Lenovo

Guida per l'utente di Lenovo XClarity Essentials UpdateXpress

Versione 4.4.0

Nota

Prima di utilizzare questa documentazione e i prodotti correlati, consultare le informazioni in Appendice B "Informazioni particolari" a pagina 41.

Questa edizione si applica a Lenovo XClarity® Essentials UpdateXpress e a tutte le modifiche e ai rilasci successivi, se non diversamente indicato nelle nuove edizioni.

Ventiquattresima edizione (Febbraio 2024)

Contenuto

Tabelle

Informazioni su questa guida

Lenovo XClarity Essentials UpdateXpress (d'ora in avanti denominato applicazione UpdateXpress) è un'applicazione che si applica ai pacchetti UpdateXpress System Packs (UXSPs) e agli aggiornamenti individuali per il server. Questa guida fornisce informazioni su come scaricare e utilizzare l'applicazione UpdateXpress.

A chi è indirizzata questa guida

Questa documentazione è stata realizzata per gli amministratori di sistema o per i responsabili dell'amministrazione del sistema che hanno familiarità con la manutenzione dei driver di dispositivo e dei firmware.

Convenzioni e terminologia

I paragrafi che iniziano con Nota, Importante o Attenzione in grassetto hanno significati specifici per evidenziare le informazioni fondamentali:

Nota: Queste informazioni forniscono suggerimenti, istruzioni o consigli importanti.

Importante: Queste informazioni possono essere utili agli utenti per evitare situazioni difficili o poco convenienti.

Attenzione: Queste informazioni indicano possibili danni a programmi, unità o dati. Gli avvisi di attenzione vengono visualizzati prima dell'istruzione o della situazione in cui potrebbe verificarsi il danneggiamento.

In questa documentazione, quando agli utenti viene richiesto di immettere un comando, digitare il comando e premere Invio.

Siti Web supportati

Questa sezione fornisce risorse Web di supporto.

- Sito Web di Lenovo XClarity Essentials

  Utilizzare questo sito Web per scaricare più strumenti di gestione del sistema per i server ThinkSystem e System x.
- Lenovo XClarity Essentials UpdateXpress

  Utilizzare questo sito Web per scaricare l'applicazione UpdateXpress.

I seguenti siti Web forniscono informazioni sulla compatibilità e il supporto dei prodotti, le garanzie, le licenze e varie risorse tecniche.
- Supporto per prodotti e servizi Lenovo Flex System
- Sito Web di ServerProven
- Libreria di risorse per server, storage e reti Lenovo

Capitolo 1. Panoramica tecnica

Lenovo XClarity Essentials UpdateXpress (d'ora in avanti denominato applicazione UpdateXpress) può essere utilizzata per acquisire e applicare pacchetti UpdateXpress System Packs (UXSPs) e aggiornamenti individuali al sistema remoto o locale. L'applicazione UpdateXpress acquisisce e distribuisce i pacchetti di aggiornamento UpdateXpress System Pack (UXSP) e gli aggiornamenti individuali. I pacchetti UXSP contengono gli aggiornamenti di firmware e driver di dispositivo.

Nella seguente sezione vengono introdotte brevemente le quattro funzioni principali dell'applicazione UpdateXpress. Per ulteriori informazioni, vedere Capitolo 3 "Utilizzo dell'applicazione UpdateXpress" a pagina 9.

Aggiornamento del server locale
Aggiorna la macchina locale su cui attualmente è in esecuzione l'applicazione UpdateXpress. Viene identificato il tipo di macchina e vengono acquisiti e applicati automaticamente gli aggiornamenti.

Aggiornamento di un server remoto
Aggiorna la macchina remota in base al controller di gestione della scheda di base in esecuzione sulla macchina. Gli utenti devono utilizzare un server SFTP (Simple File Transfer Protocol) per trasferire gli aggiornamenti alla macchina di destinazione remota.

Creazione di un repository di aggiornamenti
Selezionare uno o più tipi di macchina per cui ottenere gli aggiornamenti dal sito Web del supporto Lenovo. Gli aggiornamenti vengono scaricati nella cartella specificata, ma non verrà applicato alcun aggiornamento. Successivamente, gli utenti possono utilizzare l'applicazione UpdateXpress per applicare tali aggiornamenti, specificando di ottenere gli aggiornamenti dalla cartella invece che dal sito Web del supporto Lenovo.

Configurazione RAID remota
Configurare l'array RAID utilizzando il servizio BMC.

UpdateXpress System Pack (UXSP)

Un pacchetto UXSP è un bundle di integrazione collaudato che include aggiornamenti online di firmware e driver per i server System x e ThinkSystem. I pacchetti UXSP vengono rilasciati semestralmente per i primi tre anni e annualmente per i tre anni finali di supporto.

I pacchetti UXSP semplificano il processo di download e installazione di tutti gli aggiornamenti firmware e driver online per un determinato sistema. I pacchetti UXSP assicurano agli utenti l'applicazione e l'utilizzo di una serie di aggiornamenti più recente e completa, collaudata e distribuita da Lenovo.

I pacchetti UXSP vengono creati in base alla combinazione di sistema operativo e tipo di macchina. Pacchetti UXSP separati vengono forniti per i sistemi operativi Windows® e per ogni distribuzione Linux. Ad esempio, potrebbero essere presenti diversi pacchetti UXSP per un determinato tipo di macchina. Potrebbe essere disponibile anche un aggiornamento per il sistema operativo Windows e per ciascuna distribuzione Linux.

Inoltre è disponibile un pacchetto UXSP di piattaforma che può essere utilizzato per aggiornare un sistema in modalità fuori banda. Il pacchetto UXSP di piattaforma non contiene il sistema operativo.

Formato UXSP
Un pacchetto UXSP viene fornito in un file XML. La convenzione di denominazione di un pacchetto UXSP presenta il seguente formato:
lnvgy_utl_uxsp_*version_operatingsystem_arch*.xml

Esempio: `lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml`

Installazione degli aggiornamenti UXSP con l'applicazione UpdateXpress

Gli utenti possono utilizzare l'applicazione UpdateXpress per applicare gli aggiornamenti UXSP alla macchina in uso. L'applicazione UpdateXpress analizza la macchina su cui verrà applicato l'aggiornamento, interroga un percorso specificato per un elenco di pacchetti di aggiornamento applicabili, confronta l'inventario con l'elenco di aggiornamenti applicabili, suggerisce una serie di aggiornamenti da applicare e quindi distribuisce questi aggiornamenti alla macchina.

Per applicare gli UXSP tramite l'applicazione UpdateXpress, effettuare le seguenti operazioni:
1. Scaricare l'applicazione UpdateXpress dal sito Web del supporto Lenovo.
2. Eseguire l'applicazione UpdateXpress. Selezionare **Aggiorna la macchina locale** o **Aggiornare una macchina remota**.
3. Selezionare **Controlla il sito Web dell'assistenza Lenovo**.
4. Selezionare **Applicazione UpdateXpress System Packs (UXSPs)**.

Gli utenti possono scaricare gli aggiornamenti direttamente dal sito Web del supporto Lenovo. Scaricare il payload dell'aggiornamento e il file XML. Per comodità, scegliere la stessa cartella di destinazione per ogni UXSP scaricato. Gli utenti possono scaricare più pacchetti di sistema per tipi di macchina differenti nella stessa cartella. Una volta eseguita, l'applicazione UpdateXpress rileva il tipo di macchina e ne utilizza il contenuto corretto. In alcuni casi potrebbero essere presenti dei file comuni tra i pacchetti di sistema. I file comuni già presenti nella cartella non verranno scaricati nuovamente. In questo modo, il tempo di download complessivo è inferiore.

Gestione di un pacchetto UXSP come bundle

L'applicazione UpdateXpress è progettata per scaricare e applicare i pacchetti UXSP. Il pacchetto UXSP è una raccolta di aggiornamenti individuali, come specificato dal file XML UXSP.

Quando eseguono l'applicazione UpdateXpress, gli utenti possono scegliere di utilizzare i pacchetti UXSP o gli aggiornamenti individuali. Nella maggior parte dei casi, si consiglia di utilizzare i pacchetti UXSP, ma la possibilità di utilizzare gli aggiornamenti individuali assicura maggiore flessibilità agli utenti, in termini di scelta degli aggiornamenti da utilizzare.

Gestione dei requisiti per gli aggiornamenti

In questa sezione vengono descritte le modalità di acquisizione e applicazione dei requisiti per gli aggiornamenti.

Per applicare correttamente gli aggiornamenti, tutti i prerequisiti e i co-requisiti di un aggiornamento devono essere acquisiti e applicati. L'applicazione UpdateXpress controlla, acquisisce e applica automaticamente i prerequisiti e i co-requisiti. Gli aggiornamenti spesso richiedono agli utenti l'applicazione dei file dei prerequisiti prima di poter essere applicati correttamente o l'inclusione dei pacchetti dei co-requisiti per utilizzare correttamente l'aggiornamento applicato. Per semplificare il processo di aggiornamento, l'applicazione UpdateXpress utilizza le informazioni incluse nel file di aggiornamento per identificare i pacchetti richiesti per gli aggiornamenti specificati. L'applicazione UpdateXpress quindi applica i pacchetti richiesti.

File dei prerequisiti

I pacchetti di aggiornamento forniti da Lenovo includono informazioni sui file dei prerequisiti da applicare prima che gli utenti possano applicare correttamente l'aggiornamento. Quando gli utenti specificano un

aggiornamento, l'applicazione UpdateXpress legge queste informazioni e individua i pacchetti dei prerequisiti.

Per impostazione predefinita, l'applicazione UpdateXpress acquisisce e analizza i pacchetti di aggiornamento per determinare se le condizioni dei prerequisiti sono stati soddisfatte e, se necessario, applica automaticamente i file dei prerequisiti prima di applicare l'aggiornamento specificato. Gli utenti possono scegliere di non applicare i file dei prerequisiti. Tuttavia, ciò potrebbe causare un'errata applicazione dell'aggiornamento.

Eventuali prerequisiti o co-requisiti dei pacchetti dei prerequisiti vengono acquisiti, valutati e applicati allo stesso modo.

File dei co-requisiti

Alcuni aggiornamenti richiedono i file dei co-requisiti, ovvero pacchetti aggiuntivi che devono essere applicati per completare l'aggiornamento correttamente. Tuttavia questi pacchetti non devono essere applicati prima dell'aggiornamento specificato dall'utente.

Per impostazione predefinita, l'applicazione UpdateXpress identifica, acquisisce, valuta e applica i pacchetti dei co-requisiti come parte dell'aggiornamento.

Eventuali prerequisiti o co-requisiti dei pacchetti dei co-requisiti vengono acquisiti, valutati e applicati allo stesso modo.

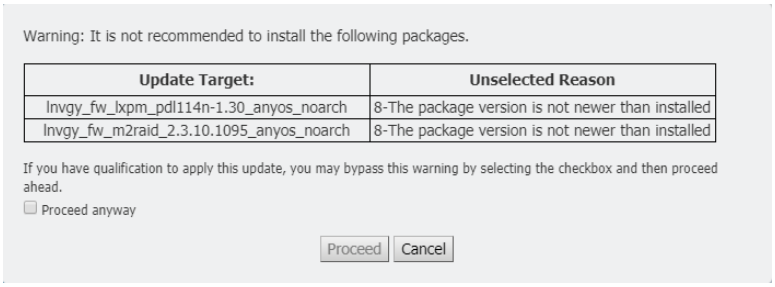
Esempio

Ad esempio, consideriamo un aggiornamento che richieda sia prerequisiti che co-requisiti. Per impostazione predefinita, l'applicazione UpdateXpress esegue le seguenti operazioni:

1. Per garantire il completamento dell'aggiornamento, l'applicazione UpdateXpress scarica innanzitutto l'aggiornamento.
2. Vengono scaricati i file dei prerequisiti.
3. Vengono scaricati i file dei co-requisiti.
4. I file dei prerequisiti o dei corequisiti vengono valutati in base allo stato corrente del sistema. Se il sistema è già al livello richiesto perché tali requisiti sono già stati applicati, la richiesta viene ignorata.
5. Vengono applicati i file dei prerequisiti necessari.
6. L'aggiornamento viene applicato.
7. Vengono applicati i file dei co-requisiti necessari.

Suggerimenti per l'aggiornamento

Per impostazione predefinita, l'applicazione UpdateXpress selezionerà i pacchetti consigliati per l'installazione o l'aggiornamento del sistema. Gli utenti possono anche selezionare manualmente questi pacchetti per l'installazione o l'aggiornamento. In questo caso, gli utenti visualizzeranno un messaggio di avvertenza simile al seguente:



Se gli utenti visualizzano questo messaggio, si consiglia di interrompere il processo di aggiornamento.

Aggiornamenti indipendenti del sistema operativo

Alcuni aggiornamenti individuali si applicano a un tipo di macchina specifico, indipendentemente dal sistema operativo utilizzato. Questi aggiornamenti individuali vengono considerati come aggiornamenti indipendenti del sistema operativo. Gli utenti possono selezionare gli aggiornamenti indipendenti del sistema operativo allo stesso modo degli aggiornamenti specifici del sistema operativo.

