



Lenovo Services Education

Introducing the Features on Demand technology

December 2016
Study guide

ES40610D

**This course is owned and published by
Lenovo Services Education.**

© Copyright Lenovo 2016

Lenovo
8001 Development Drive
Morrisville, North Carolina, 27560

Lenovo reserves the right to change product information and specifications at any time without notice. This publication might include technical inaccuracies or typographical errors. References herein to Lenovo products and services do not imply that Lenovo intends to make them available in all countries. Lenovo provides this publication as is, without warranty of any kind, either expressed or implied, including the implied warranties of merchantability or fitness for a particular purpose. Some jurisdictions do not allow disclaimer of expressed or implied warranties. Therefore, this disclaimer may not apply to you.

Data on competitive products is obtained from publicly obtained information and is subject to change without notice. Contact the manufacturer for the most recent information.

Lenovo and the Lenovo logo is a trademark or registered trademark of Lenovo Corporation or its subsidiaries in the United States, other countries, or both. Intel and the Intel logo is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States, other countries, or both. Other names and brands are the property of their respective owners.

The following terms are trademarks, registered trademarks, or service marks of Lenovo:

Access Connections, Active Protection System, Automated Solutions, Easy Eject Utility, Easy-Open Cover, IdeaCentre, IdeaPad, ImageUltra, Lenovo Care, Lenovo (logo), Lenovo, MaxBright, NetVista, New World. New Thinking, OneKey, PC As A Service, Rapid Restore, Remote Deployment Manager, Rescue and Recovery, ScrollPoint, Secure Data Disposal, Skylight, Software Delivery Center, System Information Gatherer, System Information Reporter, System Migration Assistant, System x, ThinkAccessories, ThinkCentre, ThinkDisk, ThinkDrive, ThinkLight, ThinkPad, ThinkPlus, ThinkScribe, ThinkServer, ThinkStation, ThinkStore, ThinkVantage, ThinkVision, ThinkWorld, TopSeller, TrackPoint, TransNote, UltraBase, UltraBay, UltraConnect, UltraNav, VeriFace.

For more information, go to: <http://www.lenovo.com/legal/copytrade.html>.

The terms listed for the following partners are the property of their respective owners:

[AMD](#)

[Intel](#)

[IBM](#)

[Microsoft](#)

[NVIDIA](#)

The content in this document is subject to the existing non-disclosure agreement held between Lenovo and its Authorized Service Providers.

Table of contents

Preface	4
Introducing the Features on Demand technology	4
Objectives	5
Introducing the Features on Demand technology	6
Overview	6
Key management system	11
Create a FoD account	11
Using the System x FoD Web site	12
Activating the FoD feature	13
Requesting an activation key.....	13
Retrieving history.....	17
Hardware replacement	18
Adapter mobility.....	19
Trial key.....	20
Retrieving an authorization code	21
User preferences	21
FoD activation key management through Advanced Setup Utility Overview	23
Advanced Setup Utility command syntax for keys	24
Key management on IMM device using Advanced Setup Utility.....	26
Key management on CMM device by using Advanced Setup Utility.....	27
Key management on IOM device by using Advanced Setup Utility	28
Acquire key from KMS using Advanced Setup Utility.....	29
FoD activation key management through DSA	30
FoD CLI support for portable DSA.....	30
FoD GUI support for embedded DSA Preboot	32
FoD support plan	41
Hints and tips	42
FoD servicer activities.....	44
FoD handling scope by SSRs	45
FoD key installation after hardware replacement.....	46
Preparation.....	46
Parts replacement (onsite)	49
Installation Steps (onsite)	49
Using the System Management Interface to Save and Restore FoD Files.....	51
Helpful links	53
Summary	54

Introducing the Features on Demand technology – Preface

Preface

Introducing the Features on Demand technology

This document may not be copied or sold, either in part or in whole, to non-Lenovo personnel.

Current release date: December 2016

Current release level: 4.0

The information in this publication is current as of the date of the latest revision and is subject to change at any time without notice.

To provide feedback or receive more information about this course, send an e-mail to: ServicesEdu@lenovo.com

Introducing the Features on Demand technology – Objectives

Objectives

After completing this course, you will be able to:

- Provide an overview of the Features on Demand technology.
- Explain how the key management works.
- Explain how the activation management utility works.
- Describe the activities that are required by the remote technical support agents.

Introducing the Features on Demand technology

Overview

Features on Demand (FoD) is a feature that is implemented in System x products with pre-built-in or preinstalled software and hardware features (software RAID, IMM2 Web interface, legacy hardware key for remote presence) that can be activated with proper activation keys. Users can customize and choose certain features to activate to meet their business needs. FoD handles everything from enabling and disabling features to validating the activation keys.

FoD provides factory and field upgrade support for firmware and software-activated optional function. Users can customize and choose certain features to activate to meet their business needs. The extended features include switches, chassis, systems, and options as following:

- Upgrading IMM2 to support remote presence or a Web interface
- Activating more Ethernet ports
- Activating FCoE and iSCSI on 10 Gb Ethernet ports
- Activating RAID 6 or other premium features

The common case for FoD activation is when the customer purchases features as part of a system purchase. The factory delivers preinstalled activation keys on the system and the feature functions are ready out-of-box without any customer action.

The customer must purchase an authorization code for the feature activation on the system type they are activating. The customer can redeem the authorization code for an activation key, install the activation key to the endpoint, and finally restart the system to activate the desired function.

The FoD key validation and storage is hosted on IMM2, management module, and switch firmware. FoD feature activation takes place within the software element that contains the feature's functional code (examples include the IMM, management module, switch firmware, and option card firmware). The IMM2 provides a repository and commands for software activation keys.

The activation can be done in-band or out-of-band on system endpoints. During activation, select the endpoint to be activated and connect to IBM to retrieve the activation key. Customers must replace failed components, including activation keys if the replacement involves replacing the main board where keys are stored.

Customers can restore functions with the same key whenever a replacement does not change the identity of the activated device. For replacements that involve a new device

Introducing the Features on Demand technology – Overview

identity to replace the failed one, KMS supports entitlement transfer to the new unit as part of the replacement and reactivation process.

Customers can perform an audit by checking the authorization code for activation information or the unique identifiers for entitlement.

Figure 1 shows the functionality of the FoD key with internal validation system. Tools that are used to work with FoD features and keys include:

- Key Generation Utility (KGU)
 - Utility to generate feature keys, only used by Lenovo manufacturing and KMS
- Advanced Settings Utility (ASU)
 - Utility to manage feature keys
 - Utility to acquire feature keys from KMS
- Dynamic System Analysis (DSA)
 - Utility to inventory and analyze features on a hardware
 - Provide advice to customers as to what features can be purchase
 - Help feature retrieval in the hardware replacement process

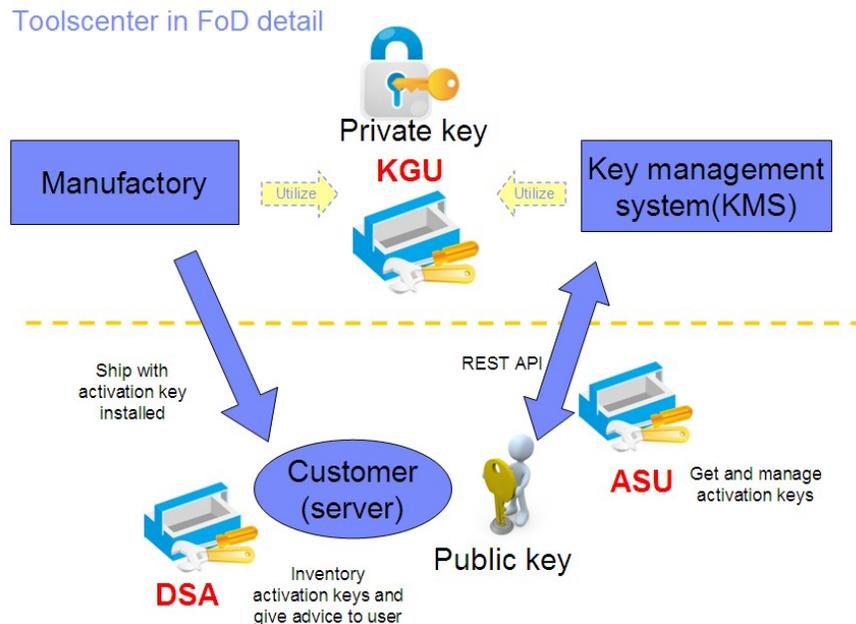


Figure 1: Functionality of the FoD Key with internal validation system

Figure 2 shows the pathways for storing keys and the relationship between the three key storage devices to the available interfaces.

Introducing the Features on Demand technology – Overview

Device and Feature support with FoD

HW category	Software feature type	Where to install the software key	How to install	Other FW involved
RAID upgrade	RAID 5,6; SW RAID, performance upgrade	IMM	Use IMM web or ASU to install	uEFI
IMM feature	Enable RP, Enable SP	IMM	Use IMM web or ASU to install	N/A
Other Vendor options (Emulex, etc)	Enable FCoE/iSCSI etc	IMM	Use IMM web or ASU to install	uEFI
Software Feature(*)	Enable software features	IMM (the one that installs software)	Use IMM web or ASU to install	N/A
CMM chassis level feature	Enable BOFM	CMM	Use CMM console or ASU to install	uEFI
IOM switches	Enable more ports	IOM	Use IOM console or ASU to install	N/A

Figure 2: Devices and pathways for storing keys

Introducing the Features on Demand technology – Overview

Table 1 provides descriptions for vocabularies that are mentioned throughout the course.

Table 1: Features on Demand vocabulary	
Vocabulary	Definitions
Activation key	A signed file that is validated by a key store; activates a specific function on a specific endpoint. Also known as a key.
Endpoint	A device that supports a FoD feature, such as IMM2 advanced, premium features, and software RAID.
Unique identifier	The unique identity of the endpoint that has a FoD feature to be activated. For example, machine type-serial number is the unique identifier for system features.
License	A signed document of entitlement that enumerates feature, quantity, and optional constraints for a licensed feature to be activated. The license is the right to enable a feature on a product or set of products.
License key	An object that acts as a proof of purchase for a FoD feature to enable that feature on a specific system instance.
Authorization code	<p>An encrypted string that is correlated with a license instance. Authorization codes are the input to the license key generation logic to properly create keys against a specific license.</p> <p>After a customer purchases a feature license for existing systems, the customer can ask for an authorization code from Lenovo sales focal and service.</p>
Unique ID	<p>A set of ID numbers that uniquely identifies a server system or server part.</p> <p>The unique ID is defined in an XML, indicating which unique ID is for each system or system parts that support FoD.</p> <p>A combination of machine type and serial number is used as system unique identifier.</p>

Introducing the Features on Demand technology – Overview

Table 2 provides descriptions for acronyms that are mentioned throughout the course.

Table 2: Features on Demand acronym definitions		
Acronym	Full name	Description
FoD	Features on Demand	Strategy and implementation on making some of the features chargeable.
KMS	Key Management System	An existing key generation and distribution system used today in the ISC and proposed for use as the fulfillment engine heart for FoD license keys.
IMM2	Integrated Management Module 2	Next generation service processor, version 2.
DSA	Dynamic System Analysis	System x ToolsCenter diagnostic tool.
ASU	Advanced settings utility	System x ToolsCenter configuration tool.
CIM	Common information model	An industry standard on modeling system management elements by DMTF (www.dmtf.org).
CMM	Chassis management module	Management module for chassis.
AMU	Activation management Utility	ToolsCenter tool for working with FoD keys.
KCS	Keyboard Controller Style	An interface often used between BMC and payload processor in the IPMI architecture.
IOM	I/O Module	Switches.

Introducing the Features on Demand technology – Key management system

Key management system

The FoD activation keys for servers are stored on the system board's IMM2. This is called the FoD key repository. If the system board is replaced, you need to reinstall all FoD keys.

It is important to first ensure that the Vital Product Data (VPD: machine type and serial number) of the server is applied to the new system board. The System Firmware update tool or ASU gives you this capability.

Most of the FoD activation keys are tied to VPD, so failure to reinstate these values prevents the FoD upgrades from being reapplied.

Create a FoD account

It is necessary to have or create a Lenovo FoD account before an authorization code can be used to obtain single or multiple activation keys. To register, follow the prompts on the FoD KMS Web site at <https://fod.lenovo.com/lkms/> as shown in **Figure 3**.

