoles)

Proceso de flujo de trabajo: aprobación en un único paso

Evaluación: Evaluar siempre la regla

Cómo configurar el flujo de trabajo basado en políticas para los eventos

El procedimiento para configurar el flujo de trabajo basado en políticas es parecido al que se utiliza para configurar el flujo de trabajo del nivel de eventos, con los pasos adicionales necesarios para definir las políticas de aprobación que determinan si se ejecuta el flujo de trabajo.

Para configurar el flujo de trabajo basado en políticas

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración, Modificar (o Crear) la tarea de administración.

   Aparecerá la pantalla Seleccionar tarea de administración.

2. Busque la tarea que desee establecer bajo el control del flujo de trabajo y haga clic en Seleccionar.

   Aparecerá la pantalla Modificar (o Crear) la tarea de administración.

3. En la ficha Perfil, compruebe que esté seleccionado Activar Flujo de trabajo.

4. En la ficha Eventos, seleccione un evento para asignar a una plantilla de proceso.

   Aparecerá la pantalla de asignación del flujo de trabajo.

5. Seleccione el botón de opción Basado en una política y haga clic en Agregar.

   Aparecerá la pantalla Política de aprobación.

6. Configure una política de aprobación (en la página 341).

7. Configure los resolvedores de los participantes como lo requiera el proceso de flujo de trabajo seleccionado.

   Las solicitudes de participantes se agregarán al proceso.

8. Haga clic en OK.

   CA Identity Manager guardará la configuración del flujo de trabajo del nivel de evento.

9. Haga clic en Enviar.

   CA Identity Manager procesa la modificación de la tarea.

Nota: La lista de procesos del flujo de trabajo incluye procesos para utilizarse con el método de la plantilla y con el método de WorkPoint:

- Cuando se selecciona un proceso con el método con plantilla (SingleStepApproval o TwoStageApprovalProcess), la página se expandirá para permitir la configuración del resolvedor de participantes.
- Cuando se selecciona un proceso con el método de WorkPoint, la página no se expandirá. Los resolvedores de participantes se configuran en el Diseñador del punto de trabajo.

Más información:

Resolvedores del participante: Método de Workpoint (en la página 304)
Cómo configurar una política de aprobación (en la página 341)

Cómo configurar el flujo de trabajo basado en políticas para tareas

El procedimiento para configurar el flujo de trabajo basado en políticas es parecido al que se utiliza para configurar el flujo de trabajo del nivel de eventos, con los pasos adicionales necesarios para definir las políticas de aprobación que determinan si se ejecuta el flujo de trabajo.

Para configurar el flujo de trabajo basado en políticas

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración, Modificar (o Crear) la tarea de administración.

   Aparecerá la pantalla Seleccionar tarea de administración.

2. Busque la tarea que desee establecer bajo el control del flujo de trabajo y haga clic en Seleccionar.

   Aparecerá la pantalla Modificar (o Crear) la tarea de administración.

3. En la ficha Perfil, compruebe que esté seleccionado Activar Flujo de trabajo.
4. En la ficha Perfil, haga clic en el icono del lápiz junto al campo Proceso de flujo de trabajo.

   Aparecerá la pantalla de asignación del flujo de trabajo.

5. Seleccione el botón de opción Basado en una política y haga clic en Agregar.

   Aparecerá la pantalla Política de aprobación.

6. Configure una política de aprobación (en la página 341).
7. Configure los resolvedores de los participantes como lo requiera el proceso de flujo de trabajo seleccionado.

   Las solicitudes de participantes se agregarán al proceso.

8. Haga clic en OK.

   CA Identity Manager guardará la configuración del flujo de trabajo del nivel de tarea.

9. Haga clic en Enviar.

   CA Identity Manager procesa la modificación de la tarea.

Nota: La lista Proceso de flujo de trabajo incluye procesos que usar con el método de plantilla para el flujo de trabajo basado en políticas en el nivel de tarea:

- Cuando se selecciona un proceso con el método con plantilla (SingleStepApproval o TwoStageApprovalProcess), la página se expandirá para permitir la configuración del resolvedor de participantes.

Más información

Cómo configurar una política de aprobación (en la página 341)

Cómo configurar una política de aprobación

La configuración de una política de aprobación para un evento o tarea implica los pasos siguientes.

1. Seleccione el objeto que se vaya a probar.
2. Defina una regla de aprobación para el objeto.
3. Para los objetos primarios, decida si es una evaluación condicional.
4. Especifique el orden de evaluación de la política.
5. Configure un proceso de flujo de trabajo para ejecutarlo si la regla es verdadera.

Para configurar una política de aprobación

1. En la pantalla Política de aprobación, seleccione un objeto para la regla que vaya a probar de la lista desplegable.

   La pantalla cambia para reflejar su selección.
2. En la nueva lista desplegable situada junto al nombre del objeto, seleccione una plantilla de expresión de condición.

   La pantalla cambia para reflejar su selección.
3. Cree y edite la expresión de condición necesaria.
4. Seleccione el botón de opción Evaluación de reglas para indicar si la regla se debe evaluar siempre o solamente si cambia un atributo de la condición de aprobación.
5. Introduzca un valor entero positivo para especificar el orden de evaluación de las políticas (en el caso de que haya varias políticas para el evento).
6. Seleccione y configure el proceso de flujo de trabajo que se ejecutará cuando la regla se evalúe como verdadera.
7. Haga clic en Aceptar para guardar la política de aprobación.

Más información:

Configuración del flujo de trabajo a nivel de evento (en la página 278)
Cómo configurar el flujo de trabajo basado en políticas para los eventos (en la página 338)
Cómo configurar el flujo de trabajo basado en políticas para tareas (en la página 340)

Flujo de trabajo basado en políticas

Los administradores de CA Identity Manager pueden mostrar el estado de las tareas que contiene políticas de aprobación de flujo de trabajo mediante el uso de las siguientes herramientas estándar del sistema:

- Ficha Ver tareas enviadas
- Ficha Historial del usuario
- Informes y registros

La información de la tarea enviada y el historial de tareas incluyen lo siguiente:

- Información de la tarea y el evento
- Información de la regla de flujo de trabajo y aprobación
- Resultados de la evaluación de las reglas de aprobación

Para obtener descripciones del historial de tareas enviadas, consulte la documentación de la ficha Sistema.

Más información:

Descripción del estado del evento (en la página 594)
Estado de la tarea en CA Identity Manager (en la página 587)

Asignación de flujo de trabajo basado en políticas en el nivel de evento global

Se puede asignar un evento a un proceso de flujo de trabajo desde la Consola de gestión o se puede asociar con políticas de aprobación de flujo de trabajo basado en políticas en una tarea concreta. La nueva tarea Configurar una política global basada en flujo de trabajo para eventos permite que los administradores configuren la asignación de flujo de trabajo basada en políticas para eventos en el nivel de entorno. A diferencia de configurar el flujo de trabajo basado en políticas para un evento en una tarea de administración, las asignaciones configuradas de flujo de trabajo basado en políticas se aplican a todas las tareas que generan el evento.

Nota: La tarea Configurar una política global basada en flujo de trabajo para eventos sólo funciona cuando se activa el flujo de trabajo. Ejecutar esta tarea cuando el flujo de trabajo está desactivado produce un error.

Esta tarea se ha agregado a la ficha Sistema. Cuando se envía una tarea, el proceso de flujo de trabajo de cada evento en esta tarea se recupera de la siguiente manera:

Cualquier flujo de trabajo configurado para el evento para esa tarea de administración va por delante. Se puede configurar un evento para el flujo de trabajo basado en políticas o que se basa en ellas. Si se configura un flujo de trabajo basado en políticas para el evento correspondiente a esa tarea de administración, se invocará el proceso de flujo de trabajo asociado con la política. Si no coincide con ninguna regla, no se invocará ningún flujo de trabajo para el evento. De igual forma, si se configura un flujo de trabajo no basado en políticas para el evento correspondiente a esa tarea de administración, se invocará el proceso de flujo de trabajo asociado con la política. Si no se configuró ningún flujo de trabajo para el evento de esa tarea de administración, la configuración global del flujo de trabajo para ese evento tiene prioridad.

Pantalla de la tarea Configurar una política global basada en flujo de trabajo para eventos

Las tareas Configurar una política global basada en flujo de trabajo para eventos permite que un administrador configure flujos de trabajo que se basan en política o no para todos los eventos en el entorno actual. Al hacer clic en la tarea se muestra la asignación de eventos predeterminada para las definiciones de proceso de flujo de trabajo. Se puede modificar o suprimir cada asignación de eventos, y se pueden agregar nuevas asignaciones de eventos para los que no se hayan configurado.

Los campos de esta pantalla son los siguientes:

Procesos de flujo de trabajo asociados con los eventos de este entorno.

Especifica los procesos de flujo de trabajo asociados con las políticas de aprobación.

Agregar nuevas asignaciones

Especifica una política de aprobación que asignar a un proceso de flujo de trabajo.

Botón Agregar

Agrega la nueva asignación.

Agregar o modificar una asignación abre la pantalla de asignación de flujo de trabajo donde puede seleccionar las asignaciones de proceso y las políticas de aprobación. El comportamiento es el mismo que la configuración de flujo de trabajo del nivel de evento. Si hace clic en el botón Agregar en la página de asignaciones de flujo de trabajo, lleva a otra página en la que puede configurar una política de aprobación.

Más información

Cómo configurar el flujo de trabajo basado en políticas para los eventos (en la página 338)
Cómo configurar una política de aprobación (en la página 341)

Configuración de una política global basada en flujo de trabajo para eventos

Configure esta ficha para el flujo de trabajo global que se basa en la política para eventos.

Nombre

Un nombre que asigna a la ficha.

Etiqueta

Un identificador de la ficha que es único dentro de esta tarea. Debe comenzar con una letra o guión bajo, y contener sólo letras, números o guiones bajos. La etiqueta se utiliza fundamentalmente para configurar valores de datos a través de documentos XML o parámetros de HTTP.

Ocultar ficha

Impide que se vea la ficha en la tarea. Esta opción es útil para aplicaciones que necesitan ocultar la ficha, pero que siguen teniendo acceso a los atributos que ella contiene.

Pantalla de búsqueda de usuarios

Define la pantalla de búsqueda que se utiliza para mostrar usuarios.

Pantalla de lista de usuarios

Define la pantalla que determina las columnas y el orden de la ficha.

Pantalla de búsqueda de grupos

Define la pantalla de búsqueda que se utiliza para mostrar los grupos.

Pantalla de lista de grupos

Define la pantalla que determina las columnas y el orden de la ficha.

Pantalla de búsqueda de roles de administrador

Define la pantalla de búsqueda que se debe usar para mostrar los roles de administrador.

Pantalla de lista de roles de administrador

Define la pantalla que determina las columnas y el orden de la ficha.

Pantalla de búsqueda de tareas de administrador

Define la pantalla de búsqueda que se debe usar para mostrar las tareas de administración.

Pantalla de lista de tareas de administración

Define la pantalla que determina las columnas y el orden de la ficha.

Solicitudes en línea

CA Identity Manager permite crear las tareas de solicitudes en línea para fines generales. La implementación de solicitudes en línea predeterminada consta de una serie de tareas relacionadas tanto para solicitudes de automodificación como para solicitudes de modificación del usuario administrativo. Sin embargo, la función de solicitud en línea podría implementarse fácilmente para otras tareas de solicitud de CA Identity Manager.

Una solicitud de modificación de usuario activa un proceso de flujo de trabajo que genera un elemento de trabajo. Los participantes del flujo de trabajo pueden aprobar e implementar el elemento, o bien rechazarlo. El usuario que inicia la tarea introduce una descripción de la solicitud en el editor del historial. Se trata de un área de texto que utiliza CA Identity Manager para mantener un historial de la solicitud. Este editor de historial se puede configurar para permitir que los participantes dejen comentarios sobre la acción que realizan en el elemento de trabajo. Estos comentarios formarán parte del historial acumulativo del elemento de trabajo.

También es posible realizar otras acciones además de (o en lugar de) las estándar de aprobación y rechazo. Por ejemplo, un participante del negocio puede aclarar o realizar un comentario sobre la solicitud, y un participante del área técnica puede implementarla. Estas actividades nuevas se pueden representar con botones de acción de flujo de trabajo nuevos como “Aclarar” e “Implementar” que puede agregar a los botones "Aprobar" y “Rechazar” estándar en la tarea de aprobación.

Tareas de solicitud en línea

Son cinco las tareas que funcionan conjuntamente para conformar la implementación de las solicitudes en línea predeterminadas. Estas tareas demuestran el uso de solicitudes personalizadas, historial y botones de acción del flujo de trabajo:

Nota: Las tareas de administración (Cambiar Mi cuenta y Crear solicitud en línea) se configuran de forma predeterminada para el flujo de trabajo a nivel de evento mediante la plantilla Proceso de consulta.

Cambiar Mi cuenta

Se trata de una tarea de administración de automodificación que crea una solicitud de cambio de cuenta de usuario. Incluye una ficha Solicitud con un editor de historial para describir la solicitud, y una ficha Perfil con detalles del usuario de solo lectura.

Crear solicitud en línea

Se trata de una tarea de administración de modificación de usuario que crea una solicitud de cambio de cuenta para un usuario en particular. Incluye una ficha Solicitud con un editor de historial para describir la solicitud, y una ficha Perfil de asunto con detalles del usuario de solo lectura.

Aprobar solicitud en línea

Se trata de una tarea de aprobación que permite al participante del negocio aprobar o rechazar la tarea, o solicitar más detalles al respecto. Incluye una ficha Solicitud con una visualización del historial y un editor de historia para consultas o comentarios, una ficha Perfil de asunto de solo lectura y una ficha Asignatarios.

Aclarar solicitud en línea

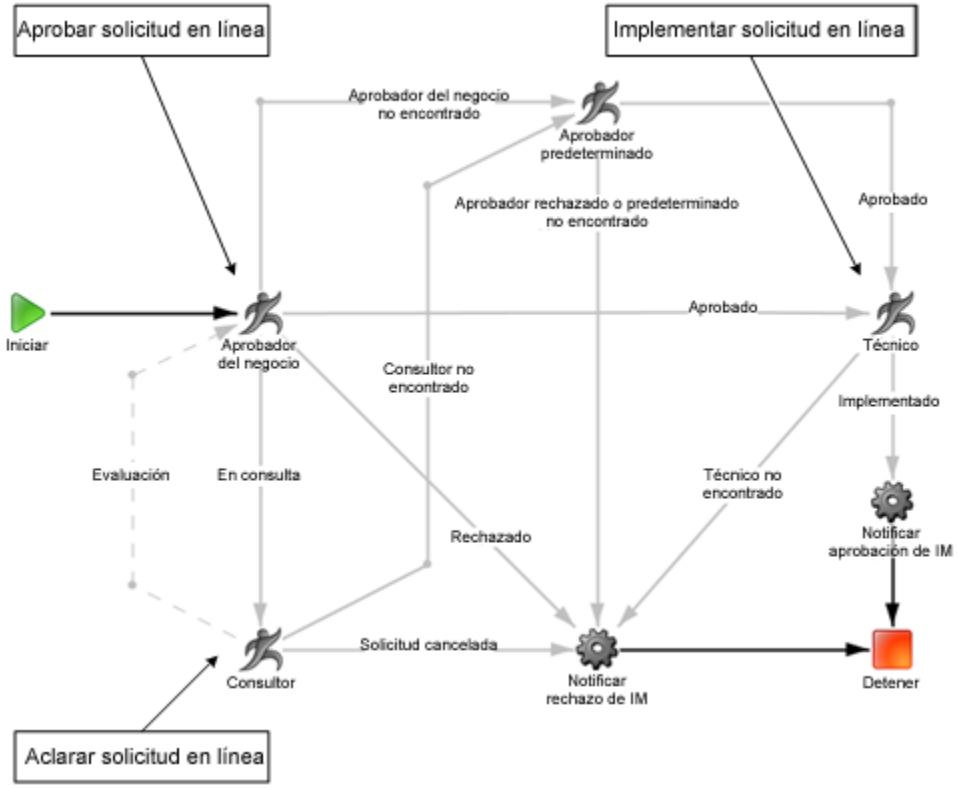
Se trata de una tarea de aprobación que permite al participante que realiza la aclaración responder a una solicitud de este tipo y devolver la tarea al participante del negocio para su aprobación. Incluye una ficha Solicitud con una visualización del historial y un editor de historial para comentarios, y una ficha Perfil de asunto de sólo lectura.

Implementar solicitud en línea

Se trata de una tarea de aprobación que permite al participante del área técnica implementar la tarea y agregar un comentario al historial. Incluye una ficha Implementar solicitud con una visualización del historial y un editor de historial para comentarios, una ficha Perfil de asunto de sólo lectura y una ficha Asignatarios.

Proceso de solicitud en línea

Las tareas de solicitud en línea están controladas por la plantilla del proceso de flujo de trabajo denominada Proceso de consulta. Así es como aparece en el Diseñador del punto de trabajo:



Esta plantilla incluye cuatro actividades manuales que corresponden a las tareas de aprobación en la implementación de solicitud en línea:

- Una actividad para el aprobador del negocio, que rechaza el elemento de trabajo, lo aprueba y lo transmite al técnico o solicita más aclaraciones al consultor.
- Una actividad para el consultor, que aclara el elemento de trabajo y lo devuelve al aprobador del negocio.
- Una actividad para el aprobador predeterminado, que asume el control si no se puede entrar en contacto con el aprobador del negocio ni con el consultor.
- Una actividad para el técnico, que implementa la solicitud y finaliza el elemento de trabajo.

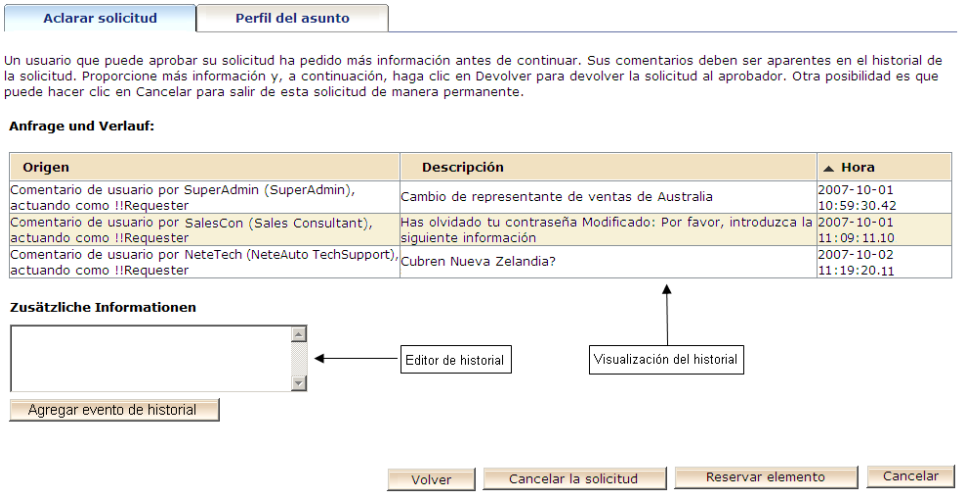
Historial de solicitud en línea

La función Historial de solicitud en línea permite a los participantes crear un registro de las acciones de elemento de trabajo. Puesto que la responsabilidad sobre el elemento de trabajo pasa de un participante a otro, el nuevo participante puede revisar el historial antes de tomar una acción.

Para implementar el historial de solicitud en línea se utilizan dos controles:

- La visualización del historial es una tabla de sólo lectura que contiene detalles sobre entradas anteriores por orden cronológico.
- El editor de historial es un cuadro de texto para crear entradas nuevas en el historial. También incluye un botón opcional para agregar varias entradas sin necesidad de enviar el elemento de trabajo.

De forma predeterminada, el editor y la visualización del historial aparecen en las fichas Solicitud de todas las tareas asociadas con la implementación de la solicitud en línea. La siguiente pantalla ilustra los controles de historial de la tarea Aclarar solicitud en línea:



Uso de solicitudes en línea

Los siguientes pasos describen el proceso de flujo de trabajo de solicitudes en línea. La tarea generada por IM en cada paso aparece entre paréntesis. En cada paso del proceso, el participante puede agregar un comentario en el editor de historial. El siguiente participante en el proceso de flujo de trabajo podrá ver este comentario en la visualización del historial.

1. El iniciador de la tarea solicita una modificación a un usuario de IM (Crear solicitud en línea).
2. El aprobador del negocio recibe el elemento de trabajo y realiza una de las siguientes acciones:
   - Aprueba el elemento de trabajo (Aprobar solicitud en línea).
   - Rechaza el elemento de trabajo y termina el proceso de flujo de trabajo. No se genera ninguna otra tarea.
   - Solicita una aclaración al consultor (Aclarar solicitud en línea).
3. El consultor recibe el elemento de trabajo y realiza una de las siguientes acciones:
   - Agrega una aclaración y devuelve el elemento de trabajo al aprobador del negocio. No se genera ninguna otra tarea.
   - Cancela el elemento de trabajo y termina el proceso de flujo de trabajo. No se genera ninguna otra tarea.
4. El técnico recibe un elemento de trabajo e implementa la solicitud (Implementar solicitud en línea).

Botones de acción del flujo de trabajo

Las tareas de aprobación en CA Identity Manager siempre han dispuesto de los botones de acción Aprobar y Rechazar que aparecen en las pantallas del elemento de trabajo correspondientes. Los botones de acción del flujo de trabajo permiten a los administradores ampliar la funcionalidad de tareas de CA Identity Manager y los flujos de trabajo mediante la adición de los botones de acción a las tareas de aprobación y eliminando o modificando los botones existentes. (Los botones estándares Aprobar y Rechazar se implementan del mismo modo que los botones de acción del flujo de trabajo personalizados).

Por ejemplo, un proceso de flujo de trabajo podría requerir una acción que permite que los participantes de medio nivel escalen ciertos casos a un participante sénior para la aprobación o el rechazo final. Estos participantes de nivel intermedio podrían agregar un comentario o recomendación mediante el editor de historial y, a continuación, enviar el elemento de trabajo al participante sénior para revisarlo y aprobarlo o rechazarlo.

La adición o eliminación de los botones de acción del flujo de trabajo requiere unos cambios adecuados en el proceso de flujo de trabajo de Workpoint para proporcionar la lógica de negocio y gestionar estas nuevas acciones.

Más información:

Configuración del botón en CA Identity Manager (en la página 351)
Botones de flujo de trabajo en tareas de aprobación (en la página 351)
Configuración de botones en el Diseñador de Workpoint (en la página 354)

Botones de flujo de trabajo en tareas de aprobación

Los botones de acción de flujo de trabajo corresponden a nodos de transición que salen de los nodos de actividad manual en un diagrama de proceso de Workpoint. Por ejemplo, en el Proceso de consulta, el nodo de actividad del técnico tiene una sola transición denominada Implementado. Esta transición se corresponde al botón "Implementado" de la tarea de aprobación Implementar solicitud en línea, que se muestra en la figura siguiente:

Nota: Los botones "Reservar elemento" y "Cerrar" se rigen por la lógica de programación de CA Identity Manager y no están bajo el control del flujo de trabajo.

Más información:

Botones de acción del flujo de trabajo (en la página 350)
Configuración del botón en CA Identity Manager (en la página 351)

Configuración del botón en CA Identity Manager

Para configurar un botón de acción de flujo de trabajo, haga clic en el botón denominado Botones de acción del flujo de trabajo en la ficha Perfil de una tarea de aprobación.

La ficha Perfil del botón incluye una tabla con una fila para cada botón de acción del flujo de trabajo. Cada fila de botones incluye estas cuatro propiedades, que corresponden a las columnas de la tabla:

Nombre para mostrar

El nombre que aparece en el botón de la pantalla de aprobación. Se trata de un valor localizado de forma condicional y puede ser una cadena o una clave de una cadena localizada en un archivo de recurso.

Acción

El valor retransmitido al proceso de flujo de trabajo cuando se selecciona una opción. Este valor es un atributo del nodo de transición correspondiente en el diagrama de proceso de Workpoint. El valor es una cadena no localizada. Los valores predeterminados son "aprobado" y “rechazado”.

Sugerencia

Una descripción breve (o sugerencia) de la acción del botón que aparece cuando un usuario desplaza el cursor sobre el botón. Se trata de un valor localizado de forma condicional y puede ser una cadena o una clave de una cadena localizada en un archivo de recurso.

Descripción larga

Una descripción más larga de la acción del botón que agrega un mensaje que describe la acción en la pantalla "Ver tareas enviadas". Si la descripción está vacía, el mensaje que se muestra en la pantalla Ver tareas enviadas es el nombre del botón. Se trata de un valor localizado de forma condicional y puede ser una cadena o una clave de una cadena localizada en un archivo de recurso.

Más información:

Configuración de botones en el Diseñador de Workpoint (en la página 354)

Cómo agregar botones de acción de flujo de trabajo

Para agregar un botón nuevo a un proceso de flujo de trabajo existente, realice los siguientes pasos avanzados:

1. Agregue un botón de flujo de trabajo en Identity Manager.

   Para obtener instrucciones, consulte Cómo agregar un botón de acción de flujo de trabajo (en la página 353).

2. Si fuera necesario, agregue claves de localización.

   Para obtener instrucciones, consulte la *Guía de configuración*.

3. Agregue los nodos requeridos en el Diseñador del punto de trabajo.

   Para obtener instrucciones, consulte la ayuda en línea del Diseñador del punto de trabajo.

4. Defina una secuencia de comandos en el nodo de transición del Diseñador del punto de trabajo.

   Para obtener instrucciones, consulte Configuración de botones en el Diseñador del punto de trabajo (en la página 354).

Más información:

Configuración de botones en el Diseñador de Workpoint (en la página 354)
Cómo agregar un botón de acción de flujo de trabajo (en la página 353)

Cómo agregar un botón de acción de flujo de trabajo

Se pueden agregar botones de acción de flujo de trabajo a tareas de aprobación en CA Identity Manager.

Para agregar un botón de acción de flujo de trabajo a una tarea de administración

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Modificar la tarea de administración.

   Aparece la pantalla Seleccionar tarea de administración.

2. Busque la tarea de aprobación y haga clic en Seleccionar.

   Aparece la pantalla Modificar la tarea de administración.

3. En la ficha Perfil, haga clic en el botón llamado Botones de acción del flujo de trabajo.

   Aparece la ficha de perfil del botón de acción de flujo de trabajo.

4. Haga clic en "Agregar botón" para agregar un botón nuevo a la tarea de aprobación.

5. Introduzca la información de propiedad del botón.

6. Haga clic en OK.

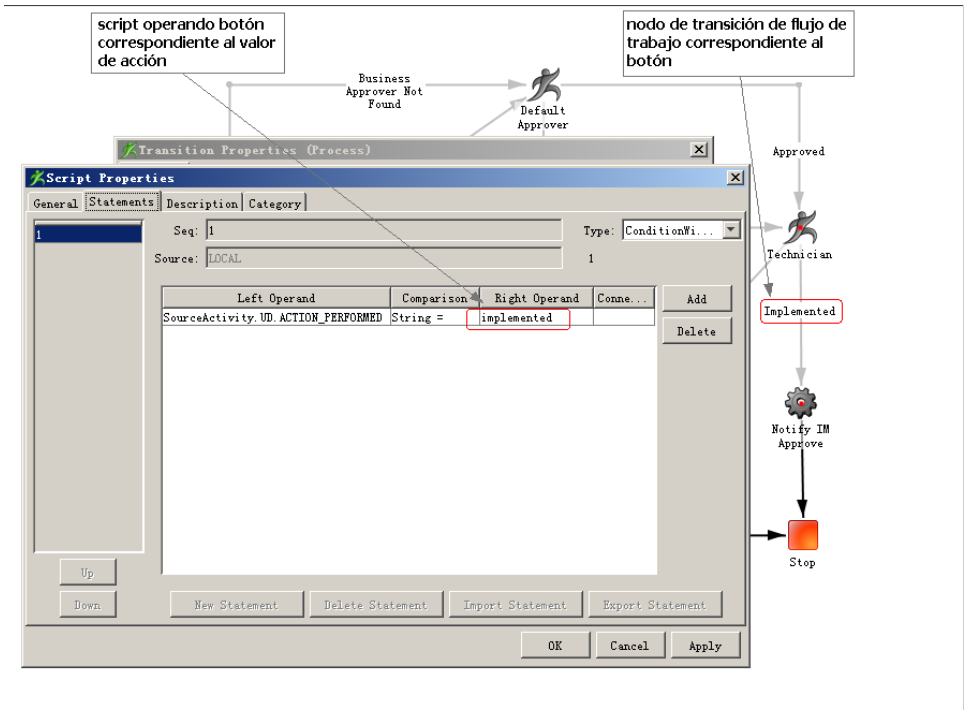
   CA Identity Manager guarda la información del botón nuevo.

7. Haga clic en Enviar.

   CA Identity Manager procesa la modificación de la tarea.

Configuración de botones en el Diseñador de Workpoint

En el Diseñador de Workpoint, los botones de acción de flujo de trabajo se configuran mediante las propiedades de la secuencia de comandos del nodo de transición, como se muestra en la figura siguiente:



De forma predeterminada, los botones de acción de flujo de trabajo usan las siguientes propiedades de secuencia de comandos para realizar una comparación de cadenas:

- Operando izquierdo: ACTION_PEFORMED, que se define en las propiedades Datos de usuario del nodo de actividad manual precedente.
- Operando derecho: el valor Acción del botón, que se define en la ficha de perfil del botón de la Consola de usuario.

Nota: Consulte la ayuda en línea del Diseñador de Workpoint para obtener información sobre las secuencias de comando y las propiedades del nodo de actividad y de transición.

Más información:

Configuración del botón en CA Identity Manager (en la página 351)

Listas y elementos de trabajo

Una *lista de trabajo* es una lista de elementos de trabajo (o tareas de aprobación) que aparece en la Consola de usuario del participante autorizado para aprobar la tarea. Los elementos de trabajo corresponden a las actividades manuales de un proceso de flujo de trabajo. Los elementos de trabajo están representados como filas en la lista de trabajo.

Es posible agregar los elementos de trabajo a una lista de estas formas:

- Un resolvedor del participante que determine una lista de aprobadores.
- La recepción de elementos de trabajo delegados de otro usuario.
- La reasignación a otro usuario.

Es posible eliminar elementos de trabajo de una lista de estas formas:

- La finalización (aprobación o rechazo) del elemento de trabajo.
- La reasignación a otro usuario.
- La reserva. Al reservar elementos de trabajo, se eliminan de la lista de trabajo de todos los participantes.

Nota: Cuando acepta o rechaza elementos de trabajo, el cambio no es inmediato. Por ejemplo, si rechaza un elemento de trabajo, el elemento seguirá apareciendo en la lista de trabajo hasta que el proceso de flujo de trabajo registre la información y avance el proceso al nodo siguiente.

Las fichas de información que aparecen en un elemento de trabajo varían en función de qué elemento haya generado un flujo de trabajo bajo control de tareas o de eventos:

- **Perfil:** ofrece información de perfil sobre el objeto afectado por el evento (sólo a nivel de evento).
- **Detalles de tarea**: ofrece información detallada de todos los eventos de la tarea (sólo a nivel de tarea).
- **Aprobadores:** detalla todos los aprobadores y delegadores individuales para la tarea o evento (a nivel de tarea y evento)

Visualización de una lista de trabajo

La lista de trabajo aparece automáticamente cuando se inicia sesión en la Consola de usuario, si ha sido asignado como participante para aprobar tareas (o elementos de trabajo) que hayan iniciado otros usuarios.

Para mostrar la lista de trabajo manualmente

1. En la Consola de usuario, seleccione Principal, Ver Mi lista de trabajo.

   Aparece la lista de trabajo.

2. Haga clic en el nombre de un elemento de trabajo para mostrarlo.

   Aparece el elemento de trabajo seleccionado.

Los administradores pueden gestionar elementos de trabajo de los usuarios dentro de su ámbito.

Nota: El hecho de gestionar los elementos de trabajo de un usuario permite a los administradores reservar uno de estos elementos. La visualización de la lista de trabajo de un usuario no permite cambios de ningún tipo en el elemento de trabajo.

Para ver la lista de trabajo de otro usuario

1. En la Consola de usuario, seleccione Usuarios, Gestionar elementos de trabajo, Ver la lista de trabajo del usuario.

   Aparece una pantalla de selección de usuarios.

2. Busque el usuario cuya lista de trabajo desea ver, y haga clic en Seleccionar.

   Se abre la lista de trabajo del usuario.

Para gestionar los elementos de trabajo de otro usuario

1. En la Consola de usuario, seleccione Usuarios, Gestionar elementos de trabajo, Gestionar elementos de trabajo del usuario.

   Aparece una pantalla de selección de usuarios.

2. Busque el usuario cuyos elementos de trabajo desea gestionar, y haga clic en Seleccionar.

   Se abre la lista de trabajo del usuario.

3. Haga clic en el nombre de un elemento de trabajo para mostrarlo.

   Aparece el elemento de trabajo seleccionado.

Reserva de elementos de trabajo

Puede reservar un elemento de trabajo para "revisarlo" y eliminarlo de la lista de trabajo de otros participantes. Al reservar un elemento de trabajo, queda retenido para el usuario que efectúa la reserva.

Si el usuario que lo reserva lo libera, vuelve a estar disponible en la lista de trabajo de otros participantes. Si el usuario que lo reserva lo aprueba o lo rechaza, queda completado y deja de estar disponible para otros participantes.

Más información:

Delegación y elementos de trabajo reservados (en la página 357)
Reasignación y elementos de trabajo reservados (en la página 357)

Reasignación y elementos de trabajo reservados

Si un usuario tiene un elemento de trabajo reservado mientras lo reasigna, lo mantiene como reservado. Pero si, a continuación, el usuario libera el elemento de trabajo, pierde el acceso a él.

Un administrador puede volver a asignar, reservar o liberar el elemento de trabajo de otro usuario, pero no puede aprobarlo ni rechazarlo. Sólo el participante ha quien se le ha asignado el elemento de trabajo puede hacerlo.

Más información:

Reasignación de elementos de trabajo (en la página 364)

Delegación y elementos de trabajo reservados

Mientras haya una delegación activa, el que la recibe o el que la delega pueden reservar un elemento de trabajo. Un elemento de trabajo reservado por un usuario no puede aparecer en la lista de trabajo de otro.

Por ejemplo, si un delegado tiene un elemento de trabajo reservado mientras se retira la delegación, éste lo mantiene como reservado. Pero si el delegado libera el elemento de trabajo, pierde el acceso a él.

Si un usuario que es delegado es suprimido mientras tiene un elemento de trabajo reservado, continúa reteniéndolo. Si, a continuación, el delegado aprueba el elemento de trabajo, la auditoría ya no puede determinar quién lo ha delegado.

Si un delegado tiene un elemento de trabajo reservado mientras se retira la delegación, retiene el acceso hasta que el elemento se haya completado o liberado.

Más información:

Delegación de elementos de trabajo (en la página 358)
Reserva de elementos de trabajo (en la página 357)

Cómo reservar o liberar un elemento de trabajo

Para "comprobar" y eliminar de la lista de trabajo de otro participante un elemento de trabajo, debe reservarlo.

Un elemento de trabajo reservado se libera para que quede disponible en la lista de trabajo de otros participantes.

Nota: El único modo de liberar un elemento de trabajo es liberarlo explícitamente.

Para reservar o liberar un elemento de trabajo

1. En la Consola de usuario, seleccione Principal, Ver Mi lista de trabajo.

   Aparece la lista de trabajo.

2. Seleccione el elemento de trabajo que desea reservar o liberar.

   Aparece la pantalla con el elemento de trabajo expandido.

3. Haga clic en Reservar elemento o Liberar elemento.

   CA Identity Manager confirmará su acción.

Delegación de elementos de trabajo

La *delegación* de elementos de trabajo permite a un usuario (el delegador) especificar que a otro usuario (el delegado) se le permita aprobar tareas de la lista de trabajo del primero. Un delegador puede asignar elementos de trabajo a otro aprobador cuando el primero esté "fuera de la oficina". Los delegadores mantienen acceso completo a los elementos de trabajo durante el período de delegación.

Los elementos de trabajo delegados no se modifican de ningún modo. El registro indica si un elemento de trabajo ha sido delegado.

La delegación implica que el delegado “toma el lugar” del delegador y visualiza los elementos de su lista de trabajo. Cuando se visualiza una lista de trabajo, los delegados ven sus propios elementos y los del delegador.

La delegación no tiene carácter transitivo. Un delegado sólo puede ver los elementos de trabajo que el delegador le ha asignado directamente. Por ejemplo, si el usuario A delega elementos de trabajo al usuario B, y el usuario B delega elementos de trabajo al usuario C, el usuario C sólo puede ver los elementos de trabajo que pertenecen al usuario B, y no aquellos elementos que podrían haber sido delegados al usuario B por parte del usuario A.

Más información:

Delegación y elementos de trabajo reservados (en la página 357)

Atributo conocido de delegación

La delegación emplea el siguiente atributo conocido:

%DELEGATORS%

Este atributo conocido almacena los nombres de los usuarios que delegan al usuario con el atributo, así como la hora en que se creó la delegación.

Cómo activar la delegación

Debe tener la delegación de aprobación de flujo de trabajo activada antes de poder delegar elementos de trabajo a otro usuario. De forma predeterminada, la función de delegación está desactivada.

Para activar la delegación de aprobación de flujo de trabajo

1. Abra la Consola de gestión de introduciendo la siguiente URL en un explorador:

   `http://hostname/iam/immanage`

   nombre de host

   Define el nombre de dominio completo del servidor en el que está instalado CA Identity Manager. Por ejemplo, miservidor.miempresa.com:puerto.

2. Haga clic en Entornos y seleccione el nombre del entorno de CA Identity Manager apropiado.
3. Haga clic en Configuración avanzada y, a continuación, en Delegación de aprobación de flujo de trabajo.
4. Seleccione la casilla de verificación Activado y haga clic en Guardar.

Más información:

Cómo delegar a sí mismo (en la página 360)
Cómo delegar a otro usuario (en la página 363)

Cómo delegar a sí mismo

Puede delegar elementos de trabajo a otro usuario en los períodos de "fuera de la oficina". Los delegadores mantienen el acceso completo a los elementos de trabajo durante el período de delegación.

Para delegar elementos de trabajo a sí mismo

1. En la Consola de usuario, seleccione Principal, Asistente Fuera de la oficina.

   Se abre la pantalla Asistente Fuera de la oficina.

2. Haga clic en Agregar usuario.

   Aparece una pantalla de selección de usuarios.

3. Busque y seleccione uno o más usuarios que actuarán como delegados.

   Los usuarios se agregan a la lista de delegados.

4. Haga clic en Enviar.

   Se envía la tarea y se guarda la delegación.

Nota: Los usuarios que ya son delegados no aparecen en los resultados de la búsqueda cuando agrega un delegado.

Más información:

Cómo activar la delegación (en la página 359)

Delegación del elemento de trabajo basado en el tiempo

En versiones anteriores, puede especificar la hora de inicio, pero no la hora de finalización para las delegaciones. Las delegaciones recién creadas tienen las fechas para la delegación definidas en verdaderas, con la hora de inicio predeterminada definida en ahora.

En el momento de la modificación, se pueden cambiar las fechas de inicio y fin. La hora de fin predeterminada es una semana contada a partir de la fecha de inicio.

Para cambiar las fechas de inicio y fin, haga lo siguiente:

1. En la ficha Principal de la Consola de usuario, seleccione Asistente Fuera de la oficina.
2. Haga clic en el icono del lápiz situado junto al ID de usuario cuya información de delegación desee cambiar.

   Aparece la pantalla Editar detalles de la delegación.
3. Haga clic en el calendario situado junto a la fecha de inicio para cambiar la fecha de inicio de la delegación.

   Nota: Aparecerá un mensaje de error cuando la fecha de inicio de delegación seleccionada sea antes de la fecha actual.
4. Si desea seleccionar una fecha final, marque la casilla de verificación Tiene fecha final.

   El campo Fecha de finalización está disponible ahora para definir la fecha de fin.
5. Haga clic en el calendario situado junto a Fecha de finalización para definir una fecha para que termine la delegación.
6. Una vez definidas las fechas, haga clic en Aceptar.

Por otra parte puede hacer lo mismo desde la ficha Delegar elementos de trabajo cuando se crea o se modifica un usuario.

Activación de la delegación del elemento de trabajo basado en el tiempo

Para activar la delegación del elemento de trabajo basada en tiempo en un entorno existente en una actualización, haga lo siguiente:

En la Consola de gestión

1. Diríjase a la página Entornos.
2. Desplácese dentro del entorno seleccionado, Advanced Settings (Configuración avanzada), Work Item Delegation (Delegación de elemento de trabajo).
3. Quite la selección de la casilla de verificación Activado.
4. Guarde los cambios y reinicie el entorno.
5. Desplácese dentro de la configuración avanzada, Work Item Delegation (Delegación de elemento de trabajo).
6. Marque la casilla de verificación Activado.
7. Guarde los cambios y reinicie el entorno.

Nota: Este procedimiento sólo es para entornos existentes. La delegación de elemento de flujo de trabajo basada en tiempo se activa para nuevos entornos.

Pantalla Asistente Fuera de la oficina

Deberá utilizar la siguiente pantalla del Asistente Fuera de la oficina para agregar y eliminar la delegación a sí mismo:

La pantalla Asistente Fuera de la oficina muestra un lista de los delegados actuales. Además de las columnas que identifican al delegado, se incluyen tres columnas adicionales:

Fecha de inicio

Muestra la fecha en que se ha creado la delegación.

Fecha de finalización

Muestra la fecha en que terminará la delegación.

Tiene delegados

Indica si el delegado ha delegado elementos de trabajo a otro usuario.

Cuando hace clic en el icono del lápiz junto al ID de usuario seleccionado, aparecerá la pantalla Editar detalles de la delegación, donde podrá cambiar la fecha de inicio y especificar la fecha de finalización para la delegación.

Cómo delegar a otro usuario

Los administradores pueden delegar elementos de trabajo de un usuario (el delegador) a otro. Por ejemplo, es posible que un usuario deba dejar la oficina de forma inesperada o que un administrador deba asignar una carga de trabajo voluminosa a varios usuarios.

Los administradores sólo pueden delegar elementos de trabajo a usuarios que se encuentren dentro de su ámbito. Del mismo modo, sólo pueden agregar a la lista de delegados o eliminarlos de la misma a usuarios que ellos mismos gestionan.

Para delegar elementos de trabajo a otro usuario

1. En la Consola de usuario, seleccione Usuarios, Gestionar elementos de trabajo, Delegar elementos de trabajo.

   Aparece una pantalla de selección de usuarios.

2. Busque el usuario cuyos elementos de trabajo desea delegar (el delegador), y haga clic en Seleccionar.

   Se abre una pantalla Delegar elementos de trabajo.

3. Haga clic en Agregar usuario.

   Aparece una pantalla de selección de usuarios.

4. Busque y seleccione uno o más usuarios que actuarán como delegados.

   Los usuarios se agregan a la lista de delegados.

5. Haga clic en Enviar.

   Se envía la tarea y se guarda la delegación.

Nota: Los usuarios que ya son delegados no aparecen en los resultados de la búsqueda cuando agrega un delegado.

Más información:

Cómo activar la delegación (en la página 359)

Cómo eliminar una delegación

Si un usuario inicia sesión en CA Identity Manager teniendo delegaciones activas, CA Identity Manager mostrará el siguiente recordatorio:

```
Tiene delegaciones vigentes. Verifique que todavía sean requeridas.
```

Para eliminar una delegación a sí mismo

1. En la Consola de usuario, seleccione Principal, Asistente Fuera de la oficina.

   Se abre la pantalla Asistente Fuera de la oficina.

2. Haga clic en el signo menos (-) de aquellos delegados que desea eliminar.

   Los delegados desaparecen de la lista.

3. Haga clic en Enviar.

   Se envía la tarea y se elimina la delegación.

Para eliminar una delegación de otro usuario

1. En la Consola de usuario, seleccione Usuarios, Gestionar elementos de trabajo, Delegar elementos de trabajo.

   Aparece una pantalla de búsqueda de usuarios.

2. Busque y seleccione el usuario cuyas delegaciones desea eliminar.

   Aparecerá la lista de delegados.

3. Haga clic en el signo menos (-) de aquellos delegados que desea eliminar.

   Los delegados desaparecen de la lista.

4. Haga clic en Enviar.

   Se envía la tarea y se elimina la delegación.

Nota: Sólo puede eliminar un delegado, si está dentro de su ámbito.

Reasignación de elementos de trabajo

La reasignación permite a los usuarios y a los administradores cambiar los asignatarios de un elemento de trabajo después de su creación. Un administrador puede:

- Ver la lista de trabajo de otro usuario
- Agregar asignatarios al elemento de trabajo y eliminarlos de ella
- Cambiar el estado de reserva de los elementos de trabajo

Por ejemplo, un administrador puede reasignar un elemento de trabajo o liberar uno que estuviera reservado desde un usuario que no esté trabajando en él.

Si un usuario tiene reservado un elemento de trabajo mientras se reasigna, el usuario lo mantiene reservado. Pero si el usuario lo publica, perderá la posibilidad de acceder a él.

Si un delegado tiene reservado un elemento de trabajo mientras se retira la delegación, el delegado conserva el acceso hasta que el elemento de trabajo se completa o se libera.

Más información:

Reasignación y elementos de trabajo reservados (en la página 357)

La ficha Aprobadores

Se realiza la reasignación en la ficha Aprobadores del elemento de trabajo, que muestra una lista de aprobadores del elemento de trabajo actual (o asignatarios). Cuando se realiza la reasignación, se asigna el elemento de trabajo abierto a todos los aprobadores de la lista. Por tanto, para volver a asignar un elemento de trabajo a un asignatario nuevo, se debe eliminar también el asignatario actual.

Cómo reasignar elementos de trabajo

Reasignar un elemento de trabajo de un usuario a otro es un proceso que consta de dos pasos:

- Seleccione un aprobador nuevo.
- Elimine el aprobador actual.

Nota: Los usuarios que va a reasignar deben estar dentro de su ámbito.

Para reasignar su propio elemento de trabajo

1. Seleccione Principal, Ver mi lista de trabajo.

   Aparece la lista de trabajo.

2. Seleccione un elemento de trabajo para expandirlo.
3. Seleccione la ficha Aprobadores.

   Se muestra la lista de todos los aprobadores actuales, incluido el usuario cuya lista de trabajo se está gestionando.

4. Haga clic en Agregar asignatarios.

   Aparece una pantalla de selección de usuarios.

5. Búsqueda y selección de uno o varios usuarios para reasignarlos.

   Nota: Para los modos de aprobación TODOS y SUBCONJUNTO, puede reasignar solo un elemento de trabajo a *un usuario.*

6. Haga clic en el botón del signo menos (-) para eliminarse como asignatario.
7. Haga clic en Realizar reasignación.

   El elemento de trabajo aparece en las listas de trabajo de los usuarios reasignados.

Nota: Un administrador puede reasignar, reservar o liberar un elemento de trabajo de otro usuario, pero no podrá aprobarlo ni rechazarlo. Solamente el propietario del elemento de trabajo puede hacerlo.

Para reasignar un elemento de trabajo de otro usuario

1. Seleccione Usuarios, Gestionar elementos de trabajo, Gestionar elementos de trabajo del usuario.

   Aparece una pantalla de selección de usuarios.

2. Busque el usuario cuyos elementos de trabajo desee reasignar y haga clic en Seleccionar.

   Se muestra la pantalla Gestionar elementos de trabajo del usuario.

3. Seleccione un elemento de trabajo para expandirlo.

4. Seleccione la ficha Aprobadores.

   Se muestra la lista de todos los aprobadores actuales, incluido el usuario cuya lista de trabajo se está gestionando.

5. Haga clic en Agregar asignatarios.

   Aparece una pantalla de selección de usuarios.

6. Búsqueda y selección de uno o varios usuarios para reasignarlos.

7. Haga clic en el botón del signo menos (-) para eliminar al asignatario actual.

8. Haga clic en Realizar reasignación.

   El elemento de trabajo aparece en las listas de trabajo de los usuarios reasignados.

Operaciones masivas en los elementos de trabajo

Con esta versión de CA Identity Manager, se pueden realizar las siguientes operaciones masivas en elementos de trabajo seleccionados:

- Aprobar
- Rechazar
- Reservar
- Liberar

En la Consola de usuario, se ha mejorado la ficha Configure Work List (Configurar lista de trabajo) para incluir la nueva casilla de verificación Es compatible con operaciones de flujo de trabajo masivo. Cuando esta casilla de verificación está activa, el usuario puede aprobar, rechazar, liberar y reservar de forma masiva los elementos de trabajo que posea o elementos de trabajo de los delegados. Los administradores pueden realizar solamente estas operaciones masivas en elementos de trabajo mediante la tarea Gestionar elementos de trabajo del usuario.

Nota: No se pueden activar operaciones masivas para ninguna tarea de tipo de vista, como por ejemplo Ver Mi lista de trabajo.

Configuración de la ficha Lista de trabajo para operaciones masivas

Para configurar la ficha Lista de trabajos para admitir operaciones masivas en los elementos de trabajo, siga este procedimiento.

En la ficha Roles y tareas de la Consola de usuario

1. Seleccione una de las siguientes opciones:
   - Roles y tareas.
   - Tareas, Roles y tareas.
2. Seleccione Tareas de administración, Gestionar tareas de administración.
3. Haga clic en Buscar.
4. Seleccione Gestionar elementos de trabajo del usuario.
5. En la ficha Fichas, haga clic en el icono del lápiz situado junto a Lista de trabajo.

   Aparece la pantalla de configuración de lista de trabajo.
6. Seleccione Es compatible con operaciones de flujo de trabajo masivo.
7. Guarde los cambios y envíe la tarea.

   Las operaciones masivas en elementos de trabajo están ahora disponibles.

Capítulo 13: Notificaciones de correo electrónico

Esta sección contiene los siguientes temas:

Notificaciones de correo electrónico en CA Identity Manager

Las notificaciones de correo electrónico informan a los usuarios de CA Identity Manager de las tareas y eventos en el sistema. Por ejemplo, CA Identity Manager puede enviar un correo electrónico a los aprobadores cuando un evento o tarea exija aprobación.

CA Identity Manager proporciona los siguientes métodos para configurar notificaciones de correo electrónico:

- **Políticas de notificación de correo electrónico**

  Las políticas de notificación de correo electrónico permiten que los administradores empresariales creen, vean, modifiquen y supriman notificaciones de correo electrónico usando tareas en la Consola de usuario. No se necesita codificación alguna para crear notificaciones de correo electrónico.

  Los administradores pueden definir el contenido de un correo electrónico, cuándo se envía y quién lo recibe. El contenido del correo electrónico, que se define en un editor de HTML, puede contener información dinámica; por ejemplo, la información de fechas o eventos actuales que CA Identity Manager rellena al enviar un correo electrónico. Por ejemplo, puede configurar una notificación de correo electrónico que se envía a un aprobador cuando se crea un nuevo usuario. El correo electrónico puede contener la información de inicio de sesión del usuario, la fecha de contratación y el gestor.

  Nota: Las políticas de notificaciones de correo electrónico son políticas de Política exprés (en la página 503) que se crean y gestionan en un conjunto independiente de tareas.

- **Plantillas de correo electrónico**

  Con este método, las notificaciones de correo electrónico se generan a partir de plantillas de correo electrónico. CA Identity Manager proporciona plantillas de correo electrónico predeterminadas que pueden utilizarse en cuanto se instalen, o bien que los administradores de sistema pueden personalizar. Estos administradores usan una API de plantilla de correo electrónico para especificar contenido dinámico, como la lista de destinatarios y la información sobre el evento que inicia el correo electrónico.

CA Identity Manager puede generar notificaciones de correo electrónico cuando ocurra lo siguiente:

- Está pendiente un evento que necesita aprobación o rechazo de un aprobador del flujo de trabajo.

  Nota: Si dispone de un proceso de aprobación de Workpoint con más de una actividad de aprobación, la notificación de correo electrónico configurada en las tareas de la Consola de usuario envía una notificación para cada actividad. Si usa las plantillas de correo electrónico para la misma notificación, sólo se envía un correo electrónico a los aprobadores (cuando el evento alcanza el estado pendiente).

- Un aprobador aprueba un evento o tarea.

- Un aprobador rechaza un evento o tarea.
- Un evento o tarea se inicia, falla o se completa.
- Se crea o se modifica un usuario.

Para utilizar las notificaciones de correo electrónico de CA Identity Manager, configure los valores de configuración de SMTP (en la página 372). Si está usando el método de plantilla de correo electrónico, también activará las notificaciones de correo electrónico en CA Identity Manager.

