Lenovo

# Lenovo XClarity Essentials UpdateXpress-Benutzerhandbuch

Version 4.4.0

**Anmerkung**

Bevor Sie diese Dokumentation und die zugehörigen Produkte verwenden, lesen Sie die Informationen unter Anhang B „Hinweise“ auf Seite 41.

Diese Ausgabe bezieht sich auf Lenovo XClarity® Essentials UpdateXpress und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

**24. Ausgabe (Februar 2024)**

# Inhaltsverzeichnis

# Tabellen

# Informationen zu diesem Benutzerhandbuch

Lenovo XClarity Essentials UpdateXpress (nachfolgend als UpdateXpress-Anwendung bezeichnet) ist eine Anwendung, die UpdateXpress System Packs (UXSPs) und einzelne Aktualisierungen auf Ihren Server anwendet. Dieses Benutzerhandbuch enthält Informationen zum Herunterladen und Verwenden der UpdateXpress-Anwendung.

## Zielgruppe für dieses Benutzerhandbuch

Diese Dokumentation richtet sich an Systemadministratoren oder andere Personen mit Verantwortung für die Systemverwaltung, die mit der Wartung von Firmware und Einheitentreibern vertraut sind.

## Konventionen und Terminologien

Absätze, die mit dem Vermerk „Hinweis“, „Wichtig“ oder „Achtung“ in Fettdruck beginnen, haben bestimmte Bedeutungen, um wichtige Informationen hervorzuheben.

**Anmerkung:** Diese Bemerkungen enthalten wichtige Hinweise, Anleitungen und Empfehlungen.

**Wichtig:** Diese Bemerkungen enthalten Informationen oder Empfehlungen, die Benutzerdabei helfen können, unangenehme oder schwierige Situationen zu vermeiden.

**Achtung:** Diese Bemerkungen weisen auf eventuelle Schäden an Programmen, Geräten oder Daten hin. Der Hinweis „Achtung“ wird vor einer Anweisung oder Situation angezeigt, bei der es zu Beschädigungen kommen kann.

Wenn Enutzer in dieser Dokumentation aufgefordert werden, einen Befehl einzugeben, geben Sie den Befehl ein und drücken Sie dann die Eingabetaste.

## Unterstützte Websites

Dieser Abschnitt enthält Webressourcen zur Unterstützung.

- Lenovo XClarity Essentials-Website

  Laden Sie über diese Website mehrere Systemverwaltungstools für ThinkSystem- und System x-Server herunter.
- Lenovo XClarity Essentials UpdateXpress

  Laden Sie über diese Website die UpdateXpress-Anwendung herunter.

Auf den folgenden Websites werden Informationen zu Produktkompatibilität und -support, Garantien und Lizenzen sowie zu verschiedenen technischen Ressourcen bereitgestellt.
- Support für Lenovo Flex System-Produkte und Services
- ServerProven-Website
- Lenovo Bibliothek zu Server-, Speicher- und Netzwerkressourcen

# Kapitel 1. Technische Übersicht

Lenovo XClarity Essentials UpdateXpress (nachfolgend als UpdateXpress-Anwendung bezeichnet) kann zum Abrufen und Anwenden von UpdateXpress System Packs (UXSPs) und einzelne Aktualisierungen auf ein lokales System oder ein fernes System verwendet werden. Die UpdateXpress-Anwendung ruft UpdateXpress System Pack-Aktualisierungspakete (UXSP) und einzelne Aktualisierungen ab und stellt diese bereit. UXSPs enthalten Firmware- und Einheitentreiberaktualisierungen.

Im folgenden Abschnitt werden kurz die vier Hauptfunktionen der UpdateXpress-Anwendung erklärt. Weitere Informationen finden Sie im Abschnitt Kapitel 3 „UpdateXpress-Anwendung verwenden“ auf Seite 9.

**Lokalen Server aktualisieren**
Aktualisieren Sie die lokale Maschine, auf der die UpdateXpress-Anwendung derzeit ausgeführt wird. Der Maschinentyp wird erkannt und die Aktualisierungen werden abgerufen und automatisch angewendet.

**Remoteserver aktualisieren**
Aktualisieren Sie die Remote-Maschine durch den Baseboard Management Controller (BMC), der auf der Maschine ausgeführt wird. Benutzer benötigen einen SFTP-Server, um die Aktualisierungen zur Ziel-Remote-Maschine zu übertragen.

**Repository mit Aktualisierungen erstellen**
Wählen Sie einen oder mehrere Maschinentypen aus, für die Aktualisierungen über die Lenovo Support-Website heruntergeladen werden sollen. Aktualisierungen werden in den angegebenen Ordner heruntergeladen, aber es werden keine Aktualisierungen angewendet. Benutzer können die UpdateXpress-Anwendung später nutzen, um diese Aktualisierungen anzuwenden, indem Sie festlegen, dass Aktualisierungen aus dem von Ihnen angegebenen Ordner statt von der Lenovo Support-Website abgerufen werden sollen.

**Remote-RAID-Konfiguration**
Konfigurieren Sie das RAID-Array mit dem BMC-Service.

## UpdateXpress System Pack (UXSP)

Ein UXSP ist ein auf Integrierbarkeit getestetes Bundle mit Online-Firmware- und Treiberaktualisierungen für Ihre System x- und ThinkSystem-Server. UXSPs werden für die ersten drei Supportjahre halbjährlich und für die letzten drei Supportjahre jährlich veröffentlicht.

UXSPs vereinfachen den Prozess zum Herunterladen und Installieren aller Online-Treiber- und Firmwareaktualisierungen für ein bestimmtes System. UXSPs stellen sicher, dass Benutzer immer mit einem vollständigen und aktuellen Satz an Aktualisierungen arbeiten, die zusammen von Lenovo getestet und paketiert wurden.

UXSPs werden für eine Kombination aus Maschinentyp und Betriebssystem erstellt. Separate UXSPs werden für Windows®-Betriebssysteme und jede Linux-Variante bereitgestellt. Beispielsweise kann es verschiedene UXSPs für einen bestimmten Maschinentyp geben. Es könnte auch eine Aktualisierung für das Windows-Betriebssystem und für jede Linux-Variante geben.

Es gibt auch eine Art Plattform-UXSP, das zur Aktualisierung eines Systems in Form einer Out-of-Band-Aktualisierung verwendet werden kann. Das Plattform-UXSP enthält kein Betriebssystem.

**UXSP-Format**
Ein UXSP wird in einer XML-Datei bereitgestellt. Die Benennungskonvention für ein UXSP weist das folgende Format auf:

lnvgy_utl_uxsp_*version_operatingsystem_arch*.xml
Beispiel: lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml

## Die UXSP-Aktualisierungen mit der UpdateXpress-Anwendung verwenden

Benutzer können die Anwendung UpdateXpress verwenden, um UXSP-Updates auf ihren Computer zu übertragen. Die UpdateXpress-Anwendung inventarisiert die Maschine, auf der die Aktualisierung angewendet wird, fragt eine bestimmte Position für eine Liste anwendbarer Aktualisierungspakete ab, vergleicht den Bestand mit der anwendbaren Aktualisierungsliste, empfiehlt eine Reihe anzuwendender Aktualisierungen und stellt diese Aktualisierungen anschließend auf der Maschine bereit.

So wenden Sie UXSPs über die UpdateXpress-Anwendung an:
1. Laden Sie die UpdateXpress-Anwendung von der Lenovo Support-Website herunter.
2. Führen Sie die UpdateXpress-Anwendung aus. Wählen Sie **Lokale Maschine aktualisieren** oder **Remote-Maschine aktualisieren** aus.
3. Wählen Sie **Lenovo Support-Website überprüfen** aus.
4. Wählen Sie **UpdateXpress application System Packs (UXSPs)** aus.

Benutzer können die Updates auch direkt von der Lenovo Support-Website herunterladen. Denken Sie daran, die Aktualisierungsnutzdaten und die XML-Datei herunterzuladen. Wählen Sie der Einfachheit halber denselben Zielordner für jeden UXSP-Download aus. Benutzer können mehrere Systempakete für verschiedene Rechnertypen in denselben Ordner herunterladen. Wenn Benutzer die UpdateXpress-Anwendung ausführen, erkennt sie den Rechnertyp und verwendet den richtigen Inhalt für diesen Rechnertyp. In einigen Fällen gibt es ggf. gemeinsame Dateien zwischen Systempaketen. Gemeinsame Dateien, die sich bereits im Ordner befinden, werden nicht erneut heruntergeladen. Aus diesem Grund reduziert sich die Gesamt-Downloadzeit.

## Umgang mit UXSP als Bundle

Die UpdateXpress-Anwendung wurde konzipiert, um UXSPs herunterzuladen und anzuwenden. Das UXSP ist eine Sammlung an einzelnen Aktualisierungen, wie durch die UXSP-XML-Datei angegeben.

Wenn Sie die UpdateXpress-Anwendung ausführen, können Sie wählen, ob Sie mit UXSPs oder einzelnen Updates arbeiten möchten. In den meisten Fällen wird empfohlen, mit UXSPs zu arbeiten, aber die Option, auch mit einzelnen Updates zu arbeiten, gibt den Benutzern mehr Flexibilität bei der Auswahl der zu verwendenden Updates.

## Umgang mit Aktualisierungsvoraussetzungen

In diesem Abschnitt wird beschrieben, wie Aktualisierungsvoraussetzungen abgerufen und angewendet werden.

Um Aktualisierungen erfolgreich anzuwenden, müssen alle Voraussetzungen und gleichzeitig zu erfüllenden Voraussetzungen für eine Aktualisierung abgerufen und angewendet werden. Die UpdateXpress-Anwendung prüft automatisch Voraussetzungen und gleichzeitig zu erfüllende Voraussetzungen, ruft diese ab und wendet sie an. Aktualisierungen erfordern häufig, dass Benutzer Vorabdateien anwenden, bevor sie erfolgreich angewendet werden können, oder dass sie Kernpakete einschließen, um das angewandte Update ordnungsgemäß zu verwenden. Zur Vereinfachung des Aktualisierungsprozesses verwendet die UpdateXpress-Anwendung Informationen, die in die Aktualisierungsdatei zur Identifizierung von erforderlichen Paketen für Ihre bestimmten Aktualisierungen einbezogen werden. Die UpdateXpress-Anwendung wendet diese erforderlichen Pakete dann an.

### Erforderliche Dateien

Das von Lenovo bereitgestellte Aktualisierungspaket enthält Informationen dazu, welche erforderlichen Dateien angewendet werden müssen, bevor Benutzer die Aktualisierung erfolgreich anwenden können. Wenn Benutzer eine Aktualisierung angeben, liest die UpdateXpress-Anwendung diese Informationen und ermittelt die erforderlichen Pakete.

Standardmäßig ruft die UpdateXpress-Anwendung die Aktualisierungspakete ab und bewertet diese, um zu bestimmen, ob die erforderlichen Bedingungen erfüllt wurden, und wendet ggf. automatisch die erforderlichen Dateien an, bevor die angegebene Aktualisierung angewendet wird. Benutzer können sich dazu entscheiden, die erforderlichen Dateien nicht anzuwenden. Jedoch kann dies dazu führen, dass die Aktualisierung nicht erfolgreich angewendet wird.

Wenn erforderliche Pakete Voraussetzungen oder gleichzeitig zu erfüllende Voraussetzungen enthalten, werden sie in derselben Art und Weise abgefragt, bewertet und angewendet.

### Gleichzeitig erforderliche Dateien

Bei einigen Aktualisierungen werden gleichzeitig erforderliche Dateien benötigt. Das bedeutet, dass zusätzliche Pakete angewendet werden müssen, um die Aktualisierung erfolgreich abzuschließen. Jedoch müssen diese Pakete nicht vor der von Ihnen angegebenen Aktualisierung angewendet werden.

Die UpdateXpress-Anwendung identifiziert, bewertet bzw. ruft die gleichzeitig erforderlichen Pakete als Teil Ihrer Aktualisierung ab und wendet sie an.

Wenn gleichzeitig erforderliche Pakete Voraussetzungen oder gleichzeitig zu erfüllende Voraussetzungen enthalten, werden sie in derselben Art und Weise abgefragt, bewertet und angewendet.

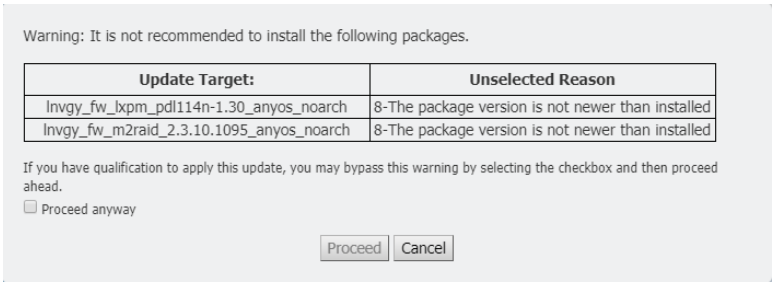
### Beispiel

Ein Beispiel könnte eine Aktualisierung sein, die sowohl Voraussetzungen als auch gleichzeitig zu erfüllende Voraussetzungen enthält. Standardmäßig führt die UpdateXpress-Anwendung die folgenden Schritte aus:

1. Um sicherzustellen, dass die Aktualisierung abgeschlossen ist, lädt die UpdateXpress-Anwendung zunächst die Aktualisierung herunter.
2. Die erforderlichen Dateien werden heruntergeladen.
3. Die gleichzeitig erforderlichen Dateien werden heruntergeladen.
4. Die erforderlichen oder zusätzlich erforderlichen Dateien werden anhand des aktuellen Status des Systems ausgewertet. Wenn das System bereits auf dem erforderlichen Stand ist, da die Voraussetzungen erfüllt wurden, wird die Voraussetzung ignoriert.
5. Die erforderlichen Dateien werden angewendet.
6. Die Aktualisierung wird angewendet.
7. Die gleichzeitig erforderlichen Dateien werden angewendet.

### Update-Empfehlung

Standardmäßig wählt die Anwendung UpdateXpress die Pakete aus, die für das System zur Installation oder Aktualisierung empfohlen werden. Benutzer können diese Pakete auch manuell auswählen, um sie zu installieren oder zu aktualisieren. In diesem Fall erhalten Benutzer eine Warnmeldung, die dieser ähnelt:



Wenn Benutzer diese Meldung sehen, wird empfohlen, den Aktualisierungsvorgang zu stoppen.

