Lenovo

Guide d'utilisation
Lenovo XClarity Essentials UpdateXpress

Version 4.4.0

Remarque

Avant d'utiliser cette documentation et les produits associés, prenez connaissance des informations figurant à la section Annexe B « Consignes » à la page 41.

La présente édition s'applique à la version de Lenovo XClarity® Essentials UpdateXpress et à toutes les éditions et modifications ultérieures sauf mention contraire dans les nouvelles éditions.

Vingt-quatrième édition (Février 2024)

Table des matières

Tableaux

À propos de ce guide

Lenovo XClarity Essentials UpdateXpress (ci-après appelé application UpdateXpress) est une application qui applique des modules UpdateXpress System Packs (UXSPs) et des mises à jour individuelles au serveur. Ce guide fournit des informations sur le téléchargement et l'utilisation de l'application UpdateXpress.

À qui s'adresse ce guide

Cette documentation est destinée aux administrateurs système et autres personnes chargées de l'administration du système qui ont une bonne connaissance de la maintenance du microprogramme et des pilotes de périphérique.

Conventions et terminologies

Les paragraphes commençant par les mentions en gras Remarque, Important ou Attention représentent des remarques d'une importance particulière, qui contiennent des informations à prendre en considération :

Remarque : Ces consignes contiennent des instructions et des conseils importants.

Important : Ces remarques contiennent des informations ou des conseils qui peuvent aider les utilisateurs à éviter les situations délicates ou difficiles.

Attention : Ces consignes de sécurité indiquent la présence d'un risque pouvant occasionner des dommages aux programmes, aux appareils ou aux données. Une consigne de type Avertissement apparaît avant l'instruction ou la situation pouvant entraîner un dommage.

Dans cette documentation, lorsque les utilisateurs sont invités à entrer une commande, tapez la commande et appuyez sur Entrée.

Sites Web pris en charge

Cette section fournit des ressources Web de support.

- Site Web Lenovo XClarity Essentials

  Ce site Web permet de télécharger plusieurs outils de gestion de système pour les serveurs ThinkSystem et System x.
- Lenovo XClarity Essentials UpdateXpress

  Ce site Web permet de télécharger l'application UpdateXpress.

Les sites Web suivants fournissent des informations sur la compatibilité et la prise en charge de produits, les garanties et licences, et d'autres ressources techniques diverses.
- Produits et services de support Lenovo Flex System
- Site Web ServerProven
- Bibliothèque de ressources serveur, réseau et stockage Lenovo

Chapitre 1. Présentation technique

Lenovo XClarity Essentials UpdateXpress (ci-après appelé application UpdateXpress) est une application qui applique des modules UpdateXpress System Packs (UXSPs) et des mises à jour individuelles au système local ou distant. L'application UpdateXpress acquiert et déploie des modules de mise à jour UpdateXpress System Pack (UXSP) et des mises à jour individuelles. Les modules UXSP contiennent des mises à jour de microprogramme et de pilote de périphérique.

La section suivante décrit brièvement les quatre principales fonctions de l'application UpdateXpress. Pour plus d'informations, voir Chapitre 3 « Utilisation de l'application UpdateXpress » à la page 9.

Mise à jour du serveur local
Mettez à jour la machine locale qui exécute actuellement cette application UpdateXpress. Le type de la machine est détecté et les mises à sont acquises, puis automatiquement appliquées.

Mise à jour du serveur distant
Mettez à jour la machine distante à l'aide du BMC (Baseboard Management Controller) qui s'exécute sur la machine. Les utilisateurs ont besoin d'un serveur SFTP (Simple File Transfer Protocol) pour transférer les mises à jour sur la machine distante cible.

Création d'un référentiel de mises à jour
Choisissez un ou plusieurs types de machine pour lesquelles les mises à sont acquises à partir du site Web de support Lenovo. Les mises à jour sont téléchargées dans le dossier spécifié, mais aucune mise à jour n'est appliquée. Les utilisateurs peuvent ultérieurement utiliser l'application UpdateXpress pour appliquer ces mises à jour en indiquant que ces mises à jour doivent être obtenues à partir du dossier indiqué et non depuis le site Web de support de Lenovo.

Configuration RAID à distance
Configurez la grappe RAID à l'aide du service BMC.

UpdateXpress System Pack (UXSP)

UXSP est un ensemble, dont l'intégration est testée, de mises à jour de pilote de périphérique et de microprogramme en ligne pour les serveurs System x et ThinkSystem. Les UXSP sont édités tous les 6 mois pendant les trois premières années et tous les ans pendant les trois dernières années du support.

Les UXSP simplifient le processus de téléchargement et d'installation de l'ensemble des mises à jour de pilote et de microprogramme en ligne pour un système donné. Avec les UXSP, les utilisateurs sont assurés de toujours disposer d'un ensemble de mises à jour complet et récent qui a été testé et collecté par Lenovo.

Les UXSP sont créés pour une combinaison type de machine/système d'exploitation. Des UXSP distincts sont fournis pour les systèmes d'exploitation Windows® et pour chacune des distributions Linux. Par exemple, il peut y avoir plusieurs UXSP pour un type de machine particulier. Il peut aussi y avoir une mise à jour pour le système d'exploitation Windows et pour chaque distribution Linux.

Un type d'UXSP de plateforme peut aussi être utilisé pour mettre à jour un système de manière hors bande. L'UXSP de plateforme ne contient pas de système d'exploitation.

Format UXSP
Un UXSP est fourni dans un fichier XML. La convention de dénomination d'un UXSP utilise le format suivant :
lnvgy_utl_uxsp_*version_operatingsystem_arch*.xml
Exemple : `lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml`

Application des mises à jour UXSP avec l'application UpdateXpress

Les utilisateurs peuvent utiliser l'application UpdateXpress pour appliquer des mises à jour UXSP à leur machine. L'application UpdateXpress effectue l'inventaire de la machine sur laquelle va être appliquée la mise à jour, interroge demande l'emplacement spécifique d'une liste de modules de mise à jour applicables, compare l'inventaire à la liste de mise à jour disponible applicable, recommande un ensemble de mises à jour à appliquer, puis déploie ces mises à jour sur la machine.

Pour appliquer des UXSPs via l'application UpdateXpress, procédez comme suit :

1. Téléchargez l'application UpdateXpress à partir du site Web de support Lenovo.
2. Exécutez l'application UpdateXpress. Sélectionnez **Mettre à jour la machine locale** ou **Mettre à jour une machine distante**.
3. Sélectionnez **Consultation du site Web de support Lenovo**.
4. Sélectionnez **Application UpdateXpress System Packs (UXSPs)**.

Les utilisateurs peuvent aussi télécharger les mises à jour directement depuis le site Web de support Lenovo. Pensez à télécharger le contenu de mise à jour ainsi que le fichier XML. Pour plus de simplicité, choisissez le même dossier de destination pour chaque téléchargement UXSP. Les utilisateurs peuvent télécharger plusieurs System Packs pour différents types de machine dans le même dossier. Lorsque utilisateurs exécutent l'application UpdateXpress, celle-ci détecte le type de machine et utilise le contenu approprié pour ce type de machine. Dans certains cas, il peut y avoir des fichiers communs entre les System Packs. Les fichiers communs qui se trouvent déjà dans le dossier ne seront pas de nouveau téléchargés. Par conséquent, le temps de téléchargement total est réduit.

Traitement d'un module UXSP en tant que paquet

L'application UpdateXpress est conçue pour le téléchargement et l'application de modules UXSP. Le module UXSP est une collection de mises à jour individuelles, comme indiqué par le fichier XML UXSP.

Lors de l'exécution de l'application UpdateXpress, les utilisateurs peuvent choisir d'utiliser des modules UXSP ou des mises à jour individuelles. Dans la plupart des cas, il est recommandé d'utiliser des modules UXSP, mais la possibilité d'utiliser également des mises à jour individuelles offre davantage de flexibilité en terme de choix des mises à jour à utiliser.

Traitement des mises à jour requises

Cette rubrique explique comment les mises à jour requises sont acquises et appliquées.

Pour appliquer les mises à jour, tous les prérequis et corequis pour une mise à jour doivent toujours être acquis et appliqués. L'application UpdateXpress vérifie, acquiert et applique automatiquement les prérequis et corequis. Les mises à jour exigent souvent l'application préalable de fichiers de prérequis pour qu'ils puissent être appliqués ou l'inclusion de modules corequis pour une utilisation correcte de la mise à jour appliquée. Pour simplifier le processus de mise à jour, l'application UpdateXpress utilise les informations inclues dans le fichier de mise à jour pour identifier les modules requis pour les mises à jour spécifiques. L'application UpdateXpress applique ensuite ces modules requis.

Fichiers prérequis

Les modules de mise à jour fournis par Lenovo incluent des informations sur les fichiers prérequis qui doivent être appliqués pour que les utilisateurs puissent appliquer la mise à jour. Lorsque les utilisateurs indiquent une mise à jour, l'application UpdateXpress lit ces informations et localise les modules prérequis.

Par défaut, l'application UpdateXpress acquiert les modules de mises à jour et les évalue afin de déterminer si les conditions prérequises sont remplies, et si nécessaire, applique les fichiers de prérequis

automatiquement avant d'appliquer la mise à jour spécifiée. Les utilisateurs peuvent choisir de ne pas appliquer les fichiers prérequis. Toutefois, il est possible dans ce cas que la mise à jour ne soit pas correctement appliquée.

Si les modules prérequis ont des prérequis ou des corequis, ils sont acquis, évalués et appliqués de la même manière.

Fichiers corequis

Certaines mises à jour nécessitent des fichiers corequis, c'est-à-dire des modules supplémentaires qui doivent être appliqués pour que la mise à jour s'effectue correctement ; mais ces modules ne doivent pas être appliqués avant la mise à jour spécifiée.

Par défaut, l'application UpdateXpress identifie, acquiert, évalue et applique les modules corequis dans le cadre de la mise à jour.

Si les modules corequis ont des prérequis ou des corequis, ils sont acquis, évalués et appliqués de la même manière.

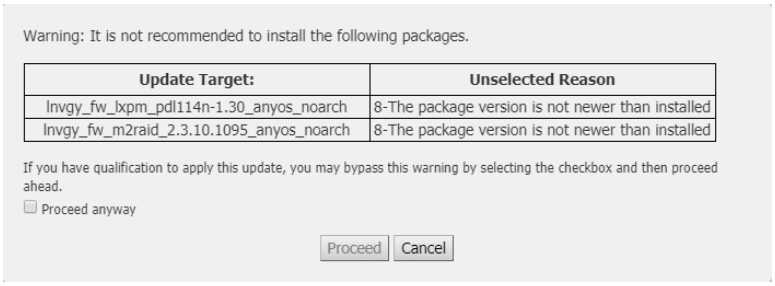
Exemple

Prenons, par exemple, une mise à jour qui comporte à la fois des prérequis et des corequis. Par défaut, l'application UpdateXpress procède aux étapes suivantes :

1. Pour garantir que la mise à jour peut être effectuée, l'application UpdateXpress télécharge d'abord la mise à jour.
2. Les fichiers prérequis sont téléchargés.
3. Les fichiers corequis sont téléchargés.
4. Les fichiers prérequis ou corequis sont évaluées selon l'état actuel du système. Si le système est déjà au niveau requis car les éléments requis ont déjà été appliqués, l'élément requis est ignoré.
5. Les fichiers prérequis nécessaires sont appliqués.
6. La mise à jour est appliquée.
7. Les fichiers corequis nécessaires sont appliqués.

Recommandation de la mise à jour

Par défaut, l'application UpdateXpress sélectionne les modules qui sont recommandés pour l'installation ou la mise à niveau du système. Les utilisateurs peuvent également sélectionner manuellement les modules à installer ou à mettre à niveau. Dans ce cas, ils reçoivent un message d'avertissement similaire à celui-ci :



Si ce message s'affiche, il est recommandé d'arrêter le processus de mise à jour.

