

Note di rilascio di OpenText™ Identity Manager CE 24.4 (v4.10)

Gennaio 2025

OpenText Identity Manager 24.4 (v4.10) include 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](https://community.opentext.com/cyberres/iga/idm) (<https://community.opentext.com/cyberres/iga/idm>) di OpenText, 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 OpenText Identity Manager](https://www.netiq.com/documentation/identity-manager-4.10/) (<https://www.netiq.com/documentation/identity-manager-4.10/>).

Per ulteriori informazioni relative a questa versione e le note sulla versione più recenti, visitare la pagina della [Documentazione](https://www.netiq.com/documentation/identity-manager-4.10/) (<https://www.netiq.com/documentation/identity-manager-4.10/>).

Per effettuare il download di questo prodotto, fare riferimento al portale [Software License and Download](https://sld.microfocus.com) (<https://sld.microfocus.com>).

- ♦ "Novità" a pagina 2
- ♦ "Funzionalità non più supportate" a pagina 3
- ♦ "Versioni supportate dei componenti" a pagina 3
- ♦ "Requisiti di sistema" a pagina 5
- ♦ "Problemi risolti" a pagina 5
- ♦ "Installazione di OpenText Identity Manager 24.4 (v4.10)" a pagina 7
- ♦ "Upgrade a OpenText Identity Manager 24.4 (v4.10)" a pagina 10
- ♦ "Problemi noti" a pagina 13
- ♦ "Contatto di OpenText" a pagina 21
- ♦ "Note legali" a pagina 22

Novità

In questa versione sono inclusi i seguenti miglioramenti a

- ♦ [“Supporto ai sistemi operativi”](#) a pagina 2
- ♦ [“Aggiornamenti del branding”](#) a pagina 2
- ♦ [“Supporto per OpenSSL 3.0.15 con TLSv1.3”](#) a pagina 2
- ♦ [“Miglioramenti del programma di installazione”](#) a pagina 2
- ♦ [“Miglioramenti di Identity Applications: visualizzazione della cronologia dei task”](#) a pagina 3

Per ulteriori informazioni sulle nuove funzioni di OpenText Identity Manager 24.4 (v4.10), vedere le [Note di rilascio di OpenText™ Identity Manager CE 24.4 \(v4.10\) Designer](#).

Supporto ai sistemi operativi

In questa versione è stato aggiunto il supporto per la piattaforma Red Hat Enterprise Linux (RHEL) 9.4. Per un elenco completo dei sistemi operativi supportati, vedere la pagina relativa ai [Requisiti di sistema per OpenText™ Identity Manager CE 24.4 \(v4.10\)](#).

Per informazioni sui componenti inclusi nel pacchetto, sui database e sui browser supportati con questa versione, vedere [“Versioni supportate dei componenti”](#) a pagina 3.

Aggiornamenti del branding

Micro Focus fa ora parte di OpenText. Per aderire al marchio OpenText, vengono aggiornati il nome del prodotto, i relativi componenti e l'interfaccia utente, i loghi, i riferimenti ai nomi aziendali e la documentazione. Il meccanismo delle versioni di OpenText utilizza il formato CY.Q (Anno solare.Trimestre). A partire dalla versione 4.10, Identity Manager è conforme alla convenzione delle versioni di OpenText. Identity Manager 4.10 è noto come OpenText Identity Manager 24.4 (v4.10).

Supporto per OpenSSL 3.0.15 con TLSv1.3

A partire da questa versione, OpenText Identity Manager utilizza OpenSSL 3.0.15. Quando si installa il prodotto, viene implementata la nuova versione di OpenSSL e viene utilizzato TLSv1.3 per la comunicazione tra i suoi componenti.

Se si esegue l'upgrade dalla versione 4.7.5, 4.8.x o 4.9.x alla versione 24.4 (v4.10), il supporto per TLSv1.2 rimarrà disponibile. Per abilitare TLSv1.3, è necessario configurare manualmente TLSv1.3 per tutti i componenti. Per ulteriori informazioni, vedere [Configuring TLSv1.3 for Tomcat Services](#) (Configurazione di TLSv1.3 per i servizi Tomcat).

Importante: La versione TLS specificata nel file `server.xml` di Tomcat sostituisce la versione TLS impostata nei componenti.

Miglioramenti del programma di installazione

Questa versione include i seguenti miglioramenti al programma di installazione:

- ♦ Viene visualizzato un nuovo prompt per la password dell'archivio chiavi master durante la configurazione e l'upgrade di Identity Applications e di Identity Reporting.

- ♦ Prompt automatizzati per la configurazione tipica di OpenText Identity Console.
- ♦ Aggiunta del driver SAP HANA nei prodotti driver finali di OpenText Identity Manager 24.4 (v4.10).

Miglioramenti di Identity Applications: visualizzazione della cronologia dei task

Ora gli utenti possono visualizzare lo stato di tutte le azioni precedenti in un'unica posizione. L'opzione **Cronologia task** del menu **Task** elenca tutti i task eseguiti da un utente, incluse le richieste di autorizzazione approvate o rifiutate. Questa funzione tiene traccia delle esecuzioni dei workflow degli utenti e semplifica la revisione delle azioni passate. Gli utenti con ruoli appropriati, come l'Amministratore di provisioning, possono anche visualizzare la cronologia dei task di altri utenti. Per ulteriori informazioni, fare clic sull'icona della guida sul Dashboard.

