



NetIQ® Identity Manager

Guida dell'utente alle applicazioni di identità

Maggio 2024

Note legali

Copyright 2009-2024 Open Text.

Le uniche garanzie per i prodotti e servizi di Open Text e dei suoi affiliati e licenziatari ("Open Text") sono quelle indicate nelle dichiarazioni di garanzia esplicite che accompagnano tali prodotti e servizi. Nulla di quanto riportato nel presente documento deve essere interpretato come garanzia aggiuntiva. Open Text non sarà da ritenersi responsabile per errori tecnici o editoriali contenuti nel presente documento né per eventuali omissioni. Le informazioni di questo documento sono soggette a modifiche senza preavviso.

Per ulteriori informazioni, ad esempio note relative alla certificazione e marchi di fabbrica, vedere <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).

Sommario

Informazioni sulla guida e sulla libreria	7
Parte I Informazioni generali su Identity Manager	9
1 Introduzione	11
Caratteristiche di ruoli e risorse	11
Caratteristiche delle applicazioni di identità	11
Informazioni sul Dashboard di Identity Manager	11
Presentazione del Dashboard	12
Informazioni sulla pagina Applicazioni	13
Comprensione dei task	14
Impieghi standard delle applicazioni di identità	14
Come funziona Self-Service identità	14
Come funzionano ruoli e risorse	14
Come funzionano le richieste di processo	16
Come funziona l'help desk?	16
2 Accesso alle applicazioni di identità	19
Considerazioni sull'accesso alle applicazioni di identità	19
Esecuzione del login per la prima volta	20
Risposta a una verifica delle impostazioni internazionali preferite	22
Risoluzione dei problemi di login	22
Password dimenticata	22
Problemi relativi al login	22
Eventuali ulteriori informazioni richieste	23
Disconnessione	23
Parte II Personalizzazione del dashboard	25
3 Gestione di widget e layout	27
Gestione del dashboard globale	28
Modifica del layout del Dashboard	28
Aggiunta di un widget	29
Aggiungere widget generici	30
Aggiunta di widget di Identity Manager	31
Aggiunta di widget di Identity Governance	32
Opzioni widget	32
Configurazione di un widget	33

Parte III Gestione delle autorizzazioni e del profilo di identità	35
4 Gestione delle richieste di autorizzazione	37
Visualizzazione delle autorizzazioni	37
Richiesta di autorizzazioni	39
Visualizzazione delle richieste	39
Controllo di una richiesta	40
Annullamento di una richiesta	40
Emissione di un ticket per l'help desk	40
Revoca delle autorizzazioni	41
Collegamento profondo a una richiesta	42
5 Gestione delle applicazioni	45
Creazione di elementi di rilievo	45
Aggiunta di un'applicazione	45
Aggiunta di un'autorizzazione	46
Aggiunta, modifica o eliminazione di una categoria	46
Per aggiungere una categoria	46
Modifica una categoria	46
Eliminazione di una categoria	47
6 Gestione di task personali	49
Visualizzazione dei task	49
Gestione delle richieste da approvare o rifiutare	50
Gestione dei task dell'help desk	51
7 Agire per conto di qualcun altro	53
Visualizzazione delle assegnazioni di utenti incaricati personali	53
Agire come utente incaricato	53
Gestione delle assegnazioni di utenti incaricati	53
8 Gestione delle deleghe	55
9 Gestione della disponibilità	57
10 Gestione del profilo personale	59
Aggiornamento del proprio profilo	59
11 Gestione dell'organigramma	61
Visualizzazione di un organigramma	61
Descrizione dell'organigramma	62
Utilizzo dell'organigramma	63
Reimpostazione della radice nella vista dell'organigramma	64
Passaggio alla vista dell'organigramma	64
Scelta di una relazione da visualizzare	65
Passaggio al livello successivo della gerarchia delle relazioni	66

Invio di e-mail agli utenti dall'organigramma	67
Visualizzazione di informazioni dettagliate su un utente	67
12 Gestione della password	69
Utilizzo di Self-Service Password Management in Identity Manager	69
Descrizione della domanda/risposta di autenticazione della password	70
Modifica della password	70
Stato norme password	71
Utilizzo della gestione password esistente	71
Autenticazione CHAP password	72
Cambio suggerimento password	73
Cambia password	73
Stato norme password	74
Stato sincronizzazione password	75
Parte IV Gestione di utenti, gruppi e team	77
13 Gestione degli utenti	79
Creazione di un utente	79
Modifica delle informazioni utente	79
Elenco degli utenti	80
Individuazione degli utenti	81
Ordinamento degli utenti	82
14 Gestione dei team	83
Visualizzazione dei team	83
Creazione di un team	84
Modifica di un team	84
15 Gestione dei gruppi	85
Creazione di un gruppo	85
Parte V Appendice	87
A Utilizzo dell'app Identity Manager Approvals	89
Requisiti del prodotto	89
Installazione dell'app Approvals	90
Configurazione dell'app Approvals	90
Richiesta dell'accesso mobile tramite l'applicazione utente	90
Utilizzo di un collegamento di configurazione o di un codice QR	91
Configurazione manuale dell'app Approvals	91
Panoramica dell'app Approvals	94
Vista Task	94
Vista Dettagli	95
Modalità in massa	95
Vista Task completati	95
Vista Impostazioni di login	96

Vista Impostazioni avanzate	96
Modifica della lingua visualizzata dell'app Approvals	96

Informazioni sulla guida e sulla libreria

In questa Guida sono descritte le varie modalità di utilizzo delle applicazioni di identità NetIQ Identity Manager da parte di utenti finali e alcuni amministratori, in particolare il Dashboard e l'Applicazione utente.

Destinatari

Le informazioni contenute in questo manuale sono rivolte a coloro che devono apprendere i concetti relativi all'amministrazione e che devono implementare un modello di amministrazione sicuro e distribuito.

Altre informazioni incluse nella libreria

Per ulteriori informazioni sulla libreria di Identity Manager, vedere il [sito Web relativo alla documentazione di Identity Manager \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

Informazioni generali su Identity Manager

NetIQ Identity Manager è un prodotto software di sistema utilizzato dalle organizzazioni per gestire in modo sicuro le esigenze di accesso delle rispettive comunità di utenti. I membri di tali comunità possono trarre vantaggio dall'utilizzo di Identity Manager in diversi modi. Identity Manager consente ad esempio alle organizzazioni di:

- ♦ Garantire agli utenti accesso immediato alle informazioni (ad esempio organigrammi, pagine bianche o funzionalità di ricerca dei dipendenti), ai ruoli e alle risorse (quali dispositivi o account su sistemi interni) di cui hanno necessità.
- ♦ Sincronizzare più password in un unico login valido per tutti i sistemi.
- ♦ Modificare o revocare immediatamente i diritti di accesso quando necessario, ad esempio nel caso di utenti che vengono trasferiti a un altro gruppo oppure che lasciano l'organizzazione.
- ♦ Mantenere la conformità alle normative di legge.

Leggere innanzitutto questa sezione contenente informazioni introduttive sulle applicazioni di identità di Identity Manager e su come iniziare a utilizzarle. Questa Guida è stata ideata per supportare i seguenti tipi di attività online all'interno dell'organizzazione dell'utente:

- ♦ Gestire l'identità online associata alle risorse organizzative.
- ♦ Visualizzare o modificare l'accesso a ruoli e risorse organizzativi.
- ♦ Approvare richieste per accedere a risorse e ruoli.
- ♦ Gestire le autorizzazioni associate alle applicazioni software e altre risorse offerte dall'organizzazione ai propri membri.

1 Introduzione

In questa sezione viene illustrato come iniziare a utilizzare le applicazioni di identità. Gli argomenti trattati sono i seguenti:

- ♦ [“Caratteristiche di ruoli e risorse” a pagina 11](#)
- ♦ [“Caratteristiche delle applicazioni di identità” a pagina 11](#)
- ♦ [“Informazioni sul Dashboard di Identity Manager” a pagina 11](#)
- ♦ [“Presentazione del Dashboard” a pagina 12](#)
- ♦ [“Comprensione dei task” a pagina 14](#)
- ♦ [“Impieghi standard delle applicazioni di identità” a pagina 14](#)

Caratteristiche di ruoli e risorse

Nelle applicazioni di identità, un'**autorizzazione** rappresenta l'accesso fornito a un utente o a un gruppo di utenti per un ruolo o una risorsa. Un **ruolo** definisce un gruppo di autorizzazioni correlate a uno o più sistemi o applicazioni di destinazione. Ad esempio, il ruolo amministratore utenti può essere autorizzato a reimpostare la password di un utente, mentre un ruolo amministratore di sistema può assegnare un utente a un server specifico. Una **risorsa** è un'entità digitale quale un account utente, un computer o un database al quale un utente dell'azienda deve poter accedere.

Caratteristiche delle applicazioni di identità

Le applicazioni di identità di Identity Manager sono un set interconnesso di applicazioni Web basate su browser. Tali applicazioni consentono alle organizzazioni di gestire gli account utente e le autorizzazioni associati a un'ampia gamma di ruoli e risorse disponibili per gli utenti. È possibile configurare le applicazioni di identità per fornire supporto self-service per gli utenti, ad esempio per richiedere ruoli o modificarne le password. È inoltre possibile configurare i workflow per migliorare l'efficienza nella gestione e nell'assegnazione di ruoli e risorse.

Informazioni sul Dashboard di Identity Manager

Il Dashboard di NetIQ Identity Manager (Dashboard) funge da portale di ingresso principale alle applicazioni di identità. Contiene uno o più widget di supporto che forniscono informazioni rapide su un'attività particolare. Dal Dashboard, è possibile eseguire le attività seguenti:

- ♦ Gestire la password e le impostazioni del profilo.
- ♦ Visualizzare i dettagli dell'organigramma.
- ♦ Rivedere e completare task, come l'approvazione delle richieste degli utenti per l'accesso.
- ♦ Richiedere autorizzazioni per ruoli, risorse o processi.
- ♦ Rivedere lo stato e la cronologia delle richieste di autorizzazioni.

- ♦ Individuare altri utenti all'interno dell'organizzazione.
- ♦ Personalizzare il dashboard, è possibile aggiungere widget e riposizionarli in base agli interessi.
- ♦ Impostare qualsiasi utente come incaricato dal sistema.
- ♦ Delegare i task ad altri utenti dal sistema.

È possibile eseguire i seguenti task con le **autorizzazioni** appropriate:

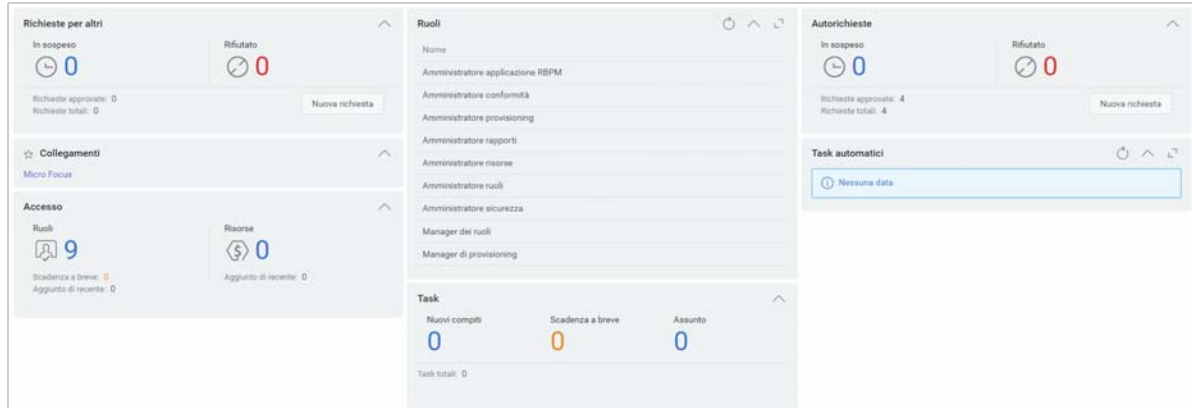
- ♦ Creare e modificare profili utente.
- ♦ Visualizzare i dettagli dell'organigramma di altri utenti.
- ♦ Creare e modificare team che rappresentano un insieme di utenti e gruppi in grado di eseguire richieste di provisioning e task di approvazione associati ai team.
- ♦ Richiedere o revocare autorizzazioni per conto di altri utenti nell'organizzazione.

Presentazione del Dashboard

Nel Dashboard sono disponibili informazioni rapide su task, autorizzazioni e richieste sotto forma di widget. È possibile spostarsi tra pagine o applicazioni specifiche con un singolo clic. È inoltre possibile aggiungere, rimuovere, riposizionare e configurare i widget sul Dashboard. Per ulteriori informazioni sulla personalizzazione del Dashboard, vedere il [Capitolo 3, “Gestione di widget e layout”](#), a pagina 27.

L'esempio qui sotto descrive le opzioni dei widget di default nel Dashboard.

Figura 1-1 Esempio di Dashboard personale



Il Dashboard di Identity Manager consente di gestire diverse attività su Identity Manager. Le pagine seguenti consentono di gestire task e attività:

Applicazione

Elenca tutte le applicazioni fornite per l'utente. Presenta collegamenti di default per diverse aree per semplificare i task di base da eseguire in Identity Manager. Per ulteriori informazioni, vedere [“Informazioni sulla pagina Applicazioni”](#) a pagina 13.

Task

Mostra tutti i task in attesa di un'azione. Con un ruolo appropriato, è possibile visualizzare i task di altri utenti, ad esempio, un manager del team.

Accesso

Consente di visualizzare autorizzazioni o richiedere autorizzazioni. Per visualizzare lo stato delle autorizzazioni richieste, selezionare **Cronologia richieste?**. Questa pagina visualizza tutte le richieste e il loro stato.

Persone

Consente di visualizzare altri utenti o gruppi nel sistema e l'**Organigramma** di altri utenti, consentendo loro di visualizzare come tali utenti e gruppi sono correlati.

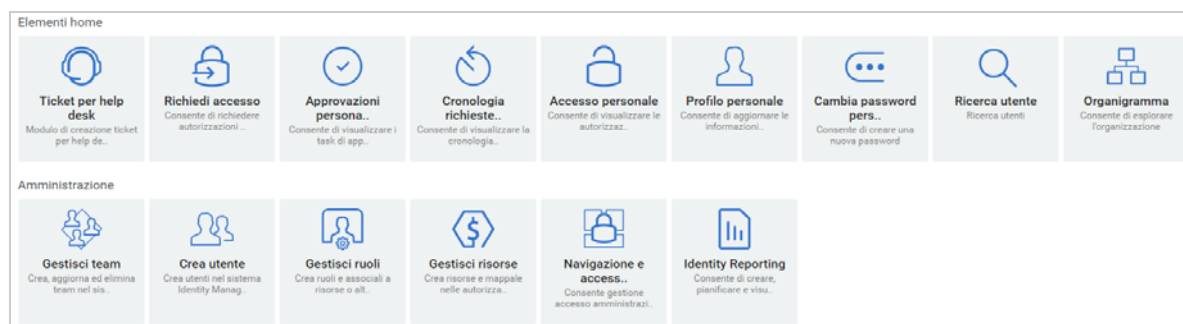
Amministrazione

Consente di visualizzare e gestire ruoli, risorse, riconciliazione autorizzazione e relative configurazioni. Questa opzione è solo per gli amministratori. Per ulteriori informazioni sui task amministrativi, vedere [Identity Applications Administration](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).

Informazioni sulla pagina Applicazioni

La seconda vista significativa nel Dashboard è la pagina **Applicazioni** (Figura 1-2), in cui sono forniti i collegamenti di default a diverse aree per semplificare i task di base che utenti finali e amministratori devono eseguire in Identity Manager.

Figura 1-2 Esempio della pagina Applicazioni nel Dashboard



Per default, **Ticket per help desk** compare sulla pagina **Applicazioni**. Questa opzione consente di emettere un ticket per l'help desk.

L'amministratore di identità personalizza la pagina **Applicazioni** in modo da includere le sezioni che si collegano alle risorse richieste comunemente o alle applicazioni alle quali accedono regolarmente gli utenti. Con il ruolo amministrativo appropriato è possibile configurare l'accesso degli utenti a questi riquadri. Accedere a **ID utente > Impostazioni > Accesso** per aggiungere trustee per gli elementi di navigazione richiesti. Per ulteriori informazioni sul provisioning degli accessi, vedere [Managing User Access](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).

Alcuni riquadri della pagina potrebbero essere visibili solo per gli utenti dotati di un ruolo amministrativo nelle applicazioni di identità. Ad esempio, una persona autorizzata a creare o modificare i ruoli dovrebbe visualizzare una sezione simile a **Crea utente** e **Gestisci ruoli**.

Per ulteriori informazioni sull'uso del Dashboard, fare clic su al suo interno.

Comprensione dei task

La pagina **Task** consente di approvare o rifiutare azioni per i task elencati.

Il Dashboard di Identity Manager consente di gestire i task di Identity Manager e Identity Governance dalla pagina Task. Adesso è possibile visualizzare e approvare sia i task di Identity Manager che i task di Identity Governance dalla stessa interfaccia utente.

Impieghi standard delle applicazioni di identità

Di seguito sono riportati alcuni esempi tipici di impiego delle applicazioni di identità in un'organizzazione.

- ♦ [“Come funziona Self-Service identità” a pagina 14](#)
- ♦ [“Come funzionano ruoli e risorse” a pagina 14](#)
- ♦ [“Come funzionano le richieste di processo” a pagina 16](#)
- ♦ [“Come funziona l'help desk?” a pagina 16](#)

Come funziona Self-Service identità

- ♦ Elena (un utente finale) recupera la sua password dimenticata tramite le funzionalità della scheda Self-service identità al momento del login.

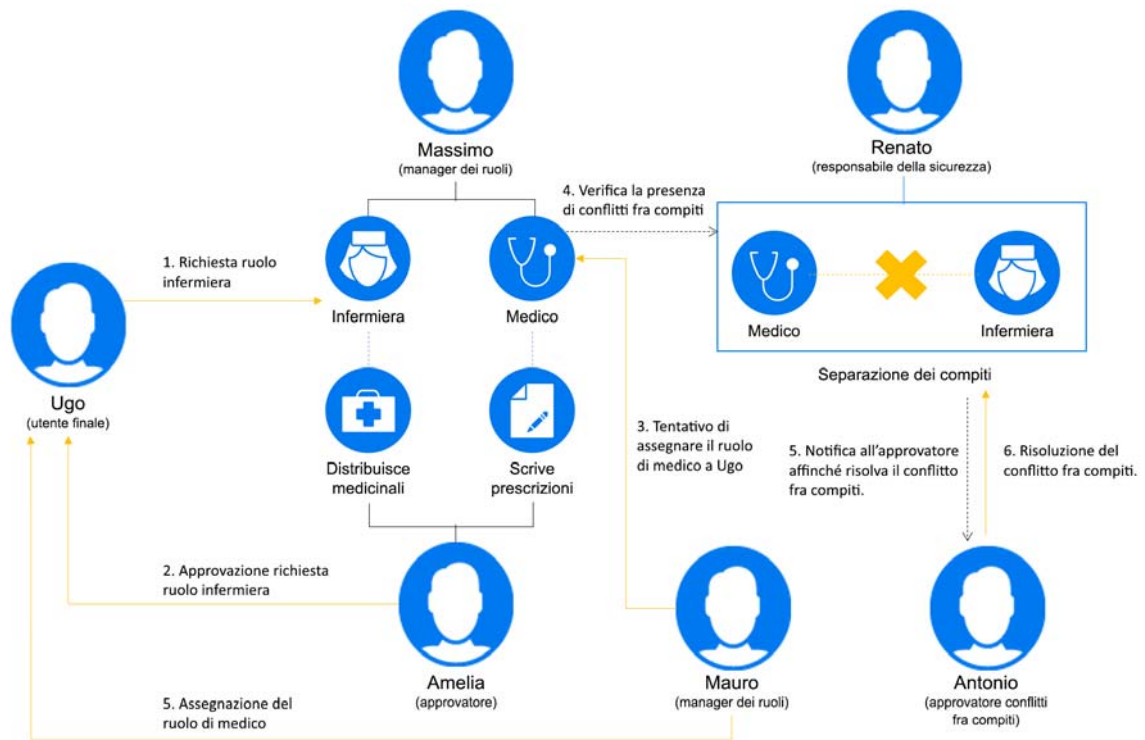
Per default, in Identity Manager viene utilizzata l'applicazione Self Service Password Reset (SSPR) per consentire agli utenti di modificare le rispettive password. Le applicazioni di identità possono tuttavia utilizzare altri metodi per gestire le password dimenticate.

- ♦ Erica, un utente finale, esegue una ricerca su tutti i dipendenti che parlano tedesco presso la sua sede.
- ♦ Edoardo (un utente finale) esplora l'organigramma, individua Elena e fa clic sull'icona dell'e-mail per inviarle un messaggio.

Come funzionano ruoli e risorse

Di seguito viene fornito un esempio che spiega il flusso della richiesta di risorse e ruoli nel sistema:

Figura 1-3 Scenario di esempio dell'assegnazione di un ruolo



- ♦ Massimo, un manager dei ruoli, crea i ruoli aziendali Infermiere e Medico e i ruoli IT Farmaci da banco e Prescrizioni ricette. Crea quindi diverse risorse necessarie per questi ruoli e le associa ai ruoli.
- ♦ Massimo, un manager dei ruoli, definisce una relazione fra i ruoli Infermiere e Farmaci da banco, specificando che il ruolo Infermiere contiene il ruolo Farmaci da banco. Massimo definisce inoltre una relazione fra i ruoli Prescrizioni ricette e Medico, specificando che il ruolo Medico contiene il ruolo Prescrizioni ricette.
- ♦ Paolo, un responsabile della sicurezza, definisce un vincolo di separazione dei compiti che specifica l'esistenza di un potenziale conflitto tra i ruoli Medico e Infermiere. Ciò significa che, di solito, lo stesso utente non dovrebbe essere assegnato a entrambi i ruoli contemporaneamente. In alcuni casi, un singolo utente che richiede un'assegnazione ruolo può richiedere di ignorare questo vincolo. Per definire un'eccezione di separazione dei compiti, il singolo utente che richiede l'assegnazione deve fornire una giustificazione.
- ♦ Ernesto, un utente finale, consulta un elenco di ruoli disponibili e richiede l'assegnazione al ruolo Infermiere.
- ♦ Francesca, un approvatore, riceve la notifica di una richiesta di approvazione tramite un messaggio e-mail, contenente un URL. Quando fa clic sul collegamento, viene visualizzato un modulo di approvazione che le consente di effettuare l'approvazione.
- ♦ Aldo, un manager dei ruoli, richiede che Ernesto venga assegnato al ruolo Medico. Riceve tuttavia la notifica di un possibile conflitto tra il ruolo Medico e il ruolo Infermiere al quale Ernesto è già stato assegnato. Aldo fornisce quindi una giustificazione per la creazione di un'eccezione del vincolo di separazione dei compiti.

- ♦ Edoardo, un approvatore della separazione dei compiti, riceve la notifica via e-mail di un conflitto di separazione dei compiti. Approva la richiesta di Aldo di ignorare il vincolo di separazione dei compiti.
- ♦ Amalia, un approvatore, riceve una notifica via e-mail di approvazione del ruolo Medico. Approva quindi la richiesta di Aldo per assegnare Ernesto al ruolo Medico.
- ♦ Marco, un revisore dei ruoli, consulta il campo Rapporto violazione separazioni dei compiti ed eccezioni e nota che Ernesto è stato assegnato a entrambi i ruoli Medico e Infermiere. Inoltre, si accorge che a Ernesto sono state assegnate le risorse associate a questi ruoli.

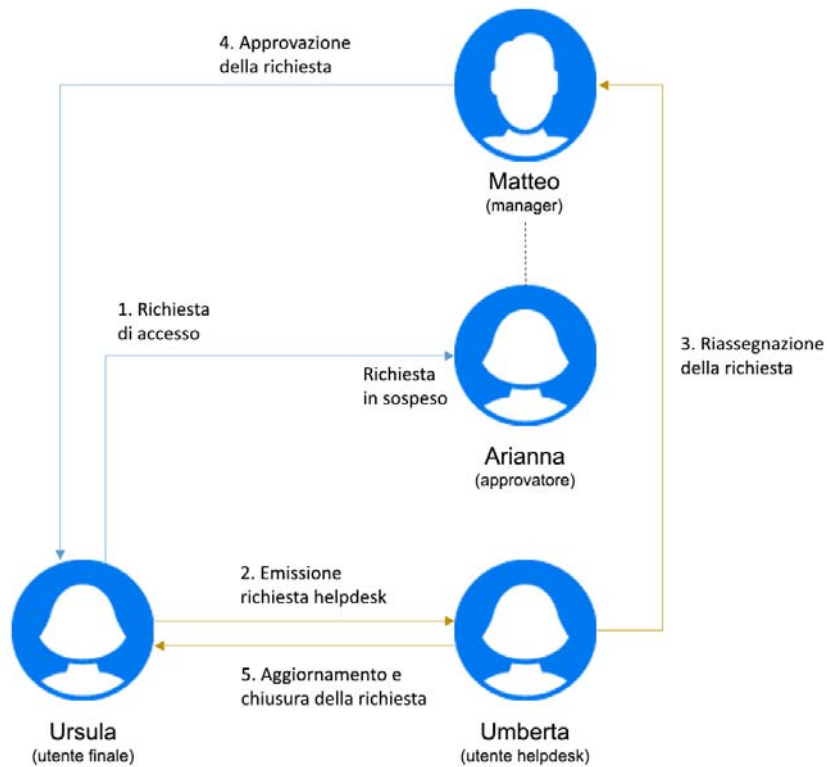
Come funzionano le richieste di processo

- ♦ Mario (un utente finale) consulta un elenco di risorse disponibili e richiede l'accesso al sistema Siebel*.
- ♦ Francesca (un utente approvatore) riceve la notifica di una richiesta di approvazione tramite un messaggio e-mail contenente un URL. Quando fa clic sul collegamento, viene visualizzato un modulo di approvazione che le consente di effettuare l'approvazione.
- ♦ Mario controlla lo stato della sua richiesta di accesso a Siebel, la quale è ora passata a un secondo utente per l'approvazione. Constata quindi che la richiesta è ancora in corso di elaborazione.
- ♦ Francesca specifica che non sarà temporaneamente disponibile per ferie. Nessun nuovo task di approvazione le verrà assegnato durante il periodo di assenza.
- ♦ Francesca apre il suo elenco di task di approvazione, constata che non può rispondere tempestivamente ai troppi task disponibili e quindi ne riassegna molti di questi ai suoi colleghi.
- ♦ Giovanni, un assistente di amministrazione che agisce in qualità di utente incaricato per Francesca, apre l'elenco dei task di quest'ultima ed esegue un task di approvazione per conto della collega.
- ♦ Massimiliano (un manager) visualizza gli elenchi di task degli utenti del suo reparto. È a conoscenza del fatto che Francesca è assente e quindi riassegna i task ad altri utenti del reparto.
- ♦ Massimiliano avvia una richiesta relativa a un conto di database per un utente del reparto che è un suo diretto subordinato.
- ♦ Massimiliano designa Daniele come delegato autorizzato di Francesca.
- ♦ Daniele, in qualità ora di utente approvatore delegato, riceve i task di Francesca quando quest'ultima non è disponibile.
- ♦ Massimiliano assume uno stagista non retribuito, il quale non deve essere inserito nel sistema di gestione delle risorse umane. L'amministratore di sistema crea il record utente per lo stagista e richiede che gli venga concesso l'accesso a Notes, Active Directory* e Oracle*.

Come funziona l'help desk?

Di seguito viene fornito un esempio che spiega il flusso del ticket dell'help desk nel sistema:

Figura 1-4 Esempio per l'help desk



- ♦ Emilia (un utente finale) ha richiesto un accesso alla stampante dell'ufficio. La richiesta è rimasta troppo tempo in sospeso. Perciò, ha emesso un ticket per l'help desk.
- ♦ Elena (utente help desk) riceve una notifica del ticket per help desk nel suo elenco di task.
- ♦ Elena analizza il problema e trova che la richiesta è assegnata ad Amelia (approvatore).
- ♦ La richiesta è in sospeso nel sistema perché Amelia non è in ufficio.
- ♦ Elena ha un'autorizzazione per riassegnare le richieste di task. Riassegna la richiesta a Mattia (superiore di Amelia).
- ♦ Mattia esamina la richiesta e l'approva. Emilia può accedere alla stampante dell'ufficio.
- ♦ Elena aggiorna e chiude il ticket per help desk.

2 Accesso alle applicazioni di identità

È possibile accedere alle applicazioni di identità, quali il Dashboard, in un browser Web. Identity Manager supporta la maggior parte delle versioni dei browser più diffusi. Per ottenere un elenco dei browser supportati e assistenza relativa all'installazione, rivolgersi all'amministratore di sistema. L'organizzazione deve fornire l'URL e le credenziali richiesti per accedere alle applicazioni.

- ♦ [“Considerazioni sull'accesso alle applicazioni di identità” a pagina 19](#)
- ♦ [“Esecuzione del login per la prima volta” a pagina 20](#)
- ♦ [“Risposta a una verifica delle impostazioni internazionali preferite” a pagina 22](#)
- ♦ [“Risoluzione dei problemi di login” a pagina 22](#)
- ♦ [“Disconnessione” a pagina 23](#)

Considerazioni sull'accesso alle applicazioni di identità

Prima di accedere al Dashboard o a una delle altre applicazioni di identità, è opportuno tener conto delle seguenti considerazioni:

- ♦ È necessario abilitare i cookie e JavaScript* nel browser Web.
- ♦ Quando si utilizza Internet Explorer, si deve impostare almeno il livello di privacy **medio**. È anche necessario selezionare l'opzione **All'apertura della pagina Web** in **Strumenti > Opzioni Internet > Generale, Cronologia esplorazioni > Impostazioni > Ricerca versioni più recenti delle pagine memorizzate**. Se non si seleziona questa opzione, è possibile che alcuni pulsanti non vengano visualizzati correttamente.
- ♦ Se precedentemente si è eseguito l'accesso all'Applicazione utente di Identity Manager, potrebbe essere possibile utilizzare gli stessi nome utente e password per accedere al Dashboard.
- ♦ Non è possibile accedere alle applicazioni di identità se nel nome dell'account è incluso uno dei seguenti caratteri:

\ / , * ? . \$ # +

- ♦ Se risulta impossibile eseguire il login, è possibile fare clic su **Password dimenticata**. Per ulteriori informazioni, consultare la [“Password dimenticata” a pagina 22](#).
- ♦ Se all'accesso all'interfaccia utente di Identity Manager viene visualizzata una pagina iniziale diversa, è probabile che l'applicazione sia stata personalizzata per l'organizzazione. Durante l'utilizzo è possibile che altre funzioni delle applicazioni di identità risultino personalizzate.

In questo caso, è consigliabile rivolgersi all'amministratore di sistema per ottenere informazioni sulle differenze delle applicazioni di identità personalizzate rispetto alla configurazione di default descritta in questa Guida.

Esecuzione del login per la prima volta

Per eseguire il login alle applicazioni di identità, come il Dashboard, è necessario essere un utente autorizzato. Per ottenere nome utente e password per il login, rivolgersi all'amministratore del sistema.

La prima volta che si esegue il login alle applicazioni di identità, in Identity Manager viene richiesto di definire i parametri di sicurezza per l'account per agevolare la reimpostazione della password in futuro. Se si dimentica la password e si tenta di reimpostarla al login successivo, in Identity Manager verranno poste le domande configurate e sarà necessario fornire la risposta corretta. Quando la risposta corrisponde a quella salvata nella pagina, è possibile reimpostare la password.

Per configurare le domande di sicurezza al primo login:

- 1 Immettere nome utente e password, quindi fare clic su **Login**.
- 2 Dalla pagina di login si viene reindirizzati automaticamente alla pagina **Domanda/risposta di autenticazione**.
- 3 Specificare le domande e le risposte per le domande di sicurezza.

Imposta Domande di Sicurezza

[Esci](#)

Nel caso dimentichi la tua password, puoi recuperarla rispondendo a domande note solo a te.

Per favore scegli domande e risposte che possono essere usate per verificare la tua identità in caso dimentichi la password. Siccome le risposte alle domande possono essere usate per accedere con il tuo utente, fai attenzione a fornire risposte che non sono facili da indovinare o scoprire.

Per favore inserisci le risposte alle tue domande di sicurezza

— Selezionare una domanda dall'elenco —



— Selezionare una domanda dall'elenco —



— Selezionare una domanda dall'elenco —



— Selezionare una domanda dall'elenco —



» Salva Risposte

« Annulla

- 4 Fare clic su **Salva risposte** per essere reindirizzati al dashboard.

Risposta a una verifica delle impostazioni internazionali preferite

Se quando si esegue il login viene richiesto di selezionare le impostazioni internazionali preferite, l'amministratore ha configurato le applicazioni di identità in modo che venga eseguita una verifica della lingua sui browser degli utenti. Tale operazione potrebbe essere necessaria per garantire che il contenuto venga visualizzato in una lingua supportata.

Quando viene richiesto di aggiungere un'impostazione internazionale, aprire l'elenco **Impostazioni internazionali disponibili**, selezionare un'impostazione internazionale e fare clic su **Aggiungi**. Per ulteriori informazioni, vedere [Adding the New Language to the Identity Applications](#) (in lingua inglese).

Risoluzione dei problemi di login

In questa sezione viene spiegato come risolvere i problemi di login più comuni, indicati di seguito:

- ♦ [“Password dimenticata” a pagina 22](#)
- ♦ [“Problemi relativi al login” a pagina 22](#)
- ♦ [“Eventuali ulteriori informazioni richieste” a pagina 23](#)

Password dimenticata

Se si dimentica la password, è possibile utilizzare il collegamento **Password dimenticata** per ottenere assistenza. Quando viene richiesto di eseguire il login, questo collegamento viene visualizzato sulla pagina per default. È possibile utilizzarlo solo se l'amministratore di sistema ha impostato una policy password appropriata per l'utente.

- 1 Quando viene richiesto di eseguire il login fare clic sul collegamento **Password dimenticata**.
- 2 Digitare il nome utente e fare clic su **Invia**.
Se in Identity Manager viene segnalato che è impossibile trovare norme per le password, consultare l'amministratore di sistema per assistenza.
- 3 Rispondere alle domande di autenticazione visualizzate. In Identity Manager viene richiesto di rispondere alle domande configurate. Quando la risposta corrisponde a quella salvata precedentemente, è possibile reimpostare la password. Fare clic su **Invia**. Ad esempio:
Rispondere alle domande di autenticazione per ricevere assistenza per la password. In base all'impostazione delle policy password da parte dell'amministratore di sistema, è possibile:
 - ♦ Ricevere un'e-mail contenente la password relativa.
 - ♦ Verrà richiesto di reimpostare la password.

Problemi relativi al login

Se non è possibile eseguire il login, accertarsi di aver immesso il nome utente e la password correttamente (ortografia, lettere maiuscole e minuscole e così via). Se il problema persiste, rivolgersi all'amministratore del sistema. In questo caso, è utile fornire i dettagli relativi al problema verificatosi (ad esempio un messaggio di errore).

Eventuali ulteriori informazioni richieste

Ai fini del login, potrebbero essere richiesti altri tipi di informazioni, in base all'eventuale impostazione della policy da parte dell'amministratore di sistema. Ad esempio:

- ♦ Se si tratta del primo login dell'utente, viene richiesto di definire le domande di autenticazione e le relative risposte
- ♦ Se la password è scaduta, viene richiesto di reimpostarla

Disconnessione

Dopo aver utilizzato il Dashboard e altre applicazioni di identità, eseguire il logout. Nel Dashboard, fare clic sul nome utente nell'angolo in alto a destra, quindi selezionare **Disconnetti**.



Personalizzazione del dashboard

Le applicazioni di identità offrono molte opzioni per modificare la visualizzazione del *Dashboard* e salvarla come vista personalizzata. Ad esempio, è possibile aggiungere widget e riposizionarli in base all'interesse. È inoltre possibile configurare i campi del widget e personalizzarli. Questo documento consente di comprendere le diverse opzioni per personalizzare il *Dashboard*.

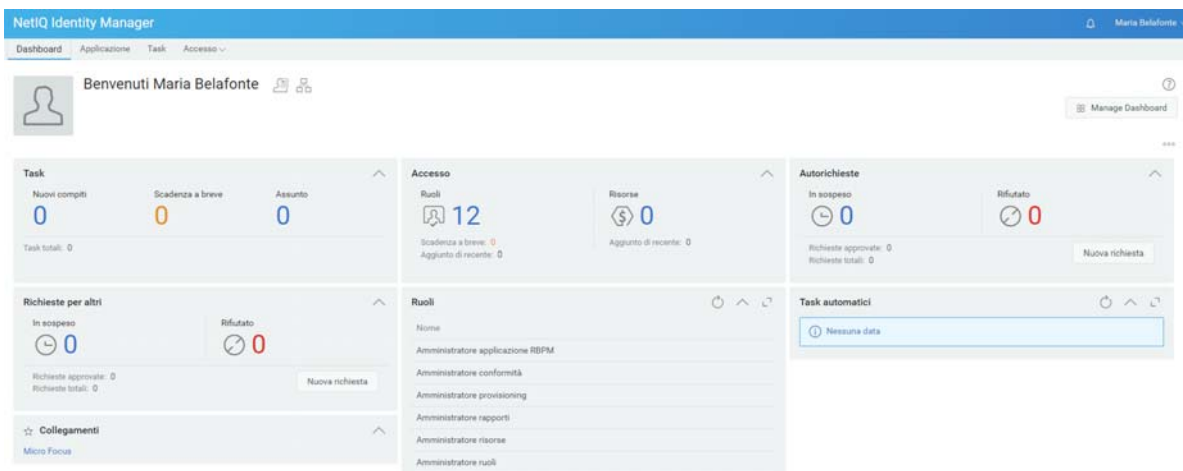
3 Gestione di widget e layout

I widget sono oggetti del Dashboard progettati per fornire a un utente dettagli specifici in merito a una determinata attività. Ad esempio, il widget **Task** offre dettagli sui nuovi task, sui task assunti o su quelli che scadranno a breve. Analogamente, è possibile configurare sul Dashboard molti altri widget.

Gli amministratori che hanno accesso alla pagina **Impostazioni** possono eseguire il provisioning dei widget per un utente, un gruppo, un container o un ruolo da **ID utente > Impostazioni > Widget dashboard**.

Per personalizzare il Dashboard, andare sul **Dashboard** e fare clic su **...**.

Figura 3-1 Personalizzare il dashboard



Utilizzare le opzioni seguenti per personalizzare il Dashboard:

Figura 3-2 Opzioni di personalizzazione



Widget

Consente di aggiungere widget al Dashboard. Vedere [“Aggiunta di un widget” a pagina 29](#).

Layout

Consente di modificare il layout del Dashboard. Vedere [“Modifica del layout del Dashboard” a pagina 28](#).

Annulla

Consente di annullare tutte le modifiche apportate al Dashboard.

