![lenovo]

Lenovo ToolsCenter Suite
User's Guide

Version 10.1

Lenovo ToolsCenter Suite User's Guide

Version 10.1

> **Note**
>
> Before using this information and the product it supports, read the information in "Notices" on page 117.

Edition notice

This edition applies to version 10.1 of Lenovo® ToolsCenter Suite and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this publication

This publication provides information about how to download and use Lenovo ToolsCenter Suite.

Conventions and terminology

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 you 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 book, when you are instructed to enter a command, type the command and press Enter.

The following table provides a description of commonly used acronyms in the *Lenovo ToolsCenter Suite User's Guide* and graphical user interface.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
BMU	Bare Metal Update
CLI	Command Line Interface
CNA	Converged Network Adapter
DIMM	Dual Inline Memory Modules
Fix-id	Unique identifier for updates.
FoD	Features on Demand
FTP	File Transfer Protocol
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTP	Hypertext Transfer Protocol
IMM	Integrated Management Module
IPMI	Intelligent Platform Management Interface
IPMI SEL	Intelligent Platform Management Interface System Event Log
iSCSI	Internet Small Computer System Interface
KCS	Keyboard Controller Style Keyboard
KMS	Key Management System
LED	Light Emitting Diode

Table 1. Acronyms (continued)

Acronym	Definition
MAC	Media Access Control
OOB	Out-of-Band
PCIE	Peripheral Component Interconnect Express
PXE	Preboot Execute Environment
TCS	ToolsCenter Suite
uEFI	Unified Extensible Firmware Interface
UTF8	8-bit Unicode Transformation Format
UXSP	UpdateXpress System Pack
UXSPI	UpdateXpress System Pack Installer
VPD	Vital Product Data
WoL	Wake on LAN

Publications and related information

To view a PDF file, you need Adobe Acrobat Reader, which can be downloaded for free from the Adobe website at www.adobe.com/products/acrobat/readstep.html.

Information centers and topic collections

The IBM ToolsCenter for System x® and BladeCenter® Information Center provides integrated information for System x and BladeCenter tools: IBM® ToolsCenter for System x and BladeCenter Information Center.

Publications

The latest version of the *Lenovo ToolsCenter Suite User's Guide* can be downloaded from http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-USRGD.

This publication provides information about how to download and use ToolsCenter Suite to collect system information, configure firmware settings, and update firmware.

Web resources

The following websites and information center topics are resources for using Lenovo ToolsCenter Suite.

Websites

- ToolsCenter Suite (TCS) for Lenovo x 86 servers

  http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-TCSUITE

  Use this website to download the Lenovo ToolsCenter Suite tool and documentation.
- Lenovo ToolsCenter for Lenovo x86 servers

  http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-CENTER

Use this website to download tools that support System x and BladeCenter products.
- IBM PureSystems Redbooks®

  http://www.redbooks.ibm.com/portals/puresystems/

  Use this website to find published Redbooks on Flex Systems.
- Using System x Features on Demand Redbook

  http://www.redbooks.ibm.com/redbooks.nsf/RedpieceAbstracts/
  redp4895.html?Open

  Use this website to download the *Using IBM System x Features on Demand* publication.
- IBM Flex System Compute Nodes

  http://pic.dhe.ibm.com/infocenter/flexsys/information/topic/
  com.ibm.acc.common.nav.doc/compute_blades.html

  Use this web page to obtain information about Flex System Compute Nodes.
- BladeCenter Support and services

  http://www-03.ibm.com/systems/bladecenter/support/

  Use this website to obtain information about online technical support, downloads and drivers, and RETAIN® tips for BladeCenter products.
- System x support and services

  http://www-03.ibm.com/systems/x/support/

  Use this website to obtain information about online technical support, downloads and drivers, and RETAIN tips for System x products.
- ServerProven®

  http://www-03.ibm.com/servers/eserver/serverproven/compat/us/
  indexsp.html

  Use this website to obtain information about the hardware compatibility of System x and BladeCenter systems with IBM applications and middleware.

Forums

- developerWorks Forums

  https://www.ibm.com/developerworks/community/forums/html/
  forum?id=11111111-0000-0000-0000-000000002691#topicsPg=0

  Use this website on ibm.com® to learn about various forums that are available to discuss technology-related and product-related issues pertaining to System x hardware and software products. This website includes a link for obtaining the forum using a Rich Site Summary (RSS) feed.
- IBM BladeCenter Forum

  https://www.ibm.com/developerworks/community/forums/html/
  forum?id=11111111-0000-0000-0000-000000000819

  Use this website on ibm.com to learn about various forums that are available to discuss technology-related and product-related issues pertaining to BladeCenter hardware and software products. This website includes a link for accessing the forum using a Rich Site Summary (RSS) feed.

New in this release

ToolsCenter Suite 10.1 provides a number of enhancements since the previous release, v9.63.

New system support

The following hardware is now supported by Lenovo ToolsCenter Suite 10.1:
- IBM Flex System x240, 8956
- Lenovo Flex System x240, 7162, 2588
- Lenovo Flex System x280 X6/x480 X6/x880 X6 Compute Node, 4258, 7196
- Lenovo Flex System x440, 7167, 2590
- Lenovo System x3500 M5, 5464
- Lenovo System x3750 M4, 8753
- Lenovo System x3850 X6/x3950 X6, 6241

New operating system support

The following new operating systems are supported by Lenovo ToolsCenter Suite 10.1:
- Red Hat Enterprise Linux, version 7.1
- Red Hat Enterprise Linux, version 6.7
- SUSE Linux Enterprise Server 12 (x86/x64)
- SUSE Linux Enterprise Server 11.4 (x86/x64)

For complete operating system support information, see the "Supported operating systems" topic of the User's Guide.

New server options support

None

Problem(s) fixed

The following problem has been fixed in ToolsCenter Suite 10.1:
- ToolsCenter Suite returns errors if some firmware settings are not found on x3250 M5.

Enhancement(s)

None

Known limitations

The Bare Metal Update function does not work with the latest IMM firmware due to an unknown issue.

Workarounds

None

Warnings

None

Dependencies

None

Chapter 1. Technical overview

Lenovo ToolsCenter Suite is a collection of server management tools that help manage your System x, BladeCenter, and Flex System environment. ToolsCenter Suite provides full support of in-band management of updates, configuration, and system information on a local machine and out-of-band (OOB) management of updates, configuration, and system information on a remote machine.

The three main functions of ToolsCenter Suite are:

Updates:
> You can use the Updates function to update the UpdateXpress System Pack firmware and drivers or individual firmware and drivers by connecting to the Lenovo website or a local repository. There are three update methods:
> - Recommended Updates
> - Individual Updates
> - Download Updates

Configuration:
> You can use the Configuration function to modify firmware settings, change frequently used settings, or change an individual configuration using the Full Settings option.
>
> **Frequently Used Settings**:
> - Activation Key Management (for Features on Demand)
> - Boot Order
> - Energy and Performance
> - IMM User Accounts
> - System Contact
> - Features on Demand Mass Activation
>
> **Full settings**:
> - BootOrder
> - IMM
> - iSCSI
> - Network
> - PXE
> - SYSTEM_PROD_DATA
> - uEFI

System Information:
> You can use the System Information function to collect full system information, catalog this information, and send the collected information to a Lenovo support team or customer site FTP server. This function also provides system health status, including the IMM system event logs and Light Path information.
>
> ToolsCenter Suite collects full system information about the following aspects of a system for both a local machine and a remote machine:
> - Alerts
> - Basic analysis and highlights

- Hardware
- Logs
- Software (including Operating Systems)

Prerequisites

ToolsCenter Suite requires the following prerequisites:
- You must have administrator or root-equivalent operating-system privileges to use ToolsCenter Suite.
- An Internet connection is required to download updates from the Lenovo website, or to send the collected system information file to the Lenovo website or the customer site FTP server.
- A browser supported by ToolsCenter Suite. For a complete list of supported browsers, refer to the Supported web browsers topic of the *ToolsCenter Suite User's Guide*.
- To ensure ToolsCenter Suite works correctly, verify that Java script and CSS are enabled in your browser settings.

Chapter 2. Lenovo ToolsCenter Suite support list

Lenovo ToolsCenter Suite has specific hardware, operating system, and browser support lists. If you attempt to run ToolsCenter Suite on a server, browser, or operating system that is not on the list, this will be at your own risk with no functional guarantee. Before you begin using ToolsCenter Suite, review the hardware, operating system, and browser support sections.

Supported hardware

ToolsCenter Suite supports the systems listed in the following table.

Table 2. Supported systems

Server	Machine type
IBM BladeCenter HS22	1911, 1936, 7809, 7870
IBM BladeCenter HS22V	1949, 7871
IBM BladeCenter HS23	1929, 7875
IBM BladeCenter HS23E	8038, 8039
IBM BladeCenter HX5	1909, 1910, 7872, 7873
IBM Flex System x220 Compute Node	2585, 7906
IBM Flex System x222 Compute Node	7916
IBM Flex System x240 Compute Node	7863, 8737, 8738, 8956
Lenovo Flex System x240 M5 Compute Node	2591, 9532
IBM Flex System x280/x480/x880 X6 Compute Node	4259, 7903
Lenovo Flex System x280 X6/x480 X6/x880 X6 Compute Node	4258, 7196
Lenovo Flex System x280 X6/x480 X6/x880 X6 Compute Node	7162, 2588
Lenovo Flex System x280/x480/x880 X6 Compute Node	7196
IBM Flex System x440 Compute Node	7917
Lenovo Flex System x440 Compute Node	2590, 7167
IBM NeXtScale nx360 M4	5455
Lenovo NeXtScale nx360 M5	5465
Lenovo NeXtScale nx360 M5 DWC	5467
IBM System x iDataPlex® Direct Water Cooled dx360 M4 server	7918, 7919
IBM System x iDataPlex dx360 M2 server	6380, 7321, 7323
IBM System x iDataPlex dx360 M3	6391
IBM System x iDataPlex dx360 M4	7912, 7913
IBM System x iDataPlex dx360 M4 Water Cooled	7918, 7919
IBM System x3100 M4	2582

Table 2. Supported systems (continued)

Server	Machine type
IBM System x3100 M5	5457
IBM System x3200 M3	7327, 7328
IBM System x3250 M3	4251, 4252, 4261
IBM System x3250 M4	2583
IBM System x3250 M5	5458
IBM System x3400 M2	7836, 7837
IBM System x3400 M3	7378, 7379
IBM System x3500 M2	7839
IBM System x3500 M3	7380
IBM System x3500 M4	7383
Lenovo System x3500 M5	5464
IBM System x3530 M4	7160
IBM System x3550 M2	4198, 7946
IBM System x3550 M3	4254, 7944
IBM System x3550 M4	7914
Lenovo System x3550 M5	5463
IBM System x3620 M3	7376
IBM System x3630 M3	7377
IBM System x3630 M4	7158
IBM System x3650 M2	4199, 7947
IBM System x3650 M3	4255, 5454, 7945
IBM System x3650 M4	7915
IBM System x3650 M4 BD	5460, 5466
Lenovo System x3650 M5	5462
IBM System x3690 X5	7147, 7148, 7149, 7192
IBM System x3750 M4	8718, 8722, 8733, 8752
Lenovo System x3750 M4	8753
IBM System x3755 M3	7164
IBM System x3850/x3950 X5	7143, 7145, 7146, 7191
IBM System x3850/x3950 X6	3837, 3839
Lenovo System x3850 X6/x3950 X6	6241

Supported operating systems

Use the information in this section to identify operating systems that are supported by ToolsCenter Suite:

Windows

ToolsCenter Suite supports the following Windows operating systems.

Microsoft Windows Server 2012 Edition
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Microsoft Windows Server 2011 Editions
- Microsoft Windows Small Business Server 2011
- Microsoft Windows Small Business Server 2011 Essentials

Microsoft Windows Server 2008 Editions
- Microsoft Windows Essential Business Server 2008 Premium Edition
- Microsoft Windows Essential Business Server 2008 Standard Edition
- Microsoft Windows Server 2008, Datacenter Edition (x86, x64)
- Microsoft Windows Server 2008, Enterprise Edition (x86, x64)
- Microsoft Windows Server 2008 Foundation
- Microsoft Windows Server 2008 HPC Edition
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 R2 HPC Edition (x64, Reseller Option Kit)
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008, Standard Edition (x86, x64)
- Microsoft Windows Server 2008, Web Edition (x86, x64)

Linux

ToolsCenter Suite supports the following Linux operating systems.

Red Hat
- Red Hat Enterprise Linux 7 Server (x64) Editions (U1)
- Red Hat Enterprise Linux 6 Server (x86 & x64) Editions, (up to U7)
- Red Hat Enterprise Linux 5 Update 10 Server (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 10 Server with Xen (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 9 Server (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 9 Server with Xen (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 8 Server (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 8 Server with Xen (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 7 Server (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Update 7 Server with Xen (x86 & x64) Editions
- Red Hat Enterprise Linux 5 Server (x86 & x64) Editions, (up to U6)
- Red Hat Enterprise Linux 5 Server with Xen (x86 & x64) Editions, (up to U6)

SUSE
- SUSE Linux Enterprise Server 12 (x86 & x64)
- SUSE Linux Enterprise Server 11 (x86 & x64) SP4
- SUSE Linux Enterprise Server 11 with Xen (x86 & x64) SP3
- SUSE Linux Enterprise Server 11 (x86 & x64) SP2
- SUSE Linux Enterprise Server 11 with Xen (x86 & x64) SP2
- SUSE Linux Enterprise Server 11 (x86 & x64) (up to SP1)
- SUSE Linux Enterprise Server 11 with Xen (x86 & x64) (up to SP1)
- SUSE Linux Enterprise Real Time 10 AMD64/EM64T
- SUSE Linux Enterprise Server 10 (x86 & x64) (up to SP4)
- SUSE Linux Enterprise Server 10 with Xen (x86 & x64) (up to SP4)

Supported browsers

To view the information that is collected by ToolsCenter Suite, you must use one of these web browsers:

- Firefox 3.6 or later
- Google Chrome 19.0 or later
- Internet Explorer 8.0 Service Pack 1 or later

Chapter 3. Downloading and starting Lenovo ToolsCenter Suite

The topics in this section describe how to download and start Lenovo ToolsCenter Suite.

Downloading ToolsCenter Suite

ToolsCenter Suite is a self-extracting application that does not require installation.

About this task

ToolsCenter Suite is available for download from ToolsCenter Suite (TCS) for Lenovo x 86 servers at http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-TCSUITE.

Procedure

1. Select one of the following shipment packages:
   - `lnvgy_utl_tcsuite_10.1_winsrvr_i386.zip`
   - `lnvgy_utl_tcsuite_10.1_winsrvr_x86-64.zip`
   - `lnvgy_utl_tcsuite_10.1_rhel5_i386.tgz`
   - `lnvgy_utl_tcsuite_10.1_rhel5_x86-64.tgz`
   - `lnvgy_utl_tcsuite_10.1_rhel6_i386.tgz`
   - `lnvgy_utl_tcsuite_10.1_rhel6_x86-64.tgz`
   - `lnvgy_utl_tcsuite_10.1_rhel7_x86-64.tgz`
   - `lnvgy_utl_tcsuite_10.1_sles10_i386.tgz`
   - `lnvgy_utl_tcsuite_10.1_sles10_x86-64.tgz`
   - `lnvgy_utl_tcsuite_10.1_sles11_i386.tgz`
   - `lnvgy_utl_tcsuite_10.1_sles11_x86-64.tgz`
   - `lnvgy_utl_tcsuite_10.1_sles12_x86-64.tgz`
2. After downloading the appropriate ToolsCenter Suite zip file, double-click the file to complete the file extraction.

Lenovo ToolsCenter Suite files

This section describes where ToolsCenter Suite files are stored.

The ToolsCenter Suite log file

The ToolsCenter Suite log file is stored in the `%ToolsCenterSuite%\apache-tomcat-7.0.26\webapps\tcsuite\WEB-INF\logs` directory. `%ToolsCenterSuite%` is the working directory.

New log information is appended to the `tcsuite_20120909225751.log` file. The number in the log file name represents: year/month/date/hour/minute/second.

Update files

The update files that are downloaded using one of the Update options are stored in the following directories.

UpdateXpress System Pack XML and binary files:
    %ToolsCenterSuite%\apache-tomcat-7.0.26\webapps\tcsuite\WEB-INF\
    depot\Update\%MachineType%\%OperatingSystem%\uxsp

Individual XML and binary files:
    %ToolsCenterSuite%\apache-tomcat-7.0.26\webapps\tcsuite\WEB-INF\
    depot\Update\%MachineType%\%OperatingSystem%\individual

%ToolsCenterSuite%:
    The ToolsCenter Suite working directory

%MachineType%:
    The four-digit machine type of the server and represents the machine type selected

%OperatingSytem%:
    The server operating system

Starting ToolsCenter Suite

After you have downloaded and copied the appropriate ToolsCenter Suite zip file for the target server and extracted the files, you can start the ToolsCenter Suite program. ToolsCenter Suite must be run on the target server.

Before you begin

When starting ToolsCenter Suite for the first time, you are prompted to read the terms of the license agreement. After accepting the terms of the license agreement, this page does not display again. If you need to reference the license agreement again, there is a link in the **About** menu item for viewing the license agreement.

Note: ToolsCenter Suite does not support running concurrent sessions of ToolsCenter Suite. If another session of ToolsCenter Suite is already open with active operations that cannot be stopped, such as configuration and inventory updates or compare and updates, a message is displayed stating:

    Another user is currently logged in and performing an operation that cannot
    be interrupted. Wait for several minutes, and log in again.

However is the session that is already open is able to stop, a message is displayed stating:

    Another user is currently logged in with the same user ID. Do you want to
    log in with the same user ID?
    If you select Yes, the user currently logged in will automatically be logged out.
    If you select No, you will return to the login page, where you can enter
    a different user ID.

About this task

Complete the appropriate steps for your operating system:
- For a Windows system, perform steps 1 and 3.
- For a Linux system, perform steps 2 and 3.

Procedure

1. For Windows, double click **run.bat**. The ToolsCenter Suite script file launches the Tomcat server and starts the default browser.

   Note: The first time using ToolsCenter Suite, the ToolsCenter Suite License Agreement page opens.
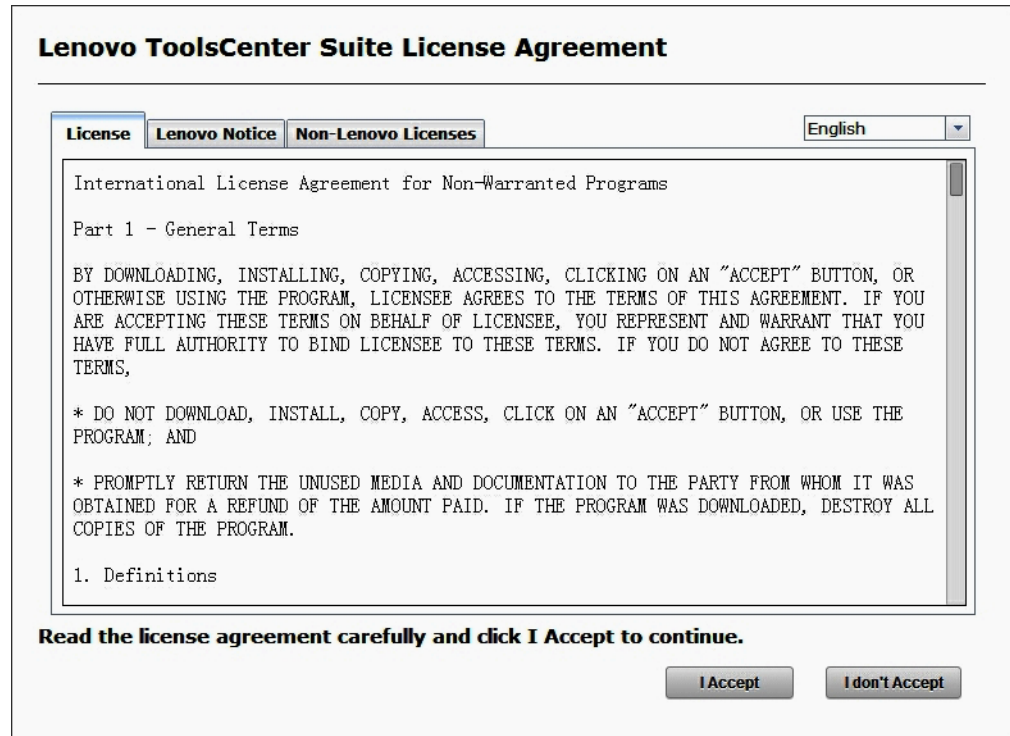
Figure 1. License Agreement

   On subsequent sessions of ToolsCenter Suite, the ToolsCenter Suite Home page opens.

2. For Linux, double click **run.sh**. The ToolsCenter Suite script file launches the Tomcat server and starts the default browser.

   Note: The first time using ToolsCenter Suite, the ToolsCenter Suite License Agreement page opens. On subsequent sessions of ToolsCenter Suite, the ToolsCenter Suite Home page opens.

3. Read the license agreement and click **I accept**.

   The ToolsCenter Suite Home page opens.
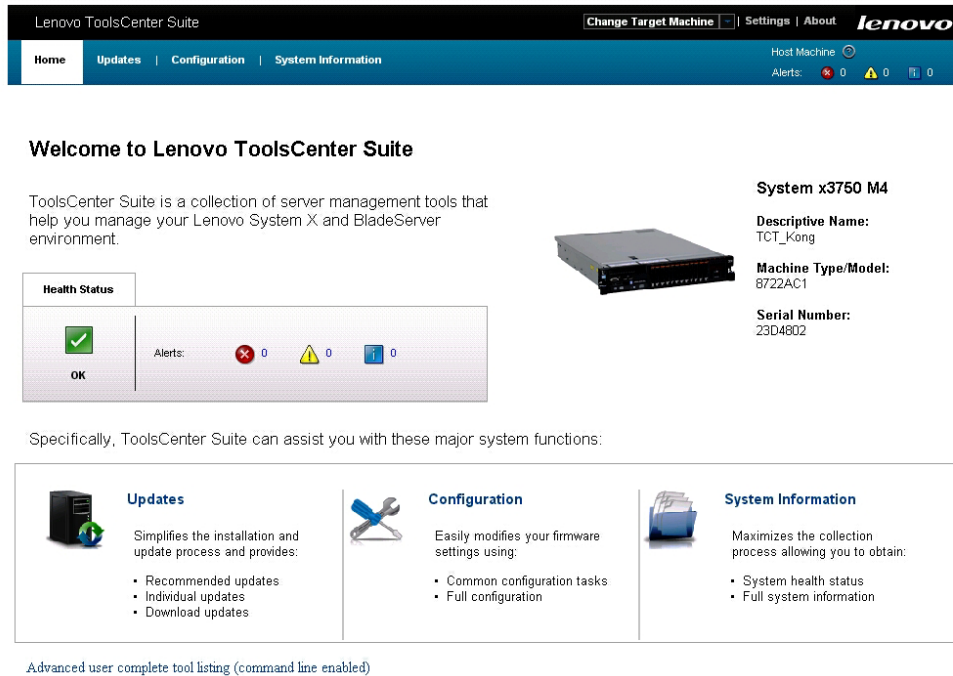
Figure 2. Home page

What to do next

The Home page provides access to the ToolsCenter Suite functions, the **Settings** and **About** menu items, the **Advanced User Complete Tool Listing**, and the following information:

- Machine name
- Descriptive Name
- Machine Type/Model
- Serial Number
- Health Status
- Alerts

Viewing the Advanced User Complete Tool Listing

The Advanced User Complete Tool Listing provides a list of command line and deployment tools and support page links for each of these advanced user tools.

Procedure

1. To view the list of the Command Line and Deployment Tools, click **Advanced User Complete Tool Listing** on the Home page. The Advanced User Complete Tools Listing window opens.
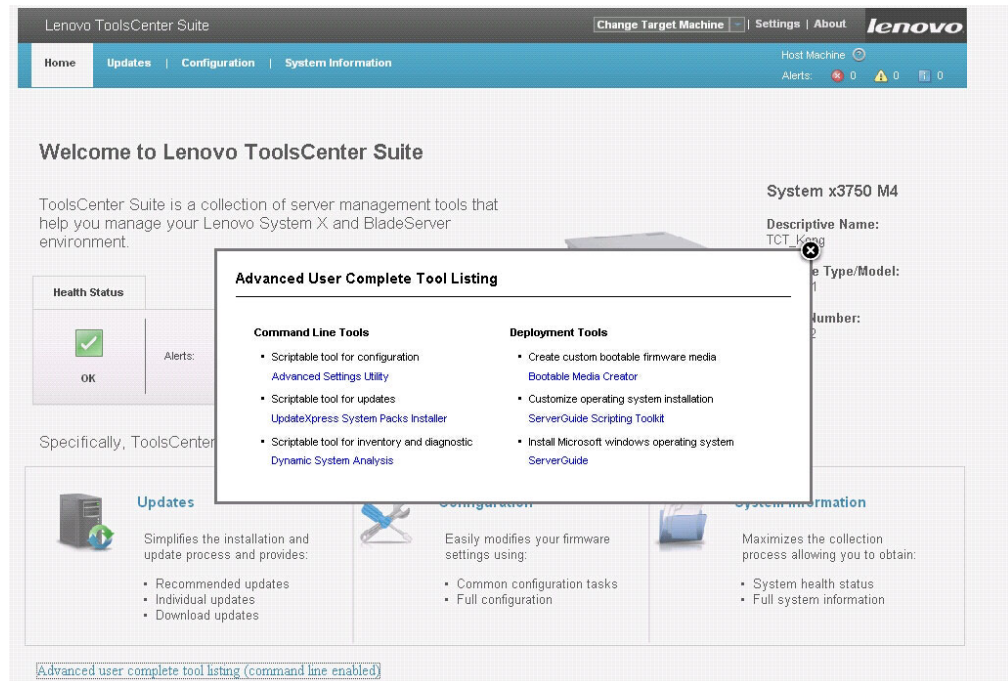
Figure 3. Advanced User Complete Tool Listing

2. To view one of the items in the list, click a link. A browser window opens for the related support page.

3. To close the Advanced User Complete Tool Listing window and return to the Home page, click **x**.

ToolsCenter Suite menu options

The ToolsCenter Suite graphical user interface (GUI) has the following menu options:

Change Target Machine
> You can use the **Change Target Machine** option to connect to a remote machine or a ToolsCenter Suite host machine.

Settings
> Configures your internet connection. For more information, see "Configuring your Internet Connection settings" on page 12.

About Provides the ToolsCenter Suite version, the terms of use link, the ToolsCenter Suite website link, and a link to download the latest version of the *ToolsCenter Suite User's Guide*.

Home Opens the ToolsCenter Suite primary page.

Updates
> Provides several options for downloading and installing firmware and driver updates.

Configuration
> Assists you in modifying firmware settings.
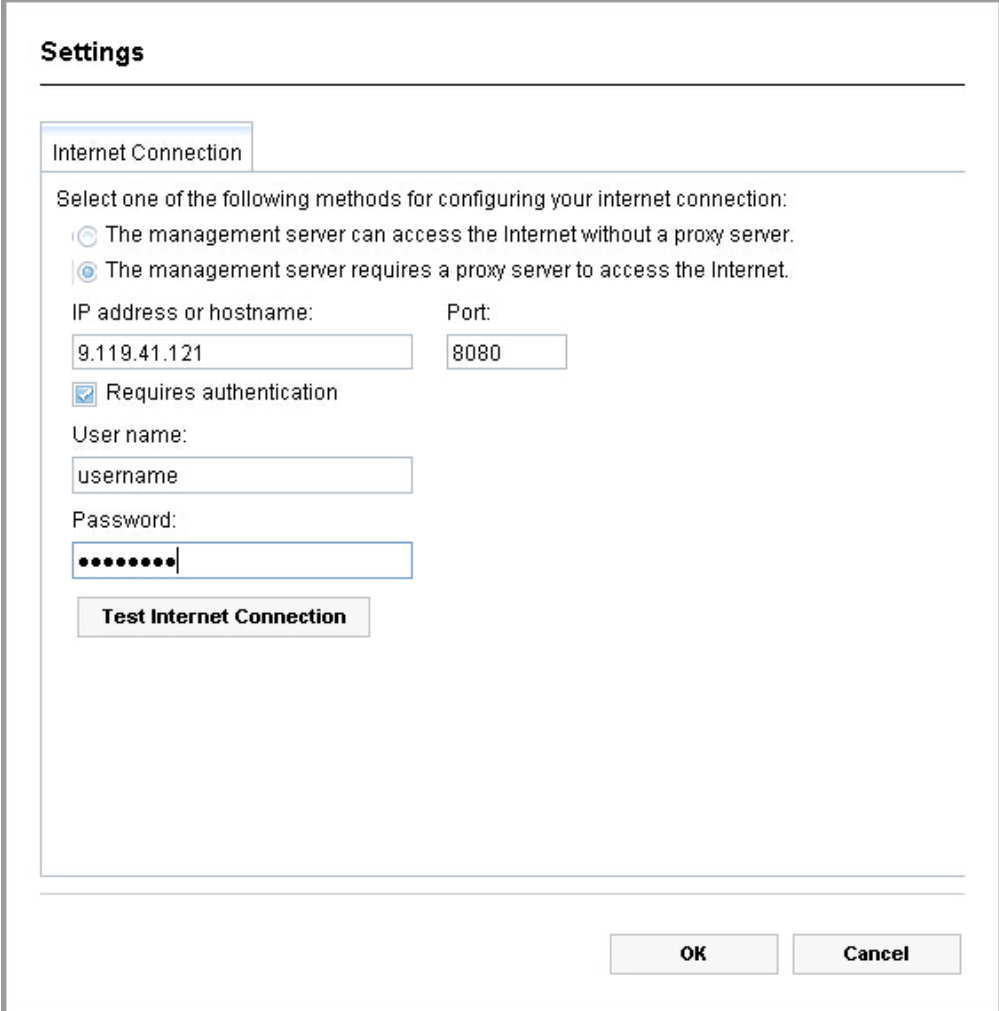
System Information
> Maximizes the system information collection process, providing system health status and full system information.

Configuring your Internet Connection settings

The following procedure describes how to configure and test your internet connection using proxy settings. Proxy settings are used for the `Send to Lenovo` and `Send to FTP` options of the **System Information** function. Proxy settings use an HTTP proxy. ToolsCenter Suite uses the **HTTP/1.1 CONNECT** method with UTF-8 encoding and passive ftp mode to connect with the HTTP proxy. An Internet connection is required for using the **Updates** and **Feature on Demand** by proxy functions.

Procedure

1. Click **Settings** on the title bar of the ToolsCenter Suite screen. The Settings dialog box opens.

Figure 4. Settings - Internet Connection

2. Select one of following options for configuring your internet connection:
   a. **The management server can access the Internet without a proxy server**. The IP address or host name, Port, Username, and Password fields are greyed out.
   b. **The management server requires a proxy server to access the Internet**. For this option, complete the following steps.
      1) Enter the `IP address or host name`.

2) Enter the `Port`.

3) Select **Requires authentication** to enable the authentication fields and enter the following information:

- `User name`
- `Password`

3. Click **Test Internet Connection**. This operation verifies whether the internet connection is working.

   The internet connection test checks the proxy settings and displays the results.

4. Click **OK** to save the internet connection settings or click **Cancel** to not save any changes and quit **Settings**.

Chapter 4. Using the Updates function

The topics in this section provide complete instructions for each of the Updates options. The Updates function checks the compliance of firmware and drivers, download and install firmware and device drivers, add support for new systems, and manage updates on a local machine using in-band mode and out-of-band (OOB) mode for a remote machine.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **Updates**.

   The Firmware and Driver Updates page opens.
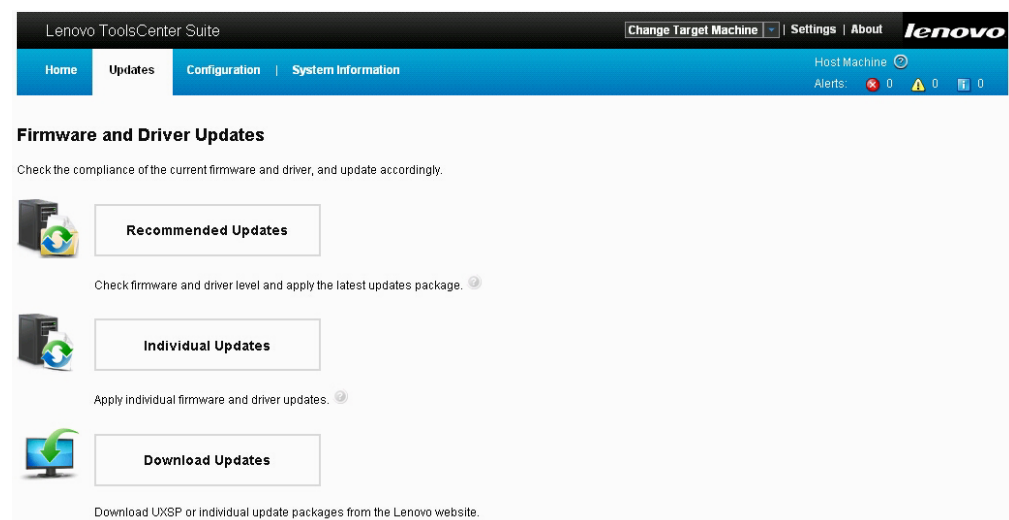
Figure 5. Firmware and Driver Updates

   Tip: To view additional information for each type of update, hover the mouse pointer over the question mark icon.