Nota: In questa versione, l'aggiunta di un nuovo widget al Dashboard non include l'opzione **Cronologia task** nella categoria **IDM**.

Funzionalità non più supportate

Le seguenti funzioni sono state rimosse o non sono più supportate e verranno rimosse in una versione futura:

La configurazione di OSP per l'utilizzo di Advanced Authentication per l'autenticazione a due fattori non è più supportata

A partire da questa versione, la configurazione di OSP per l'utilizzo di Advanced Authentication per l'autenticazione a due fattori non è più supportata. È invece possibile utilizzare l'autenticazione SAML di Advanced Authentication. Advanced Authentication fornisce inoltre molti altri metodi di autenticazione, quali Card (Scheda), OATH OTP e riconoscimento facciale durante il processo di login.

La definizione dell'indirizzo IP per il nome host non è più supportata

Quando si configura il nome host per i componenti di OpenText Identity Manager, utilizzare il nome di dominio completo (FQDN) del server. Prima di questa versione, erano consentiti sia l'indirizzo IP che l'FQDN, ma da questa versione in avanti sono supportati solo i nomi di dominio completi. Questa modifica non ha alcun impatto su Identity Reporting, che continua ad accettare l'indirizzo IP o l'FQDN per la configurazione.

Versioni supportate dei componenti

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

- ♦ [“Versioni dei componenti di OpenText Identity Manager” a pagina 3](#)
- ♦ [“Versioni dei componenti di terze parti” a pagina 4](#)
- ♦ [“Database” a pagina 4](#)
- ♦ [“Browser Web” a pagina 4](#)

Versioni dei componenti di OpenText Identity Manager

Questa versione supporta i seguenti componenti:

- ♦ OpenText™ eDirectory 24.4 (v9.3)

- ♦ OpenText™ Identity Console 24.4 (v1.9)
- ♦ Identity Manager Engine 4.10
- ♦ Identity Manager Remote Loader 4.10
- ♦ Identity Manager Fanout Agent 4.10
- ♦ Designer per OpenText™ Identity Manager 24.4 (v4.10)
- ♦ Identity Applications 24.4 (v4.10)
- ♦ One SSO Provider (OSP) 6.7.7
- ♦ Self Service Password Reset (SSPR) 4.8.0.1
- ♦ Identity Manager Identity Reporting 24.4 (v7.4)
- ♦ Sentinel Log Management for IGA 8.7.0.0 (per il controllo degli eventi)
- ♦ Driver di OpenText™ Identity Manager

Nota:

- ♦ OpenText Identity Manager 24.4 (v4.10) è compatibile solo con OpenText™ eDirectory™ 24.4 (v9.3) o versioni successive.
 - ♦ OpenText Identity Manager 24.4 (v4.10) contiene le versioni più recenti dei driver supportati. Per ulteriori informazioni, vedere la sezione **Version Shipped with 24.4 (v4.10)** (Versione fornita con 24.4 (v4.10)) nella pagina [OpenText Identity Manager Drivers \(https://www.netiq.com/documentation/identity-manager-4.10-drivers/\)](https://www.netiq.com/documentation/identity-manager-4.10-drivers/) (Driver di OpenText Identity Manager).
-

Versioni dei componenti di terze parti

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

- ♦ Zulu 11.76+21-CA
- ♦ Apache Tomcat 9.0.96
- ♦ PostgreSQL 14.14 (standalone e container)
- ♦ OpenSSL 3.0.15
- ♦ Nginx 1.24.0-1
- ♦ ActiveMQ 5.18.4

Database

Tutti i componenti del prodotto, incluso Identity Applications, sono compatibili con Oracle 21c. Tuttavia, Identity Reporting 24.4 (v7.4) continua a supportare Oracle 19c e 18c.

Browser Web

Almeno uno dei seguenti browser:

- ♦ Google Chrome 131.0.6778.85/86
- ♦ Mozilla Firefox 132.0.2
- ♦ Apple Safari 17.4.1
- ♦ Microsoft Edge 131.0.2903.63

Requisiti di sistema

Per informazioni sui requisiti hardware e sui sistemi operativi supportati, vedere la pagina [System Requirements for OpenText™ Identity Manager CE 24.4 \(v4.10\)](#) (in lingua inglese).

