Lenovo

Enabling Intel SGX on Lenovo ThinkSystem V2 Servers

Introduces the Intel Software Guard Extensions security feature

Explains the designs of SGX on new ThinkSystem V2 two-socket servers

Describes the memory DIMM population requirements of SGX

Describes the steps for enabling SGX in Lenovo ThinkSystem UEFI Setup

Jason Liu

Blake Liu

Abstract

Intel Software Guard Extensions (Intel SGX) is an extension to the Intel processor architecture that provides new CPU instructions and platform enhancements to allows applications to create private areas to protect sensitive information. Sensitive information is protected even when attackers has full control of platform. Protection is achieved through the use of private regions of memory called enclaves.

Intel SGX has now been implemented in the 3rd generation Intel Xeon Scalable processors (formerly codenamed “Ice Lake”). This paper introduces the Intel SGX technology and explains the implementation of SGX on two-socket platforms. It also describes the UEFI configuration needed to enable this new secure feature on Lenovo ThinkSystem V2 servers.

This paper is for customers who wish to learn more about SGX and how to implement it on ThinkSystem servers. This paper assumes that the reader is familiar with ThinkSystem UEFI setup configuration.

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

http://lenovopress.com

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you’re there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction to Intel SGX

Intel Software Guard Extensions (Intel SGX) is an extension to Intel architecture that provides new CPU instructions and platform enhancements to allows applications to create private areas to protect sensitive information. Sensitive information is protected even when attackers has full control of platform. Protection is achieved through the use of private regions of memory called enclaves.

Intel SGX is a feature that was first implemented in Intel client platforms and single-socket Intel Xeon E3 processors, but has now been implemented in the 3rd generation Intel Xeon Scalable processors (formerly codenamed “Ice Lake”).

Intel SGX is available in the following ThinkSystem servers:

Servers with Intel Xeon E3-2100 and E3-2200 processors (high-end processor SKUs only):

- Lenovo ThinkSystem ST50
- Lenovo ThinkSystem ST250
- Lenovo ThinkSystem SR150
- Lenovo ThinkSystem SR250

- Servers with 3rd Gen Intel Xeon Scalable processors (all processor SKUs):
  - Lenovo ThinkSystem ST650 V2
  - Lenovo ThinkSystem SR630 V2
  - Lenovo ThinkSystem SR650 V2
  - Lenovo ThinkSystem SR670 V2
  - Lenovo ThinkSystem SD630 V2
  - Lenovo ThinkSystem SD650 V2
  - Lenovo ThinkSystem SD650-N V2
  - Lenovo ThinkSystem SN550 V2

This paper covers the implementation of Intel SGX on the ThinkSystem V2 servers with 3rd Gen Intel Xeon Scalable processors.

Figure 1 shows the key components of Intel SGX. The ThinkSystem server UEFI provides the SGX initialization and reserves a contiguous memory region for enclaves. Application can use enclaves for critical data protection.

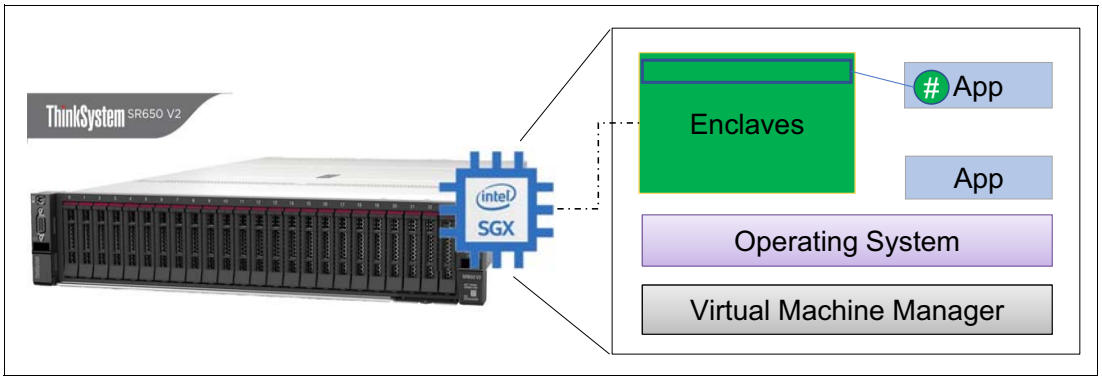

Figure 1 Applications using an SGX Enclave

Reserved Memory for SGX

The enclave region is allocated from special memory region in order to support SGX. ThinkSystem BIOS will reserve a contiguous memory region called the Processor Reserved Memory (PRM) in Processor Reserved Memory Range Registers (PRMRR).

