lenovo

Advanced Settings Utility, v10.1 User's Guide

Version 10.1

lenovo

Advanced Settings Utility, v10.1 User's Guide

Version 10.1

Note
Before using this information and the product it supports, read the information in "Notices" on page 147.

Edition notice

This edition applies to version 10.1 of Lenovo Advanced Settings Utility and to all subsequent releases and modifications until otherwise indicated in new editions.

Twenty-sixth Edition (April 2015)

Contents

Tables

Chapter 1. Using the Advanced Settings Utility

Use the Lenovo Advanced Settings Utility (ASU) to modify firmware settings from the command line on multiple operating-system platforms.

You can use the ASU to modify selected:

- Basic input and output system (BIOS) CMOS settings without restarting the system to access settings through the **F1** function
- Baseboard management controller (BMC) setup settings
- Remote Supervisor Adapter and Remote Supervisor Adapter II setup settings
- Settings in the integrated management module IMM-based servers for the IMM firmware and Lenovo System x server firmware. The IMM replaces the Remote Supervisor Adapter and baseboard management controller functions on IMM-based servers. Lenovo System x server firmware is the Lenovo implementation of Unified Extensible Firmware Interface (uEFI). The uEFI replaces the BIOS and defines a standard interface among the operating system platform firmware, and external devices.
- VPD settings on IMM-based servers
- iSCSI boot settings. To modify iSCSI settings with the ASU, you must first manually configure the values using the server Setup utility settings on IMM-based servers. For more information, see "Configuring iSCSI" on page 85.
- Connect remotely to set the listed firmware types settings on IMM-based servers. Remote connection support requires accessing the IMM external port over a LAN.

The ASU supports scripting environments because it is a command-line utility. It also offers easier scripting through its batch-processing mode.

For a list of the ASU commands and their descriptions, see Chapter 3, "Using the commands," on page 95.

Limitations

For IMM-based servers, consider the limitations in this topic.

For some settings to take effect, you might have to restart the IMM. You might also need to restart the IMM for the values that are set through ASU to be displayed in the IMM web interface.

For IMM-based servers, ASU supports the commands to generate, import, and export security certificates. The IMM version must be at least yuoo78m or later so that ASU can manage security certificates.

Supported firmware

This topic lists the firmware types and settings that are supported by the Advanced Settings Utility.

Throughout this document, the term *Remote Supervisor Adapter II* refers to both the Lenovo Remote Supervisor Adapter II and the Lenovo Remote Supervisor Adapter II SlimLine, unless otherwise noted.

The ASU supports the following firmware types:

- BIOS firmware
- Remote Supervisor Adapter firmware
- Remote Supervisor Adapter II firmware
- Baseboard management controller firmware
- Lenovo System x server firmware
- IMM firmware
- uEFI firmware
- Original design manufacturer integrated baseboard management controller firmware
- Original design manufacturer Remote Supervisor Adapter firmware

Note: The PC-DOS version of the ASU supports BIOS settings only.

Supported settings

The following settings are supported for the firmware types previously listed:

- Banked CMOS at 70h/71h (NS317)
- CMOS at 70h/71h and 72h/73h (NS417)
- CMOS at 72h/73h (AMD 8111)
- CMOS through baseboard management controller
- Serial EEPROM settings
- The following Remote Supervisor Adapter and Remote Supervisor Adapter II settings:
  - 8-bit values
  - 16-bit values
  - IP address values (32 bits)
  - Strings
  - Keystroke sequences
  - Certificate
  - Port
- The following baseboard management controller commands:
  - 8-bit values
  - 8-bit value within a block
  - IP address values (32 bits)
  - MAC address values (48 bits)
  - Strings
- Single and multi-node systems

The ASU retrieves and modifies user settings from the supported firmware types through its command-line interface. The ASU does not update any of the firmware code.

Operating system support

The following operating systems (both 32-bit and 64-bit) support the ASU.

- Microsoft Windows 2008
- Microsoft Windows 2008 R2
- Microsoft Windows 2012
- Microsoft Windows 2012 R2

  Note: For the Windows operating system, you must have administrator privileges. For more information about using the ASU on the Windows operating system, see the readme file that is included in the ASU package.
- Microsoft WinPE 1.6
- Microsoft WinPE 2.0
- Microsoft WinPE 2.1
- