Lenovo

Guía del usuario de Lenovo XClarity Essentials UpdateXpress

Versión 4.4.0

Nota

Antes de utilizar estos documentos y los productos a los que da soporte, lea la información en Apéndice B “Avisos” en la página 41.

Esta edición se aplica a Lenovo XClarity® Essentials UpdateXpress y a todas las demás versiones y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Vigésimo cuarta edición (Febrero 2024)

Contenido

Contenido i

Tablas iii

Acerca de esta guía v

A quiénes va dirigida esta guía v

Convenciones y terminología v

Sitios web admitidos v

Capítulo 1. Visión general técnica . . . 1

UpdateXpress System Pack (UXSP) 1

Aplicación de actualizaciones de UXSP mediante la aplicación UpdateXpress 2

Gestión de un UXSP como un conjunto 2

Gestión de requisitos de actualización 2

Actualizaciones independientes del sistema operativo 4

Datos de inventario faltantes o incompletos 4

Instalación de los controladores requeridos 4

Capítulo 2. Requisitos de hardware y software 5

Modelos de servidor admitidos 5

Sistemas operativos compatibles 6

Windows 6

Linux 6

Privilegios de sistema operativo 7

Capítulo 3. Uso de la aplicación UpdateXpress 9

Inicio de la aplicación UpdateXpress 9

Actualización de un servidor local desde el sitio Web 10

Actualización de un servidor local desde un directorio local 11

Actualización de un servidor remoto desde el sitio Web 12

Actualización de un servidor remoto desde un directorio local 14

Configuración de BIOS en un servidor remoto . . . 16

Recopilación de registros de un servidor remoto . . 16

Actualización de varios servidores remotos desde el sitio Web 17

Actualización de varios servidores remotos desde un directorio local 19

Configuración de BIOS para varios servidores remotos 21

Recopilación de registros para varios servidores remotos 22

Creación de un repositorio de actualizaciones . . . 22

Configuración de la matriz RAID para un servidor remoto 24

Realización de actualizaciones preconfiguradas para servidores remotos 25

Administración de actualizaciones preconfiguradas para servidores remotos. 27

Administración de la clave de autenticación de SED 28

Solicitar un servidor en ThinkShield Portal 29

Actualización del modo de control de bloqueo . . . 31

Activación del servidor en modo de bloqueo . . . 32

Configuración de los sensores de seguridad . . . 34

Gestión del servidor bajo conexión Ethernet directa 35

Visualización de comandos OneCLI en la ventana finalizar 36

Capítulo 4. Resolución de problemas 37

Apéndice A. Características de accesibilidad de UpdateXpress 39

Apéndice B. Avisos 41

Marcas registradas 42

Notas importantes 42

Índice 43

Tablas

1. Sistemas de Lenovo admitidos 5
2. Sistemas operativos Windows admitidos . . . 6
3. Sistemas operativos Linux admitidos 7

Acerca de esta guía

Lenovo XClarity Essentials UpdateXpress (en adelante denominada aplicación UpdateXpress) es una aplicación que aplica UpdateXpress System Packs (UXSP) y actualizaciones individuales al servidor. Esta guía proporciona información acerca de cómo descargar y utilizar la aplicación UpdateXpress.

A quiénes va dirigida esta guía

Esta documentación está orientada para administradores de sistema u otros individuos responsables de administrar sistemas que están familiarizados con mantenimiento de firmware y controladores de dispositivo.

Convenciones y terminología

Los párrafos que comienzan con las palabras Nota, Importante o Atención en negrita tienen significados específicos orientados a resaltar información importante dentro del documento:

Nota: Estos avisos proporcionan consejos importantes, ayuda o consejos.

Importante: Estos avisos proporcionan información o consejos que pueden ayudar a los usuarios a evitar situaciones incómodas o difíciles.

Atención: Estos avisos indican posibles daños a programas, dispositivos o datos. Un aviso de atención aparece delante de una instrucción o situación en la que puede producirse un daño.

En esta documentación, cuando a los usuarios se les indica que deben ingresar un comando, escríbalo y presione Intro.

Sitios web admitidos

En esta sección se proporcionan recursos web de soporte.

- Sitio web de Lenovo XClarity Essentials

  Utilice este sitio Web para descargar varias herramientas de gestión de sistema para servidores ThinkSystem y System x.
- Lenovo XClarity Essentials UpdateXpress

  Utilice este sitio Web para descargar la aplicación UpdateXpress.

Los siguientes sitios Web proporcionan información acerca de compatibilidad y soporte de productos, garantías y licencias y diversos recursos técnicos.
- Productos y servicios del soporte de Lenovo Flex System
- Sitio web de ServerProven
- Biblioteca de recursos de almacenamiento, redes y servidor de Lenovo

Capítulo 1. Visión general técnica

Lenovo XClarity Essentials UpdateXpress (en adelante denominada aplicación UpdateXpress) se puede usar para adquirir y aplicar UpdateXpress System Packs (UXSP) y actualizaciones individuales al sistema local o remoto. La aplicación UpdateXpress adquiere e implementa paquetes de actualización UpdateXpress System Pack (UXSP) y actualizaciones individuales. Los UXSP contienen actualizaciones de firmware y de controladores de dispositivos.

La siguiente sección presenta brevemente las cuatro funciones principales de la aplicación UpdateXpress. Para obtener más información, consulte Capítulo 3 “Uso de la aplicación UpdateXpress” en la página 9.

Actualización del servidor local
Actualice el equipo local que ejecuta actualmente la aplicación UpdateXpress. El tipo de equipo se detecta y las actualizaciones se adquieren y aplican automáticamente.

Actualización de un servidor remoto
Actualice el equipo remoto mediante el Controlador de gestión de placa base (BMC) que se ejecuta en el equipo. Los usuarios necesitan un servidor de Simple File Transfer Protocol (SFTP) para transferir las actualizaciones al equipo remoto de destino.

Creación de un repositorio de actualizaciones
Elija uno o más tipos de equipos para los cuales adquirir actualizaciones desde el sitio Web de soporte de Lenovo. Las actualizaciones se descargan a la carpeta especificada, pero no se aplicarán dichas actualizaciones. Posteriormente, los usuarios pueden utilizar la aplicación UpdateXpress para aplicar esas actualizaciones, indicando las actualizaciones que se deben obtener de la carpeta especificada, en lugar de hacerlo desde el sitio web de Lenovo.

Configuración remota de RAID
Configuración de la matriz RAID utilizando el servicio de BMC.

UpdateXpress System Pack (UXSP)

Un UXSP es un conjunto probado para la integración de actualizaciones de firmware controladores en línea para servidores System x y ThinkSystem. Los UXSP se liberan semestralmente durante los tres primeros años de soporte y anualmente para los tres años restantes.

Los UXSP simplifican el proceso de descarga e instalación de todas las actualizaciones de controladores y firmware en línea para un sistema. Los UXSP garantizan que los usuarios siempre puedan trabajar con un conjunto completo de las actualizaciones más recientes, sometidas a prueba simultánea en funcionamiento y agrupadas por Lenovo.

Los UXSP se crean para una combinación de sistema operativo y tipo de equipo específicos. Se proporcionan UXSP independientes para sistemas operativos Windows® sistemas y para cada una de las distribuciones de Linux. Por ejemplo, puede haber varios UXSP para un tipo de equipo específico. También puede haber una actualización para el sistema operativo Windows y para cada distribución Linux.

También hay un tipo de plataforma UXSP que puede utilizarse para actualizar fuera de banda a un sistema. Los UXSP de plataforma no contienen un sistema operativo.

Formato UXSP
Se entrega un UXSP en un archivo XML. El convenio de nomenclatura de los UXSP responde al siguiente formato:
lnvgy_utl_uxsp_*version_operatingsystem_arch*.xml
Ejemplo: `lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml`

Aplicación de actualizaciones de UXSP mediante la aplicación UpdateXpress

Los usuarios pueden utilizar la aplicación UpdateXpress para aplicar actualizaciones UXSP en su equipo. La aplicación UpdateXpress genera listados de los equipos en los que se aplicará la actualización, consulta una ubicación especificada para obtener una lista de paquetes de actualización aplicables, compara el inventario con la lista de actualización aplicable, recomienda un conjunto de actualizaciones por aplicar y, a continuación, despliega las actualizaciones al equipo.

Para aplicar UXSP a través de la aplicación UpdateXpress, haga lo siguiente:

1. Descargue la aplicación UpdateXpress del sitio Web de soporte de Lenovo.
2. Ejecute la aplicación UpdateXpress. Seleccione **Actualizar el equipo local** o **Actualizar un equipo remoto**.
3. Seleccione **Visite el sitio web de soporte de Lenovo**.
4. Seleccione **UpdateXpress System Packs (UXSP) de aplicación**.

Los usuarios pueden descargar las actualizaciones directamente desde el sitio web de soporte de Lenovo. Recuerde descargar la carga útil de la actualización así como el archivo XML. Para su comodidad, seleccione la misma carpeta destino para cada descarga UXSP. Los usuarios pueden descargar varios paquetes del sistema para distintos tipos de equipo a la misma carpeta. Cuando los usuarios ejecutan la aplicación UpdateXpress, esta detecta el tipo de equipo y utiliza el contenido correcto para ese tipo de equipo. En algunos casos, puede haber archivos comunes entre los paquetes del sistema. Los archivos comunes que ya se encuentran en la carpeta no se descargarán de nuevo. De este modo, se reduce el tiempo total de descarga.

Gestión de un UXSP como un conjunto

La aplicación UpdateXpress está diseñada para descargar y aplicar UXSP. Un UXSP es una colección de actualizaciones individuales especificada en el archivo XML del UXSP.

Al ejecutar la aplicación UpdateXpress, los usuarios pueden seleccionar trabajar con UXSP o con las actualizaciones individuales. En la mayor parte de los casos, es recomendable trabajar con UXSP, pero también existe la alternativa de trabajar con actualizaciones individuales, lo cual proporciona a los usuarios una mayor flexibilidad para elegir las actualizaciones a utilizar.

Gestión de requisitos de actualización

Este tema describe cómo se adquieren y aplican requisitos de actualización.

Para aplicar actualizaciones correctamente, se debe adquirir y aplicar también todos los requisitos previos y correquisitos para una actualización. La aplicación UpdateXpress automáticamente comprueba, adquiere y aplica requisitos previos y correquisitos. Con frecuencia, las actualizaciones necesitan que los usuarios apliquen archivos de requisito previo antes de que puedan aplicarse correctamente o incluir paquetes de correquisitos para usar correctamente la actualización aplicada. Para simplificar el proceso de actualización, la aplicación UpdateXpress utiliza información que se incluye en el archivo de actualización para identificar los paquetes requeridos para las actualizaciones especificadas. Posteriormente, la aplicación UpdateXpress aplica estos paquetes requeridos.

Archivos de requisito previo

Los paquetes de actualización proporcionados por Lenovo incluyen información sobre los archivos de requisito previo que deben aplicarse antes de que los usuarios apliquen la actualización correctamente. Cuando los usuarios especifican una actualización, la aplicación UpdateXpress lee esta información y localiza los paquetes de requisito previo.

De forma predeterminada, la aplicación UpdateXpress adquiere los paquetes de actualización y los evalúa para determinar si se cumplen los requisitos previos y, de ser necesario, aplica los archivos de requisito previo automáticamente antes de aplicar la actualización especificada. Los usuarios pueden elegir no aplicar los archivos de requisito previo. Sin embargo, esto puede tener como efecto que la actualización no se aplique correctamente.

Si los paquetes de requisitos previos tienen requisitos previos o correquisitos, se adquieren, evalúan y aplican del mismo modo.

Archivos de correquisito

Algunas actualizaciones requieren archivos de correquisito, esto es, paquetes adicionales que deben aplicarse para que la actualización se lleve a cabo correctamente, pero estos paquetes no deben aplicarse antes de la actualización especificada.

De forma predeterminada, la aplicación UpdateXpress identifica, adquiere, evalúa y aplica a los paquetes correquisitos como parte de la actualización.

Si los paquetes correquisitos tienen requisitos previos o correquisitos propios, se adquieren, evalúan y aplican del mismo modo.

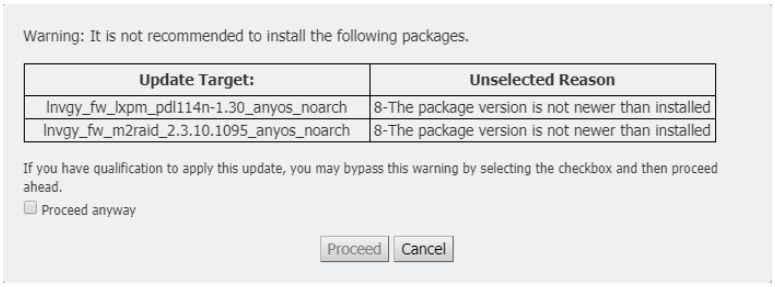
Ejemplo

Por ejemplo, supongamos la existencia de una actualización que tiene requisitos previos y correquisitos. De manera predeterminada, la aplicación UpdateXpress toma los pasos siguientes:

1. Para asegurarse de que puede realizar la actualización, primero la aplicación UpdateXpress descarga la actualización.
2. Se descargan los archivos de requisitos previos.
3. Se descargan los archivos de correquisito.
4. Los archivos de requisito previos o de correquisito se evalúan con respecto al estado actual del sistema. Si el sistema ya está en el nivel requerido porque ya se han aplicado estos requisitos, se omite el requisito.
5. Se aplican los archivos de requisitos previos necesarios.
6. Se aplica la actualización.
7. Se aplican los archivos de correquisito necesarios.

