Identity Console
Guida all'amministrazione

Settembre 2022

Note legali

Sommario

Informazioni sulla guida e sulla libreria

L'*Administration Guide* (Guida all'amministrazione) fornisce informazioni concettuali sul prodotto NetIQ Identity Console (Identity Console). Questa guida definisce la terminologia e include scenari di implementazione.

Per la versione più recente della *NetIQ Identity Console Administration Guide* (Guida all'amministrazione di NetIQ Identity Console), vedere la versione inglese della documentazione sul sito sulla documentazione online di NetIQ Identity Console.

Destinatari

Questa guida è destinata agli amministratori di rete.

Altre informazioni incluse nella libreria

La libreria contiene le risorse seguenti:

Guida all'installazione

Descrive come installare Identity Console. Questa guida è destinata agli amministratori di rete.

Informazioni su NetIQ Corporation

NetIQ Corporation è una società globale di software per le aziende, focalizzata su tre problematiche costanti dell'ambiente aziendale (cambiamento, complessità e rischio) e che offre soluzioni utili per gestirle.

Il nostro punto di vista

Adattamento al cambiamento e gestione della complessità: sfide ben note

Fra tutte le sfide da affrontare, queste sono forse le variabili principali che impediscono il controllo necessario a misurare, monitorare e gestire in modo sicuro gli ambienti informatici fisici, virtuali e cloud.

Erogazione migliore e più rapida dei servizi di business di importanza critica

Siamo convinti del fatto che le nostre soluzioni per assicurare il massimo controllo possibile alle organizzazioni IT siano il solo percorso possibile verso un'erogazione tempestiva ed economica dei servizi. Il costante processo di cambiamento delle organizzazioni e la maggiore complessità intrinseca delle tecnologie necessarie per gestirlo continueranno ad esercitare pressioni sempre più forti.

La nostra filosofia

Vendiamo soluzioni intelligenti e non semplice software

Al fine di poter garantire un controllo affidabile, prima di tutto ci dedichiamo a comprendere le situazioni reali in cui le aziende dell'IT operano quotidianamente. Questo approccio è il solo che consenta di sviluppare soluzioni IT pratiche e intelligenti, capaci di garantire risultati misurabili e comprovati, e che ci gratifica molto di più della semplice vendita di software.

Il successo degli utenti è il nostro stimolo

Il fulcro attorno al quale ruota la nostra attività aziendale è il successo degli utenti. Dall'ideazione del prodotto alla sua installazione, comprendiamo appieno l'esigenza dei nostri clienti di poter contare su soluzioni IT funzionanti che si integrino alla perfezione con i prodotti esistenti. Forniamo, inoltre, supporto costante e formazione successiva all'installazione, confermando di essere a tutti gli effetti un partner con cui è veramente facile collaborare. In sintesi: il successo degli utenti è il nostro successo.

Le nostre soluzioni

- Governance di identità e accessi
- Gestione degli accessi
- Gestione della sicurezza

- Gestione di sistemi e applicazioni
- Gestione del workload
- Gestione del servizio

Contattare l'assistenza alle vendite

Per informazioni su prodotti, prezzi e funzionalità, rivolgersi al partner locale. In caso d'impossibilità, contattare il team di assistenza alle vendite.

Sedi globali:	www.netiq.com/about_netiq/officelocations.asp
Stati Uniti e Canada:	1-888-323-6768
E-mail:	info@netiq.com
Sito Web:	www.netiq.com

Contattare il supporto tecnico

Per problemi specifici del prodotto, rivolgersi al team del supporto tecnico.

Sedi globali:	www.netiq.com/support/contactinfo.asp
Nord e Sud America:	1-713-418-5555
Europa, Medio Oriente e Africa:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Sito Web:	www.netiq.com/support

Contattare il supporto per la documentazione

NetIQ desidera fornire tutta la documentazione necessaria per indicare le soluzioni più appropriate alle esigenze degli utenti. Per inviare suggerimenti di miglioramento, fare clic su **comments on this topic** (commenti su questo argomento) in fondo a qualsiasi pagina nelle versioni in HTML della documentazione pubblicata sul sito Web www.netiq.com/documentation. È inoltre possibile inviare un'e-mail a Documentation-Feedback@netiq.com. La collaborazione degli utenti è una fonte preziosa e saremo lieti di ricevere qualsiasi suggerimento.

Contattare la comunità online di utenti

La comunità online di NetIQ, Qmunity, è una rete collaborativa che unisce utenti ed esperti di NetIQ. È una risorsa che contribuisce ad acquisire la conoscenza approfondita necessaria a sfruttare a pieno il potenziale degli investimenti IT fondamentali, in quanto offre informazioni più immediate, collegamenti e risorse utili e accesso agli esperti di NetIQ. Per ulteriori informazioni, visitare il sito http://community.netiq.com.

1 Cos'è Identity Console?

Identity Console è una console di amministrazione d'avanguardia basata sul Web che fornisce un accesso virtuale, sicuro e personalizzato alle utility di amministrazione della rete da qualsiasi postazione tramite Internet e browser Web. Identity Console semplifica notevolmente la decentralizzazione dei task amministrativi.

Funzioni di Identity Console

In Identity Console sono disponibili le seguenti funzioni:

- Amministrazione di oggetti, utenti, schemi, partizioni, repliche, diritti di eDirectory e molto altro.
- Gestione dei driver e dei set di driver di Identity Manager
- Gestire e visualizzare le statistiche sulle prestazioni del driver
- Controllo degli oggetti, visualizzazione del flusso di dati del driver, gestione delle autorizzazioni, degli ordini di lavoro e così via.
- Gestione dello stato e delle impostazioni di sincronizzazione delle password per i driver
- Gestione delle policy password e dei metodi di login
- Gestione dei certificati
- Amministrazione di varie risorse di rete
- Migliori misure di sicurezza per la protezione dei dati
- Migliore scalabilità per la gestione di oggetti eDirectory di grandi dimensioni
- Login sicuro al portale di Identity Console tramite One SSO Provider (OSP)
- Basato sulle più recenti tecnologie di interfaccia utente del settore
- Facile da installare e configurare tramite container Docker

2 Come accedere a Identity Console?

È possibile accedere a Identity Console e all'insieme completo di funzioni che fornisce da qualsiasi browser Web supportato. Anche se si riuscisse ad accedere a Identity Console tramite un browser Web non elencato, non si garantisce né si supporta la piena funzionalità con browser non ufficialmente supportati.

Importante: Per informazioni sui browser Web supportati, vedere la *Guida di installazione di Identity Console*.

Accesso a Identity Console

Per accedere alla versione di Identity Console basata su server, eseguire le operazioni riportate di seguito:

1. Immettere quanto segue nel campo dell'indirizzo (URL) di un browser Web supportato.

   Login sicuro: `https://<indirizzo-ip-server/nomehost>:<porta>/identityconsole/`

   Negli esempi, l'indirizzo IP in *<indirizzo-ip-server>* deve essere IPv4. La porta di default da utilizzare è la 9000.
2. Eseguire il login utilizzando il DN utente e la password.
3. Specificare l'IP o il DNS dell'albero eDirectory con o senza porta sicura LDAP.

Nota

- L'aggiornamento di qualsiasi scheda in Identity Console comporta il logout dell'utente per motivi di sicurezza.
- L'apertura di schede duplicate di Identity Console nel browser comporta il logout dell'utente per motivi di sicurezza.
- Il DN deve essere specificato nel formato `cn=admin,ou=sa,o=system`.
- Se eDirectory è configurato con una porta non di default, è necessario specificare il numero di porta.

---

3 Utilizzo dell'interfaccia di Identity Console

In questa sezione viene illustrato come spostarsi nell'interfaccia Web di Identity Console.

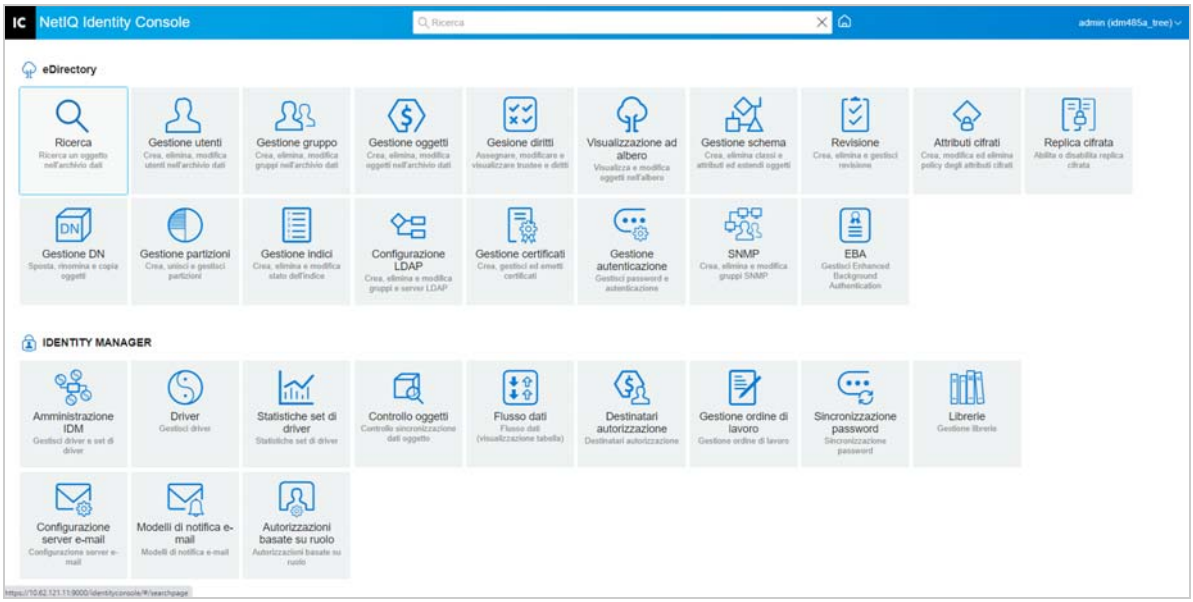
Ricerca (anteprima tecnologia)

La **Ricerca (Anteprima tecnologia)** fornisce un layout introduttivo per la funzionalità di ricerca. In questa anteprima è possibile specificare parole chiave e il campo di ricerca determina l'origine delle informazioni in cui eseguire la ricerca e la visualizzazione dei risultati corrispondenti. Tramite questa opzione è possibile cercare una risorsa e accedervi facilmente da qualsiasi pagina dell'applicazione Identity Console.

Interfaccia di Identity Console

L'interfaccia di Identity Console comprende i moduli eDirectory e Identity Manager.

Figura 3-1 *Interfaccia di Identity Console*



Importante: Diverse animazioni GIF utilizzate in questa guida funzionano solo con la documentazione online. Se si decide di passare al file PDF, verranno visualizzati solo gli screenshot.

Tabella 3-1 *Spiegazione dei vari moduli del portale Web di Identity Console*

Nome del modulo	Descrizione
Ricerca	Ricercare un oggetto nell'archivio dati. Per ulteriori informazioni, vedere Capitolo 4, “Esecuzione di ricerche”, a pagina 23.
Gestione utenti	Creare, eliminare e modificare utenti nell'archivio dati. Per ulteriori informazioni, vedere Capitolo 5, “Gestione degli utenti”, a pagina 27.
Gestione gruppo	Creare, eliminare e modificare gruppi nell'archivio dati. Per ulteriori informazioni, vedere Capitolo 6, “Gestione dei gruppi”, a pagina 37.
Gestione oggetti	Creare, eliminare e modificare oggetti nell'archivio dati. Per ulteriori informazioni, vedere Capitolo 7, “Gestione degli oggetti”, a pagina 43.
Gestione diritti	Assegnare, modificare e visualizzare trustee e diritti. Per ulteriori informazioni, vedere Capitolo 8, “Gestione dei diritti”, a pagina 51.
Visualizzazione ad albero	Visualizzare e modificare gli oggetti nell'albero. Per ulteriori informazioni, vedere Capitolo 9, “Visualizzazione ad albero”, a pagina 55.
Gestione schema	Creare ed eliminare classi, classi ausiliarie, attributi ed estensione degli oggetti. Per ulteriori informazioni, vedere Capitolo 10, “Gestione dello schema”, a pagina 59.
Revisione	Abilitare, disabilitare e gestire la revisione CEF. Per ulteriori informazioni, vedere Capitolo 11, “Gestione degli eventi di revisione”, a pagina 67.
Attributi cifrati	Creare, modificare, eliminare e visualizzare la policy degli attributi cifrati. Per ulteriori informazioni, vedere Capitolo 12, “Gestione degli attributi cifrati”, a pagina 73.
Replica cifrata	Abilitare, disabilitare e visualizzare la replica cifrata. Per ulteriori informazioni, vedere Capitolo 13, “Gestione della replica cifrata”, a pagina 77.
Gestione DN	Spostare, rinominare e copiare oggetti. Per ulteriori informazioni, vedere Capitolo 7, “Gestione degli oggetti”, a pagina 43.
Gestione partizioni	Creare, unire e spostare partizioni e repliche. Per ulteriori informazioni, vedere Capitolo 14, “Gestione delle partizioni e delle repliche”, a pagina 79.
Gestione indici	Creare e modificare indici e modificarne lo stato. Per ulteriori informazioni, vedere Capitolo 15, “Gestione degli indici”, a pagina 83.

Nome del modulo	Descrizione
Configurazione LDAP	Creare, eliminare e modificare oggetti LDAP. Per ulteriori informazioni, vedere Capitolo 16, “Configurazione di oggetti LDAP”, a pagina 87.
Gestione dei certificati	Creare e gestire certificati server e certificati Autorità di certificazione. Per ulteriori informazioni, vedere Capitolo 17, “Gestione dei certificati”, a pagina 91.
Gestione autenticazione	Creare e gestire metodi e sequenze di login e post-login. Questo modulo consente inoltre di gestire le policy password e i set di autenticazione. Per ulteriori informazioni, vedere Capitolo 18, “Gestione del framework di autenticazione”, a pagina 109.
SNMP	Creare, eliminare e modificare gruppi SNMP. Per ulteriori informazioni, vedere Capitolo 19, “Gestione di oggetti gruppo SNMP”, a pagina 125.
EBA	Gestire l'Enhanced Background Authentication. Per ulteriori informazioni, vedere Capitolo 20, “Gestione di Enhanced Background Authentication”, a pagina 129.
Amministrazione IDM	Gestire driver e set di driver di Identity Manager. Per ulteriori informazioni, vedere Capitolo 21, “Gestione di driver e set di driver”, a pagina 133. Questo modulo consente inoltre di gestire le proprietà del set di driver. Per ulteriori informazioni, vedere Capitolo 22, “Gestione delle proprietà del set di driver”, a pagina 139.
Driver’s Properties (Proprietà del driver)	Gestire le proprietà dei vari driver. Per ulteriori informazioni, vedere Capitolo 23, “Gestione delle proprietà del driver”, a pagina 151.
Statistiche set di driver	Gestire e visualizzare le statistiche del set di driver. Per ulteriori informazioni, vedere Capitolo 24, “Gestione delle statistiche del set di driver”, a pagina 183.
Controllo oggetti	Gestire l'associazione degli oggetti e la sincronizzazione dei dati. Per ulteriori informazioni, vedere Capitolo 25, “Controllo degli oggetti di Identity Manager”, a pagina 185.
Flusso dati	Gestire e visualizzare il flusso di dati dei driver. Per ulteriori informazioni, vedere Capitolo 26, “Gestione del flusso di dati”, a pagina 187.
Destinatari autorizzazione	Gestire i destinatari dell'autorizzazione. Per ulteriori informazioni, vedere Capitolo 27, “Gestione dei destinatari dell'autorizzazione”, a pagina 189.
Gestione ordine di lavoro	Gestire gli ordini di lavoro. Per ulteriori informazioni, vedere Capitolo 28, “Gestione degli ordini di lavoro”, a pagina 191.

Nome del modulo	Descrizione
Sincronizzazione password	Gestire la sincronizzazione e lo stato delle password. Per ulteriori informazioni, vedere Capitolo 29, “Gestione dello stato e della sincronizzazione delle password”, a pagina 195.
Gestione librerie	Gestire le librerie. Per ulteriori informazioni, vedere Capitolo 30, “Gestione delle librerie”, a pagina 199.
Configurazione server e-mail	Gestire le opzioni del server e-mail. Per ulteriori informazioni, vedere Capitolo 31, “Gestione delle opzioni del server e-mail”, a pagina 201.
Modelli di notifica e-mail	Gestire i modelli e-mail. Per ulteriori informazioni, vedere Capitolo 32, “Gestione dei modelli e-mail”, a pagina 203.

Gestione di eDirectory tramite Identity Console

In questa sezione vengono descritti i vari task che è possibile eseguire per gestire i server eDirectory tramite il portale di Identity Console.

4 Esecuzione di ricerche

Il riquadro Ricerca consente di specificare un'operazione di ricerca da eseguire nell'albero della directory e ne visualizza i risultati. Questa opzione consente di eseguire la ricerca di vari oggetti, utenti, gruppi e molto altro. Per eseguire un'operazione di ricerca per diversi oggetti nell'archivio dati, eseguire le operazioni riportate di seguito:

1. Specificare il nome dell'oggetto per la ricerca. Per specificare un nome parziale, utilizzare il carattere jolly asterisco. Ad esempio: `ldap*`, `*cert`, `*server*`, ecc. Se si utilizza solo un asterisco in questo campo, Identity Console restituisce tutti i risultati di ricerca in base al **Tipo** e **Contesto** selezionato.

   Nota: mediante il Browser del contesto è possibile sfogliare l'intero albero eDirectory specificando un asterisco (*) nel campo di ricerca. È inoltre possibile filtrare gli oggetti nel Browser del contesto utilizzando la ricerca con caratteri jolly. Ad esempio, `admin*`. Questo comportamento del Browser del contesto è supportato da vari moduli in Identity Console.

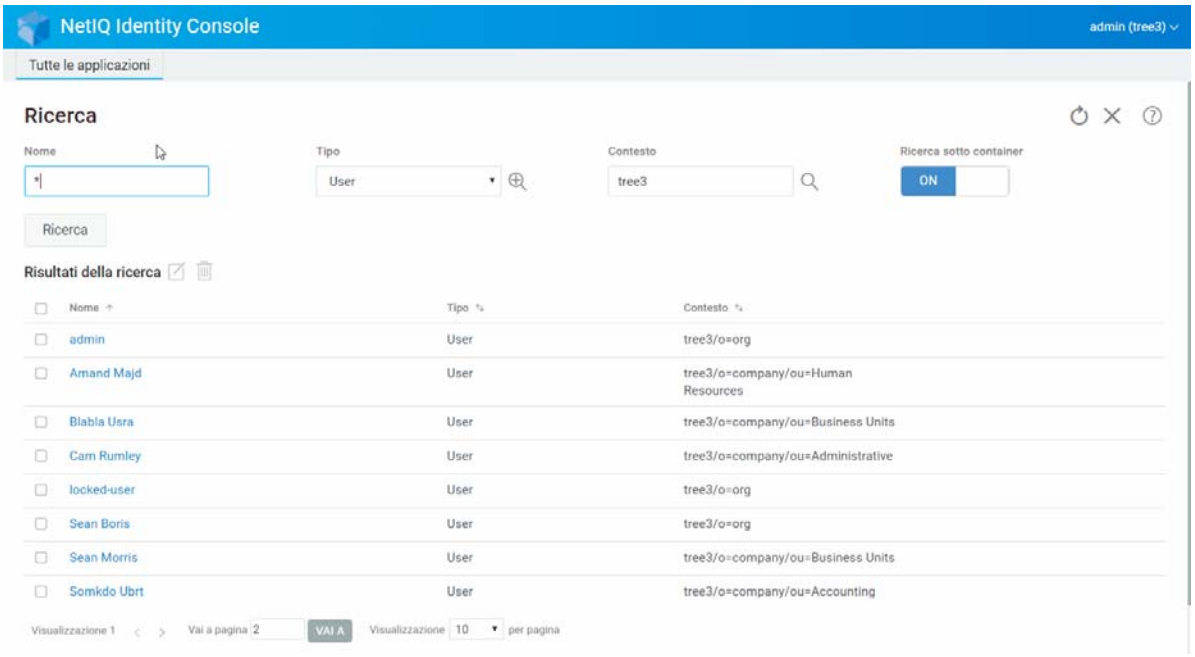
   ---

2. Selezionare il tipo di oggetto per la ricerca nel campo **Tipo**. In Identity Console vengono visualizzati solo gli oggetti del tipo specificato. Il tipo **Utente** in questo campo è selezionato per default.

   Fare clic sull'icona per definire altre impostazioni di ricerca a livello di attributo. Per ulteriori informazioni, vedere “Configurazione di ricerca avanzata” a pagina 24.

3. Specificare il container iniziale dell'operazione di ricerca nel campo **Contesto**.
4. Se si desidera che la ricerca includa container subordinati, selezionare **ATTIVO** per l'opzione Cerca container secondari.
5. Fare clic sul pulsante Ricerca.

Figura 4-1 *Esecuzione di un'operazione di ricerca*



Configurazione di ricerca avanzata

La Selezione avanzata include un ambiente più configurabile per la ricerca degli oggetti desiderati nella directory.

Tipo di oggetto: consente di specificare la classe di base dell'oggetto ricercato, ad esempio Utente.

Classi ausiliarie: Fare clic sull'icona + per specificare una Classe ausiliaria da includere nella ricerca.

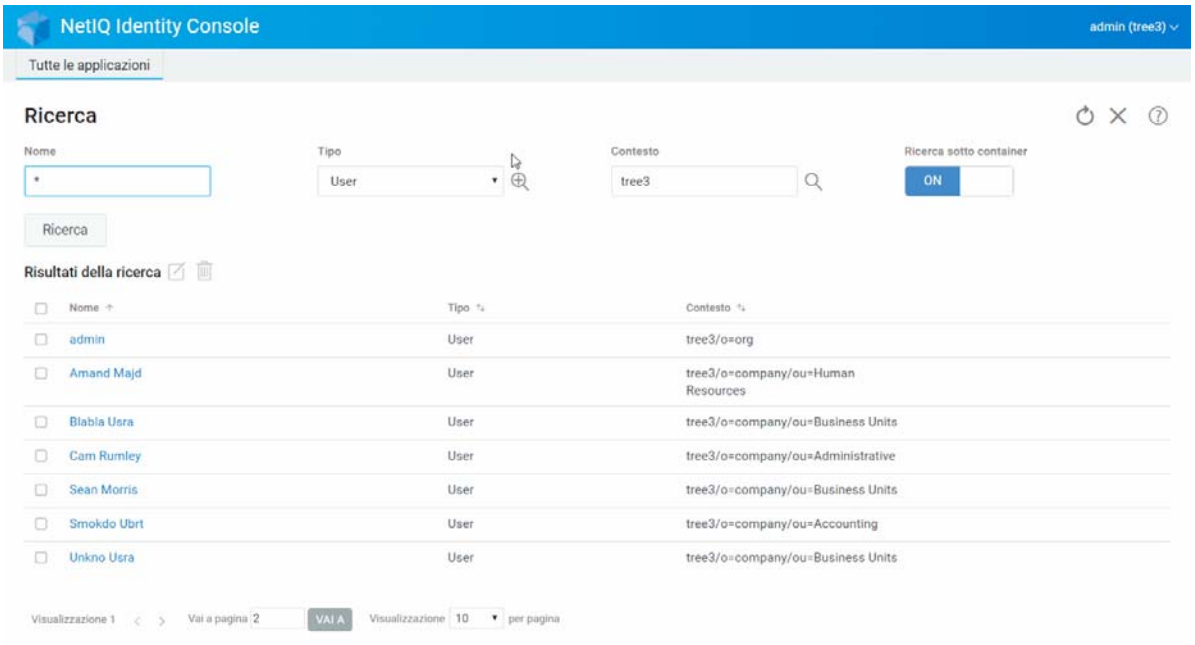
Attributo: consente di specificare un attributo (proprietà) che si desidera utilizzare come parte del filtro.

Operatore: consente di specificare l'operatore logico da applicare al filtro. Le opzioni disponibili includono.

Valore: consente di specificare il valore dell'attributo utilizzato come filtro. Per indicare parte di un valore, è possibile utilizzare l'asterisco (*) come carattere jolly, ad esempio ros*, *si e *oss*.

Inoltre, è possibile concatenare più filtri di attributo in un gruppo di filtri utilizzando l'icona + Rule per aggiungere un secondo attributo all'elenco. Quando si utilizzano più filtri di attributo, collegarli con l'operatore logico OR o AND.

Figura 4-2 *Configurazione di ricerca avanzata*



5 Gestione degli utenti

La gestione degli utenti e del loro accesso alla rete è uno scopo centrale dell'archivio dati. Tramite il portale Web di Identity Console è possibile eseguire i seguenti task relativi all'utente:

Creazione di un utente

Per creare un nuovo oggetto Utente:

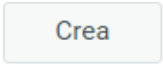
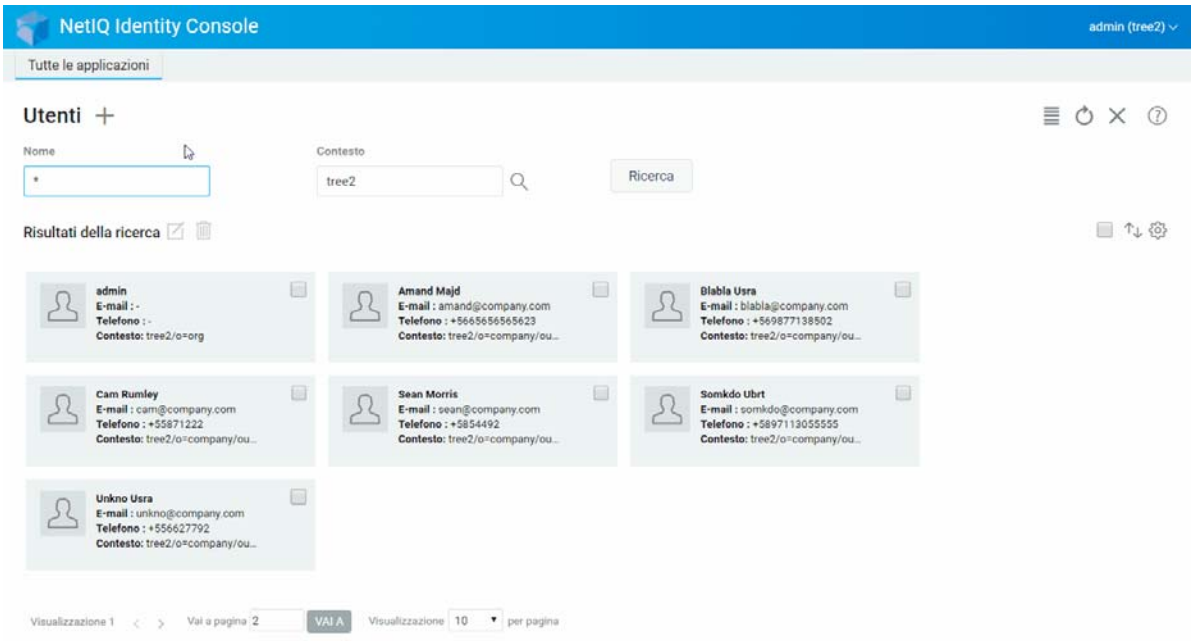
1. Fare clic sull'opzione **Gestione utenti** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona  .
3. Nella pagina Crea utente, fornire quantomeno le informazioni relative all'utente richieste, quindi fare clic sul pulsante  .
   - **Nome utente**
   - **Contesto**
   - **Cognome**
   - **Password**
4. Verrà visualizzato un messaggio di conferma che indica che l'oggetto utente è stato creato.

Figura 5-1 *Creazione di utenti*

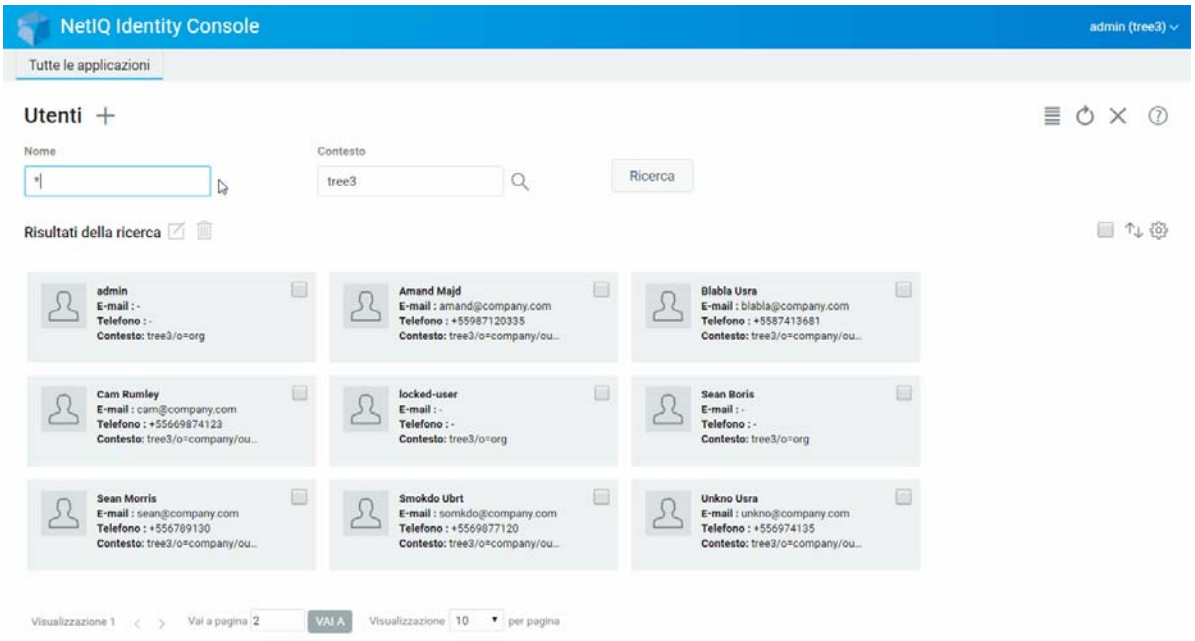


Eliminazione di un utente

Per cancellare un oggetto Utente:

1. Fare clic sull'opzione **Gestione utenti** nella pagina di destinazione di Identity Console.
2. Digitare il nome e il contesto dell'oggetto o utilizzare la funzione di ricerca per trovarlo, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'oggetto Utente dall'elenco di utenti e fare clic sull'icona 🗑.
4. Verrà visualizzato un messaggio di conferma che indica che l'oggetto utente è stato eliminato.

Figura 5-2 *Eliminazione di un utente*

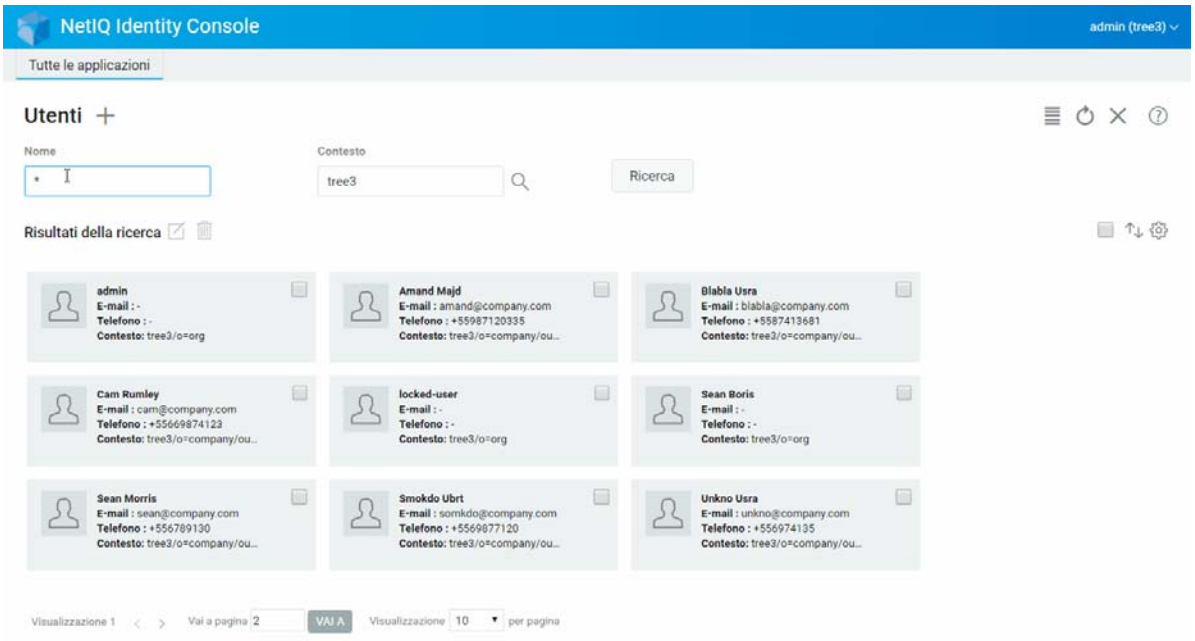


Modifica di utenti

Per modificare un oggetto utente:

1. Fare clic sull'opzione **Gestione utenti** nella pagina di destinazione di Identity Console.
2. Digitare il nome e il contesto dell'oggetto o utilizzare la funzione di ricerca per trovarlo, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'oggetto utente dall'elenco utenti e fare clic sull'icona .
4. Apportare le modifiche, quindi fare clic sul pulsante Salva.
5. Verrà visualizzato un messaggio di conferma che indica che l'oggetto utente è stato modificato.

Figura 5-3 *Modifica di un utente*

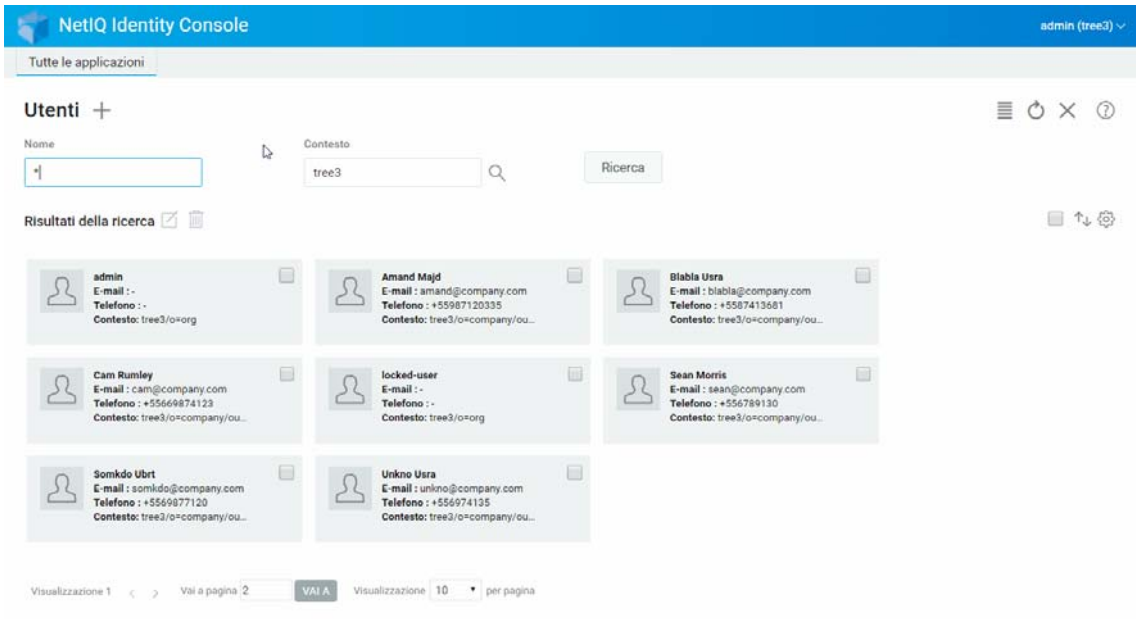


Ricerca di un utente

Per ricercare un oggetto utente:

1. Fare clic sull'opzione **Gestione utenti** nella pagina di destinazione di Identity Console.
2. È possibile eseguire la ricerca di un utente in base al nome o in base al nome e al contesto. Una volta specificate le informazioni necessarie, fare clic sull'icona Ricerca.

Figura 5-4 *Ricerca di un utente*

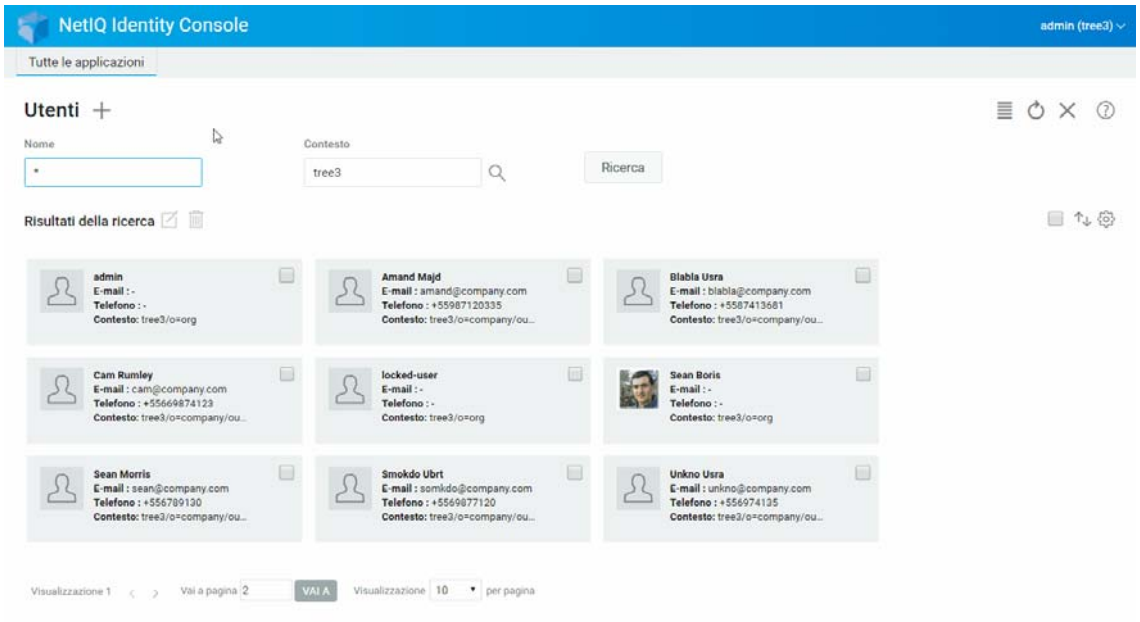


Impostazioni di restrizioni della password

Le restrizioni della password consentono di effettuare le seguenti operazioni:

- Consentono agli utenti di modificare le rispettive password
- Applicano una password per il login
- Specificano la sicurezza della password
- Applicano una modifica periodica della password
- Specificano la data di scadenza della password
- Applicano la creazione di una password univoca
- Specificano il periodo di login extra in caso di scadenza della password

Figura 5-5 *Restrizioni password*

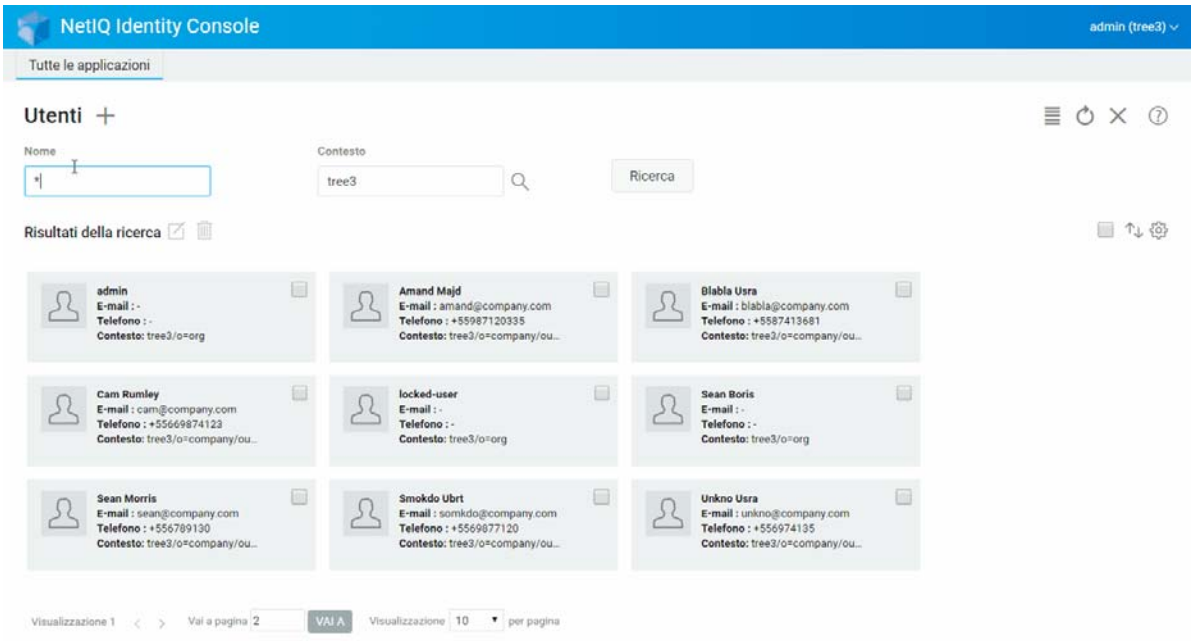


Disabilitazione e abilitazione di un account utente

Per disabilitare un account utente, eseguire le operazioni riportate di seguito:

1. Selezionare l'utente di cui deve essere disabilitato l'account e fare clic sull'icona .
2. Fare clic sulla scheda **Restrizioni** nella pagina **Modifica utente**.
3. Espandere la scheda **Restrizioni di login** e selezionare la casella di controllo **Account disattivato**.
4. Fare clic sull'icona Salva.
5. A questo punto, l'account utente è disabilitato. Per abilitare un account utente disabilitato, deselezionare la casella di controllo **Account disattivato**.

Figura 5-6 *Disabilitazione e abilitazione di un account utente*

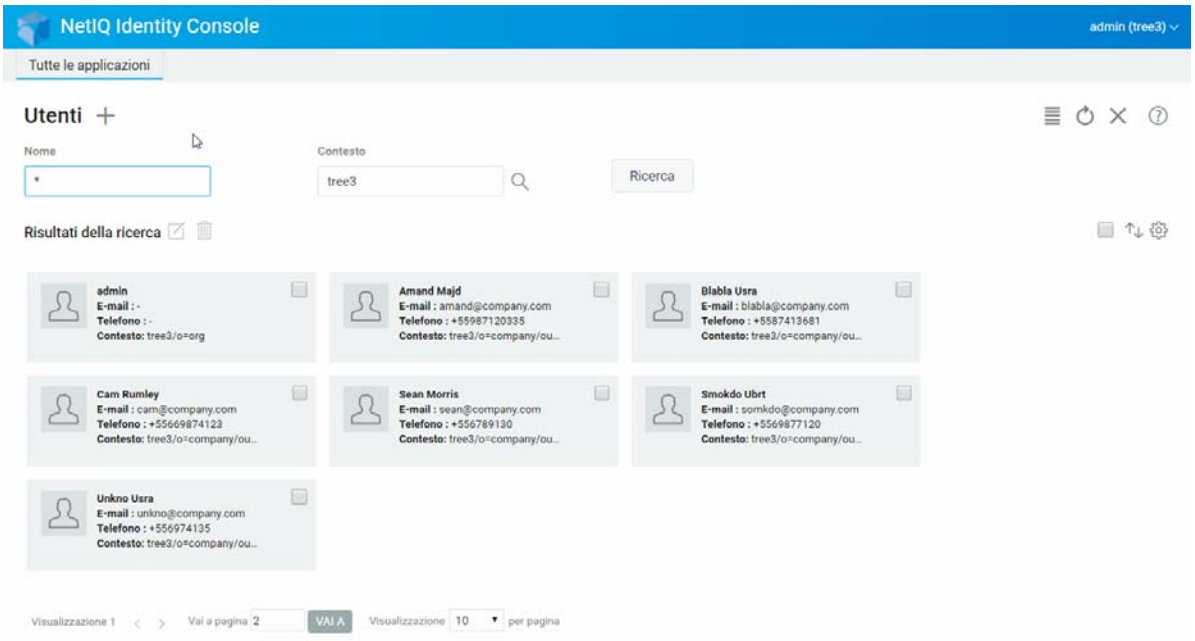


Impostazione di data di scadenza dell'account

Per impostare la data di scadenza dell'account utente, eseguire i passaggi seguenti:

1. Selezionare l'utente per il quale è necessario impostare la data di scadenza dell'account e fare clic sull'icona .
2. Fare clic sulla scheda **Restrizioni** nella pagina **Modifica utente**.
3. Espandere la scheda **Restrizioni di login**, selezionare la casella di controllo **Account con data di scadenza** e specificare la **Data di scadenza**.
4. Fare clic sull'icona Salva.

Figura 5-7 *Impostazione di data di scadenza dell'account*

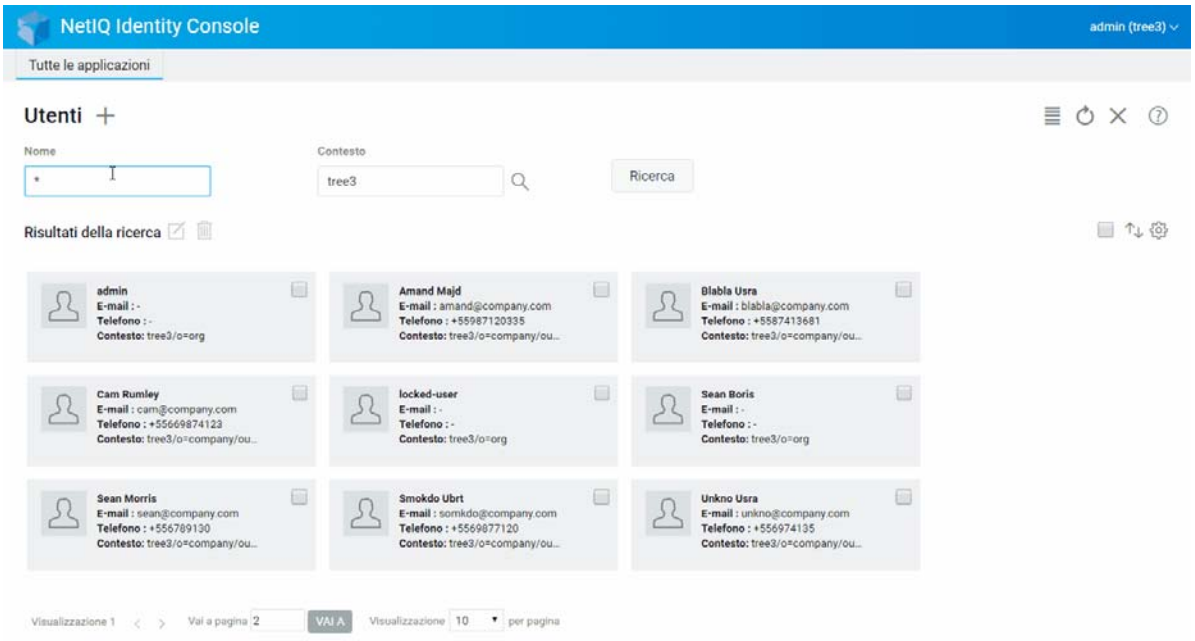


Verifica e eliminazione del blocco degli intrusi

È possibile visualizzare i dettagli del blocco degli intrusi per tutti gli account utente mediante il portale Web di Identity Console. Per visualizzare i dettagli del blocco degli intrusi:

1. Selezionare l'utente per il quale è necessario controllare i dettagli del blocco degli intrusi e fare clic sull'icona .
2. Fare clic sulla scheda **Restrizioni** nella pagina **Modifica utente**.
3. Espandere la scheda **Blocco degli intrusi** e visualizzare i dettagli del blocco degli intrusi.
4. A questo punto, selezionare la scheda **Annulla blocco** e fare clic sul pulsante Annulla bloccaggio.
5. Fare clic sul pulsante Salva.

Figura 5-8 *Verifica e eliminazione del blocco degli intrusi*



6 Gestione dei gruppi

I gruppi di solito contengono un certo numero di membri. Se un utente crea un gruppo, ne diventa automaticamente proprietario. È possibile eseguire le operazioni riportate di seguito mediante la funzione Gestione gruppi:

Per ulteriori informazioni sull'utilizzo e la configurazione degli oggetti Gruppo, vedere la *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guida all'amministrazione di NetIQ eDirectory 9.0).

Creazione di un gruppo

Per creare un gruppo:

1. Fare clic sull'opzione **Gestione gruppi** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea gruppo, immettere i seguenti dettagli:
   - Specificare il nome del gruppo
   - Specificare il contesto

   Selezionare **Gruppo dinamico** per impostare il nuovo gruppo come dinamico, appartenente alla classe `dynamicGroup`. In caso contrario, il gruppo viene creato come gruppo statico.

   Selezionare **Gruppi nidificati** per rendere il nuovo gruppo nidificato, in modo tale che venga creato con la classe ausiliaria `nestedGroupAux`.

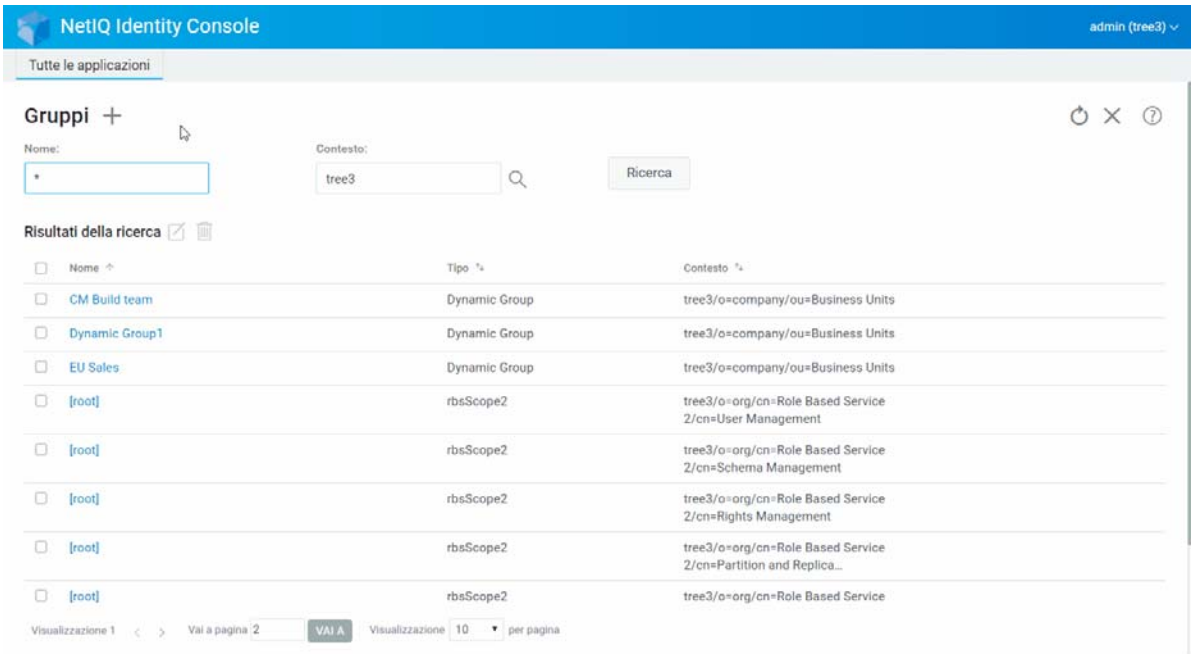
   Nota: È possibile convertire un gruppo statico in un gruppo dinamico o un gruppo annidato utilizzando la procedura menzionata in Modifica degli oggetti. In questo modo l'oggetto gruppo selezionato verrà esteso rispettivamente alla classe `dynamicGroupAux` o `nestedGroupAux`.

   Un gruppo può essere nidificato o dinamico. Non è possibile creare un gruppo che sia contemporaneamente nidificato e dinamico.

   ---

4. Una volta specificate le informazioni necessarie, fare clic sul pulsante Crea.
5. Viene visualizzato un messaggio di conferma che indica che il gruppo è stato creato.

Figura 6-1 *Creazione di un gruppo*

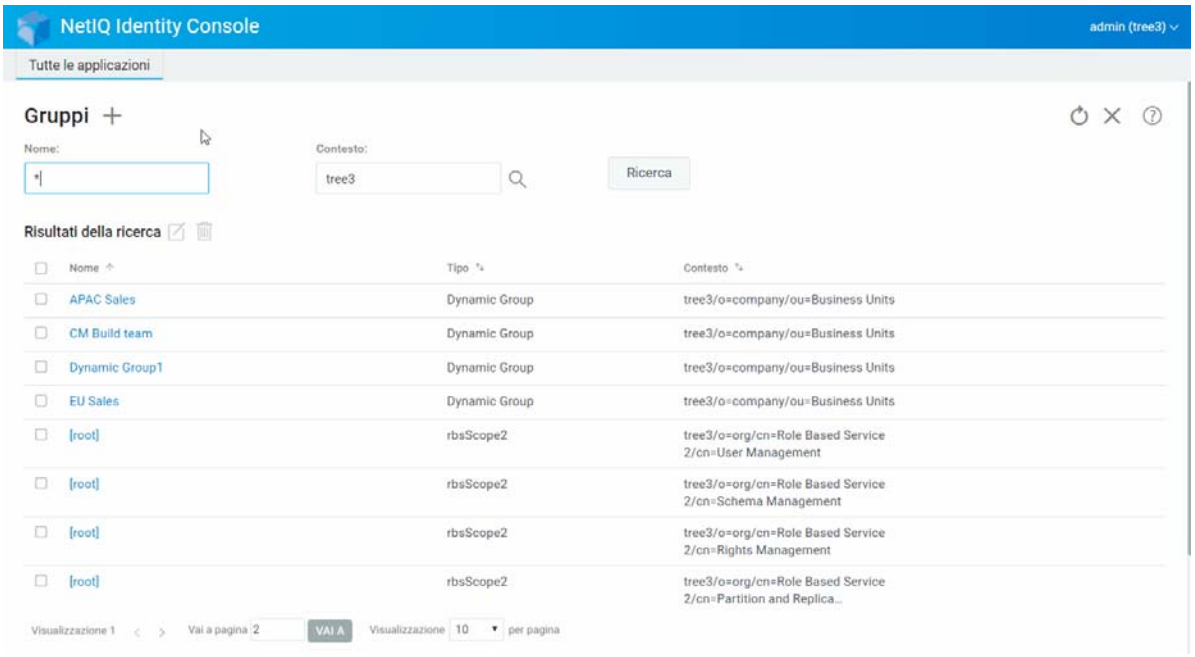


Eliminazione di gruppi

Per eliminare i gruppi:

1. Fare clic sull'opzione **Gestione gruppi** nella pagina di destinazione di Identity Console.
2. Specificare il nome e il contesto del gruppo o utilizzare la funzione di ricerca per trovarlo, quindi fare clic sul pulsante Ricerca.
3. Selezionare il gruppo da eliminare, quindi fare clic sull'icona 🗑.
4. Viene visualizzato un messaggio di conferma che indica che il gruppo è stato eliminato.

Figura 6-2 *Eliminazione di gruppi*

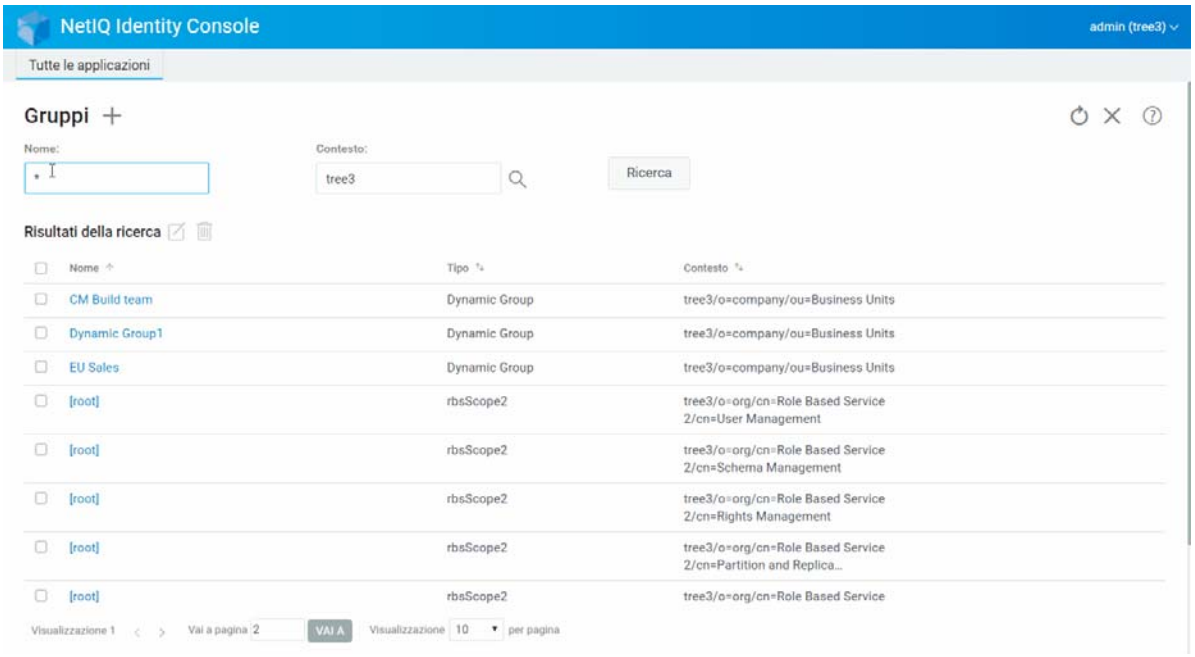


Modifica dei gruppi

Per modificare i gruppi:

1. Fare clic sull'opzione **Gestione gruppi** nella pagina di destinazione di Identity Console.
2. Digitare il nome e il contesto del gruppo, quindi fare clic sul pulsante Ricerca.
3. Selezionare il gruppo da modificare, quindi fare clic sull'icona .
4. Apportare le modifiche, quindi fare clic sul pulsante Salva.
5. Viene visualizzato un messaggio di conferma che indica che il gruppo è stato modificato.

Figura 6-3 *Modifica dei gruppi*

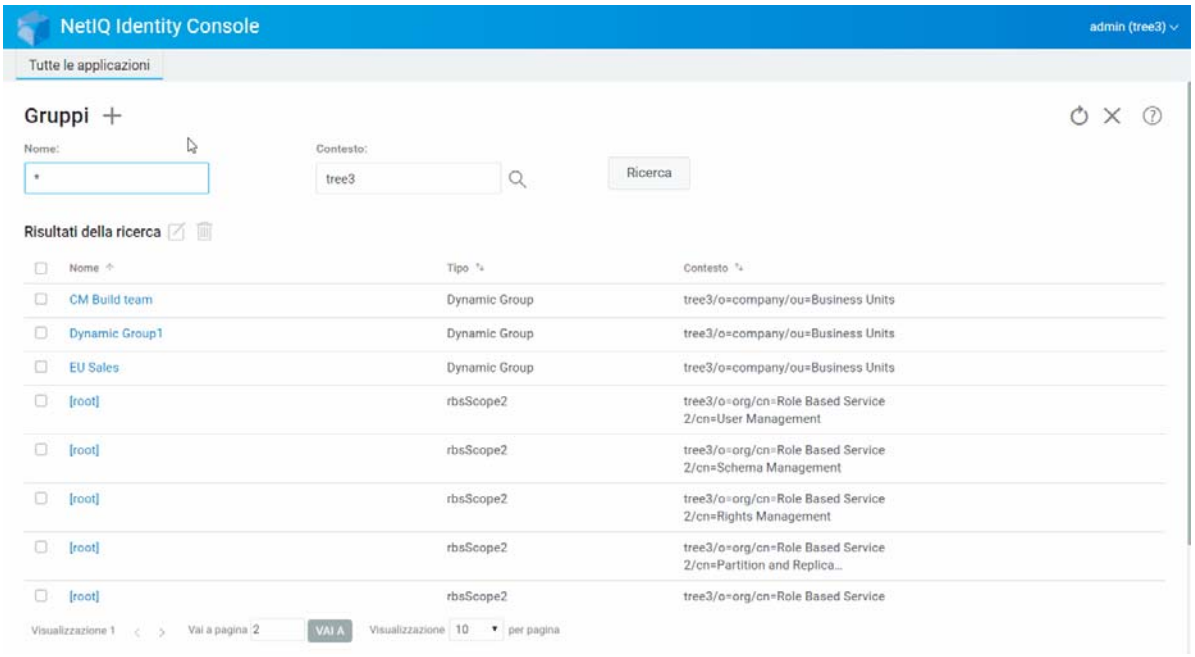


Aggiunta o modifica di membri del gruppo

Per aggiungere o modificare i membri del gruppo:

1. Fare clic sull'opzione **Gestione gruppi** nella pagina di destinazione di Identity Console.
2. Digitare il nome e il contesto del gruppo, quindi fare clic sul pulsante Ricerca.
3. Selezionare il gruppo e fare clic sull'icona .
4. Fare clic sulla scheda **Membri** nella pagina **Modifica gruppo**.
5. Utilizzare l'icona per aggiungere un nuovo membro al gruppo. Se si decide di rimuovere i membri del gruppo, fare clic sull'icona .
6. Una volta apportate le modifiche, fare clic sul pulsante Salva.
7. Viene visualizzato un messaggio di conferma che indica che il gruppo è stato modificato.

