



NetIQ® Identity Manager

Guía del usuario de Identity Applications

Mayo de 2024

Información legal

Copyright 2009-2024 Open Text.

La única garantía para los productos y servicios de Open Text y sus afiliados y licenciadores ("Open Text") está definida de forma expresa en la declaración de garantía que acompaña a estos productos y servicios. Nada en este documento debe interpretarse como constituyente de una garantía adicional. Open Text no será responsable de errores técnicos o de redacción ni de omisiones presentes en este documento. La información contenida en este documento está sujeta a cambios sin previo aviso.

Para obtener información adicional, como avisos relacionados con la certificación y marcas comerciales, consulte <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).

Tabla de contenido

Acerca de este libro y la biblioteca	7
Parte I Bienvenido al Gestor de identidades	9
1 Primeros pasos	11
Descripción de las funciones y recursos	11
Descripción de Identity Applications	11
Descripción de la consola de Identity Manager	11
Exploración de la Consola	12
Descripción de la página de aplicaciones	13
Descripción de las tareas	14
Maneras habituales de utilizar Identity Applications	14
¿Cómo funciona el autoservicio de identidades?	14
¿Cómo funcionan las funciones y los recursos?	14
¿Cómo funcionan las peticiones de procesos?	16
¿Cómo funciona el servicio de ayuda técnica?	16
2 Acceso a Identity Applications	19
Consideraciones para acceder a Identity Applications	19
Entrada por primera vez	20
Respuesta a la comprobación de configuración regional preferida	22
Solución de problemas de entrada a la sesión	22
Si olvida la contraseña	22
Si tiene problemas para entrar a la sesión	23
Si el sistema le solicita información adicional	23
Cierre de la sesión	23
Parte II Personalización de la consola	25
3 Gestión de widgets y diseños	27
Gestión de la consola global	28
Cambio del diseño de la consola	28
Adición de un widget	29
Adición de widgets generales	30
Adición de widgets de Identity Manager	31
Adición de widgets de control de identidad	32
Opciones del widget	32
Configuración de un widget	33

Parte III Gestión de sus permisos y del perfil de identidad	35
4 Gestión de las peticiones de permisos	37
Visualización de los permisos	37
Petición de permisos	39
Visualización de peticiones	39
Seguimiento de una petición	40
Cancelación de una petición	40
Generación de un ticket del servicio de ayuda técnica	41
Revocación de permisos	41
Creación de un enlace interno a una petición	42
5 Gestión de aplicaciones	45
Creación de elementos destacados	45
Adición de una aplicación	45
Adición de un permiso	46
Adición, modificación o supresión de categorías	46
Adición de una categoría	46
Modificación de una categoría	46
Supresión de una categoría	47
6 Gestión de las tareas	49
Visualización de las tareas	49
Gestión de la aprobación o el rechazo de las peticiones	50
Gestión de las tareas del servicio de ayuda técnica	51
7 Actuación en nombre de otra persona	53
Visualización de las asignaciones del apoderado	53
Actuación como apoderado	53
Gestión de asignaciones de apoderado	53
8 Gestión de delegaciones	55
9 Gestión de la disponibilidad	57
10 Gestión del perfil	59
Actualización de su perfil	59
11 Gestión del organigrama corporativo	61
Visualización de un organigrama corporativo	61
Descripción del organigrama corporativo	62
Uso del organigrama corporativo	63
Restablecer la raíz en la vista Organigrama corporativo	64
Cambiar la vista del organigrama corporativo	64
Seleccionar la relación que desea ver	65
Desplazarse hasta el siguiente nivel en la jerarquía de relaciones	66

Enviar un correo electrónico a los usuarios desde el organigrama corporativo.....	67
Ver información detallada de un usuario.....	67
12 Gestión de la contraseña	69
Uso del autoservicio de gestión de contraseñas en Identity Manager.....	69
Descripción de la respuesta a la pregunta de verificación de la contraseña	70
Cambio de la contraseña.....	70
Estado de directiva de contraseñas	71
Uso de la gestión de contraseñas legada	72
Respuesta a la pregunta de verificación de la contraseña	73
Cambio de la sugerencia de contraseña	73
Cambiar contraseña.....	74
Estado de directiva de contraseñas	75
Estado de sincronización de contraseñas	75
Parte IV Gestión de usuarios, grupos y equipos	77
13 Gestión de usuarios	79
Creación de un usuario.....	79
Edición de la información del usuario.....	79
Listas de usuarios	80
Cómo buscar usuarios	81
Clasificación de los usuarios.....	82
14 Gestión de equipos	83
Visualización de equipos	83
Creación de un equipo	84
Modificación de un equipo	84
15 Gestión de grupos	85
Creación de un grupo	85
Parte V Apéndice	87
A Uso de la aplicación de aprobaciones de Identity Manager	89
Requisitos del producto	89
Instalación de la aplicación de aprobaciones	90
Configuración de la aplicación de aprobaciones	90
Petición de acceso móvil mediante la aplicación de usuario	91
Uso de un enlace de configuración o un código QR	92
Configuración manual de la aplicación de aprobaciones	92
Descripción general de la aplicación de aprobaciones	95
Vista Tareas	95
Vista Detalles	96
Modo por lotes	96
Vista Tareas completadas	96
Vista Ajustes de inicio de sesión.....	97

Vista Configuración avanzada	97
Cambio del idioma de visualización de la aplicación de aprobaciones	97

Acerca de este libro y la biblioteca

En esta guía se describe cómo los usuarios finales y algunos administradores pueden usar NetIQ Identity Manager Identity Applications, en particular la consola y la aplicación de usuario.

A quién va dirigida

Este manual proporciona información para las personas responsables de comprender los conceptos de administración y de implementar un modelo de administración seguro y distribuido.

Otra información de la biblioteca

Para obtener más información acerca de la biblioteca para Identity Manager, consulte el [sitio Web de documentación de Identity Manager \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

Bienvenido al Gestor de identidades

El Gestor de identidades de NetIQ es un producto de software de sistema que se emplea en la organización para gestionar de forma segura las necesidades de acceso de su comunidad de usuarios. Si es miembro de dicha comunidad de usuarios, podrá disfrutar de las diversas ventajas que ofrece Identity Manager. Por ejemplo, Identity Manager permite que su organización:

- ♦ Otorgue a los usuarios acceso a información (organigramas corporativos de grupos, informes oficiales del departamento o búsqueda de empleados) y a funciones y recursos (equipos o cuentas de los sistemas internos) que necesiten a partir del primer día.
- ♦ Sincronice varias contraseñas en una única entrada a la sesión para todos los sistemas.
- ♦ Modifique o revoque derechos de acceso instantáneamente cuando sea necesario (cuando alguien pasa a otro grupo o deja la organización).
- ♦ Cumpla las regulaciones gubernamentales.

Lea esta parte en primer lugar para obtener información sobre Identity Manager Identity Applications y una explicación sobre cómo empezar a utilizar este producto. Esta guía está diseñada para ayudar con los siguientes tipos de actividades en línea de la organización:

- ♦ Gestionar la identidad en línea asociada con los recursos organizativos.
- ♦ Ver o modificar el acceso a funciones y recursos organizativos.
- ♦ Aprobar las peticiones de acceso a recursos y funciones.
- ♦ Gestionar los permisos asociados con aplicaciones de software y otros recursos que su organización proporciona a sus miembros.

1 Primeros pasos

En esta sección se describe el procedimiento para empezar a utilizar Identity Applications. Los temas son los siguientes:

- ♦ [“Descripción de las funciones y recursos” en la página 11](#)
- ♦ [“Descripción de Identity Applications” en la página 11](#)
- ♦ [“Descripción de la consola de Identity Manager” en la página 11](#)
- ♦ [“Exploración de la Consola” en la página 12](#)
- ♦ [“Descripción de las tareas” en la página 14](#)
- ♦ [“Maneras habituales de utilizar Identity Applications” en la página 14](#)

Descripción de las funciones y recursos

En Identity Applications, un **permiso** representa el acceso proporcionado a un usuario o grupo de usuarios para una función o un recurso. Una **función** define un conjunto de permisos en referencia a uno o varios sistemas o aplicaciones de destino. Por ejemplo, una función de administrador de usuarios puede tener autorización para restablecer la contraseña de un usuario, mientras que una función de administrador del sistema puede tener la capacidad de asignar a un usuario a un servidor específico. Un **recurso** es cualquier entidad digital, como una cuenta de usuario, un equipo o una base de datos que un usuario empresarial necesita para poder acceder.

Descripción de Identity Applications

Identity Manager Identity Applications son un conjunto de aplicaciones Web interconectadas basadas en el navegador. Permiten a la organización gestionar las cuentas de usuario y los permisos asociados con una amplia variedad de funciones y recursos disponibles para los usuarios. Es posible configurar Identity Applications para que proporcione autoservicio de asistencia para los usuarios, como pedir funciones o cambiar sus contraseñas. También puede configurar flujos de trabajo para mejorar la eficacia de la gestión y la asignación de funciones y recursos.

Descripción de la consola de Identity Manager

La consola de NetIQ Identity Manager funciona como portal de entrada principal a Identity Applications. La consola puede tener uno o varios widgets que le ayuden a obtener información rápidamente sobre actividades concretas. Desde la consola, puede realizar las siguientes actividades:

- ♦ Gestionar la configuración de su perfil y la contraseña.
- ♦ Ver la información del organigrama corporativo.
- ♦ Revisar y completar sus tareas, como aprobar peticiones de acceso de los usuarios.
- ♦ Pedir permisos para funciones, recursos o procesos.

- ♦ Revisar el estado y el historial de sus peticiones de permisos.
- ♦ Buscar a otros usuarios de la organización.
- ♦ Personalizar la consola, por ejemplo, añadiendo widgets y cambiando su posición en función de sus intereses.
- ♦ Establecer a cualquier usuario como apoderado desde el sistema.
- ♦ Delegar sus tareas en otros usuarios desde el sistema.

Puede llevar a cabo las siguientes tareas con los correspondientes **permisos**:

- ♦ Crear y modificar perfiles de usuario.
- ♦ Ver la información de otros usuarios en el organigrama corporativo.
- ♦ Crear y modificar equipos que representen un conjunto de usuarios y grupos que puedan llevar a cabo peticiones de provisión y tareas de aprobación asociadas a los equipos.
- ♦ Solicitar permisos o revocar permisos en nombre de otros usuarios de la organización.

Exploración de la Consola

La consola ofrece información rápida sobre sus tareas, permisos y peticiones en forma de widgets. Puede acceder a páginas o aplicaciones específicas con un solo clic. Además, es posible añadir, eliminar y configurar widgets en la consola, además de modificar la posición de esos widgets. Para obtener más información sobre cómo personalizar la consola, consulte el [Capítulo 3, “Gestión de widgets y diseños”, en la página 27](#).

A continuación se muestra un ejemplo que describe las opciones de widgets por defecto de la consola.

Figura 1-1 Ejemplo de consola personalizada



La consola de Identity Manager permite gestionar las distintas actividades en Identity Manager. A continuación se muestran las páginas que le ayudarán a gestionar sus tareas y actividades:

Aplicación

Muestra todas las aplicaciones aprovisionadas para usted. Incluye enlaces por defecto a varias zonas para simplificar las tareas básicas que debe llevar a cabo en Identity Manager. Para obtener más información, consulte [“Descripción de la página de aplicaciones” en la página 13](#).

Tareas

Muestra todas las tareas pendientes para una acción. Con una función adecuada, puede ver las tareas de otros usuarios. Por ejemplo, del supervisor de equipo.

Acceso

Permite ver permisos o pedirlos. Para ver el estado de los permisos solicitados, acceda a **Historial de peticiones**. Esta página muestra todas las peticiones y su estado.

Gente

Permite ver a los demás usuarios o grupos del sistema y el **organigrama corporativo** de otro usuario. Esto ayuda a visualizar la relación entre los usuarios y los grupos.

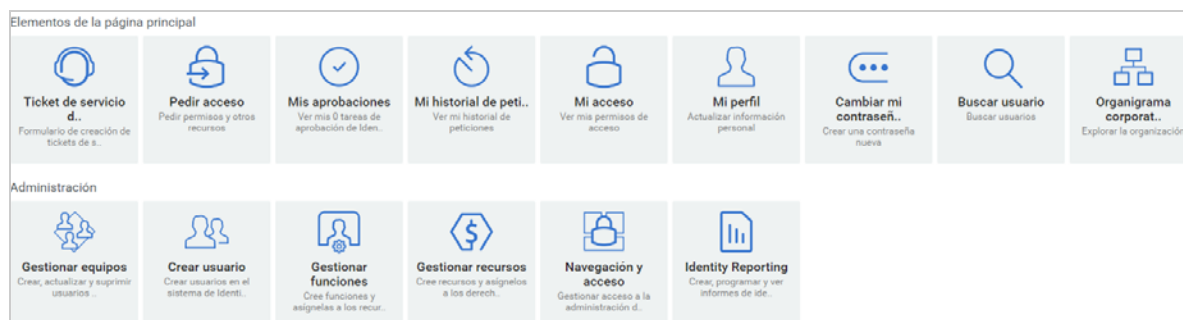
Administración

Permite ver y gestionar funciones, recursos, reconciliación de permisos y configuraciones. Esta opción solo se muestra para los administradores. Para obtener más información, consulte [Identity Applications Administration](#) (Administración de Identity Applications) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Descripción de la página de aplicaciones

La segunda vista significativa de la consola es la página **Aplicaciones** (Figura 1-2), que proporciona enlaces por defecto a diversas áreas para simplificar las tareas básicas que los usuarios finales y los administradores deben realizar en Identity Manager.

Figura 1-2 Ejemplo de la página Aplicaciones en la consola



La opción **Crear ticket del servicio de ayuda técnica** aparece por defecto en la página **Aplicaciones**. Esta opción permite generar un ticket para el servicio de ayuda técnica.

El administrador de identidades personaliza la página **Aplicaciones** para incluir mosaicos que enlacen con los recursos que se piden con más frecuencia o con las aplicaciones a las que los usuarios acceden regularmente. Es posible configurar el acceso de usuario para estos mosaicos si se cuenta con una función administrativa adecuada. Diríjase a **Su ID > Valores de configuración > Acceso** para añadir Trustees para los elementos de navegación necesarios. Para obtener más información sobre cómo proporcionar acceso, consulte [Managing User Access](#) (Gestión de acceso de usuarios) en *NetIQ Identity Manager - Administrator's Guide to Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Algunos de los mosaicos de esta página pueden aparecer solo para los usuarios con una función administrativa en Identity Applications. Por ejemplo, una persona que pueda crear o modificar funciones verá un mosaico similar a **Crear usuario** y **Gestionar funciones**.

Para obtener más información acerca del uso de la consola, haga clic en  en la consola.

Descripción de las tareas

La página **Tareas** permite aprobar o denegar las acciones para las tareas mostradas.

La consola de Identity Manager permite gestionar las tareas de Identity Manager y de Identity Governance desde la página Tareas. Ahora se pueden ver y aprobar tareas de Identity Manager y de Identity Governance desde la misma interfaz de usuario.

Maneras habituales de utilizar Identity Applications

A continuación se muestran ejemplos de cómo se suele utilizar Identity Applications en una organización.

- ♦ [“¿Cómo funciona el autoservicio de identidades?” en la página 14](#)
- ♦ [“¿Cómo funcionan las funciones y los recursos?” en la página 14](#)
- ♦ [“¿Cómo funcionan las peticiones de procesos?” en la página 16](#)
- ♦ [“¿Cómo funciona el servicio de ayuda técnica?” en la página 16](#)

¿Cómo funciona el autoservicio de identidades?

- ♦ Elena (un usuario final) recupera su contraseña que ha olvidado gracias a las funciones del Autoservicio de identidades cuando entra a la sesión.

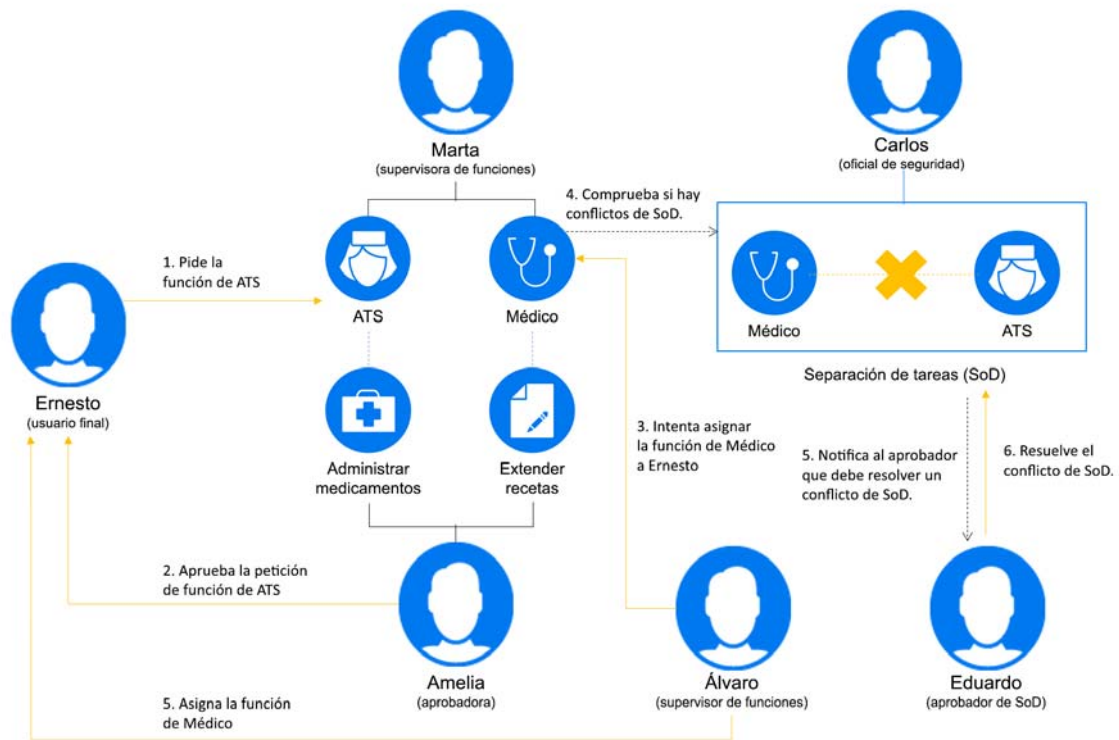
Por defecto, Identity Manager usa la aplicación de autoservicio de restablecimiento de contraseñas (SSPR, Self Service Password Reset) para permitir que los usuarios puedan modificar sus contraseñas. Sin embargo, Identity Applications puede usar otros métodos para gestionar las contraseñas olvidadas.

- ♦ Erik (un usuario final) hace una búsqueda de todos los empleados que hablan alemán en su lugar de trabajo.
- ♦ Eduardo (un usuario final) examina el organigrama corporativo, encuentra a Elena y hace clic en el icono de correo electrónico para enviarle un mensaje.

¿Cómo funcionan las funciones y los recursos?