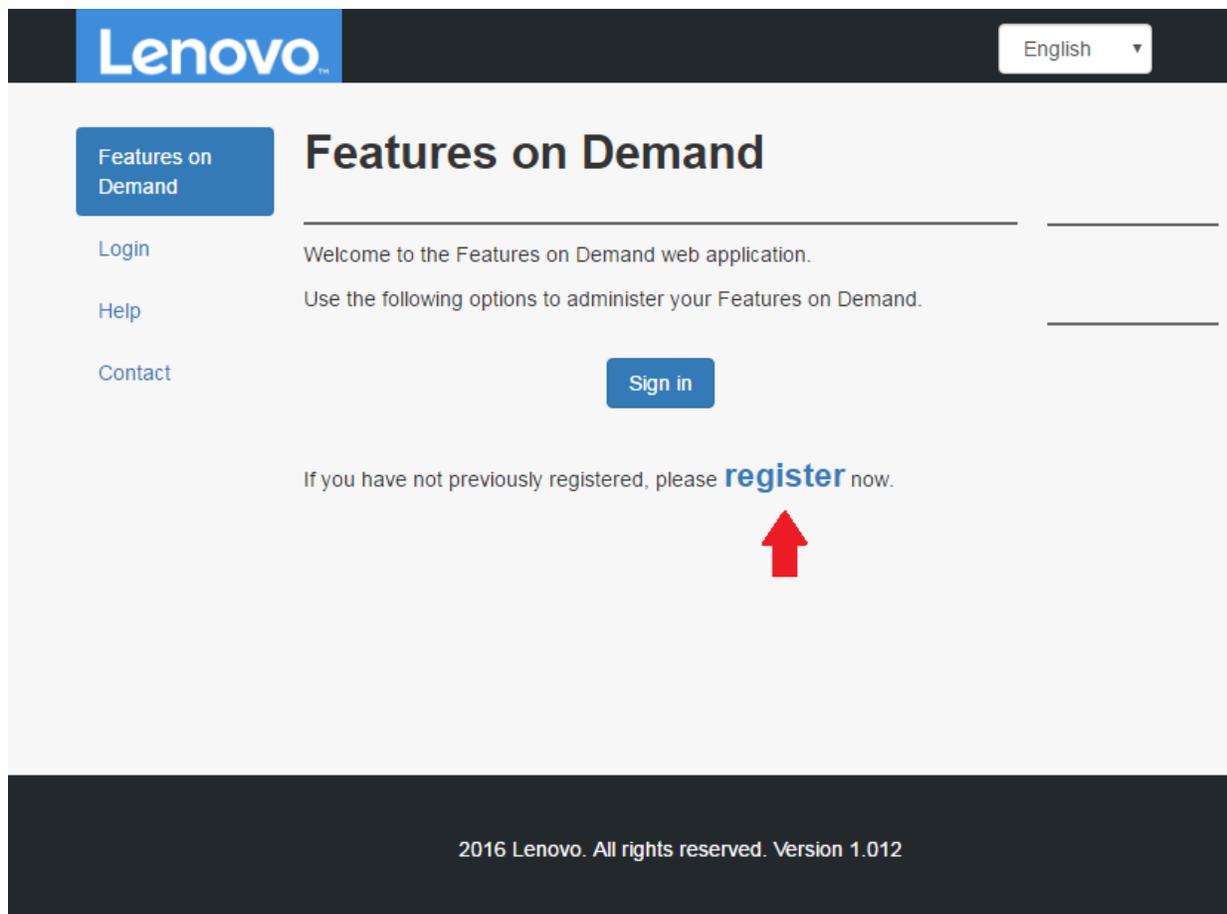


Figure 3: Sign in page of the Lenovo FoD Web site

Introducing the Features on Demand technology – Key management system

On the Register page, as shown in **Figure 4**, fill in the necessary information and then click Register to create a FoD account.

Register

If you are the end user of the product, you agree that by providing Lenovo with your contact information, Lenovo and its affiliates may store, use and process this information about you. Such information may be transferred by Lenovo to any country where Lenovo does business; and may be provided to entities acting on Lenovo's behalf in relation to software activation. Lenovo may also disclose such information where required by law. In the event that such information constitutes personal data Lenovo shall treat such personal data in accordance with applicable data protection requirements. You hereby consent and agree to the collection, processing and use by Lenovo of Personal Data for use in connection with software activation.

If you are a reseller or distributor submitting end user customer contact information, you agree that:

(i) you comply with all applicable data protection requirements including notification to the customer that their data is being transferred to a third party for purposes connected with software activation and that their data may be processed globally and:

(ii) that you will ensure that any reseller who has provided such information to you complies with all applicable data protection requirements including customer notification.

* I have read and accept the declaration

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Email Address*	<input type="text"/>
Password*	<input type="password"/>
Password Confirm*	<input type="password"/>
Country*	<input type="text"/>
Text in the image*	<input type="text"/> 
<input type="button" value="Register"/>	

Figure 4: Lenovo FoD Web site register page

Using the System x FoD Web site

The FoD Web site is the primary tool that is use to manage FoDs:

Go to the System x FoD Web site at: <https://fod.lenovo.com/lkms/> to perform the following tasks (as shown in **Figure 5**):

- Request an activation key
- Retrieve history
- Hardware replacement
- Adapter mobility
- Trial key
- Retrieve an authorization code

Introducing the Features on Demand technology – Key management system

- User Preferences

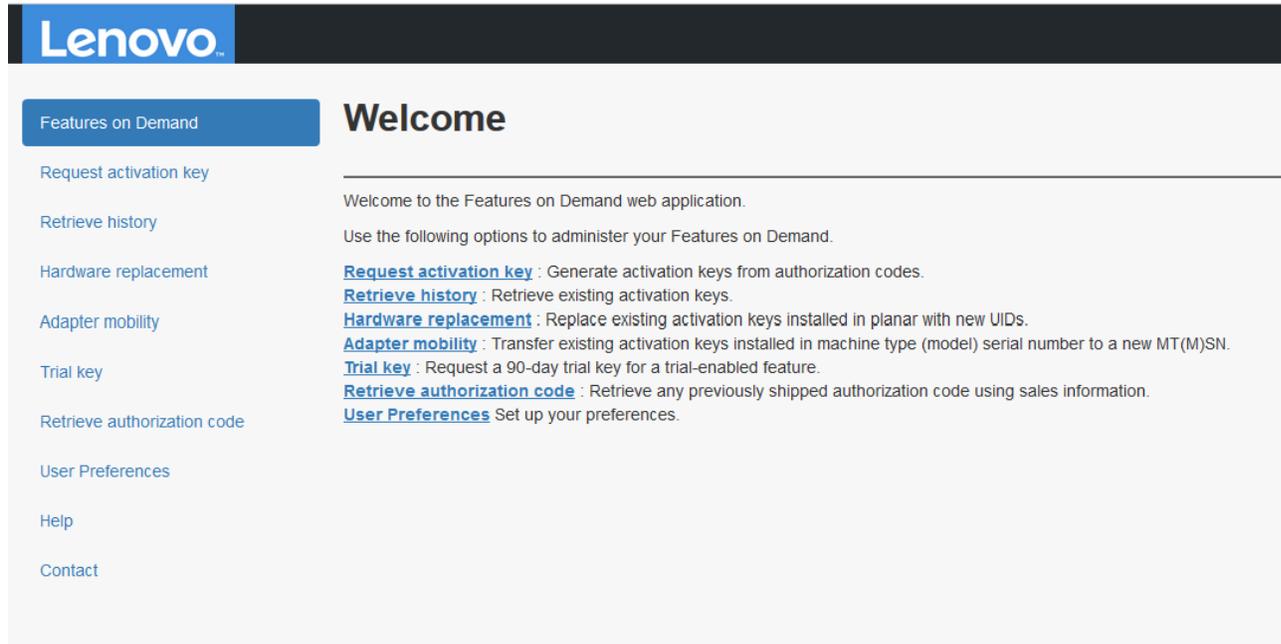


Figure 5: Lenovo FoD Web site welcome page

Activating the FoD feature

Servicers need to obtain the following items from the client before assisting with activating the FoD feature:

- The authorization code that is at the top of the Feature Activation Instructions document that was sent to clients in the e-mail.
- Access to the hardware that you want to activate.
- The server's four-digit machine type and seven-digit serial number.

Note: The server's four-digit machine type and seven-digit serial number are located in the UEFI below System Information – Product Data or from the label that is on the front bezel of the unit.

Requesting an activation key

To request an activation key, complete the following steps:

1. Select **Request activation key** from the left navigation pane of the Features on Demand Welcome page as shown in **Figure 6**.

Introducing the Features on Demand technology – Key management system

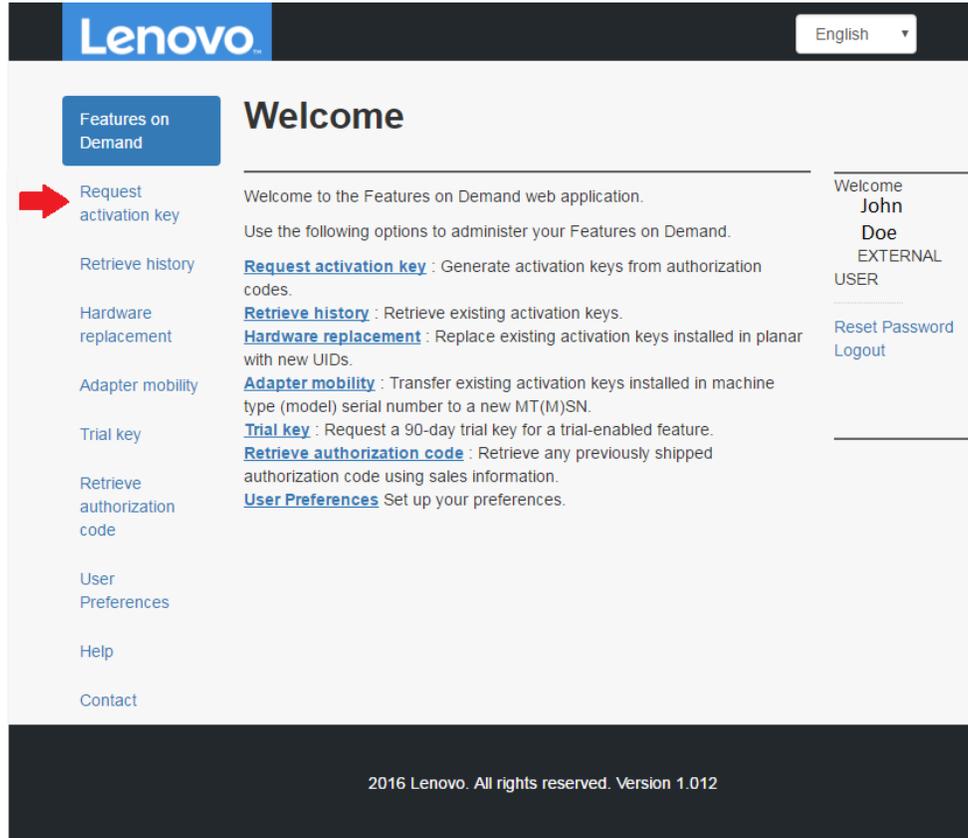


Figure 6: Key management options for license managing

2. Enter the authorization code and click

Continue on the Request activation key page as shown in **Figure 7**.

