Lenovo

Guide d'utilisation
Lenovo XClarity Essentials UpdateXpress

Version 5.2.0

Remarque

Avant d'utiliser cette documentation et les produits associés, prenez connaissance des informations figurant à la section Annexe B « Consignes » à la page 49.

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-huitième édition (Mai 2025)

© Copyright Lenovo 2017, 2025.
REMARQUE SUR LES DROITS LIMITÉS ET RESTREINTS : Si les données ou les logiciels sont fournis conformément à un contrat GSA (General Services Administration), l’utilisation, la reproduction et la divulgation sont soumises aux restrictions stipulées dans le contrat n° GS-35F-05925.

Table des matières

Table des matières i

Tableaux iii

À propos de ce guide v

À qui s'adresse ce guide ? v

Conventions et terminologies v

Sites Web pris en charge v

Chapitre 1. Présentation technique . . . 1

UpdateXpress System Pack (UXSP) 1

Application des mises à jour UXSP avec l'application UpdateXpress 2

Traitement d'un module UXSP en tant que paquet 2

Traitement des mises à jour requises 2

Mises à jour indépendantes du système d'exploitation. 3

Données d'inventaire manquantes ou incomplètes 4

Installation des pilotes de périphérique nécessaires 4

Chapitre 2. Configurations matérielle et logicielle requises 5

Modèles de serveur pris en charge 5

Systèmes d'exploitation pris en charge 7

Windows 7

Linux 7

Privilèges du système d'exploitation 8

Chapitre 3. Utilisation de l'application UpdateXpress 9

Lancement de l'application UpdateXpress 9

Mise à jour des serveurs 10

Mise à jour d'un serveur local à partir du site Web 10

Mise à jour d'un serveur local depuis un répertoire local 11

Mise à jour d'un serveur distant à partir du site Web 12

Mise à jour d'un serveur distant à partir d'un répertoire local 15

Mise à jour de plusieurs serveurs distants depuis le site Web 16

Mise à jour de plusieurs serveurs distants depuis un répertoire local 19

Gestion du serveur sous connexion Ethernet directe 21

Exécution d'une mise à jour transférée pour un serveur distant 22

Création d'un référentiel de mises à jour . . . 24

Configuration du BIOS 26

Configuration du BIOS pour un serveur distant 26

Configuration du BIOS pour plusieurs serveurs distants 27

Configuration de la grappe RAID pour un serveur distant 29

Configuration du BMC 30

Configuration du BMC pour un serveur distant 30

Configuration du BMC pour plusieurs serveurs distants 31

Collecte des journaux 32

Collecte de journaux pour un serveur distant 32

Collecte de journaux pour plusieurs serveurs distants 33

Gestion de la configuration système 34

Sauvegarde de la configuration système . . . 34

Restauration de la configuration système . . . 35

Fonctionnalités de sécurité du serveur ThinkEdge 36

Demande du serveur sur le portail ThinkShield. 36

Configuration des capteurs de sécurité 38

Gestion de la clé d'authentification SED . . . 39

Mise à niveau du mode de contrôle de verrouillage. 40

Activation du serveur en mode de verrouillage. 41

Mise à jour de la clé publique sur les serveurs ThinkEdge 43

Chapitre 4. Dépannage 45

Annexe A. Fonctions d'accessibilité pour UpdateXpress 47

Annexe B. Consignes 49

Marques 50

Remarques importantes 50

Index 51

© Copyright Lenovo 2017, 2025

Tableaux

1. Systèmes Lenovo pris en charge 6
2. Systèmes d’exploitation Windows pris en charge 7
3. Systèmes d’exploitation Linux pris en charge 8

© Copyright Lenovo 2017, 2025

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 ou à d'autres personnes responsables de l'administration système qui connaissent bien la maintenance du microprogramme et des pilotes de périphérique.

Conventions et terminologies

Les paragraphes qui commencent par la mention Remarque, Important ou Attention en gras présentent certaines informations spécifiques qui visent à mettre en évidence des détails importants :

Remarque : Ces consignes fournissent des astuces, des orientations ou des conseils importants.

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

Attention : Ces consignes indiquent que des programmes, des périphériques ou des données peuvent être endommagés. Une consigne visant à attirer l'attention est présentée avant l'instruction ou la situation au cours de laquelle des dommages peuvent survenir.

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

  Utilisez ce site Web afin de télécharger plusieurs outils de gestion du système pour les serveurs ThinkSystem et System x.
- Lenovo XClarity Essentials UpdateXpress

  Utilisez ce site Web pour télécharger l'application UpdateXpress.

Les sites Web suivants fournissent des informations sur la compatibilité et l'assistance des produits, les garanties et les licences, ainsi que diverses ressources techniques.
- Services et produits du support Lenovo Flex System
- Site Web ServerProven
- Bibliothèque de ressources serveur, réseau et stockage Lenovo

© Copyright Lenovo 2017, 2025

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 UXSP contiennent des mises à jour du microprogramme et des pilotes de périphérique.

La section ci-après présente brièvement les quatre fonctions principales 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 localMettre à jour le serveur local
Mettez à jour la machine locale qui exécute actuellement l'application UpdateXpress. Le type de machine est détecté, les mises à jour sont acquises et appliquées automatiquement.

Mise à jour d'un serveur distant
Mettez à jour la machine distante à l'aide du contrôleur de gestion de la carte mère (BMC) en cours d'exécution 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 machines pour lesquelles les mises à jour sont acquises à partir du site Web du 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 du support Lenovo.

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

UpdateXpress System Pack (UXSP)

Un UXSP est un ensemble de mises à jour en ligne destinées au microprogramme et aux pilotes, testées pour les serveurs System x et ThinkSystem. Les UXSP sont publiés semestriellement pendant les trois premières années et annuellement pendant les trois dernières années de support.

Les UXSP simplifient le processus de téléchargement et d'installation de toutes les mises à jour des pilotes et du 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 de type de machine et de système d'exploitation. Des UXSP distincts sont fournis pour les systèmes d'exploitation Windows® et toutes les distributions Linux. Par exemple, il peut y avoir plusieurs UXSP pour un type de machine particulier. En outre, il peut y avoir une mise à jour pour le système d'exploitation Windows et pour chaque distribution Linux.

Enfin, il existe une plateforme UXSP qui peut être utilisée afin de mettre à jour un système en mode hors bande. La plateforme UXSP ne contient pas de système d'exploitation.

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

© Copyright Lenovo 2017, 2025

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 réalise un inventaire sur l'ordinateur qui bénéficiera de l'application de la mise à jour, interroge un emplacement spécifié en vue d'obtenir une liste des modules de mise à jour applicables, compare l'inventaire à la liste de mise à jour applicable, recommande un ensemble de mises à jour à appliquer, puis les déploie pour mettre à jour la machine.

Procédez comme suit pour appliquer des UXSP par le biais de l'application UpdateXpress :

1. Téléchargez l'application UpdateXpress à partir du site Web du support Lenovo.
2. Exécutez l'application UpdateXpress. Sélectionnez **Mettre à jour l'ordinateur local** ou **Mettre à jour un ordinateur distant**.
3. Sélectionnez **Consultation du site Web du support Lenovo**.
4. Sélectionnez **System Packs de l'application UpdateXpress (UXSP)**.

Les utilisateurs peuvent aussi télécharger les mises à jour directement depuis le site Web du support Lenovo. N'oubliez pas de télécharger la charge utile de mise à jour, ainsi que le fichier XML. Pour plus de commodité, 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 modules du système. Les fichiers communs qui se trouvent déjà dans le dossier ne seront pas téléchargés à nouveau. Par conséquent, le temps de téléchargement global est réduit.

Traitement d'un module UXSP en tant que paquet

L'application UpdateXpress a été conçue pour télécharger et appliquer des UXSP. L'UXSP est un ensemble de mises à jour individuelles telles que spécifiées 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

La présente rubrique décrit la manière dont les conditions d'une mise à jour sont acquises et appliquées.

Afin d'appliquer correctement les mises à jour, toutes les conditions préalables et les co-conditions en vue d'une mise à jour doivent être acquises et appliquées. L'application UpdateXpress vérifie, acquiert et applique automatiquement les conditions préalables et les co-conditions. Les mises à jour exigent souvent l'application préalable de fichiers 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 incluses 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 mise à jour et les évalue afin de déterminer si les conditions préalables sont remplies. Si nécessaire, elle applique également et automatiquement les fichiers prérequis avant d'appliquer la mise à jour concernée. Les utilisateurs peuvent choisir de ne pas appliquer les fichiers prérequis. Toutefois, cela pourrait empêcher l'application de la mise à jour.

Si les modules prérequis présentent des conditions préalables ou des co-conditions, l'acquisition, l'évaluation et l'application sont effectuées 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 présentent des conditions préalables ou des co-conditions, l'acquisition, l'évaluation et l'application sont effectuées de la même manière.