Mises à jour indépendantes du système d'exploitation

Certaines mises à jour individuelles concernent un type de machine spécifique quel que soit le système d'exploitation utilisé. Ces mises à jour individuelles sont traitées comme des mises à jour indépendantes du système d'exploitation. Les utilisateurs peuvent sélectionner ces mises à jour indépendantes du système

d’exploitation, de la même façon qu’ils sélectionnent les mises à jour spécifiques à un système d’exploitation.

Remarque : Lorsque les utilisateurs sélectionnent les mises à jour spécifiques à un système d’exploitation, les mises à jour indépendantes du système d’exploitation sont incluses dans le module. Sélectionnez le mises à jour indépendantes du système d’exploitation uniquement si les utilisateurs ne sélectionnent aucune mise à jour de système d’exploitation pour un type de machine.

Données d'inventaire manquantes ou incomplètes

Parfois, un module de mise à jour s'applique à un composant pour lequel l'application UpdateXpress ne peut pas déterminer la version de microprogramme ou de pilote. Dans ce cas, l'application UpdateXpress affiche la version du module de mise à jour au lieu de la version de composant. Si aucune version de composant installé n'est détectée, la mise à jour n'est pas sélectionnée par défaut. Dans ce cas, sélectionnez le module manuellement en tant que mise à jour recommandée.

Installation des pilotes de périphérique nécessaires

L'application UpdateXpress installe les pilotes de périphériques nécessaires.

L'application UpdateXpress installe chaque pilote dans UXSP lorsque :
- Le pilote de périphérique actuel est antérieur au pilote de périphérique disponible dans le module UXSP.
- L'application UpdateXpress ne parvient pas à déterminer la version actuelle du pilote de périphérique, ce qui se produit généralement lorsque le pilote de périphérique n'est pas installé.

  Remarque : L'application UpdateXpress affiche `Non détecté` lorsque la version d'un pilote de périphérique installé n'est pas détectée.

Les utilisateurs peuvent tirer parti de ce comportement pour installer les pilotes de périphérique suivants, lesquels sont obligatoires pour les mises à jour de microprogramme :
- Intelligent Peripheral Management Interface (IPMI)
- IPMI Mapping Layer

Chapitre 2. Configurations matérielle et logicielle requises

Avant que les utilisateurs ne commencent à utiliser l'application UpdateXpress, passez en revue le matériel, le système d'exploitation et les privilèges de système d'exploitation locaux requis. Les systèmes exécutant l'application UpdateXpress nécessitent au moins 1 Go de mémoire RAM.

Modèles de serveur pris en charge

L'application UpdateXpress prend en charge les pilotes de périphérique Windows et Linux et le microprogramme qui est inclus dans les UXSP disponibles. Une liste des pilotes de périphérique de composants actuellement pris en charge est fournie dans le fichier readme de l'application UpdateXpress qui se trouve dans chaque System Pack.

Tableau 1. Systèmes Lenovo pris en charge

Série	Modèles de serveur	
ThinkEdge	• SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
ThinkSystem	• Passerelle DX1100U (7D49) • Performance/Capacité DX1100U (7D4A) • Stockage 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) • Dispositif WH5900 (7D5V)

Tableau 1. Systèmes Lenovo pris en charge (suite)

Série	Modèles de serveur	
WenTian	• WA5480 G3/WA5488 G3 (7DE7) • WR3220 G2/WR3228 G2 (7DEC)	• WR5220 G3/WR5228 G3 (7D8Y)
Solutions	• ThinkAgile série VX (7D28, 7D2Z, 7D43, 7DDK, 7Y12, 7Y13, 7Y14, 7Y92, 7Y93, 7Y94, 7Z12, 7Z13, 7Z62, 7Z63) • ThinkAgile série MX (7D19, 7D1B, 7D1H, 7D5R, 7D5S, 7D5T, 7D66, 7D67, 7D6B, 7DGG, 7Z20)	• ThinkAgile série 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	• Dispositif HX 3310 (8693) • Dispositif HX 5510/7510 (8695) • nx360 M5 (5465, 5467) • Nœud de traitement x240 (7162, 2588) • Nœud de traitement x240 M5 (2591, 9532) • Nœud de traitement x280 X6/x480 X6/ x880 X6 (4258, 7196)[2] • x440 (7167, 2590)	• x3250 M6 (3633, 3943) • x3500 M5 (5464) • x3550 M5 (5463, 8869) • x3650 M5 (5462, 8871) • x3750 M4 (8753) • x3850 X6/x3950 X6 (6241)[2]
Remarques : 1. Ce modèle de serveur est basé sur un processeur AMD à un socket. 2. Ce modèle de serveur prend en charge à la fois un nœud unique et plusieurs nœuds.		

Systèmes d'exploitation pris en charge

L'application UpdateXpress est prise en charge sur les systèmes d'exploitation Linux et Windows.

Windows

L'application UpdateXpress est prise en charge sur les systèmes d'exploitation 64 bits. Utilisez les informations du tableau suivant pour identifier les systèmes d'exploitation qui sont pris en charge par l'application UpdateXpress.

Tableau 2. Systèmes d'exploitation Windows pris en charge

Système d'exploitation	Mise à jour de la machine locale	Mise à jour de la machine distante	Référentiel local	Configuration RAID à distance
Microsoft Windows 10/11 Professionnel pour station de travail (21H2/22H2)	Oui[remarque]	Oui	Oui	Oui
Microsoft Windows Server 2016	Oui	Oui	Oui	Oui
Microsoft Windows Server 2019	Oui	Oui	Oui	Oui
Microsoft Windows Server 2022	Oui	Oui	Oui	Oui

Remarque : Les modèles de serveur prenant en charge Microsoft Windows 10/11 Pro pour stations de travail (21H2/22H2) peuvent également accéder à sa fonction de mise à jour locale.

Linux

L'application UpdateXpress version est prise en charge sur les versions de systèmes d'exploitation Linux suivantes.

Tableau 3. Systèmes d'exploitation Linux pris en charge

Système d'exploitation	Mise à jour de la machine locale	Mise à jour de la machine distante	Référentiel local	Configuration RAID à distance
Red Hat Enterprise Linux 7.X (7.6 et versions ultérieures)	Oui	Oui	Oui	Oui
Red Hat Enterprise Linux 8.X	Oui	Oui	Oui	Oui
Red Hat Enterprise Linux 9.X	Oui	Oui	Oui	Oui
SUSE Linux Enterprise Server 15.X	Oui	Oui	Oui	Oui

Remarques :
- Il est recommandé de disposer de 500 Mo d'espace disque lors de l'exécution de l'application UpdateXpress sur un système d'exploitation Linux.
- L'application UpdateXpress prend en charge la vérification partielle de système d'exploitation. Si le système d'exploitation en cours ne prend pas en charge les modules de microprogramme dans un UXSP, les modules de microprogramme peuvent aussi être répertoriés dans le résultat de comparaison de l'application UpdateXpress.
- Selon la commande `ifconfig` système d'exploitation Linux, UpdateXpress peut ne pas être installé sur RHEL 7.0 ou versions ultérieures. Pour mettre à jour le microprogramme vers RHEL 7.0 ou versions ultérieures, les utilisateurs doivent installer net-tools.
- Les mises à jour de pilote de périphérique Linux nécessitent des modules spécifiques. Les modules suivants doivent être installés :
  - Red Hat Enterprise Linux : rpm-build, perl et bash
  - SUSE Enterprise Linux : perl et bash
- Pour les systèmes d'exploitation suivants, les utilisateurs peuvent utiliser UpdateXpress 4.3.0 à la place :
  - SUSE 12.5
- Pour les systèmes d'exploitation suivants, les utilisateurs peuvent utiliser UpdateXpress 4.1.0 à la place :
  - RedHat 7.5
  - SUSE 12.4
- Pour les systèmes d'exploitation suivants, les utilisateurs peuvent utiliser UpdateXpress 3.4.0 à la place :
  - 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

Privilèges du système d'exploitation

Pour exécuter l'application UpdateXpress, les utilisateurs doivent posséder les privilèges administrateur ou root (équivalent) sur le système d'exploitation. L'application UpdateXpress renvoie une erreur si un utilisateur doté de privilèges insuffisants essaie de lancer le programme.

Stockez l'application UpdateXpress, y compris ses extractions, ainsi que tous les journaux sensibles, dans un emplacement sûr auquel ont accès seulement les utilisateurs autorisés.

Chapitre 3. Utilisation de l'application UpdateXpress

Les utilisateurs peuvent utiliser l'application UpdateXpress pour déployer de manière interactive des mises à jour. Une résolution d'écran d'au moins 1024 x 768 est recommandée lors de l'exécution de l'application UpdateXpress. Pour exécuter l'application UpdateXpress, procédez à l'extraction du fichier compressé et appelez le fichier exécutable du système d'exploitation. Aucune installation n'est requise.

Windows

Pour le système d'exploitation Windows, l'application UpdateXpress est appelée comme suit :

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

Pour chaque édition de l'application UpdateXpress, les utilisateurs peuvent distinguer le nom du fichier Windows ZIP par son numéro de version. Le fichier ZIP Windows est indiqué sous la forme **lnvgy_utl_lxce_ux{ build id }_{ version }_windows_i386.zip** où *lnvgy_utl_lxce_ux* est le nom du fichier ZIP, *build id* indique le numéro de build et *version* indique le numéro de version de l'application UpdateXpress.

Linux

Pour le système d'exploitation Linux, l'application UpdateXpress est appelée comme suit :

Système d'exploitation	Nom de l'application UpdateXpress
Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T et supérieur	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T et supérieur	`lnvgy_utl_lxce_ux{ build id }_4.x.x_linux_x86-64.tgz`

Le nom de l'application UpdateXpress version est différent pour les systèmes d'exploitation Linux et Windows. Pour plus de simplicité, <*Zipfile*> est utilisé par la suite pour faire référence au nom de l'application UpdateXpress pour les systèmes d'exploitation Windows et Linux dans la présente documentation.

Lancement de l'application UpdateXpress

Les utilisateurs peuvent utiliser l'application UpdateXpress pour acquérir les derniers modules UXSP et les mises à jour individuelles les plus récentes.

Pour lancer l'application UpdateXpress, procédez comme suit :

- **Pour Windows** :
  1. Extrayez le fichier <*Zipfile*> dans un dossier local.
  2. Effectuez l'une des opérations suivantes :
     - Cliquez deux fois sur **lxce_ux.exe**.
     - Cliquez avec le bouton droit de la souris sur **lxce_ux.exe**, puis cliquez sur **Exécuter en tant qu'administrateur** dans le menu contextuel.
- **Pour Linux** :

  Saisissez les commandes suivantes sur le terminal :

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

Mise à jour d'un serveur local depuis le site Web

L'application UpdateXpress peut mettre à jour une machine locale avec des mises à jour UXSP ou individuelles acquises depuis le site Web.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :
- L'application UpdateXpress s'exécute sur une machine locale à mettre à jour.
- La machine exécute un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour mettre à jour une machine locale depuis le site Web, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur local**. Si **Saisir les informations d'accès au BMC** est sélectionné, entrez les informations BMC dans cette fenêtre et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Paramètres de mise à jour, effectuez une ou plusieurs des actions suivantes :
   - Pour mettre à niveau le microprogramme du système de sauvegarde, sélectionnez **Mettre à jour uniquement l'image de sauvegarde du module BMC (et UEFI, le cas échéant)** et cliquez sur **Suivant**.
   - Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur** et cliquez sur **Suivant**.
6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web de support Lenovo** et cliquez sur **Suivant**.
7. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
8. Dans la fenêtre Répertoire cible, indiquez l'emplacement dans lequel vous voulez télécharger les mises à jour ou acceptez l'emplacement par défaut, puis cliquez sur **Suivant**.
9. Sur la page Accès à Internet, si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, effectuez une ou plusieurs des actions :
   - Configurer le **serveur proxy** :
     a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