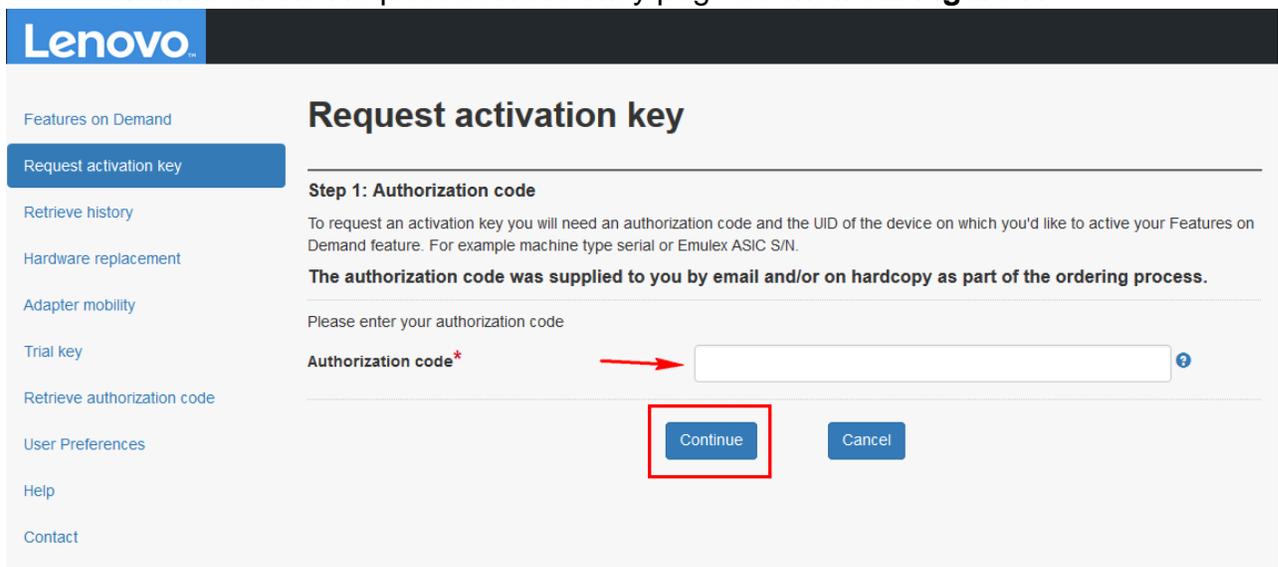


Figure 7: Request activation key page

Introducing the Features on Demand technology – Key management system

3. Enter the unique identifier (UID) specified for feature activation as shown in **Figure 8**.

Request activation key

Step 2: Machine details

Your authorization code is displayed below.

Select your machine type and model if available and enter your 7 character machine serial number. (Your machine serial number can be found on the back panel or in one of the system administration tools).

Feature code	<input type="text" value="A1ML"/>
Feature description	<input type="text" value="IBM Integrated Management Module Advanced Upgrade"/>
Part number / PID	<input type="text" value="90Y3901"/>
Remaining keys	<input type="text" value="1"/>
Machine type*	<input type="text" value="7914 - IBM System x3550 M4"/> ⓘ
Model	<input type="text" value="Please select a model ..."/> ⓘ
Machine serial number*	<input type="text"/> ⓘ

Generate key

Cancel

Figure 8: Enter machine details

Note: For server options, the UID is usually the machine type and serial number (entered together with no spaces) of the target server. For I/O modules, the UID is usually the serial number of the I/O module.

4. Select **Generate key**. A summary of what is created is displayed. Make sure that the information is correct before you select **Confirm** as shown in **Figure 9**.

Introducing the Features on Demand technology – Key management system

Request activation key

Step 3: Machine details confirm

Once confirmed, this action cannot be reversed. Please ensure the data displayed corresponds to the key you wish to create.

Authorization code	<input type="text"/>
Feature code	<input type="text" value="A1ML"/>
Feature description	<input type="text" value="IBM Integrated Management Module Advanced Upgrad"/>
UID type	<input type="text" value="Machine Type Serial Number"/>
Part number / PID	<input type="text"/>
Machine type	<input type="text" value="7914"/>
Model	<input type="text"/>
Machine serial number	<input type="text"/>

Figure 9: Machine details confirm

5. Install the activation key file on the IMM2 of the target server by using the IMM2, ASU or field tool BoMCsf2 or BoMCsf3 (depending on machine type). For more information, go to the Lenovo ToolsCenter for System x and BladeCenter Information Center at:
<http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp>.

Note: You might have to restart the server to activate the features.

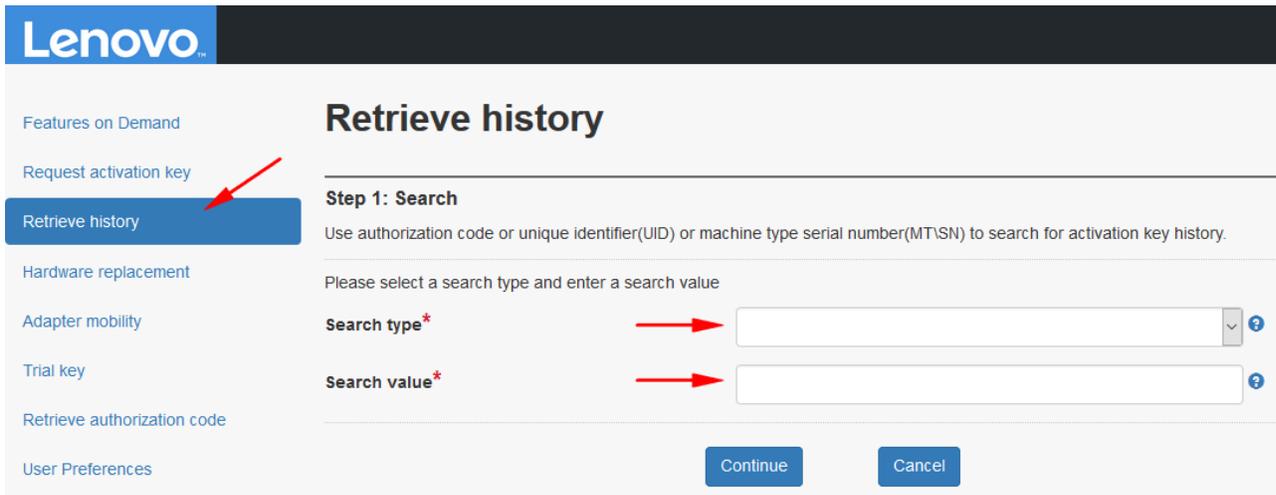
Introducing the Features on Demand technology – Key management system

Retrieving history

On the **Retrieve history** page, use the authorization code, UID, or VPD to search for activation key history.

To retrieve the history, complete the following steps:

1. Select **Retrieve history** from the left navigation pane.
2. Select **Search type** and enter the authorization code, UID, or the machine type and serial number. Click **Continue** as shown in **Figure 10**.



The screenshot shows the 'Retrieve history' page in the Lenovo Key Management System. The left navigation pane has 'Retrieve history' selected. The main content area is titled 'Retrieve history' and contains a 'Step 1: Search' section. Below the title, there is a text prompt: 'Use authorization code or unique identifier(UID) or machine type serial number(MT\SN) to search for activation key history.' Below this, there is a label 'Please select a search type and enter a search value'. There are two input fields: 'Search type*' (a dropdown menu) and 'Search value*' (a text box). Red arrows point to these fields. At the bottom right, there are 'Continue' and 'Cancel' buttons.

Figure 10: Retrieve history

3. Select one or more active keys to e-mail or to download as shown in **Figure 11**.

Introducing the Features on Demand technology – Key management system

Systems > Features on Demand >

Retrieve history

Step 2: Result

This lists the activation keys generated and installed in the machine type serial number entered.

Select the keys you want to retrieve and download the keys directly or have them sent to your registered email address: [redacted]

Note: To ensure that you continue to receive future correspondence without issues, please add FOD1@us.ibm.com as an exception to your spam filter.

Generated keys for machine: [redacted] ⓘ

Feature	Details	Expiration
<input type="checkbox"/>	A1ML ⓘ IBM Integrated Management Module Advanced Upgrade	none
<input type="checkbox"/>	Select all	

Figure 11: Keys installed on the system

Hardware replacement

When a hardware failure occurs to a network adapter or network switch in a Flex chassis, the unique identifier for the replacement part can be updated on the **Hardware replacement** page of the FoD Web site as shown in **Figure 12**.

The details can be found in the [Lenovo Press – Using System x Features on Demand guide](#). Refer to the “7.1 Hardware replacement by using the FoD Web site” section for a listing of more resources.

Introducing the Features on Demand technology – Key management system

Figure 12: Hardware replacement page

Adapter mobility

If you move an adapter with FoD features enabled to a new server, those FoD features do not automatically transfer over because the FoD key is stored in the IMM2 of the server. Therefore, you must use the **Adapter Mobility** feature of the FoD Web site to transfer the FoD features to the new server. **Figure 13** shows the Adapter mobility Web site.

The details can be found in the [Lenovo Press – Using System x Features on Demand](#). Refer to the “7.4 Moving an adapter or a switch” section for a listing of more resources.

Figure 13: Hardware replacement page

Introducing the Features on Demand technology – Key management system

Trial key

The **Trial key** page as shown in **Figure 14** can be used to get a 90-day trial key to try new capabilities.

Lenovo™

Features on Demand

Request activation key

Retrieve history

Hardware replacement

Adapter mobility

Trial key

Retrieve authorization code

User Preferences

Help

Contact

Trial key

Step 1: Feature selection

Select a feature and enter your company name, contact name, email, phone number. (Phone number is optional)

Feature*

Company name*

Contact name*

Email

Phone number

Figure 14: Trial key page

Introducing the Features on Demand technology – Key management system

Retrieving an authorization code

On the **Retrieve authorization code** page as shown in **Figure 15**, you can request to have a PDF file with an authorization code e-mailed to you.

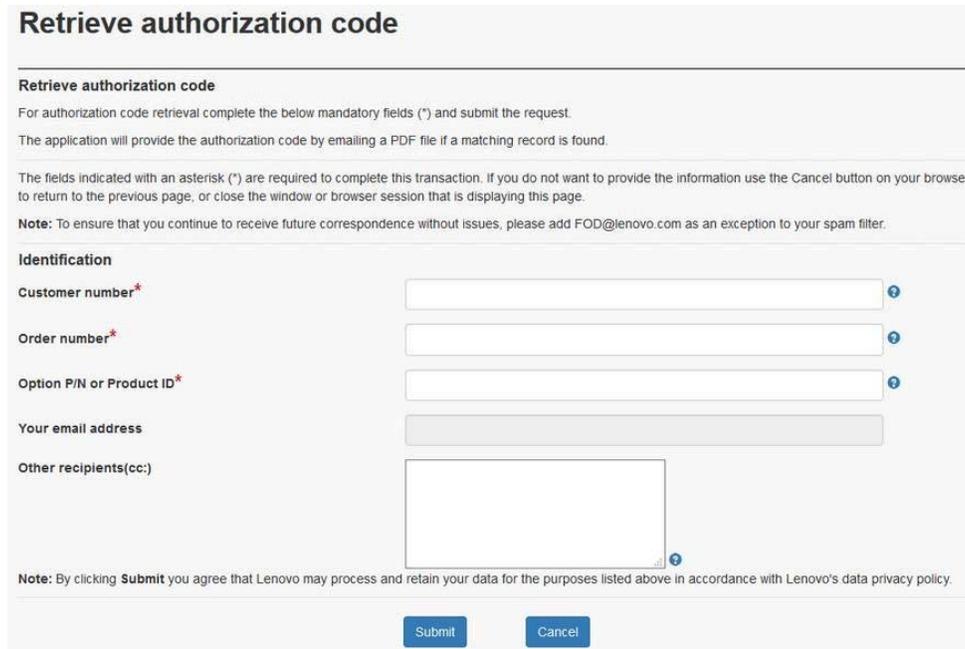


Figure 15: Retrieve authorization code

Enter the following identification needed to retrieve the authorization code as shown in **Figure 15**.

- **Customer number:** enter either legacy customer number or SAP customer number; multiple values are accepted.
- **Order number:** enter either SAP sales order number (10 characters, only available if you are the administrator for the customer number), plant order number (six characters, available to use for paper orders), FoD serial number (seven characters, starts with ISO2 country code, only for FoD orders).
- **Option P/N or product ID:** enter either product ID or part number that depends on the product, ordering system, and country.
- Enter your e-mail address, if necessary.
- Click **Submit**. A confirmation window is displayed.

User preferences

Notifications that are sent to authorized users can be customized on the **User Preferences** page as shown in **Figure 16**. Authorized users are sent notifications after the FoD keys are ready to be used. Users can select what type of information is in the

Introducing the Features on Demand technology – Key management system notification and whether notifications should be sent at all, which is all done through User Preferences on the FoD Web site.

User Preferences

This option allows you to set up how and if the website communicates with you via email. Lenovo Business Partners with access to Inventory management can also set up how their delivery emails are created, when they are being sent to their customers.