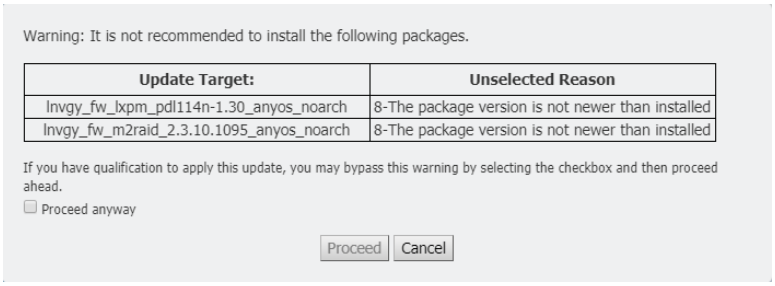
Exemple

Prenons l'exemple d'une mise à jour qui comporte à la fois des conditions préalables et des co-conditions. Par défaut, l'application UpdateXpress procède de la sorte :

1. Afin de s'assurer que la mise à jour peut être réalisée, l'application UpdateXpress commence par la télécharger.
2. Les fichiers prérequis sont téléchargés.
3. Les fichiers corequis sont téléchargés.
4. Les fichiers prérequis ou corequis sont évalués 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 mise à jour

Par défaut, l'application UpdateXpress sélectionne les modules 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 s'appliquent à 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 du microprogramme ou du pilote. Dans ce cas, l’application UpdateXpress affiche la version du module de mise à jour, et non la version du composant. Si la version du composant n’est pas détectée, alors par défaut, la mise à jour n’est pas sélectionnée. Dans ce cas, sélectionnez manuellement le module comme mise à jour recommandée.

Installation des pilotes de périphérique nécessaires

L’application UpdateXpress installe les pilotes de périphérique requis.

L’application UpdateXpress installe chaque pilote dans l’UXSP dans les cas suivants :
- Le pilote de périphérique actuel est antérieur au pilote de périphérique disponible dans l’UXSP.
- L’application UpdateXpress n’est pas en mesure de déterminer la version actuelle du pilote de périphérique. En général, cela se produit lorsqu’aucun pilote de périphérique n’est installé.

  Remarque : L’application UpdateXpress affiche le message `Non détecté` lorsqu’il est impossible de détecter la version du pilote de périphérique installé.

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)
- Couche de mappage IPMI

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 qui exécutent l'application UpdateXpress nécessitent au moins 1 Go de RAM.

Modèles de serveur pris en charge

L'application UpdateXpress prend en charge les pilotes de périphérique Windows et Linux, ainsi que le microprogramme inclus dans les UXSP disponibles. Une liste des composants, des pilotes de périphérique et du microprogramme actuellement pris en charge se trouve dans le fichier Lisez-moi de l'application UpdateXpress inclus dans chaque module du système.

© Copyright Lenovo 2017, 2025

Tableau 1. Systèmes Lenovo pris en charge

Série	Modèles de serveur	
ThinkEdge	• Nœud SE100 (7DGR) • SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
ThinkSystem	• Passerelle DX1100U (7D49) • Performance/Capacité DX1100U (7D4A) • Stockage DXN2000 (7D5W) • SC750 V4 (7DDJ) • SD530 (7X21) • SD530 V3 (7DD3, 7DDA) • SD535 V3 (7DD1,7DD8) • 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) • SR630 V4 (7DG8, 7DG9, 7DGA, 7DGB, 7DK1, 7DLM) • 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) • SR650 V4 (7DGC, 7DGD, 7DGE, 7DGF, 7DK2, 7DLN) • 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) • SR680a V3 (7DHE) • SR685a V3 (7DHC) • SR780a V3 (7DJ4) • 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) • ST50 V3 (7DF3, 7DF4) • ST58 V3 (7DF5) • 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)[3] • SE550 V2 (7D68)[3] • SR588/SR590 (7D4M) • SR588 V2/SR590 V2 (7D53)[3]	• SR660 V2/SR668 V2(7D6L)[3] • SR860P (7D5D) • Dispositif WH5900 (7D5V)
WenTian	• WA5480 G3/WA5488 G3 (7DE7)[3] • WA5480 G5/WA5488 G5 (7DHQ)[3] • WR3220 G2/WR3228 G2 (7DEC)[3]	• WR5220 G3/WR5228 G3 (7D8Y)[3] • WR5220 G5/WR5228 G5 (7DFX)[3] • WR5225 G3 (7DG2)[3]
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, 7DGP, 7DGG, 7DKB, 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)

Tableau 1. Systèmes Lenovo pris en charge (suite)

Série	Modèles de serveur	
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. 3. Ce modèle de serveur prend en charge la fonctionnalité de gestion multiple.		

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 pris en charge par l’application UpdateXpress.

Tableau 2. Systèmes d’exploitation Windows pris en charge

Système d'exploitation	Mise à jour locale	Mise à jour à distance	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
Microsoft Windows Server 2025	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 fonctionnalité de mise à jour locale.

Linux

L’application UpdateXpress est prise en charge sur les versions suivantes des systèmes d’exploitation Linux.

Tableau 3. Systèmes d'exploitation Linux pris en charge

Système d'exploitation	Mise à jour locale	Mise à jour à distance	Référentiel local	Configuration RAID à distance
Red Hat Enterprise Linux 8.x (jusqu'à U10)	Oui	Oui	Oui	Oui
Red Hat Enterprise Linux 9.x (jusqu'à U5)	Oui	Oui	Oui	Oui
SUSE Linux Enterprise Server 15.x (jusqu'à SP6)	Oui	Oui	Oui	Oui

Remarques :

- 500 Mo d'espace libre sont recommandés lors de l'exécution de l'application UpdateXpress sur un système d'exploitation Linux.
- L'application UpdateXpress prend en charge la vérification approximative du système d'exploitation. Si le système d'exploitation actuel ne prend pas en charge les modules de microprogramme dans un UXSP, les modules de microprogramme peuvent également être répertoriés dans le résultat de comparaison de l'application UpdateXpress.
- En fonction de la commande `ifconfig` sous Linux OS, il est possible qu'UpdateXpress ne soit pas installé sur RHEL 7.0 ou des versions ultérieures. Pour mettre à jour le microprogramme vers RHEL 7.0 ou des versions ultérieures, les utilisateurs doivent installer net-tools.
- Les mises à jour des pilotes 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 4.4.1 à la place :
  - RedHat 7.6/7.7/7.8/7.9
- 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

Cette section décrit les privilèges de connexion aux systèmes d'exploitation Windows et Linux. L'application UpdateXpress renverra un message d'erreur en cas d'utilisation d'un privilège insuffisant. Avant de commencer, stockez l'application UpdateXpress, y compris ses extractions, ainsi que les journaux sensibles, dans un emplacement sûr auquel seuls les utilisateurs autorisés ont accès.

- Pour le système d'exploitation Windows, le privilège d'administrateur ou équivalent à un administrateur est requis.
- Pour le système d'exploitation Linux, le compte racine est requis.