An enclave is section of an application created from virtual address space of an application but located in secure part of physical memory referred to as Enclave Page Cache (EPC). EPC is part of PRM which is protected by Intel CPU via PRMRRs.

An application can create an enclave for its protected portion. Before the enclave is built, the enclave code and data are free for inspection and analysis. The protected portion is loaded into an enclave where its code and data is measured. Once the application's protected portion of the code and data are loaded into an enclave, memory access controls are in place to restrict access by external software. An enclave can prove its identity to a remote party and provide the necessary building-blocks for secure provisioning of keys and credentials. The application can also request an enclave-specific and platform-specific key that it can use to protect keys and data that it wishes to store outside the enclave.

The size of the SGX enclave is fixed but is different depending on the processor model. Sizes range from 8 GB to 512 GB per processor. For a 2-socket ThinkSystem server, if enough DDR memory is installed, the system BIOS can reserve between 16GB and 1TB based on processor model installed.

For the enclave size supported for each Intel processor model, see the Intel Xeon Scalable Processor Reference:

https://lenovopress.com/lp1262-intel-xeon-sp-processor-reference#term=SGX

Instructions of SGX

SGX feature need a new set of CPU instructions and mechanisms for memory accesses added to Intel Architecture processors. Intel SGX can encompass two collections of instruction extensions, referred to as SGX1 and SGX2.

The SGX1 extensions allow an application to instantiate a protected container, referred to as an enclave. The SGX2 extensions allow additional flexibility in runtime management of enclave resources and thread execution within an enclave. The 3rd Gen Intel Xeon Scalable processor family supports both SGX1 and SGX2 instruction extensions.

The enclave instructions available with Intel SGX are organized as leaf functions under three instruction mnemonics: ENCLS (ring 0), ENCLU (ring 3), and ENCLV (VT root mode). Table 1 provides a summary of the Supervisor (ring 0) and User (ring 3) instruction leaves that are available in the initial implementation of Intel SGX.

Table 1 Supervisor and User Mode Enclave Instruction Leaf Functions of SGX1[1]

Supervisor Instruction	Description	User Instruction	Description
ENCLS[EADD]	Add an EPC page to an enclave.	ENCLU[EENTER]	Enter an enclave.
ENCLS[EBLOCK]	Block an EPC page.	ENCLU[EEXIT]	Exit an enclave.
ENCLS[ECREATE]	Create an enclave.	ENCLU[EGETKEY]	Create a cryptographic key.
ENCLS[EDBGRD]	Read data from a debug enclave by debugger.	ENCLU[EREPORT]	Create a cryptographic report.
ENCLS[EDBGWR]	Write data into a debug enclave by debugger.	ENCLU[ERESUME]	Re-enter an enclave.
ENCLS[EEXTEND]	Extend EPC page measurement.		
ENCLS[EINIT]	Initialize an enclave.		
ENCLS[ELDB]	Load an EPC page in blocked state.		
ENCLS[ELDU]	Load an EPC page in unblocked state.		
ENCLS[EPA]	Add an EPC page to create a version array.		
ENCLS[EREMOVE]	Remove an EPC page from an enclave.		
ENCLS[ETRACK]	Activate EBLOCK checks.		
ENCLS[EWB]	Write back/invalidate an EPC page.		

Based on these instructions, OS/driver/application can create an enclave and initialize it and use for protected portions.

For more information, including details of these instructions, see Chapter 36 “Introduction to Intel Software Guard Extensions” of Intel 64 and IA-32 Architectures Software Developer’s Manual Volume 3:

https://software.intel.com/content/www/us/en/develop/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4.html

Enabling SGX on dual-socket servers

On single-socket platforms such as ThinkSystem ST50, ST250 and SR250, as well as client platforms using the Xeon E processors, Intel SGX functionality and security properties are provided completely by the one socket. Each socket ships with per-part unique hardware keys built into the processor. Intel SGX instructions allow enclaves to access keys derived from these hardware keys to help protect secrets or securely communicate between enclaves. Unique signing keys can also be derived. These keys are common across all logical processors on a single socket, thus, a key request will result in the same answer on all the virtual cores (threads) in the socket. Operating system schedulers rely on this coherency.

