

Note di rilascio di NetIQ Identity Manager 4.9

Maggio 2024

NetIQ Identity Manager 4.9 fornisce nuove funzioni e miglioramenti, offre una migliore usabilità e rispetto alle versioni precedenti sono stati risolti molti problemi. Gli aggiornamenti di questa versione sono cumulativi. Includono correzioni software e miglioramenti presenti nella versione corrente, nonché tutte le correzioni precedentemente rilasciate da service pack, patch e hotfix. Molti miglioramenti sono stati apportati in base ai suggerimenti forniti dai clienti, che ringraziamo per la loro valida collaborazione. Confidiamo che anche in futuro continueranno ad aiutarci a migliorare i nostri prodotti affinché possano soddisfare tutte le loro esigenze. È possibile pubblicare commenti e suggerimenti nei [forum della comunità di Identity Manager](#) su NetIQ Communities, la nostra comunità online che include anche informazioni sui prodotti, blog e collegamenti a risorse utili.

Per ulteriori informazioni sulle novità rispetto alle versioni precedenti, vedere la sezione "Versioni precedenti" sul [sito Web della documentazione di Identity Manager \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/).

Per ulteriori informazioni relative a questa versione e alle note sulla versione più recenti, visitare la pagina della [Documentazione \(https://www.netiq.com/documentation/identity-manager-49/\)](https://www.netiq.com/documentation/identity-manager-49/). Per effettuare il download di questo prodotto, fare riferimento al portale [Software Licenses and Downloads \(https://sld.microfocus.com\)](https://sld.microfocus.com).

- ♦ "Novità" a pagina 2
- ♦ "Cambiamenti significativi nel comportamento o nell'utilizzo" a pagina 6
- ♦ "Funzionalità non più supportate" a pagina 6
- ♦ "Versioni supportate dei componenti" a pagina 6
- ♦ "Requisiti di sistema" a pagina 8
- ♦ "Problemi risolti" a pagina 8
- ♦ "Installazione di NetIQ Identity Manager 4.9" a pagina 12
- ♦ "Upgrade a NetIQ Identity Manager 4.9" a pagina 16
- ♦ "Problemi noti" a pagina 20
- ♦ "Contatti di Micro Focus" a pagina 30
- ♦ "Note legali" a pagina 30

Novità

Identity Manager 4.9 fornisce le seguenti nuove funzioni e i seguenti miglioramenti:

- ♦ [“Supporto al sistema operativo” a pagina 2](#)
- ♦ [“NetIQ Audit, Compliance & Data Intelligence” a pagina 2](#)
- ♦ [“I driver di Identity Manager supportano ora Java 11” a pagina 3](#)
- ♦ [“Supporto per l'autenticazione moderna” a pagina 4](#)
- ♦ [“Capacità di configurare Identity Manager in modalità FIPS” a pagina 4](#)
- ♦ [“Integrazione del Servizio workflow nel framework di monitoraggio” a pagina 4](#)
- ♦ [“Miglioramenti delle applicazioni di Identity” a pagina 4](#)
- ♦ [“Miglioramenti del programma di installazione” a pagina 6](#)

Per informazioni sulle nuove funzioni di NetIQ Identity Manager Designer 4.9, vedere le [Note di rilascio di Designer 4.9 per NetIQ Identity Manager](#).

Supporto al sistema operativo

In questa release è stato aggiunto il supporto per le seguenti piattaforme:

- ♦ Red Hat Enterprise Linux (RHEL) 9.3, 9.2, 8.9 e 8.8
- ♦ Open Enterprise Server (OES) 24.2
- ♦ For Designer per Identity Manager
 - ♦ Red Hat Enterprise Linux (RHEL) 9.2, 9.1, 8.9, 8.8 e 8.7
 - ♦ SUSE Linux Enterprise Server (SLES) 15 SP5
 - ♦ Windows 11 (desktop)
 - ♦ macOS Sonoma

Per un elenco completo dei sistemi operativi supportati, vedere la pagina relativa ai [Requisiti di sistema per Identity Manager 4.9](#). Per informazioni sui componenti inclusi nel pacchetto, sui database e sui browser supportati con questa versione, vedere [“Versioni supportate dei componenti” a pagina 6](#).

NetIQ Audit, Compliance & Data Intelligence

Identity Manager introduce Audit, Compliance & Data Intelligence (ACDI), un nuovo strumento che fornisce analisi visive per i dati relativi all'identità. La soluzione raccoglie tutti i dati relativi all'identità dalle origini di Identity Manager, li elabora e offre funzionalità di reporting e monitoraggio sul dashboard ACDI. Per ulteriori informazioni su questo strumento, vedere [NetIQ Audit, Compliance and Data Intelligence for Identity Manager](#) (in lingua inglese).

ACDI è disponibile come componente aggiuntivo insieme a Identity Manager 4.9. È possibile effettuarne il download dal portale [Software License and Download](https://sld.microfocus.com/mysoftware/index) (<https://sld.microfocus.com/mysoftware/index>). Lo strumento è disponibile solo per la soluzione off-cloud di Identity Manager 4.9, non per la distribuzione su cloud.

I driver di Identity Manager supportano ora Java 11

In questa versione è stato aggiunto il supporto di Java 11 per i driver di Identity Manager 4.9. Di seguito è riportato un elenco dei driver aggiornati.

Tabella 1 Driver di Identity Manager 4.9 e relativa versione funzionale equivalente in 4.8.x

Driver	Versione inviata con 4.9	Versione base (Identity Manager 4.8.x)
Azure Active Directory (AD)	5.2.0.0000	5.1.7.0200
Bidirectional eDirectory	4.1.0.0000	4.0.8.0300
REST	1.3.0.0000	1.2.0.0000
Testo delimitato	4.1.0.0000	4.0.2.0200
GroupWise (REST-based)	4.1.0.0000	4.0.1.1
Identity Gateway Integration Module	1.1.0.0000	1.0.1.0300
JDBC	4.3.0.0000	4.2.2.0400
JDBC Fanout	1.3.0.0000	1.2.8
JMS	4.1.0.0000	4.0.0
LDAP	4.3.0.0000	4.2.0.0200
Lotus Notes	4.2.0.0000	4.1.2.0100
Manual Task Service	4.2.0.0000	4.1.0
Oracle E-Business Suite HR	4.2.0.0000	4.1.2.1
Oracle E-Business Suite TCA	4.2.0.0000	4.1.2.1
Oracle E-Business Suite User Management	4.2.0.0000	4.1.2.0101
PeopleSoft	5.3.0.0000	5.2.4.0
Entitlements Service	4.1.0.0000	4.0.1.0
Salesforce	4.2.0.0000	4.1.0.1
SAP HR	4.1.0.0000	4.0.4.1
SAP Portal	4.1.0.0000	4.0.2.0100
SAP User Management	4.1.0.0000	4.0.4.1
SCIM	1.1.0.0000	1.0.1.0300
ServiceNow	1.1.0.0000	1.0.0
SOAP	4.2.0.0000	4.1.0.1
WorkOrder	4.1.0.0000	4.0.0.0 100
Workday	1.4.0.0000	1.3.0.0200
Identity Tracking for Sentinel	4.1.0.0000	4.0.2

Driver	Versione inviata con 4.9	Versione base (Identity Manager 4.8.x)
ID Provider	4.1.0.0000	4.0.0.0

Non sono presenti nuove funzioni, ad eccezione del file delle classi Java aggiornato. Per ulteriori informazioni, vedere la sezione **Version Shipped with 4.9** nella pagina [NetIQ Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/) (Driver di NetIQ Identity Manager).

Supporto per l'autenticazione moderna

Oltre all'autenticazione di base, le applicazioni di Identity supportano l'autenticazione moderna nelle impostazioni delle e-mail in entrata e in uscita per l'approvazione basata su posta elettronica. L'autenticazione moderna fornisce un livello più sicuro di autenticazione degli utenti e l'autorizzazione degli accessi.

Inoltre, l'autenticazione moderna è integrata con il motore di Identity Manager per [autenticare le notifiche dei lavori](#) e inviare [e-mail basate su modelli](#) durante l'esecuzione delle policy.

Nota: questa versione supporta l'autenticazione moderna solo se si utilizza il servizio di autenticazione OAuth di Office 365 fornito da Azure Active Directory (Azure AD) per Microsoft Outlook.

Capacità di configurare Identity Manager in modalità FIPS

È ora possibile configurare i componenti di Identity Manager in modalità FIPS. Per ulteriori informazioni, vedere [Configuring Identity Manager in FIPS Mode](#) (Configurazione di Identity Manager in modalità FIPS) in [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) (Guida all'installazione e all'upgrade di NetIQ Identity Manager per Linux) o [Installing and Configuring Identity Manager Components](#) (Installazione e configurazione dei componenti di Identity Manager) in [NetIQ Identity Manager Install and Upgrade Guide for Windows](#) (Guida all'installazione e all'upgrade di NetIQ Identity Manager per Windows).