2. Select one of the **Updates** options:
   - **Recommended Updates**: This option checks the firmware and driver levels of the latest UpdateXpress System Pack, from the Lenovo website or in a local directory, and compares the recommended updates with the local machine installed firmware and driver levels. You can selectively download and apply UpdateXpress System Pack firmware and driver updates from the Lenovo website or selectively apply firmware and driver UpdateXpress System Pack updates from a local directory.
   - **Individual Updates**: This option checks the firmware and driver levels and compares the currently installed firmware and drivers to the individual updates on the Lenovo website or in a local directory. You can selectively download and apply firmware and driver updates from the Lenovo website or selectively apply firmware and driver updates from a local directory.
   - **Download Updates**: This option downloads an UpdateXpress System Pack or an individual update package for a specific machine type and operating system. Updates are downloaded to a specified directory and can be applied at any time.

Example: You can download Updates that can be applied when a lab machine (A) needs to update the firmware or a driver, but does not have internet access. You can use another lab machine (B) with internet access, to download the update packages for lab machine A. Use one of the following two methods; the first method is easier to use and recommended.

a. Copy the entire ToolsCenter Suite working directory on lab machine B to lab machine A. Launch ToolsCenter Suite on lab machine A. The updates can be done from the local directory.

b. If lab machine A has ToolsCenter Suite software, copy the downloaded update packages under the ToolsCenter Suite working directory on lab machine B to ToolsCenter Suite working directory on lab machine A. Launch ToolsCenter Suite in lab machine A. The updates can then be done from the local directory.

The Recommended Update Wizard

The Recommended Updates Wizard checks the firmware and driver levels and applies a package of updates (UpdateXpress System Pack). This option is the preferred method for obtaining firmware and driver updates for the server because the UpdateXpress System Pack consists of an integration-tested software bundle of updatable firmware and device driver updates for each System x, BladeCenter server, and Flex System.

Using the latest UXSP updates package from the Lenovo website option

By using **The latest UXSP updates package from the Lenovo website** option, you can download and apply the latest UpdateXpress System Pack updates package from the Lenovo website.

Procedure

1. Click **Recommended Updates** on the Firmware and Driver Updates page. The Firmware and Driver Updates page of the Recommended Update Wizard opens.

Figure 6. Recommended Update Wizard

2. Select **The latest UXSP updates package from the Lenovo website**.

3. Optional: You can select to **Also include updates that are not installed or undetected**. Select this option only if you have any unknown devices and you need to detect all possible hardware in this system.

4. Click **Next** to complete the check firmware compliance step, or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

   - Click **OK** to quit the update wizard.
   - Click **Cancel** to continue the update process.

   The check firmware compliance step acquires the current machine's UXSP firmware and driver levels from the Lenovo website.
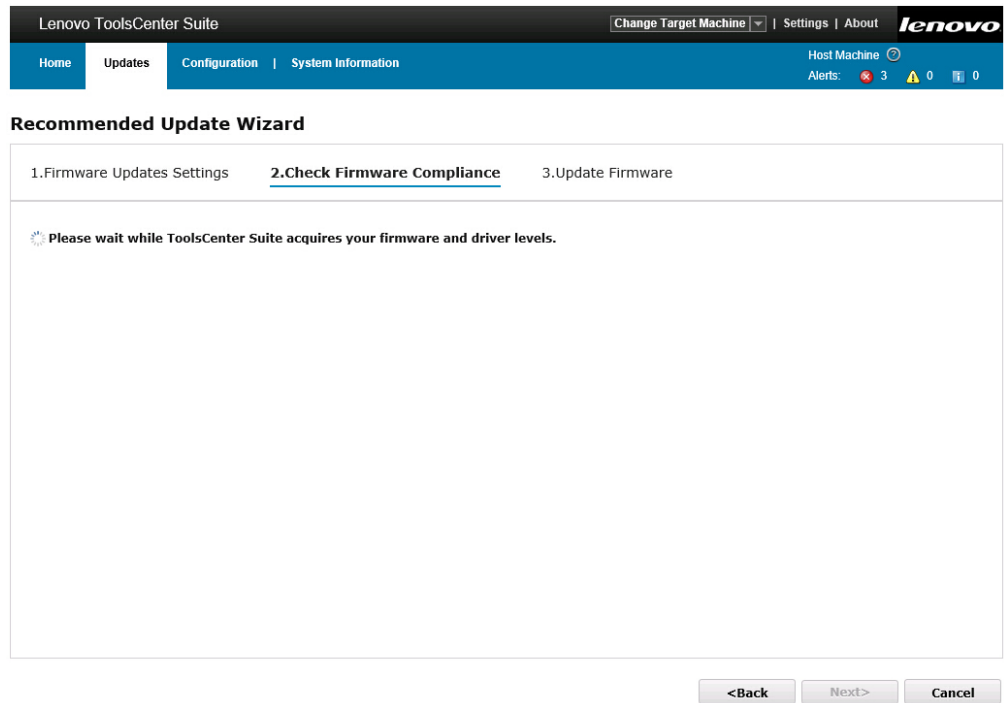
Figure 7. Recommended Updates - acquiring the current machine's UXSP firmware and driver levels

During the acquire operation, the progress icon is displayed and the current page is locked, **Cancel** is enabled, and the following message is displayed:

`Please wait while ToolsCenter Suite acquires your firmware and driver levels.`

After the acquire operation finishes, the check firmware compliance operation begins.
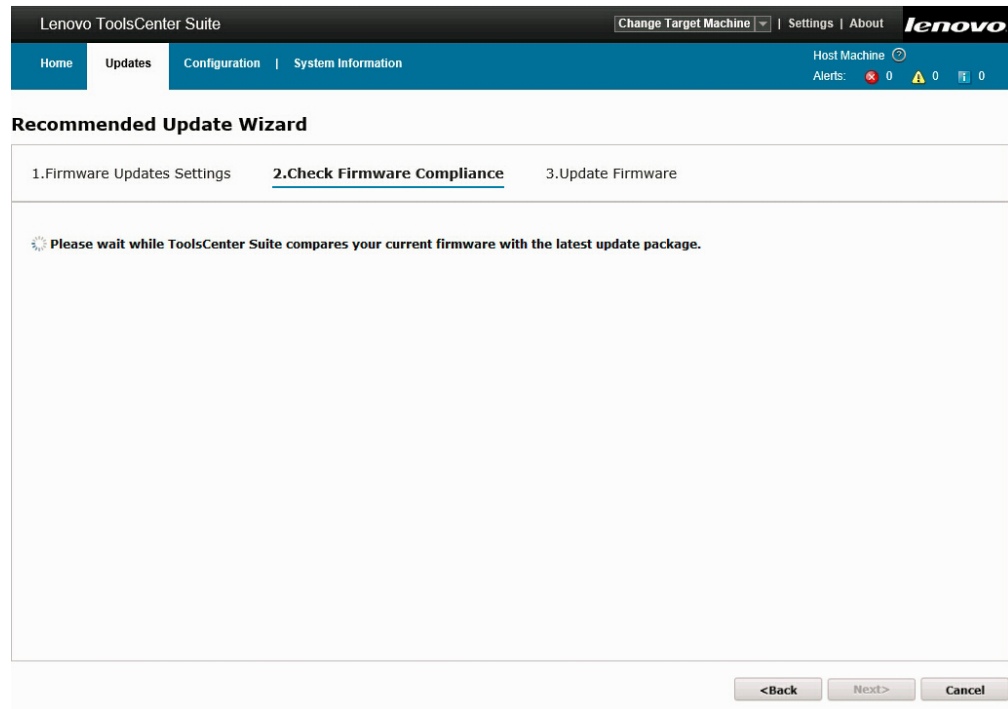
Figure 8. Recommended Updates - checking the current machine's UXSP firmware and driver levels

While the compliance check firmware compliance operation is working, the current page is locked, **Cancel** is disabled, and the following message is displayed:

```
Please wait while ToolsCenter Suite compares your current firmware and drivers
 with the latest update package.
```

Note: If you are not connected to the Internet, the Configure Internet Connection dialog box opens. Check your configuration or try again, otherwise, click **OK** to continue or **Cancel**. For more information, see "Configuring your Internet Connection settings" on page 12.

When the check firmware compliance operation finishes, the number of items with new versions is displayed above the firmware and driver updates table.

Lenovo ToolsCenter Suite   Change Target Machine ▾ | Settings | About   **lenovo**

Home   **Updates**   Configuration | System Information   Host Machine ⊙

Alerts: ⊗ 2   ⚠ 0   ▮ 0

Recommended Update Wizard

1.Firmware Updates Settings   **2.Check Firmware Compliance**   3.Update Firmware

ⓘ **Compliance check complete. Select the desired firmware components and then click "Next" to update.**

9 firmware and drivers items available. The recommended items were selected by default.

	Name	Severity	New Version	Installed Version	Reboot Required
☐	ibm_dd_mpt3sas_2.50.75.00_windows_32-64	Not Required			Yes
☐	⌐ lsi_sas3.sys (stopped)		2.50.75.00	2.50.65.00	
☐	ibm_dd_sraidmr_6.702.07.00-2_windows_32-64	Not Required			Yes

12 HBA/CNA items available. If an HBA/CNA update is needed, contact the vendor to confirm it.

	Name	Severity	New Version	Installed Version	Reboot Required
☑	brcm_dd_nic_16.8.0.3_windows_32-64	Suggested			Yes
☑	⌐ b57nd60a.sys		16.8.0.3	16.2.0.4	
☐	brcm_dd_nic_7.10.30.0_windows_32-64	Not Required			Yes

<Back   Next>   Cancel

Figure 9. Recommended Updates - Check Firmware Compliance results

By default, all updates listed in the table are checked and preselected for updating and can be deselected.

The firmware and driver updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version number
- Installed Version: current version number or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

The HBA/CNA updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version number
- Installed Version: current version number or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

5. Optional: If there are any updates that you do not want to download and install, deselect those updates in the left column.

6. Click **Next** to proceed with the update process. If you selected to install firmware or drivers that includes OS agnostic software (including uEFI/IMM/DSA/FPGA updates), for inband updates, ToolsCenter Suite checks whether the entered user name and password is able to pass the IMM user authentication.

Complete the following steps:

a. Enter the IMM credentials:

- IMM User Name
- Password

b. Click **Target the secondary firmware bank** to have the secondary or alternate flash bank targeted if it is available. If a secondary or alternate device is not supported the IMM may ignore this option.

c. Click **Continue Updates**.

If IMM authentication passes, the firmware and driver installation continues. To install the OS agnostic software, the IMM account and password must pass authentication. If you cannot pass IMM account and password authentication, deselect the OS agnostic software to continue the firmware and driver installation without the OS agnostic software.

7. Click **Continue Update** to proceed to the update firmware step by downloading the UXSP updates from the Lenovo website and applying the downloaded firmware and drivers, or click **Cancel** to return to the Firmware and Driver Updates page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box is displayed, asking if you are sure you want to cancel the whole update process? Click one of the follow options:

- Click **OK** to quit the update wizard.
- Click **Cancel** to continue the update process.

During the download operation, the progress of the current downloading item indicates the total bytes and the downloaded bytes. A progress bar provides the overall progress of all download items. The updates listed in the table display the status as either: Not Started, Downloading, and Downloaded.

You can click **Stop** to stop downloading the current item.
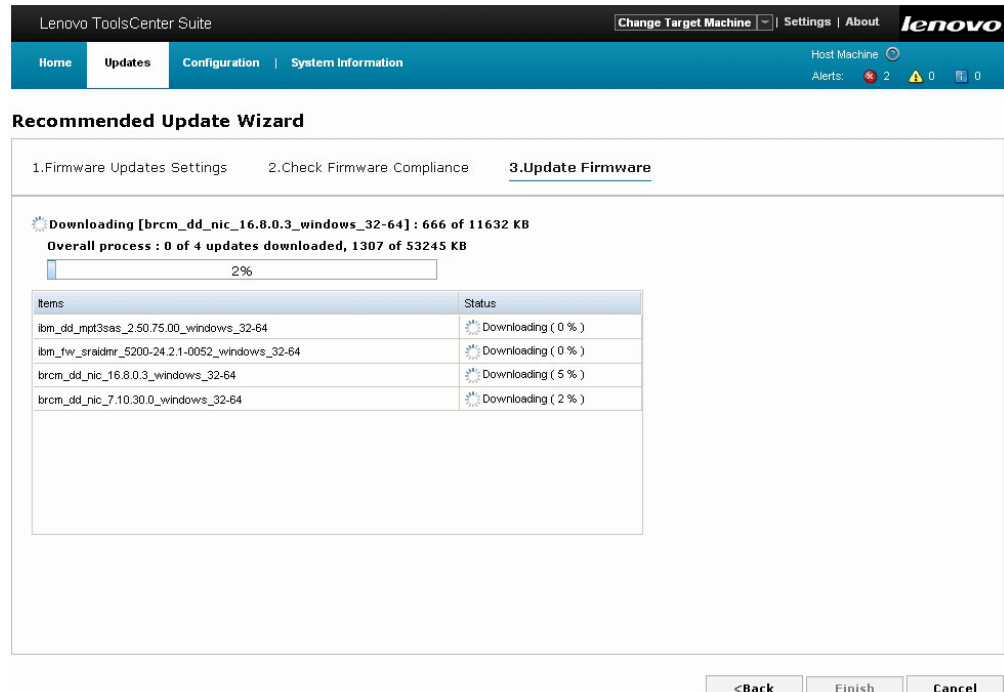
Figure 10. Recommended Updates - UXSP downloading from the Lenovo website

When the download operation finishes, the update operation begins.
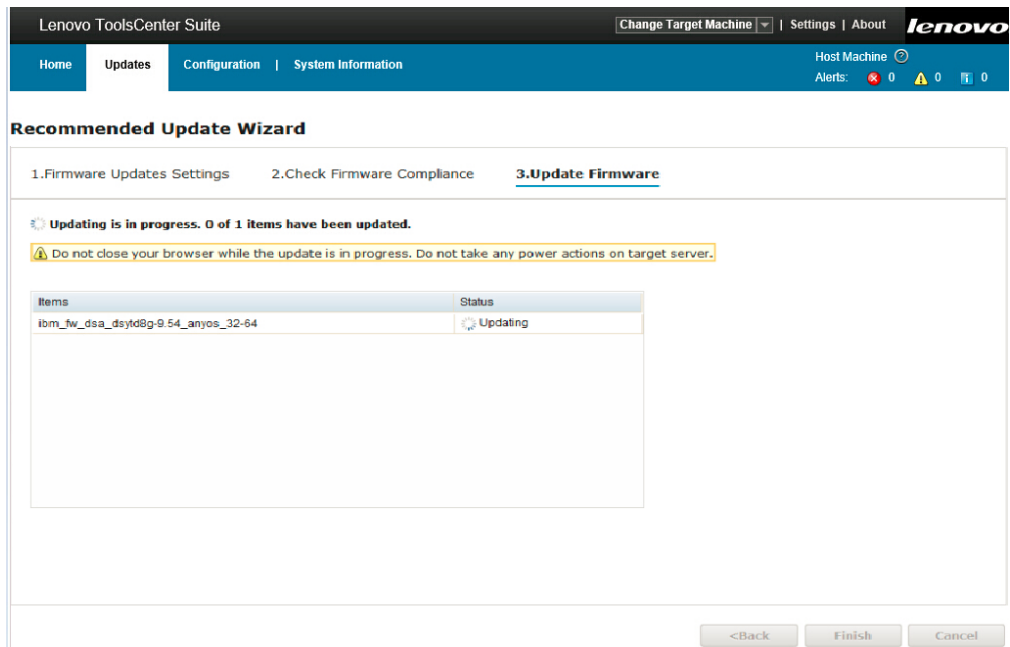
Figure 11. Recommended Updates - Update Firmware operation

During the update operation, a progress icon and the following message is displayed:

```
Updating is in progress.
x of y items have been updated.
Do not close your browser while the update is in progress.
Do not take any power actions on target server.
```

When the update operation finishes, the table provides the status of the updates. A timestamp provides the time the update operation finished.

Figure 12. Recommended Updates - Update Firmware results

8. Click **Finish** to return to the Firmware and Drivers Updates page.

Using the Import UXSP updates package option

By using the **Import UXSP updates package**option you can apply a UXSP updates package (or individual updates) from a local directory.

Procedure

1. Click **Recommended Update** on the Firmware and Driver Updates page. The Firmware Updates Settings page of the Recommended Update Wizard opens.

Recommended Update Wizard

| 1.Firmware Updates Settings | 2.Check Firmware Compliance | 3.Update Firmware |

Compare the currently installed firmware to the following source:

- ○ The latest UXSP updates package from the Lenovo website
- ● Import UXSP updates package:

  c:\UXSPI

Update Content:

- ☐ Also include updates that are not installed or undetected ⓘ

Figure 13. Recommended Updates - Firmware Updates Settings

2. Select **Import UXSP updates package**, and on the next line enter the directory path where the updates are located. If you enter an invalid local directory address, the following message is displayed:

   ```
   Cannot find the given local directory.
   Make sure the directory path is valid.
   ```

3. Optional: You can select **Also include updates that are not installed or undetected**. Select this option only if you have any unknown devices and you need to detect all possible hardware in this system

4. Click **Next** to proceed or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:

   - Click **OK** to quit the update wizard.
   - Click **Cancel** to continue the update process.

   While the check firmware compliance operation is working, the current page is locked, **Cancel** is disabled, and the following message is displayed:

   ```
   Please wait while ToolsCenter Suite compares your current firmware and drivers
    with the latest update package.
   ```

   When the check firmware compliance operation finishes, the firmware and driver updates table is displayed.

   The firmware and driver updates table provides the following information for each update listed in the table:

   - Name: update name
   - Severity: Initial Release, Suggested, Critical, or Not Required
   - New Version: new version number
   - Installed Version: current version number or Undetected
   - Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

The HBA/CNA updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version number
- Installed Version: current version number or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

5. Select one or more updates in the left column. Updates with a severity level of critical are selected by default. If you want to include additional updates, manually select them.

6. Click **Next** to proceed with the update process. If you selected to install firmware or drivers that includes OS agnostic software (including uEFI/IMM/DSA/FPGA updates), for in-band updates, ToolsCenter Suite checks whether the entered user name and password is able to pass the IMM user authentication.

   Complete the following steps:

   a. Enter the IMM credentials:
      - IMM User Name
      - Password

   b. Click **Target the secondary firmware bank** to have the secondary or alternate flash bank targeted if it is available. If a secondary or alternate device is not supported the IMM may ignore this option.

   c. Click **Continue Updates**.

   If IMM authentication passes, the firmware and driver installation continues. To install the OS agnostic software, the IMM account and password must pass authentication. If you cannot pass IMM account and password authentication, deselect the OS agnostic software to continue the firmware and driver installation without OS agnostic software.

7. Click **Continue Update** to continue the updates process from the local directory, or click **Cancel** to return to the Firmware and Driver Updates page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:

   - Click **OK** to quit the update wizard.
   - Click **Cancel** to continue the update process.

   During the update operation, a progress icon and the following message is displayed:

   ```
   Updating is in progress.
   x of y items have been updated.
   Do not close your browser while the update is in progress.
   Do not take any power actions on target server.
   ```

   The updates listed in the table display the status as either: Not Started, Downloading, and Downloaded.

   Note: For in-band and out-of-band (OOB) updates, if you selected to install a prior version of firmware or drivers, a backlevel warning dialog box opens. Click **Continue installation** to proceed or **Cancel** to stop the installation.

   When the update operation finishes, the firmware and driver updates table provides the status of the updates. A timestamp provides the time the update operation finished.

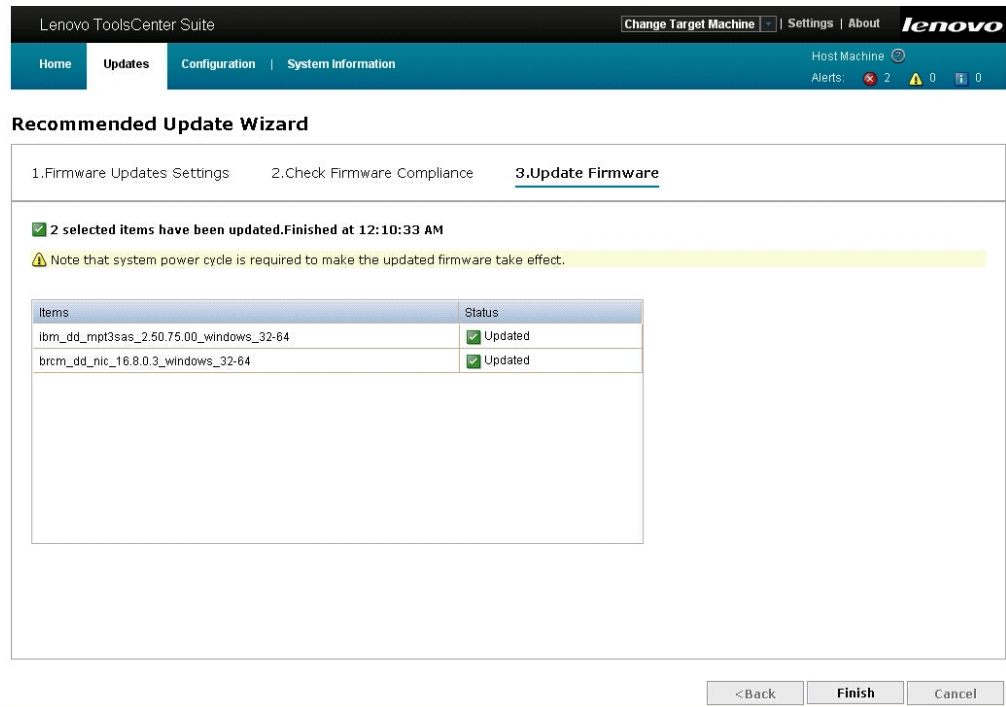8. Click **Finish** to return to the Firmware and Driver Updates page.

The Individual Update Wizard

The Individual Update Wizard checks and compares the currently installed firmware and drivers to individual updates from the Lenovo website or in a local directory. Use this method if you want to install individual updates or when Support instructs you to install individual updates.

Using the Individual updates from the Lenovo website option

By using **The Individual updates from the Lenovo website** option, you can download and apply individual firmware and driver updates from the Lenovo website.

Procedure

1. Click **Individual Updates** on the Firmware and Driver Updates page. The Firmware and Driver Updates page of the Individual Update Wizard opens.
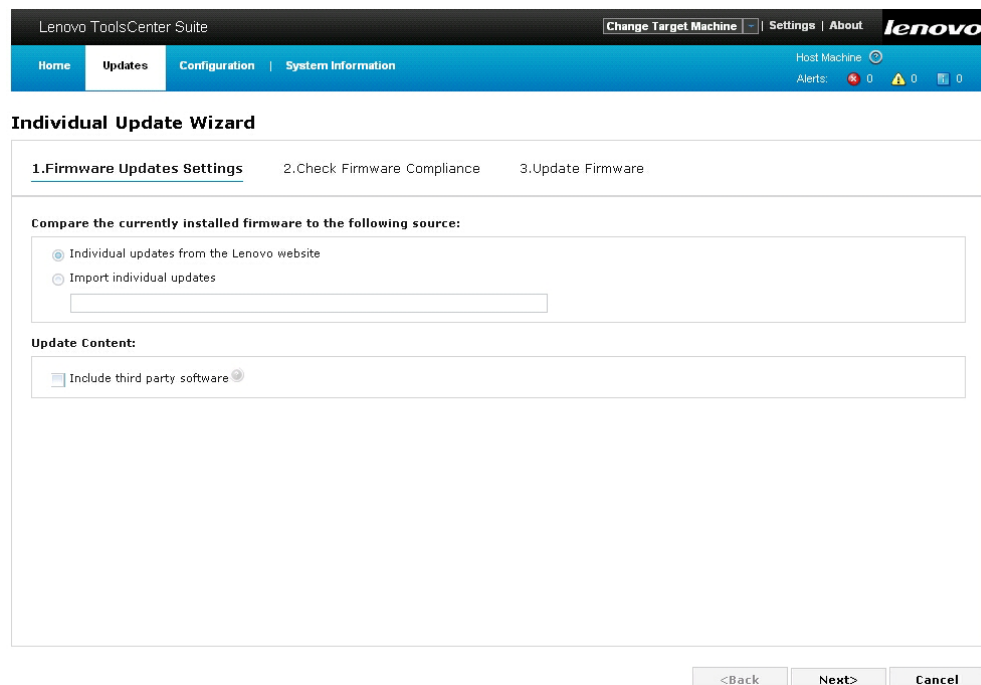
Figure 14. Individual Update Wizard

2. Select **Individual updates from the Lenovo website**.

3. Optional: You can select **Include third party's software**. Third-party software is vendor management software, such as Broadcom or LSI.

   Note: This process may take some time because the size of the third-party software may be larger than the size of the third-party firmware and device driver software.

4. Click **Next** to proceed or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:

   - Click **OK** to quit the update wizard.

- Click **Cancel** to continue the update process.

The current machine's individual firmware and driver levels are acquired from the Lenovo website. During the acquire operation, **Cancel** is enabled, and the following message is displayed:

```
Please wait while ToolsCenter Suite acquires your firmware and driver levels.
```

After the acquire operation finishes, the check firmware compliance operation begins. While the check firmware compliance operation is working, the current page is locked, **Cancel** is disabled, and the following message is displayed:

```
Please wait while ToolsCenter Suite compares your current firmware and drivers
 with the latest update package.
```

When compliance checking finishes, the number of items with new versions is displayed above the firmware and driver updates table.
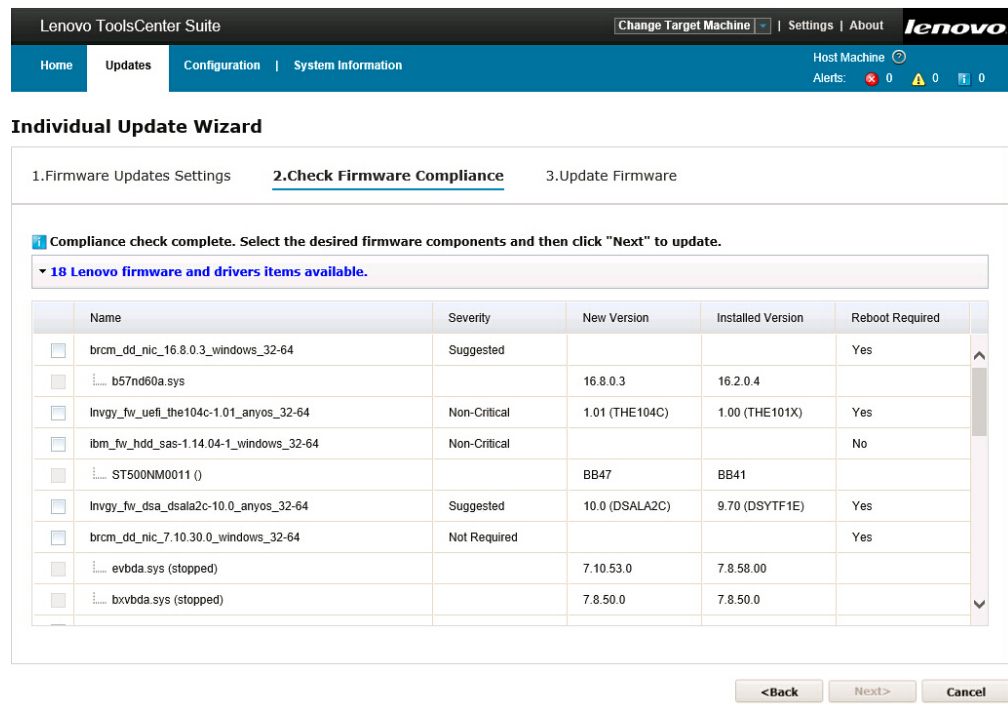
Figure 15. Individual Update - Check Firmware Compliance results

The firmware and driver updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version identifier
- Installed Version: current version identifier or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

Note: If you selected to install third-party software, a second table is displayed below the firmware and drivers update table providing a list of third-party software.

Figure 16. Individual Updates- third party software results

5. Select one or more updates in the left column.

6. Click **Next** to proceed with the update process. If you selected to install firmware or drivers that includes OS agnostic software (including uEFI/IMM/DSA/FPGA updates), for inband updates, ToolsCenter Suite checks whether the entered user name and password is able to pass the IMM user authentication.

    Complete the following steps:

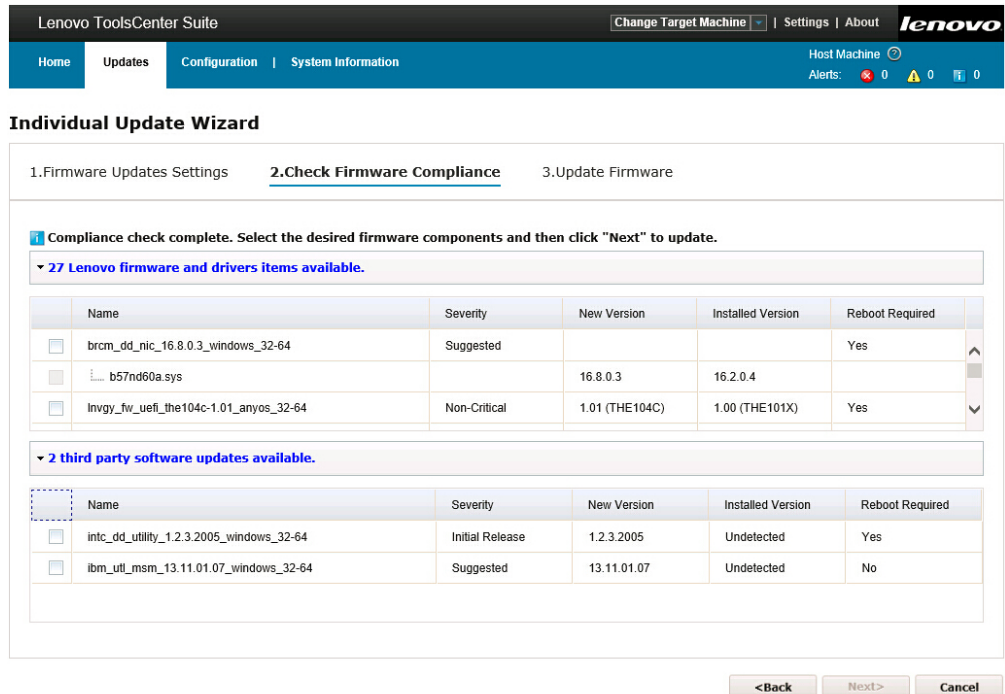   a. Enter the IMM credentials:
        -   IMM User Name
        -   Password

    b. Click **Target the secondary firmware bank** to have the secondary or alternate flash bank targeted if it is available. If a secondary or alternate device is not supported the IMM may ignore this option.

    c. Click **Continue Updates**.

    If IMM authentication passes, the firmware and driver installation continues. To install the OS agnostic software, the IMM account and password must pass authentication. If you cannot pass IMM account and password authentication, deselect OS agnostic software to continue the firmware and driver installation without the OS agnostic software.

7. Click **Continue Update** to continue the updates process by downloading the updates from the Lenovo website and apply the downloaded firmware and drivers, or click **Cancel** to return to the Firmware and Driver Updates page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:
    -   Click **OK** to quit the update wizard.
    -   Click **Cancel** to continue the update process.

During the download operation, the progress of the current downloading item indicates the total bytes and the downloaded bytes. A progress bar provides the overall progress of all download items. The updates listed in the table display the status as either: Not Started, Downloading, and Downloaded. Click **Stop** to stop the current downloading item.

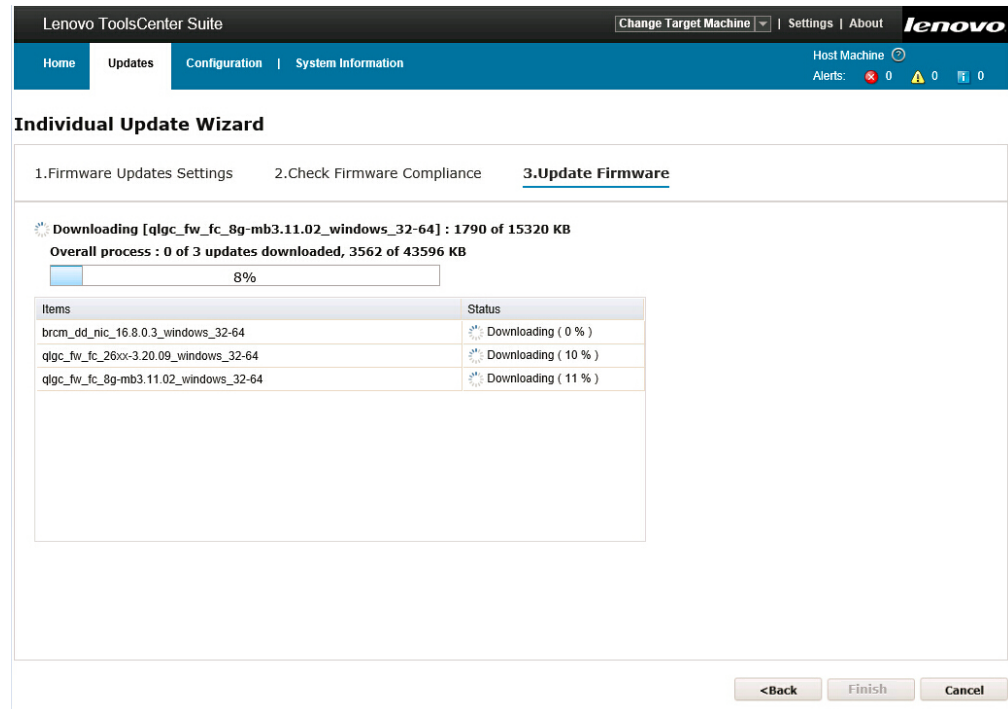*Figure 17. Individual Updates - downloading firmware from the Lenovo website*

When all of the firmware and drivers have been downloaded, the update operation begins.