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 de 1 024 x 768 ou plus 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 nommée comme suit :

```
lnvgy_utl_lxce_ux{ build id }_{ version }_windows_indiv.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_indiv.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 nommée 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 }_{ version }_linux_indiv.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T et versions ultérieures	`lnvgy_utl_lxce_ux{ build id }_{ version }_linux_indiv.tgz`

Le nom de l'application UpdateXpress est différent pour les systèmes d'exploitation Windows et Linux. Pour des raisons de commodité, <*Zipfile*> est utilisé ci-après dans le présent document afin de désigner le nom de l'application UpdateXpress dans les systèmes d'exploitation Windows et Linux.

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. Procédez à l'extraction de <*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 dans le terminal :

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

© Copyright Lenovo 2017, 2025

Mise à jour des serveurs

Mise à jour d'un serveur local à partir du site Web

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

Condition préalable :
- L'application UpdateXpress est en cours d'exécution 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 7.

Pour mettre à jour une machine locale à partir du site Web, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur local**. Si **Saisir les informations d'accès au BMC** est sélectionné, saisissez les informations du BMC dans cette fenêtre et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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**.

Etape 6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web du support Lenovo** et cliquez sur **Suivant**.

Etape 7. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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**.

Etape 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** :
  1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

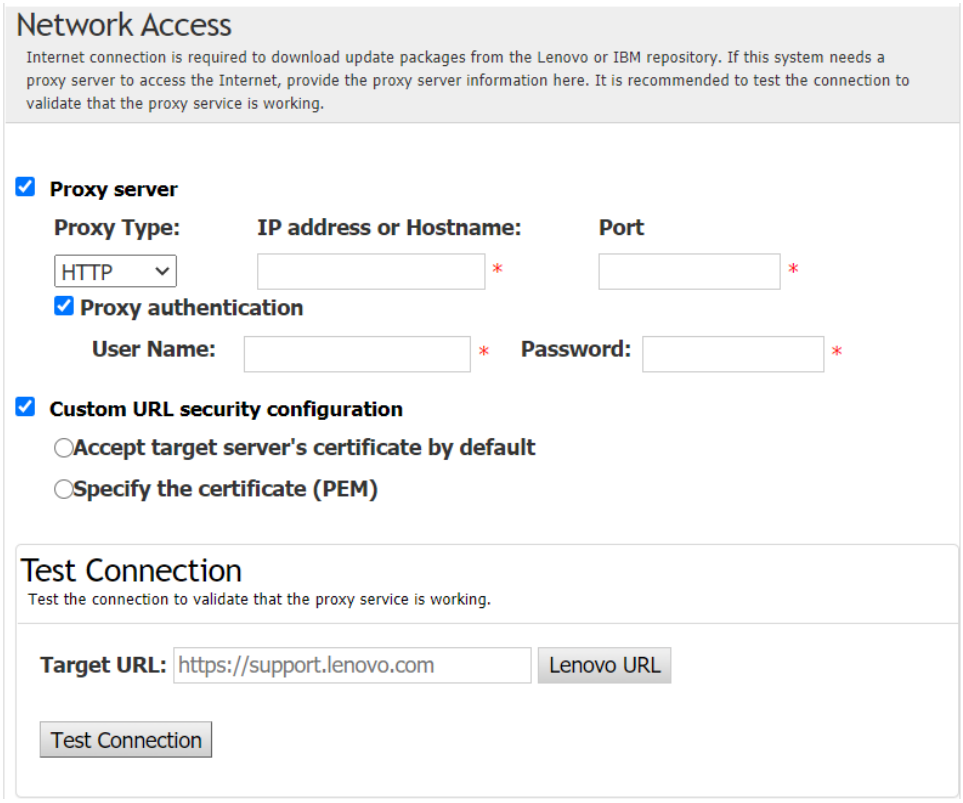
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

  2. 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)**



Etape 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**.

Etape 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 progression terminée, cliquez sur **Suivant**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 13. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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

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

Condition préalable :
- L'application UpdateXpress est en cours d'exécution 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 7.
- 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 à partir d'un répertoire local, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Server cible, sélectionnez **Gérer le serveur local** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Paramètres de mise à jour, effectuez une ou plusieurs des actions suivantes :
- Pour mettre à jour l'image de sauvegarde du BMC ou de l'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**.

Etape 6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour spécifier un dossier local, effectuez l'une des opérations suivantes :
- Cliquez sur **Parcourir**, sélectionnez le dossier cible, puis cliquez sur **Suivant**.
- Saisissez le chemin d'accès au dossier dans le champ à côté du bouton **Parcourir**, puis cliquez sur **Suivant**.

Etape 7. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 8. Dans la fenêtre Recommandation de mise à jour, effectuez l'une des actions suivantes :
- Pour afficher tous les modules de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté**.
- Cliquez sur **Commencer** pour comparer les versions installées du pilote de périphérique et du microprogramme avec les dernières versions. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.
- Sélectionnez **Comparer uniquement les périphériques installés** et cliquez sur **Commencer** pour comparer la version des périphériques installés dans le système local avec la dernière version. Une fois la progression terminée, sélectionnez un ou plusieurs modules cibles, puis cliquez sur **Suivant**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 10. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Mise à jour d'un serveur distant à partir du site Web

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

Condition préalable :

L'application UpdateXpress est en cours d'exécution sur une machine équipée d'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 7.

Pour mettre à jour une machine distante à partir du site Web, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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 copiés 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.

Etape 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**.

Etape 7. Effectuez une ou plusieurs des opérations suivantes :
- Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur**, puis 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)**, puis cliquez sur **Suivant**.

Etape 8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web du support Lenovo** et cliquez sur **Suivant**.

Etape 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**.

Etape 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**
  1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

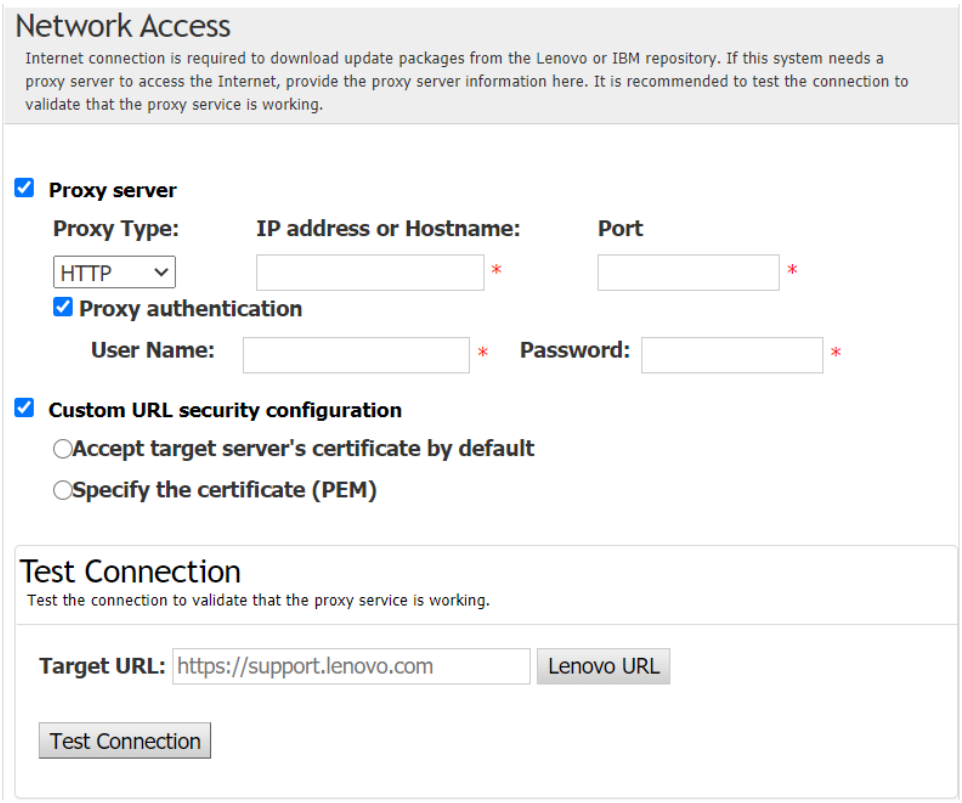
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

  2. 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)**



Etape 11. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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**.

Etape 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 progression terminée, cliquez sur **Suivant**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 15. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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

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

Condition préalable :

L'application UpdateXpress est en cours d'exécution sur une machine équipée d'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 7.

Pour mettre à jour une machine distante à partir d'un répertoire local, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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 copiés 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.

Etape 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**.

Etape 7. Effectuez une ou plusieurs des opérations suivantes :
- Pour rétrograder le microprogramme, sélectionnez **Activer la mise à jour sur un microprogramme de niveau antérieur**, puis 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)**, puis cliquez sur **Suivant**.

Etape 8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour spécifier un dossier local, effectuez l'une des opérations suivantes :
- Cliquez sur **Parcourir**, sélectionnez le dossier souhaité et cliquez sur **Suivant**.
- Saisissez le chemin d'accès au dossier dans le champ à côté du bouton **Parcourir**, puis cliquez sur **Suivant**.

Etape 9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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 modules de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 12. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 à partir du 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 en savoir plus sur les serveurs pris en charge, consultez la section **ThinkServer et série WenTian** dans « Modèles de serveur pris en charge » à la page 5.

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

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Gestion de plusieurs serveurs, effectuez une ou plusieurs des opérations suivantes :

- Pour ajouter de nouveaux serveurs dans le pool de serveurs, sélectionnez **+ Ajouter de nouveaux serveurs**. Dans la fenêtre Ajouter de nouveaux serveurs, effectuez l'une des actions suivantes :
  - Sélectionnez **Plage d'adresses IP**, saisissez la plage d'adresses IP et cliquez sur **Détecter**.
  - Sélectionnez **Détecter par SSDP**, sélectionnez l'adaptateur cible et cliquez sur **Détecter**.
- Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Action → Supprimer la sélection**.
- 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 **Action → Analyser la sélection**.
- Pour exporter la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cibles, puis cliquez sur **Action → Exporter**.

  Remarque : Par défaut, la liste du pool de serveurs est enregistrée dans le fichier JSON. Les utilisateurs peuvent également sélectionner les formats CSV et XLS.
- Pour importer la liste du pool de serveurs sur un autre serveur, sélectionnez un ou plusieurs serveurs cibles dans la liste, cliquez sur **Action → Importer**, puis sélectionnez le fichier JSON cible.
- Pour modifier le mot de passe du serveur, sélectionnez un ou plusieurs serveurs cibles, cliquez sur **Action → Modifier l'adresse IP et le mot de passe**. Sur la page Modifier l'adresse IP et le mot de passe, effectuez l'une des opérations suivantes :
  - Pour modifier le mot de passe d'un seul serveur, saisissez le nouveau nom d'utilisateur et le nouveau mot de passe, puis cliquez sur **Exécuter**. Le nouveau nom d'utilisateur et le nouveau mot de passe seront automatiquement ajoutés à la liste déroulante.
  - Pour modifier le mot de passe de plusieurs serveurs, cliquez sur **Exporter**, modifiez le mot de passe dans le fichier CSV exporté, puis enregistrez le fichier. Revenez à la page Modifier l'adresse IP et le mot de passe, cliquez sur **Importer** pour ajouter le fichier CSV, puis cliquez sur **Exécuter**.
  - Pour afficher les détails de chaque serveur, cliquez sur ⌄ du serveur cible.

  Remarque : Le rôle d'utilisateur d'**USERID** est **Administrateur**, ce qui ne peut pas être modifié.
- Pour utiliser les informations d'identification BMC communes pour la gestion, sélectionnez **Saisir les informations d'identification BMC communes -**, saisissez le nom d'utilisateur et le mot de passe.

Etape 5. Revenez à la fenêtre Gestion de plusieurs serveurs, cliquez sur **Suivant**, un message s'affiche pour rappeler aux utilisateurs de confirmer si 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.

Etape 6. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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 copiés les modules de mise à jour.

  Remarque : Entrez un chemin d'accès complet sur le serveur HTTPS/FTP. Le serveur FTP est uniquement utilisé pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.

Etape 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**.

Etape 9. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web du support Lenovo** et cliquez sur **Suivant**.

Etape 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**.

Etape 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**
  1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

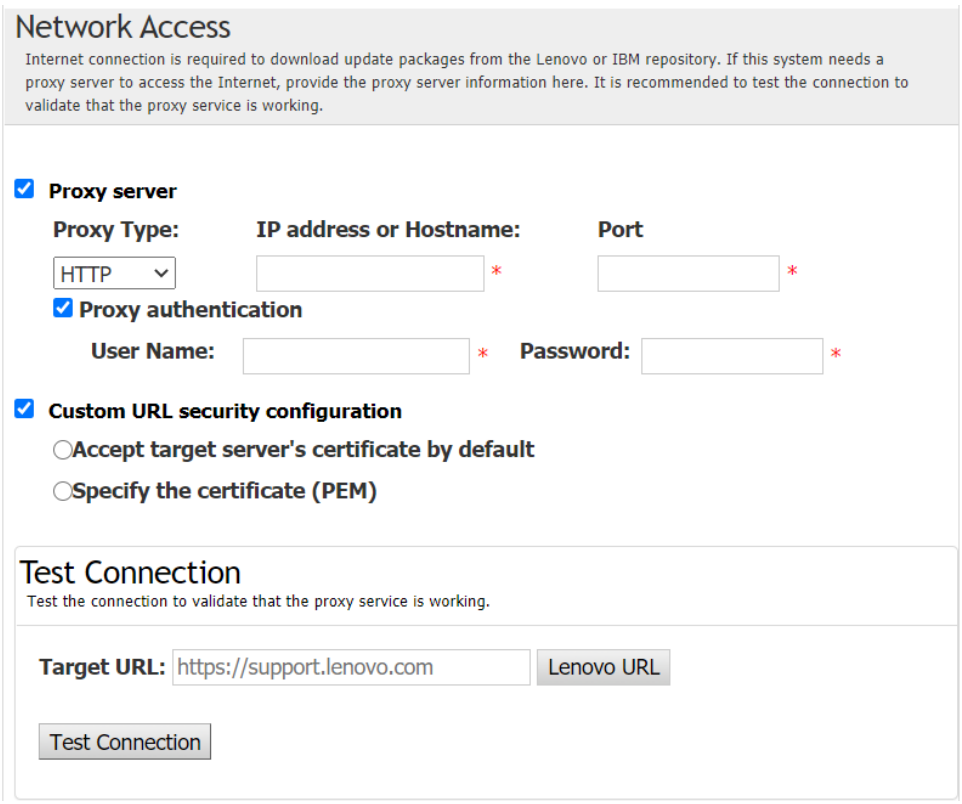
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

  2. 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)**



Etape 12. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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 modules de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.

Etape 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 progression terminée, cliquez sur **Suivant**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 16. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 à partir d'un répertoire local » à la page 15.

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 en savoir plus sur les serveurs pris en charge, consultez la section **ThinkServer et série WenTian** dans « Modèles de serveur pris en charge » à la page 5.

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

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Gestion de plusieurs serveurs, effectuez une ou plusieurs des opérations suivantes :

- Pour ajouter de nouveaux serveurs dans le pool de serveurs, sélectionnez **+ Ajouter de nouveaux serveurs**. Dans la fenêtre Ajouter de nouveaux serveurs, effectuez l'une des actions suivantes :
  - Sélectionnez **Plage d'adresses IP**, saisissez la plage d'adresses IP et cliquez sur **Détecter**.
  - Sélectionnez **Détecter par SSDP**, sélectionnez l'adaptateur cible et cliquez sur **Détecter**.
- Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Action → Supprimer la sélection**.
- 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 **Action → Analyser la sélection**.
- Pour exporter la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cibles, puis cliquez sur **Action → Exporter**.

  Remarque : Par défaut, la liste du pool de serveurs est enregistrée dans le fichier JSON. Les utilisateurs peuvent également sélectionner les formats CSV et XLS.
- Pour importer la liste du pool de serveurs sur un autre serveur, sélectionnez un ou plusieurs serveurs cibles dans la liste, cliquez sur **Action → Importer**, puis sélectionnez le fichier JSON cible.
- Pour modifier le mot de passe du serveur, sélectionnez un ou plusieurs serveurs cibles, cliquez sur **Action → Modifier l'adresse IP et le mot de passe**. Sur la page Modifier l'adresse IP et le mot de passe, effectuez l'une des opérations suivantes :
  - Pour modifier le mot de passe d'un seul serveur, saisissez le nouveau nom d'utilisateur et le nouveau mot de passe, puis cliquez sur **Exécuter**. Le nouveau nom d'utilisateur et le nouveau mot de passe seront automatiquement ajoutés à la liste déroulante.
  - Pour modifier le mot de passe de plusieurs serveurs, cliquez sur **Exporter**, modifiez le mot de passe dans le fichier CSV exporté, puis enregistrez le fichier. Revenez à la page Modifier l'adresse IP et le mot de passe, cliquez sur **Importer** pour ajouter le fichier CSV, puis cliquez sur **Exécuter**.
  - Pour afficher les détails de chaque serveur, cliquez sur ⌄ du serveur cible.

  Remarque : Le rôle d'utilisateur d'**USERID** est **Administrateur**, ce qui ne peut pas être modifié.
- Pour utiliser les informations d'identification BMC communes pour la gestion, sélectionnez **Saisir les informations d'identification BMC communes -**, saisissez le nom d'utilisateur et le mot de passe.

Etape 5. Revenez à la fenêtre Gestion de plusieurs serveurs, cliquez sur **Suivant**, un message s'affiche pour rappeler aux utilisateurs de confirmer si 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.

Etape 6. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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 copiés les modules de mise à jour.

  Remarque : Entrez un chemin d'accès complet sur le serveur HTTPS/FTP. Le serveur FTP est uniquement utilisé pour le serveur ThinkServer marqué d'un 2 en exposant (Remarque 2) dans « Modèles de serveur pris en charge » à la page 5.

Etape 8. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Rechercher dans un répertoire local**. Pour spécifier un dossier local, effectuez l'une des opérations suivantes :
- Cliquez sur **Parcourir**, sélectionnez le dossier souhaité et cliquez sur **Suivant**.
- Saisissez le chemin d'accès au dossier dans le champ à côté du bouton **Parcourir**, puis cliquez sur **Suivant**.

Etape 9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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 modules de mise à jour, sélectionnez **Afficher les mises à jour sans adaptateur détecté** avant de cliquer sur **Commencer**.

Etape 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 niveau des modules. Une fois la progression de la mise à niveau terminée, cliquez sur **Suivant**.

Etape 12. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Connexion Ethernet directe**, entrez les informations suivantes, puis cliquez sur **Suivant**.

Etape 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**.

Etape 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 à partir d'un répertoire local » à la page 15.
- **Gérer la mise à jour transférée**. Pour plus d'informations, voir l'étape 4 et les étapes ultérieures dans « Exécution d'une mise à jour transférée pour un serveur distant » à la page 22.
- **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 29.
- **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 39
  - « Demande du serveur sur le portail ThinkShield » à la page 36
  - « Mise à niveau du mode de contrôle de verrouillage » à la page 40
  - « Activation du serveur en mode de verrouillage » à la page 41
  - « Configuration des capteurs de sécurité » à la page 38

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.

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 7.

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

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Effectuer la mise à jour sur le serveur cible**, puis cliquez sur **Suivant**.

Etape 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 :
  - **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
  - **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
  - **Mot de passe** : mot de passe BMC du système cible.

- **Port** : numéro de port BMC CIM ou RSET. Si les utilisateurs n'entrent aucune valeur, le port par défaut est utilisé.
- **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**.

Etape 6. Dans la fenêtre Emplacement des mises à jour, sélectionnez **Consultation du site Web du support Lenovo** et cliquez sur **Suivant**.

Etape 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**.

Etape 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**

1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

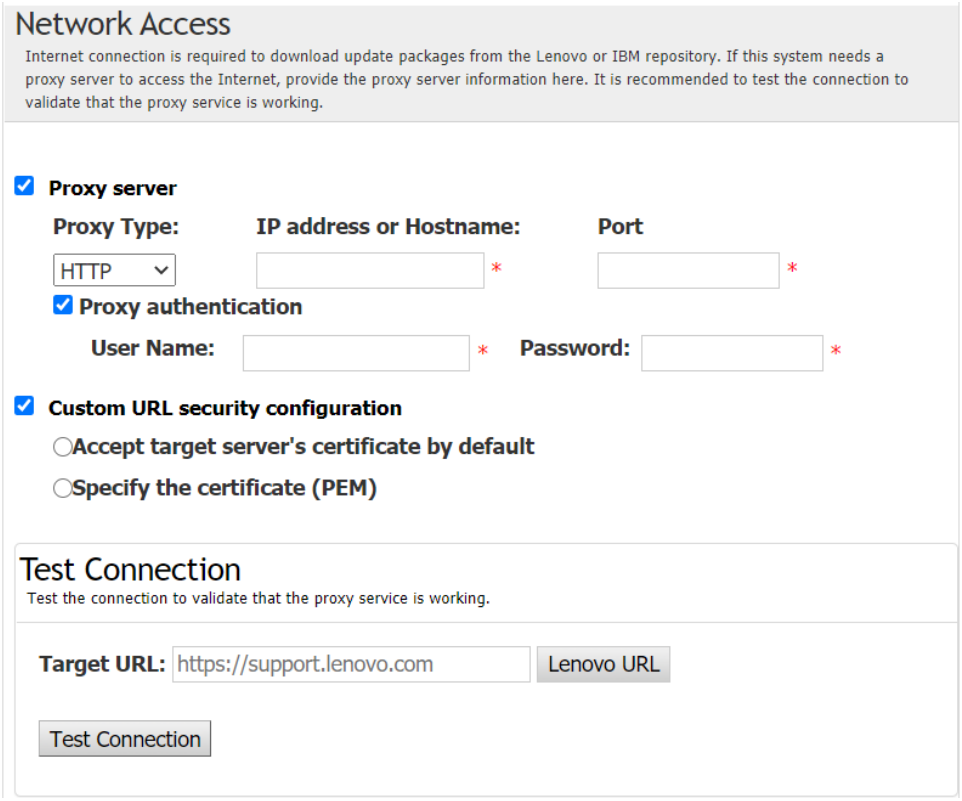
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

2. 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)**



Etape 9. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.

Etape 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**.

Etape 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 progression terminée, cliquez sur **Suivant**.

Etape 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 modules 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 modules à jour lors du prochain redémarrage du système.
- **Immediate** : Mettre immédiatement les modules à jour. Le système peut être redémarré immédiatement.
- **OnStartUpdateRquest** : Mettre les modules à jour en gérant la mise à jour transférée ou en exécutant des commandes OneCLI.

Etape 13. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Création d'un référentiel de mises à jour

L'application UpdateXpress peut créer un référentiel d'UXSP ou de mises à jour individuelles acquises à partir du site Web.

Condition préalable :
- L'application UpdateXpress est en cours d'exécution sur une machine sur laquelle 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 7.

Procédez comme suit pour créer un référentiel mis à jour :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Créer un référentiel de mises à jour** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Type de mise à jour, sélectionnez le type de mise à jour cible et cliquez sur **Suivant**.
- **UpdateXpress System Packs (UXSPs)** : Sélectionnez cette option afin de mettre à jour UXSP. Si cette option est sélectionnée, la fenêtre Mettre à jour la sélection est ignorée, mais tous les modules UXSP sont téléchargés.
- **Dernières mises à jour individuelles disponibles** : Sélectionnez cette option pour mettre à jour des modules individuels. Si cette option est sélectionnée, la fenêtre Mettre à jour la sélection est affichée à l'étape suivante. Les utilisateurs doivent alors désélectionner les modules cibles.
- **Télécharger les modules au format zip** : Sélectionnez cette option afin de télécharger les modules appropriés au format ZIP depuis le site du support Lenovo.

Etape 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**
  1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

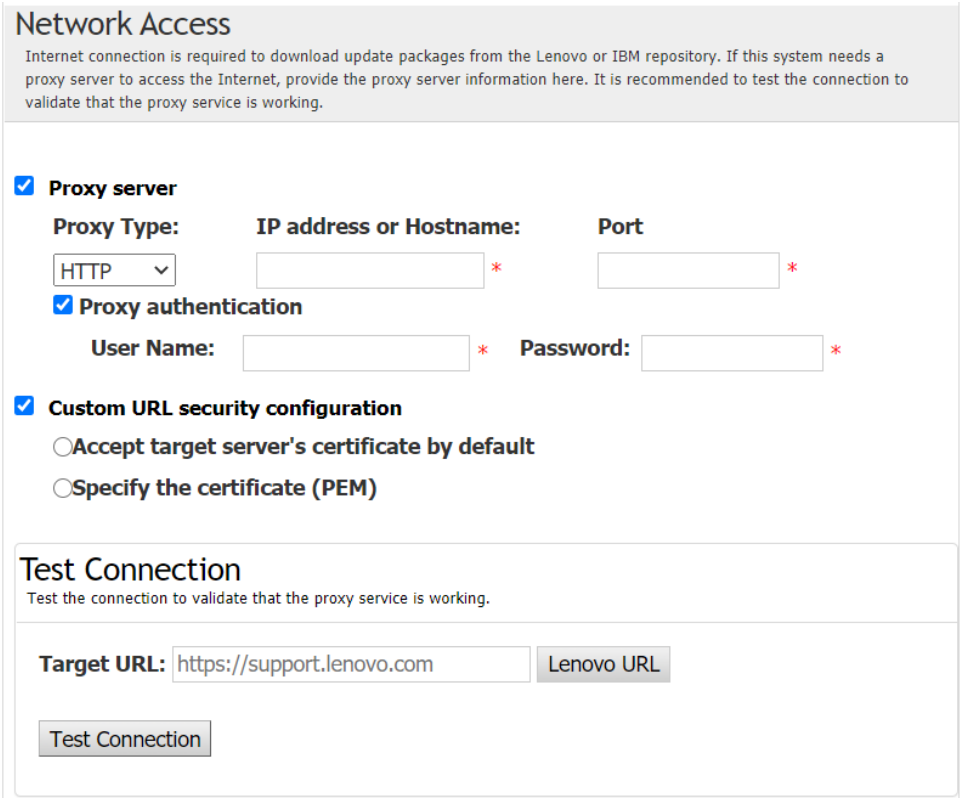
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

  2. 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)**



Etape 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 dans l'en-tête.
- Cliquez sur **Ajouter** et précisez le type de machine afin d'ajouter un type de machine.
- Sélectionnez le type de machine dans la liste et cliquez sur **Supprimer** afin de supprimer un type de machine.
- 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**.

Etape 7. Dans la fenêtre Systèmes d'exploitation, sélectionnez les systèmes d'exploitation cibles, puis cliquez sur **Suivant**.

Etape 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**.

Etape 9. (Facultatif) Sélectionnez **Dernières mises à jour individuelles disponibles**. La fenêtre Mettre à jour la sélection s'affiche alors. Sélectionnez les mises à jour cibles, puis cliquez sur **Suivant**.

Etape 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 progression terminée, cliquez sur **Suivant**.

Etape 11. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Configuration du BIOS

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 7.

Pour configurer le BIOS, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configuration du BIOS**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Mode de configuration, sélectionnez **Configuration du BIOS commune** ou **Importer le fichier de configuration du BIOS**, puis cliquez sur **Suivant**.

Etape 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**.

Etape 7. Dans la fenêtre Vue des modifications du BIOS, vérifiez ou supprimez des valeurs, puis cliquez sur **Suivant**.

Etape 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**.

Etape 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**.

Etape 10. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Configuration du 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 en savoir plus sur les systèmes d'exploitation pris en charge, consultez la section **ThinkServer et série WenTian** dans « Systèmes d'exploitation pris en charge » à la page 7.

Pour configurer le BIOS, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Gestion de plusieurs serveurs, effectuez une ou plusieurs des opérations suivantes :

- Pour ajouter de nouveaux serveurs dans le pool de serveurs, sélectionnez **+ Ajouter de nouveaux serveurs**. Dans la fenêtre Ajouter de nouveaux serveurs, effectuez l'une des actions suivantes :
  - Sélectionnez **Plage d'adresses IP**, saisissez la plage d'adresses IP et cliquez sur **Détecter**.
  - Sélectionnez **Détecter par SSDP**, sélectionnez l'adaptateur cible et cliquez sur **Détecter**.
- Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Action → Supprimer la sélection**.
- 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 **Action → Analyser la sélection**.
- Pour exporter la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cibles, puis cliquez sur **Action → Exporter**.

  Remarque : Par défaut, la liste du pool de serveurs est enregistrée dans le fichier JSON. Les utilisateurs peuvent également sélectionner les formats CSV et XLS.
- Pour importer la liste du pool de serveurs sur un autre serveur, sélectionnez un ou plusieurs serveurs cibles dans la liste, cliquez sur **Action → Importer**, puis sélectionnez le fichier JSON cible.
- Pour modifier le mot de passe du serveur, sélectionnez un ou plusieurs serveurs cibles, cliquez sur **Action → Modifier l'adresse IP et le mot de passe**. Sur la page Modifier l'adresse IP et le mot de passe, effectuez l'une des opérations suivantes :
  - Pour modifier le mot de passe d'un seul serveur, saisissez le nouveau nom d'utilisateur et le nouveau mot de passe, puis cliquez sur **Exécuter**. Le nouveau nom d'utilisateur et le nouveau mot de passe seront automatiquement ajoutés à la liste déroulante.
  - Pour modifier le mot de passe de plusieurs serveurs, cliquez sur **Exporter**, modifiez le mot de passe dans le fichier CSV exporté, puis enregistrez le fichier. Revenez à la page Modifier l'adresse IP et le mot de passe, cliquez sur **Importer** pour ajouter le fichier CSV, puis cliquez sur **Exécuter**.
  - Pour afficher les détails de chaque serveur, cliquez sur ⌄ du serveur cible.

  Remarque : Le rôle d'utilisateur d'**USERID** est **Administrateur**, ce qui ne peut pas être modifié.
- Pour utiliser les informations d'identification BMC communes pour la gestion, sélectionnez **Saisir les informations d'identification BMC communes -**, saisissez le nom d'utilisateur et le mot de passe.