Integrazione del Servizio workflow nel framework di monitoraggio

Ora è possibile utilizzare il metodo di ricerca LDAP esistente per recuperare i dati di monitoraggio per il componente Servizio workflow nell'ambiente. A tale scopo, inviare una richiesta di ricerca con una base di ricerca `cn=idm,cn=monitor` su Identity Vault. Questo miglioramento consente di monitorare lo stato del Servizio workflow utilizzando varie statistiche, ad esempio workflow totali, workflow in corso, workflow completati, nuove richieste negli ultimi 10, 60 e 300 secondi e così via.

Inoltre, in questa versione sono stati aggiunti ulteriori dati `jvm_stats` alle statistiche esistenti per l'Applicazione utente. Per ulteriori informazioni su questi miglioramenti, vedere la sezione relativa al [monitoraggio di Identity Manager](#).

Miglioramenti delle applicazioni di Identity

In questa versione sono stati introdotti i seguenti miglioramenti alle applicazioni di Identity:

Versione migliorata dello strumento Applicazioni di Identity

NetIQ Identity Manager 4.9 è stato aggiornato con una versione migliorata dello strumento Applicazioni di Identity. Lo strumento supporta ora la piattaforma Java 11. Questo miglioramento include le seguenti utility:

- ♦ [Utility di migrazione dei workflow](#)
- ♦ [Utility dell'API di migrazione dei workflow](#)
- ♦ [Utility di migrazione delle impostazioni client](#)

Per ulteriori informazioni su come utilizzare ognuna di queste utility, fare clic sul collegamento nell'elenco.

Una nuova proprietà per modificare il comportamento di default della registrazione dei workflow

Le [linee guida per abilitare la registrazione dei workflow](#) sono state aggiornate. A partire da questa versione, il livello di log specificato nel file `workflow_logging.xml` per un singolo pacchetto ha per default la precedenza. Ad esempio, se il livello di log per il pacchetto `com.novell.soa.af.impl.timers` è impostato su `DEBUG` e il livello di log per Workflow Engine (a livello globale) è impostato su `INFO`, l'applicazione registra informazioni di `DEBUG` solo per il pacchetto selezionato. Tutti gli altri pacchetti e logger vengono registrati al livello di log `INFO`.

Inoltre, è stata introdotta una nuova proprietà denominata `com.microfocus.workflow.engine.logging` che consente di ripristinare il precedente comportamento. È possibile aggiungere la proprietà `com.microfocus.workflow.engine.logging` al file `ism-configuration.properties` e impostarla su `true` se si desidera che il livello di log impostato per il motore di workflow abbia precedenza sul livello di log del pacchetto. Per ulteriori informazioni su questa proprietà, vedere [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#) (in lingua inglese).

Modifiche alla funzione `IDVault.get()`

L'API di accesso `IDMProv/rest/access/entities/list` è stata aggiornata per includere un nuovo parametro di query denominato `lookupAttr`. Per default, `lookupAttr` è impostato su `false`. Se impostato su `true`, l'API restituisce gli **Attributi consultazione** specificati nella definizione **DNLookup** dell'attributo inviato nel parametro `filterAttr`. `filterAttr` è un altro parametro di query utilizzato in questa API.

Ad esempio, per recuperare i riporti diretti di un'entità utente da Identity Vault utilizzando la funzione `IDVault.get`, la firma del metodo sarebbe la seguente:

```
IDVault.get('IDM', '/rest/access/entities/list', data.manager, 'user',  
["directReports"], true)
```

In cui `directReports` è inviato come `filterAttr` e `true` è il valore di `lookupAttr`.

Nella definizione **DNLookup** di `directReports`, gli **Attributi consultazione** per l'entità **Consultazione utente** sono Cognome, Nome e Iniziali. Aggiungendo alla funzione l'attributo `true`, l'applicazione di Identity restituisce in risposta il cognome, il nome e le iniziali dei riporti diretti. Se l'**Attributo consultazione** non è configurato, non viene restituito alcun **Attributo consultazione** nella risposta.

Miglioramenti del programma di installazione

Questa versione include i seguenti miglioramenti al programma di installazione:

- ♦ Integrazione di Identity Console nel programma di installazione di Identity Manager per Linux.
- ♦ Introduzione di un nuovo file `ism-sensitive.properties`, che memorizza in modo sicuro la password delle chiavi e la password dell'archivio master utilizzate per cifrare tutte le password.

Cambiamenti significativi nel comportamento o nell'utilizzo

In questa versione di Identity Manager 4.9 sono state introdotte modifiche che potrebbero influenzare il comportamento delle applicazioni o funzionalità esistenti.

- ♦ Per la configurazione dei componenti di Identity Manager su piattaforme Linux e Windows, è richiesto il nome distinto completo (FQDN) o il nome breve del server anziché un indirizzo IP.
- ♦ Nell'utility di configurazione (`configupdate.sh`) ora viene richiesta l'immissione di una password prima del lancio.
- ♦ In caso di configurazione del driver Workday in Identity Manager 4.9 su un server Windows, se si desidera accedere al foglio di stile di esempio, è reperibile al seguente percorso nell'immagine ISO di Windows per Identity Manager 4.9:
`\IdentityManagerServer\products\IDM\windows\setup\utilities\workday\transformation_style_sheets`

Funzionalità non più supportate

A partire da questa versione, sarà ritirato il supporto per NetIQ SecretStore. D'ora in avanti, le password degli account verranno salvate in un nuovo attributo denominato `notfSMTPMailPassword`. L'attributo appartiene alla classe `notfTemplateCollection` ed è incluso nel pacchetto User Application Driver (UAD) NOVLUABASE_4.8.8.20240401125038. Con l'installazione di Identity Manager 4.9, questo pacchetto UAD viene installato automaticamente. Tuttavia, in caso di upgrade da una versione precedente, sarà necessario aggiornare il pacchetto manualmente.

Dopo l'upgrade al più recente pacchetto UAD e il riavvio di Tomcat, le password dell'account e-mail esistenti nel repository NetIQ SecretStore verranno automaticamente sottoposte a migrazione all'attributo `notfSMTPMailPassword`. Il processo di migrazione delle password è controllato dalla proprietà `com.netiq.idm.migrate.secretstore`, disponibile nel file `ism-configuration.properties`. Per default, la proprietà è impostata su `true`. Una volta completata la migrazione, la proprietà viene automaticamente reimpostata su `false` e rimane in tale stato.

Versioni supportate dei componenti

In questa sezione vengono fornite informazioni sulle versioni supportate dei componenti.

- ♦ [“Versioni dei componenti di Identity Manager” a pagina 7](#)
- ♦ [“Versioni dei componenti di terze parti” a pagina 7](#)
- ♦ [“Database” a pagina 7](#)
- ♦ [“Browser Web” a pagina 8](#)

Versioni dei componenti di Identity Manager

Pacchetti Identity Manager 4.9 per i seguenti componenti:

- ♦ NetIQ eDirectory 9.2.9
- ♦ NetIQ Identity Console 1.7.2
- ♦ NetIQ Identity Manager Engine 4.9
- ♦ NetIQ Identity Manager Remote Loader 4.9
- ♦ NetIQ Identity Manager Fanout Agent 1.3
- ♦ NetIQ Designer for Identity Manager 4.9
- ♦ NetIQ Identity Applications 4.9
- ♦ NetIQ One SSO Provider (OSP) 6.7.0
- ♦ NetIQ Self Service Password Reset (SSPR) 4.7.0.1
- ♦ NetIQ Identity Manager Identity Reporting 7.2.0
- ♦ NetIQ Sentinel Log Management for IGA 8.6.1.0 (per il controllo degli eventi)
- ♦ Driver NetIQ Identity Manager

Nota:

- ♦ Identity Manager 4.9 è inoltre compatibile con eDirectory 9.2.8.
 - ♦ Identity Manager 4.9 contiene la versione più recente di un driver supportato. Per ulteriori informazioni, vedere la sezione **Version Shipped with 4.9** nella pagina [NetIQ Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-49-drivers/\)](https://www.netiq.com/documentation/identity-manager-49-drivers/) (Driver di NetIQ Identity Manager).
-

Versioni dei componenti di terze parti

In questa versione è stato aggiunto il supporto per i seguenti componenti di terze parti:

- ♦ Zulu 11.70+15-CA
- ♦ Apache Tomcat 9.0.85-1
- ♦ PostgreSQL 12.18 (standalone e container)
- ♦ OpenSSL 1.0.2zg-0
- ♦ Nginx 1.24.0-1
- ♦ ActiveMQ 5.18.3-1

Database

Tutti i componenti di Identity Manager 4.9, incluse le applicazioni NetIQ Identity, sono compatibili con Oracle 21c e MS SQL 2019, a eccezione di Identity Reporting. Per Identity Reporting 7.2.0, continueranno a essere supportati i database Oracle19c e MS SQL 2017.