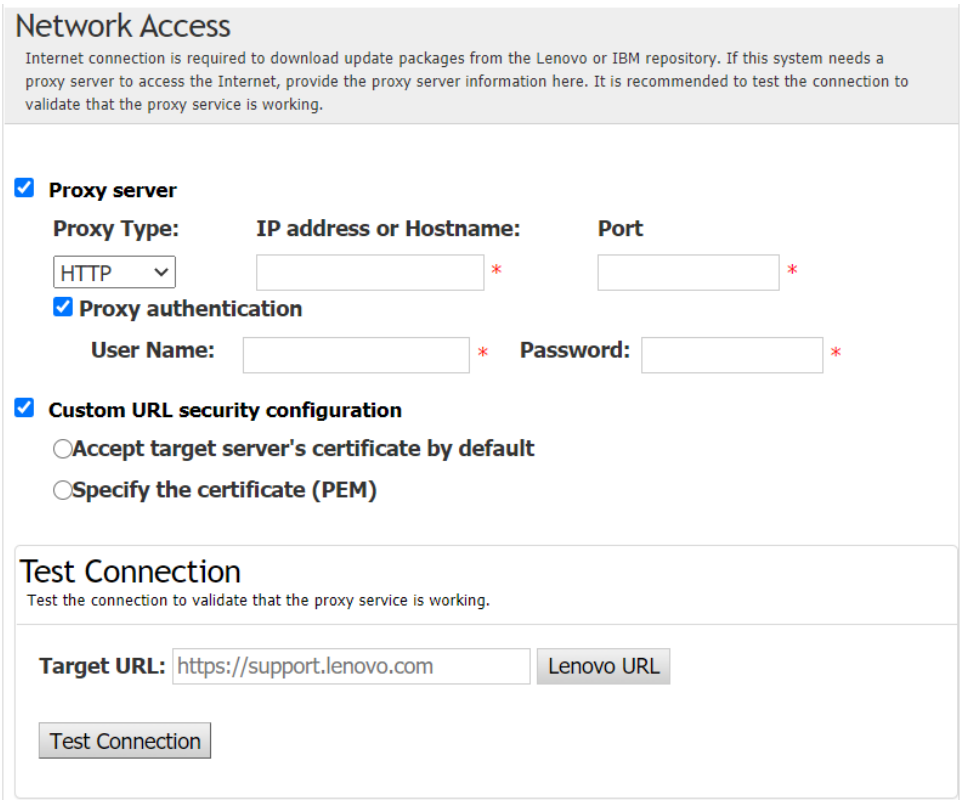
     b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

   - Configurer la **Configuration de sécurité d'URL personnalisée**

     Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :
     – **Accepter le certificat du serveur cible par défaut**

– **Indiquer le certificat (PEM)**



10. Dans la fenêtre Recommandation de mise à jour, effectuez une ou plusieurs des actions suivantes :
    - Pour afficher tous les modules de mise à jour, sélectionnez **Afficher les mises à jour des périphériques non détectés**.
    - Pour mettre à jour le composant, sélectionnez le composant cible, puis cliquez sur **Suivant**.
11. Dans la fenêtre Faire l'acquisition des mises à jour, le tableau d'acquisition affiche la progression de l'acquisition des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
12. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
13. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau et cliquez sur **Fermer** pour quitter l'application.

Mise à jour d'un serveur local depuis un répertoire local

L'application UpdateXpress peut mettre à jour une machine locale avec des mises à jour UXSP ou individuelles acquises depuis un dossier local.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :
- L'application UpdateXpress s'exécute sur une machine locale à mettre à jour.
- La machine exécute un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- L'ISO monté ne doit pas être utilisé comme répertoire local valide ; sinon, il pourrait être démonté pendant le processus de mise à jour et provoquer une défaillance du flash.

Pour mettre à jour une machine locale depuis un répertoire local, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

3. Dans la fenêtre Server cible, sélectionnez **Gérer le serveur local** et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Paramètres de mise à jour, effectuez une ou plusieurs des actions suivantes :
   - Pour mettre à jour l'image de sauvegarde de BMC ou d'UEFI, sélectionnez **Mettre à jour uniquement l'image de sauvegarde du module BMC (et UEFI, le cas échéant)** et cliquez sur **Suivant**.
   - Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur** et cliquez sur **Suivant**.
6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour indiquer un dossier local, procédez comme suit :
   - Cliquez sur **Parcourir**, sélectionnez le dossier cible, puis cliquez sur **Suivant**.
   - Entrez le chemin du dossier dans le champ situé en regard du bouton **Parcourir**, puis cliquez sur **Suivant**.
7. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
8. Dans la fenêtre Recommandation de mise à jour, effectuez l'une des actions suivantes :
   - Pour afficher tous les packages de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté**.
   - Pour comparer les versions du pilote et du microprogramme installées avec les versions les plus récentes, cliquez sur **Commencer**. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.
   - Pour comparer la version des appareils installés sur le système local avec la version la plus récente, sélectionnez **Comparer uniquement les appareils installés** et cliquez sur **Commencer**. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.
9. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
10. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau et cliquez sur **Fermer** pour quitter l'application.

Mise à jour d'un serveur distant depuis le site Web

L'application UpdateXpress peut mettre à jour une machine distante avec des mises à jour UXSP ou individuelles acquises depuis le site Web.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :

L'application UpdateXpress s'exécute sur une machine sur laquelle est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour mettre à jour une machine distante depuis le site Web, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - **(Paramètre) Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - **(Paramètre) Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - **(Paramètre) Mot de passe** : mot de passe BMC du système cible.
   - **(Paramètre) Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : Si vous ne cochez pas le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.

4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Paramètres de mise à jour, sélectionnez une ou plusieurs options. Si l'option **Utiliser un serveur distant distinct plutôt que le serveur BMC** est sélectionnée, entrez les informations suivantes :
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Nom d'utilisateur** : nom d'utilisateur du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Mot de passe** : mot de passe du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Port** : numéro de port du serveur. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Répertoire** : emplacement sur le serveur où sont copiées les modules de mise à jour.

     Remarque : Entrez un chemin d'accès complet sur le serveur SFTP/HTTP/HTTPS/FTP. Le serveur FTP est utilisé uniquement pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.
6. Pour configurer l'empreinte digitale de la clé de serveur SFTP, effectuez l'une des actions suivantes :
   - Pour vérifier l'empreinte digitale de la clé de serveur SFTP, cliquez sur **Oui**.
   - Pour ne pas vérifier l'empreinte digitale de la clé de serveur SFTP/HTTPS, sélectionnez **Ignorer l'empreinte digitale de la clé du serveur SFTP** et cliquez sur **Suivant**.
7. Effectuez une ou plusieurs des opérations suivantes :
   - Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur** et cliquez sur **Suivant**.
   - Pour mettre à niveau le microprogramme du système de sauvegarde, sélectionnez **Mettre à jour uniquement l'image de sauvegarde du module BMC (et UEFI, le cas échéant)** et cliquez sur **Suivant**.
8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web de support Lenovo** et cliquez sur **Suivant**.
9. Dans la fenêtre Répertoire cible, indiquez l'emplacement dans lequel vous voulez télécharger les mises à jour ou acceptez l'emplacement par défaut, puis cliquez sur **Suivant**.
10. Sur la page Accès à Internet, si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
    Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, configurez le **Serveur proxy** et/ou la **Configuration de sécurité d'URL personnalisée** en fonction des exigences de sécurité comme suit :
    - **Serveur proxy**
      a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

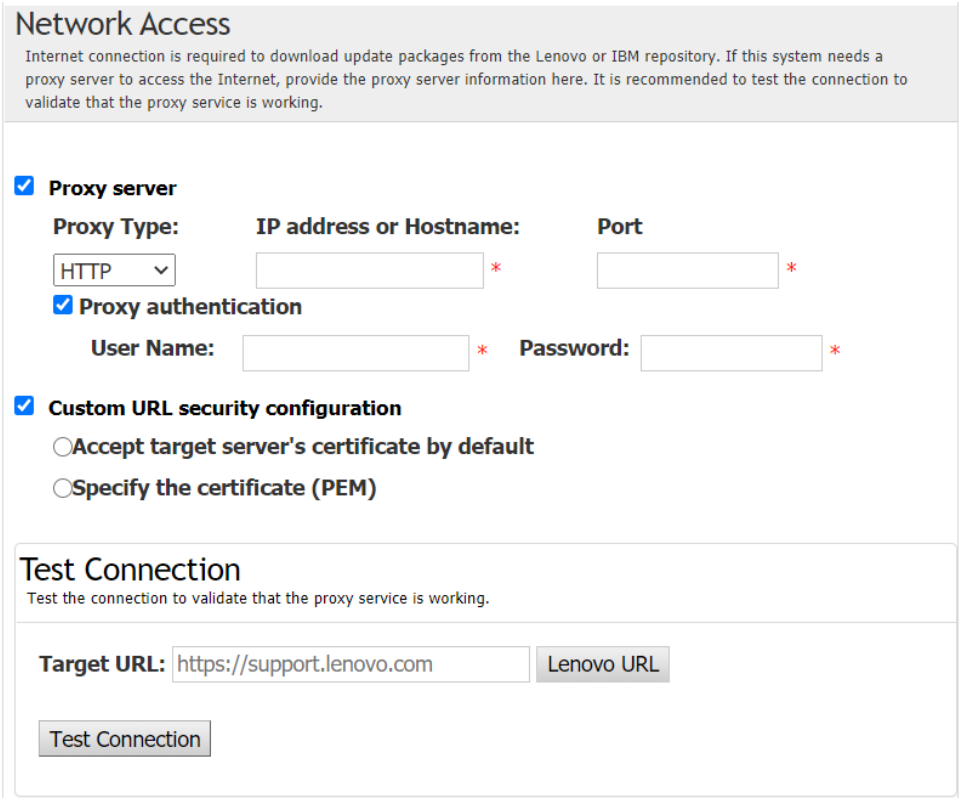
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

      b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

    - **Configuration de sécurité d'URL personnalisée**

Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :
- **Accepter le certificat du serveur cible par défaut**
- **Indiquer le certificat (PEM)**



11. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
12. Dans la fenêtre Recommandation de mise à jour, effectuez une ou plusieurs des actions suivantes :
    - Pour afficher tous les modules de mise à jour, sélectionnez **Afficher les mises à jour des périphériques non détectés**.
    - Pour mettre à jour le composant, sélectionnez le composant cible, puis cliquez sur **Suivant**.
13. Dans la fenêtre Faire l'acquisition des mises à jour, le tableau d'acquisition affiche la progression de l'acquisition des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
14. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
15. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Mise à jour d'un serveur distant depuis un répertoire local

L'application UpdateXpress peut mettre à jour une machine distante avec des mises à jour UXSP ou individuelles acquises depuis un dossier local.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :

L'application UpdateXpress s'exécute sur une machine sur laquelle est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour mettre à jour une machine distante depuis un répertoire local, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS, sélectionnez **Acceptez le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS par défaut** et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Paramètres de mise à jour, si **Utiliser un serveur distant distinct** est sélectionné, saisissez les informations suivantes :
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Nom d'utilisateur** : nom d'utilisateur du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Mot de passe** : mot de passe du serveur.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Port** : numéro de port du serveur. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
   - (Paramètre SFTP/HTTP/HTTPS/FTP) **Répertoire** : emplacement sur le serveur où sont copiées les modules de mise à jour.