In order to keep the operating system side a simple design, Intel has designed a single coherent software environment on multi-socket platforms for enabling SGX. The server UEFI will perform Platform Establishment – the processor socket contains unique, per-part hardware keys, called the Intel SGX root keys, the UEFI will derive the common “platform”

[1] From https://software.intel.com/content/www/us/en/develop/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4.html

root keys, and store these platform keys in persistent storage (flash memory) to make sure these keys are still accessible after the platform is reset.

The implementation of Intel SGX is more complex with two-socket servers. Figure 2 shows Intel SGX data protection model when two sockets are used. UEFI will initialize a platform manifest containing the platform root keys along with the information on the sockets that participated in establishing these platform root keys. Each socket encrypts its own copy of the platform keys using its hardware keys, and this ensures that if any socket fails, the remaining sockets can still access the platform keys. Each processor can handle the its own enclaves in Processor Reserved Memory (PRM).

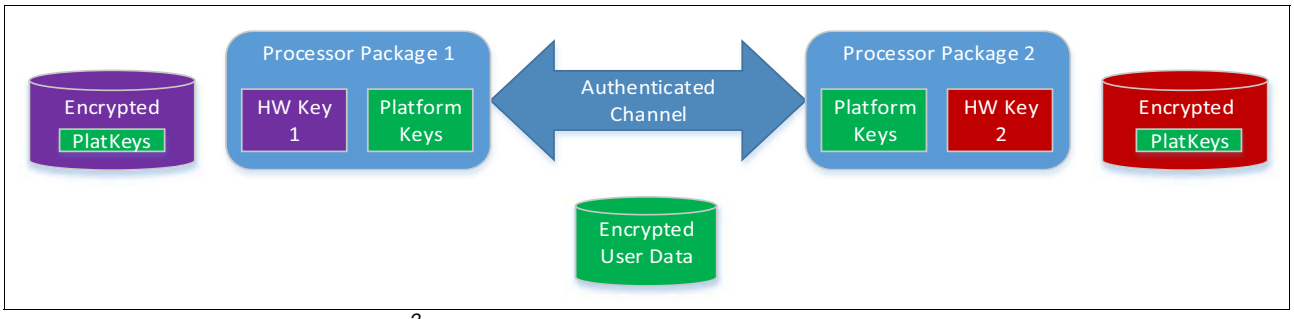

Figure 2 Multi-socket Intel SGX Keys[2]

Figure 3 shows one example of ThinkSystem SR650 V2, where each socket has 16x 16GB DIMMs for a total 512GB of memory with two processors, but the whole memory physical address range will be from 0 to 514GB because there is one 2GB hole in the system address space below 4GB. The processors each have a 64GB enclave size.

Intel SGX requires system memory to be configured as NUMA (Non-Uniform Memory Access) memory, thus each processor has its own consecutive memory space. SGX allocates its Processor Reserved Memory (PRM) which is configured into Processor Reserved Memory Range Registers (PRMRR).