Figura 6-4 *Aggiunta o modifica di membri del gruppo*

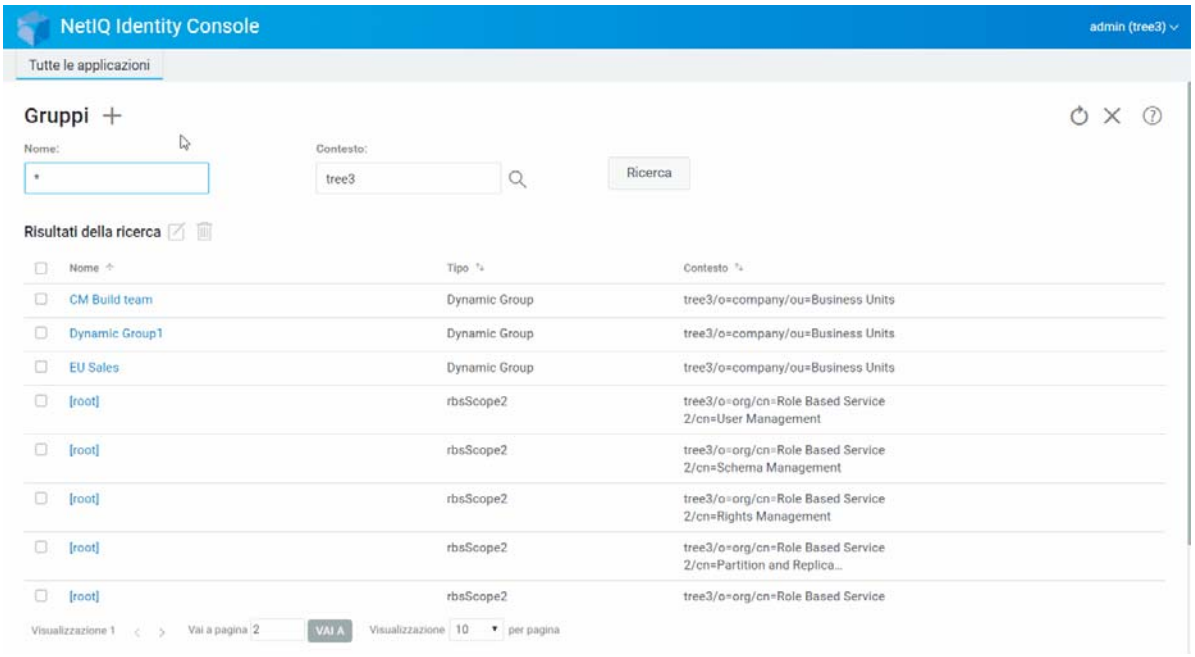


Ricerca dei gruppi

Per ricercare i gruppi:

1. Fare clic sull'opzione **Gestione gruppi** nella pagina di destinazione di Identity Console.
2. È possibile eseguire la ricerca di un gruppo in base al nome o in base al nome e al contesto.
3. Una volta specificati i dettagli richiesti, fare clic sull'icona Ricerca.

Figura 6-5 *Ricerca dei gruppi*



7 Gestione degli oggetti

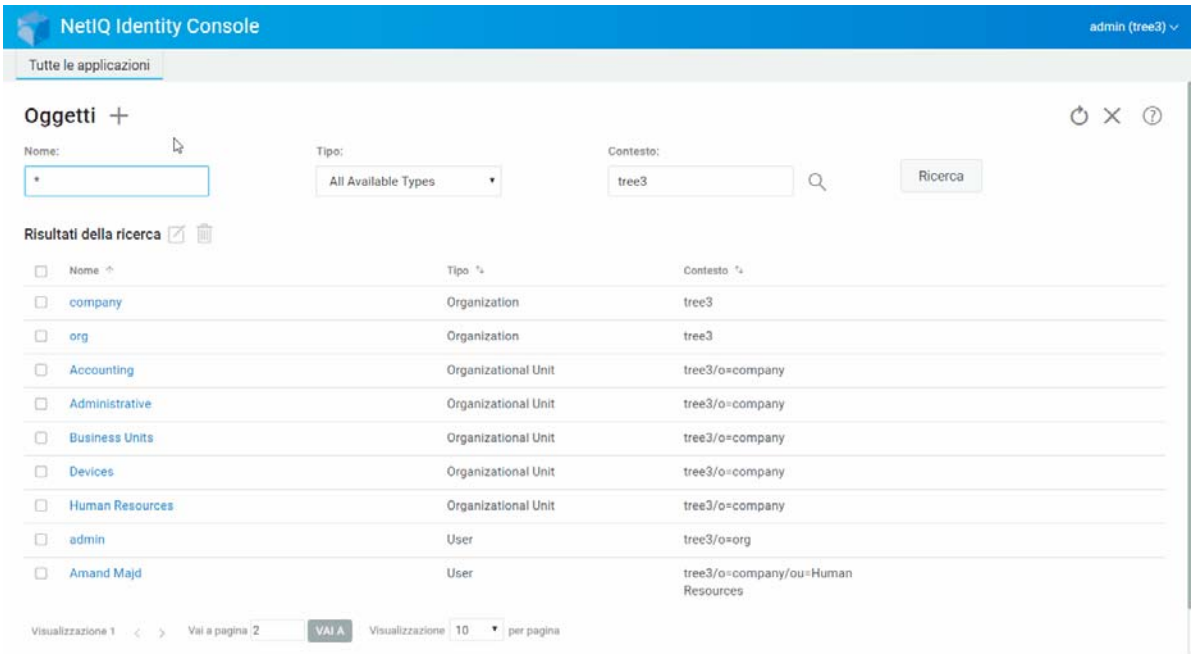
Identity Console consente di gestire diversi oggetti dell'archivio dati. L'utilizzo di questo modulo consente di creare, modificare, eliminare e ricercare gli oggetti.

Creazione di un oggetto

Per creare un nuovo oggetto:

1. Fare clic sull'opzione **Gestione oggetti** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea oggetto, inserire i seguenti dettagli:
   - Specificare il nome di un oggetto
   - Specificare il tipo
   - Specificare il contesto
4. Una volta immessi tutti i dettagli necessari, fare clic su **Avanti** > **Crea**.
5. Verrà visualizzato un messaggio di conferma che indica che l'oggetto è stato creato.

Figura 7-1 *Creazione di un oggetto*

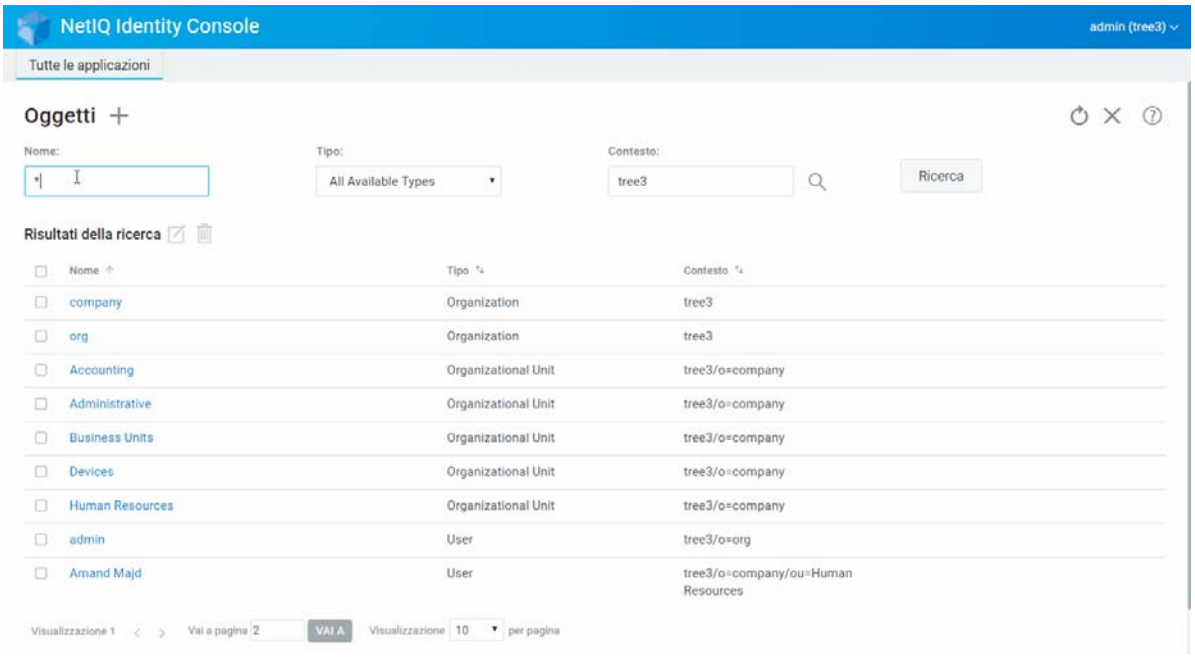


Eliminazione di oggetti

Per eliminare gli oggetti:

1. Fare clic sull'opzione **Gestione oggetti** nella pagina di destinazione di Identity Console.
2. Specificare il nome, il tipo e il contesto dell'oggetto o utilizzare la funzione di ricerca per trovarlo, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'oggetto dall'elenco di ricerca e fare clic sull'icona .
4. Verrà visualizzato un messaggio di conferma che indica che l'oggetto è stato eliminato.

Figura 7-2 *Eliminazione di oggetti*

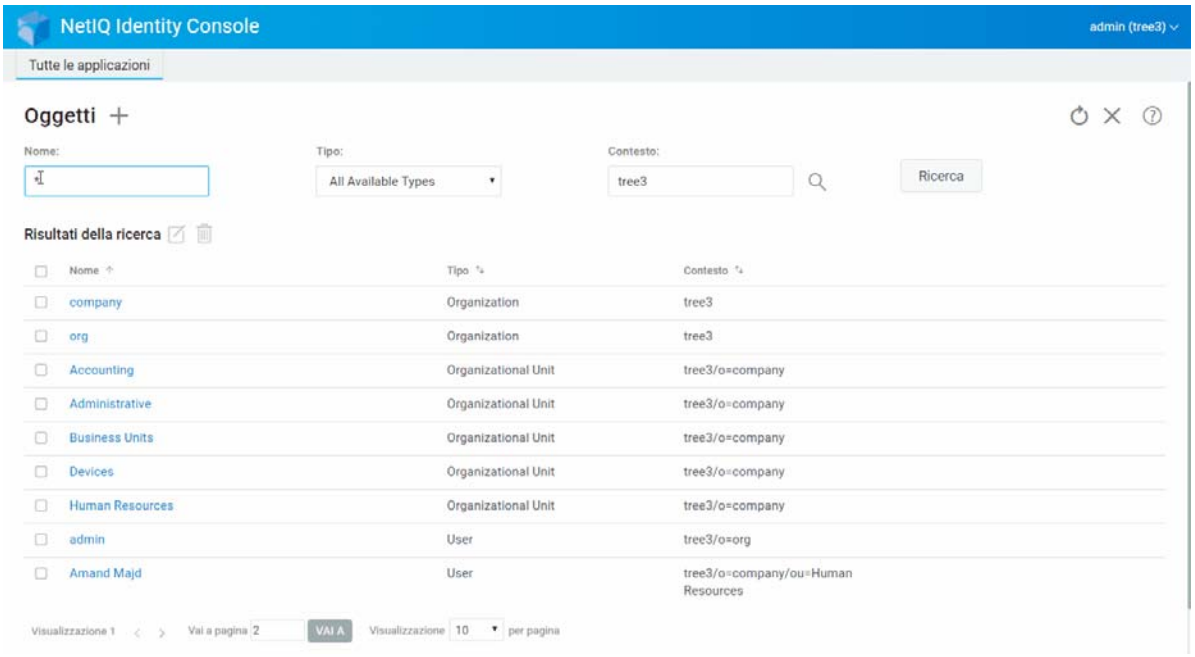


Modifica degli oggetti

Per modificare gli oggetti:

1. Fare clic sull'opzione **Gestione oggetti** nella pagina di destinazione di Identity Console.
2. Digitare il nome, il tipo e il contesto dell'oggetto, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'oggetto dall'elenco di ricerca e fare clic sull'icona .
4. Apportare le modifiche, quindi fare clic sul pulsante Salva.
5. Verrà visualizzato un messaggio di conferma che indica che l'oggetto è stato modificato.

Figura 7-3 *Modifica degli oggetti*

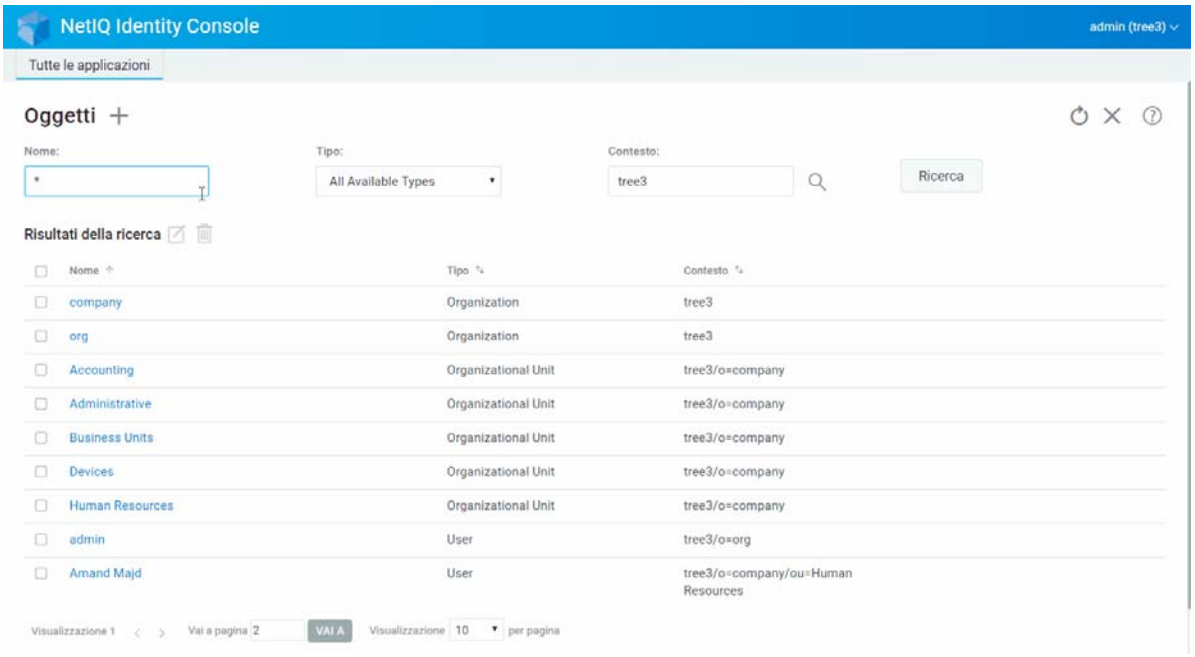


Ricerca di un oggetto

Per ricercare un oggetto:

1. Fare clic sull'opzione **Gestione oggetti** nella pagina di destinazione di Identity Console.
2. È possibile ricercare un oggetto in base al nome o in base al nome, tipo e contesto.
3. Una volta specificate le informazioni necessarie, fare clic sul pulsante Ricerca.

Figura 7-4 *Ricerca di un oggetto*



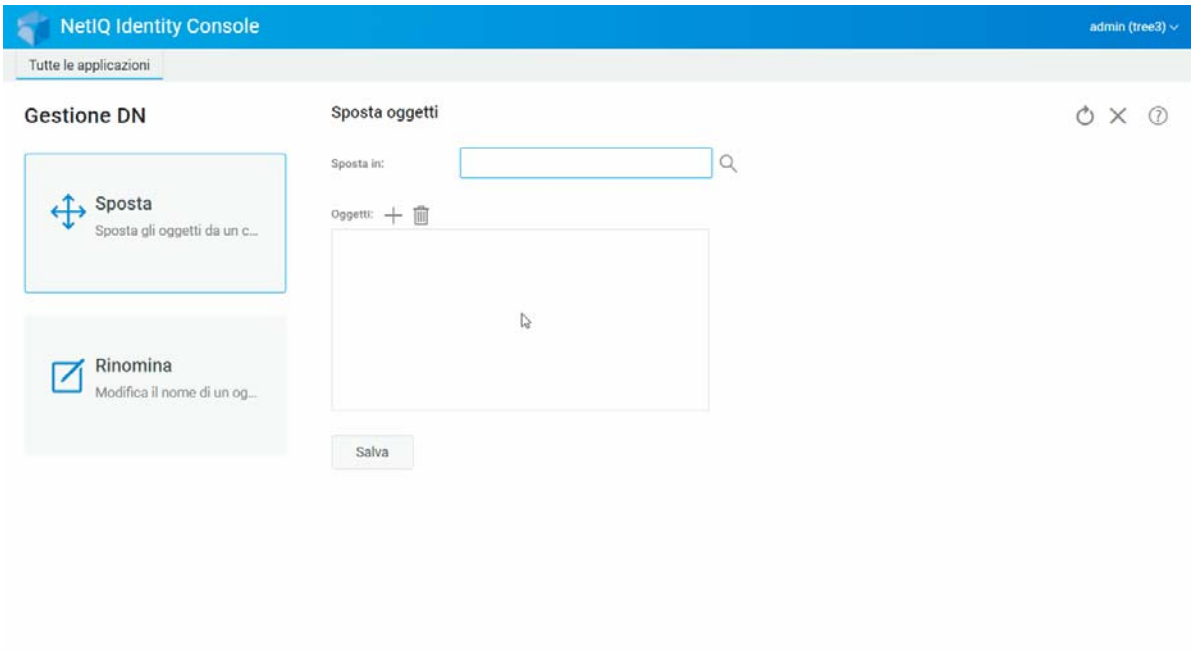
Spostamento di un oggetto

Per spostare un oggetto:

1. Fare clic sull'opzione **Gestione DN** nella pagina di destinazione di Identity Console.
2. L'opzione **Sposta oggetto** viene selezionata per default.
3. Nel campo **Sposta in**, selezionare il container in cui si desidera spostare l'oggetto.
4. Fare clic sull'icona + per aggiungere l'oggetto che si desidera spostare in un altro container.

   Se si desidera rimuovere un oggetto selezionato, fare clic sull'icona .
5. Fare clic sul pulsante Salva.
6. Verrà visualizzato un messaggio di conferma che indica che l'oggetto è stato spostato.

Figura 7-5 *Spostamento di un oggetto*

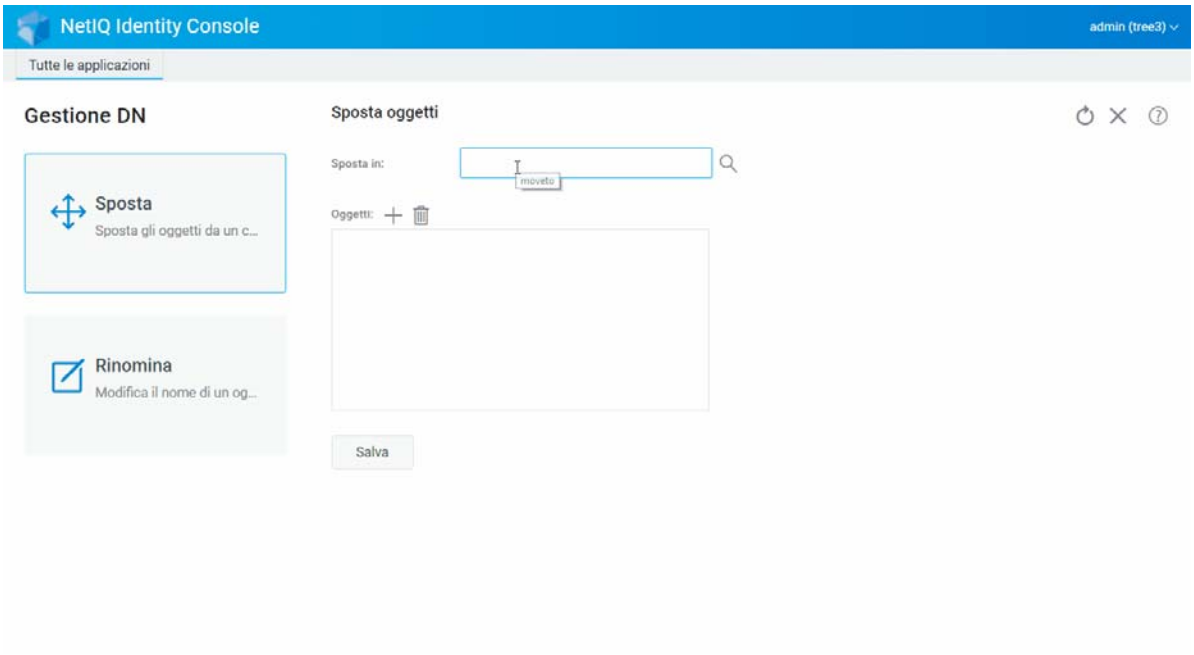


Ridenominazione di un oggetto

Per rinominare un oggetto:

1. Fare clic sull'opzione **Gestione DN** nella pagina di destinazione di Identity Console.
2. Selezionare l'opzione **Rinomina oggetto**.
3. Utilizzare la funzione di ricerca per individuare l'oggetto da rinominare nel campo **Nome oggetto**.
4. Specificare solo il nuovo nome dell'oggetto nel campo **Nuovo nome**. Non specificare il contesto.
5. Selezionare l'opzione per salvare il nome precedente, se lo si desidera.
6. Fare clic sul pulsante Salva.
7. Verrà visualizzato un messaggio di conferma che indica che l'operazione di rinomina dell'oggetto è riuscita.

Figura 7-6 *Ridenominazione di un oggetto*



8 Gestione dei diritti

Per diritti s'intendono i diritti di trustee e i trustee di eDirectory. Quando si crea un albero, le assegnazioni dei diritti default forniscono alla rete una sicurezza e un accesso generalizzato. Identity Console consente di eseguire le seguenti operazioni relative ai diritti:

- “Modifica del Filtro diritti ereditati” a pagina 51
- “Modifica dei diritti dei trustee” a pagina 52
- “Visualizzazione dei diritti effettivi” a pagina 53

Per ulteriori informazioni sui diritti di eDirectory, vedere la *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guida all'amministrazione di NetIQ eDirectory 9.0).

Modifica del Filtro diritti ereditati

In eDirectory è disponibile un meccanismo di Filtro diritti ereditati (IRF) per bloccare l'ereditarietà dei diritti sui singoli elementi subordinati.

Per ulteriori informazioni sui Filtri dei diritti ereditati, vedere la *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Guida all'amministrazione di NetIQ eDirectory 9.0).

1. Fare clic sull'opzione **Gestione diritti** nella pagina di destinazione di Identity Console.
2. Selezionare **Filtro diritti ereditati**.

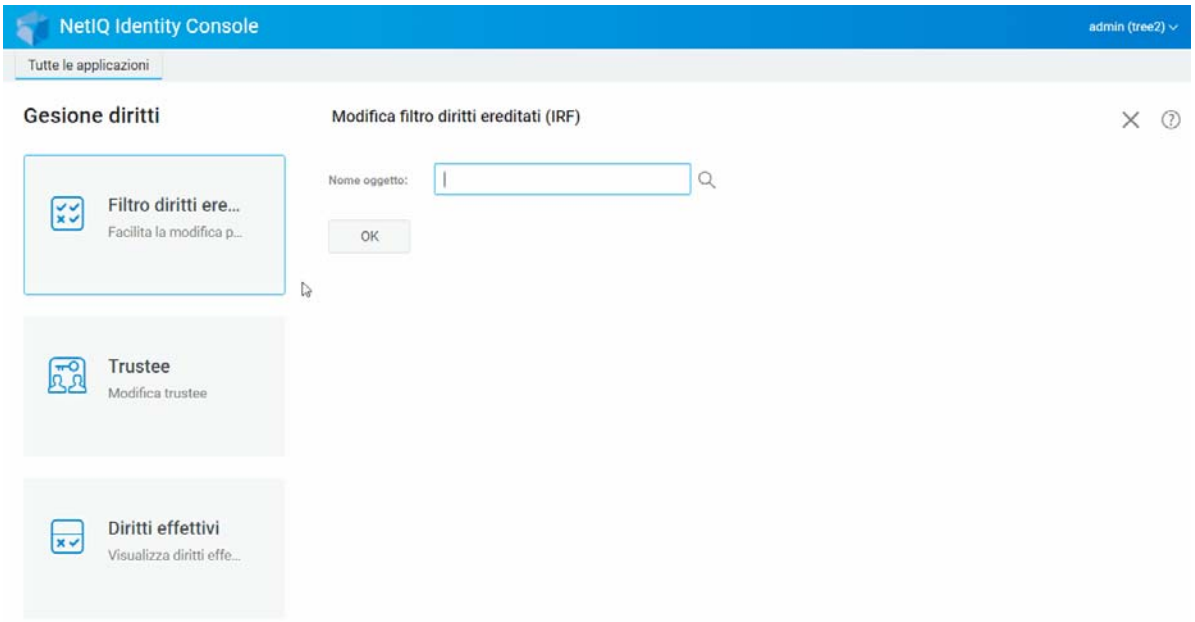
   Nota: Il Filtro diritti ereditati è selezionato di default.

3. Specificare il nome completo dell'oggetto di cui si desidera modificare il filtro dei diritti ereditati, oppure utilizzare l'icona Selettore Oggetti per trovarlo, quindi fare clic su **OK**.

   Verrà visualizzato un elenco dei filtri dei diritti ereditati già impostati per l'oggetto.
4. In **Proprietà**, modificare l'elenco dei filtri dei diritti ereditati in base alle esigenze, quindi fare clic su **Applica**.

   Per modificare l'elenco di filtri, è necessario disporre del diritto di supervisore o Controllo dell'accesso sulla proprietà ACL dell'oggetto. È possibile impostare filtri che bloccano i diritti ereditati per l’intero oggetto, per tutte le proprietà dell’oggetto e per singole proprietà.

Figura 8-1 *Modifica del Filtro diritti ereditati*



Modifica dei diritti dei trustee

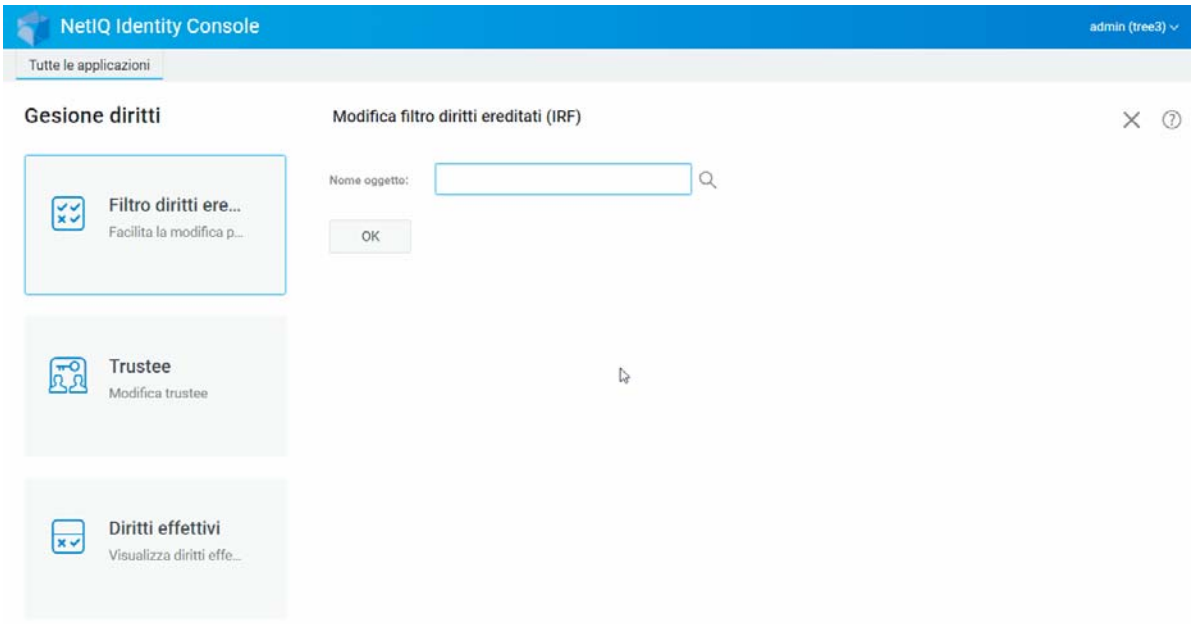
Un trustee è un oggetto a cui sono stati concessi diritti espliciti a un altro oggetto nell'albero della Directory. Per modificare un elenco di trustee per un oggetto specifico:

1. Fare clic sull'opzione **Gestione diritti** nella pagina di destinazione di Identity Console.
2. Selezionare **Trustee**.
3. Specificare il nome dell'oggetto di cui si desidera visualizzare l'elenco dei trustee o usare l'icona Selettore Oggetti per trovarlo, quindi fare clic su **OK**.

   Verrà visualizzato un elenco dei trustee dell'oggetto attualmente assegnati.
4. Modificare l'elenco di trustee in base alle esigenze, quindi fare clic su **OK**.

   - Per aggiungere un trustee, fare clic sull'icona .
   - Per rimuovere un trustee, selezionare la relativa casella di controllo e fare clic sull'icona .
   - Per modificare un'assegnazione di diritti di un trustee, selezionare il collegamento **Diritti assegnati** corrispondente.

Figura 8-2 *Modifica dei diritti dei trustee*



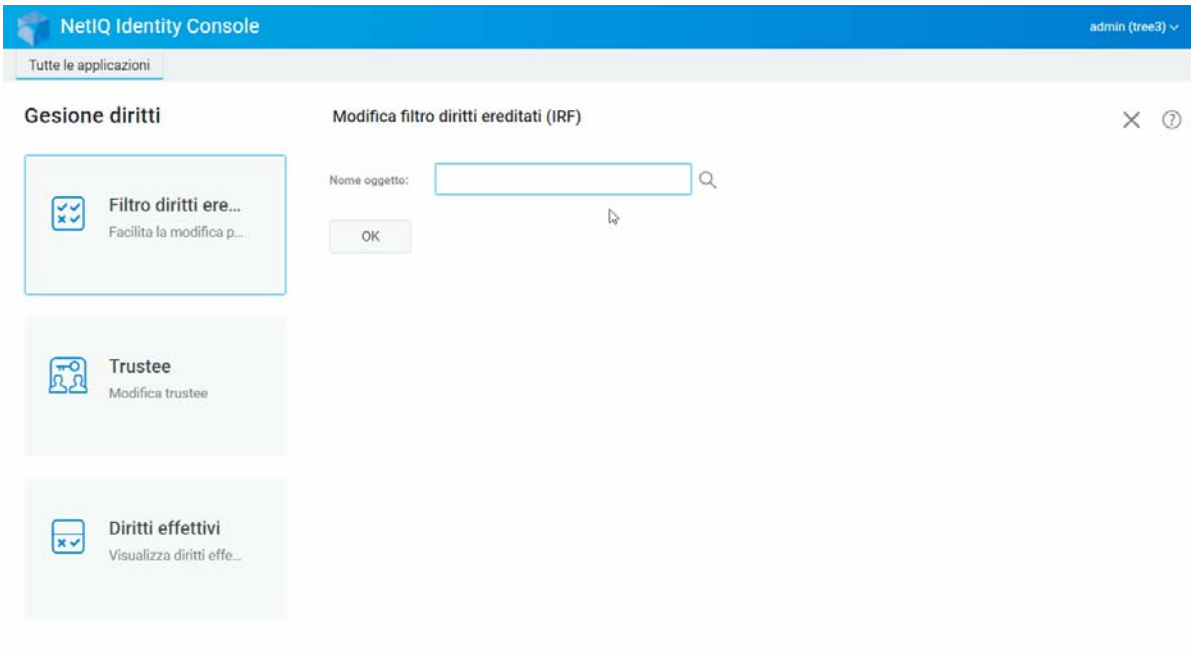
Visualizzazione dei diritti effettivi

I diritti effettivi sono una combinazione di diritti espliciti ed ereditati di cui dispone un oggetto in un punto qualsiasi dell'albero della directory. Per visualizzare i diritti effettivi di un oggetto su un altro oggetto:

1. Fare clic sull'opzione **Gestione diritti** nella pagina di destinazione di Identity Console.
2. Selezionare **Diritti effettivi**.
3. Specificare il nome del trustee di cui si desidera visualizzare i diritti o usare l'icona Selettore Oggetti per trovarlo, quindi fare clic su **OK**.
4. Nel campo del nome dell'oggetto, specificare il nome dell'oggetto per il quale si desidera visualizzare i diritti effettivi del trustee.

   In eDirectory verranno calcolati i diritti effettivi, i quali verranno visualizzati nel campo **Diritti effettivi**.

Figura 8-3 *Visualizzazione dei diritti effettivi*



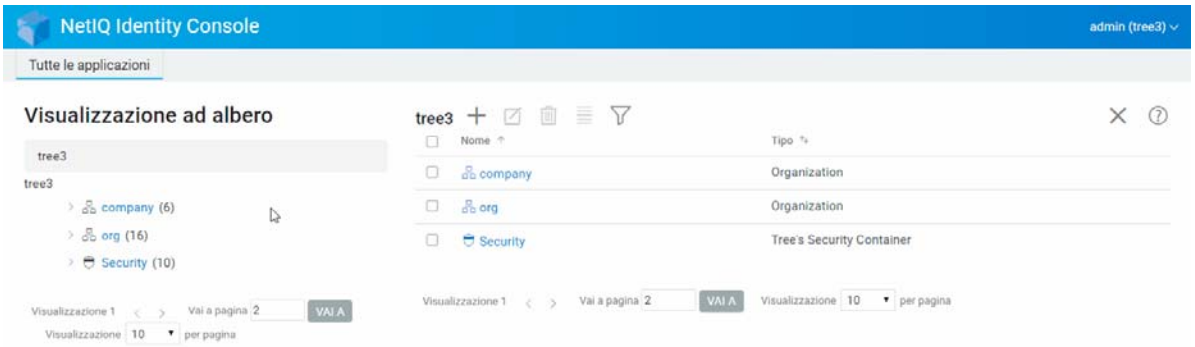
9 Visualizzazione ad albero

La visualizzazione ad albero consente di sfogliare un albero della directory e di creare, eliminare o modificare vari oggetti dell'albero. La visualizzazione ad albero presenta un frame di navigazione e un frame del contenuto.

Frame di navigazione della visualizzazione ad albero

Nella visualizzazione ad albero, il frame di navigazione visualizza la struttura della directory. Il frame di navigazione visualizza container, inclusi Volume (file system), oggetti e così via. Tutte le opzioni visualizzate nel frame di navigazione si possono cliccare per facilitare l'esplorazione della struttura delle directory. Per default, il frame di navigazione visualizza fino a 10 oggetti subordinati per ciascun container, tuttavia è possibile modificare questa impostazione al di sotto del pannello del frame di navigazione nella visualizzazione ad albero.

Figura 9-1 *Il frame di navigazione nella visualizzazione ad albero*



Frame di navigazione della vista albero

Selezionando uno degli oggetti container nel frame di navigazione, tutti gli oggetti di quel container verranno visualizzati dal frame del contenuto. Il frame del contenuto è il punto in cui è possibile visualizzare e modificare gli oggetti della directory. Il frame del contenuto include un'intestazione che contiene diverse azioni disponibili:

Barra del titolo: La barra del titolo del frame del contenuto indica il nome dell'oggetto Container attualmente selezionato.

Intestazione elenco oggetti: l'intestazione dell'elenco di oggetti fornisce l'accesso a quanto segue:

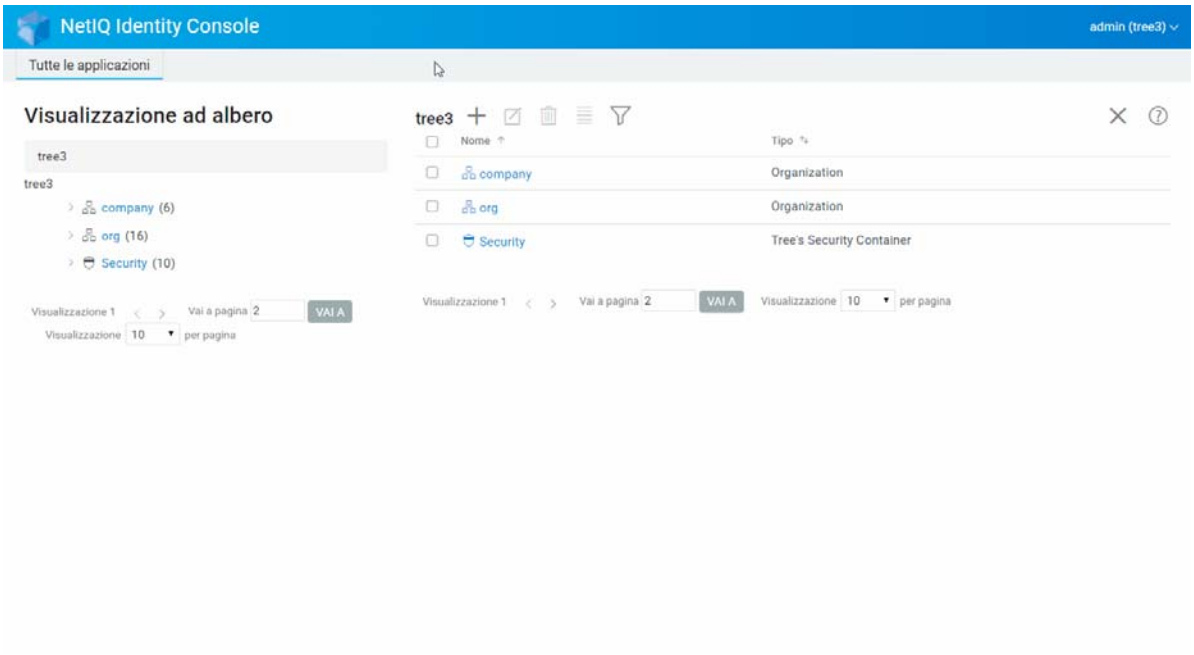
- **Aggiungi**: fare clic sull'icona per aggiungere un nuovo oggetto.
- **Modifica**: selezionare un oggetto e fare clic sull'icona per modificarlo. Viene aperto il registro delle proprietà dell'oggetto selezionato in modo da poterne modificare gli attributi. Non è possibile modificare più oggetti alla volta.
- **Elimina**: selezionare un oggetto e fare clic sull'icona per eliminare gli oggetti selezionati. È possibile eliminare più oggetti alla volta. Gli oggetti diversi da foglia non possono essere eliminati.
- **Azioni**: selezionare un oggetto e fare clic sull'icona che consente di aprire un menu a discesa con i task supportati per gli oggetti selezionati. Per eseguire un task, selezionarlo dal menu a discesa e fornire le informazioni richieste.
- **Totale di oggetti**: la visualizzazione ad albero visualizza l'elenco del numero di oggetti nella pagina attuale nella parte inferiore della pagina. Per default, il frame del contenuto visualizza fino a 20 oggetti subordinati per ciascun container, tuttavia è possibile modificare questa impostazione.
- **Seleziona tutto**: la casella di controllo nell'intestazione assume la funzione "seleziona tutto" per la pagina attuale degli oggetti.
- **Ordina**: entrambe le colonne **Nome** e **Tipo** si possono ordinare. Fare clic su una di esse per selezionare l'ordinamento alfabetico crescente o decrescente degli oggetti.
- **Filtro di ricerca**: fare clic su . per aprire la finestra popup del filtro. Con questa opzione, è possibile creare un filtro che limita gli oggetti visualizzati nell'elenco degli oggetti. È possibile filtrare in base al tipo e al nome dell'oggetto, secondo le esigenze.

  Selezionare l'opzione per aprire la finestra di dialogo Filtro Avanzato che consente di creare un filtro utilizzando quasi tutti gli attributi degli oggetti. Per ulteriori informazioni, vedere “Configurazione di ricerca avanzata” a pagina 24.

Per eseguire un'azione su un oggetto, selezionare la relativa casella di controllo, quindi selezionare l'icona d'azione dall'intestazione Elenco oggetti. Per eseguire un'azione sul container che si sta attualmente sfogliando, selezionare l'oggetto al livello attuale. È possibile eseguire le azioni riportate di seguito mediante questa opzione:

- “Modifica del Filtro diritti ereditati” a pagina 51
- “Modifica dei diritti dei trustee” a pagina 52
- “Estensione di un oggetto” a pagina 64
- “Ridenominazione di un oggetto” a pagina 48
- Imposta password
- “Visualizzazione dei diritti effettivi” a pagina 53

Figura 9-2 *Il frame del contenuto nella visualizzazione ad albero*



10 Gestione dello schema

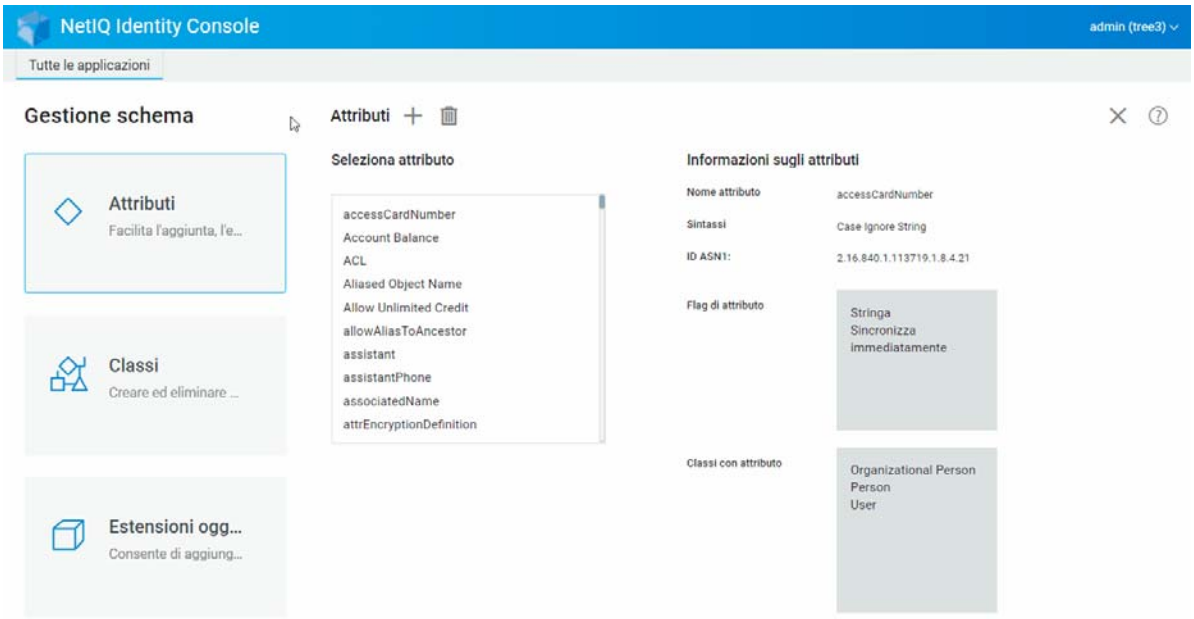
Lo schema directory definisce i tipi di oggetti che possono essere creati nell'albero (ad esempio utenti, stampanti, gruppi e così via) e quali informazioni sono obbligatorie o facoltative al momento della creazione dell'oggetto. In Identity Console sono disponibili i seguenti task relativi allo schema:

Creazione di un attributo

È possibile definire tipi personalizzati di attributi e aggiungerli come attributi opzionali alle classi di oggetti esistenti. Non è tuttavia possibile aggiungere attributi obbligatori a classi esistenti. Creazione di un attributo:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea attributo, immettere i seguenti dettagli:
   - Nome attributo
   - ID ASN1 (facoltativo)
   - Sintassi
   - Flag di attributo
4. Una volta immessi tutti i dettagli richiesti, fare clic sul pulsante Crea.
5. Viene visualizzato un messaggio di conferma che indica che l'attributo è stato creato.

Figura 10-1 *Creazione di un attributo*



Creazione di una classe

L'opzione **Gestione schema** consente di definire classi personalizzate. È quindi possibile estendere singoli oggetti con le proprietà definite nelle proprie classi. Per creare una classe:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Classi**.
2. Fare clic sull'icona +.
3. Nella pagina Crea attributo, immettere i seguenti dettagli:
   - Nome classe
   - ID ASN1 (facoltativo)
   - Flag di classe. Selezionare uno dei seguenti flag di classe:
     - **Classe effettiva:** Impostare questo flag per creare una classe effettiva, che potrà essere utilizzata per creare oggetti.
     - **Classe non effettiva:** Viene utilizzata come segnaposto per un gruppo di attributi. Una classe non effettiva non può essere utilizzata per creare gli oggetti, ma può essere specificata come classe dalla quale altre classi possono ereditare gli attributi. Ad esempio, la classe Persona è una classe non effettiva che contiene attributi ereditati dalla classe Utente.
     - **Classe ausiliaria:** Raccolta di attributi che possono essere associati solo a singoli oggetti e non a intere classi.
     - **Classe container:** Impostare questo flag per definire la classe attuale come container. Se viene utilizzata per creare oggetti, tali oggetti diventano oggetti Container (ad esempio, OU). Non impostare questo flag per la classe di un oggetto Leaf.

Nota: Se si selezionano classi effettive e non effettive, è necessario specificare anche i valori della Super Classe. Se si sceglie la classe ausiliaria, la super classe è facoltativa.

4 Dopo aver inserito tutti i dettagli richiesti, fare clic su **Successivo**.

5 Nella schermata successiva, selezionare gli attributi facoltativi, obbligatori e di denominazione, quindi fare clic su **OK**.

6 Viene visualizzato un messaggio di conferma che indica che la classe è stata creata.

Assegnazione di attributi a una classe

È possibile aggiungere attributi opzionali alle classi esistenti se è necessario modificare le informazioni dell'organizzazione o se si prevede di eseguire la fusione di alberi. Aggiunta di un attributo ad una classe esistente:

Nota: Gli attributi obbligatori possono essere definiti durante la creazione di una classe. Un attributo obbligatorio è un attributo che deve essere completato al momento della creazione dell'oggetto.

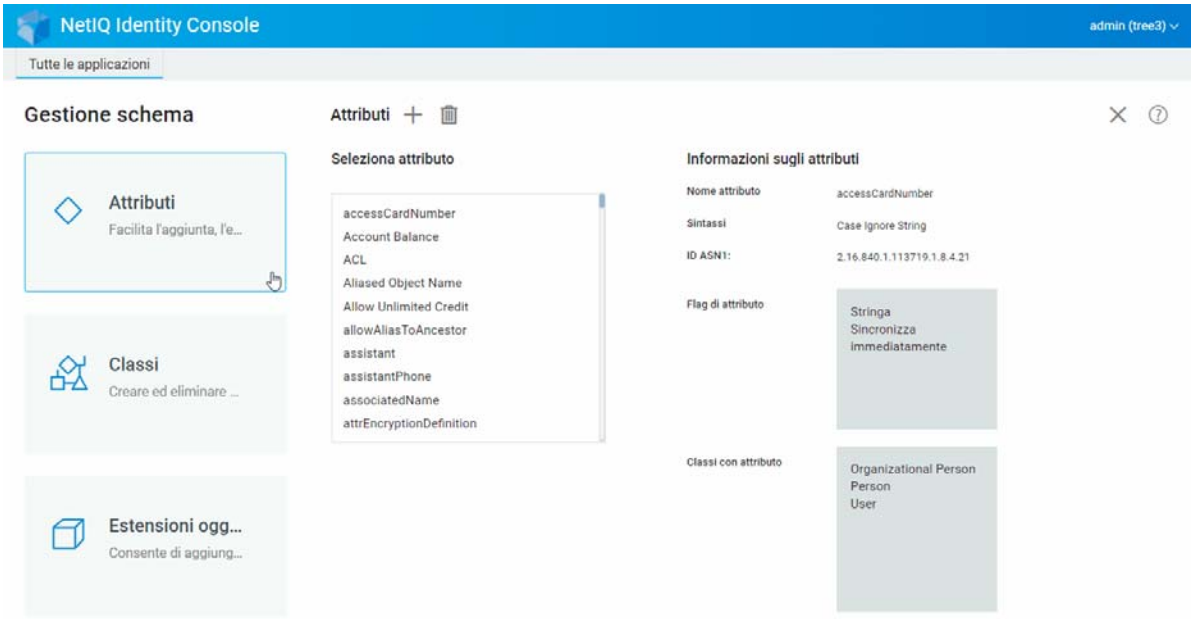
1 Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Classi**.

2 Fare clic su una delle classi elencate in **Seleziona classe**.

3 Le informazioni relative alla classe vengono visualizzate sul lato destro dello schermo.

4 Fare clic sul pulsante + accanto all'opzione **Attributi**, selezionare gli attributi che si desidera aggiungere e fare clic su **Aggiungi** > **Salva**.

Figura 10-2 *Assegnazione di attributi a una classe*

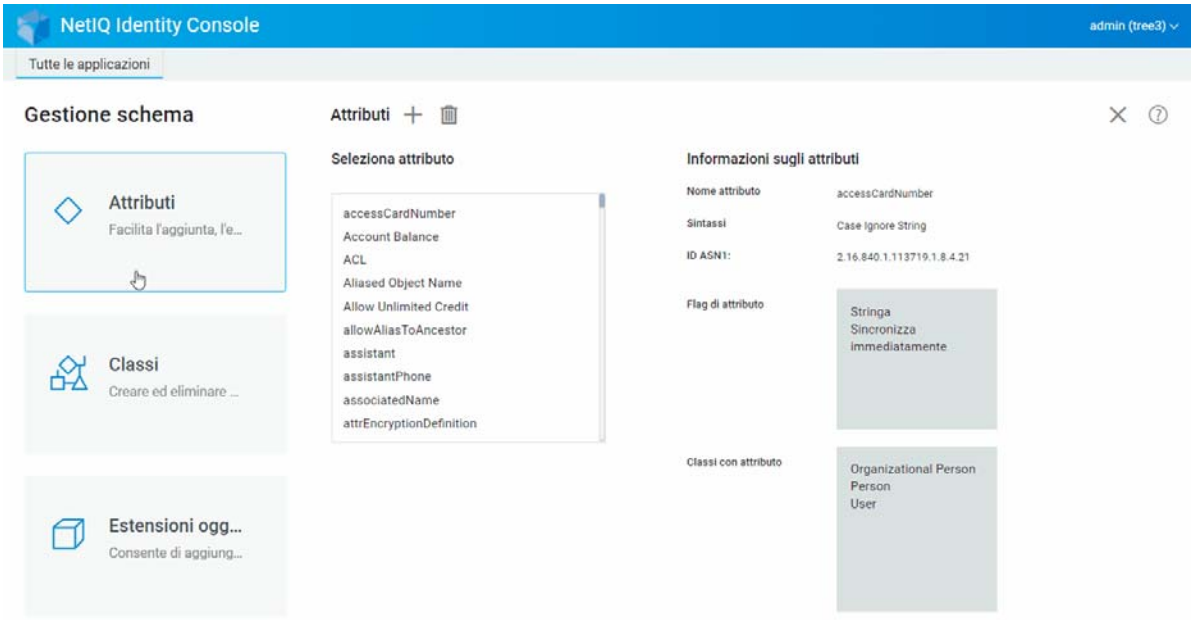


Visualizzazione delle Informazioni sugli attributi

È possibile visualizzare i dettagli strutturali di un attributo, ad esempio sintassi, flag e classi. Per visualizzare le informazioni su un attributo:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Attributi**.
2. Fare clic su uno degli attributi elencati in **Seleziona attributo**.
3. Le informazioni relative all'attributo vengono visualizzate sul lato destro dello schermo.

Figura 10-3 *Visualizzazione delle informazioni sugli attributi*



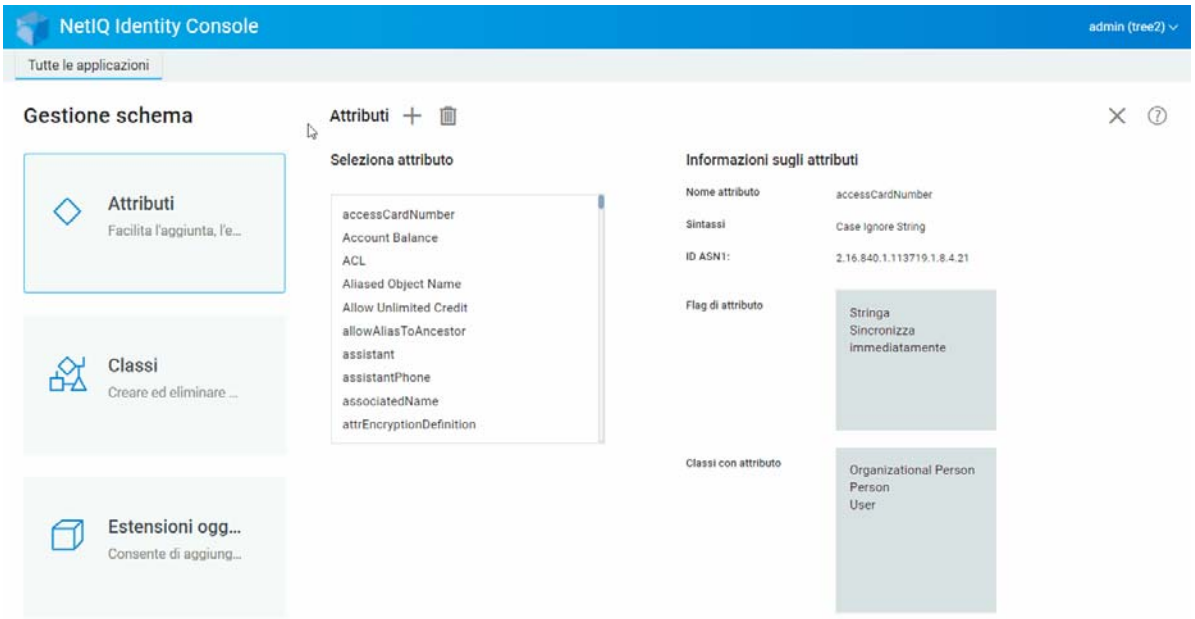
Eliminazione di un attributo

È possibile eliminare gli attributi inutilizzati che non fanno parte dello schema base dell'albero eDirectory. Può essere utile eseguire questa operazione dopo la fusione di due alberi della directory oppure se un attributo è diventato obsoleto. Per eliminare un attributo:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Attributi**.
2. Selezionare l'attributo che si desidera eliminare nell'elenco **Seleziona attributo**, quindi fare clic sull'icona .

   Nota: L'icona sarà abilitata solo quando si seleziona un attributo che può essere eliminato.
3. Fare clic su **OK** per confermare l'eliminazione.

Figura 10-4 *Eliminazione di un attributo*



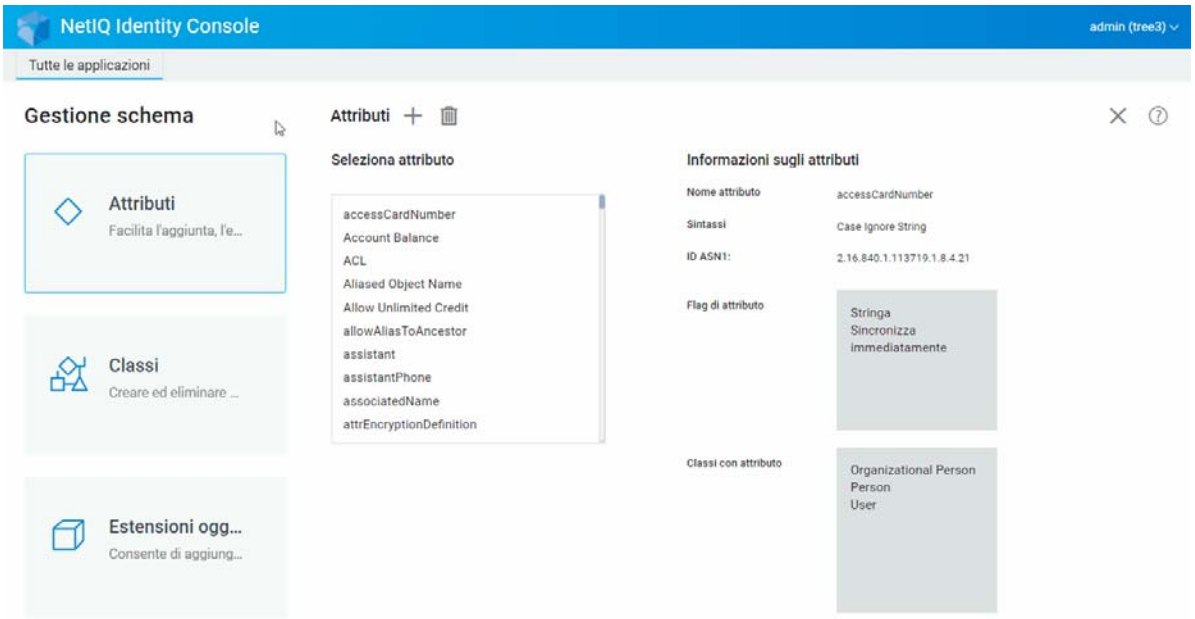
Eliminazione di una classe

È possibile eliminare le classi inutilizzate che non fanno parte dello schema base dell'albero eDirectory. Identity Console impedisce di eliminare le classi attualmente utilizzate nelle partizioni replicate localmente. Per eliminare una classe:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Classi**.
2. Selezionare la classe che si desidera eliminare nell'elenco **Seleziona classe** e fare clic sull'icona .

   Nota: L'icona sarà abilitata solo quando si seleziona una classe che può essere eliminata.
3. Fare clic su **OK** per confermare l'eliminazione.

Figura 10-5 *Eliminazione di una classe*



Estensione di un oggetto

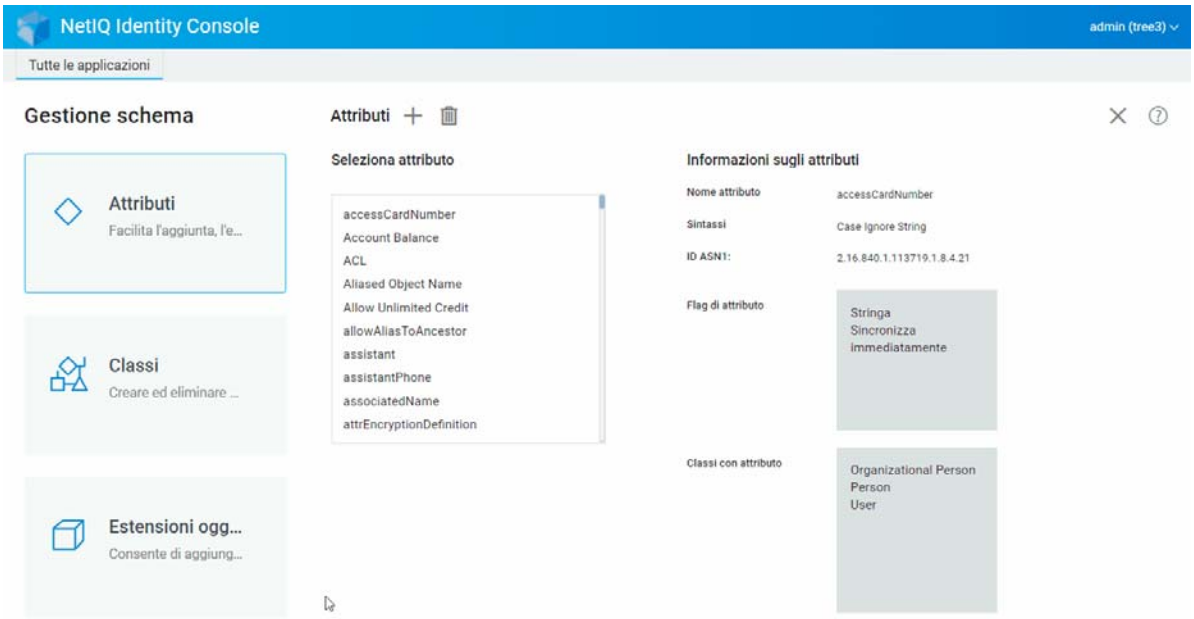
Per estendere un oggetto, eseguire le operazioni riportate di seguito:

1. Fare clic sull'opzione **Gestione schema** nella pagina di destinazione di Identity Console e selezionare **Estensione oggetto**.
2. Specificare il nome dell'oggetto oppure utilizzare il selettore oggetti per selezionare l'oggetto da estendere, quindi fare clic sull'icona .
3. Fare clic sull'icona e selezionare la classe ausiliaria, quindi fare clic su **OK**.

   Nota: Se alla classe ausiliaria selezionata è collegato un attributo obbligatorio, verrà richiesto di inserire i valori richiesti nella finestra pop-up **Attributi obbligatori**.