During the update operation, a progress icon and the following message is displayed:

```
Updating is in progress.
x of y items have been updated.
Do not close your browser while
the update is in progress.
Do not take any power actions on target server.
```
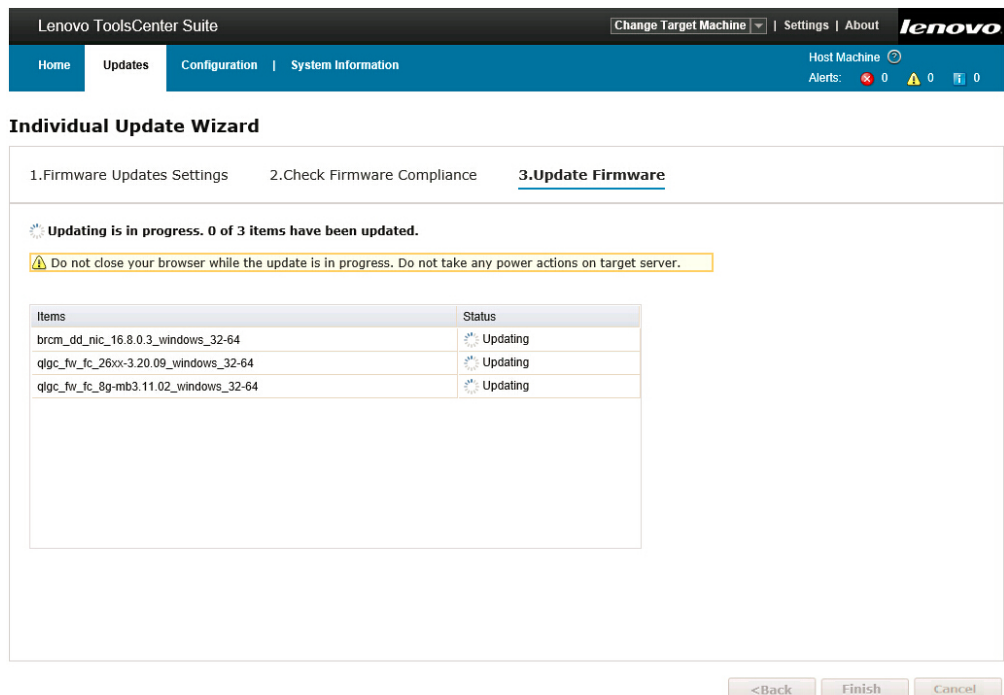
Figure 18. Individual Updates - updating firmware progress

> **Note:** For inband and out-of-band (OOB) updates, if you selected to install a prior version of firmware or drivers, a backlevel warning dialog box opens. Click **Continue installation** to proceed or click **Cancel** to stop the installation.

> When the update operation finishes, the table provides the status of the updates. A timestamp provides the time the update operation finished.

8. Click **Finish** to return to the Firmware and Driver Updates page.

Using the Import individual updates option

By using the **Import individual updates** option, you can apply previously downloaded updates (UXSP or individual) from a local directory.

Procedure

1. Click **Individual Updates** on the Firmware and Driver Updates page. The Firmware Updates Settings page of the Individual Update Wizard opens.

Figure 19. Individual Updates - importing individual updates from a local directory
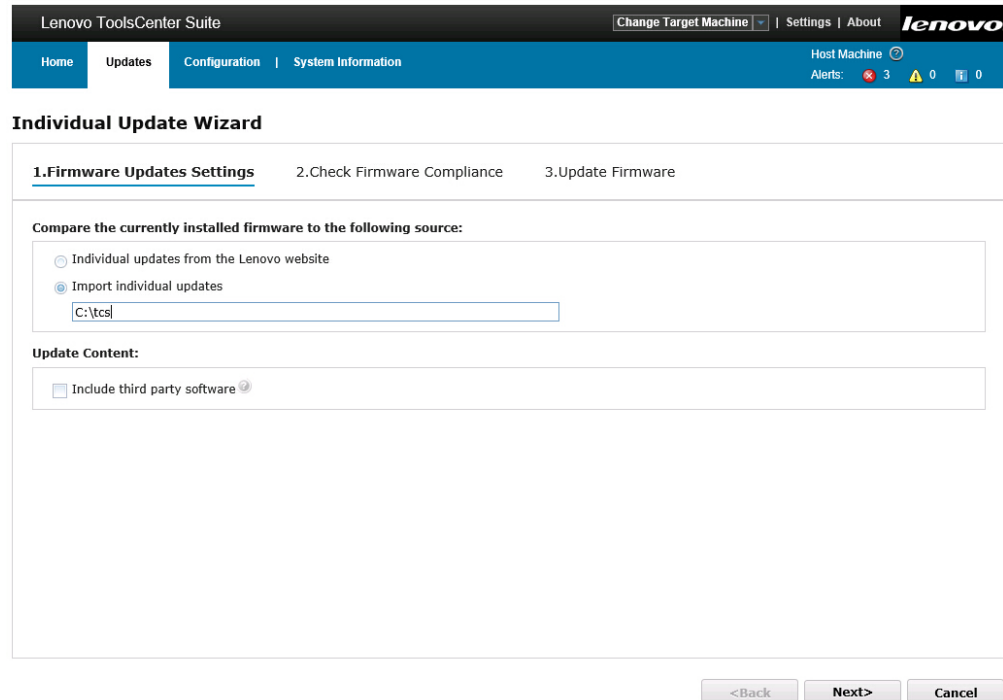
2. Select **Import individual updates** and on the next line, enter the directory path where the individual updates are located. If you enter an invalid local directory address, the following message is displayed:

   ```
   Cannot find the given local directory.
   Make sure the directory path s valid.
   ```

3. Optional: You can select **Include third party's software**. Third-party software is vendor management software, such as Broadcom or LSI.

   Note: This process may take some time because the size of the third-party software may be larger than the size of the third-party firmware and device driver software.

4. Click **Next** to proceed or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:

   - Click **OK** to quit the update wizard.
   - Click **Cancel** to continue the update process.

   While the check firmware compliance operation is working, the current page is locked, **Cancel** is disabled, and the following message is displayed:

   ```
   Please wait while ToolsCenter Suite checks your firmware and driver levels.
   ```

   When the check firmware compliance operation finishes, a table containing firmware and driver updates is displayed.

   The firmware and driver updates table provides the following information for each update listed in the table:

   - Name: update name
   - Severity: Initial Release, Suggested, Critical, or Not Required
   - New Version: new version number
   - Installed Version: current version number or Undetected

- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

  Note: If you selected to install third-party software, a second table below the firmware and drivers update table provides a list of third-party software.

5. Select one or more updates in the left column.
6. Click **Next** to proceed with the update process. If you selected to install firmware or drivers that includes OS agnostic software (including uEFI/IMM/DSA/FPGA updates), for in-band updates, ToolsCenter Suite checks whether the entered user name and password is able to pass the IMM user authentication.

   Complete the following steps:

   a. Enter the IMM credentials:
      - IMM User Name
      - Password

   b. Click **Target the secondary firmware bank** to have the secondary or alternate flash bank targeted if it is available. If a secondary or alternate device is not supported the IMM may ignore this option.

   c. Click **Continue Updates**.

   If IMM authentication passes, the firmware and driver installation continues. To install OS agnostic software, the IMM account and password must pass authentication. If you cannot pass IMM account and password authentication, deselect OS agnostic software to continue the firmware and driver installation without OS agnostic software.

7. Click **Continue Update** to continue the updates process from the local directory, or click **Cancel** to return to the Firmware and Driver Updates page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Click one of the follow options:
   - Click **OK** to quit the update wizard.
   - Click **Cancel** to continue the update process.

   During the update operation, a progress icon and the following message is displayed:

   ```
   Updating is in progress.
   x of y items have been updated.
   Do not close your browser while the update is in progress.
   Do not take any power actions on target server.
   ```

   Note: For in-band and out-of-band (OOB) updates, if you selected to install a prior version of firmware or drivers, a backlevel warning dialog box opens. Click **Continue installation** to proceed or **Cancel** to stop the installation.

   When the update operation finishes, the firmware and driver updates table provides the status of the updates. A timestamp provides the time the update operation finished.

8. Click **Finish** to return to the Firmware and Driver Updates page.

The Download Update Wizard

The Download Update Wizard downloads a UpdateXpress System Pack or an individual update package for a specific machine type and operating system. The updates are downloaded to the working directory for ToolsCenter Suite, where they are stored until you are ready to apply the updates, using either the **Recommended updates in a local directory** or the **Individual updates in a local directory** option.

Using the Download UXSP from the Lenovo Website option

By using the **Download UXSP from the Lenovo Website** option, you can selectively download a UXSP or an individual update package for a specific machine and operating system.

Procedure

1. Click **Download Updates** on the Firmware and Driver Updates page. The Download Updates Settings page of the Download Update Wizard opens.
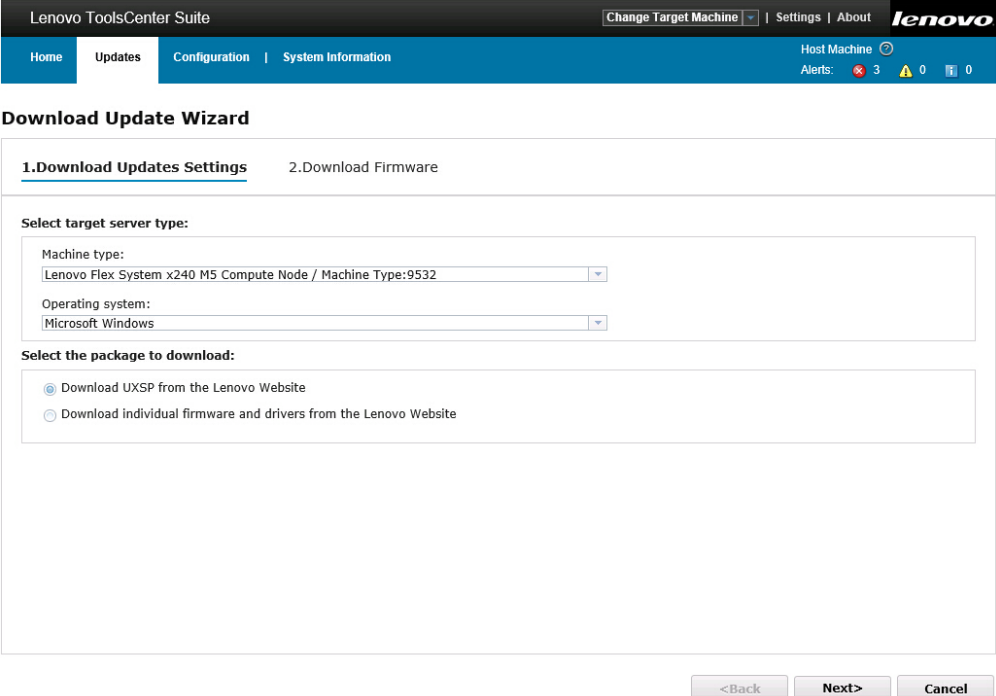

Figure 20. Download Updates - Download UXSP from the Lenovo website

2. In the Select target server type section, complete the following steps:
   - From the **Machine type** list, select the target server type.
   - From the **Operating system** list, select the operating system for the target server.
   -
3. In the **Select a package to download** section, select **Download UXSP from the Lenovo Website**.
4. Click **Next** to proceed or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

- Click **OK** to quit the update wizard.
- Click **Cancel** to continue the update process.
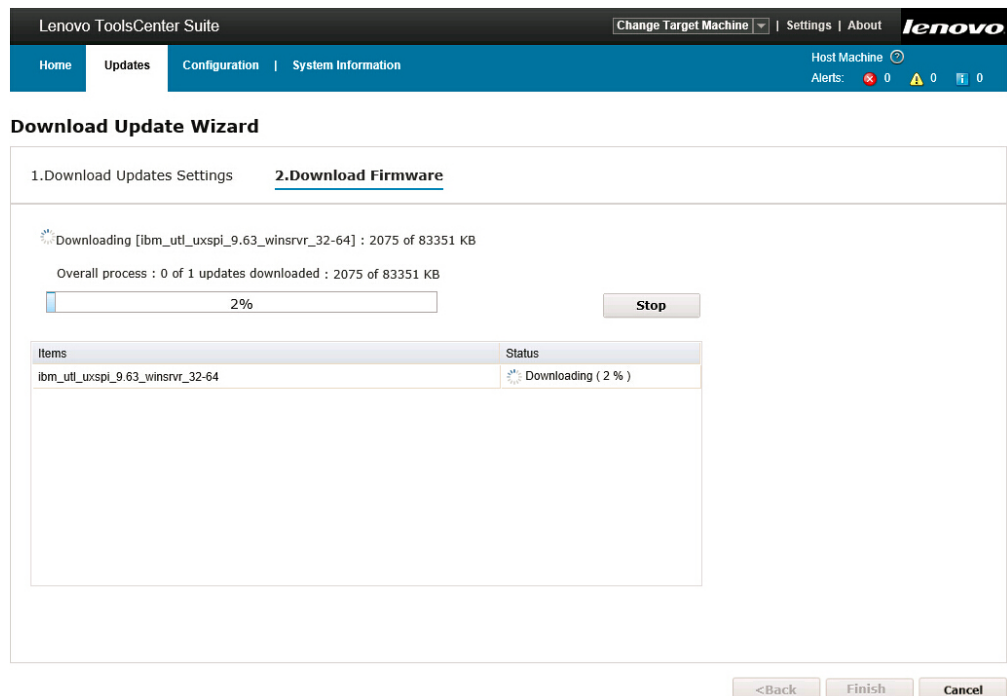
The Download Firmware page opens.

Figure 21. Download Updates - Download Firmware progress

During the download operation, the progress of the current downloading item indicates the total bytes and the downloaded bytes. A progress bar provides the overall progress of all download items. The updates listed in the table display status as either : Not Started, Downloading, or Downloaded. Click **Stop** to stop the current downloading item.

When all of the downloads are finished, the total number of items downloaded successfully and the name of the folder containing the updates is displayed. Each update has a status of Downloaded.

5. Click **Finish** to return to the Firmware and Driver Updates page.

Using the Download individual firmware and drivers from the Lenovo website option

By using the **Download individual firmware and drivers from the Lenovo Website** option, you can download individual firmware and drivers from the Lenovo website.

Procedure

1. Click **Download Updates** on the Firmware and Driver Updates page. The Download Updates Settings page of the Download Update Wizard opens.

Figure 22. Download Updates - Download individual updates

2. Select **Download individual firmware and drivers from the Lenovo Website** on the Firmware and Driver Updates page.

3. Optional: In the **Update Content** section, you can also select **Include third party's software**.

   Note: This process may take some time because the size of the third-party software may be larger than the size of the third-party firmware and device driver software.

4. Click **Next** to proceed or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

   • Click **OK** to quit the update wizard.

   • Click **Cancel** to continue the update process.
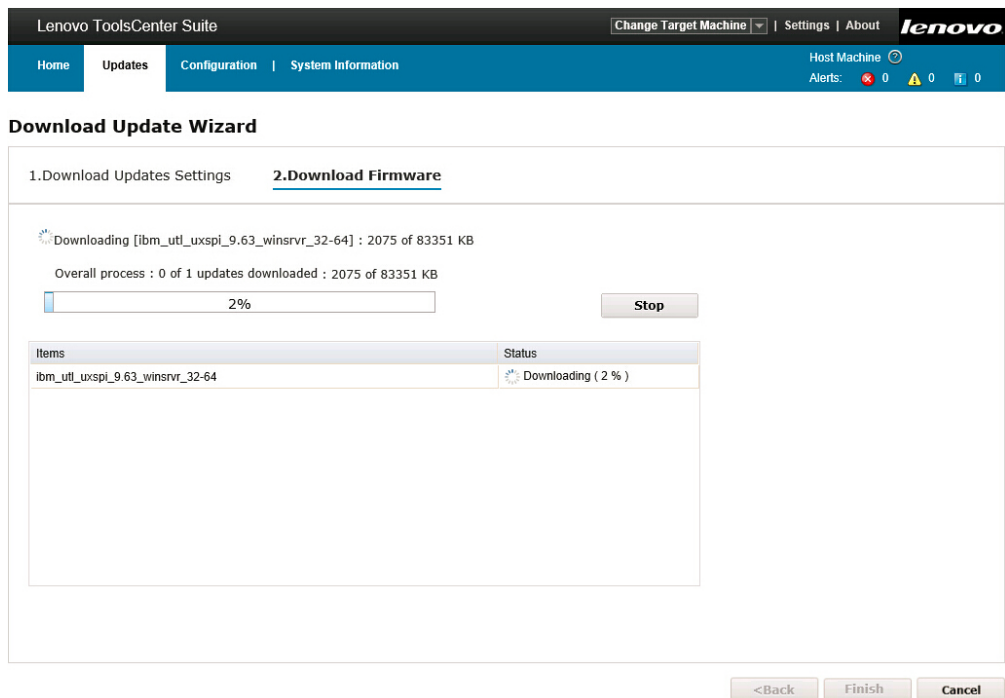
   The Download Firmware page opens.

Figure 23. Download Updates - Download individual firmware and driver updates progress

During the download operation, the progress of the current downloading item indicates the total bytes and the downloaded bytes. A progress bar provides the overall progress of all download items. The updates listed in the table display status as either: Not Started, Downloading, and Downloaded. Click **Stop** to stop the current downloading item.

When all of the downloads are finished, the total number of items downloaded successfully and the name of the folder containing the updates is displayed. Each update has a status of Downloaded.

5. Click **Finish** to return to the Firmware and Driver Updates page.

Chapter 5. Using the Configuration function

You can use the **Configuration** function to view and change one or multiple settings on your system, and manage the configuration of a local machine using inband mode and out-of-band (OOB) mode for a remote machine. This section describes how to display and configure individual and frequently used settings or perform a complete system configuration. You can also change the settings for System x IMM-based and a uEFI-based servers. IMM replaces the Remote Supervisor Adapter and baseboard management controller functions on IMM-based servers. uEFI replaces the basic input/output system (BIOS) and defines a standard interface among the operating system, platform firmware, and external devices.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **Configuration**. The Configuration Overview page opens.
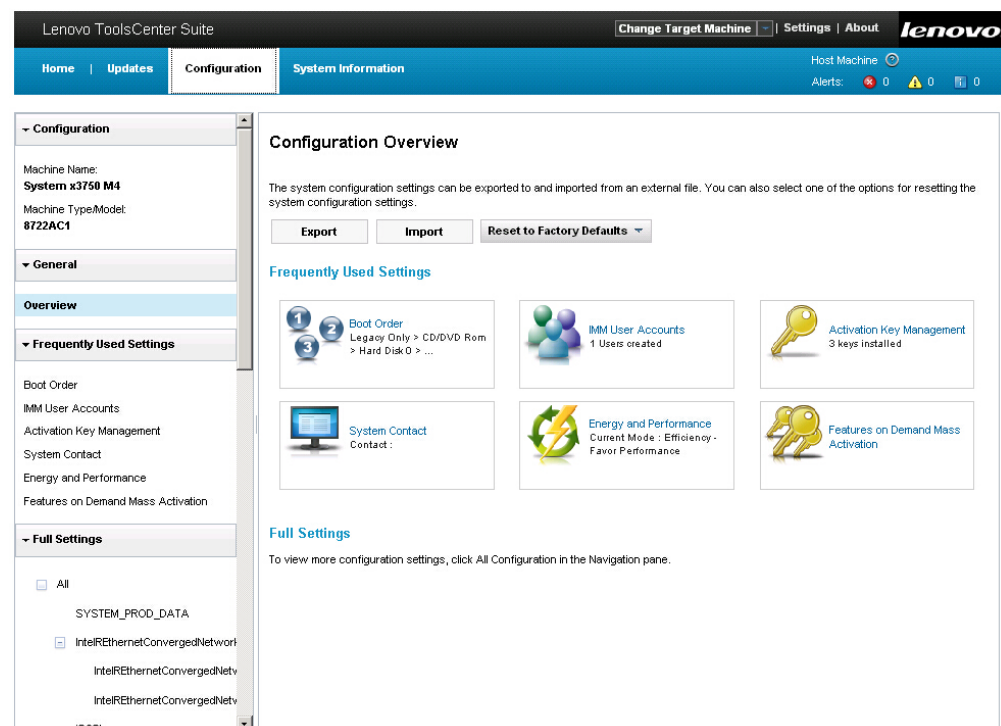

Figure 24. Configuration Overview

2. Select one of the configuration options on the Configuration Overview page:
   - System configuration setting options provide easy access for the following actions. For more information, see "Working with system configuration settings" on page 38.
     - Export
     - Import
     - Reset to Factory Defaults

- Frequently Used Settings are selected on the Configuration Overview page or from the navigation pane. For more information, see "Frequently Used Settings" on page 42.
  - Boot Order
  - IMM User Accounts
  - Activation Key Management
  - System Contact
  - Energy and Performance
  - Feature on Demand Mass Activation
- Full Settings allows you to view more configuration settings, from the navigation pane, click **Full Settings** > **All**. For more information, see "Working with the Full Settings option" on page 61.

Working with system configuration settings

The Configuration Overview page provides you with easy access to options that can assist you with exporting, importing, and resetting your system configuration settings.

About this task

The following procedure explains how to use the export, import and reset to factory defaults options.
- **Export**: Export the current machine settings before making configuration changes or installing updates.
- **Import**: Restore or replicate configuration settings to a machine after exporting the settings.
- **Reset to Factory Defaults**: Restore the machine settings to their original state before configuration changes or updates were applied.

Procedure

On the Configuration Overview page, click one of the following options:
- **Export**: The Opening saveall.out dialog box opens.

  Select one of the following export actions:
  - Click **Open**. A browser window opens displaying the export file contents.
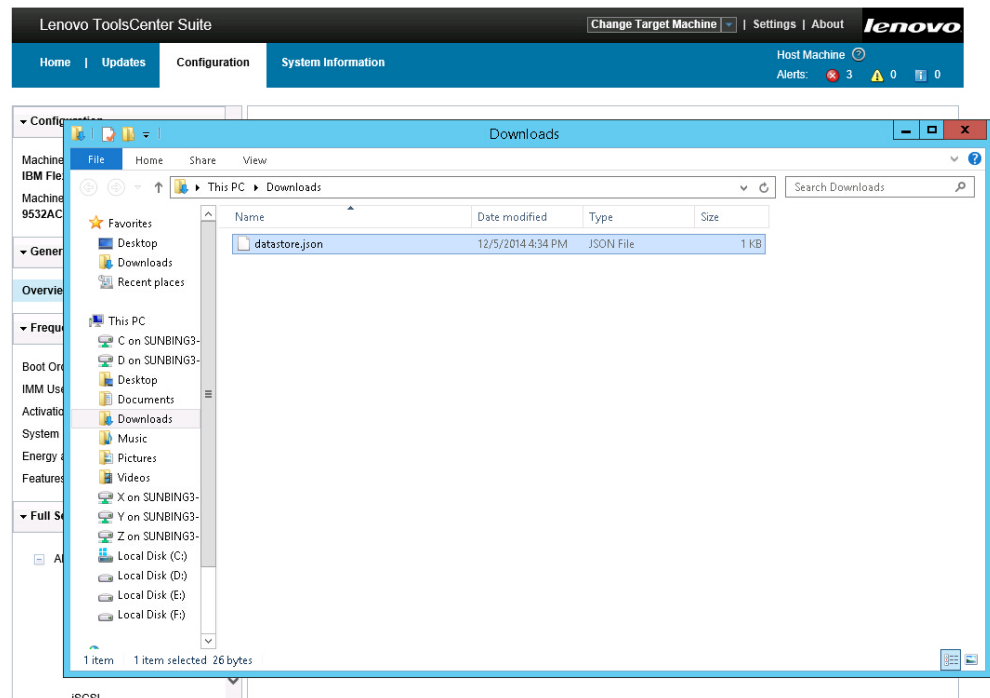 - Click **Save**. The Save As dialog box opens.

Figure 25. Configuration - Export configuration file

> Select a folder for saving the export file and click **Save** or **Cancel** to quit the Save As operation.

– Click **Cancel** to quit the Export operation.

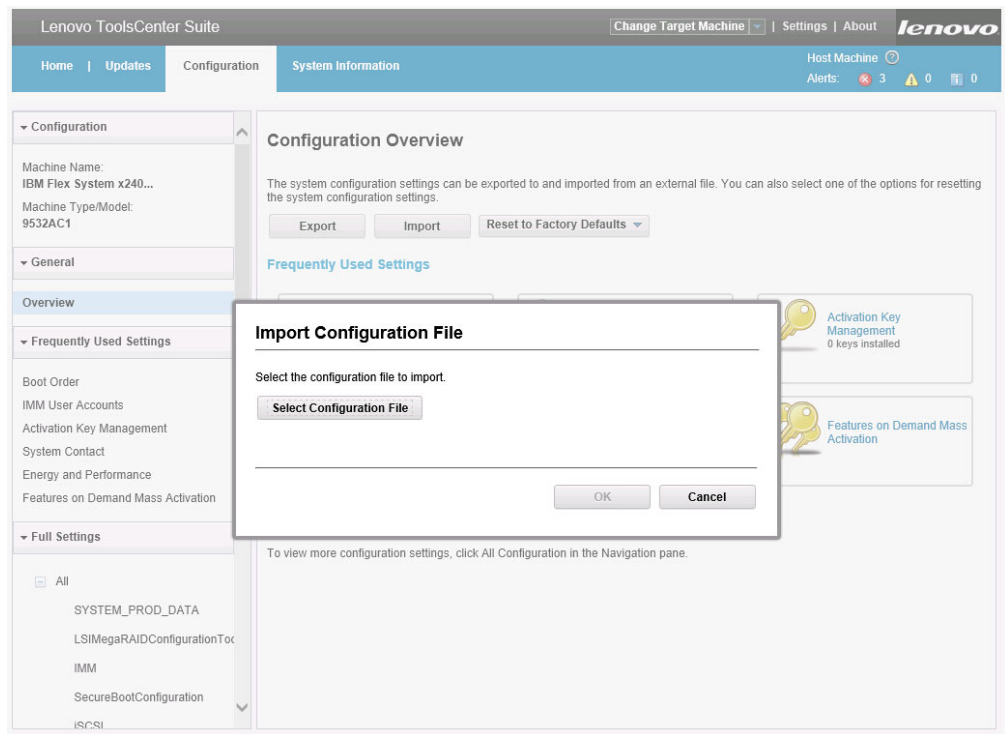• **Import**: The Import configuration file dialog box opens.

Figure 26. Configuration - Import Configuration File

Select one of the following import actions:

– Click **Select Configuration File** to select the file from the Choose File to Upload dialog box and then click **Open**, or **Cancel** to quit the file selection operation. The Import Configuration File dialog box opens displaying the name of the selected configuration file.

– Click **OK** to continue the import operation or click **Cancel** to quit this operation.

If you chose to import the configuration file exported from another machine, the Confirm to Replicate Configuration Settings dialog box opens.
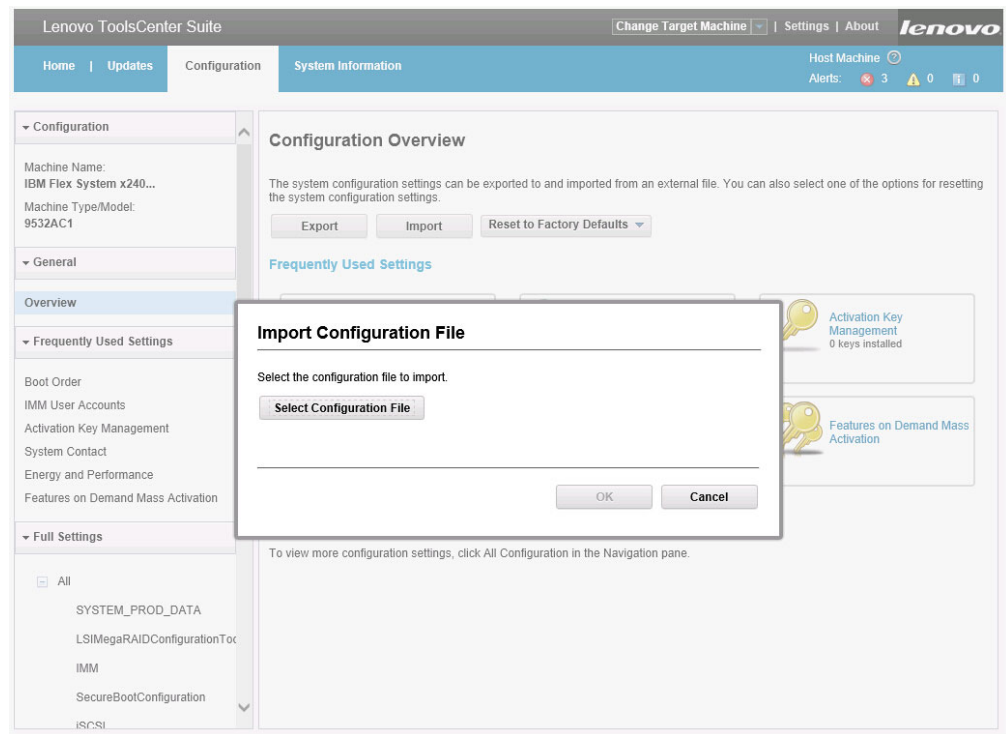
Figure 27. Configuration - Import - Replicate Configuration Settings

– Click **OK** to replicate the applicable settings for this machine or click **Cancel** to keep the original configuration settings.

–

If you chose to import the configuration file exported from the same server, the Confirm to Restore Configuration Settings dialog box opens.
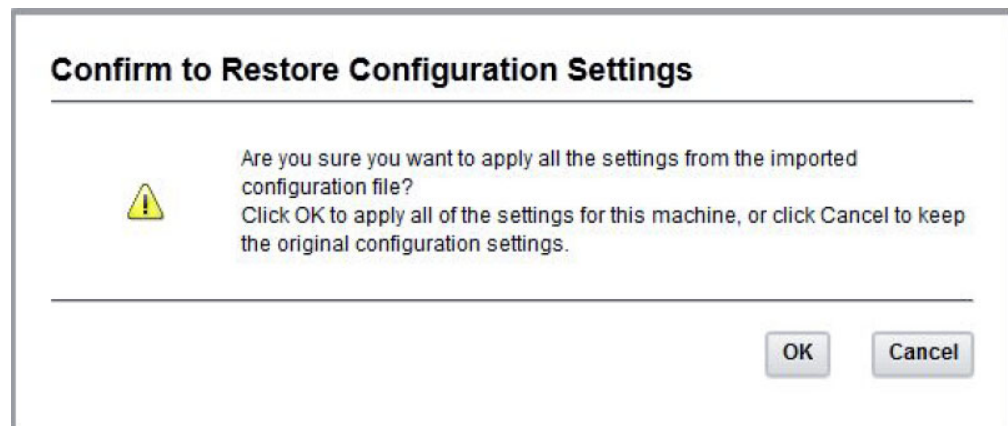

Figure 28. Configuration - Import - Restore Configuration Settings

• **Reset to Factory Defaults**: Select one of the following reset actions:
   – **Reset All Settings to Factory Defaults**:
      1. Click **OK** to reset all of the settings to the factory default settings or click **Cancel** to quit this operation.
      2. When the reset operation finishes, you must restart the system.
   – **Reset to IMM Factory Defaults**:

1. Click **OK** to reset all of the IMM settings to the factory default settings or click **Cancel** to quit this operation. The IMM will restart after the IMM settings are cleared.
2. When the IMM restarts, you must configure the IMM network interface to restore connectivity. After the IMM configuration is cleared, the IMM is restarted.

– **Reset to uEFI Factory Defaults**:

1. Click **OK** to reset the uEFI settings to the factory default settings or click **Cancel** to quit this operation.
2. When the reset operation finishes, you must restart the system.

Frequently Used Settings

You can use this option to view and change individual, frequently used settings. The Configuration Overview page provides an abbreviated, current status for each of the frequently used settings.

On the Configuration Overview page from in the navigation pane, you can select one of the following frequently used settings:

- Boot Order
- IMM User Accounts
- Activation Key Management
- System Contact
- Energy and Performance
- Features on Demand Mass Activation

Configuring, viewing, and changing Boot Order

You can use the **Boot Order** option to configure, view, and change the Boot Order and Wake on LAN Boot Order sequences for your system devices. The boot order sequence is stored in the IMM and used by the server firmware during the startup process.

