Lenovo XClarity Essentials UpdateXpress User Guide

Version 5.2.0

Note

Before using this documentation and the products it supports, read the information in Appendix B "Notices" on page 45.

This edition applies to Lenovo XClarity® Essentials UpdateXpress and to all subsequent releases and modifications until otherwise indicated in the new editions.

Twenty-eighth Edition (May 2025)

Contents

Tables

About this guide

Lenovo XClarity Essentials UpdateXpress (hereafter referred to as the UpdateXpress application) is an application that applies UpdateXpress System Packs (UXSPs) and individual updates to the server. This guide provides information about how to download and use the UpdateXpress application.

Who should read this guide

This documentation is for system administrators or other individuals responsible for system administration who are familiar with firmware and device driver maintenance.

Conventions and terminologies

Paragraphs that start with a Note, Important, or Attention in bold have specific meanings to highlight key information:

Note: These notices provide important tips, guidance, or advice.

Important: These notices provide information or advice that might help users avoid inconvenient or difficult situations.

Attention: These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

In this documentation, when users are instructed to enter a command, type the command and press Enter.

Supported websites

This section provides support web resources.

- Lenovo XClarity Essentials Web site

  Use this Web site to download multiple system-management tools for ThinkSystem and System x servers.
- Lenovo XClarity Essentials UpdateXpress

  Use this Web site to download the UpdateXpress application.

The following Web sites provide information about product compatibility and support, warranties and licenses, and various technical resources.

- Lenovo Flex System Support products and services
- ServerProven Web site
- Lenovo Server, Storage, and Networking Resource Library

Chapter 1. Technical overview

Lenovo XClarity Essentials UpdateXpress (hereafter referred to as the UpdateXpress application) can be used to acquire and apply UpdateXpress System Packs (UXSP) and individual updates to the local or remote system. The UpdateXpress application acquires and deploys UpdateXpress System Pack (UXSP) update packages and individual updates. UXSPs contain firmware and device driver updates.

The following section briefly introduces the four main functions of the UpdateXpress application. For more information, see Chapter 3 "Using the UpdateXpress application" on page 9.

Updating the local server
Update the local machine currently running the UpdateXpress application. The machine type is detected and updates are acquired and automatically applied.

Updating a remote server
Update the remote machine by the Baseboard Management Controller (BMC) running on the machine. Users need a Simple File Transfer Protocol (SFTP) server to transfer the updates to the target remote machine.

Creating a repository of updates
Choose one or more machine types for which updates are acquired from the Lenovo Support Web site. Updates are downloaded to the folder specified, but no updates are applied. Users can later use the UpdateXpress application to apply those updates by indicating that updates should be obtained from the folder specified rather than from the Lenovo Support Web site.

Remote RAID Configuration
Configure RAID array using BMC service.

UpdateXpress System Pack (UXSP)

A UXSP is an integration-tested bundle of online firmware and driver updates for System x and ThinkSystem servers. UXSPs are released semiannually for the first three years and annually for the final three years of support.

UXSPs simplify the process of downloading and installing all of the online driver and firmware updates for a given system. UXSPs ensure that users always work with a complete and most up-to-date set of updates that have been tested together and bundled by Lenovo.

UXSPs are created for a machine type and operating system combination. Separate UXSPs are provided for Windows® operating systems and each of the Linux distributions. For example, there could be several UXSPs for one particular machine type. There could also be an update for the Windows operating system and for each Linux distribution.

There is also a kind of platform UXSP which can be used to update a system in out-of-band way. The platform UXSP does not contain operating system.

UXSP format
A UXSP is delivered in an XML file. The naming convention for a UXSP has the following format:
lnvgy_utl_uxsp_*version_operatingsystem_arch*.`xml`
Example: `lnvgy_utl_uxsp_a3sp27a-1.00_windows_32-64.xml`

Applying UXSPs updates with the UpdateXpress application

Users can use the UpdateXpress application to apply UXSP updates to their machine. The UpdateXpress application inventories the machine on which the update will be applied, queries a specified location for a list of applicable update packages, compares the inventory to the applicable update list, recommends a set of updates to apply, and then deploys those updates to the machine.

To apply UXSPs through the UpdateXpress application, do the following:

1. Download the UpdateXpress application from the Lenovo Support Web site.
2. Run the UpdateXpress application. Select **Update the local machine** or **Update a remote machine**.
3. Select **Check the Lenovo Support Web site**.
4. Select **UpdateXpress application System Packs (UXSPs)**.

Users also can download the updates directly from the Lenovo Support Web site. Remember to download the update payload as well as the XML file. For convenience, choose the same destination folder for each UXSP download. Users can download multiple system packs for different machine types to the same folder. When users run the UpdateXpress application, it detects the machine type and uses the correct content for that machine type. In some cases, there might be common files between system packs. Common files that are already in the folder will not be downloaded again. Therefore, the overall download time is reduced.

Handling a UXSP as a bundle

The UpdateXpress application is designed to download and apply UXSPs. The UXSP is a collection of individual updates as specified by the UXSP XML file.

When running the UpdateXpress application, users can select to work with either UXSPs or individual updates. In most cases, it is recommended to work with UXSPs, but the option to also work with individual updates gives users greater flexibility in choosing which updates to use.

Handling update requisites

This topic describes how the update requisites are acquired and applied.

To successfully apply updates, all prerequisites and corequisites for an update must also be acquired and applied. The UpdateXpress application automatically checks for, acquires, and applies prerequisites and corequisites. Updates frequently require users to apply prerequisite files before they can be successfully applied or to include corequisite packages to properly use the applied update. To simplify the update process, the UpdateXpress application uses information included in the update file to identify requisite packages for the specified updates. The UpdateXpress application then applies these requisite packages.

Prerequisite files

The update packages provided by Lenovo include information about which prerequisite files must be applied before users can successfully apply the update. When users specify an update, the UpdateXpress application reads this information and locates the prerequisite packages.

By default, the UpdateXpress application acquires the update packages and evaluates them to determine whether the prerequisite conditions have been met, and if necessary, applies the prerequisite files automatically before applying the specified update. Users can choose not to apply the prerequisite files. However, this could cause the update not to be applied successfully.

If prerequisite packages have prerequisites or corequisites, they are acquired, evaluated, and applied in the same manner.

Corequisite files

Some updates require corequisite files, that is, additional packages that must be applied to complete the update successfully, but these packages do not have to be applied prior to the update specified.

By default, the UpdateXpress application identifies, acquires, evaluates, and applies the corequisite packages as part of the update.

If corequisite packages have prerequisites or corequisites, they are acquired, evaluated, and applied in the same manner.

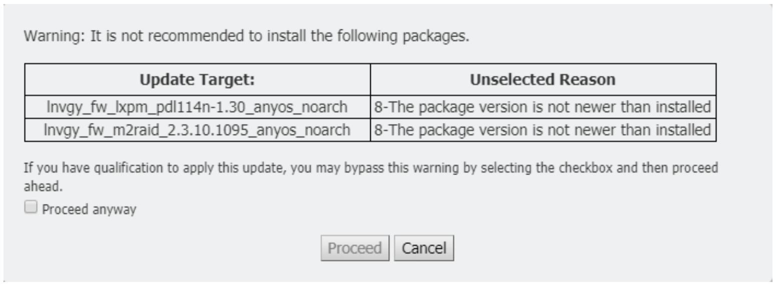
Example

As an example, consider an update that has both prerequisites and corequisites. By default, the UpdateXpress application takes the following steps:

1. To ensure that the update can be completed, the UpdateXpress application first downloads the update.
2. The prerequisite files are downloaded.
3. The corequisite files are downloaded.
4. The prerequisite or corequisite files are evaluated against the current state of the system. If the system is already at the required level because these requisites have already been applied, the requisite is ignored.
5. The necessary prerequisite files are applied.
6. The update is applied.
7. The necessary corequisite files are applied.

Update recommendation

By default, the application UpdateXpress will select the packages that are recommended for the system to install or upgrade. Users can also manually select those packages to install or upgrade. In this case, users will receive a warning message similar to the following one:



Warning: It is not recommended to install the following packages.

Update Target:	Unselected Reason
lnvgy_fw_lxpm_pdl114n-1.30_anyos_noarch	8-The package version is not newer than installed
lnvgy_fw_m2raid_2.3.10.1095_anyos_noarch	8-The package version is not newer than installed

If you have qualification to apply this update, you may bypass this warning by selecting the checkbox and then proceed ahead.

□ Proceed anyway

If users see this message, it is recommended to stop the update process.

Operating system independent updates

Some individual updates apply to a specific machine type regardless of the operating system being used. These individual updates are treated as operating system independent updates. Users can select operating system independent updates the same way of selecting operating system specific updates.

Note: When users select updates for a specific operating system, operating system independent updates are included as part of the package. Select operating system independent updates only if users are not selecting any operating system updates for a machine type.

Missing or incomplete inventory data

Sometimes an update package applies to a component for which the UpdateXpress application cannot determine the firmware or driver version. In this case, the UpdateXpress application displays the version of the update package instead of the component version. If an installed component version is not detected, the update is not selected by default. In this case, select the package as a recommended update manually.

Installing required drivers

The UpdateXpress application installs required device drivers.

The UpdateXpress application installs every driver in the UXSP when:

- The current device driver is earlier than the available device driver in the UXSP.
- The UpdateXpress application is unable to determine the current device driver version, which typically occurs when the device driver is not installed.

  Note: The UpdateXpress application displays `Undetected` when an installed device driver version is not detected.

Users can take advantage of this behavior to install the following device drivers, which are required for firmware updates:

- Intelligent Peripheral Management Interface (IPMI)
- IPMI Mapping Layer

Chapter 2. Hardware and software requirements

Before users begin to use the UpdateXpress application, review the hardware, operating system, and the local operating system privilege requirements. Systems running the UpdateXpress application require at least 1 GB of Radom-Access Memory (RAM).

Supported server models

The UpdateXpress application supports Windows and Linux device drivers and firmware that are included in available UXSPs. A list of currently supported components device drivers and firmware can be found in the UpdateXpress application readme file that is included in each system pack.