Recomendación de actualización

De manera predeterminada, la aplicación UpdateXpress seleccionará los paquetes recomendados para instalar o actualizar el sistema. Los usuarios también pueden seleccionar manualmente esos paquetes para instalarlos o actualizarlos. En este caso, los usuarios recibirán un mensaje de advertencia similar al siguiente:



Si los usuarios ven este mensaje, se recomienda detener el proceso de actualización.

Actualizaciones independientes del sistema operativo

Algunas actualizaciones individuales se aplican a tipos de equipo específicos, independientemente del sistema operativo que utilicen. Se trata a estas actualizaciones individuales como actualizaciones independientes del sistema operativo. Los usuarios pueden seleccionar actualizaciones independientes del sistema operativo del mismo modo que se seleccionan actualizaciones específicas de un sistema operativo.

Nota: Cuando los usuarios seleccionan actualizaciones para un sistema operativo específico, se incluyen actualizaciones independientes del sistema operativo como parte del paquete. Seleccione las actualizaciones independientes de sistema operativo solo si los usuarios no seleccionan actualizaciones de sistema operativo para un tipo de equipo.

Datos de inventario faltantes o incompletos

Ocasionalmente, se aplica un paquete de actualización a un componente cuya versión de firmware o controlador no es detectada por UpdateXpress. En este caso, la aplicación UpdateXpress muestra la versión del paquete de actualización en lugar de la versión del componente. Si no se detecta una versión de componente instalada, no se selecciona la actualización de forma predeterminada. En este caso, seleccione el paquete manualmente como una actualización recomendada.

Instalación de los controladores requeridos

La aplicación UpdateXpress instala controladores de dispositivo requeridos.

La aplicación UpdateXpress instala todos los controladores en el UXSP cuando:
- El controlador de dispositivo actual es anterior al controlador de dispositivo disponible en el UXSP.
- La aplicación UpdateXpress no puede determinar la versión actual del controlador de dispositivo, lo que generalmente ocurre cuando no está instalado el controlador de dispositivo.

  Nota: La aplicación UpdateXpress muestra `No Detectado` cuando no se detecta una versión del controlador de dispositivo instalado.

Los usuarios pueden aprovechar este comportamiento para instalar los siguientes controladores de dispositivos, los cuales son requisitos para las actualizaciones de firmware:
- Intelligent Peripheral Management Interface (IPMI)
- Capa de asignación de IPMI

Capítulo 2. Requisitos de hardware y software

Antes de que los usuarios comiencen a usar la aplicación UpdateXpress, revise el hardware, el sistema operativo, y los requisitos de privilegios de sistema operativo local. Los sistemas que ejecuten la aplicación UpdateXpress necesitan al menos 1 GB de memoria de acceso aleatorio (RAM).

Modelos de servidor admitidos

La aplicación UpdateXpress admite controladores de dispositivos y firmware de Windows y Linux que se incluyen en UXSP disponibles. Puede encontrar una lista de controladores de dispositivos y firmware de componentes admitidos actualmente en el archivo léame de la aplicación UpdateXpress que se incluye en cada paquete de sistema.

Tabla 1. Sistemas de Lenovo admitidos

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

Tabla 1. Sistemas de Lenovo admitidos (continuación)

Series	Modelos de servidor	
WenTian	• WA5480 G3/WA5488 G3 (7DE7) • WR3220 G2/WR3228 G2 (7DEC)	• WR5220 G3/WR5228 G3 (7D8Y)
Soluciones	• ThinkAgile Serie VX (7D28, 7D2Z, 7D43, 7DDK, 7Y12, 7Y13, 7Y14, 7Y92, 7Y93, 7Y94, 7Z12, 7Z13, 7Z62, 7Z63) • ThinkAgile Serie MX (7D19, 7D1B, 7D1H, 7D5R, 7D5S, 7D5T, 7D66, 7D67, 7D6B, 7DGG, 7Z20)	• ThinkAgile Serie HX (7D20, 7D2T, 7D46, 7D4R, 7D5U, 7X82, 7X83, 7X84, 7Y88, 7Y89, 7Y90, 7Y95, 7Y96, 7Z03, 7Z04, 7Z05, 7Z08, 7Z09, 7D0W, 7D0Y, 7D0Z, 7D11, 7D52, 7Z82, 7Z84, 7Z85)
System x	• Dispositivo HX 3310 (8693) • Dispositivo HX 5510/7510 (8695) • nx360 M5 (5465, 5467) • Nodo de cálculo x240 (7162, 2588) • Nodo de cálculo x240 M5 (2591, 9532) • x280 X6/x480 X6/x880 X6 Nodo de cálculo (4258, 7196)[2] • x440 (7167, 2590)	• x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M5 (5463, 8869) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6/x3950 X6 (6241)[2]
Notas: 1. Este modelo de servidor se basa en procesadores AMD de un zócalo. 2. Este modelo de servidor admite tanto un nodo único como varios nodos.		

Sistemas operativos compatibles

La aplicación UpdateXpress se admite en los sistemas operativos Windows y Linux.

Windows

La aplicación UpdateXpress se admite en sistemas operativos de 64 bits. Utilice la información en la tabla siguiente para identificar los sistemas operativos compatibles con la aplicación UpdateXpress.

Tabla 2. Sistemas operativos Windows admitidos

Sistema operativo	Actualización local	Actualización remota	Repositorio local	Configuración remota de RAID
Microsoft Windows 10/11 Pro para estaciones de trabajo (21H2/22H2)	Sí[nota]	Sí	Sí	Sí
Microsoft Windows Server 2016	Sí	Sí	Sí	Sí
Microsoft Windows Server 2019	Sí	Sí	Sí	Sí
Microsoft Windows Server 2022	Sí	Sí	Sí	Sí

Nota: Los modelos de servidor que admiten Microsoft Windows 10/11 Pro para estaciones de trabajo (21H2/22H2) también pueden acceder a la característica de actualización local.

Linux

La aplicación UpdateXpress se admite en las siguientes versiones de los sistemas operativos Linux.

Tabla 3. Sistemas operativos Linux admitidos

Sistema operativo	Actualización local	Actualización remota	Repositorio local	Configuración remota de RAID
Red Hat Enterprise Linux 7.X (7.6 y versiones posteriores)	Sí	Sí	Sí	Sí
Red Hat Enterprise Linux 8.X	Sí	Sí	Sí	Sí
Red Hat Enterprise Linux 9.X	Sí	Sí	Sí	Sí
SUSE Linux Enterprise Server 15.X	Sí	Sí	Sí	Sí

Notas:
- Al ejecutar la aplicación UpdateXpress en un sistema operativo Linux, es recomendable disponer de 500 MB de espacio libre de disco.
- La aplicación UpdateXpress admite la comprobación difusa de sistemas operativos. Si el sistema operativo actual no admite los paquetes de firmware en un UXSP, los paquetes de firmware también pueden aparecer en el resultado de comparación de la aplicación UpdateXpress.
- Dependiendo del comando `ifconfig` del sistema operativo Linux, es posible que UpdateXpress no esté instalado en RHEL 7.0 o versiones posteriores. Para actualizar el firmware en RHEL 7.0 o versiones posteriores, los usuarios deben instalar las herramientas de red.
- Las actualizaciones del controlador de dispositivos de Linux requieren paquetes específicos. Se requiere los siguientes paquetes para la instalación:
  - Red Hat Enterprise Linux: rpm-build, perl y bash
  - SUSE Enterprise Linux: perl y bash
- Para los siguientes sistemas operativos, los usuarios pueden utilizar UpdateXpress 4.3.0 en su lugar:
  - SUSE 12.5
- Para los siguientes sistemas operativos, los usuarios pueden utilizar UpdateXpress 4.1.0 en su lugar:
  - RedHat 7.5
  - SUSE 12.4
- Para los siguientes sistemas operativos, los usuarios pueden utilizar UpdateXpress 3.4.0 en su lugar:
  - 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

Privilegios de sistema operativo

Para ejecutar la aplicación UpdateXpress, los usuarios deben tener privilegios de administrador o de acceso a raíz equivalentes en el sistema operativo. La aplicación UpdateXpress devuelve un error cuando un usuario sin privilegios suficientes intenta ejecutar el programa.

Guarde la aplicación UpdateXpress, con sus extracciones, y todos los registros confidenciales en un espacio seguro accesible solo a usuarios autorizados.

Capítulo 3. Uso de la aplicación UpdateXpress

Los usuarios pueden utilizar la aplicación UpdateXpress para desplegar actualizaciones de forma interactiva. Es recomendable usar una resolución de pantalla de 1024 x 768 o superior al ejecutar la aplicación UpdateXpress. Para ejecutar la aplicación UpdateXpress, extraiga el archivo comprimido e invoque el archivo ejecutable para el sistema operativo. No se requiere ninguna instalación.

Windows

En sistemas operativos Windows, la aplicación UpdateXpress recibe la siguiente convención de nomenclatura:

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

Para cada versión de la aplicación UpdateXpress, los usuarios pueden distinguir el nombre del archivo ZIP para Windows según su número de versión. El archivo ZIP de Windows se especifica como **lnvgy_utl_lxce_ux{ build id }_{ version }_windows_i386.zip** donde *lnvgy_utl_lxce_ux* indica el nombre del archivo ZIP y *build id* indica el número de versión y *version* indica el número de versión de la aplicación UpdateXpress.

Linux

En sistemas operativos Linux, la aplicación UpdateXpress recibe la siguiente convención de nomenclatura:

Sistema operativo	Nombre de la aplicación UpdateXpress
Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T y superior	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T y superior	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`

El nombre de la aplicación UpdateXpress difiere en función de si está orientada a sistemas operativos Windows o Linux. Para su comodidad, en adelante se utilizará <*Zipfile*> para aludir en esta documentación al nombre de la aplicación UpdateXpress, independientemente de si es para sistema operativos Windows o Linux.

Inicio de la aplicación UpdateXpress

Los usuarios pueden utilizar la aplicación UpdateXpress para adquirir las UXSP y las actualizaciones individuales más recientes.

Para iniciar la aplicación UpdateXpress, haga lo siguiente:

- **Para Windows**:
  1. Extraiga el <*Zipfile*> a una carpeta local.
  2. Realice una de las acciones siguientes:
     - Haga doble clic en **lxce_ux.exe**.
     - Haga clic con el botón derecho en **lxce_ux.exe** y haga clic en **Ejecutar como administrador** en el menú emergente.
- **Para Linux**:

  Escriba los siguientes comandos en el terminal:

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

Actualización de un servidor local desde el sitio Web

La aplicación UpdateXpress puede actualizar un equipo local mediante UXSP o actualizaciones individuales adquiridas desde el sitio Web.