Cómo seleccionar un método de notificación de correo electrónico

En la siguiente tabla se resumen las diferencias entre políticas de notificaciones de correo electrónico y plantillas de correo electrónico:

Actividad	Tareas de gestión de correos electrónicos	Plantillas de correo electrónico
Configuración de notificaciones de correo electrónico	Los administradores utilizan tareas de administración en la Consola de usuario para crear, modificar, ver y suprimir notificaciones de correo electrónico.	Los administradores modifican plantillas predeterminadas en las herramientas administrativas de CA Identity Manager.
Configuración cuando se envían correos electrónicos	CA Identity Manager puede generar eventos de notificaciones de correo electrónico cuando se producen determinados eventos o tareas. Las tareas de gestión de correos electrónicos y las plantillas de correo electrónico son compatibles con los mismos eventos y tareas; sin embargo, las tareas de gestión de correos electrónicos proporcionan más detalles en algunos casos. Las notificaciones de correo electrónico son compatibles con los siguientes eventos y tareas: ■ Está pendiente un evento que necesita aprobación o rechazo de un aprobador del flujo de trabajo. ■ **Nota:** Si dispone de un proceso de aprobación de Workpoint con más de una actividad de aprobación, la notificación de correo electrónico configurada mediante las tareas de gestión de correos electrónicos envía una notificación para cada actividad. Si usa las plantillas de correo electrónico para la misma notificación, sólo se envía un correo electrónico a los aprobadores (cuando el evento alcanza el estado pendiente). ■ Un aprobador aprueba un evento o tarea. ■ Un aprobador rechaza un evento o tarea. ■ Un evento o tarea se inicia, falla o se completa. ■ Se crea o se modifica un usuario.	

Actividad	Tareas de gestión de correos electrónicos	Plantillas de correo electrónico
Adición de contenido dinámico a correos electrónicos	Los administradores agregan contenido dinámico al cuerpo de un mensaje de correo electrónico seleccionando en una lista de opciones de la ficha Contenido de las tareas creación o modificación de correos electrónicos. CA Identity Manager rellena automáticamente el contenido dinámico según la información en el evento o la tarea que activan la notificación.	Los administradores utilizan la API de plantilla de correo electrónico para personalizar las plantillas de correo electrónico predeterminadas, que se utilizan para generar notificaciones de correo electrónico.
Compatibilidad con las notificaciones de correo electrónico existentes	Las notificaciones de correo electrónico que se configuran mediante las tareas de gestión de correos electrónicos ser basan en las políticas de Política exprés. Si ha actualizado desde el paquete de opciones 1 de CA Identity Manager a CA Identity Manager 12.6.4, las notificaciones de correo electrónico que se han configurado en Política exprés seguirán funcionando. Sin embargo, gestione esas notificaciones de correo electrónico mediante las tareas de gestión de correos electrónicos, en lugar de Política exprés.	Las notificaciones de correo electrónico que se han creado utilizando el método de plantilla de correo electrónico en versiones anteriores de CA Identity Manager seguirán funcionando en CA Identity Manager 12.6.4.

Configuración de parámetros de SMTP

Antes de activar las notificaciones de correo electrónico, configure los parámetros de SMTP. Consulte las siguientes secciones para configurar los parámetros de SMTP para el servidor de aplicaciones.

Configuración de parámetros de SMTP en JBoss

1. En un editor de texto, abra el descriptor de implementación de servicio de correo electrónico tal y como se muestra a continuación:

   Nodo único: *jboss_home*\server\default\deploy\mail-service.xml

   Clúster: *jboss_home*\server\all\deploy\mail-service.xml

2. Modifique la propiedad mail.smtp.host con el nombre del servidor SMTP tal y como se muestra a continuación:

   ```
   <-- Change to the SMTP gateway server -->
   <property name="mail.smtp.host" value="your_smtp_server "/>
   ```

   Por ejemplo:

   ```
   <property name="mail.smtp.host" value="smtp.mailserver.company.com"/>
   ```

3. Guarde el archivo mail-service.xml.
4. En un editor de texto, abra el siguiente archivo de propiedades de correo electrónico:

   Nodo único:
   jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

   Clúster:*jboss_home*\server\all\farm\iam_im.ear\config\com\netegrity\config\email.properties
5. Para establecer la dirección del remitente del correo electrónico que se utilizará en el correo electrónico generado a partir del flujo de trabajo, busque la propiedad admin.email.address y establezca el valor de la dirección de correo electrónico adecuada. Por ejemplo:
   `admin.email.address=admin@company.com`
6. Si está utilizando el método de plantilla de correo electrónico, active también las notificaciones de correo electrónico en la Consola de gestión.

   No es necesario activar las notificaciones de correo electrónico en la Consola de gestión si se están utilizando políticas de notificaciones de correo electrónico.

Configuración de parámetros de SMTP en WebLogic

Configura los parámetros de correo electrónico en la Consola de administración de WebLogic Server y en el archivo email.properties.

Para configurar los parámetros de correo electrónico para Weblogic

1. En la Consola de administración de WebLogic Server, cree una sesión de correo con las siguientes propiedades:
   - propiedad **mail.smtp.host**. Establezca este valor en el servidor SMTP. Por ejemplo, mail.smtp.host=mymailserver.company.com
   - propiedad **mail.transport.protocol**. Establezca este valor en SMTP. Por ejemplo, mail.transport.protocol=smtp
   - **Nombre de JNDI**: nete/Mail
   - **Destino:** nombre del servidor de WebLogic.
2. En un editor de texto, abra el siguiente archivo de propiedades para CA Identity Manager:

   weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties

3. Establezca la dirección del remitente del correo electrónico que han los correos electrónicos generados a partir del flujo de trabajo buscando la propiedad admin.email.address y estableciendo el valor como la dirección de correo electrónico adecuada. Por ejemplo:
   `admin.email.address=admin@company.com`
4. Active la notificación de correo electrónico en la Consola de gestión.

   Nota: No es necesario activar las notificaciones de correo electrónico en la Consola de gestión si se están utilizando políticas de notificaciones de correo electrónico.

Configuración de parámetros de SMTP en WebSphere

La utilidad imsSetup, que se ejecuta después de haber instalado los componentes de CA Identity Manager, configura un objeto de sesión de correo nuevo denominado "mailMail".

Para que la característica de notificación de correo electrónico funcione correctamente, especifique que dicho servidor de WebSphere se conecte cuando se envíen correos electrónicos en el campo de host de transporte de correo para la sesión de mailMail.

La sesión de mailMail se encuentra en Recursos, Mail Providers (Proveedores de correo), Built-in Mail Provider (Proveedor de correo integrado), Mail Sessions (Sesiones de correo), mailMail en la consola de administración de WebSphere.

Nota: Para consultar el objeto mailMail, cambie el ámbito a Servidor en la pantalla de sesiones de correo. Si no se cambia el ámbito en el servidor, el objeto mailMail no se mostrará.

Para obtener más información sobre la configuración de proveedores de correo de WebSphere, consulte la documentación de WebSphere.

Si se está utilizando el método de plantilla de correo electrónico, active la notificación de correo electrónico en la Consola de gestión una vez que se hayan configurado los parámetros de configuración de SMTP.

Nota: No es necesario activar las notificaciones de correo electrónico en la Consola de gestión si se están utilizando políticas de notificaciones de correo electrónico.

Cómo crear políticas de notificación de correo electrónico

Puede usar la Consola de usuario para crear políticas de notificación de correo electrónico que envíen mensajes cuando sucedan acciones concretas. Por ejemplo, puede crear una política de notificación de correo electrónico que envíe un correo electrónico para notificar a los aprobadores sobre la creación de un nuevo usuario.

Siga estos pasos:

1. Seleccione Sistema, Correo electrónico, Crear correo electrónico.
2. Seleccione una de las opciones siguientes:
   - Crear un nuevo objeto del tipo Correo electrónico gestionado
   - Crear una copia de un objeto del tipo Correo electrónico gestionado

     Usa una política de notificación de correo existente como plantilla para crear una política.
3. Proporcione la información básica sobre la política de notificación de correo electrónico en la ficha Perfil.
4. Especifique cuando enviará CA Identity Manager el correo electrónico en la ficha Cuándo enviar.

   La ficha Cuándo enviar proporciona distintas opciones que permiten especificar las acciones que generan las notificaciones de correo electrónico.
5. Especifique los destinatarios del correo electrónico en la ficha Destinatarios.
6. Defina el asunto y el contenido del correo electrónico en la ficha Contenido.

   Puede especificar el contenido dinámico, como la fecha, tarea o nombre del evento, y los atributos de usuario en el contenido del correo electrónico.

Más información:

Ficha Cuándo enviar (en la página 377)
Ficha Destinatarios (en la página 379)
Contenido (en la página 380)
Ficha Perfil de notificación de correo electrónico (en la página 376)

Ficha Perfil de notificación de correo electrónico

La ficha Perfil en las tareas de gestión de correo electrónico le permite especificar información básica sobre una política de notificación de correo electrónico. Esta ficha incluye los siguientes campos:

Nombre de correo electrónico

Identifica la política de notificación de correo electrónico en la Consola de usuario.

Nota: No se muestra el nombre del correo electrónico cuando se envía el correo electrónico. Sólo se usa el nombre para gestionar la política de notificación de correo electrónico en la Consola de usuario.

Categoría

Agrupa las políticas de notificación de correo electrónico para simplificar la gestión.

Especifique una categoría existente seleccionándola de la lista desplegable, o bien seleccione el botón de la segunda opción e introduzca el nombre de una categoría nueva.

Descripción

Describe la política de notificación de correo electrónico a los administradores.

No se muestra la descripción cuando se envía el correo electrónico.

Activado

Especifica que CA Identity Manager enviará el correo electrónico cuando se cumplan las condiciones definidas en la ficha Cuándo enviar.

Personalizar datos

Crea un elemento de datos personalizados en política exprés que puede usarse para configurar destinatarios o contenido personalizados.

Los elementos de datos personalizados también se pueden usar como parámetros en otros elementos de datos.

Nota: En la sección Datos (en la página 510) se proporciona más información sobre los elementos de datos.

Cuando se hace clic en los datos personalizados, en CA Identity Manager se abre una pantalla en la que podrá agregar nuevos elementos de datos.

Reglas de entrada

Define reglas para el momento en que CA Identity Manager envía notificaciones de correo electrónico en las que las reglas predeterminadas en la ficha Cuándo enviar no son lo suficientemente granulares.

Por ejemplo, la ficha Cuándo enviar proporciona una regla predeterminada que envía correo electrónico cuando se modifica un atributo de un perfil de usuario. Si desea que CA Identity Manager envíe un correo electrónico sólo cuando cambia el departamento del usuario, podrá crear una regla de entrada personalizada. (En este caso, se crea un elemento de datos personalizado que identifica el momento en que cambia el departamento y después se crea una regla de entrada que usa el elemento de datos personalizado que creó.)

Nota: En la sección Reglas de entrada (en la página 513) se proporciona más información.

Ficha Cuándo enviar

CA Identity Manager ofrece varias opciones predeterminadas que determinan el momento en que se envía el correo electrónico. Algunas de estas opciones requieren información adicional, como el nombre de la tarea o evento. Por ejemplo, el envío de correos electrónicos cuando se inicia una tarea exige seleccionar la tarea que inicia el correo electrónico.

Puede seleccionar una o varias de las opciones Cuándo enviar siguientes:

Usuario creado

Envía un correo electrónico cuando se haya creado un usuario. Se envía el correo electrónico cuando CreateUserEvent finaliza.

Usuario modificado

Envía un correo electrónico cuando se haya modificado un usuario. Se envía el correo electrónico cuando ModifyUserEvent finaliza.

Flujo de trabajo pendiente

Envía un correo electrónico cuando el proceso de flujo de trabajo asigna un aprobador. Cuando seleccione esta opción, especifique el proceso de flujo de trabajo aplicable. El correo electrónico definido con esta política envía correos electrónicos individuales a aprobadores en todos los pasos del proceso de flujo de trabajo seleccionado.

Correo electrónico del flujo de trabajo pendiente

Envía un correo electrónico cuando un proceso de flujo de trabajo alcanza una actividad especificada. Cuando seleccione esta opción, especifique el proceso de flujo de trabajo aplicable. El correo electrónico definido con esta política envía una notificación de correo electrónico individual para cada paso de la aprobación.

Evento iniciado

Envía un correo electrónico cuando un evento llega al estado Antes. Cuando seleccione esta opción, especifique el evento.

Nota: Si especifica Evento iniciado y se produce un error al enviar el correo electrónico, no se ejecutará el evento asociado con la notificación.

Evento finalizado

Envía un correo electrónico cuando un evento llega al estado Después. Cuando seleccione esta opción, especifique el evento.

Evento aprobado

Envía un correo electrónico cuando un evento llega al estado Aprobado. Cuando seleccione esta opción, especifique el evento.

Evento rechazado

Envía un correo electrónico cuando un evento llega al estado Rechazado. Cuando seleccione esta opción, especifique el evento.

Error en el evento

Envía un correo electrónico cuando se produce un error en el evento. Cuando seleccione esta opción, especifique el evento.

Tarea enviada

Envía un correo electrónico cuando la tarea comienza el procesamiento. Cuando seleccione esta opción, especifique la tarea.

Tarea finalizada

Envía un correo electrónico cuando se termina la tarea. Cuando seleccione esta opción, especifique la tarea.

Error en la tarea

Envía un correo electrónico si se produce un error en la tarea. Cuando seleccione esta opción, especifique la tarea.

Ficha Destinatarios

Puede configurar varios destinatarios para los campos Para, CC o BCC de un correo electrónico. La lista de destinatarios puede ser estática o puede depender del tipo de acción que inicia el correo electrónico y los usuarios involucrados.

Para especificar los destinatarios, seleccione el icono Editar situado junto al campo Para, CC o BCC en la ficha Destinatarios. A continuación, seleccione una de las opciones siguientes, que le permiten configurar la lista de destinatarios:

Encargados de aprobación de flujo de trabajo

Envía el correo electrónico a todos los aprobadores del proceso de flujo de trabajo. Esta opción sólo está disponible si se envía el correo electrónico para un evento pendiente de flujo de trabajo.

Administrador

Envía el correo electrónico al gestor del usuario cuya tarea se haya llevado a cabo.

Nota: Para usar la opción de destinatario Gestor, configure el atributo del gestor para el entorno. Para configurar el atributo del gestor, vaya a Entornos, *Nombre_entorno*, Configuración avanzada, Varios en la consola de gestión. Defina managerattribute en el nombre del atributo físico que almacena el nombre único del gestor de un usuario.

Para bases de datos relacionales, especifique el atributo con el siguiente formato:

tablename.attribute

Miembros del grupo

Envía el correo electrónico a todos los miembros de un grupo. Al seleccionar esta opción se abre una lista desplegable con los nombres de grupo disponibles.

Miembros de roles

Envía el correo electrónico a todos los miembros de un rol de administración. Seleccionar esta opción abre una lista desplegable con los nombres de rol disponibles.

Dirección estática

Envía el correo electrónico a una dirección de correo electrónico seleccionada. Puede especificar la dirección de correo electrónico en el área de texto adicional disponible.

Nota: No especifique más de una dirección en el área de texto.

Usuario

Envía el correo electrónico al usuario cuya tarea se haya realizado.

Iniciador de la solicitud

Envía el correo electrónico a la persona que realizó la solicitud.

Personalizado

Le permite seleccionar un elemento de datos personalizado para definir los destinatarios.

Cuando seleccione la opción personalizada, aparece una lista desplegable con los elementos de datos personalizados que estén disponibles para su uso.

Nota: En la sección Datos (en la página 510) se proporciona más información sobre los elementos de datos.

Contenido

Puede definir el asunto y el cuerpo de un correo electrónico mediante un texto simple o agréguelos con contenido dinámico que se calcula cuando se envía el correo electrónico.

La línea del asunto es un campo de texto sin formato donde podrá escribir el mensaje. Este mensaje será el asunto del correo electrónico.

El cuerpo se muestra en un editor HTML. Puede insertar y dar formato a cualquier texto para formar el cuerpo de correo electrónico.

Para incluir contenido dinámico, seleccione opciones en una lista desplegable. El editor agrega indicadores de contenido dinámico que se parece a lo siguiente (donde se sitúa el cursor):

{*type*}

type representa uno de los tipos de contenido dinámico admitidos.

Por ejemplo, cuando seleccione el tipo de contenido dinámico Attribute y especifique el atributo FirstName, el editor HTML muestra lo siguiente en la ficha Contenido:

{'Attribute: FirstName'}

Nota: Para agregar contenido dinámico a la línea del asunto, use la lista desplegable que hay debajo de la línea del asunto. Para agregar contenido dinámico al cuerpo del correo electrónico, use la lista desplegable situada debajo del cuadro de contenido.

Cuando se envía el mensaje de correo electrónico, CA Identity Manager sustituye el contenido dinámico con el texto adecuado. El texto mantiene el formato, como los caracteres en negrita, especificados en el editor HTML.

Los tipos de contenido dinámico incluyen lo siguiente:

Fecha

Especifica la fecha actual en el formato que especifique.

Tarea

Especifica la tarea para la que se envía el correo electrónico.

Nombre de objeto

Especifica el nombre del objeto en el evento que inicia el correo electrónico. Si el evento es un evento de usuario, este campo es el nombre de inicio de sesión del usuario.

El objeto puede ser distinto a un usuario. Por ejemplo, puede ser cualquier objeto gestionado, como un grupo, rol de administración, etc.

Atributo

Especifica el valor de uno de los atributos de usuario. El usuario es el sujeto de la tarea. Esta opción exige la selección del atributo en una lista desplegable.

Atributo de gestor

Especifica el valor de uno de los atributos del gestor del usuario. El usuario es el sujeto de la tarea. Esta opción exige seleccionar el atributo de una lista desplegable.

Nota: Para usar la opción de destinatario Gestor, configure el atributo del gestor para el entorno. Para configurar el atributo del gestor, vaya a Entornos, *Nombre_entorno*, Configuración avanzada, Varios en la consola de gestión. Defina managerattribute en el nombre del atributo físico que almacena el nombre único del gestor de un usuario.

Para bases de datos relacionales, especifique el atributo con el siguiente formato:

tablename.attribute

Personalizado

Le permite seleccionar un elemento de datos personalizado para definir los destinatarios.

Cuando seleccione la opción personalizada, aparece una lista desplegable con los elementos de datos personalizados que estén disponibles para su uso.

Nota: En la sección Datos (en la página 510) se proporciona más información sobre los elementos de datos.

Modificación de las políticas de notificación de correo

Las modificaciones en la política existente de notificación de correo se realizan para ajustarse a las requisitos empresariales.

Para modificar las políticas de notificación de correo

1. Seleccione Sistema, Correo electrónico, Crear correo electrónico.

   CA Identity Manager mostrará una pantalla de búsqueda.

2. Busque y seleccione la política de notificación de correo que modificar.
3. Cambie la configuración en las fichas Perfil, Cuándo enviar, Destinatarios y Contenido, según sea necesario.

Desactivación de políticas de notificación de correo

Puede activar o desactivar las políticas de notificación de correo con la casilla de verificación Activado en la ficha Perfil cuando se crean o modifican políticas de notificación de correo. Cuando se desactivan las políticas de notificación de correo, el correo electrónico seleccionado no está activo y no se enviará ninguno.

Nota: Las políticas de notificación de correo están activadas de manera predeterminada.

Caso de uso: envío de correos electrónicos de bienvenida

Cuando se contrate un nuevo empleado, la empresa Forward, Inc. enviará un correo electrónico a ese usuario dándole la bienvenida. El correo electrónico debe proporcionar información importante para el nuevo empleado, como vínculos a la página de inicio del empleado e información sobre su gestor y el departamento.

Para crear el correo electrónico, el administrador de Recursos Humanos usa la tarea Crear correo electrónico en la Consola de usuario para configurar las opciones siguientes:

- En la ficha Cuándo enviar, seleccione Usuario creado.
- En la ficha Destinatarios, complete los pasos siguientes:
  - Haga clic en el icono Editar situado junto al campo Para.

    Seleccione Usuario y después haga clic en el signo más. Seleccione el gestor mediante el mismo método y, a continuación, haga clic en Aceptar.
  - Haga clic en el icono Editar situado junto al campo CC.

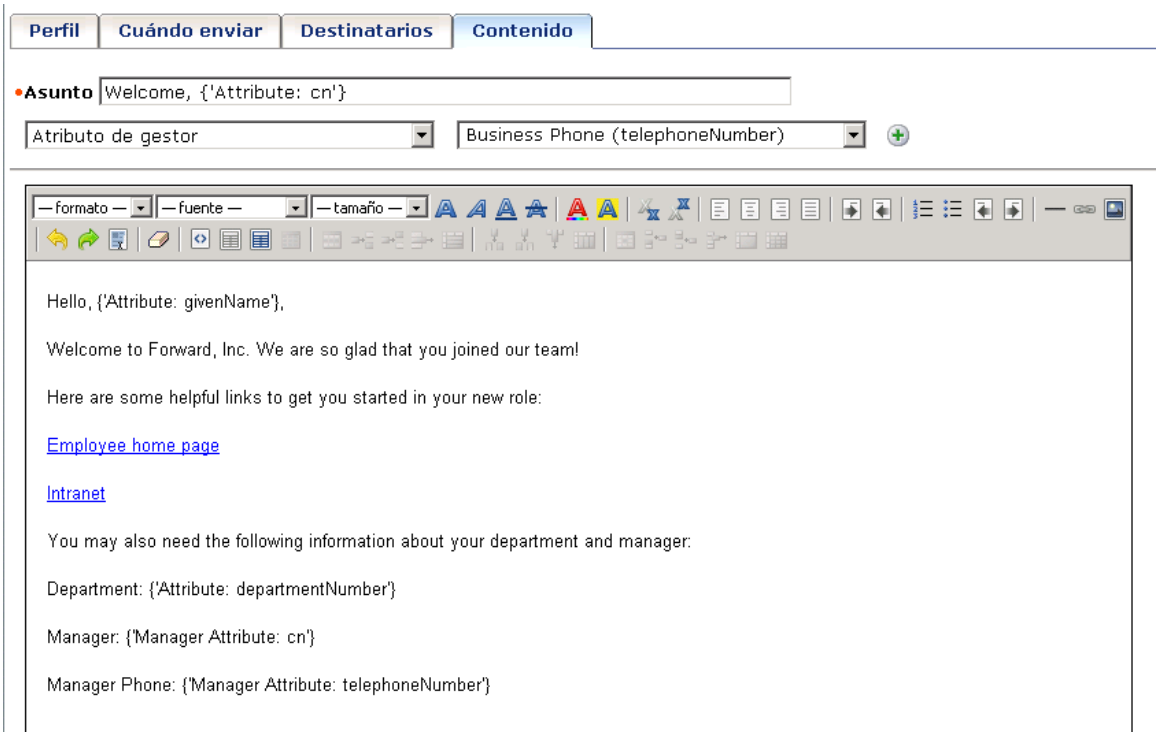
    Seleccione Iniciador, haga clic en el signo más y después en Aceptar para enviar una copia del correo electrónico al usuario que creó el empleado en CA Identity Manager.
- En la ficha Contenido, realice los siguientes pasos:
  - En el campo Asunto, escriba el texto siguiente: Le damos la bienvenida.

    Con el cursor situado al final del texto que escribió, seleccione Atributo en la lista desplegable. A continuación, seleccione la opción de nombre completo en la segunda lista desplegable y después haga clic en el signo más.

    La línea del asunto se parece a la siguiente:

    Le damos la bienvenida, {'Attribute: eTFullName'}

    Nota: El nombre del atributo depende del almacén de usuarios y del atributo que esté usando.
  - En el cuadro Contenido, agregue un texto de bienvenida. Incluya vínculos al portal de empleados y use las opciones de contenido dinámico debajo del cuadro de contenido para mostrar el departamento del usuario, el gestor y el número de teléfono del gestor de esta manera:



Cómo utilizar plantillas de correo electrónico

CA Identity Manager incluye plantillas de correo electrónico predeterminadas que se pueden utilizar para generar mensajes de correo electrónico. Puede utilizar las plantillas predeterminadas tal y como se instalan, o bien puede personalizarlas para que se ajusten a las necesidades de su negocio.

Para utilizar plantillas de correo electrónico

1. Configure los parámetros de SMTP para permitir que CA Identity Manager envíe notificaciones de correo electrónico.
2. Active la notificación de correo electrónico en la Consola de gestión (en la página 385).
3. Configure eventos o tareas para enviar correos electrónicos. (en la página 385)
4. (Opcional) Personalice las plantillas predeterminadas (en la página 391), según sea necesario.

Activación de la notificación de correo electrónico

Se puede activar o desactivar notificación de correo electrónico para un entorno de CA Identity Manager. Si se activan notificaciones de correo electrónico, CA Identity Manager enviará notificaciones de correo electrónico para los eventos y tareas que se especifiquen.

Nota: Para utilizar la función Contraseña olvidada, active la notificación de correo electrónico.\

Antes de que se activen las notificaciones de correo electrónico en CA Identity Manager, configure los valores de configuración (en la página 372) de SMTP para el servidor de aplicaciones.

Para activar las notificaciones de correo electrónico

1. En la Consola de gestión, haga clic en Entornos.

   Se mostrará una lista de entornos de CA Identity Manager.
2. Haga clic en el entorno de Identity Manager adecuado.
3. Vaya a Configuración avanzada, Correo electrónico.
4. Active la casilla de verificación Activado.
5. Configure los eventos y las tareas que activan el correo electrónico (en la página 385).
6. Haga clic en Save.
7. Reinicie la instancia del servidor de aplicaciones en que se ha instalado CA Identity Manager.

Configuración de eventos o tareas para enviar correos electrónicos

Si se activan las notificaciones de correo electrónico, se puede especificar una lista de eventos y tareas que activan notificaciones de correo electrónico. Por ejemplo, puede que desee que se envíen los correos electrónicos si se dan las siguientes circunstancias:

- A un administrador del sistema, cuando se completa una tarea Restablecimiento de la contraseña del usuario.
- Al gestor de nuevos empleados, cuando se completa una tarea Crear usuario. Además, cuando se aprueba el AddToGroupEvent que se generó en la tarea Crear usuario, se puede enviar otro correo electrónico a todos los miembros de un grupo en el que se vaya a agregar al nuevo usuario.

Para especificar eventos y tareas que activan notificaciones de correo electrónico

1. En la Consola de gestión, haga clic en Entornos.

   Se mostrará una lista de entornos de CA Identity Manager.

2. Haga clic en el entorno de CA Identity Manager adecuado.

3. Vaya a Configuración avanzada, Correo electrónico.

   Se abrirá la pantalla de propiedades de correo electrónico.

4. Active las siguientes casillas de verificación de activación según corresponda:

   - Events E-mail Enabled (Correo electrónico de eventos activado)

     Activa la notificación de correo electrónico para eventos de CA Identity Manager.

   - Tasks Email Enabled (Correo electrónico de tareas activado)

     Activa la notificación de correo electrónico para tareas de CA Identity Manager.

5. Introduzca la ubicación de las plantillas de correo electrónico que CA Identity Manager utiliza para crear los mensajes de correo electrónico.

   Las plantillas de correo electrónico se encuentran en un subdirectorio de la ubicación siguiente:

   iam_im.ear\custom\emailTemplates

   Nota: Al crear un archivo de plantilla de correo electrónico con un nombre de archivo utilizando un idioma diferente, la sesión de sistema operativo debe estar ejecutándose en un idioma compatible con el conjunto de caracteres.

6. Especifique los eventos para los que se enviarán notificaciones de correo electrónico tal y como se muestra a continuación:

   - Para agregar un evento, seleccione el evento en el cuadro de lista Evento y haga clic en Agregar.

     CA Identity Manager agrega el evento que haya seleccionado a la lista de eventos para los que se envían notificaciones de correo electrónico.

     Nota: Si se selecciona un evento que no se asocie a un proceso del flujo de trabajo, CA Identity Manager enviará una notificación de correo electrónico cuando se complete el evento.

   - Para suprimir un evento, active la casilla de verificación del evento y, a continuación, haga clic en Suprimir.

7. Especifique las tareas para los que se enviarán notificaciones de correo electrónico tal y como se muestra a continuación:

   - Para agregar una tarea, búsquela seleccionando una condición en el primer campo e introduciendo un nombre para la tarea en el segundo campo. Haga clic en Buscar.

     Se puede introducir de forma parcial un nombre para la tarea mediante el carácter comodín (*). Por ejemplo, para buscar una tarea Crear, introduzca Crear*.

     Seleccione una o varias tareas de los resultados de la búsqueda. Haga clic en Agregar.

     Nota: Las notificaciones de correo electrónico de nivel de tarea no están disponibles para las tareas que tengan la vista de tipo de acción Ver o Autovista. Para ver el tipo de acción de una tarea, vaya a Modificar la tarea de administración, seleccione una tarea y compruebe el campo de acción en el perfil de la tarea.

   - Para suprimir una tarea, active la casilla de verificación de la tarea y, a continuación, haga clic en Suprimir.

     Al suprimir una tarea, se elimina de la tabla Tarea. No suprime la tarea.

8. Al terminar de configurar las tareas y los eventos que activan notificaciones de correo electrónico, haga clic en Guardar.
9. Reinicie el servidor de aplicaciones en que se ha instalado CA Identity Manager.

Contenido del correo electrónico

Las notificaciones de correo electrónico constan de una plantilla genérica más los detalles específicos de tarea que se agregan al correo electrónico mediante la API de correo electrónico. Por ejemplo, la siguiente información se puede insertar en un correo electrónico para una tarea Crear usuario:

- El nombre del administrador que está ejecutando la tarea
- El nombre del nuevo usuario
- La dirección de correo electrónico del usuario, el nombre del departamento y otros datos de atributos
- La organización en la que se va a crear el usuario
- El estado de aprobación del flujo de trabajo y el tiempo de aprobación
- El nombre de la tarea y los nombres de los eventos de la tarea

Plantillas de correo electrónico

Se generan notificaciones de correo electrónico desde las plantillas de correo electrónico. Identity Manager proporciona plantillas de correo electrónico predeterminadas que se pueden utilizar como instaladas, o bien que se pueden utilizar para crear plantillas de correo electrónico.

Cada plantilla de correo electrónico contienen los siguientes elementos:

- **Información de entrega**: una lista de destinatarios de correo electrónico. Identity Manager genera automáticamente la lista de destinatarios según los usuarios que participen en la tarea. Por ejemplo, un correo electrónico de aprobación se envía a todos los aprobadores correspondientes a la tarea.
- **Asunto**: el texto utilizado en la línea de asunto del mensaje.
- **Contenido**: el cuerpo del mensaje. El cuerpo normalmente contiene tanto texto estático como variables que Identity Manager resuelve según la tarea o el evento que activa el correo electrónico.

Las plantillas de correo electrónico predeterminadas se encuentran en un directorio de emailTemplates donde se instalan las herramientas administrativas de Identity Manager. La ubicación de la instalación predeterminada para las herramientas administrativas es la siguiente:

- Para Windows: C:\Archivos de programa\CA\CA Identity Manager\
- Para UNIX: <home_directory>/CA/CA Identity Manager

El directorio de emailTemplates contiene cuatro carpetas. Cada carpeta se asocia a un estado de evento o tarea:

Directorio	Contenido
Aprobado	defaultEvent.tmpl: informa a los destinatarios de que se ha aprobado un evento.

Directorio	Contenido
Completado	■ CertificationNonCertifiedActionCompletedNotification.tmpl: informa al gestor de que se ha aplicado una acción de no conformidad a un empleado. ■ CertificationNonCertifiedActionPendingNotification.tmpl: informa al gestor de que se aplicará una acción de no conformidad a un empleado. ■ CertificationRequiredFinalNotification.tmpl: recordatorio final a un gestor de que una tarea Certificar usuario debe completarse para un empleado. ■ CertificationRequiredNotification.tmpl: informa al gestor de que se ha iniciado un proceso de certificación para un empleado. El gestor debe completar una tarea Certificar usuario para este empleado. ■ CertificationRequiredReminderNotification.tmpl: recuerda al gestor que se debe completar una tarea Certificar usuario para un usuario. ■ Certify Employee.tmpl.tmpl: informa a un administrador de que el proceso de certificación para un empleado se ha completado. ■ CreateProvisioningUserNotificationEvent.tmpl: envía una contraseña temporal a un usuario cuando se crea la cuenta de ese usuario en el directorio de aprovisionamiento. ■ defaultTask.tmpl: informa a los destinatarios de que Identity Manager ha completado una tarea. ■ ForgottenPassword.tmpl: envía una contraseña temporal a los usuarios que han utilizado la función de contraseña olvidada. ■ ForgottenUserID.tmpl: envía un ID de usuario a los usuarios que han utilizado la función de ID de usuario olvidado. ■ Self Registration.tmpl: informa a un usuario de que una tarea de autorregistro se ha completado correctamente.
Pendiente	■ defaultEvent.tmpl: informa a los aprobadores de que requiere un elemento de la lista de trabajo requiere su atención. ■ ModifyUserEvent.tmpl: igual que con la plantilla predeterminada, pero incluye métodos para recuperar los atributos del objeto gestionado de usuario.
Rechazado	defaultEvent.tmpl: informa a los destinatarios de que un evento se ha rechazado.

Utilice la estructura de directorio de plantillas y las plantillas de Identity Manager que se han instalado en el directorio <*im_admin_tools_dir*>\Identity Manager\
de emailTemplates como base para crear plantillas de correo electrónico personalizadas.

Directorios de plantilla

Cada directorio de la plantilla que se describe en Plantillas de correo electrónico (en la página 388) se asocia a una tarea o estado de evento concretos. Por ejemplo, si un correo electrónico se va a enviar para los eventos de rechazos en el proceso del flujo de trabajo, Identity Manager buscará en un directorio rechazado implementado la plantilla que utilizará. Identity Manager genera a continuación el correo electrónico de la plantilla de correo electrónico adecuada del directorio.

Plantillas de correo electrónico en un directorio

Cada directorio de plantilla implementado contiene una o varias plantillas de correo electrónico. Cuando se producen un evento o una tarea que tienen activados las notificaciones de correo electrónico, Identity Manager busca en el directorio de plantilla adecuado un nombre de plantilla que tenga el mismo nombre de la tarea o el evento. Si no se puede encontrar ninguna plantilla, Identity Manager utilizará la plantilla predeterminada en el directorio. Los nombres de plantilla predeterminados se muestran en Plantillas de correo electrónico (en la página 388). Por ejemplo, Identity Manager utiliza defaultEvent.tmpl en el directorio Pendiente para informar a los aprobadores de que tienen un nuevo elemento de la lista de trabajo.

Conjuntos de directorios de plantilla

En un conjunto de directorios de plantilla se incluyen un directorio aprobado, completado, pendiente y rechazado. Se pueden implementar varios conjuntos de directorios de plantilla y especificar un conjunto para un entorno de Identity Manager determinado.

La implementación de plantilla de correo electrónico (en la página 411) proporciona información sobre la implementación de conjuntos de directorios de plantilla.

Para obtener información sobre la configuración de directorios de plantilla de correo electrónico para que Identity Manager utilice el conjunto correcto para un entorno determinado, consulte la *Guía de configuración de CA Identity Manager*.

Creación de plantillas de correo electrónico

Para crear mensajes de correo electrónico personalizados

1. Abra la plantilla que desea modificar.

   Por ejemplo, si desea crear un mensaje de correo electrónico para un evento Crear usuario, abra defaultEvent.tmpl en el directorio Pendiente.

2. Guarde la plantilla en el mismo directorio con un nombre nuevo. El nombre debe coincidir con el del evento para el correo electrónico que corresponda; además, debe tener la extensión .tmpl.

   Por ejemplo, asigne este nombre al mensaje para el evento Crear usuario:

   CreateUserEvent.tmpl

   Consulte los eventos de Identity Manager para ver una lista de eventos.

   Nota: Al crear un archivo de plantilla de correo electrónico con un nombre de archivo utilizando un idioma diferente, la sesión de sistema operativo debe estar ejecutándose en un idioma compatible con el conjunto de caracteres.

3. Modifique la plantilla del mensaje según sea necesario, tal y como se describe en la siguiente sección de plantillas de correo electrónico personalizadas (en la página 391).

Plantillas de correo electrónico personalizadas

Una plantilla de correo electrónico es un archivo dinámico que es compatible tanto con HTML y con Javascript del lado de servidor incrustado. Una plantilla permite insertar valores variables en texto estático, por lo que se permite que los mensajes específicos para cada caso se generen a partir de una única plantilla.

La misma plantilla puede utilizar cualquier número de veces para imprimir texto estático reutilizable (por ejemplo, para indicar que se ha aprobado la frase) junto con texto variable específico en un contexto determinado (como el nombre del evento que se va a aprobar).

Por ejemplo, esta es una plantilla para informar de la aprobación de un evento:

```
<!-- Define the E-mail Properties --->
<%
   _to = _util.getNotifiers("ADMIN");
   _cc = "" ;
   _bcc = "";
   _subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">
```

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

Nota: Los objetos de Identity Manager _util y _eventContextInformation que se utilizan en el ejemplo anterior se describen en la API de plantilla de correo electrónico.

Si una aprobación se genera para el evento CreateUserEvent y el usuario José García se crea en la organización HR, el cuerpo de la notificación de correo electrónico que se generó a partir de la plantilla de aprobación podría tener la siguiente apariencia:

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

En las siguientes secciones se describen la sintaxis y los objetos de Identity Manager que hacen que se puedan generar mensajes de correo electrónico.

Elementos de plantilla

Las plantillas de correo electrónico de Identity Manager son compatibles con lo siguiente:

- Etiquetas de HTML estándares.
- JavaScript del lado del servidor.
- Uno o varios objetos implícitos que Identity Manager convierte en disponible para la instancia de una plantilla; es decir, un mensaje de correo electrónico.
- Etiquetas de Identity Manager que permiten incrustar JavaScript en la plantilla, llamar a los métodos en los objetos de Identity Manager implícitos e insertar valores variables en el texto estático de la plantilla.

Extensiones de etiqueta de Identity Manager

Las plantillas de correo electrónico son compatibles con las siguientes etiquetas:

<% %>

Incrusta JavaScript en una plantilla de correo electrónico.

<%= %>

Inserta un valor variable en texto estático.

Las etiquetas se describen en las siguientes secciones.

<% %>

Esta etiqueta permite incrustar JavaScript para ejecución en línea en una plantilla de correo electrónico.

Se puede utilizar cualquier objeto de JavaScript en el JavaScript incrustado. Se pueden llamar también a métodos de objeto implícitos de Identity Manager en el JavaScript incrustado.

Por ejemplo, el siguiente código modifica el cuerpo de la plantilla de aprobación que se muestra en la sección de plantillas de correo electrónico personalizadas (en la página 391). JavaScript se utiliza para determinar si un objeto secundario interviene en el evento (como objeto ORGANIZATION cuando se agrega un objeto USER primario). Si no hay ningún objeto secundario, el texto relacionado con el objeto secundario se omite del mensaje:

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
Status: <b>Approved</b>
```

<%= %>

Esta etiqueta permite insertar un valor variable en texto estático. El valor puede ser el siguiente:

- Una variable que se definiera en un JavaScript de la plantilla que se haya ejecutado anteriormente. Por ejemplo:

```
<%
var secondaryType =
     _eventContextInformation.getSecondaryObjectTypeName();
...          // More JavaScript processing
%>
...          // More HTML
El objeto primario se crea en <%=secondaryType%>.
```

- Un valor que se ha devuelto a partir de un método en un objeto implícito de Identity Manager. Por ejemplo:

```
Event <%=_eventContextInformation.getEventName()%> is approved.
```

API de plantilla de correo electrónico

Cuando un mensaje se genera a partir de una plantilla, Identity Manager convierte los siguientes objetos implícitos disponibles en el mensaje. Estos objetos permiten insertar información específica de instancias en un mensaje llamando a métodos de la API de plantilla de correo electrónico.

Una plantilla puede llamar a los métodos en algunos de los siguientes objetos:

- _contentType. Especifica el contentType para el correo electrónico.
- _priority. Especifica la prioridad para el correo electrónico.
- _to. Agrega destinatarios al campo Para del mensaje.
- _cc. Agrega destinatarios al campo de cc (enviar copiar a) del mensaje.
- _bcc. Agrega destinatarios al campo de cco (enviar copiar oculta a) del mensaje.
- _subject. Especifica el asunto del correo electrónico.
- _encoding. Especifica la codificación para el correo electrónico.
- template. Permite agregar una cadena de texto a un mensaje a partir de las líneas de código JavaScript.
- _util. Un objeto de utilidad.

- _eventContextInformation. Contiene información sobre el evento que genera la tarea actual, como el nombre del evento y estado de la aprobación.
- _taskContextInformation. Contiene una recolección de información sobre la tarea actual, como el nombre de la tarea, el nombre de la organización y los eventos que la constituyen.

Estos objetos se describen en las siguientes secciones.

_contentType

Especifica el contentType para el correo electrónico.

Si ningún contentType se especifica a través de variable _contentType, se aplica el "text/html" de contentType predeterminado.

Métodos: Ninguno.

Ejemplo:

```
<% _contentType = "text/html"; %>
```

_priority

Especifica la prioridad para el correo electrónico. Especifique 0 para ninguna prioridad (predeterminado) y 1 para la prioridad alta.

Métodos: Ninguno.

Ejemplo:

```
<% _priority = "1"; %>
```

_to.

Agrega destinatarios al campo Para del mensaje.

El valor de la variable de _to es una cadena de JavaScript. Se permiten varios destinatarios, pero la cadena se debe coincidir con la sintaxis de JavaScript, tal y como se muestra en el siguiente ejemplo.

Métodos: Ninguno.

Ejemplo:

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "" ;
_bcc = "" ;
_subject = "Your new password ";
%>
```

Nota: Cuando los correos electrónicos alertan a los participantes de que una tarea tiene un estado Pendiente y está bajo control del flujo del trabajo, el objeto _to se rellena previamente con las direcciones de los participantes. No se puede utilizar el objeto _to en una plantilla Pendiente.

_cc

Agrega destinatarios al campo de cc (enviar copiar a) del mensaje.

El valor de la variable de _to es una cadena de JavaScript. Se permiten varios destinatarios, pero la cadena se debe coincidir con la sintaxis de JavaScript, tal y como se muestra en el siguiente ejemplo.

Métodos: Ninguno.

Ejemplo:

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_bcc

Agrega destinatarios al campo de cco (enviar copiar oculta a) del mensaje.

Las direcciones de correo electrónico que se han especificado en este campo no aparecen en el correo electrónico.

El valor de la variable de _to es una cadena de JavaScript. Se permiten varios destinatarios, pero la cadena se debe coincidir con la sintaxis de JavaScript, tal y como se muestra en el siguiente ejemplo.

Métodos: Ninguno.

Ejemplo:

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_subject

Especifica el asunto del correo electrónico.

Métodos: Ninguno.

Ejemplo:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

Especifica la codificación para el correo electrónico.

Si no se especifica la codificación a través de _encoding o de la variable de LANG, es posible que los caracteres no se muestren correctamente en el correo electrónico. Asegúrese de establecer _encoding o LANG para la configuración regional adecuada.

Métodos: Ninguno.

Ejemplo:

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

Especifique los atributos de encabezado de correo electrónico adicionales en la plantilla de correo electrónico.

Se debe asignar HashMap() a este atributo. Los nombres y los valores almacenados en HashMap deben ser cadenas.

Ejemplo: adición de atributos de encabezado personalizados

El siguiente atributo muestra cómo agregar dos atributos de encabezado personalizados, "X-TCCCSWD" y "myheader":

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

Permite agregar una cadena de texto a un mensaje a partir de líneas de código JavaScript (es decir, las líneas de la etiqueta <% %>). La cadena puede contener etiquetas HTML, texto estático o los valores variables que devuelven los métodos en objetos implícitos de Identity Manager.

Nota: El objeto de plantilla no debe empezar con el carácter de guion bajo (_).

Método:

- add(String)

  El argumento debe evaluarse en una cadena, incluidas las llamadas a métodos de un objeto implícito de Identity Manager. En el ejemplo siguiente, consulte _eventContextInformation.getSecondaryObjectName().

Ejemplo:

```
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
```

_util

Objeto de utilidad.

Método:

- getNotifiers(String [,String])

  Devuelve ID de correo electrónico según las reglas de notificación.

  El primer argumento es compatible con las siguientes reglas de notificación predeterminadas, que deben utilizarse entre comillas:

  - "ADMIN". Envía el correo electrónico al administrador que ha iniciado la tarea.
  - "USER". Envía el correo electrónico al usuario en el contexto actual.
  - "USER_MANAGER". Envía el correo electrónico al gestor del usuario en el contexto actual.

Se puede hacer referencia también a una regla de notificación personalizada que se crea con la API de regla de notificación. Para obtener más información, consulte la *Guía de programación para Java.*

El segundo argumento es opcional. Se puede utilizar para pasar uno o varios pares nombre-valor en una regla de notificación personalizada. Separe cada par nombre-valor con una coma, con el siguiente formato:
`"name1=value1,name2=value2,..."`

Ejemplos:

```
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

Notificación al gestor de un usuario

Se puede utilizar la regla de notificación USER_MANAGER para enviar correos electrónicos al gestor de cualquier usuario. Identity Manager utiliza esta regla en las plantillas de correo electrónico que son compatibles con el certificado de derecho a ser usuario.

Nota: La regla de notificación USER_MANAGER solamente se aplica a eventos o tareas que crean o gestionan un único usuario.

Dado que hay diferentes formas de que especificar relaciones de usuarios a gestores en un directorio de usuarios, el adaptador de notificaciones de gestor de usuarios predeterminado resuelve esta relación según una expresión de atributo especificada en el segundo parámetro del método getNotifiers().

Ejemplo:

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

El adaptador de notificaciones de gestor de usuarios es compatible con dos opciones de búsqueda:

- managerattribute = **<***Manager AttributeName***>**, donde el objeto de usuario mantiene un atributo que indica el nombre destacado o el ID de usuario del gestor de ese usuario.
- commonattribute = **<***AttributeName***>**, donde el usuario y el gestor del usuario comparten un valor de atributo común, como "departamento".

Configure estas opciones de búsqueda en las propiedades de opciones varias para un entorno de la Consola de gestión de Identity Manager.

Para configurar la regla de notificación USER_MANAGER:

1. En la Consola de gestión de Identity Manager, seleccione las opciones de entornos de Identity Manager. A continuación, seleccione el entorno para el que se está configurando la notificación de correo electrónico.
2. Seleccione Configuración avanzada, Miscellaneous Properties (Propiedades de opciones varias).
3. En la página de propiedades de opciones varias, complete los pasos de configuración para la opción de búsqueda que desea utilizar:
   - Para utilizar la opción de búsqueda managerattribute=<Manager AttributeName>:
     a. En el campo Propiedad, introduzca managerattribute.
     b. En el campo Valor, introduzca el atributo que almacena el nombre destacado del gestor o el ID de usuario.
     c. Haga clic en Agregar.
     d. Haga clic en Save.
   - Para utilizar la opción de búsqueda commonattribute=<AttributeName>:
     a. En el campo Propiedad, introduzca commonattribute.
     b. En el campo Valor, introduzca el atributo que el usuario y el gestor del usuario tienen en común.
     c. Haga clic en Agregar.
     d. En el campo Propiedad, introduzca ismanagerfilter.

e. En el campo Valor, introduzca una expresión de búsqueda mediante la siguiente sintaxis:

   <attribute> <operator> <filter>

   Por ejemplo, título EQUALS gestor

f. Haga clic en Agregar.

g. Haga clic en Save.

Se puede escribir también un adaptador personalizado y crear reglas para notificar al gestor de un usuario. Consulte la *Guía de programación para Java*.

_eventContextInformation

Contiene información sobre el evento que genera la tarea actual, como el nombre del evento y estado de la aprobación. A esta información se la denomina "información de *contexto*" para el evento.

El objeto _eventContextInformation se crea a partir de la clase ExposedEventContextInformation en el paquete com.netegrity.imapi.

Este objeto está disponible para los mensajes de correo electrónico basados en plantillas Aprobado, pendiente y Rechazado. Para obtener información sobre estas plantillas, consulte Plantillas de correo electrónico (en la página 388).

Métodos: todos los siguientes métodos devuelven una cadena.

Método	Descripción
getAdminName()	Devuelve el nombre de la persona que ha enviado la tarea que ha generado el evento. Desaprobado en CA Identity Manager 5.6. Utilice uno de los siguientes métodos heredados: ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	Devuelve el estado de la aprobación del evento. Uno de estos valores: APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	Devuelve la hora a la que se aprobó el evento.

Método	Descripción
getEventName()	Devuelve el nombre del evento. Para obtener una lista de nombres de event, consulte Eventos de CA Identity Manager.
getOrgName()	Devuelve el nombre descriptivo de la organización donde la tarea se está ejecutando. Desaprobado en CA Identity Manager 5.6. Utilice el método heredado getObjectOrganizationFriendlyName().
getPassword()	Si el tipo de los objetos primarios es USER, devuelve la contraseña del usuario.
getPrimaryObjectTypeName()	Devuelve el tipo de objeto primario. Tipos de objeto primario que se devuelven: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getPrimaryObjectName()	Devuelve el nombre del objeto primario al que afecta el evento. Un *objeto primario* es el objeto al que afecta directamente el evento. Un *objeto secundario* es el objeto al que se ha vinculado el objeto primario, si hay alguno. Por ejemplo: ■ El tipo de objeto primario para CreateUserEvent es USER. El objeto secundario es el objeto en el que se crea el usuario; es decir, ORGANIZATION. ■ El tipo de objeto primario para CreateAdminRoleEvent es ADMINROLE. Este objeto no se vincula a otros objetos, por lo que existen objetos secundarios. Con un objeto primario del tipo USER, getPrimaryObjectName() podría devolver José García.

Método	Descripción
getSecondaryObjectTypeName()	Si existe un objeto secundario al que afectó el evento, se devuelve el tipo de objeto. Tipos de objeto secundarios que se devuelven: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getSecondaryObjectName()	Si existe un objeto secundario al que afectó el evento, se devuelve el nombre del objeto. Consulte getPrimaryObjectName() para obtener información sobre los objetos principales y secundarios. Con un objeto secundario del tipo ORGANIZATION, el método getSecondaryObjectName() podría devolver HR.

Nota: Se proporciona los métodos _eventContextInformation a través de la interfaz ExposedEventContextInformation. Como ExposedEventContextInformation hereda métodos en la API de CA Identity Manager principal, _eventContextInformation puede llamar también a estos métodos a partir de una plantilla de correo electrónico, junto con los métodos de la tabla anterior. Para obtener más información sobre estos métodos heredados, consulte Métodos adicionales (en la página 408).

Ejemplo: notificación de correo electrónico sobre eventos Pendiente:

```
<%
_cc = "" ;
_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                                " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

Se ha agregado el siguiente elemento a la lista de trabajos para la aprobación:
<br><br><br>
Event: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

Posible cuerpo de correo electrónico:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

Se ha agregado el siguiente elemento a la lista de trabajos para la aprobación:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**

Nota: El valor del campo Desde se obtiene del archivo email.properties. Para cambiar el valor, editar el siguiente archivo:
<*iam_im.ear*>\config\com\netegrity\config\email.properties

donde <*iam_im.ear*> es la ubicación de instalación de CA Identity Manager en el dominio de servidor de aplicaciones. Por ejemplo:

Para WebLogic:
<*WebLogic_home*>\user_projects\<domain>\applications\iam_im.ear

Para JBoss:
<*Identity Manager_home*>\jboss-3.2.2\server\default\deploy\iam_im.ear

Para WebSphere:
<*im_admin_tools_dir* >\WebSphere-ear\iam_im.ear

Para agregar información adicional sobre el usuario al que afecta el evento para el correo electrónico en el ejemplo anterior, agregue un texto que se parezca al siguiente:

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Posible cuerpo de correo electrónico:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

Se ha agregado el siguiente elemento a la lista de trabajos para la aprobación:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**
User information:
Last Name: Ferrigamo
First Name: Richard
Full Name: Richard Ferrigamo
Email: rferrigamo@mybank.org
Organization Membership: **Mortgages & Loans**

_taskContextInformation

Contiene una recolección de información sobre la tarea actual, como el nombre de la tarea, el nombre de la organización y los eventos que la constituyen. A esta información se la denomina "información de *contexto*" para la tarea.

Este objeto está disponible para los mensajes de correo electrónico basados en plantillas Completado. Para obtener información sobre esta plantilla, consulte Plantillas de correo electrónico (en la página 388).

Métodos: todos los métodos siguientes devuelven una cadena, excepto el método getExposedEventContexts(), que devuelve un vector de Java.