Problemi risolti

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

Componente	ID globale	Descrizione
Identity Applications	OCTCR56A582892	Il driver del Servizio ruoli e risorse non elabora in modo coerente gruppi, ruoli o risorse.
	OCTCR56A583444	Quando si cercano ruoli, la combinazione di più criteri di ricerca produce risultati irrilevanti.
	OCTCR56A583741	Quando si crea un'autorizzazione account utente in Active Directory, nel dashboard non viene visualizzato il valore dell'autorizzazione AD anche quando si utilizza l'asterisco (*) come carattere jolly per la ricerca.
	OCTCR56A583753	L'opzione Modifica dashboard in Impostazioni di accesso non funziona correttamente. Anche quando un utente o un ruolo specifico è specificato come trustee per la modifica del dashboard, l'opzione Modifica dashboard personale rimane disponibile per tutti gli utenti.
	OCTCR56A583970	Gli utenti con il ruolo di manager di provisioning non possono visualizzare l'opzione Altri in Accesso > Autorizzazioni sul dashboard.
	OCTCR56A584665	La proprietà Enable oidpInstanceData attribute clean-up del driver dell'applicazione utente ha esito negativo. Di conseguenza, quando l'attributo oidpInstanceData raggiunge il limite, gli utenti non possono eseguire il login.
	OCTCR56A584708	Se l'impostazione Enable multi-threaded Role and Resource driver (Abilita driver ruoli e risorse multithread è impostata su <code>true</code> , il driver del Servizio ruoli e risorse interrompe la traccia del proprio log e registra tutto il contenuto del file <code>driverset.log</code> ubicato in <code>/var/log/idm/driverset.log</code> .
	OCTCR56A584712	L'opzione Stato sincronizzazione password non viene visualizzata nella pagina Utenti, anche se un utente, un gruppo, un ruolo o un container è designato come trustee per la visualizzazione di tale opzione nella pagina Impostazioni di accesso.
	OCTCR56A584753	La modifica di un attributo booleano per un'entità utente nella pagina Profilo personale non viene salvata correttamente.
	OCTCR56A584827	Se un workflow con una struttura di dati del flusso nidificata contiene molti spazi, l'applicazione non li ignora e li stampa nella sezione relativa ai commenti del workflow.
	OCTCR56A584956	L'attributo <code>nrFallbackOverride</code> non funziona correttamente. Quando una risorsa che richiede l'approvazione viene mappata a un ruolo e un utente richiede tale ruolo, la risorsa viene assegnata senza attivare il processo di approvazione.

Componente	ID globale	Descrizione
	OCTCR56A585003	Il numero di membri per Assegnazioni ruoli e Assegnazioni risorse visualizza valori errati quando supera il limite massimo di visualizzazione impostato nella proprietà.
	OCTCR56A585485	Quando un ruolo viene revocato, il driver del Servizio ruoli e risorse ricalcola i ruoli per tutti gli utenti di un container, compresi quelli ereditati, causando problemi di prestazioni. Nota: Affinché le prestazioni di RRSD non siano influenzate dalla revoca di un ruolo, creare una policy di trasformazione evento personalizzata e impostare l'attributo skip-processing su true. Le operazioni di ricalcolo verranno disabilitate durante la revoca o l'assegnazione di un ruolo. Tuttavia, se si ignorano i ricalcoli, è possibile che il ruolo non venga revocato completamente, lasciando lo stato "in esecuzione." Assicurarsi di impostare nuovamente skip-processing su false dopo la revoca.
	OCTCR56A585680	Gli attributi a valore singolo per un'entità utente non sono modificabili, anche se impostati come Attributi modificabili nelle Impostazioni di personalizzazione .
	OCTCR56A587004	Nella pagina Autorizzazioni di altri , la Data di scadenza non viene visualizzata nella finestra dei dettagli del ruolo.
	OCTCR56A627092	Identity Manager non è in grado di inviare e-mail quando le policy includono l'azione <do-send-email-from-template> o <do-send-email> con la notifica del cliente impostata su HTML nel campo del messaggio all'interno dei tag <use-html>.
	OCTCR56A627201	Gli eventi di revisione provenienti da Identity Applications non possono essere inviati a Sentinel a causa di un problema di connessione.
	OCTCR56A639081	L'attributo DirXML-PasswordSyncStatus di un utente cambia da 0004: SUCCESS a 0005: PENDING quando gli utenti vengono aggiunti in massa a eDirectory.
	OCTCR56A646136	Il Generatore moduli non funziona in assenza di accesso a Internet.
	OCTCR56A647072	Gli attributi a valore singolo per le entità personalizzate non sono modificabili.
Installazione e upgrade	OCTCR56A674108	I container di Identity Manager 4.9 non gestiscono correttamente i fusi orari, con conseguente visualizzazione della registrazione orario di log e tracce in formato UTC anziché locale.

Installazione di OpenText Identity Manager 24.4 (v4.10)

Questa versione include 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 disponibili in ciascuna edizione e le opzioni per il download dei componenti del prodotto. Per informazioni sulle funzioni contenute e supportate da ciascuna edizione, vedere [OpenText™ Identity Manager CE 24.4 \(v4.10\) Overview and Planning Guide](#) (in lingua inglese).

- ♦ “Download di OpenText Identity Manager” a pagina 7
- ♦ “Individuazione degli eseguibili e dei percorsi di installazione di default” a pagina 8
- ♦ “Installazione del prodotto” a pagina 10

Download di OpenText Identity Manager

Dopo l'acquisto di OpenText Identity Manager 24.4(v4.10), 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 OpenText Identity Manager:

Nome del file	Descrizione
Identity_Manager_4.10.0_Linux.iso	Contiene il server di Identity Manager (Identity Manager Engine, Remote Loader, Fan-out Agent, OpenText Identity Console), Identity Applications e Identity Reporting.
Identity_Manager_4.10.0_RL_Linux.iso	Contiene il Remote Loader di Identity Manager per Linux.
Identity_Manager_4.10.0_Containers.tar.gz	Contiene le immagini di container individuali per Identity Manager Engine, Remote Loader, Fanout Agent, ActiveMQ, PostgreSQL, Form Renderer, OSP, Identity Applications, Identity Reporting, SSPR e OpenText Identity Console.
Identity_Manager_4.10.0_Windows.iso	Contiene il server di Identity Manager (Identity Manager Engine, Remote Loader, Fan-Out Agent e Identity Console), Identity Applications e Identity Reporting.
Identity_Manager_4.10.0_RL_Windows.iso	Contiene il Remote Loader a 64 bit e .NET per Windows.
Identity_Manager_4.10.0_Designer_Linux.tar.gz	Contiene Designer per piattaforme Linux.
Identity_Manager_4.10.0_Designer_Windows.zip	Contiene Designer per piattaforme Windows.
Identity_Manager_4.10.0_Designer_MacOSX.dmg	Contiene i file di Designer per macOS Sonoma.
SentinelLogManagementForIGA8.7.0.0.tar.gz	Contiene Sentinel Log Management per Identity Governance and Administration (IGA). Questa installazione è supportata solo su Linux.
acdi_v24.4.zip	Contiene Audit, Compliance & Data Intelligence (include il driver ACDI, i pacchetti ACDI Monitor e il pacchetto ACDI Workflow Monitor).

Nome del file	Descrizione
Importante:	
♦ Il prodotto non compila più la versione a 32 bit di Remote Loader ed è disponibile con le versioni .NET e a 64 bit. ♦ Lo strumento Analyzer non è incluso nel programma di installazione. Se Analyzer è già installato, assicurarsi di aggiornarlo alla versione 4.8.5 e utilizzarlo con OpenText Identity Manager 24.4 (v4.10). Per l'installazione e l'upgrade di Analyzer, vedere OpenText™ Identity Manager CE 24.4 (v4.10) Install and Upgrade Guide for Linux o OpenText™ Identity Manager CE 24.4 (v4.10) Install and Upgrade Guide for Windows (in lingua inglese).	

Individuazione degli eseguibili e dei percorsi di installazione di default

- ♦ [“Eseguibili e percorsi di installazione di default su Linux”](#) a pagina 8
- ♦ [“Eseguibili e percorsi di installazione di default su Windows”](#) a pagina 9

Eseguibili e percorsi di installazione di default su Linux

Componente di OpenText 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 OpenText Identity Console)	install.sh nell'ubicazione montata	♦ Motore /opt/novell/eDirectory/lib/dirxml ♦ Remote Loader: /opt/novell/dirxml/bin/x86_64 ♦ Fanout Agent: /opt/novell/dirxml/fanoutagent ♦ OpenText Identity Console: /opt/novell/eDirAPI/sbin/
Identity Applications (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.sh nell'ubicazione montata	♦ Identity Applications: /opt/netiq/idm/apps ♦ Applicazione utente: /opt/netiq/idm/apps/UserApplication ♦ Utility di Aggiornamento della configurazione: /opt/netiq/idm/apps/configupdate ♦ Form Renderer: /opt/netiq/idm/apps/sites ♦ NGINX: /opt/netiq/common/nginx
Designer per OpenText Identity Manager	/designer/packages	/root/designer
Identity Reporting	install.sh nell'ubicazione montata	/opt/netiq/idm/apps/IDMReporting
Componente della gestione password	./install.sh nella directory /sspr dall'ubicazione montata	/opt/netiq/idm/apps/sspr

Componente di OpenText Identity Manager	Ubicazione dell'eseguibile all'interno dell'ISO	Percorso di installazione di default
Sentinel Log Management per IGA	./install.sh nella directory / SentinelLogManagementForIGA del file SentinelLogManagementForIGA8.7.0.0.tar.gz	/opt/novell/sentinel

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 Identity Manager Engine, Remote Loader, Fan-Out Agent, OpenText Identity Console)	install.exe in \<ubicazione montata dell'ISO>\IdentityManagerServer\	♦ Motore C:\netiq\idm ♦ Remote Loader: C:\netiq\idm\RemoteLoader ♦ Fanout Agent: C:\netiq\idm\FanoutAgent
Identity Applications (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\	♦ Identity Applications: 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 OpenText Identity Manager	install.exe nella cartella \designer_install\ del file Identity_Manager_4.10.0_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 del prodotto

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

- ♦ Advanced Edition: [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Linux](#) o [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Windows](#) (in lingua inglese)
- ♦ Standard Edition: [Quick Start Guide for Installing and Upgrading OpenText™ Identity Manager CE 24.4 \(v4.10\) Standard Edition](#) (in lingua inglese)

Upgrade a OpenText Identity Manager 24.4 (v4.10)

È possibile eseguire direttamente l'upgrade a OpenText Identity Manager 24.4 (v4.10) dalle versioni Identity Manager 4.7.5, 4.8.x (dove x è 0, 1, 2, 3, 4, 5, 6 e 7) e 4.9.