     Remarque : Entrez un chemin d'accès complet sur le serveur SFTP/HTTP/HTTPS/FTP. Le serveur FTP est utilisé uniquement pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.
6. Pour configurer l'empreinte digitale de la clé de serveur SFTP, effectuez l'une des actions suivantes :
   - Pour vérifier l'empreinte digitale de la clé de serveur SFTP, cliquez sur **Oui**.
   - Pour ne pas vérifier l'empreinte digitale de la clé de serveur SFTP/HTTPS, sélectionnez **Ignorer l'empreinte digitale de la clé du serveur SFTP** et cliquez sur **Suivant**.
7. Effectuez une ou plusieurs des opérations suivantes :
   - Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur** et cliquez sur **Suivant**.
   - Pour mettre à niveau le microprogramme du système de sauvegarde, sélectionnez **Mettre à jour uniquement l'image de sauvegarde du module BMC (et UEFI, le cas échéant)** et cliquez sur **Suivant**.
8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour indiquer un dossier local, procédez comme suit :
   - Cliquez sur **Parcourir**, sélectionnez le dossier souhaité, puis cliquez sur **Suivant**.
   - Entrez le chemin du dossier dans le champ situé en regard du bouton **Parcourir**, puis cliquez sur **Suivant**.
9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
10. Dans la fenêtre Recommandation de mise à jour, cliquez sur **Commencer** pour comparer la version du microprogramme installée avec la version la plus récente. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.

    Remarque : Pour afficher tous les packages de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.
11. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.

12. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Configuration du BIOS pour un serveur distant

L'application UpdateXpress prend en charge la configuration des paramètres BIOS pour un serveur distant.

Condition préalable :

La fonction de configuration BIOS du serveur distant est uniquement prise en charge sur les serveurs ThinkServer/WenTian. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour configurer le BIOS, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS, sélectionnez **Acceptez le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS par défaut** et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configuration du BIOS**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Mode de configuration, sélectionnez **Configuration du BIOS commune** ou **Importer le fichier de configuration du BIOS**, puis cliquez sur **Suivant**.
6. Effectuez l'une des opérations suivantes :
   - Si **Importer le fichier de configuration du BIOS** a été sélectionné à l'étape précédente, ignorez cette étape.
   - Si **Configuration BIOS commune** est sélectionnée à l'étape précédente, sélectionnez une ou plusieurs valeurs actuelles, puis cliquez sur **Suivant**.
7. Dans la fenêtre Vue des modifications du BIOS, les données seront modifiées et indiqueront **affiché**, **vérifier** et **confirmer**. Cliquez sur **Suivant**.
8. Dans la fenêtre Exporter la configuration du BIOS, exportez la configuration en tant que fichier. Indiquez l'emplacement du fichier exporté, puis cliquez sur **Suivant**.
9. Dans la fenêtre Configuration en cours d'exécution, sélectionnez **Redémarrer manuellement** ou **Redémarrer immédiatement**, puis cliquez sur **Démarrer**. Lorsque la tâche est terminée, cliquez sur **Suivant**.
10. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de configuration et cliquez sur **Fermer** pour quitter l'application.

Collecte de journaux pour un serveur distant

L'application UpdateXpress permet de collecter les journaux d'un serveur distant.

Condition préalable :

La fonction de collecte pour un serveur distant n'est prise en charge que sur les serveurs ThinkServer/WenTian. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour collecter les journaux, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS, sélectionnez **Acceptez le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS par défaut** et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Collecter le journal**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Mode de collecte de journaux, sélectionnez **Collecter le journal BMC** ou **Collecter le journal FFDC**, ou les deux, puis cliquez sur **Suivant**.
6. Dans la fenêtre Résultats de la collecte des journaux, vérifiez les résultats, puis cliquez sur **Suivant**.
7. Dans la fenêtre Terminer, cliquez sur  pour vérifier les journaux détaillés, puis cliquez sur **Fermer** pour quitter.

Mise à jour de plusieurs serveurs distants depuis le site Web

L'application UpdateXpress prend en charge la mise à jour des serveurs distants par lots depuis le site Web.

Remarque : Pour mettre à jour un seul serveur distant à partir du site Web, reportez-vous à « Mise à jour d'un serveur distant depuis le site Web » à la page 12.

Condition préalable :

La fonction de mise à jour multiple pour les serveurs distants est uniquement prise en charge sur les serveurs ThinkServer et le serveur WenTian. Pour plus de détails sur les serveurs pris en charge, reportez-vous à la section « Modèles de serveur pris en charge » à la page 5.

Pour mettre à jour plusieurs serveurs distants depuis le site Web, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.
4. Dans la fenêtre Gestion de plusieurs serveurs, sélectionnez **Ajouter de nouveaux serveurs dans le pool de serveurs**, effectuez une ou plusieurs des actions suivantes, puis cliquez sur **Suivant**.
   - Pour ajouter de nouveaux serveurs dans le pool de serveurs, saisissez la plage d'adresses IP et cliquez sur **Détecter** dans la zone d'informations BMC, puis sélectionnez un ou plusieurs serveurs cible dans la liste du pool de serveurs.
   - Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Retirer les éléments sélectionnés**.
   - Pour vérifier si le nom d'utilisateur et le mot de passe sont corrects pour le serveur, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Scanner les éléments sélectionnés**.
   - Pour utiliser les données d'identification BMC communes pour la gestion, sélectionnez **Utiliser les données d'identification BMC communes pour la gestion**, saisissez le nom d'utilisateur et le mot de passe.
   - Pour exporter la liste du pool de serveurs du serveur actuel, cliquez sur **Exporter**. La liste du pool de serveurs sera enregistrée dans le fichier `configure.json`.

- Pour importer la liste du pool de serveurs sur l'autre serveur, cliquez sur **Importer** et sélectionnez le fichier cible `configure.json`.

5. Cliquez sur **Suivant** : un message apparaîtra pour rappeler aux utilisateurs de confirmer que le certificat doit être mis à jour. Cliquez sur **Accepter** pour mettre à jour le certificat.

   Remarque : Si les utilisateurs se connectent pour la première fois ou si le mot de passe a expiré, modifiez le mot de passe dans la fenêtre Modifier le mot de passe.
6. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
7. Dans la fenêtre Paramètres de mise à jour, sélectionnez une ou plusieurs options. Si l'option **Utiliser un serveur distant distinct plutôt que le serveur BMC** est sélectionnée, entrez les informations suivantes :
   - (Paramètre HTTPS/FTP) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte du serveur.
   - (Paramètre HTTPS/FTP) **Nom d'utilisateur** : nom d'utilisateur du serveur.
   - (Paramètre HTTPS/FTP) **Mot de passe** : mot de passe du serveur.
   - (Paramètre HTTPS/FTP) **Port** : numéro de port du serveur. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
   - (Paramètre HTTPS/FTP) **Répertoire** : emplacement sur le serveur où sont copiées les modules de mise à jour.

     Remarque : Entrez un chemin d'accès complet sur le serveur HTTPS/FTP. Le serveur FTP est utilisé uniquement pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.
8. Pour configurer l'empreinte digitale de la clé de serveur HTTPS, effectuez l'une des actions suivantes :
   - Pour vérifier l'empreinte digitale de la clé de serveur HTTPS, cliquez sur **Oui**.
   - Pour ne pas vérifier l'empreinte digitale de la clé de serveur HTTPS, sélectionnez **Ignorer l'empreinte digitale de la clé du serveur HTTPS** et cliquez sur **Suivant**.
9. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web de support Lenovo** et cliquez sur **Suivant**.
10. Dans la fenêtre Répertoire cible, indiquez l'emplacement dans lequel vous voulez télécharger les mises à jour ou acceptez l'emplacement par défaut, puis cliquez sur **Suivant**.
11. Sur la page Accès à Internet, si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
    Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, configurez le **Serveur proxy** et/ou la **Configuration de sécurité d'URL personnalisée** en fonction des exigences de sécurité comme suit :
    - **Serveur proxy**
      a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

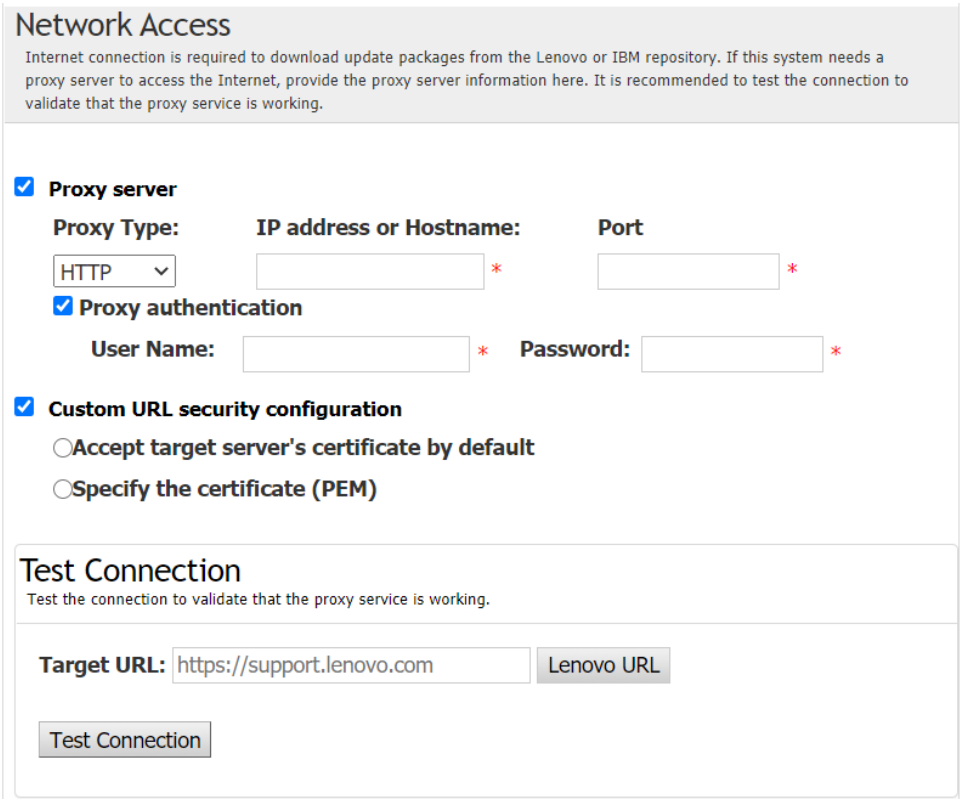
      b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

    - **Configuration de sécurité d'URL personnalisée**

      Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :

- **Accepter le certificat du serveur cible par défaut**
- **Indiquer le certificat (PEM)**



12. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
13. Dans la fenêtre Recommandation de mise à jour, cliquez sur **Commencer** pour comparer la version du microprogramme avec la version la plus récente. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.

    Remarque : Pour afficher tous les packages de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.
14. Dans la fenêtre Faire l'acquisition des mises à jour, le tableau d'acquisition affiche la progression de l'acquisition des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
15. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
16. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Mise à jour de plusieurs serveurs distants depuis un répertoire local

L'application UpdateXpress prend en charge la mise à jour des serveurs distants par lots depuis un dossier local.

Remarque : Pour mettre à jour un seul serveur distant depuis un dossier local, reportez-vous à la section « Mise à jour d'un serveur distant depuis un répertoire local » à la page 14.

Condition préalable :

La fonction de mise à jour multiple pour les serveurs distants est uniquement prise en charge sur les serveurs ThinkServer et le serveur WenTian. Pour plus de détails sur les serveurs pris en charge, reportez-vous à la section « Modèles de serveur pris en charge » à la page 5.

Pour mettre à jour plusieurs serveurs distants depuis un répertoire local, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.
4. Dans la fenêtre Gestion de plusieurs serveurs, sélectionnez **Ajouter de nouveaux serveurs dans le pool de serveurs**, effectuez une ou plusieurs des actions suivantes, puis cliquez sur **Suivant**.
   - Pour ajouter de nouveaux serveurs dans le pool de serveurs, saisissez la plage d'adresses IP et cliquez sur **Détecter** dans la zone d'informations BMC, puis sélectionnez un ou plusieurs serveurs cible dans la liste du pool de serveurs.
   - Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Retirer les éléments sélectionnés**.
   - Pour vérifier si le nom d'utilisateur et le mot de passe sont corrects pour le serveur, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Scanner les éléments sélectionnés**.
   - Pour utiliser les données d'identification BMC communes pour la gestion, sélectionnez **Utiliser les données d'identification BMC communes pour la gestion**, saisissez le nom d'utilisateur et le mot de passe.
   - Pour exporter la liste du pool de serveurs du serveur actuel, cliquez sur **Exporter**. La liste du pool de serveurs sera enregistrée dans le fichier `configure.json`.
   - Pour importer la liste du pool de serveurs sur l'autre serveur, cliquez sur **Importer** et sélectionnez le fichier cible `configure.json`.
5. Cliquez sur **Suivant** : un message apparaîtra pour rappeler aux utilisateurs de confirmer que le certificat doit être mis à jour. Cliquez sur **Accepter** pour mettre à jour le certificat.