Método	Descripción
getAdminName()	Devuelve el nombre de la persona que envía la tarea. Desaprobado en Identity Manager 5.6. Utilice uno de los siguientes métodos heredados: ■ getAdministrator() ■ getAdminFriendlyName()
getExposedEventContexts()	Devuelve un vector de Java de todos los eventos asociados a la tarea. Cada objeto del vector es un objeto de contexto de evento. Se pueden utilizar los métodos clasificados que se muestran en _eventContextInformation para recuperar la información de contexto de un objeto de evento determinado. El objeto que se devuelve es un objeto de vector de Java estándar. Se puede utilizar cualquiera de los métodos del objeto de Vector. Por ejemplo, get() y size() para gestionar los elementos en el vector.
getOrgName()	Devuelve el nombre de la organización en la que la tarea se está ejecutando. Desaprobado en Identity Manager 5.6. Utilice el método heredado getObjectOrganizationFriendlyName().
getTaskName()	Devuelve el nombre de la tarea que se ejecuta. Desaprobado en Identity Manager 5.6. Utilice uno de los siguientes métodos heredados: ■ getAdminTask() ■ getTaskFriendlyName()

Nota: Se proporciona los métodos en _taskContextInformation a través de la interfaz ExposedTaskContextInformation. Como ExposedTaskContextInformation hereda métodos en la API de Identity Manager principal, _taskContextInformation puede llamar también a estos métodos a partir de una plantilla de correo electrónico, junto con los métodos de la tabla anterior. Para obtener más información sobre estos métodos heredados, consulte Métodos adicionales (en la página 408).

Ejemplo: cuerpo de una plantilla de notificación de correo electrónico para un cambio de contraseña:

```
<%
var imsEventContexts =
            _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
   {
   for(var i=0;i<imsEventContexts.size();i++)
      {
      var eventContext = imsEventContexts.get(i);
      template.add("Hi "+ eventContext.getPrimaryObjectName()
                                                          + ",");
      template.add("<br>Your new password is: <b>"+
                              eventContext.getPassword());</br>
      template.add("<hr>");
      }
   }
%>
```

Posible cuerpo de correo electrónico:

Hola, Javier Pérez:
Su nueva contraseña es: LFH7F1226

Métodos adicionales

Los métodos en _taskContextInformation y _eventContextInformation se proporcionan a través de los objetos de Identity Manager ExposedTaskContextInformation y ExposedEventContextInformation, respectivamente.

Estos objetos heredan métodos en la API de Identity Manager principal. Por consiguiente, los métodos heredados están también disponibles en _taskContextInformation y _eventContextInformation.

Los siguientes métodos heredados del objeto TaskInfo son especialmente útiles para una plantilla de correo electrónico:

- getAdministrator(). Recupera un objeto User para el administrador que está ejecutando la tarea actual.
- getAdminTask(). Recupera un objeto AdminTask para la tarea actual.

Estos objetos recuperados permiten insertar información específica de administradores y tareas en un correo electrónico. Por ejemplo:

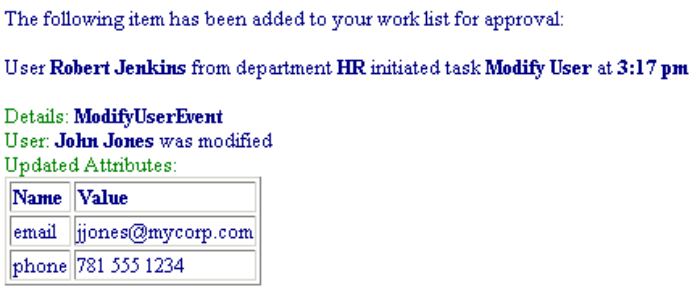
```
<!-- Define the E-mail Properties --->

<%
   _cc = "" ;
   _bcc = "" ;
   _subject = _eventContextInformation.getEventName() +
                                                " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

Se ha agregado el siguiente elemento a la lista de trabajos para la aprobación:
<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
               getAttribute(Packages.com.netegrity.llsdk6.imsapi.
                managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
               from department <b><%= _eventContextInformation.
               getAdministrator().getOrg(null).getFriendlyName()
               %></b> initiated task <b><%= _eventContextInformation.
               getAdminTask().getFriendlyName() %></b>at <b><%=
               _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
                                          getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
                               getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                                        was modified
<br>
<font color="green">Updated Attributes:</font>
<table border="1">
<tr>
<td><b>Name</b></td>
<td><b>Value</b></td>
</tr>
```

```
<%
   var event = _eventContextInformation.getEvent();
   if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
      var user = event.getUser();
      var attributes = user.getAttributes().keys();
      while(attributes.hasMoreElements()) {
         var attr = attributes.nextElement();
         var value = user.getAttribute(attr);
         if(user.hasAttributeChanged(attr)) {
            template.add("<tr><td>" + attr +"</td>");
            template.add("<td>" + value +"</td></tr>");
         }
      }
   }
%>
</table>
<br>
</body>
</html>
```

Posible cuerpo de correo electrónico:


The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**
User: **John Jones** was modified
Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

Para obtener más información sobre los métodos heredados que están disponibles para la API de plantilla de correo electrónico, consulte los objetos ExposedTaskContextInformation y ExposedEventContextInformation en Javadoc de Identity Manager.

Flujo de salida estándar de Java

Un mensaje de correo electrónico puede realizar también llamadas al flujo de salida estándar de Java de dentro de la etiqueta de JavaScript (<% %>). Por ejemplo, la siguiente llamada envía el mensaje Finalizado a la consola del servidor:

```
<%
...       // JavaScript processing
out.println("Done.");
%>
```

Referencia de Javadoc

Para obtener información sobre los objetos ExposedTaskContextInformation y ExposedEventContextInformation, incluidos los métodos que se heredan de la API de Identity Manager principal, consulte Javadoc de Identity Manager.

Las páginas de Javadoc se integran con una versión de HTML de la Guía de programación para Java, que se encuentra disponible en la biblioteca de Identity Manager.

Implementación de plantillas de correo electrónico

Cuando CA Identity Manager esté a punto de enviar el correo electrónico, busque plantillas a partir de las cuales generar el correo electrónico en la siguiente ubicación raíz en el servidor de aplicaciones:

iam_im.ear\custom\emailTemplates

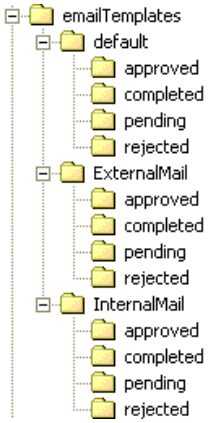
Las plantillas de correo electrónico que se implementen en esta raíz se incluyen en conjuntos de la plantilla que tienen la misma estructura de directorios; es decir, hay un directorio Aprobado, Completado, Pendiente y Rechazado en cada conjunto.

Conjuntos de plantilla

Se pueden implementar varios conjuntos de plantillas de correo electrónico en emailTemplates. Por ejemplo, durante la instalación, el siguiente conjunto de plantillas de correo electrónico se crea en iam_im.ear\custom\emailTemplates:

```
default\approved
default\completed
default\pending
default\rejected
```

El conjunto de plantillas de correo electrónico predeterminado contiene las plantillas instaladas que se describen en Plantillas de correo electrónico (en la página 388). Se pueden agregar plantillas personalizadas en el conjunto predeterminado. Se pueden implementar también otros conjuntos de plantillas de correo electrónico en estructuras de directorios que se definan al mismo nivel como conjuntos predeterminados. Por ejemplo, iam_im.ear\custom podría contener las siguientes plantillas de correo electrónico implementadas:



Nota: Para obtener información sobre cómo CA Identity Manager elige una plantilla de correo electrónico concreta en un conjunto de plantilla, consulte Directorios de la plantilla (en la página 390).

Cómo especificar un conjunto de plantilla para un entorno

Al configurar correos electrónicos para un entorno de Identity Manager, especifique el conjunto de plantillas de correo electrónico que desea utilizar para dicho entorno. Para obtener información sobre la configuración de correo electrónico para entornos de Identity Manager, consulte la *Guía de configuración de CA Identity Manager*.

Nombres de plantilla

Los directorios de un conjunto de plantillas personalizadas deben incluir plantillas predeterminadas con el mismo nombre que los que se han instalado en el conjunto de plantillas predeterminadas. Los nombres predeterminados se muestran en Plantillas de correo electrónico (en la página 388). Identity Manager utiliza las plantillas predeterminadas cuando no se puede encontrar ninguna otra plantilla con un nombre que coincida con la tarea o el evento que se está ejecutando.

Si se desea, se pueden agregar plantillas adicionales a uno o varios directorios en un conjunto de plantillas si desea que se genere un correo electrónico a partir de una plantilla concreta. Para ello, haga lo siguiente:

- Asigne a la plantilla el mismo nombre que la tarea o evento para los que se generará el correo electrónico.
- Coloque la plantilla en el directorio asociado al estado de la tarea o el evento para el que se generará el correo electrónico.

Por ejemplo, si desea que los correos electrónicos se generen a partir de una plantilla concreta cuando se rechace CreateUserEvent, coloque una plantilla denominada "CreateUserEvent.tmpl" en el directorio rechazado del conjunto de plantillas del entorno.

Capítulo 14: Generación de informes

Esta sección contiene los siguientes temas:

Descripción general de la configuración

En CA Identity Manager, se pueden ejecutar dos tipos de informes diferentes:

Informes de instantáneas

Incluye datos de la base de datos de instantáneas, que contiene información del almacén de objetos de CA Identity Manager y del almacén de usuarios de CA Identity Manager. Un ejemplo de informe de instantáneas es el informe de perfiles de usuario. Los datos que se agregan a la base de datos instantáneas se definen mediante el uso de definiciones de instantáneas que especifican la información que se incluye.

Informes que no sean de instantáneas

Incluyen datos de otros orígenes de datos como, por ejemplo, la base de datos de auditoría. Por ejemplo, CA Identity Manager incluye informes de auditoría predeterminados. (Estos informes tienen el prefijo "Audit - " en el nombre que aparece en la Consola de usuario). De manera predeterminada, CA Identity Manager solo incluye informes de auditoría, pero puede crear sus propios informes personalizados para incluir datos de otros orígenes de datos como, por ejemplo, bases de datos de flujo de trabajo o de persistencia de tareas.

Cada informe de CA Identity Manager requiere una configuración inicial antes de poder ejecutarlo. Los pasos de la configuración dependen del tipo de informe que desee ejecutar.

Los pasos siguientes resumen los procedimientos que contiene este capítulo.

Para Informes de instantáneas

1. Cree un archivo de definiciones de instantáneas para definir los datos que se agregarán a la base de datos de instantáneas.
2. Captura datos de instantánea para el informe.

3. Modifique la Tarea de informe en la Consola de usuario y realice las acciones siguientes:
   a. Asocie una definición de instantánea con la tarea.
   b. Agregue el objeto de conexión rptParamConn a la tarea.
4. Solicite el informe utilizando uno de los métodos siguientes:
   - Ejecutar el informe inmediatamente
   - Programar el informe
5. Ver el informe en la Consola de usuario.

Para Informes que no sean de instantáneas:

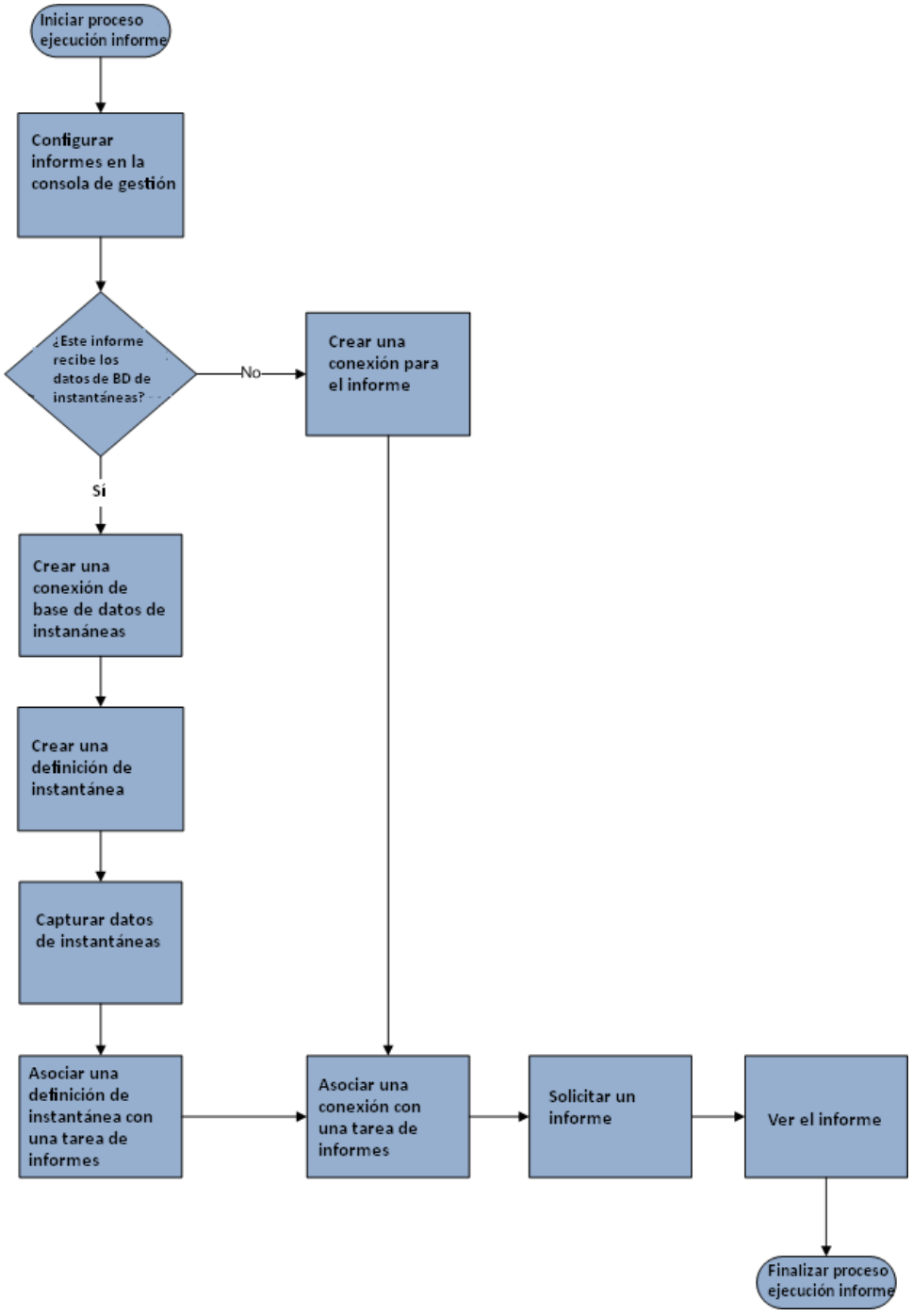
1. Cree un objeto de conexión con la información del origen de datos para el informe.
2. Modifique la tarea de informe en CA Identity Manager y agregue el objeto de conexión a la tarea.
3. Solicite el informe utilizando uno de los métodos siguientes:
   - Ejecutar el informe inmediatamente
   - Programar el informe
4. Ver el informe en la Consola de usuario.

Una vez que haya finalizado la configuración inicial del informe, se podrá solicitar un informe en CA Identity Manager. Puede ejecutar el informe inmediatamente o puede programarlo para que se ejecute más adelante. También se puede crear una programación de periodicidad para el informe en CA Identity Manager.

Por último, puede ver el informe en la Consola de usuario o puede exportarlo a varios formatos diferentes.

El proceso de informes

En la siguiente gráfica se explica el proceso que se requiere para ejecutar y ver informes:



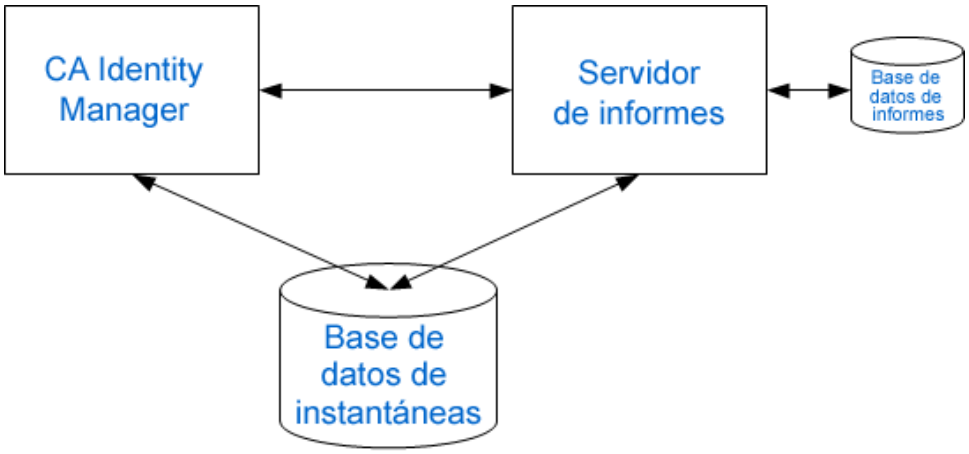
Cómo ejecutar informes de instantáneas

Los informes de CA Identity Manager permiten ver el estado actual de un entorno de CA Identity Manager. Puede utilizar esta información para garantizar la conformidad con las políticas empresariales internas o las normativas externas.

Los informes de CA Identity Manager se generan a partir de datos de gestión que describen la relación entre los objetos en un entorno de CA Identity Manager. Como ejemplos de datos de gestión podemos indicar los siguientes:

- Atributos de perfil de los usuarios
- Lista de roles que contienen una tarea determinada
- Los miembros de un rol o grupo
- Las reglas que componen un rol

En CA Identity Manager, la configuración de generación de informes requiere los tres componentes principales siguientes:



Nota: La base de datos de instantáneas de este gráfico de ilustración podría ser también la base de datos de auditoría o la base de datos de flujo de trabajo.

Servidor de informes

También conocido como CA Business Intelligence, este servidor genera informes, comunicándose directamente con CA Identity Manager y la base de datos de instantáneas.

Base de datos de informes

La base de datos donde el servidor de informes de CA (Business Objects) almacena sus propios datos.

CA Identity Manager

CA Identity Manager permite exportar los datos del objeto de CA Identity Manager a la base de datos de informes.

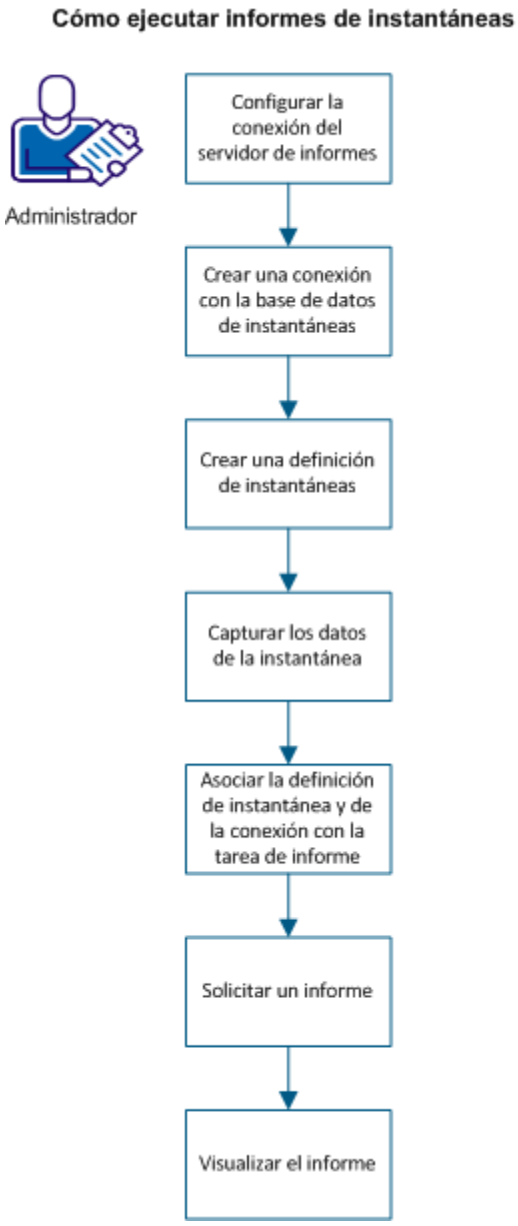
Base de datos de instantáneas

Una base de datos independiente que contiene los datos de instantánea de los objetos en CA Identity Manager

Importante: El servidor de informes utiliza Business Objects Enterprise. Si ya se dispone de un servidor de informes en el entorno y desea utilizarlo con CA Identity Manager, la versión mínima requerida por CA Identity Manager es CA Business Intelligence 3.2 SP5.

Un informes de instantánea incluye datos desde la base de datos de instantáneas y contiene información del almacén de objetos y del almacén de usuarios de CA Identity Manager. Un ejemplo de informe de instantáneas es el informe Perfil de usuario. Los datos de instantánea que se agregan a la base de datos de instantáneas se definen mediante el uso de definiciones de instantáneas que especifican la información incluida.

El gráfico siguiente ilustra el proceso para ejecutar un informe de instantánea:



Para ejecutar el informe de instantánea, realice los pasos siguientes:

1. Configuración de la conexión del servidor de informes. (en la página 436)
2. Creación de una conexión con la base de datos de instantáneas.
3. Creación de definiciones de instantáneas.
4. Captura de los datos de la instantánea.
5. Asociación de una definición de instantánea y de una conexión con la tarea de informe.

6. Solicitud de informes.
7. Visualización de informes. (en la página 440)

Configure la conexión del servidor de informes

Configure la conexión entre CA Identity Manager y el servidor de informes.

Nota: Se recomienda que todos los sistemas implicados en la generación de informes se configuren a la misma hora y zona horaria.

Para configurar la generación de informes

1. En la Consola de usuario, haga clic en Tareas, Sistema, Informe y, a continuación, Conexión del servidor de informes.
2. Introduzca la configuración del servidor de informes adecuada. Tenga en cuenta lo siguiente:
   - Nombre de host y puerto: el nombre de host y el número del puerto URL HTTP del sistema donde está instalado el servidor de informes.
   - Nombre de la carpeta de informes: ubicación predeterminada de los informes de CA Identity Manager.
   - ID de usuario: usuario creado para el servidor de informes.
   - Contraseña: contraseña para el usuario creado en el servidor de informes.
   - Conexión segura: seleccione la casilla de verificación para activar la conexión Secure Sockets Layer (SSL) entre CA Identity Manager y el servidor de informes.

     Nota: Antes de seleccionar la casilla de verificación Conexión segura, verifique que ha instalado el certificado de BOServer. Para obtener más información sobre cómo configurar SSL, consulte el capítulo "Instalación del servidor de informes" en la *Guía de instalación*.
   - Servidor Web: configurado como no IIS para Tomcat
3. Haga clic en Probar conexión para verificar la conexión.
4. Haga clic en Enviar.

Se establece la conexión del informe.

Creación de una conexión con la base de datos de instantáneas

CA Identity Manager necesita saber a dónde se deben exportar los datos de la instantánea. Cree una conexión con la base de datos de CA Identity Manager en la base de datos de instantáneas.

Para crear una conexión con la base de datos de instantáneas

1. En la Consola de usuario, haga clic en Tareas, Informes, Tareas de instantánea, Gestionar conexión a la base de datos de instantánea, Crear conexión de la base de datos de instantánea.
2. Para crear una conexión con la base de datos de instantáneas, complete todos los campos necesarios.
3. Haga clic en Enviar.

   Se creará una nueva conexión con la base de datos de instantáneas.

Creación de definiciones de instantáneas

Una instantánea refleja el estado de los objetos de CA Identity Manager en una hora determinada. Utiliza los datos de esta instantánea para generar un informe. Para capturar los datos de objeto de CA Identity Manager, se crea una definición de la instantánea que exporta los datos a la base de datos de instantánea. Mediante la definición de instantánea, se pueden definir las reglas para cargar usuarios, puntos finales, roles de administrador, roles de aprovisionamiento, grupos, y organizaciones.

Siga estos pasos:

1. En la Consola de usuario, vaya a Tareas, Informes, Tareas de instantánea, Gestionar definiciones de instantánea, Crear definición de instantánea.
2. Seleccione Crear una copia de un objeto del tipo Tipo de instantánea.
3. Haga clic en Aceptar.
4. Bajo la ficha Perfil, rellene los campos siguientes para crear un perfil de definición de instantáneas:

   Nombre de la definición de la instantánea

   Identifica el nombre único que se asigna a la definición de instantánea.

   Descripción de la definición de la instantánea

   Muestra cualquier otra información que desee para describir la instantánea.

   Activado

   Especifica que CA Identity Manager cree una instantánea en función de la definición de la instantánea actual a la hora programada.

   Nota: Si no se selecciona esta opción, la definición de instantánea no se capturará a la hora programada. Asimismo, la definición de la instantánea no aparecerá en la pantalla Datos de la instantánea de captura.

   Número de instantáneas retenidas

   Especifica el número de instantáneas correctas que se retienen en la base de datos de instantáneas.

   Nota: Si no se especifica un valor en este campo, CA Identity Manager almacenará una cantidad ilimitada de instantáneas.
5. En la ficha Políticas de instantánea, seleccione los objetos relacionados con las políticas para exportar.
6. En la ficha Configuración del rol, seleccione uno o más componentes del rol y atributos disponibles para la exportación de instantáneas.

   Nota: En la ficha Políticas de instantánea, si se selecciona Rol de acceso, Rol de administrador u objeto de Rol de aprovisionamiento, se deben seleccionar los atributos en la ficha Configuración del rol.
7. En la ficha Detalles de atributos de usuario, seleccione uno o más atributos de usuario de la instantánea que se va a exportar.

Nota: En la ficha Políticas de instantánea, si se selecciona solamente el objeto Usuario, se exportan de forma predeterminada todos los datos de atributos de usuario relacionados.

8. En la ficha Atributos de cuenta de punto final, seleccione uno más atributos de cuenta de un tipo de punto final.

   Nota: Para un tipo de punto final seleccionado, se exportan de forma predeterminada todos los datos relacionados con atributos de cuenta de punto final. Para capturar datos relacionados con un atributo específico, seleccione el atributo adecuado. Para obtener más información sobre cómo seleccionar atributos que son necesarios para la exportación de un tipo de punto final, consulte la sección Informes predeterminados de la *Guía de configuración*.

9. (Opcional) Seleccione la casilla de verificación Exportar cuentas huérfanas para incluir cuentas de punto final sin usuario global en el servidor de aprovisionamiento.

   Nota: Para exportar datos de informes para informes no estándar, tendencias no estándar e informes de cuentas huérfanas, seleccione el atributo exceptionAccount y la casilla de verificación Exportar cuentas huérfanas.

10. Haga clic en Enviar.

    CA Identity Manager se configura para crear instantáneas de los objetos mencionados en la definición de instantáneas.

Ahora que se ha creado una definición de instantáneas, se pueden capturar datos de instantáneas inmediatamente o programar la exportación de datos de la instantánea más tarde. En el tema Datos de la instantánea de captura se proporciona más información.

Más información:

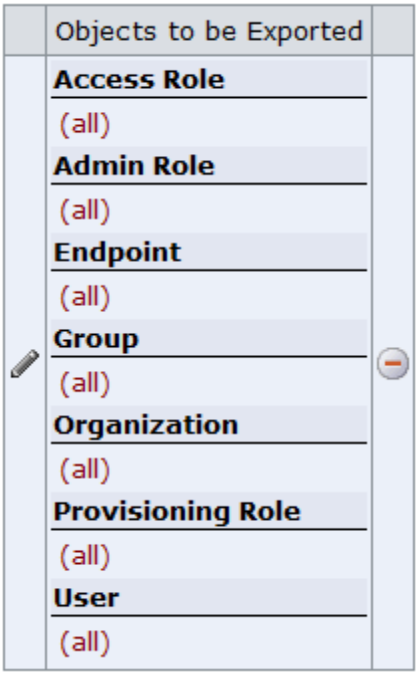
Ficha Repetición (en la página 427)

Ejemplo: creación de una definición de la instantánea para datos de atribución de usuario

En el siguiente ejemplo se muestra el proceso de creación de una definición de la instantánea para un informe de atribución de usuario:

1. En la Consola de usuario, vaya a Tareas, Informes, Tareas de instantánea, Gestionar definiciones de instantánea, Crear definición de instantánea.
2. Seleccione Crear un nuevo objeto del tipo Tipo de instantánea.
3. Introduzca el nombre de la definición de la instantánea, la descripción y el número de instantáneas que se conservan.
4. En la ficha Definición de política de instantánea, haga clic en Agregar.

   En el menú desplegable, seleccione el usuario y Todo. De forma similar, agregue el punto final, el rol de aprovisionamiento, el rol de administrador, el rol de acceso, la organización y el grupo tal y como se muestra en la siguiente pantalla:



5. En la ficha de Configuración del rol, active todas las casillas de verificación de rol de usuario.
6. En la ficha Atributos de usuario, seleccione los atributos obligatorios en la lista de valores disponibles y muévalos a la lista de valores actuales.
7. Haga clic en Enviar.

Gestión de instantáneas

CA Identity Manager permite ver, modificar y suprimir las definiciones de instantáneas. Al ver o modificar una definición de instantánea, se muestran las fichas Perfil y Mantenimiento. La ficha Mantenimiento sólo aparecerá después de que una instantánea se haya capturado una vez. En la ficha Mantenimiento, se pueden suprimir las instantáneas (aunque el estado de la instantánea sea de error).

Para ver, modificar o suprimir una definición de instantánea, vaya a Informes, Tareas de instantánea, Gestionar definiciones de instantánea, y haga clic en la tarea que desee ejecutar.

Nota: Si se está utilizando una definición de instantánea para exportar datos a la base de datos de instantáneas, no podrá suprimir tal definición. Al eliminar una definición de instantánea que se esté utilizando, la exportación de los datos a la base de datos de instantáneas se detendrá, pero la definición de la instantánea seguirá estando disponible.

Captura de datos de instantánea

Si desea capturar los datos de instantánea inmediatamente o programar la exportación de datos de instantánea más adelante o en una programación repetitiva, ejecute la tarea Datos de la instantánea de captura. Esta tarea exporta los datos inmediatamente (definidos por la definición de instantánea) a la base de datos de instantáneas.

Importante: La exportación de los datos de instantánea puede tardar unos minutos si se va a exportar una gran cantidad de datos. Es recomendable programar las instantáneas al exportar una gran cantidad de datos.

Para capturar datos de la instantánea

1. En la Consola de usuario vaya a Tareas, Informes, Tareas de instantánea, Datos de la instantánea de captura.
2. Seleccione Ejecutar ahora para ejecutar la exportación de datos inmediatamente o seleccione Programar nuevo trabajo (en la página 427) para ejecutar la exportación de datos posteriormente o en una programación repetitiva.
3. Haga clic en Siguiente.
4. Elija una definición de instantánea.
5. Haga clic en Enviar.

   Los datos de la instantánea se exportan a la base de datos de instantáneas.

Nota: Si le parece que la tarea Datos de la instantánea de captura es demasiado lenta, puede comprobar el progreso de la tarea en la ficha Sistema, haciendo clic en Ver tareas enviadas.

Ficha Repetición

Esta ficha permite programar los trabajos. A continuación se especifican los distintos campos de esta ficha:

Ejecutar ahora

Ejecuta el trabajo inmediatamente.

Programar nuevo trabajo

Programa un nuevo trabajo.

Modificar trabajo existente

Especifica la modificación de un trabajo ya existente.

Nota: Este campo sólo aparece si se ha programado un trabajo para esta tarea.

Nombre de trabajo

Especifica el nombre del trabajo que desea crear o modificar.

Zona horaria

Especifica la zona horaria del servidor.

Nota: Si su zona horaria es diferente a la zona horaria del servidor, se mostrará un cuadro desplegable que le permitirá seleccionar su zona horaria o la zona horaria del servidor cuando programe una nueva tarea. Cuando modifique un trabajo existente, no podrá cambiar la zona horaria.

Programación diaria

Especifica que el trabajo se ejecutará cada cierto número de días.

Cada (número de días)

Define cada cuantos días se ejecuta el trabajo.

Programación semanal

Especifica que el trabajo se ejecuta en un día concreto o en varios días y horas durante una semana.

Día de la semana

Especifica el día o los días de la semana en los que se ejecuta el trabajo.

Programación mensual

Especifica el día de la semana o día del mes en el que se ejecuta el trabajo mensualmente.

Programación anual

Especifica un día de la semana o día del mes en el que se ejecuta el trabajo anualmente.

Programación avanzada

Especifica información de programación adicional.

Expresión cron

Para obtener información sobre el modo de rellenar este campo, consulte lo siguiente:

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Tiempo de ejecución

Especifica la hora del día a la que se ejecuta el trabajo en formato de 24 horas. Por ejemplo, 14:15.

Asociación de una definición de instantánea con una tarea de informe

Asigne una definición de instantánea a una tarea de informe, de manera que CA Identity Manager sepa la definición de instantánea que debe utilizar al ejecutar el informe. Además, la información de los informes de CA Identity Manager puede provenir de varios orígenes, y cada informe se debe asociar con un origen de datos específico, dependiendo de la información que desee ver en el informe.

Para asociar una definición de instantánea y una conexión con una tarea de informe

1. En la Consola de usuario, vaya a Tareas, Roles y tareas, Tareas de administración, Modificar la tarea de administración.
2. Busque la tarea de informe con la que desee asociar una definición de instantánea.
3. Vaya a la ficha Fichas y haga clic en el botón Editar situado junto a la ficha Definiciones de instantáneas asociadas.
4. Haga clic en Agregar.
5. Busque la definición de instantánea con la que vaya a asociar la tarea de informe y haga clic en Seleccionar.

   Cuando asocie una definición de instantánea con una tarea de informe, tenga en cuenta lo siguiente:

   - Un informe se puede asociar con una o más definiciones de instantánea.
   - Una definición de instantánea se puede asociar con más de un informe.
   - Varias instantáneas asociadas con una tarea de informe único no deben usar el mismo tiempo de repetición.
6. Haga clic en Aceptar.
7. Vaya a la ficha Buscar y haga clic en Examinar para ubicar las pantallas de búsqueda.
8. Edite la pantalla de búsqueda de la tarea de informe y seleccione rptParamConn en Connection Object para el informe.

9. Haga clic en Aceptar.
10. Haga clic en Seleccionar.
11. Haga clic en Enviar.

Sincronización de cuentas de punto final con plantillas de cuenta

Esta tarea sincroniza una cuenta de punto final después de la modificación de una plantilla de cuenta asociada. Por ejemplo, quizás una cuenta de Active Directory no tiene ningún grupo, pero la plantilla de cuenta asociada está definida para incluir grupos.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Tareas, Puntos finales, Gestionar puntos finales, Comprobar sincronización de cuentas de puntos finales.
3. Seleccione un punto final.

   Se abrirá una pantalla que muestra las cuentas en ese punto final, las plantillas de cuenta asociadas y qué atributos no están sincronizados.
4. Haga clic en Sincronizar para hacer que los atributos de esas cuentas coincidan con lo definido en la plantilla de cuenta.

   Los cambios realizados en las plantillas de cuenta afectan a las cuentas existentes como se muestra a continuación:

   - Si se cambia el valor de un atributo de capacidad, se actualizará el atributo de cuenta correspondiente para que esté sincronizado con el valor de atributo de la plantilla de cuenta. Consulte la descripción de la sincronización débil y estricta.
   - El conector designa algunos atributos de cuenta como no actualizados por los cambios de la plantilla de cuenta. Los ejemplos incluyen ciertos atributos que el tipo de punto final solamente permite establecer durante la creación de cuenta y el atributo Contraseña.

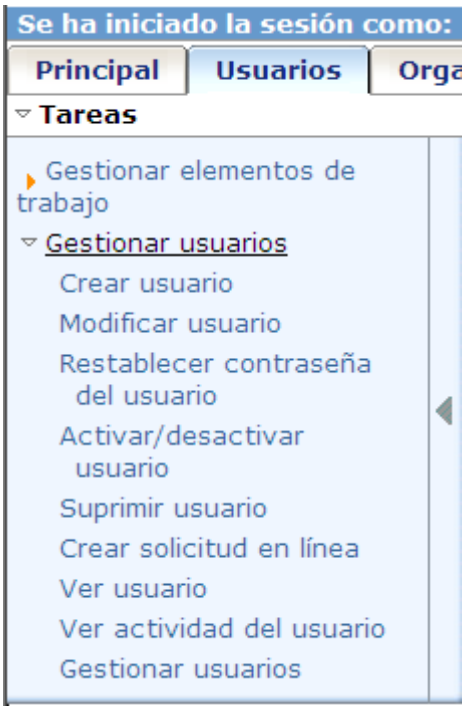
Ejemplo de una tarea de administración

Cuando se crea una tarea de administración, se define el contenido y el diseño de las pantallas de la tarea. Esta definición incluye:

- El nombre de la tarea.
- La categoría donde aparece la tarea.

- Las fichas y los campos que se utilizarán en la tarea, y las propiedades de pantalla de los campos.
- Los campos que puede usar un administrador en una consulta de búsqueda y los campos que se muestran en los resultados de la búsqueda.

Para comprender los elementos de una tarea, parta de la tarea Modificar usuario. En este caso, Usuarios es la categoría, Gestionar usuarios es una subcategoría y Modificar usuario es la tarea. Los nombres de la categoría y de la tarea se crean en el momento de crear la tarea.



Al seleccionar Modificar usuario, aparecerá una pantalla de búsqueda. La *pantalla de búsqueda* muestra las opciones para buscar el objeto que se desea ver o modificar. Cada opción se denomina *filtro* y estos filtros constituyen un límite para los objetos hallados en la búsqueda.

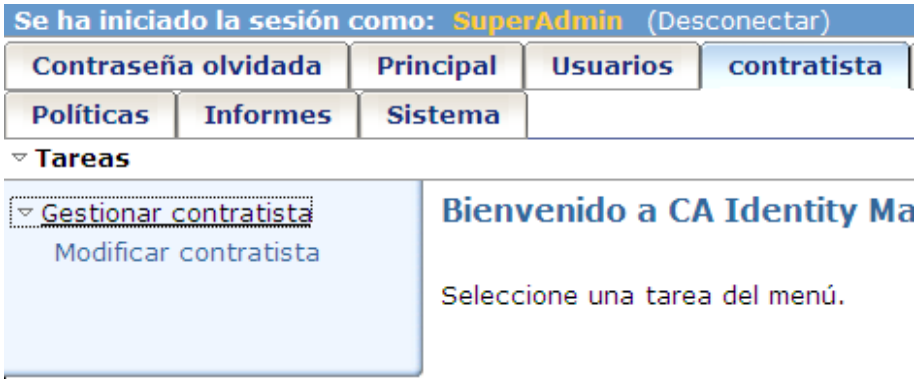
Una vez que haya completado la pantalla de búsqueda, aparece una pantalla con fichas. Por ejemplo, la siguiente ilustración muestra las fichas de la tarea Modificar usuario. La ficha Perfil es la primera en aparecer y muestra los atributos de usuario; las otras fichas muestran la función y los privilegios de grupo correspondientes al usuario.

Para las tareas que crea, debe decidir qué fichas incluir y determinar el orden y el contenido.

Por ejemplo, con la tarea Modificar usuario como plantilla, podría crear una tarea Modificar contratista, que incluya cambios en:

- Los campos de la ficha Perfil.
- Las fichas que se incluyen la tarea y su contenido.
- La categoría en la que aparece la tarea.

  Podría crear esta tarea en una categoría nueva: Contratista.



La tarea Modificar contratista incluye algunos de los campos de la ficha Perfil de la tarea Modificar usuario además de otros campos, como la fecha de inicio del contrato y la empresa del contratista. Para buscar un contratista, los administradores pueden buscar por nombre del contratista, empresa y fecha de inicio.

La nueva tarea también incluye una ficha Roles del contratista donde puede agregar roles para los contratistas.

Solicitud de informe

Para ver el informe, solicite un informe a un usuario que disponga de privilegios de administración de informes. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario con privilegios de usuario de tareas de informes.
2. Seleccione Tareas, Informes, Tareas de informes y Solicitar un informe.

   Aparecerá una lista de informes.
3. Seleccione el informe que desee solicitar.

   Aparecerá una pantalla de parámetros.

Proporcione la información de parámetros que se le solicite.

Nota: Si está ejecutando un informe de instantánea y no hay ninguna instantánea disponible para este informe, en primer lugar deberá capturar una instantánea.

- Algunos informes muestran el estado del sistema en un momento específico en el tiempo. Cuando se pide este tipo de informe, se selecciona un momento en el tiempo para el cual se desea consultar los datos del informe. A este momento en el tiempo se le llama *instantánea*.

  Nota: La fecha y hora de la instantánea que se pueden elegir son predeterminadas. Normalmente el administrador del sistema u otro usuario con privilegios de administración de informes realiza la configuración de la instantánea. Si no hay ninguna instantánea disponible para el informe que se desea solicitar, póngase en contacto con un administrador del sistema.

- Algunos informes muestran la actividad en un período de tiempo. Los títulos de estos informes normalmente empiezan con la palabra *Auditoría*. Cuando se solicita este tipo de informe, se especifica un período de tiempo para el cual se desea consultar los datos del informe. Por ejemplo, se puede ejecutar el Informe de contraseñas restablecidas según datos de auditoría de los últimos 30 días.

4. Haga clic en Programar informe y seleccione una programación para su informe.

   Ahora

   Especifica que el informe se ejecuta de inmediato.

   Una vez

   Especifica que el informe se ejecuta una vez,durante un período de tiempo específico. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

   Nota: Tenga en cuenta si desea seleccionar esta opción cuando el informe que está solicitando requiere una gran cantidad de datos. Para conservar los recursos del sistema, elija un momento en el que haya menos actividad del sistema.

5. Haga clic en Enviar.

   La solicitud de informe se ha enviado. En función de la configuración del entorno, la solicitud se ejecuta inmediatamente o se ejecuta después de la aprobación por parte de un administrador.

   Normalmente un administrador del sistema u otro usuario con privilegios de administración de informes deben aprobar una solicitud de informes antes de que el sistema la complete. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Visualización del informe

Es posible que, en función de la configuración del entorno, un informe no esté disponible para consultarlo hasta que un administrador haya aprobado la solicitud para ese informe. Si su solicitud de informes tiene una aprobación pendiente, el sistema le envía una alerta de correo electrónico. El informe que se desea consultar no aparece en la lista de búsqueda hasta que se aprueba.

Nota: Para poder ver informes en CA Identity Manager mediante el uso de la tarea Ver mis informes, es necesario activar una sesión con cookies de terceros en el explorador.

Siga estos pasos:

1. En la Consola de usuario, vaya a Tareas, Informes, Tareas de informes y, a continuación, haga clic en Ver mis informes.
2. Busque el informe generado que desea ver.

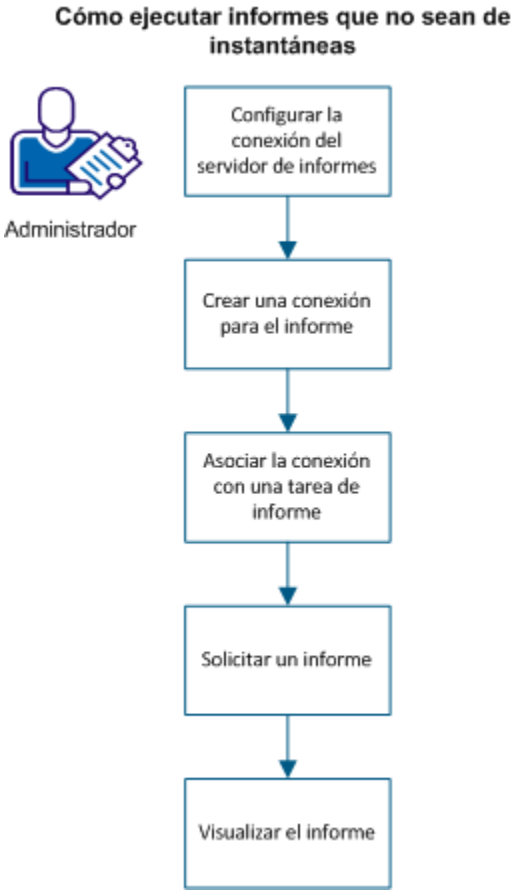
   Se mostrarán tanto las instancias de los informes generados mediante repetición como los generados a petición.

   Nota: Si el estado del informe es Pendiente/Repetición, el informe no se genera y puede tardar tiempo en completarse la acción.
3. Seleccione el informe que desea ver.
4. (Opcional) Haga clic en Exportar este informe (esquina superior izquierda) para exportar el informe a los formatos siguientes:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003), datos solo
   - Microsoft Excel (97-2003), editable
   - Formato de texto enriquecido (RTF)
   - Valores separados por comas (CSV)
   - XML

Cómo ejecutar informes que no sean de instantáneas

Un informe que no sea de instantánea incluye datos de otros orígenes de datos, como la auditoría, el flujo de trabajo o las bases de datos de persistencia de la tarea. CA Identity Manager incluye informes de auditoría predeterminados con el prefijo "Audit-" en su nombre, en la consola de usuario. De forma predeterminada, CA Identity Manager incluye solamente informes de auditoría, pero se pueden crear sus propios informes personalizados que pueden incluir datos de cualquier origen de datos.

Este escenario describe cómo configura un súperadministrador una conexión de la base de datos de informes y ejecuta un informe que no sea de instantánea.



El diagrama siguiente ilustra el proceso para ejecutar un informe de instantánea:

Para ejecutar el informe que no sea de instantánea, realice los pasos siguientes:

1. Configuración de la conexión del servidor de informes. (en la página 436)
2. Creación de una conexión para el informe.
3. Asociar una conexión con una tarea de informe

4. Solicitud de informes.
5. Visualización de informes. (en la página 440)

Configure la conexión del servidor de informes

Para recopilar datos del servidor de informes, se debe configurar la conexión al servidor de informes. Antes de empezar el procedimiento, recopile la información siguiente acerca del servidor de informes:

Nombre	Descripción
Nombre del host	El nombre de host del equipo donde se instala el servidor de informes
Puerto	El nombre de puerto del equipo donde se instala el servidor de informes
Nombre de la carpeta Informes	La ubicación de los informes de CA Identity Manager predeterminados.
ID de usuario	Especifica el usuario creado para el servidor de informes.
Contraseña	Especifica la contraseña para el usuario creado en el servidor de informes.
Conexión segura	Especifica la conexión de seguridad para el servidor de informes. Seleccione la casilla de verificación para permitir la conexión de Capa de sockets seguros (SSL) entre CA Identity Manager y el servidor de informes. **Nota**: Antes de seleccionar la casilla de verificación Conexión segura, verifique que ha instalado el certificado de BOServer. Para obtener más información sobre cómo configurar SSL, consulte el capítulo "Instalación del servidor de informes" en la *Guía de instalación*.
Servidor web	Especifique el servidor web. Configure como no IIS para Tomcat.

Nota: Se recomienda que todos los sistemas implicados en la generación de informes se configuren a la misma hora y zona horaria.

Siga estos pasos:

1. En la Consola de usuario, haga clic en Sistema, Informe y, a continuación, Conexión del servidor de informes.
2. Introduzca la configuración del servidor de informes adecuada.
3. Haga clic en Probar conexión para verificar la conexión.
4. Haga clic en Enviar.

Se establece la conexión del informe.

Creación de una conexión para el informe

La información de los informes de CA Identity Manager puede provenir de varios orígenes. Con el fin de especificar detalles de la conexión para otro origen de datos del informe, cree una conexión JDBC en CA Identity Manager.

Siga estos pasos:

1. En la Consola de usuario, vaya a Tareas, Sistema, Gestión de la conexión JDBC, Crear conexión JDBC.
2. Cree un nuevo objeto de conexión o seleccione un objeto de conexión basado en un origen de datos JNDI específico.
3. Rellene todos los campos necesarios y haga clic en Enviar.

   Se creará una nueva conexión JDBC.

Importante: Se recomienda*no* utilizar la base de datos del almacén de objetos de CA Identity Manager para generar informes.

Asociación de una conexión con una tarea de informe

La información de los informes de CA Identity Manager puede provenir de varios orígenes y cada informe se debe asociar con un origen de datos específico, dependiendo de la información que desee ver en el informe.

Para asociar una conexión con una tarea de informe

1. En la Consola de usuario, vaya a Tareas, Roles y tareas, Tareas de administración, Modificar la tarea de administración.
2. Busque la tarea de informe con la que desee asociar una conexión.
3. Vaya a la ficha Buscar y haga clic en Examinar para ubicar las pantallas de búsqueda.
4. Edite la pantalla de búsqueda de la tarea de informe y seleccione una conexión en Objeto de conexión para el informe.
5. Haga clic en Aceptar.
6. Haga clic en Seleccionar.
7. Haga clic en Enviar.

Solicitud de informe

Para ver el informe, solicite un informe a un usuario que disponga de privilegios de administración de informes. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario con privilegios de usuario de tareas de informes.
2. Seleccione Tareas, Informes, Tareas de informes y Solicitar un informe.

   Aparecerá una lista de informes.
3. Seleccione el informe que desee solicitar.

   Aparecerá una pantalla de parámetros.

   Proporcione la información de parámetros que se le solicite.

   Nota: Si está ejecutando un informe de instantánea y no hay ninguna instantánea disponible para este informe, en primer lugar deberá capturar una instantánea.

   - Algunos informes muestran el estado del sistema en un momento específico en el tiempo. Cuando se pide este tipo de informe, se selecciona un momento en el tiempo para el cual se desea consultar los datos del informe. A este momento en el tiempo se le llama *instantánea*.

     Nota: La fecha y hora de la instantánea que se pueden elegir son predeterminadas. Normalmente el administrador del sistema u otro usuario con privilegios de administración de informes realiza la configuración de la instantánea. Si no hay ninguna instantánea disponible para el informe que se desea solicitar, póngase en contacto con un administrador del sistema.
   - Algunos informes muestran la actividad en un período de tiempo. Los títulos de estos informes normalmente empiezan con la palabra *Auditoría*. Cuando se solicita este tipo de informe, se especifica un período de tiempo para el cual se desea consultar los datos del informe. Por ejemplo, se puede ejecutar el Informe de contraseñas restablecidas según datos de auditoría de los últimos 30 días.

4. Haga clic en Programar informe y seleccione una programación para su informe.

   Ahora

   Especifica que el informe se ejecuta de inmediato.

   Una vez

   Especifica que el informe se ejecuta una vez,durante un período de tiempo específico. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

   Nota: Tenga en cuenta si desea seleccionar esta opción cuando el informe que está solicitando requiere una gran cantidad de datos. Para conservar los recursos del sistema, elija un momento en el que haya menos actividad del sistema.

5. Haga clic en Enviar.

   La solicitud de informe se ha enviado. En función de la configuración del entorno, la solicitud se ejecuta inmediatamente o se ejecuta después de la aprobación por parte de un administrador.

   Normalmente un administrador del sistema u otro usuario con privilegios de administración de informes deben aprobar una solicitud de informes antes de que el sistema la complete. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Visualización del informe

Es posible que, en función de la configuración del entorno, un informe no esté disponible para consultarlo hasta que un administrador haya aprobado la solicitud para ese informe. Si su solicitud de informes tiene una aprobación pendiente, el sistema le envía una alerta de correo electrónico. El informe que se desea consultar no aparece en la lista de búsqueda hasta que se aprueba.

Nota: Para poder ver informes en CA Identity Manager mediante el uso de la tarea Ver mis informes, es necesario activar una sesión con cookies de terceros en el explorador.

Siga estos pasos:

1. En la Consola de usuario, vaya a Informes, Tareas de informes y, a continuación, haga clic en Ver mis informes.
2. Busque el informe generado que desea ver.

   Se mostrarán tanto las instancias de los informes generados mediante repetición como los generados a petición.

   Nota: Si el estado del informe es Pendiente/Repetición, el informe no se genera y puede tardar tiempo en completarse la acción.
3. Seleccione el informe que desea ver.
4. (Opcional) Haga clic en Exportar este informe (esquina superior izquierda) para exportar el informe a los formatos siguientes:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003), datos solo
   - Microsoft Excel (97-2003), editable
   - Formato de texto enriquecido (RTF)
   - Valores separados por comas (CSV)
   - XML

Establecimiento de las opciones de generación de informes

Configure el número de instancias de informe que puede generar un usuario para un informe específico.

Para modificar las opciones de informe

1. Seleccione Tareas, Informes, Tareas de informes, Establecer opciones de generación de informes.

   CA Identity Manager se conecta al servidor de informes de IAM y recupera una lista con todos los informes.

2. Elija un informe y haga clic en Modificar.

   Aparecerá el panel de atributos del informe.

3. Modifique los siguientes campos:

   Nombre

   Especifica el nombre de pantalla del informe seleccionado.

   Número de instancias

   Especifica el número de instancias permitidas que puede generar un usuario para este informe.