Browser Web

Almeno uno dei seguenti browser:

- ♦ Google Chrome 126.0.6478.8
- ♦ Mozilla Firefox 126.0
- ♦ Apple Safari 17.5
- ♦ Microsoft Edge 124.0.2478.109

Requisiti di sistema

Per informazioni sui requisiti hardware e sui sistemi operativi supportati, vedere la pagina [System Requirements for Identity Manager 4.9](#) di Identity Manager (in lingua inglese).

Problemi risolti

In questa release sono incluse le correzioni software riportate di seguito.

Componente	ID globale	Descrizione
Installazione e upgrade	OCTCR56A583299	Se il database è gestito su Microsoft SQL Server, il Workflow Engine non si avvia.
Motore di Identity Manager	OCTCR56A580623	Il driver SOAP aggiunge dati duplicati all'attributo <code>DirXML-PersistentData</code> , causando un'eccezione mentre iManager carica il Dashboard nella pagina Panoramica set di driver.
	OCTCR56A584222	La connessione al server dell'Applicazione utente si blocca quando si utilizza l'azione <code>do-invoke-rest-endpoint</code> per effettuare una richiesta REST a un endpoint.
Identity Reporting	OCTCR56A580314	Durante la cancellazione del database di reporting su MS SQL, viene visualizzato il seguente messaggio di errore: <code>Incorrect syntax near the keyword 'CASCADE'</code> (Sintassi errata in prossimità della parola chiave "CASCADE").
	OCTCR56A581810	L'evento del processo Driver Health (ID evento: <code>query-driver-ident</code>) genera il seguente messaggio di avviso: <code>Recovered from unexpected condition: @cached-time no available</code> (Recupero da condizione imprevista: <code>@cached-time</code> non disponibile).
	OCTCR56A585188	Una richiesta REST API DELETE all'endpoint <code>/IDMDCS-CORE/rpt/collectors/{identifier}/trust</code> non rimuove il certificato attendibile dal campo <code>collect_cert</code> del record dell'agente di raccolta dati.
Applicazioni di Identity	OCTCR56A572998	Le funzionalità di convalida dei campi e di aggiornamento dei valori del generatore di moduli non funzionano in scenari asincroni.
	OCTCR56A573780	Sentinel Universal Collector non riesce ad analizzare il campo del messaggio nell'evento CEF: 3152C- User Message (Messaggio utente).
	OCTCR56A580840	I campi modulo basati sul componente Entità dinamica visualizzano parentesi quadre come valori di default nell'elenco a discesa.

Componente	ID globale	Descrizione
	OCTCR56A580876	La funzione <code>RoleVault.getRolesUserIn</code>, quando utilizzata per effettuare una chiamata API REST all'endpoint <code>/rest/access/assignments/role/list</code>, recupera solo dieci autorizzazioni di assegnazione del ruolo per un determinato utente. Dopo l'aggiornamento a Identity Manager 4.9, è possibile recuperare informazioni su tutti i ruoli aggiungendo l'attributo <code>true</code> alla medesima funzione. Sintassi: questa è la firma del metodo: <pre>RoleVault.getRolesUserIn('IDM','/rest/access/assignments/role/list',userDN,true)</pre>
	OCTCR56A581016	Dopo il passaggio da una visualizzazione all'altra del Generatore moduli, i campi del modulo scompaiono durante il salvataggio.
	OCTCR56A581716	La registrazione del Workflow Engine non funziona dopo l'aggiornamento a Identity Manager 4.8.4.
	OCTCR56A581762	Quando si esegue una query su un'origine Web esterna per i dati, il componente Seleziona include una stringa <code>_regex</code> aggiuntiva.
	OCTCR56A581978	Se si utilizza il componente Entità dinamica in un modulo a più schede, il nome visualizzato dell'utente selezionato cambia quando si torna alla scheda utilizzando il pulsante Indietro .
	OCTCR56A582360	Se i controlli di convalida su un campo del modulo dinamico danno esito negativo, un modulo JSON non visualizza un errore.
	OCTCR56A582959	La funzione <code>RoleVault.getRoleAssignmentCause</code>, quando utilizzata per effettuare una chiamata API REST all'endpoint <code>/rest/access/assignments/list/v2</code>, per default recupera la causa dell'assegnazione del ruolo solo per dieci ruoli. Dopo l'aggiornamento a Identity Manager 4.9, è possibile recuperare la causa dell'assegnazione per tutti i ruoli aggiungendo l'attributo <code>true</code> alla medesima funzione. Sintassi: questa è la firma del metodo: <pre>RoleVault.getRoleAssignmentCause('IDM','/rest/access/assignments/list/v2',identityDn,roleDn,true)</pre>
	OCTCR56A583294	Se si aggiunge un gruppo al campo Richiedenti , il tentativo di modificare un team esistente non riesce.
	OCTCR56A583369	La funzionalità Aggiorna in caso di non funziona se i campi dei moduli si trovano all'interno di un componente Griglia dei dati.
	OCTCR56A583373	Un campo Giorno non convalida correttamente i dati per le lingue diverse dall'inglese.
	OCTCR56A583421	L'aggiunta di un commento con una virgoletta singola (') nella funzione Valore predefinito personalizzato danneggia il modulo.

Componente	ID globale	Descrizione
	OCTCR56A583440	Quando si utilizza la funzione <code>setFieldValue()</code> per impostare un Valore predefinito personalizzato, l'esecuzione del processo di convalida prosegue all'infinito.
	OCTCR56A583441	Se un'autorizzazione richiesta viene mappata su una risorsa con accesso controllato, la pagina Cronologia richieste nel Dashboard visualizza un messaggio di errore.
	OCTCR56A583590	Identity Manager consente a qualsiasi utente autenticato di modificare la lingua preferita di un altro utente.
	OCTCR56A583609	La visualizzazione dello Stato richiesta nella pagina Cronologia indica "provisioning effettuato" anche dopo aver rifiutato il task.
	OCTCR56A583692	Durante la modifica del riquadro Ticket per help desk o di qualsiasi altra PRD e/o altro modulo allegato come riquadro sulla pagina Gestisci applicazioni, vengono visualizzati errori nei registri della console del browser.
	OCTCR56A583714	Quando si fa clic più volte sul pulsante Crea nella pagina Crea assegnazione delega, vengono create deleghe duplicate.
	OCTCR56A583722	Quando si esaminano i dettagli di una richiesta nella pagina Cronologia richieste, l'autore del log di attività e il commento corrispondente non sono separati da uno spazio.
	OCTCR56A583747	Quando si utilizza un metodo di azione del modulo <code>alert()</code> nel codice Javascript, l' Editor JS e il JSON modulo smettono di funzionare.
	OCTCR56A583754	Eventuali funzioni personalizzate salvate nell'Editor JS scompaiono se si modifica nuovamente il modulo nel Generatore moduli.
	OCTCR56A584217	Il modulo visualizzato nel dashboard di Identity Manager è diverso dal modulo visualizzato nella modalità anteprima del Generatore moduli.
	OCTCR56A584275	Un componente Seleziona con Abilita ricerca statica impostato su <code>true</code> non può effettuare ricerche di valori con lunghezza superiore a 50 caratteri. Il componente Seleziona ora ti consente di cercare valori con lunghezza fino a 1000 caratteri.
	OCTCR56A584283	Quando si definisce una logica per qualsiasi componente, non è possibile selezionare una proprietà per un'azione attivata da un evento.
	OCTCR56A584291	Quando la Posizione etichetta del componente Seleziona e Radio è impostata su <code>Sinistra</code> (allineamento a destra), le opzioni visualizzate non sono allineate correttamente.
	OCTCR56A584322	La funzione Valore predefinito personalizzato di un componente Casella di controllo non viene eseguita al caricamento iniziale del modulo, né quando attivata da una modifica o da un'esecuzione esplicita di <code>triggerChange()</code> .
	OCTCR56A584373	La pagina Task sul Dashboard non si aggiorna automaticamente. Anche dopo l'approvazione mediante il modulo di approvazione, un task resta comunque visualizzato nell'elenco.