## Betriebssystemunabhängige Aktualisierungen

Einige einzelne Aktualisierungen gelten ungeachtet des verwendeten Betriebssystems für einen bestimmten Maschinentyp. Diese einzelnen Aktualisierungen werden als betriebssystemunabhängige Aktualisierungen behandelt. Benutzer können betriebssystemunabhängige Updates auf dieselbe Weise auswählen wie betriebssystemspezifische Updates.

**Anmerkung:** Wenn Benutzer Updates für ein bestimmtes Betriebssystem auswählen, werden betriebssystemunabhängige Updates als Teil des Pakets mitgeliefert. Wählen Sie nur dann betriebssystemunabhängige Updates aus, wenn die Benutzer keine Betriebssystem-Updates für einen Rechnertyp auswählen.

## Fehlende und unvollständige Bestandsdaten

Gelegentlich gilt ein Aktualisierungspaket für eine Komponente, für welche die UpdateXpress-Anwendung nicht die Firmware- oder Treiberversion ermitteln kann. In diesem Fall zeigt die UpdateXpress-Anwendung die Version des Aktualisierungspakets statt der Komponentenversion an. Falls eine installierte Komponentenversion nicht erkannt wird, wird die Aktualisierung nicht standardmäßig ausgewählt. Wählen Sie in diesem Fall das Paket manuell als empfohlene Aktualisierung aus.

## Erforderliche Treiber installieren

Die UpdateXpress-Anwendung installiert erforderliche Einheitentreiber.

Die UpdateXpress-Anwendung installiert in den folgenden Fällen das UXSP in jedem Treiber:
- Der aktuelle Einheitentreiber ist älter als der verfügbare Einheitentreiber im UXSP.
- Die UpdateXpress-Anwendung kann nicht die aktuelle Einheitentreiberversion feststellen. Dieser Fehler tritt in der Regel auf, wenn der Einheitentreiber nicht installiert ist.

  **Anmerkung:** Die UpdateXpress-Anwendung zeigt `Nicht erkannt` an, wenn eine installierte Einheitentreiberversion nicht erkannt wird.

Benutzer können den vollen Nutzen aus diesem Verhalten ziehen, um die folgenden Einheitentreiber zu installieren, die für Firmwareaktualisierungen erforderlich sind:
- Intelligent Peripheral Management Interface (IPMI)
- IPMI Mapping Layer

# Kapitel 2. Hardware- und Softwarevoraussetzungen

Bevor Benutzer die UpdateXpress-Anwendung verwenden, sollten Sie die Anforderungen an die Hardware, das Betriebssystem und die Berechtigungen des lokalen Betriebssystems überprüfen. Systeme, die die UpdateXpress-Anwendung ausführen, benötigen mindestens 1 GB RAM.

## Unterstützte Servermodelle

Die UpdateXpress-Anwendung unterstützt Windows- und Linux-Einheitentreiber und -Firmware, die in den verfügbaren UXSPs enthalten sind. Eine Liste der derzeit unterstützten Einheitentreiber und Firmware für Komponenten finden Sie in der readme-Datei der UpdateXpress-Anwendung, die in jedem Systempaket enthalten ist.

*Tabelle 1. Unterstützte Lenovo Systeme*

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

*Tabelle 1. Unterstützte Lenovo Systeme (Forts.)*

| Serie | Servermodelle | |
|---|---|---|
| WenTian | • WA5480 G3/WA5488 G3 (7DE7)<br>• WR3220 G2/WR3228 G2 (7DEC) | • WR5220 G3/WR5228 G3 (7D8Y) |
| Lösungen | • ThinkAgile VX Serie (7D28, 7D2Z, 7D43, 7DDK, 7Y12, 7Y13, 7Y14, 7Y92, 7Y93, 7Y94, 7Z12, 7Z13, 7Z62, 7Z63)<br>• ThinkAgile MX Series (7D19, 7D1B, 7D1H, 7D5R, 7D5S, 7D5T, 7D66, 7D67, 7D6B, 7DGG, 7Z20) | • ThinkAgile HX Serie (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 | • HX 3310 Einheit (8693)<br>• HX 5510/7510 Einheit (8695)<br>• nx360 M5 (5465, 5467)<br>• x240 Rechenknoten (7162, 2588)<br>• x240 M5 Rechenknoten (2591, 9532)<br>• x280 X6/x480 X6/x880 X6 Compute Node (4258, 7196)[2]<br>• x440 (7167, 2590) | • x3250 M6 (3633, 3943)<br>• x3500 M5 (5464)<br>• x3550 M5 (5463, 8869)<br>• x3650 M5 (5462, 8871)<br>• x3750 M4 (8753)<br>• x3850 X6/x3950 X6 (6241)[2] |
| **Anmerkungen:**<br>1. Dieses Servermodell basiert auf einem AMD One-Socket-Prozessor.<br>2. Dieses Servermodell unterstützt sowohl einzelne als auch mehrere Knoten. | | |

## Unterstützte Betriebssysteme

Die UpdateXpress-Anwendung wird unter Linux- und Windows-Betriebssystemen unterstützt.

## Windows

Die UpdateXpress-Anwendung wird unter 64-Bit-Betriebssystemen unterstützt. Verwenden Sie die Informationen in der folgenden Tabelle, um herauszufinden, welche Betriebssysteme von der UpdateXpress-Anwendung unterstützt werden.

*Tabelle 2. Unterstützte Windows-Betriebssysteme*

| Betriebssystem | Lokal aktualisieren | Remote aktualisieren | Lokales Repository | Remote-RAID-Konfiguration |
|---|---|---|---|---|
| Microsoft Windows 10/11 Pro für Workstations (21H2/22H2) | Ja,[Hinweis] | Ja | Ja | Ja |
| Microsoft Windows Server 2016 | Ja | Ja | Ja | Ja |
| Microsoft Windows Server 2019 | Ja | Ja | Ja | Ja |
| Microsoft Windows Server 2022 | Ja | Ja | Ja | Ja |

**Anmerkung:** Die Servermodelle, die Microsoft Windows 10/11 Pro für Workstations (21H2/22H2) unterstützen, können auch auf die lokale Aktualisierungsfunktion zugreifen.

## Linux

Die UpdateXpress-Anwendung wird unter den folgenden Versionen der Linux-Betriebssysteme unterstützt.

*Tabelle 3. Unterstützte Linux-Betriebssysteme*

| Betriebssystem | Lokal aktualisieren | Remote aktualisieren | Lokales Repository | Remote-RAID-Konfiguration |
|---|---|---|---|---|
| Red Hat Enterprise Linux 7.X (7.6 und spätere Versionen) | Ja | Ja | Ja | Ja |
| Red Hat Enterprise Linux 8.X | Ja | Ja | Ja | Ja |
| Red Hat Enterprise Linux 9.X | Ja | Ja | Ja | Ja |
| SUSE Linux Enterprise Server 15.X | Ja | Ja | Ja | Ja |

**Anmerkungen:**
- 500 MB an freiem Speicherplatz wird bei der Ausführung der UpdateXpress-Anwendung unter einem Linux-Betriebssystem empfohlen.
- Die UpdateXpress-Anwendung unterstützt eine Fuzzy-Überprüfung des Betriebssystems. Wenn das aktuelle Betriebssystem nicht die Firmwarepakete in einem UXSP unterstützt, sind die Firmwarepakete möglicherweise auch im Vergleichsergebnis der UpdateXpress-Anwendung aufgeführt.
- Je nach `ifconfig`-Befehl auf dem Linux-Betriebssystem wird UpdateXpress möglicherweise nicht auf RHEL 7.0 oder neueren Versionen installiert. Um die Firmware auf RHEL 7.0 oder späteren Versionen zu aktualisieren, sollten Sie net-tools installieren.
- Aktualisierungen für Linux-Einheitentreiber erfordern bestimmte Pakete. Die folgenden Pakete müssen installiert sein:
  - Red Hat Enterprise Linux: rpm-build, perl und bash
  - SUSE Enterprise Linux: perl und bash
- In den folgenden Betriebssystemen können Benutzer stattdessen UpdateXpress 4.3.0 verwenden:
  - SUSE 12.5
- In den folgenden Betriebssystemen können Benutzer stattdessen UpdateXpress 4.1.0 verwenden:
  - RedHat 7.5
  - SUSE 12.4
- In den folgenden Betriebssystemen können Benutzer stattdessen UpdateXpress 3.4.0 verwenden:
  - 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

## Betriebssystemberechtigungen

Benutzer brauchen zum Ausführen der UpdateXpress-Anwendung Administrator- oder Root-äquivalente Berechtigungen für das Betriebssystem. Die UpdateXpress-Anwendung gibt einen Fehler zurück, wenn ein Benutzer mit unzureichenden Berechtigungen versucht, das Programm auszuführen.

Speichern Sie die UpdateXpress-Anwendung, einschließlich ihrer Extrahierungen, und alle wichtigen Protokolle an einem sicheren Ort, auf den nur autorisierte Benutzer zugreifen können.

# Kapitel 3. UpdateXpress-Anwendung verwenden

Benutzer können die UpdateXpress-Anwendung verwenden, um Aktualisierungen interaktiv bereitzustellen. Es wird bei der Ausführung der UpdateXpress-Anwendung eine Bildschirmauflösung von 1.024 x 768 oder höher empfohlen. Extrahieren Sie zur Ausführung der UpdateXpress-Anwendung die komprimierte Datei und rufen Sie die ausführbare Datei für Ihr Betriebssystem ab. Es ist keine Installation erforderlich.

**Windows**

Bei einem Windows-Betriebssystem wird die UpdateXpress-Anwendung folgendermaßen bezeichnet:

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

Bei jeder Veröffentlichung der UpdateXpress-Anwendung können Benutzer den Namen der Windows-Zip-Datei durch die Versionsnummer unterscheiden. Die Windows-Zip-Datei wird mit **lnvgy_utl_lxce_ux { build id }_{ version }_windows_i386.zip** angegeben, wobei *lnvgy_utl_lxce_ux* der Name der Zip-Datei ist, *Build-ID* die Build-Nummer ist und *Version* die Versionsnummer der UpdateXpress-Anwendung darstellt.

**Linux**

Bei einem Linux-Betriebssystem wird die UpdateXpress-Anwendung folgendermaßen bezeichnet:

| Betriebssystem | Name der UpdateXpress-Anwendung |
|---|---|
| Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T und höher | `lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz` |
| SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T und höher | `lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz` |

Der Name der UpdateXpress-Anwendung unterscheidet sich bei Windows- und Linux-Betriebssystemen. Der Einfachheit halber wird nachfolgend <*Zipfile*> verwendet, um Bezug auf den Namen der UpdateXpress-Anwendung für Windows- und Linux-Betriebssysteme in dieser Dokumentation zu nehmen.

## UpdateXpress-Anwendung starten

Benutzer können die UpdateXpress-Anwendung verwenden, um die aktuellen UXSPs und einzelne Aktualisierungen abzurufen.

So wird die UpdateXpress-Anwendung gestartet:

- **Unter Windows**:
  1. Extrahieren Sie <*Zipfile*> in einen lokalen Ordner.
  2. Führen Sie einen der folgenden Schritte aus:
     - Doppelklicken Sie auf **lxce_ux.exe**.
     - Klicken Sie mit der rechten Maustaste auf **lxce_ux.exe** und dann im Popup-Menü auf **Als Administrator ausführen**.
- **Unter Linux**:

  Geben Sie die folgenden Befehle im Terminal ein:

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

## Lokalen Server über die Website aktualisieren

Die UpdateXpress-Anwendung kann eine lokale Maschine mit UXSPs oder einzelnen Aktualisierungen aktualisieren, die von der Website abgerufen werden.

Die folgenden Voraussetzungen müssen erfüllt sein, um diese Aufgabe abzuschließen:
- Die UpdateXpress-Anwendung wird auf einer lokalen Maschine ausgeführt, die aktualisiert werden muss.
- Die Maschine führt ein unterstütztes Betriebssystem aus. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

So aktualisieren Sie eine lokale Maschine über die Website:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Lokalen Server verwalten**. Wenn **BMC-Eingangszugriffsinformationen ausgewählt** sind, geben Sie die BMC-Informationen in diesem Fenster ein und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
5. Führen Sie im Fenster Aktualisierungseinstellungen je nach Bedarf eine oder mehrere der folgenden Aktionen aus:
   - Um die Sicherungssystem-Firmware zu aktualisieren, wählen Sie **Nur das Sicherungsimage des BMC (und ggf. UEFI) aktualisieren** aus und klicken Sie auf **Weiter**.
   - Wählen Sie für ein Firmware-Downgrade die Option **Aktualisierung auf veraltete Firmware aktivieren** aus und klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **Lenovo Support-Website überprüfen** aus und klicken Sie auf **Weiter**.
7. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
8. Geben Sie im Fenster Zielverzeichnis den Speicherort an, in den Sie die Aktualisierungen herunterladen möchten, oder akzeptieren Sie den Standardspeicherort und klicken Sie auf **Weiter**.
9. Wenn Sie keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf der Seite Internetzugriff auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
   Wenn Benutzer mehr Sicherheitsbedenken haben, gehen Sie wie folgt vor, bevor Sie auf **Verbindung testen** klicken:
   - Konfigurieren Sie den **Proxy-Server**:
     a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