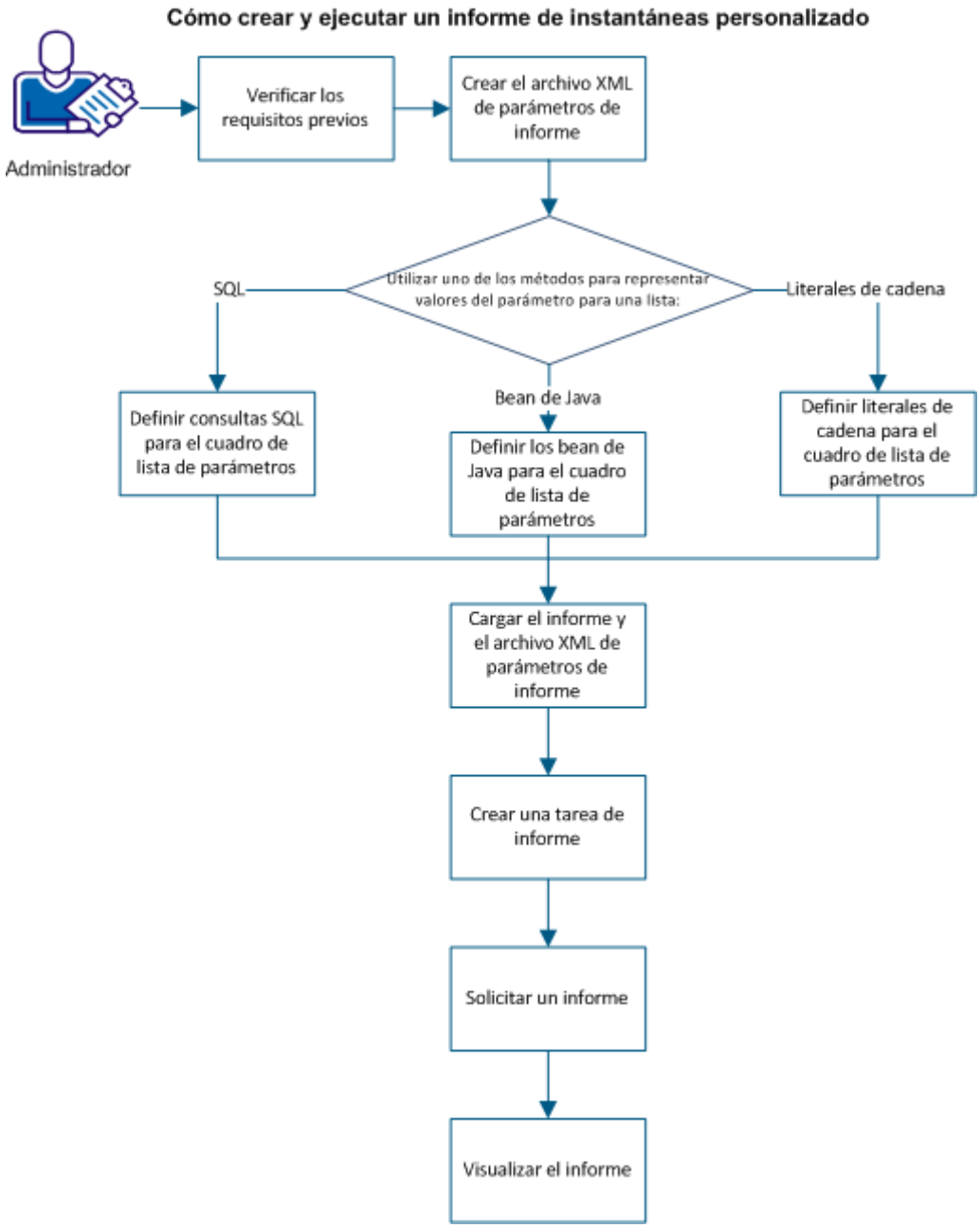
4. Haga clic en Aceptar.

   Se cambian los atributos de informes.

Cómo crear y ejecutar un informe de instantáneas personalizado

CA Identity Manager permite crear y personalizar informes para adaptarse a las necesidades de su negocio. CA Identity Manager proporciona un archivo XML de parámetros del informe que incluye todos los parámetros relacionados con atributos de generación de informes. Según las necesidades de negocio, se pueden elegir los atributos obligatorios para rellenar los datos del informe desde el origen de datos de instantánea.

El gráfico siguiente ilustra el proceso para crear y ejecutar un informe de instantáneas personalizado:



Como administrador del sistema, realice los pasos siguientes:

1. Verificación de los requisitos previos (en la página 444)
2. Creación de archivos XML de parámetros de informe (en la página 444)
3. Utilice uno de los métodos siguientes para representar valores del parámetro para una lista:

- Definición de consultas SQL para el cuadro de lista de parámetros (en la página 448)
- Definición de los bean de Java para el cuadro de lista de parámetros (en la página 449)
- Definición de los literales de cadena para el cuadro de lista de parámetros (en la página 449)

4. Carga de informes y archivos XML de parámetros de informe (en la página 449)
5. Creación de tareas de informe
6. Solicitud de informes
7. Visualización de informes (en la página 440)

Creación de informes en Crystal Reports

Para utilizar los informes personalizados en CA Identity Manager, cree un informe (archivo RPT) en Crystal Reports Developer. Para obtener más información sobre cómo crear informes en Crystal Reports, consulte la documentación de Crystal Reports.

Nota: Si tiene que utilizar el esquema de CA Identity Manager para crear informes personalizados, el esquema de la base de datos de CA Identity Manager se encuentra en la siguiente ubicación:

```
C:\Archivos de programa\CA\Identity Manager\IAM Suite\Identity
Manager\db\objectstore
```

Creación de archivos XML de parámetros de informe

Un parámetro es uno de los campos de un informe que se puede utilizar para filtrar informes. Se pueden generar informes filtrando los datos mediante parámetros. Para permitir la personalización de la pantalla de búsqueda de informes, cada informe (archivo RPT) se asocia a un archivo XML de parámetros de informe. En CA Identity Manager, se pueden crear tareas del informe y crear la pantalla de búsqueda para que un usuario pueda iniciar sesión o seleccionar los datos obligatorios durante la generación de informes.

Nota: Solamente se necesita un archivo XML de parámetros de informe si el informe consulta atributos del objeto.

El archivo XML de parámetros de informe debe tener el mismo nombre que el informe (archivo RPT) con una extensión .xml. Por ejemplo, si se carga un informe denominado "prueba1.rpt" en el servidor de informes, el archivo XML debe denominarse "prueba1.xml".

El archivo XML de parámetros de informe contiene los siguientes elementos:

<product>

Identifica el producto para el que se utilizan los parámetros. Se pueden crear parámetros diferentes para diversos productos mediante el mismo archivo XML de parámetros.

<screen>

Define los parámetros que se muestran en una pantalla. Se puede utilizar el elemento de pantalla para enlazar los parámetros con una pantalla específica. El ID de pantalla es alfanumérico y único; se utiliza para identificar las pantallas y sus parámetros.

<parameters>

Especifica la recolección de parámetros para una pantalla.

<param>

Define el elemento de parámetro que se transfiere junto con los datos especificados al informe. Los siguientes atributos se utilizan en el elemento <param>:

id

Define con qué parámetro del informe asociarse.

Nota: El ID debe tener el mismo nombre que el parámetro en el Crystal Reports.

nombre

En este momento, CA Identity Manager no utiliza este campo. Establezca este atributo con el mismo valor que el ID.

displaytext

Especifica el texto sencillo que se mostrará en la pantalla para el parámetro.

type

Define el tipo de parámetro. La visualización de la pantalla varía en función de este atributo. Los tipos de parámetros compatibles son los siguientes:

- **Cuadro de texto**

  Ejemplo: <param id="param1" displaytext="First Name" name="param1" type="string"/>

- **Fecha y hora**

  Ejemplo: <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- **Lista desplegable**

  Ejemplo: <param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- **Cuadro de lista**

  Ejemplo: <param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- **Cuadro de radio**

  Ejemplo: <param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- **Casilla de verificación**

  Ejemplo: <param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

row

Define cuántas filas se mostrarán en un cuadro de lista.

Valor predeterminado: 5

default

Define el valor predeterminado que se mostrará en la pantalla para un parámetro determinado. Este atributo se puede utilizar con los tipos de cadena, cuadro de lista y lista desplegable.

Definición de consultas SQL para el cuadro de lista de parámetros

Se pueden definir consultas SQL como parte de un cuadro de lista o un cuadro desplegable en el archivo XML de parámetros de informe. Cuando se asocia un parámetro al informe y se crea una tarea del informe, el parámetro aparecerá en el cuadro de lista o en el cuadro desplegable para el usuario. Para utilizar SQL en el cuadro desplegable o parámetro de cuadro de lista, proporcione una instrucción SQL válida en el atributo de sql.

Ejemplo:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like 'S%/>
```

En el ejemplo anterior, se proporcionan al informe todos los apellidos de los usuarios cuyo nombre empiece por *S*.

Sin embargo, la condición del nombre que empieza por *S* es estática. Esta consulta no resulta lo bastante flexible como para que un usuario cargue el valor en función del valor del parámetro introducido en una de las pantallas anteriores que se ha utilizado en el mismo grupo de parámetros de informe. Para utilizar un valor que se haya introducido anteriormente en otra pantalla, la instrucción SQL se puede aumentar con *##<parameter id>##*.

Por ejemplo, si se tiene un parámetro con la condición id=Usuario del tipo Cadena:

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

Si se desea utilizar el valor de entrada para el parámetro en SQL, la instrucción SQL podría ser la siguiente:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like '##User##'/>
```

CA Identity Manager sustituirá ##User## por el valor que se haya introducido para el parámetro con la condición id=Usuario.

Nota: El valor del parámetro que se tiene que sustituir no puede estar en la misma pantalla que el parámetro de SQL. Por ejemplo, si *lstlastname2* está en la pantalla 3, el parámetro de usuario debería estar en una de las pantallas anteriores.

Definición de los bean de Java para el cuadro de lista de parámetros

Si no se puede realizar correctamente con SQL, se pueden utilizar los bean de java para calcular valores y proporcionar la lista de pares <clave, valor> a CA Identity Manager. Los bean de Java deben estar en la ruta de clase de CA Identity Manager.

Ejemplo:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

En el ejemplo anterior, TestDataCollector recupera los valores a su manera y envía los datos al informe para la lista desplegable. Los pares <clave, valor> se separan con %1F.

Asegúrese de que el bean de Java esté en el directorio iam_im.ear\custom.

Nota: Para obtener más información sobre la implementación de bean de Java, consulte la documentación de Business Objects.

Definición de los literales de cadena para el cuadro de lista de parámetros

La forma más sencilla de representar los valores del parámetro para una lista o cuadro desplegable es mediante los literales de cadena. %1F y cada par <clave, valor> delimitan los valores clave y se separarán mediante %1E.

Ejemplo:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

Carga de informes y archivos XML de parámetros de informe

Una vez creados el informe (RPT) y el archivo XML de parámetros de informe correspondiente, cargue los dos archivos en el servidor de informes (Business Objects).

Siga estos pasos:

1. Inicie sesión en la Consola de gestión central de Business Objects.
2. Haga clic en Carpetas.
3. Seleccione la carpeta de informes de IM.
4. Cree un paquete de objetos.
5. En el nuevo paquete de objetos, busque la ubicación para agregar Crystal Report.
6. Busque el nuevo informe (RPT) que se haya creado.

   Nota: Asegúrese de que la carpeta de informes de IM esté seleccionada como la carpeta donde se guardará el informe.

7. Haga clic en OK.

   Se agrega el archivo Crystal Report.

8. En el nuevo paquete de objetos, agregue un nuevo documento local y busque la ubicación del nuevo archivo XML de parámetros del informe.
9. Seleccione el tipo de archivo como *texto*.
10. Haga clic en OK.

El informe y el archivo xml de parámetros del informe se ha cargado ahora. Para verificarlo, vaya a la carpeta de informes de IM y verifique que los dos archivos nuevos estén disponibles.

Creación de tareas de informe

Las tareas de informe se utilizan para crear, gestionar, ver y suprimir las plantillas correspondientes a los informes que se generan en la Consola de usuario.

Siga estos pasos:

1. En la Consola de usuario, vaya a Tareas, Roles y tareas, Tareas de administración, Crear tarea de administración.
2. Seleccione Crear una nueva tarea de administración y haga clic en Aceptar.
3. En la ficha Perfil, rellene los siguientes campos:

   Nombre

   Define el nombre del informe. Cada nombre de la tarea de informe debe ser único.

   Etiqueta

   Define el identificador único de la tarea. Se utiliza en una dirección URL, un servicio web o en archivos de propiedades. Debe incluir letras, números o guiones bajos, así como comenzar por una letra o guion bajo.

   Categoría

   Especifica la categoría a la que pertenece la tarea actual.

   Nota: Seleccione la categoría Informes.

   Categoría 2

   Especifica la subcategoría a la que pertenece la tarea actual. Introduzca cualquier cadena en este campo.

   Objeto primario

   Especifica el objeto sobre el que opera la tarea.

   Nota: Seleccione la instancia de informe como el objeto primario.

   Acción

   Especifica la acción que se realiza en el objeto primario.

   Nota: Seleccione Crear como acción.
4. Para crear una pantalla de búsqueda nueva para la tarea del informe, realice los pasos siguientes:
   a. Vaya a la ficha Buscar y haga clic en Examinar para buscar las pantallas de búsqueda.

      Aparecerá la lista de pantallas de búsqueda disponibles.

   b. Haga clic en Nuevo.

      Aparecerá el panel Crear pantalla.

c. Seleccione la Pantalla de selección de plantillas de informes de la lista y haga clic en Aceptar.

   CA Identity Manager se conecta al servidor de informes y muestra todos los informes.

d. Rellene los campos siguientes:

   Nombre

   Define el nombre del informe. Cada nombre de tarea de informe debe ser único.

   Etiqueta

   Actúa como un identificador único dentro de una tarea. Puede contener caracteres ASCII (a-z, A-Z), números (0-9) o signos de subrayado y comenzar por una letra o un signo de subrayado.

   Título

   Define el título de la nueva pantalla de búsqueda. El título debe ser único.

   Plantilla del informe

   Identifica el informe para asociarse con la pantalla de búsqueda.

   Nota: Elija uno de los informes agregados al servidor de informes.

   Objeto de conexión para el informe

   Define los detalles de la conexión del origen de datos que se tiene que utilizar para el informe.

5. Haga clic en Aceptar.

   La nueva pantalla de búsqueda se ha creado ahora para los informes.

6. En la ficha de creación de fichas para la tarea de informe, realice los pasos siguientes:

   a. Haga clic en Fichas.

      Aparecen las fichas que son visibles para el usuario.

   b. Seleccione Controlador de ficha estándar.

   c. Si el informe utiliza una definición de la instantánea, realice los pasos siguientes:

      a. ¿En qué fichas debería aparecer esta tarea? Seleccione las Definiciones de instantáneas asociadas.

         La ficha Definiciones de instantáneas asociadas se agrega a la lista de fichas.

      b. Haga clic en  para editar la ficha Definiciones de instantáneas asociadas.

      c. Haga clic en Agregar para asociar la tarea de informe a una definición de la instantánea.

Se mostrará una lista de las definiciones de la instantánea disponibles.

d. Seleccione una definición de la instantánea y haga clic en Aceptar.

La tarea de informe se asociará a una definición de la instantánea.

d. Haga clic en Enviar.

Se crearán las tareas de informe.

e. Asigne la nueva tarea de informe a un rol de administrador.

Los usuarios de rol de administrador de CA Identity Manager pueden utilizar la nueva tarea del informe.

La tarea del informe está ahora lista para que el administrador la utilice.

Nota: Un informe (archivo RPT) se puede asociar solamente a *una* tarea de informe.

Solicitud de informe

Para ver el informe, solicite un informe a un usuario que disponga de privilegios de administración de informes. Normalmente un administrador del sistema u otro usuario con privilegios de administración de informes deben aprobar una solicitud de informes antes de que el sistema la complete. Es necesaria una aprobación porque algunos informes pueden requerir mucho tiempo o recursos del sistema significativos para ejecutarse. Si su solicitud de informes requiere aprobación, el sistema le envía una alerta de correo electrónico.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como un usuario con acceso a las tareas de informes.
2. En el menú de navegación, seleccione Tareas, Informes, Tareas de informes, Solicitar un informe.

   Aparecerá una lista de informes.
3. Seleccione el informe que desee solicitar.

   Aparecerá una pantalla de parámetros.
4. Proporcione la información de parámetros que se le solicite.

   Nota: Si está ejecutando un informe de instantánea y no hay ninguna instantánea disponible para este informe, en primer lugar deberá capturar una instantánea.

   - Algunos informes muestran el estado del sistema en un momento específico en el tiempo. Cuando se pide este tipo de informe, se selecciona un momento en el tiempo para el cual se desea consultar los datos del informe. A este momento en el tiempo se le llama *instantánea*.

     Nota: La fecha y hora de la instantánea que se pueden elegir son predeterminadas. Normalmente el administrador del sistema u otro usuario con privilegios de administración de informes realiza la configuración de la instantánea. Si no hay ninguna instantánea disponible para el informe que se desea solicitar, póngase en contacto con un administrador del sistema.
   - Algunos informes muestran la actividad en un período de tiempo. Los títulos de estos informes normalmente empiezan con la palabra *Auditoría*. Cuando se solicita este tipo de informe, se especifica un período de tiempo para el cual se desea consultar los datos del informe. Por ejemplo, se puede ejecutar el Informe de contraseñas restablecidas según datos de auditoría de los últimos 30 días.
5. Haga clic en Programar informe y seleccione una programación para su informe.

   Ahora

   Especifica que el informe se ejecuta de inmediato.

   Una vez

Especifica que el informe se ejecuta una vez,durante un período de tiempo específico. Debe seleccionar la hora y fecha de inicio, así como de finalización a las que desee generar el informe.

Nota: Tenga en cuenta si desea seleccionar esta opción cuando el informe que está solicitando requiere una gran cantidad de datos. Para conservar los recursos del sistema, elija un momento en el que haya menos actividad del sistema.

6. Haga clic en Enviar.

   La solicitud de informe se ha enviado. En función de la configuración del entorno, la solicitud se ejecuta inmediatamente o se ejecuta después de la aprobación por parte de un administrador.

Visualización del informe

Es posible que, en función de la configuración del entorno, un informe no esté disponible para consultarlo hasta que un administrador haya aprobado la solicitud para ese informe. Si su solicitud de informes tiene una aprobación pendiente, el sistema le envía una alerta de correo electrónico. El informe que se desea consultar no aparece en la lista de búsqueda hasta que se aprueba.

Nota: Para poder ver informes en CA Identity Manager mediante el uso de la tarea Ver mis informes, es necesario activar una sesión con cookies de terceros en el explorador.

Siga estos pasos:

1. En la Consola de usuario, vaya a Tareas, Informes, Tareas de informes y, a continuación, haga clic en Ver mis informes.
2. Busque el informe generado que desea ver.

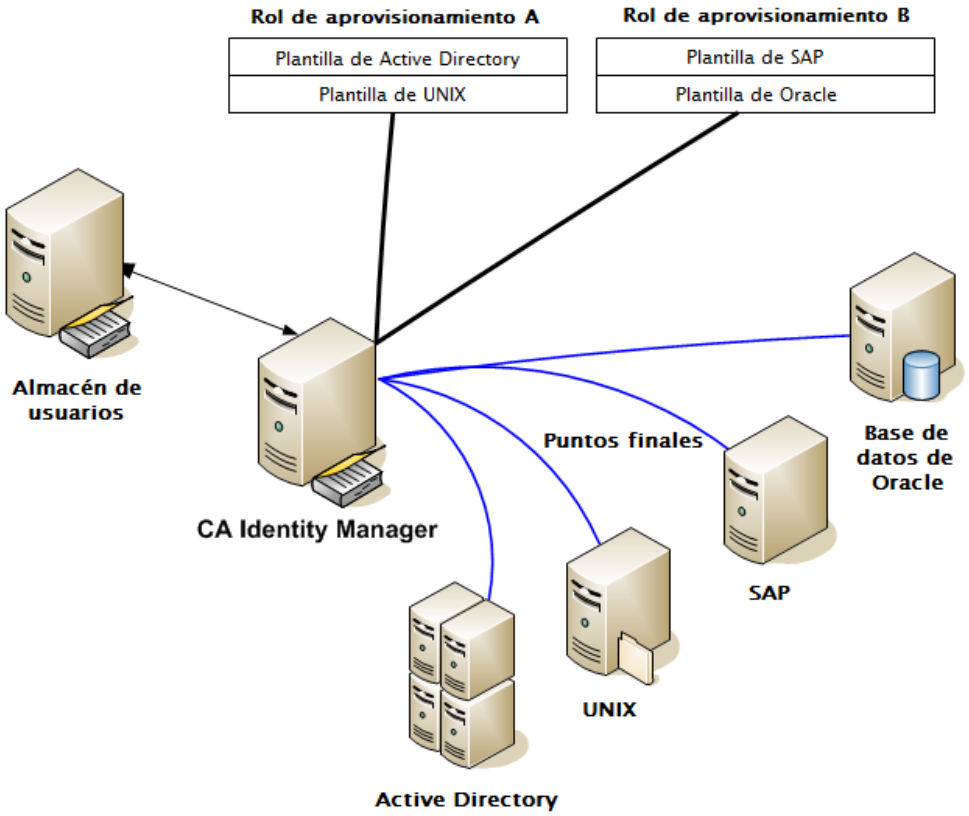
   Se mostrarán tanto las instancias de los informes generados mediante repetición como los generados a petición.

   Nota: Si el estado del informe es Pendiente/Repetición, el informe no se genera y puede tardar tiempo en completarse la acción.
3. Seleccione el informe que desea ver.
4. (Opcional) Haga clic en Exportar este informe (esquina superior izquierda) para exportar el informe a los formatos siguientes:
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003), datos solo
   - Microsoft Excel (97-2003), editable
   - Formato de texto enriquecido (RTF)
   - Valores separados por comas (CSV)
   - XML

Sincronización de usuarios, cuentas y roles

La integración de varios puntos finales y cuentas en un solo sistema de gestión de usuarios puede dar lugar a una pérdida de sincronización. Los roles de aprovisionamiento o plantillas de cuenta que se asignan a un usuario pueden diferir de las cuentas reales que existen para ese usuario.

Por ejemplo, pongamos una situación con dos roles de aprovisionamiento, uno con Active Directory y plantillas de cuenta de UNIX y otro rol con SAP y plantillas de Oracle. El usuario john_smith tiene el rol de aprovisionamiento A, que contiene Active Directory y plantillas de cuenta de UNIX, pero ese usuario solamente tiene una cuenta de Active Directory. Posiblemente la plantilla de cuenta de UNIX se ha agregado al rol después de que se asignara al usuario. Por lo tanto, el administrador sincroniza el usuario con la definición del rol actual.



Las situaciones siguientes son otros motivos por los cuales los usuarios pierden sincronización con roles de aprovisionamiento o plantillas de cuenta:

- Los intentos anteriores de crear las cuentas necesarias han producido un error debido a problemas de hardware o software en su red, causando que falten algunas cuentas.
- Los roles de aprovisionamiento y las plantillas de cuenta cambian, creando así cuentas adicionales o que faltan.
- Las cuentas se han asignado a plantillas de cuenta después de que se crearan, de manera que las cuentas existen pero no están sincronizadas con sus plantillas de cuenta.
- La creación de una nueva cuenta se retrasa porque se ha especificado que la cuenta se creará más tarde.
- Se ha adquirido un nuevo punto final. Durante la exploración y la correlación, el servidor de aprovisionamiento no asignaba roles de aprovisionamiento a los usuarios automáticamente. Se debe actualizar el rol para indicarlo a los usuarios que requieran cuentas en el punto final. Cualquier cuenta que se haya correlacionado con un usuario se clasifica como cuenta adicional cuando se sincroniza el usuario.
- Se ha asignado una cuenta existente a un usuario copiando la cuenta al usuario.
- Se ha creado una cuenta para un usuario en lugar de asignar el usuario a un rol. Por ejemplo, se ha copiado un usuario a una plantilla de cuenta que no está en un rol de aprovisionamiento para ese usuario. La cuenta se ha clasificado como cuenta adicional o como cuenta con una plantilla de cuenta adicional. Si se copia el usuario en un punto final para crear una cuenta mediante la plantilla de cuenta predeterminada, esa cuenta podría ser una cuenta adicional.

Las secciones siguientes explican cómo realizar los tres tipos de sincronización:

1. Sincronización de usuarios con roles (en la página 177).
2. Sincronización de usuario con plantillas de cuenta (en la página 177).
3. Sincronización de cuenta de punto final con plantillas de cuenta (en la página 179).

Sincronización de usuario con roles

Esta tarea crea, actualiza o suprime cuentas para que cumplan con los roles de aprovisionamiento asignados a un usuario. Por ejemplo, los administradores utilizan herramientas nativas en un punto final para agregar o suprimir cuentas, pero no ha vuelto a explorar ese punto final para actualizar el directorio de aprovisionamiento. Por lo tanto, los usuarios tendrán cuentas adicionales o que faltan. Esta tarea también asegura que cada cuenta pertenece a las plantillas de cuenta correctas.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Usuarios, Sincronización, Comprobar sincronización del rol.
3. Seleccione un usuario.

   Aparecerá una pantalla que muestra las cuentas esperadas, cuentas adicionales o cuentas que faltan.
4. Haga clic en Sincronizar para hacer que las cuentas coincidan con la plantilla de este rol.

   a. Se puede seleccionar una casilla de verificación para crear la cuenta en el punto final. Si más de una plantilla de cuenta para el usuario indica la misma cuenta, la cuenta se crea combinando todas las plantillas de cuenta relevantes.

      Esta cuenta se asigna a las plantillas de cuenta que no están actualmente sincronizadas con la cuenta.

   b. Se puede seleccionar una casilla de verificación para suprimir cuentas adicionales. Sin embargo, los usuarios pueden tener motivos legítimos para tener estas cuentas. En este caso, se debe dejar esta opción sin marcar.

      En ciertos puntos finales, la función de supresión de cuentas está desactivada; por lo tanto, la cuenta no se suprime.

Sincronización de usuario con plantillas de cuenta

Esta tarea sincroniza los atributos para las cuentas de punto final con las plantillas de cuenta asociadas para un usuario. Sin embargo, la sincronización completa depende de los siguientes factores:

- La sincronización completa de la cuenta se produce en dos situaciones. Una plantilla de cuenta utiliza la sincronización estricta (en la página 180) o dos o más plantillas de cuenta se han agregado a una cuenta.
- Si una plantilla de cuenta utiliza la sincronización débil (en la página 180), esta tarea inicia una sincronización de cuenta que implica solamente esta plantilla. Si la cuenta no estaba al principio sincronizada con otras plantillas de cuenta antes de esta actualización, es posible que no estuviera tampoco sincronizada después.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Usuarios, Sincronización, Comprobar sincronización de plantilla de cuenta.
3. Seleccione un usuario.

   Aparecerá una pantalla que muestra las cuentas esperadas, cuentas adicionales o cuentas que faltan.
4. Haga clic en Sincronizar para hacer que las cuentas coincidan con la plantilla.

   a. Se puede seleccionar una casilla de verificación para crear la cuenta en el punto final. Si más de una plantilla de cuenta para el usuario indica la misma cuenta, la cuenta se crea combinando las plantillas de cuenta relevantes.

      Esta cuenta se asigna a las plantillas de cuenta que no están sincronizadas con la cuenta. La sincronización de cuentas no es necesaria en las nuevas cuentas creadas.

   b. Se puede seleccionar una casilla de verificación para suprimir cuentas adicionales. Sin embargo, los usuarios pueden tener motivos legítimos para tener estas cuentas. En este caso, se debe dejar esta opción sin marcar.

      En ciertos puntos finales, la función de supresión de cuentas está desactivada; por lo tanto, la cuenta no se suprime.

Sincronización de cuentas de punto final con plantillas de cuenta

Esta tarea sincroniza una cuenta de punto final después de la modificación de una plantilla de cuenta asociada. Por ejemplo, quizás una cuenta de Active Directory no tiene ningún grupo, pero la plantilla de cuenta asociada está definida para incluir grupos.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario.
2. Seleccione Puntos finales, Gestionar puntos finales, Comprobar sincronización de cuentas de puntos finales.
3. Seleccione un punto final.

   Se abrirá una pantalla que muestra las cuentas en ese punto final, las plantillas de cuenta asociadas y qué atributos no están sincronizados.
4. Haga clic en Sincronizar para hacer que los atributos de esas cuentas coincidan con lo definido en la plantilla de cuenta.

   Los cambios realizados en las plantillas de cuenta afectan a las cuentas existentes como se muestra a continuación:

   - Si se cambia el valor de un atributo de capacidad, se actualizará el atributo de cuenta correspondiente para que esté sincronizado con el valor de atributo de la plantilla de cuenta. Consulte la descripción de la sincronización débil y estricta.
   - El conector designa algunos atributos de cuenta como no actualizados por los cambios de la plantilla de cuenta. Los ejemplos incluyen ciertos atributos que el tipo de punto final solamente permite establecer durante la creación de cuenta y el atributo Contraseña.

Atributos actualizados

Al cambiar los atributos de capacidad de una plantilla de cuenta, el atributo correspondiente en las cuentas cambiará. Este cambio tiene un impacto en los atributos de la cuenta. El impacto se basa en los factores siguientes:

- Si la plantilla de cuenta se ha definido para usar la sincronización débil o fuerte.
- Si la cuenta pertenece a varias plantillas de cuenta.

Sincronización débil

La *sincronización débil* garantiza que los usuarios tengan los atributos de capacidad mínimos para sus cuentas. La sincronización débil es el valor predeterminado en la mayoría de los tipos de puntos finales. Si se actualiza una plantilla que utiliza la sincronización débil, CA Identity Manager actualiza los atributos de capacidad como se muestra a continuación:

- Si se actualiza un campo de número en una plantilla de cuenta, y el nuevo número es mayor que el número de la cuenta, CA Identity Manager cambiará el valor de la cuenta para que coincida con el nuevo número.
- Si no se seleccionó una casilla de verificación en una plantilla de cuenta y, posteriormente, la selecciona, CA Identity Manager actualizará la casilla de verificación en cualquier cuenta en la que la casilla de verificación no esté seleccionada.
- Si se modifica una lista en una plantilla de cuenta, CA Identity Manager actualizará todas las cuentas para incluir los valores de la nueva lista que no estuvieran incluidos en la lista de valores de la cuenta.

Si una cuenta pertenece a otras plantillas de cuenta (tanto si estas plantillas utilizan sincronización débil como estricta), CA Identity Manager sólo consultará la plantilla que se esté modificando. Esta acción es más eficaz que comprobar cada plantilla de cuenta. Dado que la sincronización débil sólo agrega capacidades a las cuentas, generalmente no es necesario consultar otras plantillas de cuenta.

Nota: Cuando se propagan desde una plantilla de cuenta de sincronización débil, los cambios que eliminarían o reducirían las capacidades, podrían dejar algunas cuentas no sincronizadas. Recuerde que con la sincronización débil, las capacidades no se eliminan ni se reducen nunca. Sin consultar otras plantillas de una cuenta, la propagación no tiene en cuenta si es suficiente la sincronización débil.

En esta situación, utilice Sincronizar usuario con plantillas de cuenta para sincronizar la cuenta con sus plantillas de cuenta.

Sincronización estricta

La sincronización estricta garantiza que las cuentas tengan los atributos de cuenta exactos que se especifican en la plantilla de cuenta.

Por ejemplo, supongamos que se agrega un grupo a una plantilla de cuenta de UNIX existente. Originalmente, la plantilla de cuenta hacía miembros de cuentas del grupo Personal. Ahora se desean hacer miembros de cuentas tanto a los grupos de personal como al del sistema. Todas las cuentas asociadas a la plantilla de cuenta se consideran que están sincronizadas cuando cada cuenta es miembro de los grupos de sistema y personal (y de ningún otro grupo). Cualquier cuenta que no esté en el grupo de personal se agregará a ambos grupos.

Otros factores que se deben tener en cuenta:

- Si la plantilla de cuenta utiliza la sincronización estricta, cualquier cuenta que pertenezca a grupos distintos de Personal y Sistema, se eliminará de esos grupos extra.
- Si la plantilla de cuenta utiliza la sincronización débil, las cuentas se agregan a los grupos Personal y Sistema. Cualquier cuenta que tenga definidos grupos adicionales, seguirá siendo un miembro de esos grupos.

Nota: Sincronice las cuentas con sus plantillas periódicamente para garantizar que estén sincronizadas con sus plantillas de cuenta.

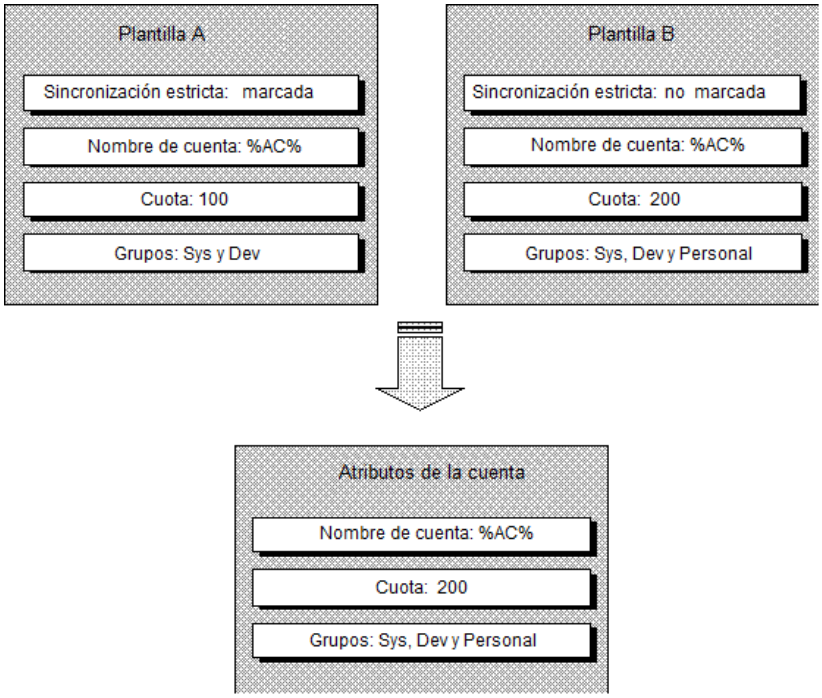
Cuentas con varias plantillas

La sincronización también depende de si la cuenta pertenece a más de una plantilla de cuenta. Si una cuenta tiene solamente una plantilla de cuenta y esa plantilla utiliza la sincronización estricta, cada atributo se actualiza para coincidir exactamente con lo que el valor del atributo de plantilla de cuenta evalúa. El resultado es el mismo que si el atributo fuera un atributo inicial.

Una cuenta puede pertenecer a varias plantillas de cuenta, como sería el caso si un usuario perteneciera a varios roles de aprovisionamiento, cada uno de los cuales indicando algún nivel de acceso en el mismo punto final gestionado. Cuando esto sucede, CA Identity Manager combina esas plantillas de cuenta en una plantilla de cuenta efectiva que indica el superconjunto de las capacidades de las plantillas de cuenta individuales. Se considera que esta plantilla de cuenta que utiliza la sincronización débil si todas sus plantillas de cuenta individuales son de sincronización débil o estricta o si alguna de las plantillas de cuenta individuales es estricta.

Nota: A menudo se utiliza solo la sincronización débil o solo la sincronización estricta para las plantillas de cuenta que controlan una cuenta, en función de si los roles de la compañía definen completamente los accesos que necesitan sus usuarios. Si sus usuarios no se ajustan en roles claros y se necesita la flexibilidad para conceder capacidades adicionales a las cuentas de sus usuarios, utilice la sincronización débil. Si se pueden definir roles para especificar exactamente los accesos que necesitan sus usuarios, utilice la sincronización estricta.

El ejemplo siguiente demuestra cómo se combinan varias plantillas de cuenta en una sola plantilla de cuenta efectiva. En este ejemplo, una plantilla de cuenta se marca para la sincronización débil y otra para la sincronización estricta. Por lo tanto, la plantilla de cuenta efectiva creada combinando las dos plantillas de cuenta se trata como una plantilla de cuenta de sincronización estricta. El atributo de cuota de entero adopta el valor mayor de las dos plantillas de cuenta y el atributo de grupos de varios valores adopta la unión de valores de las dos políticas.



Atributos exclusivos para nuevas cuentas

En una plantilla de cuenta, algunos atributos sólo se aplican cuando se crea la cuenta. Por ejemplo, el atributo de contraseña es una expresión de regla que define la contraseña para las nuevas cuentas. Esta expresión de regla nunca actualiza la contraseña de una cuenta. Los cambios de la expresión de regla de contraseña sólo repercuten en las cuentas que se crean después de que se haya configurado la expresión de regla.

De igual manera, una expresión de regla de plantilla para un atributo de cuenta de sólo lectura sólo repercute en las cuentas que se crean después de que se haya configurado la expresión de regla. El cambio no repercute en las cuentas existentes.

Resolución de problemas

En la siguiente sección se presentan temas de solución de problemas con la generación de informes.

Al intentar ver un informe, el sistema le redirige a la página de inicio de sesión de InfoView

Al ver un informe en CA Identity Manager, es posible que el sistema le redirija a la página de inicio de sesión de BusinessObjects Infoview.

Visualización del informe si se le redirige

1. Asegúrese de que utiliza el nombre de dominio completo del servidor de informes de CA (Business Objects).
2. Haga clic con el botón secundario en la página Web de inicio de sesión de InfoView y seleccione la opción para ver el código fuente.
3. Busque la dirección URL del informe.
4. Copie y pegue la dirección URL en una nueva ventana del explorador.
5. Si no ve el informe, utilice una herramienta de seguimiento HTTP para proporcionar más información.
6. Si ve el informe, intente lo siguiente para corregir la configuración del explorador:
   - Acepte las cookies de terceros.
   - Permita las cookies durante la sesión.
   - Desactive la configuración de máxima seguridad.

Generación de cuentas de usuario para más de 20000 registros

Si existen más de 20000 registros, se tendrá que llevar a cabo algunos pasos adicionales para generar informes de cuentas de usuario.

Para generar informes de cuentas de usuario para más de 20000 registros

1. Abra la consola de gestión central de BusinessObjects.
2. Haga clic en la opción de servidores y seleccione *nombreservidor*.pageserver.
3. Seleccione Unlimited records (Registros ilimitados) en la entrada Database Records To Read When Previewing Or Refreshing a Report (Registros de base de datos que se deben leer al actualizar un informe o mostrar su vista previa).
4. Utilice el diseñador de Crystal Reports para abrir el informe de cuentas de usuario.

5. Utilice Database, Set Datasource Location (Base de datos, Establecer ubicación de base de datos) para establecer la ubicación de su base de datos de instantáneas.
6. Guarde el cambio.
7. Seleccione Base de datos, Datasource Expert (Experto de orígenes de datos) y haga clic con el botón secundario del ratón en Comando, que se encuentra en la ventana del lado derecho.

   Se muestra la sintaxis SQL en el lado izquierdo y la lista de parámetros.
8. Introduzca el nombre del parámetro tal como se muestra en los campos de parámetros de la plantilla de informe.
9. Cambie la consulta en el lado izquierdo y agregue ese parámetro a la consulta.

   Por ejemplo, si tiene el parámetro reportid, la consulta será:

```
Select * from endPointAttributes, endpointview, imreport6
where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
endPointAttributes.imr_reportid = endpointview.imr_reportid
 endpointview.imr_reportid = imreport6.imr_reportid and
imreport6.imr_reportid = {?reportid}
```

10. Guarde el informe.

Capítulo 15: Políticas de identidad

Esta sección contiene los siguientes temas:

Políticas de identidad

Una política de identidad es un conjunto de cambios empresariales que se producen cuando un usuario cumple una cierta condición o regla. Puede utilizar los conjuntos de políticas de identidad para:

- Automatizar ciertas tareas de gestión de identidades, como por ejemplo la asignación de roles y la pertenencia a un grupo, la asignación de recursos o la modificación de los atributos del perfil de usuario.
- Imponer la segregación de obligaciones. Por ejemplo, puede crear un conjunto de políticas de identidad que prohíba a los miembros del rol Comprobar firmante que tengan el rol Comprobar aprobador y que impida a cualquier persona de la empresa extender un cheque superior a 10.000 $.
- Imponer el cumplimiento. Por ejemplo, puede auditar a los usuarios que tengan un título determinado y ganen más de 100.000 $.

  Las políticas de identidad que imponen el cumplimiento se denominan *políticas de cumplimiento*.

Los cambios del negocio asociados con una política de identidad incluyen:

- La asignación o revocación de roles, incluidos los roles de aprovisionamiento (sólo si se está utilizando un directorio de aprovisionamiento).
- La asignación o la revocación de una pertenencia a grupo
- La actualización de atributos en un perfil de usuario

Por ejemplo, una empresa puede crear una política de identidad que establezca que todos los vicepresidentes pertenezcan al grupo Miembro del club de campo y tengan el rol Aprobador de salario. Si el cargo de un usuario cambia a vicepresidente y dicho usuario está sincronizado con la política de identidad, CA Identity Manager agregará el usuario al rol y al grupo apropiados. Cuando un vicepresidente es ascendido a Jefe ejecutivo, ya no cumple la condición de la política de identidad de vicepresidente, de modo que los cambios aplicados por dicha política serán revocados y se pasarán a aplicar nuevos cambios basados en la política de Jefe ejecutivo.

Las acciones de cambio que se producen en función de una política de identidad contienen eventos que se pueden colocar bajo el control de flujo de trabajo y auditar. En el ejemplo anterior, el rol Aprobador de salario concede privilegios significativos a sus miembros. Para protegerlo, la empresa puede crear un proceso de flujo de trabajo que necesite un conjunto de aprobaciones antes de asignar el rol. Además, se puede configurar CA Identity Manager para que audite la asignación del rol.

Para simplificar la gestión de políticas de identidad, éstas se agrupan en un conjunto de políticas de identidad. Por ejemplo, las políticas de vicepresidente y jefe ejecutivo pueden formar parte del conjunto de políticas de identidad Privilegios ejecutivos.

Nota: CA Identity Manager incluye un tipo adicional de política de identidad denominado *política de identidad preventiva* (en la página 490). Estas políticas, que se ejecutan antes de que se envíe una tarea, permiten que un administrador compruebe si hay infracciones de política antes de asignar privilegios o cambiar atributos de perfil. Si las hubiera, el administrador podría borrar la infracción antes de enviar la tarea.

Hoja de trabajo para planificar el conjunto de políticas de identidad

Un conjunto de políticas de identidad contiene una o varias políticas de identidad. Antes de crear un conjunto de políticas de identidad, utilice la siguiente hoja de trabajo para planificar cada política de identidad del conjunto.

Pregunta	Su respuesta
¿Qué nombre desea asignar a la política de identidad?	
¿A qué usuarios se aplica la política de identidad?	
Cuando se aplica una política de identidad a un usuario, ¿qué acciones debe realizar CA Identity Manager?	
Cuando una política de identidad que antes se aplicaba a un usuario deja de aplicarse, ¿qué acciones debe realizar CA Identity Manager?	
¿CA Identity Manager debe aplicar los cambios en una política de identidad varias veces o sólo la primera vez que un usuario cumpla las condiciones de la política?	

Tras completar esta hoja de trabajo para cada política de identidad de un conjunto de políticas, compruebe que las políticas no presentan conflictos entre ellas. Por ejemplo, asegúrese de que una política no concede un privilegio que otra revoque.

Creación de un conjunto de políticas de identidad

Para crear un conjunto de políticas de identidad, debe tener la función Gestor del sistema, o una función que incluya la tarea Crear conjunto de políticas de identidad.

Para crear un conjunto de políticas de identidad, realice los siguientes pasos:

1. Defina el perfil para el conjunto de políticas de identidad. (en la página 469)
2. Creación de una regla de miembros para un conjunto de políticas (en la página 470)
3. Cree una política de identidad. (en la página 470)
4. Especifique los propietarios del conjunto de políticas de identidad. (en la página 480)

Nota: Para usar políticas para un entorno de CA Identity Manager, active las políticas de identidad en la Consola de gestión de CA Identity Manager. Para obtener más información, consulte la *Guía de configuración*.

Definición del perfil para el conjunto de políticas de identidad

La ficha Perfil le permite definir las propiedades básicas para un conjunto de políticas de identidad.

Para definir un perfil de conjunto de políticas de identidad

1. En la Consola de usuario, seleccione Políticas, Gestionar políticas de identidad, Crear conjunto de políticas de identidad.

   Debe iniciar sesión en CA Identity Manager como un usuario con privilegios para gestionar políticas de identidad. El rol Gestor del sistema incluye estos privilegios.
2. Elija entre crear un nuevo conjunto de políticas de identidad o crear una copia de un conjunto de políticas de identidad existente.
3. Introduzca un nombre para el conjunto de políticas de identidad.
4. Introduzca una categoría para el conjunto de políticas de identidad.

   La categoría agrupa conjuntos de políticas de identidad con objetivos similares para generar informes. El campo Categoría es obligatorio.
5. Opcionalmente, puede introducir una descripción del conjunto de políticas de identidad.
6. Si no desea que el conjunto de políticas de identidad esté disponible para su uso, anule la selección de la casilla de verificación Activado.
7. Cuando haya completado la ficha Perfil, seleccione la ficha Políticas para crear políticas de identidad para el conjunto de políticas de identidad.

Más información:

Creación de una política de identidad (en la página 470)
Creación de una regla de miembros para un conjunto de políticas (en la página 470)

Creación de una regla de miembros para un conjunto de políticas

Puede crear una regla de miembros para un conjunto de políticas, de manera que el conjunto de políticas sólo se aplique a determinados usuarios. La regla se evalúa antes de evaluar las políticas de identidad del conjunto, lo que puede ahorrar un tiempo significativo. Por ejemplo, si la regla de miembros limita la evaluación de políticas de identidad al 10% de los usuarios, se ahorra el 90% del tiempo de evaluación.

Para crear una regla de miembros para un conjunto de políticas

1. Seleccione la ficha Políticas.
2. Haga clic en el símbolo Editar en Policy Set Member Rule (Regla para establecer los miembros de la política).
3. Introduzca una regla para aplicar la política sólo a determinados usuarios.
4. Haga clic en Aceptar.

Más información:

Creación de una política de identidad (en la página 470)

Creación de una política de identidad

Tras definir el perfil y la regla de miembros para el conjunto de políticas de identidad, puede definir las políticas de identidad en ese conjunto de políticas.

Nota: En implementaciones grandes, la evaluación de las reglas de política de identidad puede tardar bastante tiempo. Para reducir el tiempo de evaluación de las reglas que incluyan atributos de usuario, se puede activar la opción de evaluación en memoria. Para obtener más información, consulte la *Guía de configuración*.

Para crear una política de identidad

1. Seleccione la ficha Políticas.
2. Haga clic en Agregar.
3. Escriba un nombre para la política de identidad.
4. Seleccione la casilla de verificación Aplicar una vez si desea aplicar la política sólo cuando un usuario cumpla la política por primera vez.

5. Seleccione la casilla de verificación Conformidad para indicar que se trata de una política de conformidad.

   Si se selecciona esta casilla de verificación:

   - CA Identity Manager puede generar informes para usuarios que no estén sincronizados con las políticas de cumplimiento.
   - La acción Incumplimiento de la conformidad se puede ver en el cuadro de lista Acción al aplicar/eliminar política.

6. Identifique los usuarios a quienes se aplica la política de la sección Condición de la política.
7. En la sección Acción al Aplicar política, defina las acciones que debe realizar CA Identity Manager cuando se aplique la política de identidad a un usuario.
8. En la sección Acción al Eliminar política, defina las acciones que debe realizar CA Identity Manager cuando un usuario ya no cumpla las condiciones para la política de identidad.
9. Haga clic en Aceptar.

Nota: Antes de poder utilizar la política de identidad que ha creado, debe activar las políticas de identidad en la Consola de gestión. Para obtener más información, consulte la *Guía de configuración*.

La opción Aplicar una vez

CA Identity Manager aplica una política de identidad de un modo diferente, en función de la opción Aplicar una vez.

Activación de la opción Aplicar una vez

Si la opción Aplicar una vez está activada, CA Identity Manager aplicará los cambios asociados con la política de identidad cuando un usuario cumpla *por primera vez* la condición definida en la política. Las acciones de cambio asociadas con la política sólo se producen una vez. Por lo tanto, si la política se ha aplicado anteriormente, CA Identity Manager no aplicará las actualizaciones de la política a los usuarios.

Cuando un usuario deja de cumplir la condición definida en la política, CA Identity Manager ejecuta las acciones de eliminación de la política.

La opción Aplicar una vez se suele utilizar en el momento del aprovisionamiento de recursos. Por ejemplo, es posible que tenga una política que asigne un teléfono móvil a los directores. Cuando un usuario se convierte por primera vez en director, se le asigna un teléfono móvil. CA Identity Manager sólo concede el teléfono móvil una vez, no cada vez que se evalúa la política. Si la política del teléfono móvil se actualiza para incluir un modelo de teléfono móvil más reciente, CA Identity Manager no concederá nuevos teléfonos móviles para los directores existentes.

Nota: El aprovisionamiento de recursos está disponible cuando CA Identity Manager se integra con un servidor de aprovisionamiento.

Desactivación de la opción Aplicar una vez

Si la opción Aplicar una vez no está activada, las acciones de cambio asociadas con la política de identidad se aplican cada vez que se evalúa una política de identidad. Esto significa que CA Identity Manager aplicará las acciones de cambio a todos los usuarios que cumplan las condiciones en la política, independientemente de si las acciones de cambio se aplicaron con anterioridad.

Por norma general, la opción Aplicar una vez se desactivará en una política de identidad que imponga conformidad. Por ejemplo, puede crear una política de identidad que limite las facultades de gasto de los directores a $5.000. Si CA Identity Manager encuentra un director cuyas facultades de gasto estén establecidas en 10.000 $, restablecerá las facultades de gasto a 5.000 $. Cada vez que un director se sincronice con la política de identidad, CA Identity Manager comprobará que sus facultades de gasto estén establecidas correctamente.

Si se realiza un cambio manual en un perfil de usuario que entra en conflicto con una acción de cambio, CA Identity Manager sobrescribirá el cambio cuando el usuario se sincronice con la política.

En el ejemplo anterior, si alguien aumenta manualmente las facultades de gasto de un director a 10.000 $, CA Identity Manager restablecerá estas facultadas a 5.000 $ cuando el director se sincronice con la política.

La siguiente tabla resume los efectos de activar o desactivar la opción Aplicar una vez.

Si Aplicar una vez está...	Realice las tareas siguientes...
Activado	■ Las acciones de cambio asociadas con la política de identidad sólo se aplican una vez. ■ Se preservan los cambios manuales realizados tras aplicar la política de identidad. ■ Si CA Identity Manager ha aplicado la política con anterioridad, las actualizaciones no se aplicarán a los usuarios que cumplan la condición de una política de identidad. ■ Cuando un usuario ya no cumpla la condición de la política de identidad, CA Identity Manager ejecutará las acciones de eliminación.
Desactivada	■ Las acciones de cambio asociadas con la política de identidad se aplican cada vez que un usuario se sincroniza con la política. ■ Los cambios manuales se sobrescriben cuando se aplica la política de identidad. ■ Las actualizaciones de la política se aplican cuando el usuario se sincroniza. ■ Cuando un usuario ya no cumpla la condición de la política de identidad, CA Identity Manager ejecutará las acciones de eliminación.

Condiciones de la política

Las condiciones de la política son las reglas que determinan el conjunto de usuarios a los que se aplica una política de identidad.

En la siguiente tabla se describen las opciones disponibles.