Salva

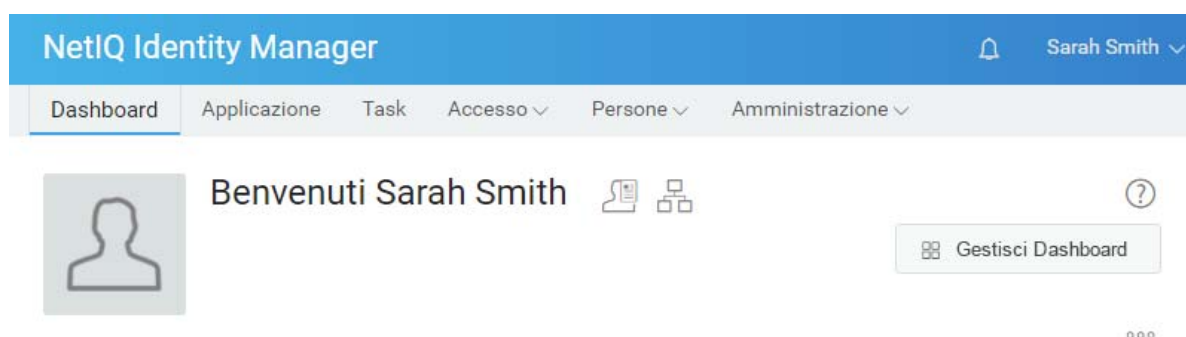
Consente di salvare le modifiche e di applicarle al Dashboard.

Gestione del dashboard globale

Nel dashboard globale è incluso un set di widget che viene visualizzato sul Dashboard di tutti gli utenti nel sistema. Gli utenti possono visualizzare tali widget in base al rispettivo accesso fornito loro da un amministratore. L'opzione **Gestisci dashboard** consente di aggiungere, modificare o rimuovere widget dal dashboard globale.

Nota: per utilizzare l'opzione **Gestisci dashboard** è necessario disporre dei diritti di accesso del trustee.

Figura 3-3 Esempio di dashboard globale



L'amministratore può aggiungere qualsiasi utente, gruppo, container o ruolo come trustee per gestire il dashboard globale. Per modificare i trustee in modo che possano gestire il dashboard, accedere a **ID utente > Impostazioni > Accesso** e dall'elenco fare clic su **Dashboard globale**. Per ulteriori informazioni su come modificare l'accesso alla configurazione, vedere [Managing Dashboard Widgets](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).

Modifica del layout del Dashboard

Le applicazioni di identità consentono di modificare il layout dell'aspetto dei widget sul Dashboard.

- 1 Nel **Dashboard** fare clic su **...**.
- 2 Selezionare **Layout**.
- 3 Scegliere il layout da vedere sul dashboard.

Figura 3-4 Cambiare i layout

MODIFICA DASHBOARD

×

Qualifica

Dashboard

Struttura

6-6

4-8

12/4-4-4

12/6-6

12/6-6/12

3-9 (12/6-6)

Importante: per applicare le modifiche, fare clic su **Salva**.

Aggiunta di un widget

Per aggiungere un nuovo widget al Dashboard, andare sul **Dashboard**, fare clic su **○○○** e selezionare **Widget**.

Figura 3-5 Aggiungere widget

AGGIUNGI NUOVO WIDGET

×

Generale

IDM

IG

Aggiungere widget generici

La categoria **Generale** consente di aggiungere al dashboard widget diversi da quelli standard di Identity Manager. È possibile specificare l'URL API REST del widget e visualizzare le informazioni desiderate sotto forma di grafici a linee, grafici a torta o tabelle.

1 Selezionare uno dei seguenti tipi di widget dall'elenco:

- ♦ **Grafico a linee:** visualizza le informazioni desiderate dell'elemento selezionato sotto forma di grafico a linee.
- ♦ **Collegamenti:** consente di salvare tra i segnalibri i collegamenti utilizzati più spesso per accedervi con rapidità.
- ♦ **Grafico a torta:** visualizza le informazioni desiderate dell'elemento selezionato sotto forma di grafico a torta.
- ♦ **Tabella:** elenca le informazioni richieste per l'elemento selezionato sotto forma di tabella.

2 Fare clic su  per configurare il widget aggiunto al dashboard.

3 (Condizionale) Per i widget **Grafico a linee**, **Grafico a torta** e **Tabella**, specificare i dettagli seguenti:

- ♦ **Titolo:** specifica il nome del widget che verrà visualizzato sul Dashboard.
- ♦ **URL:** specifica l'URL API REST del widget richiesto da visualizzare sul Dashboard.
- ♦ **Elemento radice:** specifica l'elemento del codice API REST per cui si desidera visualizzare un grafico. Questo campo fa distinzione tra maiuscole e minuscole. Occorre specificare lo stesso nome esatto indicato nel codice API REST.
- ♦ **Colonne:** specifica le colonne da visualizzare sul widget. È possibile aggiungere più colonne. **Titolo** specifica il nome di visualizzazione di una colonna. **Percorso** specifica il nome della colonna indicato nell'API REST. Il campo **Percorso** fa distinzione tra maiuscole e minuscole. Occorre specificare la stessa stringa esatta dal codice API REST.

Di seguito viene fornito un esempio di codice API REST per la pagina **Ruoli**:

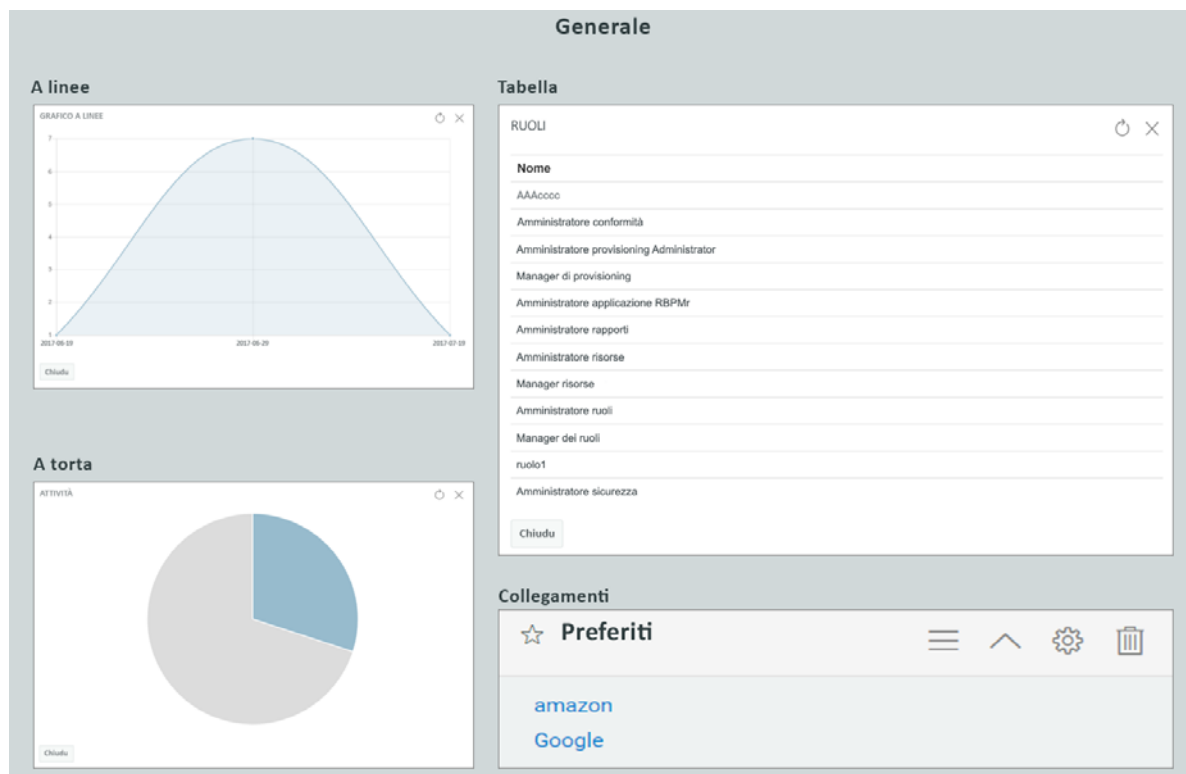
```
{
  "total": 12,
  "nextIndex": 0,
  "token": "60045d6be10f4419a2da9fa728683b06",
  "assignments": [
    {
      "id":
"cn=aaacccc,cn=level30,cn=roledefs,cn=roleconfig,cn=appconfig,cn=user
application driver,cn=driverset1,o=system",
      "name": "AAAcCCC",
      "description": "afasfdsf",
     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

In questo esempio, assignments è l'elemento radice e name è la colonna selezionata da visualizzare nel widget. È inoltre possibile salvare qualsiasi URL tra i preferiti a cui accedere dal Dashboard

- 4 (Condizionale) Per i widget **Collegamenti**, specificare il **Titolo** dei collegamenti e aggiungere quelli cui si desidera accedere dal Dashboard.
- 5 Fare clic su **Salva** per applicare le modifiche.

Di seguito sono forniti esempi di widget Collegamento e Grafico che è possibile aggiungere al dashboard:

Figura 3-6 Esempio di widget generale



Aggiunta di widget di Identity Manager

La categoria **IDM** consente di aggiungere widget standard di Identity Manager al Dashboard.

Ad esempio,

- ♦ **Accesso**: visualizza il numero di ruoli e risorse e altre informazioni relative.
- ♦ **Richiesta per altri**: visualizza il numero di richieste in sospeso e rifiutate di altri utenti e consente di creare una richiesta per tali utenti.
- ♦ **Autrichieste**: visualizza il numero di richieste in sospeso e rifiutate e consente inoltre di creare una nuova richiesta.
- ♦ **Task**: visualizza il numero di task nuovi, in sospeso o prossimi alla scadenza.

Per configurare questi widget, vedere [“Configurazione di un widget” a pagina 33](#).

Importante: per applicare le modifiche, fare clic su **Salva**.

Aggiunta di widget di Identity Governance

Per utilizzare i widget di Identity Governance, è necessario installare e configurare Identity Governance con il Dashboard di Identity Manager.

La categoria IG consente di aggiungere widget standard di Identity Governance al dashboard. Ad esempio:

Task di realizzazione

Visualizza il numero di richieste di accesso, ruoli aziendali ed errori nell'assegnazione delle autorizzazioni nel sistema.

Task di revisione

Visualizza il numero di revisioni in sospeso e completate nel sistema.

Violazioni di separazione dei compiti

Visualizza il numero delle violazioni di separazione dei compiti non riviste, approvate o in fase di risoluzione all'interno del sistema.

Opzioni widget

È possibile eseguire le operazioni seguenti sui widget:



Aggiorna schermo

Aggiorna il contenuto del widget con le informazioni più recenti.

Riposiziona

Consente di spostare il widget nel Dashboard.

Configurazione

Consente di configurare le proprietà del widget. Per ulteriori informazioni, vedere [“Configurazione di un widget” a pagina 33](#).

Rimuovi

Consente di eliminare il widget dal Dashboard.

Comprimi

Nasconde le informazioni sul widget e mostra solo il titolo del widget.

Apri widget a schermo intero

Visualizza le informazioni sul widget in modalità schermo intero.

Nota

- ♦ Le opzioni **Aggiorna** e **Apri widget a schermo intero** vengono visualizzate solo per i widget che appartengono alla categoria **Generale**.
- ♦ Per applicare le modifiche, fare clic su **Salva**.

Configurazione di un widget

È possibile configurare ciascun widget aggiunto al Dashboard. Ad esempio, è possibile attivare o disattivare i campi di un widget o cambiare il colore di visualizzazione dei campi.

1 Fare clic su  sul widget che si desidera configurare.

2 Modificare le proprietà del widget.

Ad esempio, è possibile modificare il titolo di un widget, oppure cambiare il colore di un'etichetta per un campo del widget. È inoltre possibile attivare o disattivare un campo del widget nella pagina delle proprietà.

3 Per visualizzare le modifiche nel dashboard, fare clic su **Applica**.

Ad esempio, è possibile modificare il widget task come mostrato di seguito:

Figura 3-7 Esempio di configurazione del widget

TASK

Qualifica

Tasks

Nuovi compiti

☒



Scadenza a breve

☒



Assunto

☒



Task delegati

☐



Task riassegnati

☐



Applica

Annulla

Per visualizzare le modifiche nel Dashboard, fare clic su **Applica**.



Per configurare i widget Generale, modificare le opzioni visualizzate durante l'aggiunta dei widget. Vedere [“Aggiungere widget generici” a pagina 30](#).

Importante: per applicare le modifiche, fare clic su **Salva**.



Gestione delle autorizzazioni e del profilo di identità

Il Dashboard di Identity Manager consente di richiedere l'accesso alle risorse e ai ruoli necessari per completare i propri task giornalieri. Nell'ambiente di Identity Manager è inoltre possibile intervenire su qualsiasi task assegnato, come l'approvazione di richieste per l'accesso. I proprietari di risorse e ruoli possono gestire il processo.

Quando si richiede un'autorizzazione, in Identity Manager viene avviato un processo per rivedere in modo efficiente la propria richiesta in modo da ottenere il ruolo o la risorsa necessaria. Il manager riceve una notifica tramite e-mail o nel Dashboard per rivedere la richiesta. In alcuni casi, è inoltre possibile che la richiesta venga approvata da altri utenti all'interno dell'organizzazione.

Alcuni utenti possono effettuare richieste per conto di terzi o fungere da utente incaricato per un altro utente.

- ♦ [Capitolo 4, "Gestione delle richieste di autorizzazione", a pagina 37](#)
- ♦ [Capitolo 5, "Gestione delle applicazioni", a pagina 45](#)
- ♦ [Capitolo 6, "Gestione di task personali", a pagina 49](#)
- ♦ [Capitolo 7, "Agire per conto di qualcun altro", a pagina 53](#)
- ♦ [Capitolo 8, "Gestione delle deleghe", a pagina 55](#)
- ♦ [Capitolo 9, "Gestione della disponibilità", a pagina 57](#)
- ♦ [Capitolo 10, "Gestione del profilo personale", a pagina 59](#)
- ♦ [Capitolo 11, "Gestione dell'organigramma", a pagina 61](#)
- ♦ [Capitolo 12, "Gestione della password", a pagina 69](#)

4 Gestione delle richieste di autorizzazione

Questa sezione è una guida alle seguenti attività:

- ♦ “Visualizzazione delle autorizzazioni” a pagina 37
- ♦ “Richiesta di autorizzazioni” a pagina 39
- ♦ “Visualizzazione delle richieste” a pagina 39
- ♦ “Revoca delle autorizzazioni” a pagina 41
- ♦ “Collegamento profondo a una richiesta” a pagina 42

È inoltre possibile vedere ⓘ per le informazioni sul Dashboard relative a queste attività.

Visualizzazione delle autorizzazioni

Le autorizzazioni rappresentano gli account, i ruoli o le risorse disponibili. Le autorizzazioni possono essere assegnate automaticamente all'utente dall'organizzazione o è possibile richiederle specificamente. È inoltre possibile ereditare alcune autorizzazioni indirettamente attraverso le relazioni dei ruoli o se si è membri di un gruppo o di un container.

Per visualizzare i ruoli e le risorse cui si ha accesso, nel Dashboard selezionare:

Accesso > Autorizzazioni

È quindi possibile selezionare un'autorizzazione specifica per ottenere ulteriori dettagli su tale ruolo o risorsa. L'autorizzazione potrebbe anche contenere un elenco di tutti i motivi per i quali è stata assegnata. Per trovare un'autorizzazione specifica in un elenco di grandi dimensioni, digitare il nome, il CN o la descrizione dell'autorizzazione nella casella di ricerca. È inoltre possibile filtrare l'elenco.

Nota:

- ♦ Per default, è possibile vedere gli elenchi delle autorizzazioni assegnate o approvate e direttamente riferibili all'utente. Questo comportamento, tuttavia, può variare a seconda di come l'amministratore ha configurato le impostazioni per la pagina. Per ulteriori informazioni, vedere la sezione relativa alle impostazioni dell'utente [User Settings](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).
 - ♦ Per visualizzare le autorizzazioni secondarie mappate con le autorizzazioni assegnate o approvate, fare clic su ⓘ.
-

Visualizzazione dei dettagli dell'autorizzazione