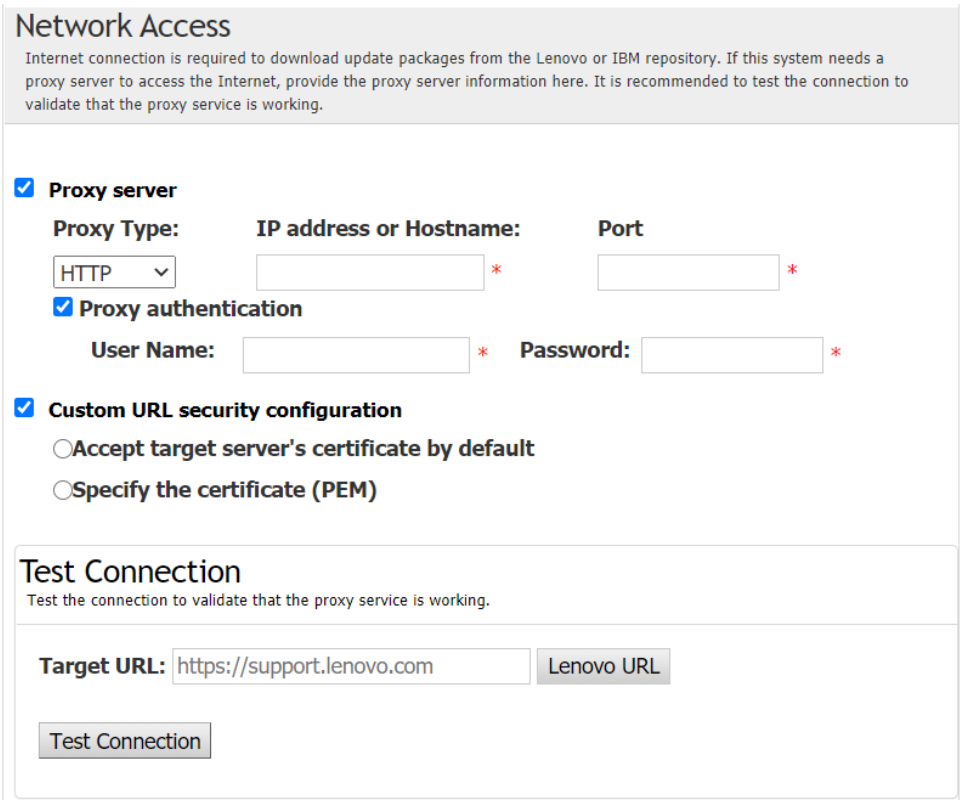
     b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

   - Konfigurieren Sie **Benutzerdefinierte URL-Sicherheitskonfiguration**

     Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
     – **Zertifikat des Zielservers standardmäßig akzeptieren**

– **Zertifikat angeben (PEM)**




10. Führen Sie im Fenster Aktualisierungsempfehlungen je nach Bedarf eine oder mehrere der folgenden Aktionen aus:
    - Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen für nicht erkanntes Gerät anzeigen** aus.
    - Um die Komponente zu aktualisieren, wählen Sie die Zielkomponente aus, und klicken Sie auf **Weiter**.
11. Im Fenster Aktualisierungen abrufen wird in der Abrufungstabelle der Fortschritt der abgerufenen Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
12. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
13. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Upgradeprotokoll zu prüfen, und klicken Sie auf **Schließen**, um das Protokoll zu verlassen.

## Lokalen Server über ein lokales Verzeichnis aktualisieren

Die UpdateXpress-Anwendung kann eine lokale Maschine mit UXSPs oder einzelnen Aktualisierungen aktualisieren, die aus einem lokalen Ordner abgerufen werden.

Die folgenden Voraussetzungen müssen erfüllt sein, um diese Aufgabe abzuschließen:
- Die UpdateXpress-Anwendung wird auf einer lokalen Maschine ausgeführt, die aktualisiert werden muss.
- Die Maschine führt ein unterstütztes Betriebssystem aus. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Das angehängte ISO sollte nicht als gültiges lokales Verzeichnis verwendet werden. Andernfalls könnte es während des Aktualisierungsvorgangs abgehängt werden und einen Flash-Fehler verursachen.

So aktualisieren Sie eine lokale Maschine über ein lokales Verzeichnis:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).

2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Lokalen Server verwalten**, und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
5. Führen Sie im Fenster Aktualisierungseinstellungen je nach Bedarf eine oder mehrere der folgenden Aktionen aus:
   - Um das Sicherungsimage von BMC oder UEFI zu aktualisieren, wählen Sie **Nur das Sicherungsimage des BMC (und ggf. UEFI) aktualisieren** aus und klicken Sie auf **Weiter**.
   - Wählen Sie für ein Firmware-Downgrade die Option **Aktualisierung auf veraltete Firmware aktivieren** aus und klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **In einem lokalen Verzeichnissuchen** aus. So geben Sie einen lokalen Ordner an:
   - Klicken Sie auf **Durchsuchen**, wählen Sie den gewünschten Zielordner aus und klicken Sie dann auf **Weiter**.
   - Geben Sie den Ordnerpfad in das Feld neben der Schaltfläche **Durchsuchen** ein und klicken Sie dann auf **Weiter**.
7. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
8. Führen Sie im Fenster Aktualisierungsempfehlungen je nach Bedarf eine der folgenden Aktionen aus:
   - Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen ohne Adapter anzeigen** aus.
   - Klicken Sie auf **Starten**, um die Versionen des installierten Treibers und der Firmware mit den aktuellen Versionen zu vergleichen. Nachdem der Aktualisierungsfortschritt abgeschlossen ist, wählen Sie ein oder mehrere Zieltpakete aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.
   - Um die Version der im lokalen System installierten Einheiten mit der neuesten Version zu vergleichen, wählen Sie **Nur installierte Einheiten vergleichen** aus und klicken Sie auf **Starten**. Nachdem der Aktualisierungsfortschritt abgeschlossen ist, wählen Sie ein oder mehrere Zieltpakete aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.
9. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
10. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Upgradeprotokoll zu prüfen, und klicken Sie auf **Schließen**, um das Protokoll zu verlassen.

## Remote-Server über die Website aktualisieren

Die UpdateXpress-Anwendung kann eine Remote-Maschine mit UXSPs oder einzelnen Aktualisierungen aktualisieren, die von der Website abgerufen werden.

Die folgende Voraussetzung muss erfüllt sein, um diese Aufgabe abzuschließen:

Die UpdateXpress-Anwendung wird auf einer Maschine ausgeführt, die mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

So aktualisieren Sie eine Remote-Maschine über die Website:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - **(Einstellung) IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - **(Einstellung) Benutzername**: BMC-Benutzername des Zielsystems.
   - **(Einstellung) Passwort**: BMC-Passwort des Zielsystems.

- **(Einstellung) Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

**Anmerkung:** Wenn das BMC-Serverzertifikat nicht überprüft wird, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.

4. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Aktualisierungseinstellungen je nach Bedarf eine oder mehrere der folgenden Optionen aus: Geben Sie die folgenden Informationen ein, wenn **Separaten fernen Server verwenden** ausgewählt ist:
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **IP-Adresse oder Hostname**: IP-Adresse oder Hostname des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Benutzername**: Benutzername des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) Kennwort: **Kennwort** des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Port**: Portnummer des Servers. Ohne Eingabe wird der Standard-Port verwendet.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Verzeichnis**: Der Ort auf dem Server, in den Aktualisierungspakete kopiert werden.

     **Anmerkung:** Geben Sie einen vollständigen Pfad auf dem SFTP/HTTP/HTTPS/FTP-Server ein. Der FTP-Server wird nur für den Server ThinkServer, der in Superscript 2 (Anmerkung 2) markiert ist „Unterstützte Servermodelle“ auf Seite 5.
6. Gehen Sie wie folgt vor, um die Fingerabdrücke des SFTP-Serverschlüssels zu konfigurieren:
   - Klicken Sie auf **Ja**, um die Fingerabdrücke des SFTP-Serverschlüssels zu überprüfen.
   - Wählen Sie den Schlüsselabdruck des SFTP/HTTPS-Serverschlüssels nicht aus, **indem Sie den Schlüsselabdruck des SFTP-Servers** überspringen und auf **Weiter** klicken.
7. Führen Sie einen oder mehrere der folgenden Schritte aus:
   - Wählen Sie für ein Firmware-Downgrade die Option **Aktualisierung auf veraltete Firmware aktivieren** aus und klicken Sie auf **Weiter**.
   - Um die Sicherungssystem-Firmware zu aktualisieren, wählen Sie **Nur das Sicherungsimage des BMC (und ggf. UEFI) aktualisieren** aus und klicken Sie auf **Weiter**.
8. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **Lenovo Support-Website überprüfen** aus und klicken Sie auf **Weiter**.
9. Geben Sie im Fenster Zielverzeichnis den Speicherort an, in den Sie die Aktualisierungen herunterladen möchten, oder akzeptieren Sie den Standardspeicherort und klicken Sie auf **Weiter**.
10. Wenn Sie keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf der Seite Internetzugriff auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
    Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie vor dem Klicken auf **Verbindung testen** den **Proxy-Server** und/oder die **Angepasste URL-Sicherheitskonfiguration** entsprechend Ihren Sicherheitsanforderungen. Gehen Sie dazu wie folgt vor:
    - **Proxy-Server**
      a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

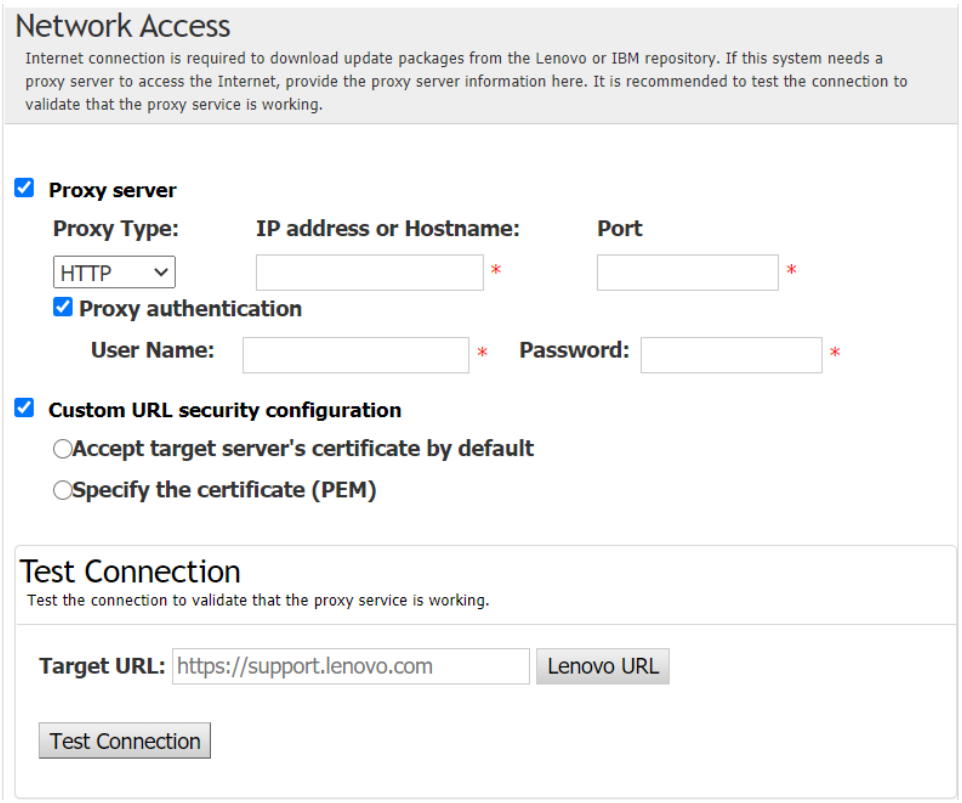
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

      b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

- **Angepasste URL-Sicherheitskonfiguration**

  Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
  - **Zertifikat des Zielservers standardmäßig akzeptieren**
  - **Zertifikat angeben (PEM)**




11. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
12. Führen Sie im Fenster Aktualisierungsempfehlungen je nach Bedarf eine oder mehrere der folgenden Aktionen aus:
    - Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen für nicht erkanntes Gerät anzeigen** aus.
    - Um die Komponente zu aktualisieren, wählen Sie die Zielkomponente aus, und klicken Sie auf **Weiter**.
13. Im Fenster Aktualisierungen abrufen wird in der Abrufungstabelle der Fortschritt der abgerufenen Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
14. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
15. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Remote-Server über ein lokales Verzeichnis aktualisieren

Die UpdateXpress-Anwendung kann eine Remote-Maschine mit UXSPs oder einzelnen Aktualisierungen aktualisieren, die aus einem lokalen Ordner abgerufen werden.

Die folgende Voraussetzung muss erfüllt sein, um diese Aufgabe abzuschließen:

Die UpdateXpress-Anwendung wird auf einer Maschine ausgeführt, die mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

So aktualisieren Sie eine Remote-Maschine über ein lokales Verzeichnis:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Sie das Zertifikat des BMC-Servers und den Schlüsselfingerabdruck des SFTP/HTTPS-Servers nicht prüfen möchten, wählen Sie **BMC-Serverzertifikat und Schlüsselfingerabdruck des SFTP/HTTPS-Servers werden standardmäßig akzeptiert** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
5. Geben Sie im Fenster Aktualisierungseinstellung die folgenden Informationen ein, wenn **Separaten fernen Server verwenden** ausgewählt ist:
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **IP-Adresse oder Hostname**: IP-Adresse oder Hostname des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Benutzername**: Benutzername des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) Kennwort: **Kennwort** des Servers.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Port**: Portnummer des Servers. Ohne Eingabe wird der Standard-Port verwendet.
   - (SFTP/HTTP/HTTPS/FTP-Einstellung) **Verzeichnis**: Der Ort auf dem Server, in den Aktualisierungspakete kopiert werden.

     **Anmerkung:** Geben Sie einen vollständigen Pfad auf dem SFTP/HTTP/HTTPS/FTP-Server ein. Der FTP-Server wird nur für den Server ThinkServer, der in Superscript 2 (Anmerkung 2) markiert ist „Unterstützte Servermodelle“ auf Seite 5.
6. Gehen Sie wie folgt vor, um die Fingerabdrücke des SFTP-Serverschlüssels zu konfigurieren:
   - Klicken Sie auf **Ja**, um die Fingerabdrücke des SFTP-Serverschlüssels zu überprüfen.
   - Wählen Sie den Schlüsselabdruck des SFTP/HTTPS-Serverschlüssels nicht aus, **indem Sie den Schlüsselabdruck des SFTP-Servers** überspringen und auf **Weiter** klicken.
7. Führen Sie einen oder mehrere der folgenden Schritte aus:
   - Wählen Sie für ein Firmware-Downgrade die Option **Aktualisierung auf veraltete Firmware aktivieren** aus und klicken Sie auf **Weiter**.
   - Um die Sicherungssystem-Firmware zu aktualisieren, wählen Sie **Nur das Sicherungsimage des BMC (und ggf. UEFI) aktualisieren** aus und klicken Sie auf **Weiter**.
8. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **In einem lokalen Verzeichnissuchen** aus. So geben Sie einen lokalen Ordner an:
   - Klicken Sie auf **Durchsuchen**, wählen Sie den gewünschten Ordner aus und klicken Sie dann auf **Weiter**.