Sintaxis	Condición	Ejemplo
(todo)	La política de identidad se aplica a todos los usuarios.	
donde <filtro-usuario>	El usuario debe cumplir uno o varios valores de atributo.	Usuarios donde título=gestor y localidad=este

Sintaxis	Condición	Ejemplo
en <regla-organización>	El usuario debe pertenecer a las organizaciones mencionadas. **Nota:** Al seleccionar esta opción, CA Identity Manager mostrará un nuevo cuadro de lista en el que se podrán seleccionar las siguientes opciones: ■ organización <organización> [e inferior]: permite utilizar la pantalla de búsqueda de organizaciones para seleccionar una y, opcionalmente, incluir las organizaciones secundarias de la inicial. ■ organizaciones donde <filtro-organización> [e inferior]: permite especificar un filtro que selecciona una o más organizaciones.	Usuarios en ventas de la organización e inferior
donde <filtro-usuario> y que están en <regla-organización>	El usuario debe cumplir los atributos de usuario específicos y pertenecer a una organización específica.	título=gestor y organización=Ventas*
que son miembros de <regla-miembro-grupo>	El usuario debe pertenecer a un grupo que cumpla con una condición especificada por los atributos del grupo. **Nota:** Al seleccionar esta opción, CA Identity Manager mostrará un nuevo cuadro de lista en el que se podrán seleccionar las siguientes opciones: ■ grupo <grupo>: use una pantalla de búsqueda de grupos para seleccionar uno. ■ grupo donde <filtro-grupo>: permite especificar un filtro que seleccione uno o más grupos.	Usuarios que son miembros de grupos donde propietario=CIO

Sintaxis	Condición	Ejemplo
que son miembros de <regla-rol>	El usuario debe ser miembro de un rol. El rol puede ser: ■ Rol de acceso ■ Rol de administrador ■ Rol de aprovisionamiento **Nota:** Para utilizar roles de aprovisionamiento, CA Identity Manager debe estar integrado con un servidor de aprovisionamiento. Para obtener más información, consulte la *Guía de instalación*.	Usuarios que son miembros del rol Help Desk
que son administradores de <regla-rol>	El usuario debe ser administrador de un rol. El rol puede ser: ■ Rol de acceso ■ Rol de administrador ■ Rol de aprovisionamiento **Nota:** Para utilizar roles de aprovisionamiento, CA Identity Manager debe estar integrado con un servidor de aprovisionamiento. Para obtener más información, consulte la *Guía de instalación*.	Usuarios que son administradores del rol Gestor de ventas
que son propietarios de <regla-rol>	El usuario debe ser un propietario de un rol. El rol puede ser: ■ Rol de acceso ■ Rol de administrador ■ Rol de aprovisionamiento **Nota:** Para utilizar roles de aprovisionamiento, CA Identity Manager debe estar integrado con un servidor de aprovisionamiento. Para obtener más información, consulte la *Guía de instalación*.	Usuarios que son propietarios del rol Gestor de usuarios
devuelto por la consulta <consulta-LDAP>	El usuario debe cumplir con una condición basada en una consulta LDAP.	Usuario que cumple las condiciones de una consulta LDAP. Por ejemplo: (Númerodepartamento=Cuentas)

Sintaxis	Condición	Ejemplo
en <restricción-unión-administrativa>	El usuario debe cumplir como mínimo una de las condiciones en una lista de condiciones. En una restricción de unión administrativa puede incluir los siguientes tipos de filtros: ■ Miembro del rol de acceso/administración/aprovisionamiento ■ Administrador del rol de acceso/administración/aprovisionamiento ■ Propietario del rol de acceso/administración/aprovisionamiento ■ Miembro de un grupo	Usuarios que son miembros del rol Certificar gestor *o* que son propietarios del rol Certificar gestor.
en <restricción-intersección-administrativa>	El usuario debe cumplir todas las condiciones de una lista de condiciones. En una restricción de unión administrativa puede incluir los siguientes tipos de filtros: ■ Miembro del rol de acceso/administración/aprovisionamiento ■ Administrador del rol de acceso/administración/aprovisionamiento ■ Propietario del rol de acceso/administración/aprovisionamiento ■ Miembro de un grupo	Usuarios que son miembros del rol Iniciador de contrato *y* el rol Aprobador de contrato.

Acciones al aplicar/eliminar políticas

Puede definir las acciones de cambio que CA Identity Manager realizará al evaluar la política de identidad. Las acciones incluyen:

Acción al Aplicar política

Un conjunto de acciones que CA Identity Manager realiza cuando un usuario cumple las condiciones de política definidas.

Acción al Eliminar política

Un conjunto de acciones que CA Identity Manager realiza cuando un usuario deja de cumplir las condiciones de política definidas.

Las acciones que CA Identity Manager puede realizar cuando se aplican o se eliminan políticas de identidad son las mismas. Si desea obtener más información, consulte la siguiente tabla.

Acción de cambio	Descripción
Agregar al grupo <nombre-grupo> [...]	Agrega usuarios a un grupo. Al seleccionar esta opción, CA Identity Manager presenta una pantalla en la que puede buscar el grupo que desee.
Agregar al grupo <nombre-grupo> en la organización del usuario	Agrega usuarios a un grupo local. Al seleccionar esta opción, CA Identity Manager presenta un cuadro de texto en el que puede introducir el nombre del grupo que desee.
Definir <atributo-usuario-único-valor> como <valor>	Establece el valor de un atributo en un perfil de usuario. Si hay un valor existente, CA Identity Manager lo sobrescribe con el valor especificado en la acción de cambio.
Agregar <valor> a <atributo-usuario-varios-valores>	Agrega un valor a un atributo de usuario con varios valores. Esta opción no sobrescribe los valores existentes.
Hacer miembro del rol de acceso	Asigna usuarios a un rol de acceso.
Hacer administrador del rol de acceso	Hace a los usuarios administradores de un rol de acceso.
Hacer miembro del rol de administrador	Hace a los usuarios miembros de un rol de administrador.
Hacer administrador del rol de administrador	Hace a los usuarios administradores de un rol de administrador.
Hacer miembro del rol de aprovisionamiento	Hace a los usuarios miembros de un rol de aprovisionamiento, que crea cuentas de punto final asociadas. **Nota:** Para utilizar roles de aprovisionamiento, CA Identity Manager debe estar integrado con un servidor de aprovisionamiento. Consulte la *Guía de instalación* de su servidor de aplicaciones.
Hacer administrador del rol de aprovisionamiento	Hace a los usuarios administradores de un rol de aprovisionamiento. **Nota:** Para utilizar roles de aprovisionamiento, CA Identity Manager debe estar integrado con un servidor de aprovisionamiento. Consulte la *Guía de instalación* de su servidor de aplicaciones.

Acción de cambio	Descripción
Eliminar del grupo <nombre-grupo> [...]	Elimina usuarios de un grupo. Al seleccionar esta opción, CA Identity Manager presenta una pantalla en la que puede buscar el grupo que desee.
Eliminar del grupo <nombre-grupo> de la organización del usuario	Elimina usuarios de un grupo local. Al seleccionar esta opción, CA Identity Manager presenta un cuadro de texto en el que puede introducir el nombre del grupo que desee.
Eliminar <valor> de <atributo-usuario-varios-valores>	Elimina un valor de un atributo de usuario con varios valores.
Eliminar miembro del rol de acceso	Revoca un rol de acceso.
Eliminar administrador del rol de acceso	Revoca los privilegios de administrador de un rol de acceso específico.
Eliminar miembro del rol de administrador	Revoca un rol de administrador.
Eliminar administrador del rol de administrador	Revoca los privilegios de administrador de un rol de administrador específico.
Eliminar miembro del rol de aprovisionamiento	Revoca un rol de aprovisionamiento.
Eliminar administrador del rol de aprovisionamiento	Revoca los privilegios de administrador de un rol de aprovisionamiento específico.
Enviar mensaje de auditoria	Envía un mensaje creado por usted a la base de datos de auditoria. Este mensaje puede aparecer en un informe que haya creado.
Infracción de cumplimiento	Envía un mensaje creado por usted a la base de datos de auditoria. Si crea un informe de cumplimiento, el mensaje aparecerá cada vez que se aplique/elimine la política de identidad de un usuario. Para obtener más información sobre la auditoría, consulte la *Guía de configuración*. **Nota:** Para que el conjunto de políticas de identidad utilice la opción de infracción de cumplimiento, debe activar la casilla de verificación Cumplimiento en la ficha Perfil.

Acción de cambio	Descripción
Aceptar (Acción al Aplicar política sólo)	Permitirá que se envíe la tarea cuando haya una infracción de política de identidad preventiva. Cuando se selecciona esta acción, proporciona un mensaje que CA Identity Manager escribe en la base de datos de auditoría y que aparece en Ver tareas enviadas cuando se produce una infracción.
Rechazar (Acción al Aplicar política sólo)	Impide que se envíe una tarea cuando se produce una infracción de política de identidad. Esta acción se usa con políticas de identidad preventivas para impedir que los usuarios reciban privilegios que pueden originar un conflicto de intereses o fraude. Cuando se selecciona esta acción, también proporciona un mensaje que CA Identity Manager muestra cuando se produce una infracción. Este mensaje se almacena en una base de datos de auditoría y se muestra en la Consola de usuario.
Advertencia (Acción al Aplicar política sólo)	Inicia un proceso de flujo de trabajo cuando se produce una infracción de política de identidad preventiva si asocia esa infracción con una política de aprobación de flujo de trabajo. CA Identity Manager permite que se envíe la tarea independientemente de si se ha configurado el flujo de trabajo o no. **Nota:** Para obtener información sobre cómo asociar un proceso de flujo de trabajo con una política de identidad preventiva, consulte Flujo de trabajo y políticas de identidad preventivas. (en la página 496) Cuando se selecciona esta acción, también proporciona un mensaje que CA Identity Manager muestra cuando se produce una infracción. El mensaje se almacena en la base de datos de auditoría y se muestra en Ver tareas enviadas.

Más información:

Políticas de identidad preventivas (en la página 490)
Flujo de trabajo y políticas de identidad preventivas (en la página 496)

Especificación de los propietarios del conjunto de políticas de identidad

En la ficha Propietarios, puede definir las reglas sobre quién puede ser propietario de un conjunto de políticas de identidad. El propietario del conjunto de políticas de identidad puede modificar la información básica sobre el conjunto de políticas, y puede agregar, cambiar o eliminar las políticas de identidad del conjunto.

Para completar la ficha Propietarios:

1. Defina las reglas de propietarios, que determinan qué usuarios pueden modificar el conjunto de políticas de identidad.
2. Haga clic en Enviar.

Gestión de un conjunto de políticas de identidad

CA Identity Manager incluye las siguientes tareas para gestionar un conjunto de políticas de identidad:

- Ver conjunto de políticas de identidad
- Modificar conjunto de políticas de identidad
- Suprimir conjunto de políticas de identidad

De forma predeterminada, cuando un administrador utiliza una de estas tareas, CA Identity Manager muestra una lista de todos los conjuntos de políticas de identidad de los que ese administrador es propietario. El administrador puede seleccionar en la lista el conjunto de políticas que necesite.

En un entorno Identity Manager que incluya muchos conjuntos de políticas de identidad, es posible que desee personalizar las tareas Ver, Modificar y Supprimir conjunto de políticas de identidad para permitir que los administradores busquen un conjunto de políticas de identidad, en lugar de mostrarlos en una lista.

Para personalizar estas tareas:

1. En la Consola de usuario, seleccione Roles y tareas, Tareas de administración y Modificar la tarea de administración.

   Se abrirá la pantalla Modificar la tarea de administración.
2. Busque y seleccione la tarea que desea personalizar.
3. En la ficha Ámbito, seleccione Todos los conjuntos de políticas de identidad.

   Al seleccionar esta opción, CA Identity Manager utilice la definición de pantalla Búsqueda predeterminada de conjuntos de políticas de identidad.
4. Haga clic en Enviar.

Cómo sincronizar usuarios y políticas de identidad

Al utilizar políticas de identidad, es importante comprender cómo CA Identity Manager evalúa y aplica las políticas a los usuarios. Si no comprende al detalle el proceso de sincronización de usuarios, es posible que configure conjuntos de políticas de identidad que produzcan resultados inesperados.

El procedimiento siguiente describe cómo CA Identity Manager evalúa y aplica políticas de identidad:

1. El proceso de sincronización de usuarios comienza:
   - **Automáticamente**: puede configurar las tareas de CA Identity Manager para que activen automáticamente la sincronización de usuarios.
   - **Manualmente**: utilice la tarea Sincronizar usuario de la Consola de usuario para sincronizar un usuario.
2. CA Identity Manager determina el conjunto de políticas de identidad que se aplican a un usuario.
3. CA Identity Manager compara el conjunto de políticas de identidad que se aplican a un usuario con la lista de políticas que ya se han aplicado a ese usuario.

   Nota: La lista de políticas que se han aplicado a un usuario se almacena en el atributo conocido %IDENTITY_POLICY% del perfil de usuario. Para obtener información sobre la configuración de este atributo, consulte la *Guía de configuración*.

   - Si una política de identidad está en la lista de políticas aplicables *y* esa política *no* se ha aplicado previamente al usuario, CA Identity Manager la agregará a una lista de asignación.
   - Si una política de identidad está en la lista de políticas aplicables, se ha aplicado previamente al usuario y la opción Aplicar una vez está desactivada para esa política, CA Identity Manager agregará la política a una lista de reasignación.
   - Si una política de identidad no está en la lista de políticas aplicables y ha sido aplicada al usuario, el usuario ya no cumplirá la condición de la política. CA Identity Manager agregará estas políticas a una lista de anulación de asignación.
4. Una vez que CA Identity Manager ha evaluado todas las políticas de un usuario, las aplica en este orden:
   a. Políticas de identidad de la lista de anulación de asignación
   b. Políticas de identidad de la lista de asignación
   c. Políticas de identidad de la lista de reasignación

5. Tras aplicar las políticas de identidad, CA Identity Manager vuelve a evaluarlas para ver si se necesitan otros cambios en función de los cambios que tuvieron lugar en el primer proceso de sincronización (pasos 2-4).

   Esto se hace para asegurar que los cambios realizados al aplicar políticas de identidad no han desencadenado otras políticas de identidad.

6. CA Identity Manager continúa evaluando y aplicando políticas de identidad hasta que el usuario se sincroniza con todas las políticas aplicables, o hasta que CA Identity Manager alcanza el nivel de recursividad máximo. Este nivel se define en la Consola de gestión.

   Por ejemplo, una política de identidad puede cambiar el departamento de un usuario al asignar una función al usuario. El nuevo departamento inicia otra política de identidad. Sin embargo, si el nivel de repetición se establece en 1, el cambio posterior no se realiza hasta que el usuario se vuelve a sincronizar.

   Para obtener más información sobre la configuración del nivel de recursividad, consulte la Ayuda en línea de la consola de gestión.

Configuración de la sincronización automática de usuarios

CA Identity Manager puede sincronizar automáticamente cuentas de usuario con políticas de identidad en diferentes puntos durante el ciclo vital de una tarea.

Una tarea de CA Identity Manager genera *eventos*, actividades detectables que se producen durante el procesamiento de las tareas. Por ejemplo, la tarea predeterminada Crear usuario genera los eventos CreateUserEvent, AddUserToGroupEvent y AssignAccessRoleEvent. Puede configurar CA Identity Manager para sincronizar los usuarios cuando finaliza una tarea o cuando finaliza cada evento.

Nota: La sección Sincronización de usuarios con políticas de identidad (en la página 481) proporciona más información sobre el proceso de sincronización de los usuarios.

Para configurar una tarea para iniciar la sincronización de usuarios

1. Inicie sesión en CA Identity Manager como un usuario que puede modificar las tareas de administración.
2. Seleccione Funciones y tareas, Tareas de administración, Modificar tarea de administración.

   CA Identity Manager mostrará una pantalla de búsqueda.

3. Busque y seleccione la tarea de administración que iniciará la sincronización de los usuarios.

4. Seleccione una de las siguientes opciones en el campo Sincronización de usuarios de la ficha Perfil para la tarea:

   - **Desactivado**: esta tarea no iniciará la sincronización de los usuarios.
   - **Al completar la tarea**: CA Identity Manager comenzará el proceso de sincronización de los usuarios después de que hayan finalizado todos los eventos. Este valor es la opción de sincronización predeterminada para las tareas Crear usuario, Modificar usuario y Suprimir usuario. La configuración predeterminada para el resto de tareas es Desactivado.

     Nota: Si selecciona la opción Al completar la tarea para una tarea que incluya varios eventos, CA Identity Manager no sincronizará los usuarios hasta que se completen todos los eventos de la tarea. Si uno o más de esos eventos requieren aprobación de flujo de trabajo, puede demorarse varios días. Para evitar que CA Identity Manager espere a aplicar políticas de identidad hasta que se terminen todos los eventos, seleccione la opción En cada evento.
   - **En cada evento**: CA Identity Manager comienza el proceso de sincronización de los usuarios cuando se completa cada evento de una tarea.

     Para tareas con un evento primario y secundario para el mismo usuario, configurar la sincronización de los usuarios a En cada evento puede dar lugar a más evaluaciones para las que las políticas se aplican a un usuario que si se selecciona la opción Al completar la tarea.

Sincronización manual de los usuarios

Es posible que desee sincronizar manualmente un usuario con un conjunto de políticas de identidad para garantizar que una cuenta de usuario tenga los privilegios correctos o que cumpla con una política de conformidad.

Puede sincronizar manualmente un usuario mediante la tarea Sincronizar usuario de la Consola de usuario de CA Identity Manager.

Nota: Para que la tarea Sincronizar usuario funcione correctamente, la opción Sincronización de usuarios debe estar desactivada, y la opción Sincronización de cuentas debe estar establecida en Al completar la tarea o En cada evento. Para obtener un mejor rendimiento, seleccione la opción Al completar la tarea. Esas opciones se establecen en la pestaña Perfil (profile) para la tarea Sincronizar usuario.

La tarea Sincronizar usuario incluye las siguientes fichas:

- **Políticas que coinciden actualmente**: muestra una lista de las políticas de identidad que CA Identity Manager aplicará al usuario cuando se envíe la tarea Sincronizar usuario.

  Nota: La ficha Políticas que coinciden actualmente sólo muestra las políticas de identidad que se aplican al usuario en el momento en que se accede a la tarea Sincronizar usuario. Cuando el usuario está sincronizado con esas políticas, pueden ocurrir cambios que iniciarán otras políticas de identidad. Para que CA Identity Manager no aplique las nuevas políticas hasta que hayan sido revisadas, establezca el nivel de repetición para los conjuntos de políticas de identidad en 1 en la Consola de gestión de CA Identity Manager. Tras enviar la tarea Sincronizar usuario, acceda a ella de nuevo para revisar las políticas.

- **Ya se han aplicado las políticas**: muestra una lista de las políticas de identidad que ya han sido aplicadas al usuario.

- **Resumen de la sincronización**: muestra todas las políticas de identidad que se aplican al usuario y las acciones de cambio para dichas políticas.

Para sincronizar una cuenta de usuario

1. Inicie sesión en Identity Manager como un usuario que pueda utilizar la tarea Sincronizar usuario. (De forma predeterminada, los usuarios con la función Gestor del sistema pueden utilizar esta tarea).
2. Seleccione Políticas, Sincronizar usuario.

   Se abrirá la tarea Sincronizar usuario.
3. Seleccione la ficha Resumen de la sincronización.
4. Revise las políticas y las acciones asociadas que CA Identity Manager aplicará al usuario, y, a continuación, haga clic en Enviar.

Verificación de la sincronización de usuario

Para verificar que se producen los cambios apropiados cuando un usuario está sincronizado con las políticas de identidad, compruebe la ficha Ya se han aplicado las políticas en la tarea Sincronizar usuario.

1. Inicie sesión en CA Identity Manager como un usuario que pueda utilizar la tarea Sincronizar usuario. (De forma predeterminada, los usuarios con la función Gestor del sistema pueden utilizar esta tarea).
2. Seleccione Políticas, Sincronizar usuario.

   Se abrirá la tarea Sincronizar usuario.
3. Seleccione la ficha Ya se han aplicado las políticas.
4. Revise las políticas y las acciones asociadas que CA Identity Manager aplicó al usuario.

Conjuntos de políticas de identidad en un entorno Identity Manager

En las siguientes secciones se describen diferentes formas de utilizar las políticas de identidad:

- Ejemplo: llenado automático de atributos de usuario (en la página 485)
- Ejemplo: asignación de recursos y derechos (en la página 486)
- Ejemplo: imposición de conformidad (en la página 487)
- Ejemplo: imposición de la segregación de funciones (en la página 488)

Ejemplo: llenado automático de atributos de usuario

Puede utilizar un conjunto de políticas de identidad para asignar automáticamente los valores de los atributos de usuario en función de otro valor de atributo o derecho del usuario. Por ejemplo, puede crear un conjunto de políticas de identidad que rellene automáticamente la dirección de correo del usuario basándose en la oficina en casa del usuario.

Para configurar un conjunto de políticas de identidad para las direcciones de los empleados, cree una política de identidad con los siguientes valores de configuración para cada ubicación de la oficina:

Opción de configuración	Valor
Condición de la política	Oficina = <ubicación_oficina>
Acción al Aplicar política	set Dirección postal = <una dirección postal> set Ciudad = <una ciudad> Set Estado/provincia = <un estado o provincia> Set Código postal = <un código postal>

En la siguiente figura se ilustran algunas políticas de muestra en el conjunto de políticas de identidad Direcciones de los empleados.

Políticas de identidad

Conjunto de políticas

	Nombre de política	Regla de miembro de política	Acción al Aplicar política
	NY	donde (Office = "NY")	Establecer Building como 109 5th Establecer City como NY Establecer State / Province como NY Establecer Postal Code como 10017
	Boston	donde (Office = "Boston")	Establecer Building como 201 Jon Establecer City como Boston Establecer State / Province como Boston Establecer Postal Code como 10021

Ejemplo: asignación de recursos y derechos

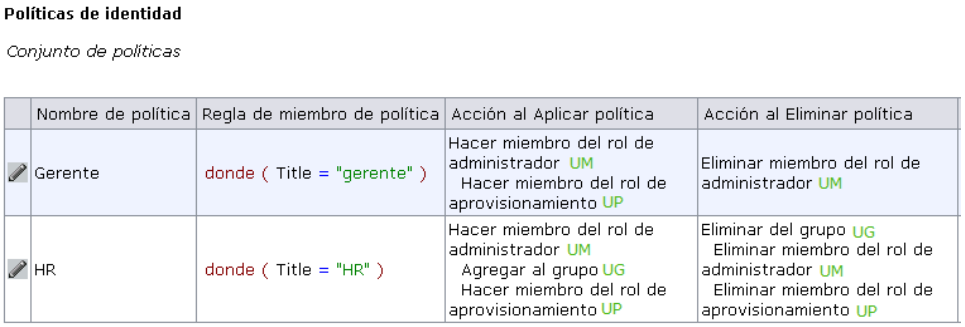
Las políticas de identidad pueden asignar recursos automáticamente (por ejemplo cuentas de dominio), o conceder derechos (por ejemplo hacer a un usuario miembro de una función), cuando los usuarios cumplen la condición de la política. Por ejemplo, puede crear un conjunto de políticas de identidad que asigne recursos y funciones en función del cargo del usuario.

Para crear un conjunto de políticas de identidad para asignar recursos y funciones, cree una política de identidad con la siguiente configuración para cada cargo de su organización:

Opción de configuración	**Valor**
Condición de la política	cargo = <un cargo>
Acción al Aplicar política	Cualquier acción que asigne recursos o derechos a los usuarios que cumplan la condición de la política, por ejemplo: ■ make member of <un grupo> ■ make member of admin role <una función de administración> ■ make member of provisioning role <una función de aprovisionamiento>

Opción de configuración	Valor
Acción al Eliminar política	Cualquier acción que elimine recursos o derechos cuando un usuario ya no cumpla la condición de la política. Por ejemplo, si Identity Manager hizo al usuario miembro de una función cuando se aplicó la política de identidad, es posible que desee configurar Identity Manager para que revoque la función cuando el usuario deje de cumplir la condición de la política.

La siguiente figura ilustra algunas políticas de muestra en el conjunto de políticas de identidad Recursos de los empleados:



Políticas de identidad

Conjunto de políticas

	Nombre de política	Regla de miembro de política	Acción al Aplicar política	Acción al Eliminar política
	Gerente	donde (Title = "gerente")	Hacer miembro del rol de administrador UM Hacer miembro del rol de aprovisionamiento UP	Eliminar miembro del rol de administrador UM
	HR	donde (Title = "HR")	Hacer miembro del rol de administrador UM Agregar al grupo UG Hacer miembro del rol de aprovisionamiento UP	Eliminar del grupo UG Eliminar miembro del rol de administrador UM Eliminar miembro del rol de aprovisionamiento UP

Ejemplo: imposición de conformidad

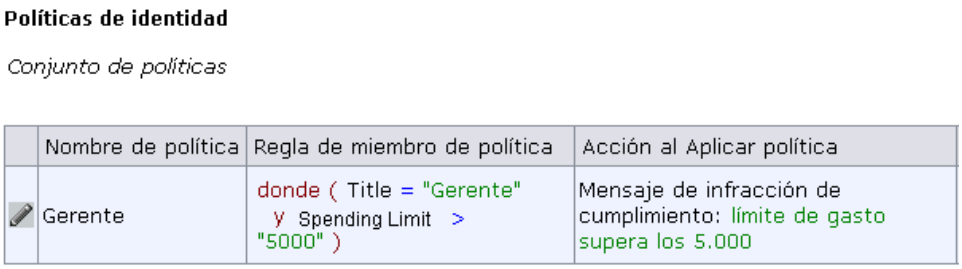
Puede configurar políticas de identidad para definir las condiciones que deben o no existir, y para realizar determinadas acciones en función de la evaluación de dichas condiciones. Por ejemplo, puede definir una política de conformidad que establezca que los directores deben tener un límite de gasto de $5.000. Si un director tiene un límite de gasto de 10.000 $, CA Identity Manager puede restablecer el límite de gasto del director y registrar una infracción de cumplimiento con fines de auditoria.

Para crear un conjunto de políticas de conformidad para la imposición de límites de gasto, cree una política de identidad con los siguientes valores de configuración:

Opción de configuración	Valor
Aplicar una vez	No activado
Conformidad	Activado
Condición de la política	Cualquier condición que defina la conformidad o el incumplimiento de la conformidad, por ejemplo: cargo=<un cargo> AND Límite de gasto=<un límite de gasto>

Opción de configuración	Valor
Acción al Aplicar política	Las acciones que debe realizar CA Identity Manager cuando se aplique la condición de la política, por ejemplo: ■ Mensaje de incumplimiento de la conformidad: Límite de gasto superado. ■ Set límite de gasto to <un valor>.

La siguiente figura muestra el ejemplo de política de conformidad descrito en este ejemplo.



Ejemplo: imposición de la segregación de funciones

Las políticas de identidad pueden definir funciones que se excluyan mutuamente y que no se puedan otorgar de forma concurrente al mismo usuario. Por ejemplo, puede evitar que un usuario director que pueda conceder subidas sea también un aprobador de salario.

Para crear un conjunto de políticas de identidad que imponga la segregación de las funciones, cree una política de identidad con los siguientes valores de configuración:

Opción de configuración	Valor
Aplicar una vez	No activado
Conformidad	Activado

Opción de configuración	Valor
Condición de la política	Utilice la opción "in <restricción-intersección-administrativa>" para definir un conjunto de condiciones que incumplan una política del negocio. Si un usuario cumple todas las condiciones, Identity Manager realizará las acciones del campo Acciones al Aplicar política. Por ejemplo, establezca la condición de la política de la siguiente manera: intersection (who are members of <una función>) and (who are members of <otra función>)
Acción al Aplicar política	Las acciones que debe realizar Identity Manager cuando se aplique la condición de la política, por ejemplo: ■ Mensaje de incumplimiento de la conformidad: el usuario tiene funciones que se excluyen mutuamente. ■ Remove member from <una función>

La siguiente figura muestra la política de identidad de este ejemplo.

Políticas de identidad

Conjunto de políticas

	Nombre de política	Regla de miembro de política	Acción al Aplicar política
	Restricción	intersección (que son miembros de (rol de administrador "Gestor de usuarios") y que son miembros de (rol de administrador "Aprobador de usuarios"))	Mensaje de infracción de cumplimiento: usuario tiene derechos mutuamente Eliminar miembro del rol de administrador Aprobador de usuarios

Políticas de identidad preventivas

La *política de identidad preventiva* es un tipo de política de identidad que impide a los usuarios recibir privilegios que pueden dar como resultado un conflicto de intereses o fraude. Estas políticas admiten requisitos de segregación de obligaciones (SOD) de la compañía.

Las políticas de identidad preventivas, que se ejecutan antes de que se envíe una tarea, permiten que un administrador compruebe si hay infracciones de política antes de asignar privilegios o cambiar atributos de perfil. Si las hubiera, el administrador podría borrar la infracción antes de enviar la tarea.

Por ejemplo, una compañía puede crear una política de identidad preventiva que prohíba a los usuarios que posean el rol Gestor de usuarios tener el rol Aprobador de usuarios. Si un administrador usa la tarea Modificar usuario para darle al Gestor de usuarios el rol Aprobador de usuarios, CA Identity Manager muestra un mensaje sobre la infracción. El administrador puede cambiar las asignaciones de rol para borrar la infracción antes de enviar la tarea.

Puede crear políticas de identidad preventivas para los cambios siguientes:

- **Miembro del rol**

  Impide que los usuarios tengan ciertos roles en el mismo momento.

  Por ejemplo, los usuarios no pueden tener los roles Gestor de usuarios y Aprobador de usuarios a la vez.

- **Administradores de roles**

  Impide que los usuarios sean administradores de ciertos roles si son administradores de otros roles.

  Por ejemplo, los usuarios no pueden ser administradores de los roles Gestor de usuarios y Aprobador de usuarios a la vez.

- **Atributos de usuario**

  Impide que los usuarios tengan ciertos atributos de perfil en el mismo momento.

  Por ejemplo, los usuarios no pueden tener el título de contable y pertenecer al departamento de TI.

- **Atributos de la organización**

  Impide que se creen los perfiles de usuario en una determinada organización.

  Por ejemplo, los administradores no pueden crear perfiles de empleado en la organización de proveedores.

- **Atributos del grupo**

  Impide que los usuarios sean miembros en algunos grupos.

  Por ejemplo, los usuarios no pueden ser miembros del grupo del equipo de proyecto ni del grupo de contabilidad.

Más información:

Acciones para infracciones de política de identidad preventivas (en la página 491)

Acciones para infracciones de política de identidad preventivas

Cuando se aplica una política de identidad preventiva a un cambio empresarial, CA realiza algunas acciones para tratar la infracción.

Cuando defina una de estas acciones en una política de identidad, especifique un mensaje que describa la infracción. Este mensaje se graba en la base de datos de auditoría. Según el tipo de acción, el mensaje también se puede mostrar a los usuarios en la Consola de usuario y grabarse en Ver tareas enviadas.

Puede configurar las acciones siguientes para una política de identidad preventiva.

Aceptar

CA Identity Manager muestra un mensaje en Ver tareas enviadas que describe la infracción, aunque permite el envío de la tarea.

Rechazar

CA Identity Manager muestra un mensaje en la Consola de usuario y prohíbe el envío de la tarea.

Advertencia

CA Identity Manager muestra un mensaje en la Consola de usuario y en Ver tareas enviadas. Esta acción puede iniciar de forma opcional un proceso de flujo de trabajo que exija aprobación de un usuario adecuado antes de que CA Identity Manager ejecute la tarea.

Para iniciar un proceso de flujo de trabajo, asocie la política de identidad preventiva con un proceso de flujo de trabajo basado en políticas (en la página 498) en tareas que pueden provocar la infracción.

Por ejemplo, si la infracción se produce cuando un usuario recibe roles determinados al mismo tiempo, configure el proceso de flujo de trabajo para todas las tareas que asignan dichos roles a los usuarios.

Nota: Cuando configure el proceso de flujo de trabajo basado en políticas para la tarea, la regla de aprobación debe hacer referencia al nombre de la política de identidad preventiva.

Cómo funcionan las políticas de identidad preventivas

El siguiente proceso de ejemplo muestra cómo funcionan las políticas de identidad preventivas:

1. Los administradores de política de identidad preventiva crean políticas de identidad preventiva que prohíben que los usuarios que tengan el título de contable pertenezcan al departamento de TI.

   Cuando se define esta política de identidad, el administrador especifica que CA Identity Manager debe rechazar los cambios que infrinjan esta política.

2. El administrador de RR. HH. usará la tarea Crear usuario para crear un perfil de usuario para un nuevo contable. El administrador de RR. HH. selecciona de forma correcta el título del usuario aunque selecciona de forma accidental el departamento de TI.

3. El administrador de RR. HH. completa los campos restantes in la tarea Crear usuario y hace clic en Enviar.

4. CA Identity Manager detecta que la tarea supone cambios que se definen en una política de identidad y evalúa los cambios para las infracciones.

5. CA Identity Manager detecta la infracción, muestra un mensaje al administrador de RR. HH. e impide el envío de la tarea.

   CA Identity Manager registra también el mensaje en la base de datos de auditoría.

6. El administrador de RR. HH. ve los detalles de la infracción en el mensaje y cambia el departamento del usuario a finanzas. A continuación, el administrador vuelve a enviar la tarea.

7. CA Identity Manager evalúa los cambios propuestos en comparación con todas las políticas de identidad aplicables y después permite que se envíe la tarea Crear usuario.

Notas importantes sobre las políticas de identidad preventivas

Antes de implementar políticas de identidad preventivas, tenga en cuenta lo siguiente:

- Las políticas de identidad preventivas sólo impiden infracciones que se producirían debido a los cambios propuestos en la tarea actual. No impiden las infracciones existentes.

  Por ejemplo, una compañía crea una política de identidad preventiva que prohíbe que los usuarios tengan roles Gestor de usuarios y Aprobador de usuarios a la vez. El administrador asigna el rol Gestor de grupos a un usuario que ya tiene los roles Gestor de usuarios y Aprobador de usuarios. CA Identity Manager permite que se produzca la nueva asignación porque ese cambio no causa una infracción de la política directamente.

- Si hay varias políticas de identidad preventivas que se aplican a un conjunto de cambios propuestos, CA Identity Manager aplica políticas con acciones de rechazo primero.

- No especifique grupos dinámicos en condiciones de política de identidad preventivas. (Las condiciones de política determinan el conjunto de usuarios al que se aplica la política de identidad preventiva.)

  Por ejemplo, una compañía tiene un grupo dinámico que incluye todos los usuarios que tienen el título de gestor. Esa compañía también crea una política de identidad preventiva que prohíbe que los miembros del grupo de gestores tengan el rol de contratistas.

  Un administrador cambia el título de un usuario que tiene el rol de contratista a gestor. Este cambio convertirá al usuario en un miembro del grupo de gestores *después* de que la tarea se envíe correctamente. Sin embargo, el título del usuario no es Gestor en el momento en que CA Identity Manager evalúa la política, de manera que no se detecta ninguna infracción.

- El filtro de propietario del rol y el de la consulta LDAP no se admiten en las condiciones de política para políticas de identidad preventivas.

Creación de políticas de identidad preventivas

Antes de crear políticas de identidad preventivas, creará un conjunto de políticas de identidad, que agrupa de forma lógica un conjunto de políticas de identidad.

Nota: Consulte Notas importantes sobre las políticas de identidad preventivas (en la página 493) antes de comenzar.

Para crear un conjunto de políticas de identidad preventivas

1. En la Consola de usuario, abra Políticas, Crear conjunto de políticas de identidad.

   Cree un nuevo conjunto de políticas de identidad o use un conjunto de políticas de identidad existentes como una plantilla.

2. Defina el perfil para el conjunto de políticas de identidad (en la página 469) en la ficha Perfil.

3. Cree una regla de miembro de conjunto de políticas (en la página 470) en la ficha Políticas.

4. Cree una política de identidad preventiva de la siguiente manera:

   a. Haga clic en Agregar.

   b. Escriba un nombre para la política de identidad.

      Nota: La configuración de cumplimiento y aplicación una vez no se aplica a las políticas de identidad preventivas.

   c. Identifique los usuarios a quienes se aplica la política de la sección Condición de la política.

      Nota: El filtro del propietario del rol y el de la consulta LDAP no se admiten para las políticas de identidad preventivas.

d. En el campo Acción al Aplicar política, define las acciones que CA Identity Manager realiza cuando CA Identity Manager detecta una infracción de política:

Aceptar

CA Identity Manager muestra un mensaje en Ver tareas enviadas que describe la infracción, aunque permite el envío de la tarea.

Rechazar

CA Identity Manager muestra un mensaje en la Consola de usuario y prohíbe el envío de la tarea.

Advertencia

CA Identity Manager muestra un mensaje en la Consola de usuario y en Ver tareas enviadas. Esta acción puede, de forma opcional, iniciar un proceso de flujo de trabajo (en la página 496).

Cuando selecciona una de estas acciones, CA Identity Manager muestra un cuadro de texto en el que podrá especificar el mensaje que aparece cuando se produce una infracción.

e. Especifique el mensaje en el cuadro de texto.

Nota: Si está localizando la Consola de usuario, podrá especificar una clave de recurso en lugar de texto en el campo del mensaje. Consulte la *guía de diseño de la Consola de usuario* para obtener más información sobre las claves de recurso.

f. Agregue acciones adicionales si fuera necesario y haga clic en Aceptar.

5. Especifique los propietarios del conjunto de políticas de identidad (en la página 480).

Nota: Antes de utilizar el conjunto de políticas de identidad que haya creado, asegúrese de que se hayan activado las políticas de identidad en la Consola de gestión. Para obtener más información, consulte la *Guía de configuración*.

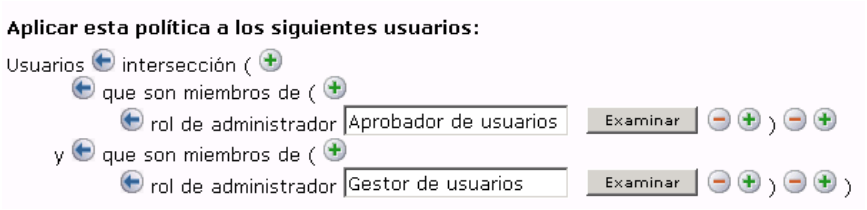
Caso: cómo impedir que los usuarios tengan roles que entren en conflicto

Forward, Inc. quiere impedir que sus empleados tengan el rol Gestor de usuarios y el rol Aprobador de usuarios a la vez. Los empleados que tienen ambos roles pueden modificar atributos de usuario, como el salario, y aprobarlos de forma inapropiada.

Para impedir esta situación, Forward, Inc. crea una política de identidad preventiva que se aplica a los usuarios que tienen los roles Gestor de usuarios y Aprobador de usuarios. Si un administrador intenta dar estos roles a un usuario, CA Identity Manager rechaza el envío de tareas y muestra un mensaje que explica la infracción.

Se configura una política de identidad preventiva para admitir este caso de la siguiente manera:

- Cree un conjunto de políticas de identidad para la política que desee crear.
- Cree una política de identidad preventiva con la configuración siguiente:
  - Condición de la política:



  - Acción al Aplicar política:
    - Rechace el mensaje: el usuario no puede ser un miembro de los roles Aprobador de usuarios y Gestor de usuarios.

Flujo de trabajo y políticas de identidad preventivas

Cuando se configura una política de identidad preventiva para emitir una advertencia, puede definir un proceso de flujo de trabajo basado en políticas en el nivel de tarea, que se asocia con la política de identidad, para las tareas que pueden iniciar una infracción. Por ejemplo, si una política de identidad prohíbe que los contables sean miembros del departamento de TI, tendrá que definir el proceso de flujo de trabajo basado en políticas del nivel de tarea en las tareas Crear usuario y Modificar usuario.

Todos los elementos de trabajo que se generan como resultado del flujo de trabajo basado en políticas en el nivel de tarea deben aprobarse antes de que CA Identity Manager ejecute la tarea. Los aprobadores verán un elemento de lista de trabajo cuando inicien sesión en la Consola de usuario. Cuando el aprobador hace clic en el elemento de lista de trabajo, aparecerá una tarea de aprobación, que incluye el mensaje de advertencia que describe la infracción. El aprobador puede optar por aprobar o rechazar la tarea, según la infracción.

Los procesos de flujo de trabajo basados en políticas se asocian con políticas de identidad preventivas por el nombre de política.

Más información:

Flujo de trabajo basado en políticas (en la página 325)

Infracciones de política de identidad en las tareas de aprobación

Cuando la política de identidad preventiva se asocia con un proceso de flujo de trabajo para una tarea, CA Identity Manager genera un elemento de lista de trabajo para los aprobadores adecuados. Estos aprobadores usan una tarea de aprobación para aprobar o rechazar el cambio que inició la infracción de política.

La tarea de aprobación predeterminada incluye una sección que muestra las infracciones de política de identidad. Puede haber más de una infracción si los cambios propuestos inician varias políticas de identidad preventivas.

Cada infracción puede tener los siguientes estados:

- **Pendiente de evaluación**

  CA Identity Manager no ha comenzado todavía a evaluar las reglas de aprobación para la tarea. Este es el estado inicial.

- **Esperando aprobación**

  CA Identity Manager encontró una coincidencia para la política de identidad definida en las reglas de aprobación e inició el proceso de flujo de trabajo asociado.

- **Aprobado**

  El aprobador aprobó los cambios propuestos. CA Identity Manager realiza los cambios que iniciaron las infracciones de política de identidad preventivas.

- **Rechazado**

  El aprobador rechazó el cambio propuesto. La tarea se ha rechazado.

- **No se ha configurado el flujo de trabajo**

  No se ha configurado ningún proceso de flujo de trabajo para esta infracción. La tarea se ejecuta sin necesidad de aprobación.

Cómo configurar el flujo de trabajo para políticas de identidad preventivas

Configure el flujo de trabajo para políticas de identidad preventivas en las tareas de administración que incluyan cambios que pueden iniciar una infracción de política de identidad.

Por ejemplo, si la política de identidad preventiva prohíbe que los usuarios tengan algunos roles de administrador a la misma vez, configure las tareas que asignan roles de administrador para admitir el flujo de trabajo para políticas de identidad preventivas.

Nota: Antes de configurar el flujo de trabajo, cree una política de identidad preventiva con la configuración siguiente:

- Un nombre de política único

  El nombre de política debe ser único en todos los conjuntos de política porque los procesos de flujo de trabajo se asocian con políticas de identidad preventivas por el nombre de política.

  Si hay varias políticas de identidad preventivas con el mismo nombre, se pueden aplicar varios procesos de flujo de trabajo.

- Advertencia en el campo Acción al Aplicar política

  Las advertencias son las únicas acciones que pueden iniciar un proceso de flujo de trabajo.

Después de configurar la política de identidad preventiva, determine las tareas que pueden iniciar la infracción de política. A continuación, cree una política de aprobación del flujo de trabajo (en la página 499) para esas tareas.

Creación de política de aprobación de flujo de trabajo para las políticas de identidad preventivas

Puede configurar un proceso de flujo de trabajo basado en políticas en el nivel de tarea para una tarea de administración. Este proceso de flujo de trabajo incluye una o varias políticas de aprobación que pueden asociar una política de identidad preventiva con un flujo de trabajo. CA Identity Manager ejecuta el flujo de trabajo cuando se produce una infracción de la política de identidad preventiva asociada.

Nota: Para obtener más información sobre procesos de flujo de trabajo basado en políticas en el nivel de tarea, consulte Flujo de trabajo basado en políticas (en la página 325).

Para crear una política de aprobación de flujo de trabajo para políticas de identidad preventivas

1. Modifique las tareas de administración que permitan cambios que puedan iniciar una infracción de una política de identidad preventiva.

   Por ejemplo, si se produjo una infracción de política de infracción porque un usuario tiene los roles Gestor de usuarios y Aprobador de usuarios, modifique las tareas de administración que permitan a los usuarios asignar roles, como los de crear usuario, modificar usuario y modificar administradores/miembros de roles de administrador.

2. Haga clic en el icono de edición situado junto al campo Proceso de flujo de trabajo en la ficha Perfil para la tarea con el fin de agregar un proceso de flujo de trabajo.

   CA Identity Manager muestra la pantalla de configuración de flujo de trabajo en el nivel de tarea.

3. Seleccione Basado en una política y, a continuación, haga clic en Agregar.

4. En la sección Regla de aprobación, seleccione el objeto Infracción de la política de identidad.

5. En el campo Política de identidad, seleccione un filtro que determina qué políticas de identidad inician el flujo de trabajo asociado con la política de aprobación.

   En el filtro, incluya el nombre de política de identidad, pero *no* el nombre del conjunto de políticas de identidad.

6. Configure los campos Evaluación de reglas, Orden de la política y Descripción de política, según sea necesario.

7. Seleccione un proceso de flujo de trabajo y después haga clic en Aceptar.

   Cuando selecciona un proceso de flujo de trabajo, CA Identity Manager muestra campos adicionales.

8. Especifique las tareas de aprobación y aprobadores según sea necesario.

   CA Identity Manager asocia el proceso de flujo de trabajo con la política de identidad preventiva.

Caso: aprobación de títulos

Forward, Inc tiene una política de empresa que define que todos los gestores deben ser empleados a tiempo completo. Sin embargo, Forward, Inc ha contratado recientemente muchos contratistas para proyectos especiales. Para llevar a cabo estos proyectos de forma eficiente, a algunos de los contratistas se les dará el título de gestor. Forward, Inc quiere la aprobación del director de Recursos Humanos antes de permitir a los administradores asignar el título de gestor a un contratista.

Para automatizar el proceso de aprobación en estas situaciones, Forward, Inc crea una política de identidad preventiva, denominada "Títulos de gestor para contratistas", que detecta cuándo el título de usuario es gestor y cuándo la organización del usuario es un contratista. Forward, Inc también configura un proceso de aprobación basado en política en la tarea Modificar usuario. Este proceso de aprobación se inicia cuando se infrinja la política Títulos de gestor para contratistas.

Cuando un administrador cambia un título de contratista a gestor, CA Identity Manager muestra un mensaje de advertencia y envía un elemento de trabajo al director de Recursos Humanos para su aprobación. CA Identity Manager no cambia el título de contratista hasta que se haya aprobado el elemento de trabajo.

Para configurar el soporte para este caso, debe completar lo siguiente en CA Identity Manager:

- Cree una política de identidad preventiva denominada "Títulos de gestor para contratistas" con la siguiente configuración:
  - Condición de la política: usuarios donde (Título = "Gestor" y Organización = "Contratista")
  - Acción al Aplicar política: advertencia con mensaje "Los gestores deben ser empleados a tiempo completo".
- Modifique la tarea Modificar usuario para incluir el proceso de flujo de trabajo con la siguiente configuración:
  - Proceso de flujo de trabajo: basado en un política
  - Objeto de regla de aprobación: infracción de la política de identidad
  - Política de identidad: donde (Nombre = "Título de gestor para contratistas")
  - Proceso de flujo de trabajo: SingleStepApproval

Combinación de políticas de identidad y políticas de identidad preventivas

Puede combinar las políticas de identidad y las políticas de identidad preventivas para afrontar los requisitos de segregación de obligaciones (SOD). En este caso, las políticas de identidad tratan las infracciones de SOD existentes mientras que las políticas de identidad preventivas prohíben nuevas infracciones.

Para poder realizar este caso, configure un conjunto de políticas de identidad con dos tipos de acciones:

- Acciones que se producen durante la sincronización de usuarios

  Estas acciones dan como resultado cambios en los atributos de usuario, miembros de grupos y roles, administradores o propietarios. Por ejemplo, una acción de este tipo puede quitar un usuario de un rol cuando se detecta una infracción.

  Estas acciones se diferencian de las acciones preventivas en que no se aplican cuando se envía una tarea. Se aplican sólo durante la sincronización de usuarios (en la página 481).

- Acciones preventivas

  Estas acciones determinan lo que CA Identity Manager hace cuando se produce una infracción de política de identidad preventiva *antes* de que se envíe una tarea. CA Identity Manager puede permitir el envío de la tarea, emitir una advertencia e iniciar un proceso de flujo de trabajo, o bien impedir que se envíe la tarea.

  En cada uno de estos casos, la infracción se registra en la base de datos de auditoría.

Imaginemos una compañía que desea impedir que los usuarios tengan roles de administrador de Recursos Humanos y de aprobador de salarios a la vez. Esa empresa crea una política de identidad con dos acciones Acción al Aplicar política:

- Eliminar al usuario del rol Aprobador de salarios

  Esta acción se produce cuando CA Identity Manager sincroniza a los usuarios con políticas de identidad.

  En este caso, esta compañía configuró la sincronización de usuarios para la tarea Modificar usuario. Cuando un administrador modifica a un usuario, CA Identity Manager evalúa todas las políticas de identidad aplicables y aplica las acciones. En este ejemplo, CA Identity Manager elimina los usuarios que tienen el rol de administrador de Recursos Humanos y de aprobador de salarios de este último rol.

- Rechazar la tarea

  Esta acción preventiva prohíbe a los administradores la asignación de estos dos roles a una persona al no permitir que el administrador envíe la tarea.

Nota: Cuando se configura una política de identidad con ambos tipos de acciones, compruebe que no haya conflictos entre ellas. Por ejemplo, puede configurar una política de identidad que impida a los usuarios tener los roles Gestor y Contratista. En la política, especifique dos acciones:

- Una advertencia que inicia un proceso de flujo de trabajo, que exige aprobación antes de asignar los roles.
- Una acción que elimina a un usuario del rol Gestor.

Los aprobadores aprueban la asignación de roles para los roles Gestor y Contratista, aunque la segunda acción elimina el usuario del rol Gestor cuando se produce la sincronización de usuarios.

Capítulo 16: Política exprés

Esta sección contiene los siguientes temas:

Descripción general de la Política exprés

La política exprés permite crear lógicas de negocios complejas (políticas) en CA Identity Manager sin la necesidad de desarrollar un código personalizado. Sin embargo, los conceptos implicados al crear políticas exprés son complejos y requieren una consideración y planificación cuidadosas. A través de las pantallas del portal de CA Identity Manager, el administrador puede configurar una política dentro de la política exprés para implementar incluso la lógica empresarial requerida más sofisticada. Como las políticas de empresa cambian, un administrador puede modificar las políticas a través de las pantallas de configuración de CA Identity Manager sin que sea necesario que un desarrollador realice cambios en el código o, lo más importante: con procedimientos de gestión de cambios adecuados, sin tener que reiniciar los servicios de CA Identity Manager.

Nota: Para obtener información más detallada sobre la política exprés, consulte la Policy Xpress Wiki.

Creación de perfiles

Para crear una política mediante la política exprés, defina los elementos básicos siguientes de la política.

Perfil

Define el tipo de política y prioridad, al tiempo que permite agrupar políticas similares para facilitar la gestión.

Eventos

Define los momentos en los que se ejecuta una política.

Nota: Asegúrese de que configura el parámetro Eventos con cuidado. La lógica del negocio debe ejecutarse en momentos específicos para evitar la corrupción de datos y para aumentar el rendimiento. Por ejemplo, un usuario deberá configurarse como activado durante su creación. Si se ejecuta esta lógica siempre, las cuentas de usuario que deben estar desactivadas podrían volver a activarse. Otro ejemplo es proporcionar al usuario un rol de aprovisionamiento que le proporcione acceso a un sistema concreto. Este rol sólo deberá asignarse al usuario después de haberle asignado y aprobado otro rol. La política exprés permite la activación de esta lógica del negocio durante el procesamiento de eventos y de los identificadores de tareas lógicas del negocio, de forma muy parecida a los adaptadores personalizados. Por lo tanto, al contrario de lo que ocurre con las políticas de identidad, la lógica puede iniciarse en cualquier momento y no exclusivamente al principio de una tarea.

Datos (elementos de datos)

Especifique los datos utilizados por la política. Cada tipo de lógica del negocio precisa una serie de datos para trabajar con ellos. Dichos datos pueden utilizarse para tomar decisiones o para construir datos más complejos. La política exprés proporciona muchos componentes individuales para recopilar datos. Dichos componentes se conocen como *Elementos de datos*. Un ejemplo de elemento de datos es un valor de atributo de usuario. Por ejemplo, la política exprés puede obtener el nombre del usuario y almacenarlo como elemento de datos para un uso posterior.

Reglas de entrada

Defina los requisitos que deben cumplirse antes de la ejecución. La definición de la reglas de entrada permite especificar el momento en el que la política exprés evalúa las políticas, lo que puede simplificar las políticas y mejorar el rendimiento. Un ejemplo de regla de entrada es ejecutar una política de 'Configurar nombre completo' *únicamente* si el nombre o los apellidos han cambiado.

Reglas de acción

Defina la acción aplicada en función de la información recopilada. Por ejemplo, en función del nombre del departamento del usuario, la política exprés podrá asignar un usuario a diversos roles o especificar valores de cuenta diferentes.

Acciones

Especifique la acción que se va a realizar. Al final del proceso, la política exprés realiza las acciones que necesita la lógica del negocio. La política exprés funciona a través de una acción vinculada a varias acciones, de modo que, cuando se cumple la regla, las acciones se realizan. Las acciones pueden incluir la asignación de valores de atributo a un usuario o cuenta, la ejecución de una línea de comandos, la ejecución de un comando SQL o la generación de un evento nuevo.

Perfil

La ficha perfil de una política exprés contiene campos que gestionan políticas y refinan capacidades de política.

Nota: Una política sólo se aplica al entorno en el que se ha creado. Por ejemplo, si crea una política mientras se encuentra en una sesión del entorno neteauto, la política sólo se ejecutará para el entorno neteauto.

Cuando cree una política, proporcione la información de perfil siguiente:

Nombre de política

Define un nombre descriptivo único para la política.

Tipo de política

Define los agentes de escucha (en la página 507) que iniciarán la política. Cada tipo de política presenta una configuración diferente.

Nota: Un vez guardado, no podrá modificar este campo.

Categoría

Define un grupo de políticas relacionadas. Este campo le permite agrupar políticas para facilitar la gestión.

Descripción

Especifica una descripción de la política.