Nota: Quando gli utenti selezionano gli aggiornamenti per un sistema operativo specifico, gli aggiornamenti indipendenti del sistema operativo sono inclusi nel pacchetto. Selezionare gli aggiornamenti indipendenti del sistema operativo solo se gli utenti non selezionano alcun aggiornamento del sistema operativo per un tipo di macchina.

Dati di inventario mancanti o incompleti

Talvolta un pacchetto di aggiornamento viene applicato a un componente per cui l'applicazione UpdateXpress non può determinare la versione del firmware o del driver. In questo caso, l'applicazione UpdateXpress visualizza la versione del pacchetto di aggiornamento invece della versione del componente. Se una versione del componente installato non viene rilevata, l'aggiornamento non viene selezionato per impostazione predefinita. In questo caso, selezionare il pacchetto come aggiornamento manuale consigliato.

Installazione dei driver richiesti

L'applicazione UpdateXpress installa i driver di dispositivo richiesti.

L'applicazione UpdateXpress installa ogni driver nel pacchetto UXSP quando:
- Il driver di dispositivo corrente è precedente al driver di dispositivo disponibile nel pacchetto UXSP.
- L'applicazione UpdateXpress non è in grado di determinare la versione del driver di dispositivo corrente. In genere, ciò si verifica quando il driver di dispositivo non è installato.

  Nota: L'applicazione UpdateXpress visualizza il messaggio `Non rilevato` quando non viene rilevata una versione del driver di dispositivo installata.

In questo caso, gli utenti possono installare i seguenti driver di dispositivo, richiesti per gli aggiornamenti firmware:
- IPMI (Intelligent Peripheral Management Interface)
- Layer di associazione IPMI

Capitolo 2. Requisiti hardware e software

Prima che gli utenti inizino a utilizzare l'applicazione UpdateXpress, verificare i requisiti hardware, del sistema operativo e dei privilegi del sistema operativo locale. I sistemi che eseguono l'applicazione UpdateXpress richiedono almeno 1 GB di RAM (Random-Access Memory).

Modelli di server supportati

L'applicazione UpdateXpress supporta i firmware e i driver di dispositivo Windows e Linux inclusi nei pacchetti UXSP disponibili. Un elenco di firmware e driver di dispositivo attualmente supportati è disponibile nel file readme dell'applicazione UpdateXpress incluso in ogni pacchetto di sistema.

Tabella 1. Sistemi Lenovo supportati

Serie	**Modelli di server**	
ThinkEdge	• SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
ThinkSystem	• Gateway DX1100U (7D49) • Prestazioni/Capacità DX1100U (7D4A) • Storage DXN2000 (7D5W) • SD530 (7X21) • SD530 V3 (7DD3, 7DDA) • SD550 V3 (7DD2, 7DD9) • SD555 V3 (7DDM, 7DDN) • SD630 V2 (7D1K) • SD650 DWC (7X58) • SD650 V2 (7D1M) • SD650 V3 (7D7M) • SD650-I V3 (7D7L) • SD650-N V3 (7D7N) • SD665 V3 (7D9P) • SD665-N V3 (7DAZ) • SD670 V2 (7D1N) • SE350 (7Z46, 7D1X, 7D27) • SN550 (7X16) • SN550 V2 (7Z69) • SN850 (7X15) • SR150/SR158 (7Y54, 7Y55) • SR250 (7Y51, 7Y52) • SR250 V2 (7D7R, 7D7Q) • SR250 V3 (7DCM, 7DCL) • SR258 V2 (7D7S) • SR258 V3 (7DCN) • SR530 (7X07, 7X08) • SR550 (7X03, 7X04) • SR570 (7Y02, 7Y03) • SR590 (7X98, 7X99) • SR630 (7X01, 7X02) • SR630 V2 (7Z70, 7Z71) • SR630 V3 (7D72, 7D73, 7D74)	• SR635 (7Y98, 7Y99)[1] • SR635 V3 (7D9G, 7D9H) • SR645 (7D2X, 7D2Y) • SR645 V3 (7D9C, 7D9D) • SR650 (7D4K, 7X05, 7X06) • SR650 V2 (7D15, 7Z72, 7Z73) • SR650 V3 (7D75, 7D76, 7D77) • SR655 (7Y00, 7Z01)[1] • SR655 V3 (7D9E, 7D9F) • SR665 (7D2V, 7D2W) • SR665 V3 (7D9A, 7D9B) • SR670 (7D4L, 7Y36, 7Y37, 7Y38) • SR670 V2 (7Z22, 7Z23) • SR675 V3 (7D9Q, 7D9R) • SR850 (7X18, 7X19) • SR850 V2 (7D31, 7D32, 7D33) • SR850 V3 (7D96, 7D97, 7D98) • SR850P (7D2H, 7D2F, 7D2G) • SR860 (7X69, 7X70) • SR860 V2 (7Z59, 7Z60, 7D42) • SR860 V3 (7D93, 7D94, 7D95) • SR950 (7X11, 7X12, 7X13) • SR950 V3 (7DC4, 7DC5, 7DC6) • ST250 (7Y45, 7Y46) • ST250 V2 (7D8F, 7D8G) • ST250 V3 (7DCF, 7DCE) • ST258 V2 (7D8H) • ST258 V3 (7DCG) • ST550 (7X09, 7X10) • ST558 (7Y15, 7Y16) • ST650 V2/ST658 V2 (7Z74, 7Z75, 7Z76) • ST650 V3 (7D7A, 7D7B) • ST658 V3 (7D7C)
ThinkServer	• DN8848 V2 (7D6A, 7D8U) • SE550 V2 (7D68) • SR588/SR590 (7D4M) • SR588 V2/SR590 V2 (7D53)	• SR660 V2/SR668 V2 (7D6L) • SR860P (7D5D) • Appliance WH5900 (7D5V)

Tabella 1. Sistemi Lenovo supportati (continua)

Serie	Modelli di server	
WenTian	• WA5480 G3/WA5488 G3 (7DE7) • WR3220 G2/WR3228 G2 (7DEC)	• WR5220 G3/WR5228 G3 (7D8Y)
Soluzioni	• ThinkAgile serie VX (7D28, 7D2Z, 7D43, 7DDK, 7Y12, 7Y13, 7Y14, 7Y92, 7Y93, 7Y94, 7Z12, 7Z13, 7Z62, 7Z63) • ThinkAgile serie MX (7D19, 7D1B, 7D1H, 7D5R, 7D5S, 7D5T, 7D66, 7D67, 7D6B, 7DGG, 7Z20)	• ThinkAgile serie HX (7D20, 7D2T, 7D46, 7D4R, 7D5U, 7X82, 7X83, 7X84, 7Y88, 7Y89, 7Y90, 7Y95, 7Y96, 7Z03, 7Z04, 7Z05, 7Z08, 7Z09, 7D0W, 7D0Y, 7D0Z, 7D11, 7D52, 7Z82, 7Z84, 7Z85)
System x	• Appliance HX 3310 (8693) • Appliance HX 5510/7510 (8695) • nx360 M5 (5465, 5467) • Nodo di elaborazione x240 (7162, 2588) • Nodo di elaborazione x240 M5 (2591, 9532) • Nodo di elaborazione x280 X6/x480 X6/ x880 X6 (4258, 7196)[2] • x440 (7167, 2590)	• x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M5 (5463, 8869) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6/x3950 X6 (6241)[2]
Nota: 1. Questo modello di server è basato su un processore AMD a un socket. 2. Questo modello di server supporta sia il singolo nodo sia quello multiplo.		

Sistemi operativi supportati

L'applicazione UpdateXpress è supportata sui sistemi operativi Linux e Windows.

Windows

L'applicazione UpdateXpress è supportata sui sistemi operativi a 64 bit. Utilizzare le informazioni nella seguente tabella per identificare i sistemi operativi supportati dall'applicazione UpdateXpress.

Tabella 2. Sistemi operativi Windows supportati

Sistema operativo	Aggiornamento locale	Aggiornamento remoto	Repository locale	Configurazione RAID remota
Microsoft Windows 10/11 Pro for Workstations (21H2/ 22H2)	Sì[nota]	Sì	Sì	Sì
Microsoft Windows Server 2016	Sì	Sì	Sì	Sì
Microsoft Windows Server 2019	Sì	Sì	Sì	Sì
Microsoft Windows Server 2022	Sì	Sì	Sì	Sì

Nota: I modelli di server che supportano Microsoft Windows 10/11 Pro for Workstations (21H2/22H2) possono accedere anche alla relativa funzione locale di aggiornamento.

Linux

L'applicazione UpdateXpress è supportata sulle seguenti versioni dei sistemi operativi Linux.

Tabella 3. Sistemi operativi supportati Linux supportati

Sistema operativo	Aggiornamento locale	Aggiornamento remoto	Repository locale	Configurazione RAID remota
Red Hat Enterprise Linux 7.X (7.6 e versioni successive)	Sì	Sì	Sì	Sì
Red Hat Enterprise Linux 8.X	Sì	Sì	Sì	Sì
Red Hat Enterprise Linux 9.X	Sì	Sì	Sì	Sì
SUSE Linux Enterprise Server 15.X	Sì	Sì	Sì	Sì

Nota:
- Quando si esegue l'applicazione UpdateXpress su un sistema operativo Linux, lo spazio su disco consigliato è di 500 MB.
- L'applicazione UpdateXpress supporta il controllo fuzzy del sistema operativo. Se il sistema operativo corrente non supporta i pacchetti firmware in un pacchetto UXSP, i pacchetti firmware potrebbero essere elencati anche nel risultato del confronto dell'applicazione UpdateXpress.
- A seconda del comando `ifconfig` sul sistema operativo Linux, UpdateXpress potrebbe non essere installato su RHEL 7.0 o versioni successive. Per aggiornare il firmware di RHEL 7.0 o versioni successive, gli utenti devono installare net-tools.
- Gli aggiornamenti dei driver di dispositivo Linux richiedono pacchetti specifici. È necessario installare i seguenti pacchetti:
  - Red Hat Enterprise Linux: rpm-build, perl e bash
  - SUSE Enterprise Linux: perl e bash
- Per i seguenti sistemi operativi, gli utenti possono utilizzare UpdateXpress 4.3.0:
  - SUSE 12.5
- Per i seguenti sistemi operativi, gli utenti possono utilizzare UpdateXpress 4.1.0:
  - RedHat 7.5
  - SUSE 12.4
- Per i seguenti sistemi operativi, gli utenti possono utilizzare UpdateXpress 3.4.0:
  - RedHat 7.0/7.1/7.2/7.3/7.4
  - SUSE 12.0/12.1/12.2/12.3
  - Windows 7/8
  - Windows Server 2008R2/2012/2012R2

Privilegi del sistema operativo

Per eseguire l'applicazione UpdateXpress, gli utenti devono disporre di privilegi di amministratore o del sistema operativo equivalenti a root. L'applicazione UpdateXpress restituisce un errore quando un utente con privilegi insufficienti tenta di eseguire il programma.

Archiviare l'applicazione UpdateXpress, inclusi i log sensibili e le relative estrazioni, in un luogo sicuro a cui possono accedere solo gli utenti autorizzati.

Capitolo 3. Utilizzo dell'applicazione UpdateXpress

Gli utenti possono utilizzare l'applicazione UpdateXpress per distribuire gli aggiornamenti in modo interattivo. Quando si esegue l'applicazione UpdateXpress si consiglia di utilizzare una risoluzione dello schermo di 1.024 x 768 o superiore. Per eseguire l'applicazione UpdateXpress, estrarre il file compresso e richiamare il file eseguibile per il sistema operativo. Non è richiesta alcuna installazione.

Windows

Per il sistema operativo Windows, il nome dell'applicazione UpdateXpress è il seguente:

```
lnvgy_utl_lxce_ux{ build id }_4.x.x_windows_x86-64.zip
```

Per ogni versione dell'applicazione UpdateXpress, gli utenti possono distinguere il nome del file ZIP di Windows in base al numero della versione. Il file ZIP di Windows è specificato come **lnvgy_utl_lxce_ux{ build id }_{ version }_windows_i386.zip** dove *lnvgy_utl_lxce_ux* è il nome del file ZIP, *build id* indica il numero di build e *versione* indica il numero di versione dell'applicazione UpdateXpress.

Linux

Per il sistema operativo Linux, il nome dell'applicazione UpdateXpress è il seguente:

Sistema operativo	Nome dell'applicazione UpdateXpress
Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T e versioni successive	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T e versioni successive	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`

Il nome dell'applicazione UpdateXpress è differente per i sistemi operativi Windows e Linux. Per comodità, d'ora in avanti in questa documentazione <*Zipfile*> viene utilizzato per fare riferimento al nome dell'applicazione UpdateXpress sia per i sistemi operativi Windows che Linux.