Selezionare l'autorizzazione per la quale si desidera visualizzare ulteriori dettagli. Nella seguente tabella sono elencati i campi visualizzati per singola autorizzazione:

Tabella 4-1 Campi e descrizione dell'autorizzazione

Campi	Descrizione
Descrizione	La descrizione del ruolo o della risorsa.
Data di inizio validità	La data e l'ora di assegnazione dell'autorizzazione.
Data di scadenza	La data dopo la quale l'autorizzazione non sarà più assegnata all'utente. Viene visualizzata solo per l'autorizzazione con l'opzione relativa alla scadenza abilitata.
Motivo	Specifica il motivo per cui l'autorizzazione viene assegnata all'utente.
Autorizzazione assegnata via	Specifica chi ha assegnato l'autorizzazione all'utente. Se viene assegnato un ruolo all'utente direttamente tramite un processo di approvazione, è possibile vedere l'elenco di chi ha approvato la richiesta di assegnazione nell'opzione Visualizza le informazioni sull'approvazione del ruolo. Se il ruolo viene ereditato dall'utente tramite l'appartenenza a un gruppo o a un container, nell'opzione Visualizza informazioni su assegnazione ruolo a gruppo sono visualizzati i seguenti dettagli: ♦ Richiesta da: specifica chi ha richiesto l'autorizzazione. ♦ Descrizione richiesta: la descrizione fornita durante la richiesta dell'autorizzazione. ♦ Dettagli approvatore: fare clic sul collegamento per vedere l'elenco di chi ha approvato la richiesta di assegnazione del ruolo.

Gli amministratori di identity applications possono visualizzare le autorizzazioni per altri membri del team nella scheda **Altri**. Accedere alla scheda **Altri** ed eseguire la ricerca per nome utente o dettagli dell'autorizzazione.

- ♦ La ricerca in base all'utente elencherà tutte le autorizzazioni assegnate di tale utente. È possibile selezionare un'autorizzazione specifica per rivedere dettagli come la data di assegnazione, chi ha assegnato l'autorizzazione ed eventuali motivi forniti per l'assegnazione dell'autorizzazione. Per ulteriori informazioni, vedere [Tabella 4-1 a pagina 38](#).
- ♦ La ricerca in base all'autorizzazione elencherà tutti gli utenti, gli individui e coloro che fanno parte di un gruppo o container, cui è stata assegnata tale autorizzazione.

Nota: la ricerca per dettagli dell'autorizzazione non è supportata per un manager del team o un supervisore. Questi, tuttavia, possono vedere le autorizzazioni dei membri del team effettuando una ricerca per nome del team o descrizione. Inoltre, per effettuare la ricerca e visualizzare le autorizzazioni di un membro specifico del team, è possibile inserire il nome utente nella pagina.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Richiesta di autorizzazioni

Per richiedere ruoli e risorse, fare clic su [Accesso > Richieste](#)

Prima di richiedere autorizzazioni, è opportuno tener conto delle seguenti considerazioni:

- ♦ Si potrebbe essere in grado di richiedere l'accesso per conto di un altro utente. I manager del team, ad esempio, di norma possono agire per conto di altri membri del team. Il processo è lo stesso, tranne che è necessario specificare che la richiesta è per **Altri** e non per **Se stessi**.
- ♦ Non fare uso di punteggiatura quando si specifica un'autorizzazione che si desidera richiedere. Se il nome dell'autorizzazione da richiedere include punteggiatura, omettere quest'ultima dalla ricerca.
- ♦ A seconda della configurazione del modulo di autorizzazione definita dall'amministratore, per le varie autorizzazioni sono necessarie informazioni diverse. Se l'autorizzazione richiede informazioni dettagliate, quando la si seleziona si verrà reindirizzati dal Dashboard a una finestra separata.
- ♦ È possibile richiedere più autorizzazioni contemporaneamente.
Se tuttavia il modulo di autorizzazione per una delle richieste necessita di informazioni speciali, potrebbe risultare impossibile includere tale autorizzazione in una richiesta di più autorizzazioni. Per richiedere più autorizzazioni contemporaneamente, per i moduli di richiesta delle varie richieste non devono essere necessarie informazioni dettagliate.
- ♦ È possibile specificare la data di scadenza mentre si richiede una risorsa o un ruolo.

Per richiedere le autorizzazioni di Identity Governance

*La procedura è valida solo in due condizioni, ovvero quando è abilitata l'opzione **Mostrare il catalogo IG nella pagina delle richieste?** nella pagina **Configurazione > Identity Governance** e quando si richiede l'autorizzazione per **Se stessi**.*

- ♦ **Cataloghi IDM:** elenca tutti i workflow, le risorse e i ruoli disponibili di Identity Manager.
- ♦ **Applicazioni IG:** elenca tutte le applicazioni raccolte in Identity Governance. È possibile selezionare le autorizzazioni associate all'applicazione selezionata.
- ♦ **Ruoli tecnici IG:** elenca tutti i ruoli tecnici di Identity Governance. Selezionare tutti i ruoli IG da richiedere e indicare il motivo della richiesta.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Visualizzazione delle richieste

Per visualizzare lo stato di una richiesta in corso e delle richieste completate, nel Dashboard selezionare:

[Accesso > Cronologia richieste](#)

Un manager del team o supervisore può vedere la cronologia delle richieste degli altri membri del team nella scheda **Altri**.

È inoltre possibile emettere un ticket per help desk per le richieste in sospeso.

- ♦ “Controllo di una richiesta” a pagina 40
- ♦ “Annullamento di una richiesta” a pagina 40
- ♦ “Emissione di un ticket per l'help desk” a pagina 40

Per ulteriori informazioni, fare clic su  nel Dashboard.

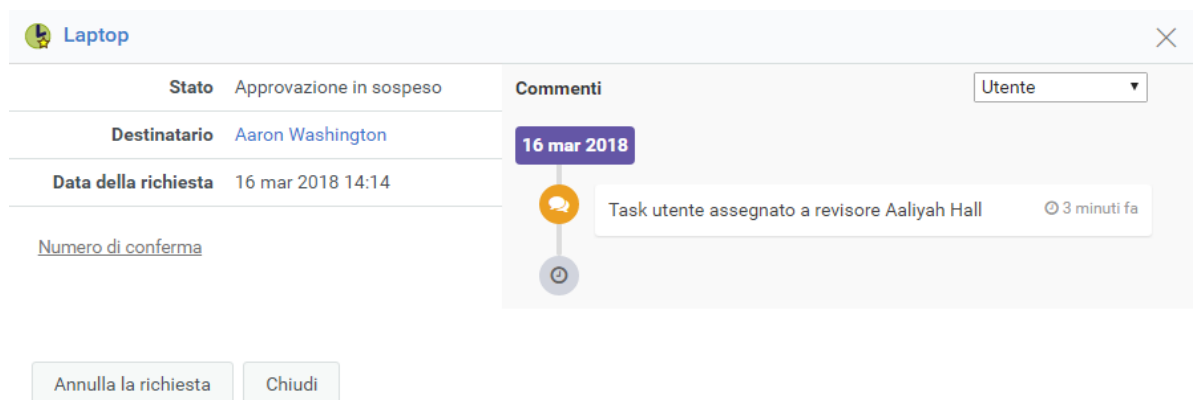
Controllo di una richiesta

Per ciascuna richiesta, oltre alle proprie azioni è possibile visualizzare il workflow implicato nell'approvazione o nel rifiuto della richiesta. Ogni passaggio del processo presenta la registrazione dell'orario.

Nota: eventuali richieste di applicazioni o ruoli tecnici effettuate dalle schede **Applicazioni IG** o **Ruoli tecnici IG** non possono essere registrate nella pagina **Cronologia richieste**. Per controllare le richieste IG, è possibile aggiungere l'URL della cronologia IG dalla pagina **Applicazioni** del dashboard.

Per controllare una richiesta in sospeso, selezionarla, quindi modificare il menu in alto a destra in **Utente e sistema**. Nel Dashboard viene mostrato lo stato attuale della richiesta nel processo di approvazione.

Figura 4-1 Controllo di una richiesta



Annullamento di una richiesta

È possibile annullare una richiesta *in sospeso* da **Cronologia richieste**. Selezionare la richiesta dall'elenco, quindi selezionare **Annulla la richiesta** nella finestra successiva.

Emissione di un ticket per l'help desk

Se è da molto che si attende assistenza per una richiesta automatica, è possibile contattare l'help desk.

È possibile emettere un ticket per l'help desk da:

- ♦ **Accesso > Richiesta**, fare clic su **Ticket per help desk**.

- ♦ **Applicazioni**, fare clic su **Ticket per help desk**.
- ♦ **Accesso > Cronologia richieste**, fare clic su  nella richiesta per la quale si desidera emettere un ticket per l'help desk.

Per ulteriori informazioni, fare clic su  nel Dashboard.

I membri dell'help desk ricevono una notifica in merito al ticket emesso. Quando il ticket è stato chiuso o risolto, l'utente riceve la notifica.

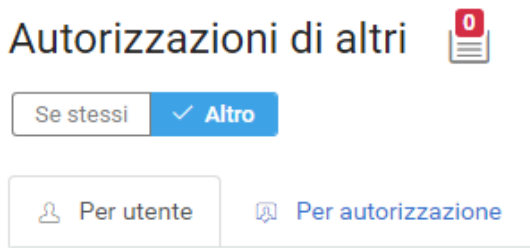
Revoca delle autorizzazioni

Se non è più necessario accedere a un ruolo o una risorsa, è possibile revocare l'autorizzazione a tale ruolo o risorsa. Per revocare un'autorizzazione, selezionare **Accesso > Autorizzazioni** e scegliere l'autorizzazione richiesta specificando un motivo per la revoca.

È inoltre possibile revocare un'autorizzazione per conto di altri utenti. Ad esempio, se il membro del team si è trasferito da Reparto 1 a Reparto 2 e il membro del team non deve più accedere a una particolare risorsa, Identity Manager fornisce la possibilità di revocare l'autorizzazione per tale utente. Per revocare un'autorizzazione, selezionare **Altri** e rimuovere l'autorizzazione. È possibile revocare più autorizzazioni alla volta. È possibile aggiungere tale autorizzazione a una coda per esaminarle prima di decidere di eliminarle.

Solo l'amministratore e il manager del team possono revocare autorizzazioni per altri utenti. L'amministratore può revocare le autorizzazioni per qualsiasi utente nell'organizzazione, mentre un manager del team può revocare le autorizzazioni solo per i membri del suo team.

È possibile revocare le autorizzazioni per altri utenti nei modi seguenti:

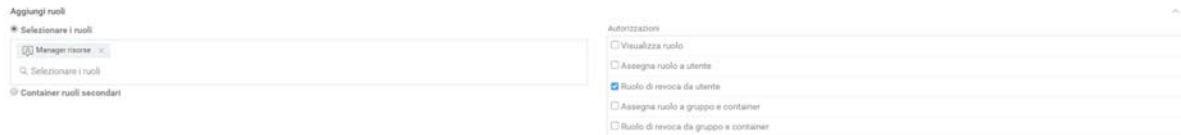


- ♦ **Cerca per utente:** consente di cercare un utente e revocarne le autorizzazioni. È possibile revocare direttamente un'autorizzazione per l'utente o aggiungere l'autorizzazione a una coda. La coda è un'area di lavoro persistente in cui è possibile inserire temporaneamente le autorizzazioni che è possibile rivedere e revocare se richiesto. È quindi possibile cercare altre autorizzazioni da revocare per l'utente e aggiungerle alla coda. Ciò consente di revocare tutte le autorizzazioni in una volta.
- ♦ **Cerca per autorizzazioni:** consente di cercare un'autorizzazione specifica. Se si seleziona un'autorizzazione, vengono elencati tutti gli utenti che dispongono di tale autorizzazione. È possibile revocare direttamente l'autorizzazione per l'utente selezionato o aggiungerla a una coda e revocarla per più utenti in una volta.

Manager del team: i manager dei team possono revocare le autorizzazioni per i membri del rispettivo team nella scheda **Altri**. Assicurarsi di disporre delle autorizzazioni necessarie per revocare le autorizzazioni di altri.

Amministratore: l'amministratore può aggiungere autorizzazioni di revoca per un manager del team, ad esempio, se desidera assegnare l'autorizzazione per la revoca del ruolo di un utente. Accedere a **Persone > Team**, modificare le autorizzazioni del team per abilitare le autorizzazioni di revoca per un manager del team.

Figura 4-2 Esempio di aggiunta di un'autorizzazione di revoca per un manager del team



Questa opzione consente al manager del team di revocare il ruolo selezionato dai membri del team.

Nota: se si revoca un'autorizzazione, la modifica potrebbe non essere immediatamente applicata, in quanto l'autorizzazione è associata al processo di revoca che non è immediato. Aggiornare l'elenco per visualizzare le modifiche.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Collegamento profondo a una richiesta

Le applicazioni di identità consentono di creare un collegamento profondo a una richiesta di processo specifica (altrimenti nota anche come richiesta di provisioning). Questa funzione consente al manager di inviare l'URL di una specifica richiesta di processo a un dipendente, in modo che questo possa richiedere rapidamente il processo senza dover passare dal Dashboard di Identity Manager. Quando si crea un collegamento profondo a una richiesta di processo, il modulo di richiesta viene visualizzato nel corpo della pagina, unitamente all'intestazione per le applicazioni di identità.

Dopo aver richiesto l'autorizzazione, è possibile visualizzare la richiesta nella pagina **Accesso > Cronologia richieste** del richiedente e nella pagina **Task** del revisore.

L'URL utilizzato per creare un collegamento profondo a una richiesta di processo utilizza il seguente formato:

- ♦ Per i moduli esistenti,

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

Ecco un esempio che mostra l'URL da utilizzare per creare un collegamento profondo a una definizione di richiesta di provisioning:

```
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
```

- ♦ Per i nuovi moduli JSON,

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

Ecco un esempio che mostra l'URL da utilizzare per creare un collegamento profondo a una definizione di richiesta di provisioning:

`https://testserver:18600/forms/#!/form/details?id=cn%3DHelp-
desk%20Request%20Form,cn%3DWorkflowForms,cn%3Dappconfig,cn%3DUser%20Ap
plication%20Driver,cn%3DdriverSet1,o%3Dsystem&recipient=&pid=cn%3Dhelp
deskticket,cn%3Drequestdefs,cn%3Dappconfig,cn%3Duser%20application%20d
river,cn%3DdriverSet1,o%3Dsystem&sid=IDM&uri=%2Frest%2Faccess%2Fforms&
formContainer=RequestForms&locale=en`

5 Gestione delle applicazioni

Gli amministratori delle applicazioni di identità possono modificare la pagina **Applicazioni** in modo che vengano visualizzate tutte le applicazioni, attività e autorizzazioni cui possono accedere gli utenti. Per default, nelle applicazioni di identità è disponibile la categoria **Elementi home** che è impossibile eliminare.

Dopo il completamento delle modifiche, fare clic su **Modifica eseguita** per tornare ad **Applicazioni**.

Creazione di elementi di rilievo

È possibile creare il numero desiderato di applicazioni e autorizzazioni da aggiungere alla pagina **Applicazioni**. Non è necessario aggiungere tali elementi in **Elementi home** o in altre categorie di **Applicazioni**.

- 1 (Condizionale) Per creare un nuovo elemento, fare clic su + nella scheda **Applicazioni** o **Autorizzazioni**.
- 2 Compilare il modulo per un'applicazione o autorizzazione. Vedere [“Aggiunta di un'applicazione” a pagina 45](#) o [“Aggiunta di un'autorizzazione” a pagina 46](#).

Nota: è necessario specificare un valore per tutti i campi contrassegnati con un asterisco (*), come il nome e la descrizione di un'applicazione.

- 3 (Opzionale) Trascinare e rilasciare la nuova applicazione o autorizzazione in una categoria.
- 4 (Condizionale) Per modificare un elemento esistente, selezionare l'icona di modifica all'interno del riquadro, quindi aggiornare i valori.

Aggiunta di un'applicazione

Per aggiungere un'applicazione, specificare i seguenti dettagli:

(Condizionale) Aggiungi a categoria

Specifica la categoria dell'applicazione.

Nome

Specifica il nome dell'applicazione.

Descrizione

Specifica la natura dell'applicazione.

(Opzionale) Immagine

Specifica un logo o un'immagine per un'applicazione.

Collegamento

Specifica un collegamento per l'applicazione. Vedere [“Collegamento profondo a una richiesta” a pagina 42](#).

(Opzionale) URL API

Specifica l'URL dell'endpoint REST con dati JSON che fornisce ulteriori dettagli, ad esempio il valore del parametro e un badge. Per ulteriori dettagli, fare riferimento alla documentazione.

Aggiunta di un'autorizzazione

Per aggiungere un'autorizzazione, specificare i seguenti dettagli:

Autorizzazioni

Specifica l'autorizzazione. Questa può essere un ruolo, una risorsa o una PRD.

(Condizionale) Aggiungi a categoria

Specifica la categoria dell'applicazione.

(Opzionale) Immagine

Specifica un logo o un'immagine per un'applicazione.

Aggiunta, modifica o eliminazione di una categoria

È possibile organizzare in categorie logiche gli elementi della pagina **Applicazioni**. È possibile creare tutte le categorie che si ritiene possano essere necessarie per l'organizzazione. È inoltre possibile ridisporre i riquadri in una categoria o spostarli in una categoria diversa.

Per aggiungere una categoria

- 1 Selezionare **Nuova categoria**.

La categoria viene aggiunta alla fine del gruppo di categorie. Potrebbe essere necessario scorrere verso il basso per visualizzare la categoria aggiunta.

- 2 Specificare il nome della nuova categoria.
- 3 Fare clic su **+**, quindi selezionare **Applicazione** o **Autorizzazione**.
- 4 Compilare il modulo per l'applicazione o l'autorizzazione.

Nota: è necessario specificare un valore per tutti i campi contrassegnati con un asterisco (*), come il nome e la descrizione di un'applicazione.

- 5 Selezionare **+Aggiungi**.

Modifica una categoria

È possibile modificare una categoria nei modi seguenti:

- ♦ Aggiunta di riquadri per applicazioni e autorizzazioni trascinandoli e rilasciandoli dalla sezione **Nuovi elementi** e **Autorizzazioni** a destra della pagina
- ♦ Rimozione di un'applicazione o autorizzazione selezionando l'icona del cestino nel riquadro dell'elemento
- ♦ Modifica delle impostazioni di un elemento

- ♦ Modifica del nome della categoria
- ♦ Riordinamento degli elementi nella categoria

Eliminazione di una categoria

Per eliminare una categoria, selezionare l'icona del cestino a destra del nome della categoria.

6 Gestione di task personali

Se si è responsabili dell'approvazione o del rifiuto di autorizzazioni richieste in Identity Manager, è possibile utilizzare il Dashboard per gestire i task, come potrebbe essere stato fatto precedentemente nell'Applicazione utente. È possibile approvare o rifiutare una richiesta alla volta o più semplici richieste per le quali non sono richieste informazioni dettagliate in blocco.

Per rivedere le richieste in sospeso, fare clic su **Task**.

In alternativa, si potrebbe ricevere una notifica e-mail contenente un collegamento che consente di approvare o rifiutare una richiesta in un'e-mail di risposta.

Prima di intervenire sulle richieste utente, è opportuno tener conto delle seguenti considerazioni:

- È possibile effettuare selezioni multiple di task per l'approvazione o il rifiuto di un batch.
- Per una richiesta più complessa per la quale sono richieste informazioni dettagliate, nel Dashboard non viene visualizzata una casella di controllo. È necessario approvare o rifiutare tali richieste selezionando ciascuna di esse e compilando i moduli.
- Quando si seleziona una richiesta più complessa da approvare o rifiutare, potrebbe essere necessario che nel Dashboard venga aperto un modulo di richiesta in una scheda del browser separata.
- In generale, è necessario fornire un commento in cui si spiega il motivo per il quale si desidera approvare o rifiutare i task selezionati.

Visualizzazione dei task

Per gestire i propri task, selezionare **Task**. Per visualizzare i task assegnati ad altri utenti, fare clic su **Altri**.

L'utente può completare i task di altri utenti per cui agisce come utente incaricato o delegato. Per ulteriori informazioni sulle assegnazioni di deleghe e utenti incaricati, vedere [Agire come utente incaricato](#).

Approvazioni IDM: la procedura è valida se è stata abilitata l'opzione **Mostra approvazioni IG nella pagina dei task nella pagina Configurazione > Identity Governance**.

In questa scheda sono elencati tutti i task di Identity Manager. Per default, elenca tutti i task **automatici**. Per visualizzare altri task con un ruolo appropriato, fare clic su **Altri**.

- È possibile cercare i propri task mediante i filtri **Task riassegnati**, **Task restituiti** o **Task delegati**. Il filtro **Task delegati** per **Se stessi** mostra solo i task delegati all'utente.
- Gli amministratori possono inoltre filtrare i task con il filtro **Assegnato a me**, **Destinatario me stesso**.
- Se si cercano altri task, è possibile utilizzare il filtro **Task restituiti**, **Task riassegnati** o **Task delegati**. Il filtro **Task delegati** per **Altri** mostra tutti i task delegati ad altri utenti nel sistema.

- ♦ È inoltre possibile ottimizzare la ricerca dei task in base ai task che si sono verificati nel sistema:
 1. Selezionare .
 2. (Condizionale) Per vedere i task creati per un determinato periodo, specificare tale periodo in **Settimane**, **Giorni** oppure **Ore**.
 3. (Condizionale) Specificare lo stato del task da filtrare.
 4. Fare clic su **Filtro**.
- ♦ Gli utenti dell'help desk possono utilizzare il filtro **Task help desk** per vedere l'elenco filtrato. Per gestire il task dell'help desk, vedere la Guida del Dashboard.

Talvolta un utente, se indicato come approvatore delle richieste nella policy Richiesta di accesso, potrebbe dover approvare elementi richiesti. Gli elementi di cui è richiesta l'approvazione sono elencati nella scheda **Approvazioni**.

Approvazioni IG: la procedura è valida se è stata abilitata l'opzione **Mostra approvazioni IG nella pagina dei task nella pagina Configurazione > Identity Governance**.

In questa scheda sono elencati tutti i task con approvazione in sospeso di Identity Governance. Possono essere riassegnati ad altri utenti con l'opzione **Riassegna**.

Gestione delle richieste da approvare o rifiutare

In alcune organizzazioni, è possibile che un gruppo di persone sia responsabile della revisione, dell'approvazione e del rifiuto delle richieste di accesso. In tal caso, ciascun membro del gruppo riceve le stesse richieste. Ad esempio, il team Servizi IT potrebbe essere responsabile delle telecomunicazione e dei dispositivi elettronici. Quando un nuovo dipendente richiede un telefono cellulare, la richiesta viene assegnata a tutti i membri del team Servizi IT. Tutti i membri del team possono esaudire la richiesta.

Per la richiesta è possibile eseguire uno dei seguenti task:

Assumere la richiesta

È possibile **assumere la responsabilità** per una richiesta e agire sul task richiesto immediatamente o in seguito. Indipendentemente dal momento in cui si agisce sul task, gli altri membri del gruppo possono non visualizzare più tale richiesta nel rispettivo elenco **Task**.

Rilasciare la richiesta

Se non si desidera agire sulla richiesta assunta, è possibile rilasciarla.

Riassegnare la richiesta

Un task assegnato all'utente può essere riassegnato a un altro utente nell'organizzazione. Le seguenti considerazioni sono valide solo per la riassegnazione dei task:

- ♦ Se non si è in grado di completare il task, è possibile riassegnarlo al proprio manager. Selezionare la richiesta nella scheda **Se stessi**, quindi scegliere **Riassegna**. Il task viene riassegnato automaticamente al manager.

- ♦ I manager del team possono solamente riassegnare task personali al proprio manager. Tuttavia, se si desidera riassegnare un task allocato a un membro del proprio team, è possibile utilizzare la scheda **Altri**. Accedere alla scheda **Altri**, selezionare la casella di controllo del task desiderato e fare clic su **Riassegna**. Dal menu a discesa **Assegna a**, selezionare il membro del team cui si desidera riassegnare il task, inserire un commento per la riassegnazione e fare clic su **Riassegna**. Il task viene riassegnato al membro del team prescelto.
- ♦ Se l'utente non ha agito sul task nell'intervallo di tempo specificato, possono verificarsi le azioni seguenti:
 - ♦ Un amministratore può riassegnare il task a un altro utente. L'amministratore ha un'autorizzazione per riassegnare un task a qualsiasi utente nell'organizzazione.
 - ♦ Il manager del team può riassegnare il task a un altro membro del team. Assicurarsi che al momento della creazione del team il relativo manager disponga dell'autorizzazione Gestisci task assegnatario.

Ciò vale solo al momento della creazione del team quando si aggiungono membri tramite l'opzione **Membri**. Per ulteriori informazioni, vedere [“Creazione di un team” a pagina 84](#)

Nota: se si utilizza l'opzione **Tutti gli utenti** o **Relazione** per creare un team, il manager non può riassegnare i task a un altro membro del team.

- ♦ L'utente dell'help desk può riassegnare il task al manager fino al livello gerarchico definito nella pagina **Impostazioni**. L'amministratore configura la gerarchia dei manager.

Se il task viene riassegnato a un utente che non è in grado di accettarlo, è possibile restituirlo all'utente che ha assegnato il task.

Restituire la richiesta

Se non si desidera agire su una richiesta assegnata, è possibile restituire la richiesta. Le applicazioni di identità assegnano automaticamente il task restituito all'approvatore effettivo.

Nota: è possibile restituire solo una richiesta riassegnata.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Gestione dei task dell'help desk

I task dell'help desk vengono generati per ogni ticket dell'help desk generato nel sistema. In base a un esempio in [“Come funziona l'help desk?” a pagina 16](#), il ticket di Emilia crea un task dell'help desk nella pagina **Task** di Elena. Elena può prendere azioni appropriate per questo task dell'help desk.

L'utente dell'help desk seleziona il Ticket per help desk che richiede un'azione. Eseguire una delle azioni indicate per il ticket per help desk selezionato:

Aggiorna

Aggiorna il ticket per help desk con un commento appropriato.

Completa

Completa il ticket per help desk con un commento sulla soluzione.

Annulla

Chiude il ticket per help desk con un commento appropriato.

Nota: è possibile **Assumere** o **Rilasciare** il task dell'help desk. Se si assume un ticket per help desk dall'elenco dei task, il ticket compare tra i propri task **Automatici**.

Per ulteriori informazioni, fare clic su  nel Dashboard.

7 Agire per conto di qualcun altro

In alcune organizzazioni, potrebbe essere consentito completare task in qualità di utente incaricato, o delegato, per conto di qualcun altro. Ad esempio, un assistente personale potrebbe eseguire azioni di utente incaricato per il capo. Oppure si potrebbe sostituire, temporaneamente, una collega in maternità e agire per conto suo.

- ♦ [“Visualizzazione delle assegnazioni di utenti incaricati personali” a pagina 53](#)
- ♦ [“Agire come utente incaricato” a pagina 53](#)
- ♦ [“Gestione delle assegnazioni di utenti incaricati” a pagina 53](#)

Per ulteriori informazioni, fare clic su  nel Dashboard.

Visualizzazione delle assegnazioni di utenti incaricati personali

Per visualizzare le assegnazioni di utenti incaricati, nel Dashboard selezionare:

[Accesso](#) > [Assegnazioni di utenti incaricati](#)

Agire come utente incaricato

Un amministratore potrebbe assegnare a un utente il compito di agire come utente incaricato per conto di un altro. In tal caso, nell'applicazione viene aggiunta un'opzione relativa all'utente incaricato nel menu dell'account situato nell'angolo in alto a destra.

[ID utente](#) > [Utente incaricato come](#)

Ad esempio, Sara Rossi gestisce le relazioni con i clienti. Le applicazioni di identità includono un team addetto alle relazioni con i clienti di cui Sarah Smith è il manager. Sarah può agire per conto di Maria Belafonte che è un membro del team. Nel Dashboard, seleziona [ssmith](#) > [Utente incaricato come](#), quindi specifica [mbelafonte](#).

Gestione delle assegnazioni di utenti incaricati

Gli amministratori o i manager del team possono creare, modificare ed eliminare un'assegnazione. Affinché un manager del team possa gestire le assegnazioni di utenti incaricati per un team, è necessario configurare il team in modo appropriato. Il manager del team può creare assegnazioni solo per i membri del team.

8 Gestione delle deleghe

In alcune organizzazioni, è consentito delegare i task a un altro utente. Se si è un utente delegato per i task di altri o se i propri task vengono delegati ad altri utenti nell'organizzazione, è possibile vedere le informazioni sulla delega in [Amministrazione > Delega](#).

È possibile vedere i task delegati nella pagina [Task](#). i task con l'icona  indicano che sono delegati.

Importante: la creazione dell'assegnazione delega richiede anche di specificare i dettagli sulla propria disponibilità. È possibile farlo durante la creazione dell'assegnazione delega o creare la delega e specificare i dettagli sulla disponibilità in un'azione separata. Se l'amministratore ha abilitato le impostazioni richieste, è possibile visualizzare l'opzione **Non disponibile da** nella pagina [Crea assegnazione delega](#). Se tuttavia non è possibile visualizzare l'opzione **Non disponibile da**, è necessario specificare i dettagli sulla disponibilità dalla pagina [Impostazioni di disponibilità](#) dopo aver creato l'assegnazione delega. Ciò assicura il corretto funzionamento della delega. Per ulteriori informazioni, fare clic su  nel Dashboard.

9 Gestione della disponibilità

È possibile specificare le richieste di risorse con assegnazione delega per le quali l'utente non è disponibile in un determinato periodo di tempo. Durante il periodo in cui un utente non è disponibile per una richiesta, l'utente delegato a utilizzare tale richiesta può elaborarla.

Per visualizzare la disponibilità, nel Dashboard selezionare

Persone > Disponibilità

Per utilizzare l'azione **Non disponibile da** è necessario disporre di almeno un'assegnazione delega da elaborare. Solo il manager del team o l'amministratore dell'applicazione di provisioning possono creare assegnazioni di deleghe per gli utenti.

Le impostazioni globali relative alla delega basata sulla disponibilità sono specificate da **Imposta disponibilità durante la creazione di un'assegnazione delega** in **Impostazioni > Personalizzazione > Elementi di navigazione > Generale**. Se si preferisce non specificare la disponibilità per ogni singola definizione della richiesta, è possibile utilizzare l'azione **Non disponibile per qualsiasi richiesta** dall'azione Cambia stato.

Per ulteriori informazioni, fare clic su  nel Dashboard.

10 Gestione del profilo personale

Le applicazioni di identità consentono di visualizzare e utilizzare le informazioni sull'identità in modo pratico. Consentono inoltre all'organizzazione di reagire più prontamente fornendo agli utenti l'accesso alle informazioni necessarie su altri utenti ogni volta che servono. Ad esempio, si potrebbe voler:

- ♦ gestire direttamente il proprio account utente;
- ♦ eseguire ricerche su richiesta di altri utenti e gruppi dell'organizzazione;
- ♦ visualizzare le relazioni tra gli utenti e gruppi ricercati;
- ♦ elencare le applicazioni a cui si è associati.

L'amministratore di sistema è responsabile della configurazione dei contenuti delle applicazioni di identità resi disponibili agli utenti e ad altri membri dell'organizzazione. I contenuti che è effettivamente possibile visualizzare dipendono in genere dai requisiti e dal livello di autorità correlati al lavoro dell'utente.

Aggiornamento del proprio profilo

Per visualizzare o aggiornare il proprio profilo di identità, nel Dashboard selezionare:

[\[ID utente\]> Profilo personale](#)

O,

Fare clic su  nel dashboard.

In questa pagina sono elencati il manager di generazione rapporti, i ruoli, le risorse e il gruppo dell'utente. per modificare le informazioni o visualizzare l'organigramma è necessario disporre dell'accesso come amministratore.

Nel profilo sono incluse informazioni quali il nome, l'indirizzo e-mail e il numero di telefono dell'utente. In questa pagina sono visualizzati gli attributi utente abilitati con gli accessi a [ricerca](#) e [lettura](#), le cui proprietà possono essere configurate in Strato di astrazione directory. Per ulteriori informazioni, vedere la sezione relativa alle proprietà degli attributi [Attribute Properties](#) nella [NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications](#) (in lingua inglese). L'organizzazione determina le impostazioni che è possibile modificare. Ad esempio, si potrebbe essere in grado di modificare il proprio numero di telefono ma non il cognome.

11 Gestione dell'organigramma

Sul Dashboard di Identity Manager è possibile cercare un'entità (un utente, un gruppo o un'entità personalizzata definita dall'amministratore) nella propria organizzazione e visualizzare il relativo organigramma. Nell'organigramma viene mostrata la gerarchia delle relazioni, ad esempio Manager-Impiegato, Appartenenza a gruppi o Gruppi di utenti tra le entità dell'organizzazione.

Per default, nella pagina **Organigramma** del Dashboard viene visualizzato il posizionamento di un'entità utente all'interno dell'organizzazione e la relativa gerarchia delle relazioni con altre entità utente in base alla relazione dell'organigramma impostata dall'amministratore. Per ulteriori informazioni sulle impostazioni di default per la pagina dell'organigramma, vedere [Customizing the Views](#). Per ulteriori informazioni su come visualizzare l'organigramma delle entità diverse dall'entità utente, vedere [Viewing the Organization Chart of an Object in NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (in lingua inglese).