Table 1. Supported Lenovo systems

Series	Server models	
ThinkEdge	• SE100 Node (7DGR) • SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
ThinkSystem	• DX1100U Gateway (7D49) • DX1100U Performance/Capacity (7D4A) • DXN2000 Storage (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) • WH5900 Appliance (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 VX Series (7D28, 7D2Z, 7D43, 7DDK, 7Y12, 7Y13, 7Y14, 7Y92, 7Y93, 7Y94, 7Z12, 7Z13, 7Z62, 7Z63) • ThinkAgile MX Series (7D19, 7D1B, 7D1H, 7D5R, 7D5S, 7D5T, 7D66, 7D67, 7D6B, 7DGP, 7DGG, 7DKB, 7Z20)	• ThinkAgile HX Series (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)

Table 1. Supported Lenovo systems (continued)

Series	Server models	
System x	• HX 3310 Appliance (8693) • HX 5510/7510 Appliance (8695) • nx360 M5 (5465, 5467) • x240 Compute Node (7162, 2588) • x240 M5 Compute Node (2591, 9532) • x280 X6/x480 X6/x880 X6 Compute Node (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]
Notes: 1. This server model is AMD one socket processor-based. 2. This server model supports both single node and multiple node. 3. This server model supports the multiple management feature.		

Supported operating systems

The UpdateXpress application is supported on Linux and Windows operating systems.

Windows

The UpdateXpress application is supported on 64-bit operating systems. Use the information in the following table to identify operating systems that are supported by the UpdateXpress application.

Table 2. Supported Windows operating systems

Operating system	Update Local	Update Remote	Local Repository	Remote RAID Configuration
Microsoft Windows 10/11 Pro for Workstations (21H2/22H2)	Yes[note]	Yes	Yes	Yes
Microsoft Windows Server 2016	Yes	Yes	Yes	Yes
Microsoft Windows Server 2019	Yes	Yes	Yes	Yes
Microsoft Windows Server 2022	Yes	Yes	Yes	Yes
Microsoft Windows Server 2025	Yes	Yes	Yes	Yes

Note: The server models supporting Microsoft Windows 10/11 Pro for Workstations (21H2/22H2) can also access to its update local feature.

Linux

The UpdateXpress application is supported on the following versions of Linux operating systems.

Table 3. Supported Linux operating systems

Operating system	Update Local	Update Remote	Local Repository	Remote RAID Configuration
Red Hat Enterprise Linux 8.x (Up to U10)	Yes	Yes	Yes	Yes
Red Hat Enterprise Linux 9.x (Up to U5)	Yes	Yes	Yes	Yes
SUSE Linux Enterprise Server 15.x (Up to SP6)	Yes	Yes	Yes	Yes

Notes:

- 500 MB of free disk space is recommended when running the UpdateXpress application on a Linux operating system.
- The UpdateXpress application supports fuzzy operating system check. If the current operating system does not support the firmware packages in a UXSP, the firmware packages might also be listed in the comparison result of the UpdateXpress application.
- Depending on the `ifconfig` command on Linux OS, UpdateXpress might not be installed on RHEL 7.0 or later versions. To update the firmware on RHEL 7.0 or later versions, users should install net-tools.
- Linux device driver updates require specific packages. The following packages are required to be installed:
  - Red Hat Enterprise Linux: rpm-build, perl, and bash
  - SUSE Enterprise Linux: perl and bash
- For the following operating systems, users can use UpdateXpress 4.4.1 instead:
  - RedHat 7.6/7.7/7.8/7.9
- For the following operating systems, users can use UpdateXpress 4.3.0 instead:
  - SUSE 12.5
- For the following operating systems, users can use UpdateXpress 4.1.0 instead:
  - RedHat 7.5
  - SUSE 12.4
- For the following operating systems,users can use UpdateXpress 3.4.0 instead:
  - 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

Operating system privileges

This sections describes the privileges for logging in to the Windows and Linux OS. The UpdateXpress application will return an error message if the insufficient privilege is used. Before you begin, store the UpdateXpress application, including its extractions, and sensitive logs to a safe place where only authorized users can access.

- For Windows OS, the administrator or administrator-equivalent privilege is required.
- For Linux OS, the root account is required.

Chapter 3. Using the UpdateXpress application

Users can use the UpdateXpress application to interactively deploy updates. A screen resolution of 1024 x 768 or higher is recommended when running the UpdateXpress application. To run the UpdateXpress application, extract the compressed file and invoke the executable file for the operating system. No installation is required.

Windows

For Windows operating system, the UpdateXpress application is named as follows:

```
lnvgy_utl_lxce_ux{ build id }_{ version }_windows_indiv.zip
```

For each release of the UpdateXpress application, users can distinguish the Windows ZIP file name by its version number. The Windows ZIP file is specified as **lnvgy_utl_lxce_ux{ build id }_{ version } _windows_indiv.zip** where *lnvgy_utl_lxce_ux* is the name of the ZIP file, *build id* indicates the build number and *version* indicates the UpdateXpress application version number.

Linux

For Linux operating system, the UpdateXpress application is named as follows:

Operating system	Name of the UpdateXpress application
Red Hat Enterprise Linux 7.X/8.X/9.X AMD64/EM64T and above	`lnvgy_utl_lxce_ux{ build id }_{ version }_linux_indiv.tgz`
SUSE Linux Enterprise Server 12.X/15.X AMD64/EM64T and above	`lnvgy_utl_lxce_ux{ build id }_{ version }_linux_indiv.tgz`

The name of the UpdateXpress application is different for Windows and Linux operating systems. For convenience, hereafter *<Zipfile>* is used to refer to the name of the UpdateXpress application for both Windows and Linux operating systems in this documentation.

Launching the UpdateXpress application

Users can use the UpdateXpress application to acquire the latest UXSPs and individual updates.

To launch the UpdateXpress application, do the following:

- **For Windows**:
  1. Extract the *<Zipfile>* to a local folder.
  2. Do one of the following:
     - Double-click **lxce_ux.exe**.
     - Right-click **lxce_ux.exe** and click **Run as administrator** in the pop-up menu.
- **For Linux**:

  Type the following commands in the terminal:

  ```
  tar xvf <Zipfile>
  ```

  ```
  ./start_lxce_ux.sh
  ```

Updating servers

Updating a local server from the Web site

The UpdateXpress application can update a local machine with UXSPs or individual updates acquired from the Web site.

Prerequisite:

- The UpdateXpress application is running on a local machine to be updated.
- The machine is running a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.

To update a local machine from the Web site, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the local server**. If **Input BMC access information** is selected, input the BMC information in this window and click **Next**.

Step 4. In the Task window, select **Perform updating on target server** and click **Next**.

Step 5. In the Update Setting window, do one or more of the following:

- To upgrade the backup system firmware, select **Only update the backup image of the BMC (and UEFI where applicable)** and click **Next**.
- To downgrade the firmware, select **Enable updating to a back-level firmware** and click **Next**.

Step 6. In the Updates Location window, select **Check the Lenovo support web site**, and click **Next**.

Step 7. In the Update Type window, select the target update type, and click **Next**.

Step 8. In the Target Directory window, specify the location for the updates to be downloaded or accept the default location, and click **Next**.

Step 9. On the Internet Access page, if users have no special requirement for security access, click **Test Connection** to check the network connection of the Target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, do one or more of the following:

- Configure **Proxy server**:
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

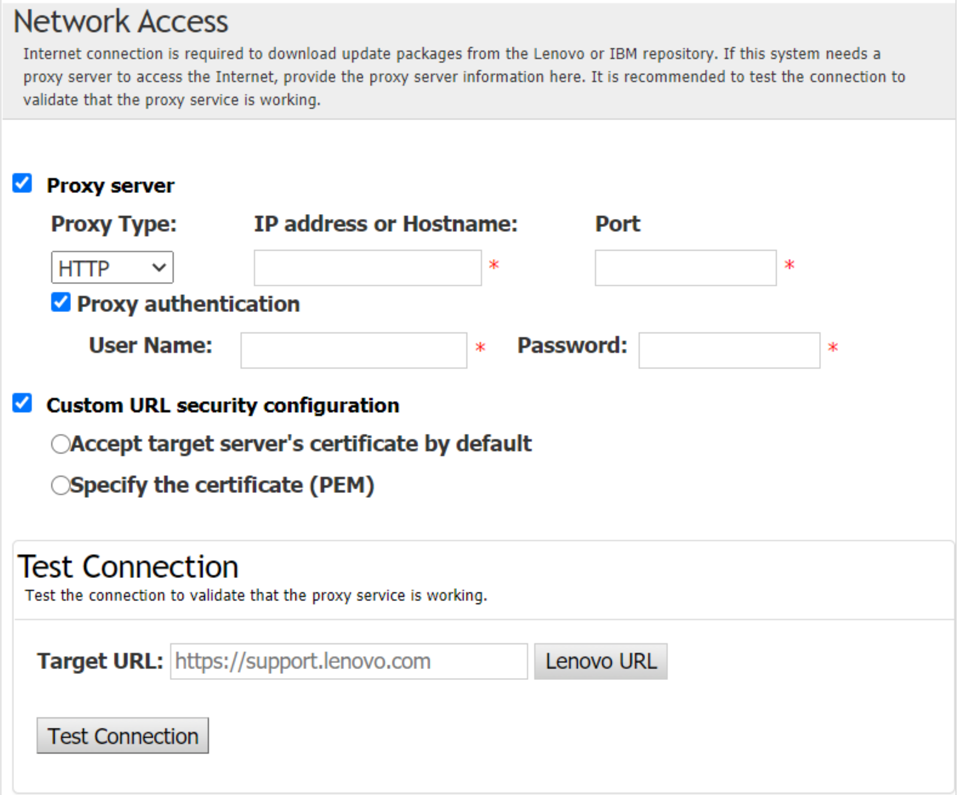
  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- Configure **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:

- **Accept target server's certificate by default**
- **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ Proxy server

Proxy Type: HTTP

IP address or Hostname: *

Port *

☑ Proxy authentication

User Name: * Password: *

☑ Custom URL security configuration

○ Accept target server's certificate by default

○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 10. In the Update Recommendation window, do one or more of the following:

- To display all update packages, select **Show updates of undetected devices**.
- To update the component, select the target component, and click **Next**.

Step 11. In the Acquire Updates window, the acquisition table displays the acquiring progress of the packages. When the progress is completed, click **Next**.

Step 12. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 13. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating a local server from a local directory

The UpdateXpress application can update a local machine with UXSPs or individual updates acquired from a local folder.

Prerequisite:

- The UpdateXpress application is running on a local machine to be updated.
- The machine is running a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- The mounted ISO should not be used as a valid local directory; otherwise, it might be unmounted during the update process and cause flash failure.

To update a local machine from a local directory, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the local server**, and click **Next**.

Step 4. In the Task window, select **Perform updating on target server**, and click **Next**.