A continuación se indica un ejemplo que explica el flujo de la petición de funciones y recursos en el sistema:

Figura 1-3 Ejemplo de asignación de funciones



- ♦ Marta (una supervisora de funciones) crea las funciones empresariales ATS y Médico y las funciones de TI Administrar medicamentos y Extender recetas. Marta crear varios recursos necesarios para estas funciones y los asocia con las funciones.
- ♦ Marta (una supervisora de funciones) define una relación entre las funciones ATS y Administrar medicamentos, especificando que la función ATS contiene la función Administrar medicamentos. También define una relación entre las funciones Extender recetas y Médico, especificando que la función Médico contiene la función Extender recetas.
- ♦ Carlos (un responsable de seguridad) define una restricción de separación de tareas que indica la existencia de un conflicto potencial entre las funciones Médico y ATS. Esto significa que normalmente el mismo usuario no deberá tener asignadas ambas funciones al mismo tiempo. En algunas circunstancias, una persona que pida una asignación de función puede desear anular esta restricción. Para definir una excepción de separación de tareas, la persona que pida la asignación debe justificarla.
- ♦ Ernesto (un usuario final) examina una lista de las funciones a su disposición y solicita una asignación para la función ATS.
- ♦ Amelia (una aprobadora) recibe una notificación de una petición de aprobación por correo electrónico (que contiene una URL). Hace clic en el enlace, obtiene un formulario de aprobación y lo aprueba.
- ♦ Álvaro (un supervisor de funciones) pide que a Ernesto se le asigne la función Médico. Se le notifica que existe un conflicto potencial entre la función Médico y la función que Ernesto tiene asignada previamente (ATS). Proporciona una justificación para hacer una excepción a la restricción de separación de tareas.

- ♦ Eduardo (un aprobador de separación de tareas) recibe por correo electrónico una notificación de conflicto de separación de tareas. Aprueba la petición de Álvaro para anular la restricción de separación de tareas.
- ♦ Amelia (una aprobadora) recibe por correo electrónico una petición de aprobación para la función Médico. Aprueba la petición de Álvaro de asignar a Ernesto la función Médico.
- ♦ Juan (un auditor de funciones) observa el informe de infracciones y excepciones de separación de tareas y observa que a Ernesto se le han asignado las funciones Médico y ATS. Observa también que a Ernesto se le han asignado los recursos asociados con estas funciones.

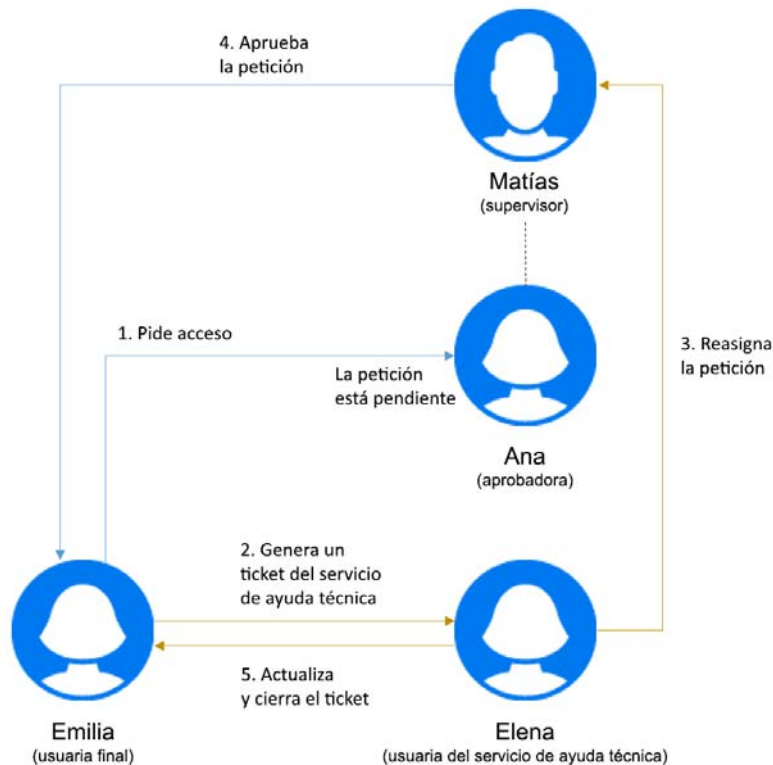
¿Cómo funcionan las peticiones de procesos?

- ♦ Enrique (un usuario final) examina una lista de recursos que puede utilizar y solicita acceso al sistema Siebel*.
- ♦ Ana (una aprobadora) recibe una notificación de una petición de aprobación por correo electrónico (que contiene una URL). Hace clic en el enlace, obtiene un formulario de aprobación y lo aprueba.
- ♦ Enrique comprueba el estado de su petición anterior de acceso a Siebel (que ahora ha pasado a una segunda persona para ser aprobada). Ve que todavía está en curso.
- ♦ Ana se va de vacaciones, por lo que indica que no estará disponible temporalmente. Mientras no esté disponible, no se le asignará ninguna nueva tarea de aprobación.
- ♦ Ana abre su lista de tareas de aprobación y se da cuenta de que hay demasiadas para poder responderlas con rapidez, así que decide reasignar algunas a otros compañeros.
- ♦ Ramón (un auxiliar administrativo, que trabaja de usuario apoderado para Ana) abre la lista de tareas de Ana y lleva a cabo una tarea de aprobación en su lugar.
- ♦ Manuel (un supervisor) observa las listas de tareas de las personas de su departamento. Sabe que Ana está de vacaciones, así que reasigna tareas a otros empleados de su departamento.
- ♦ Manuel inicia una petición de una cuenta de base de datos para alguien de su departamento que depende directamente de él.
- ♦ Manuel asigna a Daniel para que sea un delegado autorizado de Ana.
- ♦ Daniel (ahora un aprobador delegado) recibe las tareas de Ana cuando ella no está disponible.
- ♦ Manuel contrata una persona en prácticas, que no debe introducirse en el sistema de RR. HH. El administrador del sistema crea el registro de usuario de esta persona en prácticas y solicita que se le otorgue acceso a Notes, Active Directory* y Oracle*.

¿Cómo funciona el servicio de ayuda técnica?

A continuación se indica un ejemplo que explica el flujo de tickets del servicio de ayuda técnica en el sistema:

Figura 1-4 Ejemplo de ayuda técnica



- ♦ Emilia (una usuaria final) ha pedido acceso a la impresora de oficina. La petición lleva mucho tiempo pendiente. Por lo tanto, ha generado un ticket para el servicio de ayuda técnica.
- ♦ Elena (una usuaria del servicio ayuda técnica) recibe una notificación sobre el ticket en su lista de tareas.
- ♦ Elena analiza el problema y descubre que la petición ha sido asignada a Ana (una aprobadora).
- ♦ La petición está pendiente en el sistema porque Ana está fuera de la oficina.
- ♦ Elena tiene permiso para reasignar las peticiones de tareas. Reasigna la petición a Matías (el supervisor de Ana).
- ♦ Matías revisa la petición y la aprueba. Emilia ya puede acceder a la impresora de la oficina.
- ♦ Elena actualiza el ticket del servicio de ayuda técnica y lo cierra.

2 Acceso a Identity Applications

Para acceder a Identity Applications, por ejemplo a la consola, se usa un navegador Web. Identity Manager es compatible con las versiones actuales de los navegadores más populares. Consulte el administrador del sistema para que le proporcione una lista de los navegadores compatibles o pídale ayuda para instalar uno. Su organización debe proporcionarle la dirección URL y las credenciales necesarias para acceder a las aplicaciones.

- ♦ [“Consideraciones para acceder a Identity Applications” en la página 19](#)
- ♦ [“Entrada por primera vez” en la página 20](#)
- ♦ [“Respuesta a la comprobación de configuración regional preferida” en la página 22](#)
- ♦ [“Solución de problemas de entrada a la sesión” en la página 22](#)
- ♦ [“Cierre de la sesión” en la página 23](#)

Consideraciones para acceder a Identity Applications

Antes de acceder a la consola o a cualquier otra aplicación de Identity Applications, tenga en cuenta las siguientes consideraciones:

- ♦ Debe habilitar las cookies y JavaScript * en el navegador Web.
- ♦ Si utiliza Internet Explorer, debe establecer al menos el nivel de privacidad **Medio**. Debe seleccionar la opción **Cada vez que se visita la página** en **Herramientas > Opciones de Internet > General, Historial de exploración > Valores de configuración > Comprobar si hay nuevas versiones de las páginas guardadas**. Si no tiene seleccionada esta opción, puede que algunos botones no se muestren correctamente.
- ♦ Si ha accedido anteriormente a la aplicación de usuario de Identity Manager, quizás pueda usar el mismo nombre de usuario y contraseña para acceder a la consola.
- ♦ No es posible acceder a Identity Applications con cuentas cuyos nombres incluyan los siguientes caracteres:

\ / , * ? . \$ # +

- ♦ Si no puede entrar, haga clic en [¿Se ha olvidado de la contraseña](#). Para obtener más información, consulte [“Si olvida la contraseña” en la página 22](#).
- ♦ Si observa una primera página distinta al acceder a la interfaz del usuario del Gestor de identidades, normalmente significa que la organización ha personalizado la aplicación. A medida que trabaje con Identity Applications, observará que otras funciones también se habrán personalizado.

En tal caso, pregunte al administrador del sistema en qué se diferencia la aplicación de identidad personalizada de la configuración por defecto descrita en esta guía.

Entrada por primera vez

Debe ser un usuario autorizado para poder entrar a la sesión en Identity Applications, por ejemplo a la consola. Si necesita ayuda para obtener un nombre de usuario y una contraseña para proporcionarlos al entrar a la sesión, consulte al administrador del sistema.

La primera vez que entre en Identity Applications, Identity Manager requiere que establezca los parámetros de seguridad para su cuenta, a fin de que pueda restablecer su contraseña en el futuro. Si olvida su contraseña e intenta restablecerla la próxima vez que entre, Identity Manager realiza una serie de preguntas configuradas a las que es preciso dar las respuestas correctas. Si la contestación coincide con la respuesta que guardó en esta página, puede restablecer la contraseña.

Para configurar las preguntas de seguridad durante la primera entrada:

- 1 Escriba el nombre de usuario y la contraseña y, a continuación, haga clic en **Entrada**.
- 2 La página de entrada redirige automáticamente a la página de **desafío-respuesta**.
- 3 Especifique las preguntas y respuestas para las preguntas de seguridad.

Configurar preguntas de seguridad

[Salir](#)

En el caso de que olvide la contraseña, puede acceder a su cuenta contestando las preguntas de seguridad.

Elija sus preguntas y respuestas que puedan servir para verificar su identidad en caso de que olvide la contraseña. Dado que las respuestas a estas preguntas pueden utilizarse para acceder a su cuenta, asegúrese de dar respuestas que no sean fáciles de adivinar o descubrir por otras personas.

Introduzca sus respuestas de seguridad

— Seleccione una pregunta de la lista —



— Seleccione una pregunta de la lista —



— Seleccione una pregunta de la lista —



— Seleccione una pregunta de la lista —



» Guardar respuestas

« Cancelar

- Haga clic en **Guardar respuestas** y se le redirigirá a la consola.

Respuesta a la comprobación de configuración regional preferida

Si se le pide que seleccione su configuración regional preferida al entrar, significa que el administrador ha configurado Identity Applications para realizar una comprobación de idioma en los navegadores de los usuarios. Esto podría ser necesario para garantizar que el contenido que recibe se muestra en un idioma compatible.

Si se le pide que añada una configuración regional, abra la lista **Configuraciones regionales disponibles**, seleccione una y haga clic en **Añadir**. Para obtener más información, consulte [Adición de un nuevo idioma a Identity Applications](#).

Solución de problemas de entrada a la sesión

Esta sección proporciona soluciones para los siguientes tipos de problemas comunes de entrada a la sesión:

- ♦ [“Si olvida la contraseña” en la página 22](#)
- ♦ [“Si tiene problemas para entrar a la sesión” en la página 23](#)
- ♦ [“Si el sistema le solicita información adicional” en la página 23](#)

Si olvida la contraseña

Si ha olvidado la contraseña, puede utilizar el enlace **Contraseña olvidada** para obtener ayuda. Cuando el sistema solicita que entre a la sesión, este enlace aparece por defecto en la pantalla. Puede usar este enlace si el administrador del sistema ha configurado una directiva de contraseña adecuada para usted.

- 1 Cuando el sistema solicite que entre a la sesión, haga clic en el enlace **Contraseña olvidada**.
- 2 Escriba el nombre de usuario y haga clic en **Enviar**.

Si Identity Manager responde que no encuentra una directiva de contraseñas para usted, pídale ayuda al administrador del sistema.

- 3 Responda a las preguntas de seguridad que se muestran. En Identity Manager es preciso responder a las preguntas configuradas. Si la contestación coincide con la respuesta que guardó anteriormente, puede restablecer la contraseña. Haga clic en **Enviar**. Por ejemplo:

Responda a las preguntas de verificación para obtener ayuda con su contraseña. Dependiendo de cómo haya configurado su directiva de contraseñas el administrador del sistema, podrá ocurrir lo siguiente:

- ♦ Que reciba un correo electrónico con la contraseña.
- ♦ Que el programa le solicite que restablezca la contraseña.

Si tiene problemas para entrar a la sesión

Si no puede entrar a la sesión, asegúrese de que está utilizando el nombre de usuario adecuado y de que ha escrito la contraseña correctamente (compruebe la ortografía, si hay letras en mayúscula y minúscula, etc.). Si los problemas persisten, póngase en contacto con el administrador del sistema. Resultaría útil que pudiera proporcionar información sobre el problema que tiene, por ejemplo los mensajes de error.

Si el sistema le solicita información adicional

Es posible que en cuanto entre, se le pida otro tipo de información. Depende de cómo haya configurado su directiva de contraseña (si existe) el administrador del sistema. Por ejemplo:

- ♦ Si es la primera vez que entra a la sesión, se le pedirá que defina las preguntas y las respuestas de seguridad
- ♦ Si la contraseña ha caducado, se le pedirá que la restablezca

Cierre de la sesión

Cuando haya terminado de trabajar en la consola y otras aplicaciones de Identity Applications, debe salir de la sesión. En la consola, haga clic en su nombre de usuario en la esquina superior derecha y seleccione **Salir**.



Personalización de la consola

Identity Applications proporciona muchas opciones para cambiar la presentación de la *consola* y después guardarla como una vista personalizada. Por ejemplo, puede añadir widgets y cambiar su posición en función de sus intereses. También puede configurar los campos del widget y personalizarlos. Este documento le ayudará a comprender las distintas opciones para personalizar la *consola*.

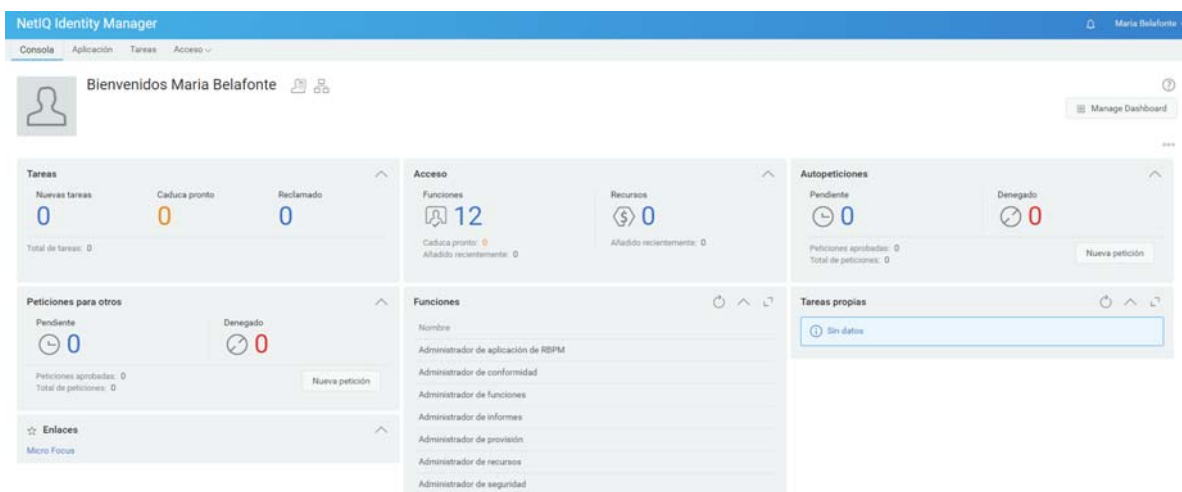
3 Gestión de widgets y diseños

Los widgets son objetos de la consola diseñados para ofrecer información específica a un usuario para una actividad concreta. Por ejemplo, el widget **Tareas** proporciona información acerca de las nuevas tareas, las tareas reclamadas o las tareas que se espera que caduquen en breve. De igual forma, puede haber muchos otros widgets que se pueden configurar en la consola.

Los administradores que dispongan de acceso la página **Valores de configuración** pueden aprovisionar widgets para un usuario, un grupo, un contenedor o una función desde **Su ID > Valores de configuración > Widgets de la consola**.

Para personalizar la consola, diríjase a **Consola** y haga clic en **...**.

Figura 3-1 Personalizar la consola



Utilice las siguientes opciones para personalizar la consola:

Figura 3-2 Opciones de personalización



Widgets

Permite añadir widgets a la consola. Véase [“Adición de un widget” en la página 29](#).

Disposición

Permite cambiar el diseño de la consola. Véase [“Cambio del diseño de la consola.” en la página 28](#).

Cancelar

Cancela todos los cambios realizados en la consola.

Guardar

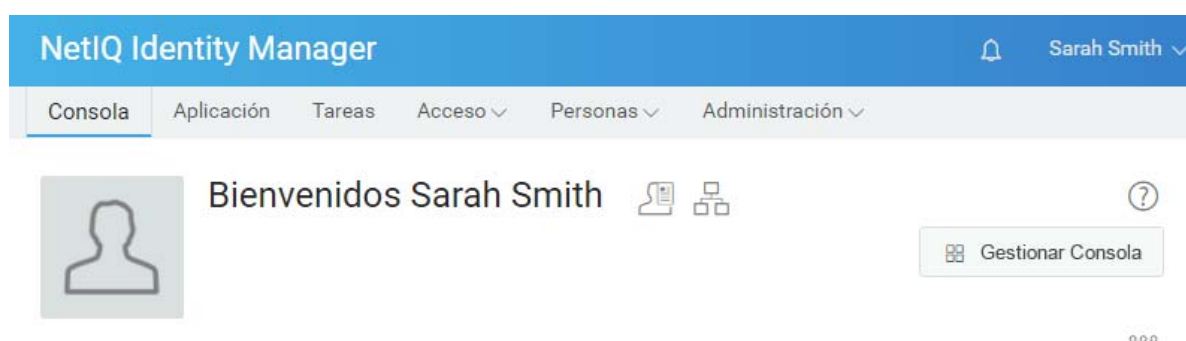
Guarda los cambios y los aplica a la consola.

Gestión de la consola global

La consola global incluye un conjunto de widgets que aparecerán en la consola de cada usuario del sistema. Los usuarios pueden ver estos widgets según el acceso del que dispongan (aprovisionado por un administrador). La opción **Editar consola** permite añadir, modificar o eliminar widgets de la consola global.

Nota: se le debe añadir como Trustee para que pueda utilizar la opción **Editar consola**.

Figura 3-3 Ejemplo de consola global



El administrador puede añadir a cualquier usuario, grupo, contenedor o función como Trustee para administrar la consola global. Para modificar los Trustees que pueden gestionar la consola, acceda a **Su ID > Valores de configuración > Acceso** y haga clic en **Consola global** en la lista. Para obtener más información acerca de cómo modificar el acceso a la configuración, consulte [Managing Dashboard Widgets](#) (Gestión de widgets de la consola) en [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Cambio del diseño de la consola.