Los siguientes requisitos previos son necesarios para completar esta tarea:
- La aplicación UpdateXpress se ejecuta desde el equipo local que se desea actualizar.
- La máquina está ejecutando un sistema operativo con una versión admitida. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para actualizar un equipo local desde el sitio Web, haga lo siguiente:
1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Administrar el servidor local**. Si se selecciona **Ingresar información de acceso a BMC** ingrese la información del BMC en esta ventana y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
5. En la ventana Actualizar configuración, lleve a cabo una o más de las siguientes acciones:
   - Para actualizar el firmware del sistema de copia de seguridad, seleccione **Actualizar solo la imagen de copia de seguridad del BMC (y la UEFI según corresponda)** y haga clic en **Siguiente**.
   - Para degradar el firmware, seleccione **Habilitar actualización en un firmware de nivel posterior** y haga clic en **Siguiente**.
6. En la ventana Ubicación de actualizaciones, seleccione **Visitar el sitio web de soporte de Lenovo** y haga clic en **Siguiente**.
7. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
8. En la ventana Directorio de destino, especifique la ubicación para descargar las actualizaciones o acepte la ubicación predeterminada y haga clic en **Siguiente**.
9. En la página Acceso a Internet, si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
   Si los usuarios tienen más inquietudes de seguridad, antes de hacer clic en **Probar conexión**, lleve a cabo una o más de las siguientes acciones:
   - Configure **Servidor proxy**:
     a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

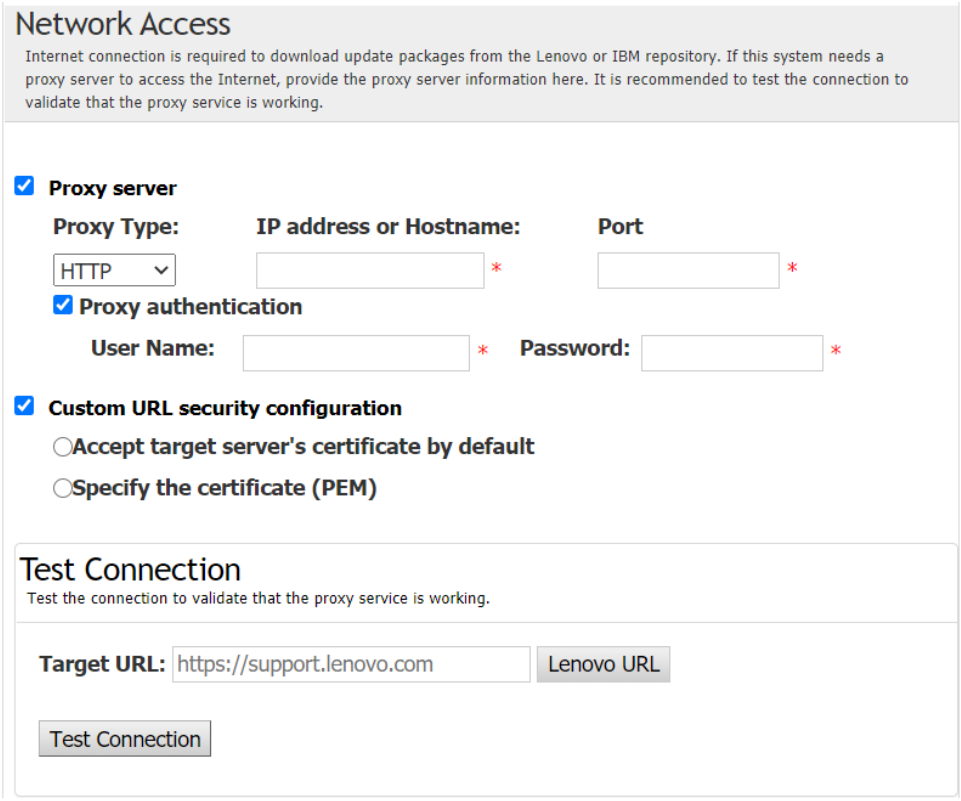
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

     b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

- Configure **Configuración de seguridad de URL personalizada**

  Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
  - **Aceptar el certificado del servidor de destino de manera predeterminada**
  - **Especificar el certificado (PEM)**



10. En la ventana Actualizar recomendación, lleve a cabo una o más de las siguientes acciones:
    - Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones de dispositivos no detectados**.
    - Para actualizar el componente, seleccione el componente de destino y haga clic en **Siguiente**.
11. En la ventana Adquirir actualizaciones, la tabla de adquisición muestra el avance de adquisición de paquetes. Al finalizar el progreso, haga clic en **Siguiente**.
12. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.
13. En la ventana Finalizar, haga clic en **Ver registro** para comprobar el registro de actualización y, a continuación, haga clic en **Cerrar** para salir.

Actualización de un servidor local desde un directorio local

La aplicación UpdateXpress puede actualizar un equipo local mediante UXSP o actualizaciones individuales adquiridas desde una carpeta local.

Los siguientes requisitos previos son necesarios para completar esta tarea:
- La aplicación UpdateXpress se ejecuta desde el equipo local que se desea actualizar.
- La máquina está ejecutando un sistema operativo con una versión admitida. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- El ISO montado no debe utilizarse como un directorio local válido; de lo contrario, podría desmontarse durante el proceso de actualización y provocar un error flash.

Para actualizar un equipo local desde un directorio local, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor local** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
5. En la ventana Actualizar configuración, lleve a cabo una o más de las siguientes acciones:
   - Para actualizar la imagen de copia de seguridad de BMC o de UEFI, seleccione **Actualizar solo la imagen de copia de seguridad del BMC (y de UEFI cuando proceda)** y, a continuación, haga clic en **Siguiente**.
   - Para degradar el firmware, seleccione **Habilitar actualización en un firmware de nivel posterior** y haga clic en **Siguiente**.
6. En la ventana Ubicación de actualizaciones, seleccione **Buscar en un directorio local**. Para especificar una carpeta local, realice una de las siguientes acciones:
   - Haga clic en **Examinar**, seleccione la carpeta de destino y, a continuación, haga clic en **Siguiente**.
   - Escriba la ruta de la carpeta en el campo ubicado junto al botón **Examinar** y haga clic en **Siguiente**.
7. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
8. En la ventana Actualizar recomendación, lleve a cabo una de las siguientes acciones:
   - Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones sin adaptadores detectados**.
   - Para comparar las versiones del firmware y del controlador instaladas con las versiones más recientes, haga clic en **Comenzar**. Una vez completado el proceso, seleccione uno o varios paquetes de destino y haga clic en **Siguiente**.
   - Para comparar la versión de dispositivos instalada en el sistema local con la versión más reciente, seleccione **Solo comparar dispositivos instalados** y haga clic en **Comenzar**. Una vez completado el proceso, seleccione uno o varios paquetes de destino y haga clic en **Siguiente**.
9. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.
10. En la ventana Finalizar, haga clic en **Ver registro** para comprobar el registro de actualización y, a continuación, haga clic en **Cerrar** para salir.

Actualización de un servidor remoto desde el sitio Web

La aplicación UpdateXpress puede actualizar un equipo remoto mediante UXSP o actualizaciones individuales adquiridas desde el sitio web.

El siguientes requisito previo es necesario para completar esta tarea:

La aplicación UpdateXpress se ejecuta en un equipo con un sistema operativo instalado. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para actualizar un equipo remoto desde el sitio web, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - **(Configuración) Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - **(Configuración) Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - **(Configuración) Contraseña**: la contraseña de BMC del sistema de destino.
   - **(Configuración) Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si no comprueba el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
5. En la ventana Actualizar configuración, seleccione una o más de las opciones: Si se selecciona **Usar un servidor remoto en lugar del correspondiente al BMC**, introduzca la siguiente información:
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Dirección IP o nombre de host**: dirección IP o nombre de host del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Nombre de usuario**: el nombre de usuario del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Contraseña**: la contraseña del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Puerto**: número de puerto del servidor. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Directorio**: la ubicación del servidor donde se copian los paquetes de actualización.

     Nota: Ingrese una ruta completa en el servidor SFTP/HTTP/HTTPS/FTP. El servidor FTP solo se usa para el dispositivo ThinkServer marcado con un superíndice 2 (Nota 2) en "Modelos de servidor admitidos" en la página 5.
6. Para configurar la huella dactilar de la clave del servidor SFTP, lleve a cabo una de las acciones siguientes:
   - Para comprobar la huella dactilar de la clave del servidor SFTP, haga clic en **Sí**.
   - Para no comprobar la huella dactilar de la clave del servidor SFTP/HTTPS, seleccione **Omitir la comprobación de la huella dactilar de la clave del servidor SFTP** y haga clic en **Siguiente**.
7. Lleve a cabo una o más de las acciones siguientes:
   - Para degradar el firmware, seleccione **Habilitar actualización en un firmware de nivel posterior** y haga clic en **Siguiente**.
   - Para actualizar el firmware del sistema de copia de seguridad, seleccione **Actualizar solo la imagen de copia de seguridad del BMC (y la UEFI según corresponda)** y luego haga clic en **Siguiente**.
8. En la ventana Ubicación de actualizaciones, seleccione **Visitar el sitio web de soporte de Lenovo** y haga clic en **Siguiente**.
9. En la ventana Directorio de destino, especifique la ubicación para descargar las actualizaciones o acepte la ubicación predeterminada y haga clic en **Siguiente**.
10. En la página Acceso a Internet, si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
    Si los usuarios tienen más consideraciones de seguridad, antes de hacer clic en **Probar conexión**, configure el **Servidor proxy** o los valores de **Configuración de seguridad de URL personalizada** en función de los requisitos de seguridad, como se indica a continuación:
    - **Servidor proxy**
      a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

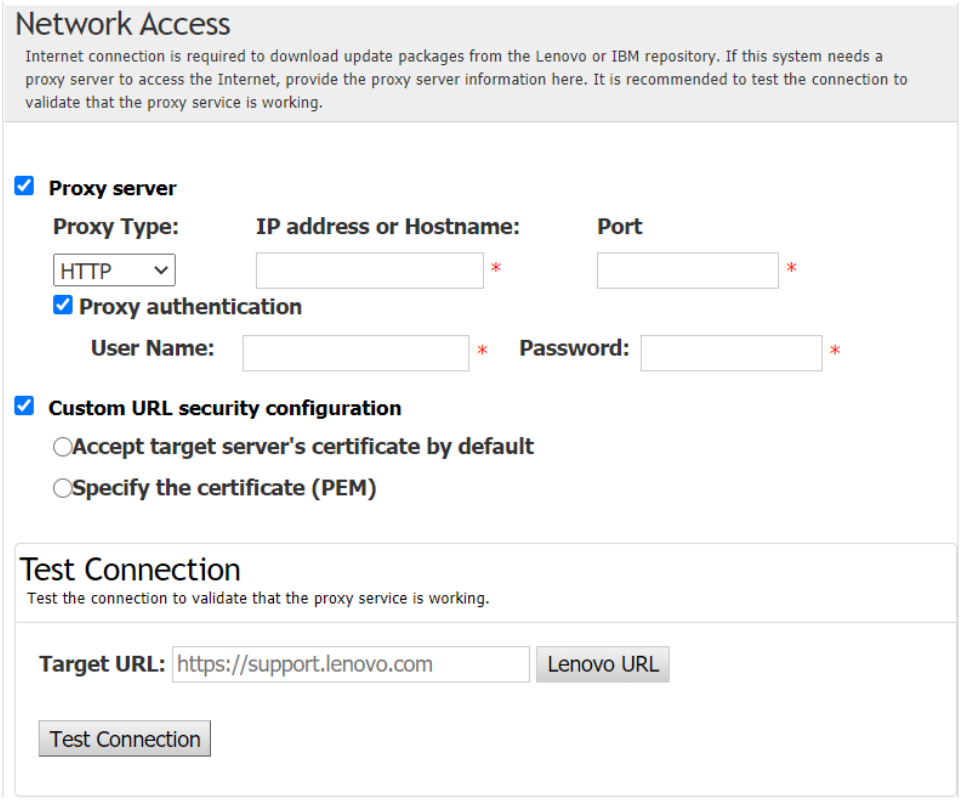
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

      b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

    - **Configuración de seguridad de URL personalizada**

Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
- **Aceptar el certificado del servidor de destino de manera predeterminada**
- **Especificar el certificado (PEM)**



11. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
12. En la ventana Actualizar recomendación, lleve a cabo una o más de las siguientes acciones:
    - Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones de dispositivos no detectados**.
    - Para actualizar el componente, seleccione el componente de destino y haga clic en **Siguiente**.
13. En la ventana Adquirir actualizaciones, la tabla de adquisición muestra el avance de adquisición de paquetes. Al finalizar el progreso, haga clic en **Siguiente**.
14. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.
15. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Actualización de un servidor remoto desde un directorio local

La aplicación UpdateXpress puede actualizar un equipo remoto mediante UXSP o actualizaciones individuales adquiridas desde una carpeta local.

El siguientes requisito previo es necesario para completar esta tarea:

La aplicación UpdateXpress se ejecuta en un equipo con un sistema operativo instalado. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.

Para actualizar un equipo remoto desde un directorio local, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no tienen intención de comprobar el certificado BMC del servidor y la huella digital de clave del servidor SFTP/HTTPS, seleccione **Aceptar certificado de servidor BMC y huella digital del servidor SFTP/HTTPS de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
5. En la ventana Actualizar configuración, si se selecciona **Usar un servidor remoto independiente**, introduzca la siguiente información:
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Dirección IP o nombre de host**: dirección IP o nombre de host del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Nombre de usuario**: el nombre de usuario del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Contraseña**: la contraseña del servidor.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Puerto**: número de puerto del servidor. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.
   - (Configuración de SFTP/HTTP/HTTPS/FTP) **Directorio**: la ubicación del servidor donde se copian los paquetes de actualización.