   ---
4. Viene visualizzato un messaggio di conferma che indica che la classe ausiliaria è stata aggiunta all'oggetto.
5. Per rimuovere una classe ausiliaria esistente dall'oggetto, selezionare la classe e fare clic sull'icona .

Figura 10-6 *Estensione di un oggetto*



11 Gestione degli eventi di revisione

In questo capitolo viene illustrato come gestire diversi eventi di revisione mediante Identity Console. Tramite questa funzione è possibile abilitare o disabilitare gli eventi di revisione per l'NCP Server.

Configurazione degli eventi di revisione CEF

1. Eseguire il login a Identity Console mediante il nome utente e la password.
2. Selezionare **Revisione**.
3. Selezionare l'NCP Server che si desidera controllare, quindi fare clic su **OK**.

   Nota: Dopo aver abilitato per la prima volta gli eventi CEF per qualsiasi NCP server, alcuni eventi saranno selezionati per default.

4. Configurare gli eventi di revisione CEF:
   - **Configurazione evento:** Abilitare o disabilitare i seguenti eventi in base alla revisione richiesta per il proprio ambiente:

Nota: Le singole categorie di eventi nella sezione di configurazione evento verranno chiuse per default. È possibile espandere ciascuna categoria per selezionare singoli eventi.

Opzioni	Descrizione
Eventi di sicurezza	Selezionare gli eventi di sicurezza per i quali si desidera registrare gli eventi. È possibile registrare gli eventi per aggiungere o eliminare membri, per rilevare intrusi, per cambiare la password, per autenticare gli utenti e molto altro ancora.
Eventi oggetto	Selezionare gli eventi oggetto per i quali si desidera registrare gli eventi. È possibile registrare gli eventi per creare oggetti da eliminare, rinominare, spostare e ricercare.
Eventi attributo	Selezionare gli eventi attributo per i quali si desidera registrare gli eventi. È possibile registrare eventi per leggere ed eliminare attributi e per aggiungere, eliminare e confrontare il valore dell'attributo.
Eventi LDAP	Selezionare gli eventi LDAP per i quali si desidera registrare gli eventi.

- **Impostazioni avanzate:** Utilizzando le impostazioni avanzate, è possibile eseguire le seguenti operazioni:
  - **Globale:** È possibile selezionare o eliminare le impostazioni globali per le voci duplicate.
    - **Non inviare eventi replicati:** Selezionare questa opzione per interrompere la ricezione di eventi duplicati dovuti alla replica da altri server.
  - **Valori dell'evento di log:** Gli eventi vengono registrati in un file di testo. I valori dell'evento con dimensioni superiori a 768 byte sono considerati "valori grandi". È possibile registrare eventi di qualsiasi dimensione.
    - **Valori di grandi dimensioni di log:** Selezionare questa opzione per registrare eventi di dimensioni superiori a 768 byte.
    - **Valori attributo di log:** Selezionare questa opzione per visualizzare i valori attributo. Questo è applicabile solo agli eventi **Aggiungi valore** ed **Elimina valore**.
    - **Valori attributo cifrato di log:** Selezionare questa opzione per visualizzare i valori attributo cifrato. Questo è applicabile solo agli eventi **Aggiungi valore** ed **Elimina valore**.

    Nota: Se la dimensione dell'evento è superiore a 768 byte, il suo valore viene troncato e salvato nel file di registro.

Descrizione dei tipi di evento CEF

È possibile configurare CEF per registrare gli eventi nelle seguenti categorie:

- Sicurezza

- Oggetti
- Attributi
- LDAP

È possibile controllare il seguente set di tipi di evento di default:

Categoria	Tipo di evento
Sicurezza	◆ ACL modificato ◆ Aggiungi membro ◆ Elimina membro ◆ Intruso rilevato ◆ Login disabilitato ◆ Login abilitato ◆ Login ◆ Modifica Sicurezza uguale a ◆ Config revisione ◆ Modifica password ◆ Sblocco account ◆ Logout ◆ Connessione ◆ Rappresenta ◆ Autentica ◆ Verifica password ◆ Modifica configurazione di login ◆ Credenziali di interrogazione
Oggetti	◆ Crea oggetto ◆ Elimina oggetto ◆ Rinomina oggetto ◆ Sposta oggetto ◆ Lettura DSA ◆ Ricerca
Attributi	◆ Leggi attributo ◆ Elimina attributo ◆ Aggiungi valore ◆ Elimina valore ◆ Confronta valore attributo

Categoria	Tipo di evento
LDAP	◆ Associazione LDAP ◆ Risposta associazione LDAP ◆ Separazione LDAP ◆ Connessione LDAP ◆ Ricerca LDAP ◆ Risposta ricerca LDAP ◆ Risposta voce ricerca LDAP ◆ Aggiungi LDAP ◆ Risposta aggiunta LDAP ◆ Confronto LDAP ◆ Risposta di confronto LDAP ◆ Modifica LDAP ◆ Risposta di modifica LDAP ◆ Elimina LDAP ◆ Risposta di eliminazione LDAP ◆ Modifica DN LDAP ◆ Modifica DN di risposta LDAP ◆ Abbandono LDAP ◆ Operazione LDAP estesa ◆ Operazione LDAP di sistema estesa ◆ Risposta operazione LDAP estesa ◆ Modifica configurazione server LDAP ◆ Operazione LDAP sconosciuta ◆ Password LDAP Modifica

Configurazione del filtro di revisione CEF

Tramite i filtri e le notifiche degli eventi, CEF è in grado di generare rapporti quando si verifica un tipo specifico di evento o quando se non si verificano. È inoltre possibile filtrare gli eventi relativi a una o più classi di oggetti o attributi specifici, a seconda del tipo di evento. CEF valuta tutti gli eventi generati sui filtri configurati sul server eDirectory e registra solo gli eventi che corrispondono a tali filtri.

In questa sezione vengono fornite le informazioni necessarie per configurare i filtri e le notifiche di sistema.

- “Filtraggio di eventi eDirectory con filtro di esclusione” a pagina 71
- “Filtraggio di eventi oggetto CEF” a pagina 71
- “Filtraggio di eventi attributo CEF” a pagina 72

Filtraggio di eventi eDirectory con filtro di esclusione

Fare clic sul collegamento **Filtro di esclusione** per configurare il filtraggio delle classi di oggetti e gli attributi per cui non si desidera generare un evento. È possibile selezionare le classi e gli attributi dell'oggetto.

Per configurare il filtraggio per gli eventi eDirectory indesiderati:

1. In Identity Console, selezionare **Revisione** nella home page.
2. Selezionare l'NCP Server che si desidera controllare, quindi fare clic su **OK**.
3. A questo punto, selezionare **Impostazioni avanzate**, quindi fare clic su **Filtro di esclusione** in **Filtri**.

   Viene visualizzata la finestra Filtraggio di esclusione CEF.
4. Nell'elenco **Classi di oggetti disponibili**, selezionare le classi di oggetti per cui non si desidera raccogliere gli eventi, quindi fare clic sulla freccia destra per spostarli nell'elenco **Classi di oggetti selezionate**.
5. Nell'elenco **Attributi disponibili**, selezionare un numero qualsiasi di attributi. Selezionare l'attributo e fare clic sulla freccia destra per aggiungere l'attributo all'elenco degli attributi selezionati.
6. Fare clic su **OK**.

Se si utilizza il filtro configurato, il modulo di revisione CEF interrompe la generazione degli eventi per tutte le classi e gli attributi dell'oggetto selezionato.

Filtraggio di eventi oggetto CEF

È possibile configurare il filtraggio degli oggetti in modo che vengano ricercati solo gli eventi specifici o un evento specifico. Ad esempio, se si desidera ricevere una notifica quando si crea un account utente su eDirectory, è possibile creare un filtro selezionando la classe di oggetti utente per registrare gli eventi per la creazione di un nuovo oggetto utente.

Per configurare il filtraggio degli account, fare clic sul collegamento Eventi oggetto, selezionare la classe, quindi fare clic su **OK** per uscire dall'applicazione.

Per configurare i filtri per gli eventi di gestione account:

1. In Identity Console, selezionare **Revisione** nella home page.
2. Selezionare l'NCP Server che si desidera controllare, quindi fare clic su **OK**.
3. A questo punto, selezionare **Impostazioni avanzate** e fare clic su **Eventi oggetto** in **Filtri**.

   Viene visualizzata la finestra Filtraggio oggetti CEF.
4. Nell'elenco **Classi di oggetti disponibili**, selezionare una classe di oggetti, quindi fare clic sulla freccia destra per spostare la classe di oggetti all'elenco **Classi di oggetti selezionate**, quindi fare clic su **OK**.

Tramite il filtro configurato, il modulo di revisione CEF controlla tutti gli eventi generati per le classi di oggetti selezionate e registra tali eventi.

Filtraggio di eventi attributo CEF

Fare clic sul collegamento **Eventi attributo** per configurare il filtraggio degli eventi attributo. Ad esempio, se si desidera ricevere una notifica quando un utente aggiunge un nuovo valore di attributo in eDirectory, è possibile creare un filtro per registrare gli eventi per l'aggiunta di un nuovo valore.

Per configurare il filtraggio per gli eventi attributo:

1. In Identity Console, selezionare **Revisione** nella home page.
2. Selezionare l'NCP Server che si desidera controllare, quindi fare clic su **OK**.
3. A questo punto, fare clic su **Impostazioni avanzate**, quindi scegliere **Eventi attributo** in **Filtri**.

   Viene visualizzata la finestra **Filtraggio configurazione attributi**.
4. Nell'elenco **Classi di oggetti disponibili**, selezionare le classi di oggetti per le quali si desidera raccogliere gli eventi, quindi fare clic sulla freccia destra per spostarli nell'elenco **Classi di oggetti selezionate**.
5. Nell'elenco **Attributi disponibili**, selezionare un numero qualsiasi di attributi per le classi di oggetti selezionate. Selezionare l'attributo e fare clic sulla freccia destra per aggiungere l'attributo all'elenco degli attributi selezionati.

   Nota: Se si seleziona una classe oggetto, vengono selezionati tutti gli eventi attributo per tutti gli attributi di quella classe oggetto. In questo caso, vengono ottenuti tutti gli eventi attributo per tutti gli attributi delle classi di oggetti selezionate.

   ---
6. Fare clic su **OK**.

Se il filtro è configurato, il modulo di revisione CEF verifica gli eventi generati per tutte le classi e gli attributi dell'oggetto selezionato e registra tali eventi.

12 Gestione degli attributi cifrati

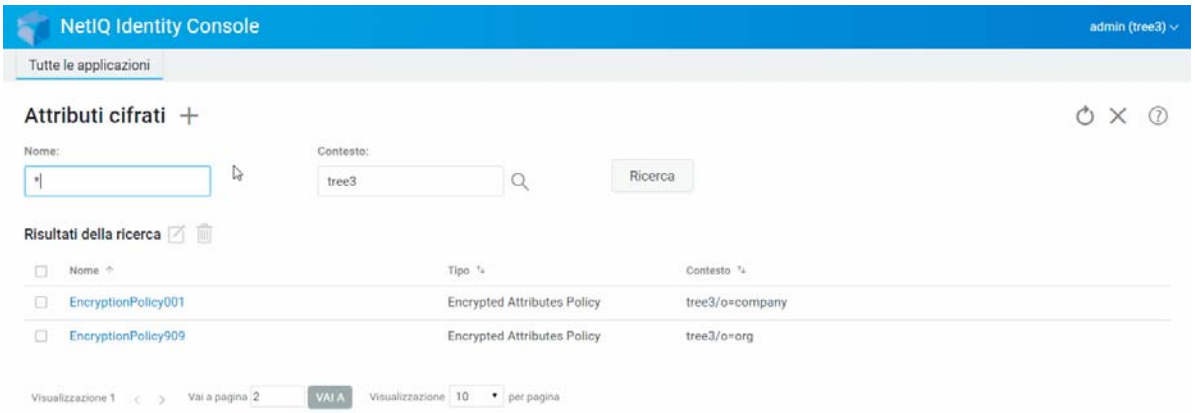
Identity Console è in grado di leggere in modo sicuro gli attributi cifrati dal server eDirectory. L'utilizzo di Identity Console consente di creare, modificare o eliminare diverse policy per tali attributi cifrati.

Creazione di una policy per gli attributi cifrati

Per creare una nuova policy di attributo:

1. Fare clic sull'opzione **Attributi cifrati** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea policy degli attributi cifrati, immettere i seguenti dettagli:
   - Specificare il nome della policy
   - Immettere o selezionare il Contesto
   - Selezionare l'NLP Server
   - Selezionare gli attributi
4. Una volta specificati tutti i dettagli richiesti, fare clic su **Fine**.
5. Viene visualizzato un messaggio di conferma che indica che la policy è stata creata.

Figura 12-1 *Creazione di una policy degli attributi cifrati*

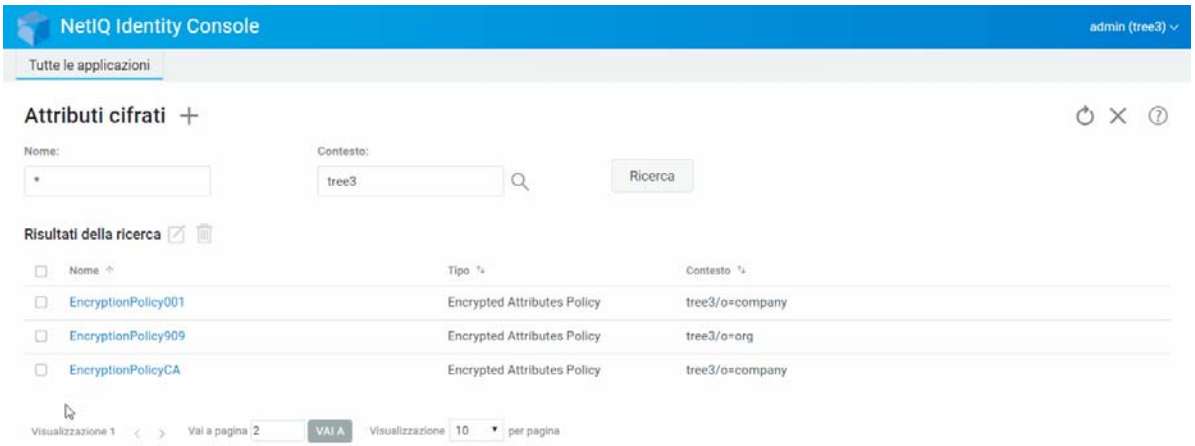


Eliminazione di una policy degli attributi cifrati

Per eliminare una policy degli attributi cifrati:

1. Fare clic sull'opzione **Attributi cifrati** nella pagina di destinazione di Identity Console.
2. Specificare il nome e il contesto dell'attributo o utilizzare la funzione di ricerca per trovarlo, quindi fare clic sul pulsante Ricerca.
3. Selezionare gli attributi dall'elenco e fare clic sull'icona 🗑.
4. Viene visualizzato un messaggio di conferma che indica che la policy è stata eliminata.

Figura 12-2 *Eliminazione di una policy degli attributi cifrati*

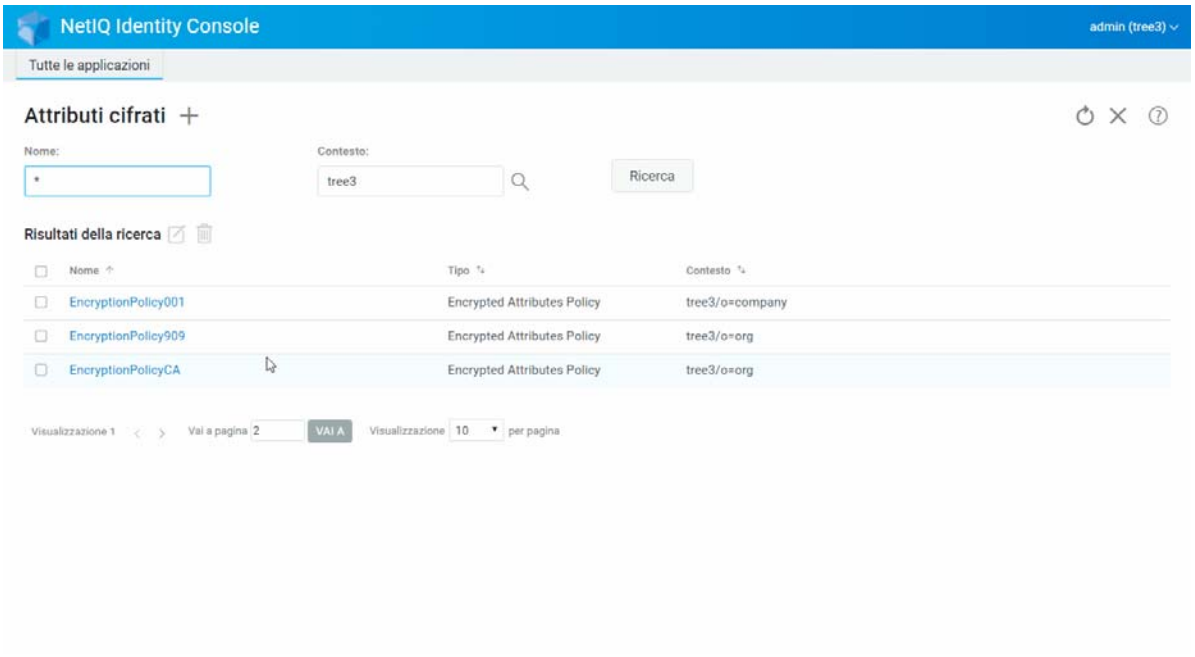


Modifica di una policy degli attributi cifrati

Per modificare una policy degli attributi cifrati:

1. Fare clic sull'opzione **Attributi cifrati** nella pagina di destinazione di Identity Console.
2. Digitare il nome e il contesto dell'oggetto, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'attributo nell'elenco degli oggetti, quindi fare clic sull'icona .
4. Apportare le modifiche, quindi fare clic sul pulsante Salva.
5. Viene visualizzato un messaggio di conferma che indica che la policy è stata modificata.

Figura 12-3 *Modifica di una policy degli attributi cifrati*



13 Gestione della replica cifrata

Per abilitare la replica cifrata, è necessario configurare una partizione della stessa. Le impostazioni di configurazione vengono memorizzate nell'oggetto Root della partizione. È possibile scegliere di abilitare la replica cifrata a livello di partizione. Quando si abilita la replica cifrata a livello di partizione, viene cifrata la replica di tutte le repliche che ospitano la partizione. Si supponga, ad esempio, che la partizione P1 contenga le repliche R1, R2, R3 e R4. È possibile cifrare la replica di tutte le repliche.

- “Abilitazione della replica cifrata per le partizioni” a pagina 77

Abilitazione della replica cifrata per le partizioni

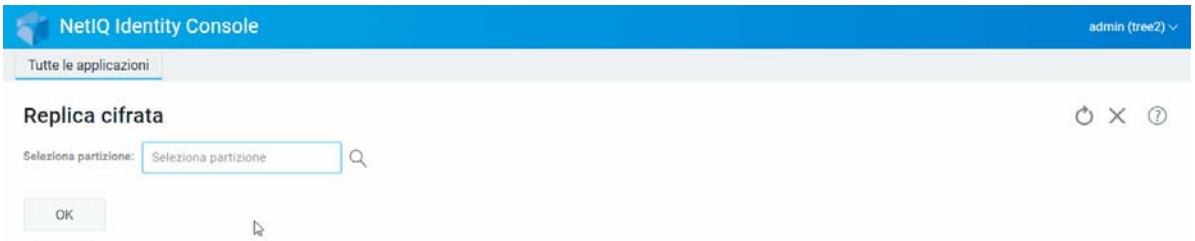
Per abilitare la replica cifrata per le partizioni:

Nota: Per abilitare una partizione per la replica cifrata, tutti i server che ospitano la partizione devono essere server eDirectory 9.2 o successivi.

---

1. Fare clic sull'opzione **Replica cifrata** nella pagina di destinazione di Identity Console.
2. Specificare o individuare la partizione per la quale si desidera abilitare la replica cifrata.
3. Selezionare l'opzione **Abilita replica cifrata**. Deselezionare questa opzione per disabilitare la replica cifrata di una partizione.
4. Fare clic su **Fine**.
5. Viene visualizzato un messaggio di conferma che indica che la replica cifrata è stata abilitata.

Figura 13-1 *Abilitazione della replica cifrata per le partizioni*



14 Gestione delle partizioni e delle repliche

Le operazioni di partizione e replica consentono di gestire la progettazione fisica e la distribuzione di eDirectory sui server di directory.

Le partizioni creano divisioni logiche dell'albero eDirectory. Ad esempio, è possibile scegliere un'unità organizzativa e definirla come nuova partizione. In tal caso, l'unità organizzativa e tutti i relativi oggetti subordinati vengono divisi dalla partizione superiore. L'unità organizzativa selezionata diventa la radice di una nuova partizione. Le repliche della nuova partizione saranno presenti sugli stessi server come repliche della partizione superiore e gli oggetti presenti nella nuova partizione faranno parte dell'oggetto Radice della nuova partizione.

Tramite il modulo Partizione è possibile eseguire i seguenti task:

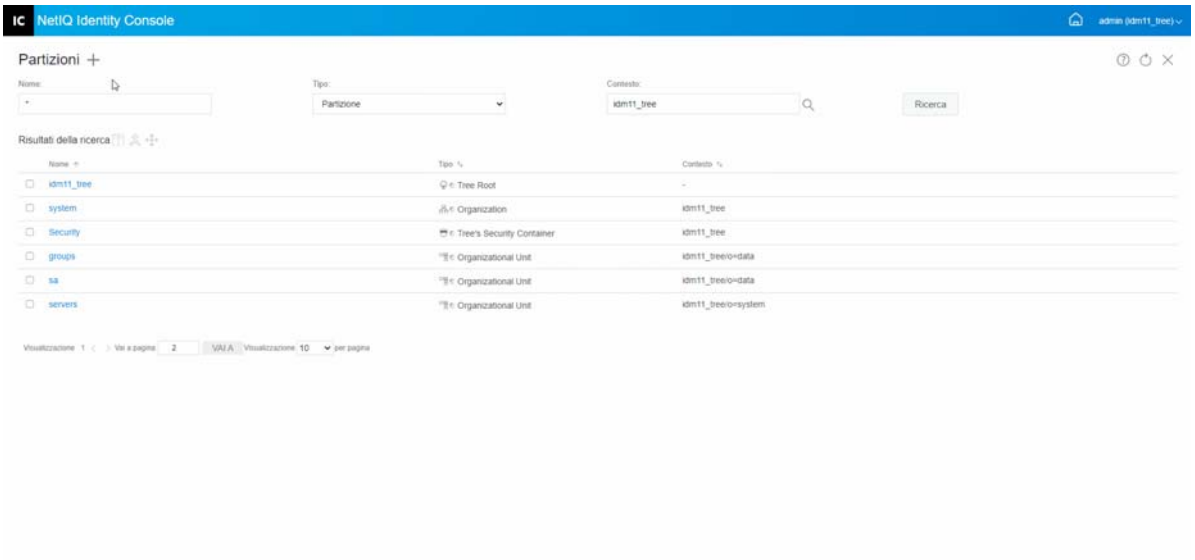
- "Creazione di una partizione" a pagina 79
- "Unire partizioni" a pagina 80
- "Modifica di partizioni" a pagina 81
- "Spostamento di una partizione" a pagina 81

Creazione di una partizione

Per creare una nuova partizione:

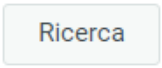
1. Fare clic sull'opzione **Gestione partizioni** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea partizione, specificare il container da utilizzare come radice della nuova partizione oppure individuarlo mediante l'icona del Selettore oggetti, quindi fare clic su **Crea**.
4. Viene visualizzato un messaggio di conferma che indica che la partizione è stata creata.

Figura 14-1 *Creazione di una nuova partizione*



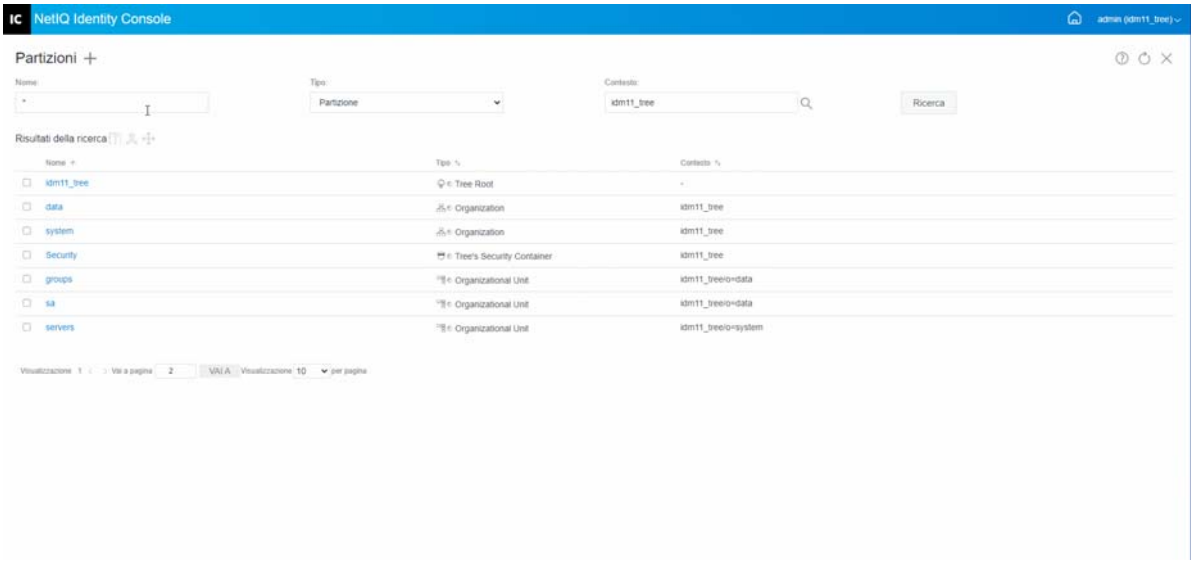
Unire partizioni

Per unire le partizioni con la relativa partizione superiore:

1. Fare clic sull'opzione **Gestione partizioni** nella pagina di destinazione di Identity Console.
2. Specificare il nome, il tipo e il contesto della partizione o utilizzare la funzione di ricerca per trovarla, quindi fare clic sul pulsante 

.
3. Selezionare la partizione dall'elenco di ricerca, fare clic sull'icona  , quindi su **OK**.
4. Viene visualizzato un messaggio di conferma che indica che la partizione è stata unita.

Figura 14-2 *Unione di partizioni*



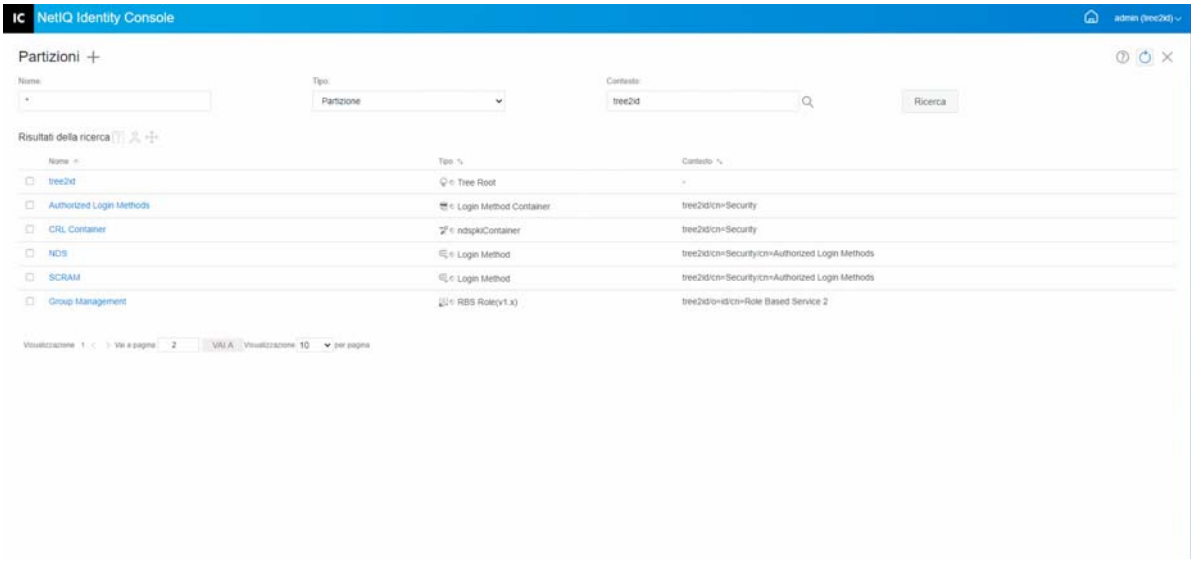
Modifica di partizioni

Per modificare le partizioni:

1. Fare clic sull'opzione **Gestione partizioni** nella pagina di destinazione di Identity Console.
2. Digitare il nome, il tipo e il contesto della partizione, quindi fare clic sul pulsante Ricerca.
3. Selezionare la partizione dall'elenco di ricerca e fare clic sull'icona .
4. Fare clic sull'opzione **Modifica** sotto **Filtro** per modificare i filtri di replica oltre alle classi e agli attributi corrispondenti, quindi fare clic su **OK**.

   Se è stato selezionato **Server** nel campo **Tipo**, verrà visualizzato l'elenco di tutti i server. Facendo clic su ciascun server viene visualizzato un elenco di tutte le partizioni presenti sul server.
5. Viene visualizzato un messaggio di conferma che indica che la partizione è stata modificata.

Figura 14-3 *Modifica di partizioni*



Spostamento di una partizione

Lo spostamento di una partizione consente di spostare un sottoalbero nell'albero della directory. Questa operazione viene anche chiamata sposta e innesta. È possibile spostare solo le partizioni che non includono partizioni subordinate. Se esistono partizioni subordinate, è innanzitutto necessario fonderle prima di eseguire l'operazione di spostamento.

Quando si sposta una partizione, tutti i riferimenti all'oggetto Radice della partizione vengono modificati da eDirectory. Contrariamente al nome comune dell'oggetto, che rimane invariato, il nome completo del container e di tutti i relativi elementi subordinati viene modificato.

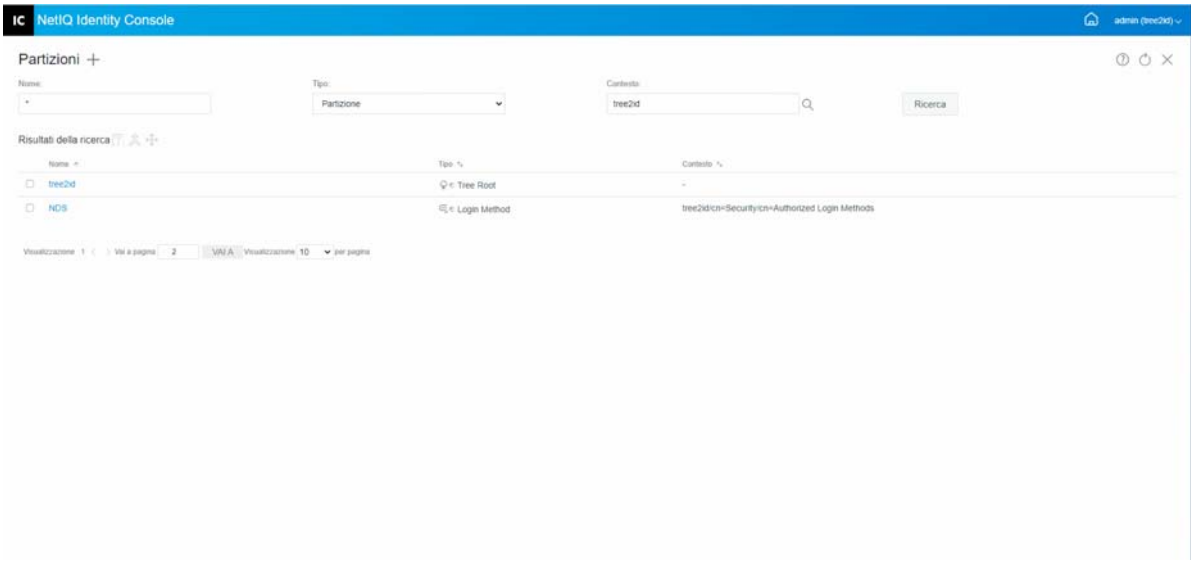
Nota: quando si sposta una partizione, è necessario attenersi alle regole di contenimento di eDirectory. Ad esempio, non è possibile spostare un'unità organizzativa direttamente nella radice dell'albero della directory, in quanto le relative regole di contenimento consentono di inserire solo oggetti Locality (Località), Country (Paese) o Organization (Organizzazione) e non oggetti Organizational Unit (Unità organizzativa).

Per spostare una partizione:

1. Fare clic sull'opzione **Gestione partizioni** nella pagina di destinazione di Identity Console.
2. Digitare il nome, il tipo e il contesto della partizione, quindi fare clic sul pulsante Ricerca.
3. Selezionare la partizione dall'elenco di ricerca e fare clic sull'icona .
4. Selezionare l'oggetto container di destinazione in cui si desidera spostare la partizione specificata e fare clic su **OK**.

   Nota: **Crea un alias in sostituzione della partizione spostata** consente di creare un puntatore alla nuova ubicazione della partizione. Tramite questa opzione tutte le operazioni dipendenti dall'ubicazione precedente continueranno a essere eseguite regolarmente fino a quando non sarà possibile aggiornarle in base alla nuova ubicazione. Gli utenti possono continuare a eseguire il login alla rete e trovare oggetti nell'ubicazione all'interno della directory originale.
5. Viene visualizzato un messaggio di conferma che indica che l'operazione di spostamento della partizione è stata completata.

Figura 14-4 *Spostamento di una partizione*



15 Gestione degli indici

Index Manager è un attributo dell'oggetto Server che consente di gestire gli indici del database. Tali indici vengono utilizzati da eDirectory per migliorare in modo significativo le prestazioni di esecuzione delle interrogazioni.

NetIQ eDirectory dispone di un set di indici che forniscono le funzionalità di base delle interrogazioni. Questi indici di default sono relativi agli attributi seguenti.

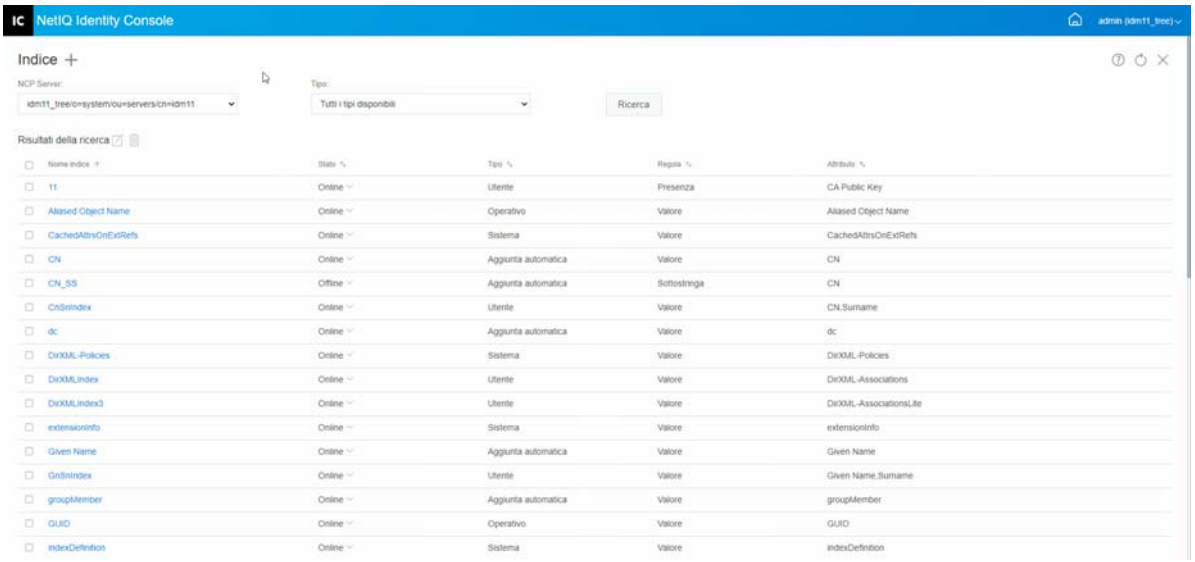
Dal modulo Indice è possibile eseguire i seguenti task:

Creazione di indici

Per creare un nuovo indice:

1. Fare clic sull'opzione **Gestione indici** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Immettere il nome dell'indice.
4. Selezionare uno o più server dall'elenco degli NCP server disponibili.
5. Selezionare gli attributi richiesti.
6. Selezionare la regola di indice:
   - 6a **Sottostringa:** individua la corrispondenza con un sottoinsieme della stringa del valore dell'attributo. Ad esempio, un'interrogazione per la ricerca di un Cognome contenente le lettere "chi" restituisce le corrispondenze Chiani, Vecchini e Bianchi. Un indice di sottostringa è il tipo di indice che richiede un maggior impiego di risorse per la creazione e la gestione.
   - 6b **Presenza:** richiede solo la presenza di un attributo anziché dei valori di attributo specifici. Ad esempio, in un'interrogazione per la ricerca di tutte le voci con attributo Script di login viene utilizzato un indice di presenza.
   - 6c **Valore:** individua la corrispondenza con l'intero valore o con la prima parte del valore di un attributo. Ad esempio, è possibile utilizzare la corrispondenza di valori per trovare le voci con un Cognome equivalente a "Giannini" e le voci con un Cognome che inizia per "Gia".
7. Fare clic sul pulsante Crea.
8. Viene visualizzato un messaggio di conferma che indica che l'indice è stato creato.

Figura 15-1 *Creazione di un nuovo indice*

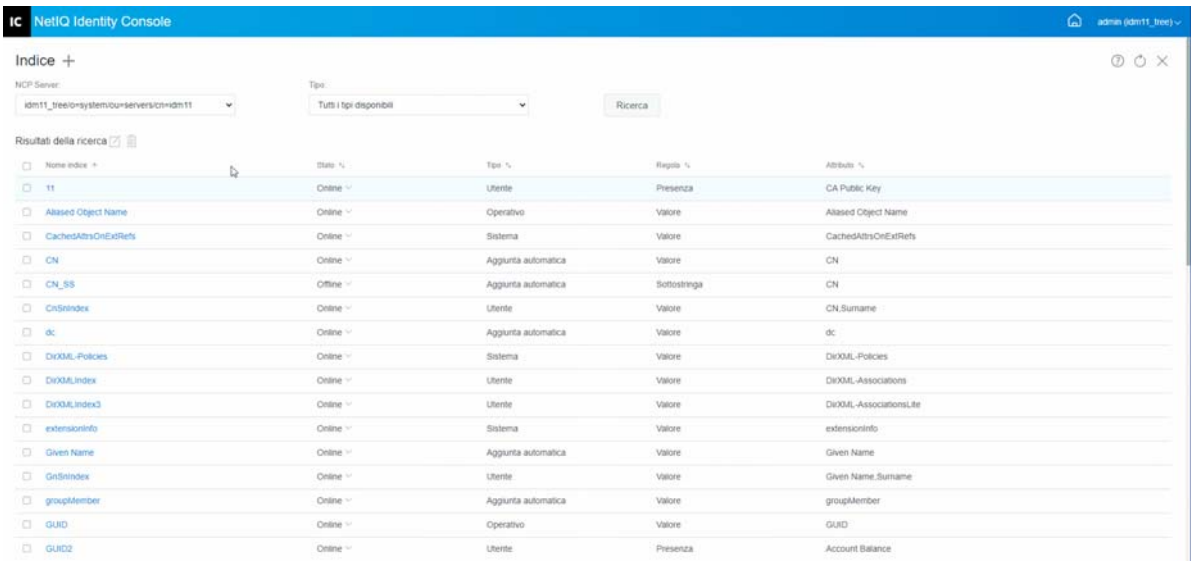


Eliminazione di un indice

Per eliminare un indice:

1. Fare clic sull'opzione **Gestione indici** nella pagina di destinazione di Identity Console.
2. Selezionare l'NCP server e il tipo di indice, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'indice dall'elenco di ricerca e fare clic sull'icona 🗑.
4. Viene visualizzato un messaggio di conferma che indica che l'indice è stato eliminato.

Figura 15-2 *Eliminazione di un indice*



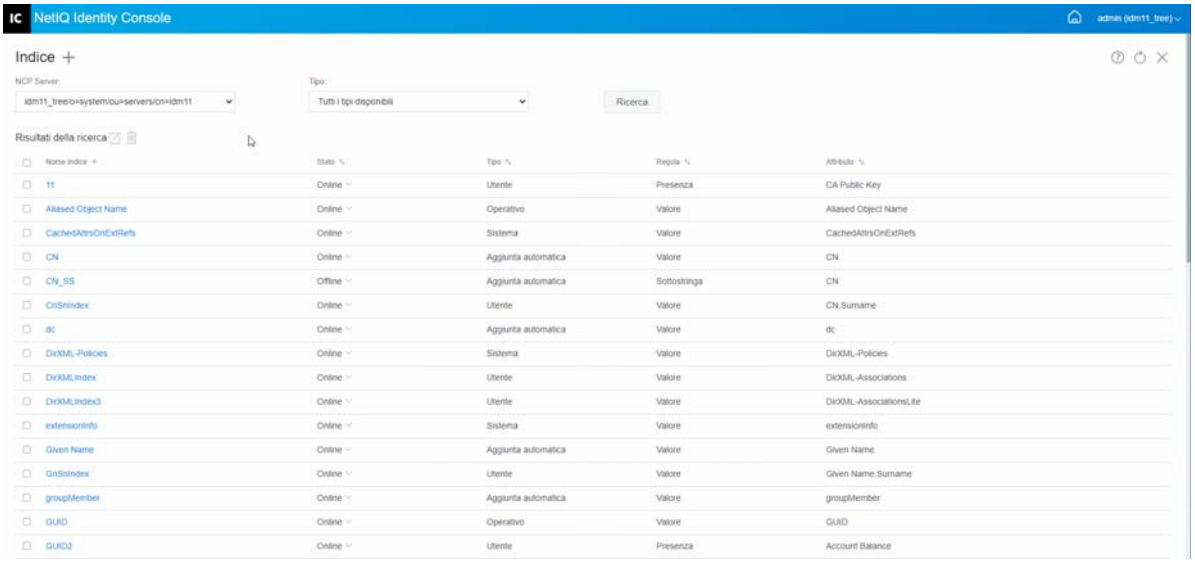
Copia di un indice

Se un determinato indice risulta utile su un server e se ne ha bisogno su un altro server, è possibile copiare la definizione dell'indice da un server a un altro. Nella revisione dei dati del predicato, potrebbe anche verificarsi l'esatto contrario: un indice necessario per più server non è più utile su uno di questi server. In questo caso, è possibile eliminare l'indice dal singolo server che non trae vantaggio dal suo utilizzo.

Per copiare un indice:

1. Fare clic sull'opzione **Gestione indici** nella pagina di destinazione di Identity Console.
2. Selezionare l'NCP server e il tipo di indice, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'indice dall'elenco di ricerca e fare clic sull'icona .
4. Selezionare gli NCP server desiderati in cui si desidera copiare l'indice e fare clic sul pulsante Salva.
5. Viene visualizzato un messaggio di conferma che indica che l'indice è stato modificato.

Figura 15-3 *Copia di un indice*



Modifica dello stato di un indice

Durante gli orari di punta può essere necessario ottimizzare le prestazioni impostando temporaneamente gli indici offline. Ad esempio, per ottenere una maggiore velocità di caricamento di massa, è possibile sospendere tutti gli indici definiti dall'utente. Poiché ogni aggiunta o modifica di

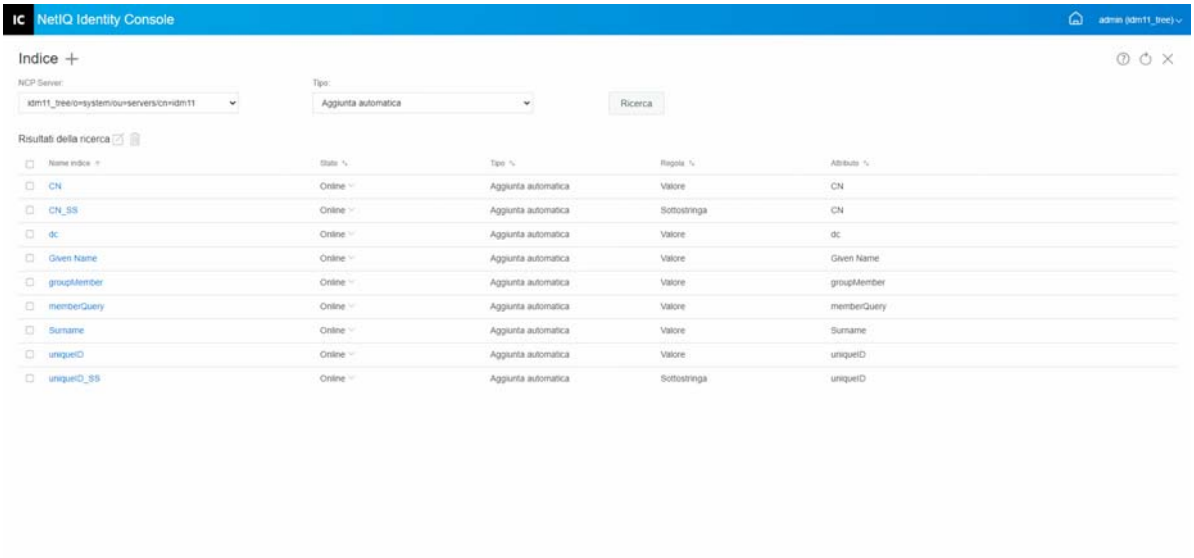
un oggetto richiede l'aggiornamento degli indici definiti, se si mantengono attivi tutti gli indici, il caricamento di massa dei dati potrebbe essere rallentato. Una volta completato il caricamento di massa, è possibile rimettere online gli indici.

Per impostare un indice offline:

1. Fare clic sull'opzione **Gestione indici** nella pagina di destinazione di Identity Console.
2. Selezionare l'NCP server e il tipo di indice, quindi fare clic sul pulsante Ricerca.
3. Fare clic sull'elenco a discesa **Stato** nell'elenco degli indici. Gli stati di un indice possono essere i seguenti:
   - **Online:** attualmente in esecuzione
   - **Offline:** sospeso. L'indice può essere riavviato.

Nota: non è possibile modificare lo stato degli indici di tipo Sistema e Operativo. Questi indici non possono neanche essere eliminati.

Figura 15-4 *Impostazione di un indice offline*



16 Configurazione di oggetti LDAP

Durante un'installazione di eDirectory viene creato un oggetto Server LDAP e un oggetto Gruppo LDAP. La configurazione di default per i servizi LDAP si trova nella directory in questi due oggetti. È possibile modificare la configurazione di default utilizzando il task LDAP Management (Gestione LDAP) in Identity Console.

L'oggetto Server LDAP rappresenta i dati di configurazione specifici del server. Tuttavia, l'oggetto Gruppo LDAP contiene informazioni di configurazione che possono essere facilmente condivise tra più server LDAP. Questo oggetto fornisce i dati di configurazione comuni e rappresenta un gruppo di server LDAP. I server dispongono di dati comuni.

È possibile associare più oggetti Server LDAP a un oggetto Gruppo LDAP. Tutti i server LDAP associati ottengono quindi la propria configurazione specifica dall'oggetto Server LDAP ma ottengono le informazioni comuni o condivise dall'oggetto Gruppo LDAP.

Dal modulo LDAP è possibile eseguire i seguenti task:

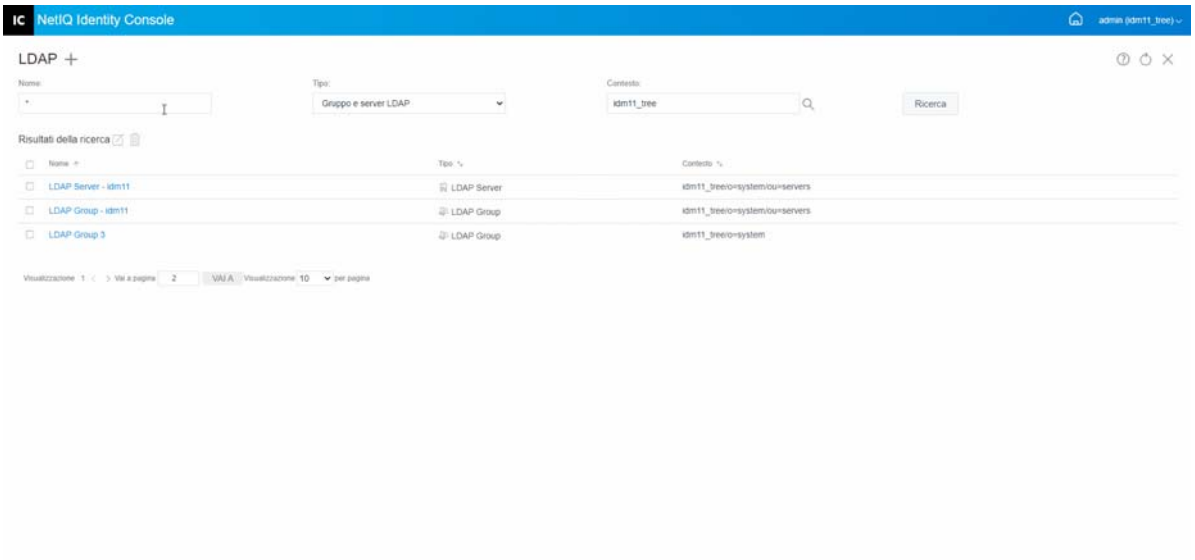
- "Creazione di oggetti LDAP" a pagina 87
- "Eliminazione di oggetti LDAP" a pagina 88
- "Modifica di oggetti LDAP" a pagina 89

Creazione di oggetti LDAP

Per creare un nuovo oggetto LDAP:

1. Fare clic sull'opzione **Configurazione LDAP** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina Crea oggetto LDAP, specificare il nome, il tipo e il contesto oppure utilizzare l'icona Ricerca contesto per individuarlo, quindi fare clic su **Crea**.
4. Viene visualizzato un messaggio di conferma che indica che l'oggetto LDAP è stato creato.

Figura 16-1 *Creazione di un nuovo oggetto LDAP*

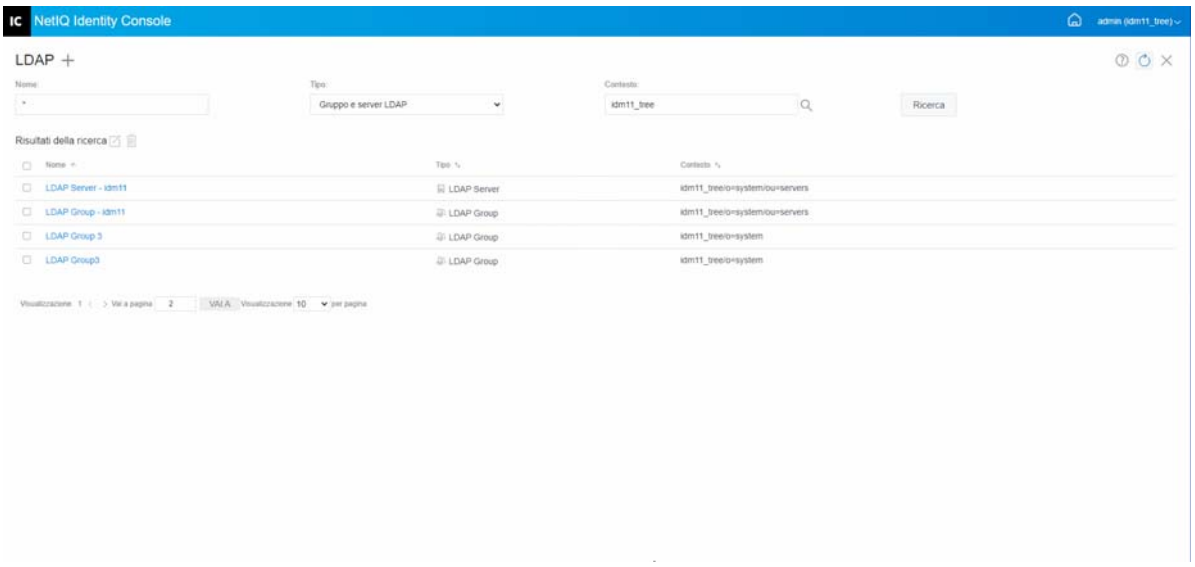


Eliminazione di oggetti LDAP

Per eliminare gli oggetti LDAP:

1. Fare clic sull'opzione **Configurazione LDAP** nella pagina di destinazione di Identity Console.
2. Specificare il nome, il tipo e il contesto dell'oggetto LDAP, quindi fare clic sul pulsante Ricerca.
3. Selezionare gli oggetti LDAP dall'elenco di ricerca e fare clic sull'icona 🗑.
4. Viene visualizzato un messaggio di conferma che indica che gli oggetti LDAP sono stati eliminati.

Figura 16-2 *Eliminazione di oggetti LDAP*

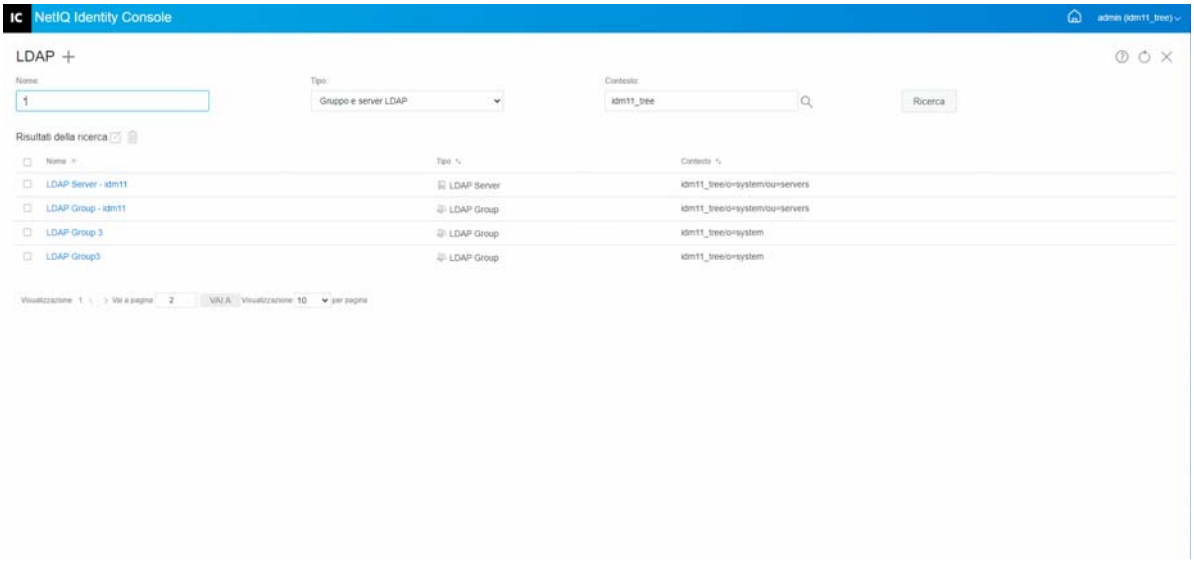


Modifica di oggetti LDAP

Per modificare gli oggetti LDAP:

1. Fare clic sull'opzione **Configurazione LDAP** nella pagina di destinazione di Identity Console.
2. Digitare il nome, il tipo e il contesto dell'oggetto LDAP, quindi fare clic sul pulsante Ricerca.
3. Selezionare l'oggetto LDAP dall'elenco di ricerca e fare clic sull'icona .
4. Modificare gli attributi e le informazioni per l'oggetto LDAP specifico in base alle esigenze, quindi fare clic sul pulsante Salva. Per ulteriori informazioni sugli attributi degli oggetti LDAP, vedere Configuring LDAP Server and LDAP Group Objects on Linux (Configurazione di oggetti Server LDAP e Gruppo LDAP su Linux) nella *NetIQ eDirectory Administration Guide* (Guida all'amministrazione di NetIQ eDirectory).
5. Viene visualizzato un messaggio di conferma che indica che l'oggetto LDAP è stato modificato.

Figura 16-3 *Modifica di oggetti LDAP*



17 Gestione dei certificati

Il server dei certificati NetIQ viene installato automaticamente al momento dell'installazione di eDirectory. Il server dei certificati fornisce servizi di crittografia asimmetrica integrati in modo nativo in eDirectory che consentono di creare, rilasciare e gestire certificati utente e certificati server. Tali servizi consentono di proteggere le trasmissioni di dati riservati tramite canali di comunicazione pubblici, ad esempio Internet.

Nota: se si desidera utilizzare il modulo Gestione certificati con Identity Console, è necessario eseguire l'upgrade del server eDirectory alla versione 9.2.4 HF2.

In Identity Console sono disponibili i seguenti task relativi alla gestione dei certificati:

Gestione dell'autorità di certificazione

Di default, durante il processo di installazione del server dei certificati NetIQ viene creata automaticamente l'Autorità di certificazione organizzativa (CA). Viene richiesto di specificare un nome dell'Autorità di certificazione organizzativa. Quando si fa clic su Fine, l'Autorità di certificazione organizzativa viene creata con i parametri di default e inserita nel container Sicurezza. Se si desidera un maggiore controllo sulla creazione dell'Autorità di certificazione organizzativa, è possibile creare l'Autorità di certificazione organizzativa manualmente utilizzando il portale di Identity Console. Inoltre, se si elimina l'Autorità di certificazione organizzativa, sarà necessario crearla nuovamente.

Tramite il modulo Autorità di certificazione è possibile eseguire i seguenti task:

Creazione di un oggetto Autorità di certificazione organizzativa

Per creare un oggetto Autorità di certificazione organizzativa, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.
2. Se non esiste alcun oggetto Autorità di certificazione organizzativa, viene visualizzata la finestra di dialogo Create an Organizational Certificate Authority Object (Creare un oggetto Autorità di certificazione organizzativa) e la procedura guidata corrispondente per la creazione dell'oggetto. Seguire le istruzioni visualizzate per creare l'oggetto.

   Nota: assicurarsi che il percorso del file CRL specificato qui sia in relazione al percorso di installazione di eDirectory.

   ---
3. Dopo aver creato l'autorità di certificazione, si consiglia di eseguire un backup della coppia di chiavi pubblica/privata della CA e di memorizzarlo in una posizione sicura. Per ulteriori informazioni, vedere "Backup dei certificati Autorità di certificazione organizzativa" a pagina 92.

Backup dei certificati Autorità di certificazione organizzativa

Si consiglia di eseguire il backup della chiave privata e dei certificati dell'Autorità di certificazione organizzativa per proteggersi nel caso in cui si verifichi un errore irreversibile del server host dell'Autorità di certificazione organizzativa. Se si verifica un errore, è possibile utilizzare il file di backup per ripristinare l'Autorità di certificazione organizzativa su qualsiasi server nell'albero.

Nota: la possibilità di eseguire il backup di un'Autorità di certificazione organizzativa è disponibile solo per le Autorità di certificazione organizzative create con Certificate Server versione 9.0 o successiva. Nelle versioni precedenti di Certificate Server, la chiave privata dell'Autorità di certificazione organizzativa veniva creata in modo da non essere esportabile.

Il file di backup contiene la chiave privata dell'Autorità di certificazione, il certificato autofirmato, il certificato a chiave pubblica e numerosi altri certificati necessari per il funzionamento. Queste informazioni vengono memorizzate nel formato PKCS #12 (noto anche come PFX).

È consigliabile eseguire il backup dell'Autorità di certificazione organizzativa quando funziona correttamente.

Per eseguire il backup dell'Autorità di certificazione organizzativa, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.
2. Fare clic sulla scheda **Certificati**.
3. Selezionare **Self Signed Certificate** (Certificato autofirmato) o **Public Key Certificate** (Certificato a chiave pubblica). Entrambi i certificati vengono scritti nel file durante l'operazione di backup. Si consiglia di selezionare separatamente il certificato autofirmato per RSA e i certificati ECDSA.
4. Fare clic sull'icona  .

5 Scegliere di esportare la chiave privata, specificare una password con 6 o più caratteri alfanumerici da utilizzare per la cifratura del file PFX e selezionare PKCS12 come formato di esportazione, quindi fare clic su **OK**.

6 Il file di backup cifrato viene scritto nell'ubicazione specificata ed è pronto per essere memorizzato in un'ubicazione sicura per l'utilizzo di emergenza.

Ripristino di un'Autorità di certificazione organizzativa

Se l'oggetto Autorità di certificazione organizzativa è stato eliminato o danneggiato o se il server host dell'Autorità di certificazione organizzativa ha riportato un errore irreversibile, è possibile ripristinare il funzionamento completo dell'Autorità di certificazione organizzativa utilizzando un file di backup creato come descritto in "Backup dei certificati Autorità di certificazione organizzativa" a pagina 92.