- Geben Sie den Ordnerpfad in das Feld neben der Schaltfläche **Durchsuchen** ein und klicken Sie dann auf **Weiter**.

9. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
10. Klicken Sie im Fenster Aktualisierungsempfehlung auf **Starten**, um die Version der installierten Firmware mit der aktuellen Version zu vergleichen. Nachdem der Aktualisierungsfortschritt abgeschlossen ist, wählen Sie ein oder mehrere Zieltpakete aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.

    **Anmerkung:** Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen ohne Adapter anzeigen** aus, bevor Sie auf **Starten**.
11. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
12. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## BIOS für einen Remote-Server konfigurieren

Mit der UpdateXpress-Anwendung können Sie die BIOS-Einstellungen für einen Remote-Server konfigurieren.

**Voraussetzung:**

Die BIOS-Konfigurationsfunktion für den Remote-Server wird nur von den ThinkServer/WenTian Servern unterstützt. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie wie folgt vor, um das BIOS zu konfigurieren:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
    - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
    - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
    - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
    - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

    **Anmerkung:** Wenn Sie das Zertifikat des BMC-Servers und den Schlüsselfingerabdruck des SFTP/HTTPS-Servers nicht prüfen möchten, wählen Sie **BMC-Serverzertifikat und Schlüsselfingerabdruck des SFTP/HTTPS-Servers werden standardmäßig akzeptiert** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Aufgabe die Option **BIOS-Konfiguration** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Konfigurationsmodus die Option **Allgemeine BIOS-Konfiguration** oder **BIOS-Konfigurationsdatei importieren** aus und klicken Sie auf **Weiter**.
6. Führen Sie einen der folgenden Schritte aus:
    - Wenn im vorherigen Schritt **BIOS-Konfigurationsdatei importieren** ausgewählt wurde, überspringen Sie diesen Schritt.
    - Wenn im vorherigen Schritt **Allgemeine BIOS-Konfiguration** ausgewählt wurde, wählen Sie einen oder mehrere aktuelle Werte aus und klicken Sie auf **Weiter**.
7. Im Fenster BIOS-Änderungsansicht werden die Daten zu **Angezeigt**, **Überprüfen** und **Bestätigen** geändert. Klicken Sie auf **Weiter**.
8. Exportieren Sie im Fenster BIOS-Konfiguration exportieren die Konfiguration als Datei. Geben Sie den exportierten Speicherort der Datei an und klicken Sie auf **Weiter**.

9. Wählen Sie im Fenster Aktuelle Konfiguration die Option **Manuell neu starten** oder **Sofort neu starten** aus und klicken Sie auf **Starten**. Klicken Sie nach Abschluss der Aufgabe auf **Weiter**.
10. Klicken Sie im Fenster Fertigstellen auf die Option **Protokoll anzeigen**, um das Konfigurationsprotokoll zu überprüfen, und klicken Sie auf **Schließen**, um das Fenster zu verlassen.

## Protokolle für einen Remote-Server erfassen

Die UpdateXpress-Anwendung unterstützt die Erfassung von Protokollen für einen Remote-Server.

**Voraussetzung:**

Die Erfassungsfunktion für einen Remote-Server wird nur von den ThinkServer/WenTian Servern unterstützt. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie wie folgt vor, um Protokolle zu erfassen:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Sie das Zertifikat des BMC-Servers und den Schlüsselfingerabdruck des SFTP/HTTPS-Servers nicht prüfen möchten, wählen Sie **BMC-Serverzertifikat und Schlüsselfingerabdruck des SFTP/HTTPS-Servers werden standardmäßig akzeptiert** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Aufgabe die Option **Protokoll erfassen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Protokollerfassungsmodus die Option **BMC-Protokoll erfassen** oder **FFDC-Protokoll erfassen** oder beide aus und klicken Sie auf **Weiter**.
6. Überprüfen Sie im Fenster Protokollerfassungsergebnis die Ergebnisse und klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster Fertigstellen auf  , um die ausführlichen Protokolle zu überprüfen, und klicken Sie auf **Schließen**, um das Fenster zu verlassen.

## Mehrere Remote-Server über die Website aktualisieren

Die UpdateXpress-Anwendung unterstützt die Stapelaktualisierung der Remote-Server von einer Website aus.

**Anmerkung:** Informationen zur Aktualisierung des einzelnen Remote-Servers über die Website finden Sie unter „Remote-Server über die Website aktualisieren“ auf Seite 12.

**Voraussetzung:**

Die Multiaktualisierungsfunktion für die Remote-Server wird nur auf den ThinkServer-Servern und dem WenUpdate-Server unterstützt. Weitere Informationen zu unterstützten Servern finden Sie unter „Unterstützte Servermodelle“ auf Seite 5.

So aktualisieren Sie mehrere Remote-Server über die Website:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Verwaltung mehrerer Server**, und klicken Sie auf **Weiter**.

4. Führen Sie im Fenster Verwaltung mehrerer Server die Option **Neue Server zum Serverpool hinzufügen**, einen oder mehrere der folgenden Schritte aus, und klicken Sie auf **Weiter**.
   - Um neue Server zum Serverpool hinzuzufügen, geben Sie den IP-Adressbereich ein, und klicken Sie im BMC-Datenbereich auf **Ermitteln**. Wählen Sie aus der Serverpoolliste einen oder mehrere Zielserver aus.
   - Um den Server aus der Liste „Serverpool“ zu entfernen, wählen Sie einen oder mehrere Zielserver aus und klicken Sie auf **Auswahl entfernen**.
   - Um zu überprüfen, ob der Benutzername und das Kennwort für den Server korrekt sind, wählen Sie einen oder mehrere Zielserver aus, und klicken Sie auf **Auswahl scannen**.
   - Um allgemeine BMC-Anmeldeinformationen für die Verwaltung zu verwenden, wählen Sie **Allgemeine BMC-Anmeldeinformationen für die Verwaltung** aus, und geben Sie den Benutzernamen und das Kennwort ein.
   - Klicken Sie **Exportieren**, um die Serverpoolliste des aktuellen Servers zu exportieren. Die Serverpoolliste wird in der Datei `configure.json` gespeichert.
   - Um die Serverpoolliste auf den anderen Server zu importieren, klicken Sie auf **Importieren** und wählen Sie die Zieldatei `configure.json` aus.
5. Wenn Sie auf **Weiter** klicken, wird eine Meldung angezeigt, die den Benutzer daran erinnert, zu bestätigen, ob das Zertifikat aktualisiert werden soll. Klicken Sie auf **Akzeptieren**, um das Zertifikat zu aktualisieren.

   **Anmerkung:** Wenn sich Benutzer zum ersten Mal anmelden oder das Kennwort abgelaufen ist, ändern Sie das Kennwort im Fenster Kennwort ändern.
6. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
7. Wählen Sie im Fenster Aktualisierungseinstellungen je nach Bedarf eine oder mehrere der folgenden Optionen aus: Geben Sie die folgenden Informationen ein, wenn **Separaten fernen Server verwenden** ausgewählt ist:
   - (HTTPS/FTP-Einstellung) **IP-Adresse oder Hostname**: IP-Adresse oder Hostname des Servers.
   - (HTTPS/FTP-Einstellung) **Benutzername**: Benutzername des Servers.
   - (HTTPS/FTP-Einstellung) **Kennwort**: Kennwort des Servers.
   - (HTTPS/FTP-Einstellung) **Port**: Portnummer des Servers. Ohne Eingabe wird der Standard-Port verwendet.
   - (HTTPS/FTP-Einstellung) **Verzeichnis**: Der Ort im Server, in den Aktualisierungspakete kopiert werden.

     **Anmerkung:** Geben Sie einen vollständigen Pfad auf dem HTTPS/FTP-Server ein. Der FTP-Server wird nur für den Server ThinkServer, der in Superscript 2 (Anmerkung 2) markiert ist „Unterstützte Servermodelle“ auf Seite 5.
8. Gehen Sie wie folgt vor, um die Fingerabdrücke des HTTPS-Serverschlüssels zu konfigurieren:
   - Klicken Sie auf **Ja**, um die Fingerabdrücke des HTTPS-Serverschlüssels zu überprüfen.
   - Wählen Sie den Schlüsselabdruck des HTTPS-Serverschlüssels nicht aus, **indem Sie den Schlüsselabdruck des HTTPS-Servers** überspringen und auf **Weiter** klicken.
9. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **Lenovo Support-Website überprüfen** aus und klicken Sie auf **Weiter**.
10. Geben Sie im Fenster Zielverzeichnis den Speicherort an, in den Sie die Aktualisierungen herunterladen möchten, oder akzeptieren Sie den Standardspeicherort und klicken Sie auf **Weiter**.
11. Wenn Sie keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf der Seite Internetzugriff auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
    Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie vor dem Klicken auf **Verbindung testen** den **Proxy-Server** und/oder die **Angepasste URL-Sicherheitskonfiguration** entsprechend Ihren Sicherheitsanforderungen. Gehen Sie dazu wie folgt vor:
    - **Proxy-Server**
      a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

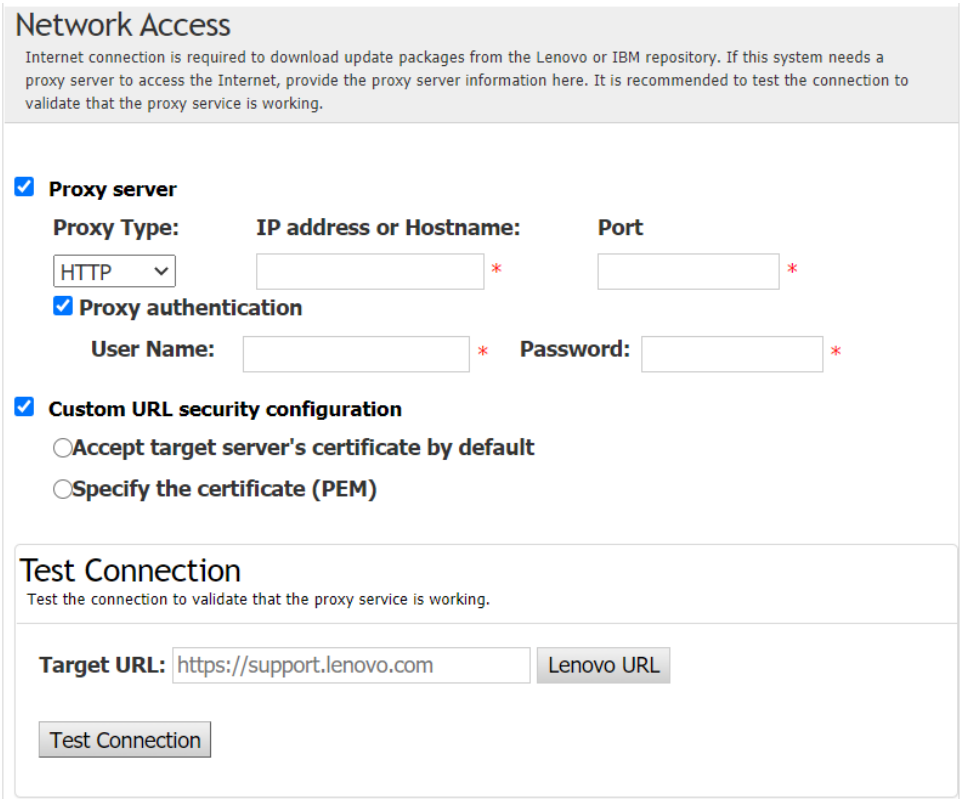
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

- **Angepasste URL-Sicherheitskonfiguration**

  Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
  - **Zertifikat des Zielservers standardmäßig akzeptieren**
  - **Zertifikat angeben (PEM)**




12. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
13. Klicken Sie im Fenster Aktualisierungsempfehlung auf **Starten**, um die Version der Firmware mit der aktuellen Version zu vergleichen. Nachdem der Aktualisierungsfortschritt abgeschlossen ist, wählen Sie ein oder mehrere Zieltpakete aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.

    **Anmerkung:** Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen ohne Adapter anzeigen** aus, bevor Sie auf **Starten**.
14. Im Fenster Aktualisierungen abrufen wird in der Abrufungstabelle der Fortschritt der abgerufenen Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
15. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der

Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.

16. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Mehrere Remote-Server über ein lokales Verzeichnis aktualisieren

Die UpdateXpress-Anwendung unterstützt die Stapelaktualisierung der Remote-Server aus einem lokalen Ordner.

**Anmerkung:** Informationen zur Aktualisierung des einzelnen Remote-Servers aus einem lokalen Ordner finden Sie unter „Remote-Server über ein lokales Verzeichnis aktualisieren“ auf Seite 15.

**Voraussetzung:**

Die Multiaktualisierungsfunktion für die Remote-Server wird nur auf den ThinkServer-Servern und dem WenUpdate-Server unterstützt. Weitere Informationen zu unterstützten Servern finden Sie unter „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie folgendermaßen vor, um mehrere Remote-Server über ein lokales Verzeichnis zu aktualisieren:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Verwaltung mehrerer Server**, und klicken Sie auf **Weiter**.
4. Führen Sie im Fenster Verwaltung mehrerer Server die Option **Neue Server zum Serverpool hinzufügen**, einen oder mehrere der folgenden Schritte aus, und klicken Sie auf **Weiter**.
   - Um neue Server zum Serverpool hinzuzufügen, geben Sie den IP-Adressbereich ein, und klicken Sie im BMC-Datenbereich auf **Ermitteln**. Wählen Sie aus der Serverpoolliste einen oder mehrere Zielserver aus.
   - Um den Server aus der Liste „Serverpool“ zu entfernen, wählen Sie einen oder mehrere Zielserver aus und klicken Sie auf **Auswahl entfernen**.
   - Um zu überprüfen, ob der Benutzername und das Kennwort für den Server korrekt sind, wählen Sie einen oder mehrere Zielserver aus, und klicken Sie auf **Auswahl scannen**.
   - Um allgemeine BMC-Anmeldeinformationen für die Verwaltung zu verwenden, wählen Sie **Allgemeine BMC-Anmeldeinformationen für die Verwaltung** aus, und geben Sie den Benutzernamen und das Kennwort ein.
   - Klicken Sie **Exportieren**, um die Serverpoolliste des aktuellen Servers zu exportieren. Die Serverpoolliste wird in der Datei `configure.json` gespeichert.
   - Um die Serverpoolliste auf den anderen Server zu importieren, klicken Sie auf **Importieren** und wählen Sie die Zieldatei `configure.json` aus.
5. Wenn Sie auf **Weiter** klicken, wird eine Meldung angezeigt, die den Benutzer daran erinnert, zu bestätigen, ob das Zertifikat aktualisiert werden soll. Klicken Sie auf **Akzeptieren**, um das Zertifikat zu aktualisieren.