Step 5. In the Update Setting window, do one or more of the following:

- To update the back-up image of BMC or UEFI, select **Only update the backup image of the BMC (and UEFI where applicable)** and click **Next**.
- To downgrade the firmware, select **Enable updating to a back-level firmware** and click **Next**.

Step 6. In the Updates Location window, select **Look in local directory**. To specify a local folder, do one of the following:

- Click **Browse**, select the target folder, and then click **Next**.
- Input the folder path into the field beside the **Browse** button, and click **Next**.

Step 7. In the Update Type window, select the target update type, and click **Next**.

Step 8. In the Update Recommendation window, do one of the following:

- To display all update packages, select **Show updates with no adapters detected**.
- To compare the versions of installed driver and firmware with the latest versions, click **Begin**. After the progress is completed, select one or more target packages, and click **Next**.
- To compare the version of devices installed in the local system with the latest version, select **Only compare installed devices**, and click **Begin**. After the progress is completed, select one or more target packages, and click **Next**.

Step 9. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 10. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating a remote server from the Web site

The UpdateXpress application can update a remote machine with UXSPs or individual updates acquired from the Web site.

Prerequisite:

The UpdateXpress application is running on a machine installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.

To update a remote machine from the Web site, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If not checking the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Perform updating on target server** and click **Next**.

Step 5. In the Update Setting window, select one or more of the options. If **Use a separate remote server instead of the BMC one** is selected, input the following information:

- (SFTP/HTTP/HTTPS/FTP Setting) **IP address or Host name**: IP address or host name of the server.

- (SFTP/HTTP/HTTPS/FTP Setting) **User Name**: User name of the server.
- (SFTP/HTTP/HTTPS/FTP Setting) **Password**: Password of the server.
- (SFTP/HTTP/HTTPS/FTP Setting) **Port**: Port number of the server. If users do not input, the default port is used.
- (SFTP/HTTP/HTTPS/FTP Setting) **Directory**: The location on the server where update packages are copied to.

  Note: Input a full path on the SFTP/HTTP/HTTPS/FTP server. The FTP server is only used for the ThinkServer marked with superscript 2 (Note 2) in "Supported server models" on page 5.

Step 6. To configure the SFTP server key fingerprint, do one of the following:
- To check the SFTP server key fingerprint, click **Yes**.
- Not to check the SFTP/HTTPS server key fingerprint, select **Skip check SFTP server's key fingerprint**, and click **Next**.

Step 7. Do one or more of the following:
- To downgrade the firmware, select **Enable updating to a back-level firmware**, and click **Next**.
- To upgrade the backup system firmware, select **Only update the backup image of the BMC (and UEFI where applicable)**, and click **Next**.

Step 8. In the Updates Location window, select **Check the Lenovo Support Web site**, and click **Next**.

Step 9. In the Target Directory window, specify the location for the updates to be downloaded or accept the default location, and click **Next**.

Step 10. On the Internet Access page, if users have no special requirement for security access, click **Test Connection** to check the network connection of the Target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, configure **Proxy server** and/or **Custom URL security configuration** depending on the security requirements as follows:
- **Proxy server**
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

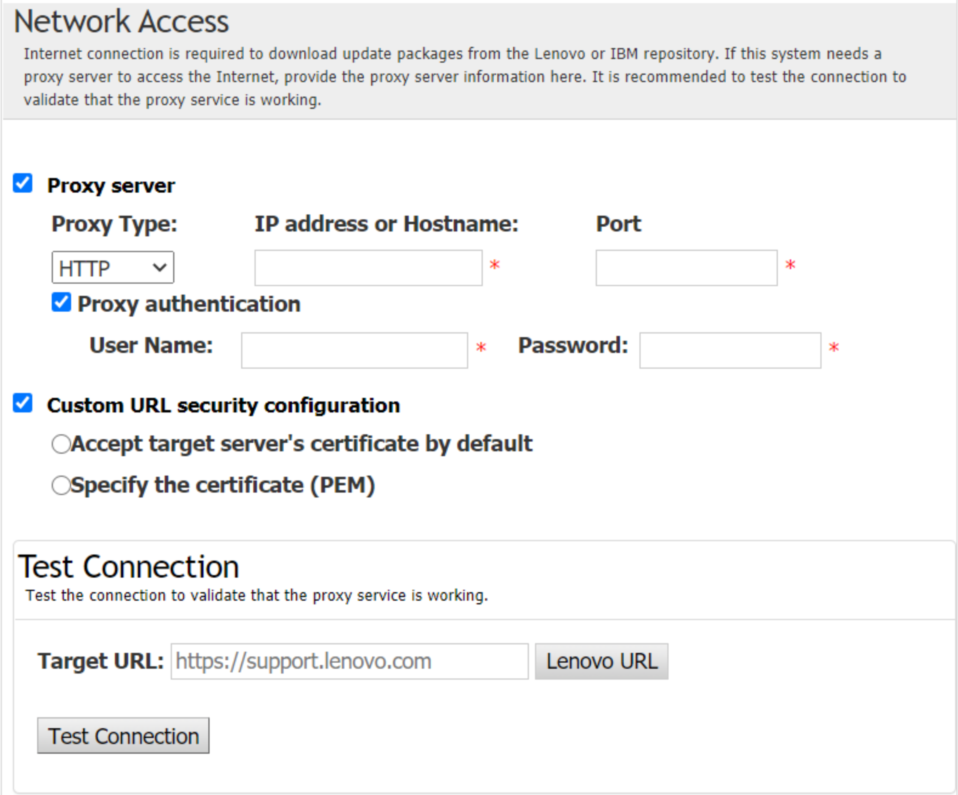
Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:
  – **Accept target server's certificate by default**
  – **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ Proxy server

Proxy Type: HTTP | IP address or Hostname: * | Port *

☑ Proxy authentication

User Name: * | Password: *

☑ Custom URL security configuration

○ Accept target server's certificate by default

○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 11. In the Update Type window, select the target update type, and click **Next**.

Step 12. In the Update Recommendation window, do one or more of the following:
- To display all update packages, select **Show updates of undetected devices**.
- To update the component, select the target component, and click **Next**.

Step 13. In the Acquire Updates window, the acquisition table displays the acquiring progress of the packages. When the progress is completed, click **Next**.

Step 14. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 15. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating a remote server from a local directory

The UpdateXpress application can update a remote machine with UXSPs or individual updates acquired from a local folder.

Prerequisite:

The UpdateXpress application is running on a machine installed with a supported operating system. For details of supported operating systems, see “Supported operating systems” on page 7.

To update a remote machine from a local directory, do the following:

Step 1. Launch the UpdateXpress application. See “Launching the UpdateXpress application” on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.
- **IP address or Host name**: BMC IP address or host name of the target system.

- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate and SFTP/HTTPS server key fingerprint, select **Accept BMC server's certificate and SFTP/HTTPS server's key fingerprint by default**, and click **Next**.

Step 4. In the Task window, select **Perform updating on target server**, and click **Next**.

Step 5. In the Update Setting window, if **Use a separate remote server** is selected, input the following information:

- (SFTP/HTTP/HTTPS/FTP Setting) **IP address or Host name**: IP address or host name of the server.
- (SFTP/HTTP/HTTPS/FTP Setting) **User Name**: User name of the server.
- (SFTP/HTTP/HTTPS/FTP Setting) **Password**: Password of the server.
- (SFTP/HTTP/HTTPS/FTP Setting) **Port**: Port number of the server. If users do not input, the default port is used.
- (SFTP/HTTP/HTTPS/FTP Setting) **Directory**: The location on the server where update packages are copied to.

  Note: Input a full path on the SFTP/HTTP/HTTPS/FTP server. The FTP server is only used for the ThinkServer marked with superscript 2 (Note 2) in "Supported server models" on page 5.

Step 6. To configure the SFTP server key fingerprint, do one of the following:

- To check the SFTP server key fingerprint, click **Yes**.
- Not to check the SFTP/HTTPS server key fingerprint, select **Skip check SFTP server's key fingerprint**, and click **Next**.

Step 7. Do one or more of the following:

- To downgrade the firmware, select **Enable updating to a back-level firmware**, and click **Next**.
- To upgrade the backup system firmware, select **Only update the backup image of the BMC (and UEFI where applicable)**, and click **Next**.

Step 8. In the Updates Location window, select **Look in local directory**. To specify a local folder, do one of the following:

- Click **Browse** , select the desired folder, and click **Next**.
- Input the folder path into the field beside the **Browse** button, and click **Next**.

Step 9. In the Update Type window, select the target update type, and click **Next**.

Step 10. In the Update Recommendation window, click **Begin** to compare the version of installed firmware with the latest version. After the progress is completed, select one or more target packages, and click **Next**.

Note: To display all update packages, select **Show updates with no adapters detected** before clicking **Begin**.

Step 11. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 12. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating multiple remote servers from the Web site

The UpdateXpress application supports to update the remote servers in batch from Web site.

Note: To update the single remote server from the Web site, refer to "Updating a remote server from the Web site" on page 12.

Prerequisite:

The multi-update function for the remote servers is only supported in the ThinkServer servers and the WenTian server. For details of supported servers, see **ThinkServer and WenTian series** in "Supported server models" on page 5.

To update multiple remote servers from the Web site, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Multi-server Management**, and click **Next**.

Step 4. In the Multi-server Management window, do one or more of the following:

- To add new servers into server pool, select **+ Add new servers**. In the Add new servers window, do one of the following:
  - Select **IP range**, input the IP address range and click **Discover**.
  - Select **Discover by SSDP**, select the target adapter and click **Discover**.
- To remove the server from the Server Pool list, select one or more target servers, and click **Action → Remove Selected**.
- To verify whether the user name and password are correct for the server, select one or more target servers, and click **Action → Scan Selected**.
- To export the Server Pool list, select one or more target servers, click **Action → Export**.

  Note: By default, the Server Pool list will be saved in the JSON file. Users can also select the CSV and XLS format.
- To import the Server Pool list to other server, select one or more target servers from the list, click **Action → Import** and select the target JSON file.
- To change the password of the server, select one or more target servers, click **Action → Change IP and Password**. On the Change IP and Password page, do one of the following:
  - To change the password for single server, input the new user name and password, and click **Execute**. The new user name and password will be automatically added to the drop-down list.
  - To change the password for multiple servers, click **Export**, modify the password in the exported CSV file, and save the file. Go back to the Change IP and Password page, click **Import** to add the CSV file, and click **Execute**.
  - To view the details of each server, click ⌄ of the target server.