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

- ♦ [“Upgrade dalle versioni 4.9.x, 4.8.x e 4.7.5 di Identity Manager” a pagina 10](#)
- ♦ [“Upgrade alla Advanced Edition” a pagina 12](#)
- ♦ [“Upgrade alla Standard Edition” a pagina 12](#)

Per ulteriori informazioni sull'upgrade di OpenText Identity Manager, vedere la sezione [“Upgrading OpenText Identity Manager”](#) in [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Linux](#) o la sezione [Upgrading OpenText Identity Manager](#) in [OpenText™ Identity Manager CE 24.4 \(v4.10\) Install and Upgrade Guide for Windows](#) (in lingua inglese).

Upgrade dalle versioni 4.9.x, 4.8.x e 4.7.5 di Identity Manager

Nella tabella seguente sono elencati i percorsi di upgrade per ciascun componente per le versioni di Identity Manager 4.9.x, 4.8.x e 4.7.5:

Componente	Versione base	Versione dell'upgrade
Identity Manager Engine	4.9.x, 4.8.x, 4.7.5	1. Effettuare l'upgrade del sistema operativo a una versione supportata. 2. Effettuare l'upgrade di Identity Vault alla versione 24.4 (v9.3). 3. Effettuare l'upgrade di Identity Manager Engine alla versione 4.10.
Remote Loader/Fanout Agent	4.9.x, 4.8.x, 4.7.5	Upgrade a Remote Loader/Fanout Agent 4.10.
Designer		Installare Designer 24.4 (v4.10).

Componente	Versione base	Versione dell'upgrade
Identity Applications	4.9.x, 4.8.x, 4.7.5	Prima dell'upgrade di Identity Applications, assicurarsi di effettuare l'upgrade di Identity Vault e di Identity Manager Engine rispettivamente alla versione 24.4 (v9.3) e 4.10. 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 di database supportate, vedere System Requirements for OpenText™ Identity Manager CE 24.4 (v4.10) (in lingua inglese). 4. (Condizionale) Se SSPR è installato su un server separato, effettuare l'upgrade del componente alla versione 4.8.0.1. 5. Aggiornare il driver dell'Applicazione utente e i pacchetti del driver di ruoli e risorse utilizzando Designer. 6. Upgrade di Identity Applications alla versione 24.4 (v4.10). 7. Avviare Tomcat.
Identity Reporting	4.9.x, 4.8.x, 4.7.5	Prima dell'upgrade di Identity Reporting, assicurarsi di effettuare l'upgrade di Identity Vault, di Identity Manager Engine e di Identity Applications rispettivamente alla versione 24.4 (v9.3), 4.10 e 24.4 (v4.10). 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 di database supportate, vedere System Requirements for OpenText™ Identity Manager CE 24.4 (v4.10) (in lingua inglese). 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 di Identity Reporting alla versione 24.4(v7.4). 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](https://www.netiq.com/documentation/identity-manager-4.10/) (<https://www.netiq.com/documentation/identity-manager-4.10/>).

Upgrade alla Advanced Edition

OpenText fornisce i seguenti percorsi per l'upgrade a OpenText Identity Manager 24.4 (v4.10) Advanced Edition da una versione Advanced Edition o Standard Edition precedente:

- ♦ Da Identity Manager 4.7.5, 4.8.x e 4.9.x Advanced Edition a 24.4 (v4.10) Advanced Edition
- ♦ Da Identity Manager 4.7.5, 4.8.x e 4.9.x Standard Edition a 24.4 (v4.10) Advanced Edition, in uno dei seguenti modi:
 - ♦ Da Identity Manager 4.7.5, 4.8.x e 4.9.x Standard Edition a 24.4 (v4.10) Standard Edition e successivamente alla versione 24.4 (v4.10) Advanced Edition
 - ♦ Da Identity Manager 4.7.5, 4.8.x e 4.9.x Standard Edition a 24.4 (v4.10) Advanced Edition e successivamente alla versione 24.4 (v4.10) Advanced Edition

Upgrade alla Standard Edition

È possibile eseguire l'upgrade a OpenText Identity Manager 24.4 (v4.10) Standard Edition da Identity Manager 4.7.5, 4.8.x e 4.9.x Standard Edition. Per istruzioni sull'upgrade, vedere [Quick Start Guide for Installing and Upgrading OpenText™ Identity Manager CE 24.4 \(v4.10\) Standard Edition](#) (in lingua inglese).

OpenText Identity Manager 24.4 (v4.10) 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 [OpenText™ Identity Manager CE 24.4 \(v4.10\) Administrator's Guide to Identity Reporting](#) (in lingua inglese).

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

Problemi noti

OpenText 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 relativamente a un problema, rivolgersi al [supporto tecnico \(https://www.opentext.com/products/identity-access-management\)](https://www.opentext.com/products/identity-access-management).

Per l'elenco dei problemi noti in Designer, consultare le [Note di rilascio di OpenText™ Identity Manager CE 24.4 \(v4.10\) Designer](#).