Per ripristinare l'Autorità di certificazione organizzativa, eseguire le operazioni riportate di seguito:

1 Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.

2 Fare clic su ↑↓ nella parte superiore della schermata (accanto a **Gestione autorità di certificazione**) per eliminare l'Autorità di certificazione organizzativa esistente.

3 Verrà richiesto di configurare una nuova Autorità di certificazione organizzativa. Viene visualizzata la finestra di dialogo Create an Organizational Certificate Authority Object (Creare un oggetto Autorità di certificazione organizzativa) e la procedura guidata corrispondente per la creazione dell'oggetto.

4 Nella finestra di dialogo di creazione, specificare il server che deve ospitare l'Autorità di certificazione organizzativa e il nome dell'oggetto Autorità di certificazione organizzativa.

5 Selezionare **Importa**.

6 Selezionare entrambi i certificati RSA e ECDSA. Certificate Server richiede che entrambi i certificati abbiano lo stesso nome del soggetto. Tuttavia, Certificate Server non supporta l'importazione di certificati Autorità di certificazione autofirmati esterni ma consente di importare certificati Autorità di certificazione subordinati.

7 Nelle schermate successive, individuare e selezionare il nome del file per RSA e ECDSA.

8 Immettere la password utilizzata per cifrare il file al momento del backup, quindi fare clic su **OK**.

9 La chiave privata e i certificati dell'Autorità di certificazione organizzativa sono stati ripristinati e l'Autorità di certificazione è completamente funzionante. È ora possibile memorizzare nuovamente il file per l'utilizzo futuro.

Convalida dei certificati dell'Autorità di certificazione organizzativa

Se si ritiene che un certificato presenti un problema o non sia più valido, è possibile convalidarlo facilmente utilizzando Identity Console. È possibile convalidare qualsiasi certificato nell'albero eDirectory, inclusi i certificati emessi da Autorità di certificazione esterne.

Il processo di convalida del certificato include diverse verifiche dei suoi dati e dei dati nella catena di certificati. Una catena di certificati è costituita da un certificato Autorità di certificazione radice e, facoltativamente, dai certificati di una o più Autorità di certificazione intermedie.

Per convalidare un certificato:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.
2. Fare clic sulla scheda **Certificati**.
3. Selezionare **Self Signed Certificate** (Certificato autofirmato) o **Public Key Certificate** (Certificato a chiave pubblica).
4. Fare clic su per convalidare i certificati Autorità di certificazione selezionati.

Sostituzione dei certificati dell'Autorità di certificazione organizzativa

Se per qualche motivo i certificati risultano danneggiati o non validi o se si desidera solo sostituire quelli esistenti, eseguire le operazioni riportate di seguito:

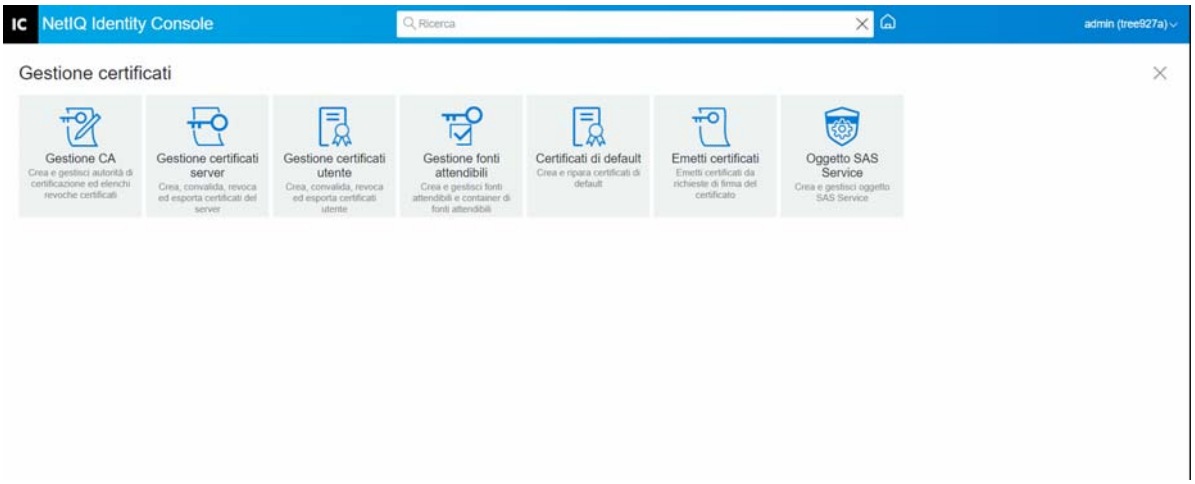
1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.
2. Fare clic sulla scheda **Certificati**.
3. Selezionare **Self Signed Certificate** (Certificato autofirmato) o **Public Key Certificate** (Certificato a chiave pubblica).
4. Fare clic su per sostituire il certificato Autorità di certificazione selezionato.
5. Importare un certificato Autorità di certificazione in formato `.pfx` o `.p12` e specificare una password per cifrare la chiave privata.
6. Fare clic su **OK**.

Revoca dei certificati dell'Autorità di certificazione organizzativa

Per revocare un certificato:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione CA** nella pagina di destinazione di Identity Console.
2. Fare clic sulla scheda **Certificati**.
3. Selezionare **Self Signed Certificate** (Certificato autofirmato) o **Public Key Certificate** (Certificato a chiave pubblica).
4. Fare clic sull'icona .
5. Leggere e valutare i rischi associati alla revoca dei certificati server.
6. Selezionare un motivo valido per la revoca dall'elenco a discesa, selezionare la data di fine validità e inserire eventuali commenti.
7. Fare clic su **OK** per completare la revoca.

Figura 17-1 *Gestione dell'autorità di certificazione*



Gestione dei certificati server

Tramite il modulo Gestione certificati server, l'amministratore può eseguire i seguenti task:

Creazione di oggetti Server Certificate

Per creare un oggetto Server Certificate, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona +.
3. Nella pagina **Crea certificato server**, specificare un **Soprannome**, il server e selezionare una delle seguenti opzioni:
   - **Standard (parametri di default):** consente di creare un oggetto Server Certificate di default di tipo RSA o ECDSA.
   - **Personalizzato (parametri specificati dall'utente):** consente di specificare i parametri personalizzati per l'oggetto Server Certificate.
   - **Importa (consente di importare un file PKCS12):** consente di importare un file PKCS12 in formato `.pfx` o `.p12`.
4. Dopo aver specificato i parametri, fare clic su **Avanti** per esaminare il riepilogo del certificato.
5. Nella schermata **Riepilogo**, fare clic su **OK** per creare un oggetto Server Certificate.

Esportazione di oggetti Server Certificate

Per esportare gli oggetti Server Certificate, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato server appropriato dall'elenco e fare clic sull'icona .
4. Nella schermata successiva, selezionare la casella di controllo **Esporta chiave privata** e specificare una password per proteggere la chiave privata. Confermare la password e selezionare il formato di esportazione.

   Nota: i certificati server possono essere esportati solo in formato PKCS12.
5. Fare clic su **OK** per esportare l'oggetto Server Certificate.

Convalida di oggetti Server Certificate

Per convalidare un oggetto Server Certificate, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato server appropriato dall'elenco e fare clic sull'icona .
4. Viene visualizzato un messaggio di conferma che indica che la convalida dell'oggetto Server Certificate è stata completata.

Sostituzione di un oggetto Server Certificate

Se per qualche motivo i certificati server risultano danneggiati o non validi o se si desidera solo sostituire quelli di default esistenti, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato server appropriato dall'elenco e fare clic sull'icona .
4. Leggere e valutare i rischi associati alla sostituzione dei certificati server e fare clic su **OK**.
5. Nella schermata successiva, individuare e selezionare il nuovo certificato server in formato `.pfx` o `.p12` e specificare una password.
6. Fare clic su **OK** per sostituire il certificato server.

Revoca di oggetti Server Certificate

Per revocare un oggetto Server Certificate, eseguire le operazioni riportate di seguito:

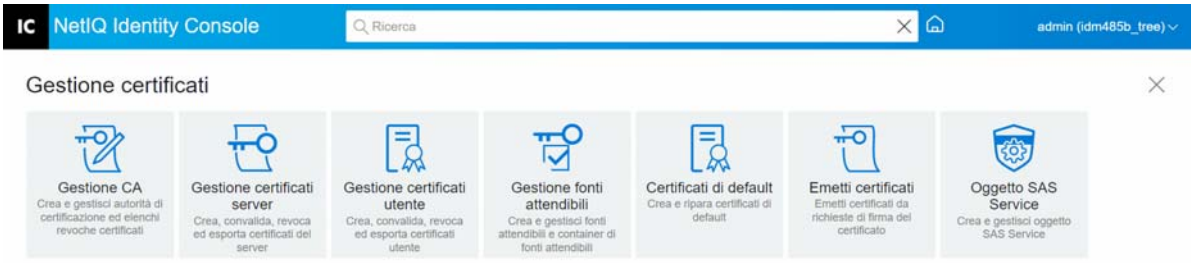
1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato server appropriato dall'elenco e fare clic sull'icona .
4. Leggere e valutare i rischi associati alla revoca dei certificati server e fare clic su **OK**.
5. Nella schermata successiva, selezionare un motivo valido per la revoca dall'elenco a discesa, selezionare la data di fine validità e inserire eventuali commenti.
6. Fare clic su **OK** per completare la revoca.

Eliminazione di oggetti Server Certificate

Per rimuovere gli oggetti Server Certificate, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati server** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato server appropriato dall'elenco e fare clic sull'icona .
4. Nella schermata successiva, fare clic su **OK**.
5. Viene visualizzato un messaggio di conferma che indica che l'eliminazione dell'oggetto Server Certificate è stata completata.

Figura 17-2 *Gestione dei certificati server*



Gestione dei certificati utente

Tramite il modulo Gestione certificati utente, è possibile eseguire il seguente task:

Creazione di oggetti certificato utente

Per creare un oggetto certificato utente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati utente** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona  .
3. Nella pagina **Crea certificato utente**, specificare un **Soprannome**, il server e selezionare una delle seguenti opzioni:
   - **Standard (parametri di default):** consente di creare un oggetto certificato utente di default di tipo RSA o ECDSA.
   - **Personalizzato (parametri specificati dall'utente):** consente di specificare i parametri personalizzati per l'oggetto certificato utente.
   - **Importa:** consente di importare un file di certificato in formato CERT o PKCS12.
4. Dopo aver specificato i parametri, fare clic su **Avanti** per esaminare il riepilogo del certificato.
5. Nella schermata **Riepilogo**, fare clic su **OK** per creare un oggetto certificato utente.

Esportazione di oggetti certificato utente

Per esportare gli oggetti certificato utente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati utente** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato utente appropriato dall'elenco e fare clic sull'icona  .
4. Nella schermata successiva, selezionare la casella di controllo **Esporta chiave privata** e specificare una password per proteggere la chiave privata. Confermare la password e selezionare il formato di esportazione.

   Nota: i certificati utente possono essere esportati solo in formato PKCS12.

5. Fare clic su **OK** per esportare l'oggetto certificato utente.

Convalida di oggetti certificato utente

Per convalidare un oggetto certificato utente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati utente** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato utente appropriato dall'elenco e fare clic sull'icona .
4. Viene visualizzato un messaggio di conferma che indica che la convalida dell'oggetto certificato utente è stata completata.

Revoca di oggetti certificato utente

Per revocare un oggetto certificato utente, eseguire le operazioni riportate di seguito:

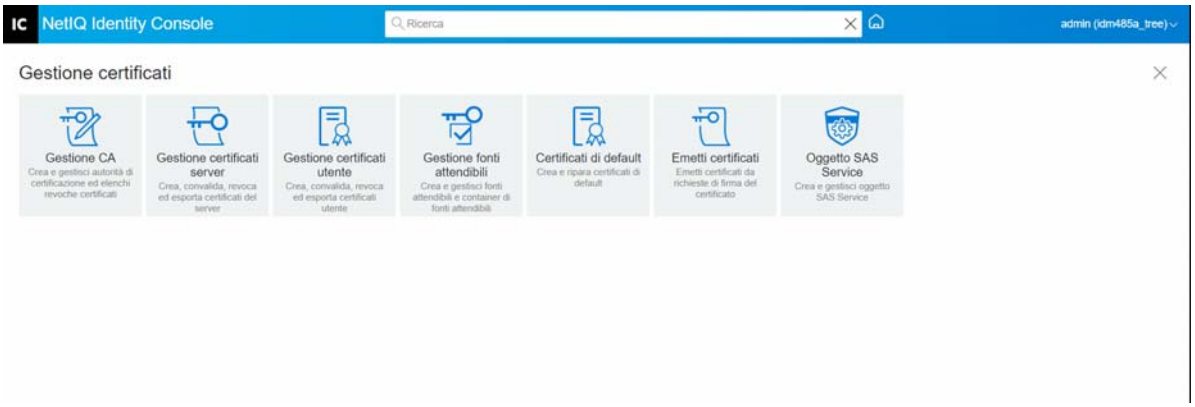
1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati utente** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato utente appropriato dall'elenco e fare clic sull'icona .
4. Leggere e valutare i rischi associati alla revoca dei certificati utente.
5. Selezionare un motivo valido per la revoca dall'elenco a discesa, selezionare la data di fine validità e inserire eventuali commenti.
6. Fare clic su **OK** per completare la revoca.

Eliminazione di oggetti certificato utente

Per rimuovere gli oggetti certificato utente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Gestione certificati utente** nella pagina di destinazione di Identity Console.
2. Selezionare il server appropriato dall'elenco a discesa.
3. Selezionare il certificato utente appropriato dall'elenco e fare clic sull'icona .
4. Nella schermata successiva, fare clic su **OK**.
5. Viene visualizzato un messaggio di conferma che indica che l'eliminazione dell'oggetto certificato utente è stata completata.

Figura 17-3 *Gestione dei certificati utente*



Gestione delle fonti attendibili e dei container

Una fonte attendibile fornisce la base di attendibilità nella crittografia asimmetrica. Le fonti attendibili vengono utilizzate per convalidare i certificati firmati da altre Autorità di certificazione. Le fonti attendibili abilitano la sicurezza per SSL, per la posta elettronica sicura e per l'autenticazione basata su certificati.

Tramite il modulo Gestione fonti attendibili è possibile eseguire i seguenti task:

- “Creazione di un container fonti attendibili” a pagina 100
- “Creazione di un oggetto certificato fonte attendibile” a pagina 101
- “Esportazione di oggetti certificato fonte attendibile” a pagina 101
- “Convalida di oggetti certificato fonte attendibile” a pagina 101
- “Eliminazione di oggetti certificato fonte attendibile” a pagina 102
- “Eliminazione di container fonti attendibili” a pagina 102

Creazione di un container fonti attendibili

Per creare un container fonti attendibili, eseguire i seguenti task:

1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default.
2. Fare clic sull'icona + per creare un nuovo container fonti attendibili.
3. Specificare un nome per il container fonti attendibili.
4. Utilizzare il selettore oggetti per individuare il container appropriato.
5. Fare clic sul pulsante **OK**.
6. Viene visualizzato un messaggio di conferma che indica che la creazione del container fonti attendibili è stata completata.

Creazione di un oggetto certificato fonte attendibile

Per creare un oggetto fonte attendibile, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default. Selezionare la casella di controllo **Fonte attendibile**.
2. Fare clic sull'icona + per creare un nuovo oggetto fonte attendibile.
3. Specificare un nome per l'oggetto fonte attendibile.
4. Selezionare il container fonti attendibili appropriato dall'elenco a discesa.
5. Individuare e selezionare il file di certificato appropriato in formato `.der` o `.b64`.

   Nota: in un oggetto Fonte attendibile può essere memorizzato qualsiasi tipo di certificato (certificati Autorità di certificazione, certificati Autorità di certificazione intermedi o certificati utente).
6. Fare clic sul pulsante **OK**.
7. Viene visualizzato un messaggio di conferma che indica che la creazione dell'oggetto fonte attendibile è stata completata.

Esportazione di oggetti certificato fonte attendibile

Per esportare gli oggetti certificato fonte attendibile, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default. Selezionare la casella di controllo **Fonte attendibile**.
2. Selezionare il certificato fonte attendibile appropriato dall'elenco e fare clic sull'icona .
3. Nella schermata successiva, selezionare la casella di controllo **Esporta chiave privata** e specificare una password per proteggere la chiave privata. Confermare la password e selezionare il formato di esportazione.

   Nota: i certificati fonte attendibile possono essere esportati solo in formato DER o BASE64.
4. Fare clic su **OK** per esportare l'oggetto certificato fonte attendibile.

Convalida di oggetti certificato fonte attendibile

Per convalidare gli oggetti certificato fonte attendibile, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default. Selezionare la casella di controllo **Fonte attendibile**.
2. Selezionare il certificato fonte attendibile appropriato dall'elenco e fare clic sull'icona .
3. Viene visualizzato un messaggio di conferma che indica che la convalida dell'oggetto certificato fonte attendibile è stata completata.

Eliminazione di oggetti certificato fonte attendibile

Per rimuovere gli oggetti certificato fonte attendibile, eseguire le operazioni riportate di seguito:

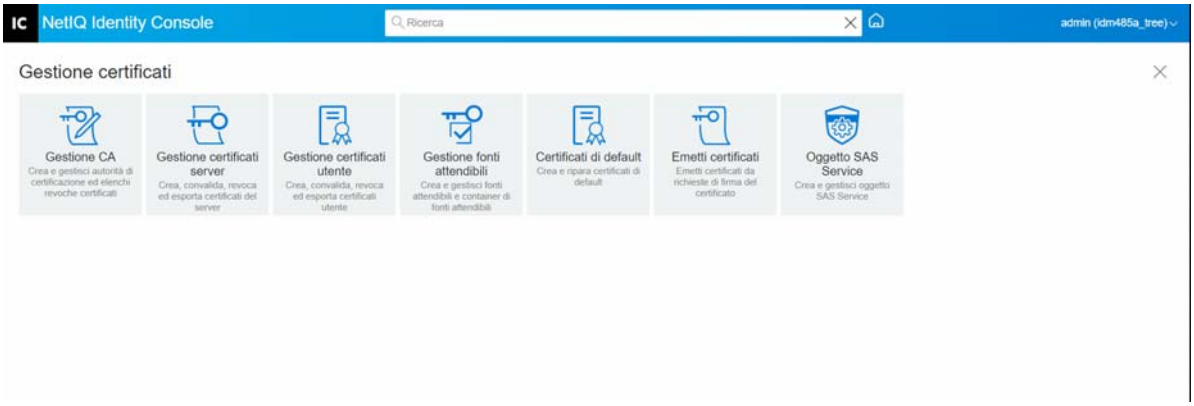
1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default. Selezionare la casella di controllo **Fonte attendibile**.
2. Selezionare il certificato fonte attendibile appropriato dall'elenco e fare clic sull'icona .
3. Fare clic su **OK** nella schermata di avviso.
4. Viene visualizzato un messaggio di conferma che indica che la rimozione dell'oggetto certificato fonte attendibile è stata completata.

Eliminazione di container fonti attendibili

Per rimuovere un container fonti attendibili, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione certificati** > **Gestione fonti attendibili** nella pagina di destinazione di Identity Console. La casella di controllo **Container fonti attendibili** è selezionata di default.
2. Selezionare il container fonti attendibili appropriato dall'elenco e fare clic sull'icona .
3. Fare clic su **OK** nella schermata di avviso.
4. Viene visualizzato un messaggio di conferma che indica che la rimozione del container fonti attendibili è stata completata.

Figura 17-4 *Gestione dei container fonti attendibili*



Creazione di oggetti Server Certificate di default

Durante l'installazione di Certificate Server vengono creati oggetti Server Certificate di default.

- CertificateDNS SSL - *nome_server*
- Un certificato per ciascun indirizzo IP configurato sul server (IPAG*xxx.xxx.xxx.xxx* - *nome_server*)
- Un certificato per ciascun nome DNS configurato sul server (DNSAG*www.esempio.com* - *nome_server*)

Nota: eDirectory non crea automaticamente CertificateIP SSL. CertificateDNS SSL contiene tutti gli IP elencati nel nome alternativo del soggetto. Quando si tenta di creare o riparare i certificati di default utilizzando Identity Console, il certificato CertificateIP SSL non viene creato o riparato di default. Tuttavia, nell'interfaccia del plug-in è disponibile una casella di controllo che è possibile selezionare per ignorare il comportamento di default e forzare la creazione/riparazione del certificato CertificateIP SSL.

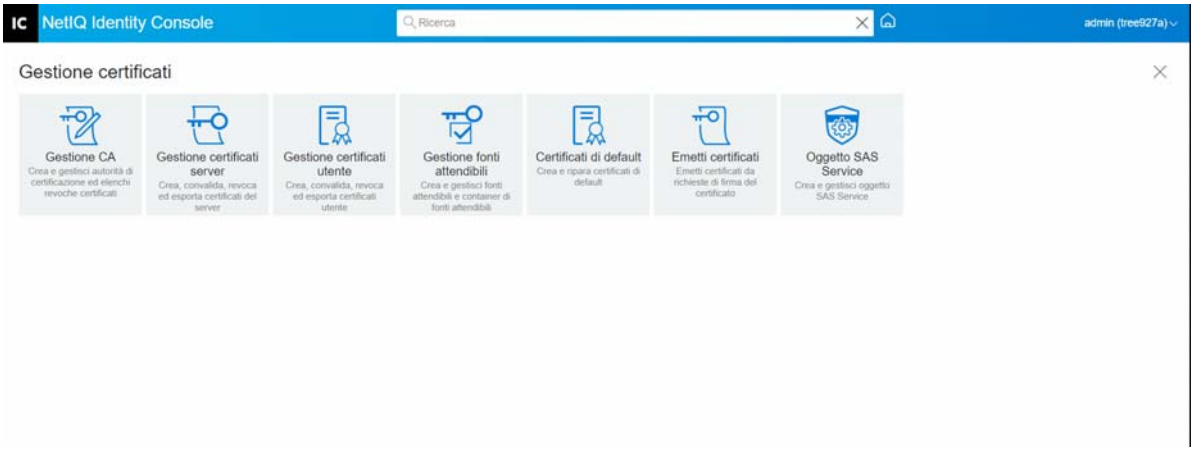
A partire dalla versione 9.0 di eDirectory, i certificati ECDSA vengono creati automaticamente se l'Autorità di certificazione organizzativa dispone di un certificato ECDSA.

Se per qualche motivo questi certificati risultano danneggiati o non validi o se si desidera solo sostituire quelli di default esistenti, è possibile utilizzare la Procedura guidata Create Default Server Certificates (Crea certificati server di default), come descritto nella procedura seguente:

1. Fare clic sulle opzioni di **Gestione certificati** > **Certificati di default** nella pagina di destinazione di Identity Console.
2. Selezionare il server o i server per cui si desidera creare i certificati di default, quindi fare clic su **Avanti**.
3. Selezionare Sì se si desidera sovrascrivere i certificati server di default esistenti o No se si desidera sovrascriverli solo se non sono validi.
4. (Solo server singolo) Se si desidera utilizzare l'indirizzo DNS esistente, selezionare tale opzione. Se si desidera utilizzare un indirizzo DNS diverso, selezionare tale opzione e specificare il nuovo indirizzo DNS.
5. (Solo server singolo) Se si desidera utilizzare l'indirizzo IP di default esistente, selezionare tale opzione. Se si desidera utilizzare un indirizzo IP diverso, selezionare tale opzione e specificare il nuovo indirizzo IP.
6. Fare clic su **Avanti**.
7. Rivedere la pagina di riepilogo e fare clic su **Fine**.

Se si desidera un maggiore controllo sulla creazione dell'oggetto Server Certificate, è possibile crearlo manualmente. Per ulteriori informazioni, vedere “Creazione di oggetti Server Certificate” a pagina 95.

Figura 17-5 *Creazione di oggetti Server Certificate di default*



Emissione di un certificato a chiave pubblica

L'Autorità di certificazione organizzativa funziona come una Autorità di certificazione esterna. Ciò significa che è in grado di emettere certificati dalle richieste di firma del certificato (CSR). È possibile emettere certificati utilizzando l'Autorità di certificazione organizzativa quando un utente invia una CSR da firmare. Pertanto, l'utente richiedente può importare il certificato emesso direttamente nell'applicazione che supporta le funzioni di cifratura.

Questo task consente di generare certificati per le applicazioni che supportano le funzioni di cifratura che non riconoscono gli oggetti Server Certificate.

Per emettere un certificato, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni di **Gestione certificati** > **Emetti certificati** nella pagina di destinazione di Identity Console.
2. Individuare e selezionare un file CSR.
3. Sotto Specifiche di utilizzo chiavi, selezionare il Tipo di chiave appropriato e l'Utilizzo chiave corrispondente. Le opzioni seguenti consentono di selezionare un tipo di chiave. A ciascun tipo di chiave sono associati valori predefiniti di utilizzo chiavi:
   - 3a **Non specificato:** Questa è l'opzione di default e non attiva alcun utilizzo chiave nel certificato.
   - 3b **Autorità di certificazione:** Questa opzione attiva l'utilizzo delle chiavi Firma del certificato e Firma CRL.
   - 3c **Cifratura:** Questa opzione attiva l'utilizzo della chiave Cifratura chiavi.
   - 3d **Firma:** Questa opzione attiva l'utilizzo della chiave Firma digitale.
   - 3e **SSL o TSL:** Questa opzione configura la chiave in modo che possa essere utilizzata nelle transazioni SSL o TLS.
   - 3f **Personalizzato:** Questa opzione consente di selezionare manualmente alcune o tutte le opzioni relative all'utilizzo delle chiavi.
   - 3g **Impostare l'estensione uso chiave su critico:** Selezionando tutti i tipi di chiave, fuorché Non specificato, è possibile contrassegnare l'estensione dell'utilizzo della chiave come critico. Qualsiasi estensione contrassegnata come critica deve essere riconosciuta dal software ricevente prima che il certificato possa essere utilizzato per qualsiasi scopo. L'impostazione di un'estensione come critica pone pertanto alcuni rischi, poiché non tutte le applicazioni sono in grado di utilizzare il certificato. Tuttavia, per le estensioni note, quale l'uso della chiave, il rischio è ridotto al minimo. In generale, se viene specificato l'uso della chiave, è consigliabile contrassegnare l'estensione come critica.
4. È possibile scegliere di codificare un'estensione **Utilizzo chiavi estese** nel certificato. Per attivare questa funzione, selezionare **Abilita utilizzo chiavi estese**:
   - 4a **Server:** Questa opzione attiva l'utilizzo della chiave estesa Autenticazione server.
   - 4b **Utente:** Questa opzione attiva l'utilizzo delle chiavi estese Autenticazione utente e Protezione e-mail.
   - 4c **Personalizzato:** Questa opzione consente di selezionare alcuni o tutti gli utilizzi delle chiavi estese.

4d **Qualsiasi:** Consente di utilizzare la chiave per qualsiasi utilizzo di chiave estesa.

4e **Impostare l'estensione di utilizzo chiavi estese su critico:** Qualsiasi estensione contrassegnata come critica deve essere riconosciuta dal software ricevente prima che il certificato possa essere utilizzato per qualsiasi scopo. L'impostazione di un'estensione come critica pone pertanto alcuni rischi, poiché non tutte le applicazioni sono in grado di utilizzare il certificato. Poiché molte applicazioni non riconoscono l'estensione Uso esteso delle chiavi, l'impostazione di questa estensione come critica comporta il rischio che il certificato non venga accettato da determinate applicazioni; è consigliabile pertanto procedere a tale impostazione solo se necessario.

5 Selezionare i **Vincoli di base** appropriati:

5a **Tipo di certificato:**

5a1 **Non specificato:** Selezionare questa opzione se non si desidera aggiungere un'estensione di vincoli di base al certificato.

5a2 **Autorità di certificazione:** Selezionare questa opzione per aggiungere un'estensione di vincoli di base Autorità di certificazione al certificato. È necessario selezionare questa opzione se il certificato è per l'Autorità di certificazione.

5a3 **Entità finale:** Selezionare questa opzione per aggiungere un'estensione di vincoli di base al certificato che indica che si tratta di un certificato di tipo Entità finale (diverso da Autorità di certificazione). Nota: se un certificato è di tipo Entità finale, è consigliabile impostare la lunghezza del percorso su Non specificata.

5b **Lunghezza percorso:**

5b1 **Non specificato:** Selezionare questa opzione se non si desidera specificare il numero di livelli di CA subordinate che è possibile creare nella CA corrente.

Nota: se un certificato è di tipo Entità finale, impostare la lunghezza del percorso solo su Non specificato.

5b2 **Specifico:** Selezionare questa opzione se si desidera specificare il numero di livelli di CA subordinate che è possibile create nella CA corrente. Fare clic sulle frecce verso l'alto e verso il basso per specificare la lunghezza del percorso.

Nota: Se il certificato che verrà creato è una CA subordinata, la lunghezza del percorso deve essere coerente con la CA superiore. Ad esempio, se la lunghezza del percorso della CA superiore è 3, la lunghezza del percorso della CA subordinata deve essere 2 o inferiore. Se la lunghezza del percorso della CA superiore non è specificata, anche la CA subordinata può avere una lunghezza di percorso non specificata o una qualsiasi lunghezza desiderata.

5c **Impostare l'estensione dei vincoli di base su critico:** In generale, l'estensione Vincoli di base deve essere impostata come critica per i certificati Autorità di certificazione. Qualsiasi estensione contrassegnata come critica deve essere riconosciuta dal software ricevente prima che il certificato possa essere utilizzato per qualsiasi scopo. L'impostazione di un'estensione come critica pone pertanto alcuni rischi, poiché non tutte le applicazioni sono in grado di utilizzare il certificato. Tuttavia, per le estensioni note, ad esempio Vincoli di base, il rischio è ridotto al minimo.

6 Specificare i seguenti parametri del certificato:

6a **Nome soggetto:** Visualizza il nome completo dell'albero eDirectory.

6b **Nome soggetto:** Visualizza il nome completo dell'albero eDirectory.

6c **Periodo di validità:** Utilizzare l'elenco a discesa per specificare il periodo di validità del certificato. L'intervallo è compreso tra 6 sei mesi e l'anno 2036 (una limitazione temporale basata sul valore della data a 32 bit). Se si seleziona l'opzione Date specifiche, sarà possibile modificare i campi Inizio validità e Data di scadenza per creare un periodo di validità personalizzato. La data massima selezionata deve rientrare nella data di validità della CA.

6c1 **Data di inizio validità:** Consente di visualizzare o modificare l'ora e la data di inizio di validità del certificato.

6c2 **Data di scadenza:** Consente di visualizzare o modificare l'ora e la data di scadenza della validità del certificato.

6d **Estensioni personalizzate:** Abilita Certificate Server al supporto di qualsiasi estensione standard o personalizzata che si desidera includere durante la creazione del certificato. È necessario che le estensioni siano state precedentemente create e memorizzate in un file (un'estensione per file). È necessario che le estensioni siano codificate ASN.1, come definito nella sezione 4.2 della specifica RFC 2459/3280 di IETF.

Se si desidera includere estensioni personalizzate nel certificato che si sta creando, fare clic su New (Nuova), quindi individuare un file contenente l'estensione personalizzata e aggiungerla al certificato. Ripetere questo processo per aggiungere più estensioni.

Per eliminare un file di estensioni personalizzate, selezionarlo e fare clic sull'icona  .

7 Selezionare il formato di certificato appropriato tra le seguenti opzioni:

7a **File in formato DER binario:** Questa opzione consente di salvare o esportare un certificato nel file indicato nel campo Nome file. Di default, il file di certificato viene esportato con un'estensione .DER nella radice dell'unità C: di una workstation Identity Console basata su Windows e nella home directory di una workstation Identity Console basata su Linux.

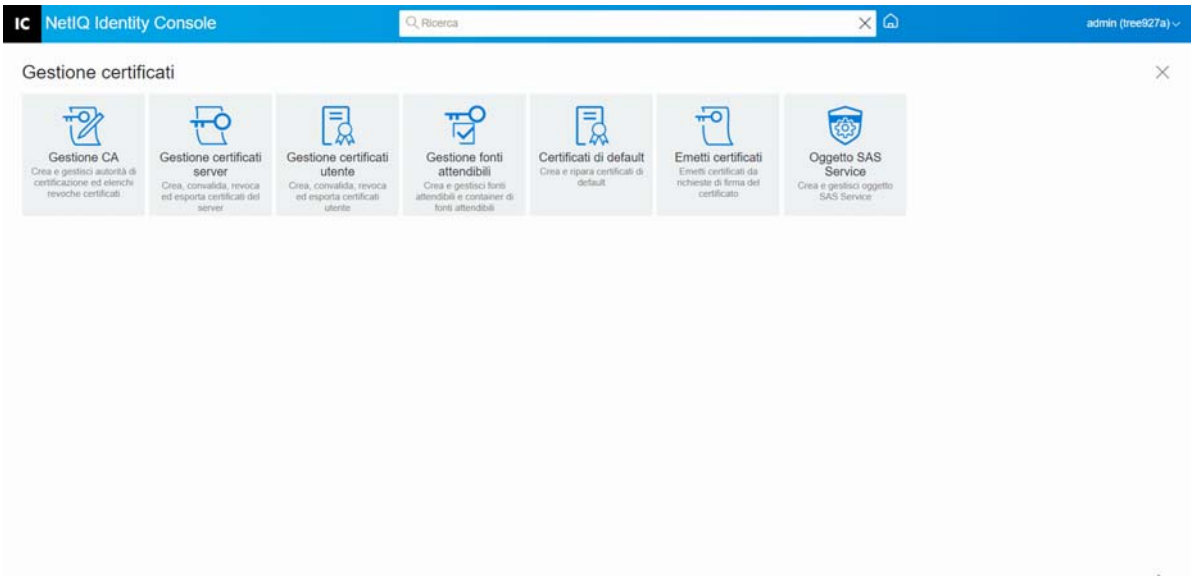
7b **File in formato Base64:** Questa opzione consente di salvare un file CSR o di esportare un certificato nel file indicato nel campo Nome file. Di default, i file del certificato e CSR vengono esportati con un'estensione .B64 nella radice dell'unità C: di una workstation Identity Console basata su Windows e nella home directory di una workstation Identity Console basata su Linux.

7c **File in formato CER:** Questa opzione consente di salvare un file CSR o di esportare un certificato nel file indicato nel campo Nome file. Di default, i file del certificato e CSR vengono esportati con un'estensione .CER nella radice dell'unità C: di una workstation Identity Console basata su Windows e nella home directory di una workstation Identity Console basata su Linux.

8 Esaminare il riepilogo del certificato nella schermata successiva e fare clic su **OK**.

9 Viene visualizzato un messaggio di conferma che indica che l'emissione del certificato è stata completata.

Figura 17-6 *Emissione di un certificato a chiave pubblica*



Gestione dell'oggetto SAS Service

L'oggetto SAS Service facilita la comunicazione tra un server e i relativi certificati. Se si rimuove un server da un albero eDirectory, è necessario eliminare anche l'oggetto SAS Service associato. Se si desidera inserire nuovamente il server nell'albero, è necessario creare l'oggetto SAS Service associato al server. In caso contrario, non sarà possibile creare nuovi certificati server.

L'oggetto SAS Service viene creato automaticamente come parte della verifica dello stato del server. Non dovrebbe essere necessario crearlo manualmente.

L'oggetto SAS Service può essere creato solo se nello stesso container dell'oggetto server non è presente un oggetto SAS Service con un nome corretto. Ad esempio, l'oggetto SAS Service del server GESTIONE deve essere denominato SAS Service - GESTIONE. L'utility aggiunge i puntatori DS dall'oggetto server all'oggetto SAS (e viceversa dall'oggetto SAS all'oggetto server) e imposta le voci ACL corrette nell'oggetto SAS Service.

Se esiste già un oggetto SAS Service con il nome corretto, non sarà possibile crearne uno nuovo. È possibile che i puntatori DS dell'oggetto SAS Service esistenti siano errati o mancanti oppure che gli elenchi ACL non siano corretti. In questo caso, è possibile eliminare l'oggetto SAS Service danneggiato e utilizzare il portale di Identity Console per crearne uno nuovo.

Creazione o eliminazione di un oggetto SAS Service

Per creare o eliminare un oggetto SAS Service, eseguire le operazioni riportate di seguito:

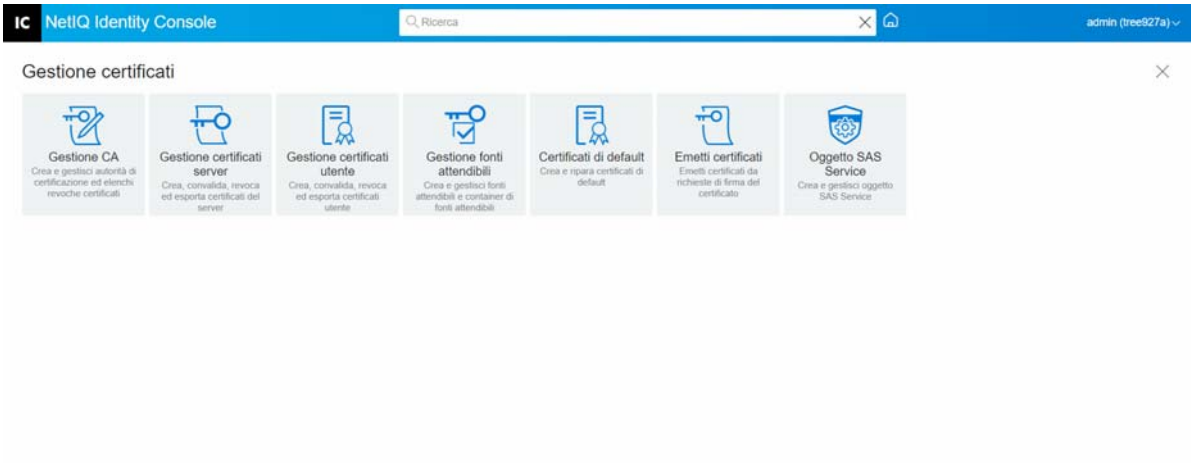
1. Fare clic sulle opzioni **Gestione certificati** > **Oggetto SAS Service** nella pagina di destinazione di Identity Console.
2. Se non è stato creato alcun oggetto SAS Service per un server esistente, fare clic sull'icona + per crearne uno nuovo.

3 Viene visualizzato un messaggio di conferma che indica che la creazione di un oggetto SAS Service è stata completata.

4 Per rimuovere un oggetto SAS Service, fare clic sull'icona .

5 Fare clic su **OK** nella schermata di conferma per rimuovere un oggetto SAS Service.

Figura 17-7 *Gestione degli oggetti SAS Service*



18 Gestione del framework di autenticazione

Tramite il modulo Autenticazione è possibile eseguire i seguenti task:

Gestione dei metodi e delle sequenze di login e post-login

NMAS include il supporto per diversi metodi di login e post-login di NetIQ e di sviluppatori di metodi di autenticazione di terze parti. Alcuni metodi richiedono hardware e software aggiuntivi. Assicurarsi di disporre dell'hardware e del software necessari per i metodi che verranno utilizzati.

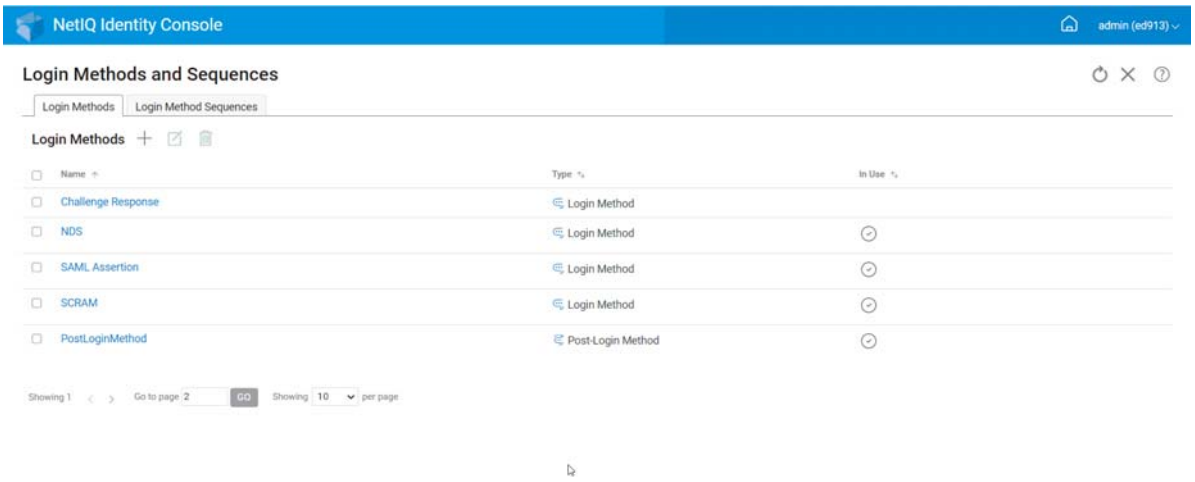
In questa sezione viene descritto come installare, impostare e configurare i metodi e le sequenze di login e post-login per NMAS.

Installazione di un metodo di login o post-login

Per installare un metodo di login, eseguire i seguenti task:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per installare un nuovo metodo di login.
3. Individuare e selezionare il file del metodo di login (.zip) che si desidera installare, quindi fare clic su **Avanti**.
4. Seguire la procedura guidata di installazione per completare il processo di installazione del metodo di login.

Figura 18-1 *Installazione di un nuovo metodo di login*

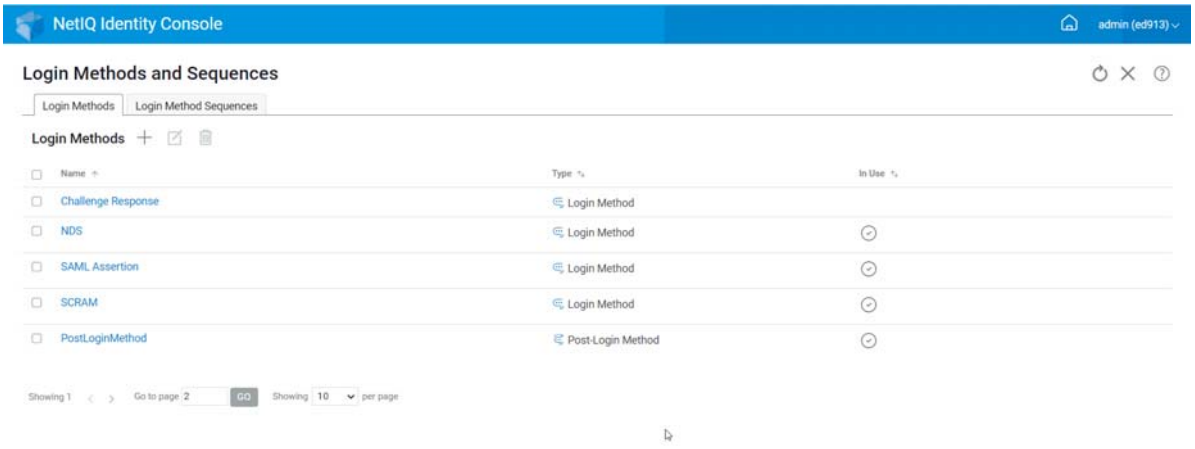


Aggiornamento di un metodo di login o post-login esistente

Per aggiornare un metodo di login esistente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare dall'elenco il metodo di login che si desidera aggiornare e fare clic sull'icona .
3. Individuare e selezionare il file del metodo di login (.zip) che si desidera aggiornare, quindi fare clic su **Avanti**.
4. Seguire la procedura guidata di aggiornamento per completare l'aggiornamento del metodo di login.

Figura 18-2 *Aggiornamento di un metodo di login esistente*

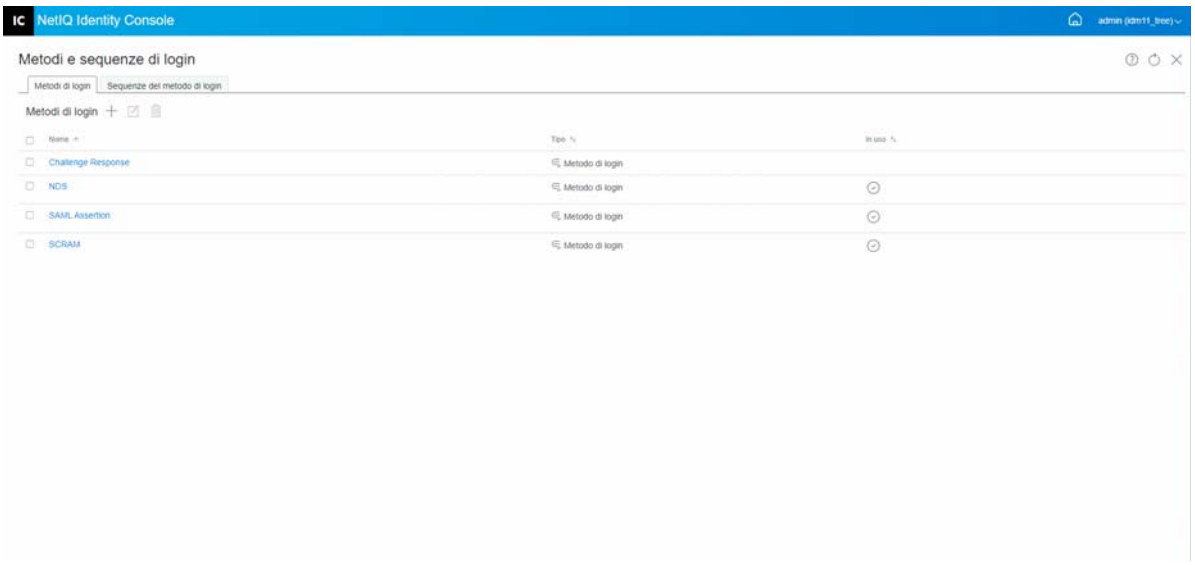


Disinstallazione dei metodi di login o post-login

Per disinstallare uno o più metodi di login o post-login, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare dall'elenco i metodi di login che si desidera disinstallare e fare clic sull'icona .
3. Nella schermata successiva, fare clic su **OK**.
4. Viene visualizzato un messaggio di conferma che indica che i metodi di login sono stati disinstallati.

Figura 18-3 *Disinstallazione di un metodo di login*



Creazione di una nuova sequenza del metodo di login

Una volta creati i vari metodi di login per il proprio ambiente, è possibile scegliere l'ordine in cui devono essere utilizzati. Per creare una nuova sequenza del metodo di login, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare la scheda **Sequenze del metodo di login**.
3. Fare clic sull'icona + per creare una nuova sequenza del metodo di login.
4. Specificare un **nome** e selezionare il **Tipo di sequenza**.
5. Selezionare i metodi di login e post-login desiderati dall'elenco dei metodi di login e post-login disponibili.

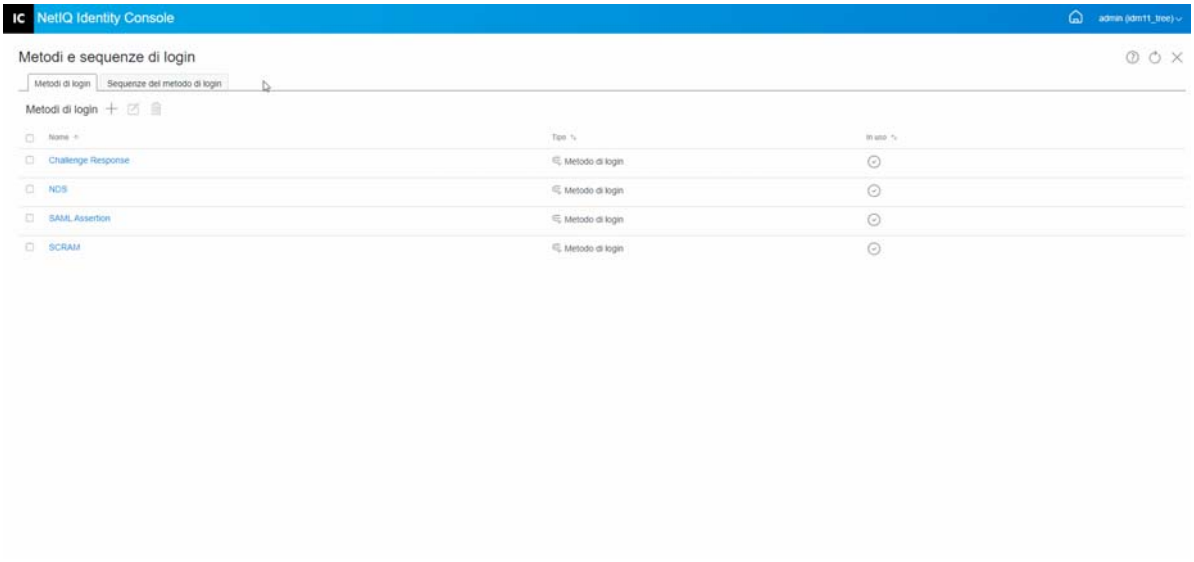
Nota: è possibile decidere l'ordine dei metodi di login facendo clic sulle frecce verso l'alto e verso il basso visibili sugli oggetti metodo di login.

---

6 Fare clic sul pulsante **Crea**.

7 Viene visualizzato un messaggio di conferma che indica che la creazione di una nuova sequenza del metodo di login è stata completata.

Figura 18-4 *Creazione di una sequenza del metodo di login*



Modifica di una sequenza del metodo di login

Per modificare una sequenza del metodo di login esistente, eseguire le operazioni riportate di seguito:

1 Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.

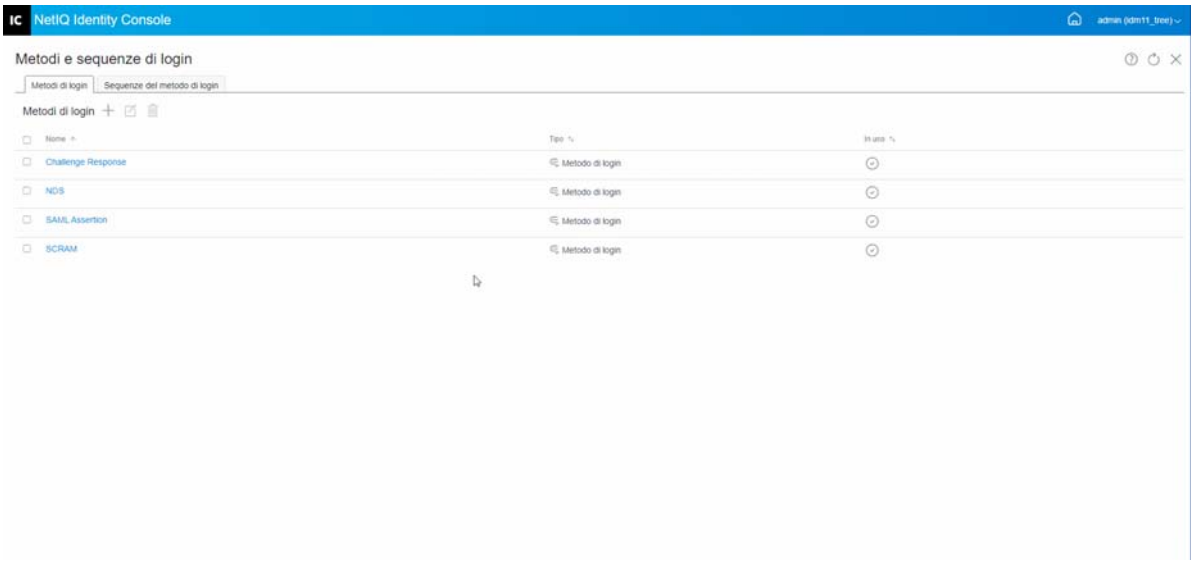
2 Selezionare la scheda **Sequenze del metodo di login**.

3 Fare clic sull'icona per modificare una sequenza del metodo di login esistente.

4 Apportare le modifiche necessarie nella pagina **Modifica sequenza del metodo di login** e fare clic su **Salva**.

5 Viene visualizzato un messaggio di conferma che indica che la modifica della sequenza del metodo di login è stata completata.

Figura 18-5 *Modifica di una sequenza del metodo di login*

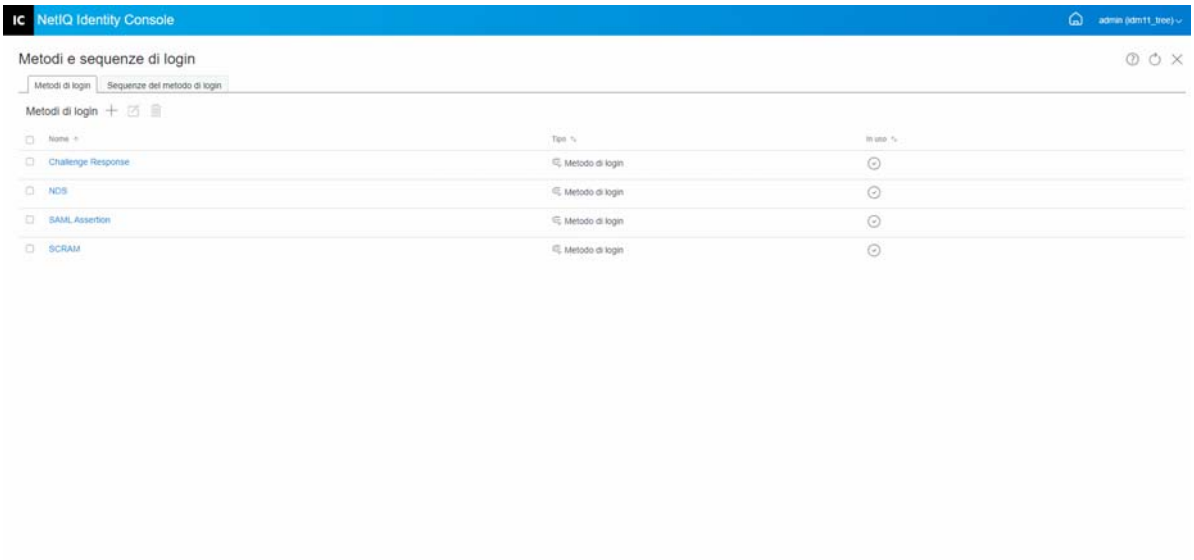


Autorizzazione o revoca dell'autorizzazione di una sequenza del metodo di login

Una sequenza del metodo di login deve essere autorizzata e impostata come default per poterla associare a utenti, container e partizioni. Per autorizzare una sequenza del metodo di login, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare la scheda **Sequenze del metodo di login**.
3. Selezionare la sequenza del metodo di login appropriata dall'elenco e fare clic sull'icona ⓥ.
4. Per revocare l'autorizzazione di una sequenza del metodo di login, selezionarla e fare clic sull'icona ⓧ.
5. In alternativa, è anche possibile autorizzare o revocare l'autorizzazione di una sequenza del metodo di login dal menu a discesa nella colonna **Autorizzato** dell'elenco Sequenze del metodo di login.

Figura 18-6 *Autorizzazione o revoca dell'autorizzazione di una sequenza del metodo di login*

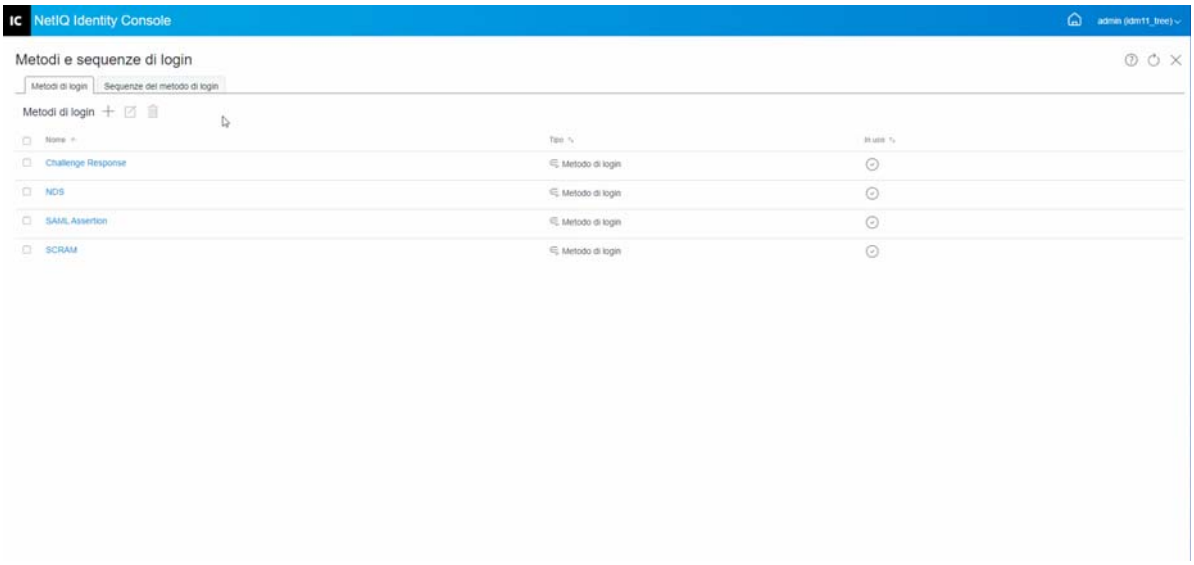


Impostazione di una sequenza del metodo di login di default

Per impostare una sequenza di login di default in modo che agli utenti non sia richiesto di specificare una sequenza di login durante il login:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare la scheda **Sequenze del metodo di login**.
3. Abilitare l'icona per impostare una sequenza del metodo di login autorizzata come default.

Figura 18-7 *Impostazione di una sequenza del metodo di login di default*

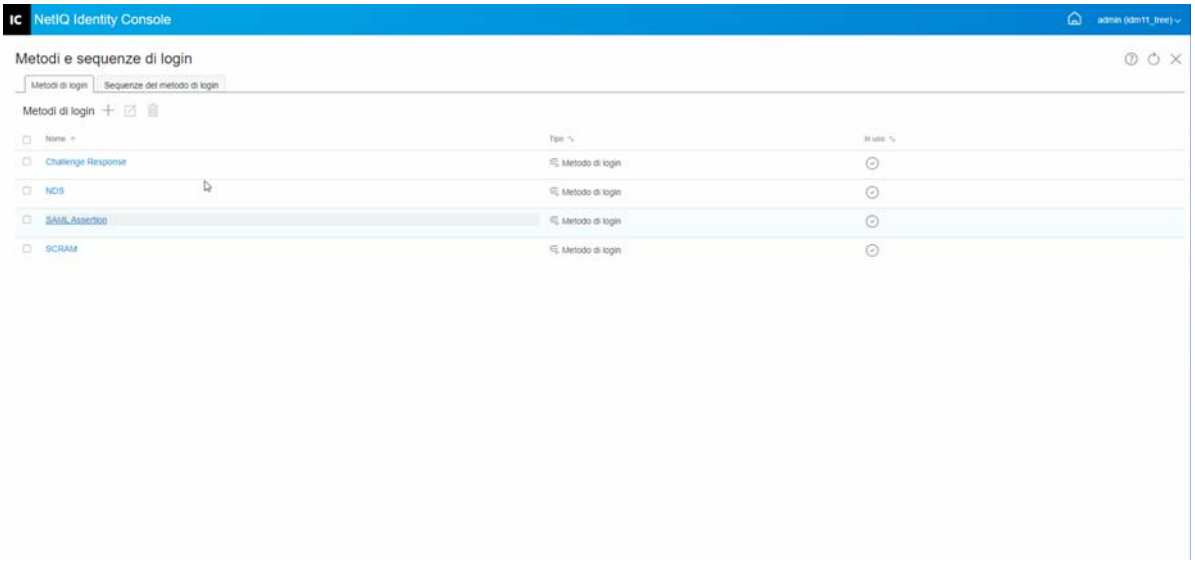


Eliminazione delle sequenze del metodo di login

Per eliminare una sequenza del metodo di login:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Metodi e sequenze di login** nella pagina di destinazione di Identity Console.
2. Selezionare la scheda **Sequenze del metodo di login**.
3. Selezionare la sequenza del metodo di login appropriata dall'elenco e fare clic sull'icona .
4. Fare clic su **OK** nella schermata di conferma successiva.

Figura 18-8 *Eliminazione di una sequenza del metodo di login*



Gestione delle policy password

Per policy password si intende una raccolta di regole definite dall'amministratore in cui sono specificati i criteri di creazione e sostituzione delle password degli utenti finali. NMAS consente di applicare policy password assegnate agli utenti in eDirectory. Le policy password possono includere anche la funzione di gestione autonoma Password dimenticata, che consente di ridurre le chiamate all'help desk per il recupero delle password. Un'altra funzione di gestione autonoma è la reimpostazione autonoma della password, che consente agli utenti di modificare le proprie password mentre visualizzano le regole specificate dall'amministratore nella policy password. Gli utenti possono accedere a queste funzioni mediante l'applicazione utente Identity Manager o Identity Console.