My preferences:

Receive emails from the website when my trial keys expire in

7 days

30 days

Receive emails from the website when orders are shipped

Yes

No

Include .pdf of the authorization code(s) as attachment(s) in the emails

Yes

No

Figure 16: User preferences page

Introducing the Features on Demand technology – Key management system

FoD activation key management through Advanced Setup Utility Overview

The Lenovo Advanced Setup Utility (ASU) is used to modify firmware settings from the command line on multiple operating-system platforms like DOS, Linux, Solaris, Windows, and WinPE. It supports BIOS code, remote supervisor adapter firmware, remote supervisor adapter II firmware, and baseboard management controller firmware. Also, since ASU 3.60, RDCLI is included in the ASU software suite. RDCLI is a utility that enables users to mount an ISO file, CD, or DVD to a remote IMM system. The following tasks can be performed by using the utility:

- Modify selected basic input or output system (BIOS) CMOS settings without the need to restart the system to access F1 settings.
- Modify selected baseboard management controller setup settings.
- Modify selected remote supervisor adapter and remote supervisor adapter II setup settings.
- Modify selected settings in IMM-based servers for the IMM firmware and Lenovo System x Server firmware. The IMM replaces the remote supervisor adapter and baseboard management controller functions on IMM-based servers. Lenovo System x Server firmware is the Lenovo implementation of UEFI. The UEFI replaces the BIOS and defines a standard interface between the operating system (OS), platform firmware, and external devices.
- Modify a limited number of VPD settings on IMM-based servers.
- Modify iSCSI boot settings.
- Remote connectivity to the systems to set up all of the listed firmware type settings on IMM-based servers.
- Mount an ISO file, CD or DVD to a remote IMM-based system (IMM must be exposed to the network and accessible).
- Manage FoD activation keys.
- The ASU supports scripting environments through its batch-processing mode.

Introducing the Features on Demand technology – Key management system

Advanced Setup Utility command syntax for keys

Enter the following commands to install, report, uninstall, or export an FoD key:

```
asu.exe fodcfg <command> <command_options> [device&interface]
[connection_options]
```

Table 3 lists the ASU commands and command options.

Table 3: ASU commands		
Command	Command_options	Description
installkey	-f <key file>	Specify the key file name to install the key.
reportkey	N/A	Inventory information of a specified key repository (for example, IMM).
uninstallkey	--keyid <keyid>	Specify which key should be removed with key ID.
exportkey	--keyid <keyid> -d <directory>	Extract one or all of the keys to the specified directory.

Device and interface

- Specify target device: --device <DEVICE>
 - The **DEVICE** variable could be: IMM, CMM, or Switch
- Specify interface: --interface <INTERFACE>
 - The **INTERFACE** variable could be: IPMI, KCS, CIM, or SNMP

Note: If the device is specified, then the default interface is all interfaces that are supported by that device. If the interface is specified, then the default device value is all devices that support this interface. If neither is specified, then the default device is IMM.

Enter the following commands to choose an interface to update a FoD key:

```
asu.exe fodcfg <command> <command_options> [device&interface]
[connection_options]
```

Introducing the Features on Demand technology – Key management system

Table 4 lists the ASU interface and command options.

Table 4: ASU installation interface		
Interface	Command_options	Description
KCS	N/A	Connect to the IMM locally (in-band) through the KCS interface.
IPMI	--host <device IP> --user <device userid> --password <device password>	All the parameters are optional, attempts to find IP address for LAN-over-USB if --host not specified.
CIM	--host <device IP> --user <device userid> --password <device password> --cimhttp --port	All the parameters are optional, attempts to find IP address for LAN-over-USB if --host not specified.
SNMP	--host <device IP> --user <snmpv3 userid> --password <snmpv3 password> --sftp <ftp IP:port> --tftp <ftp IP:port> --ftpid <userid:pw> --community <community> --authproto <MD5/SHA> --privproto <DES/AES> --privpasswd	Need extra SFTP or TFTP server for key file transaction in SNMP interface. If using sftp, also need to specify ---ftpid. If --user and --password are specified, ASU attempts to run snmpv3 or else ASU runs snmpv1v2.

Note: run `--help` for more detailed information:

```
asu.exe fodcfg -help
```

```
asu.exe fodcfg command --help
```

Introducing the Features on Demand technology – Key management system

Key management on IMM device using Advanced Setup Utility

The following figures show the command input in ASU and the results that the system responds with if the keys are installed correctly onto IMM.

Example of installed key (the `installkey` command) to IMM shown in **Figure 17**.

```
D:\test\asu>asu fodcfg installkey -f ibm_fod_0009_123456789ABCDEF0123_anyos_noarch.key --host 9.125.90.236
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Pegasus Exception: Cannot connect to 9.125.90.236:5989. Connection failed.
Executing the command through CIM interface failed, trying IPMI interface.
Connected to IMM at IP address 9.125.90.236
Succeed to install key ibm_fod_0009_123456789ABCDEF0123_anyos_noarch.key. Activation key must be validated elsewhere.
```

Figure 17: Successful installation of keys

Example of inventory key (the `reportkey` command) to IMM shown in **Figure 18**.

```
D:\test\asu>asu fodcfg reportkey --device imm --host 9.125.90.236
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Pegasus Exception: Cannot connect to 9.125.90.236:5989. Connection failed.
Executing the command through CIM interface failed, trying IPMI interface.
Connected to IMM at IP address 9.125.90.236
Number of keys installed is 3
No Key ID status Description
1 95ffd49d17aea9c4 valid Server RAID M5100 Series RAID 6 Upgrade for IBM
2 db286d495b0d0637 valid IBM Integrated Management Module Advanced Upgrade
3 883ca0abf8e67beb validated elsewhere IBM xxxxxxxxxxxx I6131 Infiniband Switch (FDR)
```

Figure 18: Successful report of keys

Example of extract key (the `exportkey` command) to IMM shown in **Figure 19**.

```
D:\test\asu>asu fodcfg exportkey --keyid all -d ./ --device imm --interface cim --host 9.125.90.236 --cimhttp --port 5988
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:9.125.90.236 on Port:5988
Success to export key 95ffd49d17aea9c4.
Success to export key db286d495b0d0637.
Success to export all keys.
```

Figure 19: Successful extraction of keys

Introducing the Features on Demand technology – Key management system

Example of remove key (the `uninstallkey` command) to IMM shown in **Figure 20**.

```
D:\test\asu>asu fodcfg uninstallkey --keyid 883ca0abf8e67beb --device imm --host
9.125.90.236 --cimhttp --port 5988
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:9.125.90.236 on Port:5988
Succeed to uninstall key 883ca0abf8e67beb.
```

Figure 20: Successful removal of keys

Note: If no interface is specified, the ASU tries CIM first and then the IPMI interface. If both the CIM and IPMI fail, ASU tries KCS if `--host` is not specified.

Key management on CMM device by using Advanced Setup Utility

The following figures show the command input in ASU and the results that the system responds with if the keys are installed correctly onto CMM.

Example of extract key (the `exportkey` command) to CMM shown in **Figure 21**.

```
D:\test\asu>asu fodcfg exportkey --keyid 0000000000000001 --device cmm --host 9.
186.9.140 --cimhttp --port 5988
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:9.186.9.140 on Port:5988
Succeed to export key 0000000000000001.
```

Figure 21: Successful export of keys

Example of remove key (the `uninstallkey` command) to CMM shown in **Figure 22**.

```
D:\test\asu>asu fodcfg uninstallkey --keyid 0000000000000001 --device cmm --host
9.186.9.140 --cimhttp --port 5988
IBM Advanced Settings Utility version 9.00.76I
Licensed Materials - Property of IBM
(C) Copyright IBM Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:9.186.9.140 on Port:5988
Succeed to uninstall key 0000000000000001.
```

Figure 22: Successful removal of keys

Introducing the Features on Demand technology – Key management system

Key management on IOM device by using Advanced Setup Utility

The IOM (switch) is designed to use SNMP for feature key management and needs an extra SFTP or TFTP server for the key file transaction. Specifying the `--tftp` or `-sftp -ftpid` is needed.

Example of key installation (the `installkey` command) to IOM (switch):

To use the `tftp` and `snmpv1v2` commands without encryption, complete the following steps:

1. Configure the switch SNMP community as **private** with both read and write access.
2. Set up tftp with address **9.125.90.200** and with both read and write access.
3. Run the following command:

```
asu.exe fodcfg installkey -f ibm_fod_0005_Y050VT16E080_anyos_noarch.key
--device switch --host 9.125.90.53 --tftp 9.125.90.200 --community
private
```

Example of inventory key (the `reportkey` command) to IOM (switch):

```
asu.exe fodcfg reportkey --device switch --host 9.125.90.53 --tftp
9.125.90.200 --community private
```

Example of extract key (the `exportkey` command) to IOM (switch):

To use `sftp` and `snmpv3` with MD5 Authorization protocol, complete the following steps:

1. Create switch `snmpv3` user for authorizing MD5 **adminmd5**. The MD5 password is **ADMINMD5**. Configure the user privacy protocol as destination, with password **adminmd5**.
2. Set up `sftp` with address **9.125.90.83**, and create user **sftpadmin** for both read and write access. The password is **sftppass**.
3. Run the following command:

```
asu.exe fodcfg exportkey --keyid 0005 --host 9.125.90.53 --device
switch --user adminmd5 --password adminmd5 --authproto md5 --
privproto des --privpasswd adminmd5 --sftp 9.125.90.83 --ftpid
sftpadmin:sftppass
```

Example of remove key (the `uninstallkey` command) to IOM (switch):

```
asu.exe fodcfg uninstallkey --keyid 0005 --host 9.125.90.53 --device switch -
-user adminmd5 --password adminmd5 --authproto md5 --privproto des --
privpasswd adminmd5 --sftp 9.125.90.83 --ftpid sftpadmin:sftppass
```

Introducing the Features on Demand technology – Key management system

Acquire key from KMS using Advanced Setup Utility

Command syntax:

```
asu64.exe fodcfg acquirekey -r -d <directory> --kmsid <userid:password> -m
<machinetype> -u <machinetypeserialnumber>
```

In the sample syntax, we make the following substitutions lists in **Table 5**.

Table 5: ASU fodcfg command substitutions	
Syntax	Description
-r	Install downloaded activation key.
-d <directory>	Download the key file to <directory> location. The default value is current folder.
--kmsid <userid:password>	KMS Web site credentials.
-m <machinetype>	The machine type of the system.
-u <machinetypeserialnumber>	Unique identifier information. The machine type and serial number of the system with no spaces or dashes.

The example command that is used is:

```
C:\ASUtil>asu.exe fodcfg acquirekey -r -d C:\fodkey --kmsid
userid@example.com:xxxxxxx -m 7915 -u 79151234567 --host 192.168.10.100 --
user USERID --password PASSW@RD
```

Introducing the Features on Demand technology – FoD activation key management through DSA

FoD activation key management through DSA

DSA provides the following functionalities for key management:

- Key installation (online)
- Key installation from removable media (offline)
- Key uninstall
- View available FoD features or installed FoD keys
- Export FoD information

FoD CLI support for portable DSA

Portable DSA provides a command-line interface for FoD key management. This interface (FoD) is launched using sub commands after DSA execution program.

Table 6 lists all of the portable DSA commands that are related to FoD.

Command syntax: `dsaexe fod command`

Table 6: DSA FoD commands	
DSA commands	Description
help	Displays a list of available commands.
export_imm_uid	Export FoD inventory information to removable media by using unique identifier (UID). The file that is generated is exported to <code>dsa_fod_id.txt</code> in the DSA output folder.
display_available_fod	Display the available FoD keys for a key repository.
download_fod_key	Acquire and download activation key from Lenovo Web site.
install_fod_key	Install activation keys from user-specified location to key repository.
export_imm_fod	Export the local FoD unique IDs to a file that is saved in DSA output path.
report_imm_active_fod	Report inventory information of IMM repository.
install_imm_fod	Download and install activation keys to IMM repository.
uninstall_imm_fod	Uninstall activation keys from IMM repository

Introducing the Features on Demand technology – FoD activation key management through DSA

Refer to the section “[Using Features on Demand for Portable Dynamic System Analysis](#)” on the Lenovo ToolsCenter Web site shown in **Figure 23** for more details about how to manage FoD key through DSA with following topics:

[Downloading the FoD key and installing with the key file](#)

[Using the FoD Key on an IMM for a portable target system](#)

[Using the FoD Key on a CMM for a portable target system](#)

[Using the FoD Key on an IOM/Switch for a portable target system](#)

The screenshot shows the Lenovo ToolsCenter web interface. On the left is a 'Contents' sidebar with a search bar at the top. The sidebar lists various categories, with 'Lenovo ToolsCenter' highlighted by a red arrow. Under 'Supporting Dynamic System Analysis Features on Demand', the article 'Using Features on Demand for Portable Dynamic System Analysis' is highlighted with a blue box and a red lightning bolt icon. The main content area on the right displays the title 'Using Features on Demand for Portable Dynamic System Analysis' and a brief introduction. Below the introduction are four sub-topics, each enclosed in a red box: 'Downloading the FoD key and installing with the key file', 'Using the FoD Key on an IMM for a portable target system', 'Using the FoD Key on a CMM for a portable target system', and 'Using the FoD Key on an IOM/Switch for a portable target system'. The parent topic is listed as 'Supporting Dynamic System Analysis Features on Demand'.