Etape 5. Revenez à la fenêtre Gestion de plusieurs serveurs, cliquez sur **Suivant**, un message s'affiche pour rappeler aux utilisateurs de confirmer si 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.

Etape 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.

Etape 7. Dans la fenêtre Mode de configuration, sélectionnez **Configuration du BIOS commune** ou **Importer le fichier de configuration du BIOS**, puis cliquez sur **Suivant**.

Etape 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**.

Etape 9. Dans la fenêtre Vue des modifications du BIOS, confirmez les paramètres modifiés du BIOS, puis cliquez sur **Suivant**.

Etape 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**.

Etape 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**.

Etape 12. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 7.

Procédez comme suit pour modifierl a grappe RAID :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 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**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 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**.

Etape 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'affichent 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**.

Etape 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.

Etape 7. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Configuration du BMC

Configuration du BMC pour un serveur distant

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

Condition préalable :

La fonction de configuration du BMC pour le serveur distant est uniquement prise en charge par 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 7.

Pour configurer le BMC, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configuration BMC**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Mode de configuration, sélectionnez l'une des options suivantes :
- **Configuration BMC commune → Suivant**
- **Importer le fichier de la configuration BMC → Sélectionner un fichier → Suivant**

Etape 6. Dans la fenêtre Configuration BMC, effectuez l'une des actions suivantes :
- Si vous avez sélectionné **Configuration BMC commune** à l'étape précédente, sélectionnez une ou plusieurs valeurs actuelles, puis cliquez sur **Suivant**.

- Si vous avez sélectionné **Importer le fichier de configuration du BMC** à l'étape précédente, ignorez cette étape.

Etape 7. Dans la fenêtre Vue des modifications du BMC, vérifiez ou supprimez des valeurs, puis cliquez sur **Suivant**.

Etape 8. Dans la fenêtre Exporter la configuration du BMC, exportez la configuration en tant que fichier. Indiquez l'emplacement du fichier exporté, puis cliquez sur **Suivant**.

Etape 9. Dans la fenêtre Exécution de BMC, cliquez sur **Exécuter → Suivant**.

Etape 10. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Configuration du BMC pour plusieurs serveurs distants

L'application UpdateXpress permet de configurer les paramètres BMC pour 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 en savoir plus sur les systèmes d'exploitation pris en charge, consultez la section **ThinkServer et série WenTian** dans « Systèmes d'exploitation pris en charge » à la page 7.

Pour configurer le BMC, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Gestion de plusieurs serveurs, effectuez une ou plusieurs des opérations suivantes :

- Pour ajouter de nouveaux serveurs dans le pool de serveurs, sélectionnez **+ Ajouter de nouveaux serveurs**. Dans la fenêtre Ajouter de nouveaux serveurs, effectuez l'une des actions suivantes :
  - Sélectionnez **Plage d'adresses IP**, saisissez la plage d'adresses IP et cliquez sur **Détecter**.
  - Sélectionnez **Détecter par SSDP**, sélectionnez l'adaptateur cible et cliquez sur **Détecter**.
- Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Action → Supprimer la sélection**.
- 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 **Action → Analyser la sélection**.
- Pour exporter la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cibles, puis cliquez sur **Action → Exporter**.

  Remarque : Par défaut, la liste du pool de serveurs est enregistrée dans le fichier JSON. Les utilisateurs peuvent également sélectionner les formats CSV et XLS.
- Pour importer la liste du pool de serveurs sur un autre serveur, sélectionnez un ou plusieurs serveurs cibles dans la liste, cliquez sur **Action → Importer**, puis sélectionnez le fichier JSON cible.
- Pour modifier le mot de passe du serveur, sélectionnez un ou plusieurs serveurs cibles, cliquez sur **Action → Modifier l'adresse IP et le mot de passe**. Sur la page Modifier l'adresse IP et le mot de passe, effectuez l'une des opérations suivantes :
  - Pour modifier le mot de passe d'un seul serveur, saisissez le nouveau nom d'utilisateur et le nouveau mot de passe, puis cliquez sur **Exécuter**. Le nouveau nom d'utilisateur et le nouveau mot de passe seront automatiquement ajoutés à la liste déroulante.

- Pour modifier le mot de passe de plusieurs serveurs, cliquez sur **Exporter**, modifiez le mot de passe dans le fichier CSV exporté, puis enregistrez le fichier. Revenez à la page Modifier l'adresse IP et le mot de passe, cliquez sur **Importer** pour ajouter le fichier CSV, puis cliquez sur **Exécuter**.
- Pour afficher les détails de chaque serveur, cliquez sur ⌄ du serveur cible.

Remarque : Le rôle d'utilisateur d'**USERID** est **Administrateur**, ce qui ne peut pas être modifié.

- Pour utiliser les informations d'identification BMC communes pour la gestion, sélectionnez **Saisir les informations d'identification BMC communes -**, saisissez le nom d'utilisateur et le mot de passe.

Etape 5. Revenez à la fenêtre Gestion de plusieurs serveurs, cliquez sur **Suivant**, un message s'affiche pour rappeler aux utilisateurs de confirmer si 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.

Etape 6. Dans la fenêtre Tâche, sélectionnez **Configuration BMC**, puis cliquez sur **Suivant**.

Remarque : Cette fonction de configuration du BMC n'est prise en charge que par les serveurs qui disposent des mêmes types de machine.

Etape 7. Dans la fenêtre Mode de configuration, sélectionnez l'une des options suivantes :
- **Configuration BMC commune → Suivant**
- **Importer le fichier de la configuration BMC → Sélectionner un fichier → Suivant**

Etape 8. Dans la fenêtre Configuration BMC, effectuez l'une des actions suivantes :
- Si vous avez sélectionné **Configuration BMC commune** à l'étape précédente, sélectionnez une ou plusieurs valeurs actuelles, puis cliquez sur **Suivant**.
- Si vous avez sélectionné **Importer le fichier de configuration du BMC** à l'étape précédente, ignorez cette étape.

Etape 9. Dans la fenêtre Vue des modifications du BMC, confirmez les paramètres BMC qui ont été modifiés, puis cliquez sur **Suivant**.

Etape 10. Dans la fenêtre Exporter la configuration du BMC, exportez la configuration en tant que fichier. Indiquez l'emplacement du fichier exporté, puis cliquez sur **Suivant**.

Etape 11. Dans la fenêtre Exécution de BMC, cliquez sur **Exécuter → Suivant**.

Etape 12. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Collecte des journaux

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 7.

Pour collecter les journaux, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Collecter le journal**, puis cliquez sur **Suivant**.

Etape 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**.

Etape 6. Dans la fenêtre Résultats de la collecte des journaux, vérifiez les résultats, puis cliquez sur **Suivant**.

Etape 7. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 en savoir plus sur les systèmes d'exploitation pris en charge, consultez la section **ThinkServer et série WenTian** dans « Systèmes d'exploitation pris en charge » à la page 7.

Pour collecter les journaux, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gestion de plusieurs serveurs** et cliquez sur **Suivant**.

Etape 4. Dans la fenêtre Gestion de plusieurs serveurs, effectuez une ou plusieurs des opérations suivantes :
- Pour ajouter de nouveaux serveurs dans le pool de serveurs, sélectionnez **+ Ajouter de nouveaux serveurs**. Dans la fenêtre Ajouter de nouveaux serveurs, effectuez l'une des actions suivantes :
  - Sélectionnez **Plage d'adresses IP**, saisissez la plage d'adresses IP et cliquez sur **Détecter**.