Procedure

1. Click **Boot Order** on the Configuration Overview page or in the navigation pane. The Configuration - Boot Order page opens.
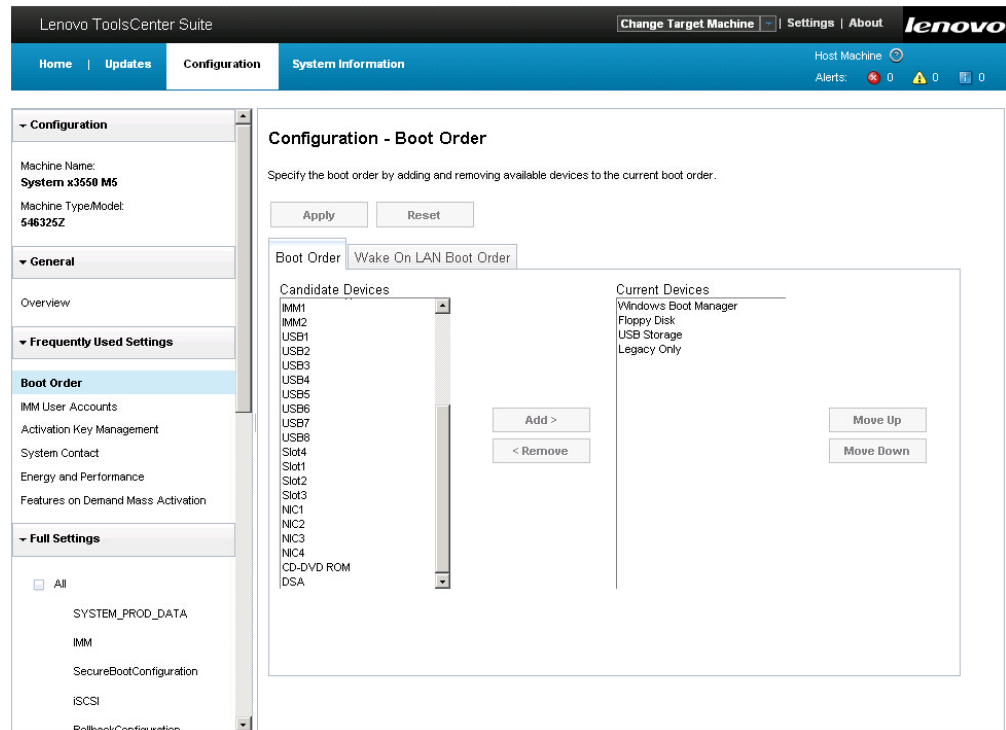
Figure 29. Configuration - Boot Order

2. Select one of the following boot order tabs:

   - Boot Order
   - Wake On LAN Boot Order

   In the dual list box, the current boot order is shown as Current Devices on the right, and the available devices is shown as Candidate Devices on the left.

3. To change the order of the Current Devices list, perform the following applicable steps:

   a. To change only the Current Devices sequence, select the device and click either the **Move Up** or **Move Down**.

   b. To add a device to the Current Devices list, select the device to be added from the Candidate Devices list, and click **Add >**.

   c. To remove a device from the Current Devices list, select the device to be removed and click **Remove >**.

4. To cancel any changes, click **Reset**.

5. To save the new current device sequence changes, click **Apply**.

Creating, modifying, and deleting an IMM User Account

You can use the **IMM User Account** option to create, modify, or delete an IMM user account.

Procedure

1. Click **IMM UserAccount** on the Configuration Overview page or in the navigation pane. The Configuration - IMM User Accounts page opens.
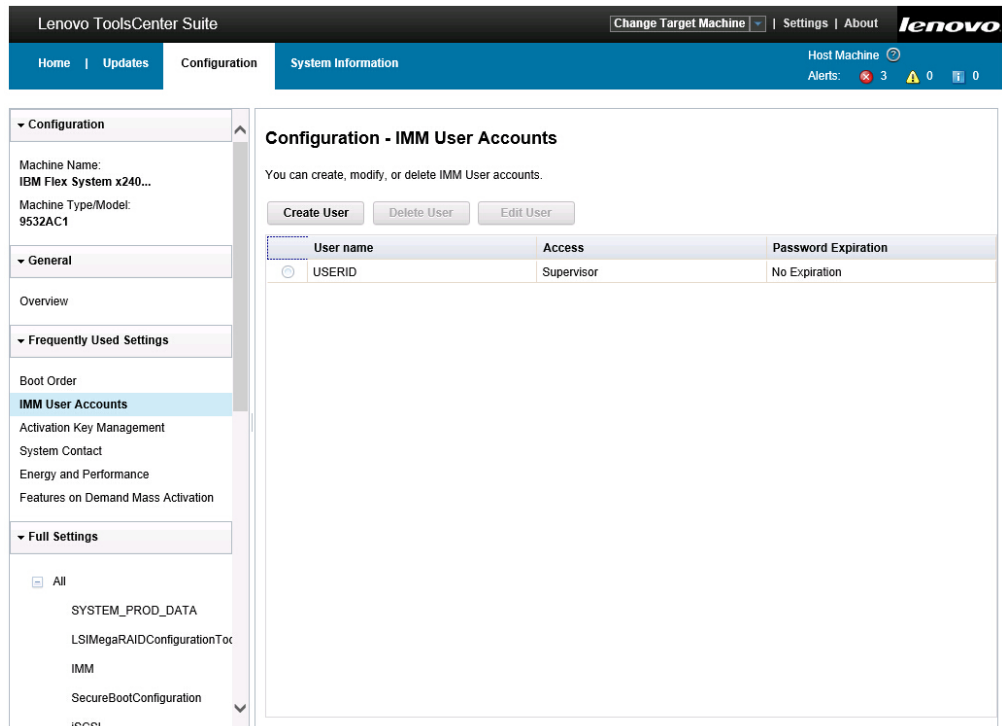
Figure 30. Configuration - IMM User Account

Existing IMM users are shown in the IMM User Account List. The list provides the following information for each user:

- User name
- Access
- Password Expiration

2. To create a new user, click **Create User**. The Create User dialog box opens.

   a. Click the **User Credentials** tab. Enter the following User Credentials and then click **OK** or click **Cancel** to close the Create User dialog box.

      - User Name
      - Password
      - Confirm password

      Note: The user name and password rules will be checked automatically after entering the information in each field, verifying whether it satisfies these rules.

      When a new user is created, it is added to the IMM User Accounts List.

   a. Click the **Authority** tab and select one of the follow user access levels:

      - Supervisor: This user has no restrictions.
      - Read-only: This user has read-only access and cannot perform any save, modify, clear, or state-affecting operations.
      - Custom: This user may or may not have any restrictions, depending on which custom authority level is assigned.

3. To delete an existing user from the IMM User Account List, select the **User name** you want to delete, and click **Delete User**. In the Delete IMM User dialog box, click **OK** to confirm the IMM User deletion or click **Cancel** to quit this operation.

4. To change an existing user, select the **User Name** and click **Edit User**. The Edit User dialog box opens. You can change the following IMM User options.
   - Click the **User Credentials** tab to change the `User name` and `Password`.
   - Click the **Authority** tab and select one of the follow user access levels:
     - Supervisor: This user has no restrictions.
     - Read-only: This user has only read-only access, and cannot perform any save, modify, clear, or state affecting operations.
     - Custom: This user may or may not have any restrictions, depending on which custom authority level is assigned.
5. When you have finished editing the user information, click **OK** or click **Cancel** to close the Edit User dialog box.

Using Activation Key Management

By using the **Activation Key Management** function, you can activate a feature on a server or activate an option with a software key, that is referred to as the Features on Demand activation key. You can use this function to view the currently installed keys list and to install keys from the Lenovo website, export locally installed keys, and delete installed key files. For more information about Features on Demand, see the Using System x Features on Demand Redbook.

About this task

The following steps provide an overview of the options available when using the Activation Key Management function:

Procedure

- Click **Activation Key Management** on the Configuration Overview page or in the navigation pane. The Configuration - Activation Key Management page opens.
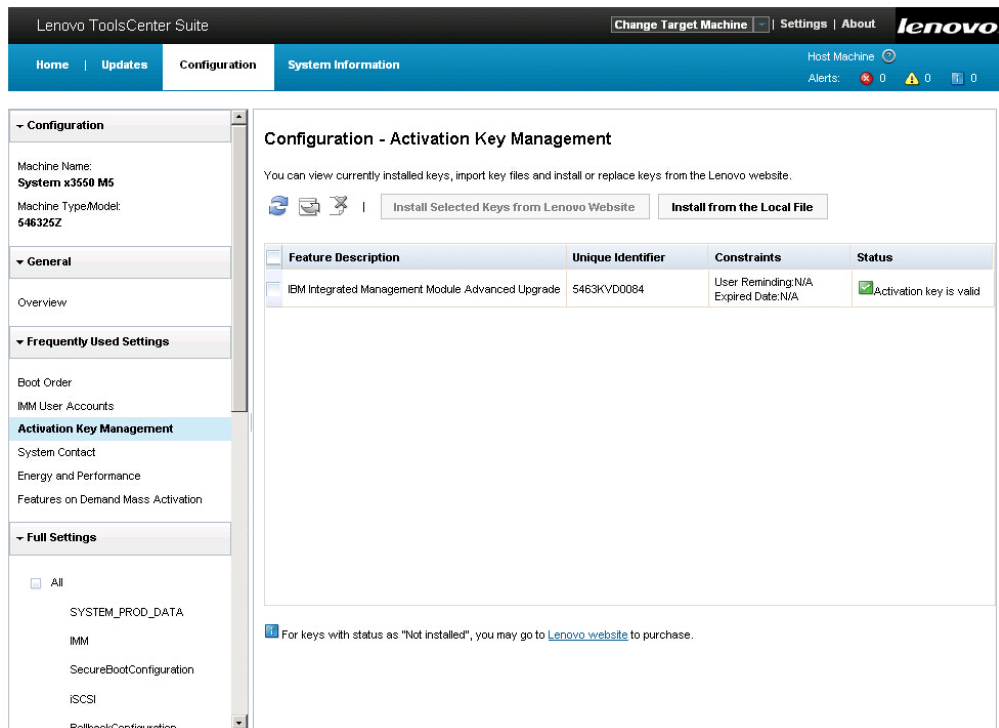
Figure 31. Configuration - Activation Key Management

The currently installed feature activation keys are displayed in the installed keys table. The table provides the following information:

– Feature Description
– Unique Identifier
– Constraints
– Status

If there is a live internet connection, the available activation keys for the current system can be purchased from the Lenovo website by using the selecting **Install Selected Keys from Lenovo Site** or by selecting **Lenovo website**.

• The Configuration - Activation Key Management page provides the following actions:

– Refresh
– Export
– Delete
– Install Selected Keys from Lenovo Website
– Install from the Local File

• To refresh the activation key status, click **Refresh**. The activation key status of the current machine is refreshed and displayed. The Unique Identifier column indicates a unique identifier for IMM and RAID, otherwise the unique identifier is *N/A*.

• To download a key file or open a key file in a browser window, select the key file and click **Export**. The File Download dialog box opens. Select one of the following options:

– Open
– Save
– Cancel

- To remove keys, select one or more key files from the list and click **Delete**. The Confirm to Remove keys dialog box opens. Select one of the following options:
  - OK
  - Cancel
- To install an activation key from the Lenovo website, select the key with a status of `Not installed` and click **Install Selected Keys from Lenovo Website**. The Install Activation Key from Lenovo website dialog box opens.
  1. Enter the following information in the Install Activation Key from Lenovo website dialog box: For IMM/RAID keys, the unique identifier is displayed, otherwise for any other key, enter the unique identifier of the hardware manually.
     - IBM ID
     - Password
     - Details for each key
  2. Click **Install Now** to install activation keys from the Lenovo website.

     If there is a IBM ID error or if the password is not recognized, the following error message is displayed:

     `The IBM ID or password is not recognized.`

     If there is an FOD ID error, the following error message is displayed:

     ```
     The Feature-On Demand IDs for the indicated license are
     not recognized. Note that an authorization code and
     Feature-On-Demand ID are required.
     ```
- To install one or more keys from the local file, select one or more key files from the list, click **Install from the Local files**. The Choose File to Upload dialog box opens. Complete the following steps:
  1. Select the File Upload directory location and click **Open**.
  2. Select the activation key files to upload to the server. The Activation Keys Installation dialog box opens. A progress bar indicates the key installation percentage and a table lists the installed activation key information.
  3. Select any local activation keys from the list and click **OK**.
  4. To refresh the current installed keys list and the available keys list, click **Refresh** at any time.

     Note: When you click **Refresh**, the installed feature activation keys for the current system and the available activation keys for that system, are both displayed in the activation key list.

Using the System Contact function

You can use the **System Contact** function to identify a system to operations and support personnel. You can also use this function to add or modify the system contact information.

Procedure

1. Click **System Contact** on the Configuration Overview page or in the navigation pane. The Configuration - System Contact page opens.
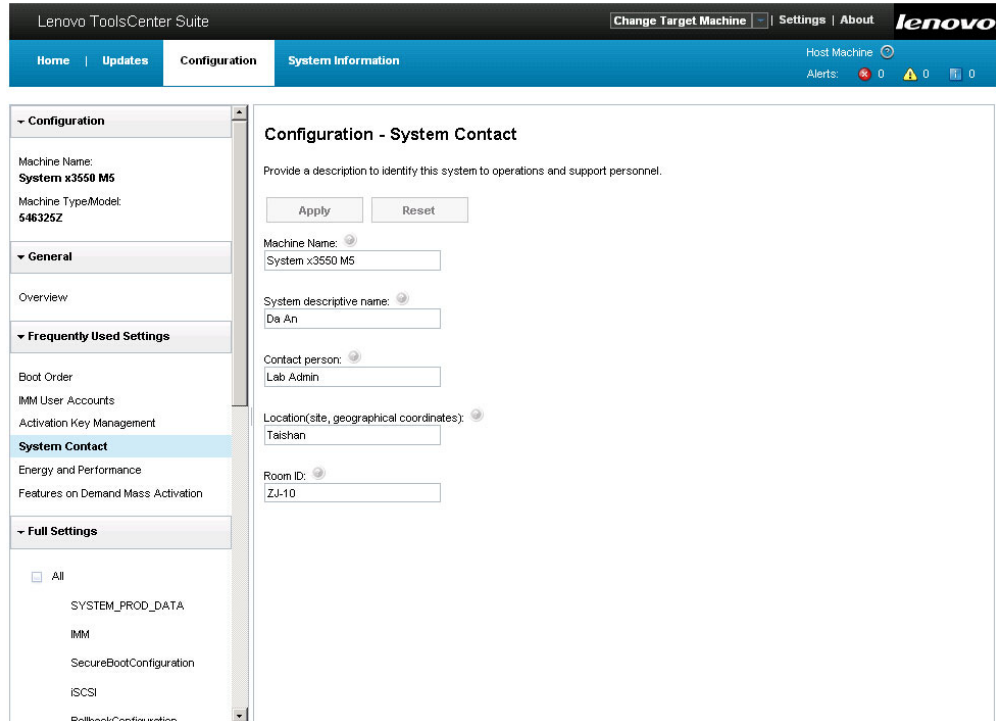
Figure 32. Configuration - System Contact

2. Enter the following applicable information for the Machine Name that is displayed on the left.
   - Machine Name
   - System descriptive name
   - Contact person
   - Location (site, geographical coordinates, etc.)
   - Room ID
3. To apply and save the new system contact information, click **Apply**.
4. To restore the original system contact information, click **Reset**.

Energy and Performance settings

The Energy and Performance settings are determined by machine type. Performance and power tuning is based on a best estimation. Due to circumstantial differences, the results may not be the same as the best estimation.

Use one of the following options to change the values of the Energy and Performance settings that is applicable for your machine type:
- Energy and Performance settings for M4 machine types
- Energy and Performance settings for pre-M4 machine types

Changing Energy and Performance settings for M4 machine types

You can use this procedure to change the values of the Energy and Performance settings for M4 machine types. M4 machines have four energy and performance options. The default state for an M4 machine is Efficiency.

Procedure

1. Click **Energy and Performance** on the Configuration Overview page or in the navigation pane. The Configuration - Energy and Performance page opens.
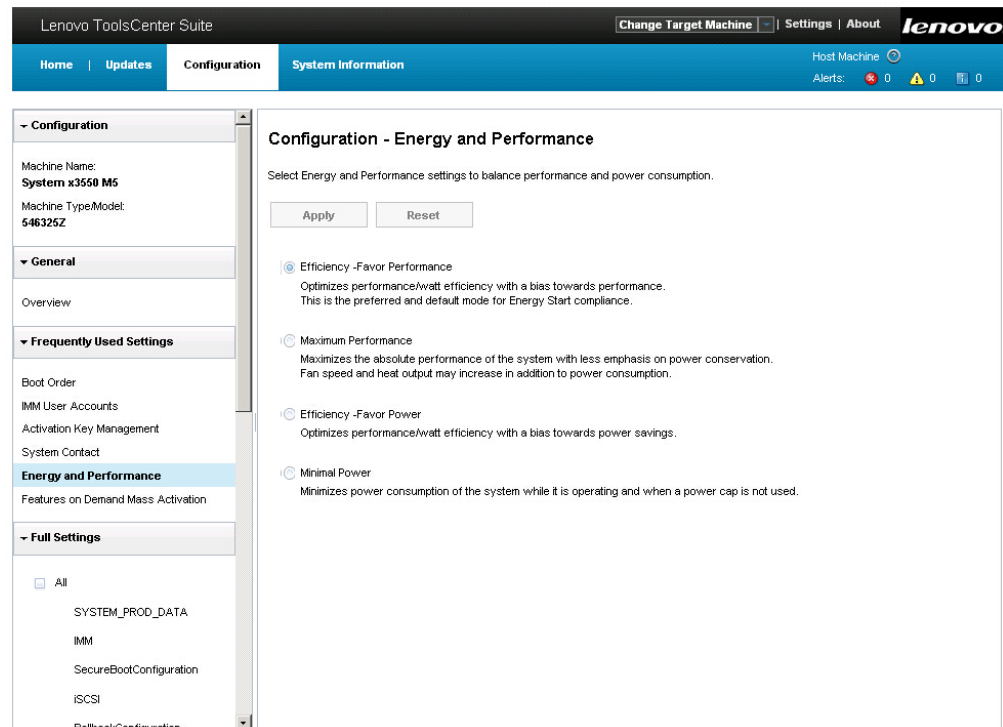
Figure 33. Configuration - Energy and Performance

2. Select one of the following performance settings for your system:
   - **Efficiency - Favor Performance**: This setting optimizes performance and watt efficiency with a bias towards performance. This is the preferred setting for Energy Star compliance.
   - **Maximum Performance**: This setting maximizes the absolute performance of the system with less emphasis on power conservation. Fan speed and heat output may increase in addition to power consumption.
   - **Efficiency - Favor Power**: This setting optimizes performance and watt efficiency with a bias towards power savings, and is applicable for M4 machine types only.
   - **Minimal Power**: This setting minimizes power consumption of the system while it is operating and when a power cap is not used.
3. Click **Apply** to apply and save the Energy and Performance setting change, or click **Reset** to return to the previous Energy and Performance setting. If no changes are made to the selected options, the **Apply** and **Reset** buttons are not available.

Changing Energy and Performance settings for pre-M4 machine types

You can use this procedure to change the values of the Energy and Performance settings for machine types that are older than M4 machines. For these machines types, there are three energy and performance options.

Procedure

1. Click **Energy and Performance** on the Configuration Overview page or in the navigation pane. The Configuration - Energy and Performance page opens.

2. Select one of the following performance settings for your system:
   - **Efficiency**: This setting optimizes performance and watt efficiency. This is the preferred setting for Energy Star compliance.
   - **Maximum Performance**: This setting maximizes the absolute performance of the system with less emphasis on power conservation. Fan speed and heat output may increase in addition to power consumption.
   - **Minimal Power**: This setting minimizes power consumption of the system while it is operating and when a power cap is not set.

3. Click **Apply** to apply and save the Energy and Performance setting change, or click **Reset** to return to the previous Energy and Performance setting. If no changes are made to the selected options, the **Apply** and **Reset** buttons are not available.

Working with Features on Demand Mass Activation

You can use the **Features on Demand Mass Activation** option to inventory systems vital product data (VPD), download activation keys from the Lenovo website, and install and export activation keys for multiple end points at the same time.

Procedure

1. Click **Features on Demand Mass Activation** on the Configuration Overview page. The Features on Demand Mass Activation primary page opens. From this page you can:
   - Acquire the VPD inventory of the target machines
   - Retrieve keys (includes acquiring and downloading keys)
   - Install keys
   - Export keys
   - View the history of the Features on Demand Mass Activation tasks

   In the following example, the VPD has been collected for one machine.
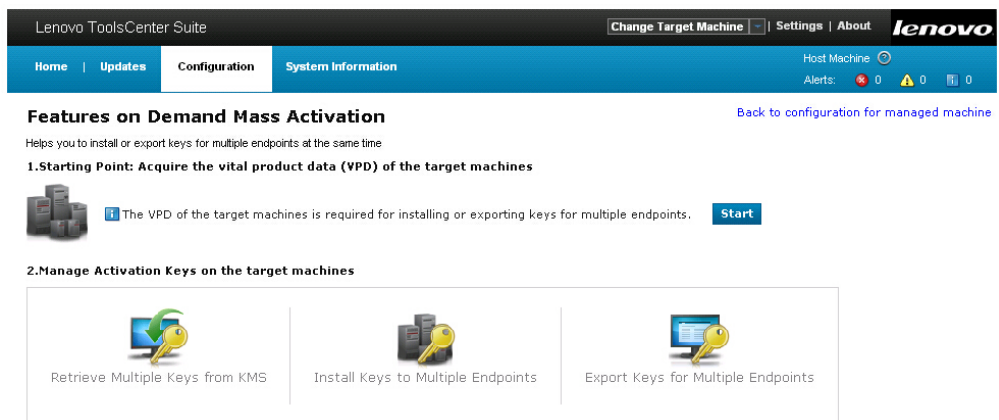
Figure 34. Configuration - Features on Demand Mass Activation primary page

2. Optional: After initially using the Features on Demand Mass Activation function, a history is available that provides information about previously completed Features on Demand Mass Activation tasks, indicating what tasks

were completed, such as a key was installed and a date stamp of when the install finished. Click **View Details** to view a list with detailed information for each history item. For more information on the History, see "Viewing the history of Features on Demand Mass Activation" on page 58.

Acquiring VPD Inventory

To manage the activation keys on target machines, you must first acquire the vital product data (VPD) for each machine.

Procedure

1. Click **Features on Demand Mass Activation** on the Configuration Overview page. The Features on Demand Mass Activation primary page opens.
2. Click **Start** to acquire the VPD of the target machines. The VPD of the target machines is required for importing or exporting mass keys.

   The Acquire the VPD of the Target Machines page opens.

Figure 35. Acquiring VPD of the target machines

3. When initially importing the VPD, click **ImportIP**. On subsequent imports of the VPD, you can click **ImportIP** or **Import IP Addresses for Target Machines**. The import file must be in CSV (.csv) format. The file contents contain the following information for each target machine:
   - IP address
   - IMM user name
   - Password

   You can create or edit an existing spread sheet (XLSX) file and save it as a CSV file. The text format for each line in a CSV file is:`<ip>,<user>,<password>`.
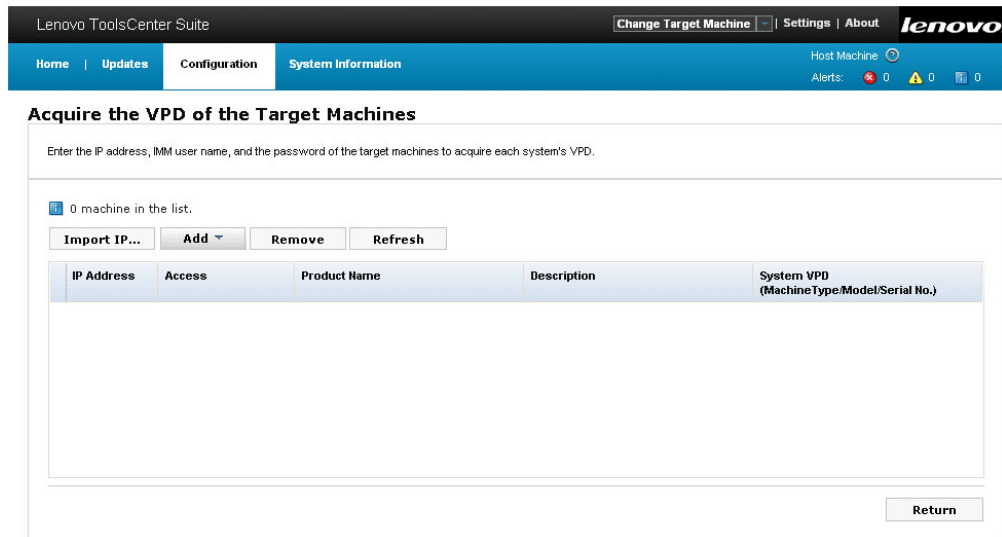
Figure 36. Acquiring VPD using an import file

4. Optional: Click **See example file** to view the contents and formatting of a sample CSV file.

5. In the Import IP Addresses for Target Machines dialog box, click **ImportFile**. In the File Upload dialog box, select the file and click **Open**. The Acquire the VPD of the Target Machines page is updated and the number of target machines successfully collected along with a list containing the VPD for each of the target machines.
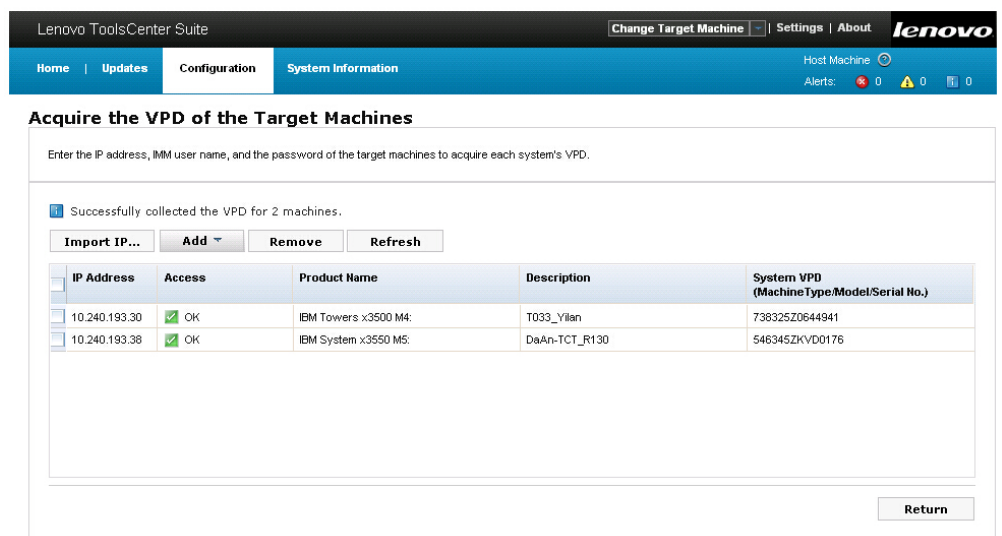
Figure 37. Acquire the VPD of the Target Machines - Imported file results

The list provides the following VPD for each target machine:

- IP Address
- Access
- Product Name
- Description
- System VPD (Machine Type/Model/Serial No.)

6. On the Acquire the VPD of the Target Machines page, to add a new machine, click **Add**. The Add New Machine dialog box opens.
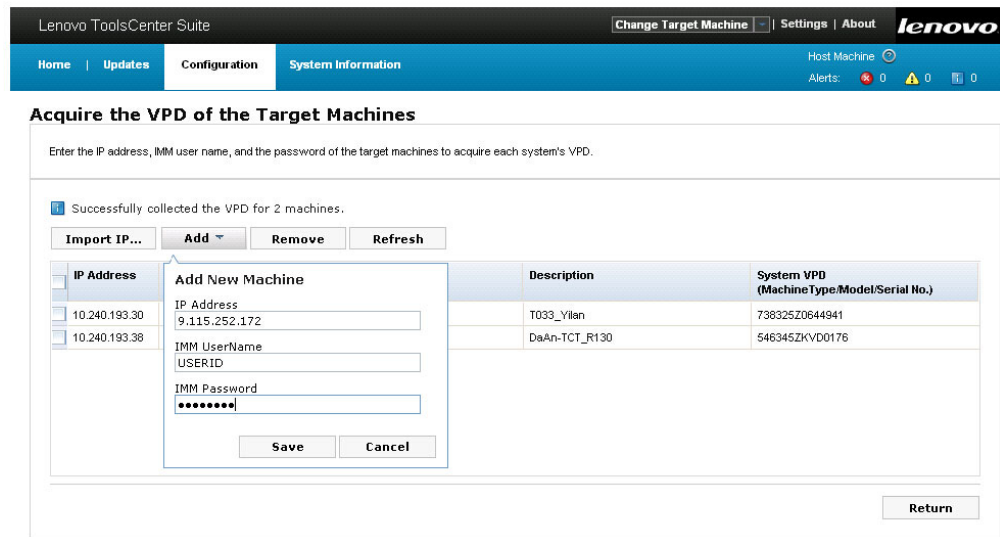
Figure 38. Acquire the VPD of the Target Machines - Adding a new machine

7. Enter the following information and then click **Save**.
   - IP Address
   - IMM UserName
   - IMM Password

   While the system is checking the new machine, a query icon is displayed. After the authentication finishes, the new machine shown in the list.

8. Optional: If you entered a duplicate IP address, the Confirm to Acquire the Duplicated IP Address dialog box opens. Click **OK** to acquire the systems with the duplicated IP address or click **Cancel** to retain the previously acquired system VPD for these machines and only acquire VPD for the new IP addresses. If the task fails, the machine list is updated and reflects there is no access to this IP address.

   Tip: To view the reason for an invalid entry in the list, hover the mouse pointer over the question mark icon.

9. Optional: To remove an invalid entry from the list, select the **IP Address** and then click **Remove**.

10. Click **Return** to return to the Features on Demand Mass Activation primary page.

Retrieving multiple keys from KMS

After acquiring vital product data (VPD) for the target machines, you can retrieve multiples keys from the Key Management System (KMS).

Procedure

1. Click **Features on Demand Mass Activation** on the Configuration Overview page. The Feature on Demand Mass Activation primary page opens.

2. In the Manage Activation Keys on the target machines section, click **Retrieve Multiple Keys from KMS**. The Retrieve Multiple Keys from KMS with a single Authorization Code page opens.

3. Enter the following information and then click **Next**.
   - IBM ID
   - User Password
   - Authorization Code

The following message is displayed while authorization is being processed:

```
Please wait while ToolsCenter Suite is acquiring the information for
the authorization code from the Lenovo website.
```


Figure 39. FoD Mass Activation - Retrieving Multiple Keys from KMS with a single Authorization Code

After the authorization code from the Lenovo website is acquired, the Select Target Machines page opens.

Figure 40. FoD Mass Activation - retrieved keys from KMS

4. On the Select Target Machines page, select the IP Address of the target machine for downloading multiple keys. The download process begins. When the download finishes, the DownloadKeys page opens indicating the number of keys that were successfully downloaded, and the Activation Key Status shows the key download status.

Figure 41. FoD Mass Activation - Downloaded Key

5. When all of the activation keys have finished downloading, click **Finish**. The Feature on Demand Mass Activation primary page opens. To install the downloaded, keys see "Installing keys to multiple endpoints"/

Installing keys to multiple endpoints

After downloading the keys, you can install the keys to multiple endpoints.

Procedure

1. Click **Install Keys to Multiple Endpoints**. All of the downloaded keys will now be installed. This process verifies the IP address and user credentials previously entered.
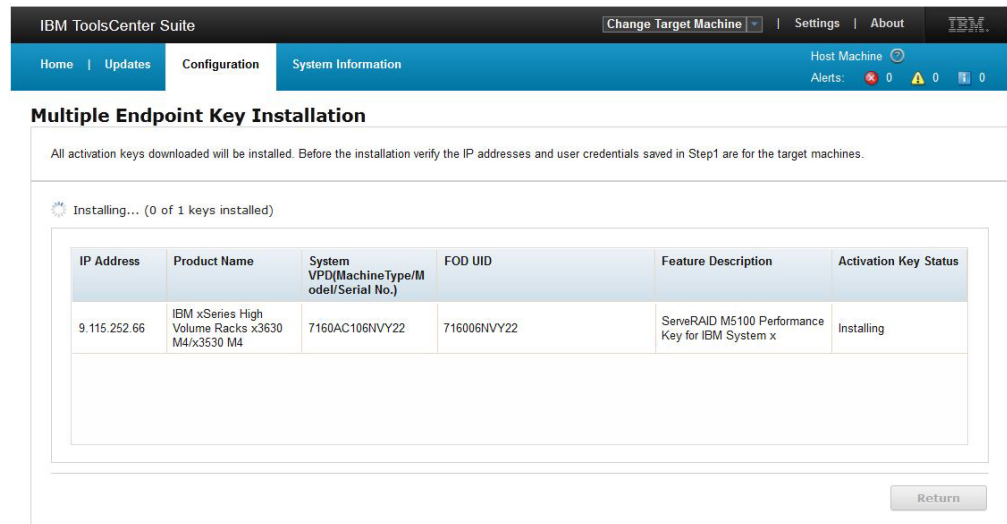
Figure 42. FoD Mass Activation - Multiple Endpoint Key Installation

If the activation keys installed successfully, the status is shown as `Installed`. If any of the activation keys failed to install successfully, the status is shown as `Failed`. The tooltip provides the reason for the installation failure.
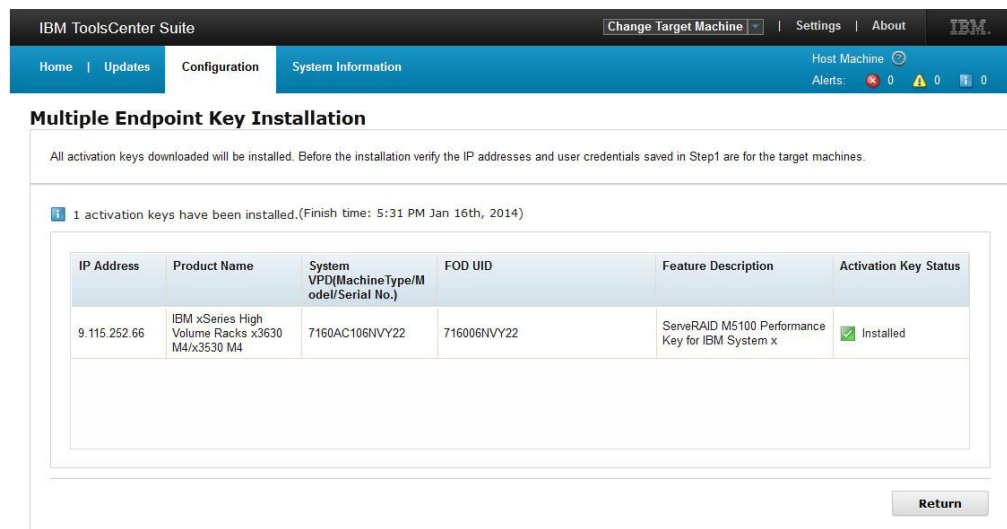
Figure 43. FoD Mass Activation key installed

2. Click **Return** to return to the Features on Demand Mass Activation primary page.

Exporting keys for multiple endpoints

The keys installed on multiple endpoints can be exported as a backup for installing again in the future.