Figure 23: Lenovo ToolsCenter Web site

Introducing the Features on Demand technology – FoD activation key management through DSA

FoD GUI support for embedded DSA Preboot

The DSA Preboot GUI enables the users to view, install, or uninstall the FoD License Key on a machine or reactivate the existing FoD activation keys on a replaced system board.

After you launch the graphical DSA environment, the License Agreement, as shown in **Figure 24**, displays. Click **I Accept** to accept the license and enter the Welcome page; or click **I don't Accept** to exit the preboot DSA GUI.



Figure 24: License agreement in DSA Preboot GUI

Select **Activation Key Management** in the navigation pane or from the top menu to open the Activation Key Management page as shown in **Figure 25**.

Introducing the Features on Demand technology – FoD activation key management through DSA

Welcome

Collection and Diagnosis | Activation Key Management

Welcome to Dynamic System Analysis

IBM Preboot Dynamic System Analysis (DSA) is a system information collection and analysis tool that is used by IBM Modular & Blade® Service and Support personnel to aid in the diagnosis of system problems.
Dynamic System Analysis can assist you with the following functions:

System Information [Change](#)
Machine Name: IBM System X3100 M5
Machine Type/Model: 5457/A2D
Serial Number: 1234567

Collect inventory and perform diagnosis

Full Inventory Collection and Diagnosis
Collect a full system inventory and perform a complete analysis and diagnosis.

Customized Inventory Collection and Diagnosis
A customized system inventory collection, analysis, and diagnosis. This option is helpful to experienced users for troubleshooting system issues.

Manage Activation Key

Activation Key Management
Perform activation key management on IMM2.

Figure 25: Manage activation key in DSA

After you click **Activation key Management**, the activation key list displays. There are six operations for Activation Key Management:

- Refresh
- Export
- Uninstall
- Install from IBM Web site
- Install from Removable Media
- Reactivate Activation Keys

If the Internet connection is not available, the Install from IBM Web site is not available as shown in **Figure 26**. The Install from Removable Media and the Reactivate Activation Keys are available.

Introducing the Features on Demand technology – FoD activation key management through DSA



Figure 26: Managing a key with Internet connection not available

If the Internet connection is available, the Install from IBM Web site is available when one or more activation keys are selected, as shown in **Figure 27**. The Install from Removable Media and the Reactivate Activation Keys are also available.



Figure 27: Managing keys with available Internet connection

Refresh

As shown in **Figure 28**, refresh the activation key list by clicking **Refresh**.

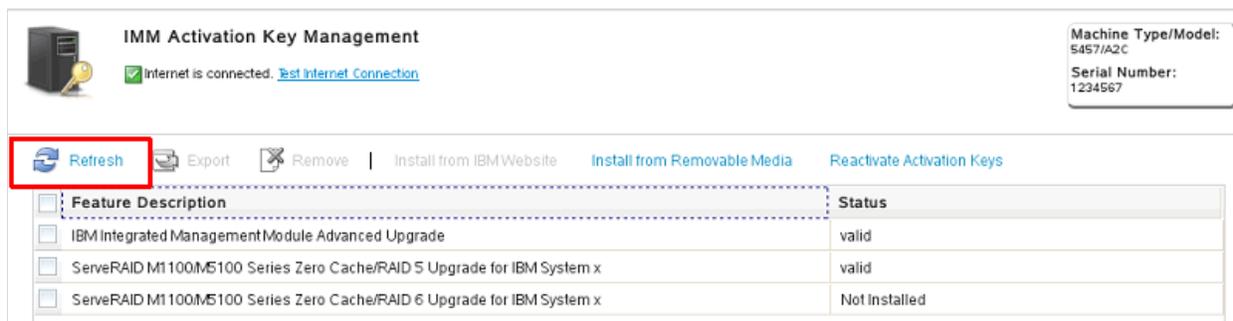


Figure 28: Refresh activation keys

Introducing the Features on Demand technology – FoD activation key management through DSA

Export

As shown in **Figure 29**, select one or more activation keys and click **Export** to export the activation key information into removable media.



Figure 29: Export activation keys

Remove

As shown in **Figure 30**, select one or more activation keys and click **Remove** to uninstall.



Figure 30: Remove activation keys

Introducing the Features on Demand technology – FoD activation key management through DSA

Figure 31 shows the uninstallation results. Uninstallation of the activation keys is completed sequentially. If an uninstall fails, an error icon is displayed. Place the cursor over the error icon to display the error message.

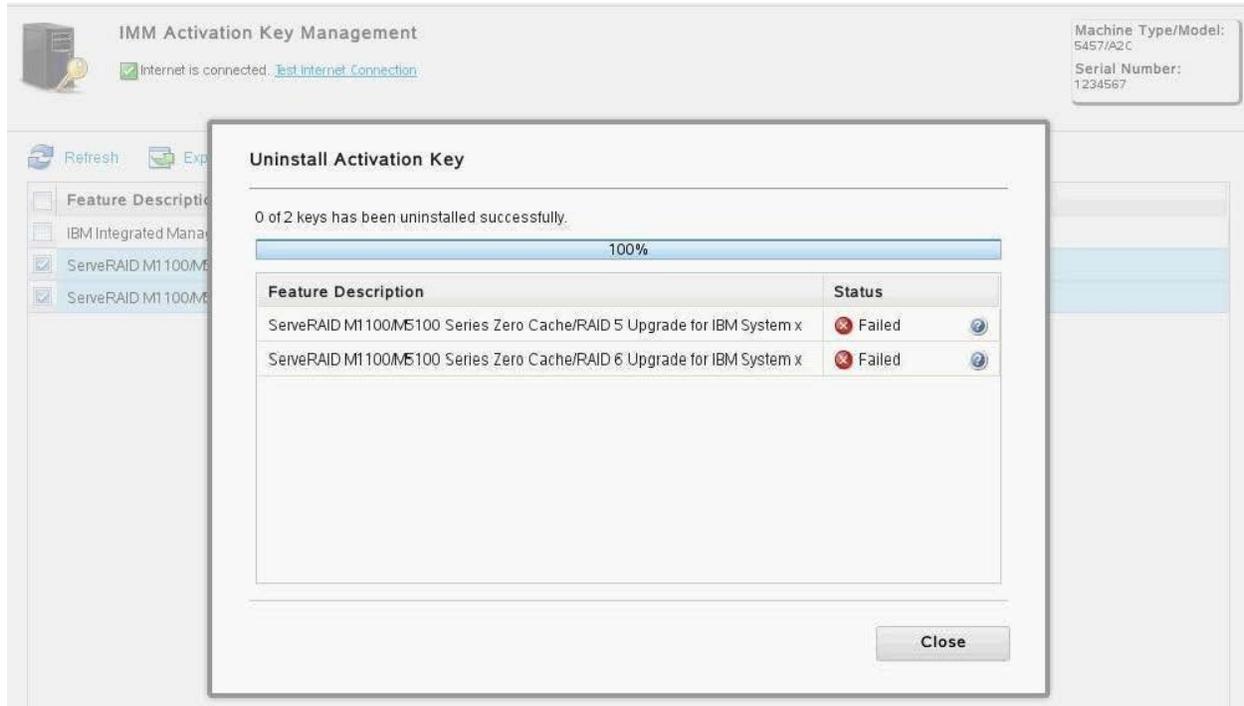


Figure 31: Uninstall activation keys result

Introducing the Features on Demand technology – FoD activation key management through DSA

Install from IBM Web site

At the time of this course writing, this function is still called **Install from IBM Web site** as shown in **Figure 32**. This function will be inaccessible without internet connection.

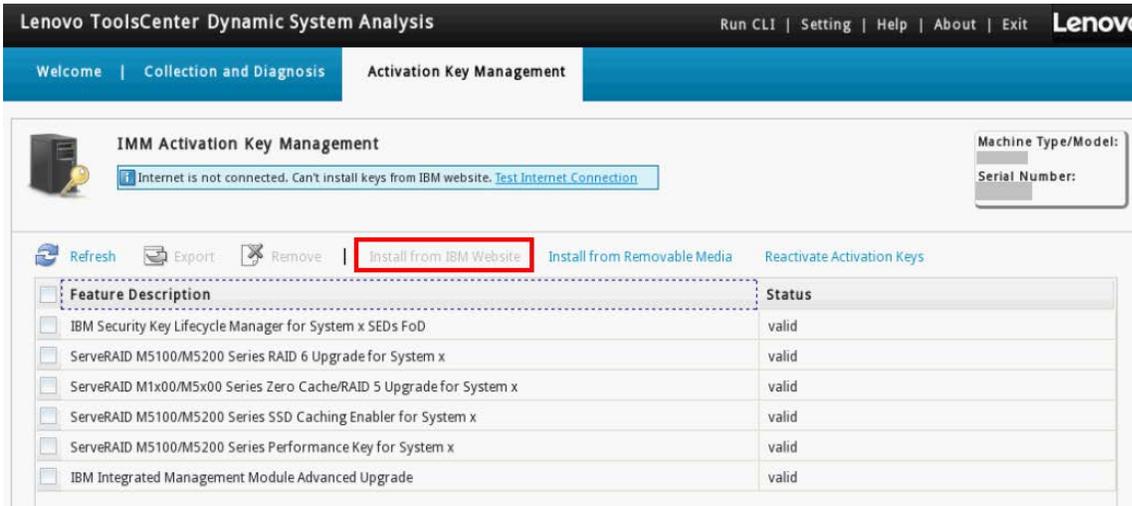


Figure 32: Install from IBM Web site

To install FoD activation keys from IBM's Web site, click **Install from IBM Web site** and enter the user's credentials (IBM ID and user password) and the Details for each key as shown as **Figure 33**. Select one or more activation keys and click **Install Now**. Installation of the activation keys is completed sequentially. If an installation fails, an error icon is displayed. Place the cursor over the error icon to display the error message.

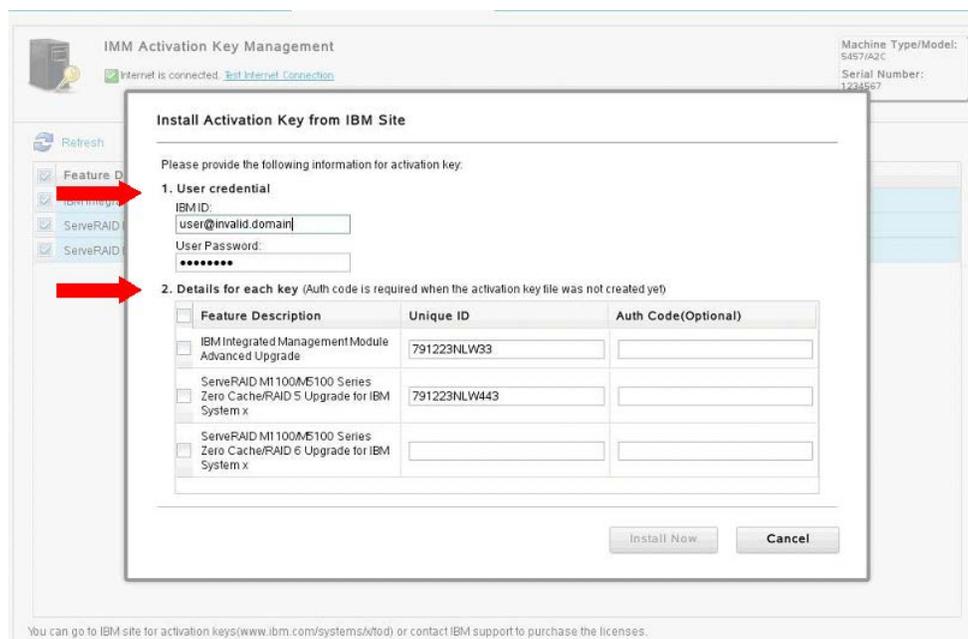


Figure 33: Install activation key from IBM site

Introducing the Features on Demand technology – FoD activation key management through DSA

Install from removable media

To install the activation keys from local removable media, click **Install Activation Key from Removable Media**, and then a dialog box displays as shown in **Figure 34**. After you select one of the removable media options, the activation key files on the removable media display. The Refresh option is used for refreshing the connected removable media.