Prioridad

Si existen varias políticas que se ejecutan en un único evento, este campo especifica cuándo se ejecuta la política. Las políticas se ejecutan en función de su prioridad. Cuanto menor sea el número, mayor será la prioridad (la prioridad 1 se ejecuta en primer lugar, la 10 se ejecuta en segundo lugar y la 50 en tercer lugar, etc.).
La configuración de la prioridad resulta útil para las políticas dependientes entre sí o para dividir una política compleja en dos sencillas, que se ejecutan una detrás de la otra.
Por ejemplo, hay tres políticas que se ejecutan si hay un valor específico en la base de datos. En lugar de hacer que cada una de las políticas verifique el valor en la base de datos, puede crear una política que se ejecute antes que las otras tres y compruebe el valor. Si la nueva política coincide con el valor indicado, la política exprés puede configurar una variable. Las otras tres políticas sólo se ejecutarán si se configura dicha variable, lo que evita el acceso redundante a la base de datos.

Activado

Especifica si la política está activa en CA Identity Manager. Si desea desactivar una política sin suprimirla, puede eliminar la selección de esta casilla de verificación.

Ejecutar una vez

Especifica si el informe se ejecuta sólo una vez. Es posible que algunas políticas tengan que ejecutarse cada vez que se cumplen unos criterios y que otras sólo tengan que ejecutarse una vez. Este valor determina si las reglas de acción que ya se han ejecutado en el pasado deben volver a ejecutarse.

Por ejemplo, si se añade un rol SAP a un usuario en función del departamento, será una acción que sólo deberá ejecutarse la primera vez que el usuario coincida con dicho departamento. Asimismo, una política que establece el salario del usuario en función del título *no* debería configurarse para que se ejecute una única vez, con el fin de garantizar que no se realicen cambios no autorizados.

Nota: La opción Ejecutar una vez se aplica a un objeto. No es de aplicación global.

Escuchas

Las políticas exprés se activan por algo que ocurre en el sistema. Para implementar esta funcionalidad, los agentes de escucha que se integran con el sistema notifican a la política exprés cuando se produce un evento y proporcionan detalles sobre el evento acontecido.

Están disponibles los agentes de escucha siguientes:

Evento

Escucha cada evento del sistema y todos los estados asociados a dicho evento (antes, aprobado, rechazado, etc.). Asimismo, el agente de escucha comunica el nombre del evento a la política exprés. Están disponibles los estados siguientes para el agente de escucha Evento:

- Antes
- Rechazado
- Aprobado
- Transcurridos
- Incorrecto

UI

Escucha las diferentes tareas que se están ejecutando en el sistema durante el estado sincronizado, lo que significa que se realiza mientras que el usuario sigue con la interfaz de usuario para la tarea abierta. Están disponibles los estados siguientes para el agente de escucha Interfaz de usuario:

- Inicio: cuando se inicia la tarea.
- Configurar asunto: cuando se encuentra el objeto principal.
- Validar al producirse un cambio: (en la página 508) cuando cambia un atributo configurado con el indicador Validar al producirse un cambio.
- Validar al enviar: al hacer clic en el botón de envío.
- Envío: cuando se envía la tarea.

Flujo de trabajo

Escucha los procesos de flujo de trabajo que han encontrado aprobadores. Este agente de escucha resulta útil para realizar la lógica basada en aprobadores, como el envío de un mensaje de correo electrónico al aprobador.

Tarea enviada

Escucha las tareas enviadas que no se están ejecutando en segundo plano. Este agente de escucha es similar al agente de escucha Evento. Sin embargo, considera la tarea un todo, en lugar de los eventos de la tarea. Están disponibles los estados siguientes para el agente de escucha Enviado:

- Tarea iniciada
- Tarea finalizada
- Error en la tarea

Sincronización inversa

Escucha las notificaciones en el sistema relacionadas con la funcionalidad Explorar de CA Identity Manager.

Validación de atributos en pantalla

Además de las activaciones definidas (tipos de políticas), la política exprés también está pendiente de la validación de atributos. Esto le permite crear políticas que se ejecutan cuando se actualiza un atributo en pantalla que se indica como “Validar al producirse un cambio”.

Esta funcionalidad puede utilizarse para crear listas desplegables dependientes. Por ejemplo, si hay dos listas desplegables en la pantalla, la política exprés se ejecuta cuando se selecciona la primera opción desplegable y, a continuación, configura los valores de la segunda lista desplegable en función de la opción seleccionada en la primera. Se pueden realizar un número ilimitado de listas desplegables y otras actualizaciones de pantalla. Esto difiere de Seleccionar datos de cuadro en que las opciones desplegables se rellenan mediante una lógica, en lugar de importar un archivo XML de opciones estáticas.

Otro uso es rellenar otros atributos en función del valor de un atributo. Por ejemplo, cuando un administrador selecciona un departamento, la política exprés puede rellenar automáticamente otros atributos, como el gestor del departamento, el número de departamento y el código de departamento de RR. HH. Esto elimina la necesidad de escribir el código personalizado de los identificadores de atributos lógicos.

Para configurar una validación con una política exprés:

1. En la consola del usuario, modifique una pantalla de perfil de una tarea y seleccione el campo que desea escuchar.
2. Acceda a las propiedades del campo y seleccione Sí en la lista desplegable para Validar al producirse un cambio.
3. En la política exprés, cree una política de tipo 'Interfaz de usuario (en la página 507)'.
4. En la ficha Ejecutar en eventos, seleccione el estado 'Validar al producirse un cambio' y la tarea modificada en el paso 1.

Caso práctico: comprobación de los nombres ofensivos

Cuando se crea un nuevo usuario, es posible que se desee comprobar si el nombre de usuario es ofensivo. El proceso siguiente indica cómo comprobar si un nombre es ofensivo mediante una política exprés.

1. Asegúrese de que los campos apropiados de la pantalla de perfil de la tarea Crear usuario estén configurados como Validar al producirse un cambio = Sí.
2. En la política exprés, cree una política de tipo 'Interfaz de usuario'.
3. En la ficha Ejecutar en eventos, seleccione el estado 'Validar al producirse un cambio' y la tarea Crear usuario.
4. Cree los elementos de datos siguientes para comprobar el nombre:
   - Obtenga el atributo del nombre (Atributos, Atributo de usuario, Obtener)
   - Analice el nombre a minúsculas (General, Analizador de cadena, A inferior)
   - Compruebe el nombre en la tabla de la base de datos de palabras ofensivas (Orígenes de datos, Datos de consulta SQL).
5. Cree elementos de datos similares a los del paso 4 para comprobar el apellido.
6. Cree una regla de acción de este modo:
   - Condición: el primer nombre no es igual a "" (esto ocurre si la consulta obtiene un mensaje de que el nombre es ofensivo).
   - Acción: se muestra un mensaje (Mensajes, Mensaje en pantalla) que indica que el nombre es ofensivo.

   Esta regla fuerza al usuario a cambiar el nombre antes de enviar de nuevo la tarea Crear usuario.
7. Cree una regla de acción similar a la del paso 6 para el apellido.

Eventos

En función del tipo de política seleccionado en la ficha del perfil, podrá configurar las horas de activación para establecer los momentos en los que se evaluará la política. Por ejemplo, una política de tipo Evento puede configurarse para su evaluación antes de Crear evento de usuario. Una política de tipo Tarea puede configurarse para su evaluación durante la configuración del asunto para un Evento de desactivación de usuario.

Para configurar una hora de activación, seleccione los campos siguientes:

Estado

Especifica el rango horario o la acción relacionados con el evento que activa la política. Por ejemplo, una política puede configurarse para que se ejecute "Antes" de que un evento tenga lugar.

Nombre de evento

Especifica el evento que activa la política, como Crear evento de usuario.

Una política puede tener más de una hora de activación. Cada vez que tiene lugar en el sistema una hora de activación específica (un estado y un evento), la política exprés busca todas las políticas con esa hora de activación y evalúa cada política basándose en su orden.

Nota: Que una política coincida con una hora de activación que tiene lugar en el sistema, no significa que la política se ejecute automáticamente. Los criterios de las reglas evaluadas posteriormente en el proceso determinan si se ha completado la política.

Elementos de datos

Los elementos de datos se utilizan para crear datos de política. Una política puede contener varios elementos de datos que representen la información utilizada por la política.

La política exprés utiliza complementos flexibles para recopilar la información de los elementos de datos. Cada complemento puede realizar una tarea pequeña y especializada. Sin embargo, pueden utilizarse varios complementos juntos para crear políticas más complejas. Un ejemplo de complemento de elemento de datos es un elemento de atributo de usuario. La finalidad del elemento es recopilar información sobre un atributo en concreto que es parte del perfil del usuario.

Los elementos de datos se calculan cuando se les llama, lo que significa que, o una regla está utilizando el elemento de datos, u otro elemento que necesita un cálculo está utilizando el elemento de datos como parámetro.
Por ejemplo, un elemento de datos de de consulta SQL puede recuperar un valor de una tabla, pero necesita que el departamento del usuario cree la consulta. En este caso, los elementos de datos del departamento deben ejecutarse antes que el elemento de datos de consulta SQL y, posteriormente, el valor podrá utilizarse como parámetro (en la página 513).

Un elemento de datos se define mediante los campos siguientes:

Nombre

Define un nombre descriptivo que describe el elemento de datos. Algunos elementos de datos son complejos (como obtener variables o recuperar información de la base de datos). Asegúrese de que selecciona un nombre con significado para simplificar la gestión del elemento de datos.

Categoría

Proporciona un grupo de elementos de datos. Este campo clasifica los elementos de datos y facilita la selección.

Tipo

Especifica el tipo de elemento de datos, cada uno con su propio uso especializado. Este campo se basa en la categoría seleccionada.

Función

Define las posibles variaciones de los mismos datos. La mayoría de los elementos de datos sólo admiten la función Obtener.

Por ejemplo, el elemento de datos de atributo de usuario presenta las funciones siguientes:

- Obtener: proporciona los valores del atributo.
- es multivalor: indica que es verdad si el valor presenta varios valores.
- es lógico: indica que es verdad si el valor es lógico.

Función Descripción

Proporciona una descripción ya introducida de la función. Cada función seleccionada presenta una descripción diferente que permite entender su uso y conocer los valores esperados.

Parámetros

Define los parámetros pasados al elemento de datos. Los elementos de datos son dinámicos y pueden hacer cosas diferentes en función de los parámetros. Un elemento de datos de atributo de usuario proporciona resultados diferentes en función del atributo seleccionado. La opción de subtipo también define el número de parámetros, sus nombres y los valores opcionales, cuando están disponibles.

Si es necesario, puede agregar parámetros adicionales. El ejemplo de consulta SQL admite dos parámetros necesarios, el origen de datos y la propia consulta. La consulta puede utilizar el símbolo "?" para sustituirlo por valores (muy similar a una instrucción preparada). Si agrega parámetros adicionales, podrá configurar dichos valores.

Nota: Cuando se visualizan elementos de datos en la política exprés, se muestra una columna llamada 'En uso'. Una marca de verificación en esta columna indica que el elemento de datos lo está utilizando una regla o un parámetro de acción, o se está utilizando como parámetro para otros elementos de datos.

Uso de los valores dinámicos de los datos o elementos de acción

Los valores dinámicos son el resultado de los elementos de datos calculados y sus valores se deciden únicamente durante el tiempo de ejecución. Entonces, esos valores pueden utilizarse como parámetros de otros elementos de datos (se calculan posteriormente en función de la prioridad).

Para utilizar un valor dinámico como parámetro para un elemento de datos:

1. En la ficha Datos de política, localice el parámetro que desea configurar como valor dinámico.
2. En el campo de texto vacío, introduzca cualquier texto regular o seleccione el valor dinámico de la lista desplegable de la derecha.
3. Haga clic en Aceptar.

Variables

La política exprés dispone de variables configuradas con acciones y guardadas como elementos de datos (categoría Variables). Las variables se comparten en todas las políticas que se ejecutan al mismo tiempo, de modo que una variable configurada la pueden utilizar otras políticas de menos prioridad.

Por ejemplo, una variable puede contener un valor calculado una vez por una política y, a continuación, compartirse con otras políticas que ya no necesitarán volver a calcular el valor. La política inicial configura un valor para la variable y las políticas que se ejecutan posteriormente leen dicho valor mediante un elemento de datos que presenta el nombre de la variable como un parámetro.

Asimismo, una variable puede activar otras políticas. En este caso, las políticas sólo se ejecutan si la política anterior se ha ejecutado.

Reglas de entrada

Las reglas de entrada definen las condiciones de cuándo se debe ejecutar una política. Estas condiciones utilizan los valores recopilados por los elementos de datos en la política.

Una política puede presentar varias reglas de entrada y una regla de entrada puede presentar varias condiciones. Al menos una regla de entrada debe coincidir, lo que significa que, para que una política pase a las reglas de acciones, deben cumplirse *todas* las condiciones de la regla de entrada.

Una regla de entrada está definida por los campos siguientes:

Nombre

Proporciona un nombre descriptivo para la regla de entrada.

Descripción

Define el significado de una regla de entrada.

Condiciones

Especifica los criterios que deben coincidir.

Nota: Las condiciones de una regla de entrada siempre presentan un operador Y entre ellas.

Más información:

Condiciones (en la página 514)

Condiciones

Las reglas de entrada y acción utilizan una condición y ésta está formada por los componentes siguientes:

- Datos de política
- Operador
- Valor

Por ejemplo, desea crear una condición que compruebe si el departamento de un usuario ha cambiado. En primer lugar, defina el elemento de datos Departamento cambiado y, a continuación, seleccione el elemento de datos Departamento cambiado, configure el operador en Es igual a y establezca el valor en Verdadero.

Más información:

Reglas de entrada (en la página 513)
Reglas de acción (en la página 514)

Reglas de acción

Las reglas de acción son similares a las de entrada en cuanto a su estructura, pero difieren en cuanto a su funcionalidad. Las reglas de acción definen cuándo se debe realizar una acción. Por ejemplo, si desea que una política realice una acción cuando el departamento de un usuario haya cambiado a Ventas, cree una regla de acción que defina cuando 'Departamento = Ventas.'

Asimismo, en lugar de tener que coincidir con una regla de entrada, puede coincidir con varias reglas de acción. La regla de acción única con la máxima prioridad (0 es la máxima) es la *única* que se utiliza.

Las reglas de acción también contienen una o más acciones divididas en Agregar acciones y Eliminar acciones.

Los siguientes parámetros definen una regla de acción:

Nombre

Proporciona un nombre descriptivo para la regla de acción. Este nombre debe ser único.

Descripción

Define el significado de una regla de acción.

Condiciones

Especifica los criterios que deben coincidir.

Prioridad

Define qué regla de acción se ejecuta, en caso de que haya varias que coincidan. Este campo resulta útil para definir las acciones predeterminadas. Por ejemplo, si tiene varias reglas, una para cada nombre de departamento, es posible configurar una predeterminada agregando una regla adicional sin condiciones, pero con una prioridad más baja (como 10 si las demás son de 5). Si no coincide ninguna regla de departamento, se utiliza la predeterminada.

Agregar acciones

Define una lista de acciones tomadas cuando la regla coincide. Por ejemplo, puede configurar una regla que indique que, si el departamento del usuario coincide con el configurado en la condición, se agregará un grupo Active Directory específico. Las reglas de acción se comportan de una forma diferente en función de la configuración de Ejecutar una vez. Si la política está configurada para ejecutarse una vez, las acciones asociadas se realizan la primera vez que la regla coincide. Las acciones no se vuelven a realizar para cada coincidencia posterior de la regla. En el ejemplo anterior, el grupo Active Directory se agrega al usuario una única vez. Si Ejecutar una vez no está configurada, las acciones se repiten cada vez que la regla coincida. Este campo es importante para que se apliquen los valores.

Eliminar acciones

Define una lista de acciones que se deben realizar cuando la regla ya no coincide. Por ejemplo, el ejemplo anterior agregó un grupo Active Directory al usuario en función del departamento. Si el departamento cambia, la eliminación de la acción elimina el grupo Active Directory.

Más información:

Condiciones (en la página 514)

Acciones

Las acciones realizan la lógica del negocio una vez que se ha completado el proceso de toma de decisiones. Una acción funciona de una forma similar a la de los elementos de datos excepto al final. Cuando se ejecuta, realiza una tarea en lugar de proporcionar un valor.

Nota: Las acciones se ejecutan en el orden que aparecen en la consola del usuario.

Una acción está definida por los campos siguientes:

Nombre de acción

Define la finalidad de la acción.

Categoría

Proporciona un grupo de acciones. Este campo clasifica las acciones y facilita la selección.

Tipo y función

Define el tipo y la función de la acción realizada.

Nota: Para obtener más información sobre Tipo y función, consulte Datos.

Función Descripción

Proporciona una descripción ya introducida de la función. Cada función seleccionada proporciona una descripción diferente que permite entender su uso y conocer los valores esperados.

Parámetros

Define los parámetros pasados a la acción.

Control de flujo

De forma predeterminada, las políticas se clasifican por prioridad y, a continuación, se evalúan una a una. Aunque este flujo se aplica casi siempre, puede modificarlo en caso necesario.

Esta funcionalidad de modificación del flujo se representa mediante una acción que se puede vincular a cualquier regla de acción. Las funciones de cambio de flujo se localizan en la categoría Sistema de la acción.

Importante: Tenga cuidado cuando cambie los flujos de procesos. El uso de estas acciones puede provocar un bucle infinito. Por ejemplo, si configura la opción 'Rehacer la política actual' en una regla de acción sin condiciones, la regla siempre será verdad y la política se reiniciará siempre y nunca finalizará.

Pueden utilizarse las cuatro funciones de cambio de flujo siguientes:

Detener procesamiento

Provoca que se ignoren todas las políticas posteriores a la actual y hace que se cierre la política exprés.
Nota: Sólo se cierra la política exprés. Si desea forzar el cierre de CA Identity Manager, puede utilizar el complemento de acción de tipo Excepción.

Reiniciar todas las políticas

Detiene el procesamiento del resto de las políticas y vuelve al inicio de la lista. Esta opción resulta útil en los casos en los que la acción de una política provoca que otra política, que se ejecuta antes que ésta y no se ha ejecutado, cumpla ahora los criterios de entrada. Entonces, dicha política vuelve a evaluarse.

Rehacer la política actual

Provoca que se vuelva a ejecutar una política. Esta opción resulta útil para la iteración. Por ejemplo, la creación de un nombre de usuario único necesita que una política se ejecute una y otra vez hasta que encuentre un nombre exclusivo.

Ir a una política específica

Esta acción precisa la selección de una política existente. Si dicha política se está ejecutando al mismo tiempo que la política actual (puede ser antes o después), la política exprés pasa a la política seleccionada. Si la nueva política presenta una prioridad inferior, se ignorarán todas las políticas entre la actual y la seleccionada. Si la nueva política presenta una prioridad superior, el proceso retrocede.

Nota: Debido a que la acción puede provocar que la política exprés se salte ciertas políticas, utilice este tipo de acción con precaución.

Definición de objetos asociados con las cuentas

Cuando se cree una acción de adición para definir un objeto asociado con una cuenta, como Miembro de, se usa un formato de relación específico para representar el objeto. Los dos tipos de formatos siguientes pueden representar el objeto en CA Identity Manager:

- Para representar relaciones sencillas entre el objeto y la cuenta, por ejemplo, grupos de Active Directory:
  `NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- Para representar relaciones de enlace entre el objeto y la cuenta, por ejemplo, roles SAP:
  `{"validFromDate":"2009\/12\/01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap endpoint,Namespace=SAP R3,Domain=im,Server=Server","validToDate":"2009\/12\/31"}`

  Las relaciones de enlace difieren de una relación sencilla en que la asociación entre el objeto y la cuenta tiene datos adicionales en ella. En el ejemplo anterior, los parámetros validFromDate y validToDate sólo incluyen datos relacionados con la asociación entre la cuenta y el rol SAP. Los datos de validFromDate y validToDate no existen en la cuenta o en el objeto del rol.

Para discernir el formato para la relación, cree un elemento de datos que obtenga el valor del objeto. El valor obtenido es el formato que se utilizará en Agregar acción para definir ese objeto.

Ejemplo: grupos de Active Directory

1. Cree una política exprés con las configuraciones siguientes:
   - Tipo de política: Evento
   - Eventos: Después – Modificar usuario
2. En la regla de acción, configure esta opción Agregar acción:
   - Categoría: Atributos
   - Tipo: Configurar datos de cuenta
   - Función: Configurar
   - Tipo de punto final: Active Directory
   - Punto final: *nombre_puntofinal*
   - Nombre de cuenta: *cuenta*
   - Atributo: Miembro de (groupMembership)
   - Valor:
     NativeGroup=Administrators,Container=Builtin,Endpoint=*nombre_puntofinal*,Namespace=ActiveDirectory,Domain=im,Server=Server

Opciones avanzadas

La política exprés permite muchas variaciones de configuración e interactúa con los componentes externos. Debido a esta flexibilidad, pueden producirse errores que no tienen que ser necesariamente problemas, como un origen de datos configurado de forma incorrecta, un valor ausente obtenido de un elemento de datos dinámicos o un punto final que no responde.

Normalmente, cuando se produce un error, el sistema detiene el cálculo de políticas para el paso actual. Sin embargo, puede modificar la respuesta de error predeterminada en función de la categoría de error. Por ejemplo, si dispone de una política que no es crítica, puede definir que el procesamiento continúe en caso de error.

La ficha Opciones avanzadas le permite cambiar las respuestas de error predeterminadas en caso necesario.

Nota: Recomendamos que dichas respuestas de error se dejen con las opciones predeterminadas, pero, para casos de usos avanzados, estas configuraciones pueden cambiarse por política. Por ejemplo, si dispone de una política que no es crítica, puede definir que dicho procesamiento continúe aunque falle la política.

En la ficha, pueden configurarse las categorías de error siguientes:

- Validación: provocado al proporcionar una información incorrecta a un complemento. Este tipo de error se comunica antes de que se intente aplicar la acción.
- Entorno: provocado por problemas en el entorno, como un servidor de base de datos que falla para el complemento SQL.
- Permitido: error no crítico. El comportamiento predeterminado de este tipo de error es seguir con el procesamiento de la solicitud, como cuando se produce un error en el envío de correos electrónicos.

Para cada uno de los errores anteriores, pueden configurarse las opciones siguientes:

- Evento erróneo: detiene la acción actual. Éste es el valor predeterminado para la mayoría de los tipos de error.
- Política errónea: detiene la política actual y todas las acciones asociadas. El resto de las políticas continúan.
- Ignorar: registra cualquier error pero no detiene las acciones ni las políticas.

Capítulo 17: Aplicación móvil de CA Identity Manager

La aplicación móvil de CA Identity Manager permite aprovechar la infraestructura existente de CA Identity Manager para que los usuarios puedan realizar las siguientes tareas en un dispositivo móvil, como un smartphone o una tableta:

- Restablecer una contraseña olvidada
- Cambiar una contraseña
- Responda a solicitudes de aprobación aceptándolas o rechazándolas. Utilice la Consola de usuario para reservar o publicar una solicitud.
- Ver información sobre el usuario

  Esta función permite a los usuarios consultar información acerca de otros usuarios de la organización. Por ejemplo, los aprobadores de elementos de trabajo pueden consultar información básica sobre el gestor de usuarios (por ejemplo, el nombre y la dirección) antes de tomar una decisión de aprobación. Si necesita más información, el aprobador puede hacer clic en un vínculo para ver el perfil completo.

Esta sección contiene los siguientes temas:

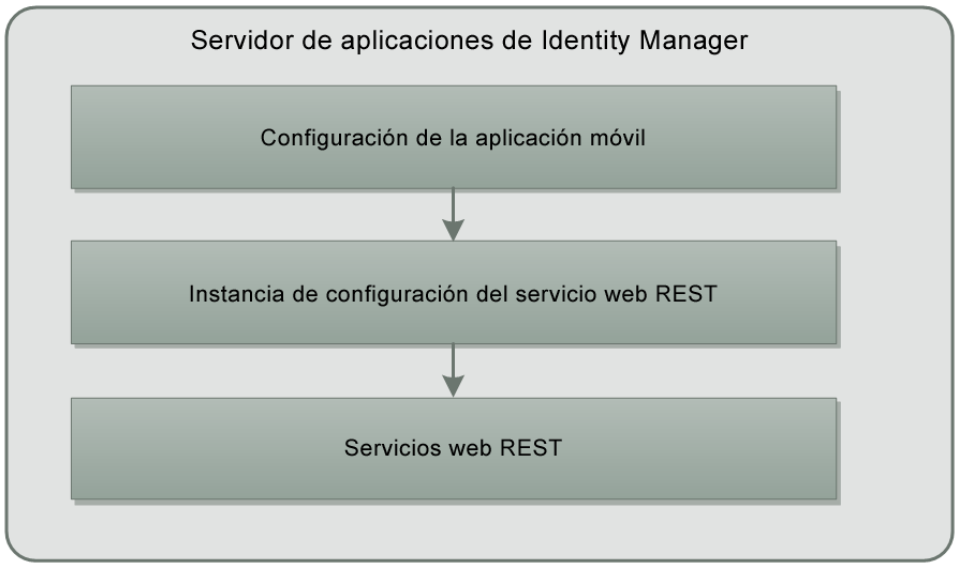
Arquitectura de la aplicación móvil de CA Identity Manager

La arquitectura de la aplicación móvil de CA Identity Manager está diseñada para proporcionar un conjunto de capacidades de CA Identity Manager a los distintos tipos de dispositivos móviles, tales como teléfonos inteligentes y tabletas. Las capacidades seleccionadas para la aplicación móvil están basadas en la necesidad empresarial crítica y para los usuarios cuya interacción es la adecuada para dispositivos más pequeños.

La arquitectura se centra en el uso de un componente de la configuración específico para la aplicación y para los servicios web RESTful que exponen las capacidades del servidor de CA Identity Manager. El servidor de CA Identity Manager es compatible con la capacidad de gestión de la configuración de la aplicación móvil de un entorno específico y la configuración de los servicios web REST utilizados por la aplicación.

Nota: A diferencia de los servicios web de ejecución de tareas basados en SOAP (TEWS), los servicios web REST pertenecen a la aplicación móvil de CA Identity Manager y no se pretende que sean API públicas.

Los servicios web REST pueden admitir varias configuraciones en función del entorno de CA Identity Manager (IME), donde cada configuración se asocia normalmente con un cliente REST concreto, como por ejemplo la aplicación móvil. A continuación, se muestra un esquema de la arquitectura de alto nivel y la relación entre la configuración de la aplicación móvil y la configuración del servicio web.



La configuración de los servicios web REST requiere la selección de un conjunto específico de opciones para que la aplicación móvil funcione. Antes de poder crear la configuración de la aplicación móvil (disponible también mediante una tarea administrativa), se debe definir la configuración del servicio web mediante la tarea de configuración del servicio web.

Detalles de la configuración del servicio web para la aplicación móvil

Una configuración de servicio web REST está formada por los elementos siguientes:

- Un perfil que define un nombre de la configuración único, un identificador y un indicador activado.
- Una configuración de seguridad que define el uso de SSL, el cifrado de la carga y una clave de cifrado.
- El conjunto de tipos de objetos gestionados y las operaciones y atributos compatibles para cada tipo mediante REST.
- Operaciones de autoservicio compatibles, tales como el restablecimiento de la contraseña y el conjunto de atributos autoservicio del usuario permitidos.
- La política de miembros para la cual se autoriza a los usuarios a invocar las operaciones de REST configuradas.

En la tabla siguiente se muestran los detalles de la configuración del servicio web y los valores de configuración requeridos para la aplicación móvil.

Sección de la configuración	Elemento	Descripción	Configuración de la aplicación móvil
Perfil	nombre	El nombre de la configuración.	Selección de la implementación
	identificador	El identificador único que un cliente específico debe establecer en el encabezado HTTP Configuration-Id (ID de la configuración) de cada solicitud del servidor de CA Identity Manager.	Selección de la implementación. El servicio de configuración de la aplicación móvil devuelve el identificador que se debe utilizar en todas las solicitudes de REST subsiguientes.
	Activado	Activa/Desactiva la configuración.	Verdadero
seguridad	Requiere comunicación segura	Define si se requiere un protocolo HTTPS.	Selección de la implementación. Valor descargado por medio del servicio de configuración de la aplicación móvil.

	Activar cifrado	Se utiliza para cifrar la carga que no es SSL. Requiere la biblioteca de cifrado del cliente, el conocimiento de claves de cifrado y la compatibilidad de la funcionalidad de cifrado y descifrado con el cliente.	No se utiliza. Se debe dejar este parámetro sin seleccionar.
	Secreto de la configuración	Secreto compartido requerido como parte del cliente REST para el modelo de confianza del servidor.	Su especificación es obligatoria. Las implementaciones deben generar el secreto al definir la instancia de configuración.
Tipos de objeto	Tipo de objeto	Los tipos de objeto expuestos como recursos REST.	El tipo de objeto de usuario.
	Métodos y atributos	Los métodos de recursos (CRUD) compatibles para un tipo de objeto seleccionado y el conjunto de atributos permitidos para esos métodos.	El tipo de objeto de usuario con permiso de visualización a los atributos siguientes, tal y como se muestra en el esquema de usuario específico de la implementación: ■ Teléfono del negocio ■ Departamento ■ correo electrónico ■ Nombre ■ Apellido ■ Gestor ■ Oficina ■ Título

Autoadministración	Regla de miembros	Una regla que indica los usuarios que tienen permiso para administrase ellos mismos.	Debe coincidir con la regla de miembros de la configuración de la aplicación móvil. El conjunto de atributos para su modificación debe estar vacío.
	Activar restablecimiento de la contraseña	Permite a los usuarios restablecer su propia contraseña.	Activado
	Atributos	El conjunto de atributos que los usuarios pueden gestionar por ellos mismos.	Lista vacía
Miembros	Miembros	Define las reglas para las cuales se autoriza a los usuarios a invocar las operaciones REST definidas para esta configuración.	Una regla de miembros que coincide con el conjunto de usuarios de la aplicación móvil.

Cómo funciona el proceso de implementación

En la configuración de aplicaciones para móviles intervienen tres tipos de usuarios. En la siguiente gráfica se muestran estos tipos de usuarios y las tareas que realizan.

Para activar a un usuario final con el fin de utilizar la aplicación para móviles con CA Identity Manager, se producen las siguientes actividades:

1. Un administrador del sistema configura la compatibilidad con la aplicación para móviles en un entorno.

   En la configuración se producen las siguientes actividades:

   - Configuración de los atributos del código de activación y restablecimiento
   - Adición de tareas, políticas de la política exprés y una plantilla de correo electrónico para el registro de usuarios de móviles
   - Creación de definiciones de servicios web
   - Modificación del correo electrónico de registro

   El administrador del sistema también configura las marcas, las direcciones URL y la funcionalidad a los que los usuarios de móviles pueden acceder.

2. Un administrador, como un técnico de Help Desk, registra los usuarios finales pertinentes en la Consola de usuario.

   El proceso de registro activa un código de activación para cada usuario final y envía automáticamente un correo electrónico con el código y las instrucciones de registro al usuario final.

3. El usuario final descarga la aplicación móvil desde la tienda de Apple y registra un dispositivo (por ejemplo, un smartphone o una tableta) siguiendo las instrucciones y el código recibido por correo electrónico.

   El usuario final puede utilizar a continuación la aplicación para móviles para acceder a la funcionalidad de CA Identity Manager.

   Nota: Si está seleccionada la opción Se debe cambiar la contraseña durante la creación del usuario, los usuarios de la aplicación móvil no podrán completar la activación.

Cómo funciona la configuración de la aplicación

La aplicación móvil recupera su configuración de las API de configuración del servidor de CA Identity Manager. Cuando se instala primero la aplicación móvil y no se ha descargado ninguna configuración, esta solicita el nombre de usuario y la contraseña al usuario y utiliza estas credenciales para descargar la configuración definida a través del vínculo proporcionado en el correo electrónico de registro del usuario.

Una vez que se descarga la configuración inicial, cada vez que se inicia la aplicación, esta compara su versión de la configuración con la última versión disponible en el servidor de CA Identity Manager. Para detectar si existe una versión posterior disponible, se utiliza la API de comprobación de versiones de configuración.

Cómo funciona el registro de usuarios

Todo aquél usuario que desea acceder a la aplicación móvil debe solicitar el acceso mediante CA Identity Manager. Si se aprueba su acceso, se actualiza el usuario con un código de activación que indica que se le ha concedido acceso a la aplicación. La política de miembros de la configuración de la aplicación móvil y la política de miembros de los servicios web subyacente deben coincidir con todos los criterios definidos para los usuarios móviles que solicitan acceso a la aplicación. Como mínimo, se debe definir el valor %ACTCODE% para Registered (Registrado) o un valor mayor de 0.

Si se elimina el acceso móvil de un usuario, el servidor de CA Identity Manager restablece los atributos de activación e impide al usuario acceder a la aplicación móvil.

Cómo configurar CA Identity Manager para que sea compatible con aplicaciones para móviles

La aplicación para móviles se comunica con CA Identity Manager (mediante los servicios Web de REST) para gestionar contraseñas y aprobaciones. Para activar esta comunicación, los administradores del sistema completarán los siguientes pasos:

1. Configurar atributos obligatorios (en la página 529)
2. Importar las tareas de administración (en la página 532)
3. Crear un servicio Web (en la página 534)
4. Modificar el correo electrónico de registro (en la página 536)
5. Opcionalmente, configurar la compatibilidad con SiteMinder para la aplicación móvil.

Configurar atributos obligatorios

En el almacén de usuarios de CA Identity Manager se deben incluir los siguientes atributos conocidos para activar el registro de usuario y el acceso a través de la aplicación para móviles:

- %ACTCODE%: identifica el atributo que almacena un número de activación generado aleatoriamente. Una vez que se ha registrado el usuario, este atributo incluye la palabra Registrado.
- %ACTCODEVAL%: identifica el atributo que almacena el código de activación que el cliente establece durante el tiempo de registro. CA Identity Manager compara este valor con el de %ACTCODE%.
- %CURRENT_AUTH_QUESTIONS%: identifica el atributo que almacena provisionalmente los valores de la pregunta de desafío. Este valor se borra después de que el usuario conteste correctamente.
- %MOBILE_PIN%: identifica el atributo que almacena el número de identificación personal o el valor de cadena que proporciona la contraseña alfanumérica compartida entre un usuario y un sistema, y que se puede utilizar para autenticar el usuario en el sistema.
- %PWRESETCODE%: identifica el atributo que almacena un código cifrado que proporciona la autenticación de factor único durante el restablecimiento de una contraseña

Asigne estos atributos conocidos a los atributos de almacén de usuarios disponibles en el archivo de configuración del directorio (directory.xml). Si no hay ningún atributo disponible, extienda el esquema de almacén de usuarios. Para obtener más información sobre la extensión del esquema, consulte la documentación del almacén de usuario.

Incluya las siguientes clasificaciones de datos en las descripciones de los atributos:

<DataClassification name="sensitive"/>

Reemplaza el valor de código restablecido por caracteres comodín en pantallas de tarea, registros de auditoría y registros de sistema.

Importante: No incluya la clasificación de datos confidenciales en la definición del atributo de %ACTCODE%. Si se incluye el atributo de datos confidenciales, la aplicación móvil no funcionará correctamente.

<DataClassification name=" AttributeLevelEncrypt "/>

Cifra y descifra el valor del código de restablecimiento tal y como está escrito y lee información del almacén de usuarios mediante la clave de cifrado definida.

<DataClassification name=" ignore_on_copy "/>

Hace que CA Identity Manager ignore un atributo cuando un administrador crea una copia de un objeto en la Consola de usuario.

Nota: Consulte el final de este tema para obtener ejemplos de estos atributos conocidos.

Siga estos pasos:

1. Inicie sesión en la Consola de gestión.
2. Seleccione Directorios y, a continuación, haga clic en el directorio que contiene usuarios de móviles.
3. Exporte el directorio.
4. Agregue o modifique una descripción del atributo para incluir el atributo conocido %ACTCODE%.

   Se puede asignar cualquier atributo disponible al atributo conocido %ACTCODE%.
5. Repita el paso 4 para definir el atributo conocido %ACTCODEVAL%. Incluya las siguientes clasificaciones de datos:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
6. Agregue una descripción del atributo para el atributo conocido %CURRENT_AUTH_QUESTIONS%. Incluya las siguientes clasificaciones de datos:
   ```
   <DataClassification name="ignore_on_copy"/>
   ```
7. Agregue una descripción de atributo para el atributo conocido %MOBILE_PIN%. Incluya las siguientes clasificaciones de datos:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
8. Agregue una descripción de atributo para el atributo conocido %PWRESETCODE%. Incluya las siguientes clasificaciones de datos:
   ```
   <DataClassification name="sensitive"/>
   <DataClassification name="ignore_on_copy"/>
   <DataClassification name=" AttributeLevelEncrypt"/>
   ```
9. Guarde el archivo directory.xml.
10. Cargue el archivo directory.xml guardado haciendo clic en Update (Actualizar) en la página Directory Properties (Propiedades de directorio) de la Consola de gestión.

Ejemplos

Nota: Se puede asignar cualquier atributo disponible a estos atributos conocidos.

%ACTCODE%

```
<ImsManagedObjectAttr
physicalname="nombre_atributo"
displayname="nombre_para_mostrar_del_atributo"
description="descripción_del_atributo"
valuetype="String"
required="false"
multivalued="false"
```

```
    wellknown="%ACTCODE%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%ACTCODEVAL%

```
    ImsManagedObjectAttr
    physicalname="nombre_atributo"
    displayname="nombre_para_mostrar_del_atributo"
    description="descripción_del_atributo"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%ACTCODEVAL%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
    <ImsManagedObjectAttr
    physicalname="nombre_atributo"
    displayname="nombre_para_mostrar_del_atributo"
    description="descripción_del_atributo"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%CURRENT_AUTH_QUESTIONS%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
    <ImsManagedObjectAttr
    physicalname="nombre_atributo"
    displayname="nombre_para_mostrar_del_atributo"
    description="descripción_del_atributo"
```

```
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%MOBILE_PIN%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%PWRESETCODE%

```
    <ImsManagedObjectAttr
    physicalname="nombre_atributo"
    displayname="nombre_para_mostrar_del_atributo"
    description="descripción_del_atributo"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%PWRESETCODE%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

Importación de tareas de administración

Antes de que los usuarios móviles puedan iniciar sesión en CA Identity Manager, los administradores los registrarán en la Consola de usuario. El proceso de registro genera un código de activación y envía un correo electrónico al usuario móvil.

Para que sea compatible con estas actividades, importe un archivo de definiciones del rol que agrega la siguiente funcionalidad a un entorno:

- Tareas de configuración móviles
- Registro de usuarios para aplicaciones para móviles y eliminación de usuarios de las tareas de aplicaciones para móviles
- Políticas exprés que generan códigos de activación y anulan el registro del cliente móvil desde una cuenta de usuario.
- Una plantilla de correo electrónico para enviar correos electrónicos a usuarios de móviles.

Siga estos pasos:

1. Inicie sesión en la Consola de gestión.
2. Seleccione Environments (Entornos) y, a continuación, haga clic en el entorno que es compatible con la aplicación para móviles.
3. Seleccione Role and Task Settings (Configuración de roles y tareas) y, a continuación, haga clic en Import (Importar) en la siguiente pantalla.
4. Seleccione las definiciones de rol para aplicaciones para móviles y, a continuación, haga clic en Finalizar.
5. Reinicie el entorno.
6. Agregue las siguientes tareas al rol Gestor del sistema:
   - Creación de una configuración móvil
   - Modificación de una configuración móvil
   - Visualización de una configuración móvil
   - Eliminación de una configuración móvil
   - Registro de usuarios para aplicaciones para móviles
   - Eliminación de usuarios de aplicaciones para móviles

   Las tareas nuevas están en las categorías de Usuario y Sistema.

Creación de una configuración de servicios Web

La aplicación para móviles utiliza servicios web de REST para comunicarse con CA Identity Manager. Para que sea compatible con la aplicación para móviles, los administradores del sistema crearán una definición de servicio web en la Consola de usuario.

Nota: Las llamadas REST no funcionan si se ha activado la funcionalidad de cifrado durante la configuración del servicio web.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario con privilegios de administrador del sistema.
2. Cree una definición de servicio web tal y como se muestra a continuación:
   a. Vaya a Sistema, Servicios web, Crear configuración de servicios web.
   b. En la ficha Perfil, complete los siguientes campos:
      - Nombre: *cualquier nombre.* Por ejemplo "RestMobile"
      - Identificador: *identificador único.* El valor predeterminado es RestMobile.

        El valor del campo Identificador debe coincidir con el de **restid** en la configuración de la aplicación para móviles.

        Se debe tener en cuenta la posibilidad de cambiar el valor de Identificador y restid para aumentar la seguridad.
      - Activar atributo: active esta casilla de verificación.

c. En la ficha Seguridad, rellene los siguientes campos:

- Determine si es necesario seleccionar la opción Requerir comunicación segura:

Nota: Considere cifrar todo el tráfico HTTP de la aplicación móvil. Normalmente existen dos formas de configurar este tráfico:

- Utilizando un servidor proxy: En este caso de uso, el servidor de CA Identity Manager estará detrás de un cortafuegos. Puede decidir no asegurar la comunicación del servidor proxy al servidor de CA Identity Manager. Sin embargo, se debe garantizar que la comunicación de HTTP entre la aplicación móvil y el servidor proxy sea segura. Para este caso de uso, NO seleccione Requiere comunicación segura.

Nota: En el caso de no integrar CA Identity Manager con SiteMinder, seleccione la opción Requiere comunicación segura para conservar la comunicación SSL para las llamadas de los servicios web.

- Directamente en el servidor de CA Identity Manager: En este caso de uso, el cliente móvil se comunica directamente con el servidor de CA Identity Manager; esta comunicación de HTTP se debe cifrar. Para exigir ese requisito, seleccione la opción Requiere comunicación segura.
- Compruebe que la opción Activar cifrado no esté seleccionada.

Nota: Si la funcionalidad de cifrado está activada, los detalles del usuario no se muestran en la aplicación móvil.

d. En la ficha Tipos de objeto, acceda a USUARIO, seleccione USUARIO y haga clic en el botón Editar.

e. Seleccione solo Permitir visualización del acceso.

Elimine otros permisos de acceso; para ello, quite la marca de las opciones Permitir modificación de acceso, Permitir creación de acceso y Permitir supresión de acceso.

f. En la ficha Autoadministración, complete los siguientes pasos:

- Seleccione el botón Agregar, situado debajo de Regla de miembros para crear un rol de miembro y especifique "todo".

  Nota: Solo se puede crear una regla de miembro.

- Active el restablecimiento de contraseña para utilizar la función Cambiar contraseña en la aplicación para móviles.

g. En la ficha Miembro, cree una regla de miembro con los siguientes criterios:

- Activation Code = Registered, or
- Activation Code >0

h. Envíe y guarde el servicio Web.

Modifique el correo electrónico de registro

Edite el correo electrónico de registro predeterminado para incluir la dirección URL del objeto de configuración móvil.

Siga estos pasos:

1. En la Consola de usuario, vaya a Sistema, Correo electrónico, Modificar correo electrónico.
2. Busque y seleccione el correo electrónico de usuario registrado para la aplicación para móviles.
3. En la ficha Contenido, haga clic en el botón de alternancia del código fuente de HTML.
4. Especifique la dirección URL del objeto de configuración móvil en la entrada href de mobileregservidm, tal y como se muestra a continuación:

   <a href="mobileregservidm://{'Attribute:%ACTCODE%'}&https://FQN/iam/im/ws/Alias/mobile/ConfigName">

   Nombre completo

   Especifique el nombre o la dirección IP del servidor CA Identity Manager.

   Alias

   Especifique el nombre del entorno.

   ConfigName

   Especifique el nombre del objeto de configuración.
5. Haga clic en Enviar.

Cómo configurar la compatibilidad con SiteMinder para la aplicación móvil

Los servicios web utilizados por la aplicación móvil pueden permiten el modo de autenticación nativa por medio de las credenciales de nombre del usuario y contraseña proporcionadas por la aplicación móvil mediante el encabezado HTTP AUTHORIZATION (AUTORIZACIÓN HTTP) o la autenticación de SiteMinder. Tal y como se ha comentado previamente, mediante la configuración de los servicios web se define la política de autorización para cada uno de los recursos REST y los métodos de solicitud.

Direcciones URL de servicio web REST de IM

Los servicios REST de IM dependen totalmente de la dirección URL base siguiente:

`http[s]://[FQN]/iam/im/ws/[Alias]`

- FQN: nombre completo y puerto del punto de acceso al servidor de CA Identity Manager
- Alias: alias público del entorno de CA Identity Manager al que conectarse.

Dirección URL de la configuración de aplicación móvil

La configuración de la aplicación móvil contiene una dirección URL específica que admite la recuperación de la información de la configuración de arranque requerida para la descarga de la configuración de la aplicación móvil. La dirección URL de configuración es la siguiente:

`http[s]://[FQN]/`
`iam/im/ws/[Alias]/mobile/[Nombre_configuración]`

ConfigName: nombre de la configuración de la aplicación móvil del entorno de CA Identity Manager para un conjunto específico de usuarios de la aplicación móvil. Una vez que se aprueba la solicitud de acceso a la aplicación móvil por parte de un usuario, se envía un correo electrónico de registro al usuario, en el que se incluye un vínculo a la dirección URL de la configuración para proporcionar el nombre de la configuración a la aplicación.

API de REST sin autenticar

API de configuración

Las API de configuración siguientes no requieren autenticación.

`http[s]://[FQN]/`
`iam/im/ws/[Alias]/mobile/[Nombre_configuración]/image`
`http[s]://[FQN]/`
`iam/im/ws/[Alias]/mobile/[Nombre_configuración]/ver`

Restablecimiento de la API de la contraseña

`http[s]://[FQN]/`
`iam/im/ws/[Alias]/myself/resetpasswordWithResetCodeAndToken`

Nota: La API resetPasswordWithResetCodeAndToken contiene tókenes de seguridad proporcionados por medio de los encabezados HTTP de la aplicación móvil. El servidor de CA Identity Manager verifica la presencia y validez de estos tókenes.

Durante la integración con SiteMinder para proteger el acceso a CA Identity Manager, estas direcciones URL se pueden definir con un dominio que no está protegido o que no está protegido por medio de un esquema de autenticación anónimo.

API de REST autenticadas

La aplicación móvil utiliza las direcciones URL siguientes, que requieren autenticación y que utilizan las políticas de la configuración del servicio web para su autorización.

Configuración

```
http[s]://[FQN]/
iam/im/ws/[Alias]/mobile/[Nombre_configuración]/conf
```

Usuario de autoservicio