   Remarque : Si les utilisateurs se connectent pour la première fois ou si le mot de passe a expiré, modifiez le mot de passe dans la fenêtre Modifier le mot de passe.
6. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
7. Dans la fenêtre Paramètres de mise à jour, sélectionnez une ou plusieurs options. Si l'option **Utiliser un serveur distant distinct plutôt que le serveur BMC** est sélectionnée, entrez les informations suivantes :
   - (Paramètre HTTPS/FTP) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte du serveur.
   - (Paramètre HTTPS/FTP) **Nom d'utilisateur** : nom d'utilisateur du serveur.
   - (Paramètre HTTPS/FTP) **Mot de passe** : mot de passe du serveur.
   - (Paramètre HTTPS/FTP) **Port** : numéro de port du serveur. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
   - (Paramètre HTTPS/FTP) **Répertoire** : emplacement sur le serveur où sont copiées les modules de mise à jour.

     Remarque : Entrez un chemin d'accès complet sur le serveur HTTPS/FTP. Le serveur FTP est utilisé uniquement pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.
8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour indiquer un dossier local, procédez comme suit :
   - Cliquez sur **Parcourir**, sélectionnez le dossier souhaité, puis cliquez sur **Suivant**.
   - Entrez le chemin du dossier dans le champ situé en regard du bouton **Parcourir**, puis cliquez sur **Suivant**.
9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
10. Dans la fenêtre Recommandation de mise à jour, cliquez sur **Commencer** pour comparer la version du microprogramme installée avec la version la plus récente. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.

Remarque : Pour afficher tous les packages de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.

11. Dans la fenêtre Exécution de la mise à jour, cliquez sur **Commencer la mise à jour et confirmer pour continuer dans la fenêtre contextuelle**. Le tableau d'exécution affiche la progression de la mise à jour des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
12. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Configurer le BIOS pour plusieurs serveurs distants

L'application UpdateXpress permet de configurer les paramètres BIOS de plusieurs serveurs distants par lots.

Condition préalable :

La fonction de configuration multiple du serveur distant est uniquement prise en charge sur les serveurs ThinkServer/WenTian. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour configurer le BIOS, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.
4. Dans la fenêtre Gestion de plusieurs serveurs, sélectionnez **Ajouter de nouveaux serveurs dans le pool de serveurs**, effectuez une ou plusieurs des actions suivantes, puis cliquez sur **Suivant**.
   - Pour ajouter de nouveaux serveurs dans le pool de serveurs, saisissez la plage d'adresses IP et cliquez sur **Détecter** dans la zone d'informations BMC, puis sélectionnez un ou plusieurs serveurs cible dans la liste du pool de serveurs.
   - Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Retirer les éléments sélectionnés**.
   - Pour vérifier si le nom d'utilisateur et le mot de passe sont corrects pour le serveur, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Scanner les éléments sélectionnés**.
   - Pour utiliser les données d'identification BMC communes pour la gestion, sélectionnez **Utiliser les données d'identification BMC communes pour la gestion**, saisissez le nom d'utilisateur et le mot de passe.
   - Pour exporter la liste du pool de serveurs du serveur actuel, cliquez sur **Exporter**. La liste du pool de serveurs sera enregistrée dans le fichier `configure.json`.
   - Pour importer la liste du pool de serveurs sur l'autre serveur, cliquez sur **Importer** et sélectionnez le fichier cible `configure.json`.
5. Cliquez sur **Suivant** : un message apparaîtra pour rappeler aux utilisateurs de confirmer que le certificat doit être mis à jour. Cliquez sur **Accepter** pour mettre à jour le certificat.

   Remarque : Si les utilisateurs se connectent pour la première fois ou si le mot de passe a expiré, modifiez le mot de passe dans la fenêtre Modifier le mot de passe.
6. Dans la fenêtre Tâche, sélectionnez **Configuration du BIOS**, puis cliquez sur **Suivant**.

   Remarque : Cette fonction de configuration du BIOS est prise en charge uniquement dans les serveurs ayant les mêmes types de machine.
7. Dans la fenêtre Mode de configuration, sélectionnez **Configuration du BIOS commune** ou **Importer le fichier de configuration du BIOS**, puis cliquez sur **Suivant**.
8. Effectuez l'une des opérations suivantes :
   - Si **Importer le fichier de configuration du BIOS** a été sélectionné à l'étape précédente, ignorez cette étape.

- Si **Configuration BIOS commune** est sélectionnée à l'étape précédente, sélectionnez une ou plusieurs valeurs actuelles, puis cliquez sur **Suivant**.

9. Dans la fenêtre Vue des modifications du BIOS, confirmez les paramètres modifiés du BIOS, puis cliquez sur **Suivant**.
10. Dans la fenêtre Exporter la configuration du BIOS, exportez la configuration en tant que fichier. Indiquez l'emplacement du fichier exporté, puis cliquez sur **Suivant**.
11. Dans la fenêtre Configuration en cours d'exécution, sélectionnez **Redémarrer manuellement** ou **Redémarrer immédiatement**, puis cliquez sur **Démarrer**. Lorsque la tâche est terminée, cliquez sur **Suivant**.
12. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de configuration et cliquez sur **Fermer** pour quitter l'application.

Collecte de journaux pour plusieurs serveurs distants

L'application UpdateXpress permet de collecter les journaux des serveurs distants par lots.

Condition préalable :

La fonction de collecte multiple du serveur distant est uniquement prise en charge sur les serveurs ThinkServer/WenTian. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour collecter les journaux, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.
4. Dans la fenêtre Gestion de plusieurs serveurs, sélectionnez **Ajouter de nouveaux serveurs dans le pool de serveurs**, effectuez une ou plusieurs des actions suivantes, puis cliquez sur **Suivant**.
   - Pour ajouter de nouveaux serveurs dans le pool de serveurs, saisissez la plage d'adresses IP et cliquez sur **Détecter** dans la zone d'informations BMC, puis sélectionnez un ou plusieurs serveurs cible dans la liste du pool de serveurs.
   - Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Retirer les éléments sélectionnés**.
   - Pour vérifier si le nom d'utilisateur et le mot de passe sont corrects pour le serveur, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Scanner les éléments sélectionnés**.
   - Pour utiliser les données d'identification BMC communes pour la gestion, sélectionnez **Utiliser les données d'identification BMC communes pour la gestion**, saisissez le nom d'utilisateur et le mot de passe.
   - Pour exporter la liste du pool de serveurs du serveur actuel, cliquez sur **Exporter**. La liste du pool de serveurs sera enregistrée dans le fichier `configure.json`.
   - Pour importer la liste du pool de serveurs sur l'autre serveur, cliquez sur **Importer** et sélectionnez le fichier cible `configure.json`.
5. Cliquez sur **Suivant** : un message apparaîtra pour rappeler aux utilisateurs de confirmer que le certificat doit être mis à jour. Cliquez sur **Accepter** pour mettre à jour le certificat.

   Remarque : Si les utilisateurs se connectent pour la première fois ou si le mot de passe a expiré, modifiez le mot de passe dans la fenêtre Modifier le mot de passe.
6. Dans la fenêtre Tâche, sélectionnez **Collecter le journal**, puis cliquez sur **Suivant**.
7. Dans la fenêtre Mode de collecte de journaux, sélectionnez **Collecter le journal BMC** ou **Collecter le journal FFDC** ou les deux, indiquez le répertoire de sortie du journal, puis cliquez sur **Suivant**.
8. Dans la fenêtre Résultats de la collecte des journaux, vérifiez les résultats, puis cliquez sur **Suivant**.
9. Dans la fenêtre Terminer, cliquez sur  pour vérifier le journal de configuration, puis cliquez sur **Fermer** pour quitter.

Création d'un référentiel de mises à jour

L'application UpdateXpress peut créer un référentiel de mises à jour UXSP ou individuelles acquises sur le site Web.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :
- L'application UpdateXpress s'exécute sur une machine où le référentiel doit être créé.
- La machine exécute un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour créer un référentiel des mises à jour, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Créer un référentiel de mises à jours** et cliquez sur **Suivant**.
4. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
   - Sélectionnez **UpdateXpress System Packs (UXSPs)** pour mettre à jour UXSP. La fenêtre Mettre à jour la sélection ne s'affiche pas si **UpdateXpress System Packs (UXSPs)** est sélectionné, mais l'ensemble des modules UXSP sont téléchargés.
   - Sélectionnez **Dernières mises à jour individuelles disponibles** pour mettre à jour des modules individuels. La fenêtre Mettre à jour la sélection s'affiche à l'étape suivante si **Dernières mises à jour individuelles disponibles** est sélectionné et les utilisateurs doivent sélectionner les modules cibles.
5. Sur la page Accès à Internet, s'il n'y a aucune exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, configurez le **Serveur proxy** et/ou la **Configuration de sécurité d'URL personnalisée** en fonction de vos exigences de sécurité comme suit :
   - **Serveur proxy**
     a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

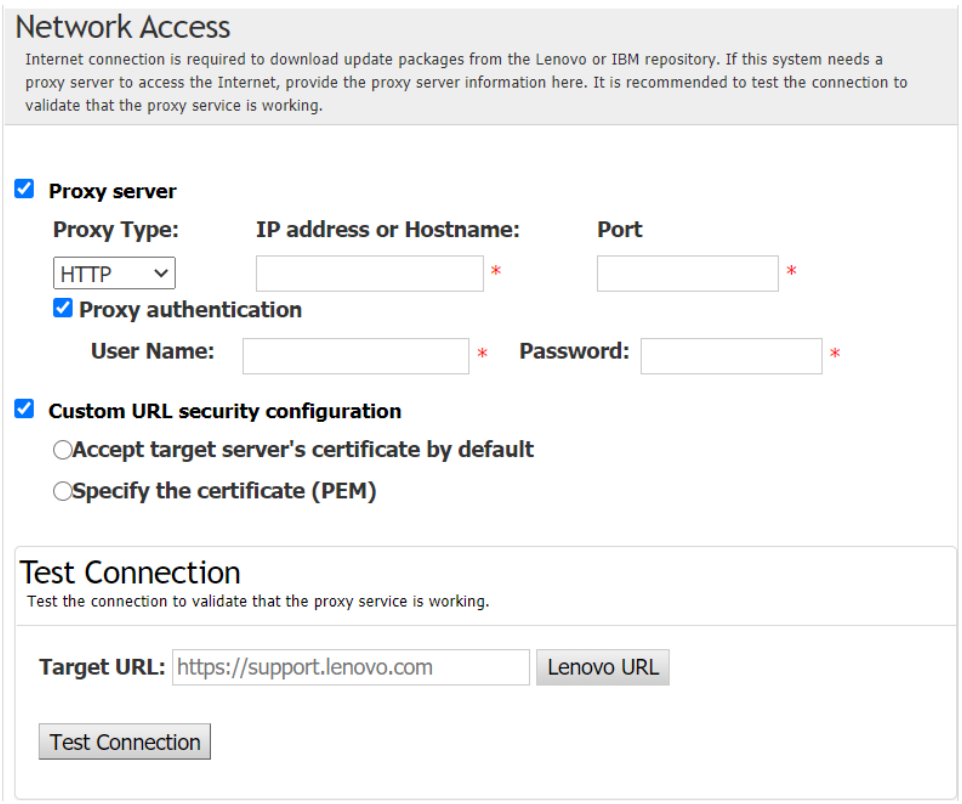
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

     b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

   - **Configuration de sécurité d'URL personnalisée**

     Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :
     – **Accepter le certificat du serveur cible par défaut**
     – **Indiquer le certificat (PEM)**



6. Dans la fenêtre Types de machine, sélectionnez les types de machine cibles, puis cliquez sur **Suivant**.
   - Pour sélectionner tous les types de machine répertoriés, cochez la case située dans l'en-tête.
   - Pour ajouter un type de machine, cliquez sur **Ajouter**, puis indiquez le type de machine.
   - Pour retirer un type de machine, sélectionnez le type de machine dans la liste, puis cliquez sur **Retirer**.
   - Pour mettre à jour la liste des types de machine vers la dernière version, cliquez sur **Mettre à jour la liste**.
   - Pour réinitialiser la liste des types de machine, cliquez sur **Réinitialiser la liste**.
7. Dans la fenêtre Systèmes d'exploitation, sélectionnez les systèmes d'exploitation cibles, puis cliquez sur **Suivant**.
8. Dans la fenêtre Répertoire cible, indiquez l'emplacement dans lequel vous voulez télécharger les mises à jour ou acceptez l'emplacement par défaut, puis cliquez sur **Suivant**.
9. (Facultatif) Sélectionnez **Dernières mises à jour individuelles disponibles**, la fenêtre Mettre à jour la sélection s'affiche. Sélectionnez les mises à jour cibles, puis cliquez sur **Suivant**.
10. Dans la fenêtre Faire l'acquisition des mises à jour, le tableau d'acquisition affiche la progression de l'acquisition des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
11. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Configuration de la grappe RAID pour un serveur distant

L'application UpdateXpress peut procéder à une configuration RAID pour un serveur distant, par exemple la collecte d'informations RAID, la création de grappe RAID, la configuration de l'état du disque et l'effacement de la configuration d'un contrôleur.