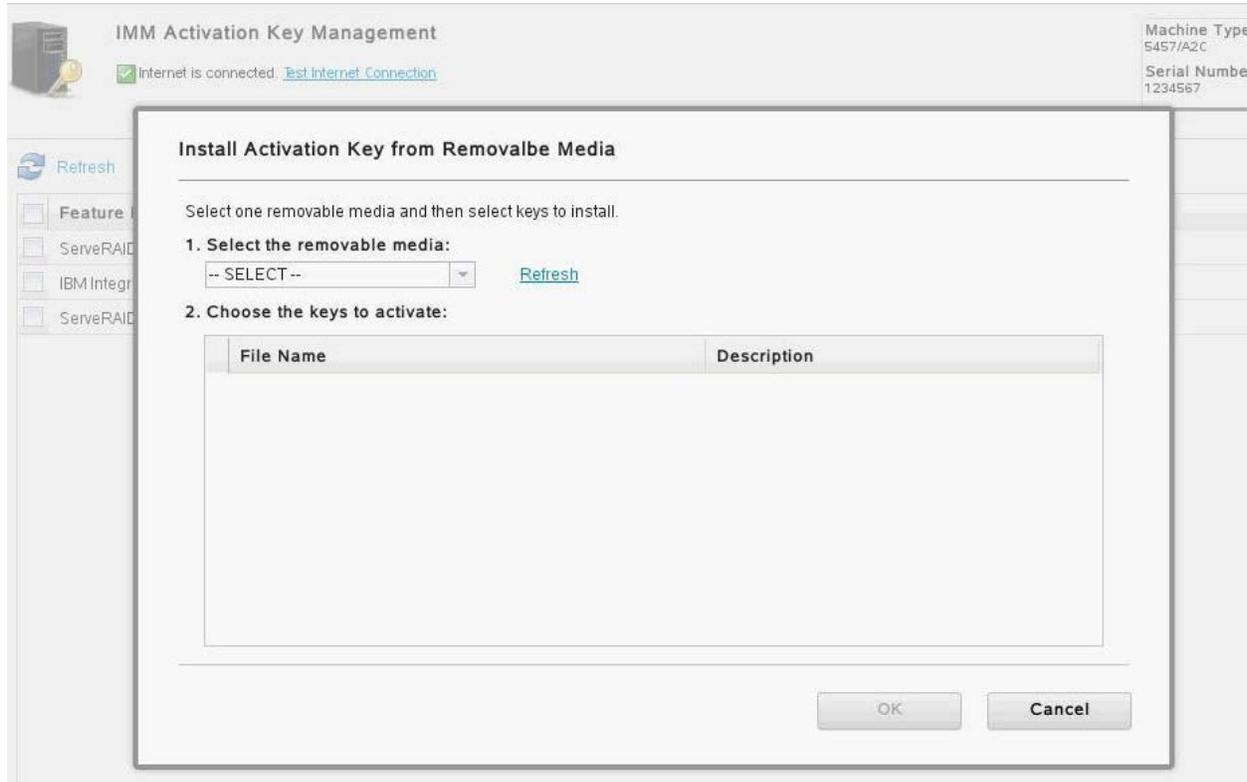


Figure 34: Install activation key from removable media

As shown in **Figure 35**, select one or more of the activation key files and click **OK** to install. Installation of the activation keys is completed sequentially. If an installation fails, an error icon is displayed. Place the cursor over the error icon to display the error message.

Introducing the Features on Demand technology – FoD activation key management through DSA

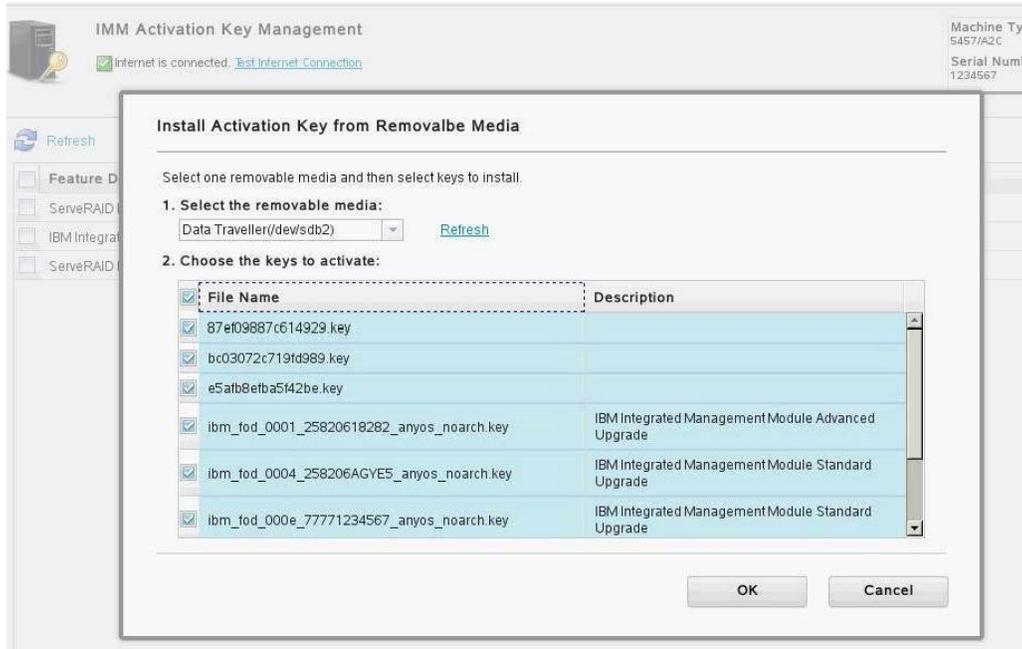


Figure 35: Install activation key from removable media

Reactivate activation keys

Click **Reactivate Activation Keys** to reactivate FoD keys. Check the machine information first and make applicable changes for the machine type, machine model, or serial number if needed as shown in **Figure 36**. After you update the machine information, click **Update Machine Info** to update the modified Vital Product Information (VPD). Choose to **OK** to restart IMM immediately to take effect or **Cancel** to restart IMM manually at another time.

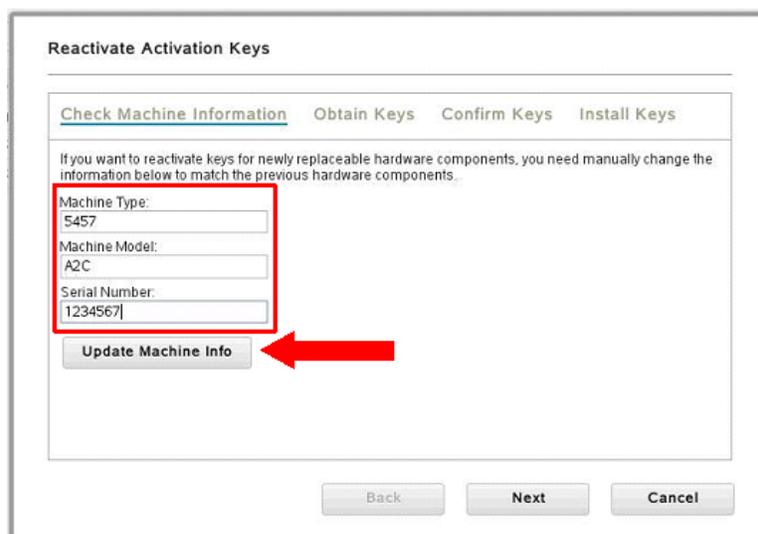


Figure 36: Reactivate activation keys

Introducing the Features on Demand technology – FoD activation key management through DSA

There are two methods to obtain the activation keys.

- **From IBM's Web site:** obtain activation keys from the IBM Web site if the machine is connected to the Internet. Then, enter the IBM ID and password as shown in **Figure 37**.

Reactivate Activation Keys

Check Machine Information Obtain Keys Confirm Keys Install Keys

Provide the following information to obtain the activation keys.

Select where to obtain the activation keys:

From IBM website
 From removable media

Input IBM ID:

IBMID: IBMID is required.
User Password:

Back Next Cancel

Figure 37: Obtain activation keys – method 1

- **From removable media:** select this item if the keys are stored on removable media or if there is no Internet connection as shown in **Figure 38**.

Reactivate Activation Keys

Check Machine Information Obtain Keys Confirm Keys Install Keys

Provide the following information to obtain the activation keys.

Select where to obtain the activation keys:

From IBM website
 From removable media

Select the removable media:

-- SELECT -- Refresh

Back Next Cancel

Figure 38: Obtain activation keys – method 2

Introducing the Features on Demand technology – FoD support plan

FoD support plan

FoD includes hardware features and software features.

When customers purchase systems with FoD, there are two conditions:

1. Manufacturing loads the system in the build stage.
2. The customer can purchase features after the system sale. SSR supports hardware in the following situations:
 - Normal support of hardware and options.
 - SSR is only responsible for hardware break-fix. Any how-to, configuration, installation, and support of the feature functionality as a part of the system should be handled by the corresponding remote support agent.
 - Hardware break-fix is covered under warranty and the user is responsible for the reactivation of FoD keys on System x hardware.

Feature entitlement, activation, reactivation, and feature troubleshooting support:

- Worldwide 24 x 7 coverage
- English only
- FoD support e-mail address: FOD@lenovo.com

Note: If the client is part of the federal government, send an e-mail to fod@us.ibm.com.

Note: It is ultimately the client's responsibility to reinstall their FoD keys. However, be advised that in most service scenarios in which a client needs to have a part replaced, the client often is not aware that they have FoD keys that are applied or might not know how to reapply the keys. In these cases, Remote Support works with the client and Field Technician to reapply the keys.

Hints and tips

1. Check an authorization code to see what feature it enables and how many remaining times it can be used to create a key. Is there a limited number of times that user can activate the features?
 - A key can be installed, uninstalled, and copied for an infinite number of times. It always activates its feature on a single piece of hardware (system, card, chassis, or switch). The specific hardware unit it activates is encoded in the unique identifier and built into the key data structure.
 - Authorization codes are credit for future key redemptions. The codes have information about the feature and supported system types for which they can be used, not information about which specific systems use them (that information does not apply until the keys are created).
 - Redemption history and remaining credit for authorization codes can be checked through KMS interfaces. In the authorization code, there is a limit to the number of new activation keys you can create with the given code, but there is no limit on the number of times on the key that you can activate the feature on the machine.
2. When a customer buys the systems with the features preloaded and activated, if the customer replaces the main board and the features are lost, where can they obtain the authorization code? Are the customers required to register on the FoD site?
 - In this situation, there are several scenarios. For the features that are bound to the key data structure of the system unit, replacing the main board should include a step in which the identity of the replacement is reprogrammed to match the original key data structure; the old keys activate the same features on the new board. Therefore, a customer can export the old keys and reinstall them on the new unit after key data structure reprogramming is complete without having to access KMS.
 - If the customer does not remember to export the keys or if the failed board prevents the keys to be exported, then the keys can be retrieved from KMS using the key data structure of the unit.
 - For features that are bound to something other than the key data structure, new keys are needed if the hardware for those features changes. If you keep the same option cards that you had before the failure, then the same keys from before the failure still work after being reinstalled.
 - To retrieve those keys from KMS, enter the cards' unique identities into KMS to retrieve their keys. The feature is bound to the card, not the system, which requires a different query. A DSA log shows the activation keys from the pre-

Introducing the Features on Demand technology – Hints and tips

failure configuration to help a customer retrieve all of the identities they need to query.

3. Under what conditions do customers need to uninstall a key?

There are two reasons why a customer uninstalls a key. The first reason is to disable the feature. The second reason is to clean up a machine after moving an option card with its activation to another machine. The second reason is recommended for moves, but not required, since the key will simply occupy storage on the IMM2 on the old system after the card is moved.

4. What condition is required to export a key from AMU? If customer can download key from the Web site, why is it necessary to export it from the local machine?

If the customer does not have easy access to KMS from where the machine is, it might be preferred to export it.