Avvio dell'applicazione UpdateXpress

Gli utenti possono utilizzare l'applicazione UpdateXpress per acquisire i pacchetti UXSP e gli aggiornamenti individuali più recenti.

Per avviare l'applicazione UpdateXpress, effettuare le seguenti operazioni:

- **Per Windows**:
  1. Estrarre il file <*Zipfile*> in una cartella locale.
  2. Effettuare una delle seguenti operazioni:
     - Fare doppio clic su **lxce_ux.exe**.
     - Fare clic con il pulsante destro del mouse su **lxce_ux.exe**, quindi fare clic su **Esegui come amministratore** nel menu a comparsa.
- **Per Linux**:

  Digitare i seguenti comandi nel terminale:

  ```
  tar xvf <Zipfile>
  ./start_lxce_ux.sh
  ```

Aggiornamento di un server locale dal sito Web

L'applicazione UpdateXpress può aggiornare una macchina locale con i pacchetti UXSP o gli aggiornamenti individuali acquisiti dal sito Web.

Per completare questa attività sono necessari i seguenti prerequisiti:
- L'applicazione UpdateXpress è in esecuzione su una macchina locale da aggiornare.
- La macchina deve eseguire un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per aggiornare una macchina locale dal sito Web, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione selezionare **Gestisci il server locale**. Se è selezionata l'opzione **Immetti informazioni di accesso BMC**, immettere le informazioni BMC in questa finestra e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
5. Nella finestra Impostazione aggiornamento, effettuare una o più delle seguenti operazioni in base alle esigenze:
   - Per aggiornare il firmware del sistema di backup, selezionare **Aggiorna solo l'immagine di backup del BMC (e UEFI dove applicabile)** e fare clic su **Avanti**.
   - Per eseguire il downgrade del firmware, selezionare **Abilita aggiornamento a una versione precedente del firmware** e fare clic su **Avanti**.
6. Nella finestra Posizione aggiornamenti selezionare **Controlla il sito Web del Supporto Lenovo** e fare clic su **Avanti**.
7. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
8. Nella finestra Directory di destinazione, specificare la posizione in cui scaricare gli aggiornamenti o accettare la posizione predefinita e fare clic su **Avanti**.
9. Nella pagina Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
   Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, effettuare una o più delle seguenti operazioni:
   - Configurare l'opzione **Server proxy**:
     a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

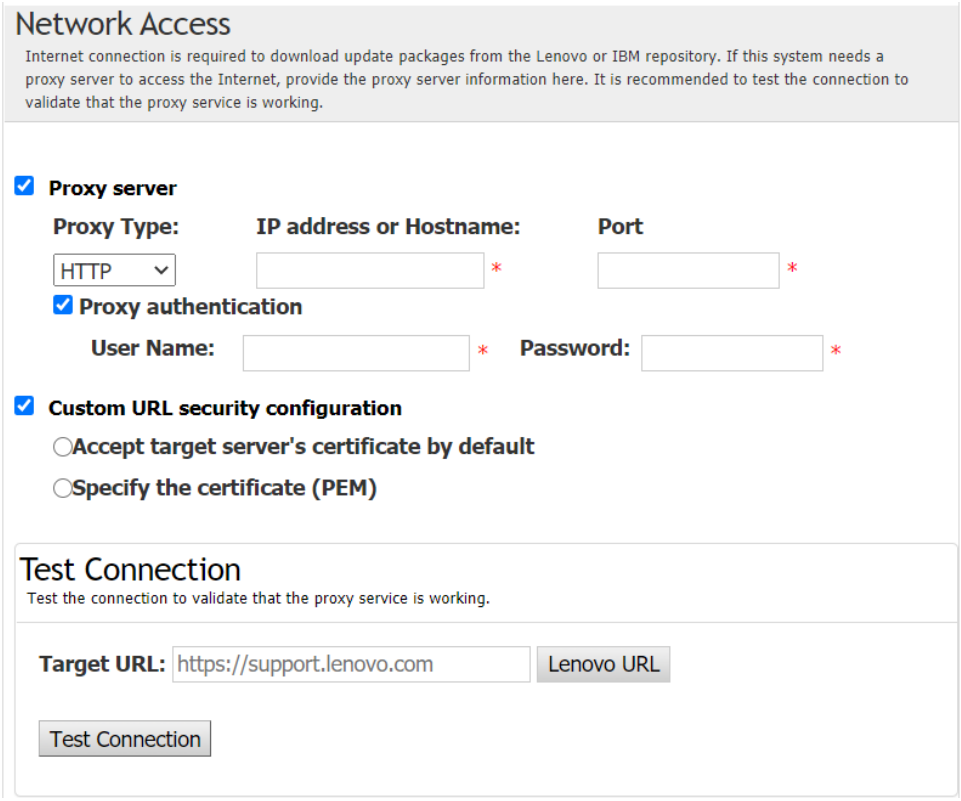
     b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

   - Configurare **Configurazione di sicurezza URL personalizzata**

     Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
     – **Accetta il certificato del server di destinazione per impostazione predefinita**

– **Specifica il certificato (PEM)**



10. Nella finestra Suggerimenti per l'aggiornamento effettuare una o più delle seguenti operazioni:
    - Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti dei dispositivi non rilevati**.
    - Per aggiornare il componente, selezionare il componente di destinazione e fare clic su **Avanti**.
11. Nella finestra Ottenere gli aggiornamenti, nella tabella di acquisizione viene visualizzato l'avanzamento dell'acquisizione dei pacchetti. Una volta completato il processo, fare clic su **Avanti**.
12. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.
13. Nella finestra Fine, fare clic su **Visualizza log** per controllare il log di aggiornamento e fare clic su **Chiudi** per uscire.

Aggiornamento di un server locale da una directory locale

L'applicazione UpdateXpress può aggiornare una macchina locale con i pacchetti UXSP o gli aggiornamenti individuali acquisiti da una cartella locale.

Per completare questa attività sono necessari i seguenti prerequisiti:
- L'applicazione UpdateXpress è in esecuzione su una macchina locale da aggiornare.
- La macchina deve eseguire un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- L'immagine ISO montata non deve essere utilizzata come directory locale valida. In caso contrario, se non dovesse essere montata durante il processo di aggiornamento, l'immagine potrebbe causare un errore flash.

Per aggiornare una macchina locale da una directory locale, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.

3. Nella finestra Server di destinazione, selezionare **Gestisci il server locale** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
5. Nella finestra Impostazione aggiornamento, effettuare una o più delle seguenti operazioni in base alle esigenze:
   - Per aggiornare l'immagine di backup di BMC o UEFI, selezionare **Aggiorna solo l'immagine di backup del BMC (e UEFI dove applicabile)** e fare clic su **Avanti**.
   - Per eseguire il downgrade del firmware, selezionare **Abilita aggiornamento a una versione precedente del firmware** e fare clic su **Avanti**.
6. Nella finestra Posizione aggiornamenti selezionare **Cerca nella directory locale**. Per specificare una cartella locale, effettuare una delle seguenti operazioni:
   - Fare clic su **Sfoglia**, selezionare la cartella di destinazione e quindi fare clic su **Avanti**.
   - Immettere il percorso della cartella nel campo accanto al pulsante **Sfoglia** e fare clic su **Avanti**.
7. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
8. Nella finestra Suggerimenti per l'aggiornamento, effettuare una o più delle seguenti operazioni:
   - Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti senza adattatori rilevati**.
   - Per confrontare le versioni di driver e firmware installati con le versioni più recenti, fare clic su **Inizia**. Una volta completato l'avanzamento, selezionare uno o più pacchetti di destinazione che si desidera aggiornare e fare clic su **Avanti**.
   - Per confrontare la versione dei dispositivi installata nel sistema locale con la versione più recente, selezionare **Confronta solo dispositivi installati** e fare clic su **Inizia**. Una volta completato l'avanzamento, selezionare uno o più pacchetti di destinazione che si desidera aggiornare e fare clic su **Avanti**.
9. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.
10. Nella finestra Fine, fare clic su **Visualizza log** per controllare il log di aggiornamento e fare clic su **Chiudi** per uscire.

Aggiornamento di un server remoto dal sito Web

L'applicazione UpdateXpress può aggiornare una macchina remota con i pacchetti UXSP o gli aggiornamenti individuali acquisiti dal sito Web.

Per completare questa attività è necessario il seguente prerequisito:

L'applicazione UpdateXpress deve essere in esecuzione su una macchina installata con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per aggiornare una macchina remota dal sito Web, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - **(Impostazione) Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - **(Impostazione) Nome utente**: il nome utente BMC del sistema di destinazione.
   - **(Impostazione) Password**: la password BMC del sistema di destinazione.
   - **(Impostazione) Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

Nota: Se non si controlla il certificato server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.

4. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
5. Nella finestra Impostazione aggiornamento selezionare una o più opzioni. Se è selezionata l'opzione **Utilizza un server remoto separato invece del server BMC**, immettere le seguenti informazioni:
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Nome utente**: il nome utente del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Password**: la password del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Porta**: il numero di porta del server. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Directory**: la posizione sul server in cui vengano copiati i pacchetti di aggiornamento.

     Nota: Immettere un percorso completo sul server SFTP/HTTP/HTTPS/FTP. Il server FTP viene utilizzato solo per ThinkServer contrassegnato con apice 2 (nota 2) in "Modelli di server supportati" a pagina 5.
6. Per configurare l'impronta digitale della chiave del server SFTP, effettuare una delle seguenti operazioni:
   - Per verificare l'impronta digitale della chiave del server SFTP, fare clic su **Sì**.
   - Per non verificare l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Ignora impronta digitale chiave del server SFTP** e fare clic su **Avanti**.
7. Effettuare una o più delle seguenti operazioni:
   - Per eseguire il downgrade del firmware, selezionare **Abilita aggiornamento a una versione precedente del firmware** e fare clic su **Avanti**.
   - Per aggiornare il firmware del sistema di backup, selezionare **Aggiorna solo l'immagine di backup del BMC (e UEFI dove applicabile)** e fare clic su **Avanti**.
8. Nella finestra Posizione aggiornamenti selezionare **Controlla il sito Web del Supporto Lenovo** e fare clic su **Avanti**.
9. Nella finestra Directory di destinazione, specificare la posizione in cui scaricare gli aggiornamenti o accettare la posizione predefinita e fare clic su **Avanti**.
10. Nella pagina Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
    Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, configurare i campi **Server proxy** e/o **Configurazione di sicurezza URL personalizzata**, a seconda dei requisiti di sicurezza, come segue:
    - **Server proxy**
      a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

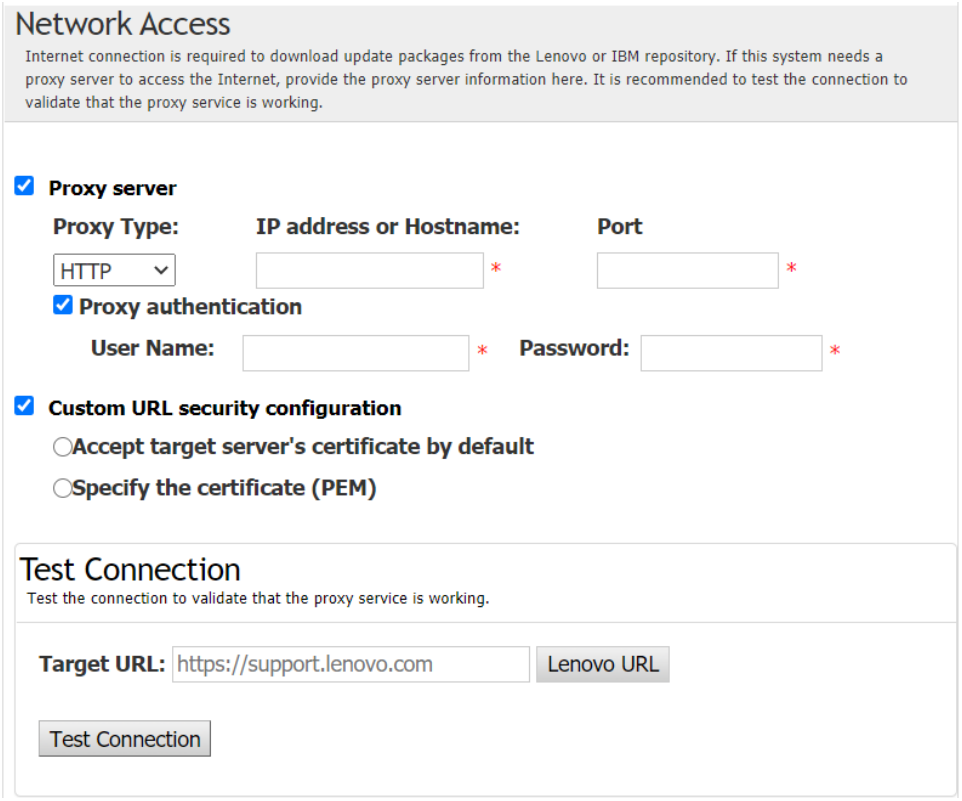
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

      b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

    - **Configurazione di sicurezza URL personalizzata**

Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
- **Accetta il certificato del server di destinazione per impostazione predefinita**
- **Specifica il certificato (PEM)**



11. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
12. Nella finestra Suggerimenti per l'aggiornamento effettuare una o più delle seguenti operazioni:
    - Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti dei dispositivi non rilevati**.
    - Per aggiornare il componente, selezionare il componente di destinazione e fare clic su **Avanti**.
13. Nella finestra Ottenere gli aggiornamenti, nella tabella di acquisizione viene visualizzato l'avanzamento dell'acquisizione dei pacchetti. Una volta completato il processo, fare clic su **Avanti**.
14. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.
15. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Aggiornamento di un server remoto da una directory locale

L'applicazione UpdateXpress può aggiornare una macchina remota con i pacchetti UXSP o gli aggiornamenti individuali acquisiti da una cartella locale.