- ♦ “Problema con il driver Ellucian Banner dopo l'upgrade” a pagina 13
- ♦ “Errore appender rilevato nei log di Catalina per WFCEF” a pagina 13
- ♦ “Rapporti di autenticazione non generati su Sentinel dopo l'upgrade” a pagina 14
- ♦ “Errore segnalato nel file di log di OpenText eDirectory dopo l'upgrade” a pagina 15
- ♦ “Errore durante l'installazione non root del motore” a pagina 15
- ♦ “Errore segnalato nel log di avvio di PostgreSQL” a pagina 15
- ♦ “Errore segnalato nel file di log dell'upgrade” a pagina 16
- ♦ “Errore segnalato nel file di log di Catalina” a pagina 16
- ♦ “L'utility della riga di comando DirXML visualizza un errore dopo l'upgrade” a pagina 17
- ♦ “Errore durante l'upgrade di SSPR con Identity Applications” a pagina 17
- ♦ “Formato dell'archivio chiavi non valido: errore durante l'upgrade” a pagina 17
- ♦ “Errore visualizzato durante l'upgrade di Identity Manager Engine” a pagina 17
- ♦ “Windows Installer visualizza un errore” a pagina 18
- ♦ “Le proprietà dirxml_remote e RLConsole mostrano la versione del prodotto obsoleta” a pagina 18
- ♦ “OpenText Identity Manager non riflette le modifiche apportate all'opzione Utilizza SMTP TLS in OpenText Identity Console” a pagina 18
- ♦ “Nella gerarchia delle relazioni mancano i pulsanti dell'organigramma per una relazione di livello 2 o superiore” a pagina 19
- ♦ “Dopo l'upgrade, Remote Loader segnala una password dell'oggetto driver non valida” a pagina 19
- ♦ “Si osserva l'errore: riconfigurazione di StatusLogger non riuscita nel file di log di Catalina” a pagina 19
- ♦ “Problemi relativi al Generatore moduli” a pagina 19

Problema con il driver Ellucian Banner dopo l'upgrade

Problema: Il modulo di integrazione per Banner di Ellucian non funziona a causa dell'incompatibilità con le librerie Jetty fornite con OpenText Identity Manager 24.4 (v4.10).

Soluzione: Se il driver è stato installato, si consiglia di utilizzarlo con Remote Loader 4.9.

Errore appender rilevato nei log di Catalina per WFCEF

Problema: Durante l'upgrade di Identity Application alla versione 4.10, è possibile che nei log di Catalina venga visualizzato un errore simile dell'append.

`com.netiq.logging.log4j2.Log4jLogger.addAppender` Errore durante l'aggiunta del WFCEF dell'append a `Logger com.microfocus`

com.netiq.logging.log4j2.Log4jLogger.addAppender Errore durante l'aggiunta del WFCEF dell'appender a Logger com.sssw

com.netiq.logging.log4j2.Log4jLogger.addAppender Errore durante l'aggiunta del WFCEF dell'appender a Logger com.novell

com.netiq.logging.log4j2.Log4jLogger.addAppender Errore durante l'aggiunta del WFCEF dell'appender a Logger workflow.log

com.netiq.logging.log4j2.Log4jLogger.addAppender Errore durante l'aggiunta del WFCEF dell'appender a Logger com.netiq

Ciò si verifica quando si configura la revisione prima dell'upgrade di Identity Applications.

[OCTCR56A679501]

Soluzione:

1 Accedere alle seguenti directory:---

- ♦ Linux: /opt/netiq/idm/apps/tomcat/conf
- ♦ Windows: C:\NetIQ\IDM\apps\tomcat\conf

Commentare le voci seguenti nel file ism-configuration.properties:

```
workflow.logging.wfs.definition.workflow.log =  
{\"name\": \"workflow.log\", \"level\": \"INFO\", \"additivity\": true, \"appenderRefs\": [\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.novell =  
{\"name\": \"com.novell\", \"level\": \"INFO\", \"additivity\": true, \"appenderRefs\": [\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.netiq =  
{\"name\": \"com.netiq\", \"level\": \"INFO\", \"additivity\": true, \"appenderRefs\": [\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.sssw =  
{\"name\": \"com.sssw\", \"level\": \"INFO\", \"additivity\": true, \"appenderRefs\": [\"WFCEF\"]}
```

```
workflow.logging.wfs.definition.com.microfocus =  
{\"name\": \"com.microfocus\", \"level\": \"INFO\", \"additivity\": true, \"appenderRefs\": [\"WFCEF\"]}
```

2 Riavviare i servizi Tomcat.

Rapporti di autenticazione non generati su Sentinel dopo l'upgrade

Problema: Dopo l'upgrade di OpenText Identity Manager alla versione 24.4 (v4.10), i rapporti *Authentication by User* (Autenticazione da parte dell'utente) e *Authentication by server* (Autenticazione da parte del server) non vengono generati in Sentinel. Questo problema è stato rilevato in SUSE Linux Enterprise Server 15 SP5.