Tramite il modulo Policy password è possibile eseguire i seguenti task:

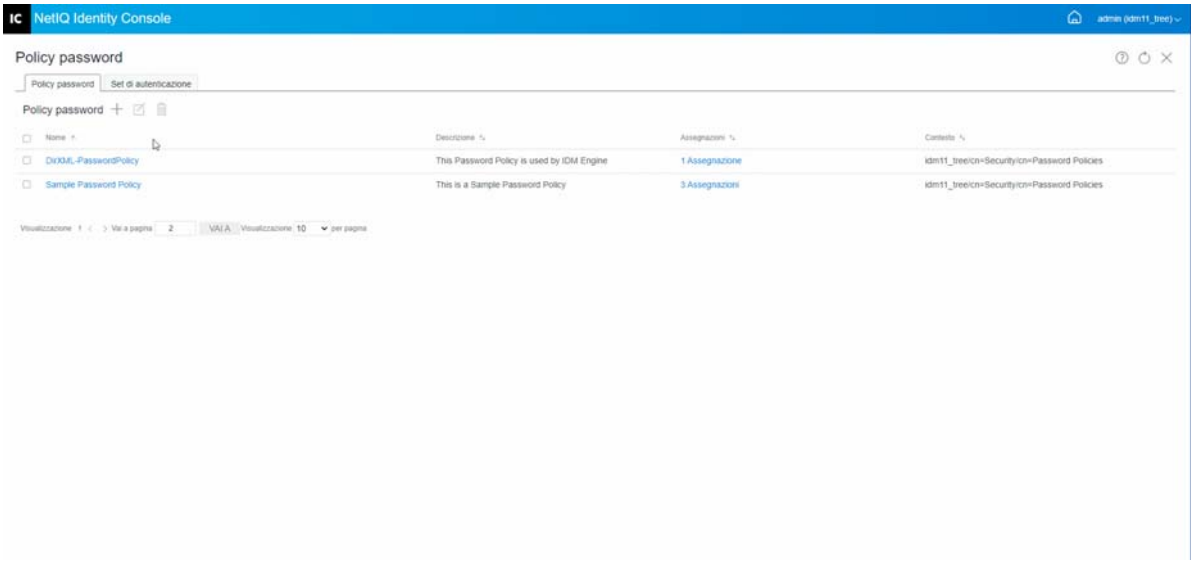
- “Creazione di una policy password con le impostazioni di default” a pagina 116
- “Creazione di una policy password con impostazioni personalizzate” a pagina 116
- “Modifica di una policy password” a pagina 120
- “Eliminazione delle policy password” a pagina 120

Creazione di una policy password con le impostazioni di default

Per creare una policy password, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Policy password** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per creare una nuova policy password.
3. Specificare il nome, il contesto, la descrizione e il messaggio di modifica della password nella schermata successiva.
4. Se si desidera creare una policy password con le impostazioni di default, selezionare la casella di controllo **Crea una nuova policy password basata sulle impostazioni di default** e fare clic su **Avanti** per visualizzare la pagina **Riepilogo**.
5. Verificare i dettagli nella pagina **Riepilogo** e fare clic su **Crea**.
6. Viene visualizzato un messaggio di conferma che indica che la creazione della policy password è stata completata.

Figura 18-9 *Creazione di una policy password con le impostazioni di default*



Creazione di una policy password con impostazioni personalizzate

Per creare una policy password con impostazioni personalizzate, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Policy password** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per creare una nuova policy password.
3. Specificare il nome, il contesto, la descrizione e il messaggio di modifica della password nella schermata successiva.
4. Se si desidera creare una policy password con impostazioni personalizzate, fare clic su **Avanti**.

5 Eseguire le seguenti azioni nella pagina **Configurazione**:

5a **Abilita Password universale:** l'abilitazione della Password universale per una policy consente di utilizzare le opzioni nella funzione Policy password. Tuttavia, prima di abilitare la Password universale per una policy, è necessario soddisfare i requisiti della Password universale per il proprio ambiente.

5b **Abilita regole password avanzate:** questa opzione abilita le regole per la password presenti in Regole password avanzate. Queste regole consentono di proteggere il proprio ambiente fornendo il controllo su criteri come la durata e il contenuto di una password, ad esempio una combinazione di lettere, numeri, lettere maiuscole o minuscole e caratteri speciali. È possibile escludere le password ritenute non sicure, ad esempio il nome della propria azienda.

5c **Sincronizzazione password:** queste opzioni determinano il modo in cui la Password universale viene sincronizzata in eDirectory con altri tipi di password di Identity Vault. La Sincronizzazione password contiene le seguenti opzioni:

5c1 **Rimuovi password NDS durante l'impostazione della password:** se questa opzione è selezionata, la password NDS viene disabilitata quando viene impostata la Password universale. Gli utenti non saranno in grado di utilizzare i metodi o le utility precedenti che eseguono il login direttamente con la password NDS invece di comunicare con NMAS. Se questa opzione è impostata, l'opzione successiva **Sincronizza password NDS durante l'impostazione della password** sarà disabilitata di default.

5c2 **Sincronizza password NDS durante l'impostazione della password:** se si seleziona questa opzione, l'impostazione della Password universale in applicazioni quali Identity Console modifica anche la password NDS.

5c3 **Sincronizza password semplice durante l'impostazione della password:** questa opzione garantisce la compatibilità con NetIQ e con i client di terze parti che utilizzano la password semplice e il provisioning utente.

5c4 **Sincronizza password di distribuzione durante l'impostazione della password:**

questa opzione determina la capacità del motore di metadirectory di recuperare o impostare una Password universale dell'utente in eDirectory.

5d **Recupero Password universale:** Sono disponibili le seguenti opzioni:

5d1 **Consenti all'utente di recuperare la password:** consente all'agente utente di recuperare la password. Questa opzione determina se la funzione di gestione autonoma Password dimenticata può eseguire il recupero di una password per conto dell'utente, in modo che questa venga inviata all'utente tramite e-mail. Se non si seleziona questa opzione, la funzione corrispondente è disattivata nella scheda Password dimenticata nella policy password.

5d2 **Consenti all'amministratore di recuperare le password:** selezionare questa casella se si dispone di un servizio specifico che richiede tale funzione. In Identity Manager non è necessario che gli amministratori recuperino le password. Tuttavia, alcuni servizi di terze parti potrebbero sfruttare questa opzione.

5d3 **Consenti il recupero delle password da parte di quanto segue:** selezionare l'utente appropriato che può recuperare la password facendo clic sull'icona +.

5e Autenticazione:

5e1 Verificare che le password esistenti siano conformi alla policy password (la verifica ha luogo durante il login): questa opzione risulta utile nel caso si voglia essere certi che le password esistenti siano conformi alle regole nuove o modificate quando si distribuisce una nuova policy password o si modificano le Regole password avanzate per una policy esistente.

Se si seleziona questa opzione, quando gli utenti eseguono il login, le password esistenti vengono analizzate per verificare che siano conformi alle Regole password avanzate nella policy password nuova o modificata. Se la password esistente non è conforme, all'utente verrà richiesto di cambiarla.

Al termine, fare clic su **Avanti**.

6 Le **Regole password avanzate** aiutano a proteggere l'ambiente fornendo il controllo su informazioni della password quali durata, frequenza di modifica e contenuto.

I caratteri speciali sono i caratteri non numerici (0-9) e non alfabetici.

Eseguire le seguenti azioni nella pagina Regole password avanzate:

6a È possibile gestire le impostazioni di sintassi delle password utilizzando la policy di complessità Microsoft (precedente a Microsoft Windows Server 2008), la policy password di Microsoft Server 2008 o la sintassi Novell.

6b Specificare le opzioni desiderate per Modifica password, Durata password, Lunghezza e composizione della password ed Esclusioni password nella procedura guidata, quindi fare clic su **Avanti**.

7 È possibile ridurre i costi di help desk impostando la funzione di gestione autonoma **Password dimenticata** per gli utenti che hanno dimenticato la password. Queste funzioni di gestione autonoma sono disponibili per gli utenti tramite il portale di Identity Console. Eseguire le seguenti azioni nella pagina Password dimenticata:

Nota: se si abilita la funzione Password dimenticata, è necessario anche specificare se è necessario un set di autenticazione per assistere l'utente nell'esecuzione del login.

7a Set di autenticazione: se si utilizzano i set di autenticazione, gli utenti non potranno utilizzare la funzione di gestione autonoma Password dimenticata finché non risponderanno alle domande del set di autenticazione. Per assicurarsi che agli utenti venga richiesto di immettere tali informazioni tramite il portale di Identity Console, selezionare l'opzione **Richiedi set di autenticazione**.

7b Azione: le opzioni disponibili in questa scheda consentono all'utente di reimpostare la password utilizzando i set di autenticazione e la Password universale, di abilitare l'invio tramite e-mail della password corrente o del suggerimento per la password e di visualizzare l'opzione di suggerimento per la password.

7c Autentica: selezionare la casella **Forza l'utente a configurare le domande di autenticazione e/o il suggerimento al momento dell'autenticazione** per fare in modo che agli utenti venga richiesto di specificare i set di autenticazione o il suggerimento per la password.

Al termine, fare clic su **Avanti**.

8 La policy non viene applicata fino a quando non viene assegnata a uno o più oggetti. Si consiglia di assegnare le policy al livello più alto possibile nell'albero, in modo da semplificarne la gestione. È possibile assegnare le policy password ai seguenti oggetti:

8a **Oggetto Policy login:** si consiglia di creare una policy password di default per tutti gli utenti dell'albero e assegnarla all'oggetto Policy login presente nel container di sicurezza.

8b **Un container che rappresenta la radice di una partizione:** se si assegna una policy a un container che rappresenta la radice di una partizione, tutti gli utenti di tale partizione, inclusi gli utenti nei sotto container, ereditano l'assegnazione delle policy.

8c **Un container che non rappresenta la radice di una partizione:** se si assegna una policy a un container che non rappresenta la radice di una partizione, solo gli utenti presenti in tale container ereditano l'assegnazione della policy. Gli utenti presenti nei sotto container non ereditano la policy.

Per applicare la policy a tutti gli utenti al di sotto di un container che non è una radice di una partizione, assegnare la policy singolarmente a ciascun sotto container.

8d **Un utente:** è possibile assegnare una policy a uno o più utenti.

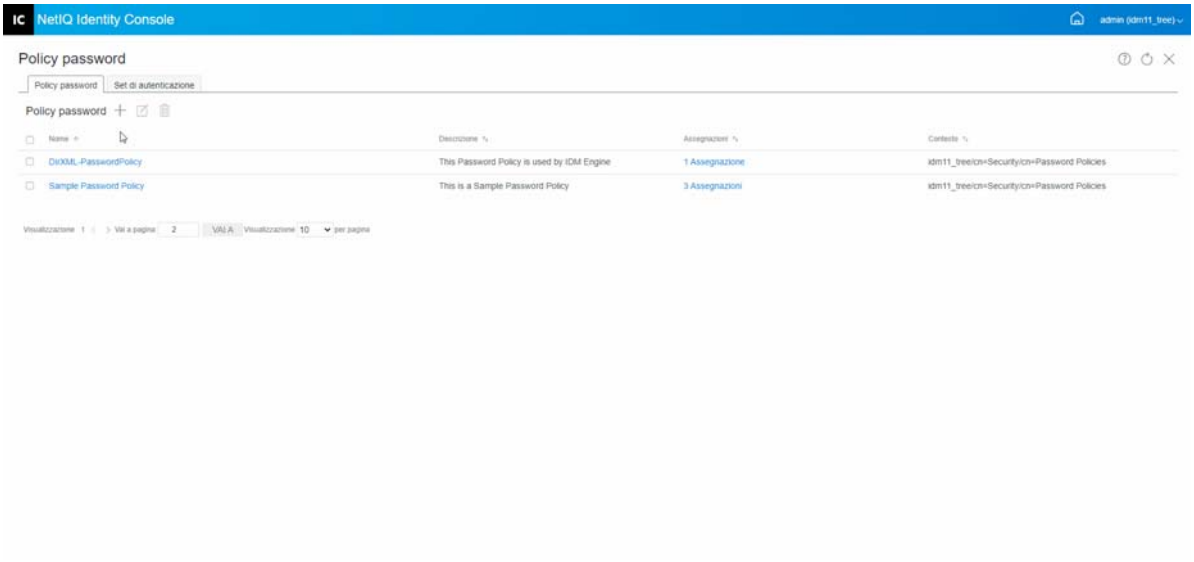
Per assegnare una policy, fare clic sull'icona +. Individuare e selezionare l'oggetto appropriato a cui assegnare la policy password.

Se si desidera rimuovere un'associazione di policy, selezionarla dall'elenco e fare clic sull'icona .

9 Verificare i dettagli nella pagina **Riepilogo** e fare clic su **Crea**.

10 Viene visualizzato un messaggio di conferma che indica che la creazione della policy password è stata completata.

Figura 18-10 *Creazione di una policy password con impostazioni personalizzate*

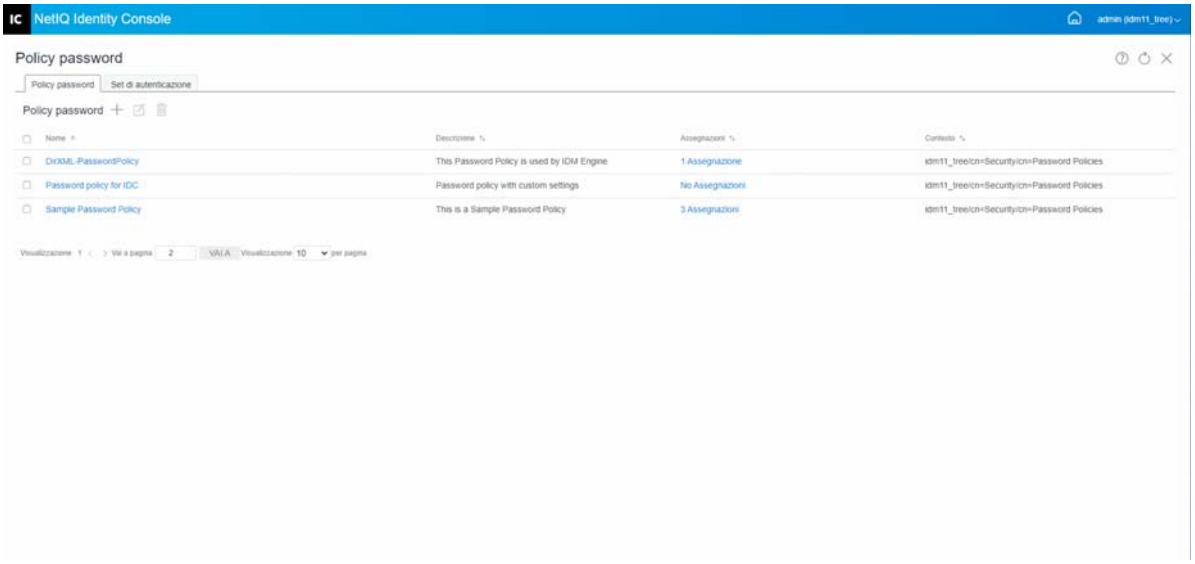


Modifica di una policy password

Per modificare una policy password esistente, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Policy password** nella pagina di destinazione di Identity Console.
2. Selezionare la policy password appropriata dall'elenco e fare clic sull'icona .
3. Apportare le modifiche necessarie nella pagina **Modifica policy password** e fare clic su **Salva**.

Figura 18-11 *Modifica di una policy password*

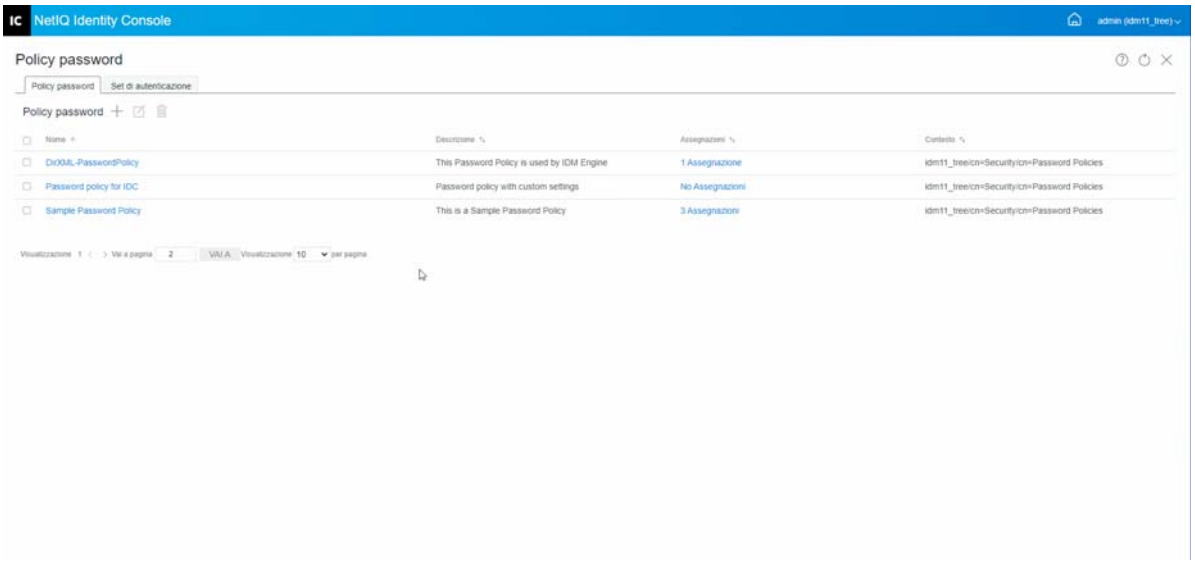


Eliminazione delle policy password

Per eliminare le policy password, eseguire le operazioni riportate di seguito:

1. Fare clic sulle opzioni **Gestione autenticazione** > **Policy password** nella pagina di destinazione di Identity Console.
2. Selezionare le policy password appropriate dall'elenco e fare clic sull'icona .
3. Nella schermata di avviso successiva, fare clic su **OK**.
4. Viene visualizzato un messaggio di conferma che indica che le policy password sono state eliminate.

Figura 18-12 *Eliminazione di una policy password*



Gestione dei set di autenticazione

Un set di autenticazione consiste in una o più domande a cui un utente risponde per convalidare la propria identità. Un set di autenticazione fa parte della funzione di assegnazione automatica delle password.

Se un utente ha problemi a ricordare o utilizzare la propria password, può utilizzare la funzione di assegnazione automatica delle password invece di chiamare l'help desk. Un set di autenticazione consente a un utente di convalidare la propria identità e di ricevere un suggerimento o una password tramite e-mail oppure di reimpostare una password tramite un browser Web.

È possibile consentire agli utenti di creare le proprie domande e fornire le risposte oppure chiedere loro di rispondere alle domande create dall'amministratore.

La pagina Set di autenticazione consente di cercare i set di autenticazione esistenti, di crearne di nuovi e di modificare quelli esistenti.

- “Creazione di un nuovo set di autenticazione” a pagina 121
- “Modifica di un set di autenticazione” a pagina 122
- “Eliminazione dei set di autenticazione” a pagina 123

Creazione di un nuovo set di autenticazione

Per creare un nuovo set di autenticazione, eseguire le operazioni riportate di seguito:

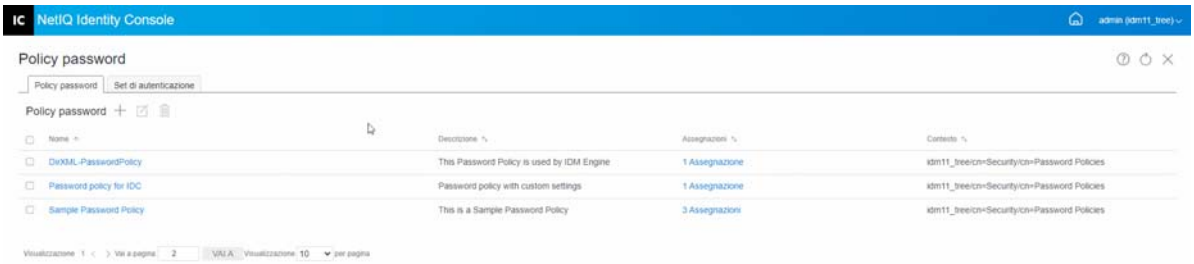
1. Fare clic su **Gestione autenticazione** > **Policy password** > **Set di autenticazione** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per creare un nuovo set di autenticazione.
3. Specificare un nome per l'oggetto set di autenticazione e selezionare il container o il sotto container in cui deve essere creato.

4 Creare un nuovo gruppo di domande da porre per il recupero della password dell'utente. È inoltre possibile effettuare una selezione dal set di domande casuali esistente.

5 Impostare il numero di domande da porre e fare clic su **Crea**.

6 Viene visualizzato un messaggio di conferma che indica che la creazione del set di autenticazione è stata completata.

Figura 18-13 *Creazione di un set di autenticazione*



Modifica di un set di autenticazione

Per modificare un set di autenticazione esistente, eseguire le operazioni riportate di seguito:

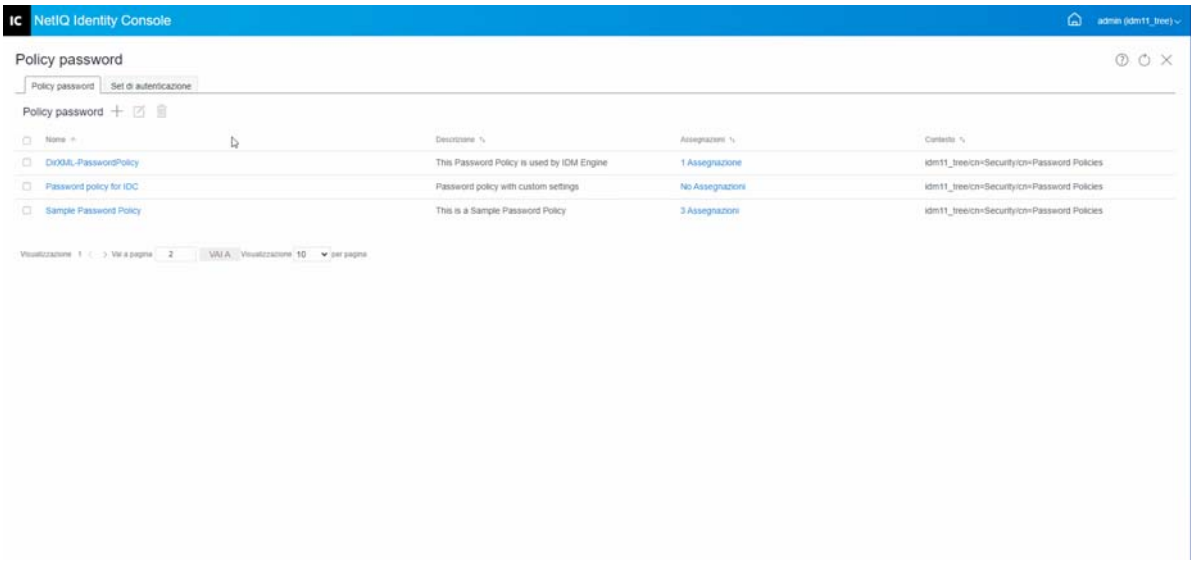
1 Fare clic su **Gestione autenticazione** > **Policy password** > **Set di autenticazione** nella pagina di destinazione di Identity Console.

2 Selezionare il set di autenticazione appropriato dall'elenco e fare clic sull'icona .

3 Apportare le modifiche necessarie nella pagina Modifica set di autenticazione e fare clic su **Salva**.

4 Viene visualizzato un messaggio di conferma che indica che la modifica del set di autenticazione è stata completata.

Figura 18-14 *Modifica di un set di autenticazione*

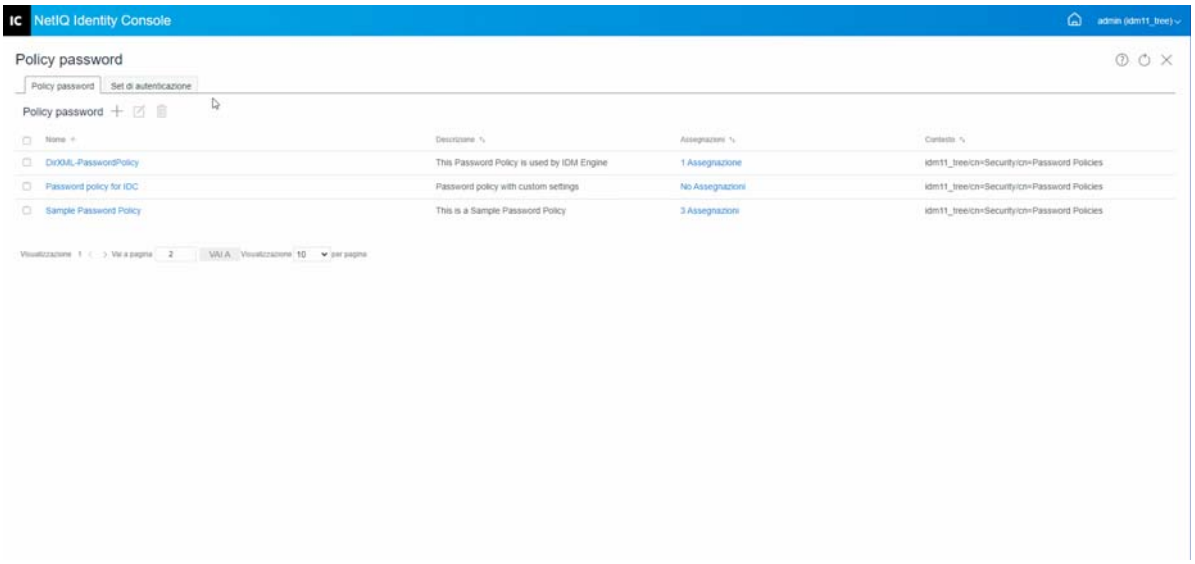


Eliminazione dei set di autenticazione

Per eliminare i set di autenticazione, eseguire le operazioni riportate di seguito:

1. Fare clic su **Gestione autenticazione** > **Policy password** > **Set di autenticazione** nella pagina di destinazione di Identity Console.
2. Selezionare il set di autenticazione desiderato dall'elenco e fare clic sull'icona .
3. Fare clic su **OK** nella schermata di conferma.
4. Viene visualizzato un messaggio di conferma che indica che l'eliminazione del set di autenticazione è stata completata.

Figura 18-15 *Eliminazione di un set di autenticazione*



19 Gestione di oggetti gruppo SNMP

SNMP (Simple Network Management Protocol) è il protocollo Internet standard per le operazioni e la manutenzione, dedicato allo scambio di informazioni di gestione tra le applicazioni della console di gestione e i dispositivi gestiti.

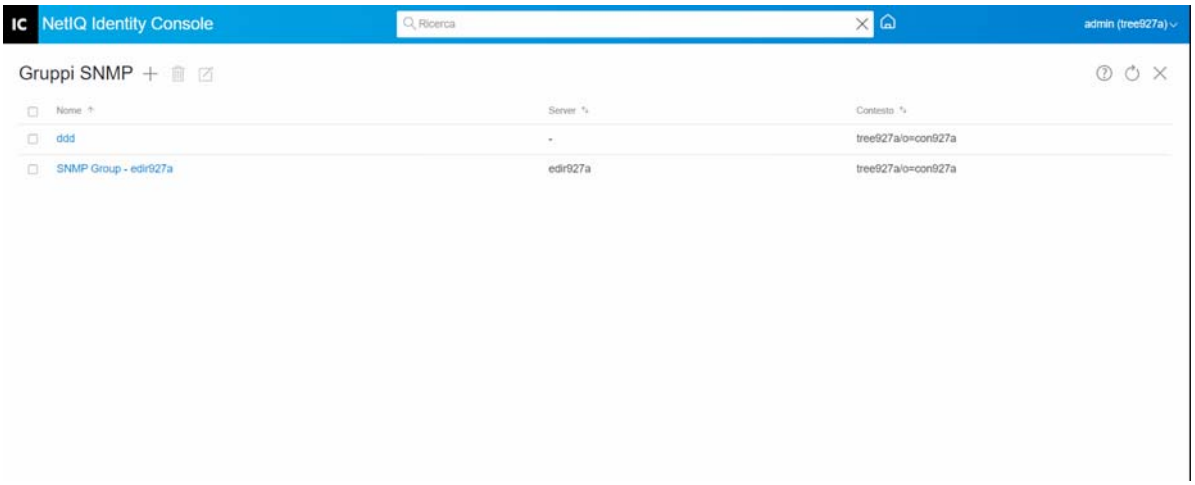
Tramite il modulo SNMP è possibile eseguire i seguenti task:

Creazione di oggetti gruppo SNMP

Per creare oggetti gruppo SNMP, eseguire le operazioni riportate di seguito:

1. Fare clic sul modulo **SNMP** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per creare un nuovo oggetto gruppo SNMP.
3. Specificare il nome e selezionare il contesto per creare un nuovo oggetto gruppo SNMP.
4. Fare clic sul pulsante **Crea**.
5. Viene visualizzato un messaggio che conferma che la creazione dell'oggetto gruppo SNMP è stata completata.

Figura 19-1 *Creazione di oggetti gruppo SNMP*

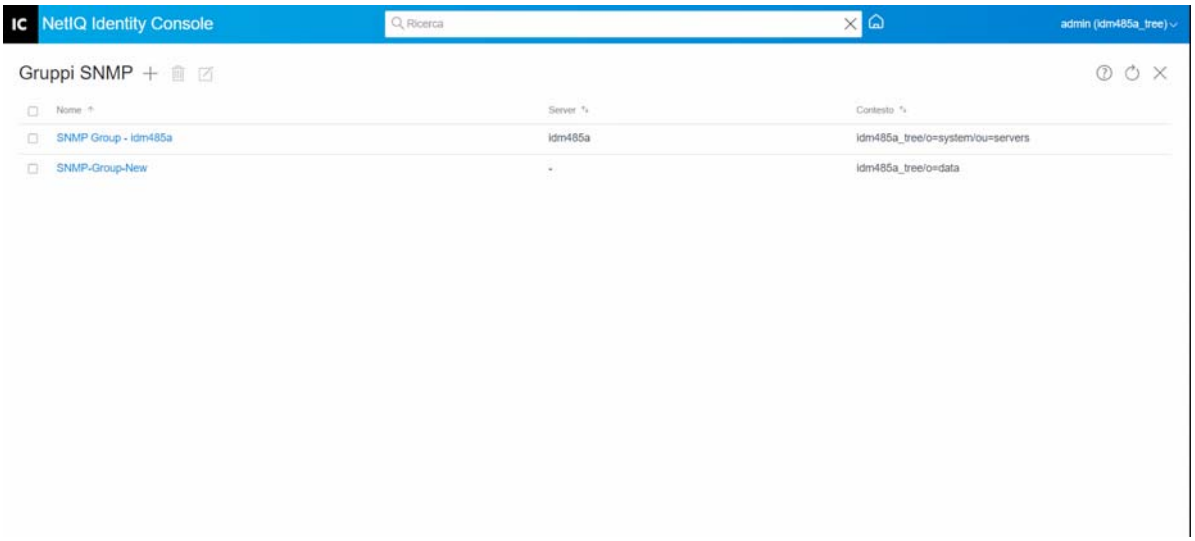


Modifica di oggetti gruppo SNMP

Per modificare oggetti gruppo SNMP, eseguire le operazioni riportate di seguito:

1. Fare clic sul modulo **SNMP** nella pagina di destinazione di Identity Console.
2. Selezionare l'oggetto gruppo SNMP che si desidera modificare e fare clic sull'icona .
3. Modificare i parametri configurabili nella pagina **Generale**/**Trap**.
4. Al termine, fare clic sul pulsante **Salva**.
5. Viene visualizzato un messaggio che conferma che la modifica dell'oggetto gruppo SNMP è stata completata.

Figura 19-2 *Modifica di oggetti gruppo SNMP*

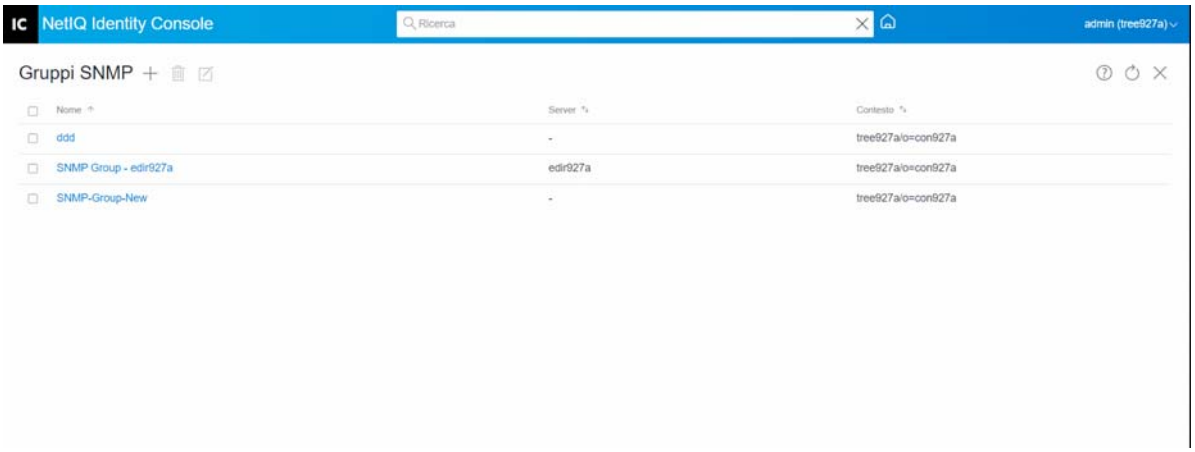


Eliminazione di oggetti gruppo SNMP

Per eliminare oggetti gruppo SNMP, eseguire le operazioni riportate di seguito:

1. Fare clic sul modulo **SNMP** nella pagina di destinazione di Identity Console.
2. Selezionare l'oggetto gruppo SNMP che si desidera modificare e fare clic sull'icona .
3. Fare clic su **OK** nella schermata successiva.
4. Viene visualizzato un messaggio che conferma che l'eliminazione dell'oggetto gruppo SNMP è stata completata.

Figura 19-3 *Eliminazione di oggetti gruppo SNMP*



20 Gestione di Enhanced Background Authentication

Per accedere a eDirectory dal plug-in EBA di Identity Console, è necessario che nell'albero sia presente un server abilitato per EBA con un file eba.p12 valido. Per ulteriori informazioni su come abilitare EBA nell'albero eDirectory, vedere Enabling EBA on an eDirectory Tree (Abilitazione di EBA in un albero eDirectory) nella *NetIQ eDirectory Administration Guide* (Guida all'amministrazione di NetIQ eDirectory).

Nota: se si desidera utilizzare il modulo EBA con Identity Console, è necessario eseguire l'upgrade del server eDirectory alla versione 9.2.4 HF2.

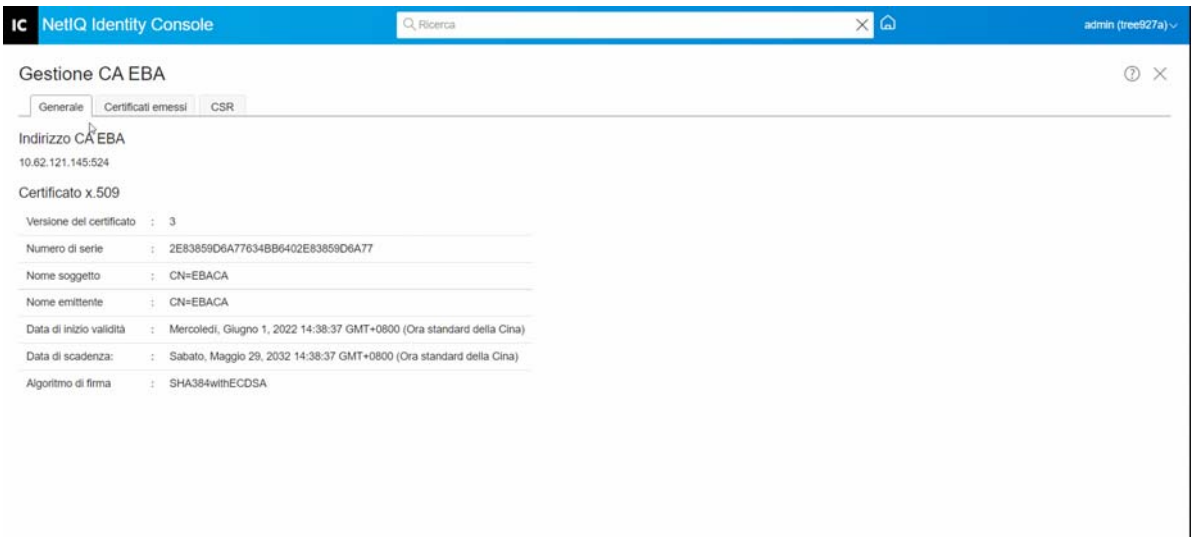
Per aprire la pagina Gestione CA EBA, eseguire il login al portale di Identity Console e fare clic sul modulo **EBA**.

La pagina Gestione CA EBA include le seguenti schede per la gestione dei diversi aspetti di CA EBA:

- **Generale:** visualizza l'indirizzo IP della EBA CA e il relativo certificato.
- **Certificati emessi:** visualizza i certificati NCP CA insieme ai relativi indirizzi IP e porte.

  Per revocare un certificato, selezionarlo e fare clic su ⊘. Utilizzare questa opzione solo in casi estremi, in quanto il server proprietario del certificato CA NCP diventerà non funzionante quando ne verrà revocato il certificato. In genere, la revoca del certificato diventa necessaria quando un server viene compromesso.
- **CSR:** elenca le richieste di firma del certificato in sospeso per l'approvazione da parte dell'amministratore. Per approvare una richiesta di firma del certificato, selezionare il certificato dall'elenco e fare clic su **Approva**.

Figura 20-1 *Gestione di Enhanced Background Authentication*



II Gestione di Identity Manager tramite Identity Console

In questa sezione vengono descritti i vari task che è possibile eseguire per gestire i server Identity Manager tramite il portale di Identity Console.

21 Gestione di driver e set di driver

Un set di driver è un container contenente i driver di Identity Manager. Su un server può essere attivo un solo set di driver alla volta. Di conseguenza, tutti i driver attivi devono essere raggruppati nello stesso set di driver. Il set di driver può essere creato utilizzando lo strumento Designer. Per ulteriori informazioni, vedere Configuring Driver Sets (Configurazione dei set di driver) nella *NetIQ Designer for Identity Manager Administration Guide* (Guida all'amministrazione di NetIQ Designer per Identity Manager).

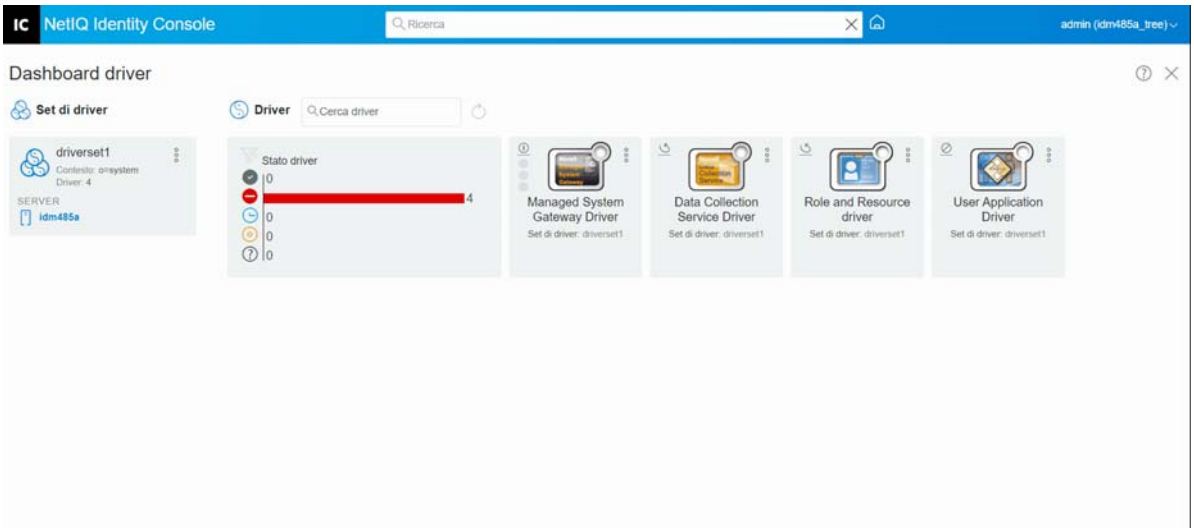
Aggiunta o eliminazione di server

È possibile associare un set di driver a uno o più server alla volta. Tuttavia, in base alle proprie esigenze, è possibile associare un oggetto set di driver diverso al server disponibile.

Per aggiungere un nuovo server, fare clic sull'icona nell'oggetto set di driver specifico > selezionare **Aggiungi server**, quindi selezionare il server appropriato dal browser del contesto.

Per eliminare un server esistente, selezionare l'opzione **Rimuovi server**.

Figura 21-1 *Aggiunta del server al set di driver*



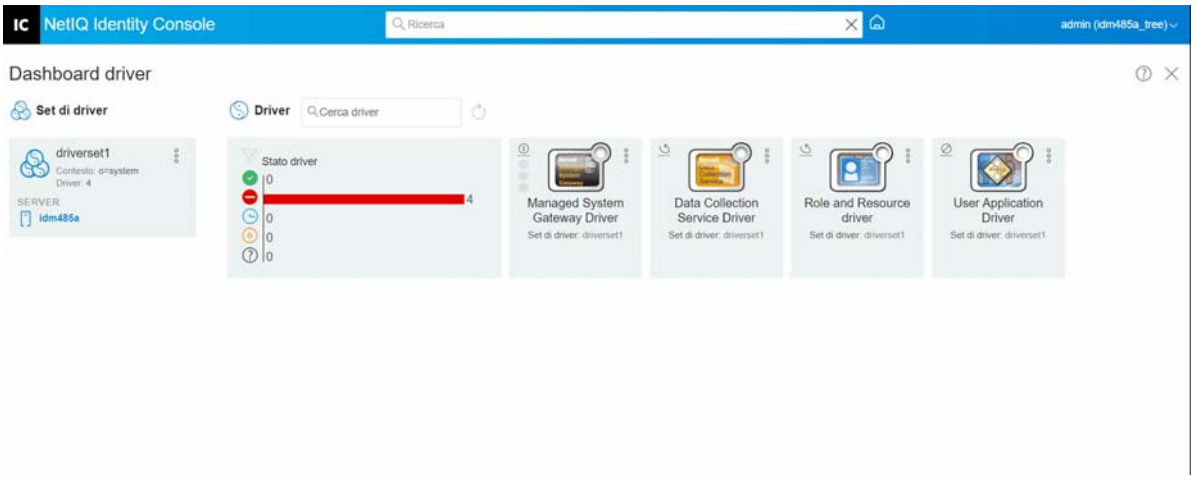
Attivazione dei set di driver tramite chiave di attivazione del prodotto

Prima di utilizzare un set di driver e i driver presenti al suo interno, è necessario attivarlo utilizzando il codice di attivazione ricevuto nell'ID e-mail. Dopo aver acquistato una licenza, NetIQ fornirà la chiave di attivazione. Eseguire le operazioni riportate di seguito per attivare il set di driver tramite chiave di attivazione:

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Fare clic sull'icona Azioni nella casella del set di driver specifico che si desidera attivare, quindi fare clic su **Installazione attivazione**.

   Quando si applica l'attivazione, in ciascuna scheda del set di driver nel riquadro Amministrazione IDM vengono visualizzate le informazioni di attivazione per tutti i server associati a tale set di driver. Queste informazioni consentono di identificare la scadenza dell'attivazione.
3. Se il file di attivazione è stato scaricato sul computer, selezionare la casella di controllo relativa all'opzione **Selezionare un file contenente credenziali**.
4. Individuare e selezionare il file di attivazione e fare clic su **Invia**.
5. In alternativa, è possibile attivare il set di driver utilizzando il contenuto del file di attivazione. Selezionare la casella di controllo relativa all'opzione **Immettere le credenziali**.
   - **5a** Aprire il file delle credenziali di attivazione del prodotto, quindi copiare il contenuto delle credenziali di attivazione del prodotto negli Appunti.
   - **5b** Se si è scelto di copiare il contenuto, non includere righe o spazi aggiuntivi. Iniziare a copiare dal primo trattino (-) delle credenziali (----BEGIN PRODUCT ACTIVATION CREDENTIAL) fino all'ultimo trattino (-) delle credenziali (END PRODUCT ACTIVATION CREDENTIAL-----), quindi fare clic su **Fine**.
6. Viene visualizzato un messaggio di conferma che indica che l'attivazione del set di driver è stata completata.

Figura 21-2 *Attivazione di set di driver*

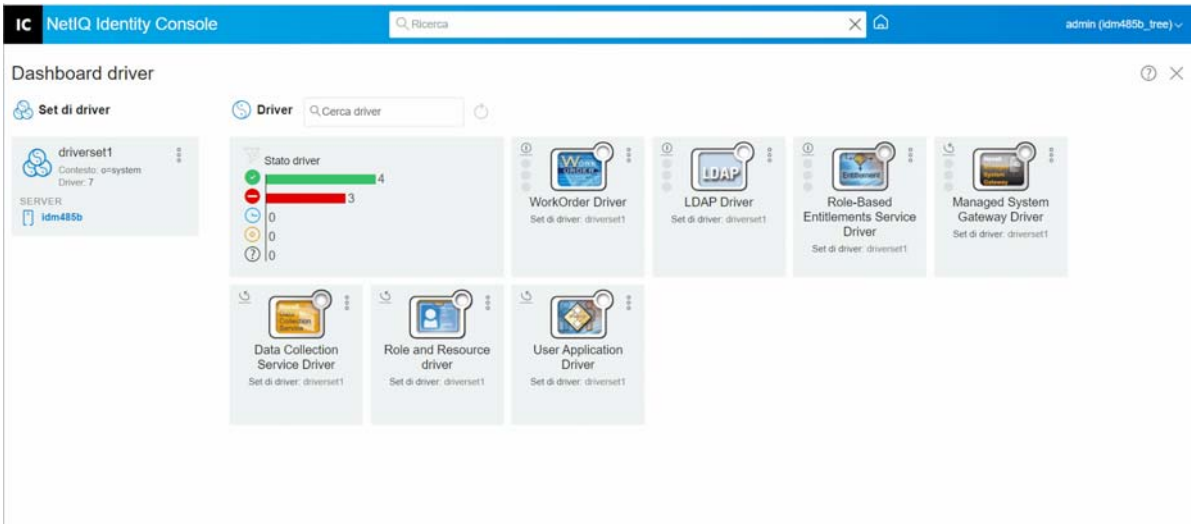


Visualizzazione delle informazioni sull'attivazione dei set di driver

Dopo aver attivato il set di driver, è necessario verificare che l'operazione sia stata eseguita correttamente. Per verificare, eseguire le operazioni riportate di seguito:

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Fare clic sull'icona Azioni sull'oggetto set di driver specifico per il quale si desidera verificare le informazioni di attivazione, quindi fare clic su **Informazioni attivazione**.
3. Viene visualizzata la finestra delle informazioni sull'attivazione. In questa pagina è possibile verificare i dettagli di attivazione del set di driver specifico.

Figura 21-3 *Visualizzazione delle informazioni sull'attivazione dei set di driver*

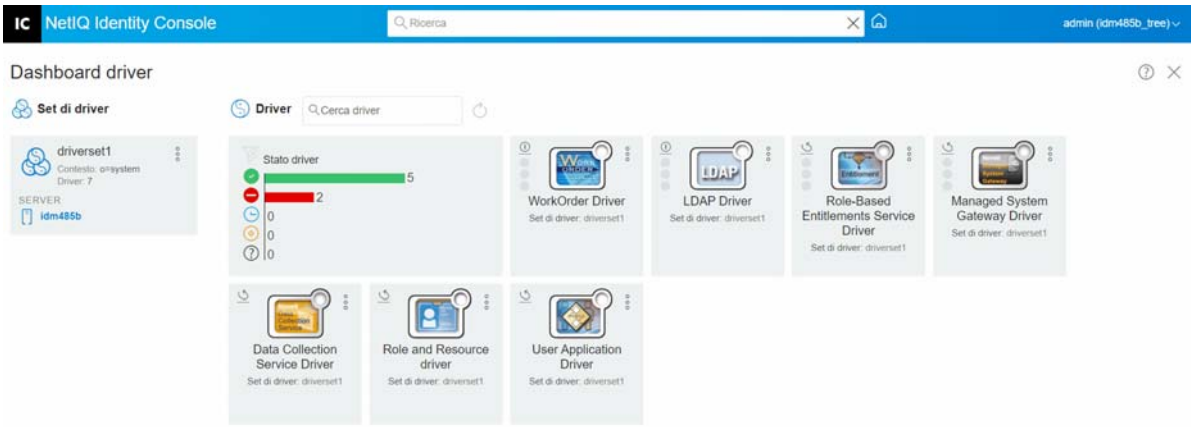


Avvio e arresto dei driver

Quando viene creato, un driver è arrestato di default. Per utilizzare il driver, è necessario avviarlo. Identity Manager è un sistema basato su eventi, pertanto dopo l'avvio, il driver rimane inattivo finché non si verifica un evento. Eseguire le operazioni riportate di seguito per avviare/arrestare i driver.

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Fare clic sull'oggetto set di driver specifico a destra dello schermo del computer per visualizzare tutti i driver ad esso associati.
3. Fare clic sull'icona Azioni sul driver specifico e selezionare **Avvia driver**.
4. Per arrestare un oggetto driver, fare clic sull'icona Azioni sul driver specifico e selezionare **Arresta driver**.
5. (Facoltativo) In alternativa, è possibile avviare o arrestare contemporaneamente tutti i driver presenti nello stesso oggetto set di driver. Fare clic sull'icona Azioni nell'oggetto set di driver e selezionare **Avvia tutti i driver** o **Arresta tutti i driver**.

Figura 21-4 *Avvio e arresto dei driver*



Ricerca dei driver

Identity Console consente di cercare un driver specifico nel server. Per cercare un driver, eseguire le operazioni riportate di seguito:

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Specificare il nome del driver nella casella **Ricerca**. L'oggetto driver specifico verrà visualizzato sullo schermo. È inoltre possibile aggiornare l'elenco dei driver facendo clic sull'icona .

Figura 21-5 *Ricerca dei driver*

Filtraggio di driver e set di driver

I driver possono essere filtrati in base al loro stato dalla pagina **Amministrazione IDM**. Per filtrare i driver:

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Fare clic sulle seguenti icone nel riquadro **Drivers' Status** (Stato driver) per filtrare i driver in base al loro stato:
   - Fare clic sull'icona per filtrare tutti i driver in esecuzione sul server.
   - Fare clic sull'icona per filtrare tutti i driver arrestati sul server.
   - Fare clic sull'icona per filtrare tutti i driver in fase di avvio.
   - Fare clic sull'icona per filtrare tutti i driver in fase di arresto.
   - Fare clic sull'icona per filtrare i driver a cui non è associato alcuno stato. Se a un set di driver non è associato alcun server, i driver presenti in tale set di driver riporteranno lo stato **Sconosciuto**.

   Per cancellare qualsiasi filtro applicato ai driver, fare clic sull'icona visualizzata nel riquadro **Drivers' Status** (Stato driver).
3. I set di driver possono anche essere filtrati tramite il portale di Identity Console. Di default, nel portale di Identity Console vengono visualizzati tutti i driver associati a tutti i set di driver presenti nel server. Se si desidera visualizzare i driver di un set di driver specifico, è necessario selezionare il set di driver appropriato dal relativo elenco sul lato sinistro del portale di Identity Console. Per cancellare la selezione del set di driver, fare nuovamente clic sul set di driver selezionato.

Figura 21-6 *Filtraggio di driver e set di driver*

Eliminazione del set di driver

Per eliminare un set di driver, eseguire le operazioni riportate di seguito:

1. Fare clic sulla scheda **Amministrazione IDM** nella schermata iniziale di Identity Console.
2. Fare clic sul pulsante delle azioni relativo al set di driver che si desidera eliminare.
3. Selezionare **Cancella**.

Azioni driver

Le seguenti azioni sono supportate facendo clic sull'icona delle azioni nel riquadro del singolo driver:

- **Avvia driver:** per avviare un driver
- **Arresta driver**: per arrestare un driver
- **Riavvia driver**: per riavviare un driver arrestato
- **Elimina driver**: per eliminare un driver
- **Statistiche**: per visualizzare le statistiche sulle prestazioni del driver
- **Copia dati**: per copiare i dati del driver da un server a un altro. Questa opzione è disponibile solo per ambienti con più server.

22 Gestione delle proprietà del set di driver

In questa sezione vengono fornite informazioni sulle proprietà comuni a tutti i set di driver. Sono incluse tutte le proprietà (password con nome, livello di log, controllo del set di driver e così via).

Questa sezione è suddivisa nelle seguenti categorie:

Configurazione dei set di driver

Per modificare la configurazione del set di driver, eseguire le operazioni riportate di seguito:

1. Fare clic su **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver**.
2. Di default, viene visualizzata la pagina **Configurazione set di driver**. Le opzioni di Configurazione set di driver sono suddivise nelle seguenti categorie:

Password con nome

Identity Manager consente di memorizzare in modo sicuro più password per un set di driver. Questa funzionalità è denominata password con nome. A ogni singola password è possibile accedere mediante una chiave o un nome.

È possibile aggiungere password con nome a un set di driver o a singoli driver. Le password con nome per un set di driver sono disponibili per tutti i driver del set.

Per utilizzare una password con nome in una policy driver, è necessario fare riferimento a essa mediante il nome della password invece di utilizzare la password effettiva, quindi il motore di Identity Manager la invia al driver. Il metodo descritto in questa sezione per la memorizzazione e il recupero delle password con nome può essere utilizzato con qualsiasi driver senza apportare modifiche allo shim del driver.

È possibile accedere a Password con nome selezionando **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Password con nome** sotto **Configurazione set di driver**.

Per aggiungere una nuova password con nome, fare clic sull'icona . Per rimuovere una password con nome esistente, selezionare la password appropriata e fare clic sull'icona .

Valori di configurazione globali

Visualizza un elenco ordinato di oggetti Configurazione globale. Gli oggetti contengono definizioni di GCV (Valori di configurazione globali) di estensione per il driver caricato da Identity Manager all'avvio del driver. È possibile aggiungere o rimuovere gli oggetti Configurazione globale e modificarne l'ordine di esecuzione. Fare clic sull'icona per salvare i GCV (Valori di configurazione globali). Per aggiornare l'elenco di GCV (Valori di configurazione globali), fare clic sull'icona .

Configurazione dei parametri dell'ambiente Java

Per configurare i parametri dell'ambiente Java, eseguire le operazioni riportate di seguito:

1. In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver**.
2. Fare clic su **Parametri ambiente Java** in **Configurazione set di driver** per visualizzare la pagina delle proprietà contenente i parametri dell'ambiente Java.
3. Modificare le seguenti impostazioni in base alle necessità:

   Aggiunte percorso della classe: specificare i percorsi aggiuntivi che JVM utilizzerà per la ricerca dei file di pacchetto (`.jar`) e di classe (`.class`). L'utilizzo di questo parametro corrisponde all'utilizzo del comando `java -classpath`. Se si immettono più percorsi della classe, separarli con un punto e virgola (;) per una JVM Windows e con due punti (:) per una JVM UNIX o Linux.

   Opzioni JVM: specificare le opzioni aggiuntive da utilizzare con JVM. Per informazioni sulle opzioni valide, consultare la documentazione di JVM.

   `DHOST_JVM_OPTIONS` è la variabile d'ambiente corrispondente che specifica gli argomenti per JVM 1.2. Ad esempio:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Ciascuna stringa di opzione è separata da uno spazio vuoto. Se una stringa di opzione contiene spazi vuoti, è necessario racchiuderla tra virgolette doppie.

   L'opzione dell'attributo del set di driver ha la precedenza rispetto alla variabile d'ambiente `DHOST_JVM_OPTIONS`. Questa variabile di ambiente viene aggiunta alla fine dell'opzione dell'attributo del set di driver.

   Dimensione heap iniziale: specificare la dimensione heap iniziale (minima) disponibile per JVM. L'aumento della dimensione heap iniziale può migliorare il tempo di avvio e le prestazioni della velocità effettiva. Utilizzare un valore numerico seguito da G, M o K. Se non viene specificata alcuna dimensione tramite lettera, la dimensione di default è byte. L'utilizzo di questo parametro corrisponde all'utilizzo del comando `java -Xms`.

   `DHOST_JVM_INITIAL_HEAP` è la variabile d'ambiente corrispondente che specifica la dimensione heap JVM iniziale in numeri decimali di byte. Tale variabile ha la precedenza rispetto all'opzione dell'attributo del set di driver.

   Fare riferimento alla documentazione di JVM per informazioni sulla dimensione heap iniziale di default di JVM.

Dimensione heap massima: specificare la dimensione heap massima disponibile per JVM. Utilizzare un valore numerico seguito da G, M o K. Se non viene specificata alcuna dimensione tramite lettera, la dimensione di default è byte. L'utilizzo di questo parametro corrisponde all'utilizzo del comando `java -Xmx`.

`DHOST_JVM_MAX_HEAP` è la variabile d'ambiente corrispondente che specifica la dimensione heap JVM massima in numeri decimali di byte. Tale variabile ha la precedenza rispetto all'opzione dell'attributo del set di driver.

Fare riferimento alla documentazione di JVM per informazioni sulla dimensione heap massima di default di JVM.

4 Fare clic su per salvare le modifiche.

5 Riavviare Identity Vault per applicare le modifiche.

Gestione dell'elenco degli attributi con valore

Per aggiungere attributi all'elenco degli attributi con valore per un set di driver specifico, eseguire le operazioni riportate di seguito:

1 In Identity Console, selezionare il modulo **Gestione oggetti**.

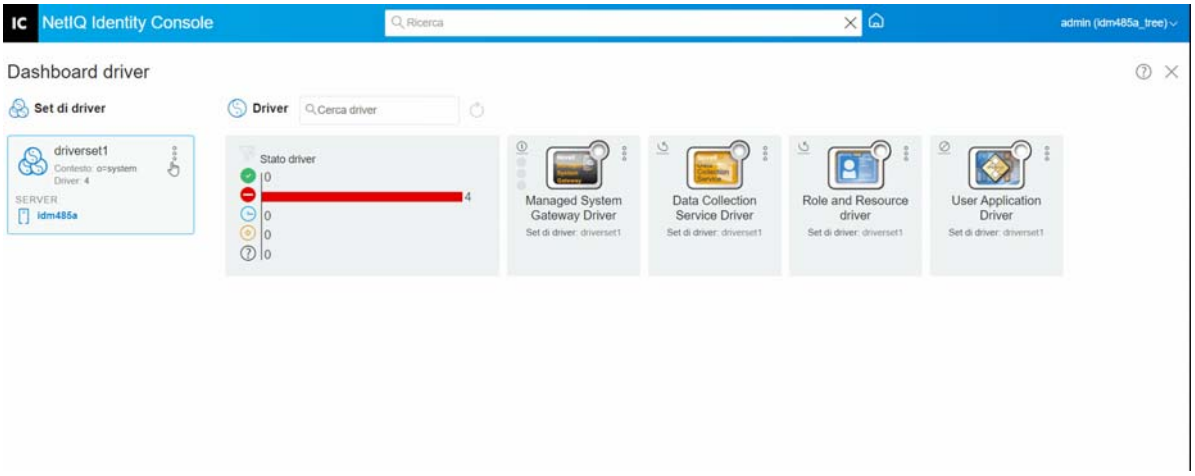
2 Selezionare il tipo **DirXML-DriverSet** dall'elenco a discesa e fare clic sul pulsante di ricerca.

3 Fare clic sul set di driver appropriato dall'elenco di ricerca.

4 Per aggiungere attributi senza valore all'elenco di attributi con valore, fare clic sull'icona accanto agli **Attributi con valore** e selezionare gli attributi senza valore appropriati dall'elenco.

5 Al termine, fare clic su **OK**.

Figura 22-1 *Gestione dei parametri di configurazione del set di driver*



Gestione dei processi per i set di driver

Identity Console consente di pianificare gli eventi utilizzando l'opzione Processi per tutti i driver presenti nel rispettivo set di driver.

La pagina Job Scheduler (Pianificazione processi) contiene il nome del processo, indica se il processo è abilitato o disabilitato, quando è pianificato per l'esecuzione e la descrizione del processo. Fare clic sul nome del processo per visualizzare la pagina Processi. Fare clic sull'icona di abilitazione/disabilitazione nella colonna Abilitato per abilitare o disabilitare il processo. Fare clic sulla descrizione del processo per visualizzarne la descrizione completa.

Per accedere alla pagina Processi, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > scheda **Avanzate** nella pagina principale di Identity Console. La scheda Processi contiene una tabella che mostra gli oggetti processo esistenti per il driver selezionato, elencato con il nome distinto completo nella voce Driver.

La pagina Job Scheduler (Pianificazione processi) consente di eseguire i seguenti task:

- **Creare il processo**: fare clic sull'icona per creare un nuovo processo.