  - Sélectionnez **Détecter par SSDP**, sélectionnez l'adaptateur cible et cliquez sur **Détecter**.
- Pour supprimer le serveur de la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cible, puis cliquez sur **Action → Supprimer la sélection**.
- 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 **Action → Analyser la sélection**.
- Pour exporter la liste du pool de serveurs, sélectionnez un ou plusieurs serveurs cibles, puis cliquez sur **Action → Exporter**.

Remarque : Par défaut, la liste du pool de serveurs est enregistrée dans le fichier JSON. Les utilisateurs peuvent également sélectionner les formats CSV et XLS.

- Pour importer la liste du pool de serveurs sur un autre serveur, sélectionnez un ou plusieurs serveurs cibles dans la liste, cliquez sur **Action → Importer**, puis sélectionnez le fichier JSON cible.
- Pour modifier le mot de passe du serveur, sélectionnez un ou plusieurs serveurs cibles, cliquez sur **Action → Modifier l'adresse IP et le mot de passe**. Sur la page Modifier l'adresse IP et le mot de passe, effectuez l'une des opérations suivantes :
  - Pour modifier le mot de passe d'un seul serveur, saisissez le nouveau nom d'utilisateur et le nouveau mot de passe, puis cliquez sur **Exécuter**. Le nouveau nom d'utilisateur et le nouveau mot de passe seront automatiquement ajoutés à la liste déroulante.
  - Pour modifier le mot de passe de plusieurs serveurs, cliquez sur **Exporter**, modifiez le mot de passe dans le fichier CSV exporté, puis enregistrez le fichier. Revenez à la page Modifier l'adresse IP et le mot de passe, cliquez sur **Importer** pour ajouter le fichier CSV, puis cliquez sur **Exécuter**.
  - Pour afficher les détails de chaque serveur, cliquez sur ⌄ du serveur cible.

  Remarque : Le rôle d'utilisateur d'**USERID** est **Administrateur**, ce qui ne peut pas être modifié.
- Pour utiliser les informations d'identification BMC communes pour la gestion, sélectionnez **Saisir les informations d'identification BMC communes -**, saisissez le nom d'utilisateur et le mot de passe.

Etape 5. Revenez à la fenêtre Gestion de plusieurs serveurs, cliquez sur **Suivant**, un message s'affiche pour rappeler aux utilisateurs de confirmer si 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.

Etape 6. Dans la fenêtre Tâche, sélectionnez **Collecter le journal**, puis cliquez sur **Suivant**.

Etape 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**.

Etape 8. Dans la fenêtre Résultats de la collecte des journaux, vérifiez les résultats, puis cliquez sur **Suivant**.

Etape 9. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Gestion de la configuration système

Sauvegarde de la configuration système

L'application UpdateXpress permet de sauvegarder la configuration du système dans un fichier externe, y compris l'inventaire du matériel et du microprogramme, les données techniques essentielles et la licence FoD.

Condition préalable :

- L'application UpdateXpress est en cours d'exécution 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 7.

Pour sauvegarder la configuration système, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Sauvegarder la configuration système**, puis cliquez sur **Suivant**.

Etape 5. Sur la page Sauvegarder le paramètre de configuration système, procédez comme suit :

a. Cliquez sur **Parcourir** pour sélectionner l'emplacement du fichier de sauvegarde. Les utilisateurs peuvent également utiliser l'emplacement par défaut.

b. Sélectionnez un ou plusieurs éléments de sauvegarde.

Remarque : Si **Configuration du microprogramme dans XCC et UEFI** ou **Clé d'authentification SED** est sélectionnée, saisissez le mot de passe deux fois et conservez le mot de passe en lieu sûr.

c. Cliquez sur **Suivant**, puis attendez quelques minutes en fonction de la configuration du serveur.

d. Une fois le processus terminé, cliquez sur **Suivant**.

Etape 6. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Après avoir terminé

Restaurez la configuration système. Voir « Restauration de la configuration système » à la page 35.

Restauration de la configuration système

L'application UpdateXpress permet de restaurer la configuration système sur les nouveaux serveurs.

Condition préalable :
- L'application UpdateXpress est en cours d'exécution 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 7.
- Sauvegardez la configuration système. Voir « Sauvegarde de la configuration système » à la page 34.

Pour restaurer la configuration système, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.

- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Restaurer la configuration système**, puis cliquez sur **Suivant**.

Etape 5. Sur la page Restaurer le paramètre de configuration système, procédez comme suit :

a. Cliquez sur **Sélectionner un fichier...** pour sélectionner le fichier de sauvegarde. Habituellement, le fichier de sauvegarde se trouve à l'emplacement par défaut.

b. Cliquez sur **Charger le fichier de sauvegarde**, sélectionnez un ou plusieurs éléments cibles.

c. Cliquez sur **Suivant**, puis attendez quelques minutes en fonction de la configuration du serveur.

d. Une fois le processus terminé, cliquez sur **Suivant**.

Etape 6. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Fonctionnalités de sécurité du serveur ThinkEdge

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 7.
- 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 :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Demander le serveur sur le portail ThinkShield** et cliquez sur **Suivant**.

Etape 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.
    1. Sélectionnez **Serveur proxy**, puis remplissez les champs suivants :

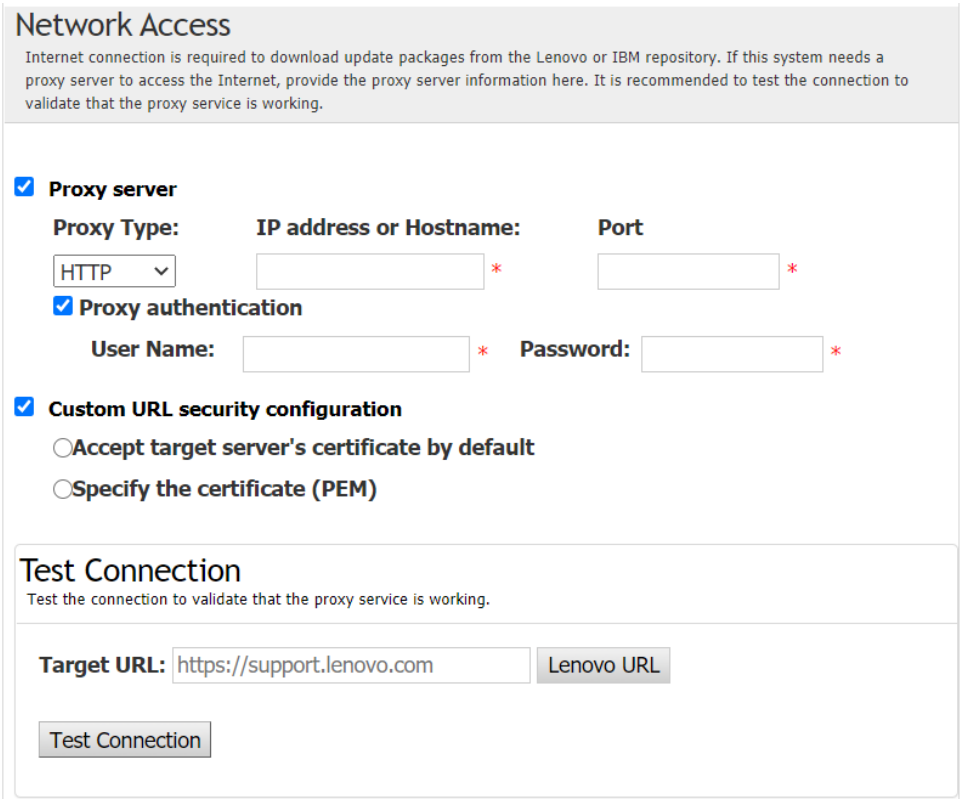
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

    2. 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)



Etape 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**.

Etape 8. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 7.
- 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.

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Configurer les capteurs de sécurité**, puis cliquez sur **Suivant**.

Etape 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.

Etape 7. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 7.
- 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 :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Fonctions de sécurité du serveur ThinkEdge, sélectionnez **Gérer la clé d'authentification SED** et cliquez sur **Suivant**.

Etape 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 passe, puis cliquez sur **Lancer la restauration**.

Etape 7. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 7.
- 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 :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 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 sans revendiquer le serveur dans ThinkShield Key Vault Portal**, puis passez à l'étape 8.

Etape 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.
    1. 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.

2. 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)

Etape 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.

Etape 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**.

Etape 9. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

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 7.
- 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 :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.
- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer les fonctions de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 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.

Etape 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**
  1. Sélectionnez **Serveur proxy** si les utilisateurs ont besoin d'un proxy HTTP/HTTPS pour se connecter au Web, et remplissez les zones suivantes :

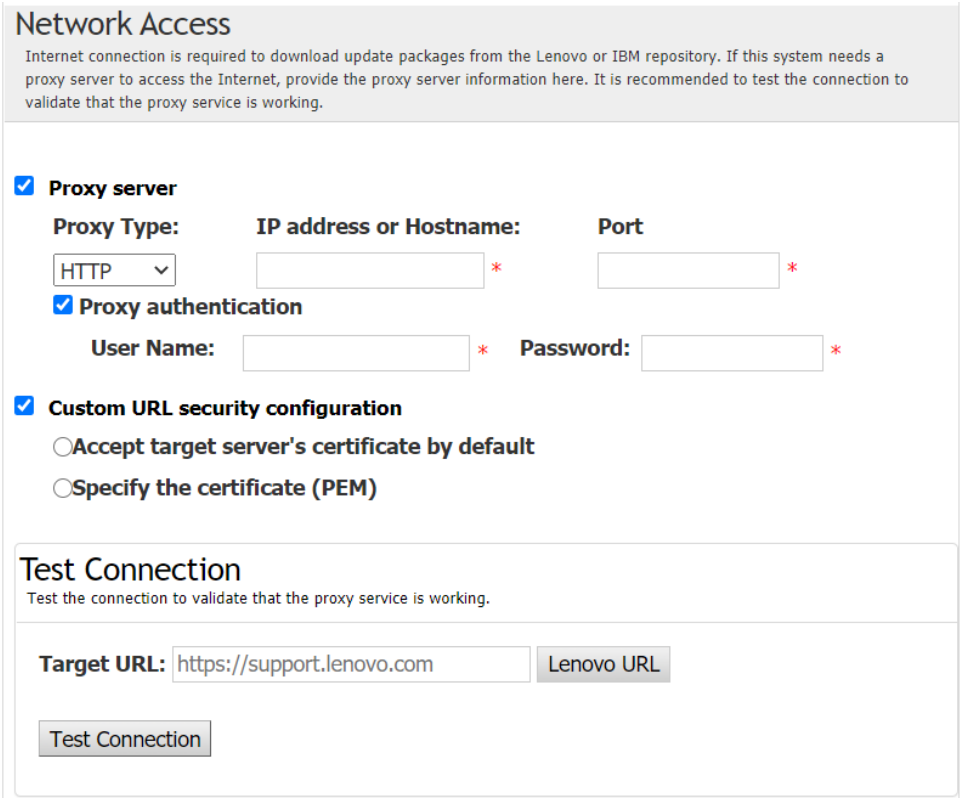
Type de proxy	Le type de proxy du serveur proxy.
Adresse IP ou nom d'hôte	Le nom d'hôte, l'adresse IP ou le nom de domaine du serveur proxy.
Port	Le numéro de port du serveur proxy.

  2. 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)**



Etape 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.

Etape 8. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Mise à jour de la clé publique sur les serveurs ThinkEdge

L'application UpdateXpress permet de mettre à jour la clé publique de la carte mère actuelle sur les serveurs ThinkEdge.

Condition préalable :
- L'application UpdateXpress est en cours d'exécution 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 7.

Pour mettre à jour la clé publique sur les serveurs ThinkEdge, procédez comme suit :

Etape 1. Lancez l'application UpdateXpress. Pour plus d'informations, voir « Lancement de l'application UpdateXpress » à la page 9.

Etape 2. Dans la fenêtre Bienvenue, cliquez sur **Suivant**.

Etape 3. Dans la fenêtre Serveur cible, sélectionnez **Gérer le serveur distant**, entrez les informations suivantes, puis cliquez sur **Suivant**.
- **Adresse IP ou nom d'hôte** : adresse IP ou nom d'hôte BMC du système cible.
- **Nom d'utilisateur** : nom d'utilisateur BMC du système cible.
- **Mot de passe** : mot de passe BMC du système cible.

- **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**.

Etape 4. Dans la fenêtre Tâche, sélectionnez **Configurer une fonctionnalité de sécurité sur le serveur ThinkEdge**, puis cliquez sur **Suivant**.

Etape 5. Dans la fenêtre Fonctionnalité de sécurité du serveur ThinkEdge, lisez les concepts de sécurité ThinkEdge, sélectionnez **J'ai lu et compris ces concepts → Mettre à jour la clé publique du serveur**, puis cliquez sur **Suivant**.

Etape 6. 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 d'autres inquiétudes quant à la sécurité, avant de cliquer sur **Tester la connexion**, sélectionnez **Serveur proxy**, puis sélectionnez **HTTP** dans la liste déroulante **Type de proxy** et renseignez 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.

Etape 7. Dans la fenêtre Mettre à jour de la clé publique du serveur, saisissez les informations suivantes, puis cliquez sur **Mettre à jour**.
- **ID d'organisation** : ID d'organisation des utilisateurs.
- **Nom d'utilisateur** : nom d'utilisateur ThinkShield du système cible.
- **Mot de passe** : mot de passe ThinkShield du système cible.
- **Type de machine** : type de machine du système cible.
- **Numéro de série** : numéro de série du système cible.
- **Code actif (ancien système)** : code actif de l'ancien système.
- **Clé publique (nouveau système)** : clé publique du nouveau système.

Etape 8. Dans la fenêtre Terminer, cliquez sur le journal pour vérifier les mises à jour, puis cliquez sur **Fermer** pour quitter la fenêtre.

Chapitre 4. Dépannage

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

Limites et problèmes

- **Lorsque vous utilisez UpdateXpress afin de configurer les attributs du BIOS CPU*_Disablebitmap* (* signifie l'indice 0, 1 etc) sur des serveurs de la série ThinkSystem WenTian G5, il est possible que le grand nombre entier soit peu précis. Par exemple, il est possible que la valeur 9223372036854775807 s'affiche en tant que 922337036854776000 sur l'interface graphique utilisateur UpdateXpress, ce qui renvoie un échec sur UpdateXpress.**

  Dans ce cas, les utilisateurs peuvent utiliser OneCLI pour configurer les paramètres du BIOS. Par exemple, exécutez la commande `OneCli.exe config set BIOS. CPU1_DisableBitmap 9223372036854775807 --bmc USERNAME:PASSWORD@IPAddress`.
- **Sur la page Gestion de plusieurs serveurs, lorsque l'on clique sur Action → Exporter pour exporter la liste du pool de serveurs, le type de fichier sélectionné (T) n'est pas appliqué à l'extension de nom de fichier (N).**

  Dans ce cas, les utilisateurs doivent saisir manuellement l'extension du nom de fichier.
- **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 comparer 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 d'accès UpdateXpress doivent utiliser des caractères alphanumériques standard de langue anglaise.**

  Tous les chemins d'accès UpdateXpress doivent utiliser des caractères alphanumériques standard en anglais et des caractères spéciaux autorisés par le système d'exploitation. Les caractères non adaptés à la langue anglaise ne sont pas autorisés.

Solutions de contournement

Il n'existe actuellement aucun problème connu ou solution de contournement pour l'application UpdateXpress.

Coexistence et compatibilité

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

© Copyright Lenovo 2017, 2025

Annexe A. Fonctions d'accessibilité pour UpdateXpress

Les fonctionnalités d'accessibilité aident les utilisateurs en situation de handicap, par exemple, une mobilité réduite ou une acuité visuelle limitée, à bien utiliser la technologie, l'informatique et les produits associés.

La liste suivante comprend les principales fonctionnalités d'accessibilité de l'application UpdateXpress :
- Fonctionnement au clavier uniquement
- Interfaces couramment 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 aux systèmes d'exploitation Windows et Linux.

Raccourci	Fonction
Tab	Permet de passer au contrôle suivant.
Maj+Tab	Permet de passer au contrôle précédent.
Flèche vers la gauche	Permet de reculer d'un caractère.
Flèche vers la droite	Permet d'avancer d'un caractère.
Retour arrière	Permet de supprimer le caractère à gauche du curseur.
Suppr	Permet de supprimer le caractère situé sous le curseur.
Flèche vers le haut	Permet de déplacer le curseur et la sélection vers le haut grâce au bouton radio.
Flèche vers le bas	Permet de déplacer le curseur et la sélection vers le bas grâce au bouton radio.
Espace	Permet de sélectionner ou de supprimer une option.

Technologie de lecture d'écran

Les technologies de lecture d'écran sont principalement axées sur les interfaces de logiciels, les systèmes d'information d'aide et divers documents en ligne. Consultez ce qui suit pour en savoir plus sur les lecteurs d'écran :
- Utilisation du lecteur d'écran JAWS :

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

  http://www.nvaccess.org/

Lenovo et l'accessibilité

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

© Copyright Lenovo 2017, 2025

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

© Copyright Lenovo 2017, 2025

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. © 2024 Lenovo.

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 du processeur, à la mémoire réelle et virtuelle ou au volume des voies de transmission, 1 Ko correspond à 1 024 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 accessible par l'utilisateur peut varier en fonction des environnements d'exploitation.

Lenovo ne prend aucun engagement et n'accorde aucune garantie concernant les produits non Lenovo. L'assistance (le cas échéant) pour les produits non Lenovo est fournie par le tiers, et non par 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

A

Application UpdateXpress 1

C

coexistence 45
compatibilité 45
composants matériels pris en charge 5
conditions requises 2
configuration requise 5
Contrôleur de gestion de la carte mère 1

D

démarrage d'UpdateXpress 9
dépannage 45
données d'inventaire 4
données d'inventaire incomplètes 4
données d'inventaire manquantes 4

E

exécution d'UpdateXpress 9

F

fonctions d'accessibilité 47

H

hors bande 1

I

installation requise du pilote de périphérique 4
installer les pilotes de périphérique requis 4
Intelligent Peripheral Management Interface 4
interface utilisateur graphique 47
inventaire 2

M

Machines AMD 7
Machines x86 7
marques 50
microprogramme 5
microprogramme pris en charge 5

O

OneCLI 45

P

pilote de périphérique 1
Pilotes de périphérique Windows 5
pilotes de périphérique Windows pris en charge 5
Pilotes de périphériques Linux 5
pilotes de périphériques Linux pris en charge 5
privilèges du système d'exploitation 8

R

remarques 49
ressources web v
restrictions 45

S

scénarios 9
Scénarios UpdateXpress 9
serveurs pris en charge 5
systèmes d'exploitation Linux pris en charge 7
systèmes d'exploitation pris en charge 7
  Linux 7
  Windows 7
systèmes d'exploitation Windows pris en charge 7
systèmes d'exploitation, pris en charge 7

U

UpdateXpress System Pack 1
utilisateurs UpdateXpress System Pack autorisés 8
utilisation d'UpdateXpress 9

© Copyright Lenovo 2017, 2025