Identity Applications permite modificar el diseño de la apariencia de los widgets en la consola.

- 1 Acceda a **Consola** y haga clic en **ooo**.
- 2 Seleccione **Disposición**.
- 3 Seleccione el diseño que desee ver en la consola.

Figura 3-4 Cambio de diseño

EDITAR CONSOLA

×

Título

Consola

Estructura

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

3-9 (12/6-6)

Importante: para aplicar los cambios, haga clic en **Guardar**.

Adición de un widget

Para añadir un widget nuevo a la consola, diríjase a **Consola**, haga clic en **⋮** y seleccione **Widgets**.

Figura 3-5 Adición de widgets

AÑADIR NUEVO WIDGET

×

General

IDM

IG

Adición de widgets generales

La categoría **General** permite añadir widgets a la consola que no sean widgets estándar de Identity Manager. Puede especificar la URL de la API REST del widget requerido y mostrar la información necesaria en forma de gráficos de líneas, sectores o tablas.

- 1 Seleccione cualquiera de los siguientes tipos de widget de la lista:
 - ♦ **Gráfico de líneas:** muestra la información solicitada para el elemento seleccionado en forma de gráfico de líneas.
 - ♦ **Enlaces:** permite añadir enlaces de uso frecuente para acceder a ellos rápidamente.
 - ♦ **Gráfico de sectores:** muestra la información solicitada para el elemento seleccionado en forma de gráfico de sectores.
 - ♦ **Tabla:** muestra la información solicitada para el elemento seleccionado en forma de tabla.
- 2 Haga clic en  para configurar el widget añadido a la consola.
- 3 (Condicional) Para los widgets de **Gráfico de líneas**, **Gráfico de sectores** y **Tabla**, especifique la siguiente información:
 - ♦ **Título:** especifique el nombre del widget que se mostrará en la consola.
 - ♦ **URL:** especifique la URL de la API REST del widget requerido que desea mostrar en la consola.
 - ♦ **Elemento raíz:** especifique el elemento del código de la API REST para el que desea mostrar un gráfico. En este campo se distingue entre mayúsculas y minúsculas. Debe introducir exactamente el mismo nombre que se menciona en el código de la API REST.
 - ♦ **Columnas:** especifique las columnas que desea mostrar en el widget. Puede añadir varias columnas. **Título** especifica el nombre de visualización de una columna. **Vía** especifica el nombre de columna, tal y como se menciona en la API REST. En el campo **Vía** se distingue entre mayúsculas y minúsculas. Debe introducir exactamente la misma cadena del código de la API REST.

A continuación, se muestra un código de ejemplo de la API REST para la página **Funciones**:

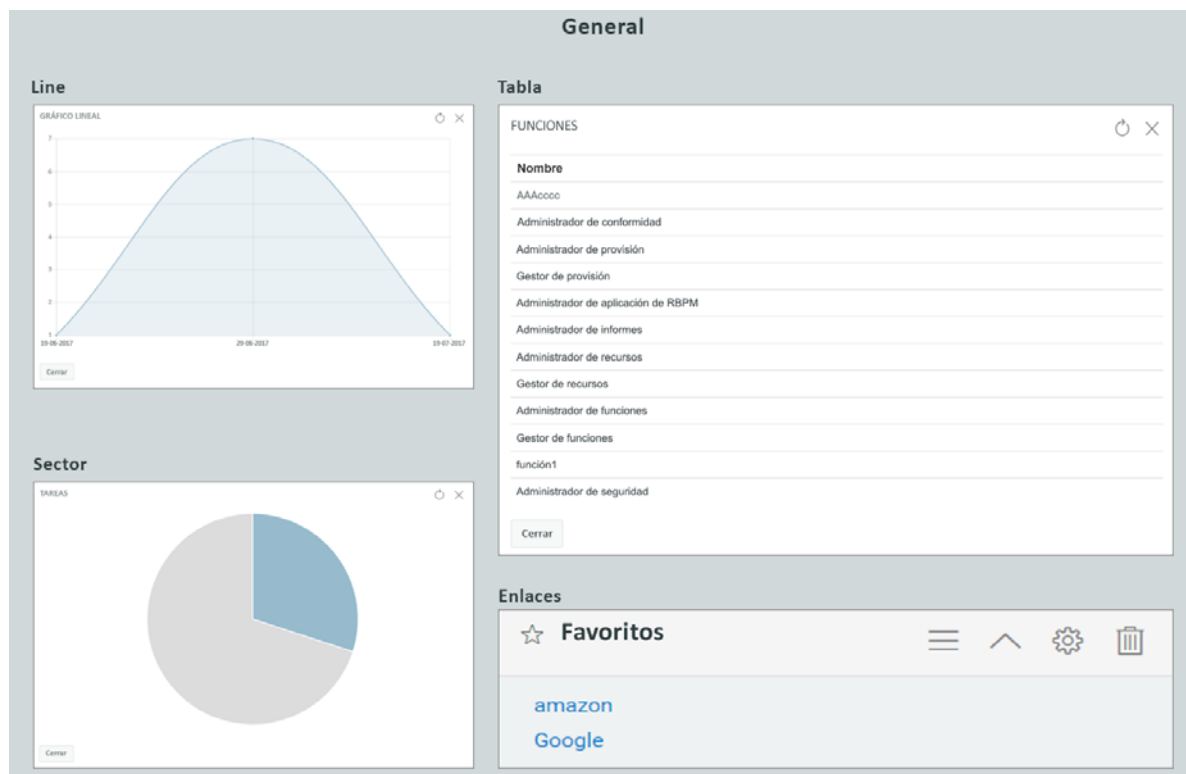
```
{
  "total": 12,
  "nextIndex": 0,
  "token": "60045d6be10f4419a2da9fa728683b06",
  "assignments": [
    {
      "id":
      "cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
      application driver,cn=driverset1,o=system",
      "name": "AAAcxxx",
      "description": "afasfdsf",
      "entityType": "role",
      "link": "/IDMProv/rest/access/assignments/item",
      "bulkRemovable": "true",
      "categories": [
        {
          "categoryId": "default",
          "categoryName": "Default"
        }
      ]
    }
  ]
}
```

En este ejemplo, assignments es el elemento raíz y name es la columna seleccionada para indicar que se mostrará en el widget. También es posible establecer un marcador a cualquier URL a la que desee acceder desde la consola.

- 4 (Condicional) Para los widgets de **Enlaces**, especifique el **Título** de los enlaces y añada los enlaces a los que desee acceder desde la consola.
- 5 Haga clic en **Guardar** para aplicar los cambios.

A continuación, se muestran widgets de gráficos y enlace de ejemplo que se pueden añadir a la consola:

Figura 3-6 Ejemplo de widgets generales



Adición de widgets de Identity Manager

La categoría **IDM** permite añadir widgets estándar o widgets específicos de Identity Manager a la consola.

Por ejemplo,

- ♦ **Acceso:** muestra el número de funciones y recursos e información adicional acerca de ellos.
- ♦ **Petición para otros usuarios:** muestra el número de peticiones pendientes y denegadas de otros usuarios y permite crear una petición para esos usuarios.
- ♦ **Autopeticiones:** muestra el número de peticiones pendientes y denegadas y permite crear una petición nueva.
- ♦ **Tareas:** muestra el número de tareas nuevas y de tareas pendientes o las tareas que están a punto de caducar.

Para configurar estos widgets, consulte la [“Configuración de un widget” en la página 33](#).

Importante: para aplicar los cambios, haga clic en **Guardar**.

Adición de widgets de control de identidad

Para utilizar los widgets de control de identidad, debe instalar y configurar Identity Governance con la consola de Identity Manager.

La categoría IG permite añadir widgets estándar o widgets específicos de Identity Governance a la consola. Por ejemplo:

Tareas de cumplimiento

Muestra el número de peticiones de acceso, las funciones empresariales y los errores de asignación de permiso del sistema.

Tareas de revisión

Muestra el número de revisiones pendientes y completadas del sistema.

Infracciones de separación de tareas (SoD)

Muestra el número de infracciones de separación de tareas (SoD) no revisadas, aprobadas o resueltas en el sistema.

Opciones del widget

Puede llevar a cabo las siguientes operaciones sobre los widgets:



Renovar

Actualiza el contenido del widget con la información más reciente.

Cambiar de posición

Permite mover el widget a través de la consola.

Configurar

Permite configurar las propiedades del widget. Para obtener más información, consulte [“Configuración de un widget” en la página 33](#).

Eliminar

Suprime el widget de la consola.

Comprimir

Ocultar la información de widget y solo muestra el título.

Abrir el widget a pantalla completa

Muestra la información del widget en el modo de pantalla completa.

Nota

- ♦ Las opciones **Actualizar** y **Abrir el widget a pantalla completa** solo se muestran para los widgets que pertenecen a la categoría **General**.
 - ♦ Para aplicar los cambios, haga clic en **Guardar**.
-

Configuración de un widget

Puede configurar todos los widgets que añada a la consola. Por ejemplo, puede habilitar o inhabilitar los campos de un widget, o bien cambiar el color de visualización de los campos.

1 Haga clic en  en el widget que desee configurar.

2 Modifique las propiedades del widget.

Por ejemplo, puede cambiar el título de un widget, o bien cambiar el color de la etiqueta de un campo del widget. También puede habilitar o inhabilitar un campo del widget en la página de propiedades.

3 Haga clic en **Aplicar** para ver los cambios en la consola.

Por ejemplo, puede modificar el widget de la tarea tal como se muestra a continuación:

Figura 3-7 Ejemplo de configuración del widget

TAREAS

×

Título

Tasks

Nuevas tareas

☒

▼

Caduca pronto

☒

▼

Reclamado

☒

▼

Tareas delegadas

☐

▼

Tareas reasignadas

☐

▼

Aplicar

Cancelar

Haga clic en **Aplicar** para ver los cambios en la consola.

Tareas

↕

⚙

🗑

^

Nuevas tareas

Caduca pronto

Reclamado

0

0

0

Total de tareas: 0

Para configurar widgets de la categoría General, modifique las opciones que aparecen mientras se añade el widget. Véase [“Adición de widgets generales” en la página 30](#).

Importante: para aplicar los cambios, haga clic en **Guardar**.



Gestión de sus permisos y del perfil de identidad

La consola de Identity Manager le ayuda a pedir acceso a los recursos y las funciones que necesita para completar sus tareas diarias. También puede realizar cualquier tarea que tenga asignada en el entorno de Identity Manager, como aprobar las peticiones de acceso. Los propietarios de los recursos y funciones pueden gestionar el proceso.

Cuando pide un permiso, se inicia un proceso en Identity Manager para revisar de forma eficaz la petición, de forma que pueda tener la función o el recurso que necesita. El administrador recibe una notificación por correo electrónico o en la consola para revisar su petición. En algunos casos, la petición también puede ser aprobada por otras personas de la organización.

Algunos usuarios también pueden realizar peticiones en nombre de otros usuarios, o actuar como apoderados de estos.

- ♦ [Capítulo 4, “Gestión de las peticiones de permisos”, en la página 37](#)
- ♦ [Capítulo 5, “Gestión de aplicaciones”, en la página 45](#)
- ♦ [Capítulo 6, “Gestión de las tareas”, en la página 49](#)
- ♦ [Capítulo 7, “Actuación en nombre de otra persona”, en la página 53](#)
- ♦ [Capítulo 8, “Gestión de delegaciones”, en la página 55](#)
- ♦ [Capítulo 9, “Gestión de la disponibilidad”, en la página 57](#)
- ♦ [Capítulo 10, “Gestión del perfil”, en la página 59](#)
- ♦ [Capítulo 11, “Gestión del organigrama corporativo”, en la página 61](#)
- ♦ [Capítulo 12, “Gestión de la contraseña”, en la página 69](#)

4 Gestión de las peticiones de permisos

En esta sección se proporcionan instrucciones para las siguientes actividades:

- “Visualización de los permisos” en la página 37
- “Petición de permisos” en la página 39
- “Visualización de peticiones” en la página 39
- “Revocación de permisos” en la página 41
- “Creación de un enlace interno a una petición” en la página 42

También puede consultar  para obtener información sobre la consola en relación con estas actividades.

Visualización de los permisos

Los permisos representan las cuentas, funciones o recursos que hay disponibles. Los permisos pueden ser asignados automáticamente por la organización o puede pedir permisos específicos. También puede heredar permisos indirectamente a través de relaciones de funciones o si es miembro de un grupo o contenedor.

Para ver las funciones y recursos a los que tiene acceso, seleccione en la consola:

Acceso > Permisos.

A continuación, puede seleccionar un permiso específico para obtener más información sobre esa función o recurso. El permiso también puede mostrar los motivos proporcionados durante su asignación. Para buscar un permiso concreto en una lista grande, escriba el nombre, el nombre completo o la descripción del permiso en el recuadro Buscar. También puede filtrar la lista.

Nota:

- Por defecto, puede ver las listas de permisos que se le han asignado o aprobado directamente. Sin embargo, puede variar en función de cómo haya configurado el administrador los ajustes de la página. Para obtener más información, consulte [User Settings](#) (Configuración del usuario) en [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager: Guía del administrador de Identity Applications).
 - Para ver los permisos hijo con los permisos aprobados o asignados, haga clic en .
-

Visualización de los detalles de los permisos

Seleccione el permiso para el que desea ver más detalles. La siguiente tabla indica los campos que se muestran para los permisos individuales:

Tabla 4-1 Campos del permiso y su descripción

Campos	Descripción
Descripción	La descripción de la función o el recurso.
Fecha en vigor	La fecha y la hora de la asignación del permiso.
Fecha de caducidad	La fecha después de la cual ya no se asignará el permiso al usuario. Solo se muestra para los permisos que tienen habilitada la opción de caducidad.
Razón	Especifica el motivo para asignar el permiso al usuario.
Permiso asignado mediante	Especifica quién asignó el permiso al usuario. Si se asigna una función al usuario directamente a través de un proceso de aprobación, puede ver la lista de aprobadores que aprobaron la petición de asignación en la opción Ver información de aprobación de función. Si el usuario hereda una función por pertenecer a un grupo o contenedor, se muestran los siguientes detalles en la opción Ver información de asignación de función a grupo: ♦ Petición de: especifica quién ha pedido el permiso. ♦ Descripción de la petición: la descripción proporcionada al pedir el permiso. ♦ Detalles del aprobador: haga clic en el enlace para ver la lista de aprobadores que aprobaron la petición de asignación de funciones.

Si es administrador de Identity Applications, puede ver los permisos de otros miembros del equipo en la pestaña **Otros**. Vaya a la pestaña **Otros** y busque por nombre de usuario o detalles de permiso.

- ♦ La búsqueda por usuario muestra todos los permisos asignados a ese usuario. Puede seleccionar un permiso específico para revisar los detalles, como la fecha asignada, quién asignó el permiso y si se ha indicado algún motivo para la asignación del permiso. Si desea información adicional, consulte la [Tabla 4-1 en la página 38](#).
- ♦ La búsqueda por permiso muestra una lista de todos los usuarios, tanto los individuales como los incluidos en un grupo o contenedor, que estén asignados a ese permiso.

Nota: los administradores de equipos y los supervisores no tienen permiso para buscar por detalles del permiso. Sin embargo, pueden ver los permisos de los miembros de su equipo buscando su nombre o descripción. Además, también se proporciona una búsqueda por nombre de usuario en la página para permitir la búsqueda y visualización de permisos de un miembro específico del equipo.

Para obtener más información, haga clic en  en la consola.

Petición de permisos

Para solicitar funciones y recursos, haga clic en [Acceso > Peticiones](#).

Antes de pedir permisos, tenga en cuenta las consideraciones siguientes:

- ♦ Podría tener la capacidad de pedir acceso en nombre de otro usuario. Por ejemplo, si es administrador del equipo, generalmente puede actuar en nombre de los miembros del equipo. El proceso es el mismo, excepto en que debe especificar que la petición es para **Otros** en lugar de un **Autoderecho**.
- ♦ Cuando especifique un permiso que desee pedir, no utilice signos de puntuación. Si el nombre del permiso que desea pedir incluye signos de puntuación, omítalos en la búsqueda.
- ♦ Para permisos diferentes, se requiere información distinta, dependiendo de cómo haya configurado el administrador el formulario del permiso. Si el permiso requiere información detallada, la consola le redirigirá a otra ventana cuando seleccione el permiso.
- ♦ Puede pedir varios permisos al mismo tiempo.
Sin embargo, si el formulario del permiso de una de las peticiones requiere tipos especiales de información, es posible que no pueda incluir ese permiso en una petición de varios permisos. Para pedir varios permisos al mismo tiempo, los formularios de petición de las distintas peticiones no deben requerir información detallada.
- ♦ Puede especificar la fecha de caducidad al solicitar un recurso o una función.

Para pedir permisos de Identity Governance:

*Solo se aplica a dos condiciones: si se ha habilitado la opción **Mostrar catálogo de IG en la página de petición** en la página **Configuración > Identity Governance** y cuando se pide el permiso como **Autoderecho**.*

- ♦ **Catálogos de IDM:** muestra todas las funciones, recursos y flujos de trabajo disponibles de Identity Manager.
- ♦ **Aplicaciones de IG:** muestra todas las aplicaciones recopiladas en Identity Governance. Puede seleccionar los permisos asociados con la aplicación seleccionada.
- ♦ **Funciones técnicas de IG:** muestra todas las funciones técnicas de Identity Governance. Seleccione las funciones de IG que desee pedir y especifique un motivo para pedir las.

Para obtener más información, haga clic en  en la consola.

Visualización de peticiones

Para ver el estado de una petición en curso y las peticiones completadas, seleccione en la Consola:

[Acceso > Historial de peticiones](#)

El administrador o supervisor de un equipo puede consultar el historial de peticiones de los demás miembros del equipo desde la pestaña **Otros**.

También puede generar un ticket del servicio de ayuda técnica para las peticiones pendientes.

- ♦ “Seguimiento de una petición” en la página 40
- ♦ “Cancelación de una petición” en la página 40
- ♦ “Generación de un ticket del servicio de ayuda técnica” en la página 41

Para obtener más información, haga clic en ⓘ en la consola.

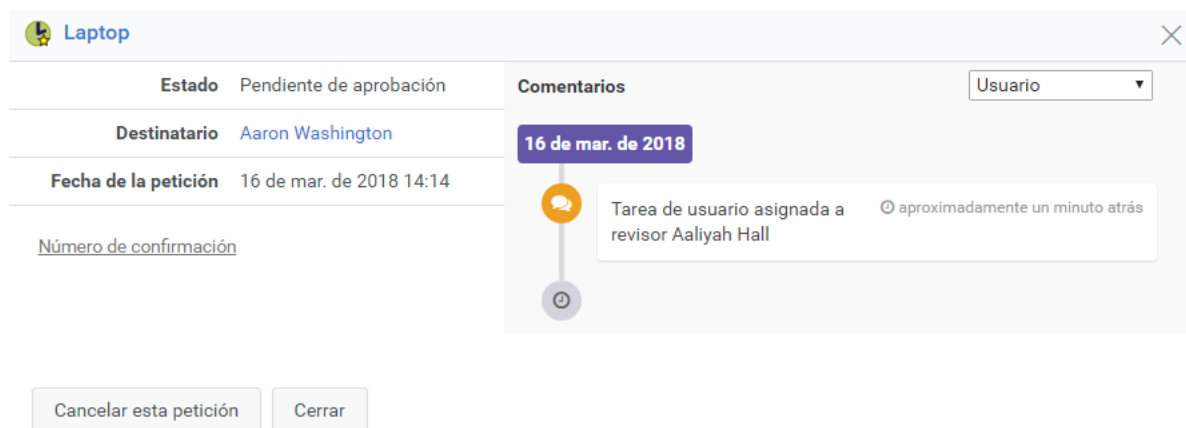
Seguimiento de una petición

Para cada petición, puede ver no solo las acciones que ha llevado a cabo, sino también el flujo de trabajo implicado en la aprobación o denegación de la petición. Cada paso del proceso incluye una marca horaria.