In questa sezione si fa riferimento all'organigramma sia usando la forma svolta del termine (organization chart), sia la forma abbreviata (org chart), perché nella versione inglese del dashboard sono presenti entrambe le versioni.

Visualizzazione di un organigramma

Per default, l'amministratore della sicurezza e l'amministratore di provisioning possono visualizzare l'organigramma per tutte le entità nel sistema.

È possibile accedere all'organigramma dell'entità utente in uno dei modi seguenti:

- Andare a **Persone > Organigramma**, in cui viene visualizzato l'organigramma dell'utente collegato basato sulla relazione dell'organigramma di default configurata nella pagina **Impostazioni**. È possibile visualizzare l'organigramma anche tramite l'icona  nelle pagine **Profilo personale**, **Dashboard** e **Applicazioni**.

Per trovare l'organigramma degli altri utenti nel sistema, digitare il loro nome nella barra di ricerca nella pagina **Organigramma**.

- Accedere a **Persone > Utenti** e selezionare un utente dall'elenco, quindi fare clic su  accanto al nome utente. Per ulteriori informazioni, consultare [Capitolo 13, "Gestione degli utenti"](#), a pagina 79.

Nota: per visualizzare l'**organigramma**, è necessario disporre dell'accesso all'**organigramma**. Per ottenere tale accesso, contattare l'amministratore. Per ulteriori informazioni, vedere la sezione relativa alle impostazioni degli utenti [User Settings](#) in [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (in lingua inglese).

Descrizione dell'organigramma

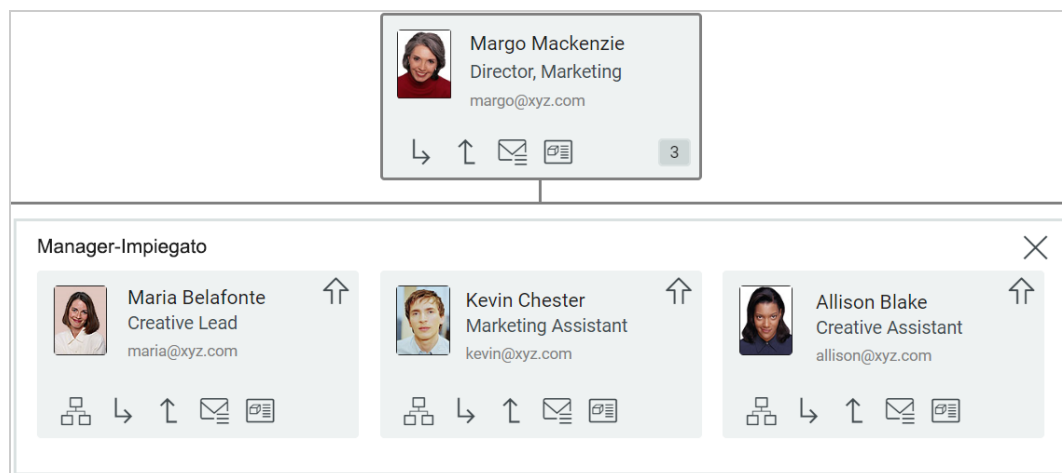
Nel grafico Organigramma, le informazioni sull'entità vengono visualizzate sotto forma di schede. Tali schede sono sistemate in ordine gerarchico in base alla relazione dell'organigramma di default configurata dall'amministratore. L'entità radice o selezionata visualizzata in alto rappresenta il punto di partenza o di orientamento nell'organigramma e l'entità secondaria direttamente sotto l'entità radice è visualizzata in basso in base alla relazione di default.

Ogni scheda contiene informazioni basate sugli attributi primari e secondari definiti dall'amministratore. Per ulteriori informazioni su come è possibile personalizzare questi attributi, vedere [Customizing the Organization Chart View](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese). Per un'entità utente specifica, la scheda è impostata in modo che venga visualizzato il nome completo dell'utente oltre agli attributi primari e secondari definiti dall'amministratore. Di conseguenza, quando l'amministratore configura il nome e il cognome come attributi primari, il nome completo dell'utente può apparire due volte nella **Vista scheda** della pagina **Utenti** e nell'organigramma.

Nota: nella vista dell'organigramma, se gli attributi primari e secondari di un'entità non sono definiti dall'amministratore, le applicazioni di identità visualizzano l'attributo CN di tale entità nella pagina **Organigramma**.

La [Figura 11-1](#) mostra un esempio di organigramma relativo all'utente *Margo Mackenzie* in cui la relazione dell'organigramma di default è impostata su Manager-Impiegato.

Figura 11-1 Esempio dell'organigramma nel Dashboard



In questo esempio, *Margo Mackenzie* è la manager e *Maria Belafonte*, *Kevin Chester* e *Allison Blake* sono gli impiegati che rispondono a lei. In ogni scheda il nome completo dell'utente è visualizzato in alto, in questo caso è *Margo Mackenzie*, seguito dal ruolo all'interno dell'organizzazione e dall'indirizzo e-mail impostati come attributi primari e secondari dall'amministratore. Il numero nell'angolo in basso a destra della scheda di *Margo Mackenzie* indica il numero di impiegati sotto la sua supervisione.

Utilizzo dell'organigramma

Sul Dashboard viene visualizzato l'organigramma dell'entità basato sull'input di ricerca immesso nella pagina **Organigramma**. È possibile eseguire altri task sulla pagina, ad esempio visualizzare le altre relazioni dell'entità, modificare l'entità radice e visualizzare il relativo organigramma oppure visualizzare l'organigramma di un'entità del livello superiore della gerarchia delle relazioni.

Per comprendere meglio i task che è possibile eseguire nella pagina **Organigramma**, esaminiamo l'esempio seguente di un team di marketing dell'azienda XYZ:

Margo Mackenzie è direttrice del team di marketing, mentre gli impiegati *Allison Blake*, *Kevin Chester* e *Maria Belafonte* sono sotto la sua supervisione. *Margo Mackenzie* è a sua volta sotto la supervisione di *Timothy Swan*, vicepresidente del team di marketing.

Andare a **Persone > Organigramma** nel Dashboard e cercare *Timothy Swan* per visualizzare il relativo organigramma. Allo stesso modo, effettuare una ricerca per *Margo Mackenzie*. Nella **Figura 11-2** e nella **Figura 11-3** sono mostrati i relativi organigrammi individuali basati sulla relazione Manager-Impiegato.

Figura 11-2 Organigramma di Timothy Swan nel ruolo di manager.

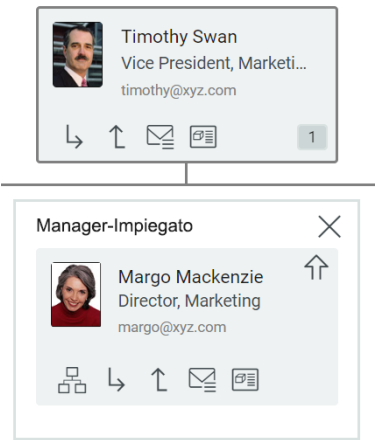
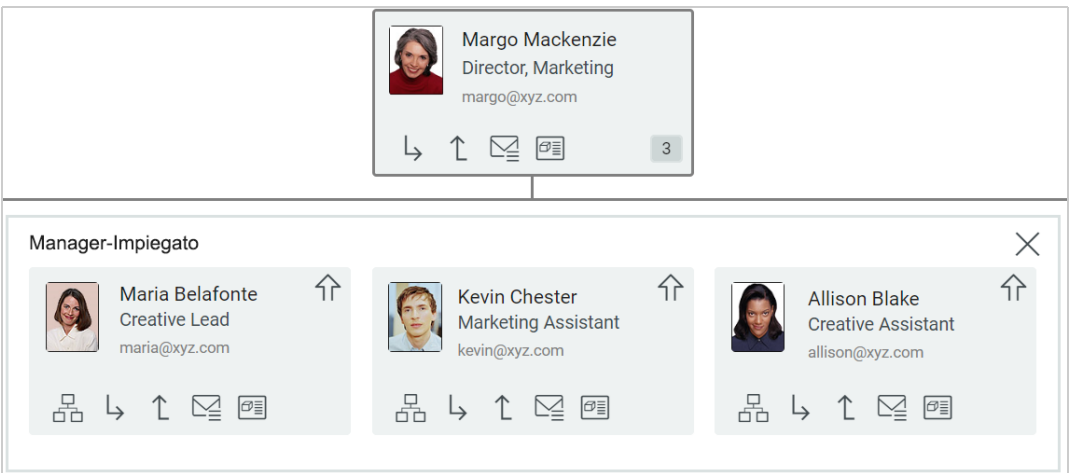


Figura 11-3 Organigramma di Margo Mackenzie nel ruolo di manager.



Esaminiamo i task che è possibile eseguire nella pagina **Organigramma** in base all'esempio riportato sopra:

- ♦ “Reimpostazione della radice nella vista dell'organigramma” a pagina 64
- ♦ “Passaggio alla vista dell'organigramma” a pagina 64
- ♦ “Scelta di una relazione da visualizzare” a pagina 65
- ♦ “Passaggio al livello successivo della gerarchia delle relazioni” a pagina 66
- ♦ “Invio di e-mail agli utenti dall'organigramma” a pagina 67
- ♦ “Visualizzazione di informazioni dettagliate su un utente” a pagina 67

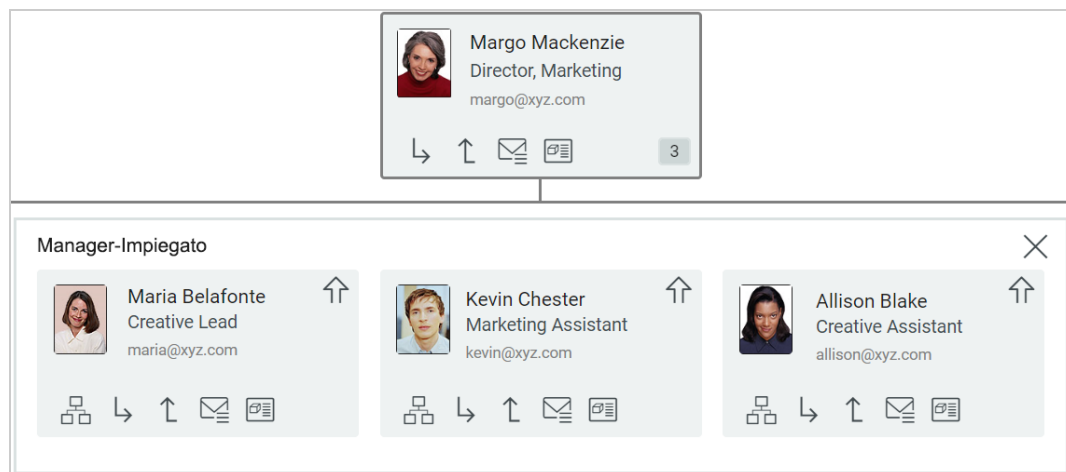
Nota: i task indicati sopra sono applicabili alle entità utente e personalizzate.

Reimpostazione della radice nella vista dell'organigramma

Per reimpostare l'utente radice nella vista dell'organigramma,

- 1 Identificare l'utente da impostare come nuova radice.
Ad esempio, si sta visualizzando l'organigramma in cui *Timothy Swan* ricopre il ruolo di manager e si desidera impostare *Margo Mackenzie* come nuova radice.
- 2 Andare alla scheda di *Margo Mackenzie* e fare clic sull'icona . Margo Mackenzie diventa la nuova radice e si trova adesso in alto nell'organigramma Manager-Impiegato. Gli impiegati sotto la supervisione di *Margo Mackenzie*, ovvero *Maria Belafonte*, *Kevin Chester* e *Allison Blake*, sono elencati sotto di lei.

Figura 11-4 Margo Mackenzie come nuova radice nella vista dell'organigramma



Passaggio alla vista dell'organigramma

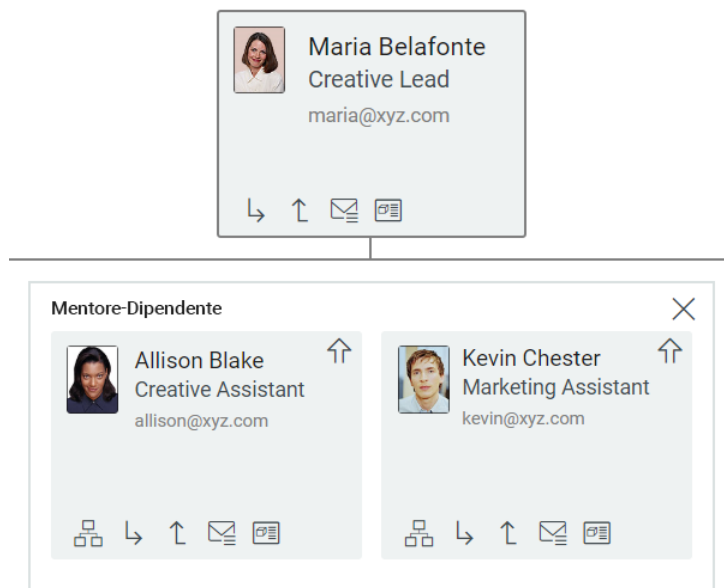
Per reimpostare l'utente radice e la relazione di default nella vista dell'organigramma, eseguire le azioni seguenti:

- 1 Identificare l'utente di cui si desidera visualizzare l'organigramma.

Ad esempio, si sta visualizzando l'organigramma in cui *Margo Mackenzie* ricopre il ruolo di manager. *Maria Belafonte*, l'impiegata sotto la supervisione di *Margo Mackenzie*, è anche mentore di *Kevin Chester* e *Allison Blake*. Si desidera visualizzare la relazione Mentore-Impiegato di *Maria Belafonte*.

- 2 Andare alla scheda di *Maria Belafonte* e fare clic su .
- 3 Dal menu a discesa, selezionare la relazione **Mentore-Impiegato**. *Maria Belafonte* diventa la radice dell'organigramma Mentore-Impiegato e *Kevin Chester* e *Allison Blake* sono elencati come impiegati sotto di lei.

Figura 11-5 Organigramma di *Maria Belafonte* nel ruolo di mentore



Scelta di una relazione da visualizzare

Per visualizzare le relazioni di un utente diverse da quelle di default, eseguire le azioni seguenti:

- 1 Identificare l'utente di cui si desidera visualizzare la relazione.
Ad esempio, si sta visualizzando l'organigramma in cui *Margo Mackenzie* ricopre il ruolo di manager. Si desidera visualizzare la relazione del gruppo di utenti di *Maria Belafonte* che fa parte del gruppo di marketing.
- 2 Andare alla scheda di *Maria Belafonte* e fare clic su .
- 3 Dal menu a discesa, selezionare la relazione **Gruppi di utenti**. Il grafico di appartenenza al gruppo di *Maria Belafonte* è aggiunto in linea nella vista dell'organigramma esistente.

Nota: il livello massimo a cui è possibile espandere l'organigramma di un utente per visualizzare le relazioni in linea è definito dall'amministratore. Per default, è possibile espandere l'organigramma fino al livello 3 e il livello 1 è sempre assegnato all'utente radice.

Passaggio al livello successivo della gerarchia delle relazioni

Per comprendere questo task, esaminiamo il secondo esempio di *Edward Miller*, amministratore del team delle vendite. *Allison Blake* e *Filla Martell* sono dipendenti di *Edward Miller*. Come è possibile vedere, *Allison Blake* è un comune membro del team delle vendite e di marketing ed è sotto la supervisione di due manager, ossia *Edward Miller* e *Margo Mackenzie*.

Per passare al livello successivo dell'albero delle relazioni ed espanderlo, eseguire le azioni seguenti:

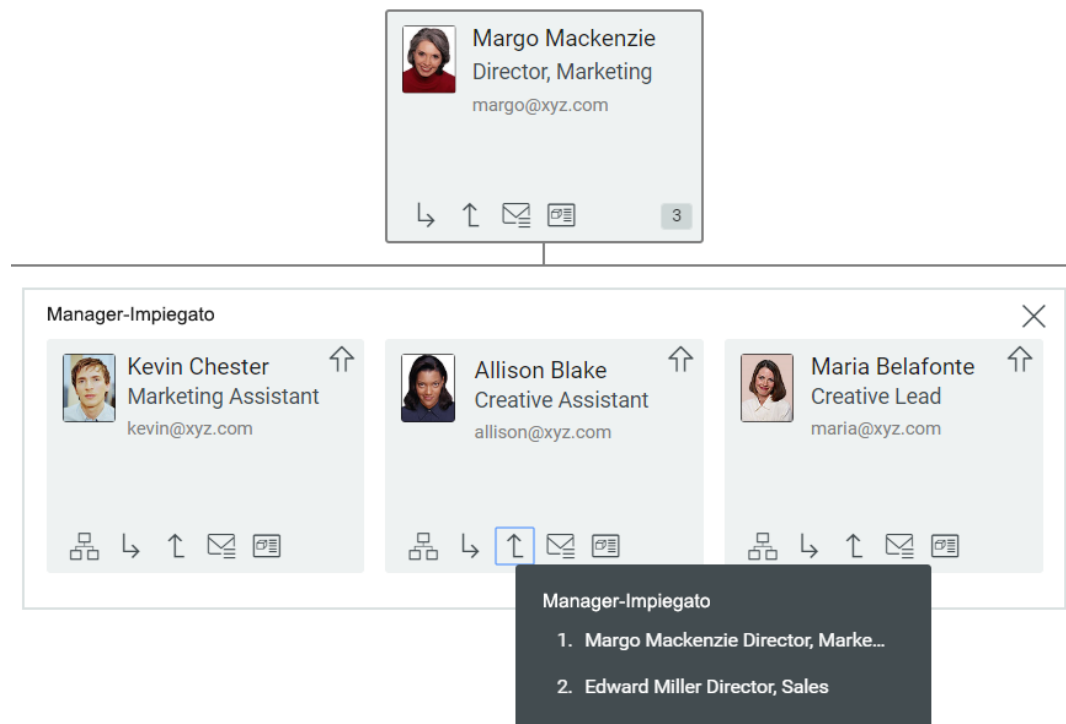
- 1 Identificare l'utente per il quale si desidera visualizzare e passare al livello successivo della gerarchia.

Ad esempio, si sta visualizzando l'organigramma in cui *Margo Mackenzie* ricopre il ruolo di manager e si desidera visualizzare l'organigramma di *Allison Blake*.

- 2 Andare alla scheda di *Allison Blake*, fare clic su  e selezionare la relazione Manager-Impiegato ricorrente dall'elenco.
- 3 Fare clic su .

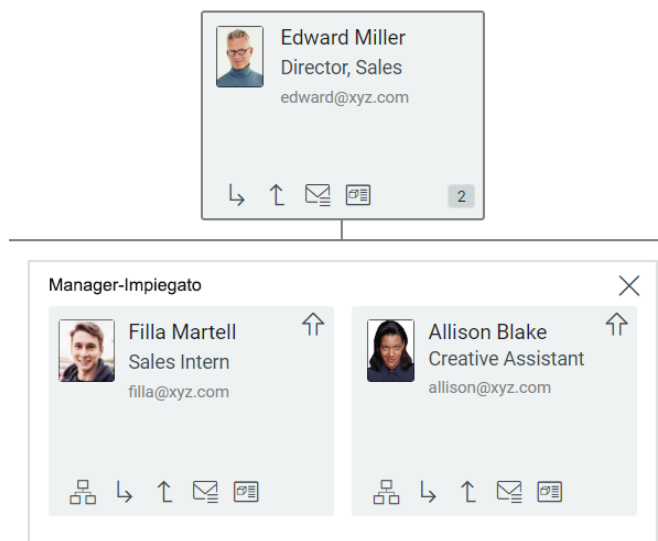
Nel menu a discesa Manager-Impiegato, per l'impiegata *Allison Blake* sono visualizzati due manager, ovvero *Margo Mackenzie* ed *Edward Miller* da cui lei dipende.

Figura 11-6 Relazione Manager-Impiegato ricorrente di *Allison Blake*



- 4 Selezionare il manager, *Edward Miller*. Viene visualizzato l'organigramma di *Allison Blake*.

Figura 11-7 Organigramma di Allison Blake



Invio di e-mail agli utenti dall'organigramma

Tramite l'opzione , è possibile:

- Inviare una e-mail all'utente selezionato.
- Condividere tramite e-mail il collegamento al profilo di un'entità.
- (Facoltativo, applicabile soltanto alla relazione Manager-Impiegato) Inviare una e-mail a tutti i membri del team che dipendono dall'utente selezionato.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Importante:

- Prima di inviare una e-mail dalla vista dell'organigramma, è necessario verificare che sul sistema sia stato configurato un client e-mail di default.
 - Per assicurare il funzionamento delle opzioni **Nuovo messaggio** e **Team e-mail**, configurare l'attributo dell'e-mail come primario o secondario nella pagina Impostazioni. Per ulteriori informazioni, vedere la sezione relativa alle impostazioni degli utenti [User Settings](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).
-

Visualizzazione di informazioni dettagliate su un utente

- 1 Identificare l'utente di cui si desidera visualizzare le informazioni.

Ad esempio, si sta visualizzando l'organigramma in cui *Margo Mackenzie* ricopre il ruolo di manager e si desidera visualizzare dettagli aggiuntivi, come i ruoli e le risorse assegnati a *Kevin Chester*.

- 2 Andare alla scheda di *Kevin Chester* e fare clic sull'icona . Nella pagina del profilo vengono visualizzate le informazioni dettagliate, inclusi i ruoli e le risorse a lui assegnati.

Se l'icona  non viene visualizzata sulla scheda di un utente, ad esempio sulla scheda del presidente dell'organizzazione XYZ *Jack Miller*, vuol dire che non si dispone delle autorizzazioni appropriate per il catalogo utenti e pertanto non è possibile visualizzare il suo profilo. Contattare l'amministratore se si necessita dell'accesso necessario per visualizzare un profilo.

Per ulteriori informazioni, fare clic su  nel Dashboard.

12 Gestione della password

In Identity Manager è inclusa l'applicazione Self Service Password Reset (SSPR) che consente di gestire il processo di modifica delle password e di reimpostazione delle password dimenticate. Durante la reimpostazione della password, SSPR utilizza un metodo di autenticazione a domanda/risposta per autenticare l'utente.

- ♦ [“Utilizzo di Self-Service Password Management in Identity Manager” a pagina 69](#)
- ♦ [“Utilizzo della gestione password esistente” a pagina 71](#)

Nota: in questa sezione sono descritte le funzioni di default per la gestione della password. Potrebbero sussistere alcune differenze correlate al ruolo e al livello di autorità dell'utente, nonché alle personalizzazioni effettuate dall'organizzazione. Per informazioni a questo proposito, rivolgersi all'amministratore del sistema.

Utilizzo di Self-Service Password Management in Identity Manager

SSPR si integra automaticamente con il processo single sign-on per le applicazioni di identità e Identity Reporting. È il programma di gestione delle password di default per Identity Manager. Quando un utente richiede la reimpostazione di una password, SSPR chiede di rispondere alla domanda di autenticazione. Se le risposte sono corrette, SSPR risponde in uno dei modi seguenti:

- ♦ Consenti agli utenti di creare una nuova password
- ♦ Crea una nuova password e inviala all'utente
- ♦ Crea una nuova password, inviala all'utente e contrassegna come scaduta la password precedente.

Per configurare la risposta, utilizzare l'editor di configurazione di SSPR. Dopo aver eseguito l'upgrade a una nuova versione di Identity Manager, è possibile configurare SSPR affinché utilizzi il metodo NMAS che solitamente viene impiegato da Identity Manager per la gestione delle password. SSPR, tuttavia, non riconosce le policy password esistenti per la gestione delle password dimenticate. È inoltre possibile configurare SSPR affinché utilizzi il rispettivo protocollo proprietario al posto di NMAS. Se si apporta questa modifica, non è possibile tornare a utilizzare NMAS senza reimpostare le policy password.

È possibile utilizzare SSPR per eseguire una delle funzioni elencate nella [Tabella 12-2, “Funzioni della gestione delle password”, a pagina 72:](#)

Tabella 12-1 Funzioni della gestione delle password

Pagina Gestione password	Per
Autenticazione CHAP	Impostare o modificare una delle opzioni seguenti: ♦ Risposte valide alle domande di autenticazione definite dall'amministratore ♦ Domande e risposte di autenticazione definite dall'utente
Cambia password	Cambiare (reimpostare) la password in base alle regole stabilite dall'amministratore di sistema
Stato	Rivedere i requisiti delle norme per le password.

Descrizione della domanda/risposta di autenticazione della password

Le Domande di autenticazione vengono utilizzate per verificare la propria identità durante il login se si è dimenticata la password. Se l'amministratore di sistema ha impostato le apposite norme per le password che abilitano questa funzione, è possibile utilizzare la pagina Autenticazione CHAP per:

- ♦ specificare le risposte valide alle domande definite dall'amministratore;
- ♦ specificare le domande e le risposte valide corrispondenti (se questa operazione è abilitata dalle norme della password).

Durante il processo di login, dalla pagina di login si viene reindirizzati automaticamente alla pagina Domanda/risposta di autenticazione. In questa pagina si configurano le risposte alle domande di autenticazione. Per ulteriori informazioni, vedere [“Password dimenticata” a pagina 22](#). Quando si esegue di nuovo il login e si tenta di reimpostare la password dimenticata, con SSPR vengono richieste le domande configurate ed è necessario fornire la risposta corretta. Quando la risposta corrisponde a quella salvata precedentemente, SSPR consente di reimpostare la password.

Modifica della password

È possibile modificare la password (purché l'amministratore di sistema abbia abilitato l'utente a compiere tale operazione).

- 1 Nel Dashboard, fare clic su **Applicazioni > Cambia password personale**.
- 2 Digitare la password attuale. Viene visualizzata la pagina Cambia password.



- 3 Immettere la nuova password nella casella di testo **Nuova password**.
- 4 Reimmettere la password nella casella di testo **Conferma password**.
- 5 Fare clic su **Modifica password**.

Se la nuova password viola una delle regole password definite dall'amministratore nella policy password, verrà visualizzato un messaggio di errore nella Pagina di modifica password.

Di norma in questa pagina sono contenute le informazioni su come specificare una password che soddisfi i requisiti della policy definiti dall'amministratore. Rivedere le regole password e riprovare.

- 6 Fare clic su **Continua**. Viene visualizzato lo stato della richiesta. Al completamento dell'operazione si tornerà alla pagina di login OSP.

Stato norme password

Nota: questa funzione è disponibile solo per gli utenti amministratori.

Vengono assegnate delle norme password dall'amministratore. Queste norme determinano le misure di sicurezza associate alla password. Non è possibile verificare i requisiti della policy password a meno che l'amministratore dell'applicazione utente non abbia fornito i diritti per eseguire tale operazione. L'amministratore dell'applicazione utente può verificare lo stato della policy password nella home page di Identity Manager. Per default, questo collegamento non esiste. Per includerlo è necessario personalizzare la home page. Per personalizzare gli elementi di default della pagina Home di Identity Manager, vedere [Capitolo 5, "Gestione delle applicazioni", a pagina 45](#).

Nella pagina di destinazione, fare clic sul collegamento **Stato e policy password**. Viene visualizzata la pagina **Stato policy e policy password**. Per modificare la password di Identity Manager, accedere a Home Identity Manager e selezionare Cambia password personale. Mediante il collegamento Home Identity Manager si viene reindirizzati all'area Modifica password di SSPR.

Utilizzo della gestione password esistente

In questo capitolo viene descritto come utilizzare la pagina Gestione password della scheda **Self-service identità** dell'applicazione utente Identity Manager. Gli argomenti trattati sono i seguenti:

- ♦ ["Autenticazione CHAP password" a pagina 72](#)
- ♦ ["Cambio suggerimento password" a pagina 73](#)
- ♦ ["Cambia password" a pagina 73](#)
- ♦ ["Stato norme password" a pagina 74](#)
- ♦ ["Stato sincronizzazione password" a pagina 75](#)

Nota: in questo capitolo vengono descritte le funzioni di default della pagina Gestione password. Potrebbero sussistere alcune differenze correlate al ruolo e al livello di autorità dell'utente, nonché alle personalizzazioni effettuate dall'organizzazione. Per informazioni a questo proposito, rivolgersi all'amministratore del sistema.

Per ulteriori informazioni di carattere generale sull'accesso e l'utilizzo della scheda **Self-service identità**, vedere il [Capitolo 10, "Gestione del profilo personale", a pagina 59](#).

È possibile utilizzare le pagine per la gestione delle password per eseguire una funzione qualsiasi elencata nella [Tabella 12-2](#), “Funzioni della gestione delle password”, a [pagina 72](#):

Tabella 12-2 Funzioni della gestione delle password

Pagina Gestione password	Per
Autenticazione CHAP	Impostare o modificare una delle opzioni seguenti: ♦ Risposte valide alle domande di autenticazione definite dall'amministratore ♦ Domande e risposte di autenticazione definite dall'utente
Cambio suggerimento password	Impostare o modificare il suggerimento per la password
Cambia password	Cambiare (reimpostare) la password in base alle regole stabilite dall'amministratore di sistema
Stato	Rivedere i requisiti delle norme per le password.
Stato sincronizzazione password	Consente di visualizzare lo stato della sincronizzazione delle password dell'applicazione con l'Identity Vault. Nota: se si accede alle applicazioni prima che il processo di sincronizzazione sia completato, possono verificarsi problemi di accesso.

Autenticazione CHAP password

Le Domande di autenticazione vengono utilizzate per verificare la propria identità durante il login se si è dimenticata la password. Se l'amministratore di sistema ha impostato le apposite norme per le password che abilitano questa funzione, è possibile utilizzare la pagina Autenticazione CHAP per:

- ♦ specificare le risposte valide alle domande definite dall'amministratore;
- ♦ specificare le domande e le risposte valide corrispondenti (se questa operazione è abilitata dalle norme della password).

Per utilizzare la pagina Autenticazione CHAP:

- 1 Nella scheda **Self-service identità** fare clic su **Autenticazione CHAP** nel menu in **Gestione password**.
Viene visualizzata la pagina Autenticazione CHAP:
- 2 Immettere una risposta appropriata in ogni casella di testo **Risposta**, obbligatoria, oppure utilizzare le risposte salvate in precedenza. Quando è selezionata l'opzione **Utilizzare la risposta memorizzata**, le risposte di autenticazione, incluse le etichette, non vengono visualizzate. Inoltre, le domande di autenticazione definite dall'utente sono disattivate.
Assicurarsi di specificare le risposte da ricordare in un secondo momento.
- 3 Specificare o modificare qualsiasi domanda definita dall'utente necessaria. Non è possibile utilizzare la stessa domanda più di una volta.

4 Fare clic su **Invia**.

Una volta salvate le risposte di autenticazione, nell'applicazione utente viene mostrato un messaggio indicante che queste sono state salvate correttamente e viene visualizzata nuovamente la schermata della risposta di autenticazione con l'opzione "Utilizzare la risposta memorizzata?" selezionata.

Cambio suggerimento password

Un suggerimento per la password viene utilizzato durante il login per facilitare la memorizzazione della password qualora venisse dimenticata. È possibile utilizzare la pagina Cambio suggerimento password per impostare o modificare il suggerimento.

1 Nella scheda **Self-service identità** scegliere **Cambio suggerimento password** dal menu in **Gestione password**.

Viene visualizzata la pagina Definizione suggerimento password.

2 Digitare il nuovo testo relativo al suggerimento.

La password non può essere visualizzata all'interno del testo del suggerimento.

3 Fare clic su **Invia**.

Viene visualizzato lo stato delle richieste.

Cambia password

È possibile utilizzare questa pagina qualora fosse necessario modificare la password, sempre che l'amministratore di sistema abbia abilitato questa funzione.

1 Nella scheda **Self-service identità** fare clic su **Cambia password** nel menu in **Gestione password**.

Viene visualizzata la pagina Cambia password. Se l'amministratore di sistema ha impostato le apposite norme per le password, in genere nella pagina Cambia password verranno visualizzate informazioni relative a come specificare una password che soddisfi i requisiti delle norme. Ad esempio:

Se non vi sono norme per le password applicabili, viene visualizzata la pagina di base di modifica della password, in cui sono disponibili i campi per la modifica della password.

L'applicazione utente supporta i seguenti tipi di sintassi della password:

- ♦ Policy di complessità Microsoft

Questo tipo di sintassi della password viene utilizzato con Active Directory 2003 per la compatibilità con versioni precedenti.

- ♦ Policy della password per Microsoft Server 2008

Si tratta di un nuovo tipo di sintassi della password aggiunto a eDirectory 8.8.7 per supportare Active Directory 2008.

Le seguenti impostazioni vengono supportate dalla policy della password per Microsoft Server 2008:

- ♦ utilizzo della policy della password per Microsoft Server 2008
- ♦ numero massimo di violazioni della policy di complessità nella password (0-5)
- ♦ Sintassi Novell

Le seguenti nuove impostazioni sono supportate dalla sintassi Novell:

- ♦ numero minimo di caratteri non alfabetici (1-512)
- ♦ numero massimo di caratteri non alfabetici (1-512)

Per tutti i tre tipi di sintassi della password, l'applicazione utente supporta le seguenti funzioni:

- ♦ Numero di caratteri differenti dalla password corrente e dalla cronologia delle password (0-6)
- ♦ Numero di password nella cronologia da considerare per l'esclusione dei caratteri (0-10)

Se l'amministratore ha abilitato la sintassi della policy di Microsoft Server 2008, compilare i seguenti campi nella Pagina di modifica password:

- 2 Immettere la password attuale nella casella di testo **Password precedente**.
- 3 Immettere la nuova password nella casella di testo **Password precedente**.
- 4 Reimmettere la password nella casella di testo **Ridigitare la password**.
- 5 Fare clic su **Invia**.

Se la nuova password viola una delle regole password definite dall'amministratore, verrà visualizzato un messaggio nella password Cambia password. Se si utilizza la policy per Microsoft Server 2008, la password effettua una violazione e l'interfaccia utente mostra questo messaggio nella parte superiore della pagina:

Password AD2008 complexity policy violation.

Se la nuova password effettua una violazione, rivedere le regole della password definite dall'amministratore e riprovare.

- 6 Può venire richiesto di specificare un suggerimento per la password, se l'amministratore ha configurato le norme di sicurezza per questo scopo. In questo caso, vedere ["Cambio suggerimento password" a pagina 73](#).
- 7 Viene visualizzato lo stato della richiesta.

Stato norme password

Vengono assegnate delle norme password dall'amministratore. Queste norme determinano le misure di sicurezza associate alla password. Per determinare i requisiti delle norme delle password, eseguire le seguenti operazioni:

- 1 Nella scheda **Self-service identità** scegliere **Stato norme password** dal menu in **Gestione password**. Verrà visualizzata la pagina **Stato norme password**.

Gli elementi contrassegnati come non validi non possono essere modificati.

Stato sincronizzazione password

Utilizzare la pagina Stato sinc password per determinare se la password è stata sincronizzata tra le varie applicazioni. Accedere a un'altra applicazione solo dopo aver sincronizzato la password. Se si accede alle applicazioni prima che il processo di sincronizzazione venga completato, possono verificarsi problemi di accesso.

- 1 Nella scheda **Self-service identità** scegliere **Stato sincronizzazione password** dal menu in **Gestione password**. Verrà visualizzata la pagina **Stato sincronizzazione password**. Le icone a colori indicano le applicazioni per cui la password è sincronizzata. Le icone inattive indicano le applicazioni non ancora sincronizzate.

Nota: solo l'amministratore può visualizzare la casella **Seleziona utente**.

IV Gestione di utenti, gruppi e team

Se si dispone del ruolo appropriato nelle applicazioni di identità, è possibile creare e gestire utenti, gruppi e team. È possibile creare utenti e team nel dashboard e nell'applicazione utente. Nell'Applicazione utente è possibile creare e gestire gruppi.

Gli amministratori di sistema possono creare utenti e gruppi. L'amministratore di sistema può concedere ad altri utenti, generalmente quelli selezionati che occupano posizioni di amministrazione o gestione, l'accesso a questa funzionalità.

Potrebbero sussistere alcune differenze tra le funzioni illustrate nel presente capitolo a causa del ruolo, del livello di autorità e delle personalizzazioni effettuate per l'organizzazione di appartenenza. Consultare l'amministratore del sistema per informazioni dettagliate.

Un team rappresenta un insieme di utenti, gruppi o utenti e gruppi in grado di eseguire richieste di provisioning e task di approvazione associati al team. Sebbene un team possa corrispondere a un gruppo esistente nella directory utente, i team non sono la stessa cosa dei gruppi. Vale a dire che un gruppo o un membro di un gruppo non può eseguire le funzionalità del team tranne quando è assegnato a un team. Vedere [Capitolo 14, "Gestione dei team", a pagina 83](#).

13 Gestione degli utenti

In questa sezione è indicato come creare utenti e gruppi nel Dashboard e nell'Applicazione utente. Gli argomenti trattati sono i seguenti:

- ♦ “Creazione di un utente” a pagina 79
- ♦ “Modifica delle informazioni utente” a pagina 79
- ♦ “Elenco degli utenti” a pagina 80
- ♦ “Individuazione degli utenti” a pagina 81
- ♦ “Ordinamento degli utenti” a pagina 82

Creazione di un utente

Nella pagina **Crea utente** sono visualizzati gli attributi utente abilitati con gli accessi a **ricerca** e **lettura** le cui proprietà possono essere configurate in Strato di astrazione directory. Per ulteriori informazioni, vedere la sezione relativa alle proprietà degli attributi [Attribute Properties](#) nella *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications* (in lingua inglese).

Per creare un utente, nel Dashboard selezionare:

Persone > Utenti > +

L'amministratore di identità definisce i valori che è possibile specificare per l'utente. Inoltre, quando si crea un utente, è possibile visualizzare il **Container** dell'utente ma non è consentito modificarne il valore. Questa limitazione assicura che tutti gli utenti vengano memorizzati nello stesso container.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Modifica delle informazioni utente

Selezionare un utente da una vista elenco e fare clic su  per modificare le informazioni utente come Qualifica, E-mail, Numero di telefono, Manager e altri dati. È consentito modificare gli attributi utente impostati dall'amministratore. Per ulteriori informazioni sulla configurazione degli attributi utente, vedere [Customizing the Views](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese). Nella vista **Gestisci utenti** è possibile eliminare utenti.

Di seguito è riportato un esempio di modifica delle informazioni utente:

Figura 13-1 Modifica delle informazioni utente

Aliyah Hall

Qualifica

Marketing Director +

Marketing Director x

Login disabilitato ☐

Numero di telefono

552538 +

552538 x

E-mail

aliyah@example.com +

aliyah@example.com x

Dipendenti diretti

🔍 Cerca utenti per Nome,Cognome

Manager

🔍 Cerca utenti per Nome,Cognome

Salva Annulla

Nota: per disabilitare un account utente, è possibile utilizzare l'interruttore **Login disabilitato**. Questo interruttore è visibile solo se l'amministratore aggiunge l'attributo **Login disabilitato** nella Vista scheda e negli Attributi modificabili nella pagina **Impostazioni > Personalizzazione**. Per ulteriori informazioni, fare clic su nel Dashboard.

Elenco degli utenti

Di seguito sono indicati vari metodi per elencare gli utenti nelle applicazioni di identità:

- ♦ **Vista elenco:** per visualizzare gli utenti in formato elenco, fare clic su . Le informazioni sull'utente vengono visualizzate sul lato destro. Per modificare le informazioni utente come Numero di telefono, E-mail, Manager e altro, fare clic su . Se si desidera visualizzare l'organigramma di un utente particolare, fare clic su .
- ♦ **Vista scheda:** per visualizzare gli utenti in formato scheda, fare clic su . Le informazioni di base degli utenti vengono visualizzate sulle schede. L'amministratore può configurare quali informazioni visualizzare sulla scheda dell'utente. Per ulteriori informazioni, vedere la sezione relativa alla personalizzazione delle viste [Customizing the Views in NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (in lingua inglese). Fare clic su per modificare le informazioni utente come **Numero di telefono**, **E-mail**, **Manager** e altri attributi. Se si desidera visualizzare l'organigramma di un utente particolare, fare clic su .

- ♦ **Vista Gestisci utenti:** per visualizzare gli utenti in formato tabella, fare clic su . Gli utenti vengono visualizzati in una tabella che consente di ordinare gli utenti in base agli attributi come Numero di telefono, E-mail, Reparto e altro. È possibile personalizzare le colonne da visualizzare in questa vista. Per ulteriori informazioni sulla personalizzazione delle colonne, fare clic su  nel Dashboard.

Questa vista consente inoltre di eliminare gli utenti dal sistema. Per eliminare gli utenti:

1. Selezionare un utente che si desidera eliminare.
2. Fare clic su .

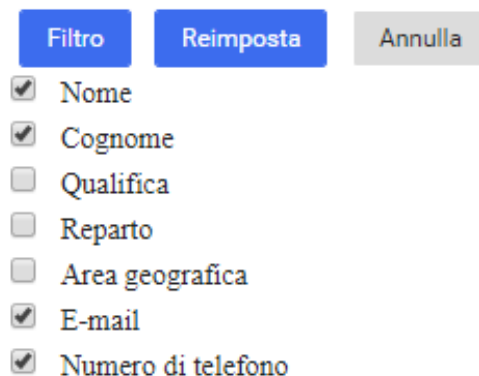
Individuazione degli utenti

Di seguito sono indicati vari metodi per trovare gli utenti nelle applicazioni di identità:

- ♦ **Ricerca rapida:** specifica l'attributo utente ed elenca gli utenti in base ai filtri selezionati. Per modificare le opzioni di filtro:

1. Fare clic su .
2. Selezionare l'opzione di filtro per cercare gli utenti.

Di seguito è riportato un esempio di attributi utente selezionati per una ricerca rapida:



Attributo	Stato
Nome	Selezionato
Cognome	Selezionato
Qualifica	Non selezionato
Reparto	Non selezionato
Area geografica	Non selezionato
E-mail	Selezionato
Numero di telefono	Selezionato

3. Fare clic su **Filtro**.

Ad esempio, per cercare un utente con il nome Rossi dove sono selezionati i filtri Nome e Cognome. La ricerca rapida elenca tutti gli utenti con Rossi in Nome e Cognome.

- ♦ **Ricerca avanzata:** questa opzione consente di recuperare un elenco più rifinito di utenti rispetto alla ricerca rapida. È possibile cercare un utente con gli attributi definiti. Per utilizzare la ricerca avanzata:

1. Fare clic su .
2. Specificare le informazioni esatte per ogni attributo utente.

Di seguito è riportato un esempio di attributi utente selezionati per una ricerca avanzata:

RICERCA AVANZATA



Ricerca per

Nome ▼	Emily	×
Cognome ▼	Cameron	×
E-mail ▼	emily.cameron@example.com	×
Numero di telefon ▼	5552368	×
+ Aggiungi		

3. Fare clic su **Filtro**.

Ad esempio, se si desidera cercare un utente con **Nome** Alina, **Cognome** Sala e **Qualifica** Direttore. È possibile specificare questi attributi nella Ricerca avanzata per trovare un utente con la serie esatta di attributi.

È inoltre possibile configurare i risultati di ricerca su una pagina impostando l'indice al fondo. Il dashboard utilizza il controllo Virtual List View (VLV) eseguito in LDAP OID 2.16.840.1.113730.3.4, in combinazione con il controllo di ordinamento.

Il dashboard di Identity Manager visualizza due diversi conteggi insieme ai risultati:

- ♦ **Conteggio totale:** il numero totale di utenti trovati nel sistema.
- ♦ **Conteggio ricerca:** il numero di utenti visualizzati per la ricerca specifica.

Ordinamento degli utenti

La vista Gestisci utenti consente di ordinare gli utenti in base ai loro attributi. Per attivare l'ordinamento, l'amministratore deve configurare gli indici composti per gli attributi utente. Per ulteriori informazioni sull'indicizzazione composta, vedere [Creating Compound Indexes](#) in *NetIQ Identity Manager Install and Upgrade Guide for Windows* (in lingua inglese).

Nota: se non è possibile ordinare gli utenti con gli attributi utente, rivolgersi all'amministratore per configurare l'indice composto per l'attributo richiesto per ordinare gli utenti.

14 Gestione dei team

Un team è costituito da due tipi di utenti:

Richiedente

Esegue le richieste di autorizzazione per conto di altri membri del team (i destinatari). A seconda di come è configurato il team, un richiedente può agire su una singola richiesta di provisioning, su una o più categorie di richiedenti o su tutte le richieste.

Il richiedente gestisce anche le assegnazioni di utenti incaricati per il membri del team.

Destinatario

Membro del team per conto del quale possono agire i richiedenti.

I destinatari del team possono essere utenti o gruppi nella directory. In alternativa, è possibile recuperarli dalle relazioni di directory. È ad esempio possibile ricavare l'elenco dei membri mediante le relazioni manager-dipendente all'interno dell'organizzazione. In questo caso i destinatari del team sono tutti gli utenti che fanno riferimento al manager del team.

Nota: l'amministratore di provisioning può configurare lo strato di astrazione della directory in modo da supportare relazioni di sovrapposizione affinché sia possibile includere in un team più livelli di un'organizzazione. Il numero di livelli da includere viene configurato dall'amministratore.

Per eseguire una delle attività seguenti, selezionare **Persone > Team**:

- ♦ [“Visualizzazione dei team” a pagina 83](#)
- ♦ [“Creazione di un team” a pagina 84](#)
- ♦ [“Modifica di un team” a pagina 84](#)

Visualizzazione dei team

Nella pagina **Team** sono elencati tutti i team di cui si dispone delle autorizzazioni per la visualizzazione. È possibile essere membro di tutti i team elencati, ma è tuttavia possibile essere anche un amministratore dotato di autorizzazioni per la visualizzazione, la modifica o la cancellazione di determinati team, senza necessariamente essere un membro.

Un membro del team può essere un **richiedente** in grado di effettuare richieste per conto di altri membri del team. Inoltre, altre persone nel team potrebbero eseguire tali azioni per conto di un membro **destinatario**. Per ulteriori informazioni, fare clic su  nel Dashboard.

Creazione di un team

Gli amministratori possono creare i team. Un **team** rappresenta un insieme di utenti, gruppi o utenti e gruppi in grado di eseguire richieste di provisioning e task di approvazione associati al team.

Per ciascun team, specificare i membri (**Destinatari**) che ricevono le autorizzazioni del team e coloro che sono autorizzati ad agire per conto dei destinatari (**Richiedenti**). Dopo aver creato un team, è possibile specificare le **Autorizzazioni** (definizioni di risorse e richieste di provisioning) valide per i membri del team. Ad esempio, è possibile aggiungere una risorsa computer portatile che potrebbe essere necessaria per i membri del team.

Per ulteriori informazioni, fare clic su  nel Dashboard.

Modifica di un team

Gli amministratori possono modificare e cancellare i team. È possibile modificare i seguenti aspetti di un team:

- ♦ Modifica del nome e della descrizione del team.
- ♦ Modifica dei richiedenti per il team.
- ♦ Aggiunta o rimozione dei membri del team.
- ♦ Aggiunta o rimozione delle autorizzazioni per un manager del team.

Per ulteriori informazioni, fare clic su  nel Dashboard.

15 Gestione dei gruppi

Un gruppo è costituito da utenti e altri account con caratteristiche comuni. Ad esempio, il gruppo Finanza è composto da tutti gli impiegati del reparto finanziario.

È possibile cercare i gruppi in base alla relativa descrizione. Tuttavia, gli amministratori con accesso alla pagina **Impostazioni** possono personalizzare gli attributi con i quali è possibile cercare un'entità del gruppo. Pertanto, quando si effettua la ricerca di un gruppo specifico per assegnargli un ruolo, renderlo il proprietario di una risorsa o semplicemente per cercarlo all'interno della pagina **Gruppi**, l'applicazione restituisce i nomi del gruppo come risultato corrispondente all'attributo cercato. Per ulteriori informazioni, vedere la sezione relativa alle impostazioni delle entità **Entity Settings** nella *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Creazione di un gruppo

Se si dispone di un ruolo amministrativo nelle applicazioni di identità, è possibile creare un gruppo.

- 1 Nel Dashboard di Identity Manager, selezionare **Persone > Gruppi**.
- 2 Fare clic su **+**.
- 3 Specificare i valori per i seguenti attributi obbligatori:

Attributo	Dati da specificare
Nome	Il nome gruppo per questo nuovo gruppo. Importante: non utilizzare questi caratteri speciali nel campo Nome : < ; \ " + # / * ~
Descrizione	Descrizione del nuovo gruppo. La descrizione viene utilizzata come criterio di ricerca del gruppo nel Dashboard. Importante: non utilizzare questi caratteri speciali nel campo Descrizione : ~
Container	Una unità organizzativa nell'identity vault in cui si desidera memorizzare il nuovo gruppo, ad esempio UO denominata gruppi. Ad esempio: ou=groups, ou=MyUnit, o=MyOrg Per informazioni relative all'utilizzo dei pulsanti forniti per specificare un container, vedere <i>"Creazione di un utente"</i> a pagina 79. Nota: non verrà richiesto di specificare un Container se l'amministratore di sistema ne ha definito uno creato di default per questo tipo di oggetto.

- 4 Fare clic su **Crea**.

In seguito alla creazione del gruppo, è possibile aggiungere gli utenti dal pannello **Membri gruppo** che viene visualizzato.

- 5 Per aggiungere utenti al gruppo, fare clic sull'icona + accanto ai membri del gruppo.
- 6 Selezionare gli utenti richiesti nella finestra modale.