     Nota: Ingrese una ruta completa en el servidor SFTP/HTTP/HTTPS/FTP. El servidor FTP solo se usa para el dispositivo ThinkServer marcado con un superíndice 2 (Nota 2) en “Modelos de servidor admitidos” en la página 5.
6. Para configurar la huella dactilar de la clave del servidor SFTP, lleve a cabo una de las acciones siguientes:
   - Para comprobar la huella dactilar de la clave del servidor SFTP, haga clic en **Sí**.
   - Para no comprobar la huella dactilar de la clave del servidor SFTP/HTTPS, seleccione **Omitir la comprobación de la huella dactilar de la clave del servidor SFTP** y haga clic en **Siguiente**.
7. Lleve a cabo una o más de las acciones siguientes:
   - Para degradar el firmware, seleccione **Habilitar actualización en un firmware de nivel posterior** y haga clic en **Siguiente**.
   - Para actualizar el firmware del sistema de copia de seguridad, seleccione **Actualizar solo la imagen de copia de seguridad del BMC (y la UEFI según corresponda)** y luego haga clic en **Siguiente**.
8. En la ventana Ubicación de actualizaciones, seleccione **Buscar en un directorio local**. Para especificar una carpeta local, realice una de las siguientes acciones:
   - Haga clic en **Examinar**, seleccione la carpeta deseada y haga clic en **Siguiente**.
   - Escriba la ruta de la carpeta en el campo ubicado junto al botón **Examinar** y haga clic en **Siguiente**.
9. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
10. En la ventana Actualizar recomendación, haga clic en **Comenzar** para comparar la versión del firmware instalada con la versión más reciente. Una vez completado el proceso, seleccione uno o varios paquetes de destino y haga clic en **Siguiente**.

    Nota: Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones sin adaptadores detectados** antes de hacer clic en **Comenzar**.
11. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.

12. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Configuración de BIOS en un servidor remoto

La aplicación UpdateXpress admite la configuración de los valores de BIOS para servidores remotos.

Requisito previo:

La función de configuración de BIOS para el servidor remoto solo se admite en servidores ThinkServer/ WenTian. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para configurar la BIOS, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no tienen intención de comprobar el certificado BMC del servidor y la huella digital de clave del servidor SFTP/HTTPS, seleccione **Aceptar certificado de servidor BMC y huella digital del servidor SFTP/HTTPS de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Configuración de BIOS** y haga clic en **Siguiente**.
5. En la ventana Modo de configuración, seleccione **Configuración común de BIOS** o **Importar archivo de configuración de BIOS** y, a continuación, haga clic en **Siguiente**.
6. Realice una de las acciones siguientes:
   - Si se seleccionó **Importar archivo de configuración de BIOS** en el paso anterior, omita este paso.
   - Si se seleccionó **Configuración común de BIOS** en el paso anterior, seleccione uno o más de los valores actuales y haga clic en **Siguiente**.
7. En la ventana Vista de cambio de BIOS, los datos se cambiarán con los valores **mostrado**, **comprobar** y **confirmar**. Haga clic en **Siguiente**.
8. En la ventana Exportar configuración de BIOS, exporte la configuración como un archivo. Especifique la ubicación del archivo exportado y haga clic en **Siguiente**.
9. En la ventana Configuración en ejecución, seleccione **Reiniciar manualmente** o **Reiniciar inmediatamente** y, a continuación, haga clic en **Iniciar**. Una vez finalizada la tarea, haga clic en **Siguiente**.
10. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de configuración y, a continuación, haga clic en **Cerrar** para salir.

Recopilación de registros de un servidor remoto

La aplicación UpdateXpress admite la recopilación de registros de un servidor remoto.

Requisito previo:

La función de recopilación múltiple para un servidor remoto solo se admite en servidores ThinkServer/ WenTian. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para recopilar registros, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no tienen intención de comprobar el certificado BMC del servidor y la huella digital de clave del servidor SFTP/HTTPS, seleccione **Aceptar certificado de servidor BMC y huella digital del servidor SFTP/HTTPS de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Recopilar registros** y haga clic en **Siguiente**.
5. En la ventana Modo de recopilación de registros, seleccione **Recopilar registro de BMC** o **Recopilar registro de FFDC**, o ambos, especifique el directorio de salida de registro y haga clic en **Siguiente**.
6. En la ventana Resultado de recopilación de registros, revise los resultados y, a continuación, haga clic en **Siguiente**.
7. En la ventana Finalizar, haga clic en  para revisar los registros detallados y, a continuación, haga clic en **Cerrar** para salir.

Actualización de varios servidores remotos desde el sitio Web

La aplicación UpdateXpress admite la actualización de servidores remotos por lotes desde un sitio Web.

Nota: Para actualizar el servidor remoto único desde el sitio Web, consulte la página Web “Actualización de un servidor remoto desde el sitio Web” en la página 12.

Requisito previo:

La función de actualización múltiple para servidores remotos solo es compatible con servidores ThinkServer y el servidor WenTian. Para obtener más detalles acerca de servidores compatibles, consulte “Modelos de servidor admitidos” en la página 5.

Para actualizar varios servidores remotos desde el sitio web, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestión de varios servidores** y haga clic en **Siguiente**.
4. En la ventana Gestión de varios servidores, seleccione **Añadir nuevos servidores al grupo de servidores**, realice uno o más de los procedimientos siguientes y, por último, haga clic en **Siguiente**.
   - Para añadir nuevos servidores al grupo de servidores, especifique el rango de direcciones IP y haga clic en **Detectar** en el área de información de BMC y, a continuación, seleccione uno o varios servidores de destino de la lista Grupo de servidores.
   - Para quitar el servidor de la lista Grupo de servidores, seleccione uno o varios servidores de destino y haga clic en **Quitar seleccionados**.
   - Para verificar si el nombre de usuario y la contraseña son correctos para el servidor, seleccione uno o varios servidores de destino y, a continuación, haga clic en **Explorar seleccionados**.
   - Para utilizar credenciales comunes de BMC para la gestión, seleccione **Usar credenciales comunes de BMC para gestión**, escriba el nombre de usuario y la contraseña.
   - Para exportar la lista de Grupo de servidores del servidor actual, haga clic en **Exportar**. La lista de grupo de servidores se guardará en el archivo `configure.json`.

- Para importar la lista de grupo de servidores al otro servidor, haga clic en **Importar** y seleccione el archivo `configure.json` de destino.

5. Haga clic en **Siguiente**; se mostrará un mensaje de recordatorio a los usuarios que confirmen si el certificado debe actualizarse. Haga clic en **Aceptar** para actualizar el certificado.

   Nota: Si los usuarios inician sesión por primera vez o la contraseña ha caducado, cambie la contraseña en la ventana Cambiar contraseña.
6. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
7. En la ventana Actualizar configuración, seleccione una o más de las opciones: Si se selecciona **Usar un servidor remoto en lugar del correspondiente al BMC**, introduzca la siguiente información:
   - (Configuración de HTTP/FTP) **Dirección IP o nombre de host**: dirección IP o nombre de host del servidor.
   - (Configuración de HTTPS/FTP) **Nombre de usuario**: el nombre de usuario del servidor.
   - (Configuración de HTTPS/FTP) **Contraseña**: la contraseña del servidor.
   - (Configuración de HTTPS/FTP) **Puerto**: número de puerto del servidor. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.
   - (Configuración de HTTPS/FTP) **Directorio**: La ubicación del servidor a donde se copian los paquetes de actualización.

     Nota: Ingrese una ruta completa en el servidor HTTPS/FTP. El servidor FTP solo se usa para el dispositivo ThinkServer marcado con un superíndice 2 (Nota 2) en “Modelos de servidor admitidos” en la página 5.
8. Para configurar la huella dactilar de la clave del servidor HTTPS, lleve a cabo una de las acciones siguientes:
   - Para comprobar la huella dactilar de la clave del servidor HTTPS, haga clic en **Sí**.
   - Para no comprobar la huella dactilar de la clave del servidor HTTPS, seleccione **Omitir la comprobación de la huella dactilar de la clave del servidor HTTPS** y haga clic en **Siguiente**.
9. En la ventana Ubicación de actualizaciones, seleccione **Visitar el sitio web de soporte de Lenovo** y haga clic en **Siguiente**.
10. En la ventana Directorio de destino, especifique la ubicación para descargar las actualizaciones o acepte la ubicación predeterminada y haga clic en **Siguiente**.
11. En la página Acceso a Internet, si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
    Si los usuarios tienen más consideraciones de seguridad, antes de hacer clic en **Probar conexión**, configure el **Servidor proxy** o los valores de **Configuración de seguridad de URL personalizada** en función de los requisitos de seguridad, como se indica a continuación:
    - **Servidor proxy**
      a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

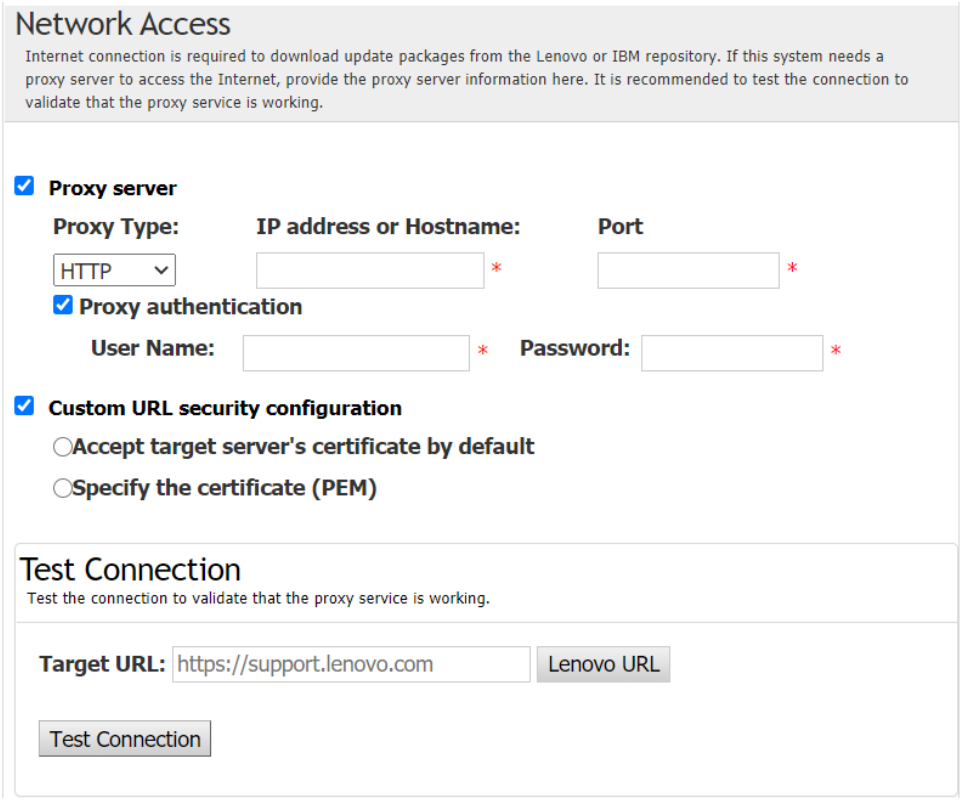
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

      b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

    - **Configuración de seguridad de URL personalizada**

Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
- **Aceptar el certificado del servidor de destino de manera predeterminada**
- **Especificar el certificado (PEM)**



12. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
13. En la ventana Actualizar recomendación, haga clic en **Comenzar** para comparar la versión del firmware con la versión más reciente. Una vez completado el proceso, seleccione uno o varios paquetes de destino y haga clic en **Siguiente**.

    Nota: Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones sin adaptadores detectados** antes de hacer clic en **Comenzar**.
14. En la ventana Adquirir actualizaciones, la tabla de adquisición muestra el avance de adquisición de paquetes. Al finalizar el progreso, haga clic en **Siguiente**.
15. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.
16. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Actualización de varios servidores remotos desde un directorio local

La aplicación UpdateXpress admite la actualización de servidores remotos por lotes desde una carpeta local.

Nota: Para actualizar un servidor remoto específico desde una carpeta local, consulte “Actualización de un servidor remoto desde un directorio local” en la página 14.

Requisito previo:

La función de actualización múltiple para servidores remotos solo es compatible con servidores ThinkServer y el servidor WenTian. Para obtener más detalles acerca de servidores compatibles, consulte “Modelos de servidor admitidos” en la página 5.

Para actualizar varios servidores remotos desde un directorio local, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestión de varios servidores** y haga clic en **Siguiente**.
4. En la ventana Gestión de varios servidores, seleccione **Añadir nuevos servidores al grupo de servidores**, realice uno o más de los procedimientos siguientes y, por último, haga clic en **Siguiente**.
   - Para añadir nuevos servidores al grupo de servidores, especifique el rango de direcciones IP y haga clic en **Detectar** en el área de información de BMC y, a continuación, seleccione uno o varios servidores de destino de la lista Grupo de servidores.
   - Para quitar el servidor de la lista Grupo de servidores, seleccione uno o varios servidores de destino y haga clic en **Quitar seleccionados**.
   - Para verificar si el nombre de usuario y la contraseña son correctos para el servidor, seleccione uno o varios servidores de destino y, a continuación, haga clic en **Explorar seleccionados**.
   - Para utilizar credenciales comunes de BMC para la gestión, seleccione **Usar credenciales comunes de BMC para gestión**, escriba el nombre de usuario y la contraseña.
   - Para exportar la lista de Grupo de servidores del servidor actual, haga clic en **Exportar**. La lista de grupo de servidores se guardará en el archivo `configure.json`.
   - Para importar la lista de grupo de servidores al otro servidor, haga clic en **Importar** y seleccione el archivo `configure.json` de destino.
5. Haga clic en **Siguiente**; se mostrará un mensaje de recordatorio a los usuarios que confirmen si el certificado debe actualizarse. Haga clic en **Aceptar** para actualizar el certificado.