Per completare questa attività è necessario il seguente prerequisito:

L'applicazione UpdateXpress deve essere in esecuzione su una macchina installata con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per aggiornare una macchina remota da una directory locale, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non desiderano controllare il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Accetta il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
5. Nella finestra Impostazione aggiornamento, se è selezionata l'opzione **Utilizza un server remoto separato**, immettere le seguenti informazioni:
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Nome utente**: il nome utente del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Password**: la password del server.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Porta**: il numero di porta del server. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.
   - (Impostazione SFTP/HTTP/HTTPS/FTP) **Directory**: la posizione sul server in cui vengano copiati i pacchetti di aggiornamento.

     Nota: Immettere un percorso completo sul server SFTP/HTTP/HTTPS/FTP. Il server FTP viene utilizzato solo per ThinkServer contrassegnato con apice 2 (nota 2) in "Modelli di server supportati" a pagina 5.
6. Per configurare l'impronta digitale della chiave del server SFTP, effettuare una delle seguenti operazioni:
   - Per verificare l'impronta digitale della chiave del server SFTP, fare clic su **Sì**.
   - Per non verificare l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Ignora impronta digitale chiave del server SFTP** e fare clic su **Avanti**.
7. Effettuare una o più delle seguenti operazioni:
   - Per eseguire il downgrade del firmware, selezionare **Abilita aggiornamento a una versione precedente del firmware** e fare clic su **Avanti**.
   - Per aggiornare il firmware del sistema di backup, selezionare **Aggiorna solo l'immagine di backup del BMC (e UEFI dove applicabile)** e fare clic su **Avanti**.
8. Nella finestra Posizione aggiornamenti selezionare **Cerca nella directory locale**. Per specificare una cartella locale, effettuare una delle seguenti operazioni:
   - Fare clic su **Sfoglia**, selezionare la cartella desiderata e fare clic su **Avanti**.
   - Immettere il percorso della cartella nel campo accanto al pulsante **Sfoglia** e fare clic su **Avanti**.
9. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
10. Nella finestra Suggerimenti per l'aggiornamento, fare clic su **Inizia** per confrontare la versione del firmware installato con quella più recente. Una volta completato l'avanzamento, selezionare uno o più pacchetti di destinazione che si desidera aggiornare e fare clic su **Avanti**.

    Nota: Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti senza adattatori rilevati** prima di fare clic su **Inizia**.
11. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.

12. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Configurazione del BIOS per un server remoto

L'applicazione UpdateXpress supporta la configurazione delle impostazioni BIOS per un server remoto.

Prerequisito:

La funzione di configurazione del BIOS per il server remoto è supportata solo nei server ThinkServer/WenTian. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per configurare il BIOS, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non desiderano controllare il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Accetta il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configurazione BIOS** e fare clic su **Avanti**.
5. Nella finestra Modalità di configurazione, selezionare **Configurazione BIOS comune** o **Importa file di configurazione BIOS** e fare clic su **Avanti**.
6. Effettuare una delle seguenti operazioni:
   - Se nel passaggio precedente è stata selezionata l'opzione **Importa file di configurazione BIOS**, ignorare questa operazione.
   - Se nel passaggio precedente è stata selezionata l'opzione **Configurazione BIOS comune**, selezionare uno o più valori correnti e fare clic su **Avanti**.
7. Nella finestra Vista modifiche BIOS, i dati verranno modificati come **mostrato**, **controlla** e **conferma**. Fare clic su **Avanti**.
8. Nella finestra Esporta configurazione BIOS, esportare la configurazione come file. Specificare il percorso del file esportato e fare clic su **Avanti**.
9. Nella finestra Configurazione in esecuzione, selezionare **Riavvia manualmente** o **Riavvia immediatamente** e fare clic su **Avvia**. Al termine dell'attività, fare clic su **Avanti**.
10. Nella finestra Fine, fare clic su **Visualizza log** per controllare il log di configurazione e fare clic su **Chiudi** per uscire.

Raccolta dei log per un server remoto

L'applicazione UpdateXpress supporta la raccolta dei log per un server remoto.

Prerequisito:

La funzione di raccolta multipla per un server remoto è supportata solo sui server ThinkServer/WenTian. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per raccogliere i log, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non desiderano controllare il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Accetta il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Raccogli log** e fare clic su **Avanti**.
5. Nella finestra Modalità di raccolta log, selezionare **Raccogli log BMC** o **Raccogli log FFDC** o entrambe le opzioni e fare clic su **Avanti**.
6. Nella finestra Risultato raccolta log, controllare i risultati e fare clic su **Avanti**.
7. Nella finestra Fine, fare clic su  per controllare i log dettagliati, quindi selezionare **Chiudi** per uscire.

Aggiornamento di più server remoti dal sito Web

L'applicazione UpdateXpress supporta l'aggiornamento dei server remoti in batch dal sito Web.

Nota: Per aggiornare il singolo server remoto dal sito Web, consultare "Aggiornamento di un server remoto dal sito Web" a pagina 12.

Prerequisito:

La funzione di multi-aggiornamento per i server remoti è supportata solo nei server ThinkServer e WenTian. Per dettagli sui server supportati, vedere "Modelli di server supportati" a pagina 5.

Per aggiornare più server remoti dal sito Web, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestione multi-server** e fare clic su **Avanti**.
4. Nella finestra Gestione multi server, selezionare **Aggiungi nuovi server nel pool di server**, effettuare una o più operazioni tra le seguenti, quindi fare clic su **Avanti**.
   - Per aggiungere nuovi server nel pool di server, immettere l'intervallo di indirizzi IP e fare clic su **Rileva** nell'area informazioni BMC e selezionare uno o più server di destinazione dall'elenco Pool di server.
   - Per rimuovere il server dall'elenco Pool di server, selezionare uno o più server di destinazione e fare clic su **Rimuovi elementi selezionati**.
   - Per verificare se il nome utente e la password sono corretti per il server, selezionare uno o più server di destinazione e fare clic su **Esegui scansione selezionata**.
   - Per utilizzare le credenziali BMC comuni per la gestione, selezionare **Utilizza credenziali BMC comuni per la gestione**, immettere nome utente e password.
   - Per esportare l'elenco Pool di server del server corrente, fare clic su **Esporta**. L'elenco dei pool di server verrà salvato nel file `configure.json`.
   - Per importare l'elenco Pool di server nell'altro server, fare clic su **Importa** e selezionare il file `configure.json` di destinazione.
5. Fare clic su **Avanti** per visualizzare un messaggio che richiede agli utenti di confermare l'aggiornamento del certificato. Fare clic su **Accetto** per aggiornare il certificato.

   Nota: Se gli utenti accedono per la prima volta o la password è scaduta, modificare la password nella finestra Modifica password.

6. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
7. Nella finestra Impostazione aggiornamento selezionare una o più opzioni. Se è selezionata l'opzione **Utilizza un server remoto separato invece del server BMC**, immettere le seguenti informazioni:
   - **Nome host o indirizzo IP** (Impostazione HTTPS/FTP): il nome host o l'indirizzo IP del server.
   - **Nome utente** (Impostazione HTTPS/FTP): il nome utente del server.
   - **Password** (Impostazione HTTPS/FTP): la password del server.
   - **Porta** (Impostazione HTTPS/FTP): il numero di porta del server. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.
   - **Directory** (Impostazione HTTPS/FTP): la posizione sul server in cui vengono copiati i pacchetti di aggiornamento.

     Nota: Immettere un percorso completo sul server HTTPS/FTP. Il server FTP viene utilizzato solo per ThinkServer contrassegnato con apice 2 (nota 2) in "Modelli di server supportati" a pagina 5.
8. Per configurare l'impronta digitale della chiave del server HTTPS, effettuare una delle seguenti operazioni:
   - Per verificare l'impronta digitale della chiave del server HTTPS, fare clic su **Sì**.
   - Per non verificare l'impronta digitale della chiave del server HTTPS, selezionare **Ignora impronta digitale chiave del server HTTPS** e fare clic su **Avanti**.
9. Nella finestra Posizione aggiornamenti selezionare **Controlla il sito Web del Supporto Lenovo** e fare clic su **Avanti**.
10. Nella finestra Directory di destinazione, specificare la posizione in cui scaricare gli aggiornamenti o accettare la posizione predefinita e fare clic su **Avanti**.
11. Nella pagina Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
    Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, configurare i campi **Server proxy** e/o **Configurazione di sicurezza URL personalizzata**, a seconda dei requisiti di sicurezza, come segue:
    - **Server proxy**
      a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

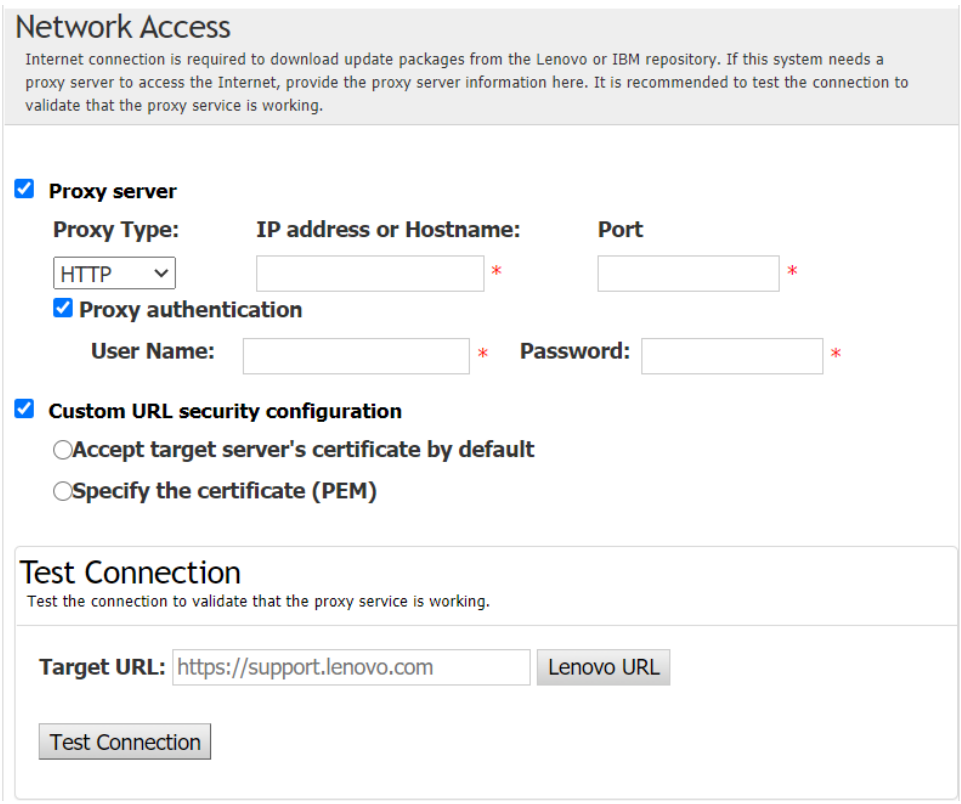
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

      b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

    - **Configurazione di sicurezza URL personalizzata**

      Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
      – **Accetta il certificato del server di destinazione per impostazione predefinita**
      – **Specifica il certificato (PEM)**



12. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
13. Nella finestra Suggerimenti per l'aggiornamento, fare clic su **Inizia** per confrontare la versione del firmware con quella più recente. Una volta completato l'avanzamento, selezionare uno o più pacchetti di destinazione che si desidera aggiornare e fare clic su **Avanti**.

    Nota: Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti senza adattatori rilevati** prima di fare clic su **Inizia**.
14. Nella finestra Ottenere gli aggiornamenti, nella tabella di acquisizione viene visualizzato l'avanzamento dell'acquisizione dei pacchetti. Una volta completato il processo, fare clic su **Avanti**.
15. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.
16. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Aggiornamento di più server remoti da una directory locale

L'applicazione UpdateXpress supporta l'aggiornamento dei server remoti in batch da una cartella locale.

Nota: Per aggiornare il singolo server remoto da una cartella locale, consultare "Aggiornamento di un server remoto da una directory locale" a pagina 14.