Nota: si pide aplicaciones o funciones técnicas en las pestañas **Aplicaciones de IG** o **Funciones técnicas de IG**, no es posible realizar un seguimiento de esas peticiones mediante la página **Historial de peticiones**. Para realizar un seguimiento de las peticiones de IG, puede añadir la URL de historial de IG en la página **Aplicaciones** de la consola.

Para realizar el seguimiento de una petición pendiente, seleccione la petición para cambiar el menú que aparece en la parte superior derecha a **Usuario y sistema**. La consola muestra el estado actual de la petición en el proceso de aprobación.

Figura 4-1 Seguimiento de una petición



Cancelación de una petición

Puede cancelar una petición *pendiente* en **Historial de peticiones**. Seleccione la petición en la lista y seleccione **Cancelar esta petición** en la ventana siguiente.

Generación de un ticket del servicio de ayuda técnica

Puede contactar con el servicio de ayuda técnica si necesita ayuda para un problema desatendido durante mucho tiempo.

Puede generar un ticket del servicio de ayuda técnica desde las siguientes ubicaciones:

- ♦ **Acceso > Petición**, haga clic en **Crear ticket del servicio de ayuda técnica**.
- ♦ **Aplicaciones**, haga clic en **Crear ticket del servicio de ayuda técnica**.
- ♦ **Acceso > Historial de peticiones**, haga clic en  en la petición para la que desea generar un ticket de servicio de ayuda técnica.

Para obtener más información, haga clic en  en la consola.

Los miembros del servicio de ayuda técnica reciben una notificación sobre el ticket. Recibirá una notificación sobre el ticket después de que se resuelva o se cierre.

Revocación de permisos

Si ya no necesita acceso a una función o un recurso, puede revocar el permiso a esa función o recurso. Para revocar un permiso, abra **Acceso > Permisos**, seleccione el permiso requerido y especifique un motivo para revocarlo.

También puede revocar un permiso en nombre de otros usuarios. Por ejemplo, si el miembro del equipo se ha trasladado del departamento 1 al 2 y ya no necesita acceso a un recurso determinado, Identity Manager permite revocar el permiso a ese usuario. Para revocar un permiso, seleccione **Otros** y elimine el permiso. Puede revocar varios permisos simultáneamente. Existe la posibilidad de añadir los permisos a una cola para revisarlos antes de tomar la decisión de revocarlos.

Solo el administrador y el supervisor del equipo pueden revocar permisos para otros usuarios. Un administrador puede revocar los permisos de cualquier usuario de la organización, mientras que un supervisor de equipo solo puede revocarlos para los miembros de su equipo.

Puede revocar los permisos para otros usuarios a través de los siguientes procedimientos:

Permisos de otros usuarios

Autoderecho ☒ Otros

 Por usuario  Por permiso

- ♦ **Busca según el usuario:** permite buscar un usuario y revocar sus permisos. Puede revocar un permiso para el usuario directamente o agregarlo a una cola. Una cola es un área de trabajo permanente donde se pueden almacenar temporalmente los permisos que puede revisar y revocar si es necesario. A continuación, puede buscar los otros permisos que desee revocar para ese usuario y añadirlos a la cola. Esto permite revocar todos los permisos a la vez.

- ♦ **Por permiso:** permite buscar un permiso específico. Si selecciona un permiso, se mostrará una lista de todos los usuarios que dispongan de él. Puede revocar directamente el permiso del usuario seleccionado o añadirlo a una cola y revocar dicho permiso para varios usuarios al mismo tiempo.

Supervisor de equipo: si usted es supervisor de equipo, puede revocar los permisos de los miembros del equipo mediante la pestaña **Otros**. Asegúrese de que dispone de los permisos necesarios para revocar los permisos de otros usuarios.

Administrador: si es administrador, puede añadir permisos de revocación para un supervisor de equipo. Por ejemplo, si desea añadir una función de revocación de un permiso de usuario para el supervisor del equipo. Vaya a **Personas > Equipos** y edite los permisos del equipo para habilitar los permisos de revocación de un supervisor del equipo.

Figura 4-2 Ejemplo para añadir permisos de revocación a un supervisor del equipo



Esta opción permite al supervisor del equipo revocar la función seleccionada de los miembros del equipo.

Nota: si revoca un permiso, la lista de permisos podría no reflejar el cambio inmediatamente. El motivo puede ser que el permiso esté asociado a un proceso de revocación que quizá tarde un tiempo en procesarse. Actualice la lista para ver los cambios.

Para obtener más información, haga clic en  en la consola.

Creación de un enlace interno a una petición

Identity Applications permite crear un enlace interno a una petición de proceso específica (también conocida como petición de aprovisionamiento). Esta característica ofrece a los administradores la capacidad de enviar una URL de petición de proceso específica a un empleado, de forma que este pueda pedir el proceso rápidamente sin tener que pasar por la consola de Identity Manager. Cuando se crea un enlace profundo a una petición de proceso, el formulario de petición se muestra en el cuerpo de la página, junto con el encabezado de Identity Applications.

Cuando se solicite un permiso, la petición aparece en la página **Acceso > Historial de peticiones** del usuario que realiza la petición, así como en la página **Tareas** del revisor.

La URL utilizada para el enlace profundo a una petición de proceso utiliza el siguiente formato:

- ♦ Para formularios legados:

```
https://<server:port>/IDMProv/
requestForm.do?uid=<PRD_ID>&aqua=true&idmdash=true&recipient=<recipient>&jsa=<operation_type>
```

A continuación se muestra un ejemplo de una URL a una definición de petición de provisión:

`https://testserver:8543/IDMProv/requestForm.do?uid=cn=request mobile approval app,cn=requestdefs,cn=appconfig,cn=user application driver,cn=driverset1,o=system&aqua=true&idmdash=true&recipient=&jsa=%7B%22submit%22%3A%22submitThenOpener%283000%29%22%2C%22cancel%22%3A%22window.close%28%29%22%7D`

- ♦ Para los nuevos formularios JSON:

`https://<server:form_renderer_port>/forms/#!/form/details?id=<formID>&recipient=<recipient>&pid=<workflowID>&sid=IDM&uri=<forms_uri>&formContainer=RequestForms&locale=<language>`

A continuación se muestra un ejemplo de una URL a una definición de petición de provisión:

`https://testserver:18600/forms/#!/form/details?id=cn%3DHelp-desk%20Request%20Form,cn%3DWorkflowForms,cn%3Dappconfig,cn%3DUser%20Application%20Driver,cn%3Ddriverset1,o%3Dsystem&recipient=&pid=cn%3Dhelpdeskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20driver,cn%3Ddriverset1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&formContainer=RequestForms&locale=en`

5 Gestión de aplicaciones

Como administrador de Identity Applications, puede modificar la página **Aplicaciones** para que muestre todas las aplicaciones, las actividades y los permisos a los que desea que accedan los usuarios. Por defecto, Identity Applications incluye una categoría **Elementos de la página principal** que no se puede suprimir.

Después de completar los cambios, haga clic en **Edición finalizada** para volver a **Aplicaciones**.

Creación de elementos destacados

Puede crear tantos permisos y aplicaciones como quiera añadir a la página **Aplicaciones**. No es necesario añadir estos elementos a **Elementos de la página principal** ni a otras categorías de **Aplicaciones**.

- 1 (Condicional) Para crear un elemento nuevo, haga clic en + en las pestañas **Aplicaciones** o **Permisos**.
- 2 Complete el formulario para una aplicación o un permiso. Consulte [“Adición de una aplicación” en la página 45](#) o [“Adición de un permiso” en la página 46](#).

Nota: debe especificar un valor para todos los campos que tienen un asterisco (*), como el nombre y la descripción de la aplicación.

- 3 (Opcional) Arrastre y suelte la aplicación o el permiso en una categoría.
- 4 (Condicional) Para modificar un elemento existente, seleccione el icono de edición del título y, a continuación, actualice los valores.

Adición de una aplicación

Para añadir una aplicación, especifique los siguientes detalles:

(Condicional) Añadir a categoría

Permite especificar la categoría de esta aplicación.

Nombre

Permite especificar el nombre de la aplicación.

Descripción

Permite especificar la naturaleza de la aplicación.

(Opcional) Imagen

Permite especificar un logotipo o una imagen para una aplicación.

Enlazar

Permite especificar un enlace para esta aplicación. Consulte [“Creación de un enlace interno a una petición” en la página 42](#).

(Opcional) URL de API

Permite especificar la URL del puesto final REST con datos JSON que proporcionan detalles adicionales, como el valor de los parámetros y un distintivo. Consulte la documentación para obtener más detalles.

Adición de un permiso

Para añadir un permiso, especifique los siguientes detalles:

Permisos

Permite especificar el permiso. Puede ser una función, un recurso o una PRD.

(Condicional) Añadir a categoría

Permite especificar la categoría de esta aplicación.

(Opcional) Imagen

Permite especificar un logotipo o una imagen para una aplicación.

Adición, modificación o supresión de categorías

Los elementos de **Aplicaciones** se pueden organizar según categorías lógicas. Puede crear cualquier número de categorías que necesite su organización. También puede reordenar los mosaicos dentro de una categoría o moverlos a otra distinta.

Adición de una categoría

1 Seleccione **Nueva categoría**.

Identity Manager añade la categoría al final de los grupos de categorías. Quizá tenga que desplazarse para ver la categoría añadida.

2 Especifique el nombre de la nueva categoría.

3 Haga clic en + y, a continuación, seleccione **Aplicación** o **Permiso**.

4 Complete el formulario para la aplicación o el permiso.

Nota: debe especificar un valor para todos los campos que tienen un asterisco (*), como el nombre y la descripción de la aplicación.

5 Seleccione **+Añadir**.

Modificación de una categoría

Existen varias maneras de modificar una categoría:

- ♦ Añadir mosaicos para aplicaciones y permisos arrastrándolos y soltándolos desde las secciones **Nuevos elementos** y **Permisos**, situados en el lado derecho de la página
- ♦ Eliminar una aplicación o un permiso seleccionando el icono de papelera en el título del elemento
- ♦ Cambiar los valores de configuración de un elemento

- ♦ Cambiar el nombre de la categoría
- ♦ Reordenar los elementos dentro de la categoría

Supresión de una categoría

Para suprimir una categoría, seleccione el icono de papelera a la derecha del nombre de la categoría.

6 Gestión de las tareas

Si es el responsable de aprobar o denegar los permisos pedidos en Identity Manager, puede utilizar la consola para gestionar las tareas, igual que en la aplicación de usuario. Puede aprobar o denegar peticiones de una en una, o aprobar o denegar varias peticiones sencillas que no requieran información detallada en lotes.

Para revisar las peticiones pendientes, haga clic en **Tareas**.

Como alternativa, podría recibir una notificación por correo electrónico con un enlace que le permite aprobar o rechazar una petición en un mensaje de respuesta.

Antes de llevar a cabo alguna acción en las peticiones de usuario, tenga en cuenta las consideraciones siguientes:

- ♦ Puede seleccionar varias tareas para aprobarlas o denegarlas en lote.
- ♦ Para una petición más compleja que requiera información detallada, en la consola no se muestran casillas de verificación. Debe aprobar o denegar dichas peticiones seleccionando cada petición y completando los formularios.
- ♦ Si selecciona una petición para aprobar o denegar más compleja, es posible que la consola deba abrir el formulario de petición en una pestaña independiente del navegador.
- ♦ En general, debe proporcionar un comentario que explique por qué desea aprobar o denegar las tareas seleccionadas.

Visualización de las tareas

Para gestionar las tareas, seleccione **Tareas**. Para ver las tareas asignadas a otros usuarios, haga clic en **Otros**.

Si actúa como apoderado o delegado para las tareas de otros, puede completar tareas que estén asignadas a otro usuario. Para obtener más información sobre las asignaciones de apoderado y de delegación, consulte [Actuación como apoderado](#).

Aprobaciones de IDM: *solo se aplica si se ha habilitado la opción **Mostrar aprobaciones de IG** en la página de tareas en la página **Configuración > Identity Governance**.*

Esta pestaña muestra todas las tareas de Identity Manager. Por defecto, muestra todas las tareas de **Tareas propias**. Para ver otras tareas con una función adecuada, haga clic en **Tareas de otros**.

- ♦ Puede buscar sus tareas mediante los filtros **Tareas reasignadas**, **Tareas devueltas** o **Tareas delegadas**. Si usa el filtro **Tareas delegadas** para la opción **Autoderecho**, solo se muestran las tareas que tiene delegadas.
- ♦ Si es administrador, también puede filtrar las tareas con los filtros **Asignado a mí** y **Destinatarios como yo**.
- ♦ Si busca otras tareas, puede utilizar los filtros **Tareas devueltas**, **Tareas reasignadas** o **Tareas delegadas**. Si usa el filtro **Tareas delegadas** para **Otros**, se muestran todas las tareas que estén delegadas a otros usuarios en el sistema.

- ♦ También puede ajustar la búsqueda de tareas según las tareas que se hayan producido en el sistema:
 1. Seleccione .
 2. (Condicional) Para ver las tareas creadas durante un período determinado, especifique dicho período en los campos **Semanas**, **> Días** u **Horas**.
 3. (Condicional) Especifique el estado de la tarea que desea usar como filtro.
 4. Haga clic en **Filtro**.
- ♦ Si utiliza el servicio de ayuda técnica, puede emplear el filtro **Tareas del servicio de ayuda técnica** para ver la lista filtrada. Para gestionar la tarea de servicio de ayuda técnica, consulte la ayuda de la consola.

En ocasiones, quizás deba aprobar elementos si en la directiva Petición de acceso se le especifica como aprobador de las peticiones. Estos elementos pedidos de aprobación aparecen en la pestaña **Aprobaciones**.

Aprobaciones de IG: *solo se aplica si se ha habilitado la opción **Mostrar aprobaciones de IG en la página de tareas** en la página **Configuración > Identity Governance**.*

Esta pestaña muestra todas las tareas de aprobación pendientes para Identity Governance. Puede reasignar las tareas a otros usuarios mediante la opción **Reasignar**.

Gestión de la aprobación o el rechazo de las peticiones

En algunas organizaciones, un grupo de usuarios puede ser responsable de revisar y aprobar o denegar las peticiones de acceso. Si se da el caso, cada miembro del grupo recibe las mismas peticiones. Por ejemplo, el equipo de Servicios de TI puede ser responsable de todas las peticiones relacionadas con las telecomunicaciones y los equipos informáticos. Cuando un nuevo empleado solicita un teléfono móvil, la petición se asigna a todos los miembros del equipo de Servicios de TI. Cualquier miembro del equipo puede completar la petición.

Puede realizar cualquiera de las siguientes tareas sobre la petición:

Reclamar la petición

Es posible **reclamar la responsabilidad** de una petición y actuar sobre la tarea inmediatamente o más tarde. Independientemente de cuándo actúe sobre la tarea, los demás miembros del grupo dejarán de ver dicha petición en sus **Tareas**.

Liberar la petición

Si no desea actuar sobre la petición que ha reclamado, puede liberar la petición.

Reasignar la petición

Una tarea que se le asigne puede asignarse a otro usuario de la organización. Para reasignar tareas se tienen en cuenta las siguientes consideraciones:

- ♦ Si no va a poder completar la tarea, puede reasignársela a su supervisor. Seleccione la petición en la pestaña **Autoderecho** y, a continuación, seleccione **Reasignar**. La tarea se reasigna automáticamente a su supervisor.

- ♦ Como supervisor de equipo, solo puede reasignar tareas propias a su propio supervisor. Sin embargo, si desea reasignar una tarea asignada a un miembro de su equipo, puede hacerlo mediante la pestaña **Otros**. Vaya a la pestaña **Otros**, seleccione la casilla de verificación de la tarea correspondiente y, a continuación, haga clic en **Reasignar**. En el menú desplegable **Asignar a**, seleccione el miembro del equipo al que desea reasignar la tarea, proporcione un comentario para la reasignación y haga clic en **Reasignar**. La tarea se reasigna al miembro del equipo elegido.
- ♦ Si no ha actuado sobre la tarea en un periodo tiempo especificado, puede ocurrir lo siguiente:
 - ♦ Un administrador puede reasignar la tarea a otro usuario. Los administradores tienen permiso para reasignar tareas a cualquier usuario de la organización.
 - ♦ El supervisor del equipo puede reasignar la tarea a otro miembro del equipo. Asegúrese de que el gestor del equipo tiene habilitado el permiso Gestionar tarea de destinatario en el momento de crear el equipo.
Esto solo se aplica si la opción **Miembros** se usa para añadir miembros al equipo en el momento de crear el equipo. Para obtener más información, consulte [“Creación de un equipo” en la página 84](#)

Nota: si usa la opción **Todos los usuarios** o **Relación** para crear un equipo, el administrador del equipo no puede reasignar las tareas a otro miembro del equipo.

- ♦ El usuario del servicio de ayuda técnica puede volver a asignar la tarea a su supervisor hasta el nivel de jerarquía definido en la página **Valores de configuración**. El administrador configura la jerarquía de los supervisores.

Si se le reasigna una tarea y no puede aceptarla, existe la posibilidad de devolvérsela al usuario que se la ha asignado.

Devolver la petición

Si no desea actuar sobre una petición que se le ha reasignado, puede devolverla. Identity Applications asigna la tarea automáticamente al aprobador real.

Nota: solo se pueden devolver las peticiones reasignadas.

Para obtener más información, haga clic en ⓘ en la consola.

Gestión de las tareas del servicio de ayuda técnica

Para cada ticket del servicio de ayuda técnica del sistema, se generan tareas del servicio de ayuda técnica. Según el ejemplo de la [“¿Cómo funciona el servicio de ayuda técnica?” en la página 16](#), el ticket de Emilia crea una tarea del servicio de ayuda técnica en la página **Tareas** de Elena. Elena puede tomar las medidas necesarias para esta tarea del servicio de ayuda técnica.

Si es usuario del servicio de ayuda técnica, seleccione el ticket que requiere su acción. Lleve a cabo una de las acciones siguientes para el ticket de servicio de ayuda técnica seleccionado:

Actualización

Actualiza el ticket con el comentario especificado.

Completado

Completa el ticket del servicio de ayuda técnica con su comentario sobre la resolución.

Cancelar

Cierra el ticket del servicio de ayuda técnica con el comentario especificado.

Nota: puede **Reclamar** o **Liberar** la tarea del servicio de ayuda técnica. Si reclama un ticket del servicio de ayuda técnica de la lista de tareas, el ticket aparecerá en sus **Tareas propias**.