Procedure

1. On the Features on Demand Mass Activation primary page, in the Manage Activation Keys on the target machines section, click **Export Keys for Multiple Endpoints**. The Export Settings page opens.

Figure 44. FoD Mass Activation Export Settings

2. In the Select local path to save activation keys section, enter the local directory where the exported activation keys will be saved.
3. In the Select target machines from inventory list section, select the IP address of the target machines for exporting activation keys. The export process begins and the status updates as each export finishes.

Figure 45. FoD Mass Activation Exporting keys

While an activation key is being exported, the status is `Exporting`. When an activation key has been exported, the status is shown as `Exported`.
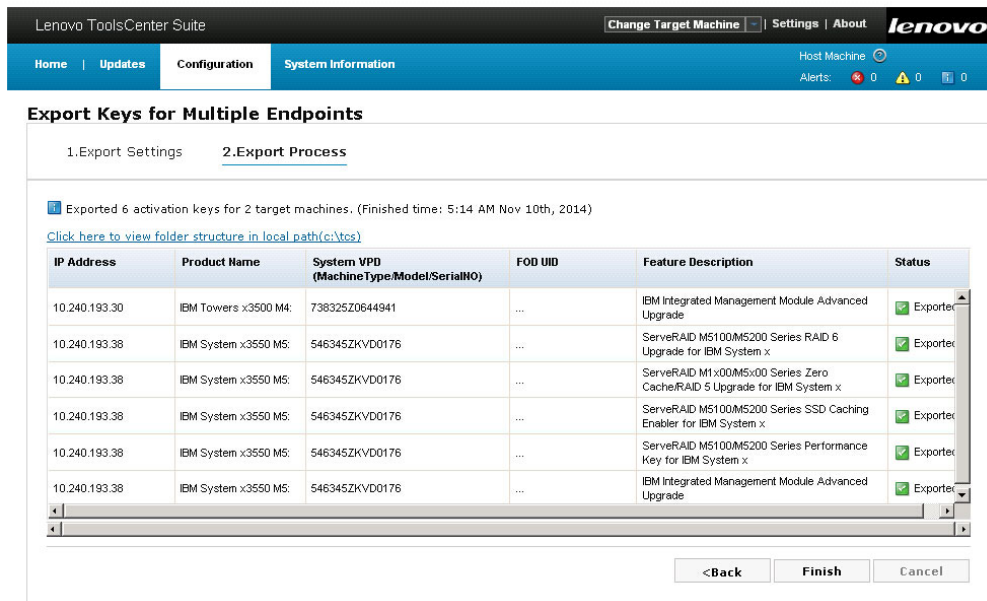

Figure 46. FoD Mass Activation Exported key

4. When the export operation finishes, you can click **Click here to view the folder structure in the local path** or click **Finish** to complete the export process and return to Features on Demand Mass Activation primary page.

Viewing the history of Features on Demand Mass Activation

The history section on the Feature on Demand Mass Activation Keys Management primary page provides information about the last successfully completed activation key management tasks.

Procedure

- To view the history detail for each Features on Demand Mass Activation task, on the Features on Demand Mass Activation primary page in the History section click **View Details** for a task.
  - This figure provides the history of the downloaded key, which is pending installation and provides the following information:
    - IP Address
    - Product Name
    - System VPD
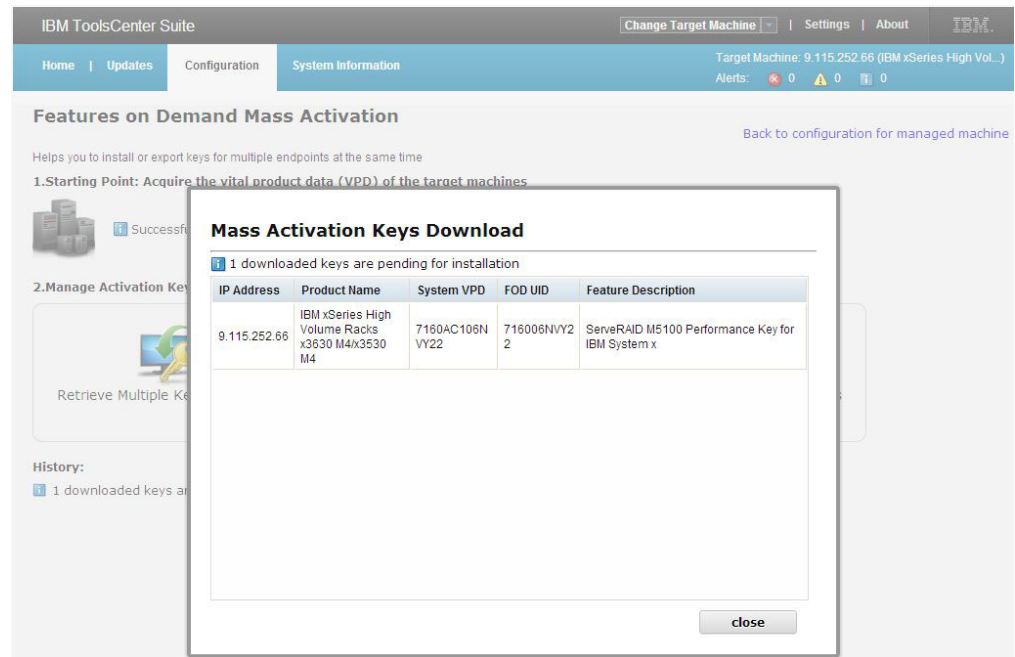   - FOD UID
    - Feature Description

Figure 47. FoD Mass Activation - downloaded keys are pending installation detail information

– This figure provides the history and detail information for an installed key and includes the following information:
   - IP Address
   - Product Name
   - System VPD
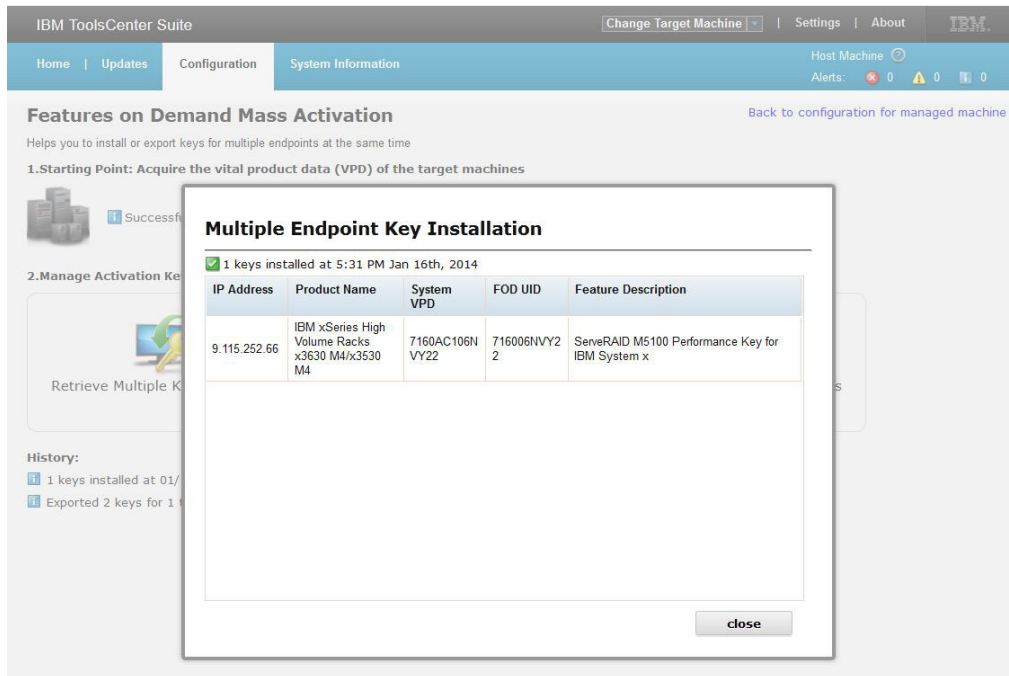   - FOD UID
   - Feature Description

Figure 48. FoD Mass Activation - installed keys detail information

– This figure provides the history and detail information for an exported key and includes the following information:

- folder location
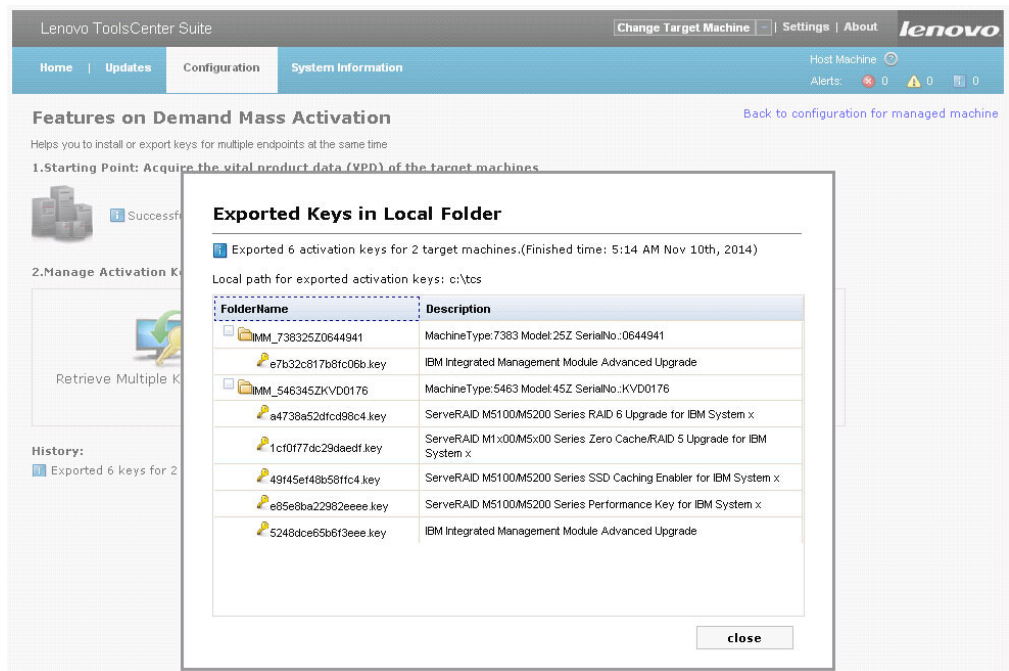- name of the key file
- a description for each activation key

Figure 49. FoD Mass Activation - exported keys detail information

• Click **Close** when you have finished viewing the details.

Working with the Full Settings option

You can use the Full Settings option to view all of your system settings. The settings listed under Full Settings varies depending on the machine type and model, and therefore it is not a fixed group of settings.

About this task

The **Full Settings** > **All** option includes:
• SYSTEM_PROD_DATA
• IMM
• iSCSI
• UEFI
• BootOrder
• PXE

The following steps provide examples for working with the Full Settings option.

Procedure

• In the navigation pane, click **Full Settings** > **All**. The Configuration - All Configuration page opens. This page provides a table listing for all of the settings, their group name, and the current value.

Tip: To view the definition of a setting, hover the mouse pointer over an entry in the table.

Figure 50. Configuration - All settings

- On this page you have several options for viewing or changing the settings.
  - To search for a setting, enter the name in the search field and click the search icon. (This is not a case sensitive search.) The best match for this setting is found and displayed in the first line of the table.
  - To change the value of a setting, in the Value column, click the arrow to view the available values and select a value from the list.
  - To apply a setting change, click **Apply**. The Apply the settings changes? dialog box opens. Click **OK** to proceed or **Cancel** to quit this operation. If you select **OK**, the following messages are displayed:

    ```
    Applying settings. Please wait...
    ```
    ```
    Update the Settings successfully.
    ```

    Click **OK** to load the settings. The following message is displayed:

    ```
    Loading, please wait...
    ```
  - To reset all of the settings, click **Reset to All Factory Defaults**. The Reset to Factory Default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel**.
- To view individual settings, in the navigation pane, click **All** and select the setting you want to view. The individual setting information is displayed in the right pane, providing the group name and current value for this setting.

Viewing and changing SYSTEM_PROD_DATA settings

You can use the **SYSTEM_PROD_DATA** option to view the current SYSTEM_PROD_DATA settings and change the values of these settings. SYSTEM_PROD_DATA is user-configurable vital product data (VPD) settings.

Procedure

1. In the navigation pane, click **Full Settings** > **All** > **SYSTEM_PROD_DATA**. The Configuration - SYSTEM_PROD_DATA Configuration page opens.
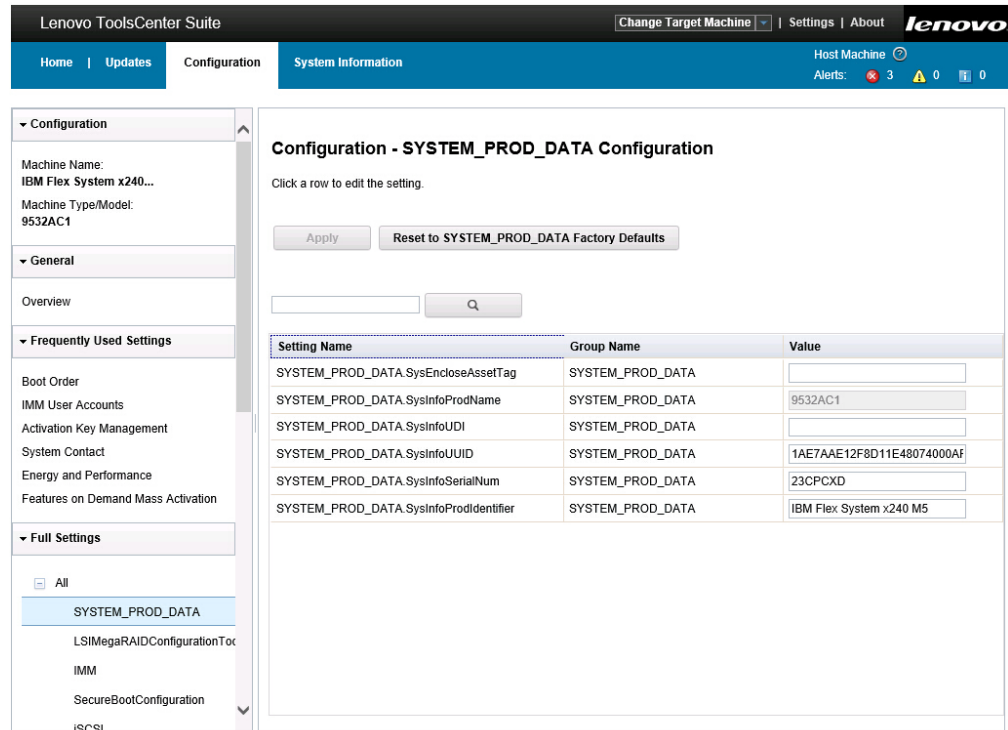
Figure 51. Configuration - SYSTEM_PROD_DATA

This page provides a table listing for all of the SYSTEM_PROD_DATA settings, their group name, and the current value.

Tip: To view a definition of a SYSTEM_PROD_DATA setting, hover the mouse point over the **Setting Name**.

2. On this page you have several options for viewing or changing SYSTEM_PROD_DATA settings.

Note: The SYS_PROD_DATA_SysInfoProdName setting's values cannot be changed.

- To search for a setting, enter the name in the search field and click on the search icon. (This is not a case sensitive search.) The best match for the setting will be found and shown in the first line of the table.

- To add or change the value of a setting, in the Value column, enter a value.

- To apply a setting change, click **Apply**. The Apply the settings changes? dialog box opens. Click **OK** to proceed or **Cancel** to quit this operation. If you select **OK**, the following messages are displayed:

  Applying settings. Please wait...

  Update the Settings successfully.

  Click **OK** to load the settings. The following message is displayed:

  Loading, please wait...

- To reset the settings, click **Reset to SYSTEM_PROD_DATA Factory Defaults**. The Reset to factory default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.

Viewing and changing the IMM settings

You can use the **IMM** settings option to view the current IMM settings and change the values of these settings.

Procedure

1. In the navigation pane, click **Full Settings** > **All** > **IMM**. The Configuration - IMM Configuration page opens.

Figure 52. Configuration - IMM settings

This page provides a table listing all of the IMM settings, their group name, and the current value.

Tip: To view a definition of an IMM setting, hover the mouse point over the **Setting Name**.

2. On this page you have several options for viewing and changing the IMM settings.

   - To search for a setting, enter the name in the search field and click the search icon. (This is not a case sensitive search.) The best match for this setting will be found and shown in the first line of the table.
   - To change the value of a setting, in the Value column, select a value from the list.
   - To apply a setting change, click **Apply**. The Apply the settings changes? dialog box opens. Click **OK** to proceed or **Cancel** to quit this operation. If you select **OK**, the following messages are displayed:

     ```
     Applying settings. Please wait...
     ```

     ```
     Update the Settings successfully.
     ```

     Click **OK** to load the settings. The following message is displayed:

```
Loading, please wait...
```

- To reset the settings, click **Reset to IMM Factory Defaults**. The Reset to factory default? dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.

Viewing and changing the iSCSI settings

You can use the **iSCSI** settings option to view and change these settings. The iSCSI settings are grouped into a record. `iSCSI.AttemptName` setting is the record key for each record. Each record represents an attempt. The term attempt is equivalent to the term instance. More than one attempt can be defined. If more than one attempt is defined, the same setting names that define the attempt group is used, but each attempt contains the next sequential instance number. For example, `iSCSI.MacAddress.1` and `iSCSI.MacAddress.2` belong to the "first" attempt and the "second" attempt respectively. The only parameter that is defined as a global iSCSI setting to all attempts and that does not require an instance index is the `iSCSI.InitiatorName`.

Procedure

1. In the navigation menu, click **Full Settings** > **All** > **iSCSI** . The Configuration - iSCSI Configuration page opens.

Figure 53. Configuration - iSCSI

This page provides a table listing for all of the iSCSI settings, and includes their group name and the current value.

Tip: To view the definition of an iSCSI setting, hover the mouse pointer over the **Setting Name**.

2. The iSCSI Configuration pages provide several options for viewing or changing iSCSI settings.

- To search for a setting, enter the name in the search field and click the search icon. (This is not a case sensitive search.) The best match for this setting is found and is shown in the first line of the table.
- To change the value of a setting, in the Value column, enter the new value.
- To apply a setting change, click **Apply**. If an incorrect value was entered, a dialog box opens and displays this information. Click **Close**. If a correct value was entered, The Apply the setting changes? dialog box is displayed. Click **OK** to proceed or **Cancel** to quit this operation. If you select **OK**, the following messages are displayed:

  ```
  Applying settings. Please wait...
  Update the Settings successfully.
  ```

  Click **OK** to load the settings. The following message is displayed:

  ```
  Loading, please wait...
  ```
- To reset the settings, click **Reset to iSCSI factory defaults**. The Reset to factory default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.

3. To view individual settings, in the navigation pane, click **All** > **iSCSI** and click the setting you want to view. The individual setting information is shown in the right pane, providing the group name and the current value for this setting.

Viewing and changing the UEFI settings

You can use the **UEFI** settings option to view and change UEFI settings.

About this task

UEFI settings include:
- BackupBankManagement
- BootModes
- DevivesandIOPorts
- LegacySupport
- Memory
- OperatingModes
- POSTAttempts
- Power
- Processors
- SystemRecovery
- SystemSecurity

Procedure

1. In the navigation pane, click **Full Settings** > **All** > **uEFI**. The Configuration - uEFI Configuration page opens.
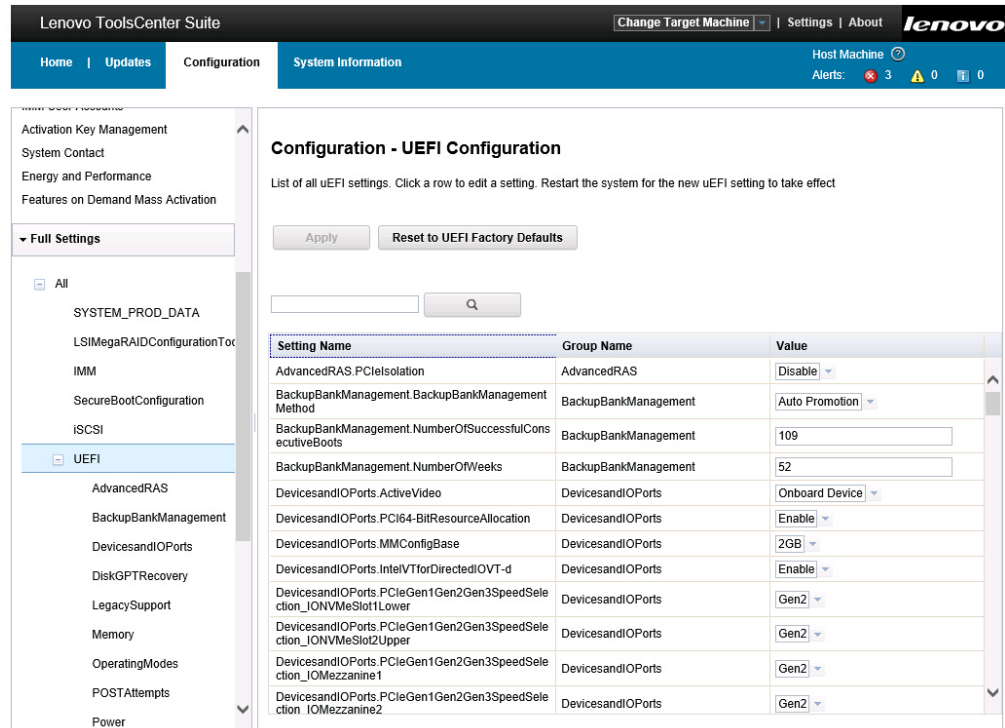
Figure 54. Configuration - UEFI settings

This page provides a table listing all of the uEFI settings, their group name, and the current value.

Tip: To view a definition of a UEFI setting, hover the mouse point over the **Setting Name**.

2. The UEFI Configuration page provides several options for viewing or changing UEFI settings.

   - To search for a setting, enter the name in the search field and click the search icon. (This is not a case sensitive search.) The best match for this setting is found and is shown in the first line of the table.

   - To change the value of a setting, in the Value column, click the **Value** list and select a value.

   - To apply a setting change, click **Apply**. The Apply the settings changes? dialog box opens. Click **OK** to proceed or **Cancel** to quit this operation. If you select **OK**, the following messages are displayed:

     `Applying settings. Please wait...`

     `Update the Settings successfully.`

     Click **OK** to load the settings. The following message is displayed:

     `Loading, please wait...`

   - To reset the settings, click **Reset to uEFI Factory Defaults**. The Reset to factory default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.

3. To view individual settings, in the navigation pane, click **All** > **uEFI** and select the setting you want to view. The individual setting information is displayed in the right pane, providing the group name and the current value for this setting.

Configuring the BootOrder settings

You can use the BootOrder settings option to view and configure the BootOrder settings. If any changes are made to BootOrder settings, the change will take affect after a system reboot.

Procedure

1. In the navigation pane, click **Full Settings** > **All** > **BootOrder** or perform a search on boot order. The Configuration - Boot Order Configuration page opens.
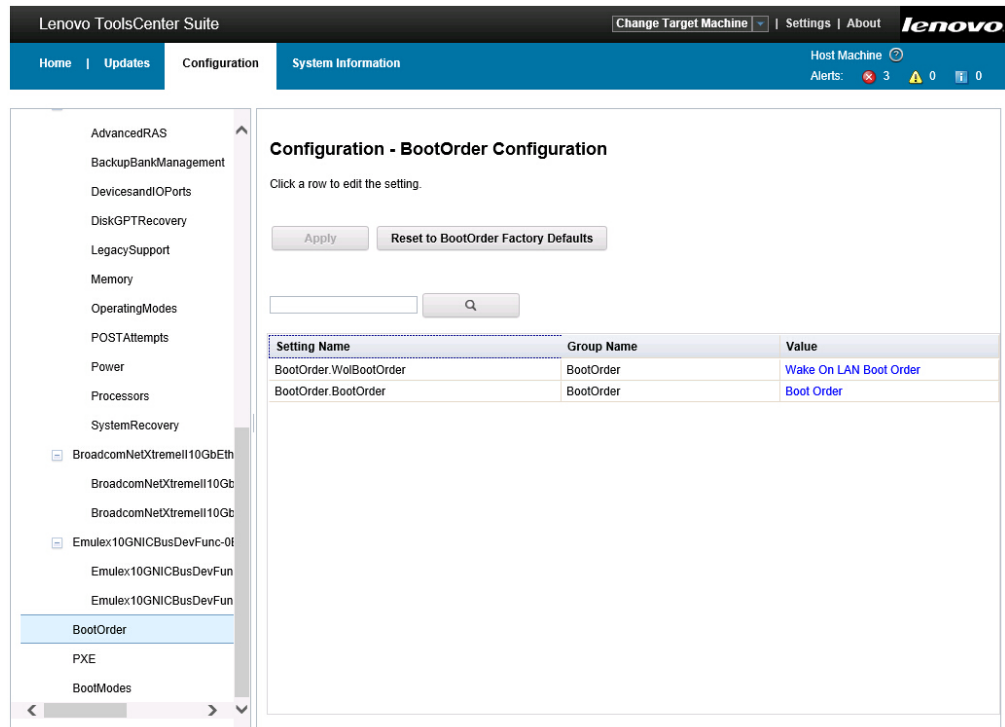

Figure 55. Configuration - Boot Order

> **Tip:** To view a definition of a boot order setting, hover the mouse point over the **Setting Name**.

2. Select one of the following options:
   - To reset the settings, click **Reset to BootOrder Factory Defaults**. The Reset to factory default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.
   - Click **Boot Order** in the Value column to select one of the boot order items listed. The Configure Boot Order dialog box opens. Click **OK** to continue or click **Cancel** to close the dialog box and return to the Configuration - BootOrder page.

Related tasks:

"Configuring, viewing, and changing Boot Order" on page 42
Provides additional information about Boot Order configuration.

Configuring the PXE settings

You can use the PXE settings option to view and configure Preboot Execute Environment (PXE) settings. PXE is an environment to boot computers using a network interface independent of data storage devices, such as hard disks or installed operating systems.

Procedure

1. In the navigation pane, click **Full Settings** > **All** > **PXE** . The Configuration - PXE page opens.
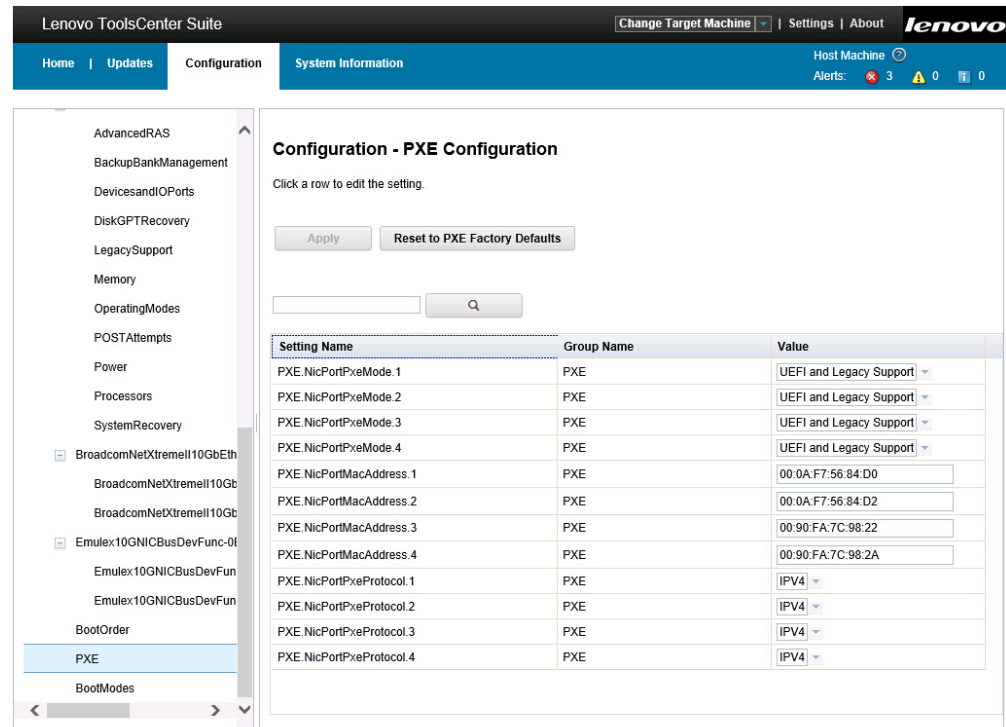

Figure 56. Configuration - PXE settings

The PXE settings table provides a list of PXE MAC addresses, PXE port devices, and PXE port protocols.

Tip: To view a definition of a PXE setting, hover the mouse point over the **Setting Name**.

2. Select one of the following options:
   - To reset the settings, click **Reset to PXE Factory Defaults**. The Reset to factory default dialog box opens. Click **OK** to proceed with resetting the values or click **Cancel** to quit this operation.
   - You can select an entry in the Value column to:
     – Change the MAC addresses by entering a new address.
     – Select a PXE port device value.
     – Select a PXE port protocol value.
   - Click **Apply** to save the new PXE settings.

Chapter 6. Using the System Information function

You can use the **System Information** function to scan and view realtime status, check active status, view light path status and event logs for your system, and manage system information on a local machine using in-band mode and out-of-band (OOB) mode for a remote machine. You can collect full system information for analysis, service, and support. These files can be sent to Lenovo Support or to a customized FTP server.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **System Information**. The System Information - Overview page opens.
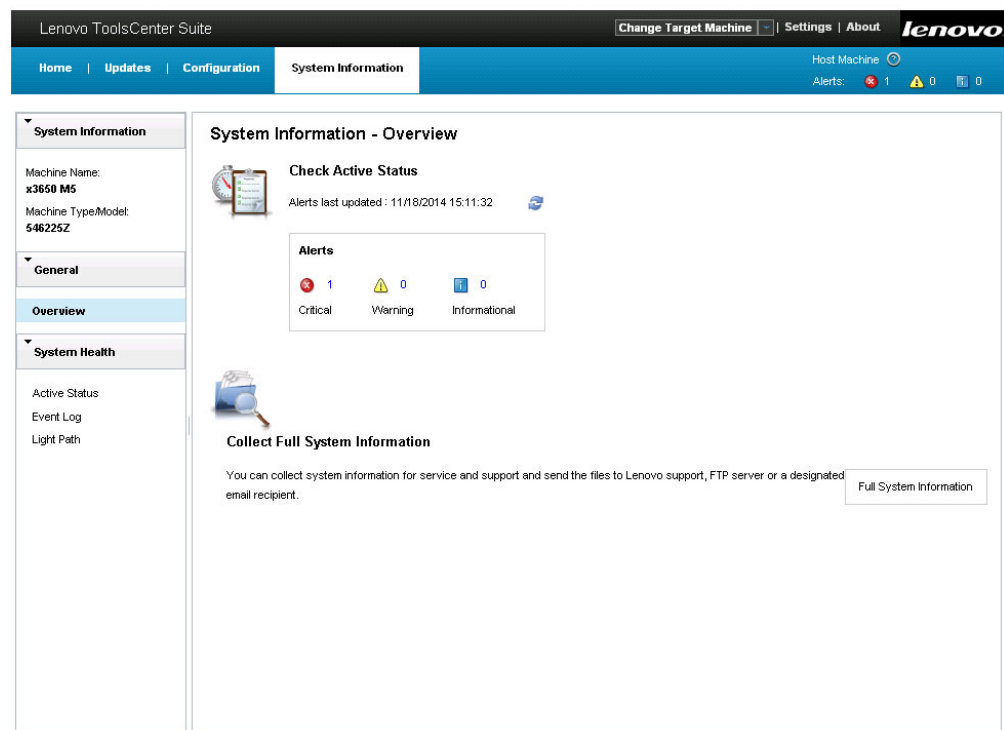

Figure 57. System Information - Overview

The **Full System Information** button can be used to collect full system information.

2. To update the Active Status, click **Refresh**. The Alerts section displays any new alerts since the Active Status was last checked. There are three types of alerts:

   - Critical: a red icon
   - Warning: a yellow icon
   - Information: a green icon

3. To view the System Overview report, click the report link in the Collect Full System Information section. The System Overview Report opens in a browser window. To return back to the System Information Overview page, close the browser window.

4. From the navigation pane, you can select the following System Health options:

- **Active Status**
- **Event Log**
- **Light Path**

Viewing Active Status

You can use the **Active Status** option to view system health status.

About this task

The following steps explain how to use the features on the Active Status page.

Procedure

- In the navigation pane, click **Active Status**. The Active Status page opens.