  Note: The user role of **USERID** is **Administrator**, which cannot be changed.
- To use common BMC credentials for management, select **Input the common BMC credentials -**, input user name and password.

Step 5. Go back to the Multi-server Management window, click **Next**, a message will be prompted to remind users to confirm whether the certificate should be updated. Click **Accept** to update the certificate.

Note: If users log in for the first time or the password is expired, change the password in the Change password window.

Step 6. In the Task window, select **Perform updating on target server** and click **Next**.

Step 7. In the Update Setting window, select one or more of the options. If **Use a separate remote server instead of the BMC one** is selected, input the following information:

- (HTTPS/FTP Setting) **IP address or Host name**: IP address or host name of the server.
- (HTTPS/FTP Setting) **User Name**: User name of the server.
- (HTTPS/FTP Setting) **Password**: Password of the server.
- (HTTPS/FTP Setting) **Port**: Port number of the server. If users do not input, the default port is used.
- (HTTPS/FTP Setting) **Directory**: The location on the server where update packages are copied to.

Note: Input a full path on the HTTPS/FTP server. The FTP server is only used for the ThinkServer marked with superscript 2 (Note 2) in "Supported server models" on page 5.

Step 8. To configure the HTTPS server key fingerprint, do one of the following:

- To check the HTTPS server key fingerprint, click **Yes**.
- Not to check the HTTPS server key fingerprint, select **Skip check HTTPS server's key fingerprint**, and click **Next**.

Step 9. In the Updates Location window, select **Check the Lenovo Support Web site**, and click **Next**.

Step 10. In the Target Directory window, specify the location for the updates to be downloaded or accept the default location, and click **Next**.

Step 11. On the Internet Access page, if users have no special requirement for security access, click **Test Connection** to check the network connection of the Target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, configure **Proxy server** and/or **Custom URL security configuration** depending on the security requirements as follows:

- **Proxy server**
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

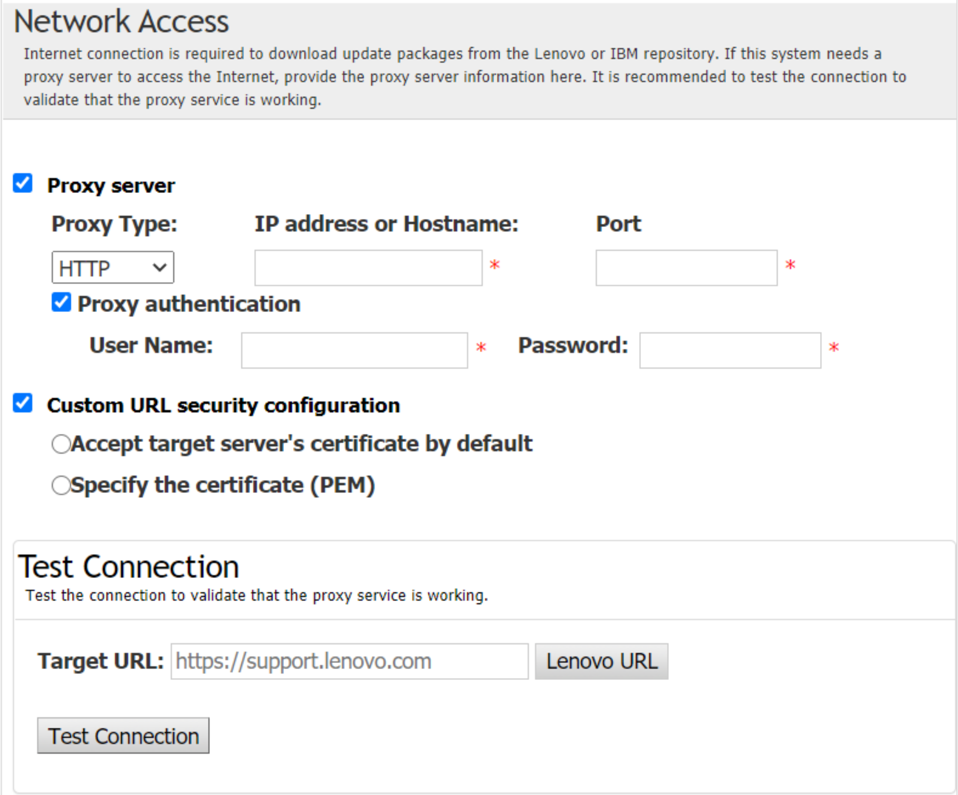
Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:
  - **Accept target server's certificate by default**
  - **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ **Proxy server**

Proxy Type:	IP address or Hostname:	Port
HTTP	*	*

☑ **Proxy authentication**

User Name:	*	Password:	*

☑ **Custom URL security configuration**

○ Accept target server's certificate by default

○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 12. In the Update Type window, select the target update type, and click **Next**.

Step 13. In the Update Recommendation window, click **Begin** to compare the version of firmware with the latest version. After the progress is completed, select one or more target packages, and click **Next**.

Note: To display all update packages, select **Show updates with no adapters detected** before clicking **Begin**.

Step 14. In the Acquire Updates window, the acquisition table displays the acquiring progress of the packages. When the progress is completed, click **Next**.

Step 15. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 16. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating multiple remote servers from a local directory

The UpdateXpress application supports to update the remote servers in batch from a local folder.

Note: To update the single remote server from a local folder, refer to "Updating a remote server from a local directory" on page 14.

Prerequisite:

The multi-update function for the remote servers is only supported in the ThinkServer servers and the WenTian server. For details of supported servers, see **ThinkServer and WenTian series** in "Supported server models" on page 5.

To update multiple remote servers from a local directory, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Multi-server Management**, and click **Next**.

Step 4. In the Multi-server Management window, do one or more of the following:

- To add new servers into server pool, select **+ Add new servers**. In the Add new servers window, do one of the following:
  - Select **IP range**, input the IP address range and click **Discover**.
  - Select **Discover by SSDP**, select the target adapter and click **Discover**.
- To remove the server from the Server Pool list, select one or more target servers, and click **Action → Remove Selected**.
- To verify whether the user name and password are correct for the server, select one or more target servers, and click **Action → Scan Selected**.
- To export the Server Pool list, select one or more target servers, click **Action → Export**.

  Note: By default, the Server Pool list will be saved in the JSON file. Users can also select the CSV and XLS format.
- To import the Server Pool list to other server, select one or more target servers from the list, click **Action → Import** and select the target JSON file.
- To change the password of the server, select one or more target servers, click **Action → Change IP and Password**. On the Change IP and Password page, do one of the following:
  - To change the password for single server, input the new user name and password, and click **Execute**. The new user name and password will be automatically added to the drop-down list.
  - To change the password for multiple servers, click **Export**, modify the password in the exported CSV file, and save the file. Go back to the Change IP and Password page, click **Import** to add the CSV file, and click **Execute**.
  - To view the details of each server, click ⌄ of the target server.

  Note: The user role of **USERID** is **Administrator**, which cannot be changed.
- To use common BMC credentials for management, select **Input the common BMC credentials -**, input user name and password.

Step 5. Go back to the Multi-server Management window, click **Next**, a message will be prompted to remind users to confirm whether the certificate should be updated. Click **Accept** to update the certificate.

Note: If users log in for the first time or the password is expired, change the password in the Change password window.

Step 6. In the Task window, select **Perform updating on target server** and click **Next**.

Step 7. In the Update Setting window, select one or more of the options. If **Use a separate remote server instead of the BMC one** is selected, input the following information:

- (HTTPS/FTP Setting) **IP address or Host name**: IP address or host name of the server.
- (HTTPS/FTP Setting) **User Name**: User name of the server.
- (HTTPS/FTP Setting) **Password**: Password of the server.
- (HTTPS/FTP Setting) **Port**: Port number of the server. If users do not input, the default port is used.
- (HTTPS/FTP Setting) **Directory**: The location on the server where update packages are copied to.

  Note: Input a full path on the HTTPS/FTP server. The FTP server is only used for the ThinkServer marked with superscript 2 (Note 2) in "Supported server models" on page 5.

Step 8. In the Updates Location window, select **Look in local directory**. To specify a local folder, do one of the following:

- Click **Browse** , select the desired folder, and click **Next**.
- Input the folder path into the field beside the **Browse** button, and click **Next**.

Step 9. In the Update Type window, select the target update type, and click **Next**.

Step 10. In the Update Recommendation window, click **Begin** to compare the version of installed firmware with the latest version. After the progress is completed, select one or more target packages, and click **Next**.

Note: To display all update packages, select **Show updates with no adapters detected** before clicking **Begin**.

Step 11. In the Update Execution window, click **Begin Update and confirm to continue on the pop window**. The execution table displays the upgrade progress of the packages. When the upgrade progress is completed, click **Next**.

Step 12. In the Finish window, click the log to check the updates, and click **Close** to exit.

Managing server under Direct Ethernet Connection

UpdateXpress application supports to manage the servers under direct Ethernet Connection. When the network cable is connected, UpdateXpress will try to access server BMC through the default BMC IP and credential.

To manage server under Direct Ethernet Connection, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Direct Ethernet Connection**, input the following information, and click **Next**.

Step 4. In the Direct Ethernet Connection Setting window, do the following:

a. Select the target adapter from the "Available network adapter" table.

b. Ensure the default IP address is **192.168.70.125**.

c. Input the user name and password.

d. Click **Test Connection** → **Next** or **Next**.

Step 5. In the Task window, select one of the following:

- **Perform updating on target server**. For details, see Step 4 and the subsequent steps in "Updating a remote server from a local directory" on page 14.
- **Manage Staged Update**. For details, see Step 4 and the subsequent steps in "Performing staged update for a remote server" on page 20.
- **Remote RAID configuration**. For details, see Step 4 and the subsequent steps in "Configuring RAID array for a remote server" on page 26.
- **Configure security feature on ThinkEdge server**. For details, see Step 4 and the subsequent steps in the following sections:
  - "Managing SED authentication key" on page 35
  - "Claiming server in ThinkShield Portal" on page 32
  - "Upgrading lockdown control mode" on page 36
  - "Activating the server in lockdown mode" on page 37
  - "Configuring security sensors" on page 34

Performing staged update for a remote server

The UpdateXpress application supports to perform staged updates for a remote server.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.

To perform staged update for a remote server, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Perform updating on target server**, and click **Next**.

Step 5. In the Update Setting window, select one or more of the options and click **Next**.