Prerequisito:

La funzione di multi-aggiornamento per i server remoti è supportata solo nei server ThinkServer e WenTian. Per dettagli sui server supportati, vedere "Modelli di server supportati" a pagina 5.

Per aggiornare più server remoti da una directory locale, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.

2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestione multi-server** e fare clic su **Avanti**.
4. Nella finestra Gestione multi server, selezionare **Aggiungi nuovi server nel pool di server**, effettuare una o più operazioni tra le seguenti, quindi fare clic su **Avanti**.
   - Per aggiungere nuovi server nel pool di server, immettere l'intervallo di indirizzi IP e fare clic su **Rileva** nell'area informazioni BMC e selezionare uno o più server di destinazione dall'elenco Pool di server.
   - Per rimuovere il server dall'elenco Pool di server, selezionare uno o più server di destinazione e fare clic su **Rimuovi elementi selezionati**.
   - Per verificare se il nome utente e la password sono corretti per il server, selezionare uno o più server di destinazione e fare clic su **Esegui scansione selezionata**.
   - Per utilizzare le credenziali BMC comuni per la gestione, selezionare **Utilizza credenziali BMC comuni per la gestione**, immettere nome utente e password.
   - Per esportare l'elenco Pool di server del server corrente, fare clic su **Esporta**. L'elenco dei pool di server verrà salvato nel file `configure.json`.
   - Per importare l'elenco Pool di server nell'altro server, fare clic su **Importa** e selezionare il file `configure.json` di destinazione.
5. Fare clic su **Avanti** per visualizzare un messaggio che richiede agli utenti di confermare l'aggiornamento del certificato. Fare clic su **Accetto** per aggiornare il certificato.

   Nota: Se gli utenti accedono per la prima volta o la password è scaduta, modificare la password nella finestra Modifica password.
6. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
7. Nella finestra Impostazione aggiornamento selezionare una o più opzioni. Se è selezionata l'opzione **Utilizza un server remoto separato invece del server BMC**, immettere le seguenti informazioni:
   - **Nome host o indirizzo IP** (Impostazione HTTPS/FTP): il nome host o l'indirizzo IP del server.
   - **Nome utente** (Impostazione HTTPS/FTP): il nome utente del server.
   - **Password** (Impostazione HTTPS/FTP): la password del server.
   - **Porta** (Impostazione HTTPS/FTP): il numero di porta del server. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.
   - **Directory** (Impostazione HTTPS/FTP): la posizione sul server in cui vengono copiati i pacchetti di aggiornamento.

     Nota: Immettere un percorso completo sul server HTTPS/FTP. Il server FTP viene utilizzato solo per ThinkServer contrassegnato con apice 2 (nota 2) in "Modelli di server supportati" a pagina 5.
8. Nella finestra Posizione aggiornamenti selezionare **Cerca nella directory locale**. Per specificare una cartella locale, effettuare una delle seguenti operazioni:
   - Fare clic su **Sfoglia**, selezionare la cartella desiderata e fare clic su **Avanti**.
   - Immettere il percorso della cartella nel campo accanto al pulsante **Sfoglia** e fare clic su **Avanti**.
9. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
10. Nella finestra Suggerimenti per l'aggiornamento, fare clic su **Inizia** per confrontare la versione del firmware installato con quella più recente. Una volta completato l'avanzamento, selezionare uno o più pacchetti di destinazione che si desidera aggiornare e fare clic su **Avanti**.

    Nota: Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti senza adattatori rilevati** prima di fare clic su **Inizia**.
11. Nella finestra Esecuzione aggiornamento, fare clic su **Inizia aggiornamento e conferma per continuare alla finestra popup**. La tabella "Esecuzione" visualizza l'avanzamento dell'aggiornamento dei pacchetti. Una volta completato l'aggiornamento, fare clic su **Avanti**.
12. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Configurazione del BIOS per più server remoti

L'applicazione UpdateXpress supporta la configurazione delle impostazioni BIOS per più server remoti in batch.

Prerequisito:

La funzione di configurazione multipla per il server remoto è supportata solo nei server ThinkServer/WenTian. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per configurare il BIOS, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestione multi-server** e fare clic su **Avanti**.
4. Nella finestra Gestione multi server, selezionare **Aggiungi nuovi server nel pool di server**, effettuare una o più operazioni tra le seguenti, quindi fare clic su **Avanti**.
   - Per aggiungere nuovi server nel pool di server, immettere l'intervallo di indirizzi IP e fare clic su **Rileva** nell'area informazioni BMC e selezionare uno o più server di destinazione dall'elenco Pool di server.
   - Per rimuovere il server dall'elenco Pool di server, selezionare uno o più server di destinazione e fare clic su **Rimuovi elementi selezionati**.
   - Per verificare se il nome utente e la password sono corretti per il server, selezionare uno o più server di destinazione e fare clic su **Esegui scansione selezionata**.
   - Per utilizzare le credenziali BMC comuni per la gestione, selezionare **Utilizza credenziali BMC comuni per la gestione**, immettere nome utente e password.
   - Per esportare l'elenco Pool di server del server corrente, fare clic su **Esporta**. L'elenco dei pool di server verrà salvato nel file `configure.json`.
   - Per importare l'elenco Pool di server nell'altro server, fare clic su **Importa** e selezionare il file `configure.json` di destinazione.
5. Fare clic su **Avanti** per visualizzare un messaggio che richiede agli utenti di confermare l'aggiornamento del certificato. Fare clic su **Accetto** per aggiornare il certificato.

   Nota: Se gli utenti accedono per la prima volta o la password è scaduta, modificare la password nella finestra Modifica password.
6. Nella finestra Attività selezionare **Configurazione BIOS** e fare clic su **Avanti**.

   Nota: Questa funzione di configurazione del BIOS è supportata solo nei server con gli stessi tipi di macchina.
7. Nella finestra Modalità di configurazione, selezionare **Configurazione BIOS comune** o **Importa file di configurazione BIOS** e fare clic su **Avanti**.
8. Effettuare una delle seguenti operazioni:
   - Se nel passaggio precedente è stata selezionata l'opzione **Importa file di configurazione BIOS**, ignorare questa operazione.
   - Se nel passaggio precedente è stata selezionata l'opzione **Configurazione BIOS comune**, selezionare uno o più valori correnti e fare clic su **Avanti**.
9. Nella finestra Vista modifiche BIOS, confermare le impostazioni del BIOS modificate e fare clic su **Avanti**.
10. Nella finestra Esporta configurazione BIOS, esportare la configurazione come file. Specificare il percorso del file esportato e fare clic su **Avanti**.
11. Nella finestra Configurazione in esecuzione, selezionare **Riavvia manualmente** o **Riavvia immediatamente** e fare clic su **Avvia**. Al termine dell'attività, fare clic su **Avanti**.
12. Nella finestra Fine, fare clic su **Visualizza log** per controllare il log di configurazione e fare clic su **Chiudi** per uscire.

Raccolta dei log per più server remoti

L'applicazione UpdateXpress supporta la raccolta dei log dei server remoti in batch.

Prerequisito:

La funzione di raccolta multipla per il server remoto è supportata solo nei server ThinkServer/WenTian. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per raccogliere i log, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestione multi-server** e fare clic su **Avanti**.
4. Nella finestra Gestione multi server, selezionare **Aggiungi nuovi server nel pool di server**, effettuare una o più operazioni tra le seguenti, quindi fare clic su **Avanti**.
   - Per aggiungere nuovi server nel pool di server, immettere l'intervallo di indirizzi IP e fare clic su **Rileva** nell'area informazioni BMC e selezionare uno o più server di destinazione dall'elenco Pool di server.
   - Per rimuovere il server dall'elenco Pool di server, selezionare uno o più server di destinazione e fare clic su **Rimuovi elementi selezionati**.
   - Per verificare se il nome utente e la password sono corretti per il server, selezionare uno o più server di destinazione e fare clic su **Esegui scansione selezionata**.
   - Per utilizzare le credenziali BMC comuni per la gestione, selezionare **Utilizza credenziali BMC comuni per la gestione**, immettere nome utente e password.
   - Per esportare l'elenco Pool di server del server corrente, fare clic su **Esporta**. L'elenco dei pool di server verrà salvato nel file `configure.json`.
   - Per importare l'elenco Pool di server nell'altro server, fare clic su **Importa** e selezionare il file `configure.json` di destinazione.
5. Fare clic su **Avanti** per visualizzare un messaggio che richiede agli utenti di confermare l'aggiornamento del certificato. Fare clic su **Accetto** per aggiornare il certificato.

   Nota: Se gli utenti accedono per la prima volta o la password è scaduta, modificare la password nella finestra Modifica password.
6. Nella finestra Attività selezionare **Raccogli log** e fare clic su **Avanti**.
7. Nella finestra Modalità di raccolta log, selezionare **Raccogli log BMC** o **Raccogli log FFDC** o entrambe le opzioni, specificare la directory di output del log e fare clic su **Avanti**.
8. Nella finestra Risultato raccolta log, controllare i risultati e fare clic su **Avanti**.
9. Nella finestra Fine, fare clic su  per controllare il log di configurazione, quindi selezionare **Chiudi** per uscire.

Creazione di un repository di aggiornamenti

L'applicazione UpdateXpress consente di creare un repository di pacchetti UXSP o di aggiornamenti individuali acquisiti dal sito Web.

Per completare questa attività sono necessari i seguenti prerequisiti:
- L'applicazione UpdateXpress deve essere in esecuzione sulla macchina dove verrà creato il repository.
- La macchina deve eseguire un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per creare un repository di aggiornamento, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.

3. Nella finestra Server di destinazione, selezionare **Crea un repository di aggiornamenti** e fare clic su **Avanti**.
4. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
   - Selezionare **Applicazione UpdateXpress System Packs (UXSPs)** per aggiornare UXSP. La finestra Selezione aggiornamenti viene ignorata se si seleziona **UpdateXpress System Packs (UXSPs)**, ma vengono scaricati tutti i pacchetti UXSP.
   - Selezionare **Ultimi aggiornamenti individuali disponibili** per aggiornare i singoli pacchetti. Se si seleziona **Ultimi aggiornamenti individuali disponibili** nel passaggio successivo viene visualizzata la finestra Selezione aggiornamenti. Gli utenti devono quindi selezionare i pacchetti di destinazione.
5. Nella pagina Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
   Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, configurare i campi **Server proxy** e/o **Configurazione di sicurezza URL personalizzata**, a seconda dei requisiti di sicurezza, come segue:
   - **Server proxy**
     a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

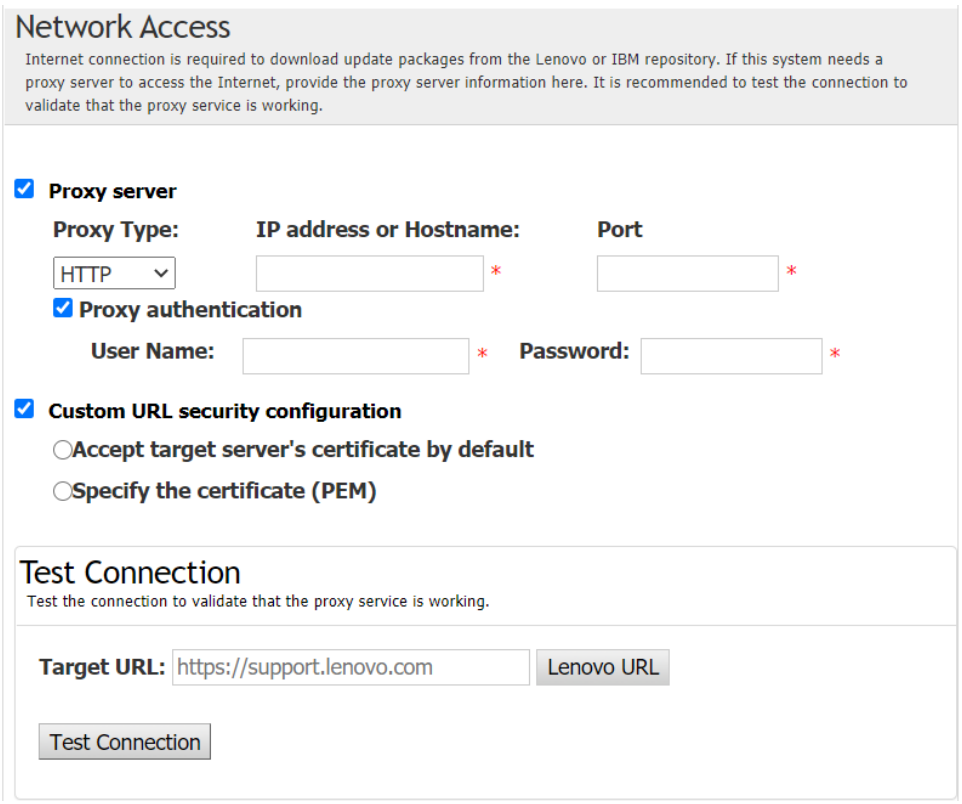
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

     b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

   - **Configurazione di sicurezza URL personalizzata**

     Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
     – **Accetta il certificato del server di destinazione per impostazione predefinita**
     – **Specifica il certificato (PEM)**



6. Nella finestra Tipi di macchina, selezionare i tipi di macchina di destinazione e fare clic su **Avanti**.
   - Per selezionare tutti i tipi di macchina elencati, selezionare la casella di controllo nell'intestazione.
   - Per aggiungere un tipo di macchina, fare clic su **Aggiungi** e specificare il tipo di macchina.
   - Per rimuovere un tipo di macchina, selezionare il tipo di macchina dall'elenco e fare clic su **Rimuovi**.
   - Per aggiornare l'elenco dei tipi di macchina alla versione più recente, fare clic su **Aggiorna elenco**.
   - Per reimpostare l'elenco dei tipi di macchina, fare clic su **Reimposta elenco**.
7. Nella finestra Sistemi operativi, selezionare i sistemi operativi di destinazione per cui si desidera acquisire gli aggiornamenti e fare clic su **Avanti**.
8. Nella finestra Directory di destinazione, specificare la posizione in cui scaricare gli aggiornamenti o accettare la posizione predefinita e fare clic su **Avanti**.
9. (Facoltativo) Selezionare **Ultimi aggiornamenti individuali disponibili** per visualizzare la finestra "Selezione aggiornamenti". Selezionare gli aggiornamenti di destinazione e fare clic su **Avanti**.
10. Nella finestra Ottenere gli aggiornamenti, nella tabella di acquisizione viene visualizzato l'avanzamento dell'acquisizione dei pacchetti. Una volta completato il processo, fare clic su **Avanti**.
11. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Configurazione dell'array RAID per un server remoto

Mediante l'applicazione UpdateXpress è possibile effettuare alcune operazioni di configurazione RAID per un server remoto, come la raccolta di informazioni RAID, la creazione di un array RAID, la configurazione dello stato del disco e la cancellazione della configurazione di un controller.