Condition préalable :

L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour configurer la grappe RAID, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**. Lorsqu'une fenêtre affichant les informations associées s'affiche, cliquez sur **OK**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS, sélectionnez **Acceptez le certificat du serveur BMC et l'empreinte digitale de la clé du serveur SFTP/HTTPS par défaut** et cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configuration RAID à distance** ou **Effectuer la mise à jour sur le serveur cible**, ou les deux, puis cliquez sur **Suivant**.
5. Dans la fenêtre Configuration RAID, UpdateXpress collectera tout d'abord les informations RAID du serveur à distance. Une fois la collecte terminée, les informations RAID s'afficheront dans la fenêtre.
   - Pour effacer la configuration d'un contrôleur, cliquez sur **Effacer le contrôleur**.
   - Pour modifier l'état de l'unité sur JBOD, cliquez sur **Définir sur JBOD**.
   - Pour modifier l'état de l'unité sur CORRECT non configuré, cliquez sur **Définir sur CORRECT**.
6. Dans la fenêtre Configuration RAID, pour créer une grappe pour le contrôleur, cliquez sur **Créer une grappe**.
   a. Dans la fenêtre Assistant, sélectionnez le niveau RAID, ajoutez des portées, des membres et des disques de secours pour la grappe, puis créez des volumes et définissez les paramètres de disque.
   b. Lorsque les informations récapitulatives s'affichent, cliquez sur **Créer** pour commencer à créer une grappe de stockage.
   c. Une fois le processus terminé, cliquez sur **Collecter** ou **Actualiser** pour collecter à nouveau les informations RAID.
   d. Cliquez sur **Suivant** si aucune autre action n'est nécessaire.
7. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Exécution d'une mise à jour transférée pour un serveur distant

L'application UpdateXpress permet d'effectuer des mises à jour transférées pour un serveur distant.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :

- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour effectuer une mise à jour transférée pour un serveur distant, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.

4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Paramètres de mise à jour, sélectionnez une ou plusieurs options et cliquez sur **Suivant**.

   Remarques :
   - Si l'option **Utiliser un serveur distant distinct plutôt que le serveur BMC** est sélectionnée, entrez les informations suivantes :
     - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
     - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
     - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
     - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
     - (Paramètre) **Répertoire** : chemin d'accès complet sur le serveur SFTP. Le fichier des mises à jour sera téléchargé dans ce répertoire. Assurez-vous que le répertoire est accessible. Par exemple : /payload
   - Pour ne pas vérifier l'empreinte digitale de la clé de serveur SFTP/HTTPS, sélectionnez **Ignorer l'empreinte digitale de la clé du serveur SFTP**.
6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web de support Lenovo** et cliquez sur **Suivant**.
7. Dans la fenêtre Répertoire cible, indiquez l'emplacement dans lequel vous voulez télécharger les mises à jour ou acceptez l'emplacement par défaut, puis cliquez sur **Suivant**.
8. Sur la page Accès à Internet, si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, configurez le **Serveur proxy** et/ou la **Configuration de sécurité d'URL personnalisée** en fonction des exigences de sécurité comme suit :
   - **Serveur proxy**
     a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

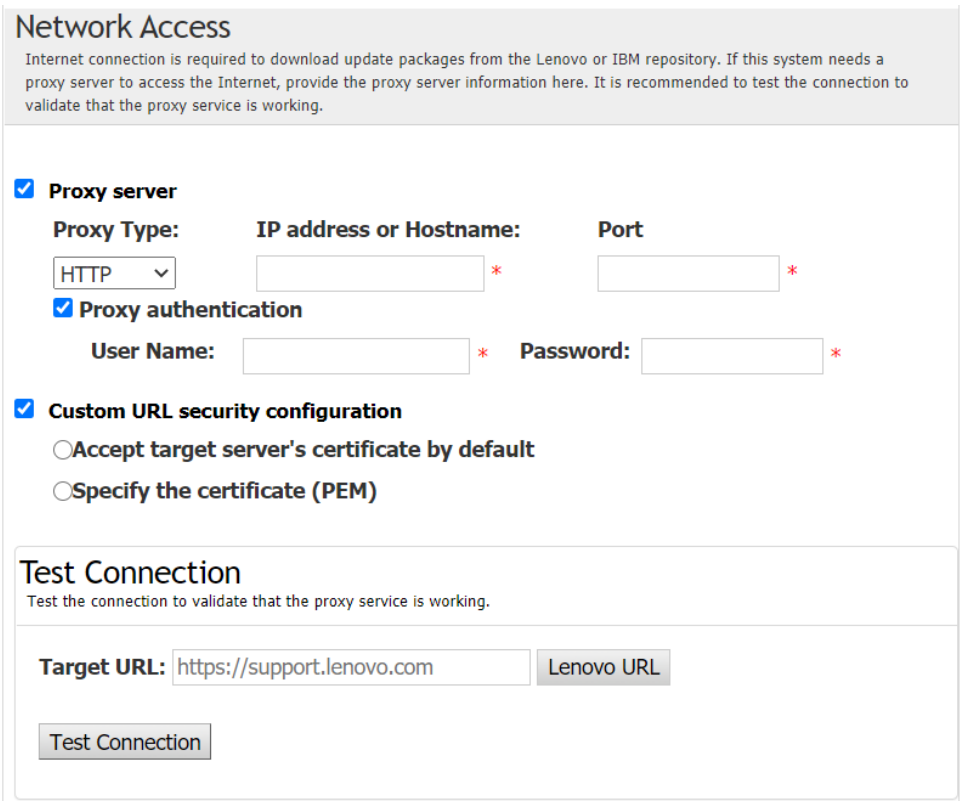
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

     b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

   - **Configuration de sécurité d'URL personnalisée**

     Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :
     - **Accepter le certificat du serveur cible par défaut**
     - **Indiquer le certificat (PEM)**



9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
10. Dans la fenêtre Recommandation de mise à jour, effectuez une ou plusieurs des actions suivantes :
    - Pour afficher tous les modules de mise à jour, sélectionnez **Afficher les mises à jour des périphériques non détectés**.
    - Pour mettre à jour le composant, sélectionnez le composant cible, puis cliquez sur **Suivant**.
11. Dans la fenêtre Faire l'acquisition des mises à jour, le tableau d'acquisition affiche la progression de l'acquisition des modules. Une fois la mise à jour terminée, cliquez sur **Suivant**.
12. Dans la fenêtre Exécution des mises à jour, cliquez sur **Commencer la mise à jour → Oui → Suivant**.

    Remarques : Pour mettre à jour le microprogramme avec des packages groupés, sélectionnez **Mettre à jour le microprogramme avec des packages groupés. Cette case à cocher et ses sous-options ne prennent en charge que XCC2** et définissent l'heure d'application.
    - **OnReset** : Mettre les packages à jour lors du prochain redémarrage du système.
    - **Immediate** : Mettre immédiatement les packages à jour. Le système peut être redémarré immédiatement.
    - **OnStartUpdateRquest** : Mettre les packages à jour en gérant la mise à jour transférée ou en exécutant des commandes OneCLI.
13. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Gestion d'une mise à jour transférée pour un serveur distant

L'application UpdateXpress prend en charge le lancement, l'annulation et l'affichage de toutes les mises à jour transférées pour un serveur distant.

Les prérequis suivants doivent être remplis pour effectuer cette tâche :

- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.

Pour gérer une mise à jour transférée pour un serveur distant, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Gérer la mise à jour transférée** et cliquez sur **Suivant**.
5. Dans la fenêtre Gestion des tâches, effectuez une ou plusieurs des actions suivantes et cliquez sur **Suivant**.
   - Pour obtenir les informations de tâche, entrez l'ID de tâche et cliquez sur  . L'ID de tâche est automatiquement renseigné pour la tâche en attente.
   - Pour lancer la mise à jour, cliquez sur **Démarrer** sur la tâche cible.
   - Pour annuler la mise à jour, cliquez sur **Annuler** sur la tâche cible.
6. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Gestion de la clé d'authentification SED

Les serveurs ThinkEdge fournissent l'accès à SED (Self-Encrypting Drive) à l'aide de la clé d'authentification. L'application UpdateXpress prend en charge la gestion de la clé d'authentification SED (AK), y compris la génération, la sauvegarde et la récupération.

Condition préalable :

- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- Cette fonction est uniquement prise en charge lorsque le serveur ThinkEdge est déverrouillé. Pour plus de détails sur les serveurs pris en charge, consultez la série ThinkEdge dans « Modèles de serveur pris en charge » à la page 5.

Pour gérer la clé d'authentification SED, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Gérer la clé d'authentification SED** et cliquez sur **Suivant**.
6. Dans la fenêtre Gestion de la clé d'authentification SED (AK), effectuez une ou plusieurs des actions suivantes :
   - Pour générer la clé SED AK, sélectionnez **Activer le chiffrement SED** lorsque SED EST désactivé, ou sélectionnez **Modifier la clé SED AK** lorsque la clé SED AK est activée. Sélectionnez la méthode cible dans la liste **Méthode** et cliquez sur **Regénérer**.

     Remarque : Il est recommandé de sauvegarder la clé AK en cas de perte de données. Les utilisateurs ne peuvent sélectionner d'autres options qu'après la sauvegarde de la clé AK.
   - Pour sauvegarder la clé SED AK, sélectionnez **Sauvegarder la clé SED AK**, saisissez l'emplacement et le mot de passe du fichier de sauvegarde, puis cliquez sur **Démarrer**. UpdateXpress enregistre le fichier de sauvegarde contenant les informations relatives à la clé SED AK.
   - Pour récupérer la clé SED AK, sélectionnez **Récupérer la clé SED AK**, procédez comme suit :
     - Pour récupérer les données à l'aide d'un fichier de sauvegarde, sélectionnez **Récupérer la clé SED AK à partir du fichier de sauvegarde** à partir de la liste déroulante **Méthode**, cliquez sur **Parcourir** pour sélectionner le fichier de sauvegarde, saisissez le mot de passe, puis cliquez sur **Démarrer la restauration**.
     - Pour récupérer les données à l'aide de phrases passe, cliquez sur **Récupérer la clé SED AK à l'aide de la phrase passe** à partir de la liste déroulante **Méthode**, saisissez la phrase de passe, puis cliquez sur **Lancer la restauration**.
7. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Demande du serveur sur le portail ThinkShield

Il est possible de demander la propriété du serveur ThinkEdge sur le portail Lenovo ThinkShield Key Vault Portal, UpdateXpress peut ensuite activer le serveur verrouillé via le portail.