   **Anmerkung:** Wenn sich Benutzer zum ersten Mal anmelden oder das Kennwort abgelaufen ist, ändern Sie das Kennwort im Fenster Kennwort ändern.
6. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
7. Wählen Sie im Fenster Aktualisierungseinstellungen je nach Bedarf eine oder mehrere der folgenden Optionen aus: Geben Sie die folgenden Informationen ein, wenn **Separaten fernen Server verwenden** ausgewählt ist:
   - (HTTPS/FTP-Einstellung) **IP-Adresse oder Hostname**: IP-Adresse oder Hostname des Servers.
   - (HTTPS/FTP-Einstellung) **Benutzername**: Benutzername des Servers.
   - (HTTPS/FTP-Einstellung) **Kennwort**: Kennwort des Servers.
   - (HTTPS/FTP-Einstellung) **Port**: Portnummer des Servers. Ohne Eingabe wird der Standard-Port verwendet.

- (HTTPS/FTP-Einstellung) **Verzeichnis**: Der Ort im Server, in den Aktualisierungspakete kopiert werden.

  **Anmerkung:** Geben Sie einen vollständigen Pfad auf dem HTTPS/FTP-Server ein. Der FTP-Server wird nur für den Server ThinkServer, der in Superscript 2 (Anmerkung 2) markiert ist „Unterstützte Servermodelle“ auf Seite 5.

8. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **In einem lokalen Verzeichnissuchen** aus. So geben Sie einen lokalen Ordner an:
   - Klicken Sie auf **Durchsuchen**, wählen Sie den gewünschten Ordner aus und klicken Sie dann auf **Weiter**.
   - Geben Sie den Ordnerpfad in das Feld neben der Schaltfläche **Durchsuchen** ein und klicken Sie dann auf **Weiter**.
9. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
10. Klicken Sie im Fenster Aktualisierungsempfehlung auf **Starten**, um die Version der installierten Firmware mit der aktuellen Version zu vergleichen. Nachdem der Aktualisierungsfortschritt abgeschlossen ist, wählen Sie ein oder mehrere Zieltpakete aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.

    **Anmerkung:** Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen ohne Adapter anzeigen** aus, bevor Sie auf **Starten**.
11. Klicken Sie im Fenster Ausführung der Aktualisierung auf **Aktualisierung starten und bestätigen, dass im Popup-Fenster fortgesetzt werden soll**. In der Ausführungstabelle wird der Aktualisierungsfortschritt der Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
12. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## BIOS für mehrere Remote-Server konfigurieren

Mit der UpdateXpress-Anwendung können Sie die BIOS-Einstellungen für mehrere Remote-Server im Batch-Verfahren konfigurieren.

**Voraussetzung:**

Die Mehrfachkonfigurationsfunktion für den Remote-Server wird nur von den ThinkServer/WenTian Servern unterstützt. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie wie folgt vor, um das BIOS zu konfigurieren:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Verwaltung mehrerer Server**, und klicken Sie auf **Weiter**.
4. Führen Sie im Fenster Verwaltung mehrerer Server die Option **Neue Server zum Serverpool hinzufügen**, einen oder mehrere der folgenden Schritte aus, und klicken Sie auf **Weiter**.
   - Um neue Server zum Serverpool hinzuzufügen, geben Sie den IP-Adressbereich ein, und klicken Sie im BMC-Datenbereich auf **Ermitteln**. Wählen Sie aus der Serverpoolliste einen oder mehrere Zielserver aus.
   - Um den Server aus der Liste „Serverpool“ zu entfernen, wählen Sie einen oder mehrere Zielserver aus und klicken Sie auf **Auswahl entfernen**.
   - Um zu überprüfen, ob der Benutzername und das Kennwort für den Server korrekt sind, wählen Sie einen oder mehrere Zielserver aus, und klicken Sie auf **Auswahl scannen**.
   - Um allgemeine BMC-Anmeldeinformationen für die Verwaltung zu verwenden, wählen Sie **Allgemeine BMC-Anmeldeinformationen für die Verwaltung** aus, und geben Sie den Benutzernamen und das Kennwort ein.

- Klicken Sie **Exportieren**, um die Serverpoolliste des aktuellen Servers zu exportieren. Die Serverpoolliste wird in der Datei `configure.json` gespeichert.
- Um die Serverpoolliste auf den anderen Server zu importieren, klicken Sie auf **Importieren** und wählen Sie die Zieldatei `configure.json` aus.

5. Wenn Sie auf **Weiter** klicken, wird eine Meldung angezeigt, die den Benutzer daran erinnert, zu bestätigen, ob das Zertifikat aktualisiert werden soll. Klicken Sie auf **Akzeptieren**, um das Zertifikat zu aktualisieren.

   **Anmerkung:** Wenn sich Benutzer zum ersten Mal anmelden oder das Kennwort abgelaufen ist, ändern Sie das Kennwort im Fenster Kennwort ändern.
6. Wählen Sie im Fenster Aufgabe die Option **BIOS-Konfiguration** aus und klicken Sie auf **Weiter**.

   **Anmerkung:** Diese BIOS-Konfigurationsfunktion wird nur in den Servern mit denselben Maschinentypen unterstützt.
7. Wählen Sie im Fenster Konfigurationsmodus die Option **Allgemeine BIOS-Konfiguration** oder **BIOS-Konfigurationsdatei importieren** aus und klicken Sie auf **Weiter**.
8. Führen Sie einen der folgenden Schritte aus:
   - Wenn im vorherigen Schritt **BIOS-Konfigurationsdatei importieren** ausgewählt wurde, überspringen Sie diesen Schritt.
   - Wenn im vorherigen Schritt **Allgemeine BIOS-Konfiguration** ausgewählt wurde, wählen Sie einen oder mehrere aktuelle Werte aus und klicken Sie auf **Weiter**.
9. Bestätigen Sie im Fenster BIOS-Änderungsansicht die geänderten BIOS-Einstellungen und klicken Sie auf **Weiter**.
10. Exportieren Sie im Fenster BIOS-Konfiguration exportieren die Konfiguration als Datei. Geben Sie den exportierten Speicherort der Datei an und klicken Sie auf **Weiter**.
11. Wählen Sie im Fenster Aktuelle Konfiguration die Option **Manuell neu starten** oder **Sofort neu starten** aus und klicken Sie auf **Starten**. Klicken Sie nach Abschluss der Aufgabe auf **Weiter**.
12. Klicken Sie im Fenster Fertigstellen auf die Option **Protokoll anzeigen**, um das Konfigurationsprotokoll zu überprüfen, und klicken Sie auf **Schließen**, um das Fenster zu verlassen.

## Protokolle für mehrere Remote-Server erfassen

Die UpdateXpress-Anwendung unterstützt die Erfassung von Protokollen für die Remote-Server im Batchformat.

**Voraussetzung:**

Die Mehrfacherfassungsfunktion für den Remote-Server wird nur von den ThinkServer/WenTian Servern unterstützt. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie wie folgt vor, um Protokolle zu erfassen:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Verwaltung mehrerer Server**, und klicken Sie auf **Weiter**.
4. Führen Sie im Fenster Verwaltung mehrerer Server die Option **Neue Server zum Serverpool hinzufügen**, einen oder mehrere der folgenden Schritte aus, und klicken Sie auf **Weiter**.
   - Um neue Server zum Serverpool hinzuzufügen, geben Sie den IP-Adressbereich ein, und klicken Sie im BMC-Datenbereich auf **Ermitteln**. Wählen Sie aus der Serverpoolliste einen oder mehrere Zielserver aus.
   - Um den Server aus der Liste „Serverpool“ zu entfernen, wählen Sie einen oder mehrere Zielserver aus und klicken Sie auf **Auswahl entfernen**.
   - Um zu überprüfen, ob der Benutzername und das Kennwort für den Server korrekt sind, wählen Sie einen oder mehrere Zielserver aus, und klicken Sie auf **Auswahl scannen**.

- Um allgemeine BMC-Anmeldeinformationen für die Verwaltung zu verwenden, wählen Sie **Allgemeine BMC-Anmeldeinformationen für die Verwaltung** aus, und geben Sie den Benutzernamen und das Kennwort ein.
- Klicken Sie **Exportieren**, um die Serverpoolliste des aktuellen Servers zu exportieren. Die Serverpoolliste wird in der Datei `configure.json` gespeichert.
- Um die Serverpoolliste auf den anderen Server zu importieren, klicken Sie auf **Importieren** und wählen Sie die Zieldatei `configure.json` aus.

5. Wenn Sie auf **Weiter** klicken, wird eine Meldung angezeigt, die den Benutzer daran erinnert, zu bestätigen, ob das Zertifikat aktualisiert werden soll. Klicken Sie auf **Akzeptieren**, um das Zertifikat zu aktualisieren.

   **Anmerkung:** Wenn sich Benutzer zum ersten Mal anmelden oder das Kennwort abgelaufen ist, ändern Sie das Kennwort im Fenster Kennwort ändern.
6. Wählen Sie im Fenster Aufgabe die Option **Protokoll erfassen** aus und klicken Sie auf **Weiter**.
7. Wählen Sie im Fenster Protokollerfassungsmodus die Option **BMC-Protokoll erfassen** oder **FFDC-Protokoll erfassen** oder beide aus, geben Sie das Protokollausgabeverzeichnis an und klicken Sie auf **Weiter**.
8. Überprüfen Sie im Fenster Protokollerfassungsergebnis die Ergebnisse und klicken Sie auf **Weiter**.
9. Klicken Sie im Fenster Fertigstellen auf  , um das Konfigurationsprotokoll zu überprüfen, und klicken Sie auf **Schließen**, um das Protokoll zu verlassen.

## Repository mit Aktualisierungen erstellen

Die UpdateXpress-Anwendung kann ein Repository an UXSPs oder einzelnen Aktualisierungen erstellen, die über die Website abgerufen wurden.

Die folgenden Voraussetzungen müssen erfüllt sein, um diese Aufgabe abzuschließen:
- Die UpdateXpress-Anwendung wird auf einer Maschine ausgeführt, auf der das Repository erstellt werden muss.
- Die Maschine führt ein unterstütztes Betriebssystem aus. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie zum Erstellen eines Aktualisierungs-Repository wie folgt vor:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Aktualisierungsaufgabe die **Option Repository mit Aktualisierungen** erstellen aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
   - Wählen Sie **UpdateXpress System Packs (UXSPs)**, um UXSP zu aktualisieren. Das Fenster „Aktualisierungsauswahl“ wird übersprungen, wenn Sie **UpdateXpress System Packs (UXSPs)** auswählen, jedoch werden alle UXSP-Pakete heruntergeladen.
   - Wählen Sie **Neueste verfügbare individuelle Updates** aus, wenn Sie die einzelnen Pakete aktualisieren möchten. Das Fenster „Aktualisierungsauswahl“ wird im folgenden Schritt angezeigt. Wenn Sie **Neueste verfügbare individuelle Updates** auswählen, sollten Sie die Zieltpakete auswählen, die heruntergeladen werden sollen.
5. Wenn Sie keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf der Seite Internetzugriff auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
   Wenn Sie mehr Sicherheitsbedenken haben, konfigurieren Sie vor dem Klicken auf **Verbindung testen** den **Proxy-Server** und/oder die **Angepasste URL-Sicherheitskonfiguration** entsprechend Ihren Sicherheitsanforderungen. Gehen Sie dazu wie folgt vor:
   - **Proxy-Server**

a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

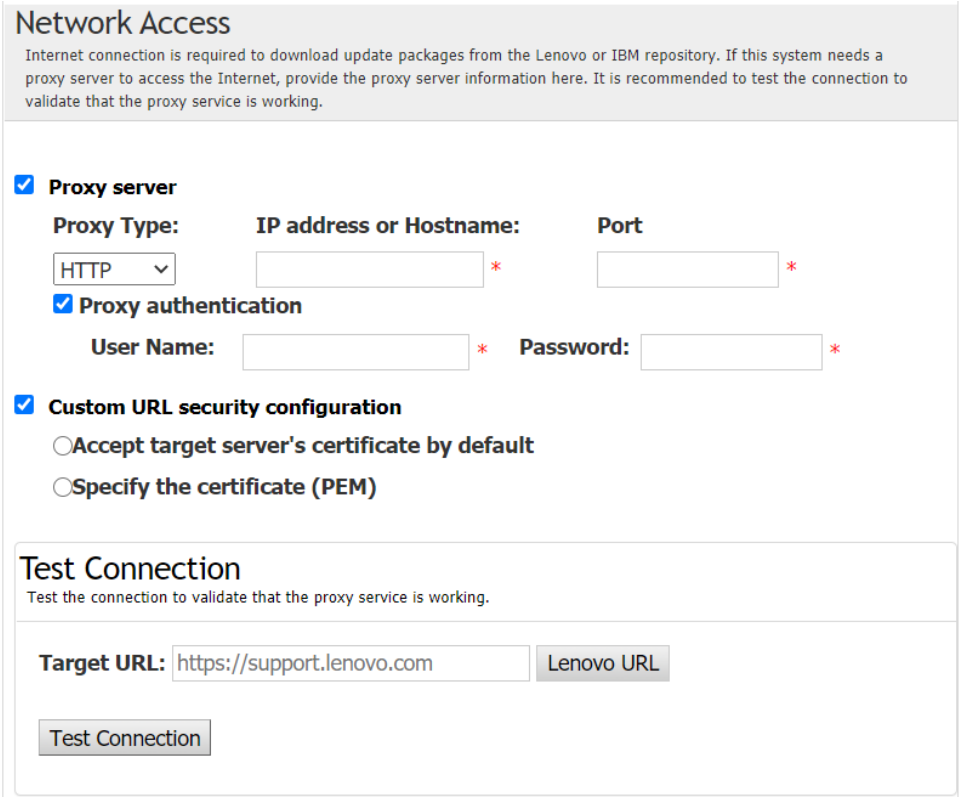
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

- **Angepasste URL-Sicherheitskonfiguration**

  Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
  - **Zertifikat des Zielservers standardmäßig akzeptieren**
  - **Zertifikat angeben (PEM)**




6. Wählen Sie im Fenster Maschinentypen den Zielmaschinentypen aus und klicken Sie auf **Weiter**.
   - Um alle aufgelisteten Maschinentypen auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile.
   - Klicken Sie zum Hinzufügen eines Maschinentyps auf **Hinzufügen** und geben Sie den Maschinentyp an.
   - Um einen Maschinentyp zu entfernen, wählen Sie den Maschinentyp in der Liste aus und klicken Sie auf **Entfernen**.
   - Um die Liste mit Maschinentypen auf die neueste Version zu aktualisieren, klicken Sie auf **Liste aktualisieren**.