Prerequisito:

L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per configurare l'array RAID, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**. Quando viene visualizzata una finestra in cui sono presenti le informazioni correlate, fare clic su **OK**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non desiderano controllare il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Accetta il certificato del server BMC e l'impronta digitale della chiave del server SFTP/HTTPS per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività, selezionare **Configurazione RAID remota** o **Esegui aggiornamento sul server di destinazione** oppure scegliere entrambi gli elementi e fare clic su **Avanti**.
5. Nella finestra Configurazione RAID, UpdateXpress raccoglierà prima le informazioni RAID del server remoto. Al termine della raccolta, le informazioni RAID verranno visualizzate nella finestra.
   - Per cancellare la configurazione di un controller fare clic su **Cancella controller**.
   - Per modificare lo stato dell'unità in JBOD, fare clic su **Imposta come JBOD**.
   - Per modificare lo stato dell'unità in Unità valida non configurata fare clic su **Imposta come valida**.
6. Nella finestra Configurazione RAID, per creare un array per il controller, fare clic su **Crea array**.
   a. Nella finestra della procedura guidata, selezionare il livello RAID, aggiungere intervalli, membri e hot-spare per l'array, quindi creare i volumi e impostare i parametri del disco.
   b. Quando vengono visualizzate le informazioni di riepilogo, fare clic su **Crea** per avviare la creazione dell'array di storage.
   c. Al termine del processo, fare clic su **Raccogli** o su **Aggiorna** per raccogliere nuovamente le informazioni RAID.
   d. Fare clic su **Avanti** se non è necessario eseguire altre operazioni.
7. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Esecuzione dell'aggiornamento in fasi per un server remoto

L'applicazione UpdateXpress supporta l'esecuzione di aggiornamenti in più fasi per un server remoto.

Per completare questa attività è necessario il seguente prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per eseguire l'aggiornamento in fasi per un server remoto, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.

4. Nella finestra Attività selezionare **Esegui aggiornamento sul server di destinazione** e fare clic su **Avanti**.
5. Nella finestra Impostazione aggiornamento selezionare una o più opzioni e fare clic su **Avanti**.

   Nota:
   - Se è selezionata l'opzione **Utilizza un server remoto separato invece del server BMC**, immettere le seguenti informazioni:
     - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
     - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
     - (Impostazione) **Password**: la password BMC del sistema di destinazione.
     - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.
     - (Impostazione) **Directory**: percorso completo sul server SFTP. Il file degli aggiornamenti verrà caricato nella stessa directory. Assicurarsi che la directory sia accessibile. Esempio: /payload
   - Per non verificare l'impronta digitale della chiave del server SFTP/HTTPS, selezionare **Ignora impronta digitale chiave del server SFTP**.
6. Nella finestra Posizione aggiornamenti selezionare **Controlla il sito Web del Supporto Lenovo** e fare clic su **Avanti**.
7. Nella finestra Directory di destinazione, specificare la posizione in cui scaricare gli aggiornamenti o accettare la posizione predefinita e fare clic su **Avanti**.
8. Nella pagina Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
   Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, configurare i campi **Server proxy** e/o **Configurazione di sicurezza URL personalizzata**, a seconda dei requisiti di sicurezza, come segue:
   - **Server proxy**
     a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

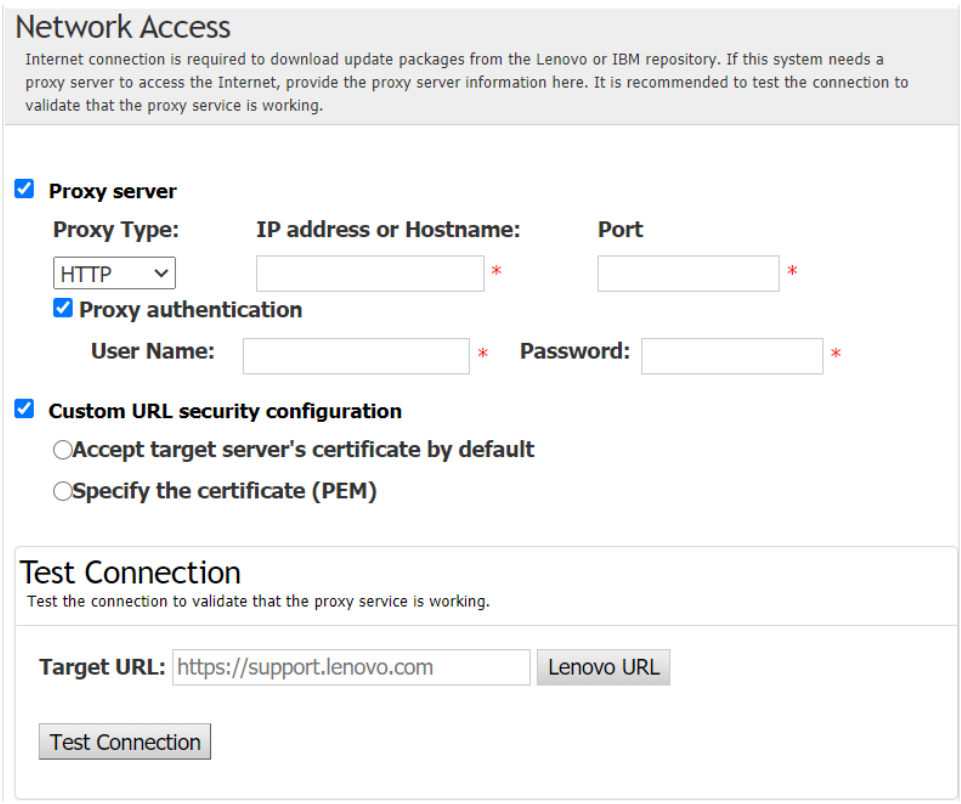
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

     b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

   - **Configurazione di sicurezza URL personalizzata**

     Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
     - **Accetta il certificato del server di destinazione per impostazione predefinita**
     - **Specifica il certificato (PEM)**



9. Nella finestra Tipo di aggiornamento, selezionare il tipo di aggiornamento di destinazione e fare clic su **Avanti**.
10. Nella finestra Suggerimenti per l'aggiornamento effettuare una o più delle seguenti operazioni:
    - Per visualizzare tutti i pacchetti di aggiornamento, selezionare **Mostra aggiornamenti dei dispositivi non rilevati**.
    - Per aggiornare il componente, selezionare il componente di destinazione e fare clic su **Avanti**.
11. Nella finestra Ottenere gli aggiornamenti, nella tabella di acquisizione viene visualizzato l'avanzamento dell'acquisizione dei pacchetti. Una volta completato il processo, fare clic su **Avanti**.
12. Nella finestra Aggiornamenti in esecuzione fare clic su **Inizia aggiornamento → Sì → Avanti**.

    Nota: Per aggiornare il firmware con i pacchetti in bundle, selezionare **Aggiorna firmware con pacchetti in bundle. Questa casella di controllo e le relative opzioni secondarie supportano solo XCC2.** e impostare i tempi di applicazione.
    - **Al riavvio**: consente di aggiornare i pacchetti al successivo riavvio del sistema.
    - **Immediatamente**: consente di aggiornare i pacchetti immediatamente. Il sistema potrebbe essere riavviato immediatamente.
    - **All'inizio della richiesta di aggiornamento**: consente di aggiornare i pacchetti mediante la gestione dell'aggiornamento in fasi o l'esecuzione dei comandi OneCLI.
13. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Gestione dell'aggiornamento in fasi per un server remoto

L'applicazione UpdateXpress supporta l'avvio, l'annullamento e la visualizzazione di tutti gli aggiornamenti in fasi per un server remoto.

Per completare questa attività è necessario il seguente prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.

Per gestire l'aggiornamento in fasi per un server remoto, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Gestisci aggiornamento in fasi** e fare clic su **Avanti**.
5. Nella finestra Gestione attività effettuare una o più delle seguenti operazioni e fare clic su **Avanti**.
   - Per ottenere le informazioni sulle attività, immettere l'ID attività e fare clic su  . L'ID attività verrà compilato automaticamente per l'attività in sospeso.
   - Per avviare l'aggiornamento, fare clic su **Avvia** in corrispondenza dell'attività di destinazione.
   - Per annullare l'aggiornamento, fare clic su **Annulla** in corrispondenza dell'attività di destinazione.
6. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Gestione della chiave di autenticazione SED

I server ThinkEdge forniscono l'accesso all'unità SED (Self-Encrypting Drive) mediante la chiave di autenticazione. L'applicazione UpdateXpress supporta la gestione della chiave di autenticazione SED (AK), inclusi generazione, backup e ripristino.

Prerequisito:

- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- Questa funzione è supportata solo quando il server ThinkEdge è sbloccato. Per le informazioni dettagliate sui server supportati, vedere la serie ThinkEdge in "Modelli di server supportati" a pagina 5.

Per gestire la chiave di autenticazione SED, procedere nel modo seguente:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configura le funzioni di sicurezza sul server ThinkEdge** e fare clic su **Avanti**.
5. Nella finestra Funzioni di sicurezza del server ThinkEdge, selezionare **Gestisci la chiave di autenticazione SED** e fare clic su **Avanti**.
6. Nella finestra Gestione SED AK (Authentication Key), effettuare una o più delle seguenti operazioni:

- Per generare la chiave SED AK, selezionare **Abilita crittografia SED** quando SED AK è disabilitato oppure scegliere **Modifica SED AK**, quando SED AK è abilitato. Selezionare il metodo di destinazione dall'elenco a discesa **Metodo** e fare clic su **Rigenera**.

  Nota: Si consiglia di eseguire il backup della chiave AK in caso di perdita di dati. Gli utenti possono solo selezionare alter opzioni dopo il backup della chiave AK.
- Per eseguire il backup del SED AK, selezionare **Backup del SED AK**, immettere la posizione e la password del file di backup e fare clic su **Avvio**. UpdateXpress salverà il file di backup contenente le informazioni sul SED AK.
- Per ripristinare la chiave SED AK, selezionare **Ripristino della chiave SED AK** ed effettuare una delle seguenti operazioni:
  - Per eseguire il ripristino utilizzando il file di backup, selezionare **Recupera SED AK dal file di backup** dall'elenco a discesa **Metodo**, fare clic su **Sfoglia** per selezionare il file di backup, immettere la password e selezionare **Avvia ripristino**.
  - Per eseguire il ripristino utilizzando la passphrase, selezionare **Ripristina SED AK utilizzando la passphrase** dall'elenco a discesa **Metodo**, immettere la passphrase e fare clic su **Avvia ripristino**.

7. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Richiesta di server nel portale ThinkShield

La proprietà del server ThinkEdge può essere richiesta in Lenovo ThinkShield Key Vault Portal, quindi UpdateXpress può attivare il server bloccato tramite il portale.

Prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- Questa funzione è supportata solo nei server ThinkEdge. Per le informazioni dettagliate sui server supportati, vedere la serie ThinkEdge in "Modelli di server supportati" a pagina 5.