Componente	ID globale	Descrizione
	OCTCR56A584374	La pagina Autorizzazioni sul Dashboard non elenca più le autorizzazioni con parentesi quadre o graffe nei risultati di ricerca.
	OCTCR56A584399	Gli attributi definiti Attributi modificabili nelle Impostazioni non sono modificabili nelle pagine Profilo personale e Utenti.
	OCTCR56A584489	Quando si richiede una PRD, la pagina Nuova richiesta visualizza i campi per inserire la Data di inizio validità e la Data di scadenza .
	OCTCR56A584625	Nei moduli localizzati mancano le etichette dei campi.
	OCTCR56A584638	Un componente Entità dinamica impostato con un limite di visualizzazione (il numero massimo di elementi da richiedere o visualizzare) non elenca tutte le entità corrispondenti nei risultati della ricerca.
	OCTCR56A584639	Dopo aver abilitato la modalità ONLINE e poi essere passati OFFLINE e tornati alla modalità ONLINE, il Generatore moduli non consente l'accesso con credenziali diverse dopo il primo login.
	OCTCR56A584666	L'opzione Container elenco utenti in Impostazioni > Personalizzazione non viene utilizzata per elencare gli utenti nella pagina Nuova richiesta per altri.
	OCTCR56A585183	La pagina Applicazioni nel Dashboard di Identity Manager visualizza le intestazioni delle categorie senza gli elementi consentiti al loro interno.
	OCTCR56A585185	In un componente Data/Ora impostato per visualizzare gli elementi del calendario e quelli dell'ora manca l'elemento di input dell'orario.
	OCTCR56A585231	Il numero di telefono inserito nell'attributo Numero di telefono nella pagina Profilo personale non può essere modificato o eliminato.
	OCTCR56A585264	Il Generatore moduli esegue la funzione Valore predefinito personalizzato ogni volta che un utente passa da una visualizzazione all'altra del Generatore moduli.
	OCTCR56A585443	La procedura per riassegnare i task ad altri membri del team non funziona nel modo indicato nella documentazione.
	OCTCR56A585477	L'attributo Firma nella pagina del profilo utente visualizza un valore di testo anziché l'immagine della firma.
	OCTCR56A585503	Il Generatore moduli non si carica correttamente quando viene avviato da Designer su un sistema Windows senza connessione Internet.
	OCTCR56A585527	Dopo l'upgrade a Identity Manager 4.8.7, il contatore delle autorizzazioni nella pagina Autorizzazione di altri non è posizionato correttamente nelle lingue supportate (con l'esclusione di inglese e portoghese).
	OCTCR56A585557	Il componente Visualizzazione DN del Generatore moduli mostra un messaggio di errore quando vengono impostate le condizioni.
	OCTCR56A585618	Impossibile accedere all'Applicazione utente e a SSPR dopo un upgrade. Il riavvio del servizio ndsd su eDirectory e Tomcat nel server Applicazioni di Identity risolve temporaneamente il problema, ma dopo un po' di tempo i componenti risultano nuovamente inaccessibili.

Componente	ID globale	Descrizione
	OCTCR56A585698	La pagina Profilo personale visualizza attributi errati quando Identity Manager è configurato per gestire più client.
	♦ OCTCR56A584920	La Vista scheda di un utente e gli attributi nella pagina Utenti del
	♦ OCTCR56A585772	Dashboard di Identity Manager visualizzano attributi diversi da quelli configurati nelle impostazioni di personalizzazione del client.

Installazione di NetIQ Identity Manager 4.9

Identity Manager 4.9 fornisce l'Advanced Edition e la Standard Edition in un unico file ISO. Prima di effettuare il download dei file di installazione, è necessario comprendere le funzionalità contenute in ciascuna edizione e le opzioni per il download dei componenti di Identity Manager.

- ♦ [“Funzionalità supportate con le edizioni Advanced e Standard di Identity Manager” a pagina 12](#)
- ♦ [“Download di Identity Manager” a pagina 13](#)
- ♦ [“Individuazione degli eseguibili e dei percorsi di installazione di default” a pagina 14](#)
- ♦ [“Installazione di NetIQ Identity Manager 4.9” a pagina 15](#)

Funzionalità supportate con le edizioni Advanced e Standard di Identity Manager

Per soddisfare le diverse esigenze dei clienti, le funzionalità di Identity Manager vengono fornite in due gruppi di prodotti:

- ♦ Identity Manager Advanced Edition
- ♦ Identity Manager Standard Edition

Le funzionalità di Identity Manager fornite con Identity Manager Standard Edition sono incluse anche in Identity Manager Advanced Edition, che offre funzionalità aggiuntive. Nella tabella seguente viene definito un confronto delle funzionalità disponibili nelle edizioni Advanced e Standard di Identity Manager:

Funzione	Advanced Edition	Standard Edition
Provisioning automatizzato degli utenti, basato su regole	Sì	Sì
Sincronizzazione dell'identità in tempo reale	Sì	Sì
Gestione password e self-service password	Sì	Sì
Strumento di informazione sull'identità uniforme (Analyzer)	Sì	Sì
Supporto single sign-on e API REST	Sì	Sì (supporto limitato)
Reportistica sullo stato attuale	Sì	Sì
Provisioning a livello aziendale, basato sui ruoli	Sì	No
Workflow di approvazione automatizzati per l'applicazione delle policy aziendali	Sì	No
Self-service avanzato nelle applicazioni di identità	Sì	No

Funzione	Advanced Edition	Standard Edition
Modello e catalogo delle risorse per semplificare il provisioning delle risorse	Sì	No
Reportistica cronologica sullo stato	Sì	No
Reportistica dei sistemi connessi	Sì	No
Amministrazione dei ruoli e delle risorse	Sì	No

Download di Identity Manager

Dopo l'acquisto di Identity Manager 4.9, accedere al portale [Software License and Download \(https://sld.microfocus.com/mysoftware/index\)](https://sld.microfocus.com/mysoftware/index) e seguire il collegamento che consente di effettuare il download del software. I seguenti file contengono i componenti di Identity Manager:

Nome del file	Descrizione
Identity_Manager_4.9_Linux.iso	Contiene il server di Identity Manager (Motore di Identity Manager, Remote Loader, Fanout Agent, Identity Console), le Applicazioni di Identity e il Reporting di Identity.
Identity_Manager_4.9_RL_Linux.iso	Contiene il Remote Loader di Identity Manager per Linux.
Identity_Manager_4.9_Containers.tar.gz	Contiene le immagini di container individuali per il Motore di Identity Manager, Remote Loader, Fanout Agent, ActiveMQ, PostgreSQL, Form Renderer, OSP, Applicazioni di Identity, Reporting di Identity, SSPR e Identity Console.
Identity_Manager_4.9_Windows.iso	Contiene il server di Identity Manager (Motore di Identity Manager, Remote Loader, Fanout Agent), le Applicazioni di Identity e il Reporting di Identity.
Identity_Manager_4.9_RL_Windows.iso	Contiene il Remote Loader a 64 bit e .NET per Windows.
Identity_Manager_4.9_Designer_Linux.tar.gz	Contiene Designer per piattaforme Linux.
Identity_Manager_4.9_Designer_Windows.zip	Contiene Designer per piattaforme Windows.
Identity_Manager_4.9_Designer_MacOSX.dmg	Contiene i file di Designer per macOS Sonoma.
SentinelLogManagementForIGA8.6.1.0.tar.gz	Contiene Sentinel Log Management per Identity Governance and Administration (IGA). Questa installazione è supportata solo su Linux.

Importante: lo strumento Analyzer non è incluso nell'immagine ISO per Identity Manager 4.9. Se Analyzer è già installato, accertarsi di aggiornarlo alla versione 4.8.5 e utilizzarlo con Identity Manager 4.9. Per l'installazione e l'upgrade di Analyzer, vedere [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) (Guida all'installazione e all'upgrade di NetIQ Identity Manager per Linux) o [NetIQ Identity Manager Install and Upgrade Guide for Windows](#) (Guida all'installazione e all'upgrade di NetIQ Identity Manager per Windows).

Individuazione degli eseguibili e dei percorsi di installazione di default

- ♦ [“Eseguibili e percorsi di installazione di default su Linux” a pagina 14](#)
- ♦ [“Eseguibili e percorsi di installazione di default su Windows” a pagina 15](#)

Eseguibili e percorsi di installazione di default su Linux

Componente di Identity Manager	Ubicazione dell'eseguibile all'interno dell'ISO	Percorso di installazione di default
Server di Identity Manager (contiene Motore di Identity Manager, Remote Loader, Fanout Agent e Identity Console)	<code>install.sh</code> nell'ubicazione montata	♦ Motore <code>/opt/novell/eDirectory/lib/dirxml</code> ♦ Remote Loader: <code>/opt/novell/dirxml/bin/x86_64</code> ♦ Fanout Agent: <code>/opt/novell/dirxml/fanoutagent</code> ♦ Identity Console: <code>/opt/novell/eDirAPI/sbin/</code>
Applicazioni di Identity (Dashboard e Interfaccia di amministrazione di Identity Manager, Applicazione utente, driver del Servizio ruoli e risorse, driver dell'Applicazione utente, utility di Aggiornamento della configurazione, One SSO Provider, Self Service Password Reset)	<code>install.sh</code> nell'ubicazione montata	♦ Applicazioni di Identity: <code>/opt/netiq/idm/apps</code> ♦ Applicazione utente: <code>/opt/netiq/idm/apps/UserApplication</code> ♦ Utility di Aggiornamento della configurazione: <code>/opt/netiq/idm/apps/configupdate</code> ♦ Form Renderer: <code>/opt/netiq/idm/apps/sites</code> ♦ NGINX: <code>/opt/netiq/common/nginx</code>
Designer per Identity Manager	<code>/designer/packages</code>	<code>/root/designer</code>
Identity Reporting	<code>install.sh</code> nell'ubicazione montata	<code>/opt/netiq/idm/apps/IDMReporting</code>
Componente della gestione password	<code>./install.sh</code> nella directory <code>sspr</code> dall'ubicazione montata	<code>/opt/netiq/idm/apps/sspr</code>
Sentinel Log Management per IGA	<code>./install.sh</code> nella directory <code>SentinelLogManagementforIGA</code> del file <code>SentinelLogManagementForIGA8.6.1.0.tar.gz</code>	<code>/opt/novell/sentinel</code>