Para obtener más información, haga clic en  en la consola.

7 Actuación en nombre de otra persona

En algunas organizaciones, puede que se le permita completar tareas como apoderado (proxy) o delegado de otra persona. Por ejemplo, un asistente personal puede realizar acciones de apoderado para su superior. Asimismo, si un compañero se encuentra de baja por maternidad o paternidad, se le podría asignar la tarea de actuar en su nombre.

- ♦ [“Visualización de las asignaciones del apoderado” en la página 53](#)
- ♦ [“Actuación como apoderado” en la página 53](#)
- ♦ [“Gestión de asignaciones de apoderado” en la página 53](#)

Para obtener más información, haga clic en ⓘ en la consola.

Visualización de las asignaciones del apoderado

Para ver las asignaciones de apoderado, seleccione en la consola:

Acceso > Asignaciones de apoderado (proxy).

Actuación como apoderado

Un administrador puede asignarle la tarea de actuar como apoderado de otro usuario. Cuando esto ocurre, en la aplicación se añade una opción de apoderado (proxy) en el menú de la cuenta, en la esquina superior derecha.

Su ID > Apoderado como

Por ejemplo, Sara Suárez es encargada del departamento de Relaciones con los clientes. Identity Applications incluye un equipo de Relaciones con los clientes en el que Sara Suárez es administradora del equipo. Sara puede actuar en nombre de María Belafonte, que es miembro de su equipo. En la consola, selecciona **ssuarez > Apoderado como** y especifica **mbelafonte**.

Gestión de asignaciones de apoderado

Como administrador o administrador de equipo puede crear, modificar y suprimir una asignación. Para que un administrador de equipo pueda gestionar las asignaciones de apoderado para un equipo, debe configurar el equipo correctamente. El administrador de equipo puede crear asignaciones solo para los miembros del equipo.

8 Gestión de delegaciones

En algunas organizaciones, se permite la delegación de tareas a otro usuario. Si se le han delegado las tareas de otro usuario de la organización o usted ha delegado las suyas, puede consultar la información de delegación en la sección [Administración > Delegación](#).

Puede consultar las tareas delegadas en la página [Tareas](#). Las tareas con el icono  indican que se han delegado.

Importante: la creación de asignaciones de delegación también requiere que se especifiquen los detalles de disponibilidad. Puede proporcionar los detalles de disponibilidad al crear la asignación de delegación, o bien crear una delegación y, a continuación, especificar los detalles de disponibilidad en una acción independiente. Esto depende de si el administrador ha habilitado los ajustes necesarios, en cuyo caso verá la opción [No disponible desde](#) en la página [Crear asignación de delegado](#). Sin embargo, si no puede ver la opción [No disponible desde](#), debe especificar los detalles de disponibilidad en la página [Valores de disponibilidad](#) después de crear la asignación de delegación. Esto garantiza que la delegación funcione como se espera. Para obtener más información, haga clic en  en la consola.

9 Gestión de la disponibilidad

Es posible especificar las peticiones de recursos con una asignación de delegado en las que no podrá trabajar durante un período de tiempo concreto. Durante el período de tiempo en que no esté disponible para una petición concreta, el usuario delegado para actuar en esa petición puede trabajar en ella.

Para ver la disponibilidad, seleccione en la consola

Personas > Disponibilidad.

Antes de utilizar la acción **No disponible desde**, debe tener al menos una asignación de delegado en la que trabajar. Deberá pedir al supervisor de su equipo (o al administrador de aplicación de provisión) que cree asignaciones de delegado para usted.

Los ajustes globales relacionados con la delegación basada en disponibilidad se especifican mediante **Definir disponibilidad al crear una asignación de delegación** en **Valores > Personalización > Elementos de navegación > General**. Si prefiere no especificar su disponibilidad para cada definición de petición individual, puede utilizar la opción **No disponible** para Todas las peticiones en la acción Cambiar estado.

Para obtener más información, haga clic en ⓘ en la consola.

10 Gestión del perfil

Identity Applications ofrece una forma cómoda de mostrar y trabajar con la información de identidad. También permiten una respuesta más ágil por parte de la organización, ya que le da acceso a la información que necesita de otros usuarios cuando la necesita. Por ejemplo, es posible que necesite realizar una de estas acciones:

- ♦ Gestionar su propia cuenta de usuario directamente
- ♦ Buscar otros usuarios o grupos de la organización a pedido
- ♦ Visualizar la relación entre los usuarios y los grupos
- ♦ Ver listas de las aplicaciones a las que está asociado

El administrador del sistema es el responsable de configurar el contenido de Identity Applications para usted y el resto de personas de la organización. Los datos que podrá ver y las operaciones que podrá realizar, normalmente, vienen determinadas por los requisitos de su puesto de trabajo y su nivel de autorización.

Actualización de su perfil

Para ver y actualizar su perfil de identidad, seleccione en la consola:

[\[su ID\]](#) > **Mi perfil**

O,

Haga clic en  en la consola.

Esta página muestra sus funciones, recursos, grupo y supervisor. Debe tener acceso de administrador para editar la información o para ver el organigrama corporativo.

El perfil incluye opciones como su nombre, la dirección de correo electrónico y el número de teléfono. Esta página muestra los atributos de usuario habilitados con accesos de **búsqueda** y de **lectura**. Estas propiedades de acceso se pueden configurar en el nivel de abstracción de directorio (DAL). Para obtener más información, consulte [Attribute Properties](#) (Propiedades del atributo) en la [NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#) (Gestor de identidades de NetIQ: Guía del administrador para el diseño de las aplicaciones de identidad). La organización determina los valores que se pueden modificar. Por ejemplo, es posible que pueda cambiar su número de teléfono, pero no sus apellidos.

11 Gestión del organigrama corporativo

La consola de Identity Manager ofrece un método sencillo para buscar una entidad en la organización y mostrar el organigrama corporativo (una entidad puede ser un usuario, un grupo o una entidad personalizada definida por el administrador). El organigrama corporativo muestra la jerarquía de las relaciones, por ejemplo, supervisor-empleado, pertenencia a un grupo o grupos de usuarios, entre las entidades de la organización.

Por defecto, la página **Organigrama corporativo** de la consola muestra la posición de una entidad de usuario dentro de la organización y su relación de jerarquía con otras entidades de usuario, según las relaciones definidas por el administrador. Para obtener más información acerca de los ajustes por defecto de la página del organigrama corporativo, consulte [Personalización de las vistas](#). Para obtener más información sobre cómo ver el organigrama corporativo de las entidades que no son de usuario, consulte [Viewing the Organization Chart of an Object](#) (Visualización del organigrama corporativo de un objeto) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Al organigrama corporativo también se le denomina simplemente "organigrama". En la consola se pueden emplear ambos términos.

Visualización de un organigrama corporativo

Por defecto, el administrador de seguridad y el administrador de provisión pueden ver el organigrama corporativo de todas las entidades del sistema.

Estos son los métodos que puede emplear para desplazarse por el organigrama corporativo de entidades de usuario:

- Diríjase a **Personas > Organigrama corporativo**. En esta página se muestra el organigrama del usuario que ha entrado a la sesión de acuerdo con las relaciones por defecto configuradas en la página **Valores de configuración**. También puede ver el organigrama corporativo mediante el icono  proporcionado en las páginas **Mi perfil**, **Consola** y **Aplicaciones**.

Para buscar el organigrama corporativo de otros usuarios del sistema, escriba el nombre del otro usuario en la barra de búsqueda de la página **Organigrama corporativo**.

- Acceda a **Personas > Usuarios**, seleccione cualquier usuario de la lista y haga clic en  junto al nombre del usuario. Para obtener más información, consulte el [Capítulo 13, "Gestión de usuarios"](#), en la página 79.

Nota: debe contar con el acceso **Organigrama corporativo** para ver el **Organigrama corporativo**. Póngase en contacto con el administrador para que le proporcione este acceso. Para obtener más información, consulte [User Settings](#) (Configuración del usuario) en *NetIQ Identity Manager - Administrator's Guide to Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Descripción del organigrama corporativo

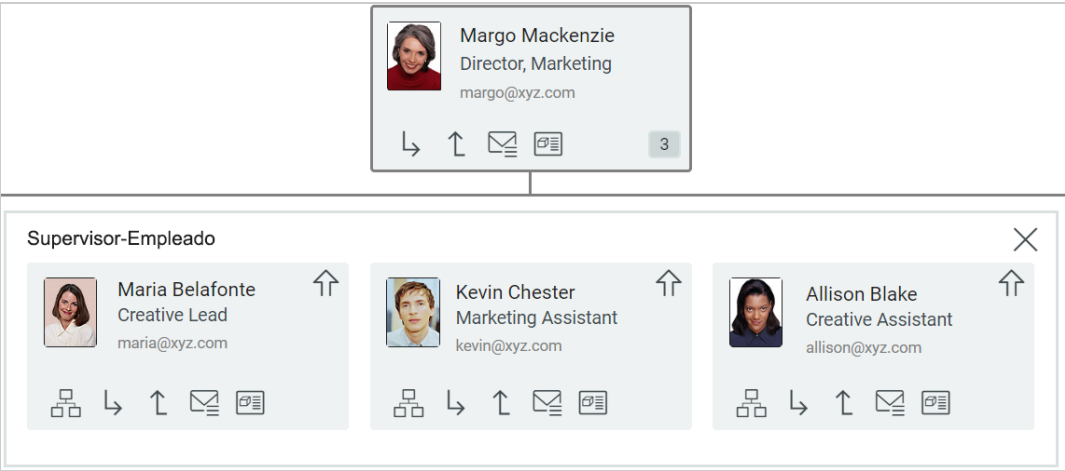
El organigrama corporativo muestra la información de la entidad en formato de tarjeta. Estas tarjetas se organizan en un orden jerárquico en función de las relaciones por defecto configuradas por el administrador. En la parte superior se muestra una entidad raíz o seleccionada que sirve de punto de partida o de orientación del organigrama. En la parte inferior se muestra la entidad subordinada directamente bajo la entidad raíz de acuerdo a la relación por defecto.

En cada tarjeta se muestra información basada en los atributos primarios y secundarios definidos por el administrador. Para obtener más información sobre cómo se pueden personalizar estos atributos, consulte [Customizing the Organization Chart View](#) (Personalización de la vistas del organigrama corporativo) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications). Específicamente para una entidad de usuario, la tarjeta está configurada para mostrar el nombre completo del usuario, además de los atributos primarios y secundarios definidos por el administrador. Como resultado, cuando el administrador configura el nombre y los apellidos como atributos principales, el nombre completo del usuario puede aparecer dos veces en la **Vista de tarjeta** de la página **Usuarios** y en el organigrama corporativo.

Nota: en la vista del organigrama corporativo, si el administrador no ha definido los atributos primarios y secundarios de una entidad, Identity Applications muestra el atributo de nombre completo de dicha entidad en la página **Organigrama corporativo**.

La **Figura 11-1** muestra un ejemplo de organigrama corporativo de la usuaria *Margo Mackenzie*, donde la relación por defecto es Supervisor-Empleado.

Figura 11-1 Ejemplo de organigrama en la consola



En este ejemplo, *Margo Mackenzie* es la supervisora y *Maria Belafonte*, *Kevin Chester* y *Allison Blake* son sus empleados subordinados. Cada tarjeta muestra el nombre completo del usuario en la parte superior, que en el caso de Margo es *Margo Mackenzie*, seguido de la función en la organización y la dirección de correo electrónico que el administrador define como atributos primarios y secundarios. El número de la esquina inferior derecha de la tarjeta de *Margo Mackenzie* indica cuántos empleados tiene subordinados.

Uso del organigrama corporativo

En función de la búsqueda que se realice en la página **Organigrama corporativo**, la consola muestra el organigrama de la entidad. Es posible realizar otras tareas en la página, como ver otras relaciones de la entidad, cambiar la entidad raíz o ver su organigrama, o bien ver el organigrama corporativo de una entidad situada en el siguiente nivel de la jerarquía.

Para obtener más información acerca de las tareas que puede llevar a cabo en la página **Organigrama corporativo**, veamos el siguiente ejemplo de un equipo de marketing de la empresa XYZ:

Margo Mackenzie es la directora del equipo de marketing y *Allison Blake*, *Kevin Chester* y *Maria Belafonte* son sus subordinados. *Margo Mackenzie* es subordinada de *Timothy Swan*, el vicepresidente del equipo de marketing.

Diríjase a **Personas > Organigrama corporativo** en la consola y busque a *Timothy Swan* para ver su organigrama corporativo. Del mismo modo, puede buscar a *Margo Mackenzie*. La **Figura 11-2** y la **Figura 11-3** muestran sus organigramas corporativos según la relación Supervisor-Empleado.

Figura 11-2 Organigrama corporativo de Timothy Swan con la función de supervisor.

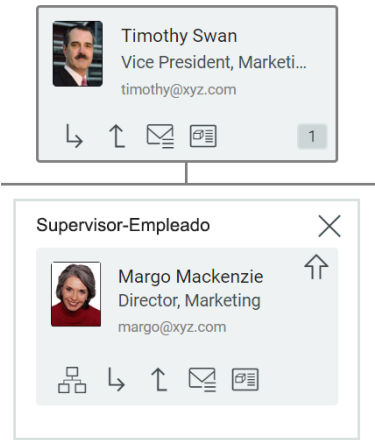
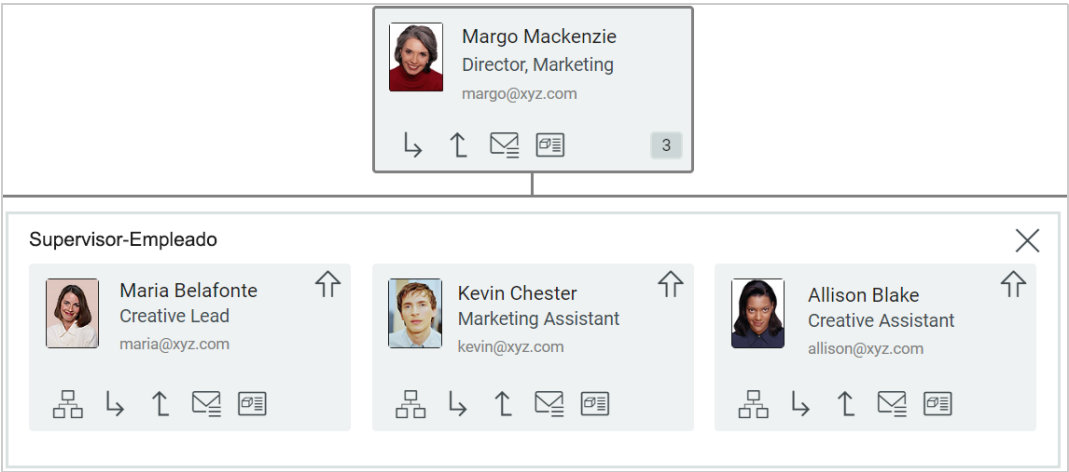


Figura 11-3 Organigrama corporativo de Margo Mackenzie con la función de supervisora.



Estas son las tareas que puede llevar a cabo en la página **Organigrama corporativo** según el ejemplo anterior:

- ♦ “Restablecer la raíz en la vista Organigrama corporativo” en la página 64
- ♦ “Cambiar la vista del organigrama corporativo” en la página 64
- ♦ “Seleccionar la relación que desea ver” en la página 65
- ♦ “Desplazarse hasta el siguiente nivel en la jerarquía de relaciones” en la página 66
- ♦ “Enviar un correo electrónico a los usuarios desde el organigrama corporativo” en la página 67
- ♦ “Ver información detallada de un usuario” en la página 67

Nota: las tareas anteriores se aplican tanto a entidades de usuario como a entidades personalizadas.

Restablecer la raíz en la vista Organigrama corporativo

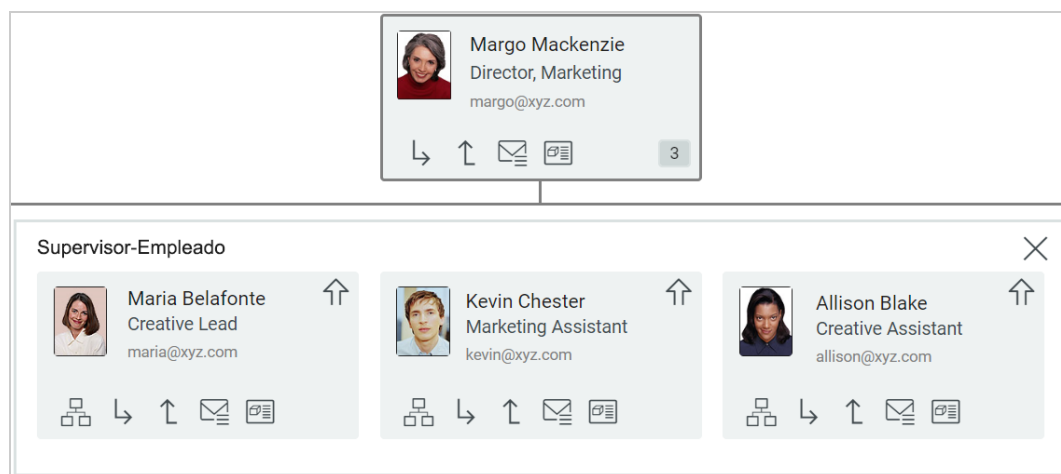
Para restablecer el usuario raíz en la vista del organigrama corporativo:

- 1 Identifique a usuario que desea convertir en la nueva raíz.

Imaginemos que muestra el organigrama corporativo en el que *Timothy Swan* tiene la función de supervisor y desea que *Margo Mackenzie* sea la nueva entidad raíz.

- 2 Vaya a la tarjeta de *Margo Mackenzie* y haga clic en el icono . Margo se convierte en la nueva raíz y ahora está en la parte superior del organigrama de Supervisor-Empleado. Los empleados que dependen de *Margo Mackenzie*, son *Maria Belafonte*, *Kevin Chester* y *Allison Blake* y se muestran debajo de ella.

Figura 11-4 Margo Mackenzie como nueva entidad raíz en la vista de organigrama



Cambiar la vista del organigrama corporativo

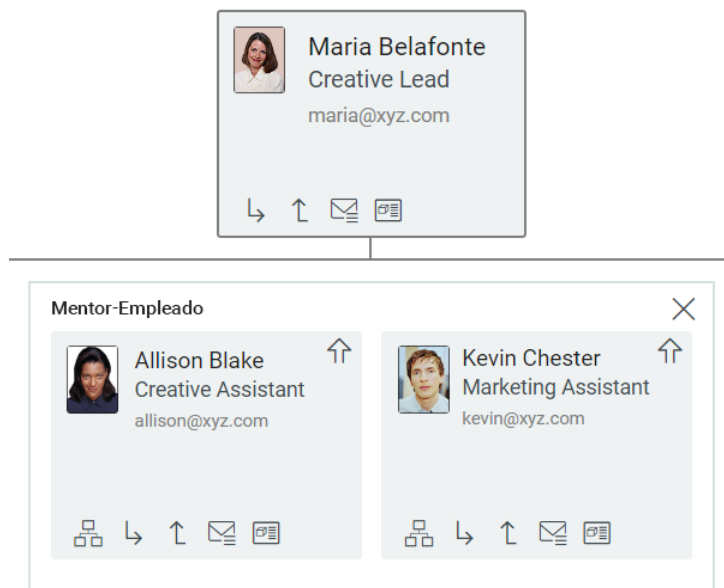
Para restablecer el usuario raíz y la relación por defecto en la vista del organigrama corporativo, lleve a cabo las siguientes acciones:

- 1 Identifique al usuario cuyo organigrama desea ver.