[OCTCR56A655281]

Soluzione: Eliminare la policy di sincronizzazione dei dati esistente nel servizio di raccolta dati di Identity Manager (idmdcs) e in Sentinel Log Management for IGA, quindi crearne una nuova. Per ulteriori informazioni su come creare una policy di sincronizzazione dei dati, vedere la [Administrator Guide to Identity Reporting \(https://www.netiq.com/documentation/identity-manager-4.10/report_setup/data/dcs-settings.html#t44exgvft7eh\)](https://www.netiq.com/documentation/identity-manager-4.10/report_setup/data/dcs-settings.html#t44exgvft7eh) (Guida dell'amministratore di Identity Reporting).

Errore segnalato nel file di log di OpenText eDirectory dopo l'upgrade

Problema: Dopo l'upgrade di OpenText Identity Manager dalla versione 4.9 alla versione 24.4 (v4.10), è possibile che si verifichi il seguente errore nel file ndsd.log :

```
Loader Failed:for lib/opt/novell/eDirectory/lib64/nds-modules/
libdxevent.so.3.so,error lib/opt/novell/eDirectory/lib64/nds-modules/
libdxevent.so.3.so: cannot open shared object file: No such file or
directory,errno 2
```

Questo problema è stato rilevato nella configurazione server *All-in-One* per OpenText Identity Manager su Linux. [OCTCR56A639009]

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

Errore durante l'installazione non root del motore

Problema: Durante l'installazione di OpenText Identity Manager Engine, gli utenti non root possono riscontrare il seguente errore nel file idminstall.log:

```
novell-edirectory-xdaslog-9.3.0.0000-1error: lsetfilecon: (/opt/novell,
system_u:object_r:usr_t:s0) Operation not permittederror: Plugin selinux: hook
fsm_file_prepare failed#####error: unpacking of
archive failed on file /opt/novell: cpio: (error 0x2)error: novell-edirectory-
xdaslog-9.3.0.0000-169.x86_64: install failed
```

Ciò si verifica quando si decompone l'RPM novell-edirectory-xdaslog-<version> nell'ubicazione /opt/novell perché un utente non root non dispone dell'accesso necessario a questa directory. [OCTCR56A647216]

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

Errore segnalato nel log di avvio di PostgreSQL

Problema: Quando si configurano i componenti Identity Applications and Identity Reporting nel database PostgreSQL, è possibile che nei log di avvio si verifichino i seguenti errori:

```

[16154] ERROR: relation "databasechangelog" does not exist at character 13
[16154] STATEMENT: insert into databasechangelog(id, author, filename, dateexecuted, orderexecuted, exectype,
description, comments, liquibase) values('410', 'IDMRBPM', 'ProvisioningViewValueConstraint45.xml', now(),
796, 'EXECUTED', 'sql', 'Dummy RECORD - TEMP SOLUTION', '3.2.2')
[16220] ERROR: relation "public.databasechangeloglock" does not exist at character 22
[16220] STATEMENT: SELECT COUNT(*) FROM public.databasechangeloglock
[16249] ERROR: relation "public.databasechangeloglock" does not exist at character 22
[16249] STATEMENT: SELECT COUNT(*) FROM public.databasechangeloglock
[15803] LOG: received fast shutdown request
[15803] LOG: aborting any active transactions
[15803] LOG: background worker "logical replication launcher" (PID 15810) exited with exit code 1
[15805] LOG: shutting down
[15803] LOG: database system is shut down
[1389] LOG: starting PostgreSQL 14.13 on x86_64-pc-linux-gnu, compiled by gcc (SUSE Linux) 7.4.1 20190424
[gcc-7-branch revision 270538], 64-bit
[1389] LOG: listening on IPv4 address "0.0.0.0", port 5432
[1389] LOG: listening on IPv6 address ":::", port 5432
[1389] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
[1389] LOG: could not open configuration file "/opt/netiq/idm/postgres/data/pg_hba.conf": Permission denied
[1389] FATAL: could not load pg_hba.conf
[1389] LOG: database system is shut down
[1473] LOG: starting PostgreSQL 14.13 on x86_64-pc-linux-gnu, compiled by gcc (SUSE Linux) 7.4.1 20190424
[gcc-7-branch revision 270538], 64-bit
[1473] LOG: listening on IPv4 address "0.0.0.0", port 5432
[1473] LOG: listening on IPv6 address ":::", port 5432
[1473] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
[1474] LOG: database system was shut down at 2024-10-05 07:39:04 IST
[1473] LOG: database system is ready to accept connections
[1679] ERROR: relation "idm_rpt_data.databasechangeloglock" does not exist at character 22
[1679] STATEMENT: select count(*) from idm_rpt_data.databasechangeloglock
[1733] ERROR: relation "idm_rpt_cfg.databasechangeloglock" does not exist at character 22
[1733] STATEMENT: select count(*) from idm_rpt_cfg.databasechangeloglock

```

[OCTCR56A662182]

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

Errore segnalato nel file di log dell'upgrade

Problema: Dopo aver eseguito l'upgrade di OpenText Identity Manager alla versione 24.4 (v4.10), è possibile che nel file `idmupgrade.log` vengano riportati seguenti errori relativi a SSPR:

```

ERROR password.pwm.util.cli.MainClass - 5083 ERROR_ENVIRONMENT_ERROR (unable to
establish operating environment: file for option 'outputFile' at '/opt/netiq/idm/
apps/sspr/sspr_data/SSPRConfiguration.xml' already exists)

```

[OCTCR56A662286]

Soluzione: Questi errori non influiscono su alcuna funzionalità. È possibile ignorarlo.