Condition préalable :
- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- Cette fonction est uniquement prise en charge sur les serveurs ThinkEdge. Pour plus de détails sur les serveurs pris en charge, consultez la série ThinkEdge dans « Modèles de serveur pris en charge » à la page 5.

Pour demander le serveur sur le portail ThinkShield, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Demander le serveur sur le portail ThinkShield** et cliquez sur **Suivant**.

6. Dans la fenêtre Accès à Internet, effectuez l'une des actions suivantes :
   - Si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   - Si les utilisateurs ont des inquiétudes quant à la sécurité, configurez un ou plusieurs des paramètres suivants et cliquez sur **Tester la connexion** :
     – **Serveur proxy** : accès au réseau via un proxy HTTP/HTTPS.
       a. Sélectionnez **Serveur proxy**, puis remplissez les champs suivants :

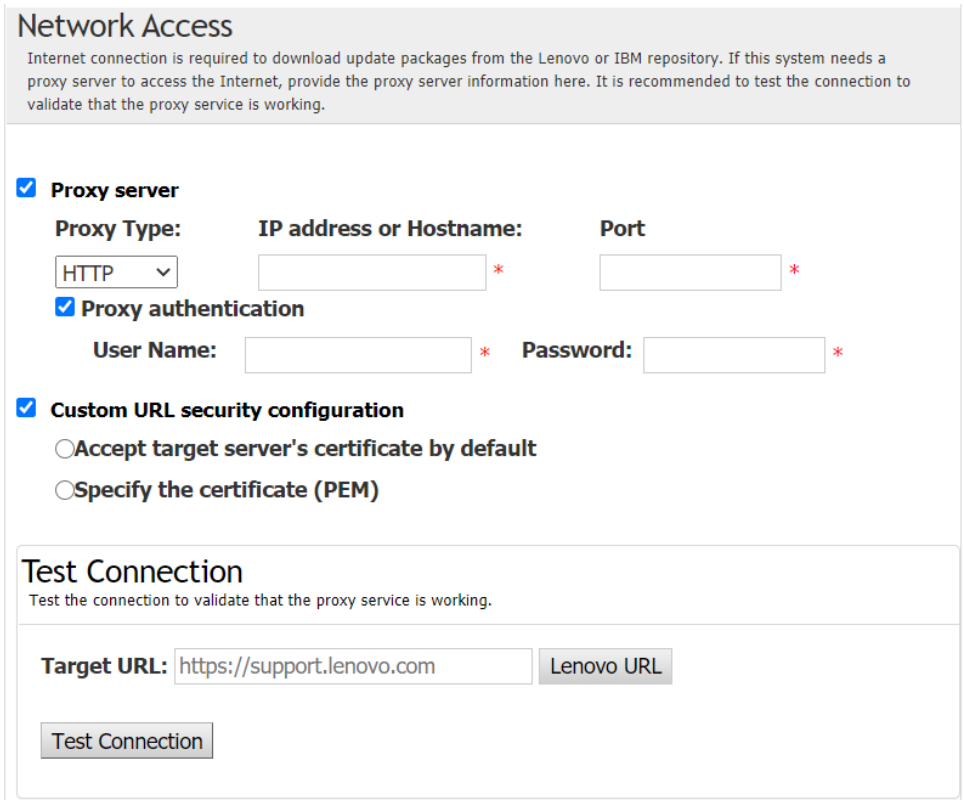
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

       b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

     – **Configuration de sécurité d'URL personnalisée** : accès au réseau via un proxy inversé.

       Sélectionnez l'une des opérations suivantes :
       – Accepter le certificat du serveur cible par défaut
       – Indiquer le certificat (PEM)



7. Dans la fenêtre Demander le serveur, saisissez l'ID de l'organisation, le nom d'utilisateur et le mot de passe du portail ThinkShield Key Vault Portal, puis cliquez sur **Demander**.
8. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Mise à niveau du mode de contrôle de verrouillage

Le serveur ThinkEdge est équipé des capteurs de sécurité qui détectent les événements d'altération, ce qui permet également de verrouiller le serveur à la détection d'une altération. UpdateXpress prend en charge la mise à niveau du mode de contrôle de verrouillage du serveur, de l'activation du serveur via XClarity Controller à la gestion du serveur via le portail ThinkShield.

Condition préalable :
- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- Cette fonction est uniquement prise en charge sur les serveurs ThinkEdge. Pour plus de détails sur les serveurs pris en charge, consultez la série ThinkEdge dans « Modèles de serveur pris en charge » à la page 5.

Pour mettre à niveau le mode de contrôle de verrouillage, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Fonctionnalités de sécurité ThinkEdge Server, cliquez sur **Contrôle de verrouillage du système**, puis sur **Suivant**, sélectionnez l'une des options suivantes pour revendiquer ou non la propriété du serveur sur le site ThinkShield Key Vault Portal et cliquez à nouveau sur **Suivant**.
   - Sélectionnez **Oui, je souhaite revendiquer le serveur**, et passez à l'étape 6.
   - Sélectionnez **Non, je souhaite poursuivre dans revendiquer le serveur dans ThinkShield Key Vault Portal**, puis passez à l'étape 8.
6. Dans la fenêtre Accès à Internet, effectuez l'une des actions suivantes :
   - Si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   - Si les utilisateurs ont des inquiétudes quant à la sécurité, configurez un ou plusieurs des paramètres suivants et cliquez sur **Tester la connexion** :
     – **Serveur proxy** : accès au réseau via un proxy HTTP/HTTPS.
       a. Sélectionnez **Serveur proxy**, puis remplissez les champs suivants :

Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

       b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

- **Configuration de sécurité d'URL personnalisée** : accès au réseau via un proxy inversé.

  Sélectionnez l'une des opérations suivantes :
  - Accepter le certificat du serveur cible par défaut
  - Indiquer le certificat (PEM)

7. Dans la fenêtre Valider le compte ThinkShield Portal, saisissez l'ID de l'organisation, le nom d'utilisateur et le mot de passe du portail ThinkShield Key Vault Portal, puis cliquez sur **Valider**. Une fois la vérification terminée, cliquez sur **Suivant**.

   Remarque : Les informations saisies doivent être valides. Sinon, le bouton **Suivant** ne sera *pas* activé.
8. Dans la fenêtre Contrôle de verrouillage système, saisissez manuellement **OUI**, puis cliquez sur **OK**. Lorsque le processus de mise à niveau est terminé, cliquez sur **Suivant**.
9. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Activation du serveur en mode de verrouillage

Le serveur ThinkEdge est équipé des capteurs de sécurité qui détectent les événements d'altération, ce qui permet également de verrouiller le serveur à la détection d'une altération. UpdateXpress prend en charge l'activation du serveur verrouillé via le portail ThinkShield Key Portal ou XClarity Controller.

Condition préalable :
- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- Cette fonction est uniquement prise en charge sur les serveurs ThinkEdge. Pour plus de détails sur les serveurs pris en charge, consultez la série ThinkEdge dans « Modèles de serveur pris en charge » à la page 5.

Pour activer le serveur en mode de verrouillage, procédez comme suit :
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Activer le serveur avec le portail ThinkShield** et cliquez sur **Suivant**.

   Remarque : Le contrôle de verrouillage du système par défaut est géré par XClarity Controller. Lorsque le contrôle de verrouillage est géré sur le portail ThinkShield, les utilisateurs ne peuvent activer le serveur en mode de verrouillage qu'après avoir été authentifiés par le portail ThinkShield Key Vault Portal.

6. Dans la fenêtre Accès à Internet, si les utilisateurs n'ont pas d'exigence spéciale relative à l'accès sécurisé, cliquez sur **Tester la connexion** pour vérifier la connexion réseau de l'URL cible, puis cliquez sur **Suivant**.
   Si les utilisateurs ont des inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, configurez le **Serveur proxy** et/ou la **Configuration de sécurité d'URL personnalisée** en fonction des exigences de sécurité comme suit :
   - **Serveur proxy**
     a. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

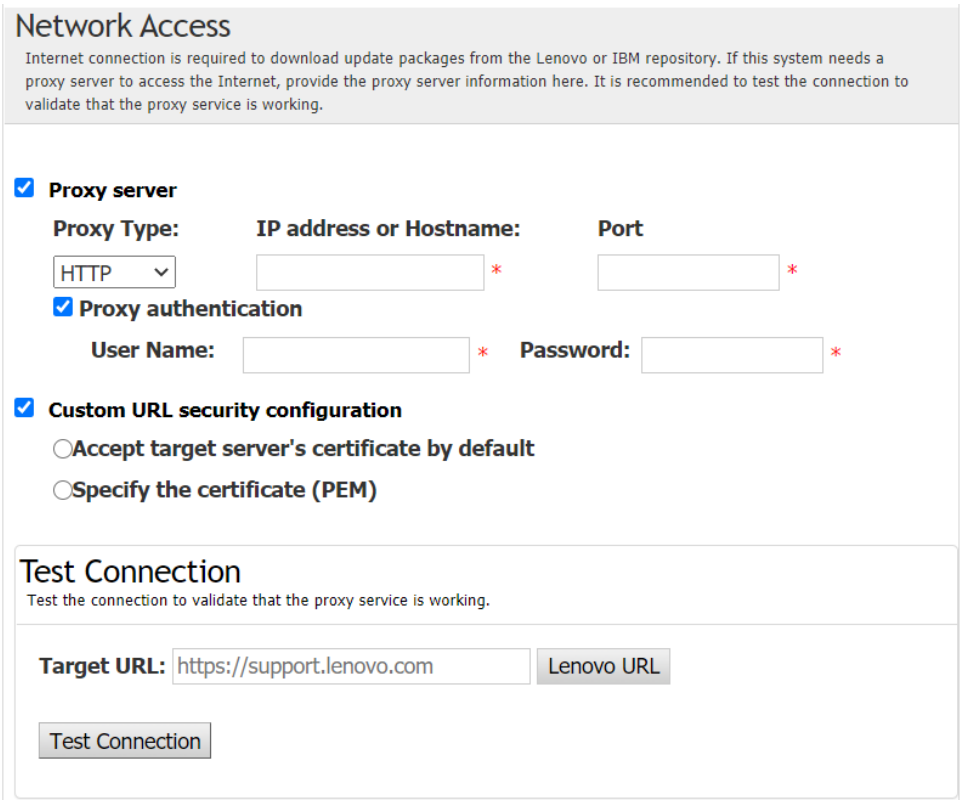
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

     b. Sélectionnez **Authentification de proxy** si les données d'identification doivent être spécifiées pour l'authentification sur le serveur proxy, et remplissez les zones suivantes :

Nom d'utilisateur	Le nom d'utilisateur pour l'authentification sur le serveur proxy.
Mot de passe	Le mot de passe pour le nom d'utilisateur spécifié.

   - **Configuration de sécurité d'URL personnalisée**

     Sélectionnez **Configuration de sécurité d'URL personnalisée** si les utilisateurs ont besoin d'un proxy inversé, puis sélectionnez l'une des options suivantes :
     – **Accepter le certificat du serveur cible par défaut**
     – **Indiquer le certificat (PEM)**



7. Dans la fenêtre Activer le serveur, saisissez l'ID de l'organisation ThinkShield Key Vault Portal, le nom d'utilisateur et le mot de passe, puis cliquez sur **Activer**. Lorsque le processus d'activation est terminé, cliquez sur **Suivant**.

   Remarque : Si le serveur est géré par XClarity Controller, les utilisateurs *n'ont pas* besoin d'entrer les informations de ThinkShield Key Vault Portal.
8. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Configuration des capteurs de sécurité

Les serveurs ThinkEdge sont équipés de capteurs de sécurité permettant de détecter les événements d'altération. UpdateXpress prend en charge l'activation, la désactivation et la modification du seuil du capteur de détection de mouvement et du détecteur d'intrusion de châssis.