Supongamos que muestra el organigrama corporativo en el que *Margo Mackenzie* tiene la función de supervisor. *Maria Belafonte*, la subordinada de *Margo Mackenzie*, también es mentora de *Kevin Chester* y *Allison Blake*. Desea ver la relación de Mentor-Empleado de *María Belafonte*.

- 2 Vaya a la tarjeta de *Maria Belafonte* y haga clic en .
- 3 En el menú desplegable, seleccione la relación **Mentor-Empleado**. *María Belafonte* se convierte en la entidad raíz del organigrama Mentor-Empleado y *Kevin Chester* y *Allison Blake* aparecen como empleados.

Figura 11-5 Organigrama de *María Belafonte* con la función de mentora



Seleccionar la relación que desea ver

Para ver las relaciones de un usuario distintas a aquellas por defecto, realice las acciones siguientes:

- 1 Identifique al usuario cuya relación desea ver.

Supongamos que muestra el organigrama corporativo en el que *Margo Mackenzie* tiene la función de supervisor. Desea ver la relación de grupo de usuario de *Maria Belafonte* que formen parte del grupo de marketing.

- 2 Vaya a la tarjeta de *Maria Belafonte* y haga clic en .
- 3 En el menú desplegable, seleccione la relación **Grupos de usuarios**. El organigrama de pertenencia al grupo de *Maria Belafonte* se añade en la vista del organigrama corporativo actual.

Nota: el administrador define el número máximo de niveles que se puede expandir el organigrama corporativo de un usuario y el número de relaciones que se pueden mostrar. Por defecto, es posible expandir hasta el nivel 3, siendo siempre el nivel 1 el usuario raíz.

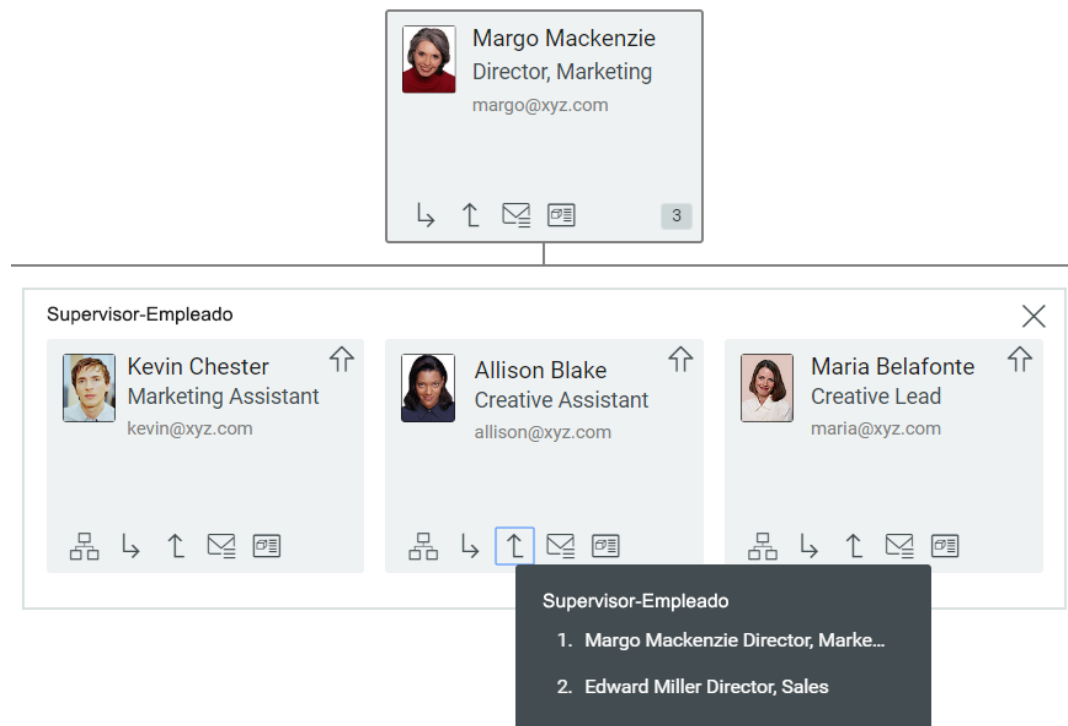
Desplazarse hasta el siguiente nivel en la jerarquía de relaciones

Para comprender esta tarea, tomemos como ejemplo a *Edward Miller*, que es director del equipo de ventas. *Allison Blake* y *Filla Martell* son subordinados de *Edward Miller*. Como se puede ver, *Allison Blake* es un miembro sin cargo del equipo de ventas y marketing y está subordinada a dos supervisores: *Edward Miller* y *Margo Mackenzie*.

Para desplazarse al siguiente nivel y expandirlo en el árbol de relaciones, realice las acciones siguientes:

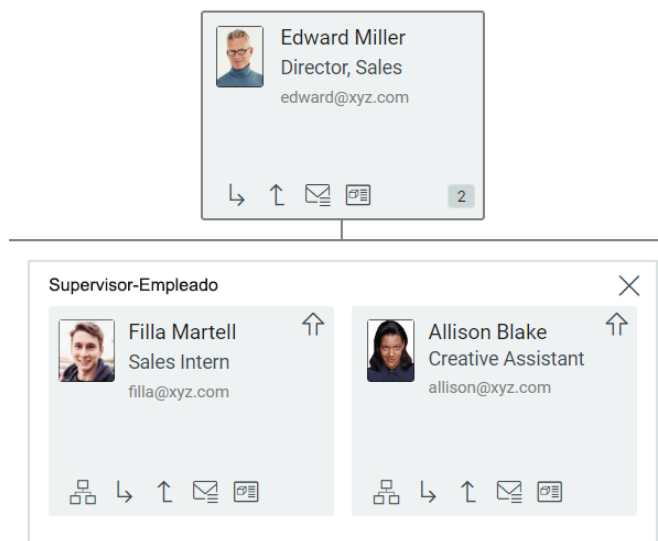
- 1 Identifique al usuario cuyo siguiente nivel de la jerarquía desea ver.
Imaginemos que está viendo el organigrama corporativo en el que *Margo Mackenzie* tiene la función de supervisora y desea ver el organigrama de *Allison Blake*.
 - 2 Diríjase a la tarjeta de *Allison Blake*, haga clic en  y seleccione la relación Supervisor-Empleado recurrente de la lista.
 - 3 Haga clic en .
- En el menú desplegable Supervisor-Empleado, el empleado *Allison Blake* tiene dos supervisores: *Margo Mackenzie* y *Edward Miller*.

Figura 11-6 Relación recurrente Supervisor-Empleado de Allison Blake



- 4 Seleccione al supervisor, *Edward Miller*. Se muestra el organigrama corporativo de *Allison Blake*.

Figura 11-7 Organigrama corporativo de Allison Blake



Enviar un correo electrónico a los usuarios desde el organigrama corporativo

Con la opción , es posible hacer lo siguiente:

- Enviar un mensaje de correo electrónico al usuario seleccionado.
- Compartir el enlace del perfil de una entidad por correo electrónico.
- (Opcional, solo aplicable a la relación Supervisor-Empleado) Enviar un correo electrónico a todos los miembros del equipo subordinados al usuario seleccionado.

Para obtener más información, haga clic en  en la consola.

Importante:

- Antes de enviar un correo electrónico desde la vista del organigrama corporativo, asegúrese de que haya configurado un cliente de correo electrónico por defecto en el sistema.
 - Para asegurarse de que las opciones **Nuevo correo electrónico** y **Equipo de correo electrónico** funcionan, configure el atributo Correo electrónico como atributo primario o secundario en la página Valores. Para obtener más información, consulte [User Settings](#) (Configuración del usuario) en *NetIQ Identity Manager - Administrator's Guide to Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).
-

Ver información detallada de un usuario

- 1 Identifique al usuario cuya información desea ver.

Imaginemos que está viendo el organigrama corporativo en el que *Margo Mackenzie* tiene la función de supervisora y desea ver detalles adicionales, como las funciones y los recursos asignados a *Kevin Chester*.

- 2 Vaya a la tarjeta de *Kevin Chester* y haga clic en el icono . La página de perfil muestra información detallada, como las funciones y los recursos que tiene asignados.

Si no ve el icono  en una tarjeta de usuario, por ejemplo, en la de *Jack Miller*, presidente de la organización XYZ, eso significa que no tiene los permisos adecuados para el catálogo de usuarios y, por lo tanto, no puede ver su perfil. Póngase en contacto con el administrador si necesita acceso para ver un perfil.

Para obtener más información, haga clic en  en la consola.

12 Gestión de la contraseña

El Gestor de identidades incluye una aplicación de autoservicio de restablecimiento de contraseñas (SSPR) con la que puede gestionar el proceso para cambiar y restablecer las contraseñas olvidadas. Durante el restablecimiento de la contraseña, SSPR usa un método de autenticación de respuesta a la pregunta de seguridad para autenticarle.

- ♦ [“Uso del autoservicio de gestión de contraseñas en Identity Manager” en la página 69](#)
- ♦ [“Uso de la gestión de contraseñas legada” en la página 72](#)

Nota: en esta sección se describen las funciones por defecto de la gestión de la contraseña. Es posible que encuentre diferencias a causa de la función de su trabajo, su nivel de autorización y las personalizaciones realizadas para su organización. Para obtener más información, póngase en contacto con el administrador del sistema.

Uso del autoservicio de gestión de contraseñas en Identity Manager

SSPR se integra automáticamente con el proceso de entrada única para Identity Applications e Identity Reporting. Es el programa de gestión de contraseñas por defecto de Identity Manager. Cuando un usuario solicita restablecer la contraseña, SSPR pide al usuario que responda a la pregunta de seguridad. Si las respuestas son correctas, SSPR actúa de una de estas formas:

- ♦ Permite a los usuarios crear una contraseña nueva.
- ♦ Crea una contraseña nueva y se la envía al usuario.
- ♦ Crea una contraseña nueva, se la envía al usuario y marca la contraseña antigua como caducada.

Puede configurar esta acción en el editor de configuración de SSPR. Después de actualizar a una versión nueva de Identity Manager, puede configurar SSPR para que use el método NMAS que se usaba tradicionalmente en Identity Manager para la gestión de contraseñas. Sin embargo, SSPR no reconoce las directivas de contraseñas existentes para la gestión de contraseñas olvidadas. También puede configurar SSPR para que use su protocolo propio en lugar de NMAS. Si realiza este cambio, no podrá volver a usar NMAS sin restablecer las directivas de contraseñas.

Puede usar SSPR para llevar a cabo todas las funciones indicadas en la [Tabla 12-2, “Funciones de Gestión de contraseñas”, en la página 72:](#)

Tabla 12-1 Funciones de Gestión de contraseñas

Mediante esta página de la Gestión de contraseñas	Podrá hacer lo siguiente
Respuesta a la pregunta de verificación de la contraseña	Definir o cambiar los elementos siguientes: ♦ Las respuestas válidas para preguntas de verificación definidas por el administrador ♦ Preguntas y respuestas de verificación definidas por el usuario
Cambio de contraseña	Cambiar (restablecer) la contraseña de acuerdo con las reglas establecidas por el administrador del sistema.
Estado de directiva de contraseñas	Revisar los requisitos de la directiva de contraseñas.

Descripción de la respuesta a la pregunta de verificación de la contraseña

Las preguntas de verificación se utilizan para comprobar la identidad durante la entrada a la sesión si ha olvidado la contraseña. Si el administrador del sistema ha configurado una directiva de contraseñas que habilite esta función para usted, podrá utilizar la página Respuesta a la pregunta de verificación de la contraseña para:

- ♦ Especificar respuestas que se considerarán válidas para usted cuando conteste las preguntas definidas por el administrador
- ♦ Especificar sus propias preguntas y las respuestas válidas a éstas (si su directiva de contraseña lo permite)

Durante el proceso de entrada, la página de entrada redirige automáticamente a la página de respuesta a la pregunta de seguridad. En esta página se configuran las respuestas a las preguntas de seguridad. Para obtener más información, consulte [“Si olvida la contraseña” en la página 22](#). Cuando se vuelve a entrar y se intenta restablecer la contraseña olvidada, SSPR pregunta las cuestiones configuradas y se le pide que las conteste correctamente. Si la contestación coincide con la respuesta que guardó anteriormente, SSPR permite restablecer la contraseña.

Cambio de la contraseña

Puede cambiar la contraseña (siempre y cuando el administrador del sistema le otorgue la capacidad para ello).

- 1 En la consola, haga clic en **Aplicaciones > Cambiar mi contraseña**.
- 2 Escriba su contraseña actual. Aparecerá la página Cambiar contraseña.

- 3 Escriba la contraseña nueva en el recuadro de texto **Contraseña nueva**.
- 4 Vuelva a escribir la contraseña nueva en el recuadro de texto **Confirmar contraseña**.
- 5 Haga clic en **Cambiar contraseña**.

Si la nueva contraseña infringe alguna de las reglas de contraseña definidas por el administrador en la directiva de contraseñas, verá un mensaje de error en la página Cambiar contraseña.

Esta página suele proporcionar información sobre cómo se debe especificar una contraseña para que cumpla los requisitos de la directiva definida por el administrador. Revise las reglas de contraseñas y vuelva a intentarlo.

- 6 Haga clic en **Continuar**. Se mostrará el estado de la petición. Si se realiza correctamente, volverá a la página de entrada de OSP.

Estado de directiva de contraseñas

Nota: esta función solo está disponible para los usuarios administradores.

El administrador asigna una directiva de contraseñas a cada usuario. La directiva determina las medidas de seguridad asociadas a su contraseña. Los requisitos de la directiva de contraseñas no se pueden comprobar a menos que el administrador de la aplicación de usuario le haya otorgado derechos para hacerlo. El administrador de la aplicación de usuario puede comprobar el estado de la directiva de contraseñas en la página de inicio de Identity Manager. Este enlace no existe por defecto. Debe personalizar la página de inicio para incluirla. Para personalizar los elementos por defecto de la página de inicio de Identity Manager, consulte el [Capítulo 5, “Gestión de aplicaciones”](#), en la [página 45](#).

En la página de inicio, haga clic en el enlace **Estado y directiva de la contraseña**. Se abre la página **Estado de la directiva de contraseñas**. Para cambiar la contraseña del Gestor de identidades, diríjase a la página de inicio del Gestor de identidades y seleccione Cambiar mi contraseña. El enlace de la página de inicio del Gestor de identidades redirige a la sección Cambiar contraseña de SSPR.

Uso de la gestión de contraseñas legada

En este capítulo se describe cómo utilizar las páginas Gestión de contraseñas de la pestaña **Autoservicio de identidades** de la aplicación de usuario de Identity Manager. Los temas son los siguientes:

- ♦ [“Respuesta a la pregunta de verificación de la contraseña” en la página 73](#)
- ♦ [“Cambio de la sugerencia de contraseña” en la página 73](#)
- ♦ [“Cambiar contraseña” en la página 74](#)
- ♦ [“Estado de directiva de contraseñas” en la página 75](#)
- ♦ [“Estado de sincronización de contraseñas” en la página 75](#)

Nota: en este capítulo se describen las funciones por defecto de las páginas Gestión de contraseñas. Es posible que encuentre diferencias a causa de la función de su trabajo, su nivel de autorización y las personalizaciones realizadas para su organización. Para obtener más información, póngase en contacto con el administrador del sistema.

Para obtener más información general sobre cómo acceder a la pestaña **Autoservicio de identidades** y cómo utilizarla, consulte el [Capítulo 10, “Gestión del perfil”, en la página 59](#).

Puede utilizar las páginas Gestión de contraseñas para ejecutar cualquiera de las funciones indicadas en la [Tabla 12-2, “Funciones de Gestión de contraseñas”, en la página 72](#):

Tabla 12-2 Funciones de Gestión de contraseñas

Mediante esta página de la Gestión de contraseñas	Podrá hacer lo siguiente
Respuesta a la pregunta de verificación de la contraseña	Definir o cambiar los elementos siguientes: ♦ Las respuestas válidas para preguntas de verificación definidas por el administrador ♦ Preguntas y respuestas de verificación definidas por el usuario
Cambio de la sugerencia de contraseña	Definir o cambiar la sugerencia de la contraseña.
Cambiar contraseña	Cambiar (restablecer) la contraseña de acuerdo con las reglas establecidas por el administrador del sistema.
Estado de directiva de contraseñas	Revisar los requisitos de la directiva de contraseñas.
Estado de sincronización de contraseñas	Muestra el estado de sincronización de las contraseñas de las aplicaciones con el repositorio seguro de identidades. Nota: el intento de acceso a las aplicaciones antes de que finalice la sincronización provoca problemas de acceso a las aplicaciones.

Respuesta a la pregunta de verificación de la contraseña

Las preguntas de verificación se utilizan para comprobar la identidad durante la entrada a la sesión si ha olvidado la contraseña. Si el administrador del sistema ha configurado una directiva de contraseñas que habilite esta función para usted, podrá utilizar la página Respuesta a la pregunta de verificación de la contraseña para:

- ♦ Especificar respuestas que se considerarán válidas para usted cuando conteste las preguntas definidas por el administrador
- ♦ Especificar sus propias preguntas y las respuestas válidas a éstas (si su directiva de contraseña lo permite)

Para utilizar la página Respuesta a la pregunta de verificación de la contraseña:

- 1 En la pestaña **Autoservicio de identidades**, haga clic en **Respuesta a la pregunta de verificación de la contraseña** del menú (en **Gestión de contraseñas**).

Aparecerá la página Respuesta a la pregunta de verificación de la contraseña.

- 2 Escriba una respuesta adecuada en cada recuadro de texto **Respuesta** (todos son obligatorios) o utilice la respuesta almacenada previamente. Si el recuadro **¿Desea utilizar la respuesta almacenada?** está marcado, las respuestas de verificación no se muestran, incluidas las etiquetas. Además, las preguntas de verificación definidas por el usuario se inhabilitan.

Asegúrese de especificar respuestas que pueda recordar más adelante.

- 3 Especifique o cambie las preguntas definidas por el usuario necesarias. No podrá utilizar la misma pregunta más de una vez.
- 4 Haga clic en **Enviar**.

Después de guardar las respuestas de verificación, la aplicación de usuario muestra un mensaje que indica que las respuestas de verificación se han guardado correctamente y vuelve a mostrar la pantalla de la respuesta de verificación con la opción **¿Desea utilizar la respuesta almacenada?** marcada.

Cambio de la sugerencia de contraseña

Una sugerencia de contraseña se utiliza durante la entrada a la sesión para ayudarle a recordar la contraseña si la ha olvidado. Utilice la página Cambio de la sugerencia de contraseña para definir o cambiar la sugerencia de la contraseña.

- 1 En la pestaña **Autoservicio de identidades**, haga clic en **Cambio de la sugerencia de contraseña** del menú (en **Gestión de contraseñas**).

Aparecerá la página Definición de la sugerencia de la contraseña.

- 2 Escriba el texto nuevo de la sugerencia.

La contraseña no debe aparecer en el texto de la sugerencia.

- 3 Haga clic en **Enviar**.

Aparecerá el estado de la petición.