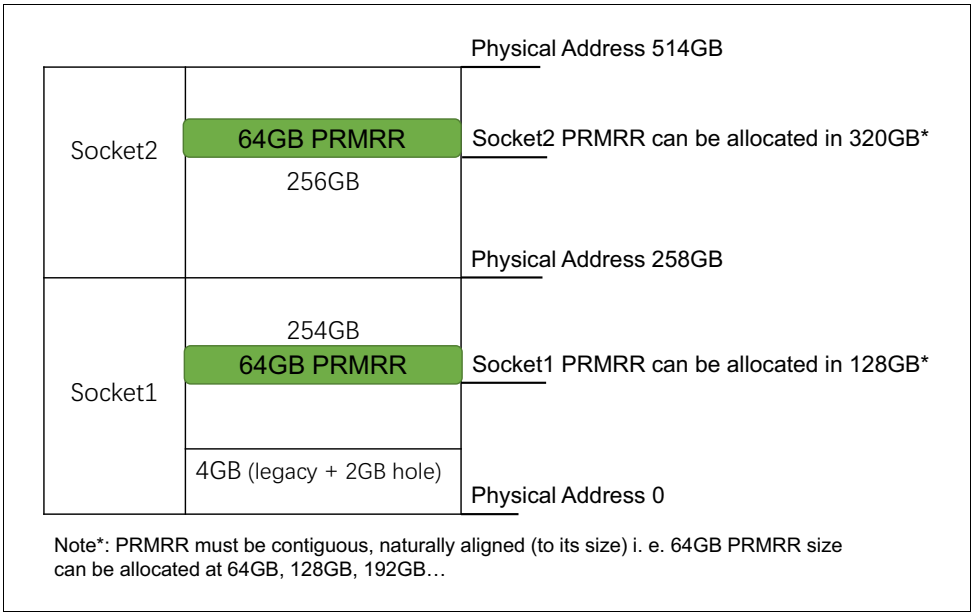

Figure 3 PRMRR Allocation Example in ThinkSystem

[2] From https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions/supporting-sgx-on-multi-socket-platforms.html

Memory DIMM population requirement

3rd Gen Intel Xeon Scalable processors have four Integrated Memory Controllers (iMC), and each iMC has two DDR channels and each channel supports two DDR4 DIMMs, so one processor can have a maximum of 16 DDR4 DIMMs. 3rd Gen Scalable processors only support SGX feature with specific DIMM configurations.

DIMM population requirements are as follows:

- Only configurations of 8 DIMMs, 12 DIMMs and 16 DIMMs are supported.
- Figure 4 shows the DIMM installation (that is, the exact DDR channels and slots of each processor) required to enable SGX.
- If different DIMMs are populated in the system, then the populated DIMMs must be symmetric between {iMC0, iMC1} and {iMC2, iMC3}, and the populated DIMMs must be identical between socket 1 and socket 2 if two processors are installed.
- Memory Mirroring is not supported and must be disabled.

IMC#	**IMC0**				**IMC1**				**IMC2**				**IMC3**			
Channel	Chann 0 (A)		Chann 1 (B)		Chann 0 (C)		Chann 1 (D)		Chann 0 (E)		Chann 1 (F)		Chann 0 (G)		Chann 1 (H)	
DDR4	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1
8	DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4	
12	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	
16	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

Figure 4 SGX Supported Memory Configuration

For the specific memory population rules to enable SGX on a ThinkSystem server, see the Setup Guide for the server, located in the Information Center:

https://thinksystem.lenovofiles.com/help/index.jsp

Enabling SGX in System Setup

By default, SGX is disabled on ThinkSystem servers. To enable SGX, perform the following steps:

1. Boot the server and press F1 when prompted to enter System Setup.
2. Configured the system so that memory is configured as NUMA and each processor has its own PRMRR and consecutive memory space. Select **System Settings** → **Processors** → **UMA-Based Clustering** and set it to **Disabled**.
3. Enable Intel Total Memory Encryption (TME). 3rd Gen Scalable processors require TME enabled for the use of SGX. Select **System Settings** → **Processors** → **Total Memory Encryption (TME)** and set it to **Enabled**.
4. Save the settings however you do not need to reboot at this stage.

> **Tip:** The SGX setting does not appear in the menu until you disable UMA-Based Clustering and then save the changes.

5. Enable SGX by selecting **System Settings** → **Processors** → **SW Guard Extension (SGX)** and set it to **Enabled**.

Figure 5 shows the settings on the Processors page in System Setup after SGX is enabled.