  Nella finestra popup **Nuovo processo**, eseguire le seguenti operazioni per creare un nuovo processo:

  1. Specificare il nome del processo.
  2. Selezionare il tipo di processo.
  3. Fare clic sull'icona e selezionare il server in cui eseguire il processo dall'elenco di server disponibili. In alternativa, specificare il nome di un server e selezionare il server.
  4. Fare clic sul pulsante **Crea**.
- **Avviare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Arrestare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Abilitare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Disabilitare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Ottenere lo stato**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Eliminare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .

Fare clic su un processo per accedere alla pagina **Job Property** (Proprietà processo). Qui è possibile impostare la modalità di esecuzione del processo.

Generale: mostra il nome della classe Java del processo. Utilizzare questa pagina per abilitare o disabilitare il processo, per eliminarlo dopo l'esecuzione, per selezionare il server o i server in cui deve essere eseguito, per specificare il server e-mail e assegnare al processo un nome visualizzato e una descrizione diversi.

Pianificazione: consente di impostare quando eseguire il processo. Specificare un valore temporale per l'opzione Avvia processo alle e se eseguire il processo giornalmente, settimanalmente, mensilmente o annualmente. È inoltre possibile personalizzare quando eseguire il processo oppure abilitare l'interruttore per eseguirlo manualmente.

Ambito: consente di definire gli oggetti a cui applicare il processo. Un oggetto può essere un container, un gruppo dinamico, un gruppo o un oggetto Foglia. Fare clic su Aggiungi per selezionare l'oggetto a cui si desidera applicare il processo. È possibile utilizzare il pulsante Sfoglia per selezionare un oggetto, quindi fare clic su OK. Per rimuovere un oggetto dall'elenco di ambiti, selezionare un oggetto ambito facendo clic sulla casella a sinistra dell'oggetto DN, quindi fare clic su Rimuovi.

Quando si aggiunge un oggetto, selezionarlo per visualizzare ulteriori opzioni. Se si seleziona un oggetto Gruppo, è possibile applicare il processo ai membri del gruppo o solo al gruppo. Se si seleziona un oggetto Container, è possibile applicare il processo a tutti gli elementi discendenti di tale container, a tutti gli elementi secondari del container o solo al container.

Parametri: consente di aggiungere ulteriori parametri al processo e di visualizzare i parametri così come sono attualmente impostati. Questi parametri cambiano a seconda del tipo di processo selezionato.

Risultati: consente di definire le attività da eseguire con i risultati del processo. La pagina Risultati è suddivisa in due parti: Intermediate Result (Risultato intermedio) e Final Result (Risultato finale), con i seguenti risultati consentiti: Operazione completata, Avviso, Errore e Interrotti. A destra della colonna Risultati è presente la colonna Azione. Facendo clic sulla colonna Azione è possibile impostare la modalità di notifica desiderata per ciascun risultato. Le azioni includono l'invio di un risultato di revisione o l'invio di un'e-mail al completamento del risultato. Se non si seleziona un'opzione, non viene eseguita alcuna azione per il risultato.

Nella scheda **Traccia** è possibile configurare la traccia per un driver specifico. Per ulteriori informazioni, vedere “Configurazione del livello di traccia” a pagina 171.

Gestione delle librerie per un set di driver specifico

Gli oggetti libreria memorizzano più policy e altre risorse condivise da uno o più driver. È possibile creare un oggetto libreria in un oggetto set di driver o in qualsiasi container eDirectory. In un albero eDirectory possono essere presenti più librerie. I driver possono fare riferimento a qualsiasi libreria nell'albero purché il server su cui è in esecuzione il driver contenga una replica in Lettura/Scrittura o Master dell'oggetto della libreria.

I fogli di stile, le policy, le regole e altri oggetti risorsa possono essere memorizzati in una libreria a cui fanno riferimento uno o più driver.

Tramite il modulo Library Management (Gestione librerie) è possibile eseguire i seguenti task:

- “Visualizzazione ed eliminazione di una libreria esistente” a pagina 144
- “Visualizzazione ed eliminazione di oggetti dalla libreria” a pagina 144

Visualizzazione ed eliminazione di una libreria esistente

Per visualizzare ed eliminare una libreria esistente, eseguire le operazioni riportate di seguito:

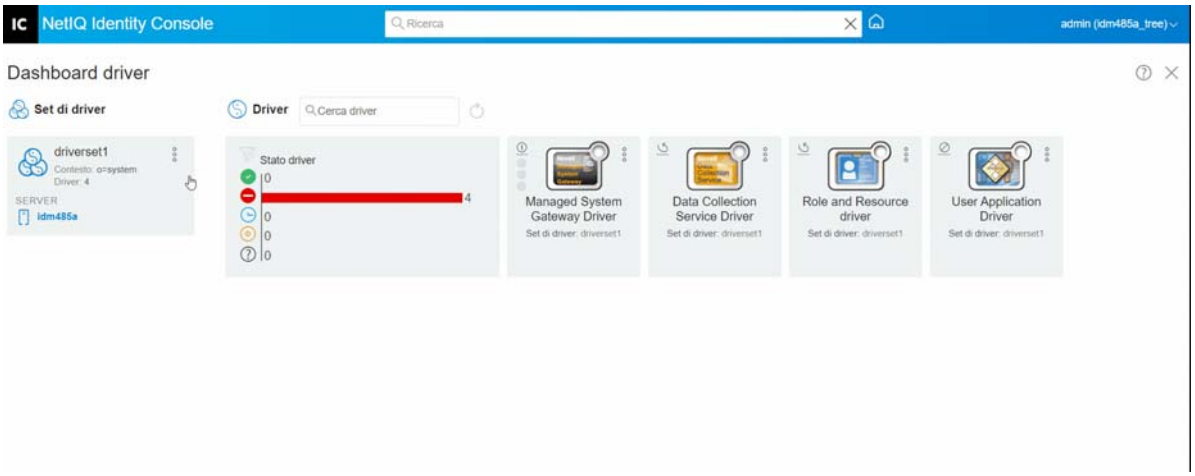
1. In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Avanzate** > **Librerie**.
2. Selezionare la libreria appropriata dall'elenco.
3. Fare clic sull'icona . Fare clic su **OK** per confermare.

Visualizzazione ed eliminazione di oggetti dalla libreria

È possibile visualizzare ed eliminare policy e tabelle mappature dagli oggetti libreria. Per eliminare gli oggetti, eseguire le operazioni riportate di seguito:

1. In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Avanzate** > **Librerie**.
2. Fare clic sulla libreria appropriata dall'elenco.
3. Per eliminare le policy, selezionare la scheda **Policy**.
4. Selezionare la policy appropriata dall'elenco e fare clic sull'icona .
5. Per eliminare le tabelle mappature, selezionare la scheda **Tabelle mappature**.
6. Selezionare la tabella mappature appropriata dall'elenco e fare clic sull'icona .
7. Fare clic su **OK** per confermare.

Figura 22-2 *Gestione dei processi e delle librerie per i set di driver*



Configurazione dei livelli di log e di traccia dei set di driver

Per configurare il log e la traccia per i set di driver, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > scheda **Configurazione log e traccia** nella pagina principale di Identity Console. Questa sezione è suddivisa nelle seguenti categorie:

Configurazione del livello di log

Ciascun set di driver dispone di un campo del livello di log in cui è possibile definire il livello degli errori di cui tenere traccia. Il livello qui configurato determina quali messaggi sono disponibili per i log. Di default, il livello di log è impostato per tenere traccia dei messaggi di errore. Sono inclusi anche i messaggi di errore irreversibile. Per tenere traccia di altri tipi di messaggi, modificare il livello di log. Per configurare il livello di log, in Identity Console selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Configurazione log e traccia** > **Livello log**. La seguente tabella descrive le impostazioni del livello di log:

Opzione	Descrizione
Disattivare la registrazione dei log del set di driver, del sottoscrittore e del produttore	Disattiva del tutto la registrazione per tutti i driver dell'oggetto set di driver, del sottoscrittore e del produttore.
Numero massimo di voci nel log (50-500)	Numero di voci nel log. Il valore di default è 50.

Livelli di log	È possibile scegliere tra i seguenti livelli di log:
	◆ **Registra errori**: registra solo gli errori
	◆ Registra errori e avvisi: registra gli errori e gli avvisi
	◆ **Registra eventi specifici**: registra gli eventi selezionati. Se si seleziona questa opzione, viene abilitato il seguente elenco di eventi:
	  ◆ **Eventi motore di metadirectory**
	  ◆ **Eventi di stato**
	  ◆ **Eventi operazione**
	  ◆ **Eventi di trasformazione**
	  ◆ **Eventi provisioning credenziali**
	◆ **Aggiorna solo l'ora ultimo log**: aggiorna l'ora dell'ultimo log.
	◆ **Registrazione disattivata**: disattiva la registrazione per il driver.

Configurazione del livello di traccia

È possibile configurare la traccia per un set di driver specifico. A seconda del livello di traccia specificato per un set di driver, la traccia visualizza gli eventi correlati al driver quando il motore elabora gli eventi. Il livello di traccia del driver influisce solo sul driver o sul set di driver su cui è impostata la traccia. Se si utilizza l'oggetto Configurazione del caricatore remoto, il file di traccia dell'oggetto Configurazione del caricatore remoto viene impostato direttamente sull'oggetto Configurazione del caricatore remoto e contiene solo la traccia dello shim del driver.

Per configurare la traccia per un set di driver, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Configurazione log e traccia** > scheda **Traccia**. La seguente tabella descrive le impostazioni della traccia:

Parametro	Driver
Livello di traccia	All'aumentare del livello di traccia del driver, aumenta la quantità di informazioni visualizzate in Traccia. Il livello di traccia 1 mostra gli errori ma non la loro causa. Se si desidera visualizzare le informazioni sulla sincronizzazione delle password, impostare il livello di traccia a 5. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.
Livello traccia XSL	Traccia visualizza gli eventi XSL. Impostare questo livello di traccia solo per la risoluzione dei problemi relativi ai fogli di stile XSL. Se non si desidera visualizzare le informazioni XSL, impostare il livello a 0.
Porta di debug Java	Consente agli sviluppatori di collegare un debugger Java. Riavviare Identity Vault dopo aver collegato il debugger Java.
File di traccia	Specificare un nome file e l'ubicazione in cui vengono scritte le informazioni di Identity Manager per il driver selezionato. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.
Codifica file di traccia	Il file di traccia utilizza la codifica di default del sistema. Se necessario, è possibile specificare un'altra codifica. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.
Limite dimensione file di traccia	Consente di impostare un limite per il file di traccia Java. Se si imposta la dimensione del file su Nessun limite, le dimensioni del file aumentano fino all'esaurimento dello spazio su disco. **Nota:** se si imposta il limite delle dimensioni del file, il file di traccia viene creato in più file. Identity Manager divide automaticamente le dimensioni massime dei file per dieci e crea dieci file separati. La dimensione combinata di questi file equivale alla dimensione massima del file di traccia. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.

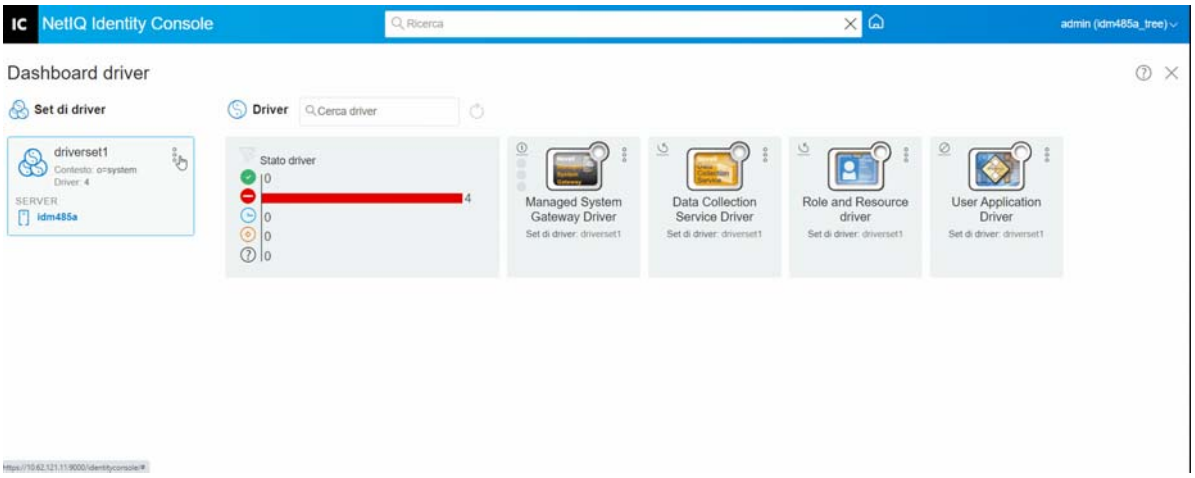
Traccia DirXML Script

L'opzione Traccia DirXML Script consente di selezionare un livello di traccia per un set di driver. La selezione viene applicata a tutte le policy nel set di driver. È possibile scegliere tra le seguenti opzioni di traccia di DirXML Script:

- Traccia per tutti i DirXML Script attivata
- Traccia per tutti i DirXML Script disattivata
- Traccia regola DirXML Script attivata
- Traccia regola DirXML Script disattivata

Fare clic su per salvare le modifiche.

Figura 22-3 *Gestione dei livelli di log e di traccia dei set di driver*



Gestione del controllo del set di driver e delle statistiche

È possibile utilizzare Driver Set Inspector (Controllo set di driver) per visualizzare informazioni dettagliate sugli oggetti associati a un set di driver. Questa sezione è suddivisa nelle seguenti categorie:

- “Visualizzazione delle statistiche del set di driver” a pagina 148
- “Visualizzazione delle informazioni sulla versione” a pagina 148
- “Visualizzazione delle Statistiche di associazione” a pagina 149

Visualizzazione delle statistiche del set di driver

È possibile utilizzare il portale di Identity Console per visualizzare numerose statistiche relative a un singolo driver o a un intero set di driver. Sono incluse statistiche quali le dimensioni del file di cache, le dimensioni delle transazioni non elaborate nel file di cache, le transazioni meno recenti e più recenti e il numero totale di transazioni non elaborate per categoria (aggiunta, rimozione, modifica e così via). Per visualizzare le statistiche del set di driver:

1. In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Controllo e statistiche** > **Statistiche**.
2. Selezionare il server appropriato dall'elenco a discesa.

   Viene visualizzata una pagina che consente di visualizzare le statistiche relative a tutti i driver contenuti nel set di driver.

   - Per aggiornare le statistiche, fare clic sull'icona .
   - Per chiudere le statistiche relative a un driver, fare clic sul pulsante nell'angolo in alto a destra della finestra delle statistiche del driver.
   - Per aprire le statistiche relative a tutti i driver, fare clic su **Azioni** > **Mostra tutto**.
   - Per comprimere l'elenco delle transazioni non elaborate per un driver, fare clic sul pulsante situato sopra l'elenco. Per comprimere l'elenco delle transazioni non elaborate per tutti i driver, fare clic su **Azioni** > **Comprimi tutte le transazioni**.
   - Per espandere l'elenco delle transazioni, fare clic sul pulsante . Per espandere l'elenco delle transazioni non elaborate per tutti i driver, fare clic su **Azioni** > **Espandi tutte le transazioni**.
   - Per chiudere il dashboard delle statistiche dei driver disabilitati, fare clic su **Azioni**, quindi selezionare **Close Disabled Drivers** (Chiudi driver disabilitati).

Visualizzazione delle informazioni sulla versione

Il motore di Identity Manager, gli shim del driver e i file di configurazione del driver contengono ciascuno un numero di versione separato. L'opzione Rilevazione versione di Identity Console consente di individuare le versioni del motore di Identity Manager e le versioni degli shim del driver. I file di configurazione del driver contengono la propria convenzione di denominazione. Per visualizzare le informazioni sulla versione:

1. In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Controllo e statistiche** > **Rilevazione versione**.
2. Visualizzare una schermata di livello superiore delle informazioni sul controllo delle versioni:
   - L'albero eDirectory a cui si è autenticati

     Nota: eDirectory viene chiamato Identity Vault se utilizzato nell'ambiente Identity Manager.
   - Il set di driver selezionato
   - I server associati al set di driver

Se il set di driver è associato a due o più server, è possibile visualizzare le informazioni di Identity Manager su ciascun server.

- Driver

3 Fare clic sull'icona **Visualizza** per visualizzare una rappresentazione testuale delle stesse informazioni contenute nella visualizzazione di livello superiore.

4 Fare clic sul pulsante Esporta per esportare e salvare il testo in un file sull'unità locale o di rete.

Visualizzazione delle Statistiche di associazione

Tramite la funzione Statistiche di associazione di Identity Manager è possibile trovare i dettagli di associazione delle identità gestite da Identity Manager. Identity Manager utilizza le statistiche di associazione per ottenere il conteggio delle associazioni per i driver di Identity Manager.

Per ottenere gli oggetti attivi, inattivi e gestiti dal sistema per un driver, eseguire il processo delle statistiche di associazione. È possibile pianificare il processo delle statistiche di associazione su base giornaliera, settimanale, mensile o annuale. Di default, l'esecuzione del processo è pianificata su base settimanale.

Nel dashboard Statistiche di associazione vengono visualizzati i dettagli di associazione. In alternativa, è possibile visualizzare i dettagli esportando le associazioni in un file.

Nota

- Il conteggio delle associazioni per i driver viene calcolato per singolo server. Se un oggetto è associato a più di un driver, il conteggio delle associazioni viene calcolato in modo univoco per ciascun driver.
- Se si dispone di più di 200.000 associazioni, si consiglia di impostare la dimensione heap massima per il set di driver a 2 GB o più. Per informazioni sull'impostazione della dimensione heap, vedere "Configurazione dei parametri dell'ambiente Java" a pagina 140.

Per visualizzare le statistiche di associazione:

1 In Identity Console, selezionare **Amministrazione IDM** > **Fare clic sul menu contestuale (tre puntini) del set di driver appropriato** > **Proprietà set di driver** > **Controllo e statistiche** > **Statistiche di associazione**.

2 Selezionare il server per il quale si desidera eseguire le statistiche di associazione.

3 Il conteggio delle associazioni visualizza il risultato calcolato in precedenza.

Identity Console visualizza il conteggio delle associazioni per gli oggetti attivi, inattivi e gestiti dal sistema per tutti i driver associati al set di driver.

Identity Console considera i gruppi e le unità organizzative come oggetti gestiti dal sistema. Identity Console considera un oggetto inattivo se l'attributo `Login disabilitato` nell'oggetto è impostato su true (vero) e l'oggetto non è stato modificato negli ultimi 120 giorni. Tutti gli oggetti rimanenti vengono considerati come oggetti gestiti attivi.

4 Fare clic sull'icona per ottenere i risultati aggiornati.

Se un driver è disabilitato sul server, Identity Console non lo visualizza nel dashboard.

5 Fare clic sull'icona per esportare i dettagli di sistema e del conteggio delle associazioni per i driver associati al server.

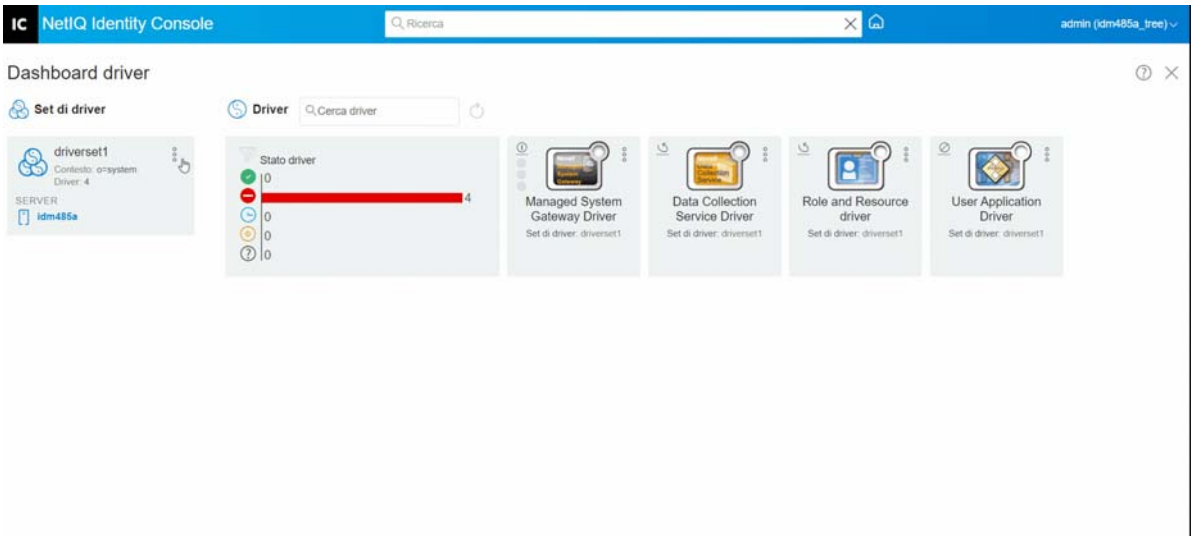
6 Per esportare gli oggetti associati a un driver specifico, fare clic su accanto agli oggetti richiesti e salvare il file.

Nota: nel caso dei driver di fan-out, vengono esportati solo oggetti univoci. Se un oggetto è associato a più istanze di un driver di fan-out, Identity Console visualizza tutti i conteggi delle associazioni nel dashboard. Tuttavia, se si sceglie di esportare gli oggetti in un file, Identity Console esporta solo gli oggetti univoci.

---

7 Fare clic su **Azioni** e selezionare l'opzione richiesta per organizzare il dashboard del conteggio delle associazioni.

Figura 22-4 *Gestione delle statistiche del set di driver*



23 Gestione delle proprietà del driver

In questa sezione vengono fornite informazioni sulle proprietà comuni a tutti i driver. Sono incluse tutte le proprietà (Password con nome, Valori di controllo del motore, Livello log e così via).

Vengono visualizzate le informazioni di attivazione per un driver che ricordano all'utente di intraprendere un'azione di attivazione del driver in scadenza.

Per modificare la configurazione del driver, eseguire le operazioni riportate di seguito:

1. Fare clic sulla scheda **Driver** nella schermata iniziale di Identity Console.
2. Fare clic sul riquadro del rispettivo driver per visualizzare la pagina di configurazione del driver.

   Di default, viene visualizzata la pagina **Parametri di connessione**. Le opzioni di configurazione del driver sono suddivise nelle seguenti categorie:

Parametri di connessione

I parametri di connessione controllano se il driver deve essere eseguito localmente o in remoto.

- **Java:** utilizzare questa opzione per specificare il nome della classe Java di cui viene creata un'istanza per il componente shim del driver. Questa classe può essere collocata nella directory delle classi come file di classe o nella directory `lib` come file `.jar`. Selezionare questa opzione per eseguire il driver localmente. È inoltre necessario specificare la Password oggetto driver e il Limite cache del driver. È possibile impostare una nuova password facendo clic sul collegamento **Imposta password**.

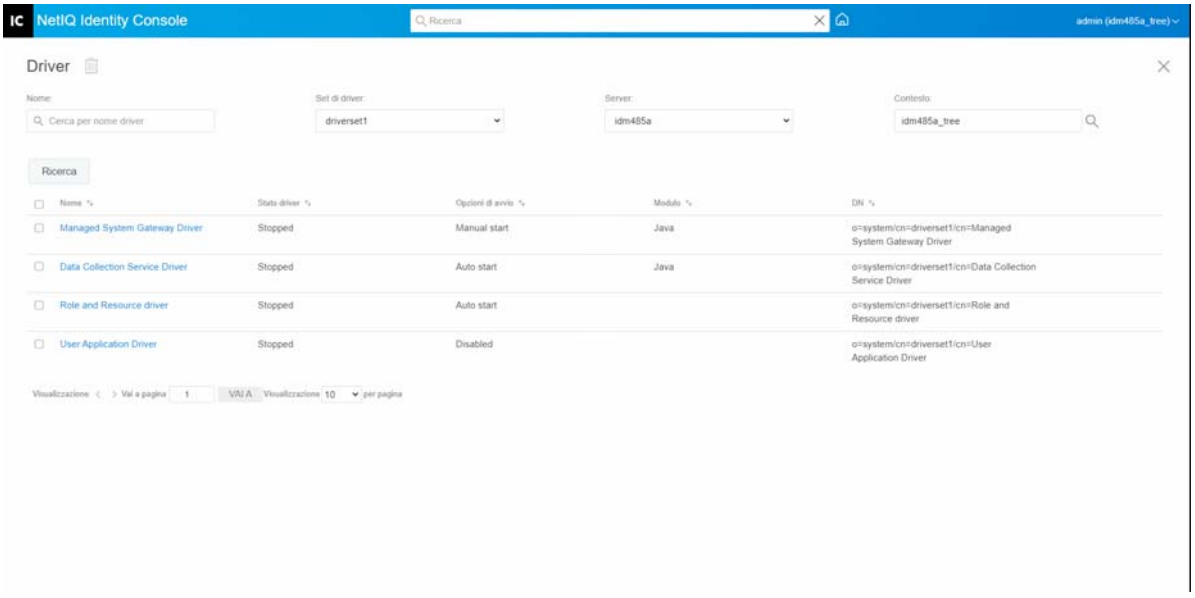
  Ad esempio, `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Nativo:** questa opzione viene utilizzata per specificare il nome del file `.dll` sviluppato in linguaggio nativo (ad esempio C++) per il driver. È inoltre necessario specificare la Password oggetto driver e il Limite cache del driver. È possibile impostare una nuova password facendo clic sul collegamento **Imposta password**.

  Ad esempio, `addriver.dll`

- **Connetti a oggetto Configurazione del caricatore remoto**: questa opzione viene utilizzata quando il driver si connette in remoto al sistema connesso. Se questa opzione è selezionata, è necessario specificare le seguenti opzioni secondarie:
  - **Parametri di connessione oggetto Configurazione del caricatore remoto**: include informazioni sui dettagli relativi all'ambiente dell'oggetto Configurazione del caricatore remoto quali il nome host, la porta di connessione e così via.
  - **Password oggetto Configurazione del caricatore remoto**: la password dell'oggetto Configurazione del caricatore remoto.
  - **Password oggetto driver**: specifica una password per l'oggetto driver. Se si utilizza l'oggetto Configurazione del caricatore remoto, è necessario immettere una password in questa pagina. L'oggetto Configurazione del caricatore remoto utilizza questa password per autenticarsi con lo shim del driver remoto.
- **Autenticazione**: i parametri di autenticazione vengono utilizzati per autenticare il motore di Identity Manager e i server dell'oggetto Configurazione del caricatore remoto. Specificare i seguenti parametri:
  - **ID autenticazione**: specificare un ID applicazione utente. Questo ID viene utilizzato per trasmettere le informazioni di sottoscrizione di Identity Vault all'applicazione.
  - **Contesto di autenticazione**: specificare l'indirizzo IP o il nome del server con cui deve comunicare lo shim dell'applicazione.
  - **Password applicazione**: opzione per impostare la password di autenticazione dell'applicazione.

Al termine, fare clic sull'icona per salvare la configurazione.

Figura 23-1 *Gestione dei parametri di connessione*



Driver Configuration (Configurazione driver)

La sezione di configurazione del driver consente di configurare i parametri specifici del driver, i valori di controllo del motore, i valori di configurazione globali e così via. Quando si modificano i parametri del driver, il comportamento del driver viene ottimizzato in modo da allinearsi con l'ambiente di rete. Questa sezione è suddivisa nelle seguenti categorie:

Parametri driver

I parametri del driver sono suddivisi in Impostazioni driver, Impostazioni sottoscrittore e Impostazioni produttore. Tali impostazioni verranno popolate in base alla configurazione del driver. Per ulteriori informazioni sui parametri del driver, fare riferimento alla guida specifica del driver nella documentazione relativa ai driver di Identity Manager (in lingua inglese).

Al termine, è possibile salvare i parametri facendo clic sul pulsante  . Se si desidera impostare i parametri al valore di default, fare clic sull'icona  . Per modificare la configurazione del driver utilizzando il file xml, fare clic sull'icona  .

Valori di configurazione globali

Visualizza un elenco ordinato di oggetti Configurazione globale. Gli oggetti contengono definizioni di GCV (Valori di configurazione globali) di estensione per il driver caricato da Identity Manager all'avvio del driver. È possibile visualizzare o modificare gli oggetti nella scheda **Valori di configurazione globali** utilizzando l'editor XML. Fare clic sull'icona  per salvare i GCV (Valori di configurazione globali). Per aggiornare l'elenco di GCV (Valori di configurazione globali), fare clic sull'icona  . Per eliminare i GCV (Valori di configurazione globali), selezionare l'oggetto GCV appropriato e fare clic sull'icona  .

Valori di controllo del motore

I valori di controllo del motore rappresentano un modo per modificare determinati comportamenti di default del motore di Identity Manager. È possibile accedere ai valori solo se all'oggetto set di driver è associato un server.

Opzione	Descrizione
Subscriber channel retry interval in seconds (Intervallo tentativi sottoscrittore in secondi)	L'intervallo dei tentativi del sottoscrittore determina la frequenza con cui il motore di Identity Manager riprova l'elaborazione di una transazione memorizzata nella cache dopo che l'oggetto Sottoscrittore dello shim dell'applicazione restituisce uno stato retry (nuovo tentativo).
Qualified form for DN-syntax attribute values (Formato qualificato per valori attributo di sintassi DN)	La specifica qualificata per i valori di attributo di sintassi DN determina se i valori degli attributi della sintassi DN sono presentati in formato unqualified-slash o qualified-slash. Un'impostazione True (Vero) indica che i valori sono presentati in formato qualificato.
Qualified form from rename events (Formato qualificato da eventi di ridenominazione)	Il formato qualificato per gli eventi di ridenominazione determina se la parte relativa al nuovo nome degli eventi di ridenominazione provenienti da Identity Vault viene presentata al sottoscrittore con qualificatori di tipo. Ad esempio, CN=. Un'impostazione True (Vero) indica che i nomi sono presentati in formato qualificato.
Maximum eDirectory replication wait time in seconds (Tempo massimo di attesa per la replica di eDirectory in secondi)	Questa impostazione controlla il tempo massimo di attesa del motore di Identity Manager per la replica di una modifica specifica tra la replica locale e una replica remota. Ciò influisce solo sulle operazioni in cui al motore di Identity Manager viene richiesto di contattare un server eDirectory remoto nello stesso albero per eseguire un'operazione in cui potrebbe essere necessario attendere la replica di alcune modifiche verso o dal server remoto prima di poter completare l'operazione (ad esempio, gli spostamenti di oggetti quando il server di Identity Manager non possiede la replica master dell'oggetto spostato; operazioni sui diritti del file system per gli utenti creati da un modello).
Use non-compliant backwards-compatible mode for XSLT (Usa modalità di compatibilità con le versioni precedenti non conforme per XSLT)	Questo controllo imposta il processore XSLT utilizzato dal motore di Identity Manager su una modalità compatibile con le versioni precedenti. La modalità compatibile con le versioni precedenti fa sì che il processore XSLT utilizzi uno o più comportamenti non conformi agli standard XPath 1.0 e XSLT 1.0. Questa operazione viene eseguita per garantire la compatibilità con i fogli di stile DirXML esistenti che dipendono da comportamenti non standard. Ad esempio, il comportamento dell'operatore XPath "!=" quando un operando è un set-nodi e l'altro operando è diverso da un set-nodi non è corretto nelle versioni di DirXML fino a Identity Manager 2.0 incluso. Questo comportamento è stato corretto; tuttavia, il comportamento corretto è disabilitato di default mediante questo controllo a favore della compatibilità con le versioni precedenti dei fogli di stile DirXML esistenti.
Maximum application objects to migrate at once (Numero massimo di oggetti applicazione di cui eseguire la migrazione contemporaneamente)	Questo controllo consente di limitare il numero di oggetti applicazione che il motore di Identity Manager richiede a un'applicazione durante una singola interrogazione eseguita come parte di un'operazione Migrate Objects from Application (Esegui migrazione degli oggetti dall'applicazione). Se si verificano errori java.lang.OutOfMemoryError durante un'operazione Migrate from Application (Esegui migrazione dall'applicazione), questo numero deve essere impostato su un valore inferiore a quello di default. Il valore di default è 50. **Nota:** questo controllo non limita il numero di oggetti applicazione che è possibile migrare; limita semplicemente le dimensioni del batch.

Opzione	Descrizione
Set creatorsName on objects created in Identity Vault (Imposta creatorsName su oggetti creati in Identity Vault)	Questo controllo viene utilizzato dal motore di Identity Manager per determinare se l'attributo creatorsName deve essere impostato sul DN di questo driver su tutti gli oggetti creati in Identity Vault da questo driver. L'impostazione dell'attributo creatorsName consente di identificare facilmente gli oggetti creati da questo driver ma comporta anche una riduzione delle prestazioni. Se questa opzione non è impostata, l'attributo creatorsName viene impostato di default sul DN dell'oggetto NCP Server che ospita il driver.
Write pending associations (Scrivi associazioni in sospeso)	Questo controllo determina se il motore di Identity Manager deve scrivere un'associazione in sospeso su un oggetto durante l'elaborazione del sottoscrittore. La scrittura di un'associazione in sospeso non comporta alcun vantaggio sostanziale ma comporta una riduzione le prestazioni. Tuttavia, l'opzione viene fornita per garantire la compatibilità con le versioni precedenti.
Use password event values (Utilizza valori evento password)	Questo controllo determina l'origine del valore riportato per l'attributo nspmDistributionPassword per gli eventi Add (Aggiungi) e Modify (Modifica) del sottoscrittore. Se si imposta il controllo su False (Falso), il valore corrente di nspmDistributionPassword viene ottenuto e riportato come valore dell'evento dell'attributo. Ciò significa che è disponibile solo il valore della password corrente. Si tratta del comportamento di default. Se si imposta il controllo su True (Vero), il valore registrato con l'evento eDirectory viene decifrato e riportato come valore dell'evento dell'attributo. Ciò significa che sono disponibili sia il valore della password precedente (se esistente) che il valore della password di sostituzione al momento dell'evento. Tale comportamento risulta utile per sincronizzare le password con determinate applicazioni che richiedono la password precedente per abilitare l'impostazione di una nuova password.
Retry Out of Band events (Nuovo tentativo eventi fuori banda)	Questo controllo determina se gli eventi di sincronizzazione fuori banda devono essere ripetuti o meno se viene ricevuto lo stato **retry** (nuovo tentativo) per l'evento di sincronizzazione fuori banda. Se il controllo è impostato su False (Falso), la sincronizzazione fuori banda non viene ripetuta. Se è impostata su True (Vero), la sincronizzazione fuori banda viene ripetuta fino al completamento dell'operazione.
Use Rhino ECMAScript engine (Usa motore ECMAScript Rhino)	Determina se il motore di Identity Manager deve utilizzare il motore Rhino ECMAScript. Il motore utilizza Rhino come motore ECMAScript di default. Questo controllo è impostato su **true** (vero) di default, se si imposta questo controllo su **false** (falso), il motore utilizza lo script Nashorm.

Opzione	Descrizione
Enable Subscriber Service Channel(Abilita canale Servizio sottoscrittore)	Determina se il motore di Identity Manager deve elaborare le interrogazioni fuori banda sul canale Servizio sottoscrittore del driver. Alcuni esempi comuni di queste interrogazioni sono l'aggiornamento della mappa dei codici, la raccolta dati e le interrogazioni attivate da dxcmd. Se questo controllo è impostato su true (vero), il canale elabora separatamente queste interrogazioni senza interrompere la normale elaborazione degli eventi. Attualmente, questo controllo è disponibile solo per l'utilizzo con il driver di fan-out JDBC (abilitato di default).
Enable password synchronization status reporting (Abilita generazione rapporti sullo stato di sincronizzazione password)	Questo controllo determina se il motore di Identity Manager deve generare rapporti sullo stato degli eventi di modifica della password del sottoscrittore. La generazione di rapporti sullo stato degli eventi di modifica della password del sottoscrittore consente ad applicazioni quali l'applicazione utente Identity Manager di monitorare l'avanzamento della sincronizzazione di una modifica della password da sincronizzare con l'applicazione connessa.
Combine values from template object with those from add operation (Combina i valori dell'oggetto modello con quelli dell'operazione di aggiunta)	Questo valore determina se il motore di Identity Manager deve combinare valori simili da un modello di creazione e da un'operazione di aggiunta durante l'esecuzione dell'operazione di aggiunta. Se si imposta il valore su True (Vero), i valori degli attributi multivalore del modello vengono utilizzati in aggiunta ai valori dello stesso attributo specificati nell'operazione di aggiunta. Se si imposta il valore su False (Falso), i valori del modello vengono ignorati se sono presenti valori provenienti dallo stesso attributo specificato nell'operazione di aggiunta.
Allow event loopback from publisher to subscriber channel (Consenti loopback eventi dal produttore al sottoscrittore)	Questo valore determina se il motore di Identity Manager deve consentire a un evento di eseguire un ciclo dal produttore del driver al sottoscrittore. Se si imposta il valore su False (Falso), il motore di Identity Manager non consente il loopback degli eventi. Se si imposta il valore su True (Vero), il motore di Identity Manager consentirà agli eventi di eseguire un ciclo dal produttore al sottoscrittore.

Opzione	Descrizione
Revert to calculated membership value behavior (Ripristina comportamento del valore di appartenenza calcolato)	Questo valore determina il metodo utilizzato dal motore di Identity Manager durante l'esecuzione di azioni di lettura e ricerca correlate all'appartenenza ai gruppi. Se si imposta questo valore su False (Falso, impostazione di default), il motore di Identity Manager, durante la lettura o la ricerca degli attributi Membro e Membro del gruppo degli oggetti Identity Vault, restituisce solo i valori "statici". I valori statici sono oggetti che hanno ricevuto l'appartenenza al gruppo per assegnazione diretta al gruppo anziché per assegnazione ereditata tramite un gruppo nidificato. Se si imposta questo valore su True (Vero), il motore di Identity Manager tornerà al metodo utilizzato prima di Identity Manager 3.6. Nelle versioni precedenti alla 3.6, la ricerca degli attributi Membro e Membro del gruppo da parte del motore di Identity Manager recuperava tutti i valori "calcolati". I valori calcolati includono oggetti con 1) appartenenza assegnata staticamente o con 2) appartenenza assegnata dinamicamente in virtù dei calcoli della gerarchia dei gruppi nidificati utilizzati da eDirectory. La ricerca dell'attributo Membro del gruppo restituisce tutti gli oggetti assegnati direttamente al gruppo o a cui è stata assegnata l'appartenenza tramite un gruppo nidificato.
Maximum time to wait for driver shutdown in seconds (Tempo massimo di attesa per l'arresto del driver in secondi)	Questa impostazione consente di controllare il tempo massimo di attesa del motore di Identity Manager per l'arresto del produttore del driver. Se il driver non viene arrestato entro l'intervallo di tempo specificato, il motore di Identity Manager lo arresta.
Regular Expression escape meta-characters (Metacaratteri di escape dell'espressione regolare)	Questo controllo determina i metacaratteri di escape durante l'espansione della variabile locale utilizzata in un contesto di espressione regolare. Tutti i caratteri che devono essere preceduti da escape devono essere aggiunti come elenco separato da virgole per questo valore di controllo. Se un metacarattere non è presente nel valore del controllo, non verrà preceduto da escape durante l'espansione della variabile locale contenente un'espressione regolare. Durante l'utilizzo di questo controllo, verificare quanto segue: ◆ Il valore non viene lasciato vuoto. Di default, viene popolato con ***$***. Questo carattere è necessario per l'espansione della variabile locale. ◆ Il valore deve essere un elenco separato da virgole (,), in caso contrario si verificheranno errori durante la valutazione delle policy. ◆ Per utilizzare tutti i metacaratteri di escape, specificare "\,$,^,.,?,*,+,[,],(,),|" come valore. ◆ Se non è necessario utilizzare il metacarattere come carattere di escape, rimuoverlo tale carattere dal valore. ◆ Per utilizzare come escape qualsiasi metacarattere, specificare il metacarattere seguito da una barra rovesciata (\).

Opzione	Descrizione
Ignore Entitlement Changes of other drivers (Ignora modifiche di autorizzazione di altri driver)	Questo controllo determina se il motore di Identity Manager deve ignorare o elaborare le modifiche di autorizzazione di altri driver. Il valore di default è True (Vero). Ciò significa che il driver ignora automaticamente le modifiche di autorizzazione di altri driver. Se questo controllo è impostato su False (Falso), le modifiche di autorizzazione di altri driver vengono memorizzate nella cache ed elaborate da questo driver.
Allow Entitlement event loopback from cprs to subscriber channel (Consenti loopback eventi autorizzazione da cprs a sottoscrittore)	Questo controllo determina se il motore di Identity Manager deve consentire a un evento di autorizzazione generato da un'assegnazione CPRS di eseguire il loopback al sottoscrittore del driver. Il valore di default è False (Falso). Ciò significa che l'evento non è soggetto a loopback al sottoscrittore. Se questo controllo è impostato su True (Vero), l'evento passa al sottoscrittore del driver.

Opzioni di avvio

Le Opzioni di avvio consentono di impostare lo stato del driver all'avvio del server di Identity Manager.

- **Avvio automatico**: il driver viene avviato a ogni avvio del server di Identity Manager.
- **Manuale**: il driver non viene avviato all'avvio del server di Identity Manager. Il driver deve essere avviato mediante il portale di Identity Console.
- **Disabilitato**: il driver dispone di un file di cache in cui sono memorizzati tutti gli eventi. Se il driver è impostato su Disabilitato, questo file viene eliminato e nel file non vengono memorizzati nuovi eventi finché lo stato del driver non viene modificato in Manuale o Avvio automatico.

Dopo aver impostato l'opzione di avvio preferita, fare clic sull'icona di salvataggio  . Per reimpostare l'opzione di avvio, fare clic sull'icona  .

Password con nome

Identity Manager consente di memorizzare in modo sicuro più password per un driver. Questa funzionalità è denominata password con nome. A ogni singola password è possibile accedere mediante una chiave o un nome.

È possibile aggiungere password con nome a un set di driver o a singoli driver. Le password con nome per un set di driver sono disponibili per tutti i driver del set. Le password con nome per un singolo driver sono disponibili solo per tale driver.

Per utilizzare una password con nome in una policy driver, è necessario fare riferimento a essa mediante il nome della password invece di utilizzare la password effettiva, quindi il motore di Identity Manager la invia al driver. Il metodo descritto in questa sezione per la memorizzazione e il recupero delle password con nome può essere utilizzato con qualsiasi driver senza apportare modifiche allo shim del driver.

Per aggiungere una nuova password con nome, fare clic sull'icona  . Per rimuovere una password con nome esistente, fare clic sull'icona . Per salvare l'elenco, fare clic sull'icona .

Sicurezza uguale a

Utilizzare la pagina Sicurezza uguale a per visualizzare o modificare l'elenco degli oggetti dei quali il driver è l'equivalente di sicurezza esplicito. Questo oggetto dispone di tutti i diritti sugli oggetti elencati.

È possibile aggiungere un nuovo oggetto all'elenco Sicurezza uguale a facendo clic sull'icona . Se si aggiunge o si elimina un oggetto dall'elenco, il sistema aggiunge o elimina automaticamente l'oggetto nella proprietà "Sicurezza uguale a se stessi" di tale oggetto. Non è necessario aggiungere all'elenco il trustee [Public] (Pubblico) o i container superiori dell'oggetto, poiché l'oggetto è già definito come equivalente di sicurezza di essi in modo implicito.

Per rimuovere un oggetto esistente dall'elenco, fare clic sull'icona . Per salvare l'elenco, fare clic sull'icona .

Oggetti esclusi

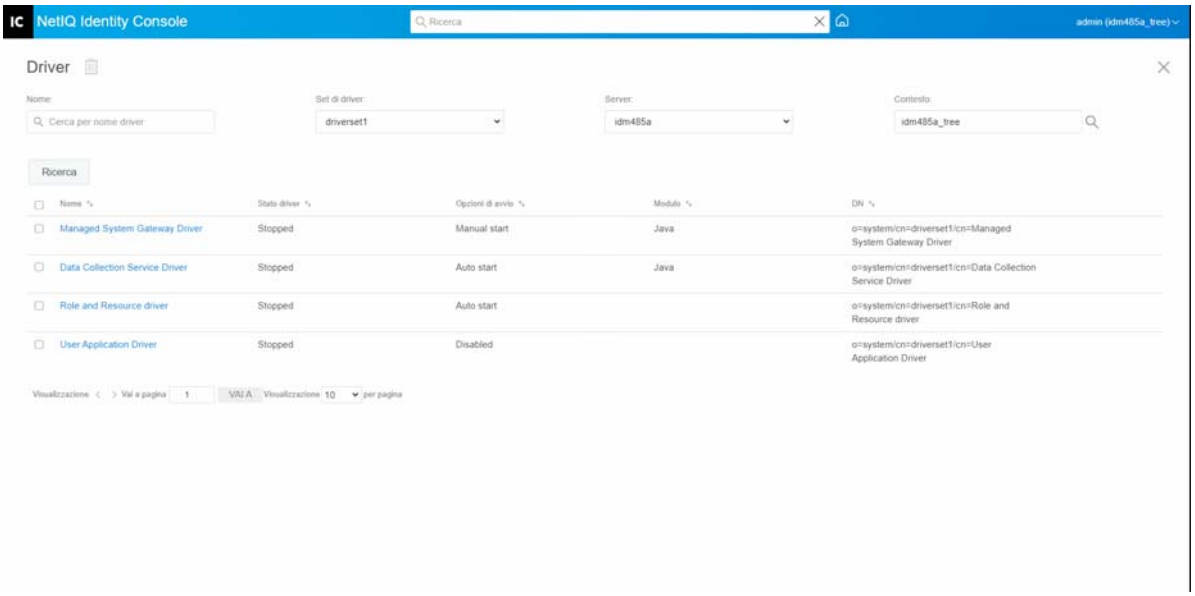
Utilizzare questa opzione per creare un elenco di oggetti che non verranno replicati nell'applicazione. Si consiglia di aggiungere all'elenco tutti gli oggetti che rappresentano un ruolo amministrativo, ad esempio l'oggetto Admin. È possibile aggiungere un nuovo oggetto all'elenco facendo clic sull'icona . Per rimuovere un oggetto esistente dall'elenco, fare clic sull'icona . Per salvare l'elenco, fare clic sull'icona .

Gestione dell'elenco degli attributi con valore

Per aggiungere attributi all'elenco degli attributi con valore per un driver specifico, eseguire le operazioni riportate di seguito:

1. In Identity Console, selezionare il modulo **Gestione oggetti**.
2. Selezionare il tipo **DirXML-Driver** dall'elenco a discesa e fare clic sul pulsante di ricerca.
3. Fare clic sul driver appropriato dall'elenco di ricerca.
4. Per aggiungere attributi senza valore all'elenco di attributi con valore, fare clic sull'icona accanto agli **Attributi con valore** e selezionare gli attributi senza valore appropriati dall'elenco.
5. Al termine, fare clic su **OK**.

Figura 23-2 *Gestione della configurazione dei driver*



Trasformazione e sincronizzazione dati

Questa sezione è suddivisa nelle seguenti categorie:

Visualizzazione sincronizzazione dati

La pagina della panoramica del driver è suddivisa nelle seguenti categorie:

Filtro

Per il driver sono disponibili i filtri che consentono di specificare le classi e gli attributi che un'applicazione può inviare e ricevere da Identity Vault. Se si desidera che una classe specifica passi attraverso il motore di metadirectory per l'elaborazione, è necessario aggiungere la classe al filtro sul canale appropriato. È inoltre possibile filtrare gli oggetti in base a un valore di attributo specifico definito.

Per aggiungere classi e attributi da includere per la sincronizzazione e modificare il filtro del driver, fare clic su **Filtro** nel canale Produttore o Sottoscrittore.

Nota: La rappresentazione grafica della panoramica mostra due oggetti separati per il filtro del driver nei canali Produttore e Sottoscrittore. Sebbene siano visualizzati due oggetti, per entrambi i canali viene utilizzato lo stesso filtro.

Tutte le policy

Di default viene visualizzata la pagina Tutte le policy. È possibile importare una policy esistente nel container facendo clic sull'icona . È inoltre possibile rimuovere tutte le policy non necessarie. Per selezionare un livello di traccia per il driver, fare clic sull'icona . È possibile spostare le policy in alto e in basso nell'elenco utilizzando le icone e .

Nota: Identity Console non supporta l'aggiunta e la distribuzione di nuove policy per i driver. A tal scopo si consiglia di utilizzare iManager e Identity Designer.

Migrazione dei dati in Identity Vault

Con questo task è possibile definire i criteri utilizzati da Identity Manager per eseguire la migrazione degli oggetti da un'applicazione in Identity Vault. Quando si esegue la migrazione di un oggetto, il motore di metadirectory applica all'oggetto tutte le policy Corrispondenza, Posizionamento e Creazione, nonché il filtro Produttore. La migrazione degli oggetti in Identity Vault viene eseguita in base all'ordine specificato nell'elenco Classe. Con questa opzione è possibile eseguire i seguenti task:

1. **Add Class and Attributes** (Aggiungi classe e attributi): per aggiungere o rimuovere classi e attributi di cui si desidera eseguire la migrazione, fare clic sull'icona . Selezionare quindi la classe e i rispettivi attributi da aggiungere. Dopo aver selezionato la classe e gli attributi, fare clic su **Aggiungi** per salvare le modifiche.
2. **Edit Attribute Value** (Modifica valore attributo): per modificare il valore dell'attributo di migrazione specificato durante la modifica dell'elenco, fare clic sull'icona Edit Attribute (Modifica attributo) .
3. **Re-order the Class List** (Riordina elenco delle classi): utilizzare i pulsanti e per modificare l'ordine delle classi nell'elenco. La migrazione degli oggetti in Identity Vault viene eseguita in base all'ordine specificato nell'elenco Classe.
4. **Aggiorna**: fare clic sull'icona per aggiornare l'elenco.

Migrazione dei dati da Identity Vault

Tramite la scheda **Esporta**, è possibile selezionare i container o gli oggetti di cui si desidera eseguire la migrazione da Identity Vault a un'applicazione. Quando si esegue la migrazione di un oggetto, il motore di metadirectory applica all'oggetto tutte le policy Corrispondenza, Creazione e Posizionamento, nonché il filtro Sottoscrittore.

Per eseguire la migrazione di oggetti o container da Identity Vault a un'altra applicazione, fare clic sull'icona  . Individuare e selezionare l'oggetto di cui si desidera eseguire la migrazione, quindi fare clic su **OK** per aggiungere l'oggetto all'elenco di migrazione. Per rimuovere oggetti dall'elenco di migrazione, fare clic sull'icona  .

Dopo aver selezionato gli oggetti di cui si desidera eseguire la migrazione, fare clic su  per iniziare la migrazione. L'avanzamento della migrazione verrà visualizzato sullo schermo. Per interrompere la migrazione, fare clic sul pulsante  .

Sincronizzazione degli oggetti

L'operazione di sincronizzazione ricerca gli oggetti modificati e li sincronizza. È possibile selezionare **Esaminare tutti gli oggetti** per avviare immediatamente la sincronizzazione. In alternativa, è possibile impostare una data e un'ora in cui avviare la sincronizzazione.

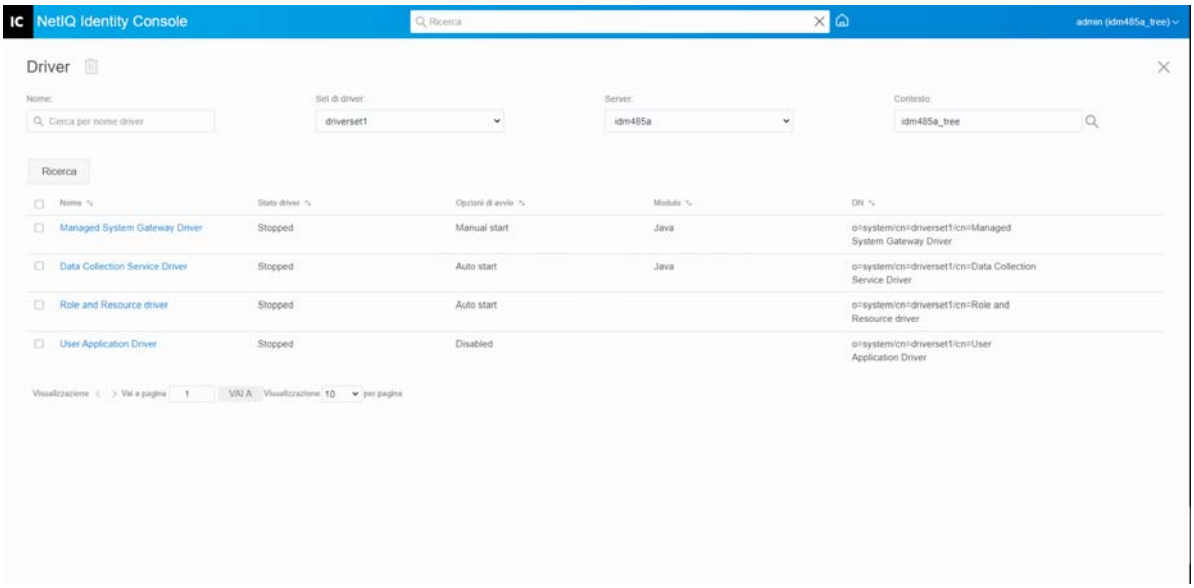
Traccia DirXML Script

L'opzione Tracing DirXML Scripts (Traccia DirXML Script) consente di selezionare un livello di traccia per un driver. Vengono inoltre applicate le impostazioni di traccia a tutti i produttori e sottoscrittori. È possibile scegliere tra le seguenti opzioni di traccia di DirXML Script:

- Traccia per tutti i DirXML Script attivata
- Traccia per tutti i DirXML Script disattivata
- Traccia regola DirXML Script attivata
- Traccia regola DirXML Script disattivata

Fare clic su  per salvare le modifiche.

Figura 23-3 *Gestione della sincronizzazione dati dei driver*



Filtri classe/attributo

I filtri degli attributi e delle classi consentono di specificare le classi e gli attributi che un'applicazione può inviare e ricevere da Identity Vault. Se si desidera che una classe specifica passi attraverso il motore di metadirectory per l'elaborazione, è necessario aggiungere la classe al filtro sul canale appropriato. È inoltre possibile filtrare gli oggetti in base a un valore di attributo specifico definito dall'utente. Tramite questa opzione è possibile eseguire le seguenti azioni:

- **Imposta modello**: utilizzare questa opzione per impostare le opzioni di default per tutti gli attributi aggiunti al filtro. Fare clic sull'icona accanto all'etichetta Filtri classe/attributo.
- **Aggiungere una nuova classe**: aggiungere una nuova classe facendo clic sull'icona .
- **Aggiungere un nuovo attributo**: aggiungere un nuovo attributo facendo clic sull'icona .
- **Copia filtro da**: questa opzione consente di copiare un filtro da un altro driver. Fare clic sull'icona per copiare il filtro.
- **Modifica XML**: modificare le impostazioni del filtro delle classi e degli attributi tramite l'icona Modifica XML.
- **Eliminare classi o attributi**: eliminare una classe o un attributo facendo clic sull'icona accanto alla rispettiva classe o attributo.

È possibile impostare le seguenti opzioni per un valore di classe e di attributo sia sul produttore che sullo sottoscrittore:

- Sincronizza
- Ignora
- Notifica
- Reimposta

Unisci autorità

Se un attributo non viene sincronizzato in entrambi i canali, non viene eseguita alcuna unione.

Se un attributo viene sincronizzato in un canale e non nell'altro, tutti i valori esistenti nella destinazione del canale vengono rimossi e sostituiti con quelli dell'origine per tale canale. Se l'origine dispone di più valori e la destinazione può contenere un solo valore, viene utilizzato solo uno dei valori sul lato di destinazione.

Se un attributo viene sincronizzato in entrambi i canali e entrambi i lati possono contenere un solo valore, l'applicazione connessa acquisisce i valori memorizzati in Identity Vault a meno che Identity Vault non disponga di alcun valore. In questo caso, Identity Vault acquisisce i valori dall'applicazione connessa.

Se un attributo viene sincronizzato in entrambi i canali e solo un lato è in grado di contenere più valori, il valore del canale con valore singolo viene aggiunto al canale multivalore se non è già presente. Se non è presente alcun valore sul lato singolo, è possibile scegliere il valore da aggiungere al lato singolo. È possibile impostare le seguenti opzioni per Unisci autorità:

- Predefinito
- Identity Vault
- Applicazione
- Nessuno

Fare clic su per salvare le modifiche.

Script ECMA

Visualizza un elenco ordinato di file di risorse ECMAScript. I file contengono definizioni di estensione per il driver caricato da Identity Manager all'avvio del driver. È possibile importare file aggiuntivi facendo clic su , rimuovere i file esistenti facendo clic su o modificare l'ordine di esecuzione dei file. È inoltre possibile spostare gli script in alto o in basso nell'elenco. È possibile salvare l'elenco di script ECMA facendo clic sull'icona .

Mappatura di attributi reciproci

Le mappature di attributi reciproci consentono di creare e gestire i backlink (o riferimenti) tra oggetti. Ad esempio, l'oggetto Gruppo include un attributo Membri che fa riferimento a tutti gli oggetti Utente appartenenti a tale gruppo. Analogamente, ciascun oggetto Utente include un attributo Appartenenza gruppo che fa riferimento agli oggetti Gruppo di cui l'utente è membro. Affinché il motore di metadirectory mantenga l'oggetto Gruppo > attributo Membri sincronizzato con l'oggetto Utente > attributo Appartenenza gruppo per tutti gli oggetti Gruppo e Utente in Identity Vault, è necessario collegare tali attributi. I collegamenti tra gli attributi dell'oggetto sono noti come mappature di attributi reciproci.

Tramite questo modulo è possibile eseguire le seguenti azioni:

- “Creazione di mappature di attributi reciproci personalizzate” a pagina 165
- “Aggiunta di una nuova mappatura di attributi reciproci” a pagina 165

Creazione di mappature di attributi reciproci personalizzate

Questa sezione è applicabile solo se nella pagina Mappatura di attributi reciproci è visualizzata la richiesta **Il driver non contiene mappature di attributi reciproci personalizzate. Fare clic sull'icona '+' in alto per creare mappature di attributi reciproci di base**.

1. Fare clic sull'icona + per creare un nuovo elenco di mappature di attributi reciproci personalizzate.
2. Vengono visualizzate le mappature di attributi di default del driver. È ora possibile aggiungere mappature oppure modificare o eliminare quelle esistenti.

Aggiunta di una nuova mappatura di attributi reciproci

Quando si crea una mappatura di attributi reciproci, è necessario aggiungere prima uno degli attributi all'elenco delle mappature reciproche.

1. Fare clic sull'icona + accanto al menu a discesa Azioni.
2. Nella nuova voce di attributo, selezionare l'attributo desiderato dall'elenco a discesa.
3. Specificare i dettagli della mappatura reciproca:
   - 3a **Classe di origine**: specifica il nome della classe a cui è associato l'attributo nell'elenco delle mappature. Ad esempio, se l'attributo Appartenenza gruppo è stato inserito nell'elenco delle mappature reciproche, la classe di origine associata è Utente.
   - 3b **Classe di destinazione**: specifica il nome della classe associata all'attributo per cui si desidera creare una mappatura reciproca. Ad esempio, se l'attributo Appartenenza gruppo è stato inserito nell'elenco delle mappature reciproche, la classe di destinazione associata è Gruppo.
   - 3c **Attributo reciproco**: specifica il nome dell'attributo per cui si desidera creare una mappatura reciproca.
4. Se si desidera mappare l'attributo a un altro attributo reciproco, fare clic sull'icona + a destra del nome dell'attributo.

   Alla fine dell'elenco degli attributi viene aggiunta una nuova sezione per l'attributo. Selezionare la classe di origine, la classe di destinazione e l'attributo reciproco.

Rimozione di una mappatura di attributi reciproci

Per rimuovere una mappatura di attributi reciproci:

1. Selezionare la casella di controllo relativa alla mappatura di attributi reciproci che si desidera eliminare in corrispondenza della **Classe di origine**.
2. Fare clic sull'icona accanto all'elenco a discesa degli attributi.

Rimozione di un attributo dall'elenco delle mappature reciproche

Per rimuovere un attributo dall'elenco delle mappature reciproche:

1. Selezionare l'attributo che si desidera rimuovere selezionando la casella di controllo corrispondente all'attributo.
2. Fare clic sull'icona accanto all'elenco a discesa **Azioni**.

Riordinamento degli attributi mappati

Le mappature di attributi vengono risolte nell'ordine elencato, dall'alto verso il basso. È possibile spostare gli attributi mappati verso l'alto o il basso nell'elenco per assicurarsi che vengano risolti nell'ordine corretto. In generale, è consigliabile elencare prima le mappature specifiche seguite dalle mappature più generali. Ad esempio, una mappatura per l'attributo Membro su un oggetto Gruppo deve essere elencata prima di una mappatura per l'attributo Membro su qualsiasi oggetto (opzione <Any Class>, Qualsiasi classe).