```
http[s]://[FQN]/iam/im/ws/[Alias]/myself
```

Lista de trabajos

```
http[s]://[FQN]/iam/im/ws/[Alias]/worklist
```

Usuario

```
http[s]://[FQN]/iam/im/ws/[Alias]/mo/User
```

Configuración de una aplicación para móviles

Los administradores del sistema configuran la aplicación móvil de CA Identity Manager en la Consola de usuario.

Un entorno puede incluir varias configuraciones de la aplicación móvil. La creación de diferentes configuraciones permite que admita diferentes marcas o funcionalidades para distintos tipos de usuarios móviles. Por ejemplo, se puede crear una configuración para los cambios de la contraseña del empleado y otra configuración para que los gestores aprueben elementos de trabajo.

Los administradores pueden configurar las siguientes propiedades en la aplicación para móviles:

- Marcas

  Especifique el logotipo de la empresa en la aplicación para móviles.

- Funcionalidad

  Active la siguiente funcionalidad:

  - Soporte de contraseña olvidada
  - Compatibilidad con el cambio de contraseña
  - Cola de aprobación del flujo de trabajo
  - Visualización del vínculo de gestor

- Información de soporte
- Asignación de atributos

  Asigne los atributos del almacén de usuarios a los atributos que se muestran en la aplicación para móviles.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como usuario que pueda utilizar las tareas de configuración móviles.
2. Haga clic en Tareas, Sistema, Configuración móvil, Crear configuración móvil.
3. Acepte la opción predeterminada Crear un nuevo objeto del tipo Configuración móvil.
4. En la ficha General, rellene los siguientes campos: Se puede especificar una imagen para la aplicación móvil.

   Dirección URL base

   Verifique la dirección URL base del entorno actual. La dirección URL base se rellena automáticamente cuando se crea una configuración móvil.

   CA Identity Manager utiliza la dirección URL base para recuperar el nombre del servidor, puerto y protocolo, que la aplicación móvil utiliza para construir la dirección URL para las llamadas REST.

   Configuración

   Busque una configuración o introduzca un nombre único para la configuración.

   Versión

   Aumente el número de versión todas las veces que se modifique y se guarde una configuración.

   La aplicación para móviles utiliza el número de versión para determinar cuándo descargar una nueva versión de la configuración. Cuando la aplicación móvil se inicia, compara el número de versión del servidor con la versión de la configuración cargada. Si una versión nueva está disponible, la aplicación móvil actualizará la configuración.

   Nota: No incremente el número de versión cuando modifique al principio el archivo.

   Imagen de marca

   Especifique la dirección URL completa de una imagen PNG con un fondo transparente. La imagen aparece en la parte superior de la pantalla de la aplicación móvil.

5. En la ficha Funciones, seleccione las funciones para la aplicación móvil.

   Comportamiento de restablecimiento de la contraseña

   Seleccione el método que se utilizará en el comportamiento, que se determina cuando se configuran los atributos obligatorios:

   - Predeterminado
   - Desafío de PIN
   - Desafío de QnA

   Nota: Si se selecciona el desafío de QnA, se debe ir a Tareas, Environment Administrator (Administrador de entorno), y, a continuación, seleccionar Question and Answer Configuration (Configuración de pregunta y respuesta). Asegúrese de seleccionar el cuadro Activar, introduzca el número de preguntas de autenticación (desde 1 hasta 5) y, a continuación, haga clic en Enviar. Debe hacer clic en el botón Enviar para que los valores de configuración se apliquen, aunque no realice cambios en los valores de configuración predeterminados.

6. En la ficha Soporte, especifique información de soporte para los usuarios móviles.

7. En la ficha Asignación de atributos, asigne atributos de la aplicación móvil a los atributos en el almacén de usuarios de CA Identity Manager. Se pueden asignar los atributos a atributos físicos o a atributos conocidos.

8. En la ficha Propiedades adicionales, especifique los pares de valor de la propiedad adicional para admitir la nueva funcionalidad o los campos en la aplicación móvil.

   Utilice el siguiente formato:

   Clave1=valor1

   Clave2=valor2

   Clave3=valor3

   Nota: CA Technologies proporcionará instrucciones cuando los administradores deban agregar propiedades adicionales. En esta versión, no es necesario especificar propiedades adicionales.

9. En la ficha Miembros, especifique las reglas que determinan el conjunto de usuarios que ven esta configuración en su aplicación móvil.

10. Haga clic en Enviar.

Configuración de propiedades adicionales

Una vez configurada la aplicación móvil, se pueden especificar opcionalmente pares valor-clave para propiedades adicionales para admitir nuevas funcionalidades en la aplicación móvil. En la ficha Propiedades adicionales, introduzca los valores siguientes:

Utilice el siguiente formato:

- demoMode="Desactivar/Activar"
- maxPinRetries=<cualquier valor numérico positivo>
- multiAccount="Desactivar/Activar"
- managerTraversal="Desactivar/Activar"
- startupWithBrandLogo="verdadero/falso"

Nota: CA Technologies proporcionará instrucciones cuando los administradores deban agregar propiedades adicionales.

Sin embargo, estas tres funciones están activadas de forma predeterminada en las configuraciones móviles:

- DemoMode: permite visualizar la versión de demostración de la aplicación móvil. Esta opción está disponible en la sección Configuración de la aplicación móvil.
- maxPinRetries: permite al administrador configurar el número de intentos de entrada de un número PIN incorrecto o erróneo para los usuarios móviles. El número predeterminado de intentos erróneos es 5.
- MultiAccount: permite agregar varias cuentas, específicamente mediante la adición de varios usuarios móviles registrados con sus códigos de activación.
- ManagerTraversal: muestra los detalles de gestor del aprobador y del solicitante en los detalles del elemento de trabajo.
- startupWithBrandLogo: permite al usuario especificar un logotipo de cuenta personalizado (la imagen de personalización de la marca de la cuenta) para que aparezca en lugar del logotipo de CA predeterminado. Si se establece este par clave-valor como verdadero, pero por algún motivo, el campo del logotipo de la marca no contiene ninguna dirección URL o la dirección URL especificada no es correcta, durante el inicio se mostrará una pantalla de arranque vacía. El logotipo de CA siempre aparece cuando se inicia la aplicación justo después de la instalación. Esta propiedad adicional forma parte de los datos de una cuenta. En el arranque inicial, los datos de la cuenta no están disponibles.
  Nota: Estos cambios se reflejarán en el siguiente inicio, una vez que se haya establecido una comunicación correcta con el servidor de CA Identity Manager.

Para desactivar estas funciones en el cliente móvil, se debe agregar el par valor-clave siguiente en la ficha Propiedades adicionales de la configuración móvil de CA Identity Manager

- Para activar o desactivar DemoMode

  Establezca el valor Activar o Desactivar para DemoMode

  - demoMode="Desactivar/Activar"

- Para activar o desactivar la función maxPinRetries

  Establezca cualquier valor numérico positivo para maxPinRetries.

  - maxPinRetries=<cualquier valor numérico positivo>. Tenga en cuenta que el número predeterminado de intentos erróneos es 5.

- Para activar o desactivar la función MultiAccount

  Establezca el valor Activar o Desactivar para MultiAccount

  - multiAccount="Desactivar/Activar"

- Para activar o desactivar la función ManagerTraversal

  Establezca el valor Activar o Desactivar para ManagerTraversal.

  - managerTraversal="Desactivar/Activar"

- Para activar o desactivar la función startupWithBrandLogo

  Establezca startupWithBrandLogo como verdadero o falso.

  - startupWithBrandLogo="verdadero/falso"

Siga estos pasos:

1. Inicie sesión en la Consola de usuario de CA Identity Manager como administrador (superusuario).
2. Haga clic en Tareas, Sistema, Configuración móvil, Crear configuración móvil.
3. En la ficha Propiedades adicionales, especifique los pares clave-valor de las propiedades adicionales para admitir las nuevas funcionalidades en la aplicación móvil.
   - demoMode="Desactivar/Activar"
   - maxPinRetries=<cualquier valor numérico positivo>. El número predeterminado de intentos erróneos es 5.
   - multiAccount="Desactivar/Activar"
   - managerTraversal="Desactivar/Activar"
   - startupWithBrandLogo="verdadero/falso"

Descarga de la aplicación móvil

Una vez que la aplicación móvil se configura, los usuarios finales la pueden descargar de Apple Store. Para encontrar la aplicación móvil en el Apple Store, busque CA Identity Manager.

El usuario final puede registrar su dispositivo, por ejemplo su teléfono inteligente o tableta, mediante las instrucciones e introduciendo el código que reciban por correo electrónico.

Solución de problemas de la aplicación para móviles

Permiso de solicitud de un archivo de registro por parte del equipo de soporte

Si un usuario tiene una incidencia con la aplicación para móviles, los ingenieros de soporte pueden solicitar un archivo de registro para ayudar a solucionar los problemas.

El usuario de móviles activa la depuración en iPhone o iPad. Una vez que se activa la depuración, el usuario de móviles puede utilizar la aplicación para móviles para enviar el registro a una dirección de correo electrónico de soporte.

Para permitir que la aplicación para móviles genere un registro, el usuario de móviles completará los siguientes pasos.

1. En el teléfono o iPad, vaya a Configuración, Identity Manager, Depuración.
2. Se ha activado la pulsación.
3. Reinicie la aplicación y realice las acciones que desea que se muestren en el registro.
4. En la ficha Configuración de la aplicación para móviles de CA Identity Manager, pulse Registro de correo electrónico.

   La aplicación para móviles crea un correo electrónico con el archivo de registro adjunto. El correo electrónico se puede enviar a la dirección de correo electrónico que se ha especificado para la asistencia en la Consola de usuario.

Error de ejecución de la opción QnA como comportamiento de restablecimiento de la contraseña mediante los valores de configuración de pregunta y respuesta predeterminados en Administrador del entorno de las tareas de Identity Manager

Síntoma

Si se selecciona la opción QnA como comportamiento de restablecimiento de contraseña con los valores de configuración de pregunta y respuesta predeterminados, se produce el error siguiente al restablecer la contraseña:

"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file" [ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Se ha producido un error al procesar las preguntas para la obtención de las credenciales del usuario. Message:java.lang.NullPointerException en el archivo de registro del servidor].

Solución:

Lleve a cabo los pasos siguientes para que funcione el restablecimiento de la contraseña con la opción QnA como comportamiento de restablecimiento de la contraseña:

Siga estos pasos:

1. Inicie sesión en CA Identity Manager como superadministrador.
2. Vaya a Tareas, Environment Administrator (Administrador del entorno) y, a continuación, seleccione Configuración de las preguntas y respuestas.
3. Haga clic en el botón Enviar.

   Nota: Los valores predeterminados de las opciones Activar y Número de preguntas de autenticación únicamente se aplican una vez que se ha realizado este paso.

Capítulo 18: CA User Activity Reporting

Esta sección contiene los siguientes temas:

Funcionalidad de CA Enterprise Log Manager

Cuando CA Enterprise Log Manager se integra con CA Identity Manager, se obtiene la siguiente funcionalidad:

- El agente de CA Enterprise Log Manager recopila información de auditoría de CA Identity Manager y la envía a CA Enterprise Log Manager para que la convierta en Gramática de eventos comunes (CEG).
- La Consola de usuario de CA Identity Manager puede recuperar perfectamente informes o consultas de CA Enterprise Log Manager con la información de contexto de CA Identity Manager que se utiliza para filtrar la información que se devuelve.
- CA Identity Manager se suministra con un número de informes predeterminados, así como con una infraestructura que permite agregar informes o consultas de CA Enterprise Log Manager a una tarea existente o nueva.
- El agente de CA Enterprise Log Manager se instala en el equipo de [Base de datos de auditoría] de CA Identity Manager.
- El conector de CA Identity Manager se configura en el agente de CA Enterprise Log Manager.
- Se crea el registro de producto de CA Enterprise Log Manager para el entorno de Identity Manager.
- Se crea el filtro de acceso a los datos de CA Enterprise Log Manager opcional para el registro de producto.

Componentes de CA Enterprise Log Manager

Cuando CA Identity Manager se integra con CA Enterprise Log Manager, se agregan los componentes a la arquitectura de CA Identity Manager:

- La ficha del visor de CA ELM permite incrustar objetos de CA Enterprise Log Manager en cualquier tarea nueva o existente.

  Nota: Se requiere una conexión de servidor de CA Enterprise Log Manager configurada.
- Definiciones del rol que se pueden importar

Limitaciones de la integración

A continuación, se muestran limitaciones conocidas de la integración de marco de trabajo con el servidor de CA Enterprise Log Manager:

- El proceso de recuperar listas de informes y consultas en el momento de la ejecución de la configuración de tareas puede resultar lento.
- Las API de CA Enterprise Log Manager solamente reconocen las zonas horarias denominadas de Java predeterminadas.
- La operación EQUAL distingue mayúsculas de minúsculas al utilizarse en un filtro compuesto.
- La versión mínima del servidor de CA Enterprise Log Manager es la del servidor de CA ELM (45.10) con las siguientes actualizaciones de suscripción aplicadas en orden de publicación:
  1. Parche de suscripción SP-1
  2. Parche de contenido M5
  3. Actualización de la API abierta
- Solamente es compatible una conexión al mismo tiempo al servidor de CA Enterprise Log Manager.

Cómo integrar CA Enterprise Log Manager con CA Identity Manager

Antes de poder ver y gestionar informes y consultas de CA Enterprise Log Manager, un administrador tendrá que realizar lo siguiente:

1. Instalar el agente de CA Enterprise Log Manager
2. Crear un nuevo conector
3. Activar la auditoría en CA Identity Manager
4. Configurar el servidor de CA Enterprise Log Manager

Requisitos previos de instalación del agente de CA Enterprise Log Manager

Se debe realizar lo siguiente antes de instalar el agente de CA Enterprise Log Manager:

- Asegúrese de que el equipo del servidor de CA Enterprise Log Manager sea accesible desde el equipo que ejecuta CA Identity Manager u hospeda la base de datos de auditoría de CA Identity Manager.
- Asegurarse de que el equipo del agente sea accesible desde el equipo del servidor.
- Configure el origen de datos en el equipo del agente. Haga clic aquí (en la página 549) para obtener instrucciones.
- Verifique que la versión de Adobe Flash Player es la 9.0.28 o posterior. Se puede descargar el reproductor aquí:

  http://www.adobe.com/go/getflash
- Descargue los archivos binarios del agente. Haga clic aquí (en la página 550) para obtener instrucciones.
- Obtenga la clave de autenticación del agente. Haga clic aquí (en la página 550) para obtener instrucciones.
- Cómo hacer que acceder a la IP o el nombre del servidor sea sencillo
- Haga que acceder a la información de cuenta sea sencillo sin poner en riesgo la seguridad. Esta es la cuenta de identidad en la que el agente se ejecuta como servicio (Windows).
- Si el conector ya existe, exporte la información del conector predeterminado y haga que esté disponible fácilmente.
- Asegúrese de que el equipo cuente con 4 GB de RAM.

Configuración del origen de datos en el equipo del agente

Siga este procedimiento para configurar el origen de datos en el equipo del agente.

Para configurar orígenes de datos

1. Vaya a Panel de control, Herramientas administrativas, Orígenes de datos (ODBC).
2. En la ficha DSN de sistema, agregue el

   origen de datos (ODBC) imsauditevent12 que apunte a la base de datos de auditoría.
3. Haga clic en Aplicar/aceptar.

   Ya se ha configurado el origen de datos.

Descarga de binarios del agente

Siga este procedimiento para descargar binarios del agente.

Para descargar archivos binarios de agente

1. Inicie sesión en el servidor de CA Enterprise Log Manager con la siguiente dirección URL:

   https://<host>:5250/spin/calm/CALMSpindle.csp

2. Vaya a Administración, Recopilación de registros, Explorador de agente, Descargar binarios de agente, <OS> <version>.
3. Guarde el archivo.

Obtención de la clave de autenticación del agente

Utilice este procedimiento para obtener la clave de autenticación del agente.

Para obtener la clave de autenticación del agente

1. En el servidor de CA Enterprise Log Manager, vaya a Administración, Recopilación de registros, Explorador de agente, Clave de autenticación del agente.
2. Haga que acceder a la clave sea sencillo sin poner en riesgo la seguridad.

Instalación del agente de CA Enterprise Log Manager

El agente de CA Enterprise Log Manager se encarga de recopilar eventos y enviar esa información al servidor de CA Enterprise Log Manager. Instale el agente en un equipo de punto final o servidor de base de datos de CA Identity Manager para activar el registro.

Nota: El agente de CA Enterprise Log Manager es compatible con Windows y Linux.

Para instalar el agente de CA Enterprise Log Manager

1. En el servidor de base de datos, ejecute la instalación de ca-elmagent-<version>.exe e indique la siguiente información:

   El nombre del servidor o la IP de CA Enterprise Log Manager, así como el código de autenticación.

   La información de cuenta del servidor del agente que se tiene que utilizar para ejecutar el agente como servicio/daemon.

2. Especifique, si procede, el archivo de lista de conectores predeterminados.
3. Inicie sesión en el servidor de CA Enterprise Log Manager con la siguiente dirección URL:

   https://<host> :5250/spin/calm/CALMSpindle.csp

4. Vaya a Administración, Recopilación de registros, Explorador de agente, Grupo de agentes predeterminado
5. Seleccione el equipo del agente e inicie la vista Estado y comando.

   El estado debe estar ejecutándose.

Importación de definiciones del rol

Antes de que se pueda configurar la conexión de Enterprise Log Manager en la Consola de usuario, se deben importar primero las definiciones del rol de CA Enterprise.

Para importar las definiciones del rol:

1. Inicie sesión en la Consola de gestión con la siguiente dirección URL.

   `http://host:port/iam/immanage`

2. Vaya a Entorno, Role and Task Settings (Configuración de roles y tareas), haga clic en el botón Importar y seleccione Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml.
3. Haga clic en Guardar y cerrar.
4. En la ficha Sistema de la Consola de usuario, haga clic en Configurar conexión de Enterprise Log Manager, rellene la información obligatoria y haga clic en Enviar.

Creación de nuevos conectores

Siga este procedimiento para crear nuevos conectores.

Para crear nuevos conectores

1. Inicie sesión en el servidor de CA Enterprise Log Manager con la siguiente dirección URL:

   `https://<host> :5250/spin/calm/CALMSpindle.csp`

2. Vaya a Administración, Recopilación de registros, Explorador de agente, Grupo de agentes predeterminado
3. Seleccione el equipo del agente.
4. Cambie a la vista Conectores.
5. Haga clic en el botón Crear nuevo conector e introduzca la siguiente información:

   Detalles del conector

   Seleccione el tipo de integración CAIdentityManager y cambie el nombre del conector si lo desea.

   Configuración del conector

   Cadena de conexión

   - Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

   Nombre de usuario: <Auditing DB User>

   Contraseña: <Auditing DB User Password>

6. Aplique los siguientes cambios de configuración en el conector de CA Identity Manager para utilizarlo con 12.6.4.

   - SourceName: nombre del origen de datos del equipo del agente - imsauditevent12
   - AnchorSQL: select max(id) from imsauditevent12
   - AnchorField: IMS_EVENTID
   - EventSQL:

     ```
     select imsauditevent12.id as IMS_EVENtid ,imsauditevent12.audit_time as
     IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME
     ,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn
     as ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID
     ,imsauditevent12.event_description as EVENTINFO
     ,imsauditevent12.event_state as EVENTSTATE
     ,imsauditevent12.tasksession_oid as TASKOID
     ```

```
,imsaudittasksession12.task_name as TASKNAME
,imsauditeventobject12.object_type as OBJECTTYPE ,
imsauditeventobject12.object_name as
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as ATTRNAME
,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRNEWVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE from
imsaudittasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsaudittasksession12.id and
imsauditevent12.tasksession_oid = imsaudittasksession12.tasksession_oid
and
imsauditeventobject12.parent_event_id = imsauditevent12.id and
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id
ORDER BY
imsauditevent12.id ASC;
```

7. Guarde y cierre.

Para verificar que el conector esté funcionando

1. Vaya a Administración, Recopilación de registros, Explorador de agente, Grupo de agentes predeterminado
2. Seleccione el equipo del agente.
3. Cambie a la vista Conectores y haga clic en los botones de vista de comando y estado de inicio.

   El estado debe estar ejecutándose.

Activación de la auditoría en CA Identity Manager

Para activar la auditoría en CA Identity Manager

1. Apertura de la consola de gestión

   `http://host:port//iam/immanage`

2. Vaya a Environments (Entornos), <Entorno>, Advanced Setting (Configuración avanzada), Auditing (Auditoría).

3. Exporte la configuración existente y guarde el archivo.

4. Modifique el archivo guardado con la siguiente información y guarde:

   - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
   - Agregue el perfil de auditoría para las políticas de contraseñas en el último perfil de auditoría que ya está definido:

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>

5. Vuelva a importar el archivo en la Consola de gestión y realice una de las siguientes acciones para activar la agregación de información de auditoría:

   - Tareas realizadas en el objeto gestionado del usuario
   - Tareas realizadas en el objeto gestionado del grupo
   - Tareas realizadas en el objeto gestionado de las políticas de contraseñas

6. Inicie sesión en el servidor de CA Enterprise Log Manager con la siguiente dirección URL:

   https://<host> : 5250/spin/calm/CALMSpindle.csp

7. Para ejecutar informes existentes, vaya a Consultas e informes, Consultas, CA Identity Manager

   Nota: El servidor de Enterprise Log Manager ya debe estar configurado.

8. En función de qué tareas se hayan ejecutado, abra los siguientes informes predeterminados para verificar que se producen los siguientes eventos:

   - Que la tarea Todos los eventos del sistema por usuario invoca a CA Identity Manager - Todos los eventos del sistema con un filtro de ID de usuario
   - Que la tarea Gestión de cuentas por host invoca a Gestión de cuentas por host tal cual
   - Que la tarea Creaciones de cuentas por cuenta invoca a Creaciones de cuentas por cuenta tal cual
   - Que la tarea Supresiones de cuentas por cuenta invoca a Supresiones de cuentas por cuenta tal cual
   - Que la tarea Bloqueos de cuenta por cuenta invoca a Bloqueos de cuenta por cuenta tal cual

- Que la tarea Actividad de proceso de certificación por host invoca a CA Identity Manager - Actividad de proceso por host tal cual
- Que la tarea Actividad de modificación de política de contraseñas invoca a CA Identity Manager - Actividad de modificación de política tal cual

Configurar el servidor de CA Enterprise Log Manager

Antes de que se pueda configurar el servidor de CA Enterprise Log Manager para gestionarlo, asegúrese de lo siguiente:

- Se deben tener credenciales de EiamAdmin.
- Se debe tener la versión de Adobe Flash Player 9.0.28 o posterior.

Una vez que se configure el servidor de CA Enterprise Log Manager, la siguiente funcionalidad estará disponible:

- Una jerarquía federada o un servidor de CA Enterprise Log Manager utilizan varios entornos que producen eventos de auditoría.
- Se puede implementar la autorización de los datos para sistemas remotos a través del filtro de acceso a los datos de CA Enterprise Log Manager.

Para configurar el servidor de CA Enterprise Log Manager

1. Inicie sesión en la página de registro de producto del servidor de CA Enterprise Log Manager con las credenciales de administrador de CA Enterprise Log Manager mediante la siguiente dirección URL:

   `https://host:port/spin/calmapi/products.csp`

2. Registre su entorno de CA Identity Manager haciendo clic en el botón Registrar e indicando el nombre y la contraseña del certificado.

   Nota: Cada entorno debe tener pares de registro independientes (nombre y contraseña del certificado).

3. Vaya a Administración, Gestión de usuarios y accesos, New Data Access Filter (Nuevo filtro de acceso a los datos) e indique un nombre para que se cree el filtro.
4. Vaya al paso siguiente.
5. Mantenga seleccionadas las identidades en Todas las identidades y continúe con el siguiente paso.
6. Cree un filtro de acceso haciendo clic en botón Nuevo filtro de evento.

   Configure el filtro de acceso a los datos limitando el certificado creado al nombre del entorno o la máquina únicamente para los registros recopilados de CA Identity Manager. Se puede limitar también el certificado para acceder a información de punto final nativa solamente para puntos finales gestionados.

7. Guarde y cierre.
8. Abra Políticas de acceso haciendo clic en el botón para abrir las políticas de acceso.
9. Seleccione Obligation Policies (Políticas de obligación) y haga clic en la única política disponible.
10. Desactive Todas las identidades y agregue el nombre del certificado.
11. Guarde la política.

12. Inicie sesión en la Consola de usuario de Identity Manager y configure la conexión de gestión de Enterprise Log.

Configuración de conexión de Enterprise Log Manager

Utilice esta pantalla para gestionar las tareas de conexión de CA Enterprise Log Manager recién agregadas.

Los campos de esta pantalla se muestran a continuación:

Nombre de conexión

Especifica el nombre exclusivo utilizado para el objeto gestionado de conexión exclusivo de CA ELM.

Éste es un campo de sólo lectura.

Descripción

Describe la conexión de CA ELM.

Nombre de host

Especifica el nombre de host o la dirección IP de CA Enterprise Log Manager.

Éste es un campo obligatorio.

Núm. de puerto

Especifica el puerto de conexión de servidor de CA Enterprise Log Manager.

Predeterminado: 52520

Éste es un campo obligatorio.

Certificar certificado SSL firmado por autoridades

Si se selecciona, especifica una comprobación estricta del certificado SSL en la conexión a un servidor de CA Enterprise Log Manager.

Si tiene un certificado de SSL autofirmado, por ejemplo un certificado instalado con CA Enterprise Log Manager de forma predeterminada, esta casilla de verificación no se deberá seleccionar, dado que la ruta de confianza a entidad emisora raíz no existe.

Nombre del certificado

Especifica el nombre del certificado de CA Enterprise Log Manager que se utiliza para autenticación.

Éste es un campo obligatorio.

Certificate Password (Contraseña de certificado)

Especifica la contraseña de CA Enterprise Log Manager.

Éste es un campo obligatorio.

Atributo

No admitido. La versión se recupera al intentar guardar la información de conexión como una prueba.

Supresión de conexión de Enterprise Log Manager

Seleccione una conexión de la lista y haga clic en Suprimir. Se suprimirá la tarea de conexión de CA Enterprise Log Manager.

Integración de informes o consultas adicionales de CA Enterprise Log Manager con CA Identity Manager

Se pueden integrar informes o consultas adicionales de CA Enterprise Log Manager con CA Identity Manager mediante la ficha del visor de Enterprise Log Manager. Se pueden combinar estos nuevos informes o consultas con las tareas existentes (incluidos los asistentes) y las nuevas. Los datos federados de CA Enterprise Log Manager también se pueden incluir si resulta necesario. Mediante la ficha del visor de Enterprise Log Manager, se pueden aplicar filtros a la información recuperada. Estos filtros pueden utilizar lo siguiente:

- Valores constantes
- Atributos del objeto gestionado
  - Por ejemplo, para atributos físicos - ::Mi AtributoFísico::

    Para atributos lógicos - ::|MiAtributoLógico|::
- Cualquier campo tal y como se describe en la Gramática de eventos comunes (CEG) de CA Enterprise Log Manager
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid
  - ...

Configuración de la ficha del visor de Enterprise Log Manager

Configure la ficha del visor de CA Enterprise Log Manager para que se muestre alguno de los campos siguientes o todos ellos:

Nombre

Un nombre que asigna a la ficha.

Etiqueta

Un identificador de la ficha que es único dentro de esta tarea. Debe comenzar con una letra o guión bajo, y contener sólo letras, números o guiones bajos. La etiqueta se utiliza principalmente para configurar valores de datos a través de documentos XML o parámetros de HTTP.

Ocultar ficha

Impide que se vea la ficha en la tarea. Esta opción es útil para aplicaciones que necesitan ocultar la ficha, pero que aún conservan el acceso a los atributos que contiene.

Consulta de Enterprise Log Manager

Especifica que se mostrarán las consultas de CA Enterprise Log Manager.

Nota: Puede especificar la consulta de CA Enterprise Log Manager o el informe de CA Enterprise Log Manager, pero no ambos.

Informa de Enterprise Log Manager

Especifica que se mostrarán los informes de CA Enterprise Log Manager.

Nota: Puede especificar la consulta de CA Enterprise Log Manager o el informe de CA Enterprise Log Manager, pero no ambos.

ID de Enterprise Log Manager

Especifica el ID de la consulta o el informe.

Incluir datos federados

Incluye o excluye los datos federados de CA Enterprise Log Manager en los resultados. De forma predeterminada, este campo está seleccionado.

Mostrar aviso

Especifica únicamente las consultas de aviso de CA Enterprise Log Manager. De forma predeterminada, este campo está seleccionado.

Filtro

Especifica las condiciones avanzadas basadas en SQL usadas para limitar los resultados devueltos por las consultas o los informes de CA Enterprise Log Manager. Se pueden incluir valores constantes y dinámicos. A continuación, se proporciona una expresión de muestra:

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username EQUAL
::logical.attribute.Y:: ))
```

Entre las operaciones admitidas se incluyen:

- igual a (EQUAL)
- no igual a (NEQ)
- menor (LESS)
- mayor (GREATER)
- menor o igual (LEQ)
- mayor o igual (GREATEQ)
- coincide (LIKE)
- no coincide (NOTLIKE)
- en conjunto (INSET)
- no en conjunto (NOTINSET)

Entre las conjunciones admitidas se encuentran:

- AND
- OR

Los paréntesis son obligatorios. Si el valor a la izquierda de la expresión de condición no tiene el marcador "::" en ambos extremos, el valor se considera una constante y se envía a CA Enterprise Log Manager tal cual.

Tabla de parámetros/valores

Especifica los campos y los valores que se van a utilizar para el ámbito.

Sólo se seleccionarán consultas o informes con etiquetas coincidentes y lógica de etiquetas de ámbito.

Parámetro

Especifica los valores de los parámetros Inicio, Detener y Limit (Limitar). Se admiten los parámetros siguientes:

- Granularidad del tiempo (sólo para tendencias)
- Hora de inicio
- Hora de finalización
- El primer evento agrupado tiene fecha posterior a (sólo para consultas agrupadas)
- El último evento agrupado tiene fecha posterior (sólo para consultas agrupadas)
- El último evento agrupado tiene fecha anterior (sólo para consultas agrupadas)

- El número mínimo de eventos para la agrupación (sólo para consultas agrupadas)
- El número máximo de eventos en la agrupación (sólo para consultas agrupadas)

Capítulo 19: Roles de acceso

Los roles de acceso proporcionan una forma adicional de proporcionar autorizaciones en CA Identity Manager u otra aplicación. Por ejemplo, se pueden utilizar los roles de acceso para realizar las siguientes tareas:

- Proporcionar acceso indirecto a un atributo de usuario
- Crear expresiones complejas
- Establecer un atributo en un perfil de usuario, que otra aplicación utiliza para determinar las autorizaciones

Los roles de acceso son similares para identificar políticas de identidad ya que aplican un conjunto de cambios de negocio a un usuario o grupo de usuarios. Sin embargo, cuando se utiliza un rol de acceso para aplicar cambios de negocio, se puede consultar a qué usuarios se aplican los cambios visualizando los miembros del rol de acceso.

En la mayoría de los casos, los roles de acceso no están asociados a tareas.

Nota: Cuando CA Identity Manager se integra con CA SiteMinder, los roles de acceso pueden proporcionar también acceso a aplicaciones que protege CA SiteMinder. En este caso, los roles de acceso incluyen tareas de acceso. Para obtener más información, consulte el capítulo sobre la integración de SiteMinder en la *Guía de configuración*.

Esta sección contiene los siguientes temas:

Cómo gestionan los roles de acceso las autorizaciones

Se pueden utilizar roles de acceso para gestionar autorizaciones especificando acciones de cambio, que ocurren cuando se agrega o se elimina un usuario como miembro o como administrador de un rol.

Para utilizar roles de acceso, complete los pasos siguientes:

1. Un administrador crea un rol de acceso.
2. En la ficha Miembros, el administrador especifica si se agregan o eliminan acciones que determinan las acciones que CA Identity Manager lleva a cabo cuando el rol de acceso se asigna a un usuario.
3. El administrador especifica políticas de administrador y propietario, según sea necesario, y envía la tarea para crear el rol de acceso.
4. Los administradores del rol de acceso asignan el rol de acceso a los usuarios.
5. CA Identity Manager completa las acciones agregadas especificadas en el rol.

Ejemplo: Modificación del atributo de perfil indirecta

Se pueden utilizar roles de acceso para cambiar indirectamente un atributo en un perfil de usuario. Por ejemplo, es posible que una compañía no desee permitir a ningún usuario cambiar directamente el título de otro usuario. Esa compañía puede crear un rol de acceso que cambia un título cuando un administrador asigna el rol a un usuario.

Para cambiar indirectamente un atributo, se deben establecer las acciones de cambio para el rol de acceso. Cuando un administrador asigna el rol, la acción de cambio puede realizar uno o más cambios a un atributo en el perfil del usuario.

Para utilizar un rol de acceso para modificar indirectamente un atributo, realice los siguientes pasos:

1. Cree un rol de acceso.
2. En la ficha Miembros, seleccione la casilla de verificación Los administradores pueden agregar y eliminar miembros de este rol y haga clic en el icono de flecha.

   CA Identity Manager muestra los campos adicionales Agregar acción y Eliminar acción.
3. En los campos Agregar acción o Eliminar acción, seleccione una acción del cuadro de lista.

   CA Identity Manager muestra los campos adicionales en función de la opción seleccionada.
4. Configure las funciones Agregar o Eliminar acciones según sea necesario.

5. Seleccione la ficha Administrador para especificar a los administradores quién pueden agregar miembros al rol de acceso que se está creando.
6. Seleccione la ficha Propietarios para especificar a los administradores quién pueden modificar la definición del rol de acceso.
7. Haga clic en Enviar para completar la creación del rol de acceso.
8. Asigne el rol de acceso a los usuarios, según sea necesario.

Creación de una función de acceso

La creación de un rol de de acceso implica los siguientes pasos:

- Inicio de la creación de la función de acceso. (en la página 565)
- Definición del perfil de la función de acceso. (en la página 566)
- Definición de las políticas de miembros de la función de acceso. (en la página 566)
- Definición de las políticas de administración de la función de acceso. (en la página 567)
- Definición de las reglas de propietarios de la función de acceso. (en la página 567)

Inicio de la creación de la función de acceso

1. Inicie sesión en una cuenta de Identity Manager con una función que incluya una tarea para crear funciones de acceso.
2. Haga clic en Funciones de acceso, Crear función de acceso.

   Seleccione la opción para crear una nueva función o una copia de una función. Si selecciona Copiar, busque la función.
3. Continúe con la siguiente sección, Definición del perfil de la función de acceso.

Definición del perfil de la función de acceso

Para definir el perfil de la función de acceso

1. Introduzca el nombre, la descripción y complete los atributos personalizados definidos para la función.

   Nota: Puede especificar atributos personalizados en la ficha Perfil que especifica información adicional acerca de los roles de acceso. Esta información adicional se puede usar para simplificar la búsqueda de roles en entornos que incluyan un gran número de roles.

2. Seleccione Activado si está listo para dejar la función disponible para ser utilizada en cuanto la haya creado.

3. Continúe con la siguiente sección, Definición de las políticas de miembros de la función de acceso (en la página 566).

Definición de las políticas de miembros de la función de acceso

En la ficha Miembros:

1. Seleccione Agregar para definir las políticas de miembros.

2. (Opcional) En la página Política de miembros, puede definir una regla de miembros para quienes puedan utilizar esta función.

   De esta manera la función se asigna automáticamente a los usuarios que cumplan los criterios de la política de miembros.

3. Verifique que la política de miembros aparece en la ficha Miembros.

   Para editar una política, haga clic en el símbolo de flecha a la izquierda. Para eliminarla, haga clic en el icono con el signo menos.

4. En la ficha Miembros, active la casilla de verificación Los administradores pueden agregar y eliminar miembros de esta función.

   Una vez que active esta función, podrá definir Agregar acción y Eliminar acción. Estas acciones definen qué ocurre cuando se agrega o se elimina un usuario como miembro de la función.

5. Continúe con la siguiente sección, Definición de las políticas de administración de la función de acceso (en la página 567).

Definición de las políticas de administración de la función de acceso

En la ficha Administradores:

1. Si desea que la opción Gestionar administradores esté disponible, active la casilla de verificación Los administradores pueden agregar y eliminar miembros de esta función.

   Una vez que active esta función, podrá definir las acciones para cuando se agrega o se elimina un usuario como administrador de la función.

2. En la ficha Administradores, agregue políticas de administración que incluyan reglas de administración y de ámbito, así como privilegios de administrador. Cada política necesita como mínimo un privilegio (Gestionar miembros o Gestionar administradores).

   Puede agregar varias políticas de administración con diferentes reglas y diferentes privilegios para los administradores que cumplan la regla.

3. Para editar una política, haga clic en el símbolo de flecha a la izquierda. Para eliminarla, haga clic en el icono con el signo menos.

4. Continúe con la siguiente sección, Definición de las reglas de propietarios de la función de acceso (en la página 567).

Definición de las reglas de propietarios de la función de acceso

En la ficha Propietarios:

1. Defina las reglas de propietarios, que determinan qué usuarios pueden modificar la función.

2. Haga clic en Enviar.

   Aparecerá un mensaje indicando que la tarea se ha enviado. Puede producirse un retraso momentáneo antes de que un usuario pueda utilizar la función.

Capítulo 20: Tareas del sistema

Esta sección contiene los siguientes temas:

Tareas del sistema predeterminadas

CA Identity Manager incluye las tareas siguientes, que permiten a los administradores gestionar un entorno de CA Identity Manager:

- Tareas de Ver tareas enviadas

  Permite a los administradores ver el estado de las tareas del entorno. También elimina tareas obsoletas de las pantallas de Ver tareas enviadas.

- Tareas del Cargador masivo

  Carga archivos de alimentador que se utilizan para manipular grandes cantidades de objetos gestionados simultáneamente.

- Tarea masiva

  Ejecuta una tarea en un objeto como, por ejemplo, el usuario, según los atributos del objeto, como el departamento, la ciudad, la fecha de terminación, etc. Puede ejecutar esta tarea periódicamente, como por ejemplo todos los sábados.

  Puede utilizar también esta tarea para hacer cambios del usuario masivo.

- Tareas de Seleccionar datos de cuadro

  Permite a los administradores cargar archivos que se utilizan para completar opciones en campos, como cuadros de selección, en las tareas de administración.

- Tareas del Identificador de atributos lógicos

  Permite a los administradores gestionar los atributos lógicos, que se usan para mostrar los atributos del almacén de usuarios (denominados atributos físicos) en un formato sencillo en las pantallas de tareas.

- Tareas de Gestión de la conexión JDBC

  Configura los detalles de conexión del servidor de base de datos en CA Identity Manager.

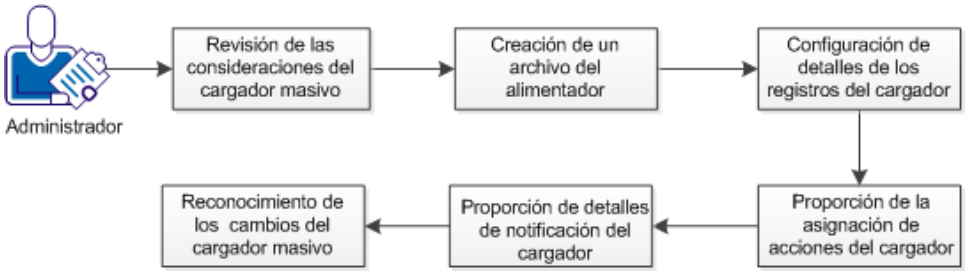
- Tareas de correo electrónico

  Gestiona las políticas de notificación de correo electrónico.

Cómo agregar usuarios con un archivo del alimentador

Puede utilizar la ficha Cargador masivo para cargar archivos de alimentador que se utilizan para manipular grandes cantidades de objetos gestionados simultáneamente. Por ejemplo, puede crear 1.000 usuarios manualmente en el sistema o puede usar el Cargador masivo. La tarea Cargador masivo también se puede asignar a un proceso de flujo de trabajo.

El cliente de carga masiva es una utilidad de línea de comandos que existe para el procesamiento por lotes. Se recomienda el empleo del cliente de carga masiva si el entorno se encuentra en un clúster (para el equilibrio de carga). El cliente de carga masiva se encuentra en el medio de componentes de aprovisionamiento.



Siga estos pasos:

1. Revisión de las consideraciones del Cargador masivo (en la página 571).
2. Creación de un archivo del alimentador de CSV o XLS (en la página 574) y carga de éste.
3. Configuración de la ficha Detalles de los registros del cargador (en la página 575).

   Esta ficha permite especificar los campos de acción e identificador en el archivo del alimentador.
4. Proporción de la asignación de acciones del cargador (en la página 576).

   Esta ficha permite seleccionar el objeto primario y especificar la tarea que se ejecutará para la acción en un objeto.
5. Proporción de los detalles de notificación del cargador (en la página 577).

   Esta ficha permite seleccionar usuarios para certificar los cambios de la tarea del cargador masivo.
6. Reconocimiento y modificación del progreso de los cambios de la tarea del cargador masivo (en la página 577).

Consideraciones del cargador masivo

Puede utilizar la ficha Cargador masivo para cargar archivos de alimentador que se utilizan para manipular grandes cantidades de objetos gestionados simultáneamente. Tenga en cuenta las consideraciones siguientes al utilizar el Cargador masivo:

- Considere la programación de grandes cargas masivas durante horas de menor actividad, como por ejemplo durante la noche. Las cargas masivas grandes pueden afectar al rendimiento. En algunos casos, una carga masiva que incluye muchas subtareas puede hacer que las tareas enviadas por el usuario no se completen hasta que la carga masiva finalice.
- Si el servidor deja de funcionar durante la ejecución de una tarea prolongada, como la carga de una gran cantidad de objetos, reinicie la tarea en la ficha Ver tareas enviadas. Cuando la tarea se reinicia, comienza desde el último registro que se haya ejecutado correctamente.
- Si utiliza LDAP como almacén de usuario con Solaris, el cargador masivo se puede bloquear durante la importación. Para solucionar este problema, consulte el tema Cómo especificar la configuración de la conexión LDAP de la *Guía de configuración* y aplique la configuración que se indica.

- Si utiliza el cargador masivo para importar una gran cantidad de usuarios, puede que vea excepciones que no se encuentran en la memoria. Para solucionar esta incidencia, ajuste los parámetros de memoria de tamaño de la memoria dinámica siguientes:
  - -Xmx
  - -XX:maxPermSize

    Nota: Para obtener más información sobre el ajuste de los parámetros de la memoria dinámica, consulte la documentación del servidor de aplicaciones.
- La utilización del cargador masivo para manipular muchos objetos gestionados, así como para crear muchos usuarios, puede afectar al rendimiento. Para mejorar el rendimiento, tenga en cuenta las recomendaciones siguientes:
  - Divida un archivo CSV grande en pequeños archivos al utilizar la Consola de usuario para realizar cargas masivas. Por ejemplo, realizar diez cargas masivas de 10.000 usuarios es más rápido que hacer una carga masiva de 100.000 usuarios.

    Nota: Un archivo CSV con más de 50 000 entradas puede causar incidencias en el sistema.
  - Limite el número de tareas que tiene el usuario que está realizando la carga masiva. Por ejemplo, el rendimiento mejora cuando el administrador que inicia la carga masiva tiene solamente algunas tareas. Cuando el administrador tiene muchas tareas, CA Identity Manager tiene que hacer más comprobaciones de permisos extensas, lo cual puede afectar al rendimiento.
  - Limite el número de políticas de exprés que están asociadas con cambios masivos que implican el aprovisionamiento. También se puede considerar la creación de políticas exprés simples que no afecten al rendimiento así como políticas complejas durante una operación de carga masiva.
  - Verifique que tiene suficientes recursos del sistema.

Limitación de la validación de datos para mejorar el rendimiento de carga masiva

Una tarea de administración incluye normalmente varias fichas. De forma predeterminada, las operaciones masivas validan datos en cada ficha de una tarea.

La validación puede afectar al rendimiento de operaciones masivas. Para mejorar el rendimiento, se puede desactivar la validación de los datos para las fichas de la tarea, si no se requiere la validación.

Siga estos pasos:

1. Inicie sesión en la Consola de usuario como un usuario con privilegios para modificar tareas administrativas.
2. Seleccione Tareas, Roles y tareas, Tareas de administración, Modificar la tarea de administración.

3. Busque y seleccione la tarea que se aplica a la operación masiva.
4. Seleccione Fichas y, a continuación, la ficha que desee modificar.
5. Seleccione No validar en operaciones masivas y, a continuación, haga clic en Aceptar.
6. Repita los pasos 4 y 5 para cada ficha que no requiera la validación de datos.
7. Haga clic en Enviar.

   Se desactiva la validación de datos para las fichas modificadas.

Limitación de la lógica del negocio personalizada

Incluyendo la lógica del negocio personalizada, como identificadores de las tareas lógicas del negocio y escuchas de eventos, las tareas que se utilizan en operaciones masivas pueden afectar al rendimiento.

Para mejorar el rendimiento, desactive la lógica del negocio personalizada en operaciones de carga masiva.

Siga estos pasos:

1. Abra la Consola de gestión.
2. Seleccione el entorno aplicable que incluye la escucha de eventos o el identificador de tareas lógicas del negocio.
3. Seleccione Configuración avanzada, Identificadores de tareas lógicas del negocio (si es aplicable).
4. Establezca el valor de la propiedad UseInBulkOperation como falso y, a continuación, haga clic en Guardar.
5. Repita el paso 4 para las escuchas de eventos.
6. Una vez que se han finalizado las modificaciones para los identificadores de las tareas lógicas del negocio y las escuchas de eventos, reinicie el entorno.

Creación de un archivo del alimentador

Los archivos del Cargador masivo se utilizan para automatizar acciones repetitivas que se realizan en un gran número de objetos gestionados. Cuando se carga un archivo del alimentador, el sistema analiza y lee el archivo del alimentador.

Este archivo del alimentador debe tener una extensión CSV o XLS y las siguientes propiedades:

- El archivo debe contener una línea de encabezamiento que especifique los atributos físicos, los atributos lógicos o los nombres de atributos conocidos de un objeto gestionado.
- La línea de encabezamiento debe incluir una columna que indique la acción que se debe realizar en los registros.
- Cada fila del archivo del alimentador se denomina "registro". Los registros contienen los valores de cada uno de los atributos especificados en la línea de encabezamiento. Las siguientes opciones son valores aceptables para un atributo:
  - Valor: el atributo se establece en el valor que especifique.
  - Valor;Valor;Valor;..: el atributo se establece en el atributo con varios valores que haya especificado.
  - ' ' (vacío): no se cambia el atributo.
  - NULO: el atributo se elimina. La secuencia de eliminación se establece con el valor NULO de forma predeterminada, pero se puede editar en la pantalla Búsqueda en la carga de archivos del cargador masivo.

Nota: Para usar una almohadilla (#) en el archivo del alimentador, póngala entre comillas dobles, es decir, user#1 debe especificarse como "user#1".

Importante: El archivo del alimentador debe guardarse con codificación UTF-8.