Eseguibili e percorsi di installazione di default su Windows

Componente di Identity Manager	Ubicazione dell'eseguibile all'interno dell'ISO	Percorso di installazione di default
Server di Identity Manager (contiene Motore di Identity Manager, Remote Loader e Fanout Agent)	install.exe in \<ubicazione montata dell'ISO>\IdentityManagerServer\	♦ Motore C:\netiq\idm ♦ Remote Loader: C:\netiq\idm\RemoteLoader ♦ Fanout Agent: C:\netiq\idm\FanoutAgent
Applicazioni di Identity (Dashboard e Interfaccia di amministrazione di Identity Manager, Applicazione utente, driver del Servizio ruoli e risorse, driver dell'Applicazione utente, utility di Aggiornamento della configurazione, One SSO Provider, Self Service Password Reset)	install.exe in \<ubicazione montata dell'ISO>\IdentityApplications\	♦ Applicazioni di Identity: C:\netiq\idm\apps\ ♦ Applicazione utente: C:\netiq\idm\apps\UserApplication ♦ Utility di Aggiornamento della configurazione: C:\netiq\idm\apps\configupdate ♦ Form Renderer: C:\netiq\idm\apps\sites ♦ NGINX: C:\netiq\common\nginx
Designer per Identity Manager	install.exe nella cartella \designer_install\ del file Identity_Manager_4.8_Designer_Windows.zip	C:\netiq\
Identity Reporting	install.exe in \<ubicazione montata dell'ISO>\IdentityReporting\	C:\netiq\idm\apps\IdentityReporting
Componente della gestione password	install.exe in \<ubicazione montata dell'ISO>\common\sspr	C:\netiq\idm\apps\common\sspr

Installazione di NetIQ Identity Manager 4.9

A seconda della versione che si sta installando, rivedere le informazioni fornite da una delle seguenti risorse:

- ♦ Advanced Edition: [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) o [NetIQ Identity Manager Install and Upgrade Guide for Windows](#) (in lingua inglese)
- ♦ Standard Edition: [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.9 Standard Edition](#) (in lingua inglese)

Upgrade a NetIQ Identity Manager 4.9

È possibile eseguire direttamente l'upgrade a Identity Manager 4.9 dalle versioni Identity Manager 4.7.5 e 4.8.x (dove x è 0, 1, 2, 3, 4, 5, 6 e 7).

Prima di iniziare l'upgrade, rivedere le informazioni contenute nelle note di rilascio della versione corrente.

- ♦ [“Upgrade dalle versioni di Identity Manager 4.8.x” a pagina 16](#)
- ♦ [“Upgrade dalle versioni di Identity Manager 4.7.x” a pagina 18](#)
- ♦ [“Upgrade alla Advanced Edition” a pagina 19](#)
- ♦ [“Upgrade alla Standard Edition” a pagina 19](#)

Per ulteriori informazioni sull'upgrade di Identity Manager, vedere la sezione [“Upgrading Identity Manager”](#) in [NetIQ Identity Manager Install and Upgrade Guide for Linux](#) o la sezione [Upgrading Identity Manager](#) in [NetIQ Identity Manager Install and Upgrade Guide for Windows](#) (in lingua inglese).

Upgrade dalle versioni di Identity Manager 4.8.x

Nella tabella seguente sono elencati i percorsi di upgrade per ciascun componente per le versioni di Identity Manager 4.8.x:

Componente	Versione base	Versione dell'upgrade
Motore di Identity Manager	4.8.x	1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Effettuare l'upgrade di Identity Vault alla versione 9.2.9. 3. Effettuare l'upgrade del motore di Identity Manager alla versione 4.9.
Remote Loader/Fanout Agent	4.8.x	Upgrade a Remote Loader/Fanout Agent 4.9.
Designer		Installare Designer 4.9.

Componente	Versione base	Versione dell'upgrade
Applicazioni di Identity	4.8.x	Prima dell'upgrade delle applicazioni di Identity, assicurarsi di effettuare l'upgrade di Identity Vault e del motore di Identity Manager rispettivamente alla versione 9.2.9 e 4.9. 1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Arrestare Tomcat. 3. Effettuare l'upgrade del database a una versione supportata. Per le versioni del database supportate, consultare il sito Web delle informazioni tecniche di NetIQ Identity Manager. 4. (Condizionale) Se SSPR è installato su un server separato, effettuare l'upgrade del componente alla versione 4.9. 5. Aggiornare il driver dell'Applicazione utente e i pacchetti del driver di ruoli e risorse utilizzando Designer. 6. Upgrade delle Applicazioni di Identity alla versione 4.9 7. Avviare Tomcat.
Identity Reporting	4.8.x	Prima dell'upgrade del Reporting di Identity, assicurarsi di effettuare l'upgrade di Identity Vault, del motore di Identity Manager e delle Applicazioni di Identity rispettivamente alla versione 9.2.9, 4.9 e 4.9. 1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Effettuare l'upgrade del database a una versione supportata. Per ulteriori informazioni sulle versioni del database supportate, consultare il sito Web delle informazioni tecniche di NetIQ Identity Manager. 3. Effettuare l'upgrade di SLM per IGA a una versione supportata. 4. Aggiornare i pacchetti dei driver dei Servizi di raccolta dati e del Gateway servizi gestiti. 5. Effettuare l'upgrade del Reporting di Identity alla versione 7.2.0. 6. (Condizionale) Creare una policy di sincronizzazione dati dalla pagina Servizi di raccolta dati di Identity Manager. 7. Avviare Tomcat.

Prima di iniziare l'upgrade, rivedere le informazioni fornite dalle note di rilascio per la propria versione nella pagina della [documentazione NetIQ](https://www.netiq.com/documentation/identity-manager-49/) (<https://www.netiq.com/documentation/identity-manager-49/>).

Upgrade dalle versioni di Identity Manager 4.7.x

Nella tabella seguente sono elencati i percorsi di upgrade per ciascun componente per le versioni di Identity Manager 4.7.x:

Componente	Versione base	Versione dell'upgrade
Motore di Identity Manager	4.7.5	1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Effettuare l'upgrade di Identity Vault alla versione 9.2.9. 3. Effettuare l'upgrade del motore di Identity Manager alla versione 4.9.
Remote Loader/ Fanout Agent	4.7.5	Upgrade a Remote Loader/Fanout Agent 4.9.
Designer		Installare Designer 4.9.
Applicazioni di Identity	4.7.5	Prima dell'upgrade delle applicazioni di Identity, assicurarsi di effettuare l'upgrade di Identity Vault e del motore di Identity Manager rispettivamente alla versione 9.2.9 e 4.9. 1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Arrestare Tomcat. 3. Aggiornare il driver dell'Applicazione utente e i pacchetti del driver di ruoli e risorse. 4. Effettuare l'upgrade del database a una versione supportata. Per le versioni del database supportate, consultare il sito Web delle informazioni tecniche di NetIQ Identity Manager. 5. (Condizionale) Se SSPR è installato su un server separato, effettuare l'upgrade del componente alla versione 4.9. 6. Upgrade delle Applicazioni di Identity alla versione 4.9 7. Avviare Tomcat.

Componente	Versione base	Versione dell'upgrade
Identity Reporting	4.7.5	Prima dell'upgrade del Reporting di Identity, assicurarsi di effettuare l'upgrade di Identity Vault, del motore di Identity Manager e delle Applicazioni di Identity rispettivamente alla versione 9.2.9, 4.9 e 4.9. 1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Effettuare l'upgrade del database a una versione supportata. Per ulteriori informazioni sulle versioni del database supportate, consultare il sito Web delle informazioni tecniche di NetIQ Identity Manager. 3. Effettuare l'upgrade di SLM per IGA a una versione supportata. 4. Aggiornare i pacchetti dei driver dei Servizi di raccolta dati e del Gateway servizi gestiti. 5. Effettuare l'upgrade del Reporting di Identity alla versione 7.2.0. 6. Avviare Tomcat.