Errore segnalato nel file di log di Catalina

Problema: Dopo l'installazione o l'upgrade a OpenText Identity Manager 24.4 (v4.10), è possibile che si verifichi un errore durante l'avvio di Tomcat. L'errore viene segnalato nel file di log `catalina.out`.

```

[RPT-CORE] Error validating report configuration
schema.com.netiq.persist.PersistenceException: java.lang.RuntimeException: Cannot
use default schema name idm_rpt_cfg on Microsoft SQL Server because the login
schema of the current user (dbo) is different and MSSQL does not support setting
the default schema per session.

```

Questo problema si verifica quando Identity Manager Engine e Identity Reporting sono configurati in una configurazione server distribuita nel database MS SQL 2019. [OCTCR56A667011]

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

L'utility della riga di comando DirXML visualizza un errore dopo l'upgrade

Problema: Dopo aver eseguito l'upgrade di OpenText Identity Manager alla versione 24.4 (v4.10), all'avvio dell'utility da riga di comando DirXML può verificarsi il seguente errore LDAP:

```
Connection lost waiting for results from 10.71.142.57:636 (91) Connect Error
javax.net.ssl.SSLException: Unexpected error:
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must
be non-emp
```

Questo problema si verifica quando OpenText Identity Manager è configurato per funzionare in modalità abilitata per FIPS. [Problema: OCTCR56A669101]

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

Errore durante l'upgrade di SSPR con Identity Applications

Problema: Se Identity Applications e Self-Service Password Reset (SSPR) sono presenti sullo stesso server, è possibile che si verifichi un errore di operazione IO durante l'upgrade del servizio SSPR. Questo errore può verificarsi durante l'upgrade dalla versione 4.8.x alla versione 24.4 (v4.10) in Linux. [OCTCR56A670098]

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

Formato dell'archivio chiavi non valido: errore durante l'upgrade

Problema: Durante l'upgrade di OpenText Identity Manager in modalità abilitata per FIPS, è possibile che si verifichi il seguente errore durante l'importazione del certificato a chiave pubblica reCAPTCHA nell'archivio chiavi:

```
keytool error: java.io.IOException: Invalid keystore format
```

[Problema: OCTCR56A671139]

Soluzione: Importare il certificato a chiave pubblica dal file cacerts nell'archivio chiavi idm.bcfks utilizzando il seguente comando:

```
keytool -importkeystore -srckeystore /opt/netiq/common/jre/lib/security/cacerts -
srcstorepass changeit -srcstoretype BCFKS -destkeystore /opt/netiq/idm/apps/
tomcat/conf/idm.bcfks -deststorepass novell -deststoretype BCFKS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath $CLASSPATH
--noprompt
```

Errore visualizzato durante l'upgrade di Identity Manager Engine

Problema: Durante l'upgrade di Identity Manager Engine in modalità FIPS, è possibile che in Linux e Windows si verifichi l'eccezione seguente:

```
LDAPException: Error configuring LDAP SSL/TLS. (82) Local
Error:java.security.KeyStoreException: BCFKS not found
```

[Problema: OCTCR56A670109]

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

Windows Installer visualizza un errore

Problema: Dopo l'installazione dei componenti di OpenText Identity Manager 24.4 (v4.10), all'avvio di Tomcat viene visualizzato il seguente errore: 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 di OpenText Identity Manager 24.4 (v4.10). [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 è disponibile in C:\NetIQ\idm\apps\tomcat\conf

Le proprietà dirxml_remote e RLConsole mostrano la versione del prodotto obsoleta

Problema: in caso di installazione o upgrade di Remote Loader tramite Identity_Manager_4.10.0_RL_Windows.iso o Identity_Manager_4.10.0_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 di Remote Loader. È possibile verificare il valore di **Versione file** nella stessa finestra per verificare l'installazione di Remote Loader.

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

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

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

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 24.4 (v4.10) su 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 24.4(v4.10), 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 OpenText Identity Manager 24.4 (v4.10) su Windows, è possibile che venga visualizzato il seguente 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 sono chiari” a pagina 20](#)
- ♦ [“Il generatore moduli si blocca durante lo scorrimento” a pagina 20](#)
- ♦ [“Il componente Pulsante non funziona” a pagina 20](#)
- ♦ [“Problemi relativi al componente Albero” a pagina 21](#)

I messaggi di convalida dei campi non sono chiari

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 in 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 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.

Il componente 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 viene risolto 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]

Contatto di OpenText

Per problemi specifici del prodotto, visitare la pagina di assistenza di OpenText all'indirizzo <https://community.opentext.com/> (in lingua inglese).

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 di OpenText: <https://www.microfocus.com/communities/> (<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.