Per richiedere il server nel portale ThinkShield, effettuare le seguenti operazioni:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configura le funzioni di sicurezza sul server ThinkEdge** e fare clic su **Avanti**.
5. Nella finestra Funzioni di sicurezza di ThinkEdge Server, selezionare **Richiedi server in portale ThinkShield** e fare clic su **Avanti**.
6. Nella finestra Accesso Internet, effettuare una o più delle seguenti operazioni:
   - Se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
   - Se gli utenti riscontrano ulteriori problemi di sicurezza, configurare una o più delle seguenti opzioni e fare clic su **Test della connessione**:

– **Server proxy**: accesso alla rete mediante un proxy HTTP/HTTPS.
  a. Selezionare **Server proxy** e compilare i seguenti campi:

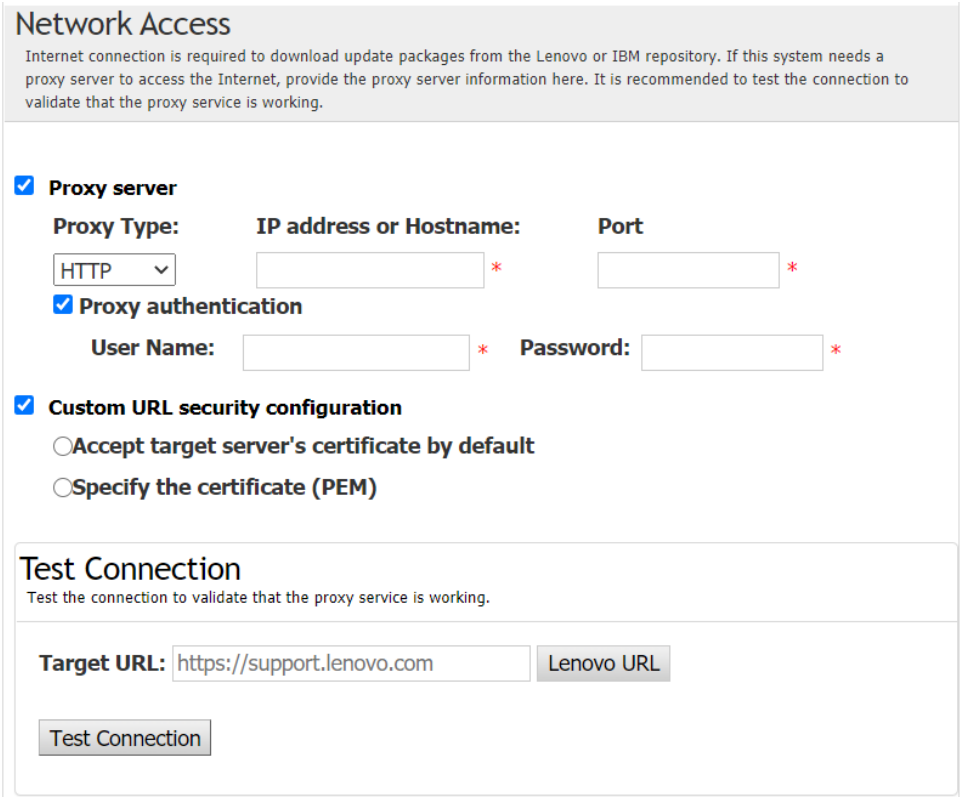
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

  b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

– **Configurazione di sicurezza URL personalizzata**: accesso alla rete con un proxy inverso.

  Selezionare una delle seguenti opzioni:
  – Accetta il certificato del server di destinazione per impostazione predefinita
  – Specifica il certificato (PEM)



7. Nella finestra Richiedi server, immettere l'ID organizzazione, il nome utente e la password di ThinkShield Key Vault Portal, quindi fare clic su **Richiedi**.
8. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Aggiornamento della modalità di controllo del blocco

Il server ThinkEdge è dotato dei sensori di sicurezza per rilevare gli eventi di manomissione, che bloccheranno anche il server in fase di rilevamento. UpdateXpress supporta l'aggiornamento della modalità

di controllo del blocco del server dall'attivazione del server tramite XClarity Controller alla gestione del server tramite il portale ThinkShield.

Prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- Questa funzione è supportata solo nei server ThinkEdge. Per le informazioni dettagliate sui server supportati, vedere la serie ThinkEdge in "Modelli di server supportati" a pagina 5.

Per aggiornare la modalità di controllo del blocco, procedere nel modo seguente:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configura le funzioni di sicurezza sul server ThinkEdge** e fare clic su **Avanti**.
5. Nella finestra Funzioni di sicurezza del server ThinkEdge, selezionare **Controllo di blocco del sistema**, fare clic su **Avanti**, selezionare una delle seguenti opzioni per richiedere o meno la proprietà del server a ThinkShield Key Vault Portal e fare nuovamente clic su **Avanti**.
   - Selezionare **Sì, desidero richiedere il server ora**, andare al passaggio 6.
   - Selezionare **No, desidero procedere senza richiedere il server in ThinkShield Key Vault Portale,** andare al passaggio 8.
6. Nella finestra Accesso Internet, effettuare una o più delle seguenti operazioni:
   - Se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione e fare clic su **Avanti**.
   - Se gli utenti riscontrano ulteriori problemi di sicurezza, configurare una o più delle seguenti opzioni e fare clic su **Test della connessione**:
     – **Server proxy**: accesso alla rete mediante un proxy HTTP/HTTPS.
       a. Selezionare **Server proxy** e compilare i seguenti campi:

Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

       b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

     – **Configurazione di sicurezza URL personalizzata**: accesso alla rete con un proxy inverso.

       Selezionare una delle seguenti opzioni:
       – Accetta il certificato del server di destinazione per impostazione predefinita
       – Specifica il certificato (PEM)

7. Nella finestra Convalida account ThinkShield Portal, immettere l'ID organizzazione, il nome utente e la password di ThinkShield Key Vault Portal, quindi fare clic su **Convalida**. Al termine della verifica, fare clic su **Avanti**.

   Nota: L'immissione di informazioni deve essere valida; in caso contrario, il pulsante **Avanti** *non* verrà abilitato.
8. Nella finestra Controllo del blocco di sistema, immettere manualmente **SÌ** e fare clic su **OK**. Al termine del processo di aggiornamento, fare clic su **Avanti**.
9. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Attivazione del server in modalità di blocco

Il server ThinkEdge è dotato dei sensori di sicurezza per rilevare gli eventi di manomissione, che bloccheranno anche il server in fase di rilevamento. UpdateXpress supporta l'attivazione del server bloccato tramite ThinkShield Key Vault Portal o XClarity Controller.

Prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- Questa funzione è supportata solo nei server ThinkEdge. Per le informazioni dettagliate sui server supportati, vedere la serie ThinkEdge in "Modelli di server supportati" a pagina 5.

Per attivare il server in modalità di blocco, procedere nel modo seguente:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configura le funzioni di sicurezza sul server ThinkEdge** e fare clic su **Avanti**.
5. Nella finestra Funzioni di sicurezza di ThinkEdge Server, selezionare **Attiva server con portale ThinkShield** e fare clic su **Avanti**.

   Nota: Il controllo del blocco di sistema predefinito è gestito da XClarity Controller. Quando il controllo del blocco è gestito dal portale ThinkShield, gli utenti possono attivare il server solo in modalità di blocco dopo essere stati autenticati da ThinkShield Key Vault Portal.
6. Nella finestra Accesso Internet, se non è presente un requisito speciale per l'accesso di sicurezza degli utenti, fare clic su **Test della connessione** per verificare la connessione di rete dell'URL di destinazione, quindi fare clic su **Avanti**.
   Se gli utenti riscontrano ulteriori problemi di sicurezza, prima di fare clic su **Test della connessione**, configurare i campi **Server proxy** e/o **Configurazione di sicurezza URL personalizzata**, a seconda dei requisiti di sicurezza, come segue:
   - **Server proxy**
     a. Selezionare **Server proxy** se gli utenti richiedono un proxy HTTP/HTTPS per connettersi al Web e completare i seguenti campi:

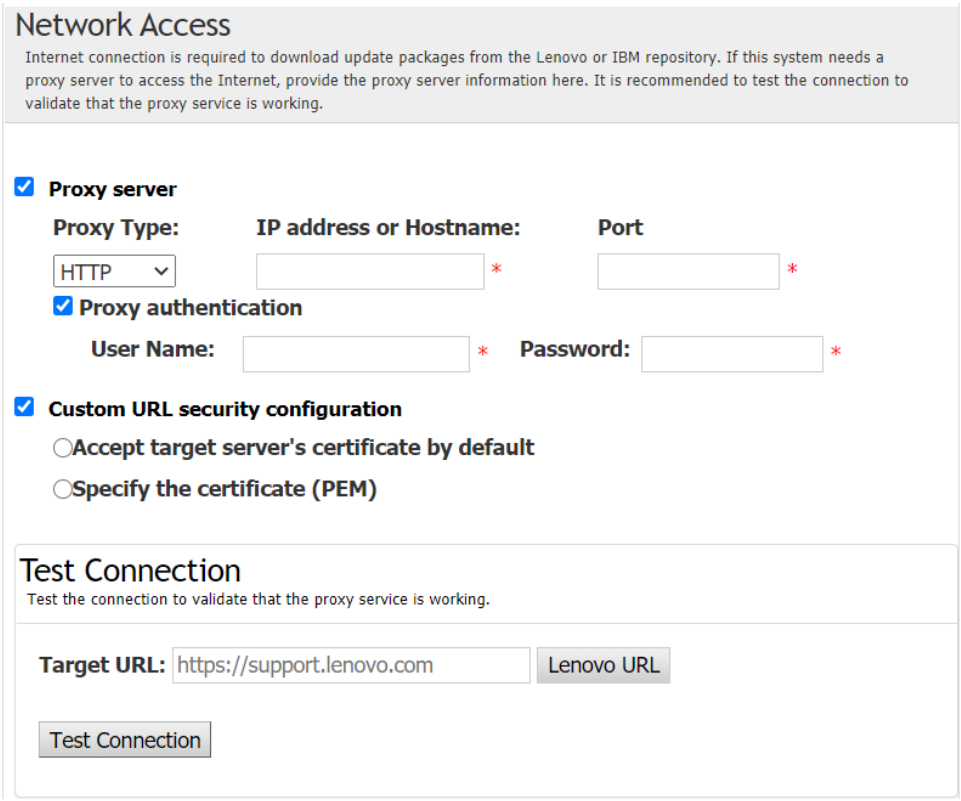
Tipo di proxy	Il tipo di proxy del server proxy.
Indirizzo IP o Nome host	Il nome host, l'indirizzo IP o il nome di dominio del server proxy.
Porta	Il numero di porta del server proxy.

b. Selezionare **Autenticazione proxy** se è necessario specificare le credenziali per eseguire l'autenticazione al server proxy e completare i seguenti campi:

Nome utente	Il nome utente per l'autenticazione con il server proxy.
Password	La password per il nome utente specificato.

- **Configurazione di sicurezza URL personalizzata**

  Selezionare **Configurazione di sicurezza URL personalizzata** se gli utenti richiedono un proxy inverso e selezionare una delle seguenti opzioni:
  - **Accetta il certificato del server di destinazione per impostazione predefinita**
  - **Specifica il certificato (PEM)**



7. Nella finestra Attivato server, immettere l'ID organizzazione, il nome utente e la password di ThinkShield Key Vault Portal, quindi fare clic su **Attivato**. Al termine del processo di attivazione, fare clic su **Avanti**.

   Nota: Se il server è gestito da XClarity Controller, gli utenti *non* devono immettere le informazioni di ThinkShield Key Vault Portal.
8. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Configurazione dei sensori di sicurezza

I server ThinkEdge sono dotati di sensori di sicurezza per rilevare gli eventi di manomissione. UpdateXpress supporta abilitazione, disabilitazione e modifica della soglia del sensore di rilevamento del movimento e del sensore di intrusione dello chassis.

Prerequisito:
- L'applicazione UpdateXpress deve essere in esecuzione su un server installato con un sistema operativo supportato. Per le informazioni dettagliate sui sistemi operativi supportati, vedere "Sistemi operativi supportati" a pagina 6.
- Questa funzione è supportata solo nei server ThinkEdge. Per le informazioni dettagliate sui server supportati, vedere la serie ThinkEdge in "Modelli di server supportati" a pagina 5.

Per configurare i sensori di sicurezza, procedere come segue:
1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Gestisci server remoto**, immettere le seguenti informazioni e fare clic su **Avanti**.
   - (Impostazione) **Nome host o indirizzo IP**: il nome host o l'indirizzo IP BMC del sistema di destinazione.
   - (Impostazione) **Nome utente**: il nome utente BMC del sistema di destinazione.
   - (Impostazione) **Password**: la password BMC del sistema di destinazione.
   - (Impostazione) **Porta**: il numero di porta BMC CIM o RSET. Se gli utenti non specificano alcun valore, verrà utilizzata la porta predefinita.