Cambiar contraseña

Puede utilizar esta página siempre que precise cambiar la contraseña (siempre y cuando el administrador del sistema le otorgue la capacidad para ello).

- 1 En la pestaña **Autoservicio de identidades**, haga clic en **Cambiar contraseña** en el menú (en **Gestión de contraseñas**).

Aparecerá la página Cambiar contraseña. Si el administrador del sistema ha configurado una directiva de contraseña para usted, la página Cambiar contraseña, normalmente, proporciona información sobre cómo especificar una contraseña que satisfaga los requisitos de la directiva. Por ejemplo:

Si no se aplica ninguna directiva de contraseñas, verá la página Cambiar contraseña básica, en la que solo se presentan campos para cambiar la contraseña.

La aplicación de usuario admite los siguientes tipos de sintaxis de contraseña:

- ♦ Directiva de complejidad de Microsoft

Este tipo de sintaxis de contraseña se usa para la compatibilidad inversa con Active Directory 2003.

- ♦ Directiva de contraseñas de Microsoft Server 2008

Se trata de un tipo de sintaxis de contraseña nuevo añadido a eDirectory 8.8.7 para admitir Active Directory 2008.

Los ajustes siguientes se admiten con la directiva de contraseñas de Microsoft Server 2008:

- ♦ Uso de la directiva de contraseñas de Microsoft Server 2008
- ♦ Número máximo de infracciones de la directiva de complejidad en la contraseña (0-5)
- ♦ Sintaxis de Novell

Con la sintaxis de Novell se admiten los siguientes ajustes nuevos:

- ♦ Número mínimo de caracteres no alfabéticos (1-512)
- ♦ Número máximo de caracteres no alfabéticos (1-512)

Para los tres tipos de sintaxis de contraseña, la aplicación de usuario admite las siguientes funciones:

- ♦ Número de caracteres distintos respecto a la contraseña actual y las contraseñas del historial (0-6)
- ♦ Número de contraseñas del historial que se deben tener en cuenta para la exclusión de caracteres (0-10)

Si el administrador ha habilitado la sintaxis de directiva de Microsoft Server 2008, complete los campos siguiente en la página Cambiar contraseña:

- 2 Escriba la contraseña actual en el recuadro de texto **Contraseña antigua**.
- 3 Escriba la contraseña nueva en el recuadro de texto **Contraseña nueva**.
- 4 Vuelva a escribir la contraseña nueva en el recuadro de texto **Reescriba la contraseña**.
- 5 Haga clic en **Enviar**.

Si la nueva contraseña infringe alguna de las reglas de contraseña definidas por el administrador, verá un mensaje de error en la página Cambiar contraseña. Si utiliza la directiva de Microsoft Server 2008 y su contraseña la infringe, la interfaz del usuario mostrará este mensaje en la parte superior de la página:

Password AD2008 complexity policy violation.

Si la nueva contraseña infringe la directiva, revise las reglas de contraseña definidas por el administrador y vuelva a intentarlo.

- 6 Puede que el sistema solicite que proporcione una sugerencia de contraseña si el administrador ha configurado la directiva de seguridad para ello. Si es así, consulte [“Cambio de la sugerencia de contraseña” en la página 73](#).
- 7 Se mostrará el estado de la petición.

Estado de directiva de contraseñas

El administrador asigna una directiva de contraseñas a cada usuario. La directiva determina las medidas de seguridad asociadas a su contraseña. Puede comprobar los requisitos de la directiva de contraseñas del modo siguiente:

- 1 En la pestaña **Autoservicio de identidades**, haga clic en **Estado de directiva de contraseñas** en el menú (en **Gestión de contraseñas**). Aparecerá la página **Estado de directiva de contraseñas**.

Los elementos etiquetados como no válidos no se pueden modificar.

Estado de sincronización de contraseñas

Utilice la página Estado de sincronización de contraseñas para determinar si la contraseña se ha sincronizado entre las aplicaciones. Acceda a otra aplicación solo después de sincronizar las contraseñas. El intento de acceso a las aplicaciones antes de que finalice la sincronización provoca problemas de acceso a las aplicaciones.

- 1 En la pestaña **Autoservicio de identidades**, haga clic en **Estado de sincronización de contraseñas** en el menú (en **Gestión de contraseñas**). Aparecerá la página **Estado de sincronización de contraseñas**. Los iconos en color indican las aplicaciones cuyas contraseñas están sincronizadas. Los iconos atenuados indican las aplicaciones cuyas contraseñas aún no están sincronizadas.

Nota: solo el administrador puede ver el recuadro **Seleccionar usuario**.

IV

Gestión de usuarios, grupos y equipos

Si tiene la función adecuada en Identity Applications, puede crear y gestionar usuarios, grupos y equipos. Puede crear usuarios y equipos en la consola y en la aplicación de usuario. Puede crear y gestionar grupos en la aplicación de usuario.

Los administradores del sistema pueden crear usuarios y grupos. El administrador del sistema puede proporcionar acceso a esta función a otros usuarios (normalmente, personal seleccionado de puestos de administración o gestión).

Es posible que detecte algunas diferencias en las funciones documentadas en esta sección a causa de la función de su trabajo, su nivel de autorización y las personalizaciones realizadas para su organización. Para obtener más información, póngase en contacto con el administrador del sistema.

Un equipo representa un conjunto de usuarios, grupos o usuarios y grupos que pueden llevar a cabo tareas de aprobación y solicitudes de provisión asociadas al equipo. Aunque un equipo puede coincidir con un grupo que exista en el directorio de usuarios, los equipos no son lo mismo que los grupos. Es decir, un grupo o un miembro de un grupo no puede realizar funciones de equipo, a menos que sea asignado a un equipo. Véase [Capítulo 14, “Gestión de equipos”, en la página 83](#).

13 Gestión de usuarios

En esta sección se explica cómo crear usuarios y grupos en la consola y en la aplicación de usuario. Los temas son los siguientes:

- ♦ “Creación de un usuario” en la página 79
- ♦ “Edición de la información del usuario” en la página 79
- ♦ “Listas de usuarios” en la página 80
- ♦ “Cómo buscar usuarios” en la página 81
- ♦ “Clasificación de los usuarios” en la página 82

Creación de un usuario

La página **Crear usuario** muestra los atributos de usuarios habilitados con accesos de **búsqueda** y de **lectura**. Estas propiedades de acceso se pueden configurar en el nivel de abstracción de directorio (DAL). Para obtener más información, consulte [Attribute Properties](#) (Propiedades del atributo) en la *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications* (Gestor de identidades de NetIQ: Guía del administrador para el diseño de las aplicaciones de identidad).

Para crear un usuario, seleccione en la consola:

Personas > Usuarios > +

El administrador de identidad define los valores que se pueden especificar para el usuario. Asimismo, cuando se crea un usuario, es posible ver el **contenedor** de usuarios, pero no modificar su valor. Esta limitación garantiza que todos los usuarios se almacenan en el mismo contenedor.

Para obtener más información, haga clic en ⓘ en la consola.

Edición de la información del usuario

Seleccione un usuario de una vista de lista, haga clic en  para modificar la información de usuario, como el título, el correo electrónico, el número de teléfono, el administrador y otros datos. Puede modificar los atributos de usuario definidos por el administrador. Para obtener más información sobre cómo personalizar los atributos de usuario, consulte [Personalización de las vistas](#) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications). Puede eliminar usuarios mediante la vista **Gestionar usuarios**.

A continuación encontrará un ejemplo de cómo editar la información de un usuario:

Figura 13-1 Edición de la información del usuario

Aliyah Hall

Título

Marketing Director +

Marketing Director X

Entrada inhabilitada ☐

Teléfono

552538 +

552538 X

Correo electrónico

aliyah@example.com +

aliyah@example.com X

Personas a cargo

Q Buscar usuarios por Nombre de pila,Apellido

Supervisor

Q Buscar usuarios por Nombre de pila,Apellido

Guardar Cancelar

Nota: el conmutador **Entrada inhabilitada** se puede utilizar para inhabilitar una cuenta de usuario. Este conmutador solo está visible si el administrador añade el atributo **Entrada inhabilitada** en **Vista de tarjeta** y **Atributos editables** en la página **Valores de configuración > Personalización**. Para obtener más información, haga clic en en la consola.

Listas de usuarios

A continuación se muestran las distintas formas para generar listas de usuarios en Identity Applications:

- ♦ **Vista de lista:** para ver los usuarios en forma de lista, haga clic en . Se muestra información del usuario en el lado derecho. Para editar la información del usuario, como el número de teléfono, el correo electrónico, el supervisor y mucho más, haga clic en . Si desea ver el organigrama corporativo de un usuario concreto, haga clic en .
- ♦ **Vista de tarjeta:** para ver a los usuarios en forma de tarjeta, haga clic en . Se muestra la información básica de los usuarios en forma de tarjetas. El administrador puede configurar qué información se debe mostrar en la tarjeta de cada usuario. Para obtener más información, consulte [Customizing the Views](#) (Personalización de las vistas) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del

administrador de Identity Applications). Haga clic en  para editar la información de usuario, como el **teléfono**, el **correo electrónico**, el **supervisor** y otros atributos. Si desea ver el organigrama corporativo de un usuario concreto, haga clic en .

- ♦ **Vista Gestionar usuarios:** para ver a los usuarios en forma de tabla, haga clic en . Los usuarios se mostrarán en una vista de tabla. Esta vista permite ordenar a los usuarios según atributos como el número de teléfono, el correo electrónico, el departamento y otros. Puede personalizar las columnas que se deben mostrar en esta vista. Para obtener más información acerca de la personalización de columnas, haga clic en  en la consola.

Esta vista también permite suprimir usuarios del sistema. Para suprimir usuarios:

1. Seleccione al usuario que quiera suprimir.
2. Haga clic en .

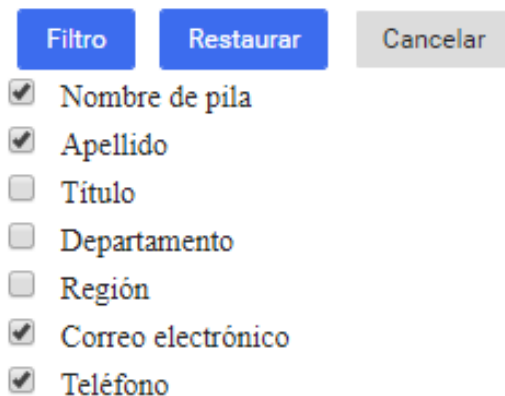
Cómo buscar usuarios

A continuación se muestran las distintas formas para buscar usuarios en Identity Applications:

- ♦ **Búsqueda rápida:** permite especificar el atributo de usuario y muestra los usuarios en función de los filtros seleccionados. Para modificar las opciones de filtro:

1. Haga clic en .
2. Seleccione las opciones de filtro para buscar usuarios.

A continuación, encontrará un ejemplo de los atributos de usuario seleccionados para una búsqueda rápida:



Atributo	Seleccionado
Nombre de pila	✓
Apellido	✓
Título	✗
Departamento	✗
Región	✗
Correo electrónico	✓
Teléfono	✓

3. Haga clic en **Filtro**.

Por ejemplo, para buscar a un usuario que se llame Sánchez con los filtros de nombre y apellidos seleccionados. La búsqueda rápida muestra a todos los usuarios con el atributo Sánchez en los campos de nombre o apellido.

- ♦ **Búsqueda avanzada:** esta opción recupera una lista de usuarios más afinada que la búsqueda rápida. Puede buscar a un usuario con los atributos de usuario deseados. Para usar la búsqueda avanzada:

1. Haga clic en .
2. Especifique la información exacta del usuario para cada atributo.

A continuación, encontrará un ejemplo de los atributos de usuario especificados para una búsqueda avanzada:

BÚSQUEDA AVANZADA ✕

Buscar por

Nombre de pila ▼	Emily	✕
Apellido ▼	Cameron	✕
Correo electrónico ▼	emily.cameron@example.com	✕
Teléfono ▼	5552368	✕

+ Añadir

3. Haga clic en **Filtro**.

Por ejemplo, si desea buscar a un usuario con el **Nombre** Alberto, el **Apellido** López y el **Título** Director. Puede especificar estos datos en la búsqueda avanzada para buscar un usuario que tenga este conjunto exacto de atributos.

También puede configurar los resultados de búsqueda de una página definiendo el índice en la parte inferior. La consola utiliza un control de vista de lista virtual (VLV) que se ejecuta en LDAP OID 2.16.840.1.113730.3.4. Esto funciona en combinación con el control de la clasificación.

La consola de Identity Manager ofrece dos totales distintos al mostrar los resultados:

- ♦ **Recuento total:** número total de usuarios encontrados en el sistema.
- ♦ **Recuento de la búsqueda:** número de usuarios mostrados para la búsqueda específica.

Clasificación de los usuarios

La vista Gestionar usuarios permite ordenar a los usuarios según sus atributos. El administrador debe configurar índices compuestos para los atributos de usuario para que sea posible realizar la clasificación. Para obtener más información acerca del índice compuesto, consulte [Creating Compound Indexes](#) (Creación de índices compuestos) en *NetIQ Identity Manager Install and Upgrade Guide for Windows* (Guía de instalación y actualización de NetIQ Identity Manager para Windows).

Nota: si no puede clasificar a los usuarios según los atributos de usuario, contacte con el administrador para que configure el índice compuesto con el atributo necesario para clasificar a los usuarios.

14 Gestión de equipos

Un equipo consta de dos tipos de usuarios:

Solicitante

Lleva a cabo las peticiones de permisos en nombre de los demás miembros del equipo (los destinatarios). Dependiendo de cómo esté configurado el equipo, un solicitante puede actuar sobre una petición de provisión individual, una o varias categorías de peticiones o todas las peticiones.

También gestiona las asignaciones de apoderados de los miembros del equipo.

Destinatario

Miembro del equipo en cuyo nombre pueden actuar los solicitantes.

Los destinatarios del equipo pueden ser usuarios o grupos del directorio. Opcionalmente, pueden proceder de relaciones de directorios. Por ejemplo, la lista de miembros puede proceder de la relación de supervisores y empleados de la organización. Si se da el caso, todos los miembros del equipo serían usuarios que dependen del administrador del equipo.

Nota: el administrador de provisión puede configurar la capa de abstracción del directorio para que sea compatible con las relaciones en cascada, en cuyo caso se podrían incluir varios niveles de una organización en un equipo. El administrador puede configurar el número de niveles que desea incluir.

Para llevar a cabo cualquiera de las siguientes actividades, acceda a **Personas > Equipos**:

- ♦ “Visualización de equipos” en la página 83
- ♦ “Creación de un equipo” en la página 84
- ♦ “Modificación de un equipo” en la página 84

Visualización de equipos

En la página **Equipos** puede consultar una lista de todos los equipos que pueda ver según sus permisos. Puede ser miembro de todos los equipos indicados. Sin embargo, también es posible que sea un administrador con permisos para ver, modificar o suprimir determinados equipos, aunque no pertenezca a ellos.

Como miembro del equipo, es posible que sea **Solicitante** y pueda realizar peticiones en nombre de otros miembros del equipo. Además, otros usuarios del equipo podrían estar capacitados para realizar estas acciones en nombre de usted, el **Destinatario**. Para obtener más información, haga clic en ⓘ en la consola.

Creación de un equipo

Como administrador, puede crear equipos. Un **equipo** representa un conjunto de usuarios, grupos o usuarios y grupos que pueden llevar a cabo tareas de aprobación y solicitudes de provisión asociadas al equipo.

Para cada equipo, debe especificar los miembros del equipo (**destinatarios**) que reciben los permisos del equipo y aquellos que pueden realizar acciones en nombre de los destinatarios (**solicitantes**). Después de crear un equipo, puede especificar los **permisos** (recursos y definiciones de peticiones de provisión) que se aplican a los miembros del equipo. Por ejemplo, puede añadir como recurso un portátil que debe proporcionarse a los miembros del equipo.

Para obtener más información, haga clic en ⓘ en la consola.

Modificación de un equipo

Como administrador, puede modificar y eliminar equipos. Puede modificar los siguientes aspectos de un equipo:

- ♦ Cambio de nombre y descripción del equipo.
- ♦ Modificación de los solicitantes del equipo.
- ♦ Adición o eliminación de miembros del equipo.
- ♦ Adición o eliminación de permisos para un administrador de equipo.

Para obtener más información, haga clic en ⓘ en la consola.

15 Gestión de grupos

Un grupo está formado por usuarios y otras cuentas que tienen características comunes. Por ejemplo, el grupo Finanzas está formado por todos los empleados del departamento de Finanzas.

Los grupos se pueden buscar según su descripción. Sin embargo, los administradores que tienen acceso a la página **Valores de configuración** pueden personalizar los atributos por los que se podrá buscar una entidad de grupo. Esto significa que cuando se busca un grupo específico al asignar una función a un grupo, al hacer que un grupo sea el propietario de un recurso o al realizar una búsqueda simple en la página **Grupos**, la aplicación devolverá como resultado los nombres del grupo que coincida con el atributo buscado. Para obtener más información, consulte [Entity Settings](#) (Configuración de la entidad) en *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Creación de un grupo

Si tiene una función administrativa en Identity Applications, puede crear un grupo.

- 1 En la consola del Gestor de identidades, diríjase a **Personas > Grupos**.
- 2 Haga clic en **+**.
- 3 Especifique valores para los siguientes atributos obligatorios:

Atributo	Datos que se deben especificar
Nombre	El nombre de grupo de este grupo nuevo. Importante: no use los caracteres especiales siguientes en el campo Nombre: < ; \ " + # / * ~
Descripción	Descripción del nuevo grupo. La descripción se utiliza como criterio de búsqueda de grupos en la consola. Importante: no use los caracteres especiales siguientes en el campo Descripción: ~
Contenedor	Una unidad administrativa en el repositorio seguro de identidades en el que desea almacenar el grupo nuevo (como una unidad administrativa denominada grupos). Por ejemplo: ou=groups,ou=MyUnit,o=MyOrg Para obtener información sobre cómo utilizar los botones que se proporcionan para especificar un contenedor, consulte "Creación de un usuario" en la página 79. Nota: el sistema no solicitará un contenedor si el administrador del sistema ha establecido un contenedor de creación por defecto para este tipo de objeto.

4 Haga clic en **Crear**.

Cuando el grupo se cree correctamente, se muestra el panel **Miembros del grupo**, que permite añadir los usuarios al grupo recién creado.

5 Para añadir usuarios al grupo, haga clic en el icono **+** situado junto a los miembros del grupo.

6 Seleccione los usuarios necesarios en la ventana modal.

7 Haga clic en **Añadir**.

V Apéndice

En el apéndice siguiente, se proporciona información de referencia adicional y se describen temas avanzados de la aplicación de usuario de Identity Manager.

A Uso de la aplicación de aprobaciones de Identity Manager

Además de la interfaz del usuario de la aplicación de usuario usada por los clientes de Identity Manager, ahora puede usar una nueva aplicación iOS que permite a los usuarios de Identity Manager aprobar o denegar de forma remota las peticiones mediante el módulo de provisión basada en reglas de Identity Manager.

Cuando instale y configure la aplicación de aprobaciones, podrá ver en ella las mismas tareas de aprobación que vería normalmente en la interfaz de la aplicación de usuario. Todos los cambios se sincronizan entre la aplicación de aprobaciones y la aplicación de usuario.