Notes:

- If **Use a separate remote server instead of the BMC one** is selected, input the following information:
  - **IP address or Host name**: BMC IP address or host name of the target system.
  - **User Name**: BMC user name of the target system.
  - **Password**: BMC password of the target system.
  - **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.
  - **Directory**: Full path on the SFTP server. The updates file will be upload to that directory. Ensure that the directory is accessible. For example: /payload
- Not to check the SFTP/HTTPS server key fingerprint, select **Skip check SFTP server's key fingerprint**.

Step 6. In the Updates Location window, select **Check the Lenovo Support web site**, and click **Next**.

Step 7. In the Target Directory window, specify the location for the updates to be downloaded or accept the default location, and click **Next**.

Step 8. On the Internet Access page, if users have no special requirement for security access, click **Test Connection** to check the network connection of the target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, configure **Proxy server** and/or **Custom URL security configuration** depending on the security requirements as follows:

- **Proxy server**
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

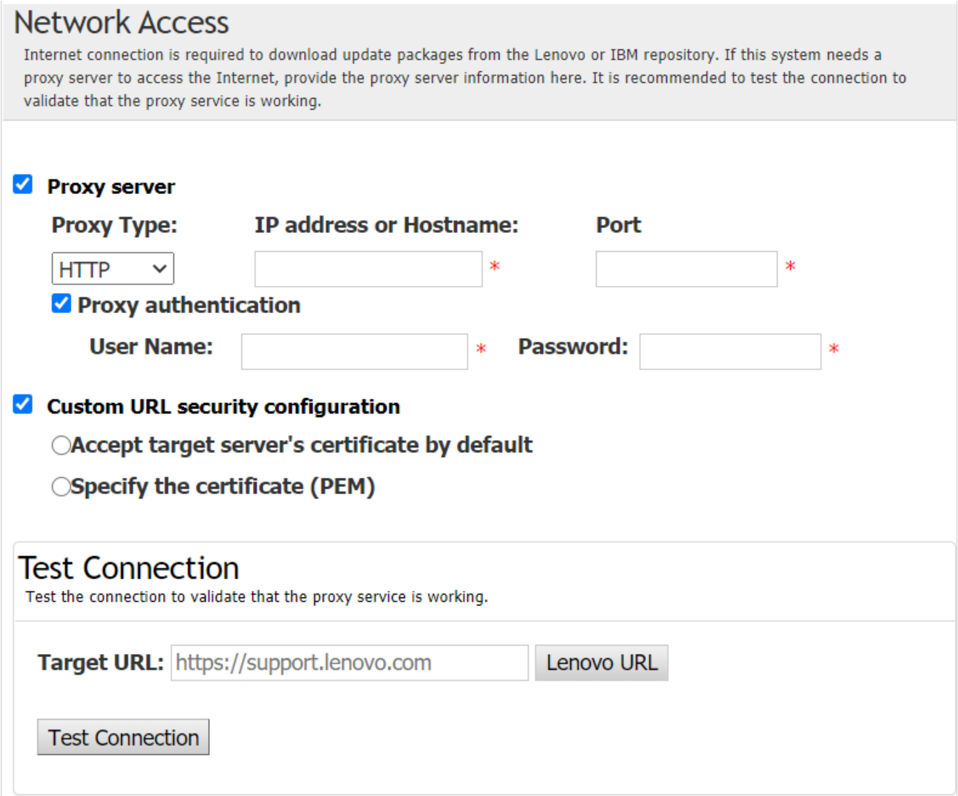
  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:

- **Accept target server’s certificate by default**
- **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ **Proxy server**

Proxy Type: HTTP

IP address or Hostname: *

Port *

☑ **Proxy authentication**

User Name: * **Password:** *

☑ **Custom URL security configuration**

○ **Accept target server's certificate by default**

○ **Specify the certificate (PEM)**

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 9. In the Update Type window, select the target update type, and click **Next**.

Step 10. In the Update Recommendation window, do one or more of the following:

- To display all update packages, select **Show updates of undetected devices**.
- To update the component, select the target component, and click **Next**.

Step 11. In the Acquire Updates window, the acquisition table displays the acquiring progress of the packages. When the progress is completed, click **Next**.

Step 12. In the Running updates window, click **Begin Update → Yes → Next**.

Notes: To update the firmware with bundled packages, select **Update firmware with bundled package(s). This checkbox and its suboptions only support XCC2.**, and set the apply time.

- **OnReset**: Update the packages when the system is restarted next time.
- **Immediate**: Update the packages immediately. The system might be restarted immediately.
- **OnStartUpdateRquest**: Update the packages through managing the stage update or running OneCLI commands.

Step 13. In the Finish window, click the log to check the updates, and click **Close** to exit.

Creating a repository of updates

The UpdateXpress application can create a repository of UXSPs or individual updates acquired from the Web site.

Prerequisite:

- The UpdateXpress application is running on a machine where the repository is to be created.
- The machine is running a supported operating system. For details of supported operating systems, see “Supported operating systems” on page 7.

To create an update repository, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Create a repository of updates**, and click **Next**.

Step 4. In the Update Type window, select the target update type, and click **Next**.

- **UpdateXpress System Packs (UXSPs)**: Select this option to update UXSP. The Update Selection window is skipped if this option is selected, but all the UXSP packages are downloaded.
- **Latest available individual updates**: Select this option to update individual packs. The Update Selection window is displayed in the following step if this option is selected, users should select the target packages.
- **Download the zip format packages**: Select this option to download the appropriate ZIP packages from the Lenovo support site.

Step 5. On the Internet Access page, if there are no special requirement for security access, click **Test Connection** to check the network connection of the Target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, configure **Proxy server** and/or **Custom URL security configuration** depending on the security requirements as follows:

- **Proxy server**
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

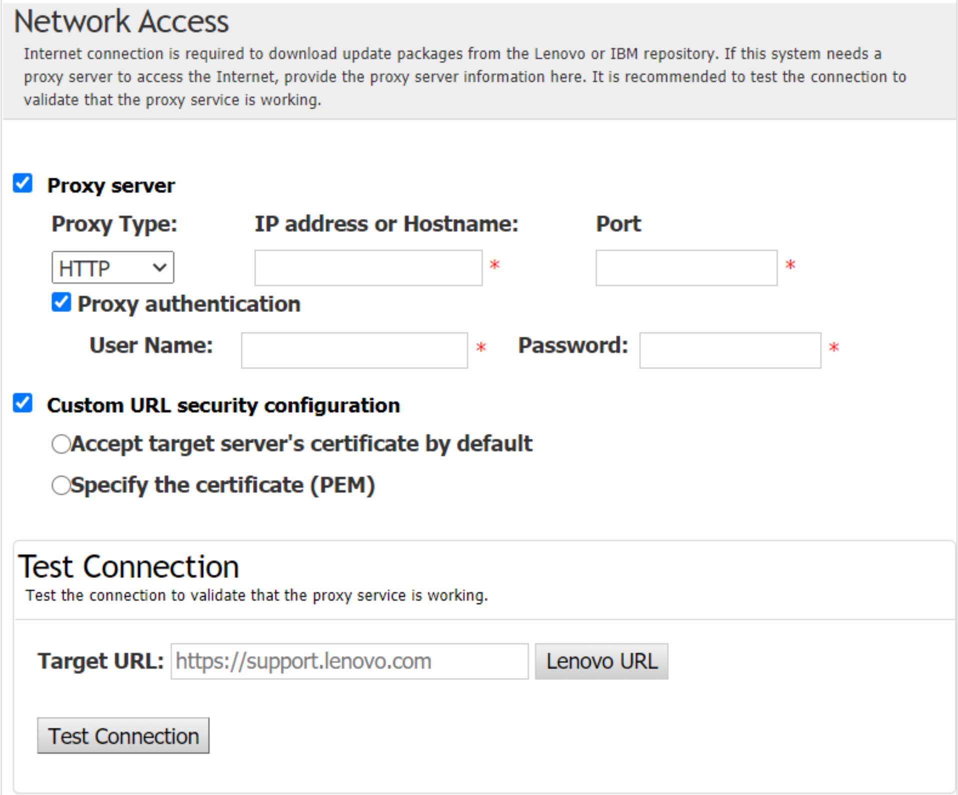
Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:
  - **Accept target server's certificate by default**
  - **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ Proxy server

Proxy Type: HTTP | IP address or Hostname: * | Port *

☑ Proxy authentication

User Name: * | Password: *

☑ Custom URL security configuration

○ Accept target server's certificate by default

○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 6. In the Machine Types window, select the target machine types, and click **Next**.

- To select all listed machine types, select the check box in the header.
- To add a machine type, click **Add**, and specify the machine type.
- To remove a machine type, select the machine type from the list, and click **Remove**.
- To update the machine type list to the latest version, click **Update List**.
- To reset the machine type list, click **Reset List**.

Step 7. In the Operating Systems window, select the target operating systems, and click **Next**.

Step 8. In the Target Directory window, specify the location for the updates to be downloaded or accept the default location, and click **Next**.

Step 9. (Optional) Select **Latest available individual updates**, the Update Selection window is displayed. Select the target updates, and then click **Next**.

Step 10. In the Acquire Updates window, the acquisition table displays the acquiring progress of the packages. When the progress is completed, click **Next**.

Step 11. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring BIOS

Configuring BIOS for a remote server

The UpdateXpress application supports to configure the BIOS settings for a remote server.

Prerequisite:

The BIOS configuration function for the remote server is only supported in the ThinkServer/WenTian servers. For details of supported operating systems, see "Supported operating systems" on page 7.

To configure BIOS, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate and SFTP/HTTPS server key fingerprint, select **Accept BMC server's certificate and SFTP/HTTPS server's key fingerprint by default**, and click **Next**.

Step 4. In the Task window, select **BIOS configuration**, and click **Next**.

Step 5. In the Configuration Mode window, select **Common BIOS Configuration** or **Import BIOS Configuration File**, and click **Next**.

Step 6. Do one of the following:

- If **Import BIOS configuration File** is selected in the previous step, skip this step.
- If **Common BIOS Configuration** is selected in the previous step, select one or more current values, and click **Next**.

Step 7. In the BIOS Change View window, check or remove the values and click **Next**.

Step 8. In the Export BIOS Configuration window, export the configuration as a file. Specify the exported file location, and click **Next**.

Step 9. In the Running Configuration window, select **Restart Manually** or **Restart Immediately**, and click **Start**. After the task is finished, click **Next**.

Step 10. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring BIOS for multiple remote servers

The UpdateXpress application supports to configure the BIOS settings for multiple remote servers in batch.