   Nota: Se gli utenti non devono controllare il certificato del server BMC, selezionare **Accetta certificato server BMC per impostazione predefinita** e fare clic su **Avanti**.
4. Nella finestra Attività selezionare **Configura le funzioni di sicurezza sul server ThinkEdge** e fare clic su **Avanti**.
5. Nella finestra Funzioni di sicurezza del server ThinkEdge selezionare **Configura sensori di sicurezza** e fare clic su **Avanti**.
6. Nella finestra Configura sensori di sicurezza effettuare una o più delle seguenti operazioni e fare clic su **Avanti**.
   - Per abilitare o disabilitare **Rilevamento del movimento** o **Rilevamento intrusione chassis**, selezionare le opzioni dall'elenco a discesa oppure fare clic sull'interruttore per attivare o disattivare lo stato.

     Nota: In caso di perdita di dati, si consiglia di eseguire il backup della chiave AK prima di selezionare qualsiasi elemento.
   - Per reimpostare il contapassi per il rilevamento di movimento, fare clic su **Reimposta contapassi**. UpdateXpress reimposta il numero di passi su 0.
   - Per modificare i passi della soglia per bloccare il rilevamento di movimento, selezionare il livello dei passi di destinazione in **Soglia di blocco**.

     Nota: Il server ThinkEdge verrà bloccato quando il sensore di sicurezza rileva l'evento di manomissione.
7. Nella finestra Fine fare clic su **Visualizza log** per controllare il log dell'aggiornamento, copiare e salvare i comandi generati e fare clic su **Chiudi** per uscire.

Gestione del server in Connessione Ethernet diretta

L'applicazione UpdateXpress supporta la gestione dei server tramite connessione Ethernet diretta. Una volta collegato il cavo di rete, UpdateXpress tenterà di accedere al server BMC mediante le credenziali e l'IP BMC predefiniti.

Per gestire il server in Connessione Ethernet diretta, effettuare le seguenti operazioni:

1. Avviare l'applicazione UpdateXpress. Vedere "Avvio dell'applicazione UpdateXpress" a pagina 9.
2. Nella finestra Benvenuto, fare clic su **Avanti**.
3. Nella finestra Server di destinazione, selezionare **Connessione Ethernet diretta**, immettere le seguenti informazioni e fare clic su **Avanti**.
4. Nella finestra Impostazione connessione Ethernet diretta, effettuare le seguenti operazioni:
   a. Selezionare l'adattatore di destinazione dalla tabella "Scheda di rete disponibile".
   b. Verificare che l'indirizzo IP predefinito sia **192.168.70.125**.
   c. Immettere il nome utente e la password.
   d. Fare clic su **Test della connessione → Avanti** o **Avanti**.
5. Nella finestra Attività, selezionare una delle seguenti opzioni:
   - **Esegui aggiornamento sul server di destinazione**. Per informazioni dettagliate, vedere il passaggio 4 e i passaggi successivi in "Aggiornamento di un server remoto da una directory locale" a pagina 14.
   - **Gestisci aggiornamento in fasi**. Per informazioni dettagliate, vedere il passaggio 4 e i passaggi successivi in "Gestione dell'aggiornamento in fasi per un server remoto" a pagina 27.
   - **Configurazione RAID remota**. Per informazioni dettagliate, vedere il passaggio 4 e i passaggi successivi in "Configurazione dell'array RAID per un server remoto" a pagina 24.
   - **Configurare la funzione di sicurezza del server ThinkEdge**. Per dettagli, vedere il passaggio 4 e i passaggi successivi nelle seguenti sezioni:
     – "Gestione della chiave di autenticazione SED" a pagina 28
     – "Richiesta di server nel portale ThinkShield" a pagina 29
     – "Aggiornamento della modalità di controllo del blocco" a pagina 30
     – "Attivazione del server in modalità di blocco" a pagina 32
     – "Configurazione dei sensori di sicurezza" a pagina 34

Visualizzazione dei comandi OneCLI nella finestra Fine

UpdateXpress esegue gli aggiornamenti richiamando i comandi OneCLI nella procedura guidata GUI. UpdateXpress 2.7.0 e versioni successive visualizzano questi comandi nella casella del nuovo messaggio nella finestra Fine. Gli utenti possono salvare e utilizzare i comandi per richiamare la stessa funzione in modalità CLI.

Esempio di comandi OneCLI:

```
<LXCE OneCLI> update flash --uselocalimg --imm USERID:***@xx.xxx.xxx.xxx --dir
D:\build\Onegui\105980\lnvgy_utl_lxce_uxO1k-2.7.0_windows_i386\workingdir --output
D:\build\Onegui\105980\lnvgy_utl_lxce_uxO1k-2.7.0_windows_i386\Lenovo_Support\ --platform --log 5
```

Capitolo 4. Risoluzione dei problemi

Questo capitolo fornisce informazioni su come procedere in caso si verifichi un problema con l'applicazione UpdateXpress.

Limitazioni e problemi

- **Quando si specifica il certificato per la configurazione personalizzata di sicurezza proxy/URL nel processo di esecuzione di UpdateXpress in Linux, se gli utenti fanno clic su Sfoglia per la seconda volta, la finestra Sfoglia potrebbe non essere visualizzata nell'interfaccia di UpdateXpress.**

  Nella pagina Accesso Internet selezionare **HTTPS** nell'elenco a discesa **Tipo di proxy**, selezionare **Configurazione di sicurezza proxy personalizzata** e **Configurazione di sicurezza URL personalizzata** e fare clic su **Sfoglia…** per specificare il certificato per entrambe le selezioni. Quando gli utenti fanno clic su Sfoglia per la seconda volta, la finestra Sfoglia potrebbe non essere visualizzata.

  Soluzione alternativa: effettuare una o più delle operazioni seguenti.
  - Passare manualmente alla finestra Sfoglia in background.
  - Regolare le dimensioni della finestra per visualizzare la finestra Sfoglia in background.
  - Utilizzare UpdateXpress su Windows.
- **UpdateXpress non riesce a impostare il driver non aggiornato come predefinito in alcuni dispositivi, quando si esegue l'aggiornamento da un driver incluso a uno esterno.**

  UpdateXpress richiama OneCLI per eseguire l'attività di aggiornamento. OneCLI non riesce a confrontare le versioni incoerenti di driver inclusi ed esterni e a selezionare la versione corretta per l'aggiornamento. In questo caso, UpdateXpress non è stato in grado di selezionare il driver esterno per l'aggiornamento e gli utenti devono selezionare manualmente il driver esterno di destinazione per sovrascrivere il driver incluso.
- **Tutti i percorsi UpdateXpress devono utilizzare caratteri alfanumerici standard in lingua inglese.**

  Tutti i percorsi UpdateXpress devono utilizzare caratteri alfanumerici standard in lingua inglese e non devono includere spazi, caratteri speciali o caratteri non in lingua inglese.

Soluzioni alternative

Attualmente non sono presenti soluzioni alternative o problemi noti per l'applicazione UpdateXpress.

Coesistenza e compatibilità

L'applicazione UpdateXpress è basata su OneCLI, ma non interagisce con altri programmi del sistema. Non eseguire contemporaneamente l'applicazione UpdateXpress e OneCLI.

Appendice A. Caratteristiche di accesso facilitato per UpdateXpress

Le funzioni di accesso facilitato consentono agli utenti disabili, ad esempio con mobilità ridotta o problemi visivi, di utilizzare correttamente i prodotti IT.

L'elenco riportato di seguito include le principali funzioni di accesso facilitato dell'applicazione UpdateXpress:
- Utilizzo della sola tastiera
- Interfacce comuni utilizzate dalle utilità per la lettura dello schermo

Navigazione mediante tastiera

Gli utenti possono utilizzare la tastiera per spostarsi tramite l'interfaccia utente grafica.

Le seguenti scelte rapide da tastiera sono applicabili ai sistemi operativi Windows e Linux.

Scelta rapida	Funzione
Tab	Vai al controllo successivo.
Maiusc + Tab	Vai al controllo precedente.
Freccia sinistra	Torna indietro di un carattere.
Freccia destra	Vai avanti di un carattere.
Backspace	Elimina il carattere a sinistra del cursore.
Elimina	Elimina il carattere sotto il cursore.
Freccia su	Sposta lo stato attivo e la selezione verso l'alto tramite il pulsante di scelta.
Freccia giù	Sposta lo stato attivo e la selezione verso il basso tramite il pulsante di scelta.
Spazio	Seleziona o cancella un'opzione.

Tecnologia di lettura dello schermo

Le tecnologie di lettura dello schermo sono basate principalmente sulle interfacce dei programmi software, sulle informazioni della guida e su vari documenti online. Per ulteriori informazioni sulle utilità per la lettura dello schermo, fare riferimento a:
- Utilizzo dell'utilità per la lettura dello schermo JAWS:

  http://www.freedomscientific.com/Products/Blindness/JAWS
- Utilizzo dell'utilità per la lettura dello schermo NVDA:

  http://www.nvaccess.org/

Lenovo e l'accesso facilitato

Per ulteriori informazioni sull'impegno di Lenovo per l'accesso facilitato, visitare il sito Web http://www.lenovo.com/lenovo/us/en/accessibility.html.

Appendice B. Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, servizi o funzioni Lenovo non implicano che la Lenovo intenda renderli disponibili in tutti i paesi in cui opera. Consultare il proprio rappresentante Lenovo locale per in formazioni sui prodotti e servizi disponibili nel proprio paese.

Qualsiasi riferimento a un prodotto, programma o servizio Lenovo non implica che debba essere utilizzato esclusivamente quel prodotto, programma o servizio Lenovo. Qualsiasi prodotto, programma o servizio funzionalmente equivalente che non violi alcun diritto di proprietà intellettuale Lenovo può essere utilizzato. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri prodotti, programmi o servizi.

Lenovo può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura di questo documento non implica la concessione di alcuna licenza per questi brevetti. È possibile inviare per iscritto richieste di informazioni sulle licenze a:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO FORNISCE QUESTA PUBBLICAZIONE "COSÌ COM'È" SENZA ALCUN TIPO DI GARANZIA, SIA ESPRESSA SIA IMPLICITA, INCLUSE, MA NON LIMITATE, LE GARANZIE IMPLICITE DI NON VIOLAZIONE, COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcune giurisdizioni non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi la presente dichiarazione potrebbe non essere applicabile all'utente.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. Lenovo si riserva il diritto di apportare miglioramenti e modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

I prodotti descritti in questa documentazione non sono destinati all'utilizzo di applicazioni che potrebbero causare danni a persone. Le informazioni contenute in questa documentazione non influiscono o modificano le specifiche o le garanzie dei prodotti Lenovo. Nessuna parte di questa documentazione rappresenta l'espressione o una licenza implicita fornita nel rispetto dei diritti di proprietà intellettuale di Lenovo o di terze parti. Tutte le informazioni in essa contenute sono state ottenute in ambienti specifici e vengono presentate come illustrazioni. Quindi è possibile che il risultato ottenuto in altri ambienti operativi varii.

Lenovo può utilizzare o distribuire le informazioni fornite dagli utenti secondo le modalità ritenute appropriate, senza incorrere in alcuna obbligazione nei loro confronti.

Tutti i riferimenti ai siti Web non Lenovo contenuti in questa pubblicazione sono forniti per consultazione; per essi Lenovo non fornisce alcuna approvazione. I materiali reperibili presso questi siti non fanno parte del materiale relativo al prodotto Lenovo. L'utilizzo di questi siti Web è a discrezione dell'utente.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Quindi è possibile che il risultato ottenuto in altri ambienti operativi varii significativamente. Alcune misurazioni possono essere state effettuate sul sistemi a livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate mediante estrapolazione. I risultati reali possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il proprio ambiente specifico.

Marchi

LENOVO, FLEX SYSTEM, SYSTEM X e NEXTSCALE SYSTEM sono marchi di Lenovo. Intel e Intel Xeon sono marchi di Intel Corporation negli Stati Uniti e in altri paesi. Internet Explorer, Microsoft e Windows sono marchi del gruppo di società Microsoft. Linux è un marchio registrato di Linus Torvalds. Tutti gli altri marchi sono di proprietà dei rispettivi titolari. © 2024 Lenovo.

Note importanti

La velocità del processore indica la velocità del clock interno del microprocessore; anche altri fattori influenzano le prestazioni dell'applicazione.

Quando si fa riferimento alla memoria del processore, alla memoria reale e virtuale o al volume dei canali, KB indica 1.024 byte, MB indica 1.048.576 byte e GB indica 1.073.741.824 byte.

Quando si fa riferimento alla capacità dell'unità disco fisso o ai volumi di comunicazioni, MB indica 1.000.000 byte e GB indica 1.000.000.000 byte. La capacità totale accessibile all'utente potrebbe variare a seconda degli ambienti operativi.

Lenovo non fornisce garanzie sui prodotti non Lenovo. Il supporto, se presente, per i prodotti non Lenovo viene fornito dalla terza parte e non da Lenovo.

Qualche software potrebbe risultare differente dalla corrispondente versione in commercio (se disponibile) e potrebbe non includere guide per l'utente o la funzionalità completa del programma.

Indice