   Nota: Si los usuarios inician sesión por primera vez o la contraseña ha caducado, cambie la contraseña en la ventana Cambiar contraseña.
6. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
7. En la ventana Actualizar configuración, seleccione una o más de las opciones: Si se selecciona **Usar un servidor remoto en lugar del correspondiente al BMC**, introduzca la siguiente información:
   - (Configuración de HTTP/FTP) **Dirección IP o nombre de host**: dirección IP o nombre de host del servidor.
   - (Configuración de HTTPS/FTP) **Nombre de usuario**: el nombre de usuario del servidor.
   - (Configuración de HTTPS/FTP) **Contraseña**: la contraseña del servidor.
   - (Configuración de HTTPS/FTP) **Puerto**: número de puerto del servidor. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.
   - (Configuración de HTTPS/FTP) **Directorio**: La ubicación del servidor a donde se copian los paquetes de actualización.

     Nota: Ingrese una ruta completa en el servidor HTTPS/FTP. El servidor FTP solo se usa para el dispositivo ThinkServer marcado con un superíndice 2 (Nota 2) en “Modelos de servidor admitidos” en la página 5.
8. En la ventana Ubicación de actualizaciones, seleccione **Buscar en un directorio local**. Para especificar una carpeta local, realice una de las siguientes acciones:
   - Haga clic en **Examinar**, seleccione la carpeta deseada y haga clic en **Siguiente**.
   - Escriba la ruta de la carpeta en el campo ubicado junto al botón **Examinar** y haga clic en **Siguiente**.
9. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
10. En la ventana Actualizar recomendación, haga clic en **Comenzar** para comparar la versión del firmware instalada con la versión más reciente. Una vez completado el proceso, seleccione uno o varios paquetes de destino y haga clic en **Siguiente**.

Nota: Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones sin adaptadores detectados** antes de hacer clic en **Comenzar**.

11. En la ventana Ejecución de la actualización, haga clic en **Iniciar actualización y confirmar para continuar en la ventana emergente**. La tabla de ejecución muestra el progreso de la actualización de los paquetes. Al finalizar el progreso de la actualización, haga clic en **Siguiente**.
12. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Configuración de BIOS para varios servidores remotos

La aplicación UpdateXpress admite la configuración de los valores de BIOS para varios servidores remotos por lotes.

Requisito previo:

La función de configuración múltiple para el servidor remoto solo se admite en servidores ThinkServer/ WenTian. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para configurar la BIOS, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestión de varios servidores** y haga clic en **Siguiente**.
4. En la ventana Gestión de varios servidores, seleccione **Añadir nuevos servidores al grupo de servidores**, realice uno o más de los procedimientos siguientes y, por último, haga clic en **Siguiente**.
   - Para añadir nuevos servidores al grupo de servidores, especifique el rango de direcciones IP y haga clic en **Detectar** en el área de información de BMC y, a continuación, seleccione uno o varios servidores de destino de la lista Grupo de servidores.
   - Para quitar el servidor de la lista Grupo de servidores, seleccione uno o varios servidores de destino y haga clic en **Quitar seleccionados**.
   - Para verificar si el nombre de usuario y la contraseña son correctos para el servidor, seleccione uno o varios servidores de destino y, a continuación, haga clic en **Explorar seleccionados**.
   - Para utilizar credenciales comunes de BMC para la gestión, seleccione **Usar credenciales comunes de BMC para gestión**, escriba el nombre de usuario y la contraseña.
   - Para exportar la lista de Grupo de servidores del servidor actual, haga clic en **Exportar**. La lista de grupo de servidores se guardará en el archivo `configure.json`.
   - Para importar la lista de grupo de servidores al otro servidor, haga clic en **Importar** y seleccione el archivo `configure.json` de destino.
5. Haga clic en **Siguiente**; se mostrará un mensaje de recordatorio a los usuarios que confirmen si el certificado debe actualizarse. Haga clic en **Aceptar** para actualizar el certificado.

   Nota: Si los usuarios inician sesión por primera vez o la contraseña ha caducado, cambie la contraseña en la ventana Cambiar contraseña.
6. En la ventana Tarea, seleccione **Configuración de BIOS** y haga clic en **Siguiente**.

   Nota: Esta función de configuración de BIOS solo se admite en servidor con los mismos tipos de equipo.
7. En la ventana Modo de configuración, seleccione **Configuración común de BIOS** o **Importar archivo de configuración de BIOS** y, a continuación, haga clic en **Siguiente**.
8. Realice una de las acciones siguientes:
   - Si se seleccionó **Importar archivo de configuración de BIOS** en el paso anterior, omita este paso.
   - Si se seleccionó **Configuración común de BIOS** en el paso anterior, seleccione uno o más de los valores actuales y haga clic en **Siguiente**.
9. En la ventana Vista de cambio de BIOS, confirme los valores modificados de BIOS y, a continuación, haga clic en **Siguiente**.

10. En la ventana Exportar configuración de BIOS, exporte la configuración como un archivo. Especifique la ubicación del archivo exportado y haga clic en **Siguiente**.
11. En la ventana Configuración en ejecución, seleccione **Reiniciar manualmente** o **Reiniciar inmediatamente** y, a continuación, haga clic en **Iniciar**. Una vez finalizada la tarea, haga clic en **Siguiente**.
12. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de configuración y, a continuación, haga clic en **Cerrar** para salir.

Recopilación de registros para varios servidores remotos

La aplicación UpdateXpress admite la recopilación de registros de servidores remotos por lotes.

Requisito previo:

La función de recopilación múltiple para el servidor remoto solo se admite en servidores ThinkServer/ WenTian. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.

Para recopilar registros, haga lo siguiente:
1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestión de varios servidores** y haga clic en **Siguiente**.
4. En la ventana Gestión de varios servidores, seleccione **Añadir nuevos servidores al grupo de servidores**, realice uno o más de los procedimientos siguientes y, por último, haga clic en **Siguiente**.
   - Para añadir nuevos servidores al grupo de servidores, especifique el rango de direcciones IP y haga clic en **Detectar** en el área de información de BMC y, a continuación, seleccione uno o varios servidores de destino de la lista Grupo de servidores.
   - Para quitar el servidor de la lista Grupo de servidores, seleccione uno o varios servidores de destino y haga clic en **Quitar seleccionados**.
   - Para verificar si el nombre de usuario y la contraseña son correctos para el servidor, seleccione uno o varios servidores de destino y, a continuación, haga clic en **Explorar seleccionados**.
   - Para utilizar credenciales comunes de BMC para la gestión, seleccione **Usar credenciales comunes de BMC para gestión**, escriba el nombre de usuario y la contraseña.
   - Para exportar la lista de Grupo de servidores del servidor actual, haga clic en **Exportar**. La lista de grupo de servidores se guardará en el archivo `configure.json`.
   - Para importar la lista de grupo de servidores al otro servidor, haga clic en **Importar** y seleccione el archivo `configure.json` de destino.
5. Haga clic en **Siguiente**; se mostrará un mensaje de recordatorio a los usuarios que confirmen si el certificado debe actualizarse. Haga clic en **Aceptar** para actualizar el certificado.

   Nota: Si los usuarios inician sesión por primera vez o la contraseña ha caducado, cambie la contraseña en la ventana Cambiar contraseña.
6. En la ventana Tarea, seleccione **Recopilar registros** y haga clic en **Siguiente**.
7. En la ventana Modo de recopilación de registros, seleccione **Recopilar registro de BMC** o **Recopilar registro de FFDC** o ambos, especifique el directorio de salida de registro y haga clic en **Siguiente**.
8. En la ventana Resultado de recopilación de registros, compruebe los resultados y, a continuación, haga clic en **Siguiente**.
9. En la ventana Finalizar, haga clic en  para revisar el registro de configuración y, a continuación, haga clic en **Cerrar** para salir.

Creación de un repositorio de actualizaciones

La aplicación UpdateXpress puede crear un repositorio de UXSP o actualizaciones individuales adquiridas desde el sitio Web.

Los siguientes requisitos previos son necesarios para completar esta tarea:
- La aplicación UpdateXpress se ejecuta en un equipo en el que se creará el repositorio.
- La máquina está ejecutando un sistema operativo con una versión admitida. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.

Para crear un repositorio de actualizaciones, haga lo siguiente:
1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Crear un repositorio de actualizaciones** y haga clic en **Siguiente**.
4. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
   - Seleccione **UpdateXpress System Packs (UXSP)** para actualizar USXP. La ventana Selección de actualizaciones se omite si se selecciona **UpdateXpress System Packs (UXSP)**, pero se descargarán todos los paquetes UXSP.
   - Seleccione **Últimas actualizaciones individuales disponibles** para actualizar los paquetes individuales. En el paso siguiente, aparecerá la ventana Selección de actualizaciones si se selecciona **Últimas actualizaciones individuales disponibles**, los usuarios deben seleccionar los paquetes de destino.
5. En la página Acceso a Internet, si no hay requisitos especiales con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y, luego, haga clic en **Siguiente**.
   Si los usuarios tienen más consideraciones de seguridad, antes de hacer clic en **Probar conexión**, configure el **Servidor proxy** o los valores de **Configuración de seguridad de URL personalizada** en función de los requisitos de seguridad, como se indica a continuación:
   - **Servidor proxy**
     a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

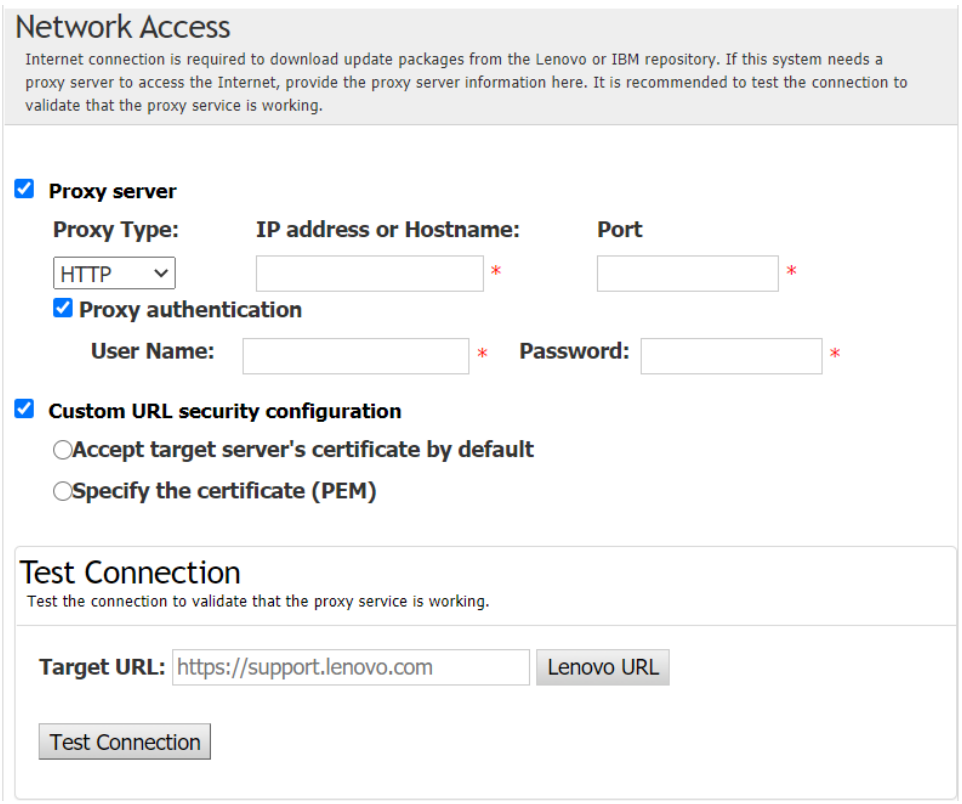
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

     b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

   - **Configuración de seguridad de URL personalizada**

     Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
     – **Aceptar el certificado del servidor de destino de manera predeterminada**
     – **Especificar el certificado (PEM)**



6. En la ventana Tipos de equipo, seleccione los tipos de equipo de destino y haga clic en **Siguiente**.
   - Para seleccionar todos los tipos de equipo enumerados, seleccione la casilla de verificación en el encabezado.
   - Para añadir un tipo de máquina, haga clic en **Añadir** y especifique el tipo de equipo.
   - Para quitar un tipo de equipo, seleccione el tipo de equipo de la lista y haga clic en **Quitar**.
   - Para actualizar la lista de tipos de equipo a la versión más reciente, haga clic en **Actualizar lista**.
   - Para restablecer la lista de tipos de equipo, haga clic en **Restablecer lista**.
7. En la ventana Sistemas operativos, seleccione los sistemas operativos de destino y haga clic en **Siguiente**.
8. En la ventana Directorio de destino, especifique la ubicación para descargar las actualizaciones o acepte la ubicación predeterminada y haga clic en **Siguiente**.
9. (Opcional) Seleccione **Úitimas actualizaciones individuales disponibles**, aparecerá la ventana Selección de actualizaciones. Seleccione las actualizaciones de destino y haga clic en **Siguiente**.
10. En la ventana Adquirir actualizaciones, la tabla de adquisición muestra el avance de adquisición de paquetes. Al finalizar el progreso, haga clic en **Siguiente**.
11. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Configuración de la matriz RAID para un servidor remoto

La aplicación UpdateXpress puede llevar a cabo cierta configuración RAID para un servidor remoto, como recopilar información de RAID, crear la matriz RAID, configurar el estado del disco y borrar la configuración de un controlador.