Prerequisite:

The multi-configuration function for the remote server is only supported in the ThinkServer/WenTian servers. For details of supported operating systems, see **ThinkServer and WenTian series** in "Supported operating systems" on page 7.

To configure BIOS, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Multi-server Management**, and click **Next**.

Step 4. In the Multi-server Management window, do one or more of the following:

- To add new servers into server pool, select **+ Add new servers**. In the Add new servers window, do one of the following:
  - Select **IP range**, input the IP address range and click **Discover**.
  - Select **Discover by SSDP**, select the target adapter and click **Discover**.
- To remove the server from the Server Pool list, select one or more target servers, and click **Action → Remove Selected**.

- To verify whether the user name and password are correct for the server, select one or more target servers, and click **Action → Scan Selected**.
- To export the Server Pool list, select one or more target servers, click **Action → Export**.

  Note: By default, the Server Pool list will be saved in the JSON file. Users can also select the CSV and XLS format.
- To import the Server Pool list to other server, select one or more target servers from the list, click **Action → Import** and select the target JSON file.
- To change the password of the server, select one or more target servers, click **Action → Change IP and Password**. On the Change IP and Password page, do one of the following:
  - To change the password for single server, input the new user name and password, and click **Execute**. The new user name and password will be automatically added to the drop-down list.
  - To change the password for multiple servers, click **Export**, modify the password in the exported CSV file, and save the file. Go back to the Change IP and Password page, click **Import** to add the CSV file, and click **Execute**.
  - To view the details of each server, click ⌄ of the target server.

  Note: The user role of **USERID** is **Administrator**, which cannot be changed.
- To use common BMC credentials for management, select **Input the common BMC credentials -**, input user name and password.

Step 5. Go back to the Multi-server Management window, click **Next**, a message will be prompted to remind users to confirm whether the certificate should be updated. Click **Accept** to update the certificate.

Note: If users log in for the first time or the password is expired, change the password in the Change password window.

Step 6. In the Task window, select **BIOS configuration**, and click **Next**.

Note: This BIOS configuration function is only supported in the severs with the same machine types.

Step 7. In the Configuration Mode window, select **Common BIOS Configuration** or **Import BIOS Configuration File**, and click **Next**.

Step 8. Do one of the following:

- If **Import BIOS configuration File** is selected in the previous step, skip this step.
- If **Common BIOS Configuration** is selected in the previous step, select one or more current values, and click **Next**.

Step 9. In the BIOS Change View window, confirm the modified BIOS settings, and click **Next**.

Step 10. In the Export BIOS Configuration window, export the configuration as a file. Specify the exported file location, and click **Next**.

Step 11. In the Running Configuration window, select **Restart Manually** or **Restart Immediately**, and click **Start**. After the task is finished, click **Next**.

Step 12. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring RAID array for a remote server

The UpdateXpress application can do some RAID configuration for a remote server, such as collecting RAID information, creating RAID array, configuring disk status and clearing the configuration of a controller.

Prerequisite:

The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.

To configure RAID array, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**. When a window displaying the related information pops up, click **OK**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate and SFTP/HTTPS server key fingerprint, select **Accept BMC server's certificate and SFTP/HTTPS server's key fingerprint by default**, and click **Next**.

Step 4. In the Task window, select **Remote RAID Configuration** or **Perform updating on target server**, or both items, and click **Next**.

Step 5. In the RAID Configuration window, UpdateXpress will first collect RAID information of the remote server. After it finishes collecting, RAID information will be displayed in the window.

- To clear the configuration of a controller, click **Clear Controller**.
- To change drive status to JBOD, click **Make JBOD**.
- To change drive status to Unconfigured GOOD, click **Make Good**.

Step 6. In the RAID Configuration window, to create array for controller, click **Create Array**.

a. In the wizard window, select RAID level, add spans, members and hot spares for the array, and create volumes and set disk parameters.

b. When the summary information is displayed, click **Create** to start creating storage array.

c. After the process is completed, click **Collect** or **Refresh** to collect RAID information again.

d. Click **Next** if there is no other action needed.

Step 7. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring BMC

Configuring BMC for a remote server

The UpdateXpress application supports to configure the BMC settings for a remote server.

Prerequisite:

The BMC configuration function for the remote server is only supported in the ThinkServer/WenTian servers. For details of supported operating systems, see "Supported operating systems" on page 7.

To configure BMC, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate and SFTP/HTTPS server key fingerprint, select **Accept BMC server's certificate and SFTP/HTTPS server's key fingerprint by default**, and click **Next**.

Step 4. In the Task window, select **BMC configuration**, and click **Next**.

Step 5. In the Configuration Mode window, select one of the following:
- **Common BMC Configuration → Next**
- **Import BMC Configuration File → Select file → Next**

Step 6. In the BMC configuration window, do one of the following:
- If **Common BMC Configuration** is selected in the previous step, select one or more current values, and click **Next**.
- If **Import BMC Configuration File** is selected in the previous step, skip this step.

Step 7. In the BMC Change View window, check or remove the values and click **Next**.

Step 8. In the Export BMC Configuration window, export the configuration as a file. Specify the exported file location, and click **Next**.

Step 9. In the BMC Execute window, click **Execute → Next**.

Step 10. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring BMC for multiple remote servers

The UpdateXpress application supports to configure the BMC settings for multiple remote servers in batch.

Prerequisite:

The multi-configuration function for the remote server is only supported in the ThinkServer/WenTian servers. For details of supported operating systems, see **ThinkServer and WenTian series** in "Supported operating systems" on page 7.

To configure BMC, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Multi-server Management**, and click **Next**.

Step 4. In the Multi-server Management window, do one or more of the following:
- To add new servers into server pool, select **+ Add new servers**. In the Add new servers window, do one of the following:
  - Select **IP range**, input the IP address range and click **Discover**.
  - Select **Discover by SSDP**, select the target adapter and click **Discover**.
- To remove the server from the Server Pool list, select one or more target servers, and click **Action → Remove Selected**.
- To verify whether the user name and password are correct for the server, select one or more target servers, and click **Action → Scan Selected**.
- To export the Server Pool list, select one or more target servers, click **Action → Export**.

  Note: By default, the Server Pool list will be saved in the JSON file. Users can also select the CSV and XLS format.
- To import the Server Pool list to other server, select one or more target servers from the list, click **Action → Import** and select the target JSON file.

- To change the password of the server, select one or more target servers, click **Action → Change IP and Password**. On the Change IP and Password page, do one of the following:
  - To change the password for single server, input the new user name and password, and click **Execute**. The new user name and password will be automatically added to the drop-down list.
  - To change the password for multiple servers, click **Export**, modify the password in the exported CSV file, and save the file. Go back to the Change IP and Password page, click **Import** to add the CSV file, and click **Execute**.
  - To view the details of each server, click ﹀ of the target server.

  Note: The user role of **USERID** is **Administrator**, which cannot be changed.
- To use common BMC credentials for management, select **Input the common BMC credentials -**, input user name and password.

Step 5. Go back to the Multi-server Management window, click **Next**, a message will be prompted to remind users to confirm whether the certificate should be updated. Click **Accept** to update the certificate.

Note: If users log in for the first time or the password is expired, change the password in the Change password window.

Step 6. In the Task window, select **BMC configuration**, and click **Next**.

Note: This BMC configuration function is only supported in the severs with the same machine types.

Step 7. In the Configuration Mode window, select one of the following:
- **Common BMC Configuration → Next**
- **Import BMC Configuration File → Select file → Next**

Step 8. In the BMC configuration window, do one of the following:
- If **Common BMC Configuration** is selected in the previous step, select one or more current values, and click **Next**.
- If **Import BMC Configuration File** is selected in the previous step, skip this step.

Step 9. In the BMC Change View window, confirm the modified BMC settings, and click **Next**.

Step 10. In the Export BMC Configuration window, export the configuration as a file. Specify the exported file location, and click **Next**.

Step 11. In the BMC Execute window, click **Execute → Next**.

Step 12. In the Finish window, click the log to check the updates, and click **Close** to exit.

Collecting logs

Collecting logs for a remote server

The UpdateXpress application supports to collect logs for a remote server.

Prerequisite:

The collection function for a remote server is only supported on ThinkServer servers/WenTian servers. For details of supported operating systems, see "Supported operating systems" on page 7.

To collect logs, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate and SFTP/HTTPS server key fingerprint, select **Accept BMC server's certificate and SFTP/HTTPS server's key fingerprint by default**, and click **Next**.

Step 4. In the Task window, select **Collect Log**, and click **Next**.

Step 5. In the Log Collection Mode window, select **Collect BMC Log** or **Collect FFDC Log**, or both of them, and click **Next**.

Step 6. In Log Collection Result window, check the results, and click **Next**.

Step 7. In the Finish window, click the log to check the updates, and click **Close** to exit.

Collecting logs for multiple remote servers

The UpdateXpress application supports to collect logs for the remote servers in batch.

Prerequisite:

The multi-collection function for the remote server is only supported in the ThinkServer/WenTian servers. For details of supported operating systems, see **ThinkServer and WenTian series** in "Supported operating systems" on page 7.

To collect logs, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Multi-server Management**, and click **Next**.

Step 4. In the Multi-server Management window, do one or more of the following:

- To add new servers into server pool, select **+ Add new servers**. In the Add new servers window, do one of the following:
  - Select **IP range**, input the IP address range and click **Discover**.
  - Select **Discover by SSDP**, select the target adapter and click **Discover**.
- To remove the server from the Server Pool list, select one or more target servers, and click **Action → Remove Selected**.
- To verify whether the user name and password are correct for the server, select one or more target servers, and click **Action → Scan Selected**.
- To export the Server Pool list, select one or more target servers, click **Action → Export**.

  Note: By default, the Server Pool list will be saved in the JSON file. Users can also select the CSV and XLS format.
- To import the Server Pool list to other server, select one or more target servers from the list, click **Action → Import** and select the target JSON file.
- To change the password of the server, select one or more target servers, click **Action → Change IP and Password**. On the Change IP and Password page, do one of the following:
  - To change the password for single server, input the new user name and password, and click **Execute**. The new user name and password will be automatically added to the drop-down list.

  - To change the password for multiple servers, click **Export**, modify the password in the exported CSV file, and save the file. Go back to the Change IP and Password page, click **Import** to add the CSV file, and click **Execute**.
  - To view the details of each server, click ⌄ of the target server.

  Note: The user role of **USERID** is **Administrator**, which cannot be changed.
- To use common BMC credentials for management, select **Input the common BMC credentials -**, input user name and password.