Prima di iniziare l'upgrade, rivedere le informazioni fornite dalle note di rilascio per la propria versione nella pagina della [documentazione NetIQ](https://www.netiq.com/documentation/identity-manager-49/) (<https://www.netiq.com/documentation/identity-manager-49/>).

Upgrade alla Advanced Edition

NetIQ fornisce i seguenti percorsi per l'upgrade a Identity Manager 4.9 Advanced Edition da una versione Advanced Edition o Standard Edition precedente:

- ♦ Da Identity Manager 4.8 Advanced Edition a 4.9 Advanced Edition
- ♦ Da Identity Manager 4.8 Standard Edition a 4.9 Advanced Edition, in uno dei seguenti modi:
 - ♦ Da Identity Manager 4.8 Standard Edition a 4.9 Standard Edition e successivamente a 4.9 Advanced Edition
 - ♦ Da Identity Manager 4.8 Standard Edition a 4.8 Advanced Edition e successivamente a 4.9 Advanced Edition
- ♦ Da Identity Manager 4.7.5 Advanced Edition a 4.9 Advanced Edition
- ♦ Da Identity Manager 4.7.5 Standard Edition a 4.9 Advanced Edition, in uno dei seguenti modi:
 - ♦ Da Identity Manager 4.7.5 Standard Edition a 4.9 Standard Edition e successivamente a 4.9 Advanced Edition
 - ♦ Da Identity Manager 4.7.5 Standard Edition a 4.7.5 Advanced Edition e successivamente a 4.9 Advanced Edition

Upgrade alla Standard Edition

È possibile effettuare l'upgrade a Identity Manager 4.9 Standard Edition da Identity Manager 4.8 Standard Edition. Per istruzioni sull'upgrade, vedere [Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.9 Standard Edition](#) (in lingua inglese).

Identity Manager 4.9 Standard Edition continua a fornire supporto per i seguenti rapporti:

- ♦ Autenticazione da parte dell'utente
- ♦ Autenticazione da parte del server

- ♦ Statistiche del database
- ♦ Modifiche della password personale
- ♦ Reimpostazioni delle password
- ♦ Rapporto associazioni driver Identity Vault, stato corrente
- ♦ Rapporto utenti Identity Vault, stato corrente
- ♦ Riepilogo eventi di modifica password utente

Per ulteriori informazioni, vedere [Administrator Guide to NetIQ Identity Reporting](#) (in lingua inglese).

Importante: per utilizzare i rapporti, importare le definizioni dei rapporti più recenti nel Reporting di Identity. Eseguire il login all'applicazione di Reporting e utilizzare la pagina **Download** all'interno dell'applicazione per effettuare il download dei rapporti.

Problemi noti

NetIQ si impegna affinché i propri prodotti forniscano soluzioni di qualità che soddisfino le esigenze software aziendali. I problemi elencati di seguito sono attualmente in fase di studio. Per ulteriore assistenza su un problema, rivolgersi al [supporto tecnico](#). Per l'elenco dei problemi noti in Designer, consultare le [Note di rilascio di Designer 4.9 per NetIQ Identity Manager](#).

- ♦ [“Il programma di installazione di Windows mostra un'eccezione” a pagina 20](#)
- ♦ [“Si verifica un errore durante l'accesso a Identity Manager in caso di utilizzo dell'autenticazione a due fattori” a pagina 21](#)
- ♦ [“Le proprietà di dirxml_remote e RLConsole mostrano la versione del prodotto obsoleta” a pagina 21](#)
- ♦ [“Il programma di installazione genera file SQL vuoti per lo schema del database” a pagina 21](#)
- ♦ [“Alcuni rapporti non recuperano dati durante l'utilizzo del database MS SQL” a pagina 22](#)
- ♦ [“Identity Manager non riflette le modifiche apportate all'opzione Utilizza SMTP TLS in Identity Console” a pagina 25](#)
- ♦ [“Su Linux, iManager visualizza una pagina vuota dopo l'upgrade” a pagina 25](#)
- ♦ [“Avvertenza: si è verificata un'operazione di accesso riflettente illegale” a pagina 26](#)
- ♦ [“Dopo l'upgrade di Identity Manager alla versione 4.9, Tomcat non si avvia su RHEL 8.x e 9.x” a pagina 26](#)
- ♦ [“Nella gerarchia delle relazioni mancano i pulsanti dell'organigramma per una relazione di livello 2 o superiore” a pagina 26](#)
- ♦ [“Dopo l'upgrade, Remote Loader segnala una password dell'oggetto driver non valida” a pagina 27](#)
- ♦ [“Si osserva l'errore: riconfigurazione di StatusLogger non riuscita nel file di log di Catalina” a pagina 27](#)
- ♦ [“Problemi relativi al Generatore moduli” a pagina 27](#)

Il programma di installazione di Windows mostra un'eccezione

Problema: l'avvio di Tomcat dopo aver installato i componenti di Identity Manager 4.9 mostra la seguente eccezione: SEVERE [main]

```
org.apache.catalina.util.LifecycleBase.handleSubClassException Failed to start component [Connector["ajp-nio-<IP_address>-8010"]]
```

Questo problema si verifica dopo una nuova installazione e dopo l'upgrade a Identity Manager 4.9.

[Problema: OCTCR56A607041]

Soluzione: non determina alcuna perdita di funzionalità. Tuttavia, per risolvere il problema, cancellare la seguente riga nel file `server.xml`:

```
<Connector port="8010" protocol="AJP/1.3" redirectPort="8543"/>
```

Il file `server.xml` si trova in `C:\NetIQ\idm\apps\tomcat\conf`

Si verifica un errore durante l'accesso a Identity Manager in caso di utilizzo dell'autenticazione a due fattori

Problema: gli utenti potrebbero riscontrare errori di login se NetIQ One SSO Provider (OSP) sul server Identity Manager è configurato con NetIQ Advanced Authentication per l'autenticazione a due fattori. Il file di log OSP visualizza il seguente errore: Unexpected error while searching:

```
internal.atlaslite.jcce.exception.CoreInitializationException: No administrator password is configured.
```

[Problema: OCTCR56A605248]

Soluzione: nessuna soluzione disponibile.

Le proprietà di `dirxml_remote` e `RLConsole` mostrano la versione del prodotto obsoleta

Problema: in caso di installazione o upgrade dell'oggetto Configurazione del caricatore remoto tramite `Identity_Manager_4.9_RL_Windows.iso` o `Identity_Manager_4.9_RL_Linux.iso`, è possibile notare che il valore di **Versione prodotto** non cambia nella finestra **Proprietà `dirxml_remote`**. Continua a mostrare **4.8.0.0**. Lo stesso problema si verifica nelle proprietà di **RLConsole**. [Problema: OCTCR56A608072]

Soluzione: non determina alcun impatto per la funzionalità dell'oggetto Configurazione del caricatore remoto. È possibile verificare il valore di **Versione file** nella stessa finestra per verificare l'installazione dell'oggetto Configurazione del caricatore remoto.

Il programma di installazione genera file SQL vuoti per lo schema del database

Problema: durante l'upgrade del componente Applicazioni di Identity, se si sceglie l'opzione di `scrittura su file` per la creazione dello schema del database, il programma di installazione crea i file `databaseschema.sql` e `wfedatabaseschema.sql` vuoti. In quanto tali, non è possibile utilizzarli per creare lo schema del database una volta completato l'upgrade. [Problema: OCTCR56A586043]

Soluzione: effettuare il download del file jar del database appropriato sul server per applicazioni o da un sito Web di terze parti per il database delle Applicazioni di Identity. Installarlo su un server o un sistema separato insieme alle Applicazioni di Identity.

Quando il programma di installazione richiede di immettere il percorso del **file jar JDBC del database per le Applicazioni di Identity e per il Motore del workflow** durante l'aggiornamento delle Applicazioni di Identity, specificare l'ubicazione del file jar del database installato.