Requisito previo:

La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.

Para configurar la matriz RAID, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**. Cuando aparece una ventana que muestra la información relacionada, haga clic en **Aceptar**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no tienen intención de comprobar el certificado BMC del servidor y la huella digital de clave del servidor SFTP/HTTPS, seleccione **Aceptar certificado de servidor BMC y huella digital del servidor SFTP/HTTPS de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Configuración remota de RAID** o **Realizar actualización en el servidor de destino**, o ambos elementos, y haga clic en **Siguiente**.
5. En la ventana Configuración RAID, UpdateXpress primero recopilará la información de RAID del servidor remoto. Una vez que termine la recopilación, la información de RAID se mostrará en la ventana.
   - Para borrar la configuración de un controlador, haga clic en **Borrar controlador**.
   - Para cambiar el estado de la unidad a JBOD, haga clic en **Hacer JBOD**.
   - Para cambiar el estado de la unidad a una unidad en buen estado sin configurar, haga clic en **Hacer bien**.
6. En la ventana Configuración RAID, para crear un controlador, haga clic en **Crear matriz**.
   a. En la ventana del asistente, seleccione el nivel de RAID, agregue intervalos, miembros y repuestos dinámicos, cree volúmenes y establezca parámetros de disco.
   b. Cuando se muestre la información de resumen, haga clic en **Crear** para comenzar a crear la matriz de almacenamiento.
   c. Una vez completado el proceso, haga clic en **Recopilar** o **Actualizar** para volver a recopilar información de RAID.
   d. Haga clic en **Siguiente** si no se necesita ninguna otra acción.
7. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Realización de actualizaciones preconfiguradas para servidores remotos

La aplicación UpdateXpress admite la realización de actualizaciones preconfiguradas para servidores remotos.

El siguientes requisito previo es necesario para completar esta tarea:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte "Sistemas operativos compatibles" en la página 6.

Para realizar actualizaciones preconfiguradas para servidores remotos, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte "Inicio de la aplicación UpdateXpress" en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.

- (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Realizar actualización en el servidor de destino** y haga clic en **Siguiente**.
5. En la ventana Configuración de actualización, seleccione una o más de las opciones y, a continuación, haga clic en **Siguiente**.

   Notas:
   - Si se selecciona **Usar un servidor remoto en lugar del correspondiente al BMC**, introduzca la siguiente información:
     - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
     - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
     - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
     - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.
     - (Configuración) **Directorio**: la ruta completa en el servidor SFTP. El archivo de actualizaciones se debe cargar en ese directorio. Asegúrese de que se pueda acceder al directorio. Por ejemplo: /payload
   - Para no comprobar la huella dactilar de la clave del servidor SFTP/HTTPS, seleccione **Omitir la comprobación de la huella dactilar de la clave del servidor SFTP**.
6. En la ventana Ubicación de actualizaciones, seleccione **Visitar el sitio web de soporte de Lenovo** y haga clic en **Siguiente**.
7. En la ventana Directorio de destino, especifique la ubicación para descargar las actualizaciones o acepte la ubicación predeterminada y haga clic en **Siguiente**.
8. En la página Acceso a Internet, si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
   Si los usuarios tienen más consideraciones de seguridad, antes de hacer clic en **Probar conexión**, configure el **Servidor proxy** o los valores de **Configuración de seguridad de URL personalizada** en función de los requisitos de seguridad, como se indica a continuación:
   - **Servidor proxy**
     a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

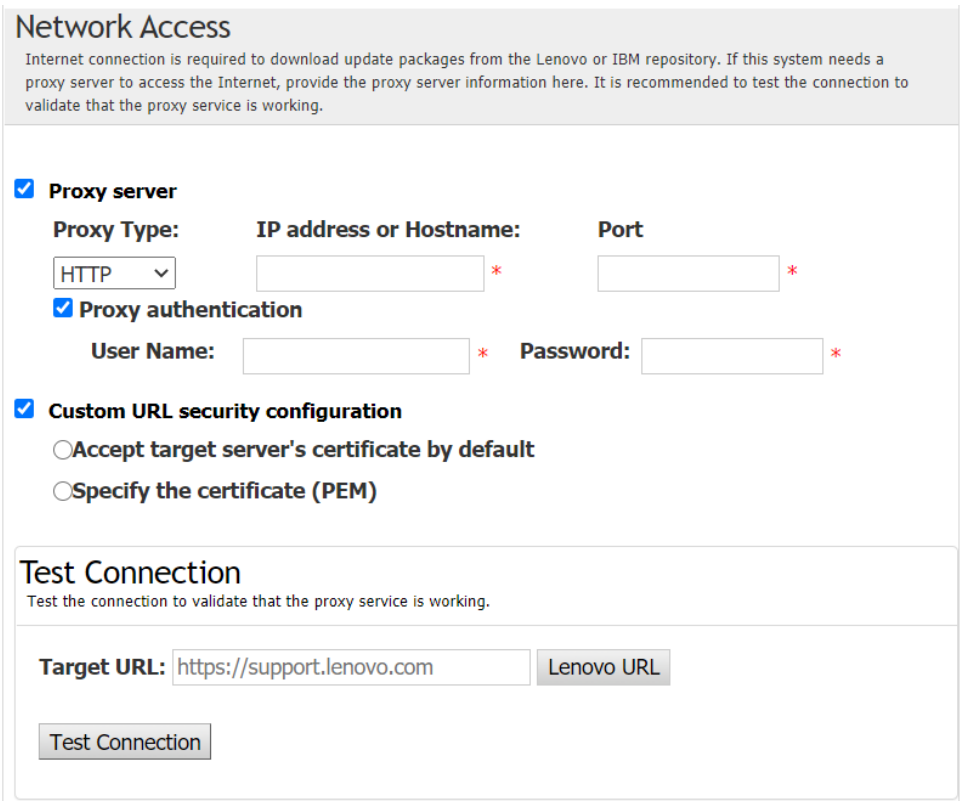
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

     b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

   - **Configuración de seguridad de URL personalizada**

     Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
     - **Aceptar el certificado del servidor de destino de manera predeterminada**
     - **Especificar el certificado (PEM)**



9. En la ventana Tipo de actualización, seleccione el tipo de actualización de destino y haga clic en **Siguiente**.
10. En la ventana Actualizar recomendación, lleve a cabo una o más de las siguientes acciones:
    - Para mostrar todos los paquetes de actualización, seleccione **Mostrar actualizaciones de dispositivos no detectados**.
    - Para actualizar el componente, seleccione el componente de destino y haga clic en **Siguiente**.
11. En la ventana Adquirir actualizaciones, la tabla de adquisición muestra el avance de adquisición de paquetes. Al finalizar el progreso, haga clic en **Siguiente**.
12. En la ventana Ejecución de actualizaciones, haga clic en **Iniciar actualización → Sí → Siguiente**.

    Notas: Para actualizar el firmware con paquetes agrupados, seleccione **Actualizar firmware con paquetes agrupados. Esta casilla de verificación y sus opciones secundarias solo admiten XCC2.** y especifique la hora de aplicación.
    - **OnReset**: los paquetes se actualizan la próxima vez que se reinicie el sistema.
    - **Immediate**: se actualizan los paquetes de inmediato. Es posible que el sistema se reinicie de inmediato.
    - **OnStartUpdateRquest**: los paquetes se actualizan gestionando la actualización preconfigurada o con la ejecución de comandos OneCLI.
13. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Administración de actualizaciones preconfiguradas para servidores remotos

La aplicación UpdateXpress admite el inicio, la cancelación y la visualización de todas las actualizaciones preconfiguradas de servidores remotos.

El siguientes requisito previo es necesario para completar esta tarea:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.

Para administrar actualizaciones preconfiguradas para servidores remotos, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Administrar actualización preconfigurada** y, a continuación, haga clic en **Siguiente**.
5. En la ventana Administración de tareas, realice uno o varios de los procedimientos siguientes y, a continuación, haga clic en **Siguiente**.
   - Para obtener la información de la tarea, introduzca el identificador de la tarea y, a continuación, haga clic en  . El identificador de tarea se completará automáticamente con la tarea pendiente.
   - Para comenzar la actualización, haga clic en **Iniciar** en la tarea deseada.
   - Para cancelar la actualización, haga clic en **Cancelar** en la tarea deseada.
6. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Administración de la clave de autenticación de SED

Los servidores ThinkEdge proporcionan acceso a la unidad de autocifrado (SED) utilizando la clave de autenticación. La aplicación UpdateXpress admite la gestión de la clave de autenticación de SED (AK), lo que incluye la generación, la copia de seguridad y la recuperación.

Requisito previo:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- Esta función solo es compatible cuando el servidor ThinkEdge está desbloqueado. Para obtener más detalles acerca de servidores compatibles, consulte la serie ThinkEdge en “Modelos de servidor admitidos” en la página 5.

Para gestionar la clave de autenticación SED, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Configurar funciones de seguridad de servidor ThinkEdge** y haga clic en **Siguiente**.
5. En la ventana Características de seguridad del servidor ThinkEdge, seleccione **Administrar la clave de autenticación SED** y, a continuación, haga clic en **Siguiente**.
6. En la ventana Administración de clave de autenticación (AK) de SED, realice uno o varios de los procedimientos siguientes:
   - Para generar SED AK, seleccione **Habilitar el cifrado SED** con SED AK deshabilitado o seleccione **Cambiar SED AK** con SED AK habilitado. Seleccione el método de destino en la lista desplegable **Método** y, a continuación, haga clic en **Regenerar**.

     Nota: Se recomienda crear una copia de seguridad de AK como prevención en caso de pérdida de datos. Los usuarios pueden seleccionar otras opciones solo después de realizar una copia de seguridad de AK.
   - Para hacer una copia de seguridad de la SED AK, seleccione **Crear copia de seguridad de SED AK**, especifique la ubicación y contraseña del archivo de copia de seguridad y haga clic en **Iniciar**. UpdateXpress guardará el archivo de copia de seguridad que contiene la información de la SED AK.
   - Para recuperar SED AK, seleccione **Recuperar la SED AK**, a continuación, realice uno de los procedimientos siguientes:
     – Para realizar una recuperación utilizando el archivo de copia de seguridad, seleccione **Recuperar SED AK desde el archivo de copia de seguridad** en la lista desplegable **Método**, haga clic en **Examinar** para seleccionar el archivo de copia de seguridad, introduzca la contraseña y haga clic en **Iniciar restauración**.
     – Para realizar la recuperación mediante una frase de paso, seleccione **Recuperar SED AK con frase de paso** en la lista desplegable **Método**, introduzca la frase de paso y, a continuación, haga clic en **Iniciar restauración**.
7. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Solicitar un servidor en ThinkShield Portal

La propiedad del servidor ThinkEdge puede realizarse en Lenovo ThinkShield Key Vault Portal y, a continuación, UpdateXpress puede activar el servidor bloqueado a través del Portal.

Requisito previo:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- Esta función solo es compatible con servidores ThinkEdge. Para obtener más detalles acerca de servidores compatibles, consulte la serie ThinkEdge en “Modelos de servidor admitidos” en la página 5.