- 7 Fare clic su **Aggiungi**.

V Appendice

Nella seguente appendice vengono fornite informazioni di riferimento aggiuntive e argomenti avanzati per l'applicazione utente Identity Manager.

A Utilizzo dell'app Identity Manager Approvals

Oltre all'interfaccia dell'applicazione utente utilizzata dai clienti di Identity Manager, adesso è possibile utilizzare una nuova app iOS che consente agli utenti di Identity Manager di approvare o rifiutare le richieste in remoto per mezzo del Modulo di provisioning basato su ruoli per Identity Manager.

Una volta installata e configurata l'app Approvals, in quest'ultima è possibile visualizzare gli stessi task di approvazione che normalmente vengono visualizzati nell'interfaccia dell'applicazione utente. Tra l'app Approvals e l'applicazione utente vengono sincronizzate tutte le modifiche.

È inoltre possibile lavorare in modalità offline quando si è disconnessi dal server del Modulo di provisioning basato su ruoli di Identity Manager, tutte le modifiche verranno sincronizzate automaticamente dall'app Approvals una volta ripristinata la connettività.

In questa appendice sono contenute le informazioni necessarie per l'installazione e l'utilizzo della nuova app Approvals. Per informazioni su come gli amministratori di Identity Manager possono configurare il rispettivo ambiente per consentire agli utenti di utilizzare l'app, vedere [“Configuring the Identity Manager Approvals App”](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).

Per ulteriori informazioni sull'app Approvals, consultare le seguenti sezioni:

- ♦ [“Requisiti del prodotto”](#) a pagina 89
- ♦ [“Installazione dell'app Approvals”](#) a pagina 90
- ♦ [“Configurazione dell'app Approvals”](#) a pagina 90
- ♦ [“Panoramica dell'app Approvals”](#) a pagina 94
- ♦ [“Modifica della lingua visualizzata dell'app Approvals”](#) a pagina 96

Requisiti del prodotto

Per l'app Approvals è necessario un iPhone o un iPad Apple sul quale sia installato Apple iOS 6 o iOS 7 o qualsiasi dispositivo con sistema operativo Android 5.0 o versione successiva.

Nota: se l'amministratore non ha abilitato l'uso dell'app Approvals, potrebbe risultare impossibile configurare l'app dopo l'installazione. Per informazioni su come gli amministratori possono configurare l'ambiente di Identity Manager per abilitare l'uso dell'app Approvals, vedere [“Configuring the Identity Manager Approvals App”](#) in *NetIQ Identity Manager - Administrator's Guide to the Identity Applications* (in lingua inglese).

Installazione dell'app Approvals

È possibile installare l'app NetIQ Identity Manager Approvals nel proprio dispositivo dalla [pagina dell'app Approvals](#) dell'Apple Store.

Dopo aver installato l'app Approvals, è necessario configurarla in modo che possa connettersi al server del Modulo di provisioning basato su ruoli.

Nota: se la password dell'applicazione utente è scaduta, si consiglia di modificarla prima di installare e configurare l'app Approvals. Se la policy password definita per l'ambiente consente un numero limitato di login extra allo scadere di una password, è possibile che l'app Approvals utilizzi tutti questi login nel tentativo di sincronizzare i task di Identity Manager con il dispositivo dell'utente.

Configurazione dell'app Approvals

È possibile configurare l'app NetIQ Identity Manager Approvals in diversi modi, a seconda delle esigenze dell'ambiente dell'utente e in base a come l'amministratore ha configurato Identity Manager:

- ♦ Effettuare una richiesta nell'interfaccia dell'applicazione utente per accedere all'app Approvals, quindi avviare quest'ultima sul dispositivo dal collegamento inviato tramite e-mail dall'amministratore di Identity Manager. Nel collegamento sono incluse tutte le informazioni necessarie per la configurazione.
- ♦ Fare clic su un collegamento di configurazione oppure effettuare la scansione di un codice QR della configurazione utilizzando il dispositivo, dove il collegamento o il codice QR fornisce tutte le informazioni necessarie per la configurazione o le informazioni sulla configurazione generiche per la società.
- ♦ Immettere manualmente le informazioni sulla configurazione per l'ambiente in uso nell'app stessa.

Importante: affinché gli utenti siano in grado di configurare automaticamente l'app Approvals tramite un collegamento o un codice QR, l'amministratore dell'ambiente di Identity Manager deve prima abilitare il collegamento o il codice QR.

Richiesta dell'accesso mobile tramite l'applicazione utente

Se è stato configurato dall'amministratore, è possibile richiedere l'accesso all'app Approvals tramite l'applicazione utente. Identity Manager invia quindi un'e-mail contenente un collegamento personalizzato che è possibile aprire sul dispositivo in modo da configurare automaticamente l'app con le informazioni dell'utente.

Per richiedere l'accesso mobile tramite l'applicazione utente:

- 1 In un browser Web, eseguire il login all'applicazione utente Identity Manager utilizzando il protocollo HTTPS (`https://`).

Nota: per richiedere l'accesso all'app Approvals, è necessario eseguire il login all'applicazione utente utilizzando il protocollo HTTPS.

- 2 Fare clic su **Effettua richiesta di processo**.
- 3 Fare clic sul menu a discesa Categoria richiesta processo e selezionare **Account**.
- 4 Fare clic su **Continua**.
- 5 Fare clic su **Richiedi applicazione di approvazione mobile**.

Nota: la categoria e il nome della richiesta di processo possono variare a seconda di come l'amministratore ha configurato il processo di richiesta dell'app Approvals.

- 6 Fornire le informazioni richieste nel modulo di richiesta del processo e fare clic su **Invia**.
- 7 Alla ricezione di un'e-mail da parte dell'amministratore di Identity Manager, aprirla sul dispositivo e fare clic sul collegamento fornito per connettere il dispositivo al server del Modulo di provisioning basato su ruoli.

Nota: se in precedenza si è installata l'app, è possibile che in quest'ultima venga visualizzato un messaggio di errore per informare l'utente che le impostazioni esistenti verranno sovrascritte. Accertarsi che il nome host visualizzato nel messaggio di avviso sia lo stesso host nel quale si è eseguito l'accesso dopo aver richiesto di accedere all'app. In caso di dubbio, non fare clic sul collegamento e contattare l'amministratore.

Se il nome host è corretto, fare clic su **Accetta** per sovrascrivere le impostazioni esistenti.

- 8 All'avvio dell'app, immettere la password e fare clic sull'icona Test connessione  per verificare le impostazioni.

Utilizzo di un collegamento di configurazione o di un codice QR

L'amministratore di Identity Manager può fornire un collegamento di configurazione per configurare l'app Approvals. Aprire il collegamento in un browser sul dispositivo per configurare automaticamente l'app.

Questo collegamento può tuttavia fornire solo alcune delle impostazioni richieste. Di norma, un collegamento o un codice può fornire solo i dettagli relativi al server del Modulo di provisioning basato su ruoli necessari per il funzionamento dell'app Approvals. Dopo aver fatto clic sul collegamento, è necessario configurare manualmente le impostazioni relative a Nome utente e Password, nonché tutte le altre impostazioni che non vengono configurate automaticamente.

In alcuni ambienti potrebbe risultare impossibile accedere all'e-mail dal dispositivo. Se non è possibile ricevere l'e-mail sul dispositivo, in alternativa si può utilizzare quest'ultimo per effettuare la scansione di un codice QR personalizzato fornito dall'amministratore di Identity Manager.

Se necessario, visualizzare sul computer o su una pagina stampata il codice QR fornito, quindi effettuare la scansione del codice utilizzando un lettore di codici QR sul dispositivo. Dopo la configurazione automatica dell'app Approvals effettuata tramite il codice QR per il rispettivo ambiente, configurare manualmente le impostazioni relative a Nome utente e Password.

Configurazione manuale dell'app Approvals

Se l'amministratore dell'ambiente di Identity Manager non fornisce un collegamento o un codice QR da utilizzare per la configurazione dell'app Approvals, è possibile configurare le impostazioni richieste anche manualmente.

Avviso: poiché la configurazione manuale dell'app sul dispositivo richiede una conoscenza approfondita dei componenti di Identity Manager, è consigliabile che venga eseguita solo da utenti esperti del Modulo di provisioning basato su ruoli e dell'ambiente dell'applicazione utente all'interno dell'azienda. Gli altri utenti devono contattare il rispettivo amministratore di Identity Manager per le informazioni su come configurare l'app.

Nell'app, fare clic sull'icona Impostazioni , specificare le impostazioni richieste, quindi fare clic sull'icona Test connessione  per verificare le impostazioni configurate.

L'app Approvals richiede le seguenti impostazioni:

Nome impostazione di login	Descrizione impostazione di login
Nome utente	Specifica il nome utente da utilizzare per accedere al server del Modulo di provisioning basato su ruoli.
Password	Specifica la password da utilizzare per accedere al server del Modulo di provisioning basato su ruoli.
Sincronizzazione dati	Specifica se si desidera utilizzare l'app per sincronizzare attivamente i dati con il server del Modulo di provisioning basato su ruoli.
Avanzate > Dettagli server > Server	Specifica il nome di dominio completo o l'indirizzo IP del server del Modulo di provisioning basato su ruoli.
Avanzate > Dettagli server > Porta sicura	Specifica la porta HTTPS utilizzata dall'app per connettersi al server.
Avanzate > Dettagli server > Contesto	Specifica il contesto utilizzato durante l'installazione del file WAR dell'applicazione utente. Il valore di default è IDMPROV.
Avanzate > Dettagli server > Container utente	Specifica il DN completo del container di Identity Vault in cui vengono memorizzate le informazioni dell'utente.
Avanzate > Dettagli server > Timeout	Specifica il numero di secondi di attesa dell'app durante il tentativo di connettersi al server prima di annullare la connessione. Il valore di default è 5 secondi.
Avanzate > Impostazioni definizione dati > Entità utente	Specifica l'entità LDAP che rappresenta un utente in Identity Vault. Il valore di default è user.
Avanzate > Impostazioni definizione dati > Formato nome	Specifica la rappresentazione dell'attributo DAL utilizzata dall'app per definire il formato del nome completo di un utente. Il valore di default è FirstName LastName.
Avanzate > Impostazioni definizione dati > Attributo nome	Specifica il nome dell'attributo DAL che rappresenta il nome di battesimo di un utente. Il valore di default è FirstName.

Nome impostazione di login	Descrizione impostazione di login
Avanzate > Impostazioni definizione dati > Attributo cognome	Specifica il nome dell'attributo DAL che rappresenta il cognome di un utente. Il valore di default è LastName.
Avanzate > Impostazioni definizione dati > Attributo foto utente	Specifica il nome dell'attributo DAL che contiene la foto di un utente. Il valore di default è UserPhoto. Nota: se non è stata configurata un'immagine in Identity Manager o se le impostazioni di Identity Manager sono state configurate in modo che non venga visualizzata un'immagine, l'app visualizzerà un'immagine generica.
Avanzate > Impostazioni definizione dati > Attributo telefono ufficio	Specifica il nome dell'attributo DAL che rappresenta il numero di telefono dell'ufficio di un utente. Il valore di default è TelephoneNumber.
Avanzate > Impostazioni definizione dati > Attributo telefono cellulare	Specifica il nome dell'attributo DAL che rappresenta il numero di telefono del cellulare di un utente. Il valore di default è mobile.
Avanzate > Impostazioni definizione dati > Attributo e-mail	Specifica il nome dell'attributo DAL che rappresenta l'indirizzo e-mail di un utente. Il valore di default è Email.
Avanzate > Impostazioni definizione dati > Attributo LDAP foto	Specifica il nome dell'attributo LDAP che contiene la foto dell'utente. Il valore predefinito è photo.
Avanzate > Impostazioni definizione dati > Attributo di denominazione	Specifica l'attributo DAL di denominazione utilizzato in Identity Vault per descrivere un nome. Il valore predefinito è cn.
Avanzate > Impostazioni definizione dati > Amministratore provisioning	Specifica se l'utente è un amministratore di provisioning nel server del Modulo di provisioning basato su ruoli.
Avanzate > Certificati accettati	Specifica tutti i certificati non validi o firmati da se stessi dal server del Modulo di provisioning basato su ruoli che si consente che vengano accettati dall'app Approvals. Quando l'app Approvals rileva un certificato firmato da se stessi o non valido, viene richiesto di accettarlo o rifiutarlo. Se si accetta il certificato, l'app aggiunge un certificato all'elenco Certificati accettati. È possibile rimuovere un certificato dall'elenco Certificati accettati facendo clic sul nome del certificato e riavviando l'app. Nota: se il certificato del server del Modulo di provisioning basato su ruoli è valido, l'app non lo aggiunge all'elenco dei certificati accettati. Per default l'app accetta i certificati validi.

Nome impostazione di login	Descrizione impostazione di login
Avanzate > Certificati rifiutati	Specifica tutti i certificati non validi o firmati da se stessi dal server del Modulo di provisioning basato su ruoli che non si desidera che vengano accettati dall'app Approvals. Quando l'app Approvals rileva un certificato firmato da se stessi o non valido, viene richiesto di accettarlo o rifiutarlo. Se si rifiuta il certificato, l'app aggiunge un certificato all'elenco Certificati rifiutati. Se il server presenta quindi un certificato rifiutato, per l'app sarà impossibile connettersi al server. È possibile rimuovere un certificato dall'elenco Certificati rifiutati facendo clic sul nome del certificato.

Panoramica dell'app Approvals

In questa sezione è riportata una panoramica dell'interfaccia utente dell'app NetIQ Identity Manager Approvals. Gli argomenti trattati sono i seguenti:

- ♦ [“Vista Task” a pagina 94](#)
- ♦ [“Vista Dettagli” a pagina 95](#)
- ♦ [“Modalità in massa” a pagina 95](#)
- ♦ [“Vista Task completati” a pagina 95](#)
- ♦ [“Vista Impostazioni di login” a pagina 96](#)
- ♦ [“Vista Impostazioni avanzate” a pagina 96](#)

Vista Task

Task è la vista di default dell'app Approvals. In questa vista sono visualizzati tutti i task attualmente assegnati o assunti dall'utente e sono riportati il titolo del task e il nome e la foto del destinatario del task. Nella vista sono elencati i task in ordine di scadenza: i task prossimi alla scadenza vengono visualizzati in alto e quelli senza data di scadenza in basso.

Nota

- ♦ se non è stata configurata un'immagine dell'utente in Identity Manager o se le impostazioni di Identity Manager sono state configurate in modo che non venga visualizzata un'immagine, l'app visualizzerà un'immagine generica.
- ♦ Con l'app Approvals non è possibile approvare o rifiutare task che utilizzano moduli complessi.
- ♦ Attualmente l'app Approvals non supporta nuovi moduli JSON su entrambe le piattaforme, iOS e Android. Pertanto è possibile che venga visualizzato un messaggio di errore o che non si riesca a visualizzare i dettagli del task.

Se si desidera approvare o rifiutare una richiesta o per visualizzare i dettagli di un determinato task, fare clic sul task o sul nome del destinatario del task. Se si desidera contattare un destinatario del task, fare clic sull'immagine corrispondente.

Vista Dettagli

Nella vista Dettagli sono visualizzati i dettagli di un determinato task assegnato all'utente. I campi visualizzati variano a seconda della richiesta.

Per approvare o rifiutare un task, fornire tutte le informazioni necessarie e fare clic su **Approva** o **Rifiuta**.

Modalità in massa

Se si deve approvare o rifiutare un numero elevato di task simili, nella vista Task è possibile passare dalla modalità a task singolo alla modalità in massa.

Nota: è impossibile approvare tutti i task in modalità in massa. Per task più complessi, come quelli di attestazione, è necessario approvare ogni task di attestazione separatamente in modalità a task singolo. Quando si fa clic sull'icona Modalità in massa, nell'app vengono visualizzati solo i task presenti nell'elenco che è possibile approvare in massa.

Per approvare o rifiutare più task:

- 1 Nella vista Task fare clic sull'icona Modalità in massa .
- 2 Selezionare i task da approvare o rifiutare. È impossibile approvare alcuni task e rifiutarne altri contemporaneamente.
- 3 (Opzionale) Se si desidera approvare o rifiutare tutti i task, fare clic su **Tutto**.
- 4 (Opzionale) Se si cambia idea e non si desidera approvare o rifiutare alcun task, fare clic sull'icona della modalità a task singolo .
- 5 Fare clic su **Approva** o **Rifiuta**.
- 6 (Opzionale) Fornire un commento in merito all'operazione in massa.
- 7 Fare clic su **Conferma**.

Vista Task completati

Per visualizzare i task completati, fare clic sull'icona Task completati . Nella vista è visualizzato il task completato, nonché l'ora in cui il task è stato approvato o rifiutato. È possibile fare clic su un task completato per visualizzarne i dettagli. Per richieste più complesse, è possibile fare clic su **Valori modulo** per visualizzare informazioni specifiche relative alla richiesta.

Se necessario, è possibile eliminare uno o più task completati dalla vista Task completati. Per

eliminare i task, fare clic sull'icona Modalità in massa , selezionare i task da eliminare e fare clic su **Elimina**.

Nota: nella vista Task completati vengono visualizzati solo i task completati nel dispositivo. È impossibile visualizzare i task completati nell'applicazione utente o in un altro dispositivo se è installata l'app Approvals.

Vista Impostazioni di login

Nella vista Impostazioni di login è possibile visualizzare o modificare le impostazioni di login.

Avviso: se l'amministratore di Identity Manager ha fornito un collegamento o un codice QR per configurare automaticamente le impostazioni dell'app, si consiglia di non modificare tali impostazioni di default salvo istruzioni diverse da parte dell'amministratore.

Vista Impostazioni avanzate

Nella vista Impostazioni avanzate è possibile visualizzare o modificare le impostazioni avanzate e determinare la modalità di ricezione dei dati da parte del server del Modulo di provisioning basato su ruoli.

Avviso: se l'amministratore di Identity Manager ha fornito un collegamento o un codice QR per configurare automaticamente le impostazioni dell'app, si consiglia di non modificare tali impostazioni di default salvo istruzioni diverse da parte dell'amministratore.

Se nella vista Impostazioni avanzate si modificano incidentalmente le impostazioni per la definizione dei dati, fare clic su **Ripristina valori di default** per ripristinare le impostazioni di default fornite da Identity Manager. L'impostazione **Ripristina valori di default** non modifica il nome utente, la password o le impostazioni relative ai dettagli del server.

Modifica della lingua visualizzata dell'app Approvals

Nell'app Approvals sono incluse stringhe di testo localizzate in più lingue. Per modificare la lingua utilizzata dall'app Approvals, modificare le impostazioni relative alla lingua e al formato regionale nel dispositivo iOS. Con le impostazioni relative al formato regionale è possibile configurare come vengono visualizzati sul dispositivo le date, le ore e i numeri di telefono.

Per modificare le impostazioni relative a lingua e paese:

- 1 Nel dispositivo iOS fare clic su **Impostazioni**.
- 2 Fare clic su **Generale**.
- 3 Fare clic su **Internazionale**.
- 4 (Opzionale) Se si desidera modificare la lingua utilizzata dal dispositivo, fare clic su **Lingua**, selezionare la lingua da utilizzare e fare clic su **Fine**.
- 5 (Opzionale) Se si desidera modificare il formato regionale utilizzato dal dispositivo per le date e le ore, fare clic su **Formato regionale**, selezionare il formato da utilizzare e fare clic su **Internazionale**.
- 6 Tornare alla schermata home del dispositivo.