Step 5. Go back to the Multi-server Management window, click **Next**, a message will be prompted to remind users to confirm whether the certificate should be updated. Click **Accept** to update the certificate.

Note: If users log in for the first time or the password is expired, change the password in the Change password window.

Step 6. In the Task window, select **Collect Log**, and click **Next**.

Step 7. In the Log Collection Mode window, select **Collect BMC Log** or **Collect FFDC Log** or both of them, specify the log output directory, and click **Next**.

Step 8. In the Log Collection Result window,check the results, and click **Next**.

Step 9. In the Finish window, click the log to check the updates, and click **Close** to exit.

Managing system configuration

Backing up system configuration

The UpdateXpress application can backup the system configuration to the external file, including hardware and firmware inventory, VPD, FoD license.

Prerequisite:
- The UpdateXpress application is running on a local machine to be updated.
- The machine is running a supported operating system. For details of supported operating systems, see “Supported operating systems” on page 7.

To back up the system configuration, do the following:

Step 1. Launch the UpdateXpress application. See “Launching the UpdateXpress application” on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.
- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If not checking the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Backup System Configuration** and click **Next**.

Step 5. In the Backup System Configuration Setting page, do the following:

a. Click **Browse** to select the backup file location. Users can also use the default location.

b. Select one or more backup items.

Note: If **Firmware Configuration in XCC and UEFI** or **SED Authentication Key** is selected, input the password twice, and record the password in a safe place.

c. Click **Next**, and wait for several minutes depending on your server configuration.

d. After the process is completed, click **Next**.

Step 6. In the Finish window, click the log to check the updates, and click **Close** to exit.

After you finish

Restore the system configuration. See "Restoring system configuration" on page 32.

Restoring system configuration

The UpdateXpress application can restore system configuration to the new servers.

Prerequisite:

- The UpdateXpress application is running on a local machine to be updated.
- The machine is running a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- Back up the system configuration. See "Backing up system configuration" on page 31.

To restore the system configuration, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If not checking the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Restore System Configuration** and click **Next**.

Step 5. In the Restore System Configuration Setting page, do the following:

a. Click **Select file...** to select the backup file. Usually the backup file is in the default location.

b. Click **Load backup file**, select one or more target items.

c. Click **Next**, and wait for several minutes depending on your server configuration.

d. After the process is completed, click **Next**.

Step 6. In the Finish window, click the log to check the updates, and click **Close** to exit.

ThinkEdge sever security features

Claiming server in ThinkShield Portal

The ThinkEdge server ownership can be claimed in Lenovo ThinkShield Key Vault Portal, and then UpdateXpress can activate the locked-down server through the Portal.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- This function is only supported in the ThinkEdge servers. For details of supported servers, see the ThinkEdge series in "Supported server models" on page 5.

To claim the server in ThinkShield Portal, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security features on ThinkEdge server**, and click **Next**.

Step 5. In the ThinkEdge Server Security Features window, select **Claim server in ThinkShield Portal** and click **Next**.

Step 6. In the Internet Access window, do one of the following:

- If users have no special requirement for security access, click **Test Connection** to check the network connection of the target URL, and click **Next**.
- If users have more security concerns, configure one or more of the following and click **Test Connection**:
  - **Proxy server**: Access to network through an HTTP/HTTPS proxy.
    1. Select **Proxy Server**, and complete the following fields:

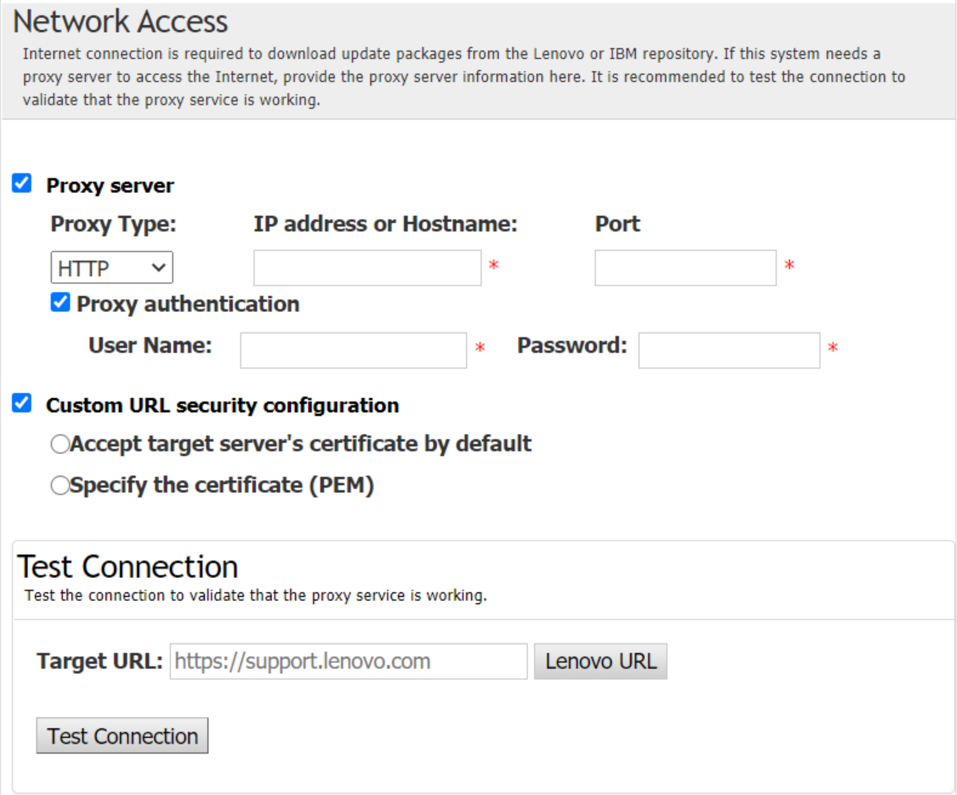
Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

    2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

  - **Custom URL security configuration**: Access to network through a reverse proxy.

    Select one of the following:
    - Accept target server's certificate by default
    - Specify the certificate (PEM)



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ Proxy server

Proxy Type: HTTP

☑ Proxy authentication

☑ Custom URL security configuration

○ Accept target server's certificate by default

○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 7. In the Claim Server window, input the organization ID, user name, and password of the ThinkShield Key Vault Portal, and click **Claim**.

Step 8. In the Finish window, click the log to check the updates, and click **Close** to exit.

Configuring security sensors

The ThinkEdge servers is equipped with the security sensors to detect tamper event. UpdateXpress supports to enable, disable, and modify the threshold of the motion detection sensor and chassis intrusion sensor.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- This function is only supported in the ThinkEdge servers. For details of supported servers, see the ThinkEdge series in "Supported server models" on page 5.

To configure the security sensors, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security features on ThinkEdge server**, and click **Next**.

Step 5. In the ThinkEdge Server Security Features window, select **Configure Security Sensors** and click **Next**.

Step 6. In the Configure Security Sensors window, do one or more of the following, and click **Next**.

- To enable or disable **Motion Detection** or **Chassis Intrusion Detection**, select the options from the drop-down list or click the switch button to toggle the status.

  Note: In case of data loss, it is recommended to backup AK before selecting any items.
- To reset the step count for the motion detection, click **Reset Step Counter**. UpdateXpress will reset the step count to 0.
- To change threshold steps for locking down the motion detection, select the target step level in **Threshold To Lockdown**.

  Note: The ThinkEdge server will be locked down once the tamper event is detected by the security sensor.

Step 7. In the Finish window, click the log to check the updates, and click **Close** to exit.

Managing SED authentication key

The ThinkEdge servers provides the access to the Self-Encrypting Drive(SED) using the authentication key. UpdateXpress application supports to manage the SED Authentication Key (AK), including generate, backup, and recover.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- This function is only supported when the ThinkEdge server is unlocked. For details of supported servers, see the ThinkEdge series in "Supported server models" on page 5.

To manage the SED authentication key, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security features on ThinkEdge server**, and click **Next**.

Step 5. In the ThinkEdge Server Security Features window, select **Manage the SED authentication key** and click **Next**.

Step 6. In the SED Authentication Key (AK) Management window, do one or more of the following:

- To generate the SED AK, select **Enable SED Encryption** when SED AK is disabled, or select **Change the SED AK** when SED AK is enabled. Select the target method from the **Method** drop-down list, and click **Regenerate**.

  Note: It's recommended to back up AK in case of data loss. Users can only select other options after backing up AK.

- To back up the SED AK, select **Back up the SED AK**, input the location and password of the backup file, and click **Start**. UpdateXpress will save the backup file containing the SED AK information.
- To recover the SED AK, select **Recover the SED AK**, do one of the following:
  - To recover by using the backup file, select **Recover SED AK from Backup file** from the **Method** drop-down list, click **Browse** to select the backup file, input the password, and click **Start Restore**.
  - To recover by using passphrase, select **Recover SED AK using Passphrase** from the **Method** drop-down list, input the passphrase, and click **Start Restore**.

Step 7. In the Finish window, click the log to check the updates, and click **Close** to exit.

Upgrading lockdown control mode

The ThinkEdge server is equipped with the security sensors to detect tamper event, which will also lock down the server in the tamper detection. UpdateXpress supports to upgrade the server lockdown control mode from activating server through XClarity Controller to managing the server through ThinkShield Portal.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- This function is only supported in the ThinkEdge servers. For details of supported servers, see the ThinkEdge series in "Supported server models" on page 5.

To upgrade the lockdown control mode, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security features on ThinkEdge server**, and click **Next**.

Step 5. In the ThinkEdge Server Security Features window, select **System Lockdown Control**, click **Next**, select one of the following options to claim or not claim the ownership of the server to ThinkShield Key Valut Portal, and click **Next** again.

- Select **Yes, I want to claim the server now**, go to Step 6.
- Select **No, I want to proceed without claiming server in ThinkShield Key Vault Portal**, go to Step 8.

Step 6. In the Internet Access window, do one of the following:

- If users have no special requirement for security access, click **Test Connection** to check the network connection of the target URL, and click **Next**.
- If users have more security concerns, configure one or more of the following and click **Test Connection**:
  - **Proxy server**: Access to network through an HTTP/HTTPS proxy.
    1. Select **Proxy Server**, and complete the following fields:

Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

– **Custom URL security configuration**: Access to network through a reverse proxy.

  Select one of the following:
  – Accept target server's certificate by default
  – Specify the certificate (PEM)

Step 7. In the Validate ThinkShield Portal Account window, input the organization ID, user name, and password of the ThinkShield Key Vault Portal, and click **Validate**. After the verification is completed, click **Next**.