Condition préalable :
- L'application UpdateXpress s'exécute sur un serveur sur lequel est installé un système d'exploitation pris en charge. Pour plus de détails sur les systèmes d'exploitation pris en charge, voir « Systèmes d'exploitation pris en charge » à la page 6.
- Cette fonction est uniquement prise en charge sur les serveurs ThinkEdge. Pour plus de détails sur les serveurs pris en charge, consultez la série ThinkEdge dans « Modèles de serveur pris en charge » à la page 5.

Pour configurer les capteurs de sécurité, procédez comme suit.
1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
   - (Paramètre) **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
   - (Paramètre) **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
   - (Paramètre) **Mot de passe** : mot de passe BMC du système cible.
   - (Paramètre) **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.

   Remarque : S'il n'est pas prévu que les utilisateurs vérifient le certificat du serveur BMC, sélectionnez **Accepter le certificat du serveur BMC par défaut**, puis cliquez sur **Suivant**.
4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.
5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Configurer les capteurs de sécurité**, puis cliquez sur **Suivant**.
6. Dans la fenêtre Configurer les capteurs de sécurité, effectuez une ou plusieurs des opérations suivantes, puis cliquez sur **Suivant**.
   - Pour activer ou désactiver **Détection de mouvement** ou **Détection d'intrusion de châssis**, sélectionnez les options dans la liste déroulante ou cliquez sur le bouton bascule pour changer l'état.

     Remarque : En cas de perte de données, il est recommandé de faire une sauvegarde des AK avant de sélectionner des éléments.
   - Pour réinitialiser le décompte d'étapes pour la détection de mouvement, cliquez sur **Réinitialiser le compteur d'étapes**. UpdateXpress réinitialise le nombre d'étapes à 0.
   - Pour modifier les étapes de seuil pour verrouiller la détection de mouvement, sélectionnez le niveau de l'étape cible dans **Seuil avant verrouillage**.

     Remarque : Le serveur ThinkEdge sera verrouillé une fois que l'événement d'altération a été détecté par le capteur de sécurité.

7. Dans la fenêtre Terminer, cliquez sur **Afficher le journal** pour consulter le journal de mise à niveau, copiez et enregistrez les commandes générées, puis cliquez sur **Fermer** pour quitter l'application.

Gestion du serveur sous connexion Ethernet directe

L'application UpdateXpress prend en charge la gestion des serveurs sous connexion Ethernet directe. Lorsque le câble réseau est connecté, UpdateXpress essaie d'accéder au BMC du serveur via l'adresse IP et les données d'identification BMC par défaut.

Pour gérer le serveur sous connexion Ethernet directe, procédez comme suit :

1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.
2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.
3. Dans la fenêtre Serveur cible, sélectionnez **Connexion Ethernet directe**, entrez les informations suivantes, puis cliquez sur **Suivant**.
4. Dans la fenêtre Paramètres de connexion Ethernet directe, procédez comme suit :
   a. Sélectionnez la carte cible dans le tableau « Carte réseau disponible ».
   b. Assurez-vous que l'adresse IP par défaut est bien **192.168.70.125**.
   c. Entrez le nom d'utilisateur et le mot de passe.
   d. Cliquez sur **Tester la connexion → Suivant** ou **Suivant**.
5. Dans la fenêtre Tâche, sélectionnez l'une des opérations suivantes :
   - **Effectuer la mise à jour sur le serveur cible**. Pour plus d'informations, voir l'étape 4 et les étapes ultérieures dans « Mise à jour d'un serveur distant depuis un répertoire local » à la page 14.
   - **Gérer la mise à jour transférée**. Pour plus d'informations, voir l'étape 4 et les étapes ultérieures dans « Gestion d'une mise à jour transférée pour un serveur distant » à la page 27.
   - **Configuration RAID à distance**. Pour plus d'informations, voir l'étape 4 et les étapes ultérieures dans « Configuration de la grappe RAID pour un serveur distant » à la page 24.
   - **Configurer la fonction de sécurité sur le serveur ThinkEdge**. Pour plus d'informations, voir l'étape 4 et les étapes ultérieures dans les sections suivantes :
     – « Gestion de la clé d'authentification SED » à la page 28
     – « Demande du serveur sur le portail ThinkShield » à la page 29
     – « Mise à niveau du mode de contrôle de verrouillage » à la page 31
     – « Activation du serveur en mode de verrouillage » à la page 32
     – « Configuration des capteurs de sécurité » à la page 34

Affichage des commandes OneCLI dans la fenêtre Terminer

UpdateXpress exécute des mises à jour en appelant des commandes OneCLI dans l'assistant de l'interface graphique. UpdateXpress 2.7.0 et les versions ultérieures affichent ces commandes dans la boîte de nouveau message de la fenêtre Terminer. Les utilisateurs peuvent enregistrer et utiliser les commandes pour invoquer la même fonction en mode CLI.

Exemple de commandes 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
```

Chapitre 4. Dépannage

Ce chapitre fournit des informations sur les actions à entreprendre en cas de problème au niveau de l'application UpdateXpress.

Limitations et problèmes

- **Lors de la spécification du certificat pour la configuration de sécurité du proxy ou de l'URL personnalisée lors de l'exécution d'UpdateXpress sous Linux, si les utilisateurs cliquent sur Parcourir pour la deuxième fois, la fenêtre de navigation peut ne pas s'afficher dans l'interface UpdateXpress.**

  Sur la page Accès à Internet, sélectionnez **HTTPS** dans la liste déroulante **Type de proxy**, sélectionnez **Configuration de sécurité de proxy personnalisé** et **Configuration de sécurité d'URL personnalisée**, puis cliquez sur **Parcourir...** pour spécifier le certificat pour les deux sélections. Lorsque les utilisateurs cliquent sur Parcourir pour la deuxième fois, il se peut que la fenêtre de navigation ne s'affiche pas.

  Solution de contournement : effectuez l'une ou plusieurs des actions suivantes :
  - Passez manuellement à la fenêtre de navigation en arrière-plan.
  - Ajustez la taille de la fenêtre pour afficher la fenêtre de navigation en arrière-plan.
  - Utilisez UpdateXpress sous Windows à la place.
- **UpdateXpress ne parvient pas à définir le pilote prêt à l'emploi comme pilote par défaut sur certains appareils lors du passage d'un pilote fourni à un pilote non fourni.**

  UpdateXpress appelle OneCLI pour effectuer une tâche de mise à jour. OneCLI n'a pas pu compare les versions incohérentes du pilote fourni et du pilote non fourni, puis sélectionner la version correcte pour la mise à jour. Dans ce cas, UpdateXpress n'a pas pu sélectionner le pilote non fourni pour la mise à jour, et les utilisateurs doivent sélectionner manuellement le pilote cible non fourni pour remplacer le pilote fourni.
- **Tous les chemins UpdateXpress doivent utiliser des caractères alphanumériques anglais standard.**

  Tous les chemins de UpdateXpress doivent utiliser des caractères alphanumériques anglais standard et ne doivent pas contenir d'espaces, de caractères spéciaux ou des caractères non anglais.

Solutions

Il n'y a actuellement aucun problème ou solution de contournement connus pour l'application UpdateXpress.

Coexistence et compatibilité

L'application UpdateXpress repose sur OneCLI, mais elle n'a aucune interaction avec d'autres programmes du système. N'exécutez pas l'application UpdateXpress et OneCLI en même temps.

Annexe A. Fonctions d'accessibilité pour UpdateXpress

Les fonctions d'accessibilité permettent aux utilisateurs souffrant d'un handicap, telles qu'une vision ou une mobilité réduite, d'utiliser avec succès des logiciels.

La liste suivante inclut les principales fonctions d'accessibilité de l'application UpdateXpress :
- Utilisation du clavier uniquement
- Interfaces généralement utilisées par les lecteurs d'écran

Navigation au clavier

Les utilisateurs peuvent utiliser le clavier pour naviguer au sein de l'interface graphique utilisateur (GUI).

Les raccourcis clavier suivants s'appliquent sur les systèmes d'exploitation Windows et Linux.

Raccourci	Fonction
Tab	Passer au contrôle suivant.
Maj+Tab	Passer au contrôle précédent.
Flèche gauche	Revenir en arrière d'un caractère.
Flèche droite	Avancer d'un caractère.
Retour arrière	Supprimer le caractère à gauche du curseur.
Suppr	Supprimer le caractère sous le curseur.
Flèche haut	Déplacer le curseur et la sélection vers le haut à l'aide du bouton d'option.
Flèche bas	Déplacer le curseur et la sélection vers le bas à l'aide du bouton d'option.
Espace	Sélectionner ou désélectionner une option.

Technologie de lecteur d'écran

Les technologies de lecteur d'écran sont essentiellement axées sur les interfaces de programme logicielles, les systèmes d'information d'aide et différents documents en ligne. Pour plus d'informations sur les lecteurs d'écran, consultez le site suivant :
- Utilisation du lecteur d'écran JAWS :

  http://www.freedomscientific.com/Products/Blindness/JAWS
- Utilisation du lecteur d'écran NVDA :

  http://www.nvaccess.org/

Accessibilité et Lenovo

Pour plus d'informations sur l'engagement de Lenovo en matière d'accessibilité, accédez à http://www.lenovo.com/lenovo/us/en/accessibility.html.

Annexe B. Consignes

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services Lenovo non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial Lenovo.

Toute référence à un produit, logiciel ou service Lenovo n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit de Lenovo. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par Lenovo.

Lenovo peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

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

LE PRÉSENT DOCUMENT EST LIVRÉ « EN L'ÉTAT ». LENOVO DÉCLINE TOUTE RESPONSABILITÉ, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFAÇON ET D'APTITUDE A L'EXÉCUTION D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Lenovo peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être implantés ou utilisés dans un environnement où un dysfonctionnement pourrait entraîner des dommages corporels ou le décès de personnes. Les informations contenues dans ce document n'affectent ni ne modifient les garanties ou les spécifications des produits Lenovo. Rien dans ce document ne doit être considéré comme une licence ou une garantie explicite ou implicite en matière de droits de propriété intellectuelle de Lenovo ou de tiers. Toutes les informations contenues dans ce document ont été obtenues dans des environnements spécifiques et sont présentées en tant qu'illustration. Les résultats peuvent varier selon l'environnement d'exploitation utilisé.

Lenovo pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les références à des sites Web non Lenovo sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit Lenovo et l'utilisation de ces sites relève de votre seule responsabilité.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas

garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Marques

LENOVO, FLEX SYSTEM, SYSTEM X et NEXTSCALE SYSTEM sont des marques de Lenovo. Intel et Intel Xeon sont des marques d'Intel Corporation aux États-Unis et/ou dans certains autres pays. Internet Explorer, Microsoft et Windows sont des marques du groupe Microsoft. Linux est une marque de Linus Torvalds. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

Remarques importantes

La vitesse du processeur correspond à la vitesse de l'horloge interne du microprocesseur. D'autres facteurs peuvent également influer sur les performances d'une application.

Lorsqu'il est fait référence à la mémoire principale, à la mémoire réelle et virtuelle ou au volume des voies de transmission, 1 ko correspond à 1024 octets, 1 Mo correspond à 1 048 576 octets et 1 Go correspond à 1 073 741 824 octets.

Lorsqu'il est fait référence à la capacité de l'unité de disque dur ou au volume de communications, 1 Mo correspond à un million d'octets et 1 Go correspond à un milliard d'octets. La capacité totale à laquelle l'utilisateur a accès peut varier en fonction de l'environnement d'exploitation.

Lenovo ne prend aucun engagement et n'accorde aucune garantie concernant les produits non Lenovo. Seuls les tiers sont chargés d'assurer directement le support des produits non Lenovo.

Les applications fournies avec les produits Lenovo peuvent être différentes des versions mises à la vente et ne pas être fournies avec la documentation complète ou toutes les fonctions.

Index