Archivo del alimentador de muestra para crear usuarios

Este archivo del alimentador de muestra crea usuarios con algunos atributos necesarios.

```
acción,%ID_USUARIO%,%NOMBRE%,%APELLIDO%,%NOMBRE_COMPLETO%,%CONTRASEÑA%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

En el código anterior, el archivo del alimentador tiene las siguientes propiedades:

Encabezamiento

La primera línea del código es la línea de encabezamiento. Esta línea tiene los atributos físicos o atributos conocidos del objeto gestionado 'Usuario'.

Acción

La columna de acción identifica la tarea que se debe realizar para cada registro. Por ejemplo, el archivo anterior especifica que se debe realizar la acción 'create' (crear) en el nombre 'John'.

Archivo del alimentador de muestra para activar usuarios

Este archivo del alimentador de muestra cambia el valor del atributo lógico |activado|. Se debe epecificar el atributo lógico en el encabezado y el valor (en este caso, verdadero o falso) en cada entrada de usuario del archivo.

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

Ficha Detalles de los registros del cargador

Esta ficha muestra una breve vista previa de los registros disponibles en el archivo del alimentador. La tabla de la vista previa muestra un máximo de cinco registros. Esta tabla ayuda a los usuarios a identificar si están cargando el archivo correcto. Además, esta ficha permite identificar la acción que desea realizar en los objetos gestionados especificados en el archivo del alimentador. Deberá especificar los siguientes campos:

¿Qué campo representa a la acción que se va a realizar en el objeto?

Identifica los campos del archivo del alimentador que mencionan la acción que se va a realizar en los objetos gestionados. Por ejemplo, puede usar un archivo del alimentador con un campo 'acción' que lleve los valores Crear, Modificar y Suprimir. Debe asignar cada una de estas acciones a una tarea de administración en Asignación de acciones del cargador (en la página 576).

¿Qué campo se utilizará para identificar de forma única el objeto?

Identifica el campo del archivo del alimentador que puede identificar de forma única al objeto primario.

Nota: Si el archivo del alimentador tiene un encabezamiento no válido, no se mostrarán los registros de este archivo en la ficha Detalles de los registros del cargador. Si los encabezamientos no son válidos, seleccione otro archivo de alimentador. Si el archivo de alimentador contiene algunos registros no válidos, el estado detallado de la carga aparecerá en la ficha Ver tareas enviadas.

Ficha Asignación de acciones del cargador

La ficha Asignación de acciones del cargador permite seleccionar el objeto primario en el que se ejecutarán las acciones especificadas en el archivo del alimentador. También se deben asignar las acciones desde el archivo del alimentador a las tareas de administración para el objeto primario seleccionado.

¿Qué es el objeto primario?

Identifica el objeto primario que manipulará CA Identity Manager mediante el archivo del alimentador. Puede seleccionar cualquiera de estos objetos primarios:

- Usuario
- Grupos
- Organización

Seleccione la tarea que desea ejecutar para la acción

Identifica las tareas de administración que se deberán ejecutar para cada acción especificada en el archivo del alimentador como, por ejemplo, las tareas Suprimir o Modificar.

Nota: Deberá asignar todas las acciones del archivo del alimentador a una tarea de administración. Además, las tareas de administración que se muestran en este campo dependerán del objeto primario seleccionado. Por ejemplo, si se ha seleccionado 'Usuario' como el objeto primario, sólo se mostrarán las tareas de administración relacionadas con 'Usuario'.

Seleccione una tarea de un objeto no existente para la 'acción'.

Identifica las tareas de administración alternativas que se llevarán a cabo para una acción especificada en el archivo de alimentación en caso de que el objeto gestionado no exista aún en CA Identity Manager como, por ejemplo, la tarea Crear.

Ficha Detalles de notificación del cargador

Importante: De forma predeterminada, esta ficha no se incluye en el asistente de cargador masivo. Se debe agregarlo manualmente mediante la modificación de la tarea del cargador masivo y la adición de la ficha de Detalles de notificación del cargador. Además, esta ficha requiere que active el flujo de trabajo en el entorno.

La ficha Detalles de notificación del cargador le permite seleccionar gestores de certificación para la tarea del cargador masivo. Cuando se completa una tarea del cargador masivo, CA Identity Manager crea una notificación del cargador masivo para todos los gestores de certificación configurados para dicha tarea. Esta notificación aparece en la ficha Principal en Notificaciones del cargador masivo. Al hacer clic en la notificación, se muestran detalles para las tareas iniciadas por el funcionamiento del cargador masivo. A continuación, los gestores de certificación pueden revisar y reconocer los cambios detallados en las notificaciones.

Nota: Para proporcionar una lista de gestores de certificación, use cualquiera de los asignadores de participante disponibles en la lista desplegable. Para obtener más información sobre los asignadores de participante, consulte la sección de Flujo de trabajo de esta guía.

Reconozca los cambios de la tarea del cargador masivo

Las notificaciones del cargador masivo contienen detalles de todos los cambios iniciados por la tarea del cargador masivo. Los gestores de certificación pueden revisar y reconocer los cambios iniciados por una tarea del cargador masivo.

Para revisar y reconocer los cambios de la tarea del cargador masivo

1. Inicie sesión en la Consola de usuario como un usuario que aparece como gestor de certificación para una tarea del cargador masivo.
2. Vaya a Principal, Ver mis notificaciones del cargador masivo.

3. Seleccione la notificación del cargador masivo que desea revisar.

   Aparecerá la pantalla Gestionar notificaciones del cargador masivo aparece y mostrará una tabla con los cambios de la tarea del cargador masivo que se iniciaron.

   Desde esta pantalla puede hacer lo siguiente:

   - Para revisar detalles específicos de la tarea para Crear o Modificar objeto, haga clic en el hipervínculo situado bajo la columna de descripción.
   - Si existen infracciones de cumplimiento, o si se desea eliminar un rol agregado a un usuario, se puede editar el usuario directamente en la pantalla de notificación haciendo clic en el icono Editar situado junto al ID de usuario.
   - Para revisar los roles agregados a un usuario, haga clic en el hipervínculo situado bajo la columna de Asignaciones de rol solicitadas asociada con el ID de usuario.

4. Una vez que ha revisado todos los cambios para un objeto específico, seleccione la casilla de verificación Reconocer para ese objeto.
5. Una vez que se han realizado los cambios de reconocimiento, haga clic en Reconocer para eliminar de la lista todas las notificaciones de cambio seleccionadas.

   Nota: Se puede seleccionar Reconocer todo para reconocer todos los cambios de una notificación del cargador masivo. Esto suprime la notificación del cargador masivo de la ficha Principal. Además, se puede seleccionar la casilla de verificación situada en la parte superior de la columna Reconocer para seleccionar todas las notificaciones de cambio presentes en la pantalla en ese momento y reconocer los cambios pantalla por pantalla.

   Cuando se reconocen todos los cambios del usuario asociados con una tarea del cargador masivo, la notificación del cargador masivo desaparece de la ficha Principal.

Configuración de notificaciones de correo electrónico para tareas del cargador masivo

En algunos entornos, las notificaciones de correo electrónico de operaciones masivas se configuran de forma predeterminada. Para comprobar si se han configurado notificaciones de correo electrónico de operaciones masivas en el sistema, vaya a Sistema, Correo electrónico, Ver correo electrónico, y busque el término "Masivo".

Si no hay ninguna notificación de correo electrónico configurada en el entorno, configure el correo electrónico que se enviará cuando finalice una operación masiva.

Siga estos pasos:

1. Vaya a Sistema, Correo electrónico, Crear correo electrónico en la Consola de usuario.
2. Complete los siguientes campos en la ficha Perfil:
3. En la ficha Cuándo enviar, complete los pasos siguientes:
   a. Seleccione La tarea finaliza en el primer campo.
   b. Seleccione Cargador masivo en el segundo campo.
4. Complete las fichas Destinatarios y Contenido y después haga clic en Enviar.

   Se han configurado notificaciones de correo electrónico para las tareas del cargador masivo.

Programación de una tarea Cargador masivo

La tarea del cargador masivo se puede programar en el sistema. Para programar la tarea Cargador masivo, agregue una ficha Programador (en la página 68) a la tarea.

Modificación del archivo del Analizador para el Cargador masivo

Para modificar el analizador utilizado para analizar los archivos del alimentador, configure la tarea de administración correspondiente.

Para modificar la tarea de administración Cargador masivo

1. Vaya a Roles y tareas, Tareas de administración, Gestionar tarea de administración.
2. Busque la tarea Cargador masivo.
3. Seleccione la tarea Cargador masivo y haga clic en Seleccionar.
4. Seleccione la ficha Buscar de la tarea Cargador masivo.

5. Haga clic en Examinar para ubicar las pantallas de búsqueda.

   Aparecerá la lista de pantallas de búsqueda disponibles.

6. Seleccione una pantalla de búsqueda y haga clic en Editar.

   Aparecerán los detalles de la pantalla Buscar.

7. (Opcional) Modifique el nombre totalmente cualificado del analizador.

   El nombre totalmente cualificado del analizador debe coincidir con el del archivo del analizador.

   Nota: Para obtener más información sobre cómo crear un analizador de CSV personalizado, consulte el Javadoc para la clase FeederParser. Si utiliza JBoss como servidor de aplicaciones y crea un analizador personalizado, el archivo del analizador personalizado debe estar en el directorio iam_im.ear/user_console_war/WEB-INF/classes.

8. Haga clic en OK.

Compatibilidad de servicio Web para el cargador masivo

El cargador masivo tiene una API del servicio web que se puede ejecutar mediante la interfaz TEWS (Task Execution Web Service) de CA Identity Manager. TEWS permite a las aplicaciones cliente enviar tareas remotas a CA Identity Manager para su ejecución. Esta interfaz implementa los estándares abiertos WSDL y SOAP para proporcionar acceso remoto a CA Identity Manager.

CA Identity Manager incluye ejemplos de cliente Java que muestran la ejecución del cargador masivo como un servicio web. Los ejemplos de Java se encuentran en el siguiente archivo de origen:

admin_tools\samples\WebService\Axis\optional\ObjectsFeeder.java

Los ejemplos de datos y la documentación para ejecutar el cargador masivo como un servicio web se encuentran en el directorio siguiente:

admin_tools\samples\Feeder\

Nota: Para obtener más información, consulte la *Guía de programación para Java*.

Gestión de la conexión JDBC

La información de los informes de CA Identity Manager puede proceder de varios orígenes, y cada informe se debe asociar con un origen de datos específico, dependiendo de la información que desee ver en el informe.

Para establecer diferentes orígenes de datos para crear informes (como, por ejemplo, una base de datos de auditoría o una base de datos de persistencia de tareas), cree un objeto gestionado de conexión en CA Identity Manager. Después de crear la conexión, puede asociar un informe con un objeto gestionado de conexión específico mediante la modificación de la tarea de informe y la configuración del objeto de conexión para el informe que se encuentra en la ficha de búsqueda de la tarea de informe.

Creación de una conexión JDBC

Utilice los pasos siguientes para proporcionar detalles de conexión en CA Identity Manager.

Para crear una conexión JDBC

1. Haga clic en Sistema, Gestión de la conexión JDBC, Crear conexión JDBC.
2. Cree un nuevo objeto de conexión o seleccione un objeto de conexión basado en un origen de datos JNDI específico.
3. Rellene todos los campos necesarios y haga clic en Enviar.

   Se creará una nueva conexión JDBC.

Identificadores de atributos lógicos

Los atributos lógicos de CA Identity Manager permiten mostrar los atributos del almacén de usuarios (denominados atributos físicos) en un formato sencillo en las pantallas de la tarea. Los administradores de CA Identity Manager utilizan las pantallas de tarea para realizar funciones en CA Identity Manager. Los atributos lógicos no están presentes en un almacén de usuarios. Normalmente, representan uno o más atributos físicos para simplificar la presentación. Por ejemplo, el atributo lógico fecha puede representar los atributos físicos mes, día y año.

Los atributos lógicos se procesan mediante identificadores de atributos lógicos, que son objetos Java que se escriben utilizando la API de atributos lógicos. (Consulte la *Guía de programación para Java*). Por ejemplo, cuando se muestra una pantalla de tarea, un identificador de atributos lógicos puede convertir los datos de los atributos físicos del almacén de usuarios en datos de atributos lógicos, que se muestran en la pantalla de tarea. Se pueden utilizar los atributos lógicos predefinidos y los identificadores de atributos lógicos incluidos con CA Identity Manager o crear otros nuevos mediante la API de atributos lógicos.

Nota: Para obtener más información sobre los atributos lógicos, consulte la *Guía de programación para Java*.

En la Consola de usuario, la categoría Entorno contiene tareas para gestionar los identificadores de atributos lógicos. La lista incluye los identificadores predefinidos que se incluyen en CA Identity Manager y los identificadores personalizados definidos en su sitio.

Desde la categoría de tareas Entorno, puede llevar a cabo lo siguiente:

- Crear un nuevo identificador de atributos lógicos con CA Identity Manager.
- Copiar un identificador.
- Suprimir un identificador.
- Modificar la configuración de un identificador existente.

Nota: Para cambiar el orden de ejecución de los identificadores de atributos lógicos, utilice la Consola de gestión.

Creación de un identificador de atributos lógicos

Para crear un identificador de atributos lógicos

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Crear identificador de atributos lógicos, seleccione Crear identificador de atributos lógicos estándar y haga clic en Aceptar.
3. En la pantalla Crear identificador de atributos lógicos, configure las opciones del identificador de atributos lógicos.

   Para obtener una descripción de cada campo, haga clic en el enlace de ayuda de la pantalla.
4. Haga clic en Enviar.

   El identificador se agregará a la lista de identificadores en la pantalla Identificadores de atributos lógicos.

Nota: No es necesario que reinicie el servidor de aplicaciones después de configurar los identificadores de atributos lógicos mediante la Consola de usuario.

Copia de un identificador de atributos lógicos

Para copiar un identificador de atributos lógicos

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Crear identificador de atributos lógicos, seleccione Crear una copia de una definición de identificador de atributos lógicos y haga clic en Buscar.
3. Seleccione un identificador de atributos lógicos (por ejemplo, ConfirmPasswordHandler) y haga clic en Aceptar.
4. En la pantalla Crear identificador de atributos lógicos, configure las opciones del identificador de atributos lógicos.

   Para obtener una descripción de cada campo, haga clic en el enlace de ayuda de la pantalla.
5. Haga clic en Enviar.

   El identificador se agregará a la lista de identificadores en la pantalla Identificadores de atributos lógicos.

Nota: No es necesario que reinicie el servidor de aplicaciones después de configurar los identificadores de atributos lógicos mediante la Consola de usuario.

Creación de un identificador de atributos lógicos ForgottenPasswordHandler

El identificador de atributos lógicos ForgottenPasswordHandler utiliza atributos lógicos independientes para lo siguiente:

- configuración
- preguntas y respuestas en tiempo de ejecución

Para crear un identificador de atributos lógicos ForgottenPasswordHandler

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Crear identificador de atributos lógicos, seleccione Crear identificador de atributos lógicos estándar y haga clic en Buscar.
3. Seleccione el identificador ForgottenPasswordHandler y haga clic en Aceptar.

4. En la pantalla Crear identificador de atributos lógicos: ForgottenPasswordHandler, configure las opciones del identificador de atributos lógicos.

   Para obtener una descripción de cada campo, haga clic en el enlace de ayuda de la pantalla.

5. Haga clic en Enviar.

   El identificador se agregará a la lista de identificadores en la pantalla Identificadores de atributos lógicos.

Nota: No es necesario que reinicie el servidor de aplicaciones después de configurar los identificadores de atributos lógicos mediante la Consola de usuario.

Supresión de un identificador de atributos lógicos

Para suprimir un identificador de atributos lógicos

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Suprimir identificador de atributos lógicos, seleccione la casilla de verificación a la izquierda de cada atributo lógico que se vaya a suprimir.
3. Haga clic en Seleccionar.

   CA Identity Manager muestra un mensaje de confirmación.
4. Haga clic en Sí para confirmar la eliminación.

Modificación de un identificador de atributos lógicos

Para modificar un identificador de atributos lógicos

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Modificar identificador de atributos lógicos, seleccione el identificador que desee modificar y haga clic en Seleccionar.
3. Seleccione un identificador de atributos lógicos (por ejemplo, ConfirmPasswordHandler) y haga clic en Aceptar.
4. En la pantalla Modificar identificador de atributos lógicos, configure los valores del identificador de atributos lógicos.

   Para obtener una descripción de cada campo, haga clic en el enlace de ayuda de la pantalla.
5. Haga clic en Enviar.

Nota: No es necesario que reinicie el servidor de aplicaciones después de configurar los identificadores de atributos lógicos mediante la Consola de usuario.

Visualización de un identificador de atributos lógicos

Para ver un identificador de atributos lógicos

1. Vaya a Sistema, Atributos lógicos, Crear identificador de atributos lógicos.
2. En la pantalla Ver identificador de atributos lógicos, seleccione el identificador que desee ver y haga clic en Seleccionar.
3. Visualice las propiedades del identificador de atributos lógicos y haga clic en Cerrar.

Seleccionar datos de cuadro

Puede completar las opciones que están disponibles en los siguientes campos:

- Casilla de verificación de multiselección
- Desplegable
- Cuadro combinado desplegable
- Multiselección
- Seleccionador de opciones
- Seleccionador de opciones combinado
- Botón de selección de una única selección
- Selección única

Estas opciones se almacenan en los archivos XML Seleccionar datos de cuadro. Por ejemplo, puede usar los archivos XML Seleccionar datos de cuadro para completar las opciones del cuadro desplegable Ciudad o Estado en una ficha Perfil de la tarea Crear usuario.

También puede utilizar este archivo para configurar una dependencia entre dos campos de una tarea de administración. Por ejemplo, las opciones disponibles en el campo Ciudad pueden depender de la opción que el usuario seleccione en el campo Estado.

Nota: Para obtener más información acerca de Seleccionar datos de cuadro, consulte la *User Console Design Guide.*

Pantalla de la tarea Configuración de atributos de correlación

Este tema se aplica solamente a CA CloudMinder.

Utilice la pantalla de la tarea Configuración de atributos de correlación para configurar reglas de correlación para el entorno.

CA Identity Manager lee los parámetros de configuración en la memoria y sincroniza periódicamente la versión de la memoria con la versión de la base de datos del DSA común. Ya que los atributos de correlación son específicos del cliente, el servidor de aprovisionamiento lee los atributos de correlación del DSA del cliente correspondiente durante la operación Explorar y correlacionar. Las reglas de correlación actualizadas se aplican inmediatamente sin necesidad de esperar el tiempo de actualización de los parámetros.

Pantalla de la tarea Configurar una política global basada en flujo de trabajo para eventos

Las tareas Configurar una política global basada en flujo de trabajo para eventos permite que un administrador configure flujos de trabajo que se basan en política o no para todos los eventos en el entorno actual. Al hacer clic en la tarea se muestra la asignación de eventos predeterminada para las definiciones de proceso de flujo de trabajo. Se puede modificar o suprimir cada asignación de eventos, y se pueden agregar nuevas asignaciones de eventos para los que no se hayan configurado.

Los campos de esta pantalla son los siguientes:

Procesos de flujo de trabajo asociados con los eventos de este entorno.

Especifica los procesos de flujo de trabajo asociados con las políticas de aprobación.

Agregar nuevas asignaciones

Especifica una política de aprobación que asignar a un proceso de flujo de trabajo.

Botón Agregar

Agrega la nueva asignación.

Agregar o modificar una asignación abre la pantalla de asignación de flujo de trabajo donde puede seleccionar las asignaciones de proceso y las políticas de aprobación. El comportamiento es el mismo que la configuración de flujo de trabajo del nivel de evento. Si hace clic en el botón Agregar en la página de asignaciones de flujo de trabajo, lleva a otra página en la que puede configurar una política de aprobación.

Más información

Cómo configurar el flujo de trabajo basado en políticas para los eventos (en la página 338)
Cómo configurar una política de aprobación (en la página 341)

Estado de la tarea en CA Identity Manager

Es posible que los administradores deseen realizar un seguimiento del estado de las tareas de CA Identity Manager una vez que se hayan enviado para el procesamiento. CA Identity Manager ofrece los métodos siguientes para ver el estado de la tarea:

- **Ficha Ver tareas enviadas**

  Esta ficha permite buscar y mostrar las tareas de CA Identity Manager que se han enviado para su procesamiento.

  Los administradores pueden ver los datos de la tarea a un nivel avanzado o ver otros niveles de detalle.

  La ficha Ver tareas enviadas se incluye en dos tareas predeterminadas:

  - Ver mis tareas enviadas

    Permite a los administradores buscar y mostrar información sobre tareas que han enviado para el procesamiento.

  - Ver tareas enviadas

    Permite a los administradores buscar y mostrar información sobre tareas que otros administradores han enviado para el procesamiento.

- **Ficha Historial del usuario**

  Esta ficha, que puede agregar a las tareas del usuario, como Ver o Modificar usuarios, permite a los administradores ver la siguiente información sobre un usuario seleccionado:

  - Tareas realizadas en el usuario
  - Tareas realizadas por el usuario
  - Aprobaciones de flujo de trabajo realizadas por el usuario

- **Informes**

  Los informes de CA Identity Manager permiten ver el estado actual de un entorno de CA Identity Manager. Puede utilizar esta información para garantizar la conformidad con las políticas empresariales internas o las normativas externas.

  En la sección Generación de informes encontrará más información sobre la configuración y el uso de los informes.

- **Registros**

  Muestran información sobre todos los componentes de una instalación de CA Identity Manager, así como detalles de todas las operaciones de CA Identity Manager.

  Consulte la *Guía de configuración* para obtener más información acerca de los registros de CA Identity Manager.

Cómo CA Identity Manager determina el estado de la tarea

Una *tarea* es una función administrativa que puede realizar un usuario en CA Identity Manager. Las tareas incluyen *eventos*, es decir, acciones que lleva a cabo CA Identity Manager para completar la tarea. Una tarea puede incluir varios eventos. Por ejemplo, la tarea Crear usuario puede incluir eventos que crean el perfil del usuario, agregan el usuario a un grupo y asignan funciones.

Las tareas y los eventos de CA Identity Manager pueden estar asociados con un proceso de flujo de trabajo, que determina la forma en que CA Identity Manager realiza las acciones requeridas, y otra lógica del negocio personalizada. Las tareas también pueden estar asociadas con otras tareas, denominadas tareas anidadas. En este caso, CA Identity Manager procesa las tareas anidadas con la tarea original.

El estado de una tarea depende del estado de los eventos asociados, los procesos de flujo de trabajo, las tareas anidadas y la lógica del negocio personalizada.

Ver tareas enviadas

CA Identity Manager incluye la ficha Ver tareas enviadas. Esta ficha ofrece información sobre las tareas de un entorno de CA Identity Manager. Puede usar esta ficha para buscar y ver información avanzada sobre las acciones que realiza CA Identity Manager. La pantalla de detalles proporciona información adicional acerca de cada tarea y cada evento.

En función del estado del tarea, puede usar la ficha Ver tareas enviadas para cancelar o volver a enviar una tarea.

La ficha Ver tareas enviadas permite llevar un seguimiento del procesamiento de una tarea desde el principio hasta el final. Por ejemplo, si una tarea de CA Identity Manager incluye la asignación de roles de aprovisionamiento, y dicha asignación activa la creación de cuentas en otros sistemas, la ficha Ver tareas enviadas mostrará todos los detalles de la tarea original y los detalles de las creaciones de las cuentas.

Ver tareas enviadas incluye detalles de las operaciones realizadas en el sistema. Estas operaciones pueden ser el resultado de un evento de CA Identity Manager como, por ejemplo, EnableUserEvent. Las notificaciones enviadas por el sistema se agrupan en este evento. La ficha Ver tareas enviadas muestra un mensaje que indica que las notificaciones están en proceso hasta que se envía la notificación de fin de detalles. A continuación, el mensaje cambia a Completado.

De forma predeterminada, CA Identity Manager incluye la ficha Ver tareas enviadas en dos tareas:

- Ver tareas enviadas
- Visualización de mis tareas enviadas

Buscar tareas enviadas

Realice los pasos siguientes para buscar las tareas enviadas.

Para buscar tareas enviadas

1. Seleccione Sistema, Ver tareas enviadas.

   Aparece la página Ver tareas enviadas.

2. Especifique los criterios de búsqueda, introduzca la cantidad de filas que desea mostrar y haga clic en Buscar.

   Se mostrarán las tareas que coincidan con los criterios de búsqueda.

   Nota: Para obtener más información sobre cómo especificar los atributos en los criterios de búsqueda, consulte la sección Búsqueda de atributos para Ver tareas enviadas (en la página 590).

Búsqueda de atributos para Ver tareas enviadas

Para revisar las tareas que se han enviado para procesamiento, puede utilizar la función de búsqueda incluida en Ver tareas enviadas. Puede buscar tareas en función de los siguientes criterios:

Iniciado por

Identifica el nombre del usuario que ha iniciado una tarea como el criterio de búsqueda. Las búsquedas se basan en el nombre del usuario. Para comprobar si ha introducido un nombre de usuario válido, utilice el botón Validar.

Tareas de aprobación realizadas por

Identifica el nombre del aprobador de la tarea como el criterio de búsqueda. Las búsquedas se basan en el nombre del usuario. Para comprobar si ha introducido un nombre de usuario válido, utilice el botón Validar.

Nota: Si selecciona el criterio Tareas de aprobación realizadas por para filtrar las tareas, también se activa el criterio Mostrar tareas de aprobación de forma predeterminada.

Nombre de tarea

Identifica el nombre de la tarea como el criterio de búsqueda. Para refinar la búsqueda pueden especificarse condiciones como: igual a, contiene, empieza por o finaliza con el valor del campo Donde el nombre de tarea. Por ejemplo, para especificar el criterio de búsqueda "nombre de tarea igual a Crear usuario", seleccione la condición igual a, e introduzca Crear usuario en el campo del texto.

Estado de la tarea

Identifica el estado de la tarea como el criterio de búsqueda. Para seleccionar el estado de la tarea, active la opción Donde el estado de la tarea igual a, y seleccione la condición. Puede refinar la búsqueda aún más en función de las condiciones siguientes:

- Completado
- En proceso
- Erróneo
- Rechazado
- Completado parcialmente
- Anulado
- Programado

Nota: Consulte Descripción del estado de tarea (en la página 592) para obtener más información.

Prioridad de la tarea

Identifica la prioridad de la tarea como el criterio de búsqueda. Para seleccionar la prioridad de la tarea, active la opción Donde la prioridad de la tarea igual a, y seleccione la condición. Puede refinar la búsqueda aún más en función de las condiciones siguientes:

Bajo

Especifica que puede buscar tareas que tengan una prioridad baja.

Medio

Especifica que puede buscar tareas que tengan una prioridad media.

Alto

Especifica que puede buscar tareas que tengan una prioridad alta.

Realizado en

Identifica tareas que se realizan en la instancia seleccionada del objeto. Si no selecciona una instancia del objeto, se mostrarán las tareas que se realizaron en todas las instancias de dicho objeto.

Nota: Este campo sólo aparece cuando se completa el campo Configurar Realizado en de la pantalla de configuración de tareas enviadas. Esta pantalla se utiliza para configurar la ficha Tareas enviadas. Para obtener más información, consulte la ayuda en línea de dicha pantalla.

Intervalo de fechas

Identifica las fechas entre las que desea buscar las tareas enviadas. Debe indicar las fechas de inicio y de finalización.

Mostrar tareas que no se han enviado

Identifica las tareas que se encuentran en el estado Auditado. Identifica aquellas que han iniciado otras tareas o las tareas que no han sido enviadas. Si selecciona esta ficha, se auditarán y mostrarán todas las tareas de ese tipo.

Mostrar tareas de aprobación

Identifica las tareas que deben ser aprobadas como parte de un flujo de trabajo.

Buscar tareas enviadas en el archivo

Identifica las tarea enviadas que se han archivado.

Más información:

Descripción del estado de las tareas (en la página 592)

Descripción del estado de las tareas

Existe una tarea enviada en uno de los estados que se describen a continuación. En función del estado de la tarea, puede realizar acciones como cancelarla o volverla a enviar.

Nota: Para cancelar o volver a enviar una tarea, debe configurar la ficha Ver tareas enviadas para que muestre los botones de cancelar o volver a enviar en función del estado de la tarea. Para obtener más información sobre cómo cancelar o volver a enviar tareas, consulte Personalización de la ficha Ver tareas enviadas (en la página 595).

En proceso

Se muestra cuando se da alguna de las siguientes situaciones:

- Se ha iniciado el flujo de trabajo, pero aún no está completado.
- Hay tareas que se iniciaron antes que las tareas actuales en proceso.
- Se han iniciado tareas anidadas, pero aún no están completadas.
- Se inicia el evento primario, pero aún no está completado.
- Se inician eventos secundarios, pero aún no están completados.

Puede cancelarse una tarea en este estado.

Nota: Si cancela una tarea se cancelarán todas las tareas anidadas y los eventos incompletos de la tarea actual.

Cancelado

Se muestra cuando se cancela cualquiera de las tareas o eventos en proceso.

Rechazado

Se muestra cuando CA Identity Manager rechaza un evento o una tarea que forma parte de un proceso de flujo de trabajo. El usuario puede volver a enviar una tarea rechazada.

Nota: Cuando vuelve a enviar una tarea, CA Identity Manager vuelve a enviar todas las tareas anidadas o los eventos rechazados o que presentaron un error.

Completado parcialmente

Se muestra cuando se cancelan algunos eventos o tareas anidadas. El usuario puede volver a enviar un evento o tarea anidada completado parcialmente.

Completado

Se muestra cuando se ha completado una tarea. Una tarea está completa cuando las tareas y los eventos anidados de la tarea actual están completos.

Erróneo

Se muestra cuando una tarea, una tarea anidada o un evento anidado no son válidos en la una tarea actual. Este estado se muestra cuando se produce un error en la tarea. El usuario puede volver a enviar una tarea errónea.

Programado

Se muestra cuando se programa la tarea para ejecutarse en una fecha posterior. Puede cancelarse una tarea en este estado.

Auditado

Se muestra cuando se realiza la auditoría de la tarea actual.

Visualización de los detalles de la tarea

CA Identity Manager incluye los detalles de la tarea, como el estado de una tarea enviada, las tareas anidadas y los eventos asociados con una tarea.

Para ver los detalles de una tarea enviada

1. Haga clic en el icono de flecha derecha situado junto a la tarea seleccionada en la ficha Ver tareas enviadas.

   Aparecerán los detalles de la tarea.

   Nota: Los eventos y las tareas anidadas (si los hay) se muestran en la página Detalles de la tarea. Puede ver los detalles de cada tarea y evento.

2. Haga clic en Cerrar.

   Se cierra la ficha Detalles de la tarea y CA Identity Manager muestra la ficha Ver tareas enviadas con la lista de tareas.

Visualización de detalles de evento

CA Identity Manager proporciona detalles de los eventos, como el estado de un evento enviado, atributos del evento y cualquier otra información sobre los eventos.

Para ver los detalles de un evento enviado

1. Haga clic en el icono de flecha derecha situado junto a un evento en la página de visualización de los detalles de la tarea.

   Aparecerán los detalles del evento.

2. Haga clic en Cerrar.

   Se cierra la página Detalles del evento.

Descripción del estado del evento

Los eventos de CA Identity Manager pueden encontrarse en uno de los estados que se describen a continuación. En función del estado del evento, puede cancelar o volver a enviar un evento para su ejecución.

Nota: Para permitir que los administradores cancelen o vuelvan a enviar un evento, debe configurar la ficha Ver tareas enviadas para que muestre los botones Cancelar o Volver a enviar eventos. Al configurar la tarea, puede especificar qué administradores pueden cancelar y volver a enviar eventos. Para obtener más información sobre cómo cancelar y volver a enviar eventos, consulte Personalización de la ficha Ver tareas enviadas (en la página 595).

En proceso

Se muestra cuando se da alguna de las siguientes situaciones:

- El flujo de trabajo o los eventos previos se han iniciado, están en proceso o aprobados.
- CA Identity Manager está ejecutando el evento.
- CA Identity Manager ejecuta eventos posteriores.

Puede cancelar un evento en este estado.

Rechazado

Se muestra cuando CA Identity Manager rechaza un evento que forma parte del flujo de trabajo. Puede volver a enviar un evento rechazado.

Cancelado

Se muestra cuando cancela cualquiera de los eventos en proceso. Puede volver a enviar un evento cancelado.

Completado

Se muestra cuando se ha completado un evento.

Erróneo

Se muestra cuando CA Identity Manager detecta una excepción durante la ejecución de un evento. Puede volver a enviar un evento cancelado.

Nota: No puede volver a enviar un evento secundario hasta que el evento primario se encuentre en el estado completado.

Programado

Se muestra cuando se programa el evento para ejecutarse en una fecha posterior. Puede cancelar un evento en este estado.

Auditado

Se muestra cuando se realiza la auditoría del evento actual.

Personalización de la ficha Ver tareas enviadas

Puede personalizar la ficha Ver tareas enviadas de la siguiente manera:

- Especificar un nombre de tarea y una etiqueta diferentes.
- Cambiar las propiedades de pantalla predeterminadas. Tras la instalación, los usuarios ven una pantalla de búsqueda en la que pueden introducir los criterios que determinan las tareas que aparecen en la ficha. Puede configurar la ficha para que muestre automáticamente las tareas enviadas correspondientes al día actual y, de esta manera, evitar que el usuario tenga que introducir criterios de búsqueda.
- Determinar si los eventos de auditoría aparecerán en la página Detalles de la tarea.
- Agregar otra columna a la pantalla de la tarea.
- Especificar los criterios para cancelar o volver a enviar tareas y eventos.

Nota: Entre los detalles de las tareas y los eventos se pueden incluir datos como, por ejemplo, salarios o contraseñas, que no deben aparecer sin cifrar en la ficha Ver tareas enviadas. Estos atributos se pueden ocultar mediante la especificación de parámetros de clasificación de datos al definir los atributos en el archivo directory.xml. Para obtener más información acerca del archivo directory.xml, consulte la *Guía de configuración*.

Para configurar la ficha Ver tareas enviadas, debe modificar la tarea de administración correspondiente.

Para configurar la ficha Ver tareas enviadas

1. Haga clic en Funciones y tareas, Tareas de administración, Modificar tareas de administración.

   Aparece la página Seleccionar tarea de administración.

2. Seleccione Nombre o Categoría en el campo Buscar tareas de administración, introduzca la cadena que desea buscar y haga clic en Buscar.

   CA Identity Manager muestra las tareas de administración que cumplen con los criterios de búsqueda.

3. Elija Ver tareas enviadas y haga clic en Seleccionar.

   CA Identity Manager muestra los detalles de la tarea de administración Ver tareas enviadas.

4. Haga clic en la ficha Fichas.

   Se muestran las fichas que se utilizan para la ficha Ver tareas enviadas.

5. Haga clic en el icono de flecha derecha para editar la ficha Tareas enviadas.

   Aparecen los detalles de la ficha.

6. Modifique los campos para personalizar la ficha Ver tareas enviadas según sea necesario. Consulte Valores de configuración de la ficha Tareas enviadas (en la página 596).

Valores de configuración de la ficha Ver tareas enviadas

Utilice los siguientes campos para modificar la apariencia y la funcionalidad de la ficha Ver tareas enviadas.

Nombre

Define el nombre de la tarea.

Etiqueta

Define el identificador único de la tarea. Se utiliza en direcciones URL, servicios Web o archivos de propiedades. Debe contener letras, números o guiones bajos, y comenzar con una letra o guión bajo.

Ocultar ficha

Indica que los usuarios pueden ver la ficha, pero que no se ejecutará. Si selecciona esta opción, CA Identity Manager mostrará un error a los usuarios.

Mostrar lista de tareas al cargarse

Muestra las tareas que se han enviado para el día actual.

Nota: Si esta opción está activada, los usuarios que hagan clic en Ver tareas enviadas podrán ver directamente las tareas que fueron enviadas el mismo día.

Mostrar eventos de auditoría

Especifica si se incluyen eventos auditados en las tareas de la página Ver tareas enviadas.

Permitir columna personalizada

Indica que puede añadir una columna personalizada a la tabla de tareas que puede ver en las fichas Ver tareas enviadas e Historial del usuario. Por ejemplo, puede añadir una columna "ID de usuario" a la tabla de tareas que se muestra en la ficha Historial del usuario.

Encabezamiento de columna personalizada

Indica el nombre de pantalla de la columna personalizada.

Atributo de columna personalizada

Indica el atributo que se utilizará para completar la columna personalizada en la tabla de tareas. Por ejemplo, si está buscando tareas que se realizan sobre los empleados de una organización, puede añadir una columna de la organización que muestre la organización de cada empleado.

Cancelar tareas y eventos

Identifica los criterios para cancelar tareas o eventos. Para establecer el ámbito de este campo, seleccione una de las siguientes opciones:

El creador de la tarea debe ser el usuario actual

Identifica que puede cancelar o volver a enviar tareas o eventos que ha creado.

El creador de la tarea debe estar en el ámbito

Identifica que puede cancelar o volver a enviar tareas iniciadas por otros usuarios que coincidan con las reglas de ámbito del usuario correspondientes a las funciones de administración que le dan acceso a la ficha.

Por ejemplo, ha recibido la función Gestor de usuarios (que incluye Ver tareas enviadas), porque cumple con los criterios de la regla de pertenencia que extiende el ámbito sobre todos los usuarios de la organización Empleado. Puede cancelar o volver a enviar las tareas que envían todos los usuarios en la organización Empleado.

Sin restricciones

Identifica que cualquier usuario puede cancelar o volver a enviar una tarea o evento.

No está permitido

Especifica que no se puede cancelar ni volver a enviar una tarea o evento.

Volver a enviar tareas y eventos

Identifica los criterios para volver a enviar una tarea o evento. Para establecer el ámbito de este campo, seleccione una de las siguientes opciones:

El creador de la tarea debe ser el usuario actual

Identifica que puede cancelar o volver a enviar tareas o eventos que ha creado.

El creador de la tarea debe estar en el ámbito

Identifica que puede cancelar o volver a enviar tareas iniciadas por otros usuarios que coincidan con las reglas de ámbito del usuario correspondientes a las funciones de administración que le dan acceso a la ficha.

Por ejemplo, ha recibido la función Gestor de usuarios (que incluye Ver tareas enviadas), porque cumple con los criterios de la regla de pertenencia que extiende el ámbito sobre todos los usuarios de la organización Empleado. Puede cancelar o volver a enviar las tareas que envían todos los usuarios en la organización Empleado.

Sin restricciones

Identifica que cualquier usuario puede cancelar o volver a enviar una tarea o evento.

No está permitido

Especifica que no se puede cancelar ni volver a enviar una tarea o evento.

Ficha Historial del usuario

La ficha Historial del usuario permite ver las tareas que se relacionan con un usuario. Los detalles de la tarea que aparecen en esta ficha se pueden ver también en la ficha Ver tareas enviadas.

Nota: No se puede agregar esta ficha para crear tareas, como Crear usuario.

Se puede utilizar esta ficha para ver un historial de las tareas siguientes:

- **Tareas realizadas en el usuario**

  Muestra todas las tareas que se realizan en el usuario seleccionado.

- **Tareas realizadas por el usuario**

  Muestra todas las tareas que realiza el usuario seleccionado.

- **Aprobaciones de flujo de trabajo realizadas por el usuario**

  Muestra todas las tareas que el usuario ha aprobado como parte de un flujo de trabajo.

Nota: El tipo de tareas que se pueden ver en esta ficha dependen de la configuración de la ficha. Personalización de la ficha Historial del usuario (en la página 600) proporciona más información.

Atributos de búsqueda para ver el historial del usuario

Para revisar las tareas que se han enviado para procesamiento, puede utilizar la función de búsqueda incluida en Ver tareas enviadas. Puede buscar tareas en función de los siguientes criterios:

Nombre de tarea

Identifica el nombre de la tarea como el criterio de búsqueda. Para refinar la búsqueda puede especificar condiciones como: igual a, contiene, empieza por o finaliza con el valor del campo Donde el nombre de tarea. Por ejemplo, para especificar el criterio de búsqueda nombre de tarea igual a Crear usuario, seleccione la condición igual a, e introduzca Crear usuario en el campo del texto.

Estado de tarea

Identifica el estado de la tarea como el criterio de búsqueda. Para seleccionar el estado de la tarea, active la opción Donde el estado de la tarea igual a, y seleccione la condición. Puede refinar la búsqueda aún más en función de las condiciones siguientes:

- Completado
- En proceso
- Incorrecto
- Rechazado
- Completado parcialmente
- Cancelado
- Programado

Nota: Consulte Descripción del estado de tarea (en la página 592) para obtener más información.

Prioridad de la tarea

Identifica la prioridad de la tarea como el criterio de búsqueda. Para seleccionar la prioridad de la tarea, active la opción Donde la prioridad de la tarea igual a, y seleccione la condición. Puede refinar la búsqueda aún más en función de las condiciones siguientes:

Bajo

Especifica que puede buscar tareas que tengan una prioridad baja.

Medio

Especifica que puede buscar tareas que tengan una prioridad media.

Alto

Especifica que puede buscar tareas que tengan una prioridad alta.

Intervalo de fechas

Identifica las fechas entre las que desea buscar las tareas enviadas. Debe indicar las fechas de inicio y de finalización.

Personalización de la ficha Historial del usuario

Los administradores pueden personalizar la ficha Historial del usuario de la siguiente manera:

- Especificar un nombre de tarea y una etiqueta diferentes.
- Cambiar las propiedades de pantalla predeterminadas. De forma predeterminada, los usuarios pueden introducir criterios que determinan qué tareas aparecen en la ficha. Los administradores pueden configurar la ficha para que muestre automáticamente las tareas del día actual y, de esta manera, evitar que el usuario deba introducir los criterios de búsqueda.
- Determinar si los eventos de auditoría aparecerán en la página Detalles de la tarea.
- Agregar una columna a la pantalla de la tarea.
- Especificar los criterios para cancelar o volver a enviar tareas y eventos.

Siga estos pasos:

1. Vaya a Roles y tareas, Tareas de administración, Gestionar tareas de administración.

   Aparece la página Seleccionar tarea de administración.

2. Seleccione Nombre o Categoría en el campo Buscar tareas de administración, introduzca la cadena que desea buscar y haga clic en Buscar.

   CA Identity Manager muestra las tareas de administración que cumplen con los criterios de búsqueda.

3. Seleccione la tarea que incluye la ficha Historial del usuario y haga clic en Seleccionar.

   CA Identity Manager muestra los detalles de la tarea de administración.

4. Haga clic en la ficha Fichas.

5. Haga clic en el icono Editar que se encuentra junto a la ficha Historial del usuario.

   Aparecen los detalles de la ficha.

6. Modifique los campos para personalizar la ficha Historial del usuario.

Valores de configuración de la ficha Historial del usuario

Utilice los campos siguientes para modificar la apariencia y la funcionalidad de la ficha Historial del usuario.

Nombre

Define el nombre de la tarea.

Etiqueta

Define el identificador único de la tarea. Se utiliza en direcciones URL, servicios Web o archivos de propiedades. Debe contener letras, números o guiones bajos, y comenzar con una letra o guión bajo.

Ocultar ficha

Indica que los usuarios pueden ver la ficha, pero que no se ejecutará. Si selecciona esta opción, CA Identity Manager mostrará un error a los usuarios.

Mostrar lista de tareas al cargarse

Muestra las tareas que se han enviado para el día actual.

Nota: Si esta opción está activada, los usuarios que hagan clic en Ver tareas enviadas podrán ver directamente las tareas que fueron enviadas el mismo día.

Mostrar eventos de auditoría

Especifica si se incluyen eventos auditados en las tareas de la página Ver tareas enviadas.

Permitir columna personalizada

Indica que puede añadir una columna personalizada a la tabla de tareas que puede ver en las fichas Ver tareas enviadas e Historial del usuario. Por ejemplo, puede añadir una columna "ID de usuario" a la tabla de tareas que se muestra en la ficha Historial del usuario.

Encabezamiento de columna personalizada

Indica el nombre de pantalla de la columna personalizada.

Atributo de columna personalizada

Indica el atributo que se utilizará para completar la columna personalizada en la tabla de tareas. Por ejemplo, si está buscando tareas que se realizan sobre los empleados de una organización, puede añadir una columna de la organización que muestre la organización de cada empleado.

Cancelar tareas y eventos

Identifica los criterios para cancelar tareas o eventos. Para establecer el ámbito de este campo, seleccione una de las siguientes opciones:

El creador de la tarea debe ser el usuario actual

Identifica que puede cancelar o volver a enviar tareas o eventos que ha creado.

El creador de la tarea debe estar en el ámbito

Identifica que puede cancelar o volver a enviar tareas iniciadas por otros usuarios que coincidan con las reglas de ámbito del usuario correspondientes a las funciones de administración que le dan acceso a la ficha.

Por ejemplo, ha recibido la función Gestor de usuarios (que incluye Ver tareas enviadas), porque cumple con los criterios de la regla de pertenencia que extiende el ámbito sobre todos los usuarios de la organización Empleado. Puede cancelar o volver a enviar las tareas que envían todos los usuarios en la organización Empleado.

Sin restricciones

Identifica que cualquier usuario puede cancelar o volver a enviar una tarea o evento.

No está permitido

Especifica que no se puede cancelar ni volver a enviar una tarea o evento.

Volver a enviar tareas y eventos

Identifica los criterios para volver a enviar una tarea o evento. Para establecer el ámbito de este campo, seleccione una de las siguientes opciones:

El creador de la tarea debe ser el usuario actual

Identifica que puede cancelar o volver a enviar tareas o eventos que ha creado.

El creador de la tarea debe estar en el ámbito

Identifica que puede cancelar o volver a enviar tareas iniciadas por otros usuarios que coincidan con las reglas de ámbito del usuario correspondientes a las funciones de administración que le dan acceso a la ficha.

Por ejemplo, ha recibido la función Gestor de usuarios (que incluye Ver tareas enviadas), porque cumple con los criterios de la regla de pertenencia que extiende el ámbito sobre todos los usuarios de la organización Empleado. Puede cancelar o volver a enviar las tareas que envían todos los usuarios en la organización Empleado.

Sin restricciones

Identifica que cualquier usuario puede cancelar o volver a enviar una tarea o evento.

No está permitido

Especifica que no se puede cancelar ni volver a enviar una tarea o evento.

Mostrar tareas

Determina las tareas que aparecen en la ficha Historial del usuario.

Tareas realizadas en el usuario

Muestra todas las tareas que se realizan en el usuario seleccionado.

Tareas realizadas por el usuario

Muestra todas las tareas que realiza el usuario seleccionado.

Aprobaciones de flujo de trabajo realizadas por el usuario

Muestra todas las tareas que ha aprobado el usuario como parte de un flujo de trabajo.

La tarea Ver actividad del usuario

La actividad del usuario comprende un historial de las tareas relacionadas con un determinado usuario. Los administradores pueden utilizar la tarea Ver actividad del usuario para hacer un seguimiento de la siguiente información:

- Tareas realizadas en el usuario
- Tareas realizadas por el usuario
- Aprobaciones de flujo de trabajo realizadas por el usuario

Para ver la actividad del usuario

1. Vaya a Usuarios, Gestionar usuarios, Ver actividad del usuario.

   Aparecerá la pantalla Seleccionar usuario.

2. Busque un usuario y haga clic en Seleccionar.

   Aparecerá la pantalla Ver actividad del usuario.

Nota: Para obtener más información sobre las actividades del usuario que se muestran, consulte la Ayuda en línea de la Consola de usuario.

Limpieza de las tareas enviadas

Con cada tarea enviada, el rendimiento en tiempo de ejecución de las tareas y los eventos se reduce a medida que aumenta la base de datos de persistencia de las tareas. La recolección de basura de los procedimientos almacenados atenúa la posibilidad de problemas de rendimiento o interrupciones del sistema debidos a que la base de datos de persistencia de las tareas se ejecute con espacio en disco insuficiente. La posibilidad de archivar las tareas proporciona al administrador la capacidad de ver información de la tarea y el evento actual, así como de las tareas y los eventos que se han suprimido.

En la Consola de usuario, los administradores de CA Identity Manager pueden programar trabajos para realizar la recolección de basura automáticamente y archivar de forma repetitiva.

Ficha Repetición

Esta ficha permite programar los trabajos. A continuación se especifican los distintos campos de esta ficha:

Ejecutar ahora

Ejecuta el trabajo inmediatamente.

Programar nuevo trabajo

Programa un nuevo trabajo.

Modificar trabajo existente

Especifica la modificación de un trabajo ya existente.

Nota: Este campo sólo aparece si se ha programado un trabajo para esta tarea.

Nombre de trabajo

Especifica el nombre del trabajo que desea crear o modificar.

Zona horaria

Especifica la zona horaria del servidor.

Nota: Si su zona horaria es diferente a la zona horaria del servidor, se mostrará un cuadro desplegable que le permitirá seleccionar su zona horaria o la zona horaria del servidor cuando programe una nueva tarea. Cuando modifique un trabajo existente, no podrá cambiar la zona horaria.

Programación diaria

Especifica que el trabajo se ejecutará cada cierto número de días.

Cada (número de días)

Define cada cuantos días se ejecuta el trabajo.

Programación semanal

Especifica que el trabajo se ejecuta en un día concreto o en varios días y horas durante una semana.

Día de la semana

Especifica el día o los días de la semana en los que se ejecuta el trabajo.

Programación mensual

Especifica el día de la semana o día del mes en el que se ejecuta el trabajo mensualmente.

Programación anual

Especifica un día de la semana o día del mes en el que se ejecuta el trabajo anualmente.

Programación avanzada

Especifica información de programación adicional.

Expresión cron

Para obtener información sobre el modo de rellenar este campo, consulte lo siguiente:

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Tiempo de ejecución

Especifica la hora del día a la que se ejecuta el trabajo en formato de 24 horas. Por ejemplo, 14:15.

Ejecución inmediata de trabajos

Para ejecutar un trabajo de inmediato, utilice el asistente para la limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia del asistente.

2. Seleccione Ejecutar ahora y, a continuación, Siguiente.

   Aparecerá el paso Limpiar tareas enviadas del asistente.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea y, a continuación, haga clic en Finalizar.

   El trabajo se enviará de inmediato.

Programación de trabajos nuevos

Para programar un trabajo nuevo, utilice el asistente de limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia.

2. Seleccione Programar un trabajo nuevo, escriba el nombre del trabajo y la información de programación para el trabajo, y haga clic en Siguiente.

   Aparecerá el paso Limpiar tareas enviadas.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea y, a continuación, haga clic en Finalizar.

   Se programará el trabajo nuevo.

Modificación de trabajos existentes

Para modificar un trabajo existente, utilice el asistente de limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia.

2. Seleccione Modificar un trabajo existente y elija un trabajo existente, modifique la información de programación y haga clic en Siguiente.

   Aparecerá el paso Limpiar tareas enviadas.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y la información de límite de la tarea y, a continuación, haga clic en Finalizar.

   Se modificará el trabajo existente.

Supresión de tareas repetitivas

Para suprimir una tarea repetitiva, siga este procedimiento.

Siga estos pasos:

1. Vaya a Sistema, Seleccionar Suprimir tarea repetitiva.
2. Seleccione la tarea que desee suprimir.
3. Haga clic en Enviar.

Ficha Limpiar tareas enviadas

Esta ficha se utiliza para especificar la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea. Haga clic en Finalizar cuando haya completado todos los campos obligatorios. A continuación se especifican los distintos campos de esta ficha:

Antigüedad mínima

Especifica la antigüedad mínima de las tareas que se encuentran en estado final (Completado, Error, Rechazado, Cancelado o Anulado) para que se limpien. Por ejemplo, si se especifica 1 mes, todas las tareas que hayan alcanzado su estado final durante el último mes se conservarán. Aquellas tareas que hayan alcanzado su estado final hace más de un mes se limpiarán o se archivarán.

Éste es un campo obligatorio.

Archivar

Realiza una copia de seguridad de las tareas en la base de datos de archivo antes de suprimirlas de la base de datos de tiempo de ejecución.

Una vez que se ejecuta el trabajo, si se selecciona el archivo, los datos se asignan a la base de datos de archivo y se eliminan de la base de datos de persistencia de tareas de tiempo de ejecución. Los datos no se eliminan hasta que no se produzca una asignación correcta en la base de datos de archivo.

Tiempo de espera de la auditoría

Especifica el tiempo que transcurre antes de que se limpien las tareas en estado de auditoría. Las tareas en estado de auditoría no se consideran en estado final hasta que transcurre este período de tiempo. Las tareas en estado de auditoría no se envían.

Límite de tiempo

Limita la limpieza a un período de tiempo específico.

Límite de tareas

Limita la limpieza a un número de tareas específico.

Supresión de tareas repetitivas

Cuando no es necesario seguir ejecutando una tarea de forma repetitiva, el administrador de CA Identity Manager tiene la posibilidad de suprimirla. Una vez que la tarea se ha suprimido, deja de llevarse a cabo la recolección de basura y el archivo de esa tarea.

Todas las tareas programadas mediante el uso del asistente Limpiar tareas enviadas: Repetición se muestran en esta página y el administrador de CA Identity Manager puede seleccionar las tareas que desea suprimir.

Nota: Las tareas siguen presentes en la base de datos y sólo se suprime la repetición de la programación.

Configuración de conexión de Enterprise Log Manager

Utilice esta pantalla para gestionar las nuevas tareas de conexión agregadas de CA User Activity Reporting (CA UAR).

Nota: Se ha renombrado CA Enterprise Log Manager. Ahora se llama CA UAR.

Los campos de esta pantalla se muestran a continuación:

Nombre de la conexión

Especifica el nombre exclusivo utilizado para el objeto gestionado de conexión único de CA UAR.

Éste es un campo de sólo lectura.

Descripción

Describe la conexión de CA UAR.

Nombre del host

Especifica el nombre de host o la dirección IP del servidor de CA UAR.

Éste es un campo obligatorio.

Núm. de puerto

Especifica el puerto de conexión del servidor de CA UAR.

Predeterminado: 52520

Éste es un campo obligatorio.

Certificar certificado SSL firmado por autoridades

Si se selecciona, especifica una comprobación estricta del certificado SSL en la conexión a un servidor de CA UAR.

Si tiene un certificado de SSL autofirmado, por ejemplo un certificado instalado con CA UAR de forma predeterminada, esta casilla de verificación no se deberá seleccionar, dado que la ruta de confianza a la entidad emisora raíz no existe.

Nombre del certificado

Especifica el nombre del certificado de CA UAR que se utiliza para la autenticación.

Éste es un campo obligatorio.

Certificate Password (Contraseña de certificado)

Especifica la contraseña de CA UAR.

Éste es un campo obligatorio.

Atributo

No admitido. La versión se recupera al intentar guardar la información de conexión como una prueba.

Supresión de conexión de Enterprise Log Manager

Seleccione una conexión de la lista y haga clic en Suprimir. La conexión de CA UAR se habrá suprimido.

Gestión de claves secretas

Utilice claves secretas para gestionar 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.

Cada entorno tiene un conjunto de claves dinámicas y una contraseña de almacén de claves. Si los entornos comparten un directorio de usuarios, utilice las mismas claves dinámicas y la contraseña del almacén de claves para cada entorno.

Las contraseñas de almacén de claves se cifran mediante claves incrustadas en el código de cifrado o los parámetros que se introducen durante instalación del servidor de CA Identity Manager. En un clúster, todos los nodos comparten los valores para las claves dinámicas y la contraseña del almacén de claves.

Las operaciones de cifrado utilizan la última clave dinámica para el entorno y el algoritmo correspondientes. Las operaciones de descifrado comprueban si existe un ID de clave en los datos cifrados para que se utilice la clave correcta. En la sección Formatos de texto cifrado de la *Guía de configuración* encontrará más detalles.

Siga estos pasos:

1. Introduzca o modifique la contraseña en el almacén de claves.
2. Haga clic en Agregar una clave si necesita otra clave.
3. Seleccione un algoritmo.
4. Introduzca una contraseña para la clave.

   Para PBE (cifrado basado en contraseña) y RC2, la longitud clave máxima es de 128 bytes.

   Para AES, los tamaños clave válidos son 16, 24 y 32 bytes.
5. Haga clic en Enviar.
6. Si se ha modificado la Contraseña del almacén de claves, haga clic en Enviar.

   CA Identity Manager cifra de nuevo los valores de las claves.

Capítulo 21: Persistencia de la tarea

Esta sección contiene los siguientes temas:

Archivo y recopilación de datos residuales de persistencia de tareas automatizadas

En esta versión, los administradores pueden programar y modificar los trabajos con parámetros específicos mediante la tarea Limpiar tareas enviadas para limpiar y archivar la información de eventos y tareas de la base de datos de persistencia de tareas y suprimir las tareas repetitivas si es necesario.

En la ficha Sistema, seleccione Limpiar tareas enviadas para iniciar un asistente. El asistente le guiará a través de la configuración y la programación de trabajos y le permitirá si desea archivar o no los datos. También puede elegir si desea suprimir los trabajos repetitivos si es necesario. Para ello, seleccione Suprimir tareas repetitivas en la ficha Sistema.

Al programar las tareas para limpiar y archivar los datos de tareas, la probabilidad de problemas de rendimiento o interrupciones del sistema se reduce en gran medida. Con la función de archivo, puede realizar una copia de seguridad de las tareas en la base de datos de archivo antes de suprimirlas de la base de datos de tiempo de ejecución. Si necesita volver atrás y ver las tareas suprimidas, marque la casilla de verificación Buscar tareas enviadas en el archivo en Ver tareas enviadas para buscar y ver una lista de todas las tareas que se han suprimido y archivado.

Ficha Recurrencia

Utilice esta ficha para programar su trabajo. A continuación se especifican los distintos campos de esta ficha:

Ejecutar ahora

Ejecuta el trabajo inmediatamente.

Programar nuevo trabajo

Programa un nuevo trabajo.

Modificar trabajo existente

Especifica que desea modificar un trabajo que ya existe.

Nota: Este campo sólo aparece si se ha programado un trabajo para esta tarea.

Nombre de tarea

Especifica el nombre del trabajo que desea crear o modificar.

Zona horaria

Especifica la zona horaria del servidor.

Nota: Si su zona horaria es diferente a la zona horaria del servidor, se mostrará un cuadro desplegable que le permitirá seleccionar su zona horaria o la zona horaria del servidor cuando programe una nueva tarea. Cuando modifique un trabajo existente, no podrá cambiar la zona horaria.

Programación semanal

Especifica que el trabajo se ejecuta un día específico o varios días y horas durante una semana.

Programación avanzada

Especifica información de programación adicional.

Día de la semana

Especifica el día o los días de la semana en los que se ejecuta el trabajo.

Tiempo de ejecución

Especifica la hora del día a la que se ejecuta el trabajo, en formato de 24 horas. Por ejemplo, 14:15.

Expresión cron

Para obtener información sobre el modo de rellenar este campo, consulte lo siguiente:

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Nota: Este campo aparece cuando se selecciona Programación avanzada.

Más información

Supresión de tareas repetitivas (en la página 606)
Programación de trabajos nuevos (en la página 606)
Modificación de trabajos existentes (en la página 606)
Ejecución inmediata de trabajos (en la página 605)

Ficha Limpiar tareas enviadas

Esta ficha se utiliza para especificar la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea. Haga clic en Finalizar cuando haya completado todos los campos obligatorios. A continuación se especifican los distintos campos de esta ficha:

Antigüedad mínima

Especifica la antigüedad mínima de las tareas que se encuentran en estado final (Completado, Error, Rechazado, Cancelado o Anulado) para que se limpien. Por ejemplo, si se especifica 1 mes, todas las tareas que hayan alcanzado su estado final durante el último mes se conservarán. Aquellas tareas que hayan alcanzado su estado final hace más de un mes se limpiarán o se archivarán.

Éste es un campo obligatorio.

Archivar

Realiza una copia de seguridad de las tareas en la base de datos de archivo antes de suprimirlas de la base de datos de tiempo de ejecución.

Una vez que se ejecuta el trabajo, si se selecciona el archivo, los datos se asignan a la base de datos de archivo y se eliminan de la base de datos de persistencia de tareas de tiempo de ejecución. Los datos no se eliminan hasta que no se produzca una asignación correcta en la base de datos de archivo.

Tiempo de espera de la auditoría

Especifica el tiempo que transcurre antes de que se limpien las tareas en estado de auditoría. Las tareas en estado de auditoría no se consideran en estado final hasta que transcurre este período de tiempo. Las tareas en estado de auditoría no se envían.

Límite de tiempo

Limita la limpieza a un período de tiempo específico.

Límite de tareas

Limita la limpieza a un número de tareas específico.

Ejecución inmediata de trabajos

Para ejecutar un trabajo de inmediato, utilice el asistente para la limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia del asistente.

2. Seleccione Ejecutar ahora y, a continuación, Siguiente.

   Aparecerá el paso Limpiar tareas enviadas del asistente.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea y, a continuación, haga clic en Finalizar.

   El trabajo se enviará de inmediato.

Programación de trabajos nuevos

Para programar un trabajo nuevo, utilice el asistente de limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia.

2. Seleccione Programar un trabajo nuevo, escriba el nombre del trabajo y la información de programación para el trabajo, y haga clic en Siguiente.

   Aparecerá el paso Limpiar tareas enviadas.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y el límite de tareas de la tarea y, a continuación, haga clic en Finalizar.

   Se programará el trabajo nuevo.

Modificación de trabajos existentes

Para modificar un trabajo existente, utilice el asistente de limpieza de tareas enviadas.

Siga estos pasos:

1. Vaya a Sistema, Limpieza de tareas enviadas.

   Aparecerá el paso Recurrencia.

2. Seleccione Modificar un trabajo existente y elija un trabajo existente, modifique la información de programación y haga clic en Siguiente.

   Aparecerá el paso Limpiar tareas enviadas.

3. Especifique la antigüedad mínima, el archivo, el tiempo de espera de la auditoría, el límite de tiempo y la información de límite de la tarea y, a continuación, haga clic en Finalizar.

   Se modificará el trabajo existente.

Supresión de tareas repetitivas

Para suprimir una tarea repetitiva, siga este procedimiento.

Siga estos pasos:

1. Vaya a Sistema, Seleccionar Suprimir tarea repetitiva.
2. Seleccione la tarea que desee suprimir.
3. Haga clic en Enviar.

Cómo migrar la base de datos de persistencia de la tarea

En versiones anteriores, la migración se realiza al instante y se utiliza la Consola de gestión. Se ha proporcionado una herramienta de migración de línea de comandos para eliminar cuellos de botella de rendimiento al migrar grandes cantidades de tareas. También se puede también ajustar la migración a un entorno específico, un estado de la tarea y las tareas que se han creado y que se ejecutan durante un intervalo de fechas específico. La herramienta de línea de comando, runmigration, se encuentra en la siguiente carpeta:

```
admin_tools/tools/tpmigration
```

Para migrar la base de datos de persistencia de la tarea, se deben realizar los siguientes pasos:

1. Actualice el archivo tpmigration125.properties.
2. Establezca la variable JAVA_HOME.
3. Ejecute la herramienta runmigration.

Actualización del archivo tpmigration125.properties

Para configurar la migración de la base de datos de persistencia de la tarea, se debe actualizar el archivo tpmigration.properties con el almacén de objetos y la información de persistencia de la tarea, incluidos los valores de almacén. El archivo tpmigration125.properties se encuentra en la siguiente ubicación:

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetpto125

Para configurar la migración, complete la siguiente información en el archivo de propiedades:

```
############################################################
# The object store is required to obtain the environment details.
############################################################
os.db.hostname=<hostname>
os.db.dbname=<database-name or SID>
os.db.username=<db user name>
os.db.password=<db user's password>
os.db.port=<db port number>
os.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for
oracle 'oracle'>

############################################################
# Task persistence data where the old and new tables are.
############################################################
tp.db.hostname=<hostname>
tp.db.dbname=<database-name or SID>
tp.db.username=<db user name>
tp.db.password=<db user's password>
tp.db.port=<db port number>
tp.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for
oracle 'oracle'>
```

Establezca la variable JAVA_HOME.

Para que la herramienta runmigration se ejecute correctamente, se debe asegurar de que la variable de entorno JAVA_HOME.

Ejecución de la herramienta runmigration

Para iniciar la migración, lleve a cabo el siguiente procedimiento.

Desde una línea de comandos

1. Ejecute la herramienta runmigration.

   Para Windows:

   ```
   runmigration.bat
   ```

   Para UNIX:

   ```
   runmigration.sh
   ```

2. Introduzca la información siguiente:

   - El alias protegido de entorno ("todo" para todos los entornos).

     Nota: Si no se especifica todo, solamente se podrá introducir un entorno.

   - El estado de la tarea.
     Nota: Si no se especifica todo, solamente se podrá introducir un estado de la tarea.

   - La versión de CA Identity Manager para migrar desde (1-8.x y 2-12.0).

   - Si desea especificar un intervalo de fechas para las tareas que tienen que migrarse (sí o no).

     Nota: Si decide que sí, debe introducir lo siguiente:

     - La fecha de inicio (dd/mm/aa)
     - La fecha de finalización (dd/mm/aa)

   Los inicios de la migración.

Una vez que se complete la migración, el estado indica cuántas tareas se han migrado.