Note: The information input should be valid; otherwise, the **Next** button will *not* be enabled.

Step 8. In the System Lockdown Control window, manually input **YES**, and click **OK**. After upgrade process is completed, click **Next**.

Step 9. In the Finish window, click the log to check the updates, and click **Close** to exit.

Activating the server in lockdown mode

The ThinkEdge server is equipped with the security sensors to detect tamper event, which will also lock down the server in the tamper detection. UpdateXpress supports to activate the lock-down server through ThinkShield Key Vault Portal or XClarity Controller.

Prerequisite:

- The UpdateXpress application is running on a server installed with a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.
- This function is only supported in the ThinkEdge servers. For details of supported servers, see the ThinkEdge series in "Supported server models" on page 5.

To activate the server in lockdown mode, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If users are not intended to check the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security features on ThinkEdge server**, and click **Next**.

Step 5. In the ThinkEdge Server Security Features window, select **Activate server with ThinkShield Portal** and click **Next**.

Note: The default system lockdown control is XClarity Controller managed. When the lockdown control is ThinkShield portal managed, users can only activate the server in locked down mode after being authenticated by ThinkShield Key Vault portal.

Step 6. In the Internet Access window, if users have no special requirement for security access, click **Test Connection** to check the network connection of the target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, configure **Proxy server** and/or **Custom URL security configuration** depending on the security requirements as follows:

- **Proxy server**
  1. Select **Proxy Server** if users require an HTTP/HTTPS proxy to connect to the Web, and complete the following fields:

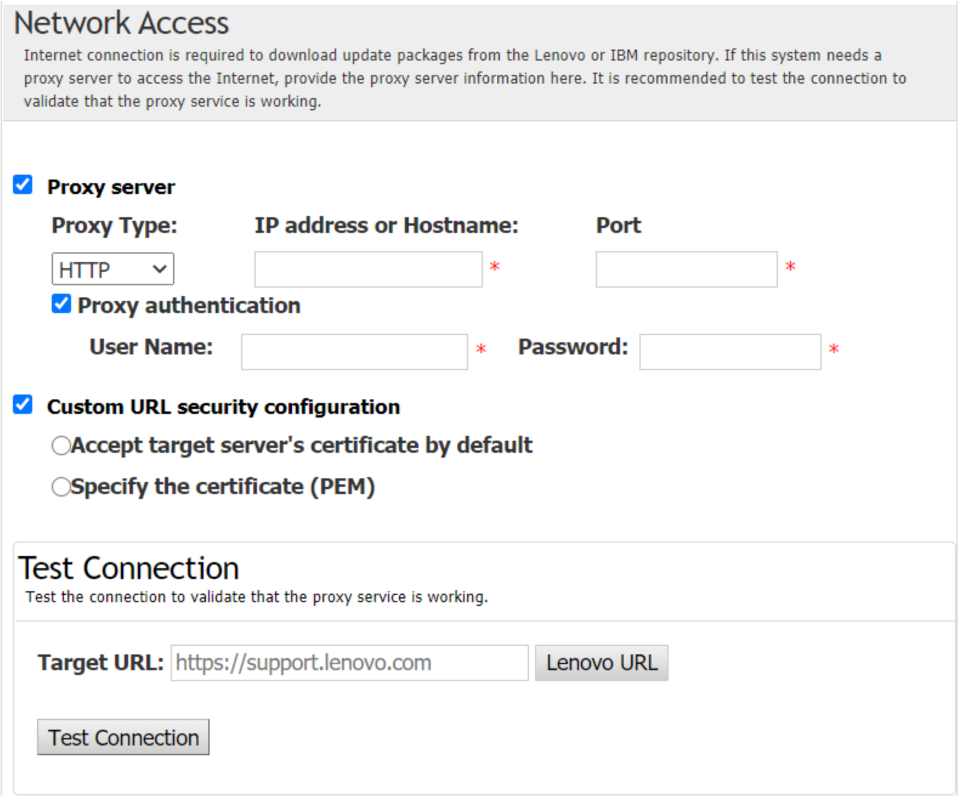
Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

  2. Select **Proxy authentication** if credentials must be specified to authenticate to the proxy server, and complete the following fields:

User Name	The user name for authenticating to the proxy server.
Password	The password for the specified user name.

- **Custom URL security configuration**

  Select **Custom URL security configuration** if users require a reverse proxy, and select one of the following options:
  - **Accept target server's certificate by default**
  - **Specify the certificate (PEM)**



Network Access

Internet connection is required to download update packages from the Lenovo or IBM repository. If this system needs a proxy server to access the Internet, provide the proxy server information here. It is recommended to test the connection to validate that the proxy service is working.

☑ Proxy server

Proxy Type: HTTP
IP address or Hostname: *
Port *

☑ Proxy authentication

User Name: * Password: *

☑ Custom URL security configuration

○ Accept target server's certificate by default
○ Specify the certificate (PEM)

Test Connection

Test the connection to validate that the proxy service is working.

Target URL: https://support.lenovo.com

Step 7. In the Activate Server window, input the ThinkShield Key Vault Portal organization ID, user name, and password, and click **Activate**. After the activation process is completed, click **Next**.

Note: If the sever is managed by XClarity Controller, users *don't* need to input the information of ThinkShield Key Vault Portal.

Step 8. In the Finish window, click the log to check the updates, and click **Close** to exit.

Updating public key on ThinkEdge servers

The UpdateXpress application can update the public key for the current system board on ThinkEdge servers.

Prerequisite:

- The UpdateXpress application is running on a local machine to be updated.
- The machine is running a supported operating system. For details of supported operating systems, see "Supported operating systems" on page 7.

To update public key on ThinkEdge servers, do the following:

Step 1. Launch the UpdateXpress application. See "Launching the UpdateXpress application" on page 9.

Step 2. In the Welcome window, click **Next**.

Step 3. In the Target Server window, select **Manage the remote server**, input the following information, and click **Next**.

- **IP address or Host name**: BMC IP address or host name of the target system.
- **User Name**: BMC user name of the target system.
- **Password**: BMC password of the target system.
- **Port**: BMC CIM or RSET port number. If users do not input, the default port is used.

Note: If not checking the BMC server certificate, select **Accept BMC server's certificate by default**, and click **Next**.

Step 4. In the Task window, select **Configure security feature on ThinkEdge server** and click **Next**.

Step 5. In the ThinkEdge Server security Feature window, read the ThinkEdge security concepts, select **I have read and understand these concepts → Update Server's Public Key**, and click **Next**.

Step 6. On the Internet Access page, if users have no special requirement for security access, click **Test Connection** to check the network connection of the Target URL, and click **Next**.
If users have more security concerns, before clicking **Test Connection**, select **Proxy Server**, select **HTTP** from the **Proxy Type** drop-down list, and complete the following fields:

Proxy Type	The proxy type of the proxy server.
IP address or Hostname	The host name, IP address, or domain name of the proxy server.
Port	The port number of the proxy server.

Step 7. In the Update Server's Public Key window, input the following information, and click **Update**.

- **Organization ID**: Organization ID of users.
- **User Name**: ThinkShield user name of the target system.
- **Password**: ThinkShield password of the target system.
- **Machine Type**: Machine type of the target system.
- **Serial Number**: Serial number of the target system.
- **Active Code (old system)**: Active code of the previous system.
- **Public Key (new system)**: Public key of the new system.

Step 8. In the Finish window, click the log to check the updates, and click **Close** to exit.

Chapter 4. Troubleshooting

This chapter provides information about what to do if users experience a problem with the UpdateXpress application.

Limitations and problems

- **When using UpdateXpress to configure BIOS attributes CPU*_Disablebitmap* (* means index 0, 1 etc) on ThinkSystem WenTian G5 series servers, the large integer number might be imprecise. For example, the value 9223372036854775807 might be displayed as 922337036854776000 on UpdateXpress GUI, which will report failure on UpdateXpress.**

  In this case, users can use OneCLI to configure the BIOS settings. For example, run the command `OneCli.exe config set BIOS. CPU1_DisableBitmap 9223372036854775807 --bmc USERNAME:PASSWORD@IPAddress`.
- **On the Multi-server Management page, when clicking Action → Export to export the Server Pool list, the selected file type (T) is not applied to the file name extension (N).**

  In this case, users should manually input the file name extension.
- **UpdateXpress fails to set the out-of-box driver as default on some devices when upgrading from in-box driver to out-of-box one.**

  UpdateXpress calls OneCLI to perform update task. OneCLI could not compare the inconsistent versions of in-box driver and out-of-box driver and select the correct version for update. In this case, UpdateXpress could not select the out-of-box driver for update, and users should manually select the target out-of-box driver to override the in-box driver.
- **All UpdateXpress paths must use standard English-language alphanumeric characters.**

  All UpdateXpress paths must use standard English-language alphanumeric characters and OS permitted special characters. The non-English-language characters are not permitted.

Workarounds

There are presently no known problems or workarounds for the UpdateXpress application.

Coexistence and compatibility

The UpdateXpress application builds on OneCLI, but has no interactions with other programs on the system. Do not run the UpdateXpress application and OneCLI at the same time.

Appendix A. Accessibility features for UpdateXpress

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information, technology, and products successfully.

The following list includes the major accessibility features in the UpdateXpress application:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers

Keyboard navigation

Users can use the keyboard to navigate through the graphical user interface (GUI).

The following keyboard shortcuts are applicable on both the Windows and Linux operating systems.

Shortcut	Function
Tab	Go to the next control.
Shift+Tab	Move to the previous control.
Left arrow	Move back one character.
Right arrow	Move forward one character.
Backspace	Delete the character to the left of the cursor.
Delete	Delete the character under the cursor.
Up arrow	Move focus and selection upwards through the radio button.
Down arrow	Move focus and selection downwards through the radio button.
Space	Select or clear an option.

Screen-reader technology

Screen-reader technologies are primarily focused on software program interfaces, help information systems, and various online documents. For additional information about screen readers, see the following:

- Using the JAWS screen reader:

  http://www.freedomscientific.com/Products/Blindness/JAWS
- Using the NVDA screen reader:

  http://www.nvaccess.org/

Lenovo and accessibility

For more information about the Lenovo commitment to accessibility, go to http://www.lenovo.com/lenovo/us/en/accessibility.html.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO, FLEX SYSTEM, SYSTEM X, and NEXTSCALE SYSTEM are trademarks of Lenovo. Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both. Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies. Linux is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.© 2024 Lenovo.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity might vary depending on operating environments.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products are provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Index

Lenovo