- Um die Liste mit Maschinentypen zurückzusetzen, klicken Sie auf **Liste zurücksetzen**.

7. Wählen Sie im Fenster Betriebssysteme die Betriebssysteme aus, für die Sie Aktualisierungen abrufen möchten, und klicken Sie dann auf **Weiter**.
8. Geben Sie im Fenster Zielverzeichnis den Speicherort an, in den Sie die Aktualisierungen herunterladen möchten, oder akzeptieren Sie den Standardspeicherort und klicken Sie auf **Weiter**.
9. (Optional) Wenn Sie **Neueste verfügbare individuelle Updates** auswählen, wird das Fenster „Aktualisierungsauswahl“ angezeigt. Wählen Sie die gewünschten Zieltaktualisierungen aus und klicken Sie auf **Weiter**.
10. Im Fenster Aktualisierungen abrufen wird in der Abrufungstabelle der Fortschritt der abgerufenen Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
11. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## RAID-Array für einen Remote-Server konfigurieren

Die UpdateXpress-Anwendung kann einige RAID-Konfigurationen für einen Remote-Server durchführen, wie z. B. das Erfassen von RAID-Informationen, das Erstellen von RAID-Arrays, das Konfigurieren des Festplattenstatus und das Löschen der Konfiguration eines Controllers.

**Voraussetzung:**

Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie wie folgt vor, um ein RAID-Array zu konfigurieren:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**. Wenn ein Fenster mit den zugehörigen Informationen angezeigt wird, klicken Sie auf **OK**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Sie das Zertifikat des BMC-Servers und den Schlüsselfingerabdruck des SFTP/HTTPS-Servers nicht prüfen möchten, wählen Sie **BMC-Serverzertifikat und Schlüsselfingerabdruck des SFTP/HTTPS-Servers werden standardmäßig akzeptiert** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Remote-RAID-Konfiguration** oder **Aktualisieren auf Zielserver ausführen** oder beide Elemente ausführen aus und klicken Sie auf **Weiter**.
5. Im Fenster RAID-Konfiguration sammelt UpdateXpress zunächst RAID-Informationen des entfernten Servers. Anschließend werden die RAID-Informationen im Fenster angezeigt.
   - Sie können die Konfiguration eines Controllers löschen, indem Sie auf **Controller löschen** klicken.
   - Um den Laufwerkstatus in JBOD zu ändern, klicken Sie auf **Als JBOD festlegen**.
   - Um den Status des Laufwerks auf Unkonfiguriert GUT zu ändern, klicken Sie auf **Als GUT festlegen**.
6. Im Fenster RAID-Konfiguration können Sie ein Array für den Controller erstellen, indem Sie auf **Array erstellen** klicken.
   a. Wählen Sie im Assistenten die RAID-Stufe aus, fügen Sie Spannen, Mitglieder und Hot-Spares für das Array hinzu und erstellen Sie Datenträger und legen Sie Datenträgerparameter fest.
   b. Wenn die Zusammenfassungsinformationen angezeigt werden, klicken Sie auf **Erstellen**, um mit der Erstellung der Speicher-Array zu beginnen.

c. Klicken Sie nach Abschluss des Prozesses auf **Sammeln** oder **Aktualisieren**, um die RAID-Informationen erneut zu sammeln.
d. Klicken Sie auf **Weiter**, falls keine weitere Aktion erforderlich ist.

7. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Durchführen von Stufenaktualisierungen für eine Remote-Server

Die UpdateXpress-Anwendung unterstützt die Ausführung von Stufenaktualisierungen für einen Remote-Server.

Die folgende Voraussetzung muss erfüllt sein, um diese Aufgabe abzuschließen:

- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie folgendermaßen vor, um eine Stufenaktualisierung für einen Remote-Server durchzuführen:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Aktualisierung auf Zielserver durchführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Aktualisierungseinstellungen eine oder mehrere der Optionen aus und klicken Sie auf **Weiter**.

   **Anmerkungen:**
   - Geben Sie die folgenden Informationen ein, wenn **Separaten fernen Server verwenden** ausgewählt ist:
     – (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
     – (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
     – (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
     – (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.
     – (Einstellung) **Verzeichnis**: Vollständiger Pfad auf dem SFTP-Server. Die Aktualisierungsdatei wird in dieses Verzeichnis hochgeladen. Stellen Sie sicher, dass auf das Verzeichnis zugegriffen werden kann. Beispiel: /payload
   - Wählen Sie den Schlüsselabdruck des SFTP/HTTPS-Serverschlüssels nicht aus, indem Sie den **Schlüsselabdruck des SFTP-Servers überspringen**.
6. Wählen Sie im Fenster Speicherort für Aktualisierungen die Option **Lenovo Support-Website überprüfen** aus und klicken Sie auf **Weiter**.
7. Geben Sie im Fenster Zielverzeichnis den Speicherort an, in den Sie die Aktualisierungen herunterladen möchten, oder akzeptieren Sie den Standardspeicherort und klicken Sie auf **Weiter**.
8. Wenn Sie keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf der Seite Internetzugriff auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.

Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie vor dem Klicken auf **Verbindung testen** den **Proxy-Server** und/oder die **Angepasste URL-Sicherheitskonfiguration** entsprechend Ihren Sicherheitsanforderungen. Gehen Sie dazu wie folgt vor:

- **Proxy-Server**
  a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

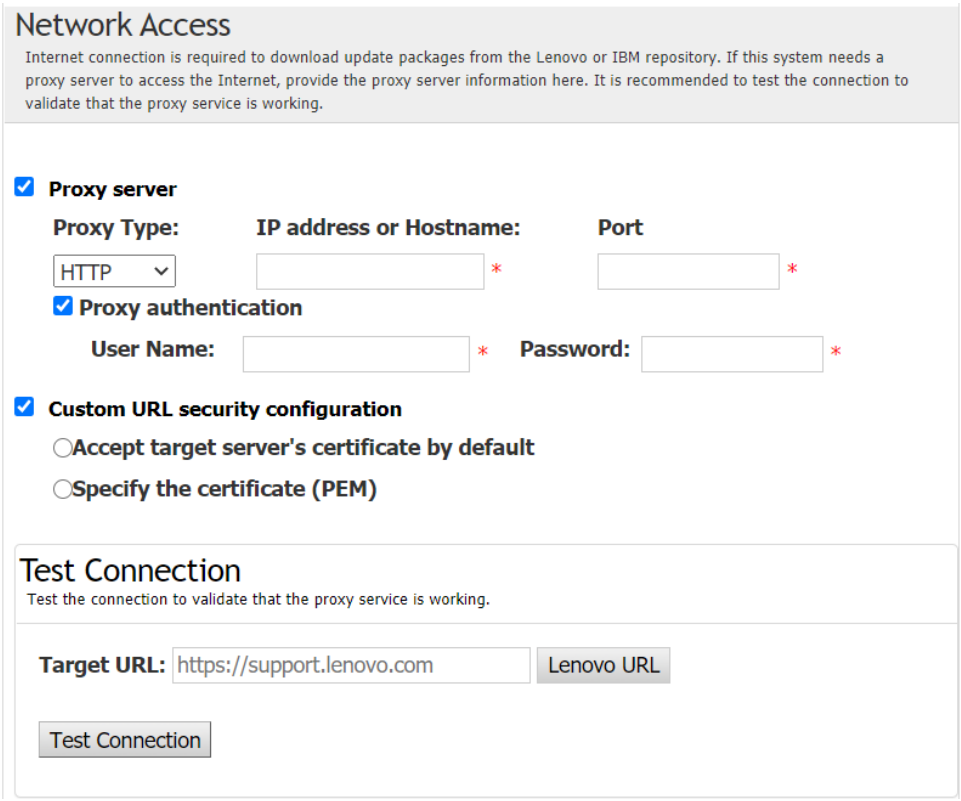
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

  b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

- **Angepasste URL-Sicherheitskonfiguration**

  Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
  – **Zertifikat des Zielservers standardmäßig akzeptieren**
  – **Zertifikat angeben (PEM)**




9. Wählen Sie im Fenster Aktualisierungstyp die Option Lokalen Server aktualisieren aus und klicken Sie auf **Weiter**.
10. Führen Sie im Fenster Aktualisierungsempfehlungen je nach Bedarf eine oder mehrere der folgenden Aktionen aus:

- Um alle Aktualisierungspakete anzuzeigen, wählen Sie **Aktualisierungen für nicht erkanntes Gerät anzeigen** aus.
- Um die Komponente zu aktualisieren, wählen Sie die Zielkomponente aus, und klicken Sie auf **Weiter**.

11. Im Fenster Aktualisierungen abrufen wird in der Abrufungstabelle der Fortschritt der abgerufenen Pakete angezeigt. Klicken Sie nach Abschluss des Aktualisierungsfortschritts auf **Weiter**.
12. Klicken Sie im Fenster Laufende Aktualisierungen auf **Aktualisierung starten → Ja → Weiter**.

    **Anmerkungen:** Um die Firmware mit gebündelten Paketen zu aktualisieren, wählen Sie **Firmware mit gebündelten Paketen aktualisieren aus. Dieses Kontrollkästchen und seine Unteroptionen unterstützen nur XCC2.** Legen Sie dann die Anwendungszeit fest.
    - **OnReset**: Pakete aktualisieren, wenn das System das nächste Mal neu gestartet wird.
    - **Sofort**: Pakete sofort aktualisieren. Möglicherweise wird das System sofort neu gestartet.
    - **OnStartUpdateRquest**: Aktualisierung der Pakete durch Verwaltung der Stufenaktualisierung oder Ausführung von OneCLI-Befehlen.
13. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Verwalten von Stufenaktualisierungen für einen Remote-Server

Die UpdateXpress-Anwendung unterstützt das Starten, Abbrechen und Anzeigen aller Stufenaktualisierungen für einen Remote-Server.

Die folgende Voraussetzung muss erfüllt sein, um diese Aufgabe abzuschließen:
- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.

Gehen Sie folgendermaßen vor, um eine Stufenaktualisierung für einen Remote-Server zu verwalten:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Stufenweise Aktualisierung verwalten** aus und klicken Sie auf **Weiter**.
5. Gehen Sie im Fenster Task-Verwaltung wie folgt vor und klicken Sie auf **Weiter**.
   - Um die Taskinformationen zu erhalten, geben Sie die Task-ID ein und klicken Sie auf  . Die Task-ID wird automatisch für die anstehende Aufgabe ausgefüllt.
   - Klicken Sie für den Start der Aktualisierung in der Zielaufgabe auf **Starten**.
   - Klicken Sie zum Abbrechen der Aktualisierung in der Zielaufgabe auf **Abbrechen**.
6. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## SED-Authentifizierungsschlüssel verwalten

Die ThinkEdge-Server bieten über den Authentifizierungsschlüssel Zugriff auf das Selbstverschlüsselende Laufwerk (Self-Encrypting Drive, SED). Die UpdateXpress-Anwendung unterstützt die Verwaltung des SED-Authentifizierungsschlüssels (AK), einschließlich Generierung, Sicherung und Wiederherstellung.

**Voraussetzung:**
- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Diese Funktion wird nur unterstützt, wenn der ThinkEdge-Server nicht gesperrt ist. Details zu unterstützten Servern finden Sie in der ThinkEdge-Serie in „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie wie folgt vor, um den SED-Authentifizierungsschlüssel zu verwalten:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Sicherheitseinrichtungen auf ThinkEdge-Server ausführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster mit den ThinkEdge Server-Sicherheitseinrichtungen die Option **SED-Authentifizierungsschlüssel verwalten** aus und klicken Sie auf **Weiter**.
6. Gehen Sie im Fenster Verwaltung des SED-Authentifizierungsschlüssels (AK) wie folgt vor:
   - Um den SED AK zu generieren, wählen Sie bei deaktiviertem SED AK **SED-Verschlüsselung aktivieren** oder bei aktiviertem SED AK **SED AK ändern** aus. Wählen Sie die Zielmethode aus der Dropdown-Liste **Methode** aus und klicken Sie auf **Schlüssel erneut generieren**.

     **Anmerkung:** Es wird empfohlen, den AK bei Datenverlust zu sichern. Benutzer können andere Optionen nur nach dem Sichern des AKs auswählen.
   - Um den SED AK zu sichern, wählen Sie **SED AK sichern** aus, geben Sie die Position und das Kennwort der Sicherungsdatei ein, und klicken Sie auf **Starten**. UpdateXpress speichert die Sicherungsdatei mit den SED-AK-Informationen.
   - Wählen Sie zum Wiederherstellen des SED AK die Option **SED AK wiederherstellen** aus und führen Sie einen der folgenden Schritte aus:
     – Wählen Sie zur Wiederherstellung mithilfe der Sicherungsdatei die Option **SED AK aus Sicherungsdatei wiederherstellen** aus der Dropdown-Liste **Methode** aus. Klicken Sie auf **Durchsuchen**, um die Sicherungsdatei auszuwählen, das Kennwort einzugeben und auf **Wiederherstellen starten** zu klicken.
     – Wählen Sie zur Wiederherstellung mithilfe der Passphrase die Option **SED AK mit Passphrase wiederherstellen** aus der Dropdown-Liste **Methode** aus, geben Sie das Kennwort ein und klicken Sie auf **Wiederherstellung starten**.
7. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Server im ThinkShield Portal beanspruchen

Die Inhaberschaft des ThinkEdge-Servers kann im Lenovo ThinkShield Key Vault Portal übertragen werden. Anschließend kann UpdateXpress den gesperrten Server über das Portal aktivieren.