También puede trabajar en modo sin conexión cuando se desconecte del servidor del módulo de provisión basada en funciones del Gestor de identidades y la aplicación de aprobaciones sincronizará automáticamente los cambios cuando se recupere la conexión.

En este apéndice, se proporciona información sobre la instalación y el uso de la nueva aplicación de aprobaciones. Para obtener información sobre cómo pueden los administradores del Gestor de identidades configurar su entorno para permitir que los usuarios utilicen la aplicación, consulte la sección [“Configuring the Identity Manager Approvals App”](#) (Configuración de la aplicación de aprobaciones del Gestor de identidades) en la [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (Gestor de identidades de NetIQ: Guía del administrador de las aplicaciones de usuario).

Para obtener información más detallada sobre la aplicación de aprobaciones, consulte las secciones siguientes:

- ♦ [“Requisitos del producto” en la página 89](#)
- ♦ [“Instalación de la aplicación de aprobaciones” en la página 90](#)
- ♦ [“Configuración de la aplicación de aprobaciones” en la página 90](#)
- ♦ [“Descripción general de la aplicación de aprobaciones” en la página 95](#)
- ♦ [“Cambio del idioma de visualización de la aplicación de aprobaciones” en la página 97](#)

Requisitos del producto

La aplicación de aprobaciones requiere un Apple iPhone o un iPad con los sistemas operativos iOS 6 o iOS 7 de Apple instalados, o bien cualquier dispositivo con Android 5.0 o una versión posterior.

Nota: si el administrador no ha habilitado el uso de la aplicación de aprobaciones, no podrá configurarla después de la instalación. Para obtener información sobre cómo pueden los administradores configurar el entorno de Identity Manager para habilitar el uso de la aplicación de aprobaciones, consulte la sección [“Configuring the Identity Manager Approvals App”](#) (Configuración

de la aplicación de aprobaciones de Identity Manager) en [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (NetIQ Identity Manager: Guía del administrador de Identity Applications).

Instalación de la aplicación de aprobaciones

Puede instalar la aplicación de aprobaciones de NetIQ Identity Manager desde la [página de la aplicación](#) de la App Store de Apple en el dispositivo.

Después de instalar la aplicación de aprobaciones, debe configurar la aplicación para poder conectar con el servidor del módulo de provisión basada en funciones.

Nota: si la contraseña de la aplicación de usuario ha caducado, es recomendable cambiarla antes de instalar y configurar la aplicación de aprobaciones. Si la directiva de contraseñas de su entorno permite un número limitado de entradas de gracia cuando caduca la contraseña, la aplicación de aprobaciones podría usar todas esas entradas al intentar sincronizar las tareas de Identity Manager con el dispositivo.

Configuración de la aplicación de aprobaciones

Es posible configurar la aplicación de aprobaciones de NetIQ Identity Manager de varias formas, según las necesidades de su entorno y del modo en el que el administrador haya configurado Identity Manager:

- ♦ Realice una petición en la interfaz de la aplicación de usuario para acceder a la aplicación de aprobaciones y, a continuación, lance la aplicación en el dispositivo desde el enlace del correo electrónico proporcionado por el administrador de Identity Manager. En enlace incluye toda la información de configuración necesaria.
- ♦ Haga clic en un enlace de configuración o explore un código QR de configuración mediante el dispositivo. El enlace o el código QR proporcionan toda la información necesaria o datos de configuración generales para la empresa.
- ♦ Introduzca manualmente la información de configuración de su entorno en la aplicación.

Importante: para que los usuarios puedan configurar automáticamente la aplicación de aprobaciones mediante un enlace o un código QR, el administrador del entorno de Identity Manager primero debe habilitar este enlace o código QR.

Petición de acceso móvil mediante la aplicación de usuario

Si el administrador lo ha configurado, puede pedir acceso a la aplicación de aprobaciones mediante la aplicación de usuario. Identity Manager envía a continuación un correo electrónico con un enlace personalizado que puede abrir en el dispositivo para configurar automáticamente la aplicación de aprobaciones con los datos necesarios.

Para pedir acceso móvil mediante la aplicación de usuario:

- 1 En un navegador Web, entre en la aplicación de usuario de Identity Manager con el protocolo HTTPS (`https://`).

Nota: para pedir acceso a la aplicación de aprobaciones, debe entrar en la aplicación de usuario con el protocolo HTTPS.

- 2 Haga clic en **Realizar una petición de proceso**.
- 3 Haga clic en el menú desplegable Categoría de petición de proceso y seleccione **Cuentas**.
- 4 Haga clic en **Continuar**.
- 5 Haga clic en **Pedir aplicación de aprobación móvil**.

Nota: la categoría y el nombre de la petición de proceso pueden variar, según cómo haya configurado el administrador el proceso de petición de la aplicación de aprobaciones.

- 6 Proporcione la información necesaria en el formulario de la petición de proceso y haga clic en **Enviar**.
- 7 Cuando reciba el correo electrónico del administrador de Identity Manager, ábralo en el dispositivo y haga clic en el enlace proporcionado para conectar el dispositivo con el servidor del módulo de provisión basada en funciones.

Nota: si ha instalado anteriormente la aplicación, esta podría mostrar un mensaje de advertencia que indica que la configuración existente se sobrescribirá. Asegúrese de que el nombre del host mostrado en el mensaje de advertencia es el mismo al que accedió cuando pidió acceso a la aplicación. Si no está seguro, no haga clic en el enlace y póngase en contacto con el administrador.

Si el nombre del host está correcto, haga clic en **Aceptar** para sobrescribir la configuración existente.

- 8 Cuando la aplicación se inicie, introduzca su contraseña y haga clic en el icono Probar conexión  para verificar la configuración.

Uso de un enlace de configuración o un código QR

El administrador de Identity Manager puede proporcionarle un enlace para configurar la aplicación de aprobaciones. Abra el enlace en un navegador en el dispositivo para configurar la aplicación automáticamente.

Sin embargo, este enlace solo puede proporcionar parte de la configuración necesaria. Normalmente, un enlace o un código solo pueden proporcionar los detalles del servidor del módulo de provisión basada en funciones necesarios para que la aplicación de aprobaciones funcione. Después de hacer clic en el enlace, debe configurar manualmente los valores de Nombre de usuario y Contraseña, así como aquellos valores que no se configuren automáticamente.

En algunos entornos, es posible que no pueda acceder al correo electrónico desde el dispositivo. Si no puede recibir correo electrónico en su dispositivo, puede usar en su lugar el dispositivo para explorar un código QR personalizado que le proporcione el administrador de Identity Manager.

Muestre el código QR proporcionado en su equipo o en una página impresa, si fuera necesario, y explórelo con un lector de código QR en el dispositivo. Después de que el código QR haya configurado automáticamente la aplicación de aprobaciones para su entorno, configure manualmente los valores de Nombre de usuario y Contraseña.

Configuración manual de la aplicación de aprobaciones

Si el administrador del entorno de Identity Manager no le proporciona un enlace ni un código QR para configurar la aplicación de aprobaciones, puede hacerlo manualmente.

Advertencia: dado que la configuración manual de la aplicación en el dispositivo requiere conocimientos profundos de los componentes de Identity Manager, se recomienda que solo los usuarios avanzados con conocimientos del módulo de provisión basada en funciones y el entorno de la aplicación de usuario de la empresa realicen la configuración manual de la aplicación. Los demás usuarios deberán ponerse en contacto con el administrador de Identity Manager para obtener información sobre cómo configurar la aplicación.

En la aplicación, haga clic en el icono Configuración , especifique la configuración necesaria y haga clic en el icono Probar conexión  para verificar la configuración.

La aplicación de aprobaciones requiere los valores siguientes:

Login Setting Name (Nombre del valor de entrada)	Login Setting Description (Descripción del valor de entrada)
Username (Nombre de usuario)	Especifica el nombre de usuario que se usa para acceder al servidor del módulo de provisión basada en funciones.
Password (Contraseña)	Especifica la contraseña que se usa para acceder al servidor del módulo de provisión basada en funciones.

Login Setting Name (Nombre del valor de entrada)	Login Setting Description (Descripción del valor de entrada)
Data Sync (Sincronización de datos)	Especifica si desea que la aplicación sincronice de forma activa los datos con el servidor del módulo de provisión basada en funciones.
Advanced > Server Details > Server (Opciones avanzadas > Detalles del servidor > Servidor)	Especifica el nombre completo o la dirección IP del servidor del módulo de provisión basada en funciones.
Advanced > Server Details > Secure Port (Opciones avanzadas > Detalles del servidor > Puerto seguro)	Especifica el puerto HTTP que usa la aplicación para conectarse con el servidor.
Advanced > Server Details > Context (Opciones avanzadas > Detalles del servidor > Contexto)	Especifica el contexto usado al instalar el archivo WAR de la aplicación de usuario. El valor por defecto es IDMProv.
Advanced > Server Details > User Container (Opciones avanzadas > Detalles del servidor > Contenedor de usuarios)	Especifica el nombre completo del contenedor del repositorio seguro de identidades donde se almacena la información del usuario.
Advanced > Server Details > Timeout (Opciones avanzadas > Detalles del servidor > Tiempo límite)	Especifica el número de segundos que la aplicación espera al intentar conectar con el servidor antes de cancelar la conexión. El valor por defecto es 5 segundos.
Advanced > Data Definition Settings > User Entity (Opciones avanzadas > Configuración de definición de datos > Entidad de usuario)	Especifica la entidad LDAP que representa a un usuario en el repositorio seguro de identidades. El valor por defecto es user.
Advanced > Data Definition Settings > Name Format (Opciones avanzadas > Configuración de definición de datos > Formato de nombre)	Especifica la representación del atributo DAL que usa la aplicación para dar formato al nombre completo de un usuario. El valor por defecto es FirstName LastName.
Advanced > Data Definition Settings > First Name Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de nombre)	Especifica el nombre del atributo DAL que representa el nombre de un usuario. El valor por defecto es FirstName.
Advanced > Data Definition Settings > Last Name Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de apellidos)	Especifica el nombre del atributo DAL que representa los apellidos de un usuario. El valor por defecto es LastName.
Advanced > Data Definition Settings > User Photo Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de foto de usuario)	Especifica el nombre del atributo DAL que contiene la foto de un usuario. El valor por defecto es UserPhoto. Nota: si no tiene ninguna imagen configurada en Identity Manager o ha configurado Identity Manager para que no muestre ninguna imagen, la aplicación muestra en su lugar una imagen genérica.
Advanced > Data Definition Settings > Work Phone Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de teléfono del trabajo)	Especifica el nombre del atributo DAL que representa el número de teléfono del trabajo de un usuario. El valor por defecto es TelephoneNumber.

Login Setting Name (Nombre del valor de entrada)	Login Setting Description (Descripción del valor de entrada)
Advanced > Data Definition Settings > Mobile Phone Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de teléfono móvil)	Especifica el nombre del atributo DAL que representa el número móvil de un usuario. El valor por defecto es <code>mobile</code> .
Advanced > Data Definition Settings > Email Attr (Opciones avanzadas > Configuración de definición de datos > Atributo de correo electrónico)	Especifica el nombre del atributo DAL que representa la dirección de correo electrónico de un usuario. El valor por defecto es <code>Email</code> .
Advanced > Data Definition Settings > Photo LDAP Attr (Opciones avanzadas > Configuración de definición de datos > Atributo LDAP de foto)	Especifica el nombre del atributo LDAP que contiene la foto del usuario. El valor por defecto es <code>photo</code> .
Advanced > Data Definition Settings > Naming Attribute (Opciones avanzadas > Configuración de definición de datos > Atributo de denominación)	Especifica el atributo DAL de denominación usado en el repositorio seguro de identidades para describir un nombre. El valor por defecto es <code>CN</code> .
Advanced > Data Definition Settings > Provisioning Admin (Opciones avanzadas > Configuración de definición de datos > Administrador de provisión)	Especifica si el usuario es un administrador de provisión en el servidor del módulo de provisión basada en funciones.
Advanced > Accepted Certificates (Opciones avanzadas > Certificados aceptados)	Especifica cualquier certificado no válido o autofirmado del servidor del módulo de provisión basada en funciones que se permite que la aplicación de aprobaciones acepte. Cuando la aplicación de aprobaciones detecte un certificado autofirmado o no válido, le pedirá que acepte o rechace el certificado. Si acepta el certificado, la aplicación lo añadirá a la lista de certificados aceptados. Es posible eliminar un certificado de la lista de certificados aceptados. Para ello, debe hacer clic en el nombre del certificado y reiniciar la aplicación. Nota: si el certificado del servidor del módulo de provisión basada en funciones es válido, la aplicación no añade el certificado a la lista de certificados aceptados. La aplicación acepta por defecto los certificados válidos.

Login Setting Name (Nombre del valor de entrada)	Login Setting Description (Descripción del valor de entrada)
Advanced > Rejected Certificates (Opciones avanzadas > Certificados rechazados)	Especifica cualquier certificado no válido o autofirmado del servidor del módulo de provisión basada en funciones que no desea que la aplicación de aprobaciones acepte. Cuando la aplicación de aprobaciones detecte un certificado autofirmado o no válido, le pedirá que acepte o rechace el certificado. Si rechaza el certificado, la aplicación lo añade a la lista de certificados rechazados. Si el servidor presenta entonces un certificado rechazado, la aplicación no puede crear una conexión con el servidor. Es posible eliminar un certificado de la lista de certificados rechazados. Para ello, debe hacer clic en el nombre del certificado.

Descripción general de la aplicación de aprobaciones

En esta sección se proporciona una descripción general de la interfaz del usuario de la aplicación de aprobaciones de NetIQ Identity Manager. Los temas son los siguientes:

- ♦ [“Vista Tareas” en la página 95](#)
- ♦ [“Vista Detalles” en la página 96](#)
- ♦ [“Modo por lotes” en la página 96](#)
- ♦ [“Vista Tareas completadas” en la página 96](#)
- ♦ [“Vista Ajustes de inicio de sesión” en la página 97](#)
- ♦ [“Vista Configuración avanzada” en la página 97](#)

Vista Tareas

La vista por defecto de la aplicación de aprobaciones es la vista Tareas. En ella se muestran todas las tareas que tiene asignadas actualmente o que ha reclamado, con el título de la tarea y el nombre y la imagen del destinatario. La vista muestra las tareas ordenadas por fecha de caducidad, con las que caducan antes en la parte superior y las que no tienen fecha de caducidad abajo.

Nota

- ♦ Si un usuario no tiene ninguna imagen configurada en Identity Manager o ha configurado Identity Manager para que no muestre ninguna imagen, la aplicación muestra en su lugar una imagen genérica.
- ♦ Con la aplicación de aprobación, no es posible aprobar ni denegar tareas que utilicen formularios complejos.
- ♦ En la actualidad, la aplicación de aprobaciones no admite nuevos formularios JSON en las plataformas iOS ni Android. Como resultado, es posible que se produzca un mensaje de error o que no pueda ver los detalles de la tarea.

Si desea aprobar o denegar una petición, o si desea ver los detalles de una tarea concreta, haga clic en la tarea o en el nombre del destinatario. Si desea ponerse en contacto con el destinatario de una tarea, haga clic en su imagen.

Vista Detalles

La vista Detalles muestra detalles sobre una tarea concreta que tenga asignada. Los campos que se muestran varían según la petición.

Para aprobar o denegar una tarea, proporcione la información necesaria y haga clic en **Aprobar** o en **Denegar**.

Modo por lotes

Si necesita aprobar o denegar muchas tareas similares, puede cambiar del modo por defecto de una sola tarea al modo por lotes en la vista Tareas.

Nota: no es posible aprobar todas las tareas en el modo por lotes. Las tareas más complejas, como las de certificación, se deben aprobar por separado en el modo de una sola tarea. Cuando se hace clic en el icono del modo por lotes, la aplicación muestra solo las tareas de la lista que se pueden aprobar en este modo.

Para aprobar o denegar varias tareas:

- 1 En la vista Tareas, haga clic en el icono del modo por lotes .
- 2 Seleccione las tareas que desea aprobar o denegar. No es posible aprobar algunas tareas y denegar otras al mismo tiempo.
- 3 (Opcional) Si desea aprobar o denegar todas las tareas, haga clic en **Todas**.
- 4 (Opcional) Si cambia de opinión y no desea aprobar o denegar varias tareas, haga clic en el icono del modo de una sola tarea .
- 5 Haga clic en **Aprobar** o en **Denegar**.
- 6 (Opcional) Incluya un comentario sobre la operación por lotes.
- 7 Haga clic en **Confirmar**.

Vista Tareas completadas

Para ver las tareas completadas, haga clic en el icono Tareas completadas . La vista muestra las tareas completadas, así como la hora a la que se aprobó o denegó la tarea. Puede hacer clic en una tarea completada para ver sus detalles concretos. En el caso de las peticiones más complejas, puede hacer clic en **Form Values** (Valores del formulario) para ver información específica de la petición.

Si fuera necesario, puede suprimir una o varias tareas completadas de la vista Tareas completadas.

Para suprimir tareas, haga clic en el icono del modo por lotes , seleccione las tareas que desea suprimir y haga clic en **Suprimir**.

Nota: la vista Tareas completadas solo muestra las tareas completadas en el dispositivo. No es posible ver las que se han completado en la aplicación de usuario ni en otros dispositivos que tengan instalada la aplicación de aprobaciones.

Vista Ajustes de inicio de sesión

La vista Ajustes de inicio de sesión permite ver o modificar la configuración de entrada.

Advertencia: si su administrador de Identity Manager le ha proporcionado un enlace o un código QR para configurar automáticamente la aplicación, es recomendable que no modifique los valores por defecto, a no ser que el administrador le indique que lo haga.

Vista Configuración avanzada

La vista Configuración avanzada permite ver o modificar los valores avanzados que determinan cómo se reciben los datos desde el servidor del módulo de provisión basada en funciones.

Advertencia: si su administrador de Identity Manager le ha proporcionado un enlace o un código QR para configurar automáticamente la aplicación, es recomendable que no modifique los valores por defecto, a no ser que el administrador le indique que lo haga.

Si cambia por accidente la configuración de la definición de datos de la vista Configuración avanzada, haga clic en **Restaurar valores por defecto** para recuperar la configuración por defecto proporcionada con Identity Manager. **Restaurar valores por defecto** no cambia el nombre de usuario, la contraseña ni ningún valor de los detalles del servidor.

Cambio del idioma de visualización de la aplicación de aprobaciones

La aplicación de aprobaciones incluye cadenas de texto traducidas en varios idiomas. Para cambiar el idioma que se usa en la aplicación de aprobaciones, cambie el valor de idioma y el formato regional del dispositivo iOS. El valor de formato regional permite configurar cómo se muestran las fechas, las horas y los números de teléfono en el dispositivo.

Para modificar el idioma y la configuración regional:

- 1 En el dispositivo iOS, haga clic en **Ajustes**.
- 2 Haga clic en **General**.
- 3 Haga clic en **Internacional**.
- 4 (Opcional) Si desea cambiar el idioma que se usa en el dispositivo, haga clic en **Idioma**, seleccione el idioma que desea usar y haga clic en **Hecho**.
- 5 (Opcional) Si desea cambiar el formato regional que se usa en el dispositivo para las fechas y las horas, haga clic en **Formato regional**, seleccione el formato que desea usar y haga clic en **Internacional**.
- 6 Vuelva a la pantalla de inicio del dispositivo.