Figure 58. System Health - Active Status

- In Active Status table, you can click a row to view details for that row. See Figure 59 on page 73.
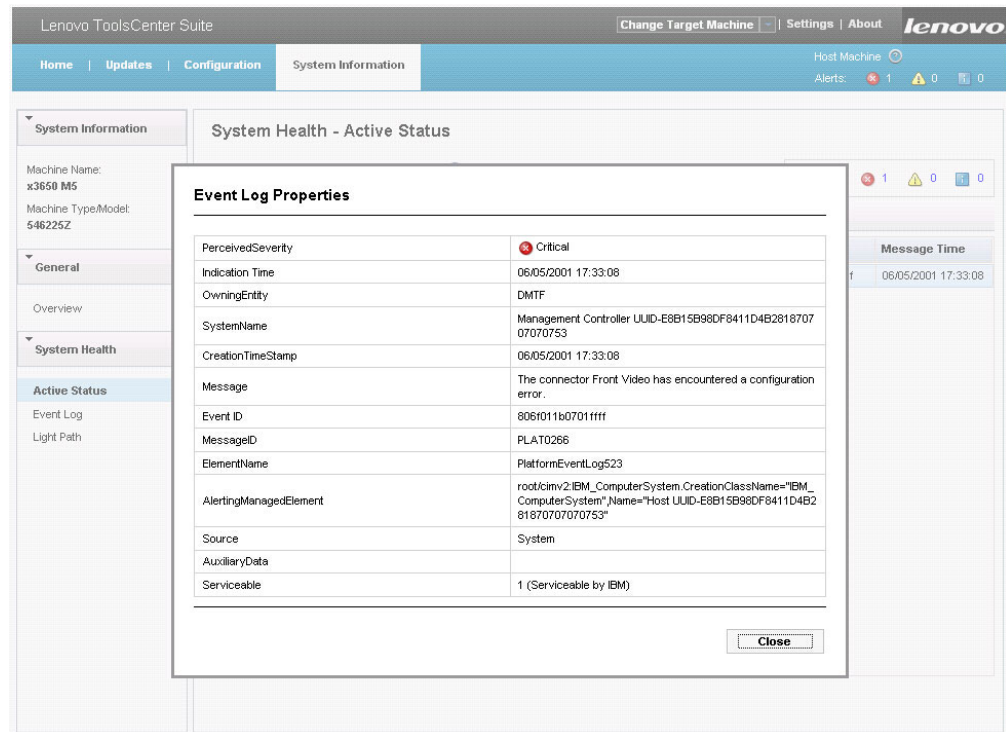
Figure 59. System Health - Active Status Property example

- To update the Active Status, click **Refresh**. The Alerts section displays any new alerts since the Active Status was last checked. There are three types of alerts:
  - Critical: a red icon
  - Warning: a yellow icon
  - Information: a green icon
- The Alerts table can be sorted to view information specific to the three table categories:
  - Severity
  - Message
  - Message Time
- From the Severity list, select and to view one of the following severity levels in the Alerts table.
  - Critical
  - Warning
  - Informational

Viewing Event Log information

You can use the Event Log option to view detailed information for critical, warning, and informational events collected from the IMM system event logs.

About this task

The following steps explain how to use the features on the Event Log page, beginning with the options at the top of the page.

Procedure

1. In the navigation pane, click **Event Log**. The System Information - Event Log page opens.

   There are three levels of severity recorded in the event logs:

   - Critical: a red icon

   - Warning: a yellow icon

   - Informational: a green icon

Figure 60. System Information - Event Log

2. To collect the latest Event Log status, click **Refresh**. When you initially open the Event Log page, previously-collected Event log information is listed in the table.

3. Click **Installation and Service Guide** to view suggested actions for detected problems found in the event logs.

   The following page is an example of the Installation and Service Guide. The Installation and Service Guide provides installation and service guide information.
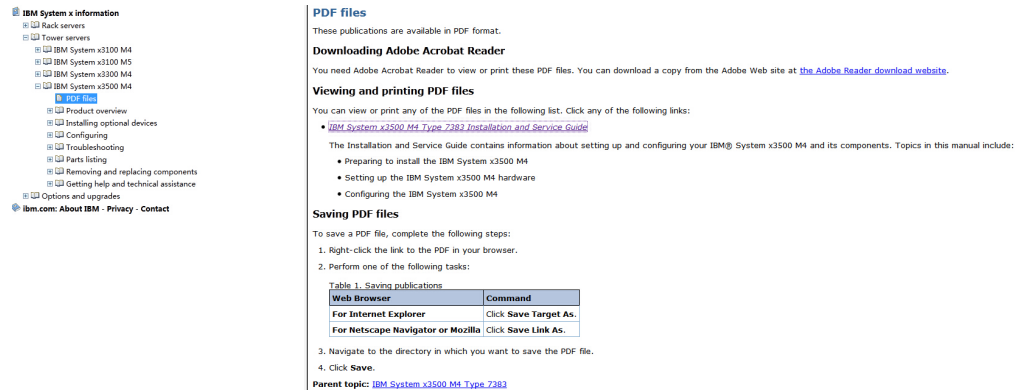
Figure 61. Installation and Service Guide

4. From the Severity list, you can select one of the following filtering options:
   - Any
   - Critical
   - Warning
   - Informational

5. From the Source list, you can select one of the following filtering options:
   - All
   - Audit
   - Cooling
   - Power
   - Disks
   - Memory
   - Processors
   - System
   - Test
   - Other
   - Unknown

6. You can sort by report category by clicking a column heading. The Event Log has the following column headings:
   - Severity
   - Message
   - Event ID
   - Source
   - Message Time

7. You can double click an Event ID to view an Event Log Property.

   The following figure provides an example of an Event Log property with a `PerceivedSeverity` of Critical.
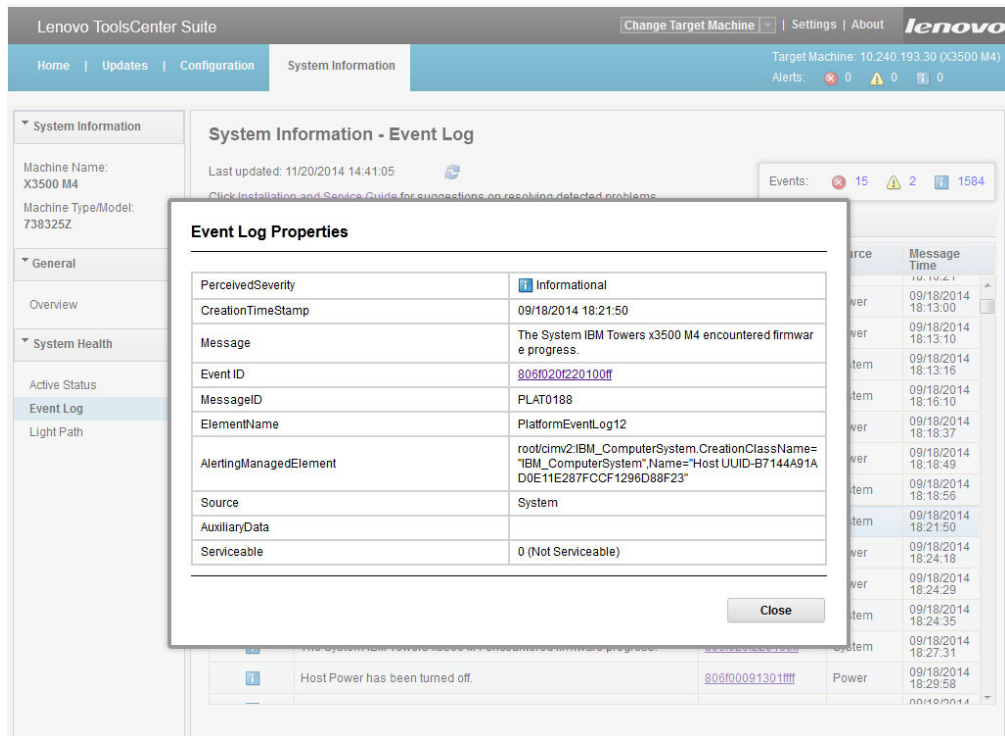
Figure 62. Event Log Properties

8. Click the Event ID link to view additional information to assist you with problem determination and resolution.

   The Event ID links to Info Center event ID link:
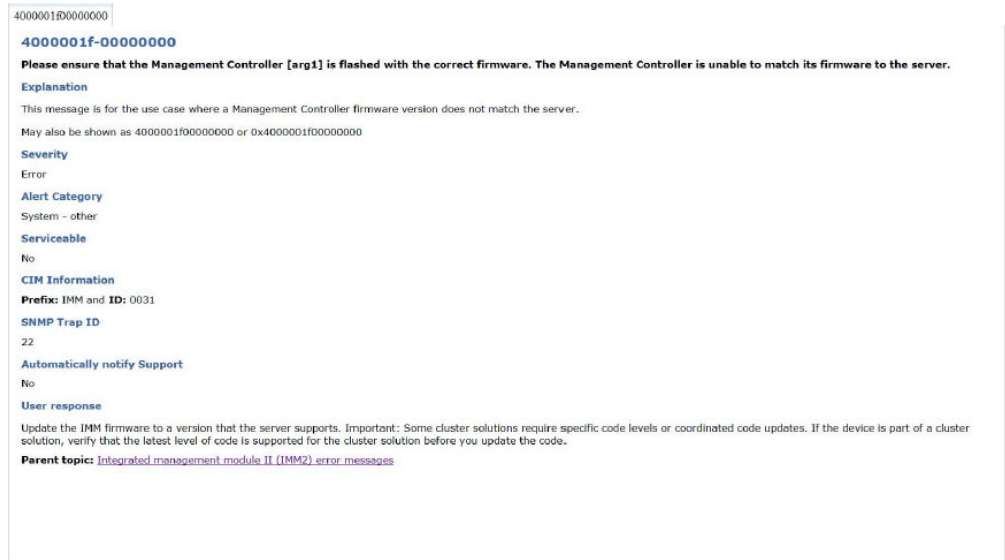
Figure 63. Event Log Event ID Link

Viewing Light Path status

You can use the **Light Path** option to view the location and status for light emitting diodes (LEDs) located on the front panel and Detail LEDs in various locations on the planar.

Procedure

1. In the navigation pane, click **Light Path** . The System Information - Light Path page opens.
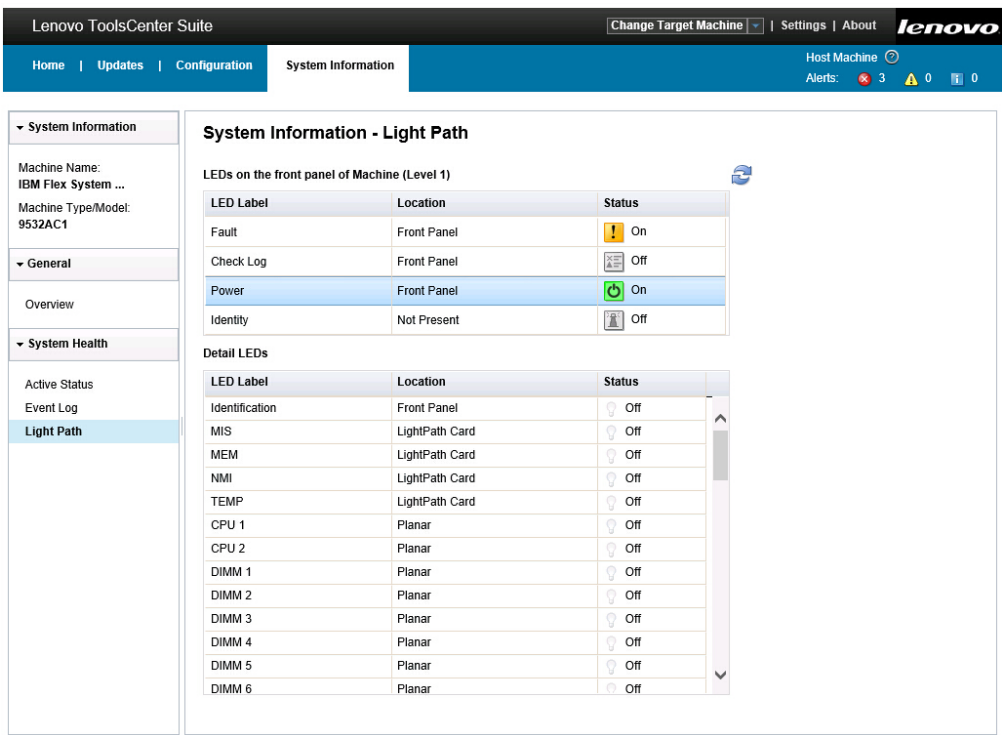
Figure 64. System Information - Light Path status

2. To collect the latest light path information, click **Refresh**. When you initially open the System Information - Light Path page, previously-collected light path information is listed in the tables.

3. You can view the following light path status on this page:

   LEDs on the front panel of the machine (Level 1):
   - Fault
   - Identity
   - Power
   - Check Log

   The status reported for front-panel LEDs is either **On** or **Off**. The location is either **Front Panel** or **Not Present**.

   Detail LEDs:
   - CPU 1
   - CPU 2
   - DIMM 1
   - DIMM 2

- DIMM 2
- DIMM 4
- DIMM 5
- DIMM 6
- DIMM 7
- DIMM 8
- DIMM 9
- DIMM 10
- DIMM 11
- DIMM 12
- DIMM 13
- DIMM 14
- DIMM 15
- DIMM 16
- PCIE 1
- PCIE 2
- Battery
- IMM2 Heartbeat
- Mezz Card

The status reported for Detail LEDs is either **On** or **Off**, except IMM2 Heartbeat, which has a status of Blinking. The location varies for each machine type.

Collecting Full System Information

You can use the Full System Information option to query a system and view full system information for analysis, service, and support. The files generated by the collection process can be sent to Lenovo support, sent to an FTP server, or saved locally.

Procedure

1. On the System Information - Overview page, the first time you are collecting information, click **System Full Information** . Click **Collect Again** after the information has been initially collected to refresh the full system information before viewing the report. The Collect Full System Information dialog box is displayed while the full system information is being collected.
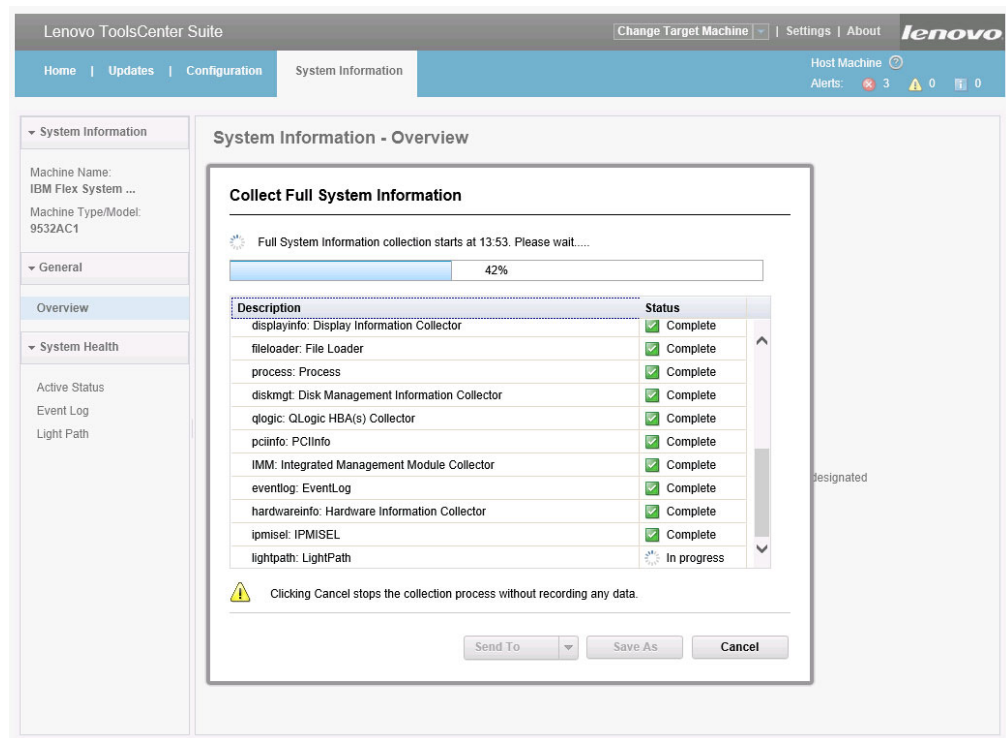
Figure 65. System Information - Collect Full System Information

As the collection progresses, an inventory list is generated which provides the status for each inventory item, indicating *Initializing* while collecting information and *Complete* when the collection process is finished. When the Full System Information collection is finished, the following page is displayed.
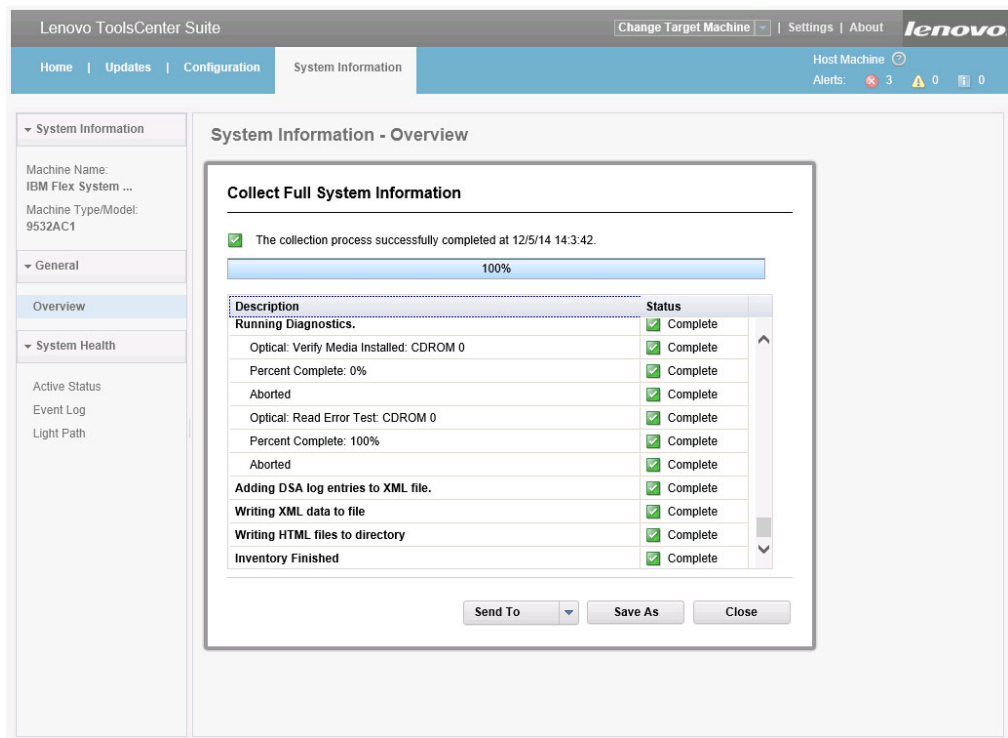
Figure 66. System Information - Collect Full System Information Status is Complete

2. Click **Send To** and then select one of the following options, which are explained in further detail below.

- Lenovo Support
- Custom FTP
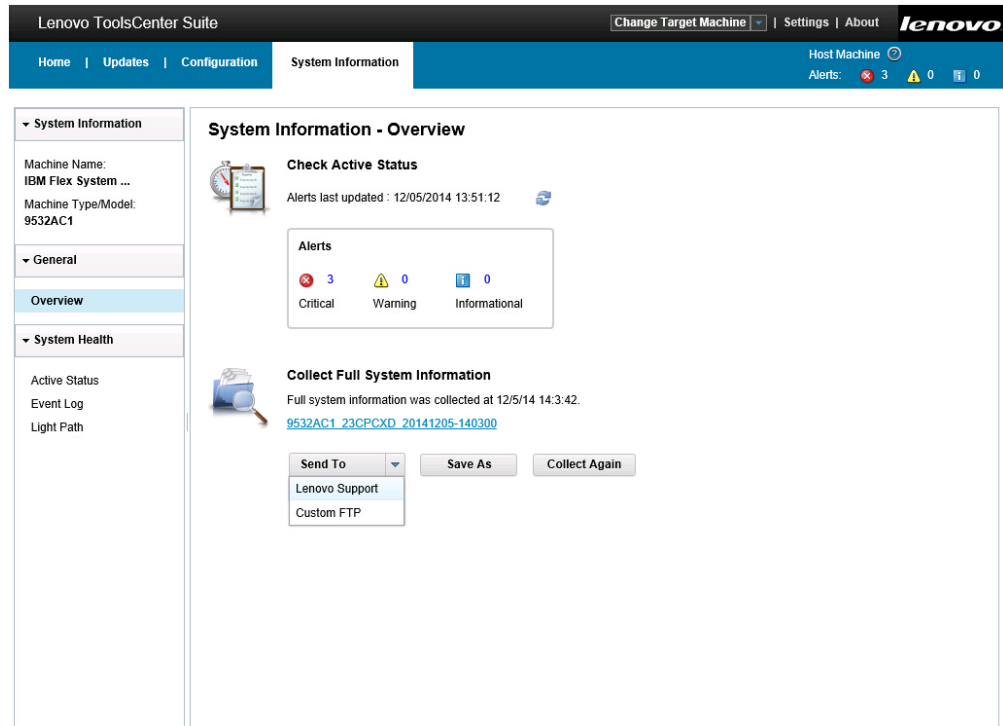
Figure 67. Full System Information Send To options

- To send the full system information report directly to Lenovo Support, click **Send to Lenovo Support**. The following message is displayed while the collection is being sent.
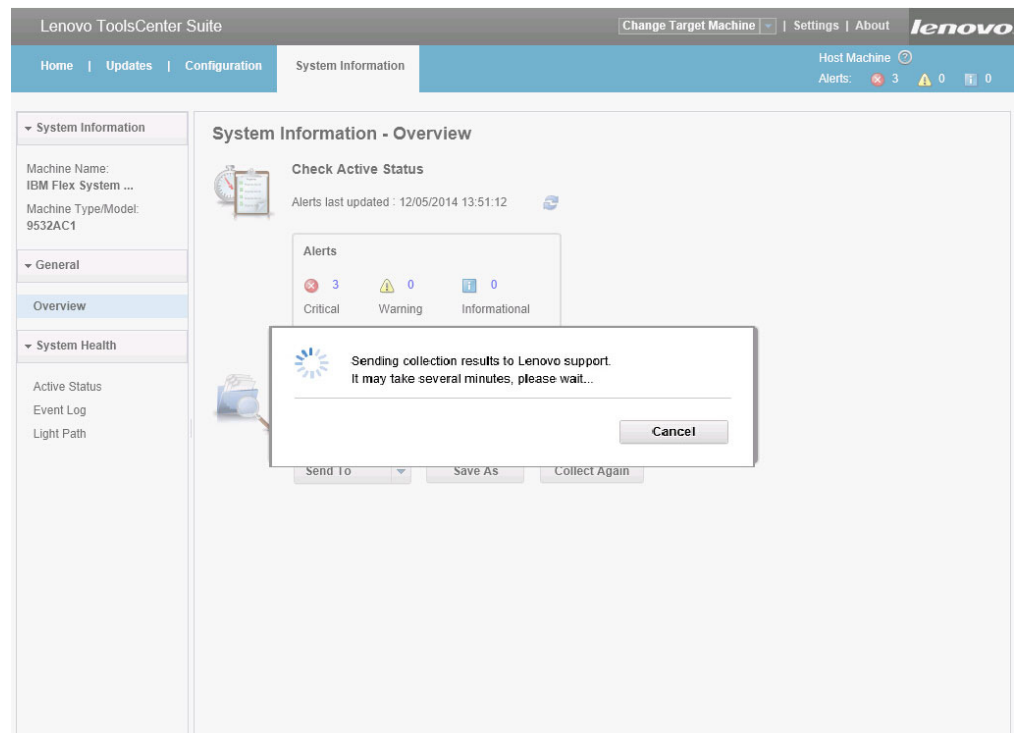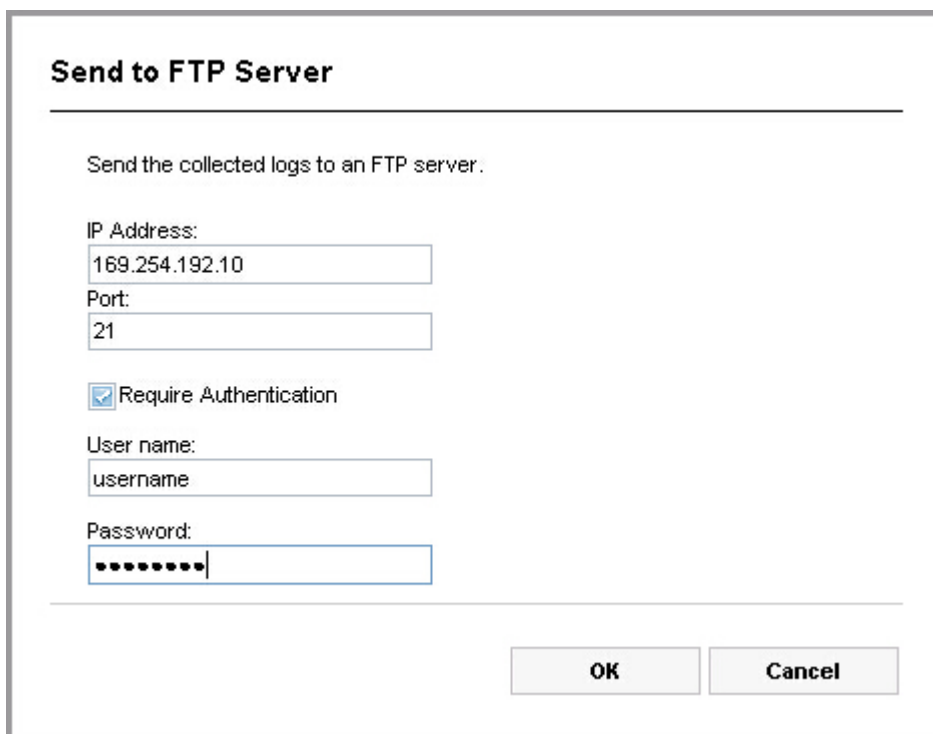
Figure 68. Full System Information being sent to Lenovo Support

When this operation is finished, click **Close**. If the send to Lenovo Support fails, the Configure Internet Connection dialog box opens.

Note: If you are not connected to the Internet, the Configure Internet Connection dialog box is displayed. Check your configuration and try again, otherwise, click **OK** to continue or **Cancel** to quit this operation. For more information see "Configuring your Internet Connection settings" on page 12.

- To send the collected logs to a customized FTP server, click **Send to FTP Server**. The Send to FTP Server dialog box opens.

Send to FTP Server

Send the collected logs to an FTP server.

IP Address:
169.254.192.10

Port:
21

☑ Require Authentication

User name:
username

Password:
••••••••

OK   Cancel

Figure 69. Full System Information Report being sent to FTP server

Complete the following steps and then click **OK**.
- Enter the `IP Address`
- Enter the `Port`
- Optional: Select **Require Authentication**. If you select this option, enter the following information:
  - User name
  - Password

After entering the FTP server information, the following message is displayed while the collection is being sent.
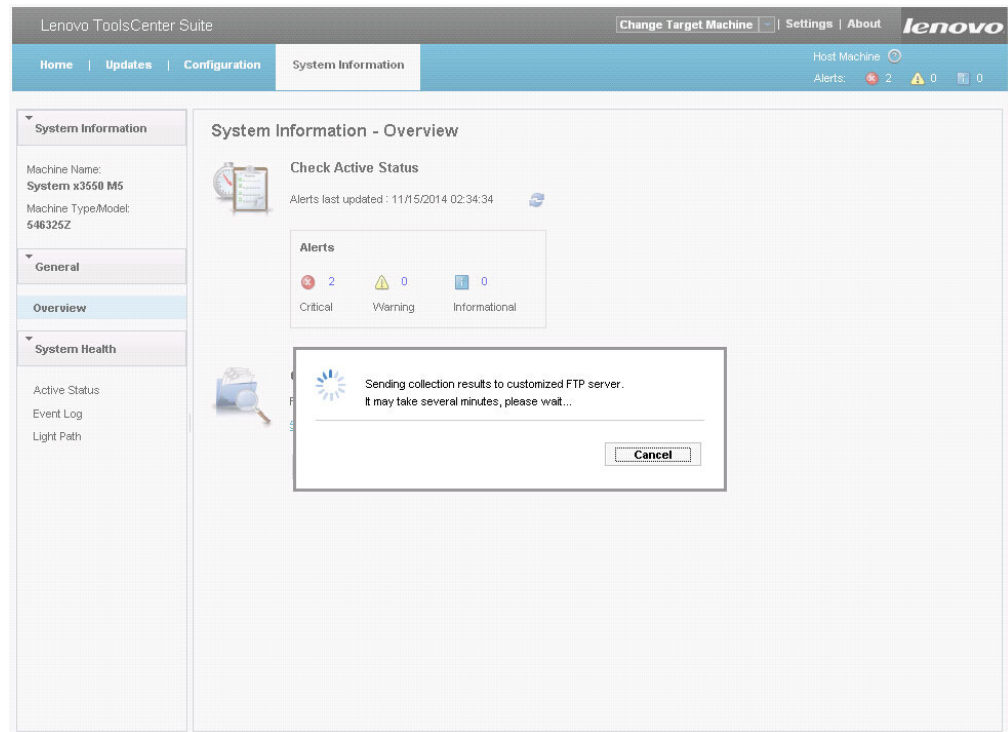
Figure 70. Full System Information being sent to customized FTP Server

3. To download the Full Collection Information zip file to a local directory, click **Save As**. The Save As file dialog box provides the name of the full system report zip file.
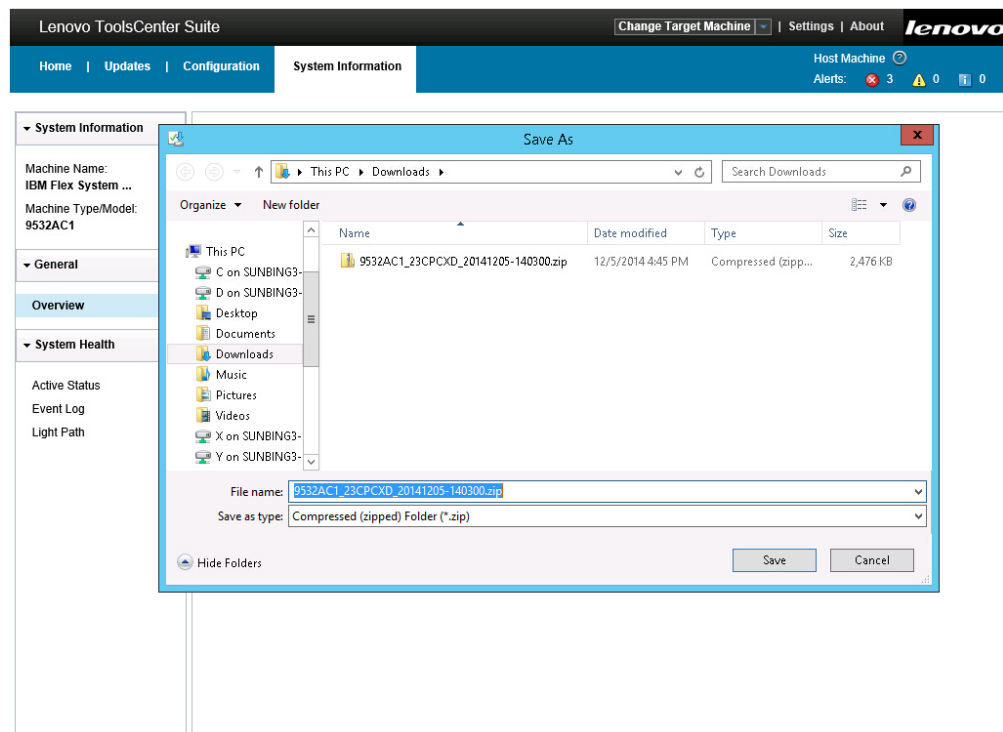
Figure 71. Full System Information Save As option

Select one of the following options.

- Click **Save** to save the Full Collection Information zip file.

  The Save As dialog box opens to select a folder for saving the zip file.

- Click **Cancel** to quit this operation.

Viewing the ToolsCenter Suite report

You can use this option to view the ToolsCenter Suite report and detailed information produced by the Collect Full System Information function.

Procedure

1. Click the **Full System Information report** link on the System Information - Overview page to view the full system information report. The System Overview report is displayed in a browser window as shown below.

   You can also click **Collect Again** to collect full system information again before viewing the report. The Collect Full System Information dialog box is displayed while the full system information is updated. For more information, see "Collecting Full System Information" on page 78.

Figure 72. System Information - Full System Information Report

2. From the navigation pane, you can select specific items listed within the five main report categories to get more detailed information. The available report information is determined by machine type, operating system, installed hardware and software. Information that is not applicable to your system will be greyed out in the navigation menu.