**Voraussetzung:**

- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Diese Funktion wird nur in ThinkEdge-Servern unterstützt. Details zu unterstützten Servern finden Sie in der ThinkEdge-Serie in „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie wie folgt vor, um den Server im ThinkShield Portal zu beanspruchen:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Sicherheitseinrichtungen auf ThinkEdge-Server ausführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Sicherheitsfunktionen von ThinkEdge Server die Option **Server im ThinkShield Portal beanspruchen** aus und klicken Sie auf **Weiter**.
6. Führen Sie im Fenster Internetzugriff je nach Bedarf eine der folgenden Aktionen aus:
   - Wenn Benutzer keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
   - Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie eine der folgenden Optionen und klicken Sie auf **Verbindung testen**:
     – **Proxy-Server**: Zugriff auf das Netzwerk über einen HTTP-/HTTPS-Proxy.
       a. Wählen Sie **Proxy-Server** aus und füllen Sie die folgenden Felder aus:

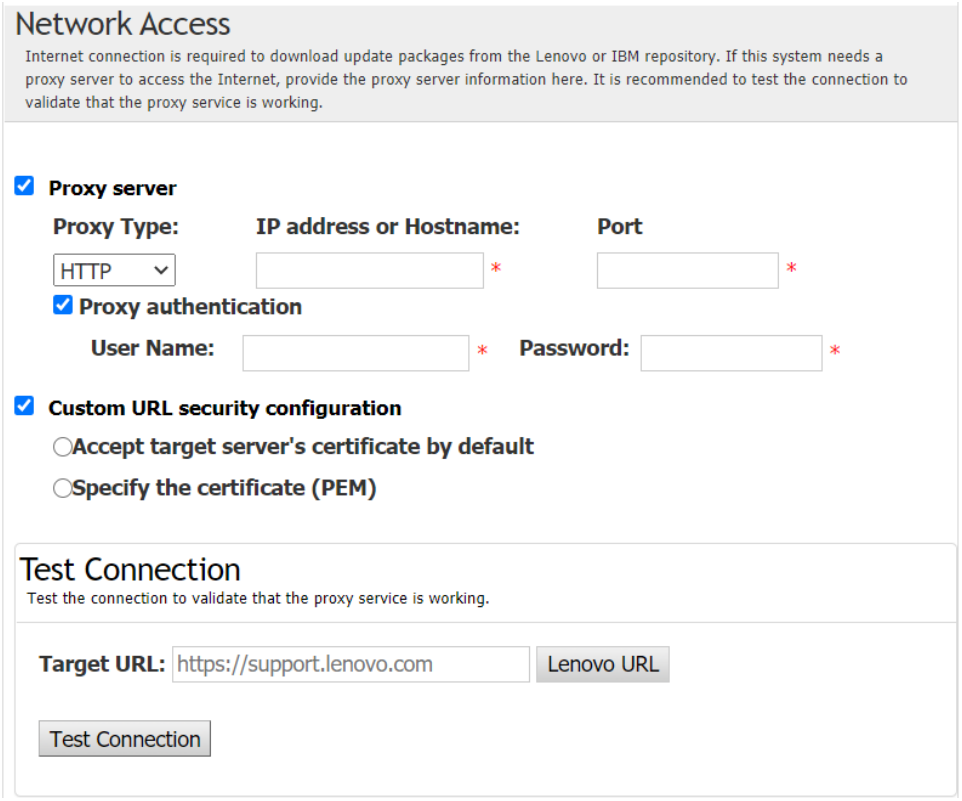
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

       b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

     – **Angepasste URL-Sicherheitskonfiguration**: Netzwerkzugriff über einen Reverse-Proxy.

       Wählen Sie eine der folgenden Optionen aus:
       – Zertifikat des Zielservers standardmäßig akzeptieren
       – Zertifikat angeben (PEM)




7. Geben Sie im Fenster Server beanspruchen die Organisations-ID des ThinkShield Key Vault Portals, den Benutzernamen und das Kennwort ein, und klicken Sie auf **Beanspruchen**.
8. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Modus zur Sperrungssteuerung aktualisieren

Der ThinkEdge-Server ist mit Sicherheitssensorik ausgestattet, um ein Manipulationsereignis zu erkennen, wodurch auch der Server bei der Manipulationserkennung gesperrt wird. UpdateXpress unterstützt ein Upgrade des Serversperrmodus durch die Aktivierung des Servers über XClarity Controller, um den Server über das ThinkShield Portal zu verwalten.

**Voraussetzung:**

- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Diese Funktion wird nur in ThinkEdge-Servern unterstützt. Details zu unterstützten Servern finden Sie in der ThinkEdge-Serie in „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie wie folgt vor, um den Sperrmodus zu aktualisieren:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

**Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.

4. Wählen Sie im Fenster Task die Option **Sicherheitseinrichtungen auf ThinkEdge-Server ausführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Sicherheitsfunktionen von ThinkEdge-Server die Option **Systemsperrungssteuerung** aus, klicken Sie auf **Weiter** und wählen Sie eine der folgenden Optionen aus, um das Eigentum am Server für das ThinkShield Key Vault Portal geltend zu machen oder nicht. Klicken Sie dann erneut auf **Weiter**.
   - Wählen Sie **Ja, ich möchte den Server jetzt geltend machen** aus und fahren Sie mit Schritt 6 fort.
   - Wählen Sie **Nein, ich möchte fortfahren, ohne den Server im ThinkShield Key Vault Portal geltend zu machen** aus und fahren Sie mit Schritt 8 fort.
6. Führen Sie im Fenster Internetzugriff je nach Bedarf eine der folgenden Aktionen aus:
   - Wenn Benutzer keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
   - Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie eine der folgenden Optionen und klicken Sie auf **Verbindung testen**:
     – **Proxy-Server**: Zugriff auf das Netzwerk über einen HTTP-/HTTPS-Proxy.
       a. Wählen Sie **Proxy-Server** aus und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

       b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

     – **Angepasste URL-Sicherheitskonfiguration**: Netzwerkzugriff über einen Reverse-Proxy.

       Wählen Sie eine der folgenden Optionen aus:
       – Zertifikat des Zielservers standardmäßig akzeptieren
       – Zertifikat angeben (PEM)
7. Geben Sie im Fenster ThinkShield Portal-Konto überprüfen die Organisations-ID, den Benutzernamen und das Kennwort für das ThinkShield Key Vault Portal ein und klicken Sie auf **Überprüfen**. Klicken Sie nach Abschluss der Überprüfung auf **Weiter**.

   **Anmerkung:** Die Informationseingabe sollte gültig sein. Andernfalls wird die Schaltfläche **Weiter** *nicht* aktiviert.
8. Geben Sie im Fenster Systemsperrungssteuerung manuell **JA** und klicken Sie auf **OK**. Klicken Sie nach Abschluss des Aktualisierungsprozesses auf **Weiter**.
9. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Server im Sperrmodus aktivieren

Der ThinkEdge-Server ist mit Sicherheitssensorik ausgestattet, um ein Manipulationsereignis zu erkennen, wodurch auch der Server bei der Manipulationserkennung gesperrt wird. UpdateXpress unterstützt die Aktivierung des gesperrten Servers über das ThinkShield Key Vault Portal oder den XClarity Controller.

**Voraussetzung:**
- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Diese Funktion wird nur in ThinkEdge-Servern unterstützt. Details zu unterstützten Servern finden Sie in der ThinkEdge-Serie in „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie wie folgt vor, um den Server im Sperrmodus zu aktivieren:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.
   - (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
   - (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

   **Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster Task die Option **Sicherheitseinrichtungen auf ThinkEdge-Server ausführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster mit den ThinkEdge Server-Sicherheitseinrichtungen die Option **Server mit ThinkShield Portal aktivieren** aus und klicken Sie auf **Weiter**.

   **Anmerkung:** Die Standard-Systemsperrungssteuerung wird von XClarity Controller verwaltet. Wenn die Sperrungssteuerung vom ThinkShield Portal verwaltet wird, können Benutzer den Server nur im gesperrten Modus aktivieren, nachdem sie sich über das ThinkShield Key Vault Portal authentifiziert haben.
6. Wenn Sie im Fenster Internetzugriff keine spezielle Anforderung für den Sicherheitszugriff haben, klicken Sie auf **Verbindung testen**, um die Netzwerkverbindung der Ziel-URL zu überprüfen, und klicken Sie dann auf **Weiter**.
   Wenn Benutzer mehr Sicherheitsbedenken haben, konfigurieren Sie vor dem Klicken auf **Verbindung testen** den **Proxy-Server** und/oder die **Angepasste URL-Sicherheitskonfiguration** entsprechend Ihren Sicherheitsanforderungen. Gehen Sie dazu wie folgt vor:
   - **Proxy-Server**
     a. Wählen Sie **Proxy-Server** aus, wenn für die Verbindung mit dem Web ein HTTP/HTTPS-Proxy erforderlich ist, und füllen Sie die folgenden Felder aus:

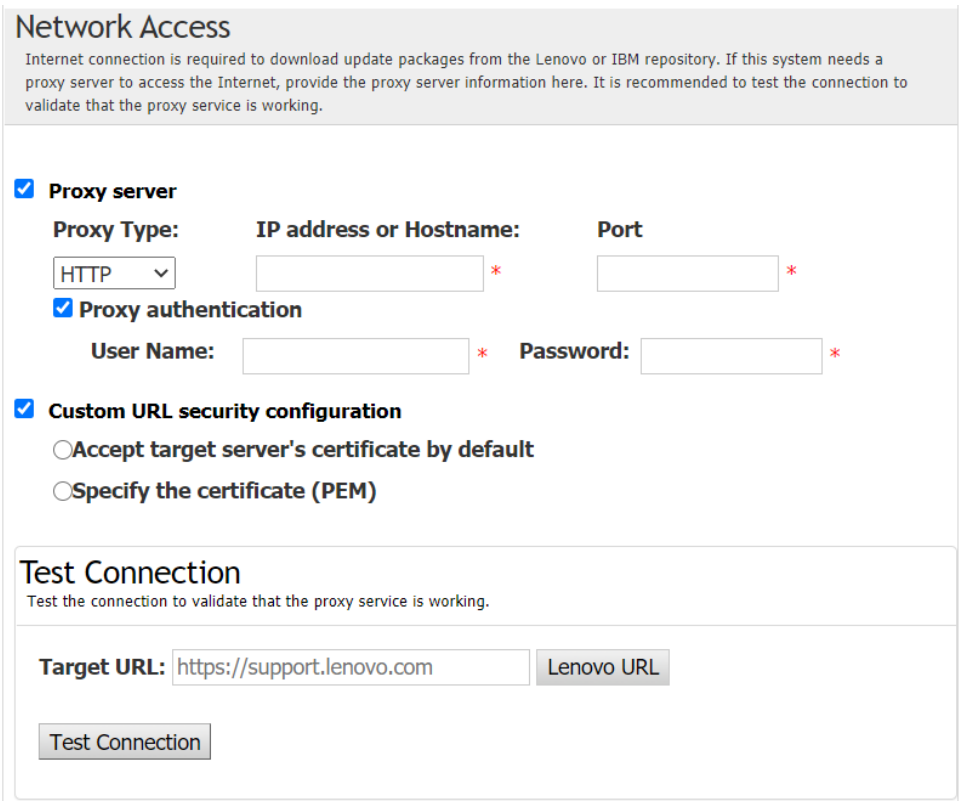
| | |
|---|---|
| **Proxy-Typ** | Proxy-Typ des Proxy-Servers. |
| **IP-Adresse oder Hostname** | Hostname, IP-Adresse oder Domänenname des Proxy-Servers. |
| **Port** | Portnummer des Proxy-Servers. |

     b. Wählen Sie **Proxy-Authentifizierung** aus, wenn Anmeldeinformationen für die Authentifizierung beim Proxy-Server angegeben werden müssen, und füllen Sie die folgenden Felder aus:

| | |
|---|---|
| **Benutzername** | Benutzername für die Authentifizierung beim Proxy-Server. |
| **Kennwort** | Kennwort zum angegebenen Benutzernamen. |

   - **Angepasste URL-Sicherheitskonfiguration**

     Wählen Sie **Angepasste URL-Sicherheitskonfiguration** aus, wenn Sie einen Reverse-Proxy benötigen, und wählen Sie eine der folgenden Optionen aus:
     – **Zertifikat des Zielservers standardmäßig akzeptieren**
     – **Zertifikat angeben (PEM)**




7. Geben Sie im Fenster Server aktivieren die Organisations-ID des ThinkShield Key Vault Portals, den Benutzernamen und das Kennwort ein, und klicken Sie auf **Aktivieren**. Klicken Sie nach Abschluss des Aktivierungsvorgangs auf **Weiter**.

   **Anmerkung:** Wenn der Server von XClarity Controller verwaltet wird, müssen die Benutzer die Informationen des ThinkShield Key Vault Portals *nicht* eingeben.
8. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Sicherheitssensoren konfigurieren

Die ThinkEdge-Server sind mit Sicherheitssensoren ausgestattet, um ein Manipulationsereignis zu erkennen. UpdateXpress unterstützt das Aktivieren, Deaktivieren und Ändern des Schwellenwerts für den Bewegungserkennungssensor und den Sensor für unbefugten Zugriff auf das Gehäuse.

**Voraussetzung:**
- Die UpdateXpress-Anwendung wird auf einem Server ausgeführt, der mit einem unterstützten Betriebssystem ausgeführt wird. Informationen zu unterstützten Betriebssystemen finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 6.
- Diese Funktion wird nur in ThinkEdge-Servern unterstützt. Details zu unterstützten Servern finden Sie in der ThinkEdge-Serie in „Unterstützte Servermodelle“ auf Seite 5.