Alcuni rapporti non recuperano dati durante l'utilizzo del database MS SQL

Problema: in caso di utilizzo di MS SQL come database di Identity Reporting, i rapporti **Richieste di accesso in base a destinatario**, **Richieste di accesso in base a richiedente** e **Richieste di accesso in base a risorsa** non restituiscono dati. [Problema: OCTCR56A604404]

Soluzione: per recuperare i dati per questi rapporti, eseguire i passaggi seguenti:

- 1 Eseguire il login al server in cui è installato Identity Reporting.
- 2 Aprire uno strumento per l'amministrazione dei database, ad esempio SQL Server Management Studio.
- 3 Eseguire l'interrogazione seguente:

Nota: specificare il nome del database Identity Reporting appropriato nel campo <nome database identity reporting>.

```
USE [<identity reporting database name>]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
DROP FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
GO

/***** Object: UserDefinedFunction [IDM_RPT_DATA].[get_formatted_user_dn]
Script Date: 5/9/2020 7:03:55 PM *****/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

CREATE FUNCTION [IDM_RPT_DATA].[get_formatted_user_dn]
(
    -- Add the parameters for the function here
    @user_path nvarchar(max)
    , @user_name nvarchar(200)
)
RETURNS nvarchar(max)
AS
BEGIN
    DECLARE
        @new_path          nvarchar(200),
        @new_path_2        nvarchar(max),
        @l_user_path        nvarchar(max),
        @l_old_delimiter    nvarchar(1) = '\\',
        @l_new_delimiter    nvarchar(1) = '.',
        @MyCursor CURSOR,
        @MyField nvarchar(max);

    if @user_path is not null
    BEGIN
        SET @l_user_path = SUBSTRING(@user_path , 2 , (LEN(@user_path)-1));
        SET @MyCursor = CURSOR FOR
            SELECT value FROM STRING_SPLIT( @l_user_path ,
```

```

@l_old_delimiter )
OPEN @MyCursor
FETCH NEXT FROM @MyCursor
INTO @MyField
WHILE @@FETCH_STATUS = 0
BEGIN
    if @MyField is not null
    BEGIN
        SET @new_path = @l_new_delimiter + @MyField;
    END
    if @new_path_2 is not null
    BEGIN
        SET @new_path = @new_path + @new_path_2;
    END
    SET @new_path_2 = @new_path;
    FETCH NEXT FROM @MyCursor
    INTO @MyField
END
CLOSE @MyCursor
DEALLOCATE @MyCursor

if @new_path is not null
BEGIN
    SET @new_path = @user_name + @new_path;
END
else
BEGIN
    SET @new_path = @user_name;
END
END
return LTRIM(RTRIM(@new_path));
END;

GO

CREATE FUNCTION [IDM_RPT_DATA].[patternReplace]
(
    @InputString VARCHAR(4000),
    @Pattern VARCHAR(100),
    @ReplaceText VARCHAR(4000)
)
RETURNS VARCHAR(4000)
AS
BEGIN
    DECLARE @Result VARCHAR(4000) SET @Result = ''
    -- First character in a match
    DECLARE @First INT
    -- Next character to start search on
    DECLARE @Next INT SET @Next = 1
    -- Length of the total string -- 8001 if @InputString is NULL
    DECLARE @Len INT SET @Len = COALESCE(LEN(@InputString), 8001)
    -- End of a pattern
    DECLARE @EndPattern INT

```

```

        WHILE (@Next <= @Len)
        BEGIN
            SET @First = PATINDEX('%' + @Pattern + '%', SUBSTRING(@InputString, @Next,
@Len))
            IF COALESCE(@First, 0) = 0 --no match - return
            BEGIN
                SET @Result = @Result +
                    CASE --return NULL, just like REPLACE, if inputs are NULL
                        WHEN @InputString IS NULL
                        OR @Pattern IS NULL
                        OR @ReplaceText IS NULL THEN NULL
                    ELSE SUBSTRING(@InputString, @Next, @Len)
                END
            BREAK
        END
    ELSE
    BEGIN
        -- Concatenate characters before the match to the result
        SET @Result = @Result + SUBSTRING(@InputString, @Next, @First - 1)
        SET @Next = @Next + @First - 1

        SET @EndPattern = 1
        -- Find start of end pattern range
        WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) = 0
            SET @EndPattern = @EndPattern + 1
        -- Find end of pattern range
        WHILE PATINDEX(@Pattern, SUBSTRING(@InputString, @Next, @EndPattern)) > 0
            AND @Len >= (@Next + @EndPattern - 1)
            SET @EndPattern = @EndPattern + 1

        --Either at the end of the pattern or @Next + @EndPattern = @Len
        SET @Result = @Result + @ReplaceText
        SET @Next = @Next + @EndPattern - 1
    END
    END
    RETURN(@Result)
END;

GO

```

- 4 Passare al sito Web di [CDN](#).
- 5 Fare clic sul rapporto **Richieste di accesso in base a destinatario**.
- 6 Effettuare il download dei file .rpz e .zip per il rapporto **Richieste di accesso in base a destinatario**.
- 7 Eseguire i passaggi [Passo 5](#) e [Passo 6](#) per i rapporti **Richieste di accesso in base a destinatario** e **Richieste di accesso in base a risorsa**.

Identity Manager non riflette le modifiche apportate all'opzione Utilizza SMTP TLS in Identity Console

Problema: se durante la configurazione di un server di posta elettronica in Identity Console si sceglie di abilitare o disabilitare l'attributo `notSMTPUseTLS` per il modello di notifica di default nella Vista ad albero, si può notare che lo stesso valore non viene visualizzato nella pagina Approvazione basata su e-mail in Identity Manager. Tuttavia, la selezione viene salvata e il server di posta elettronica viene aggiornato in base alle preferenze dell'utente.

Questo avviene perché l'attributo LDAP `notfSMTPUseTLS` viene aggiornato in modo diverso nelle Applicazioni di Identity e in Identity Console. Quando si effettua la modifica in Identity Console, l'attributo viene aggiornato direttamente. Invece, quando si modifica il valore **Utilizza SMTP TLS** nelle **Impostazioni e-mail in uscita** della pagina Approvazione basata su e-mail di Identity Manager, viene aggiornata la proprietà `com.netiq.rbpm.smtp.tls` nel file `ism-configuration.properties`. Tuttavia, viene comunque applicato il valore selezionato in Identity Console, anche se non compare nella pagina Approvazione basata su e-mail in Identity Manager. [Problema: OCTCR56A585739]

Soluzione: per garantire un comportamento coerente, è possibile modificare il valore **Utilizza SMTP TLS** nelle **Impostazioni e-mail in uscita** sulla pagina Approvazione basata su e-mail di Identity Manager in base al valore selezionato in Identity Console.

Su Linux, iManager visualizza una pagina vuota dopo l'upgrade

Problema: dopo l'upgrade di Identity Manager alla versione 4.9, iManager non funziona più se installato con altri componenti. Quando si tenta di avviare una versione precedentemente installata, iManager visualizza una pagina vuota.

Soluzione: installare e utilizzare Identity Console al posto di iManager. Tuttavia, per continuare a utilizzare iManager dopo aver effettuato l'upgrade di Identity Manager alla versione 4.9, assicurarsi che:

- ♦ iManager sia installato su un server autonomo.
- ♦ Il server disponga di una versione supportata di Java. Ad esempio, iManager 3.2.6.0200 su Java JDK 1.0.8 Update 342 in Identity Manager 4.8.6.

Attenersi alla seguente procedura per riutilizzare i precedenti file Java:

1. Crea una nuova directory utilizzando il seguente comando:

```
mkdir -p /opt/novell/iManager/java_iman
```

2. Copiare i file Java esistenti di iManager nella nuova directory:

```
cp -r /opt/netiq/common/jre/ /opt/novell/iManager/java_iman
```

3. Per modificare la proprietà della nuova directory, eseguire il seguente comando:

```
chown -R novlwww:novlwww /opt/novell/iManager/java_iman
```

4. Accedere a `/etc/opt/novell/tomcat9/` e aggiornare le variabili `JAVA_HOME` e `JRE_HOME` con il nuovo percorso Java nel file `tomcat9.conf`.

5. Riavviare Tomcat utilizzando il seguente commento:

```
rcnovell-tomcat9 restart
```

Avvertenza: si è verificata un'operazione di accesso riflettente illegale

Problema: durante la configurazione delle Applicazioni di Identity, è possibile che venga visualizzato il seguente messaggio:

Warning: An illegal reflective access operation has occurred

Il messaggio compare perché la versione corrente delle Applicazioni di Identity utilizza Java 11. [Problema: OCTCR56A583685]

Soluzione: l'avviso non influisce su alcuna funzionalità. È possibile ignorarlo.

Dopo l'upgrade di Identity Manager alla versione 4.9, Tomcat non si avvia su RHEL 8.x e 9.x

Problema: quando si effettua l'upgrade di Identity Manager alla versione 4.9 su un server che esegue RHEL 8.x o RHEL 9.x (dove x è la versione supportata in 4.9), OSP non si avvia a causa di un problema di connessione al database. Generalmente il problema si verifica quando il processo di generazione della chiave casuale richiede più tempo del previsto mentre l'OSP è in corso di distribuzione. Di conseguenza, anche i servizi Tomcat non si avviano. [Problema: OCTCR56A584564]

Soluzione: modificare le seguenti linee nel file `java.security` ubicato in `/opt/netiq/common/jre/conf/security` e riavviare Tomcat:

Nota: prima di implementare la soluzione, fare riferimento alla [documentazione di RHEL \(https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator\)](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator) per ulteriori informazioni sui generatori di numeri casuali.