Selezionare la casella di controllo corrispondente all'attributo mappato che si desidera spostare, quindi fare clic su per spostare l'attributo verso l'alto o su per spostarlo verso il basso.

Rimozione della mappatura di attributi reciproci personalizzata

È possibile eliminare le mappature di attributi personalizzate create. In questo modo il motore di metadirectory utilizza le mappature di attributi di default per il driver.

Per rimuovere una mappatura di attributi reciproci personalizzata, fare clic sull'icona nella parte superiore della schermata.

Modifica del codice XML dell'attributo reciproco

Se necessario, è possibile modificare direttamente il codice XML per un attributo reciproco. A questo scopo, fare clic sull'icona Modifica XML nella pagina Mappature di attributi reciproci personalizzate. Viene aperto un editor XML di base che consente di modificare il codice XML. Al termine, fare clic su OK o Annulla per chiudere l'editor XML.

Impostazioni avanzate

Le impostazioni avanzate sono suddivise nelle seguenti categorie:

Gestione delle autorizzazioni

La pagina Autorizzazioni contiene una tabella che mostra tutte le autorizzazioni attualmente definite nel driver selezionato (elencate con il proprio nome distinto completo). In questa pagina sono consentite le seguenti azioni:

- **Edit in XML**(Modifica in XML): per modificare le autorizzazioni nel file XML, selezionare l'autorizzazione dall'elenco e fare clic sull'icona . Selezionare quindi la casella **Enable XML Editing** (Abilita modifica XML).
- **Elimina**: per eliminare un'autorizzazione, fare clic sulla casella a sinistra del nome dell'autorizzazione, quindi fare clic sull'icona . Viene visualizzato un messaggio che indica che l'operazione non può essere annullata e viene chiesto se si desidera procedere con l'eliminazione dell'autorizzazione selezionata. Fare clic su **OK** per eliminare l'autorizzazione oppure su **Annulla** per interrompere l'operazione. È possibile selezionare più caselle per eliminare più autorizzazioni oppure fare clic sulla casella in alto a sinistra per eliminare tutte le autorizzazioni.

Gestione della tabella mappature oggetti

Le policy di Identity Manager utilizzano le tabelle mappature per mappare un set di valori a un altro set di valori corrispondenti. Quando si installa il pacchetto delle autorizzazioni, le policy del pacchetto vengono aggiunte al set di policy di avvio del driver. Il driver esegue tali policy solo una volta all'avvio del driver. Per ulteriori informazioni, vedere Mapping Table Objects (Oggetti della tabella mappature) nella *NetIQ Identity Manager Driver Administration Guide* (Guida all'amministrazione dei driver di NetIQ Identity Manager).

Tramite la tabella mappature oggetti è possibile eseguire le seguenti azioni:

- **Modificare una mappatura esistente**: per modificare una tabella mappature oggetti esistente, fare clic sulla mappatura dall'elenco ed eseguire le azioni seguenti nella schermata successiva:
  - Aggiungere una nuova colonna.

    Specificare un valore per la colonna, quindi scegliere se il valore fa distinzione o meno tra maiuscole e minuscole o se è numerico.
  - Aggiungere una nuova riga e specificare un valore per la riga.
  - Fare clic sull'icona .

- **Eliminare una mappatura**: per rimuovere una mappatura dall'elenco, selezionare la mappatura appropriata dall'elenco e fare clic sull'icona .
- **Modificare in XML**: per modificare una mappatura nel file XML, fare clic sulla mappatura dall'elenco e selezionare l'icona . Selezionare quindi la casella **Enable XML Editing** (Abilita modifica XML.

Gestione dei processi per i driver

Identity Console consente di pianificare gli eventi utilizzando l'opzione Processi per tutti i singoli driver.

La pagina Job Scheduler (Pianificazione processi) contiene il nome del processo, indica se il processo è abilitato o disabilitato, quando è pianificato per l'esecuzione e la descrizione del processo. Fare clic sul nome del processo per visualizzare la pagina Job (Processo). Fare clic sull'icona di abilitazione/disabilitazione nella colonna Abilitato per abilitare o disabilitare il processo. Fare clic sulla descrizione del processo per visualizzarne la descrizione completa.

La scheda Processi contiene una tabella che mostra gli oggetti processo esistenti per il driver selezionato, elencato con il nome distinto completo nella voce Driver.

La pagina Job Scheduler (Pianificazione processi) consente di eseguire i seguenti task:

- **Creare il processo**: fare clic sull'icona per creare un nuovo processo.

  Nella finestra popup **Nuovo processo**, eseguire le seguenti operazioni per creare un nuovo processo:

  1. Specificare il nome del processo.
  2. Selezionare il tipo di processo.
  3. Fare clic sull'icona e selezionare il server in cui eseguire il processo dall'elenco di server disponibili. In alternativa, specificare il nome di un server e selezionare il server.
  4. Fare clic sul pulsante **Crea**.
- **Avviare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Arrestare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Abilitare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Disabilitare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Ottenere lo stato**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .
- **Eliminare il processo**: selezionare un processo facendo clic sulla casella a sinistra del processo, quindi fare clic sull'icona .

Fare clic su un processo per accedere alla pagina **Job Property** (Proprietà processo). Qui è possibile impostare la modalità di esecuzione del processo.

Generale: mostra il nome della classe Java del processo. Utilizzare questa pagina per abilitare o disabilitare il processo, per eliminarlo dopo l'esecuzione, per selezionare il server o i server in cui deve essere eseguito, per specificare il server e-mail e assegnare al processo un nome visualizzato e una descrizione diversi.

Pianificazione: consente di impostare quando eseguire il processo. Specificare un valore temporale per l'opzione Avvia processo alle e se eseguire il processo giornalmente, settimanalmente, mensilmente o annualmente. È inoltre possibile personalizzare quando eseguire il processo oppure abilitare l'interruttore per eseguirlo manualmente.

Ambito: consente di definire gli oggetti a cui applicare il processo. Un oggetto può essere un container, un gruppo dinamico, un gruppo o un oggetto Foglia. Fare clic su Aggiungi per selezionare l'oggetto a cui si desidera applicare il processo. È possibile utilizzare il pulsante Sfoglia per selezionare un oggetto, quindi fare clic su OK. Per rimuovere un oggetto dall'elenco di ambiti, selezionare un oggetto ambito facendo clic sulla casella a sinistra dell'oggetto DN, quindi fare clic su Rimuovi.

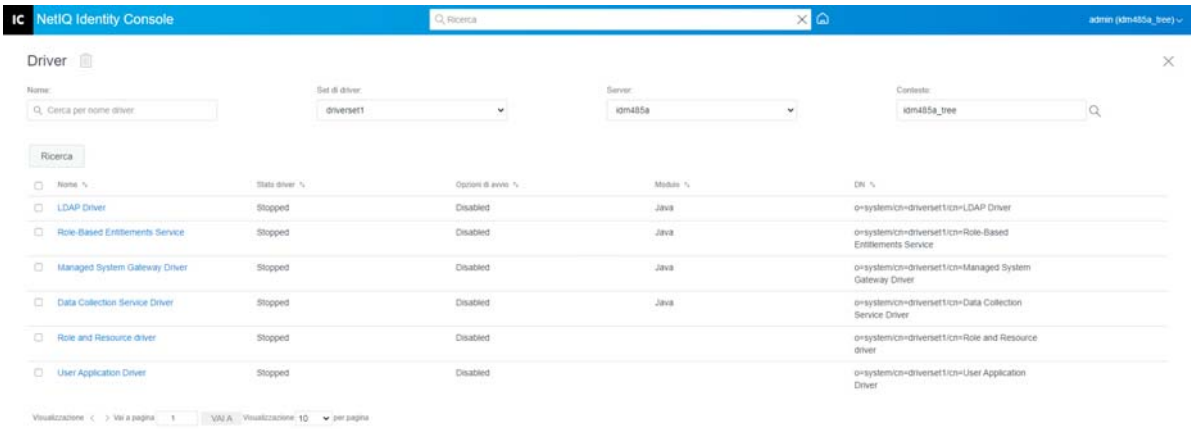
Quando si aggiunge un oggetto, selezionarlo per visualizzare ulteriori opzioni. Se si seleziona un oggetto Gruppo, è possibile applicare il processo ai membri del gruppo o solo al gruppo. Se si seleziona un oggetto Container, è possibile applicare il processo a tutti gli elementi discendenti di tale container, a tutti gli elementi secondari del container o solo al container.

Parametri: consente di aggiungere ulteriori parametri al processo e di visualizzare i parametri così come sono attualmente impostati. Questi parametri cambiano a seconda del tipo di processo selezionato.

Risultati: consente di definire le attività da eseguire con i risultati del processo. La pagina Risultati è suddivisa in due parti: Intermediate Result (Risultato intermedio) e Final Result (Risultato finale), con i seguenti risultati consentiti: Operazione completata, Avviso, Errore e Interrotti. A destra della colonna Risultati è presente la colonna Azione. Facendo clic sulla colonna Azione è possibile impostare la modalità di notifica desiderata per ciascun risultato. Le azioni includono l'invio di un risultato di revisione o l'invio di un'e-mail al completamento del risultato. Se non si seleziona un'opzione, non viene eseguita alcuna azione per il risultato.

Nella scheda **Traccia** è possibile configurare la traccia per un driver specifico. Per ulteriori informazioni, vedere “Configurazione del livello di traccia” a pagina 171.

Figura 23-4 *Gestione delle impostazioni avanzate*



Configurazione dei livelli di log e di traccia dei driver

Per configurare il log e la traccia per i driver, selezionare la scheda **Driver** > **Configurazione log e traccia** nella pagina principale di Identity Console. Questa sezione è suddivisa nelle seguenti categorie:

- “Configurazione del livello di log” a pagina 170
- “Configurazione del livello di traccia” a pagina 171

Configurazione del livello di log

Ciascun driver dispone di un campo del livello di log in cui è possibile definire il livello degli errori di cui tenere traccia. Il livello qui configurato determina quali messaggi sono disponibili per i log. Di default, il livello di log è impostato per tenere traccia dei messaggi di errore. Sono inclusi anche i messaggi di errore irreversibile. Per tenere traccia di altri tipi di messaggi, modificare il livello di log. Per configurare il livello di log, selezionare la scheda **Configurazione log e traccia** > **Livello log**. La seguente tabella descrive le impostazioni del livello di log:

Opzione	Descrizione
Utilizza impostazioni log da set di driver	Se questa opzione è selezionata, il driver registra gli eventi in base alle impostazioni di log dell'oggetto set di driver.
Disattivare la registrazione dei log del set di driver, del sottoscrittore e del produttore.	Disattiva del tutto la registrazione per questo driver dell'oggetto set di driver, del sottoscrittore e del produttore.
Numero massimo di voci nel log (50-500)	Numero di voci nel log. Il valore di default è 50.

Opzione	Descrizione
Livelli di log	È possibile scegliere tra i seguenti livelli di log: ◆ **Registra errori**: registra solo gli errori ◆ Registra errori e avvisi: registra gli errori e gli avvisi ◆ **Registra eventi specifici**: registra gli eventi selezionati. Se si seleziona questa opzione, viene abilitato il seguente elenco di eventi: ◆ **Eventi motore di metadirectory** ◆ **Eventi di stato** ◆ **Eventi operazione** ◆ **Eventi di trasformazione** ◆ **Eventi provisioning credenziali** ◆ **Aggiorna solo l'ora ultimo log**: aggiorna l'ora dell'ultimo log. ◆ **Registrazione disattivata**: disattiva la registrazione per il driver.

Configurazione del livello di traccia

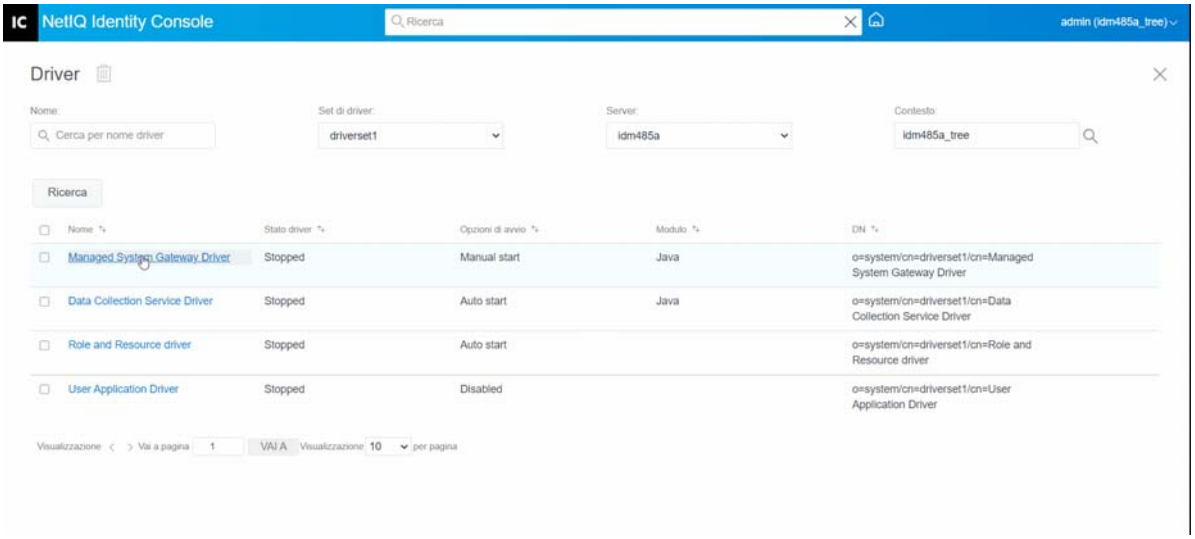
È possibile configurare la traccia per un driver specifico. A seconda del livello di traccia specificato per un driver, la traccia visualizza gli eventi correlati al driver quando il motore elabora gli eventi. Il livello di traccia del driver influisce solo sul driver o sul set di driver su cui è impostata la traccia. Se si utilizza l'oggetto Configurazione del caricatore remoto, il file di traccia dell'oggetto Configurazione del caricatore remoto viene impostato direttamente sull'oggetto Configurazione del caricatore remoto e contiene solo la traccia dello shim del driver.

Per configurare la traccia per un driver, selezionare la scheda **Configurazione log e traccia** > **Traccia**. La seguente tabella descrive le impostazioni della traccia:

Parametro	Driver
Livello di traccia	All'aumentare del livello di traccia del driver, aumenta la quantità di informazioni visualizzate in Traccia. Il livello di traccia 1 mostra gli errori ma non la loro causa. Se si desidera visualizzare le informazioni sulla sincronizzazione delle password, impostare il livello di traccia a 5. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.
File di traccia	Specificare un nome file e l'ubicazione in cui vengono scritte le informazioni di Identity Manager per il driver selezionato. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.

Parametro	Driver
Nome della traccia	Ai messaggi di traccia del driver viene aggiunto come prefisso il valore immesso anziché il nome del driver. Utilizzare questa opzione se il nome del driver è molto lungo.
Codifica file di traccia	Il file di traccia utilizza la codifica di default del sistema. Se necessario, è possibile specificare un'altra codifica.
Limite dimensione file di traccia	Consente di impostare un limite per il file di traccia Java. Se si imposta la dimensione del file su Nessun limite, le dimensioni del file aumentano fino all'esaurimento dello spazio su disco. **Nota:** se si imposta il limite delle dimensioni del file, il file di traccia viene creato in più file. Identity Manager divide automaticamente le dimensioni massime dei file per dieci e crea dieci file separati. La dimensione combinata di questi file equivale alla dimensione massima del file di traccia. Se si seleziona **Use setting from Driver Set** (Usa impostazione da set di driver), il valore viene preso dal set di driver.

Figura 23-5 *Gestione dei livelli di log e di traccia dei driver*



Controllo dei driver

È possibile utilizzare Controllo driver per visualizzare informazioni dettagliate sugli oggetti associati a un set di driver. Questa sezione è suddivisa nelle seguenti categorie:

- “Controllo driver” a pagina 173
- “Controllo cache del driver” a pagina 174
- “Controllo cache sincronizzazione fuori banda” a pagina 175
- “Manifesto del driver” a pagina 175
- “Monitoraggio dello stato del driver” a pagina 175

Controllo driver

Per visualizzare gli oggetti associati a un driver:

1. In Identity Console, selezionare **Driver** > **Controllo** > scheda **Controllo driver**.
2. Nel campo **Driver**, specificare il nome distinto completo del driver che si desidera controllare oppure fare clic sull'icona Sfoglia per individuare e selezionare il driver desiderato.
3. Dopo aver selezionato il driver da controllare, fare clic su **OK** per visualizzare la pagina Controllo driver.

   Nella pagina vengono visualizzate le informazioni sugli oggetti associati al driver selezionato. È possibile eseguire le seguenti azioni:

   - **Elimina:** rimuove l'associazione tra il driver e un oggetto. Selezionare la casella di controllo corrispondente all'oggetto che non si desidera più associare al driver, fare clic sull'icona  , quindi fare clic su **OK** per confermare l'eliminazione.
   - **Aggiorna:** selezionare l'icona di aggiornamento per leggere nuovamente tutti gli oggetti associati al driver e aggiornare le informazioni.
   - **Mostra:** selezionare il numero di associazioni da visualizzare per pagina. È possibile selezionare un numero predefinito (25, 50 o 100) oppure specificare un altro numero a scelta. Il valore di default è 10 associazioni per pagina. Se sono presenti più associazioni rispetto al numero visualizzato, è possibile utilizzare i pulsanti freccia per visualizzare le pagine di associazioni successive e precedenti.
   - **Azioni:** eseguire azioni sugli oggetti associati al driver. Fare clic su **Azioni**, quindi selezionare una delle seguenti opzioni:
     - **Mostra tutte le associazioni:** visualizza tutti gli oggetti associati al driver.
     - **Filtro per associazioni in stato Disabilitato:** visualizza tutti gli oggetti associati al driver con stato Disabilitato.
     - **Filtro per associazioni in stato Manuale:** visualizza tutti gli oggetti associati al driver con stato Manuale.
     - **Filtro per associazioni in stato Migrazione:** visualizza tutti gli oggetti associati al driver il cui stato è Migrazione.
     - **Filtro per associazioni in stato In sospeso:** visualizza tutti gli oggetti associati al driver con stato In sospeso.
     - **Filtro per associazioni in stato Elaborato:** visualizza tutti gli oggetti associati al driver con stato Elaborato.
     - **Filtro per associazioni in stato Non definito:** visualizza tutti gli oggetti associati al driver con uno stato Non definito.
     - **Riepilogo associazioni:** visualizza lo stato di tutti gli oggetti associati al driver.
   - **DN oggetto:** visualizza il DN degli oggetti associati.
   - **Stato:** visualizza lo stato di associazione dell'oggetto.
   - **ID oggetto:** visualizza il valore dell'associazione.

Controllo cache del driver

È possibile visualizzare le transazioni in un file della cache del driver utilizzando Identity Console. Il **Controllo cache del driver** visualizza informazioni sul file della cache, incluso un elenco degli eventi che devono essere elaborati dal driver.

1. In Identity Console, selezionare **Driver** > **Controllo** > scheda **Controllo cache del driver**.
2. Nel campo **Driver**, specificare il nome distinto completo del driver di cui si desidera ispezionare la cache oppure fare clic sull'icona Sfoglia per individuare e selezionare il driver desiderato, quindi fare clic su **OK** per visualizzare la pagina Controllo cache del driver.

   Il file di cache di un driver può essere letto solo quando il driver non è in esecuzione. Se il driver viene arrestato, nella pagina Controllo cache del driver viene visualizzata la cache. Se il driver è in esecuzione, nella pagina viene visualizzata la nota `Il driver non è stato arrestato, impossibile leggere la cache` al posto delle voci della cache. Per arrestare il driver, fare clic sul pulsante  ; la cache viene quindi letta e visualizzata.

   - **Cache del driver sul server:** elenca il server che contiene questa istanza del file della cache. Se il driver è in esecuzione su più server, è possibile selezionare un altro server nell'elenco per visualizzare il file della cache del driver per tale server.
   - **Icone Avvia/Arresta driver:** visualizzano lo stato corrente del driver e consente di avviarlo o arrestarlo. La cache può essere letta solo quando il driver è arrestato.
   - **Elimina:** selezionare le voci nella cache, quindi fare clic sull'icona  per rimuoverle dal file di cache.
   - **Azioni:** consente di eseguire azioni sulle voci nel file di cache. Fare clic su **Azioni** per espandere il menu, quindi selezionare una delle seguenti opzioni:
     - **Cancella tutti gli eventi nella cache:** consente di cancellare tutti gli eventi memorizzati nella cache.
     - **Riepilogo cache:** riepiloga tutti gli eventi memorizzati nel file della cache.

Visualizzazione dei dettagli del sistema connesso per i driver

Per visualizzare i dettagli del sistema connesso per un driver specifico, eseguire le azioni riportate di seguito:

1. In Identity Console, fare clic sul modulo **Controllo oggetti**.
2. Individuare e selezionare l'oggetto driver specifico per il quale si desidera visualizzare i sistemi connessi.
3. Sul computer verranno visualizzati tutti i dettagli del sistema connesso per l'oggetto Driver selezionato.

Controllo cache sincronizzazione fuori banda

Per visualizzare gli eventi nella cache di sincronizzazione fuori banda:

1. In Identity Console, selezionare **Driver** > **Controllo** > scheda **Controllo cache sincronizzazione fuori banda**.
2. Nel campo **Driver**, specificare il nome distinto completo del driver di cui si desidera controllare la cache oppure fare clic sull'icona Sfoglia per individuare e selezionare il driver desiderato, quindi fare clic su **OK**.

   Il file di cache di un driver può essere letto solo quando il driver non è in esecuzione. Se il driver viene arrestato, nella pagina Controllo cache del driver viene visualizzata la cache. Se il driver è in esecuzione, nella pagina viene visualizzata la nota `Il driver non è stato arrestato, impossibile leggere la cache` al posto delle voci della cache. Per arrestare il driver, fare clic sul pulsante  ; la cache viene quindi letta e visualizzata.

   - **Nome file di cache:** visualizza il nome del file di cache.
   - **Cache del driver sul server:** elenca il server che contiene questa istanza del file della cache. Se il driver è in esecuzione su più server, è possibile selezionare un altro server nell'elenco per visualizzare il file della cache del driver per tale server.
   - **Icone Avvia/Arresta driver:** visualizzano lo stato corrente del driver e consente di avviarlo o arrestarlo. La cache può essere letta solo quando il driver è arrestato.
   - **Elimina:** selezionare le voci nella cache, quindi fare clic sull'icona  per rimuoverle dal file di cache.
   - **Azioni:** consente di eseguire azioni sulle voci nel file di cache. Fare clic su **Azioni** per espandere il menu, quindi selezionare una delle seguenti opzioni:
     - **Riepilogo cache:** riepiloga tutti gli eventi memorizzati nel file della cache.
     - **Cancella tutti gli eventi nella cache:** consente di cancellare tutti gli eventi memorizzati nella cache.

Manifesto del driver

Il manifesto del driver è simile a un curriculum per il driver. Indica gli elementi supportati dal driver e include alcune impostazioni di configurazione. Il Manifesto del driver deve essere fornito dallo sviluppatore del driver. In genere, un amministratore di rete non deve modificare il Manifesto del driver. Se l'amministratore desidera modificare il manifesto del driver, è possibile farlo selezionando **Driver** > **Controllo** > **Manifesto del driver** > **Enable XML Editing** (Abilita modifica XML).

Monitoraggio dello stato del driver

Il monitoraggio dello stato del driver consente di visualizzare lo stato corrente di un driver tramite i colori verde, giallo o rosso, nonché di definire le azioni da eseguire in risposta a ciascuno di questi stati.

È possibile creare le condizioni (criteri) che determinano ciascuno stato ed è possibile definire le azioni eseguite ogni volta che cambia lo stato del driver. Ad esempio, se lo stato del driver cambia da verde a giallo, è possibile eseguire azioni come il riavvio del driver, la chiusura del driver e l'invio di un'e-mail alla persona delegata per la risoluzione dei problemi relativi al driver.

Tramite questo modulo è possibile eseguire i seguenti task:

- “Modifica delle condizioni di stato del driver” a pagina 176
- “Modifica delle azioni di stato del driver” a pagina 178
- “Creazione di uno stato personalizzato” a pagina 180
- “Modifica di uno stato personalizzato” a pagina 180

Modifica delle condizioni di stato del driver

È possibile controllare le condizioni che determinano ciascuno stato. Lo stato di colore verde rappresenta un driver integro e uno stato di colore rosso rappresenta un driver non integro.

Le condizioni per lo stato di colore verde vengono valutate per prime. Se il driver non soddisfa le condizioni di colore verde, vengono valutate le condizioni di colore giallo. Se il driver non soddisfa le condizioni di colore giallo, al driver viene assegnato automaticamente lo stato di colore rosso.

Per modificare le condizioni di uno stato:

1. In Identity Console, aprire la pagina Configurazione di stato del driver relativa al driver di cui si desidera modificare le condizioni:
   - **1a** Aprire la home page di Identity Console.
   - **1b** Selezionare **Driver** > **Fare clic sul driver appropriato dall'elenco** > **Controllo** > **Configurazione di stato del driver**.
2. Fare clic sulla scheda dello stato (Verde o Giallo) da modificare.

   La scheda visualizza le condizioni correnti relative allo stato. Le condizioni sono organizzate in gruppi e gli operatori logici AND oppure OR vengono utilizzati per combinare ciascuna condizione e ciascun gruppo. Si consideri l'esempio seguente per lo stato Verde:

   ```
   GROUP1
   Condition1 and
   Condition2
   Or
   GROUP2
   Condition1 and
   Condition2 and
   Condition3
   ```

   Nell'esempio, al driver viene assegnato uno stato Verde se le condizioni di GROUP1 o GROUP2 vengono valutate come vere. Se nessuno dei gruppi di condizioni è vero, vengono valutate le condizioni per lo stato Giallo.

   Le condizioni che possono essere valutate sono:

   - **Stato driver:** in esecuzione, arrestato, in fase di avvio, non in esecuzione o in fase di chiusura. Ad esempio, una delle condizioni di default per lo stato Verde è che il driver è in esecuzione.
   - **Driver in overflow cache:** lo stato della cache utilizzata per la memorizzazione delle transazioni del driver. Se il driver è in overflow della cache, significa che è stata utilizzata tutta la cache disponibile. Ad esempio, la condizione di default per lo stato Verde è che la condizione Driver in overflow cache sia falsa e la condizione di default per lo stato Giallo è che la condizione Driver in overflow cache sia vera.

- **Più recente:** l'età della transazione più recente nella cache.
- **Meno recente:** l'età della transazione meno recente nella cache.
- **Dimensione totale:** la dimensione della cache.
- **Dimensione non elaborata:** la dimensione di tutte le transazioni non elaborate nella cache.
- **Transazioni non elaborate:** il numero di transazioni non elaborate nella cache. È possibile specificare tutti i tipi di transazione o tipi di transazione specifici (ad esempio aggiunte, rimozioni o ridenominazioni).
- **Cronologia transazioni:** numero di transazioni elaborate in vari punti del sottoscrittore o del produttore in un determinato periodo di tempo. Questa condizione utilizza più elementi nel seguente formato:

  <*tipo di transazione*> <*ubicazione della transazione e periodo di tempo*> <*operatore relazionale*> <*numero transazione*>.

  - <*tipo di transazione*>: specifica il tipo di transazione valutata. Può trattarsi di tutte le transazioni, aggiunte, rimozioni, ridenominazioni e così via.
  - <*ubicazione della transazione e periodo di tempo*>: specifica la posizione nel sottoscrittore o nel produttore e il periodo di tempo valutato. Ad esempio, è possibile valutare il numero totale di transazioni elaborate come eventi riportati del produttore nelle ultime 48 ore. Di default, i dati della cronologia delle transazioni vengono conservati per due settimane; pertanto, non è possibile specificare un periodo di tempo superiore a due settimane, a meno che non venga modificata l'impostazione Transaction Data Duration (Durata dati transazione) di default.
  - <*operatore relazionale*>: specifica che le transazioni identificate devono essere uguali a, diverse da, minori di, minori o uguali a, maggiori di o maggiori o uguali al <numero transazione>.
  - <*numero transazione*>: specifica il numero di transazioni utilizzate nella valutazione.

  Di seguito viene riportato un esempio di condizione Cronologia transazioni:

  ```
  <numero di aggiunte> <come comandi produttore> <negli ultimi 10 minuti> <è minore di> <1000>
  ```

- **Cronologia disponibile:** la quantità di dati della cronologia delle transazioni disponibili per la valutazione. Lo scopo principale di questa condizione è garantire che la condizione Cronologia transazioni non causi errori nello stato attuale perché non dispone di dati della cronologia delle transazioni sufficienti per il periodo di tempo in fase di valutazione.

  Ad esempio, si supponga di voler utilizzare la condizione Cronologia transazioni per valutare il numero di aggiunte come comandi produttore nelle ultime 48 ore (l'esempio mostrato nella sezione Cronologia transazioni illustrata in precedenza). Tuttavia, non si desidera che la condizione generi un errore se non sono ancora disponibili dati per la durata di 48 ore, ad esempio dopo la configurazione iniziale dello stato del driver o se il server del driver viene riavviato (poiché i dati della cronologia delle transazioni sono conservati in memoria). Di conseguenza, è possibile creare gruppi di condizioni simili ai seguenti:

  ```
  Cronologia disponibile di Group1 <è minore di> <48 ore> o la Cronologia disponibile di Group2 <è maggiore o uguale a> <48 ore> e la Cronologia transazioni <numero di aggiunte> <come comandi produttore> <nelle ultime 48 ore> <è minore di> <1000>
  ```

Lo stato viene valutato come vero se uno dei gruppi di condizioni è vero, vale a dire che a) sono disponibili meno di 48 ore di dati o b) sono disponibili almeno 48 ore di dati e il numero di aggiunte come comandi produttore nelle ultime 48 ore è inferiore a 1000.

Lo stato viene valutato come falso se entrambe le condizioni vengono valutate come false, vale a dire che a) sono disponibili almeno 48 ore di dati e b) il numero di aggiunte come comandi produttore nelle ultime 48 ore è maggiore di 1000.

3 Modificare i criteri in base alle necessità.

- Per aggiungere un nuovo gruppo, fare clic sull'icona + accanto ai **Gruppi di condizioni**.
- Per aggiungere una condizione, fare clic sull'icona + accanto agli operatori logici (AND/OR). In alternativa, è anche possibile fare clic sul collegamento **Aggiungi nuova condizione**.
- Per riordinare i gruppi di condizioni o le singole condizioni, selezionare la casella di controllo accanto al gruppo o alla condizione che si desidera spostare, quindi fare clic sui pulsanti freccia per spostare il gruppo o la condizione verso l'alto o il basso. È inoltre possibile utilizzare i pulsanti freccia per spostare una condizione da un gruppo a un altro.

4 Al termine, salvare le modifiche facendo clic sul pulsante **Salva**.

5 Se si desidera modificare le azioni associate alle condizioni impostate, continuare con "Modifica delle azioni di stato del driver" a pagina 178.

Modifica delle azioni di stato del driver

È possibile determinare le azioni che si desidera eseguire quando cambia lo stato del driver. Ad esempio, se lo stato cambia da Verde a Giallo, è possibile arrestare o riavviare il driver, generare un evento o avviare un workflow. Oppure, se lo stato cambia da Giallo a Verde, vengono eseguite tutte le azioni associate allo stato Verde.

Le azioni di uno stato vengono eseguite una sola volta ogni volta che vengono soddisfatte le condizioni; finché lo stato rimane vero, le azioni non vengono ripetute. Se lo stato cambia perché le sue condizioni non sono più soddisfatte, le azioni vengono nuovamente eseguite al successivo verificarsi delle condizioni.

1 In Identity Console, aprire la pagina Configurazione di stato del driver relativa al driver di cui si desidera modificare le azioni:

1a Aprire la home page di Identity Console.

1b Selezionare **Driver** > **Fare clic sul driver appropriato dall'elenco** > **Controllo** > **Configurazione di stato del driver**.

2 Fare clic sulla scheda **Verde**, **Giallo** o **Rosso** per lo stato di cui si desidera modificare le azioni.

3 Fare clic sull'icona con il segno più (+) accanto all'intestazione **Azioni** per aggiungere un'azione, quindi selezionare il tipo di azione desiderato:

- **Avvia driver:** avvia il driver.
- **Arresta driver:** arresta il driver.
- **Riavvia driver:** arresta e avvia il driver.
- **Cancella cache del driver:** rimuove dalla cache tutte le transazioni, incluse quelle non elaborate.

- **Invia e-mail:** invia un'e-mail a uno o più destinatari. Il modello che si desidera utilizzare nel corpo del messaggio e-mail deve essere già presente. Per includere nell'e-mail il nome del driver, il nome del server e le informazioni sullo stato attuale, aggiungere i token `$Driver$`, `$Server$` e `$HealthState$` al modello e-mail, quindi includere i token nel testo del messaggio. Ad esempio:

  ```
  The current health state of the $Driver$ driver running on $Server$
  is $HealthState$.
  ```

  Importante: per inviare e-mail a più utenti, separare ogni indirizzo e-mail solo con una virgola (,). Non utilizzare il punto e virgola al posto della virgola.

- **scrivi messaggio traccia:** Scrive un messaggio nel file di log del processo Stato del driver o nel file di log del set di driver se il file di traccia non è configurato sul processo Stato del driver.
- **Genera evento:** genera un evento che può essere utilizzato da Audit e Sentinel.
- **Esegui ECMAScript:** esegue un ECMAScript esistente.

  Per informazioni su come creare script ECMA, vedere Using ECMAScript in Policies (Utilizzo di ECMAScript nelle policy) nella guida *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager - Utilizzo di Designer per la creazione di policy).
- **Avvia workflow:** avvia un workflow di provisioning.
- **Su errore:** se un'azione ha esito negativo, indica come procedere con le azioni rimanenti, lo stato corrente e il processo Stato del driver.
  - **Incidere sulle azioni tramite:** è possibile continuare a eseguire le azioni rimanenti, interrompere l'esecuzione delle azioni rimanenti o impostare come default l'impostazione corrente. L'impostazione corrente viene applicata solo se sono disponibili più azioni Su errore e se si configura l'opzione Incidere sulle azioni tramite in una delle azioni Su errore precedenti.
  - **Incidere sullo stato tramite:** è possibile salvare lo stato corrente, rifiutare lo stato corrente o impostare come default l'impostazione corrente. Se si salva lo stato, le relative condizioni continuano a essere valutate come vere. Se si rifiuta lo stato, le condizioni dello stato vengono valutate come false. L'impostazione corrente viene applicata solo se sono disponibili più azioni Su errore e se si configura l'opzione Incidere sullo stato tramite in una delle azioni Su errore precedenti.
  - **Incidere sul processo di stato del driver tramite:** è possibile continuare a eseguire il processo, interrompere e disabilitare il processo oppure impostare come default l'impostazione corrente. Se si continua con l'esecuzione, il processo termina la valutazione delle condizioni per determinare lo stato del driver ed eseguire eventuali azioni associate allo stato. L'interruzione e la disabilitazione del processo interrompe l'attività corrente del processo e lo arresta; l'esecuzione del processo non riparte fino a quando non viene abilitato. L'impostazione corrente viene applicata solo se sono disponibili più azioni Su errore e se si configura l'impostazione Incidere sul processo di stato del driver tramite in una delle azioni Su errore precedenti.

4 Al termine, salvare le modifiche facendo clic sul pulsante **Salva**.

Creazione di uno stato personalizzato

È possibile creare uno o più stati personalizzati per eseguire azioni indipendentemente dallo stato corrente del driver (Verde, Giallo, Rosso). Se vengono soddisfatte le condizioni di uno stato personalizzato, le relative azioni vengono eseguite indipendentemente dallo stato corrente.

Come per gli stati Verde, Giallo e Rosso, le azioni di uno stato personalizzato vengono eseguite solo una volta ogni volta che vengono soddisfatte le condizioni; finché lo stato rimane vero, le azioni non vengono ripetute. Se lo stato cambia perché le sue condizioni non sono più soddisfatte, le azioni vengono nuovamente eseguite al successivo verificarsi delle condizioni.

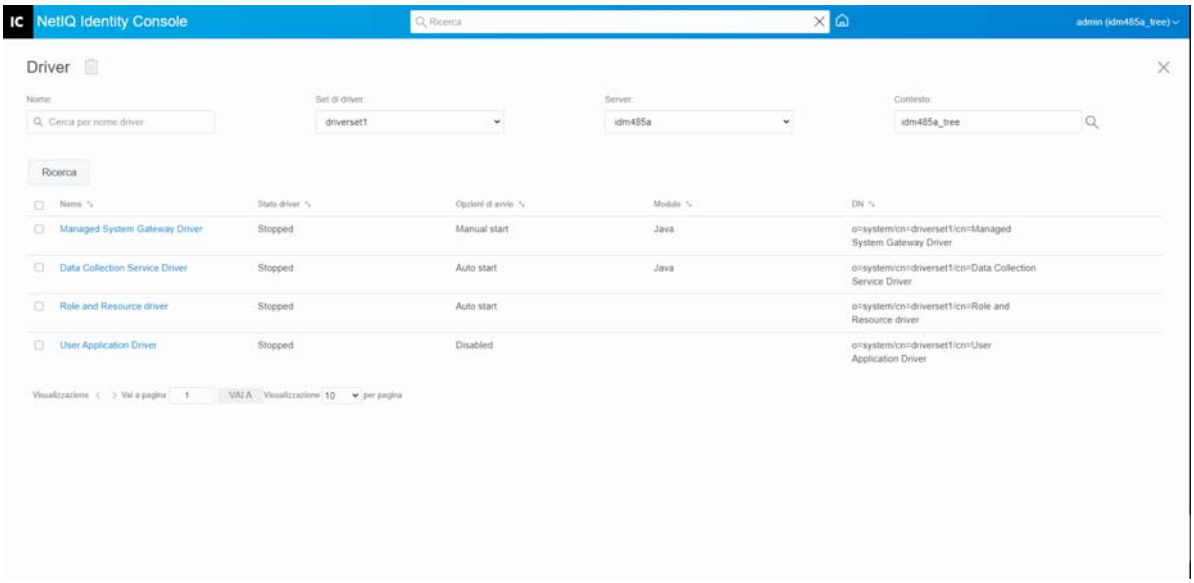
1. In Identity Console, aprire la pagina Configurazione di stato del driver per un driver per cui si desidera creare uno stato personalizzato:
   - **1a** Aprire la home page di Identity Console.
   - **1b** Selezionare **Driver** > **Fare clic sul driver appropriato dall'elenco** > **Controllo** > **Configurazione di stato del driver**.
2. Fare clic sull'icona + accanto alle icone relative allo stato del driver (verde, giallo e rosso)
3. Attenersi alle istruzioni riportate in “Modifica delle condizioni di stato del driver” a pagina 176 e “Modifica delle azioni di stato del driver” a pagina 178 per definire le condizioni e le azioni dello stato personalizzato.

Modifica di uno stato personalizzato

Per modificare gli stati personalizzati, eseguire le operazioni riportate di seguito:

1. In Identity Console, aprire la pagina Configurazione di stato del driver per un driver per cui si desidera creare uno stato personalizzato:
   - **1a** Aprire la home page di Identity Console.
   - **1b** Selezionare **Driver** > **Fare clic sul driver appropriato dall'elenco** > **Controllo** > **Configurazione di stato del driver**.
2. Fare clic sull'icona  accanto alle icone relative allo stato del driver (verde, giallo e rosso)
3. Attenersi alle istruzioni riportate in “Modifica delle condizioni di stato del driver” a pagina 176 e “Modifica delle azioni di stato del driver” a pagina 178 per definire le condizioni e le azioni dello stato personalizzato.

Figura 23-6 *Gestione dei controlli driver*



24 Gestione delle statistiche del set di driver

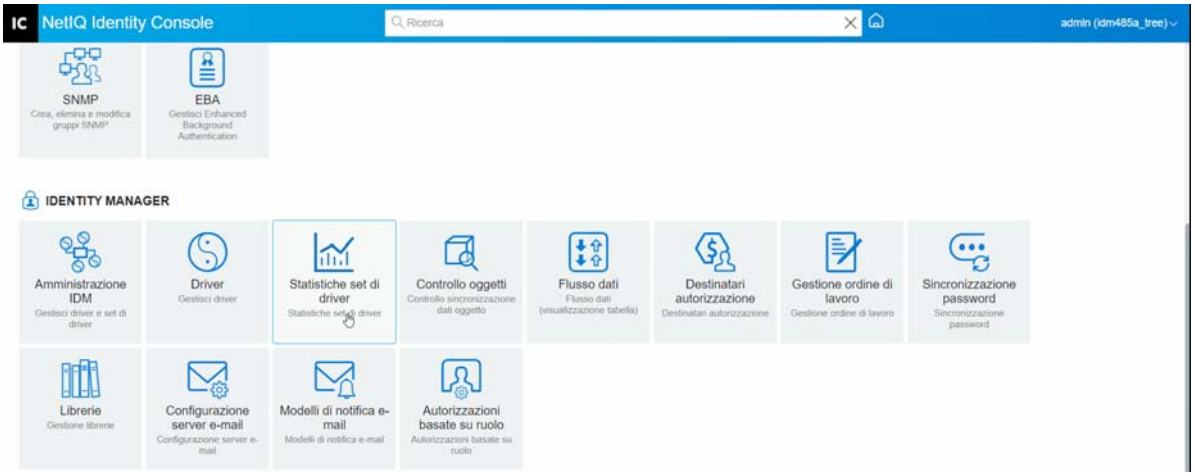
È possibile utilizzare il portale di Identity Console per visualizzare numerose statistiche relative a un singolo driver o a un intero set di driver. Sono incluse statistiche quali le dimensioni del file di cache, le dimensioni delle transazioni non elaborate nel file di cache, le transazioni meno recenti e più recenti e il numero totale di transazioni non elaborate per categoria (aggiunta, rimozione, modifica e così via). Per visualizzare le statistiche del set di driver:

1. In Identity Console, aprire la pagina **Statistiche set di driver**.
2. Selezionare il server appropriato dall'elenco a discesa.

   Viene visualizzata una pagina che consente di visualizzare le statistiche relative a tutti i driver contenuti nel set di driver.

   - Per aggiornare le statistiche, fare clic sull'icona .
   - Per chiudere le statistiche relative a un driver, fare clic sul pulsante nell'angolo in alto a destra della finestra delle statistiche del driver.
   - Per aprire le statistiche relative a tutti i driver, fare clic su **Azioni** > **Mostra tutto**.
   - Per comprimere l'elenco delle transazioni non elaborate per un driver, fare clic sul pulsante situato sopra l'elenco. Per comprimere l'elenco delle transazioni non elaborate per tutti i driver, fare clic su **Azioni** > **Comprimi tutte le transazioni**.
   - Per espandere l'elenco delle transazioni, fare clic sul pulsante . Per espandere l'elenco delle transazioni non elaborate per tutti i driver, fare clic su **Azioni** > **Espandi tutte le transazioni**.
   - Per chiudere il dashboard delle statistiche dei driver disabilitati, fare clic su **Azioni**, quindi selezionare **Close Disabled Drivers** (Chiudi driver disabilitati).

Figura 24-1 *Gestione delle statistiche del set di driver*



25 Controllo degli oggetti di Identity Manager

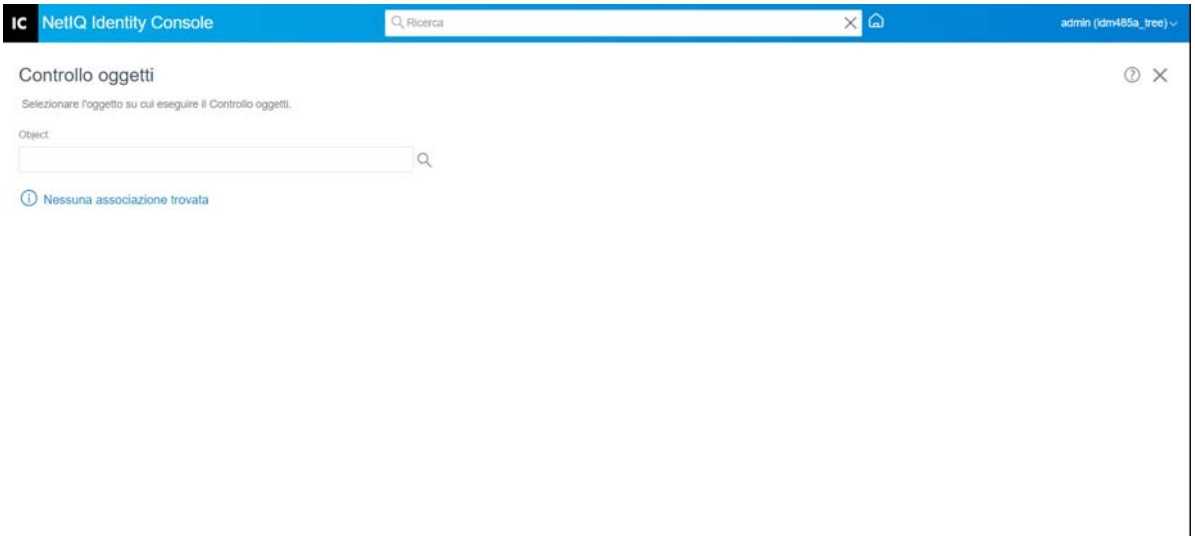
È possibile utilizzare Controllo oggetti per visualizzare informazioni dettagliate sulla partecipazione di un oggetto alle relazioni di Identity Manager. Tali relazioni includono i sistemi connessi associati all'oggetto, la modalità del flusso dei dati tra l'Identity Vault e i sistemi connessi, i valori degli attributi attualmente memorizzati in Identity Vault e nei sistemi connessi, le configurazioni dei driver del sistema connesso e così via.

Per controllare gli oggetti di Identity Manager, fare clic sull'opzione **Controllo oggetti** nella pagina principale di Identity Console. Specificare il nome distinto completo dell'oggetto che si desidera controllare oppure fare clic sull'icona Sfoglia per individuare e selezionare l'oggetto desiderato.

Nella sezione Sistemi connessi sono elencati tutti i sistemi connessi ai quali è associato l'oggetto. Tramite la pagina **Controllo oggetti**, è possibile eseguire le seguenti azioni:

- **Aggiunta di un'associazione**: per aggiungere una nuova associazione a un sistema connesso, fare clic sull'icona +. Individuare e selezionare l'**Oggetto driver integrazione** e specificare l'**ID oggetto associato**.
- **Eliminazione di un'associazione**: per eliminare un'associazione a un sistema connesso, selezionare la casella di controllo a sinistra dell'associazione e fare clic sull'icona 🗑. Per eliminare tutte le associazioni, selezionare la casella di controllo sotto alla colonna Elimina, quindi fare clic sull'icona 🗑.

Figura 25-1 *Controllo degli oggetti di Identity Manager*



26 Gestione del flusso di dati

Il flusso di dati illustra i canali produttore e sottoscrittore per diversi driver in un'unica visualizzazione. Questa opzione consente di visualizzare e aggiornare la proprietà dei dati per tutti i driver.

Per accedere alla visualizzazione tabella del flusso di dati, fare clic sul modulo **Flusso dati (visualizzazione tabella)** nella pagina principale di Identity Console. Individuare e selezionare il container appropriato per visualizzare l'elenco dei driver.

Per gestire la proprietà dei dati di singoli driver, eseguire le operazioni riportate di seguito:

1 Ciascun driver dispone di due pulsanti che consentono di gestire il flusso dei dati attraverso i canali produttore e sottoscrittore. Il pulsante a sinistra gestisce il flusso di dati sul produttore, il pulsante a destra gestisce il flusso di dati sul sottoscrittore.

   1a **Sincronizza**: selezionare questa opzione per sincronizzare l'attributo specifico. Dopo aver selezionato questa opzione, l'icona viene modificata in ↑ nel produttore e in ↓ nel sottoscrittore.

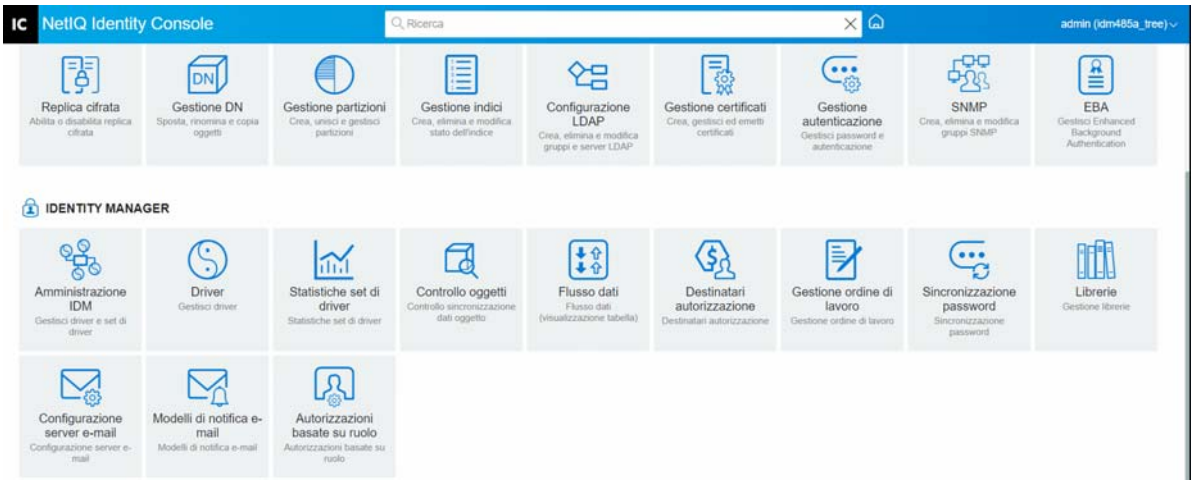
   1b **Ignora**: selezionare questa opzione per interrompere la sincronizzazione dell'attributo specifico. Dopo aver selezionato questa opzione, l'icona viene modificata in ⊘.

   1c **Notifica**: selezionare questa opzione per ricevere una notifica delle modifiche apportate a un attributo specifico. La modifica non verrà sincronizzata automaticamente. Dopo aver selezionato questa opzione, l'icona viene modificata in 🔔.

   1d **Reimposta**: selezionare questa opzione per reimpostare il valore dell'attributo al valore specificato dall'altro canale. Dopo aver selezionato questa opzione, l'icona viene modificata in ↻.

   Nota: è possibile impostare questo valore sia sul produttore che sul sottoscrittore. Non è possibile impostare questo valore su entrambi i canali contemporaneamente.

Figura 26-1 *Gestione del flusso di dati*



27 Gestione dei destinatari dell'autorizzazione

I riferimenti e i risultati delle autorizzazioni vengono mantenuti sugli oggetti per i quali è stata concessa o revocata un'autorizzazione. I riferimenti e i risultati delle autorizzazioni contengono informazioni sull'attuale concessione o revoca dell'autorizzazione per tale oggetto. I destinatari dell'autorizzazione sono tutti gli oggetti contenenti riferimenti a un'autorizzazione.

Riferimenti di autorizzazione

Per visualizzare i riferimenti e i risultati delle autorizzazioni, fare clic sull'opzione **Destinatari autorizzazione** nella pagina principale di Identity Console e selezionare Riferimenti di autorizzazione. Specificare quindi il nome distinto completo dell'oggetto che rappresenta un `DirXML-EntitlementRecipient`. È possibile fare clic sul pulsante Selettore oggetti  per selezionare l'oggetto.

Entitlement Results (Risultati autorizzazione)

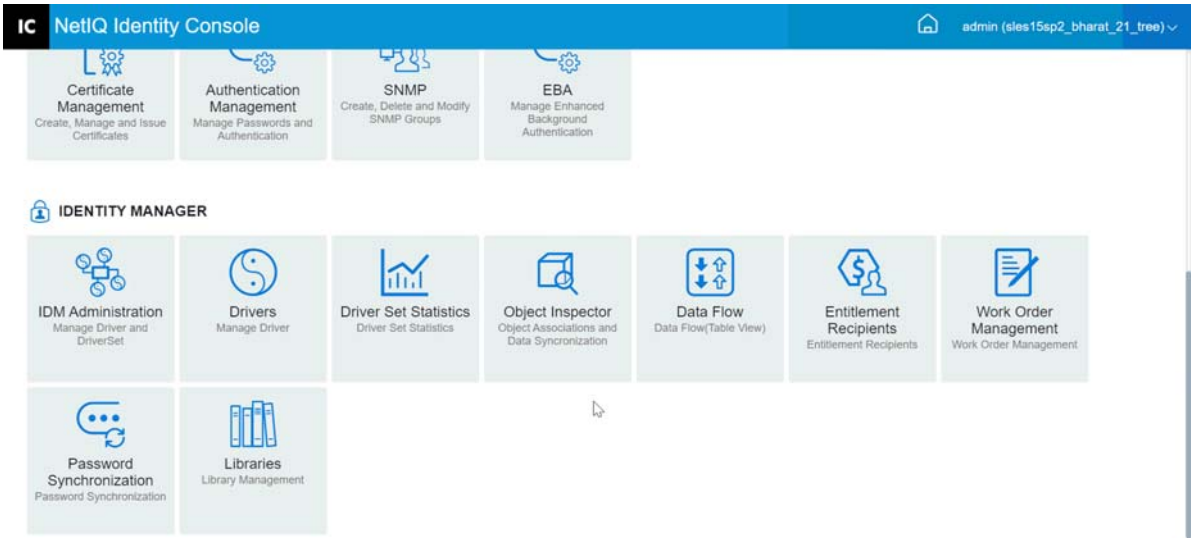
Nella tabella Entitlement Results (Risultati autorizzazione) di Identity Console sono elencati i risultati dell'autorizzazione associati all'oggetto selezionato. Per visualizzare l'autorizzazione associata, selezionare il DN autorizzazione. Per visualizzare i risultati dell'autorizzazione in formato XML, selezionare l'ID risultato corrispondente.

- **Intestazioni di colonna dei risultati autorizzazione**: le intestazioni di colonna includono il nome distinto completo dell'autorizzazione, lo stato attuale di concessione o revoca, l'origine dei risultati, lo stato del risultato, eventuali messaggi allegati al risultato, la data, l'ora e l'identificazione del risultato.
  - **DN autorizzazione**: fare clic sul nome distinto completo dell'autorizzazione per visualizzare la pagina Modifica oggetto. Questa pagina consente di visualizzare le modalità di assegnazione degli attributi eDirectory all'oggetto. In questa pagina è inoltre possibile modificare gli attributi dell'oggetto. Il numero di categorie visualizzate nella pagina Modifica oggetto dipende dall'oggetto selezionato.
  - **Stato**: visualizza se l'autorizzazione è stata concessa o revocata. Se vengono rilevati altri valori nel flusso XML, il plug-in li visualizza direttamente.
  - **Messaggio:** tutti i messaggi associati dallo shim DirXML allo stato dei risultati. Le informazioni memorizzate nella porzione <msg></msg> del file dei risultati XML. Fare clic sulla voce Results ID (ID risultati) per visualizzare i dettagli completi dei risultati in una pagina del visualizzatore XML.

- **Registrazione orario**: l'ora in cui il motore di autorizzazione ha elaborato e scritto il risultato. Fare clic sulla voce Results ID (ID risultati) per visualizzare i dettagli completi dei risultati in una pagina del visualizzatore XML.
- **Results ID (ID risultati):** fare clic sulla voce Results ID (ID risultati) per visualizzare i dettagli completi dei risultati in una pagina del visualizzatore XML. Dopo aver visualizzato i risultati, fare clic su Chiudi.

Per eliminare una voce dei risultati dell'autorizzazione, fare clic sulla casella di controllo a sinistra della voce dei risultati dell'autorizzazione e selezionare **Elimina**.

Figura 27-1 *Gestione dei destinatari dell'autorizzazione*



28 Gestione degli ordini di lavoro

I driver di Identity Manager possono creare ordini di lavoro a seguito di eventi elaborati dai driver. Ad esempio, se si utilizza un driver per risorse umane (SAP HR, PeopleSoft e così via), è possibile fare in modo che il driver generi un ordine di lavoro ogni volta che viene aggiunto un nuovo utente.

È possibile utilizzare Identity Console per creare e gestire gli ordini di lavoro creati per vari driver che supportano questa funzionalità specifica.

Creazione di un nuovo ordine di lavoro

Per creare un nuovo ordine di lavoro, eseguire le operazioni riportate di seguito:

1. Fare clic sull'opzione **Ordine di lavoro** nella pagina di destinazione di Identity Console.
2. Fare clic sull'icona + per creare un nuovo ordine di lavoro.
3. Specificare un nome per l'ordine di lavoro, quindi fare clic su **OK**.

   Il nome viene utilizzato per il nome dell'oggetto WorkOrder in Identity Vault.
4. Immettere le informazioni nei campi:

   Stato: lo stato di un nuovo ordine di lavoro può essere **In sospeso** o **In attesa**. In genere, lo stato dell'ordine di lavoro è **In sospeso**. È possibile interrompere un ordine di lavoro selezionando **In attesa**. Dopo l'elaborazione di un ordine di lavoro, in questo campo viene visualizzato lo stato dell'ordine di lavoro risultante.

   Data di scadenza: è possibile scegliere di far eseguire immediatamente l'ordine di lavoro al driver o di pianificare l'ordine di lavoro. Per pianificare una data di scadenza, fare clic sull'icona del calendario. Utilizzare il calendario per scegliere la data. Utilizzare le frecce per selezionare il mese, l'anno e l'ora.

   Ripeti ordine di lavoro: selezionare questa opzione per fare in modo che l'ordine di lavoro venga elaborato più volte. Specificare l'intervallo di tempo scegliendo il numero di settimane, giorni, ore o minuti prima che l'ordine di lavoro venga ripetuto. L'elaborazione dell'ordine di lavoro viene interrotta alla data di eliminazione, a meno che l'ordine di lavoro non venga eliminato/modificato manualmente o il driver non restituisca un messaggio di errore.

   Data di eliminazione: utilizzare il controllo del calendario per selezionare una data di eliminazione degli ordini di lavoro configurati. Gli ordini di lavoro con uno stato di errore non vengono eliminati a meno che non si seleziona **Elimina ordine di lavoro anche se contiene un errore**.

Ordini di lavoro dipendenti: quando si crea un nuovo ordine di lavoro, è possibile renderlo dipendente da uno o più ordini di lavoro. Fare clic su  per ricercare e selezionare gli ordini di lavoro dipendenti. Per rimuovere un ordine di lavoro dall'elenco, selezionare l'ordine di lavoro, quindi fare clic su  .

Tipo: utilizzare questo campo per specificare un tipo di ordine di lavoro. Il driver non modifica questo attributo. L'attributo viene passato all'oggetto WorkToDo al momento dell'elaborazione dell'ordine di lavoro.

Numero ordine di lavoro: numero univoco dell'ordine di lavoro. Questo valore può essere assegnato da un sistema di ordini di lavoro aziendale diverso da NetIQ eDirectory, ad esempio un database per gli ordini di lavoro.

Informazioni di contatto: informazioni di contatto della persona responsabile dell'ordine di lavoro.

Log di elaborazione ordine di lavoro: dopo l'elaborazione di un ordine di lavoro, in questo campo il driver registra i risultati dell'ordine di lavoro, incluso lo stato. In questo modo è possibile controllare lo stato attuale dell'ordine di lavoro e identificare eventuali problemi riscontrati dal driver durante il tentativo di configurazione dell'ordine di lavoro.

L'attributo di stato dell'ordine di lavoro rimane in sospeso finché l'ordine di lavoro non viene elaborato. L'ordine di lavoro viene elaborato al raggiungimento della data di scadenza. Il driver genera rapporti sui risultati dell'elaborazione impostando l'attributo di stato su Configurato, Avviso o Errore. Se l'ordine di lavoro è In attesa, l'ordine di lavoro viene ignorato.

- **In sospeso:** il driver è in attesa della scadenza per completare l'ordine di lavoro.
- **Configurato:** l'ordine di lavoro è stato elaborato correttamente.
- **Errore:** il driver non è riuscito a eseguire l'ordine di lavoro.
- **Avviso:** viene visualizzato un avviso relativo all'ordine di lavoro. Ad esempio, se l'ordine di lavoro include un ordine di lavoro dipendente con una scadenza successiva, il driver invia un avviso.

Descrizione: la descrizione dell'ordine di lavoro.

Contenuto ordine di lavoro: i dati in questo campo vengono utilizzati dalle regole del driver per elaborare l'ordine di lavoro. Ad esempio, potrebbe essere l'XML utilizzato dalla regola di trasformazione di comandi per elaborare l'ordine di lavoro.