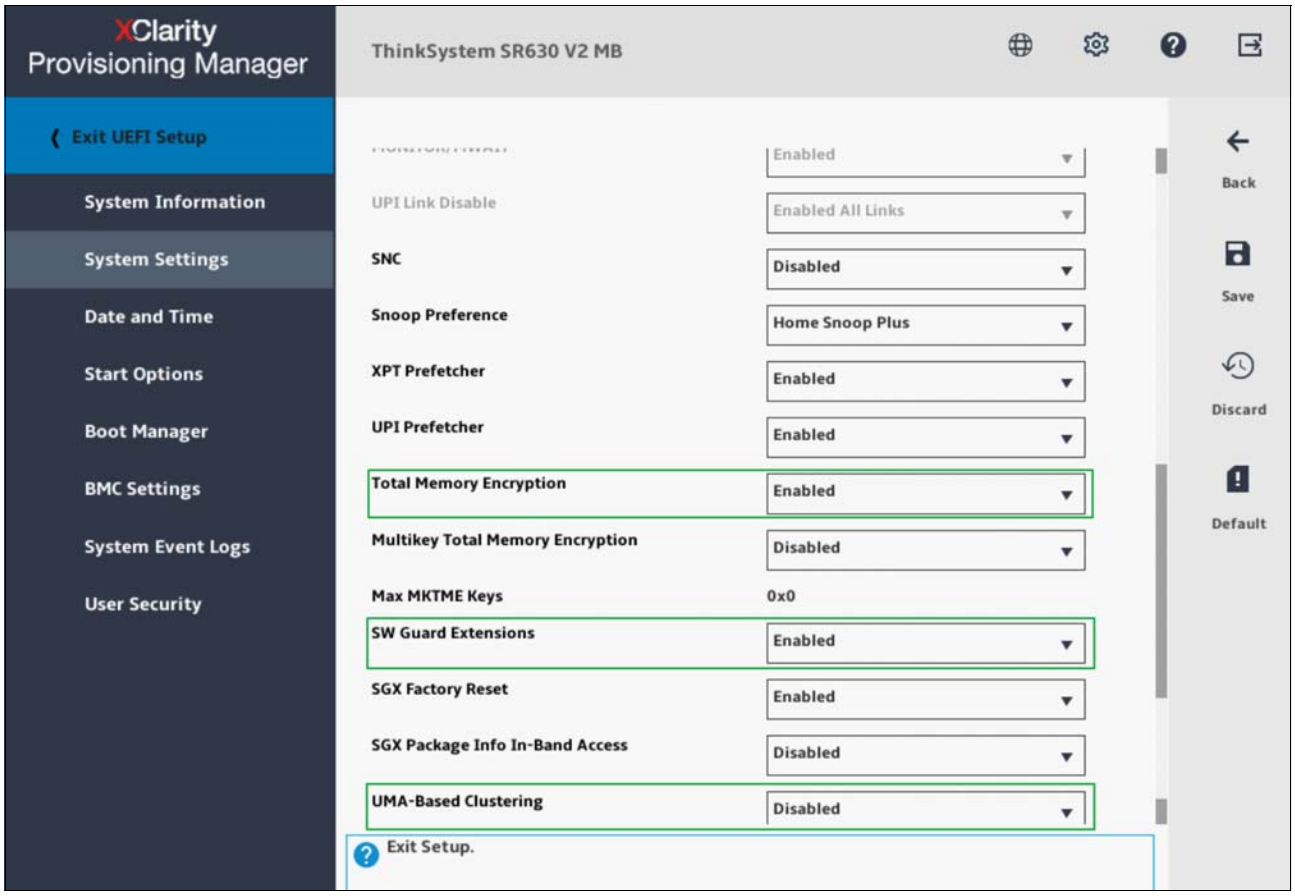

Figure 5 Processors UEFI Setup Page with SGX Enabled

6. Save the settings and reboot the system.
7. During the system reboot, ThinkSystem UEFI will perform an SGX initialization and enable the feature.

You can now use SGX feature in a supported operating system.

References

For more information, see the following documents:

- Intel SGX public web has more introduction:

  https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html

- Chapter 36 “Introduction to Intel ® Software Guard Extensions” of Intel® 64 and IA-32 Architectures Software Developer’s Manual Volume 3:

  https://software.intel.com/content/www/us/en/develop/download/intel-64-and-ia-32-architectures-sdm-combined-volumes-1-2a-2b-2c-2d-3a-3b-3c-3d-and-4.html

- Supporting Intel® SGX on Multi-Socket Platforms

  https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions/supporting-sgx-on-multi-socket-platforms.html

Authors

Jason Liu is a Principal Engineer and Senior UEFI Architect at Lenovo Infrastructure Solutions Group. Jason provides high-level infrastructure design support for Lenovo ThinkSystem UEFI firmware and leads the enabling, customization and innovation of new technologies into UEFI firmware. Jason also leads Reliability, Availability and Serviceability (RAS) architecture design and Secure feature design for ThinkSystem firmware.

Blake Liu is a Senior Engineer at Lenovo Infrastructure Solutions Group. Blake is a technical leader in UEFI Secure domain, responsible for secure feature design and implementation, and also leads PSIRT issue tracking and fixing for ThinkSystem UEFI firmware.

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.
1009 Think Place - Building One
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.

This document was created or updated on April 20, 2021.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp1471

Trademarks