- ♦ Sostituire `securerandom.source=file:/dev/random`
con
`securerandom.source=file:/dev/./urandom`
- ♦ Sostituire `securerandom.strongAlgorithms=NativePRNGBlocking:SUN`
con
`securerandom.strongAlgorithms=SHA1PRNG:SUN`

Nella gerarchia delle relazioni mancano i pulsanti dell'organigramma per una relazione di livello 2 o superiore

Problema: per una relazione di livello 2 o superiore, l'organigramma non mostra le opzioni che consentono di scegliere una relazione da visualizzare, passare al livello successivo nella gerarchia della relazione, inviare e-mail e visualizzare ulteriori informazioni su tale entità. Questo problema si verifica quando la profondità gerarchica nelle **Impostazioni generali** è impostata a livello 2 (o superiore). [Problema: OCTCR56A585426]

Soluzione: per visualizzare i pulsanti dell'organigramma per la relazione di livello 2 (o superiore), cercare l'utente/l'entità di livello 2 nell'organigramma.

Dopo l'upgrade, Remote Loader segnala una password dell'oggetto driver non valida

Problema: dopo l'upgrade alla versione 4.9 su piattaforma Windows, Remote Loader non è in grado di eseguire la connessione al driver Active Directory utilizzando la password di autenticazione di base.

[Problema: OCTCR56A584022]

Soluzione: dopo l'upgrade di Identity Manager alla versione 4.9, attenersi alla seguente procedura:

- 1 Arrestare l'istanza di Remote Loader sul server di Remote Loader.
- 2 Reimpostare la password dell'oggetto driver e la password di Remote Loader.
- 3 Avviare l'istanza di Remote Loader per il driver Active Directory.

Si osserva l'errore: riconfigurazione di StatusLogger non riuscita nel file di log di Catalina

Problema: dopo aver installato Identity Manager 4.9 su una piattaforma Windows, è possibile che venga visualizzato il seguente messaggio di errore nei log catalina.out:

```
ERROR StatusLogger Reconfiguration failed: No configuration found for '<xxxxxxx>'
at 'null' in 'null'
```

[Problema: OCTCR56A584800]

Soluzione: l'errore non influisce su alcuna funzionalità. È possibile ignorarlo.

Problemi relativi al Generatore moduli

Si potrebbero riscontrare i seguenti problemi in caso di utilizzo di moduli JSON nel Generatore moduli.

- ♦ [“I messaggi di convalida dei campi non veicolano il messaggio in modo chiaro” a pagina 27](#)
- ♦ [“Il campo di un modulo visualizza un errore di convalida non array dopo l'upgrade di Designer alla versione 4.9” a pagina 28](#)
- ♦ [“Il generatore moduli si blocca durante lo scorrimento” a pagina 28](#)
- ♦ [“L'azione Pulsante non funziona” a pagina 29](#)
- ♦ [“Problemi relativi al componente Albero” a pagina 29](#)

I messaggi di convalida dei campi non veicolano il messaggio in modo chiaro

Problema: i messaggi di convalida dei campi dei moduli inviano una notifica agli utenti quando immettono un valore non valido o non accettabile in un campo. Questi messaggi sono in genere costituiti da una coppia chiave-valore, con il valore visualizzabile per l'utente. Tuttavia, in questa versione, i campi dei moduli mostrano le chiavi, anziché i valori corrispondenti. Ad esempio, l'immissione di un indirizzo e-mail non valido mostra `invalid_email` anziché `Email must be a valid email`.

[Problema: OCTCR56A598009]

Soluzione: per aggiungere i messaggi per la lingua inglese:

1. Avviare il Generatore moduli.

2. Fare clic sull'icona  Localizzazione.
3. Fare clic su **Inglese** per espandere la visualizzazione.
4. Aggiungere una virgola finale e le coppie chiave-valore per i messaggi fino all'ultima riga.

Ad esempio:

```
{
  "Submit": "",
  "error": "Please fix the following errors before submitting.",
  "invalid_date": "{{field}} is not a valid date.",
  "invalid_email": "{{field}} must be a valid email.",
  "invalid_regex": "{{field}} does not match the pattern {{regex}}.",
  "mask": "{{field}} does not match the mask.",
  "max": "{{field}} cannot be greater than {{max}}.",
  "maxLength": "{{field}} must be shorter than {{length}} characters.",
  "min": "{{field}} cannot be less than {{min}}.",
  "minLength": "{{field}} must be longer than {{length}} characters.",
  "next": "Next",
  "pattern": "{{field}} does not match the pattern {{pattern}}",
  "previous": "Previous",
  "required": "{{field}} is required"
}
```

5. Fare clic su **Salva**.

Il campo di un modulo visualizza un errore di convalida non array dopo l'upgrade di Designer alla versione 4.9

Problema: se il campo di un modulo a valore singolo contiene più valori, il Generatore moduli ora visualizza un errore di convalida non array. Questo controllo di convalida è stato aggiunto nell'ultima versione del Generatore moduli. Pertanto, quando si effettua l'upgrade di Designer alla versione 4.9, si verifica questo problema nei moduli esistenti. [Problema: OCTCR56A586045]

Soluzione: per correggere l'errore, eseguire una delle seguenti azioni:

- ♦ Aprire il modulo nel Generatore moduli e selezionare la casella di controllo **Valori multipli** nel campo del modulo interessato. Al campo verrà aggiunto un pulsante **Aggiungi un altro**, che consente agli utenti di immettere altri valori.
- ♦ Modificare la funzione Valore predefinito personalizzato nel campo interessato per visualizzare solo il primo valore restituito in un array, anche se l'array contiene un singolo valore.

Il generatore moduli si blocca durante lo scorrimento

Problema: il Generatore moduli si blocca occasionalmente durante lo scorrimenti nei moduli JSON in corrispondenza delle viste **Modulo JSON** ed **Editor JS**. Questo problema si verifica in due scenari:

- ♦ Durante l'utilizzo di un modulo JSON contenente molti metodi e funzioni.
- ♦ Quando la risoluzione dello schermo differisce dal valore consigliato dal sistema.

[Problema: OCTCR56A602415]

Soluzione: nessuna soluzione disponibile. È possibile riavviare il Generatore moduli.

L'azione Pulsante non funziona

Problema: dopo l'upgrade a Designer 4.9, il componente Pulsante nei moduli JSON non funziona per le azioni di approvazione e richiesta. [Problema: OCTCR56A604329]

Soluzione: eseguire i passaggi seguenti:

- 1 Passare alla scheda **Visualizza** del componente Pulsante.
- 2 Copiare la logica specificata nei campi **Logica richiesta pulsante** o **Logica approvazione pulsante**.
- 3 Modificare **Azione** in **personalizzata**.
- 4 Specificare la logica copiata dal **Passo 2**.
- 5 Fare clic su **Salva**.

Problemi relativi al componente Albero

Si potrebbero riscontrare i seguenti problemi con il componente Albero nel Generatore moduli:

- ♦ I campi mostrano un errore di convalida non array nel modulo **Anteprima**. Questo errore si verifica quando il componente Albero è impostato per visualizzare un valore predefinito. Non è possibile inviare il modulo finché non si risolve l'errore di convalida. [Problema: OCTCR56A585664]

Per risolvere l'errore, modificare il valore predefinito con l'ID di tale campo nella vista **Modulo JSON**.

- ♦ La funzionalità di espansione di un componente Albero non funziona come previsto. Il modulo **Anteprima** non consente di espandere o selezionare un container secondario.
- ♦ Quando si seleziona un container o un container secondario, il campo mostra il valore **dn**, anziché **name**.

Il seguente **JSON non elaborato di origine dati** contiene dati di esempio del componente Albero:

```

{
  "dn": "unique id",
  "name": "container data",
  "data": "any meta-data attached with the container",
  "subContainers": [
    {
      "dn": "id1",
      "name": "container data1",
      "icon": "glyphicon glyphicon-cloud"
    },
    {
      "dn": "id2",
      "name": "container data2",
      "data": "any meta-data attached with the container",
      "subContainers": [
        {
          "dn": "id3",
          "name": "container data3",
          "icon": "glyphicon glyphicon-cloud"
        }
      ]
    }
  ]
}

```

Quando si seleziona l'opzione **container data** in **Anteprima**, il campo mostra `unique id`, anziché `container data`. [Problema: OCTCR56A603396]

Contatti di Micro Focus

Per problemi specifici del prodotto, visitare la pagina di assistenza di Micro Focus all'indirizzo <https://www.microfocus.com/it-it/support>.

Ulteriori informazioni tecniche o suggerimenti sono disponibili da diverse origini:

- ♦ Documentazione del prodotto, articoli della knowledge base e video: <https://www.microfocus.com/it-it/support>
- ♦ Pagine della Comunità Micro Focus: <https://www.microfocus.com/communities/>

Note legali

Copyright 2009-2024 Open Text.

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

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