Gehen Sie wie folgt vor, um die Sicherheitssensoren zu konfigurieren:
1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Remote-Server verwalten**, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
   - (Einstellung) **IP-Adresse oder Hostname**: BMC IP-Adresse oder Hostname des Zielsystems.
   - (Einstellung) **Benutzername**: BMC-Benutzername des Zielsystems.

- (Einstellung) **Passwort**: BMC-Passwort des Zielsystems.
- (Einstellung) **Port**: BMC CIM oder RSET Portnummer. Ohne Eingabe wird der Standard-Port verwendet.

**Anmerkung:** Wenn Benutzer das BMC-Serverzertifikat nicht überprüfen sollen, wählen Sie das standardmäßig **Zertifikat des BMC-Servers akzeptieren** aus und klicken Sie auf **Weiter**.

4. Wählen Sie im Fenster Task die Option **Sicherheitseinrichtungen auf ThinkEdge-Server ausführen** aus und klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster Sicherheitsfunktionen ThinkEdge-Server die Option **Sicherheitssensoren konfigurieren** aus und klicken Sie auf **Weiter**.
6. Gehen Sie im Fenster Sicherheitssensoren konfigurieren wie folgt vor und klicken Sie auf **Weiter**.
   - Um die **Bewegungserkennung** oder die **Gehäuseeingrifferkennung auf das Gehäuse** zu aktivieren oder zu deaktivieren, wählen Sie die Optionen aus der Dropdown-Liste aus oder klicken Sie auf den Umschalter, um den Status ein-/auszuschalten.

     **Anmerkung:** Bei Datenverlust sollten Sie AK sichern, bevor Sie Elemente auswählen.
   - Klicken Sie auf **Schrittzähler zurücksetzen**, um die Anzahl der Schritte für die Erkennung von Bewegungen zurückzusetzen. UpdateXpress setzt die Anzahl der Schritte auf 0 zurück.
   - Um Die Schwellenwertschritte für das Sperren der Bewegungserkennung zu ändern, wählen Sie die Zielschrittebene unter **Schwellenwert zum Sperren** aus.

     **Anmerkung:** Der ThinkEdge-Server wird gesperrt, sobald das Manipulationsereignis vom Sicherheitssensor erkannt wurde.
7. Klicken Sie im Fenster Fertig stellen auf **Protokoll anzeigen**, um das Aktualisierungsprotokoll zu überprüfen, kopieren und speichern Sie die generierten Befehle und klicken Sie auf **Schließen** zum Beenden.

## Server über direkte Ethernet-Verbindung verwalten

Die UpdateXpress-Anwendung unterstützt die Verwaltung der Server über eine direkte Ethernet-Verbindung. Wenn das Netzwerkkabel angeschlossen ist, versucht UpdateXpress, über die BMC-Standard-IP-Adresse und die Anmeldeinformationen auf den Server BMC zuzugreifen.

Gehen Sie wie folgt vor, um den Server über eine direkte Ethernet-Verbindung zu verwalten:

1. Starten Sie die UpdateXpress-Anwendung. (siehe „UpdateXpress-Anwendung starten“ auf Seite 9).
2. Klicken Sie im Begrüßungsfenster auf **Weiter**.
3. Wählen Sie im Fenster Zielserver die Option **Direkte Ethernet-Verbindung** aus, geben Sie die folgenden Informationen ein und klicken Sie auf **Weiter**.
4. Führen Sie im Fenster Einstellungen für direkte Ethernet-Verbindung folgende Aktionen aus:
   a. Wählen Sie den Zieladapter aus der Tabelle „Verfügbare Netzwerkadapter“ aus.
   b. Stellen Sie sicher, dass die Standard-IP-Adresse **192.168.70.125** lautet.
   c. Geben Sie den Benutzernamen und das Kennwort ein.
   d. Klicken Sie auf **Verbindung testen → Weiter** oder **Weiter**.
5. Wählen Sie im Fenster Aufgabe eine der folgenden Optionen aus:
   - **Aktualisieren auf Zielserver ausführen**. Weitere Informationen finden Sie in Schritt 4 und den nachfolgenden Schritten in „Remote-Server über ein lokales Verzeichnis aktualisieren“ auf Seite 15.
   - **Stufenweise Aktualisierung verwalten**. Weitere Informationen finden Sie in Schritt 4 und den nachfolgenden Schritten in „Verwalten von Stufenaktualisierungen für einen Remote-Server“ auf Seite 28.
   - **Remote-RAID-Konfiguration** Weitere Informationen finden Sie in Schritt 4 und den nachfolgenden Schritten in „RAID-Array für einen Remote-Server konfigurieren“ auf Seite 25.
   - **Sicherheitsfunktion auf dem ThinkEdge-Server konfigurieren**. Weitere Informationen finden Sie in Schritt 4 und den nachfolgenden Schritten in den folgenden Abschnitten:
     – „SED-Authentifizierungsschlüssel verwalten“ auf Seite 29
     – „Server im ThinkShield Portal beanspruchen“ auf Seite 30

- „Modus zur Sperrungssteuerung aktualisieren“ auf Seite 31
- „Server im Sperrmodus aktivieren“ auf Seite 32
- „Sicherheitssensoren konfigurieren“ auf Seite 34

## OneCLI-Befehle im Fenster „Fertig stellen“ anzeigen

UpdateXpress führt Aktualisierungen aus, indem es OneCLI-Befehle im GUI-Assistenten aufruft. UpdateXpress 2.7.0 und neuere Versionen zeigen diese Befehle im Fenster „neuer Text“ im Fenster „Fertig stellen“ an. Benutzer können die Befehle speichern und verwenden, um dieselbe Funktion je nach Ihren Anforderungen im CLI-Modus aufzurufen.

Beispiel für OneCLI-Befehle:

```
<LXCE OneCLI> update flash --uselocalimg --imm USERID:***@xx.xxx.xxx.xxx --dir
D:\build\Onegui\105980\lnvgy_utl_lxce_ux01k-2.7.0_windows_i386\workingdir --output
D:\build\Onegui\105980\lnvgy_utl_lxce_ux01k-2.7.0_windows_i386\Lenovo_Support\ --platform --log 5
```

# Kapitel 4. Fehlerbehebung

Dieses Kapitel enthält Informationen zur Vorgehensweise bei einem Problem mit der UpdateXpress-Anwendung.

### Einschränkungen und Probleme

- **Wenn Benutzer bei der Ausführung von UpdateXpress unter Linux das Zertifikat für die benutzerdefinierte Proxy-/URL-Sicherheitskonfiguration angeben und ein zweites Mal auf Durchsuchen klicken, wird das Durchsuchen-Fenster auf der UpdateXpress-Oberfläche möglicherweise nicht angezeigt.**

  Wählen Sie auf der Seite Internetzugriff in der Dropdown-Liste **Proxytyp** die Option **HTTPS** aus, wählen Sie die **Sicherheitskonfiguration des angepassten Proxys** und die **Sicherheitskonfiguration mit angepasster URL** aus und klicken Sie auf **Durchsuchen**, um das Zertifikat für beide Auswahlen anzugeben. Wenn Benutzer zum zweiten Mal auf „Durchsuchen“ klicken, wird das Fenster „Durchsuchen“ möglicherweise nicht angezeigt.

  **Problemumgehung**: Führen Sie einen oder mehrere der folgenden Schritte aus:
  - Wechseln Sie manuell zum Browse-Fenster im Hintergrund.
  - Passen Sie die Fenstergröße an, um das Durchsuchen-Fenster im Hintergrund anzuzeigen.
  - Verwenden Sie stattdessen UpdateXpress unter Windows.
- **UpdateXpress kann bei einigen Geräten den Out-of-Box-Treiber nicht als Standard festlegen, wenn ein Upgrade vom In-Box-Treiber auf den Out-of-Box-Treiber durchgeführt wird.**

  UpdateXpress ruft OneCLI auf, um die Aktualisierungsaufgabe durchzuführen. OneCLI konnte die inkonsistenten Versionen des Inbox-Treibers und des Out-of-Box-Treibers nicht vergleichen und die richtige Version für die Aktualisierung auswählen. In diesem Fall konnte UpdateXpress den Out-of-Box-Treiber nicht für die Aktualisierung auswählen und die Benutzer sollten den Ziel-Out-of-Box-Treiber manuell auswählen, um den In-Box-Treiber zu überschreiben.
- **Alle UpdateXpress-Pfade müssen alphanumerische Standard-Zeichen in englischer Sprache verwenden.**

  Alle UpdateXpress-Pfade müssen alphanumerische Standard-Zeichen in englischer Sprache verwenden und dürfen keine Leerzeichen, Sonderzeichen oder nicht-englischsprachige Zeichen enthalten.

### Lösungsstrategien

Es gibt derzeit keine bekannten Probleme oder Problemumgehungen für die UpdateXpress-Anwendung.

### Koexistenz und Kompatibilität

Die UpdateXpress-Anwendung basiert auf OneCLI, hat jedoch keine Interaktionen mit anderen Programmen auf dem System. Führen Sie die UpdateXpress-Anwendung und OneCLI nicht gleichzeitig aus.

# Anhang A. Eingabehilfefunktionen für UpdateXpress

Die Eingabehilfefunktionen helfen Benutzern mit körperlichen Behinderungen wie etwa mit eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen dabei, Softwareprodukte erfolgreich einzusetzen.

Die folgende Liste enthält die wichtigsten Eingabehilfefunktionen in der UpdateXpress-Anwendung:
- Ausschließliche Ausführung über die Tastatur
- Schnittstellen für Sprachausgabeprogramme

### Navigation über die Tastatur

Benutzer können die Tastatur verwenden, um durch die grafische Benutzerschnittstelle (GUI) zu navigieren.

Die folgenden Tastenkombinationen gelten für Windows- und Linux-Betriebssysteme.

| Kurzbefehl | Funktion |
|---|---|
| Tabulatortaste | Zum nächsten Steuerelement navigieren. |
| Umschalttaste+Tabulatortaste | Zum vorherigen Steuerelement navigieren. |
| Nach-links-Taste | Ein Zeichen zurück gehen. |
| Nach-rechts-Taste | Ein Zeichen nach vorne gehen. |
| Rückschritttaste | Das Zeichen links vom Cursor löschen. |
| Löschen | Das Zeichen unter dem Cursor löschen. |
| Nach-oben-Taste | Fokus und Auswahl mit der Optionsschaltfläche nach oben bewegen. |
| Nach-unten-Taste | Fokus und Auswahl mit der Optionsschaltfläche nach unten bewegen. |
| Leerzeichen | Eine Option auswählen oder löschen. |

### Sprachausgabetechnologie

Sprachausgabetechnologien werden vor allem bei Softwareprogrammschnittstellen, Hilfeinformationssystemen und verschiedenen Online-Dokumenten eingesetzt. Weitere Informationen zu Sprachausgabeprogrammen finden Sie hier:
- JAWS-Sprachausgabeprogramm verwenden:

  http://www.freedomscientific.com/Products/Blindness/JAWS
- NVDA-Sprachausgabeprogramm verwenden:

  http://www.nvaccess.org/

### Lenovo und Barrierefreiheit

Weitere Informationen zum Engagement von Lenovo zur Barrierefreiheit finden Sie unter http://www.lenovo.com/lenovo/us/en/accessibility.html.

# Anhang B. Hinweise

Möglicherweise bietet Lenovo die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim Lenovo Ansprechpartner erhältlich.

Hinweise auf Lenovo Lizenzprogramme oder andere Lenovo Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von Lenovo verwendet werden können. Anstelle der Lenovo Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von Lenovo verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es Lenovo Patente oder Patentanmeldungen geben. Mit der Auslieferung dieser Dokumentation ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an die nachstehende Adresse zu richten. Anfragen an diese Adresse müssen auf Englisch formuliert werden.

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

LENOVO STELLT DIESE VERÖFFENTLICHUNG IN DER VORLIEGENDEN FORM (AUF „AS-IS“-BASIS) ZUR VERFÜGUNG UND ÜBERNIMMT KEINE GARANTIE FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE FREIHEIT DER RECHTE DRITTER. Einige Rechtsordnungen erlauben keine Garantieausschlüsse bei bestimmten Transaktionen, sodass dieser Hinweis möglicherweise nicht zutreffend ist.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Lenovo kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Die in diesem Dokument beschriebenen Produkte sind nicht zur Verwendung bei Implantationen oder anderen lebenserhaltenden Anwendungen, bei denen ein Nichtfunktionieren zu Verletzungen oder zum Tode führen könnte, vorgesehen. Die Informationen in diesem Dokument beeinflussen oder ändern nicht die Lenovo Produktspezifikationen oder Garantien. Keine Passagen in dieser Dokumentation stellen eine ausdrückliche oder stillschweigende Lizenz oder Anspruchsgrundlage bezüglich der gewerblichen Schutzrechte von Lenovo oder von anderen Firmen dar. Alle Informationen in dieser Dokumentation beziehen sich auf eine bestimmte Betriebsumgebung und dienen zur Veranschaulichung. In anderen Betriebsumgebungen werden möglicherweise andere Ergebnisse erzielt.

Werden an Lenovo Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses Lenovo Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten überprüfen, welche Daten für ihre jeweilige Umgebung maßgeblich sind.

## Marken



## Wichtige Anmerkungen

Die Prozessorgeschwindigkeit bezieht sich auf die interne Taktgeschwindigkeit des Mikroprozessors. Das Leistungsverhalten der Anwendung ist außerdem von anderen Faktoren abhängig.

Bei Angaben in Bezug auf Hauptspeicher, realen/virtuellen Speicher oder Kanalvolumen steht die Abkürzung KB für 1.024 Byte, MB für 1.048.576 Byte und GB für 1.073.741.824 Byte.

Bei Angaben zur Kapazität von Festplattenlaufwerken oder zu Übertragungsgeschwindigkeiten steht MB für 1.000.000 Byte und GB für 1.000.000.000 Byte. Die gesamte für den Benutzer verfügbare Speicherkapazität kann je nach Betriebsumgebung variieren.

Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch Lenovo.

Manche Software kann sich von der im Einzelhandel erhältlichen Version (falls verfügbar) unterscheiden und enthält möglicherweise keine Benutzerhandbücher bzw. nicht alle Programmfunktionen.

# Index