Para solicitar el servidor en ThinkShield Portal, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Configurar funciones de seguridad de servidor ThinkEdge** y haga clic en **Siguiente**.
5. En la ventana Características de seguridad del servidor ThinkEdge, seleccione **Solicitar servidor en ThinkShield Portal** y haga clic en **Siguiente**.
6. En la ventana Acceso a Internet, lleve a cabo una de las siguientes acciones:
   - Si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
   - Si los usuarios tienen más inquietudes de seguridad, configure una o más de las siguientes acciones y haga clic en **Probar conexión**:
     – **Servidor proxy**: Acceso a la red mediante un proxy HTTP/HTTPS.
       a. Seleccione **Servidor proxy** y complete los campos siguientes:

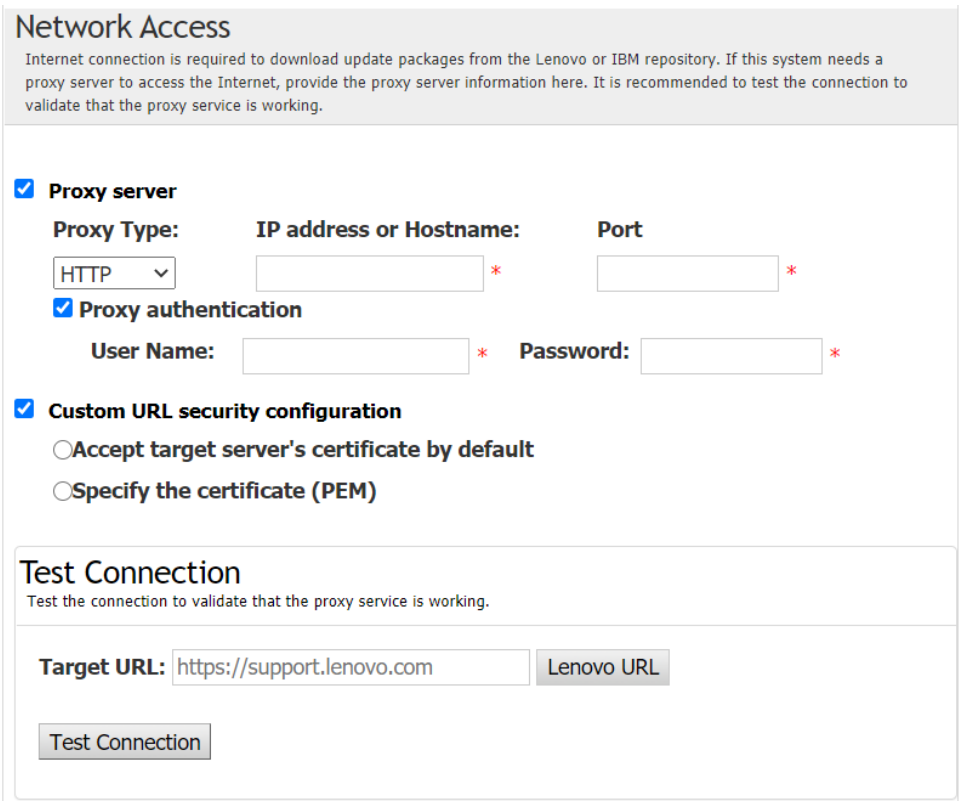
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

       b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

     – **Configuración de seguridad de URL personalizada**: Acceso a la red mediante un proxy inverso.

       Seleccione una de las siguientes opciones:
       – Aceptar el certificado del servidor de destino de manera predeterminada
       – Especificar el certificado (PEM)



7. En la ventana Solicitar servidor, especifique el Id. de organización, el nombre de usuario y la contraseña de ThinkShield Key Vault Portal y, a continuación, haga clic en **Reclamación**.
8. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Actualización del modo de control de bloqueo

El servidor ThinkEdge está equipado con sensores de seguridad para detectar sucesos de alteración, lo que también bloqueará al servidor durante la detección de alteraciones. UpdateXpress admite actualizar el modo de control de bloqueo del servidor al activar el servidor mediante XClarity Controller y gestionar el servidor mediante ThinkShield Portal.

Requisito previo:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- Esta función solo es compatible con servidores ThinkEdge. Para obtener más detalles acerca de servidores compatibles, consulte la serie ThinkEdge en “Modelos de servidor admitidos” en la página 5.

Para actualizar el modo de control de bloqueo, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Configurar funciones de seguridad de servidor ThinkEdge** y haga clic en **Siguiente**.
5. En la ventana Características de seguridad de servidor ThinkEdge, seleccione **Control de bloqueo del sistema**, haga clic en **Siguiente**, seleccione una de las opciones siguientes para reclamar o no la propiedad del servidor a ThinkShield Key Vault Portal y, a continuación, vuelva a hacer clic en **Siguiente**.
   - Seleccione **Sí, quiero reclamar el servidor ahora**, vaya al paso 6.
   - Seleccione **No, quiero continuar sin reclamar el servidor en ThinkShield Key Portal**, vaya al paso 8.
6. En la ventana Acceso a Internet, lleve a cabo una de las siguientes acciones:
   - Si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
   - Si los usuarios tienen más inquietudes de seguridad, configure una o más de las siguientes acciones y haga clic en **Probar conexión**:
     - **Servidor proxy**: Acceso a la red mediante un proxy HTTP/HTTPS.
       a. Seleccione **Servidor proxy** y complete los campos siguientes:

Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

       b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

     - **Configuración de seguridad de URL personalizada**: Acceso a la red mediante un proxy inverso.

       Seleccione una de las siguientes opciones:
       - Aceptar el certificado del servidor de destino de manera predeterminada
       - Especificar el certificado (PEM)
7. En la ventana Validar la cuenta del portal de ThinkShield, especifique el Id. de organización, el nombre de usuario y la contraseña de ThinkShield Key Vault Portal y, a continuación, haga clic en **Validar**. Una vez completada la verificación, haga clic en **Siguiente**.

   Nota: Se debe validar la entrada de información debe ser válida; de lo contrario, el botón **Siguiente** *no* se habilitará.
8. En la ventana Control de bloqueo del sistema, introduzca manualmente **SÍ** y, a continuación, haga clic en **Aceptar**. Una vez completado el proceso de actualización, haga clic en **Siguiente**.
9. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Activación del servidor en modo de bloqueo

El servidor ThinkEdge está equipado con sensores de seguridad para detectar sucesos de alteración, lo que también bloqueará al servidor durante la detección de alteraciones. UpdateXpress admite la activación del servidor bloqueado mediante ThinkShield Key Vault Portal o XClarity Controller.

Requisito previo:

- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- Esta función solo es compatible con servidores ThinkEdge. Para obtener más detalles acerca de servidores compatibles, consulte la serie ThinkEdge en “Modelos de servidor admitidos” en la página 5.

Para activar el servidor en el modo de bloqueo, realice los siguientes pasos:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.
   - (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
   - (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

   Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.
4. En la ventana Tarea, seleccione **Configurar funciones de seguridad de servidor ThinkEdge** y haga clic en **Siguiente**.
5. En la ventana Características de seguridad del servidor ThinkEdge, seleccione **Activar servidor con ThinkShield Portal** y haga clic en **Siguiente**.

   Nota: El control de bloqueo predeterminado del sistema se gestiona con XClarity Controller. Cuando el control de bloqueo se gestiona en el portal ThinkShield, los usuarios solo pueden activar el servidor en modo de bloqueo después de ser autenticados en ThinkShield Key Vault Portal.
6. En la ventana Acceso a Internet, si los usuarios no tienen ningún requisito especial con respecto al acceso de seguridad, haga clic en **Probar conexión** para revisar la conexión de red de la URL de destino y haga clic en **Siguiente**.
   Si los usuarios tienen más consideraciones de seguridad, antes de hacer clic en **Probar conexión**, configure el **Servidor proxy** o los valores de **Configuración de seguridad de URL personalizada** en función de los requisitos de seguridad, como se indica a continuación:
   - **Servidor proxy**
     a. Seleccione **Servidor proxy** si los usuarios requieren un proxy HTTP/HTTPS para conectarse a la Web y complete los siguientes campos:

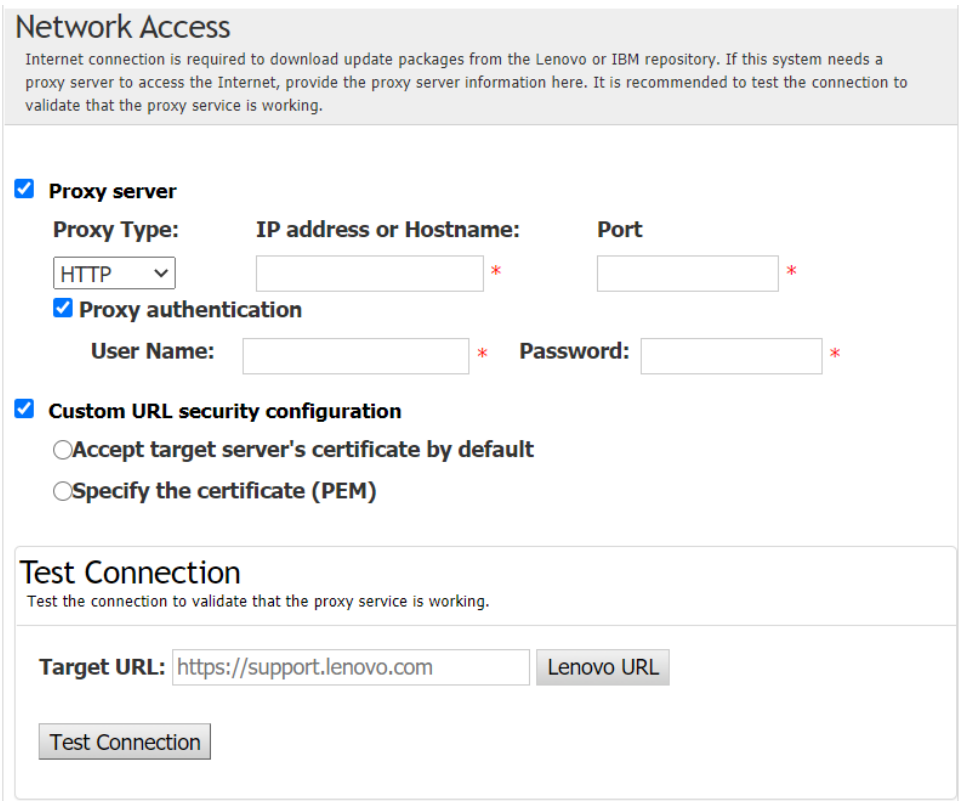
Tipo de proxy	El tipo de proxy del servidor proxy.
Dirección IP o nombre de host	El nombre de host, la dirección IP o el nombre de dominio del servidor proxy.
Puerto	El número de puerto del servidor proxy.

     b. Seleccione **Autenticación de proxy** si es necesario especificar credenciales para autenticarse en el servidor proxy y complete los siguientes campos:

Nombre de usuario	El nombre del usuario para su autenticación en el servidor proxy.
Contraseña	La contraseña para el nombre de usuario especificado.

   - **Configuración de seguridad de URL personalizada**

     Seleccione **Configuración de seguridad de URL personalizada** si los usuarios requieren un proxy inverso y seleccione una de las siguientes opciones:
     – **Aceptar el certificado del servidor de destino de manera predeterminada**
     – **Especificar el certificado (PEM)**



7. En la ventana Activar servidor, especifique el Id. de organización, el nombre de usuario y la contraseña de ThinkShield Key Vault Portal y, a continuación, haga clic en **Activar**. Una vez completado el proceso de activación, haga clic en **Siguiente**.

   Nota: Si XClarity Controller gestiona el servidor, los usuarios *no* necesitan introducir la información de ThinkShield Key Vault Portal.
8. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Configuración de los sensores de seguridad

Los servidores ThinkEdge están equipados con los sensores de seguridad para detectar sucesos de alteración. UpdateXpress admite habilitar, deshabilitar y modificar el umbral del sensor de detección de movimiento y el sensor de intrusión del chasis.

Requisito previo:
- La aplicación UpdateXpress está en ejecución en un servidor con un sistema operativo compatible. Para obtener detalles de los sistemas operativos compatibles, consulte “Sistemas operativos compatibles” en la página 6.
- Esta función solo es compatible con servidores ThinkEdge. Para obtener más detalles acerca de servidores compatibles, consulte la serie ThinkEdge en “Modelos de servidor admitidos” en la página 5.

Para configurar los sensores de seguridad, lleve a cabo los pasos siguientes:
1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Gestionar el servidor remoto**, introduzca la siguiente información y haga clic en **Siguiente**.
   - (Configuración) **Dirección IP o nombre de host**: dirección IP o nombre de host de BMC del sistema de destino.
   - (Configuración) **Nombre de usuario**: el nombre de usuario de BMC del sistema de destino.

- (Configuración) **Contraseña**: la contraseña de BMC del sistema de destino.
- (Configuración) **Puerto**: número del puerto del CIM de BMC o de RSET. Si los usuarios no escriben esta información, se utilizará el puerto predeterminado.

Nota: Si los usuarios no contarán con las facultades para comprobar el certificado BMC del servidor, seleccione **Aceptar certificado de servidor BMC de forma predeterminada** y haga clic en **Siguiente**.

4. En la ventana Tarea, seleccione **Configurar funciones de seguridad de servidor ThinkEdge** y haga clic en **Siguiente**.
5. En la ventana Características de seguridad del servidor ThinkEdge, seleccione **Configurar sensores de seguridad** y haga clic en **Siguiente**.
6. En la ventana Configurar sensores de seguridad, realice uno o varios de los procedimientos siguientes y, a continuación, haga clic en **Siguiente**.
   - Para habilitar o deshabilitar la **Detección de movimiento** o la **Detección de intrusión del chasis**, seleccione las opciones de la lista desplegable o haga clic en el botón del conmutador para alternar el estado.