5. When are emergency keys, temporary keys, and permanent keys required? How long is the duration for temporary keys?

An emergency key is similar to a standard key, but is obtained differently. Emergency keys are generally requested when customers are urged to obtain keys. Temporary keys are supported on features that support trials or time-based activations. Not every feature provides temporary keys. For those features that do, when it is needed depends upon the feature and the time period it is used. Duration is encoded into temporary keys and can be varied to the needs of the business for each feature instance. Every other key is a permanent key.

6. Can L1 open a support ticket on FoD cases? If so, under what conditions do they open ticket for FoD, and under what conditions do they redirect customers to the URL?

L1 opens a support ticket referencing the machine type and serial number that is entitled for support for FoD problems that are not resolved using the problem resolution path in the FoD user guide.

Introducing the Features on Demand technology – FoD servicer activities

FoD servicer activities

The e-mail address for customers is fod@lenovo.com.

When the servicer receives calls regarding the activation problem, complete the following steps:

1. Run DSA (online or pDSA both collect FoD key inventory information). If the call center is involved, customers are instructed to upload results to Multitool.
2. Look at the DSA information (**Figure 39**) on the FoD key status to verify that the inventory AMU to query the IMM directly with the report function of the tool.

The customer or servicer can also look at DSA information for firmware and software levels to ensure that prerequisites are met for feature enablement.

If the inventory information is displayed correctly, then the issue resolution goes into the feature itself. The inventory has different methods and tools for further diagnosis and debugging based on the different features.

If the inventory information looks incorrect, the customer or servicer can go to the FoD Web site and retrieve the information about entitlement based upon the key data structure of the server. Based on this query, servicers can redownload keys and reinstall the keys, if needed.

Lenovo Dynamic System Analysis IBM Server x3650 M5

FoD Activation Key	
Activation Key	
Description	IBM Integrated Management Module Advanced Upgr
Feature Description	IMM Remote Presence
Expire Date	
Identifier Type	Machine Type and Serial Number
Identifier	
Status	Valid
User Count	0
User Limit	0
Description	IBM Security Key Lifecycle Manager for System
Feature Description	32796
Expire Date	
Identifier Type	Machine Type and Serial Number
Identifier	
Status	Valid
User Count	0
User Limit	0
Description	ServeRAID M1x00/M5x00 Series Zero Cache/RAID 5
Feature Description	32780
Expire Date	
Identifier Type	Machine Type and Serial Number
Identifier	
Status	Valid

Figure 39: FoD information in DSA

Introducing the Features on Demand technology – FoD handling scope by SSRs

FoD handling scope by SSRs

- If the customer provides the FoD key(s) then the SSR will restore the FoD key(s) after the system board replacement.
- If a machine is bootable with an accessible IMM, the SSR will provide his or her best effort to pull the FoD keys using the IMM BoMCsft2, or BoMCsft3 key, and restore the FoD key(s) after system board replacement.
- If the IMM is not available, the SSR or Call Center will search the FoD Web site for the FoD keys attached to the MT/SN. If available, the SSR will obtain the keys from the site and use them to restore the FoD key(s) after the system board replacement.
- If the FoD is not able to be pulled using the IMM or from the Lenovo FoD Web site, then the SSR will disengage and direct the customer to the FoD team for further support. The Lenovo Web site for FoD is <https://fod.lenovo.com/lkms/> and the e-mail address is fod@lenovo.com. Customers should be directed here by the SSR. Refer to *Using System x Features on Demand* at <https://lenovopress.com/redp4895.pdf> for more details.
- If the FoD key is attached to the RAID Card or another piece of hardware and the key is not tied to the machine serial, then the SSR will disengage, but make the customer aware of the needed key. The Lenovo Web site for FoD is <https://fod.lenovo.com/lkms/> and the e-mail address is fod@lenovo.com. Customers should be directed here by the SSR. Refer to *Using System x Features on Demand* at <https://lenovopress.com/redp4895.pdf> for more details.

Introducing the Features on Demand technology – FoD key installation after hardware replacement

FoD key installation after hardware replacement

This section provides the steps required to re-install the FoD keys, which were previously purchased and installed on a Lenovo System x machine. This procedure must be completed after a system board or RAID part replacement to restore full functionality to the customer's machine post hardware replacement activity.

Note: This section does not cover the key replacement process after replacement of option cards such as Qlogic and Emulex communication adapters.

The preferred method in the field to save and restore FoD key files is by using the BoMCSft2 or BoMCSft3 tool (depending on machine type). There is another method that may be used if the customer will allow direct access to the system management interface (IMM). Refer to the section in this document "[Using the System Management Interface to Save and Restore FOD Files](#)" method.

Note: The BoMCSft2 or BoMCSft3 tool is for certified service personnel only. You need to access the [GLOSSE BoMCSft2 & BoMCSft3 Tools](#). GLOSSE access credentials are required.

Preparation

Check the service call to confirm that the system uses FoD features that must be reinstalled.

If the machine boots successfully and the part being replaced is a system board, then boot using BoMCSft2 or BoMCSft3 to back up the FoD keys following these steps:

1. Insert the BoMCSft2/3 USB key in to the machine.
2. Boot the machine to F1, UEFI setup, and then select **Boot Manager** → **Boot from device**.
3. Select the USB port containing the BoMCSft2 device (usually USB front) as shown in **Figure 40**.

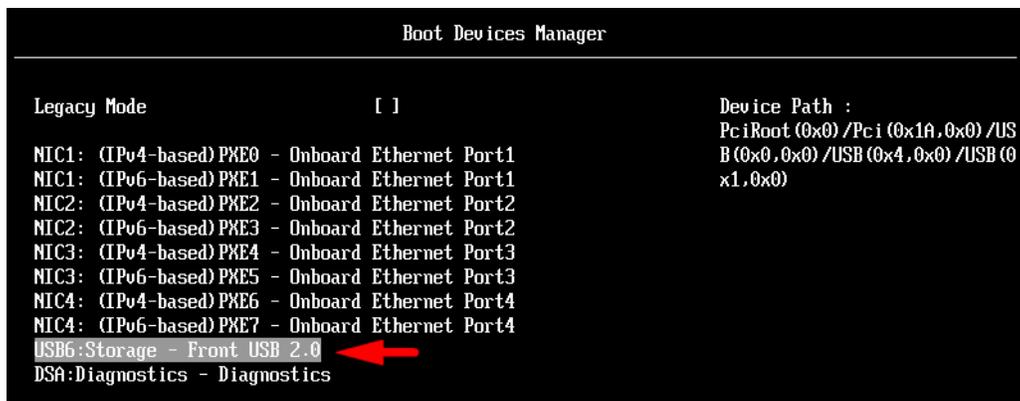


Figure 40: Boot device manager

Introducing the Features on Demand technology – FoD key installation after hardware replacement

Note: You can also boot the machine to select the USB device to boot by pressing **F12** during startup as shown in **Figure 41**.



Figure 41: Select boot device

4. Select **3rd Party Tool** as shown in **Figure 42** after booting the machine using BoMCsft2/3 successfully.

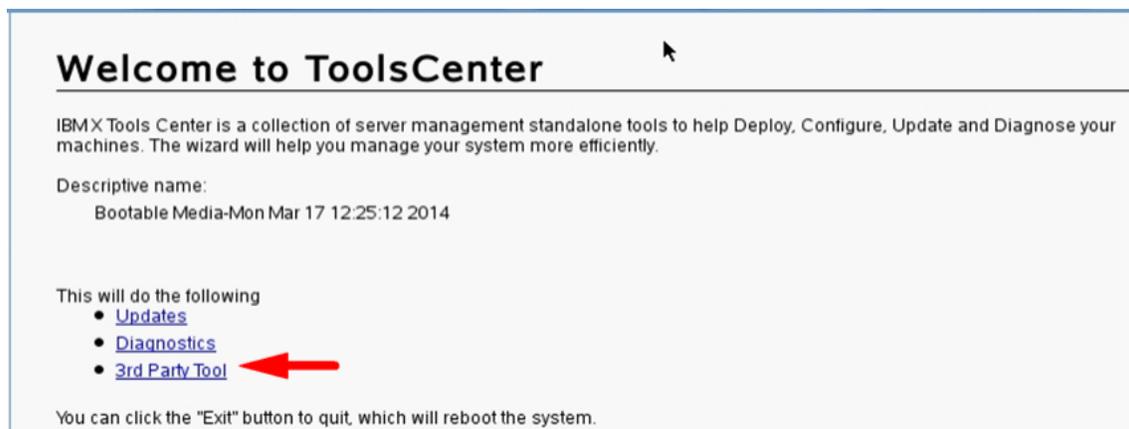


Figure 42: Select 3rd Party Tool

5. Select **Backup and Restore All System Settings** (number 3) after the Service Tools for SSRs blue menu appears to back up the system board configuration settings, which includes the FoD keys onto the USB key. If successful, then skip to "[Parts Replacement](#)" section.

Introducing the Features on Demand technology – FoD key installation after hardware replacement

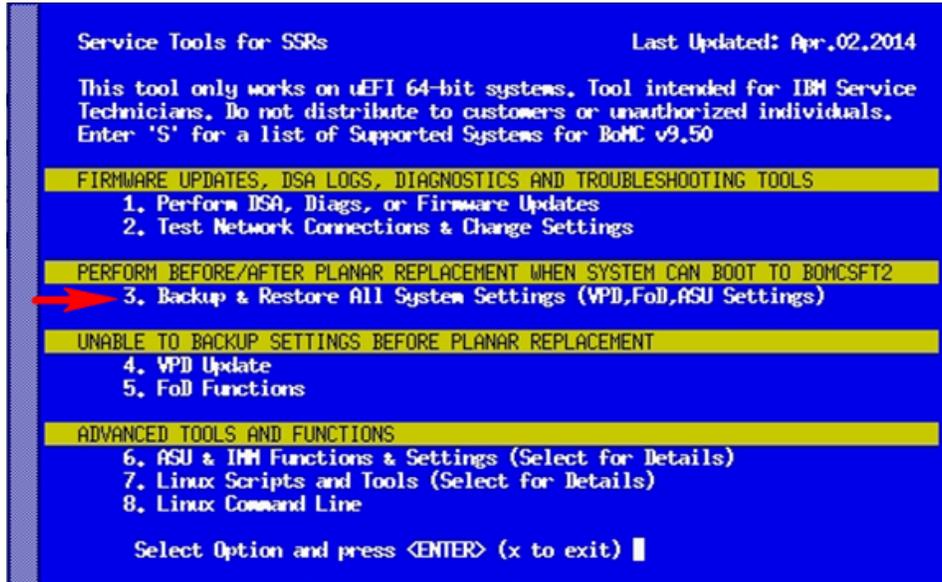


Figure 43: Blue Menu

The FoD must be obtained from the Lenovo FoD portal at <https://fod.lenovo.com/lkms/>. Refer to the “[Creating an FoD account](#)” section if you do not yet have access to the Web site.

6. Select **Retrieve History** on the FoD KMS Web site. Refer to **Figure 10** on “[Retrieve history](#)” topic for the details.
7. Select **Search history via machine type serial number** below the **Search type** drop-down menu as shown in **Figure 44**.
8. Enter the System x Machine Type and Serial Number in the **Search value** field.

Format: MMMSSSSSSSS where M = Type, S = Serial. Ensure uppercase letters are used. Do NOT use the Appliance Machine Type and Serial Number.

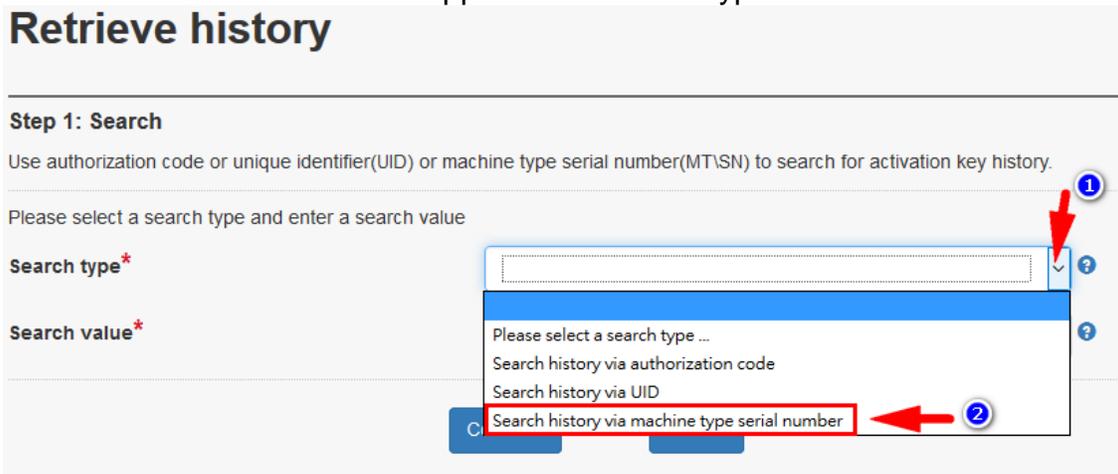


Figure 44: Retrieve history

Introducing the Features on Demand technology – FoD key installation after hardware replacement

9. Download all of the listed .key files to your root directory of your BoMCsft2 or BoMCsft3 USB Key.

Note: Steps 5 to 9 can be performed before arriving at the customer site.

Parts replacement (onsite)

Perform parts replacement by following the steps in the Installation & Service Guide (ISG), Problem Determination & Service Guide (PDSG), or Problem Determination & Service Guide Addendum, whichever is applicable to the Lenovo System x Appliance.

Installation Steps (onsite)

1. Insert the BoMCsft2/3 USB key in to the machine.
2. Boot the machine to F1, UEFI setup, and then select **Boot Manager → Boot from device**.
3. Select the USB port containing the BoMCsft2 device (usually USB front).
4. Select **3rd Party Tool** after booting the machine using BoMCsft2/3 successfully.
5. If you were able to back up the system board configuration prior to replacing parts, skip to step 8. Otherwise, use BoMCsft2's blue menu option 4 **VPD Update** as shown in **Figure 45** to set the VPD information.

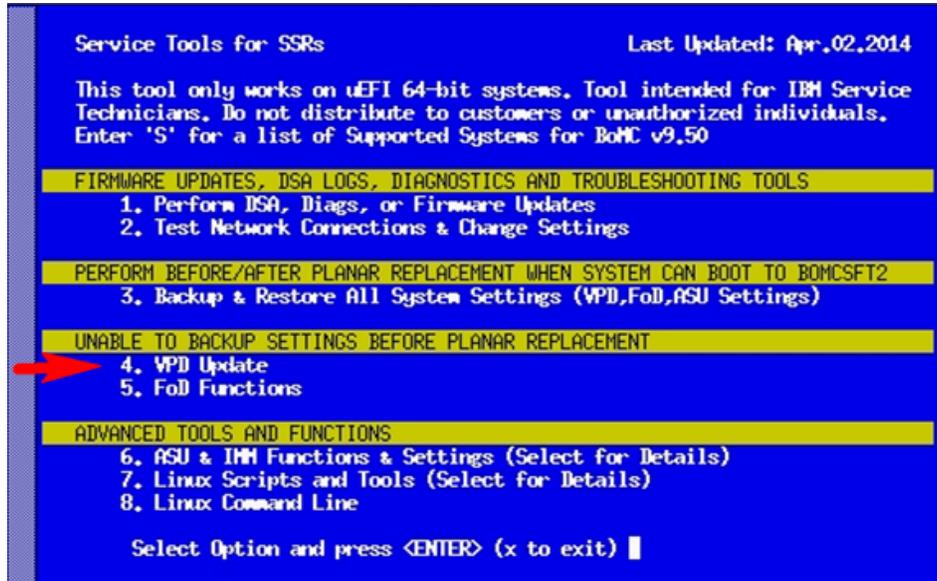


Figure 45: Blue menu option 4

6. Select blue menu option 5 **FoD Functions** as shown in **Figure 45**.
7. Select **Install FoD Key(s) Previously Saved for this server** (sub-option 4 as shown in **Figure 46**).

Introducing the Features on Demand technology – FoD key installation after hardware replacement

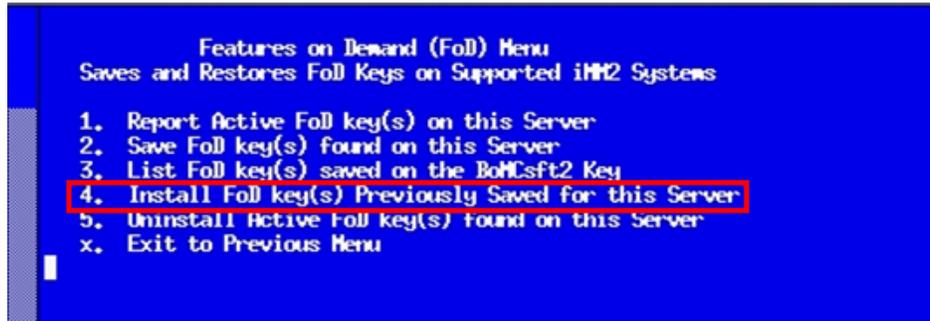


Figure 46: Sub option of blue menu option 5

8. Select blue menu option 3 **Backup and Restore All System Settings**.

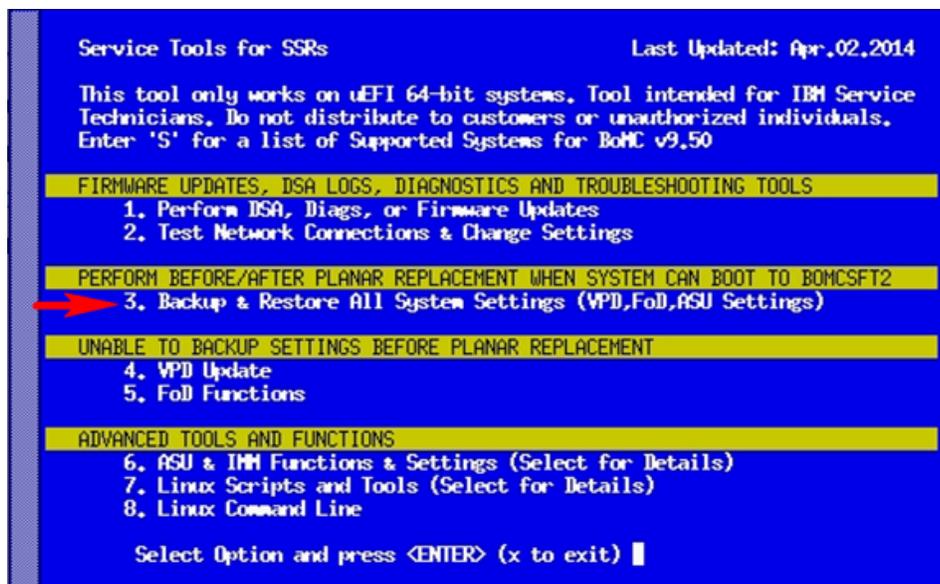


Figure 47: Blue menu option 3

9. Select **Restore Settings, VPD and FoD key(s)**, (sub option 3 as shown in **Figure 48**) if applicable to restore the system board configuration from the USB key.

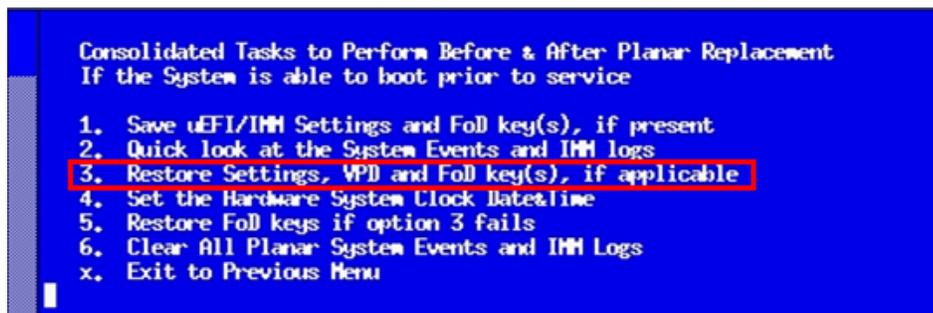


Figure 48: Sub option of blue menu option 3

Introducing the Features on Demand technology – FoD key installation after hardware replacement

Note: This will include restoring FoD key files that should already exist on the USB Key in the root directory from the steps above as well as the system VPD information. Depending on the machine involved, restarting the IMM (or rebooting the machine) may be required for the FoD to activate successfully.

Any issues with FoD activation should be directed to SSR Support. Refer to the [“FOD Handling Scope by SSRs”](#) section.

Using the System Management Interface to Save and Restore FoD Files

This method of saving and restoring FoD key files requires IP access and log in information to the system IMM. With the client’s permission, the field technician may connect a laptop directly to the IMM interface; however, the client also needs to provide the log in credentials. The default IMM IP address and login may be used after the system board is replaced.

Note: The BoMCsft2/3 tool will still need to be used to set the system MT and SN after system board replacement.

Start here to retrieve the FoD key files from the system with original system board installed. Skip to step 4 if the key files were already retrieved using the FoD portal (refer to the [Preparation section](#)).

1. Connect a laptop to the system management interface to access the IMM browser for the target machine.
2. Log in to the IMM browser interface and navigate to IMM Management – Activation Key Management as shown in **Figure 49**.

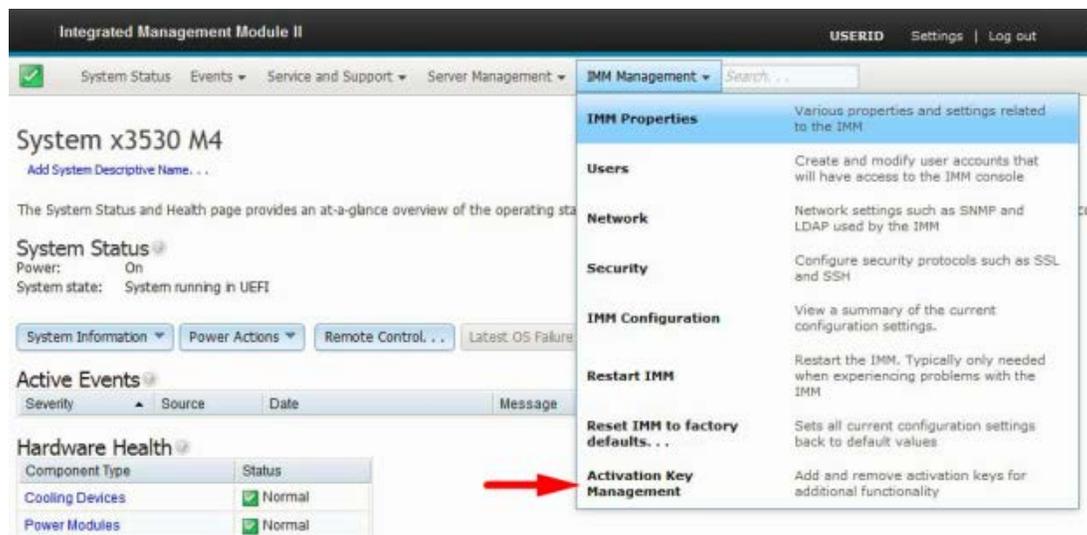


Figure 49: IMM Activation key management

Introducing the Features on Demand technology – FoD key installation after hardware replacement

3. Select each key in the list and select **Export** to download the file to your local storage.
4. Finish servicing the machine and after the new system board is installed, connect to the system management interface.
5. Verify that the correct MT and serial number are displayed for system VPD. If not, use the BOMCsft2/3 tool to fix the VPD, refer to step 5 in section “[Installation Steps \(onsite\)](#)”.
6. Login to the IMM browser interface and navigate to IMM Management – **Activation Key Management**.
7. Use the Add function (**Figure 50**), and select each of the key files that were previously downloaded to your local storage and upload them to the new system board.



Figure 50: Add activation key

8. Verify that the activation keys are installed and are valid, and then boot the machine.

Introducing the Features on Demand technology – Helpful links

Helpful links

Table 7: Helpful links	
Title	Link to materials
Portable DSA	http://support.lenovo.com/documents/SERV-DSA
User's Guide - Features on Demand	https://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=migr-5089568
Using System x Features on Demand	https://lenovopress.com/redp4895-using-system-x-features-on-demand
Introduction to the Lenovo KMS Portal	https://fod.lenovo.com/lkms/rest/contact/user_guide

Summary

This course enabled you to:

1. Provide an overview of the Features on Demand technology.
2. Explain how the key management works.
3. Explain how the activation management utility works.
4. Describe the connections between IBM Systems Director and Features on Demand.
5. Describe the activities that are required by the remote technical support agents.