Eliminazione di un ordine di lavoro esistente

Per eliminare un ordine di lavoro esistente, eseguire le operazioni riportate di seguito:

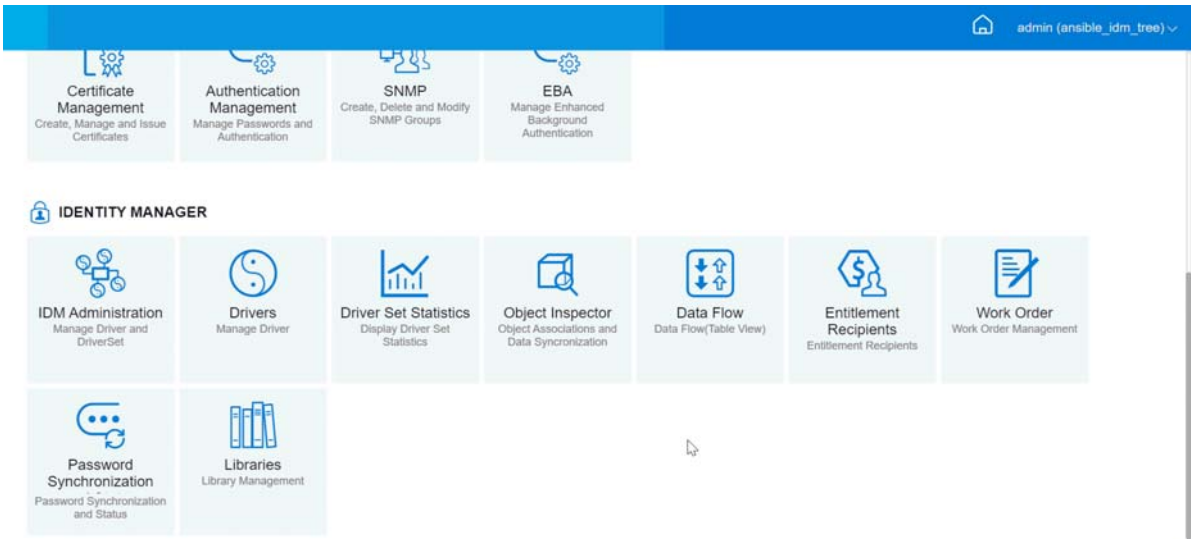
1. Fare clic sull'opzione **Ordine di lavoro** nella pagina di destinazione di Identity Console.
2. Selezionare l'ordine di lavoro che si desidera eliminare.
3. Fare clic sull'icona  .

Filtraggio dell'elenco degli ordini di lavoro

Per filtrare l'elenco degli ordini di lavoro, eseguire le operazioni riportate di seguito:

1. Fare clic sull'opzione **Ordine di lavoro** nella pagina di destinazione di Identity Console.
2. Fare clic su **Azioni** in Gestione ordine di lavoro.
3. Dal menu a discesa, selezionare il tipo di filtro:
   - **Mostra tutto:** vengono elencati tutti gli ordini di lavoro associati al driver.
   - **Configurato:** vengono elencati solo gli ordini di lavoro configurati associati al driver.
   - **Errore:** vengono elencati solo gli ordini di lavoro con uno stato di errore.
   - **In attesa:** vengono elencati gli ordini di lavoro che sono stati messi in attesa manualmente.
   - **In sospeso:** vengono elencati gli ordini di lavoro non ancora scaduti.

Figura 28-1 *Gestione degli ordini di lavoro*



29 Gestione dello stato e della sincronizzazione delle password

È possibile verificare la sincronizzazione e lo stato delle password dei singoli driver tramite il portale di Identity Console. Per eseguire la verifica, selezionare il modulo **Sincronizzazione password** dalla pagina principale di Identity Console.

Questo modulo consente di eseguire le seguenti azioni:

- "Controllo dello stato di sincronizzazione password" a pagina 195
- "Verifica delle impostazioni di sincronizzazione delle password" a pagina 196

Controllo dello stato di sincronizzazione password

È possibile determinare se la password di distribuzione per un utente specifico è la stessa del sistema connesso. Per controllare lo stato di sincronizzazione password, eseguire i passaggi seguenti:

1. In Identity Console, selezionare **Sincronizzazione password** > **Stato password**.
2. Individuare e selezionare l'utente per il quale si desidera controllare lo stato della password.
3. È possibile visualizzare i seguenti stati della password:
   - Le password sono sincronizzate.
   - Le password NON sono sincronizzate.
   - Lo stato della password è sconosciuto perché il sistema connesso non può essere contattato per richiedere un controllo della password.
   - Si è verificato un errore.

Nota: per visualizzare ulteriori dettagli su ciascuno degli stati descritti in precedenza, posizionare il puntatore del mouse sullo stato nella colonna **Stato password**.

Il task Stato password consente al driver di eseguire un'azione Controllo password oggetto. Non tutti i driver supportano il controllo delle password. Tali driver devono contenere una funzionalità di controllo della password nel manifesto del driver. Identity Console non consente l'invio di operazioni di controllo della password a driver che non contengono questa funzionalità nel manifesto.

L'azione Controllo password oggetto controlla la password di distribuzione. Se la password di distribuzione non viene aggiornata, Controllo password oggetto potrebbe segnalare che le password non sono sincronizzate.

La password di distribuzione non viene aggiornata se si verifica una delle seguenti condizioni:

- Si utilizza il metodo di sincronizzazione mediante l'uso della password NDS per la sincronizzazione o l'uso della Password universale per la sincronizzazione. Per ulteriori informazioni, vedere "Creazione di una policy password con impostazioni personalizzate" a pagina 116.

Nota: l'azione Stato password controlla la password NDS anziché la Password universale per Identity Vault. Di conseguenza, se la policy password dell'utente non specifica di sincronizzare la password NDS con la Password universale, le password vengono sempre segnalate come non sincronizzate. È infatti possibile che la password di distribuzione e la password del sistema connesso siano sincronizzate ma il controllo dello stato delle password non sarà accurato a meno sia la password NDS che la password di distribuzione non siano sincronizzate con la Password universale.

Verifica delle impostazioni di sincronizzazione delle password

La Sincronizzazione password consente di sincronizzare le password tra sistemi connessi tramite Identity Manager. Per visualizzare le impostazioni di Sincronizzazione password per i sistemi connessi, selezionare il set di driver appropriato dall'elenco a discesa.

Tramite la Sincronizzazione password è possibile configurare i sistemi connessi in modo da eseguire le seguenti operazioni:

- Pubblicare le password in Identity Manager.
- Eseguire la sottoscrizione alle password provenienti da Identity Manager o da altri sistemi connessi.
- Applicare le policy password sui sistemi connessi.
- Inviare e-mail di notifica.

Per controllare le impostazioni di sincronizzazione delle password, eseguire i passaggi seguenti:

1. In Identity Console, selezionare **Sincronizzazione password** > **Sincronizzazione password** dalla pagina principale.
2. Selezionare il set di driver contenente il driver di cui si desidera controllare le impostazioni.
3. Fare clic sul nome del driver dall'elenco.

   Nota: le impostazioni abilitate e disabilitate variano a seconda del driver. Sono disponibili solo le impostazioni per le funzioni supportate dal driver.

4. Verificare che le impostazioni siano configurate correttamente.

   Identity Manager accetta le password (produttore): se questa opzione è abilitata, Identity Manager consente il flusso delle password dal sistema connesso a Identity Vault. Se si disabilita questa opzione, non viene consentito il flusso di elementi <password> a Identity Manager. Le password vengono rimosse dall'XML mediante una policy di sincronizzazione delle password del produttore.

   Questa impostazione si applica alle password utente fornite dal sistema connesso stesso e ai valori delle password creati da una policy del produttore.

   Se questa opzione è abilitata ma l'opzione Distribution Password (Password di distribuzione) sottostante è disabilitata, un valore <password> proveniente dal sistema connesso viene scritto direttamente in Password universale in Identity Vault. Se la policy password dell'utente non abilita la Password universale, la password viene scritta nella password NDS.

   Utilizza password di distribuzione per la sincronizzazione password: questa impostazione è disponibile solo se è abilitata l'impostazione **Identity Manager accetta le password (produttore)**.

Se questa opzione è abilitata, il valore della password proveniente dal sistema connesso viene scritto nella password di distribuzione. La password di distribuzione è reversibile, ovvero può essere recuperata dall'archivio dati di Identity Vault per la sincronizzazione delle password. Questa impostazione viene utilizzata da Identity Manager per la sincronizzazione bidirezionale delle password con i sistemi connessi. Per consentire a Identity Manager di distribuire le password da questo sistema ad altri sistemi, è necessario che questa opzione sia abilitata.

Accetta la password solo se è conforme alla policy password dell'utente: questa impostazione è disponibile solo se è abilitata l'opzione **Utilizza password di distribuzione per la sincronizzazione password**.

Se questa opzione è selezionata, Identity Manager non scrive una password da questo sistema connesso alla password di distribuzione in Identity Vault né la pubblica nei sistemi connessi, a meno che la password non sia conforme alla policy password dell'utente.

Se una password non è conforme, abilitare l'impostazione **Reset the user's password to the Distribution Password** (Reimposta la password utente alla password di distribuzione) per reimpostare la password dell'utente sul sistema connesso. Ciò consente di applicare la policy password sia al sistema connesso che a Identity Vault. Se non si seleziona questa opzione, le password utente possono diventare non sincronizzate sui sistemi connessi. Tuttavia, è necessario prendere in considerazione le policy password del sistema connesso quando si decide se utilizzare questa opzione. È possibile che alcuni sistemi connessi non consentano la reimpostazione perché non consentono la ripetizione delle password.

Utilizzando l'opzione **Inviare all'utente la notifica dell'errore di sincronizzazione password tramite e-mail** è possibile informare gli utenti quando non è possibile impostare o reimpostare una password. La notifica è particolarmente utile per questa opzione. Se l'utente passa a una password consentita dal sistema connesso ma rifiutata da Identity Manager a causa della policy password, l'utente non saprà che la password è stata reimpostata fino a quando non riceve una notifica o non tenta di eseguire il login al sistema connesso con la password precedente.

Accetta sempre la password; ignora le policy password: questa impostazione è disponibile solo se è abilitata l'opzione **Utilizza password di distribuzione per la sincronizzazione password**.

Se si seleziona questa opzione, Identity Manager non applica la policy password dell'utente per il sistema connesso. Identity Manager scrive la password da questo sistema connesso nella password di distribuzione in Identity Vault e la distribuisce ad altri sistemi connessi indipendentemente dalla conformità alla policy password.

L'applicazione accetta le password (sottoscrittore): se si abilita questa opzione, il driver invia le password da Identity Vault al sistema connesso. Ciò significa inoltre che se un utente modifica la password su un altro sistema connesso che pubblica le password nella password di distribuzione in Identity Vault, la password viene modificata su questo sistema connesso.

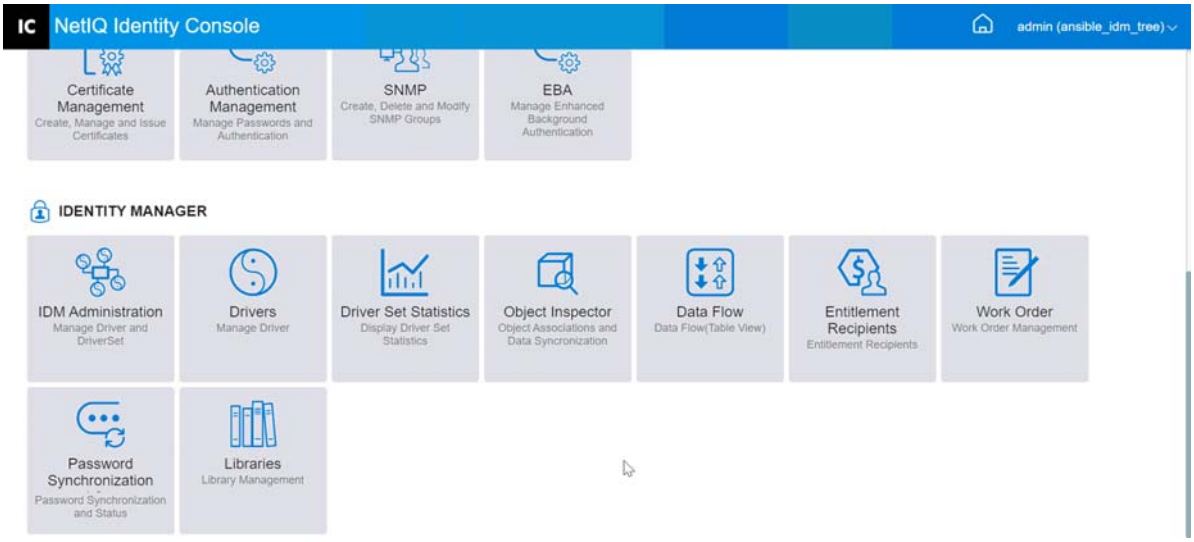
Di default, la password di distribuzione corrisponde alla Password universale in Identity Vault, pertanto le modifiche alla Password universale effettuate in Identity Vault vengono inviate anche al sistema connesso.

Inviare all'utente la notifica dell'errore di sincronizzazione password tramite e-mail: se si abilita questa opzione, all'utente viene inviata un'e-mail se la password non è sincronizzata, impostata o reimpostata. L'e-mail inviata all'utente si basa su un modello e-mail. Tale modello viene fornito dall'applicazione di sincronizzazione password. Tuttavia, per il corretto funzionamento del modello, è necessario personalizzarlo e specificare un server e-mail per

l'invio dei messaggi di notifica. Per istruzioni, vedere Configuring E-Mail Notification (Configurazione delle notifiche e-mail) nella *NetIQ Identity Manager Password Management Guide* (Guida alla gestione delle password di NetIQ Identity Manager).

5 Al termine, fare clic su **Salva** per salvare le modifiche. Le impostazioni vengono salvate come Valori di configurazione globali.

Figura 29-1 *Gestione della sincronizzazione delle password*



30 Gestione delle librerie

Gli oggetti libreria memorizzano più policy e altre risorse condivise da uno o più driver. È possibile creare un oggetto libreria in un oggetto set di driver o in qualsiasi container eDirectory. In un albero eDirectory possono essere presenti più librerie. I driver possono fare riferimento a qualsiasi libreria nell'albero purché il server su cui è in esecuzione il driver contenga una replica in Lettura/Scrittura o Master dell'oggetto della libreria.

I fogli di stile, le policy, le regole e altri oggetti risorsa possono essere memorizzati in una libreria a cui fanno riferimento uno o più driver.

Tramite il modulo Library Management (Gestione librerie) è possibile eseguire i seguenti task:

- "Visualizzazione ed eliminazione di una libreria esistente" a pagina 199
- "Visualizzazione ed eliminazione di oggetti dalla libreria" a pagina 199

Visualizzazione ed eliminazione di una libreria esistente

Per visualizzare ed eliminare una libreria esistente, eseguire le operazioni riportate di seguito:

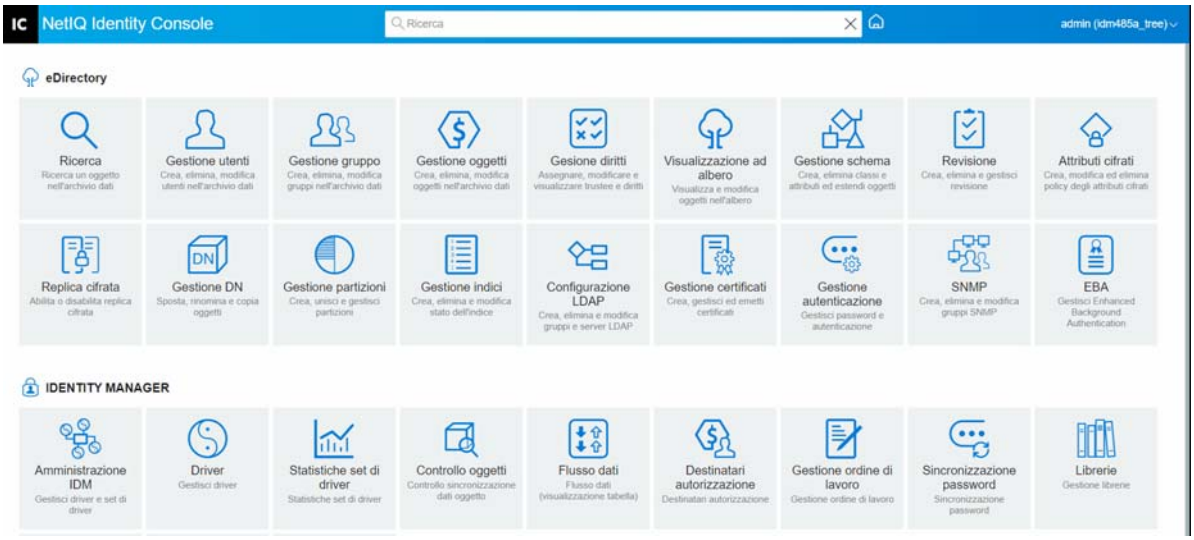
1. In Identity Console, selezionare il modulo **Librerie** nella home page.
2. Selezionare la libreria appropriata dall'elenco.
3. Fare clic sull'icona  . Fare clic su **OK** per confermare.

Visualizzazione ed eliminazione di oggetti dalla libreria

È possibile visualizzare ed eliminare policy e tabelle mappature dagli oggetti libreria. Per eliminare gli oggetti, eseguire le operazioni riportate di seguito:

1. In Identity Console, selezionare il modulo **Librerie** nella home page.
2. Fare clic sulla libreria appropriata dall'elenco.
3. Per eliminare le policy, selezionare la scheda **Policy**.
4. Selezionare la policy appropriata dall'elenco e fare clic sull'icona  .
5. Per eliminare le tabelle mappature, selezionare la scheda **Tabelle mappature**.
6. Selezionare la tabella mappature appropriata dall'elenco e fare clic sull'icona  .
7. Fare clic su **OK** per confermare.

Figura 30-1 *Gestione delle librerie*



31 Gestione delle opzioni del server e-mail

È possibile utilizzare Opzioni server e-mail per specificare le impostazioni per il server e-mail SMTP.

Nome host

Il nome host del server e-mail SMTP. Il nome host può essere costituito da un indirizzo IP. È inoltre possibile specificare una porta personalizzata seguita dal nome host o dall'indirizzo IP.

Importante: Utilizzare i due punti (:) come separatore tra il nome host o l'indirizzo IP e la porta.

Da

È possibile specificare un indirizzo e-mail valido visualizzato come campo Da dell'intestazione dell'e-mail.

Valore di timeout

L'opzione di timeout consente di impostare il limite di tempo (in secondi) per l'invio delle e-mail di notifica.

Abilita SSL

Se necessario, è possibile scegliere di abilitare l'opzione SSL.

Autenticarsi sul server tramite credenziali

Utilizzare questa opzione per un server SMTP sicuro. Se il server richiede l'autenticazione prima dell'invio dei messaggi e-mail, specificare qui il nome utente e la parola d'ordine.

Sebbene le informazioni di autenticazione vengano specificate qui, potrebbe inoltre essere necessario specificarle separatamente per l'applicazione che invia i messaggi e-mail di notifica.

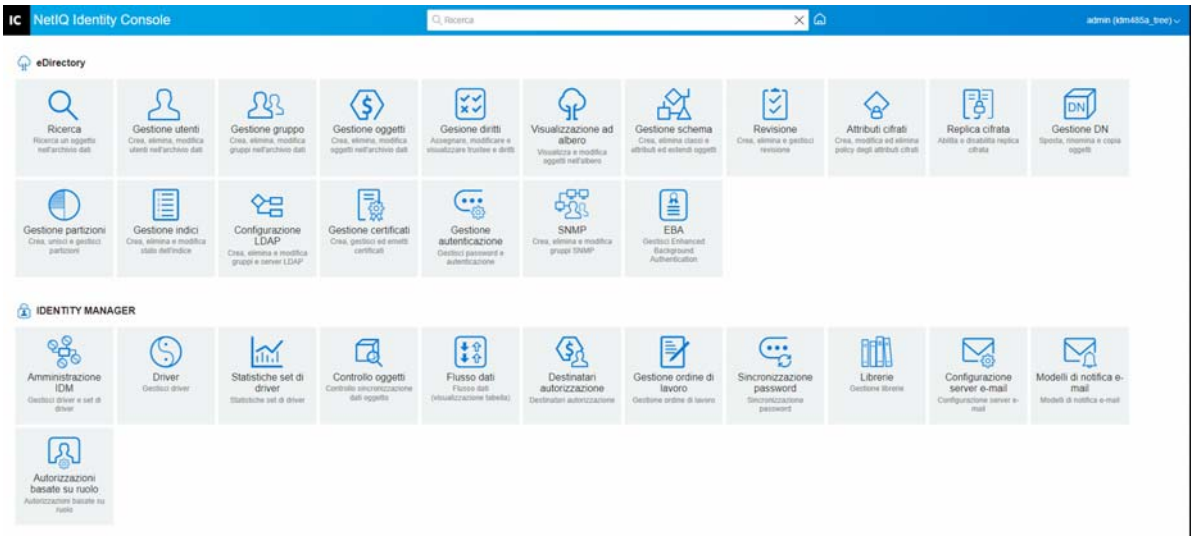
Ad esempio, è possibile utilizzare le informazioni di autenticazione specificate qui per inviare notifiche e-mail relative al recupero della password. Tuttavia, la sincronizzazione delle password di Identity Manager utilizza la policy driver per inviare le e-mail di notifica. Potrebbe essere necessario fornire le informazioni di autenticazione anche nella policy driver.

Per eseguire l'autenticazione sul server, eseguire i passaggi seguenti:

1. Selezionare l'opzione **Autenticarsi sul server tramite credenziali**.
2. Specificare il **Nome utente** e la **Password**.
3. Fare clic su **Prova connessione al server** per verificare la connettività.
4. Fare clic su **Salva**.

Nota: Dopo aver salvato i dettagli delle credenziali, la **Prova connessione al server** viene disabilitata.

Figura 31-1 *Configurazione server e-mail*



32 Gestione dei modelli e-mail

Questo elenco mostra i modelli di notifica disponibili. Utilizzare questi modelli per inviare un messaggio e-mail agli utenti dell'albero. È possibile personalizzare il testo dei modelli.

Alcune applicazioni forniscono modelli propri. Gli oggetti Modello si trovano nel container di sicurezza che in genere si trova alla radice dell'albero dell'utente.

È possibile ordinare l'elenco in base al nome, alla data o all'oggetto.

Oggetto

Testo visualizzato dall'utente nell'intestazione Oggetto di un'e-mail. Per modificare un modello, fare clic sull'intestazione Oggetto del modello. Mediante l'interfaccia Modifica modello di notifica e-mail, è possibile modificare il modello e i relativi dettagli.

Nome modello

Ciascun modello ha un nome univoco. L'applicazione che invia il messaggio e-mail fa riferimento a questo nome.

Ultima modifica

La data e l'ora dell'ultima modifica del modello.

Nuovo

Consente di creare un nuovo modello e-mail.

1. Fare clic sull'icona +.
2. Specificare un nome per il nuovo modello (ad esempio Approvazione) e fare clic su **OK**.

Se sono state disabilitate le finestre popup, verrà visualizzata nuovamente la finestra popup Modifica modello di notifica e-mail. Il nome del nuovo modello viene visualizzato nella colonna Nome, ma nella colonna dell'intestazione Oggetto viene visualizzato [No Subject] (Nessun oggetto). In questo caso, fare clic su [No Subject] (Nessun oggetto) in modo da poter fornire i dettagli nel nuovo modello.

Modifica modello di notifica e-mail

La pagina Modifica modello di notifica e-mail consente di modificare il modello e-mail. È possibile personalizzare il testo del modello.

Nome modello

Visualizza il nome del modello.

Oggetto

Testo visualizzato dall'utente nell'intestazione Oggetto di un'e-mail. È possibile modificare il testo dell'oggetto; il nome effettivo del modello rimarrà lo stesso.

Invia come

Il formato utilizzato dal server SMTP per inviare l'e-mail: Testo o HTML.

Token o tag sostitutivi

Grazie ai tag sostituivi è possibile personalizzare il messaggio per l'utente. È possibile copiare i tag sostitutivi dall'elenco dei tag disponibili e incollarli nel messaggio.

Ciascun modello include token o tag sostitutivi di default, ovvero le variabili necessarie per la personalizzazione del messaggio e-mail in base all'utente. Ad esempio, il modello e-mail Password dimenticata per l'invio della password all'utente, include il token o il tag sostitutivo di default denominato '$CurrentPassword'.

Aggiungi: è possibile definire altri token o tag di sostituzione da utilizzare nel corpo del messaggio.

Per aggiungere un token o un tag sostitutivo, eseguire i passaggi seguenti:

1. Fare clic sull'icona  .
2. Specificare il **Nome** e la **Descrizione** nella finestra **Add Replacement Tag** (Aggiungi tag sostitutivo).
3. Fare clic su **OK**.
4. Il nuovo token o tag sostitutivo viene elencato nella colonna Tag sostitutivi.

Copia tag: fare clic su  per copiare il tag selezionato nel buffer del sistema, quindi fare clic sul mouse per incollarlo e utilizzarlo nella riga dell'oggetto o nel corpo del messaggio.

Elimina: selezionare un token o un tag sostitutivo nell'elenco e fare clic su  per eliminare il tag dall'elenco. Assicurarsi di non rimuovere i tag necessari per il corpo del messaggio.

Corpo del messaggio

Il testo del messaggio e-mail.

Fare clic su **Aggiorna** dopo aver specificato tutte le modifiche apportate al modello di notifica e-mail.

Elimina

Rimuove (da Identity Vault) i modelli creati dall'utente. Non è possibile eliminare i modelli di default forniti con applicazioni quali Identity Manager.

1. Selezionare il modello che si desidera eliminare.

   Se si fa clic sull'intestazione dell'oggetto del modello, in Identity Console viene visualizzata la finestra di dialogo Edit Email Templates (Modifica modelli e-mail).
2. Fare clic sull’icona Elimina.
3. Fare clic su **OK**.

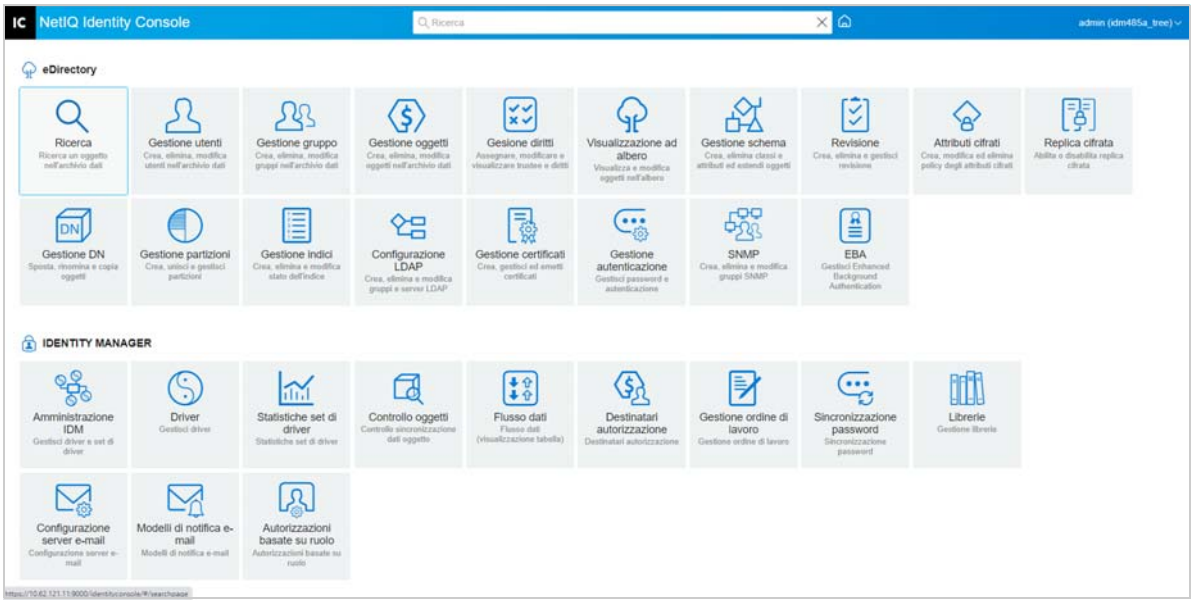
Filtra modelli

Consente di filtrare il modello e-mail che si desidera visualizzare. Verranno visualizzati solo i modelli selezionati. L'opzione Filter by all (Filtra per tutti) visualizza tutti i modelli.

Aggiorna modelli

Fare clic sull'icona per aggiornare e rimuovere tutti i filtri applicati ai modelli.

Figura 32-1 *Modelli di notifica e-mail*



33 Gestione delle autorizzazioni basate su ruolo

L'autorizzazione basata su ruolo consente di concedere autorizzazioni su sistemi connessi a un gruppo di utenti di NetIQ® Identity Console. Le policy autorizzazione basata su ruolo semplificano la gestione delle policy aziendali e riducono la necessità di configurare i driver di Identity Manager.

Il modulo Autorizzazioni basate su ruolo presenta le seguenti opzioni:

Autorizzazioni basate su ruolo

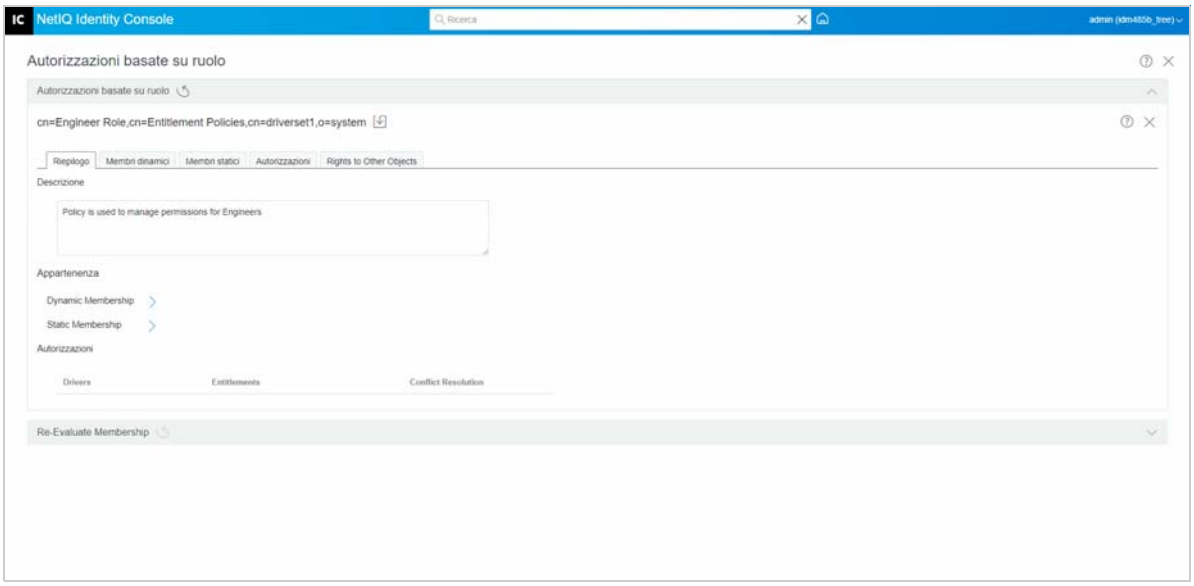
Una policy autorizzazione basata su ruolo è un oggetto Gruppo dinamico di Identity Console con funzioni aggiuntive che consentono di concedere le autorizzazioni basate su ruolo sui sistemi connessi. Quando si crea una policy autorizzazione basata su ruolo, si definiscono l'appartenenza della policy e le autorizzazioni che devono essere concesse ai membri della policy autorizzazione basata su ruolo. Ciascuna policy autorizzazione basata su ruolo è associata a un singolo oggetto Set di driver assegnato a un determinato server. Analogamente a un driver di Identity Manager, ciascuna policy autorizzazione è in grado di gestire solo gli oggetti contenuti in una replica master o in lettura/scrittura sul server a cui è assegnata.

Le seguenti sezioni spiegano in dettaglio l'autorizzazione basata sul ruolo:

Riepilogo

In questa pagina viene fornito un riepilogo di una vista di alto livello dei criteri di appartenenza e delle autorizzazioni per la policy autorizzazione.

Figura 33-1 *Pagina di riepilogo*



Appartenenza:

I criteri specificati per l'appartenenza dinamica vengono visualizzati nella sintassi di un filtro LDAP. Identità di ricerca indica quali diritti dell'oggetto vengono utilizzati durante l'interrogazione per l'appartenenza dinamica, mentre DN di base e Ambito indicano la parte dell'albero inclusa nell'interrogazione.

È possibile visualizzare le inclusioni e le esclusioni delle appartenenze statiche selezionando la casella di controllo.

L'elenco combinato di tutti i membri non viene visualizzato nella pagina Riepilogo poiché l'elenco potrebbe essere lungo. Per visualizzare un elenco combinato di tutti i membri della policy autorizzazione, sia dinamici che statici, utilizzare la scheda Appartenenza > View Membership (Visualizza appartenenza).

Autorizzazioni:

Le autorizzazioni sui sistemi connessi concesse ai membri della policy autorizzazione. Tenere presente che le autorizzazioni basate su ruolo sono vagamente coerenti con i sistemi connessi. Ciò significa che lo stato di un'autorizzazione su un sistema connesso non viene visualizzato nell'interfaccia della policy autorizzazione. Se si concede un'autorizzazione a una policy autorizzazione e successivamente tale autorizzazione non è più disponibile nel sistema connesso, l'autorizzazione rimane elencata nella policy autorizzazione fino a quando non viene rimossa manualmente dall'elenco.

Conflict Resolution (Risoluzione dei conflitti):

Per le policy autorizzazione basata su ruolo che dispongono di valori, questi metodi vengono utilizzati per determinare quali valori vengono concessi a un utente se due o più policy autorizzazione basata su ruolo concedono valori diversi a tale utente. Un esempio di autorizzazione con valori è l'appartenenza agli elenchi di distribuzione e-mail, in cui i valori corrispondono ai nomi degli elenchi di distribuzione.

Il metodo di risoluzione dei conflitti viene impostato separatamente per ciascuna singola autorizzazione su ciascun oggetto Driver. Se un'autorizzazione viene utilizzata in più policy autorizzazione basata su ruolo, il metodo di risoluzione dei conflitti è lo stesso in tutte le policy autorizzazione basata su ruolo. Per modificare il metodo di risoluzione dei conflitti per un'autorizzazione, modificare l'impostazione di tale autorizzazione nel manifesto del relativo driver.

- **Unrecognized (Non riconosciuta):** la policy autorizzazione basata su ruolo non è stata completata nella procedura guidata o l'impostazione è stata digitata in modo errato nel manifesto del driver.
- **Merge (Unione):** l'impostazione di default è Merge (Unione) (`union` (unione) nel manifesto del driver). Ciò significa che a un utente vengono concessi tutti i valori per questa autorizzazione da tutte le policy autorizzazione basata su ruolo di cui è membro.

  Quando si utilizza l'impostazione di default Merge (Unione), l'ordine di priorità dell'elenco di policy non è importante per questa autorizzazione particolare.

  Ad esempio, a un utente viene concessa l'appartenenza agli elenchi di distribuzione e-mail per il Driver A di GroupWise® da due diverse policy autorizzazione basata su ruolo, la policy Manager e la policy Membri del team. Nella Policy 1 viene concessa all'utente l'appartenenza all'elenco di distribuzione e-mail Manager e nella Policy 2 viene concessa all'utente l'appartenenza all'elenco di distribuzione e-mail Membri del team. Con l'impostazione di Merge (Unione), all'utente viene concessa l'appartenenza a entrambi gli elenchi di distribuzione e-mail.
- **Priority (Priorità):** questa impostazione indica che se più policy autorizzazione basata su ruolo concedono a un utente valori diversi per la stessa autorizzazione dallo stesso oggetto Driver, all'utente vengono concessi solo i valori specificati nella policy autorizzazione basata su ruolo al primo posto nell'elenco.

  Quando si utilizza l'impostazione di Priority (Priorità), l'ordine di priorità dell'elenco di policy è importante per questa autorizzazione particolare.

  Ad esempio, a un utente viene concessa l'appartenenza agli elenchi di distribuzione e-mail per il Driver A di GroupWise® da due diverse policy autorizzazione basata su ruolo, la policy Manager e la policy Membri del team. Nella policy Manager viene concessa all'utente l'appartenenza all'elenco di distribuzione e-mail Manager e nella policy Membri del team viene concessa all'utente l'appartenenza all'elenco di distribuzione e-mail Membri del team. La policy Manager è elencata a un livello superiore nell'elenco delle policy rispetto alla policy Membri del team. Con l'impostazione di Priority (Priorità), all'utente viene concessa l'appartenenza solo all'elenco di distribuzione e-mail Manager.

  L'utilizzo della priorità per la risoluzione dei conflitti può essere utile se, ad esempio, un attributo nel sistema connesso consente solo un valore singolo. Se due policy autorizzazione basata su ruolo diverse concedono un valore per l'attributo allo stesso utente, l'utente riceve il valore concesso dalla policy autorizzazione basata su ruolo al primo posto nell'elenco.

Nota: Per le autorizzazioni che non dispongono di valori, ad esempio un account, non viene fornita un'impostazione per la risoluzione dei conflitti. Le autorizzazioni che non dispongono di valori vengono concesse sempre ai membri della policy autorizzazione basata su ruolo, indipendentemente dalla priorità delle policy presenti nell'elenco.

Membri dinamici

I criteri specificati per l'appartenenza dinamica vengono visualizzati nella sintassi di un filtro LDAP. Identità di ricerca indica quali diritti dell'oggetto vengono utilizzati durante l'interrogazione per l'appartenenza dinamica, mentre DN di base e Ambito indicano la parte dell'albero inclusa nell'interrogazione.

Filtro appartenenza

È possibile definire criteri di appartenenza, ad esempio la posizione nell'albero e gli attributi dell'oggetto. Ad esempio, l'appartenenza può dipendere dalla presenza dell'utente nel container Attivo o dalla presenza della parola Manager nella qualifica. Gli utenti che soddisfano i criteri vengono resi automaticamente membri della policy autorizzazione basata su ruolo, senza dover aggiungere specificatamente ciascun utente alle policy. L'appartenenza dinamica è la stessa di un oggetto Gruppo dinamico.

Se un oggetto viene modificato in modo da non soddisfare più i criteri per l'appartenenza dinamica, le autorizzazioni vengono automaticamente revocate alla successiva rivalutazione dell'utente.

Set Search Parameters (Imposta parametri di ricerca)

Specificare la posizione degli utenti che si desidera gestire con la policy Autorizzazione. Scegliere il container contenente gli utenti (DN di base) e il livello di distanza dal container desiderato per la ricerca (Scope of Search (Ambito di ricerca)). Per consentire alla policy Autorizzazione di gestire gli utenti nei container specificati, gli utenti devono essere in modalità lettura/scrittura o in una replica master sul server.

Per Scope of Search (Ambito di ricerca) vengono fornite le seguenti opzioni:

- Questo container e i sottocontainer: gli utenti al di sotto di questo container nell'albero sono membri della policy Autorizzazione se soddisfano i criteri specificati per l'appartenenza dinamica. Anche gli utenti all'interno dei sottocontainer sono membri se soddisfano i criteri.
- Solo questo container: gli utenti all'interno di questo container sono membri della policy Autorizzazione solo se soddisfano i criteri specificati per l'appartenenza dinamica. Gli utenti all'interno dei sottocontainer al di sotto di questo container non sono membri anche se soddisfano i criteri.

Define Filter Criteria (Definisci criteri del filtro)

Specificare le caratteristiche che determinano quali utenti sono membri della policy Autorizzazione.

Nella pagina Riepilogo di una policy Autorizzazione, i criteri di appartenenza dinamica specificati vengono visualizzati nella sintassi di un filtro LDAP.

Di default, l'appartenenza dinamica è impostata in modo da includere tutti gli oggetti della classe Utente (e gli oggetti delle classi derivate dalla classe Utente) nell'ambito di ricerca come membri della policy Autorizzazione.

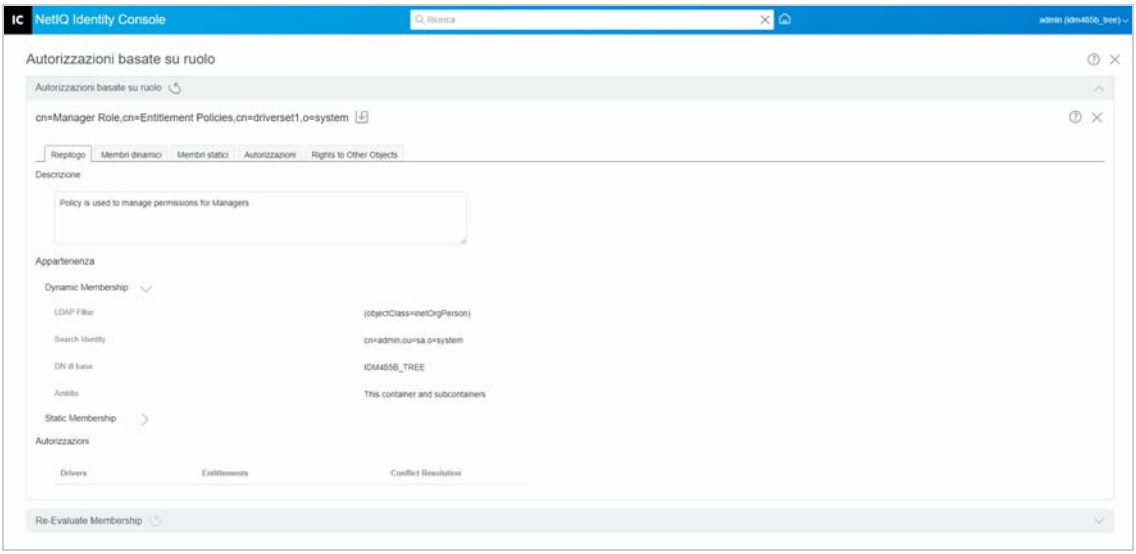
Nota: Se si crea una nuova classe di oggetti derivata da Utente, una policy Autorizzazione esistente non viene a conoscenza di tale classe fino a quando non si apporta una modifica alla policy Autorizzazione. Ciò impedisce di concedere involontariamente le autorizzazioni agli utenti di una nuova classe. Quando si apportano modifiche alla policy Autorizzazione, viene aggiornato l'elenco delle classi derivate dall'utente per la policy.

Creazione di un'appartenenza dinamica

Nella scheda Membri dinamici, eseguire le operazioni seguenti:

1. Fare clic sulla scheda **Membri dinamici**.
2. Utilizzare i filtri **Identità di ricerca**, **Inizia ricerca in** e **Ambito ricerca** in base alle proprie esigenze.
3. Fare clic sulla voce **Crea gruppo** specifica per creare una nuova condizione o una nuova riga, quindi specificare i criteri o le condizioni di ricerca richiesti.

Figura 33-2 *Membri dinamici*



Ambito di ricerca: l'ambito di ricerca indica l'insieme di voci in corrispondenza o al di sotto del DN di base della ricerca che possono essere considerate corrispondenze potenziali per un'operazione di ricerca.

Criteri di ricerca: è possibile limitare una ricerca per individuare un record o un gruppo di record specifico all'interno di un numero elevato di record.

DN di base: un DN di base rappresenta il punto da cui un server eseguirà la ricerca di utenti.

Gruppo LDAP: è un'organizzazione gerarchica di utenti, gruppi e unità organizzative che fungono da container per utenti e gruppi.

Nota: L'utente può creare uno o più gruppi con condizioni. Le condizioni sono costituite da attributi, operatori e valori. Di default, viene popolato **Object Class** (Classe di oggetti) > **è uguale a** > **Utente**.

Membri statici

I membri statici sono classi di membri dichiarati mediante parole chiave statiche. Un membro statico dispone di determinati accessi limitati.

Nella scheda Membri statici è possibile eseguire le seguenti operazioni:

Include Members (Includi membri):

Aggiungere in modo statico i membri non inclusi nel filtro di appartenenza dinamico.

Exclude Members (Escludi membri):

Escludere i membri che soddisfano i criteri del filtro ma che non devono essere inclusi nella policy autorizzazione.

Autorizzazioni

La policy autorizzazione basata su ruolo consente di concedere autorizzazioni sui sistemi connessi e diritti in Identity Manager. Le autorizzazioni possono essere dei seguenti tipi:

- Account sui sistemi connessi.
- Appartenenza alle liste di distribuzione e-mail sui sistemi connessi.
- Appartenenza a gruppi nei sistemi connessi.
- Attributi per gli oggetti corrispondenti nei sistemi connessi, popolati con i valori specificati.

Nota: La funzionalità Autorizzazioni fa parte di Identity Manager, pertanto è necessario che i driver di Identity Manager siano installati e configurati per supportare le autorizzazioni prima di concedere autorizzazioni sui sistemi connessi.

Creare autorizzazioni

Nella scheda Autorizzazioni, eseguire le operazioni seguenti:

1. Fare clic sulla scheda **Autorizzazione**.
2. Fare clic su + per selezionare **Add Drivers** (Aggiungi driver) e fornire autorizzazioni sui sistemi connessi.

   Viene visualizzata la schermata **Add Driver** (Aggiungi driver).
3. Selezionare il driver dall'elenco a discesa.
4. Fare clic su **Aggiungi**.

   Viene visualizzata la schermata **Add Entitlements** (Aggiungi autorizzazioni).
5. Dal menu a discesa utilizzare **Select an Entitlement** (Selezionare un'autorizzazione) per scegliere il gruppo di autorizzazioni che si desidera aggiungere.
6. Selezionare il tipo di interrogazione tramite **Query Type** (Tipo di interrogazione):
   - **Cached (Memorizzata nella cache):** se le interrogazioni sono state eseguite in precedenza.
   - **External Query (Interrogazione esterna):** se le interrogazioni sono nuove.

Viene visualizzata la schermata **Add Group Entitlement** (Aggiungi autorizzazione gruppo).

7 Selezionare l'autorizzazione gruppo dal menu a discesa, quindi fare clic su **Seleziona**.

Rights to other Objects (Diritti su altri oggetti)

Utilizzare questa pagina per assegnare a un oggetto eDirectory i diritti di trustee delle policy Autorizzazione. Ciascun membro della policy Autorizzazione diventa un trustee dell'oggetto.

Oltre ad assegnare diritti a tutti gli attributi, è possibile fare clic su Add Property (Aggiungi proprietà) per assegnare diritti a proprietà specifiche.

La casella di controllo Eredita determina se i diritti devono essere assegnati verso il basso nell'albero. Ad esempio, se si assegnano diritti a un oggetto Container e si desidera che la policy Autorizzazione disponga degli stessi diritti sugli oggetti e sui sottocontainer al di sotto di tale container, selezionare la casella di controllo Eredita.

I diritti sugli oggetti in eDirectory vengono concessi ai membri della policy Autorizzazione dopo aver completato le modifiche in questa pagina. Per contro, le autorizzazioni nei sistemi connessi vengono concesse a ciascun membro della policy Autorizzazione alla successiva modifica di un attributo utilizzato per l'appartenenza dinamica per tale utente oppure quando l'utente viene spostato o rinominato. Lo stesso vale quando vengono revocati diritti e autorizzazioni. Utilizzare il task Rivaluta appartenenza per forzare un aggiornamento.

Creare diritti su altri oggetti

Per creare diritti:

1 Fare clic sulla scheda **Rights to Other Objects** (Diritti su altri oggetti).

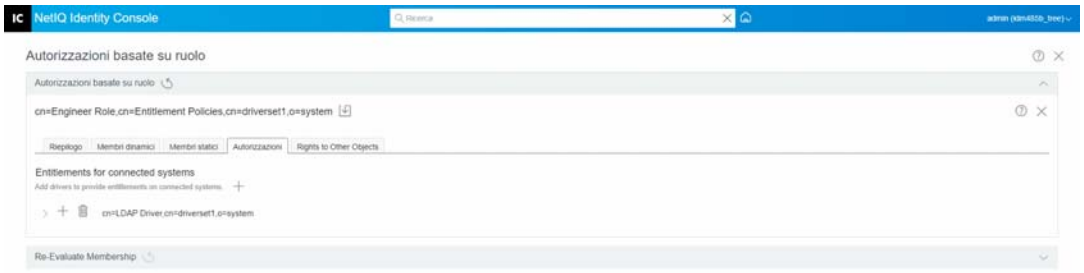
Qui è possibile aggiungere un nuovo oggetto e cercare gli oggetti per cui si desidera impostare questa policy Autorizzazione come trustee.

1a Per aggiungere un oggetto, fare clic sul pulsante  .

Viene visualizzata la pagina **BROWSER DEL CONTESTO**. La pagina è costituita da `oggetti`.

1b Espandere gli `oggetti`, selezionare gruppi o singoli utenti in base alle proprie esigenze e assegnare loro i diritti.

Figura 33-3 *Rights to other Objects (Diritti su altri oggetti)*

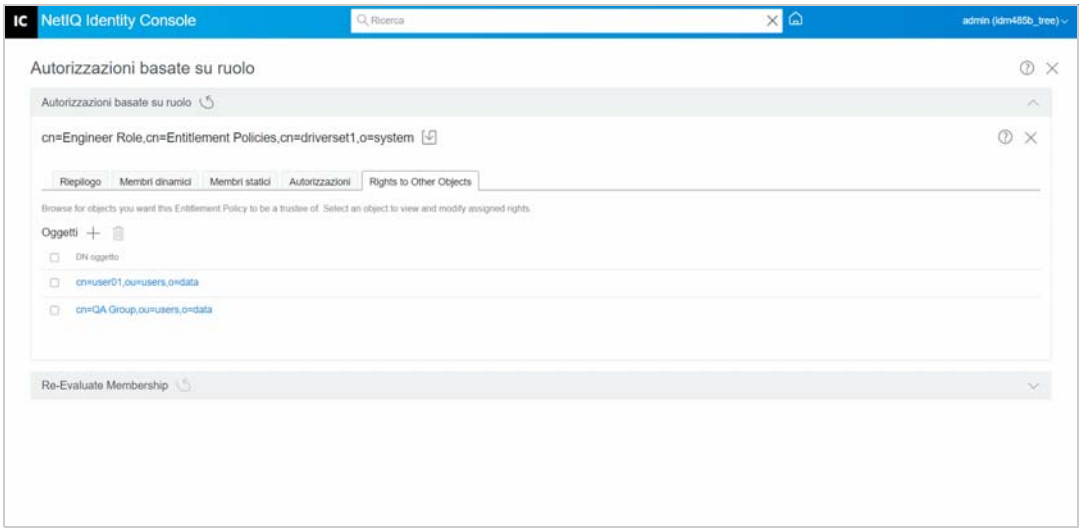


1c Per aggiungere altre proprietà, fare clic su +.

Viene visualizzata la pagina **SELECT PROPERTIES** (SELEZIONA PROPRIETÀ). Questa pagina riporta l'elenco delle proprietà disponibili per un oggetto.

1d Fare clic su **Fatto**.

Figura 33-4 *Selezionare Proprietà*



2 (Facoltativo) Utilizzare le frecce **Su** e **Giù** per assegnare priorità alle policy autorizzazione basata su ruolo.

La definizione delle priorità per la policy consente di risolvere i conflitti di autorizzazione tra più policy. La policy di livello più alto ha la priorità più alta. Per ulteriori informazioni, vedere: "Assegnare la priorità alle policy autorizzazione basata su ruolo" a pagina 215

Assegnare la priorità alle policy autorizzazione basata su ruolo

Quando si creano policy autorizzazione basata su ruolo, è possibile che si creino conflitti tra le policy relative a un determinato utente.

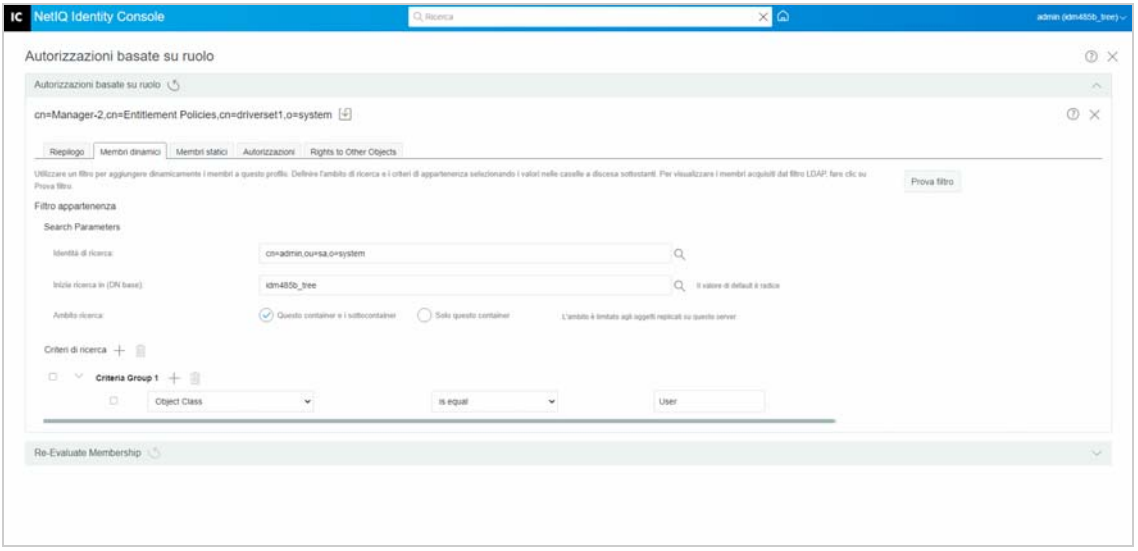
L'ordine delle policy autorizzazione basata su ruolo nell'elenco rappresenta la priorità. È possibile modificare l'ordine dell'elenco utilizzando i pulsanti freccia su e giù.

- Questa impostazione può essere utile se, ad esempio, un attributo sul sistema connesso consente solo un valore singolo. Se due policy autorizzazione basata su ruolo diverse concedono un valore per l'attributo allo stesso utente, l'utente riceve il valore concesso dalla policy autorizzazione basata su ruolo al livello più in alto nell'elenco. Come altro esempio, è possibile che l'ambiente sia stato configurato in modo da utilizzare le autorizzazioni per inserire gli utenti in una struttura gerarchica su un altro sistema. Potrebbe essere necessario collocare l'utente in una posizione o in un'altra, non in due posizioni contemporaneamente.
- Tenere presente che l'impostazione è indipendente per ciascuna autorizzazione offerta da ciascun driver.
- Di regola, è consigliabile collocare le policy di amministratore o manager nell'elenco a un livello superiore rispetto alle policy per gli utenti finali o i singoli collaboratori. È consigliabile collocare i gruppi con un'appartenenza più stretta a un livello superiore rispetto ai gruppi con un'appartenenza più ampia.

Per impostare la priorità delle policy autorizzazione basata su ruolo:

1. Selezionare la policy autorizzazione che si desidera portare a un livello superiore o inferiore.
2. Utilizzare le frecce **Su** o **Giù** per assegnare priorità alle policy autorizzazione basata su ruolo.

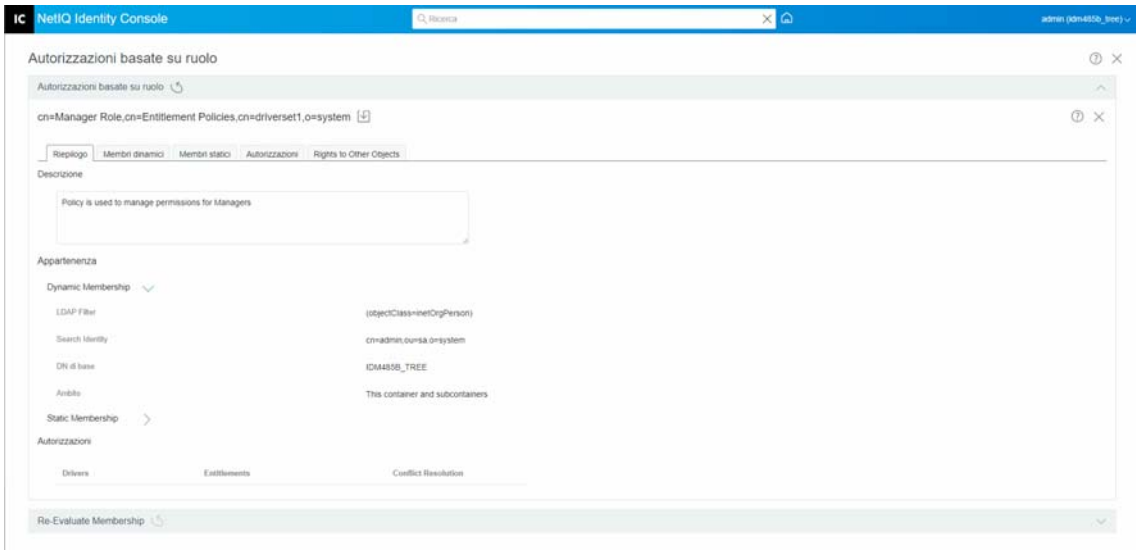
   Figura 33-5 *Assegnazione della priorità alle policy*



3. Fare clic sul pulsante Salva .

   Il riepilogo dei dettagli relativi all'appartenenza alla policy viene visualizzato nella scheda **Riepilogo**.
4. Riavviare il driver.

Figura 33-6 *Chiusura e riavvio*



Nota: Per applicare le modifiche è necessario riavviare il driver.

Rivaluta appartenenza

La funzione **Autorizzazioni basate su ruolo** consente di concedere autorizzazioni su sistemi connessi a un gruppo di utenti.

Quando si crea o si modifica una policy autorizzazione basata su ruolo, è necessario rivalutare l'appartenenza di ciascun utente per stabilire se è necessario concedere, modificare o revocare le autorizzazioni sui sistemi connessi. Di default, la rivalutazione viene eseguita un utente per volta, alla successiva modifica di un attributo che influisce sull'appartenenza di ciascun utente o quando un utente viene spostato o rinominato. Questo comportamento di default riduce al minimo l'utilizzo delle risorse di sistema ma potrebbe verificarsi un ritardo significativo tra la modifica della policy autorizzazione basata su ruolo e la concessione, la modifica o la revoca delle autorizzazioni per un determinato utente.

È possibile assicurarsi che le autorizzazioni utente siano aggiornate tutte contemporaneamente utilizzando il task “Rivalutazione delle policy autorizzazione basata su ruolo” a pagina 217 per specificare gli utenti da rivalutare immediatamente. Si consiglia di eseguire questa operazione ogni volta che si crea o si modifica una policy autorizzazione basata su ruolo.

Nelle versioni antecedenti a Identity Manager 3.6, la rivalutazione dell'appartenenza veniva eseguita per tutte le policy autorizzazione basata su ruolo in un set di driver, non per una singola policy Autorizzazione. Tuttavia, Identity Manager 3.6 consente di **valutare** una policy autorizzazione basata su ruolo e di **aggiungere** i membri all'**elenco di oggetti** selezionato. Se è stata definita una policy Autorizzazione ed è stato creato un elenco di appartenenze, verrà visualizzata l'intestazione Valutare una policy autorizzazione per **aggiungere** i suoi membri all'elenco accanto alla voce Oggetti selezionata. Selezionare la policy, quindi fare clic sull'icona + per aggiungere i membri della policy all'**elenco di oggetti** selezionato. È possibile aggiungere o rimuovere membri o oggetti dall'**elenco di oggetti** selezionato.

Per utilizzare in modo ottimale le risorse di sistema, si consiglia di apportare tutte le modifiche alle policy autorizzazione basata su ruolo in un determinato set di driver prima di utilizzare "Rivalutazione delle policy autorizzazione basata su ruolo" a pagina 217 (Rivaluta policy autorizzazione basata su ruolo).

Nota: La rivalutazione delle autorizzazioni è necessaria solo per le autorizzazioni sui sistemi connessi. Quando si modificano i diritti di Identity Console per una policy autorizzazione basata su ruolo, le modifiche vengono applicate immediatamente per ciascun utente. Per poter eseguire le rivalutazioni dell'appartenenza, è necessario che il driver servizi autorizzazioni sia in esecuzione.

Rivalutazione delle policy autorizzazione basata su ruolo

Per rivalutare l'appartenenza:

1. Fare clic su **Rivaluta appartenenza** > **Seleziona set di driver**.

   Verrà visualizzato un elenco di policy create.

2. Selezionare la policy da valutare e fare clic su **Evaluate**

(Valuta).

   Nella scheda **Oggetti** verranno visualizzati gli utenti che fanno parte del gruppo.

3. (Facoltativo) Per aggiungere un utente specifico, fare clic su  .

   Se gli utenti non sono presenti nell'elenco e si desidera aggiungere utenti specifici, è possibile utilizzare la funzione **Aggiungi**  .

4. (Facoltativo) Per rimuovere un utente specifico, fare clic su .

   Se è necessario rimuovere utenti specifici dall'elenco, è possibile utilizzare la funzione **Elimina** .

5. Fare clic sul pulsante Rivaluta appartenenza .

Figura 33-7 *Rivaluta appartenenza*