   - **Software:**
     - System Overview
     - Installed Packages
     - Kernel Modules
     - Network Settings
     - Resource Utilization

- Processes
- OS Configuration
- Linux Config Files
- **Hardware:**
  - Hardware Inventory
  - PCI Information
  - Firmware/VPD
  - IMM Configuration
  - Environmentals
  - Drive Health
  - LSI Controller
  - LSI IDE Controller
  - Mellanox Adapter
  - PMC RAID
  - ServeRAID™
  - ServeRAID Logs
  - Qlogic
  - Emulex
  - Broadcom
  - Brocade Adapter
  - VMware ESXi
  - Light Path
  - IMM Built-in Self Test
  - FoD Activation Key
- **Platform Logs:**
  - /var/log/boot.log
  - /var/log/cron
  - /var/log/dmesg
  - /var/log/messages
  - /var/log/secure
- **IMM Logs:**
  - Chassis Event Log
  - IPMI Event
- **Analysis:**
  - Merged Log
  - UpdateXpress
  - File Loader Results
  - Diagnostics Log
  - DSA Error Log

3. When you have finished viewing the information, close the browser window.

Chapter 7. Using the Change Target Machine function for remote connectivity
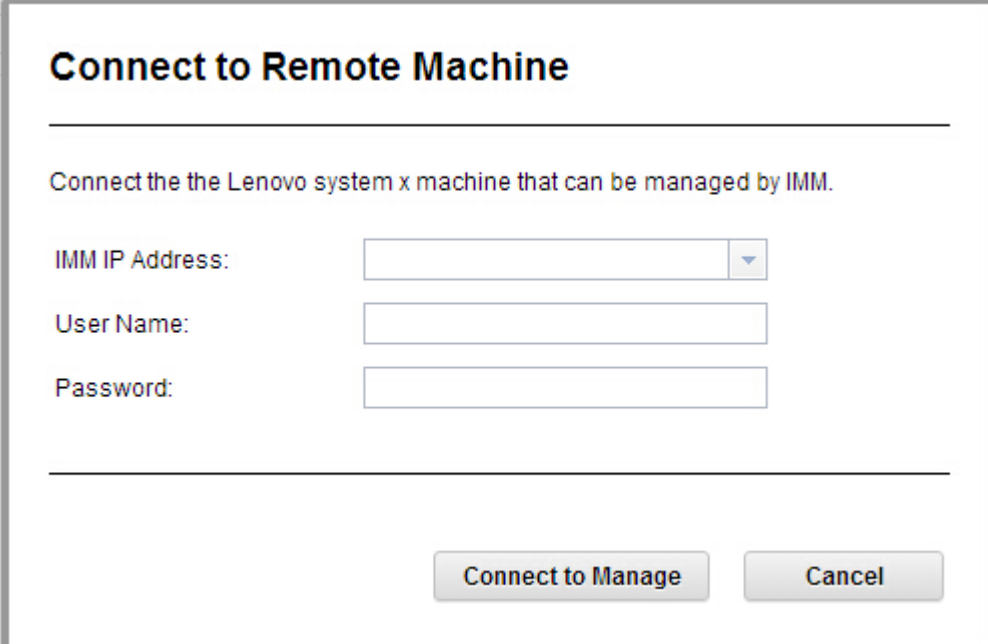
The topics in this section describe how to use the **Change Target Machine** function for connecting to remote machines from the ToolsCenter Suite host machine.

Connecting to a remote machine

The ToolsCenter Suite host can connect to remote machines, manage them in out-of-band mode (OOB) using IMM. The out-of-band management functionality includes: Configuration, System Information, and Updates for System x firmware.

Procedure

1. On the Home page, click **Change Target Machine** > **Connect to remote machines**. The Connect to Remote Machine dialog box opens.

Connect to Remote Machine

Connect the the Lenovo system x machine that can be managed by IMM.

IMM IP Address:

User Name:

Password:

Connect to Manage   Cancel

Figure 73. OOB log in

2. Enter the following information and then click **OK**.
   - IMM IP Address

     Note: After a connection to a remote machine has been made, the IMM IP Address can be selected from the IMM IP Address list.
   - User Name
   - Password

   While the Host Machine connects to the remote machine, a message stating "`Connecting to the remote machine...`" is displayed.

   When the remote connection is complete, the ToolsCenter Suite Home page opens on the remote machine. In the menu banner, the target machine

information is displayed.

Figure 74. Remote machine Home page

Results

If the remote machine is a Flex system, ToolsCenter Suite has the ability to use the CIM credentials to connect to IMM and create an IPMI account. The IMM IPMI account dialog box is displayed.
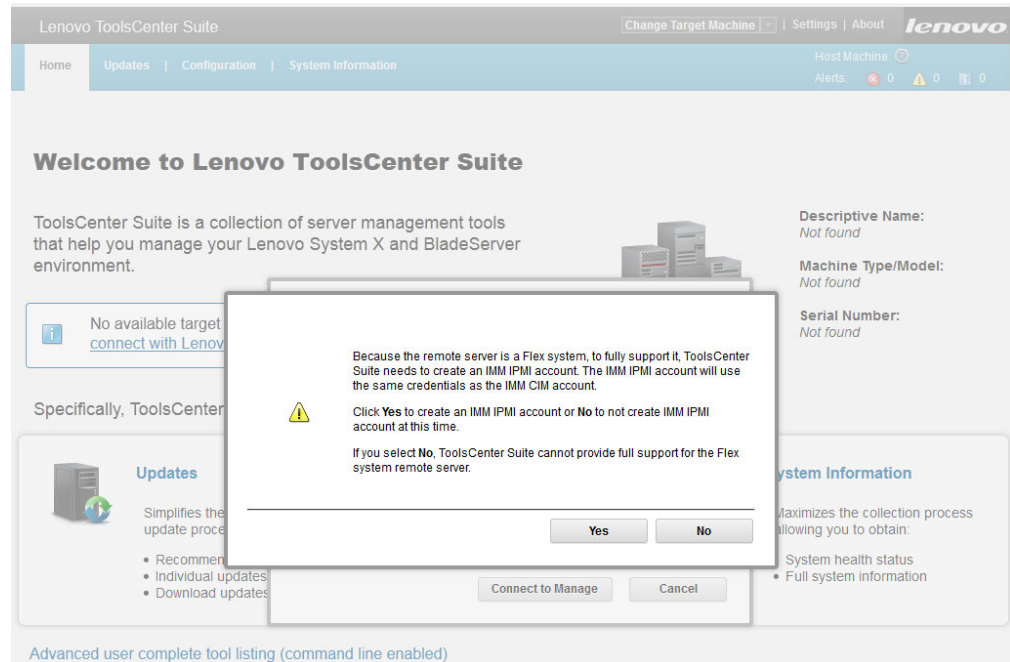
Figure 75. Remote machine - creating an IMM IPMI account

1. Click **Yes** to create an IPMI account. The IMPI account is created and ToolsCenter Suite automatically logs in to the IMM of the remote Flex system with the CIM account credentials.

2. Click **No** to not create an IPMI account at this time.

   Note: If you select **No**, ToolsCenter Suite support for the Flex System remote server is limited.

Related reference:

"ToolsCenter Suite menu options" on page 11
The ToolsCenter Suite graphical user interface (GUI) has the following menu options:

Using the Updates function on a remote machine

You can update firmware and add support for a remote machine using the Updates function. The topics in this section describe how to check the compliance of firmware, how to download and install updates, and how to use the Bare Metal Update option that allows you to download and install an earlier version of firmware.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **Updates**. The Firmware Updates page opens.
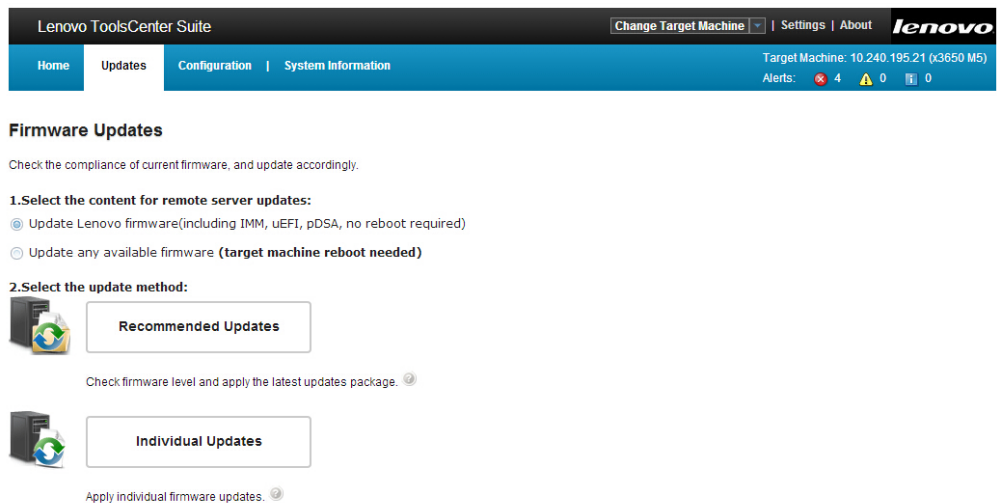
Figure 76. Remote machine - Firmware Updates

> **Tip:** To view additional information for each update type, hover the mouse pointer over the question mark icon.

2. In the Select the content for remote server updates section, select one of the following options:

   - **Update Lenovo firmware (including IMM, uEFI, pDSA, no reboot required)**
   - **Update any available firmware (target machine reboot needed)**

   Update any available firmware (target machine reboot needed) is the Bare Metal Update option that requires the target machine is rebooted. It also checks the target machine's firmware levels. If the target machine's IMM or pDSA version does not satisfy the bare metal update requirement, the following warning message is displayed:

   ```
   The target server's IMM and DSA version don't meet the selected feature
   requirement, please update the IBM firmware first.
   IMM: 1A0049W or higher version
   DSA: DSYTB7U or higher version
   ```
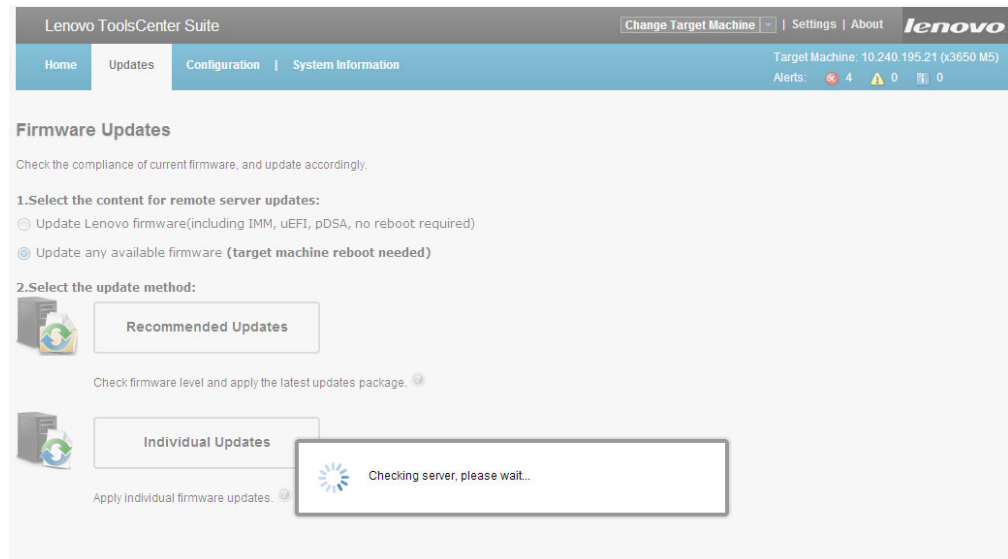
Figure 77. Remote machine - Bare metal update firmware check

> If you selected the **Update any available firmware (target machine reboot needed)** option and the target machine's firmware level satisfies the bare metal update requirement, the following message is displayed:
>
> ```
> The target system will reboot to enter a bare metal machine update environment,
> because you have chosen to update any available firmware. Compare the currently
> installed firmware to the following source:
> ```

3. In the Select the update method section, you can select one of the following update options:

   - **Recommended Updates**: Check firmware level and apply the latest updates package.
   - **Individual Updates**: Apply individual firmware updates.

   Refer to the corresponding update method in this section for complete instructions.

Using the Recommended Updates from the Lenovo website option for a remote machine

You can use the **Recommended Updates from the Lenovo website** option to check the firmware levels of the remote machine and applies the latest updates package (IMM, uEFI, pDSA UXSP firmware) that was downloaded from the Lenovo website.

Before you begin

Start ToolsCenter Suite on the host computer and connect to a remote machine. See "Connecting to a remote machine" on page 87.

About this task

This procedure provides an example of using Recommended Updates from the Lenovo website and includes the Bare Metal Update option.

Procedure

1. On the Firmware Updates page, in the Select the content for remote server updates section, click one of the following options:
   - **Update IBM firmware (including IMM, uEFI, pDSA, no reboot required)**
   - **Update any available firmware (target machine reboot needed)**

   Update any available firmware (target machine reboot needed) is the Bare Metal Update option that requires the target machine is rebooted. It also checks the target machine's firmware levels. If the target machine's IMM or pDSA version does not satisfy the bare metal update requirement, the following warning message is displayed:

   ```
   The target server's IMM and DSA version don't meet the selected feature
   requirement, please update the IBM firmware first.
   IMM: 1A0049W or higher version
   DSA: DSYTB7U or higher version
   ```

2. In the Select the update method section, click **Recommended Updates** and then click **Next**.

   If you selected the **Update any available firmware (target machine reboot needed)** option and the target machine's firmware level satisfies the bare metal update requirement, the following message is displayed.

   ```
   The target system will reboot to enter a bare metal machine update environment,
   because you have chosen to update any available firmware. Compare the currently
   installed firmware to the following source:
   ```


Figure 78. Remote machine - Recommended Updates using the latest UXSP from the Lenovo website - bare metal update reboot message

3. Click **The latest UXSP updates package from the Lenovo website** and then click **Next**.

   The check firmware compliance process begins by acquiring the current machine's firmware levels from the Lenovo website. During the acquire operation, **Cancel** is enabled, and the following message is displayed:

```
Please wait while ToolsCenter Suite acquires your firmware levels.
```
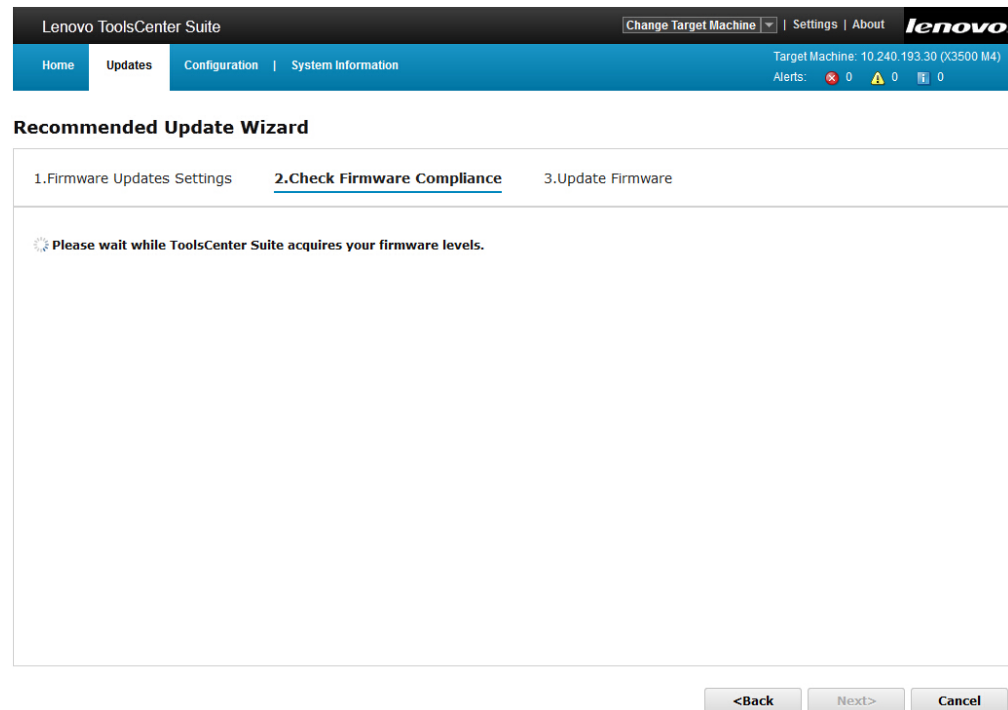

Figure 79. Remote machine - Recommended Updates - ToolsCenter Suite acquiring current machine's firmware levels for a bare metal update

After the acquire operation finishes, the check firmware compliance operation begins.

However, if you selected to **Update any available firmware (target machine reboot needed)**, the Updates page is locked, **Cancel** is disabled, and the following message is displayed:

```
Rebooting the target server to enter a bare metal machine update environment.
```
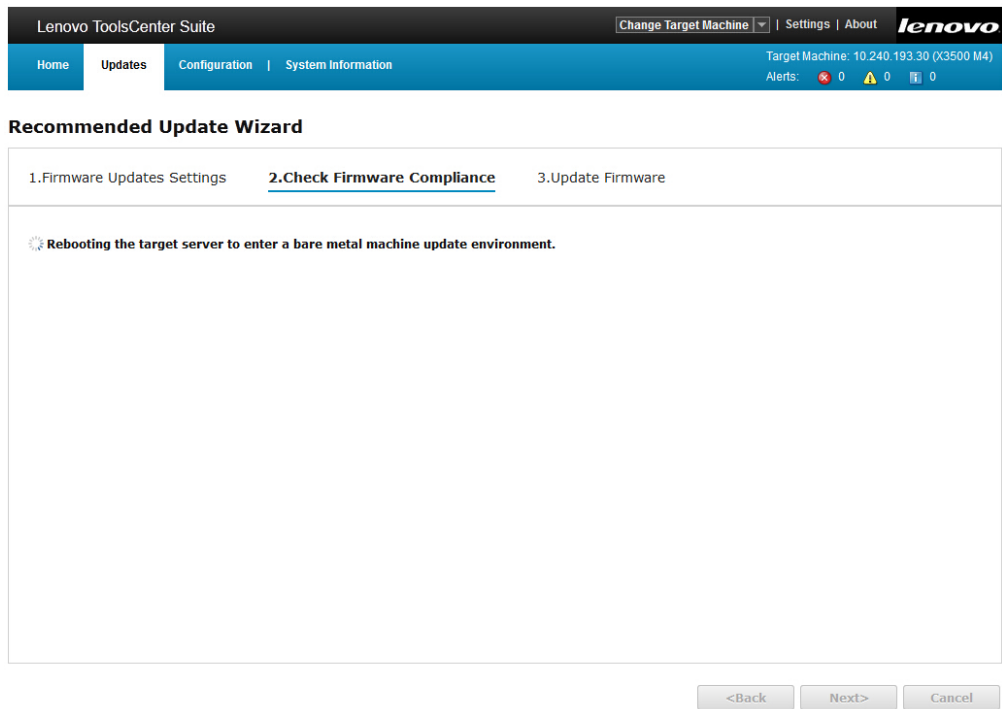
Figure 80. Remote machine - Recommended Updates - target server rebooting to bare metal environment

If the IMM and/or DSA version does not satisfy the bare metal update requirements, ToolsCenter Suite downloads the latest version of IMM and/or DSA and flashes the target machine's IMM and/or DSA.

While the compliance checking operation is working, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

```
Please wait while ToolsCenter Suite compares your current firmware
 with the latest update package.
```
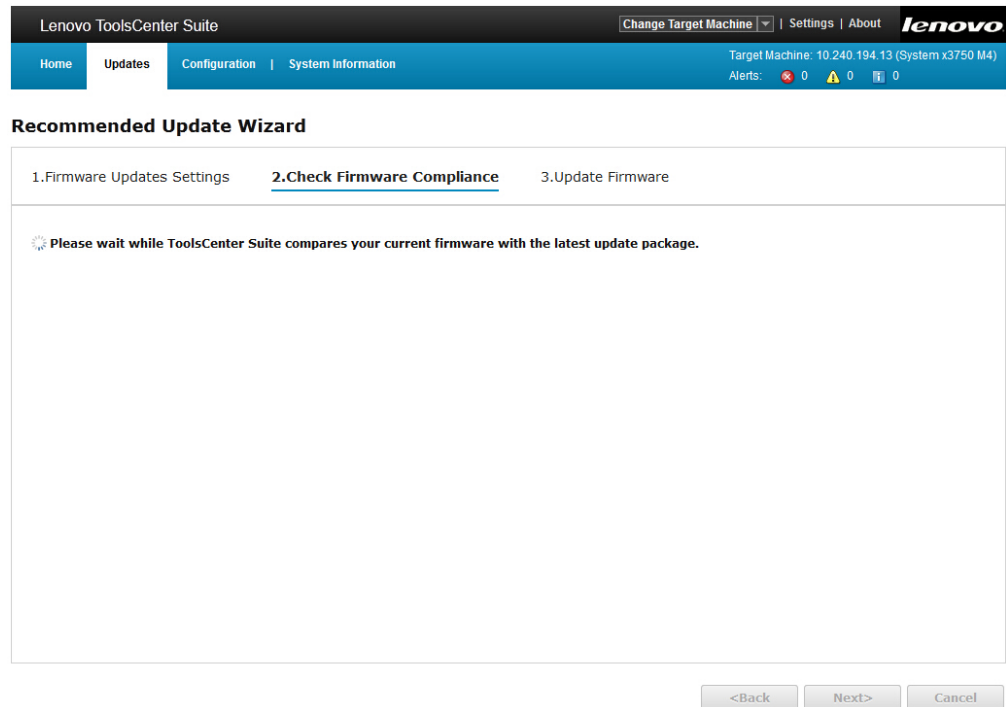
Figure 81. Remote machine - Recommended Updates - ToolsCenter Suite compares current firmware with the latest update package

> **Note:** If you are not connected to the Internet, the Configure Internet Connection dialog box opens. Check your configuration or try again, otherwise, click **OK** to continue or **Cancel** to quit this operation. For more information, see "Configuring your Internet Connection settings" on page 12.

> When the check firmware compliance operation finishes, the number of firmware items available is displayed above the firmware updates table.
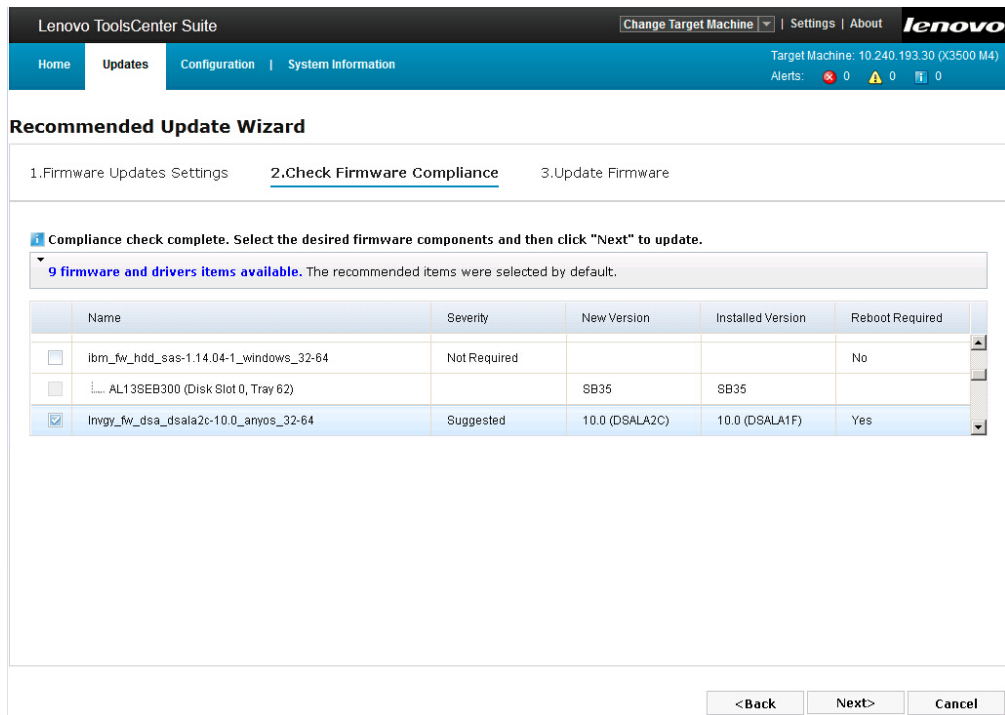
Figure 82. Remote machine - Recommended Updates - Check Firmware Compliance results

The firmware updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version identifier
- Installed Version: current version identifier or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

4. Select one or more firmware components in the left column.

5. Click **Next** to proceed with the Update Firmware process by downloading the firmware updates from the Lenovo website and applying the downloaded firmware, or click **Cancel** to return to the Firmware Updates page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

- Click **OK** to quit the update wizard.
- Click **Cancel** to continue the update process.

Important: If you selected to install an earlier version of firmware, the following message is displayed:

```
There are risks associated when downgrading any firmware yourself.
Please confirm the versions.
```

If you want to continue installing the earlier version, select **I'm willing to take on the risks to downgrade the firmware component below.** Click **Continue Updates**.

When the update operation finishes, the table provides the status of the updates indicating whether an update was successful or failed. A timestamp provides the time the update operation finished.

If you selected the **Update any available firmware (target machine reboot needed)** option, the following message is displayed:

```
You need reboot IMM / OS to make IMM / uEFI to take effect.
```


Figure 83. Remote machine - Recommended Updates - Bare Metal Updates - Firmware update results

6. Optional: If an IMM is installed, click **Restart IMM**. When this operation is complete, the Firmware Updates primary page is displayed.
7. Optional: If a uEFI is installed, click **Restart OS**. When this operation is complete, the Firmware Updates primary page is displayed.
8. Click **Finish**.

Using the Recommended Updates in a local repository option for the remote machine

You can use the **Recommended Updates in a local repository** option to check the firmware levels of the remote machine and applies the IMM, uEFI, pDSA UXSP package previously downloaded and located in a local repository.

Before you begin

Start ToolsCenter Suite on the host computer and connect to a remote machine. See "Connecting to a remote machine" on page 87.

About this task

This procedure provides an example of using Recommended Updates from a local repository and includes the Bare Metal Update option.

Procedure

1. On the Firmware Updates page, in the Select the content for remote server updates section, click one of the following options:

   - **Update IBM firmware (including IMM, uEFI, pDSA, no reboot required)**
   - **Update any available firmware (target machine reboot needed)**

   Update any available firmware (target machine reboot needed) is the Bare Metal Update option that requires the target machine is rebooted. It also checks the target machine's firmware levels. If the target machine's IMM or pDSA version does not satisfy the bare metal update requirement, the following warning message is displayed:

   ```
   The target server's IMM and DSA version don't meet the selected feature
   requirement, please update the Lenovo firmware first.
   IMM: 1A0049W or higher version
   DSA: DSYTB7U or higher version
   ```

2. In the Select the update method section, click **Recommended Updates** and then click **Next**.

   If you selected the **Update any available firmware (target machine reboot needed)** option, and the target machine's firmware level satisfies the bare metal update requirement, the following message is displayed:

   ```
   The target system will reboot to enter a bare metal machine update environment,
   because you have chosen to update any available firmware. Compare the currently
   installed firmware to the following source:
   ```

3. Click **Import UXSP updates package** and on the next line enter the local directory of the updates package.

   If you enter an invalid local directory address, the following message is displayed:

   ```
   Cannot find the given local directory.
   Make sure the directory path is valid.
   ```
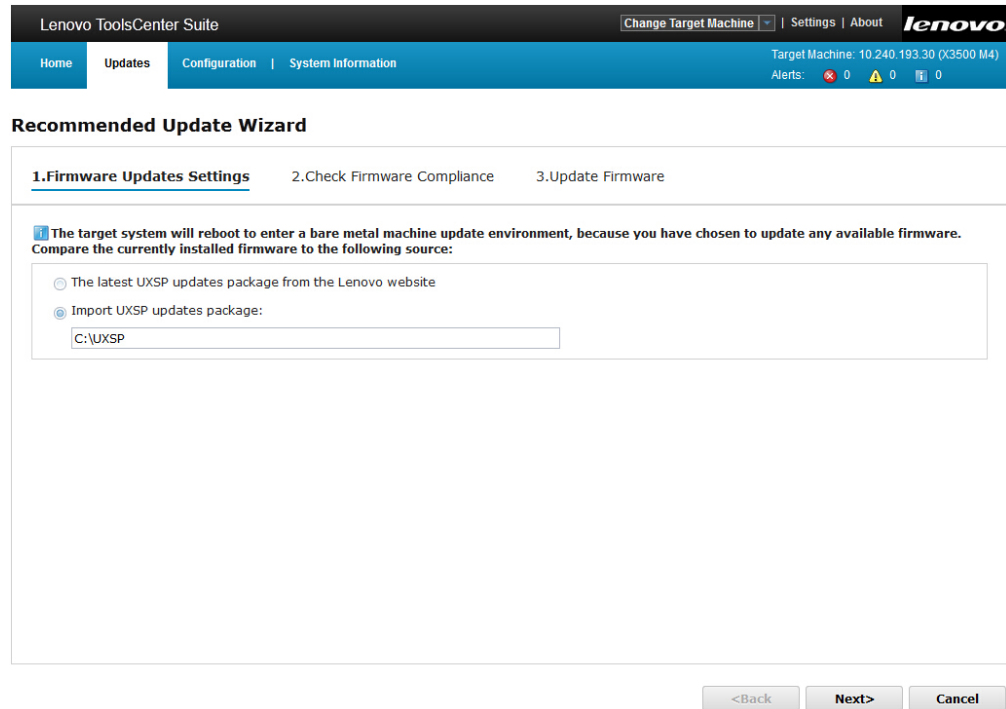
Figure 84. Remote machine - Recommended Updates - Import UXSP updates package

If the remote machine's IMM or pDSA version satisfies the bare metal update requirement, ToolsCenter Suite starts to boot to the bare metal environment. However, if the remote machine's IMM or pDSA does not support the bare metal update requirement, ToolsCenter Suite downloads the latest version of IMM or DSA and flashes the target machine's IMM and/or DSA.

4. Click **Next** to proceed with the Check Firmware Compliance process, or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

   • Click **OK** to quit the update wizard.

   • Click **Cancel** to continue the update process.

   While the compliance checking operation is working, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

   ```
   Please wait while ToolsCenter Suite checks your firmware levels.
   ```

   When the check firmware compliance operation finishes, the number of firmware items available is displayed above the firmware updates table.
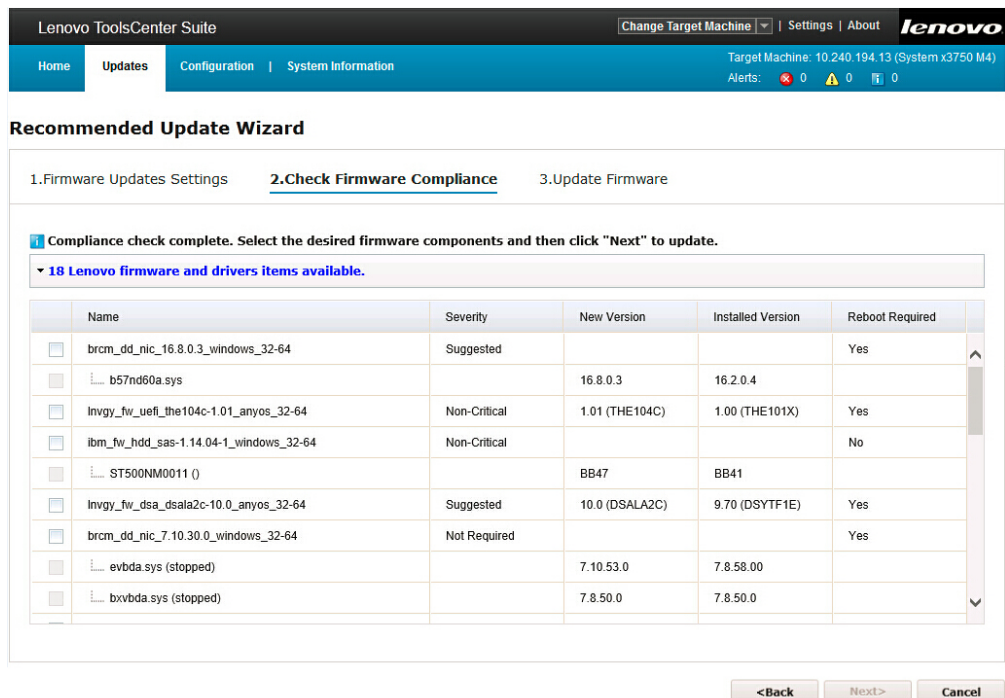
Figure 85. Remote machine - Recommended Updates - Check Firmware Compliance results

The firmware updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version identifier
- Installed Version: current version identifier or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

5. Select one or more firmware components in the left column.
6. Click **Next** to proceed with the update process.

   During the update operation, a progress icon and the following message is displayed:

   ```
   Updating is in progress.
   x of y items have been updated.
   Do not close your browser while the update is in progress.
   Do not take any power actions on target server.
   ```

   The status for each update is displayed as: Pending, Updating, Updated, or Failed.

   Important: If you selected to install an earlier version of firmware, the following message is displayed:

   ```
   There are risks associated when downgrading any firmware yourself.
   Please confirm the versions.
   ```

   If you want to continue installing the earlier version, select **I'm willing to take on the risks to downgrade the firmware component below.** Click **Continue Updates**.

When the update operation finishes, the table provides the status of the updates indicating whether the update was successful or failed. A timestamp provides the time the update operation finished.

If you selected the **Update any available firmware (target machine reboot needed)** option, the following message is displayed:

```
Note that system power cycle is required to make the updated firmware
take effect.
```

7. Click **Finish** to start the system reboot back to the original system.

Using the Individual Updates from the Lenovo website option for a remote machine

You can use the **Individual Updates from the Lenovo website** option to check the firmware and driver levels of the remote machine and applies the IMM, uEFI, pDSA firmware downloaded from the Lenovo website.

Before you begin

Start ToolsCenter Suite on the host computer and connect to a remote machine. See "Connecting to a remote machine" on page 87.

About this task

This procedure provides an example of using Individual Updates from the Lenovo website and includes the Bare Metal Update option.