     Nota: En caso de pérdida de datos, se recomienda hacer una copia de seguridad de AK antes de seleccionar cualquier elemento.
   - Para restablecer el recuento de pasos para la detección de movimiento, haga clic en **Restablecer contador de pasos**. UpdateXpress restablecerá el recuento de pasos a 0.
   - Para cambiar los pasos del umbral para bloquear la detección de movimiento, seleccione el nivel de paso de destino en **Umbral de bloqueo**.

     Nota: El servidor ThinkEdge será bloqueado una vez que el sensor de seguridad detecte el suceso de alteración.
7. En la ventana Finalizar, haga clic en **Ver registro** para revisar el registro de actualización; copie y guarde los comandos generados y haga clic en **Cerrar** para salir.

Gestión del servidor bajo conexión Ethernet directa

La aplicación UpdateXpress admite la gestión de servidores bajo conexión Ethernet directa. Cuando el cable de red esté conectado, UpdateXpress intentará acceder al BMC del servidor mediante la IP y la credencial predeterminadas del BMC.

Para gestionar un servidor bajo la conexión Ethernet directa, haga lo siguiente:

1. Inicie la aplicación UpdateXpress. Consulte “Inicio de la aplicación UpdateXpress” en la página 9.
2. En la ventana Bienvenida, haga clic en **Siguiente**.
3. En la ventana Servidor de destino, seleccione **Conexión Ethernet directa**, introduzca la siguiente información y haga clic en **Siguiente**.
4. En la ventana Configuración de conexión Ethernet directa, haga lo siguiente:
   a. Seleccione el adaptador de destino en la tabla de “Adaptador de red disponible”.
   b. Asegúrese de que la dirección IP es **192.168.70.125**.
   c. Introduzca el nombre de usuario y la contraseña.
   d. Haga clic en **Probar conexión → Siguiente** o **Siguiente**.
5. En la ventana Tarea, seleccione una de las opciones siguientes:
   - **Realizar actualización en el servidor de destino**. Para obtener más detalles, consulte el paso 4 y los pasos posteriores en “Actualización de un servidor remoto desde un directorio local” en la página 14.
   - **Administrar actualización preconfigurada**. Para obtener más detalles, consulte el paso 4 y los pasos posteriores en “Administración de actualizaciones preconfiguradas para servidores remotos” en la página 27.
   - **Configuración remota de RAID**. Para obtener más detalles, consulte el paso 4 y los pasos posteriores en “Configuración de la matriz RAID para un servidor remoto” en la página 24.
   - **Configurar funciones de seguridad de servidor ThinkEdge**. Para obtener más detalles, consulte el paso 4 y los pasos posteriores en las secciones siguientes:

– “Administración de la clave de autenticación de SED” en la página 28
– “Solicitar un servidor en ThinkShield Portal” en la página 29
– “Actualización del modo de control de bloqueo” en la página 31
– “Activación del servidor en modo de bloqueo” en la página 32
– “Configuración de los sensores de seguridad” en la página 34

Visualización de comandos OneCLI en la ventana finalizar

UpdateXpress realiza actualizaciones invocando comandos OneCLI en el asistente de GUI. UpdateXpress 2.7.0 y versiones posteriores muestran estos comandos en el cuadro de mensaje nuevo en la ventana de Finalización. Los usuarios pueden guardar y utilizar los comandos para invocar la misma función en el modo de CLI.

Ejemplo de comandos OneCLI:

```
<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
```

Capítulo 4. Resolución de problemas

Este capítulo proporciona información acerca de qué hacer si los usuarios experimentan un problema con la aplicación UpdateXpress.

Limitaciones y problemas

- **Al especificar el certificado de configuración de seguridad de proxy/URL personalizada en el proceso de ejecución de UpdateXpress en Linux, si los usuarios hacen clic en Examinar por segunda vez, es posible que la ventana de exploración no se muestre en la interfaz de UpdateXpress.**

  En la página Acceso a Internet, seleccione **HTTPS** en la lista desplegable **Tipo de proxy**, seleccione **Configuración de seguridad de proxy personalizada** y **Configuración de seguridad de URL personalizada**, y haga clic en **Examinar…** para especificar el certificado para ambas selecciones. Si los usuarios hacen clic en Examinar por segunda vez, es posible que la ventana de exploración no se muestre.

  Solución: lleve a cabo una o más de las siguientes acciones:
  - Cambie manualmente a la ventana de exploración en segundo plano.
  - Ajuste el tamaño de la ventana para ver la ventana de exploración en segundo plano.
  - Use UpdateXpress en Windows en su lugar.
- **UpdateXpress no puede configurar el controlador de uso inmediato como predeterminado en algunos dispositivos al actualizar de controlador incorporado a controlador de uso inmediato.**

  UpdateXpress llama a OneCLI para realizar la tarea de actualización. OneCLI no pudo comparar las versiones incoherentes de controlador incorporado y controlador de uso inmediato y seleccionar la versión correcta para la actualización. En este caso, UpdateXpress no podía seleccionar el controlador de uso inmediato para actualización, y los usuarios deben seleccionar manualmente el controlador de uso inmediato para reemplazar al controlador incorporado.
- **Todas las rutas de UpdateXpress deben usar caracteres alfanuméricos estándar del inglés.**

  Todas las rutas de UpdateXpress deben usar caracteres alfanuméricos estándar del inglés y no pueden incluir espacios, caracteres especiales ni caracteres de idiomas distintos del inglés.

Soluciones alternativas

Actualmente, no hay problemas conocidos ni soluciones alternativas para la aplicación UpdateXpress.

Coexistencia y compatibilidad

La aplicación UpdateXpress se basa en OneCLI, pero no tiene interacciones con otros programas en el sistema. No ejecute la aplicación UpdateXpress y OneCLI al mismo tiempo.

Apéndice A. Características de accesibilidad de UpdateXpress

Las características de accesibilidad ayudan a los usuarios que tienen discapacidades, tales como movilidad restringida o visión limitada, a usar los productos de tecnología de la información correctamente.

La siguiente lista incluye las funciones de accesibilidad principales de la aplicación UpdateXpress:
- Operación solo con teclado
- Interfaces que usan generalmente los lectores de pantalla

Desplazamiento con el teclado

Los usuarios pueden utilizar el teclado para desplazarse a través de la interfaz gráfica de usuario (GUI).

Los siguientes métodos abreviados de teclado aplican tanto a sistemas operativos Windows como Linux.

Acceso directo	Función
Tab	Ir al siguiente control.
Mayús+Tab	Moverse al control anterior.
Flecha izquierda	Volver atrás un caracter.
Flecha derecha	Mover adelante un caracter.
Retroceso	Eliminar el caracter a la izquierda del cursor.
Suprimir	Eliminar el carácter bajo el cursor.
Flecha arriba	Mover el enfoque y la selección hacia arriba, a través del botón de selección.
Flecha abajo	Mover el enfoque y la selección hacia abajo, a través del botón de selección.
Espacio	Seleccionar o eliminar una opción.

Tecnología de lectura de pantalla

Las tecnologías de lectura de pantalla se concentran principalmente en las interfaces de programas, sistemas de información de ayuda y diversos documentos en línea. Para obtener información adicional acerca de los lectores de pantalla, consulte lo siguiente:
- Utilización del lector de pantalla JAWS:

  http://www.freedomscientific.com/Products/Blindness/JAWS
- Utilización del lector de pantalla NVDA:

  http://www.nvaccess.org/

Lenovo y accesibilidad

Para obtener más información acerca del compromiso de Lenovo con la accesibilidad, visite http://www.lenovo.com/lenovo/us/en/accessibility.html.

Apéndice B. Avisos

Puede que Lenovo no comercialice en todos los países los productos, servicios o características a los que se hace referencia en este documento. Póngase en contacto con su representante local de Lenovo para obtener información acerca de los productos y servicios disponibles actualmente en su zona.

Las referencias a productos, programas o servicios de Lenovo no pretenden afirmar ni implicar que solo puedan utilizarse esos productos, programas o servicios de Lenovo. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de Lenovo. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier otro producto, programa o servicio.

Lenovo puede tener patentes o solicitudes de patentes pendientes que aborden temas descritos en este documento. No obstante, la posesión de este no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

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

LENOVO PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, por lo que puede haber usuarios a los que no afecte dicha norma.

Esta información podría incluir inexactitudes técnicas o errores tipográficos. La información aquí contenida está sometida a modificaciones periódicas, las cuales se incorporarán en nuevas ediciones de la publicación. Lenovo se reserva el derecho a realizar, si lo considera oportuno, cualquier modificación o mejora en los productos o programas que se describen en esta publicación.

Los productos descritos en este documento no están previstos para su utilización en implantes ni otras aplicaciones de reanimación en las que el funcionamiento incorrecto podría provocar lesiones o la muerte a personas. La información contenida en este documento no cambia ni afecta a las especificaciones o garantías del producto de Lenovo. Ninguna parte de este documento deberá regir como licencia explícita o implícita o indemnización bajo los derechos de propiedad intelectual de Lenovo o de terceros. Toda la información contenida en este documento se ha obtenido en entornos específicos y se presenta a título ilustrativo. Los resultados obtenidos en otros entornos operativos pueden variar.

Lenovo puede utilizar o distribuir la información que le suministre el cliente de la forma que crea oportuna, sin incurrir con ello en ninguna obligación con el cliente.

Las referencias realizadas en esta publicación a sitios web que no son de Lenovo se proporcionan únicamente en aras de la comodidad del usuario y de ningún modo pretenden constituir un respaldo de los mismos. La información de esos sitios web no forma parte de la información para este producto de Lenovo, por lo que la utilización de dichos sitios web es responsabilidad del usuario.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Así pues, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Es posible que algunas mediciones se hayan realizado en sistemas en desarrollo, por lo que no existen garantías de que estas sean las mismas en los sistemas de disponibilidad general. Además, es posible que la estimación de

algunas mediciones se haya realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de la presente publicación deben verificar los datos pertinentes en su entorno de trabajo específico.

Marcas registradas

LENOVO, FLEX SYSTEM, SYSTEM X y NEXTSCALE SYSTEM son marcas registradas de Lenovo. Intel e Intel Xeon son marcas registradas de Intel Corporation en Estados Unidos y/o en otros países. Internet Explorer, Microsoft y Windows son marcas registradas del grupo de empresas Microsoft. Linux es una marca registrada de Linus Torvalds. El resto de las marcas registradas son propiedad de sus propietarios respectivos.

Notas importantes

La velocidad del procesador indica la velocidad del reloj interno del microprocesador; también hay otros factores que afectan al rendimiento de la aplicación.

Cuando se hace referencia al almacenamiento del procesador, al almacenamiento real y virtual, o al volumen del canal, KB representa 1024 bytes, MB representa 1.048.576 bytes y GB representa 1.073.741.824 bytes.

Cuando se hace referencia a la capacidad de la unidad de disco duro o al volumen de comunicaciones, MB representa 1 000 000 bytes y GB representa 1 000 000 000 bytes. La capacidad total a la que puede acceder el usuario puede variar en función de los entornos operativos.

Lenovo no ofrece declaraciones ni garantía de ningún tipo respecto a productos que no sean de Lenovo. El soporte (si existe) para productos que no sean de Lenovo lo proporcionan terceros y no Lenovo.

Es posible que parte del software difiera de su versión minorista (si está disponible) y que no incluya manuales de usuario o todas las funciones del programa.

Índice

A

Aplicación UpdateXpress 1
avisos 41

C

características de accesibilidad 39
coexistencia 37
compatibilidad 37
componentes de hardware admitidos 5
controlador de dispositivo 1
Controlador de gestión de placa base 1
Controladores de dispositivos de Linux 5
controladores de dispositivos de Linux admitidos 5
Controladores de dispositivos de Windows 5
controladores de dispositivos de Windows admitidos 5

D

datos de inventario 4
datos de inventario incompletos 4
datos de inventario perdidos 4

E

ejecutar UpdateXpress 9
Equipos AMD 6
equipos x86 6
escenarios 9
Escenarios de UpdateXpress 9

F

firmware 5
firmware admitido 5
fuera de banda 1

I

iniciar UpdateXpress 9
instalación de controladores de dispositivo requeridos 4
instalar controladores de dispositivo requeridos 4
Intelligent Peripheral Management Interface 4
interfaz gráfica de usuario 39
inventario 2

L

limitaciones 37

M

marcas registradas 42

O

OneCLI 37

P

privilegios de sistema operativo 7

R

recursos Web v
requisitos 5
requisitos previos 2
resolución de problemas 37

S

servidores admitidos 5
sistemas operativos admitidos 6
sistemas operativos compatibles 6
  Linux 6
  Windows 6
sistemas operativos Linux admitidos 6
sistemas operativos Windows admitidos 6

U

UpdateXpress System Pack 1
usar UpdateXpress 9
usuarios permisibles de UpdateXpress System Pack 7