Procedure

1. On the Firmware Updates page, in the Select the content for remote server updates section, click one of the following options:
   • **Update IBM firmware (including IMM, uEFI, pDSA, no reboot required)**
   • **Update any available firmware (target machine reboot needed)**

   Update any available firmware (target machine reboot needed) is the Bare Metal Update option that requires the target machine is rebooted. It also checks the target machine's firmware levels. If the target machine's IMM or pDSA version does not satisfy the bare metal update requirement, the following warning message is displayed:

   ```
   The target server's IMM and DSA version don't meet the selected feature
   requirement, please update the Lenovo firmware first.
   IMM: 1A0049W or higher version
   DSA: DSYTB7U or higher version
   ```

2. In the Select the update method section, click **Individual Updates** and then click **Next**.

   If you selected the **Update any available firmware (target machine reboot needed)**, option and the target machine's firmware level satisfies the bare metal update requirement, the following message is displayed.

   ```
   The target system will reboot to enter a bare metal machine update environment,
   because you have chosen to update any available firmware. Compare the currently
   installed firmware to the following source:
   ```

Figure 86. Remote machine - Individual updates from the Lenovo website - bare metal update reboot message

3. Click **Individual updates from the Lenovo website** and then click **Next**.

   The check firmware compliance process begins by acquiring the current machine's firmware levels from the Lenovo website. During the acquire operation, **Cancel** is enabled, and the following message is displayed:

   `Please wait while ToolsCenter Suite acquires your firmware levels.`

   After the acquire operation finishes, the check firmware compliance operation begins.

   However, if you selected to **Update any available firmware**, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

   `Rebooting the target server to enter a bare metal machine update environment.`

   If the remote machine's IMM or pDSA version satisfies the bare metal update requirement, ToolsCenter Suite starts to boot to the bare metal environment. However, if the remote machine's IMM or pDSA does not support the bare metal update requirement, ToolsCenter Suite downloads the latest version of IMM or DSA and flashes the remote machine's IMM and/or pDSA.

   While the compliance checking operation is working, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

   `Please wait while ToolsCenter Suite compares your current firmware`
   `  with the latest update package.`

   Note: If you are not connected to the Internet, the Configure Internet Connection dialog box opens. Check your configuration or try again, otherwise, click **OK** to continue or **Cancel** to exit this operation. For more information, see "Configuring your Internet Connection settings" on page 12.

When the check firmware compliance operation finishes, the number of firmware items available is displayed above the firmware updates table.
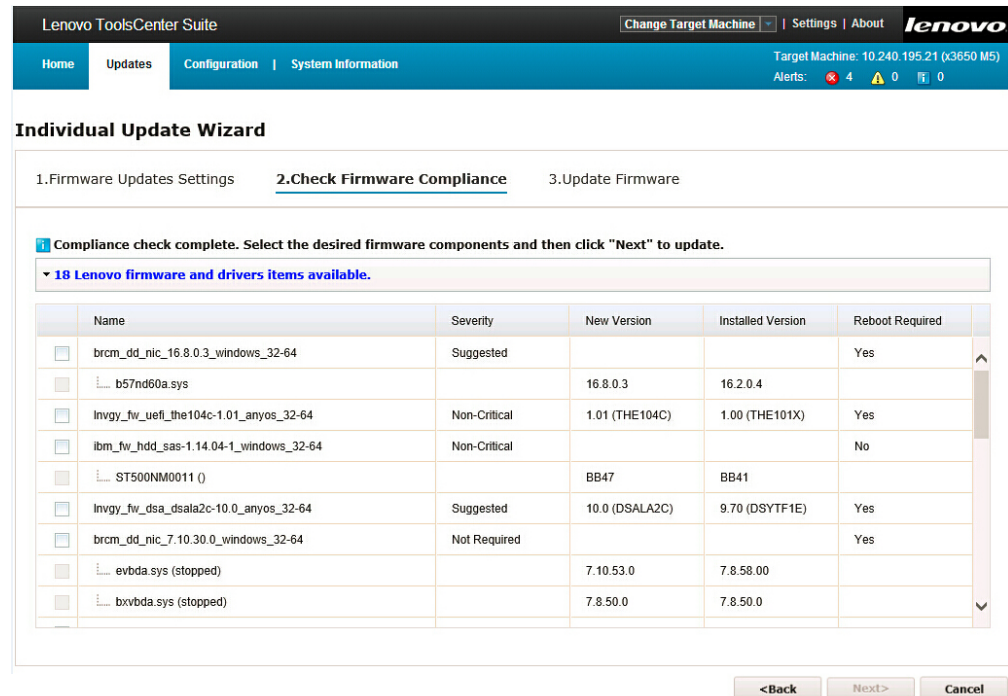
Figure 87. Remote machine - Individual Updates - Check Firmware Compliance results

The firmware updates table provides the following information for each update listed in the table:

- Name: update name
- Severity: Initial Release, Suggested, Critical, or Not Required
- New Version: new version identifier
- Installed Version: current version identifier or Undetected
- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

4. Select one or more firmware components in the left column.

5. Click **Next** to continue the Update Firmware process by downloading the firmware updates from the Lenovo website and applying the downloaded firmware, or click **Cancel** to return to the Update Firmware page. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

- Click **OK** to quit the update wizard.
- Click **Cancel** to continue the update process.

Important: If you selected to install an earlier version of firmware, the following message is displayed:

```
There are risks associated when downgrading any firmware yourself.
Please confirm the versions.
```

If you want to continue installing the earlier version, click **I'm willing to take on the risks to downgrade the firmware component below.** and then click **Continue Updates**.

During the download operation, the progress of the current downloading item indicates the total bytes and the downloaded bytes. A progress bar provides the overall progress of all download items. The updates listed in the table display the status as either: Not Started, Downloading, and Downloaded. Click **Stop** to stop the current downloading item.
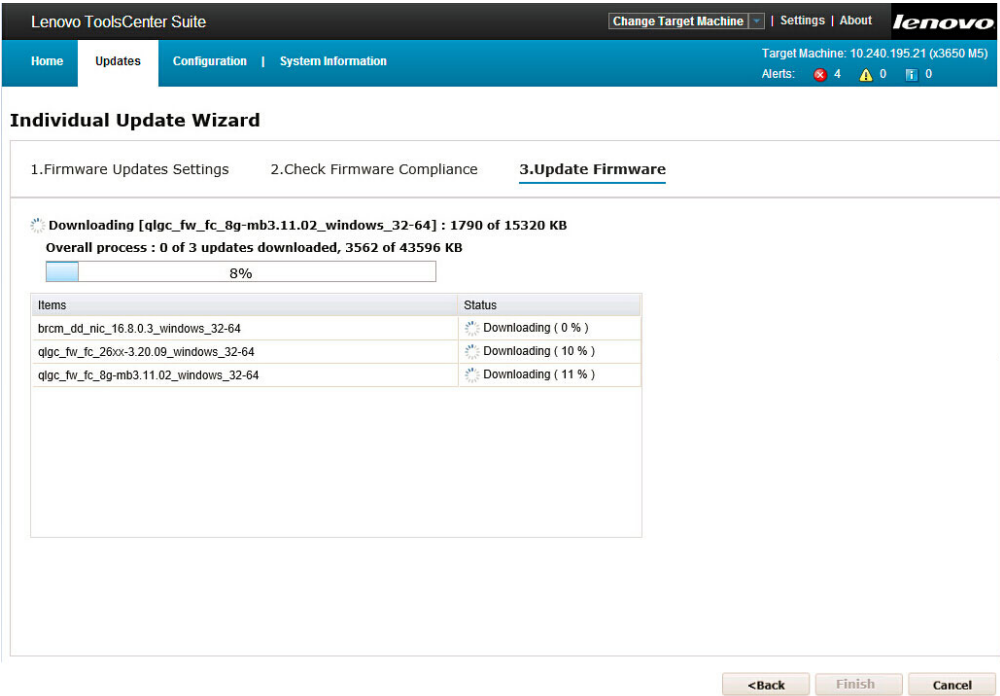
Figure 88. Individual updates - downloading bare metal updates from the Lenovo web site

When the download operation finishes, the update operation begins.

During the update operation, a progress icon and the following message is displayed:

```
Updating is in progress.
x of y items have been updated.
Do not close your browser while the update is in progress.
Do not take any power actions on target server.
```
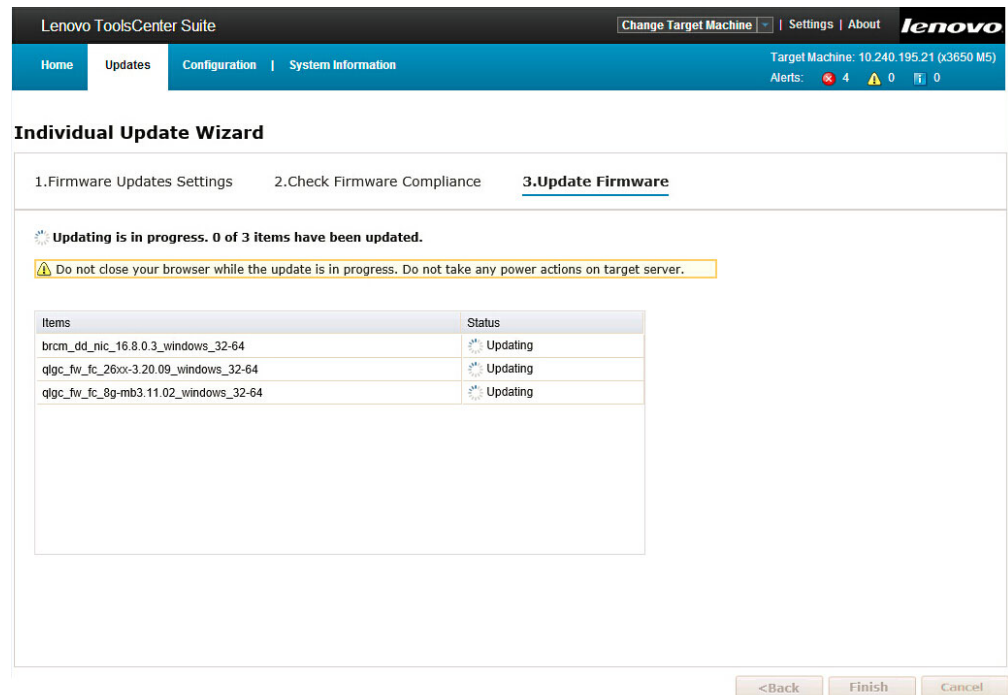
Figure 89. Individual updates - update firmware status

When the update operation finishes, the table provides the status of the updates indicating whether an update was successful or failed. A timestamp provides the time the update operation finished.
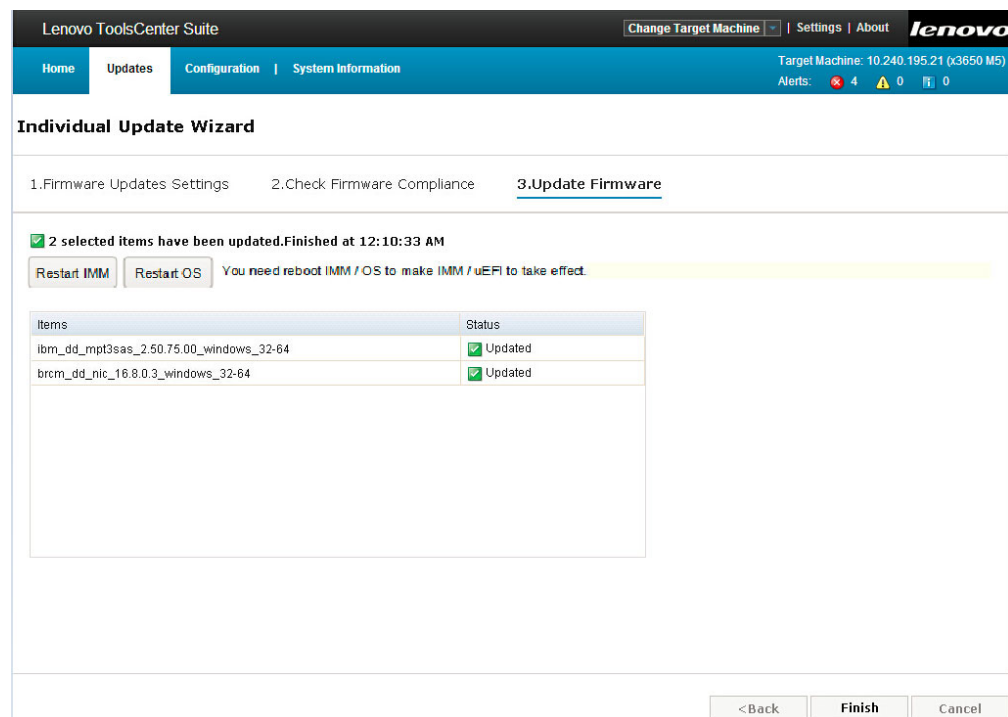
Figure 90. Remote machine - Individual Updates - Bare Metal Updates Firmware results

If you selected the **Update any available firmware (target machine reboot needed)** option, the following message is displayed:

```
You need reboot IMM / OS to make IMM / uEFI to take effect.
```

6. Optional: If an IMM is installed, click **Restart IMM**. When this operation is complete, the Firmware Updates primary page is displayed.

7. Optional: If a uEFI is installed, click **Restart OS**. When this operation is complete, the Firmware Updates primary page is displayed.

8. Click **Finish** to start the system reboot back to the original system.

Using the Individual Updates in a local repository option for a remote machine

You can use the **Individual Updates in a local repository** option to check the firmware of the remote machine and applies the IMM, uEFI, pDSA firmware previously downloaded and located in a local repository.

Before you begin

Start ToolsCenter Suite on the host computer and connect to a remote machine. See "Connecting to a remote machine" on page 87.

About this task

This procedure provides an example of using Individual Updates from a local repository and includes the Bare Metal Update option.

Procedure

1. On the Firmware Updates Settings page, in the Select the content for remote server updates section, click one of the following options:
   - **Update IBM firmware (including IMM, uEFI, pDSA, no reboot required)**
   - **Update any available firmware (target machine reboot needed)**

   Update any available firmware (target machine reboot needed) option is a Bare Metal Update and that requires the target machine is rebooted. It also checks the target machine's firmware levels. If the target machine's IMM or pDSA version does not satisfy the bare metal update requirement, the following warning message is displayed:

```
The target server's IMM and DSA  version don't meet the selected feature
requirement, please update the Lenovo firmware first.
IMM: 1A0049W or higher version
DSA: DSYTB7U or higher version
```

2. In the Select the update method section, click **Individual Updates** and then click **Next**.

   If you selected the **Update any available firmware (target machine reboot needed)** option, and the target machine's firmware level satisfies the bare metal update requirement, the following message is displayed:

```
The target system will reboot to enter a bare metal machine update environment,
because you have chosen to update any available firmware. Compare the currently
installed firmware to the following source:
```

3. Click **Import individual updates** and on the next line enter the local directory of the individual updates. If you enter an invalid local directory address, the following message is displayed:

```
Cannot find the given local directory.
Make sure the directory path is valid.
```
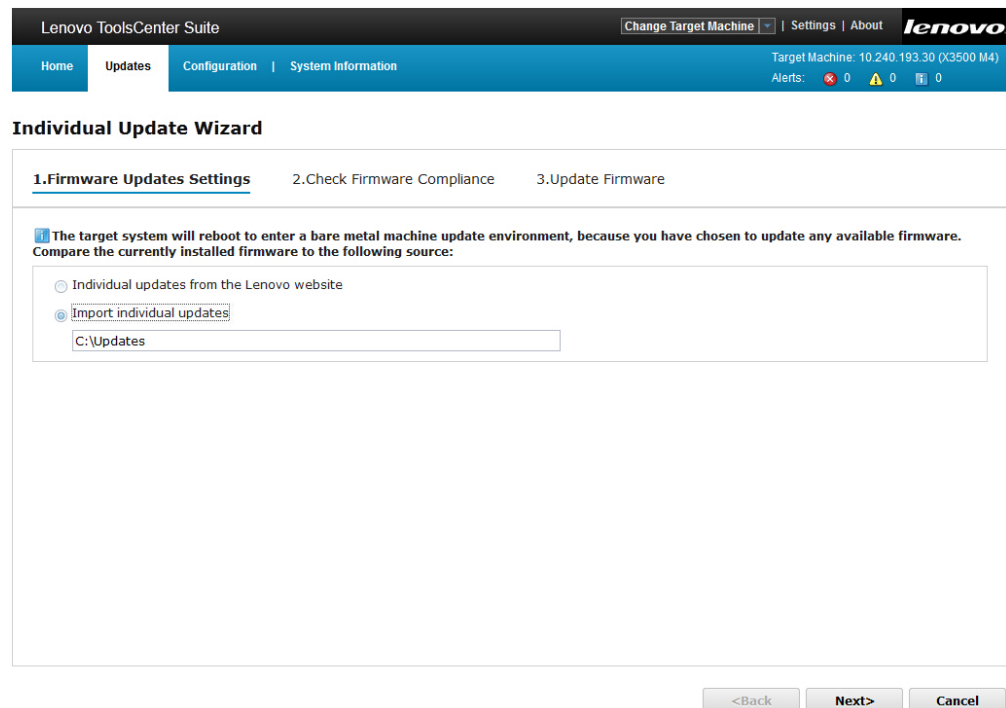
Figure 91. Remote machine - Individual Updates - Import individual updates

4. Click **Next** to proceed with the Check Firmware Compliance process, or **Cancel** to quit this operation. If **Cancel** is selected, the Confirm to Cancel Updates dialog box opens, asking if you are sure you want to cancel the whole update process? Select one of the follow options:

   • Click **OK** to quit the update wizard.

   • Click **Cancel** to continue the update process.

   While the compliance checking operation is working, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

   `Please wait while ToolsCenter Suite checks your firmware levels.`

   However, if you selected to **Update any available firmware**, the Check Firmware Compliance page is locked, **Cancel** is disabled, and the following message is displayed:

   `Rebooting the target server to enter a bare metal machine update environment.`

   If the remote machine's IMM or pDSA version satisfies the bare metal update requirement, ToolsCenter Suite starts to boot to the bare metal environment. However, if the remote machine's IMM or pDSA does not support the bare metal update requirement, ToolsCenter Suite downloads the latest version of IMM or DSA and flashes the remote machine's IMM and/or pDSA.

   When the check firmware compliance operation finishes, the number of firmware items available is displayed above the firmware updates table.

   • Name: update name

   • Severity: Initial Release, Suggested, Critical, or Not Required

   • New Version: new version identifier

   • Installed Version: current version identifier or Undetected

- Reboot Required: Yes - rebooting is necessary for the update or No - rebooting is not necessary for the update

5. Select one or more firmware components in the left column.

6. Click **Next** to proceed with the update process.

   During the update operation, a progress icon and the following message is displayed:

   ```
   Updating is in progress.
   x of y items have been updated.
   Do not close your browser while the update is in progress.
   Do not take any power actions on target server.
   ```

   The status for each update is displayed as either: Pending, Updating, Updated, or Failed.

   Important: If you selected to install an earlier version of firmware, the following message is displayed:

   ```
   There are risks associated when downgrading any firmware yourself.
   Please confirm the versions.
   ```

   If you want to continue installing the earlier version, click **I'm willing to take on the risks to downgrade the firmware component below** and click **Continue Updates**.

   When the update operation finishes, the table provides the status of the updates indicating whether the update was successful or failed. A timestamp provides the time the update operation finished.

   If you selected the **Update any available firmware (target machine reboot needed)** option, the following message is displayed:

   ```
   Note that system power cycle is required to make the updated firmware
   take effect.
   ```

7. Click **Finish** to start the system reboot back to the original system.

Using the Configuration function on a remote machine

The **Configuration** function can be used on a remote machine in the same way it is used on a host machine. On the remote machine, you can view and change one or multiple settings on your system and configure individual and frequently used settings, or perform a complete system configuration. You can also change the settings for System x IMM-based and a uEFI-based server. IMM replaces the Remote Supervisor Adapter and the baseboard management controller functions on IMM-based servers. uEFI replaces the basic input/output system (BIOS) and defines a standard interface among the operating system, platform firmware, and external devices.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **Configuration**. The Configuration Overview page opens.
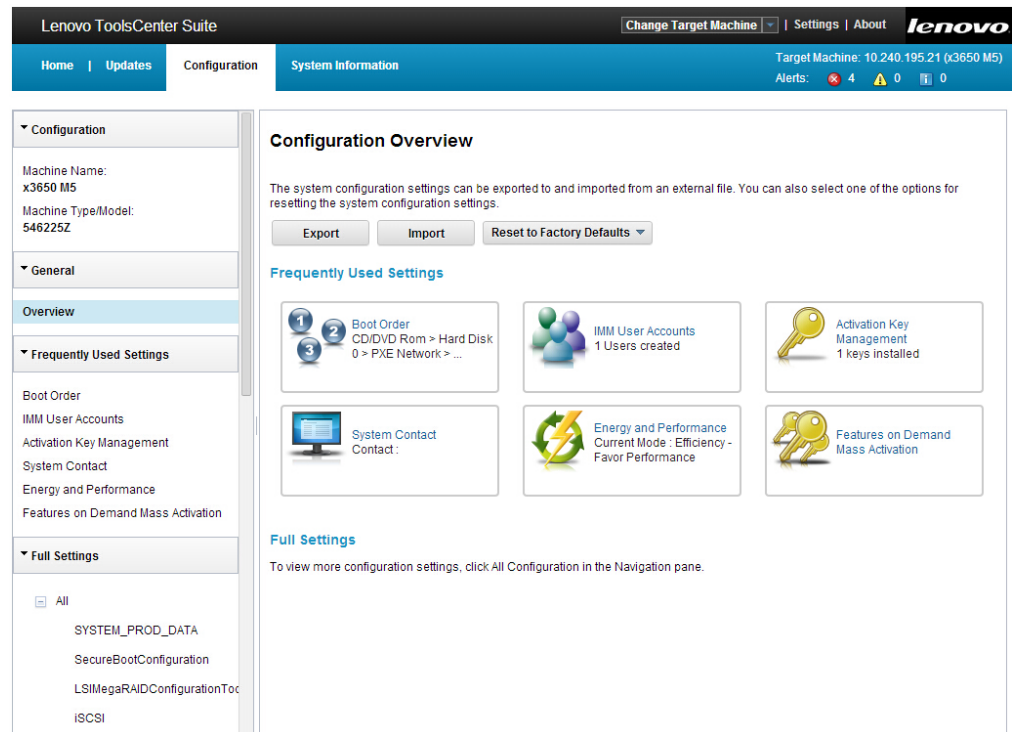
Figure 92. Remote machine - Configuration Overview

2. For detailed information about using the Configuration function, see Chapter 5, "Using the Configuration function," on page 37.

Using the System Information function on a remote machine

The **System Information** function can be used on a remote machine in the same way it is used on a host machine. On the remote machine, you can scan and view real-time status, check active status, light path status, and event logs for your system. You can collect full system information for analysis, service, and support. These files can be sent to Lenovo Support or to a customized FTP server.

Procedure

1. On the Home page or from the ToolsCenter Suite menu, click **System Information**.

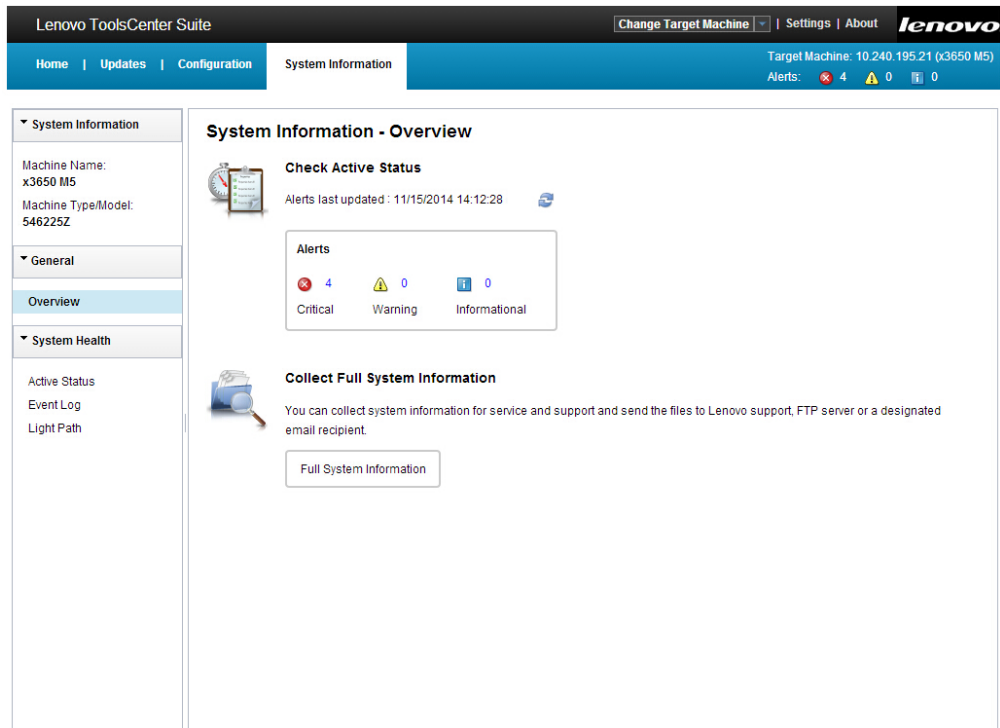   The System Information - Overview page opens.

Figure 93. Remote machine - System Information Overview

2. For detailed information about using the System Information function, seeChapter 6, "Using the System Information function," on page 71.

Chapter 8. Troubleshooting and support

Use this section to troubleshoot and resolve problems with Lenovo ToolsCenter Suite.

Known limitations

The current known limitations for ToolsCenter Suite 10.1 are:

The Bare Metal Update function does not work with the latest IMM firmware due to an unknown issue.

Activation Key Management:
If you are using Internet Explorer version 8, 9, or 10, when you click **Install from the Local File**, the file dialog box may not open.

Multi-Node System Support:
ToolsCenter Suite shows only the Primary Node information on the Home and Information pages. ToolsCenter Suite provides only the Configuration Function for the Primary Node.

FoD Mass Activation: (Root Cause: IMM CIM Class IBM_ActivationKey did not provide the FoD UID of the device on which the key installed.)
Note the following:
- In the 10.1 release, ToolsCenter Suite FoD Mass Activation is unable to support the scenario of more than one identical adapters being installed on a server, while a key is installed only on some of these adapters. In this situation, ToolsCenter Suite will not install the key for any adapters even it does not have this key installed.
- ToolsCenter Suite cannot display FOD UID when exporting keys for Multiple Endpoints in FoD Mass Activation.

OOB connect to Flex System
If you have already created an IPMI account with a username that is the same as the CIM, if it has a different password, ToolsCenter Suite will fail to create the IPMI account with the same credential as the CIM account.

In this case, to continue providing support for that remote Flex Server:
1. You need create another CIM account whose username is different from that of the IPMI account, and then input this account in TCS.
2. Either you or TCS (when user is aware of that) can change the IPMI account password to make it same as the CIM account password.

Unzipping the downloaded ToolsCenter Suite package to the ToolsCenter Suite working directory causes the system to crash
Unzipping the downloaded ToolsCenter Suite package to the ToolsCenter Suite working directory causes the system to crash because the ToolsCenter Suite working directory name is too long. Unzip the downloaded ToolsCenter Suite package under the system root directory.

Windows 64-bit operating systems
For all Windows 64-bit operating systems, you will get RAW data and be missing the logic device table information on Windows OS.

Full Settings option
In the Full Settings option, when changing the value of

Power.PowerPerformenceBias, there is no error message reported even though the setting change is not successful.

In Firefox, for Boot Order in Configuration
In Firefox, for Boot Order in Configuration, select the blank row of the list builder widget. The last row of the list builder widget will be selected and highlighted.

Workarounds

The following workarounds are applicable to ToolsCenter Suite 10.1:

When using Firefox on Red Hat Enterprise Linux 6 Server Update 6, the browser shows "Issuer certificate is invalid". (Error code: sec_error_ca_cert_invalid).
Workaround:
Set the property "*security.use_mozillapkix_verification*" to true on the about:config page.

Custom mode is not currently supported for Energy and Performance of Frequently Used Settings of Configuration.
Workaround:
Use Full Settings to change these values.

When using IE on some Windows operating systems, the progress icon may not rotate
Workarounds:
For Windows 2008, under **Windows Server Manager** > **Configure IE ESC**, turn off the **Internet Explore Enhanced Security Configuration** for the current user.

When using IE on some Windows operating systems, there is no activation key install progress page when install activation key from Local file.
Workarounds:
- For Windows 2012, under **Server Manager** > **Local Server**, turn off the IE Enhanced Security Configuration.
- For Windows 2008, under **Windows Server Manager** > **Configure IE ESC**, turn off the Internet Explore Enhanced Security Configuration for the current user.

Warnings

The following warnings are applicable to ToolsCenter Suite 10.1:
- The Bare Metal Update function is currently incompatible with IBM brand systems.
- FoD functions, including FoD configuration and FoD mass activation, only work on IMMv2.
- OOB and BMU updates only work on an IMMv2 system.
- For Red Hat and SUSE Linux, to run ToolsCenter Suite you need to run the "**/usr/sbin/setenforce 0**"command to close SELINUX.
- In Internet Explorer v10 (IE10), the password entry field now has an Eye icon. The Eye icon allows you to read the password info. This is a new function of IE 10.

- We do not recommend that you use browser actions such as back, forward, refresh in a browser window. ToolsCenter Suite does not fully support back, forward, and refresh. Under some circumstances, using these browser functions can cause unexpected results.
- System Information and Updates use the proxy configured in the Setting menu item and not the proxy configured in the browser configuration.
- `SYSTEM_PROD_DATA.SysInfoProdName` in the Full Settings option of the Configuration function is not editable, to ensure the server behaves correctly.

Getting help and technical assistance

Use this information to locate technical assistance for your System x, BladeCenter, Flex System tools.

About this task

If you need help, service, or technical assistance or just want more information about products, you will find a wide variety of sources available to assist you. This section contains information about where to go for additional information about products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Review and use this information before you call Service and Support to report a problem.

About this task

Complete these steps to try and resolve the problem yourself:
- Ensure that you have the latest version of the tool installed.
- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to the IBM Support Portal at http://www-947.ibm.com/support/entry/portal to check for technical information, hints, tips, and new device drivers.
- Use an IBM discussion forum to ask questions.

You can solve many problems without assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your product. The documentation that comes with your systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your system, preinstalled software, or an optional device is available in the documentation that comes with the product. Product documentation can include: information centers, online documents, printed documents, readme files, and help files.

About this task

The troubleshooting information in your system documentation has instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might indicate that you need additional or updated device drivers or other software.

IBM Support Portal has the latest technical information, device drivers, and updates.

The IBM Publications Center has additional documentation.

Getting help from the World Wide Web

You can get the latest information for supported systems, optional devices, services, and support from this list of website links.
- System x support and services at http://www-03.ibm.com/systems/x/support/
- BladeCenter Support and services at http://www-03.ibm.com/systems/bladecenter/support/
- IBM Workstations at http://www-03.ibm.com/systems/intellistation/
- IBM Flex System Overview at http://www-03.ibm.com/systems/pureflex/flex-converged-infrastructure.html

Software service and support

You can get assistance for your System x and BladeCenter tools by contacting Service and Support.
- The Support Line provides fee-based telephone assistance with usage, configuration, and software problems for System x servers, BladeCenter products, IntelliStation® workstations, and other components. For information about which products are supported by the Support Line in your country or region, see the IBM Supported product list website at http://www-03.ibm.com/systems/x/support/.
- In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).
- For a directory of worldwide IBM support telephone numbers, see the IBM Directory of worldwide contacts website at http://www.ibm.com/planetwide/.
- For IBM IT services, see the IT Services website at http://www-935.ibm.com/services/us/en/it-services/gts-it-service-home-page-1.html.

Hardware service and support

You can get assistance with ordering new equipment or requesting service support. Hardware service and support is available from Service and Support or from your Lenovo reseller, if your reseller is an authorized Lenovo warranty service provider.
-
- In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. For the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).
- In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m. For a directory of worldwide IBM support telephone numbers, see the IBM Directory of worldwide contacts website at http://www.ibm.com/planetwide/.

Appendix. Accessibility features for Lenovo ToolsCenter Suite

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

Lenovo and accessibility

See the Lenovo Accessibility website at http://www.lenovo.com/lenovo/us/en/ accessibility.html for more information about the commitment that Lenovo has to accessibility.

Accessibility

The following list includes the major accessibility features in ToolsCenter Suite:
• Can be operated using only the keyboard
• Communicates all information independent of color
• Supports the attachment of alternate output devices
• Provides online documentation in an accessible format

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

The command line interface (CLI) is controlled by the keyboard.

You can use the following keyboard shortcuts from the graphical user interface:

Shortcut (Linux)	Shortcut (Windows)	Action
Alt+C	Alt+C	Close the graphical user interface.
Alt+N	Alt+N	Go to the next page.
Alt+P	Alt+P	Go to the previous page.
Tab	Tab	Go to the next control.
Shift+Tab	Shift+Tab	Move to the previous control.
Left arrow	Left arrow	Move back one character.
Right arrow	Right arrow	Move forward one character.
Backspace	Backspace	Delete the character to the left of the cursor.
Delete	Delete	Delete the character under the cursor.
Up arrow	Up arrow	Move focus and selection upwards through the radio buttons.
Down arrow	Down arrow	Move focus and selection downwards through the radio buttons.
Space	Space	Select or clear an option.

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.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, and NeXtScale System are trademarks of Lenovo in the United States, other countries, or both.

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.

Other company, product, or service names may be trademarks or service marks of others.

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 1 024 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 can 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 is 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®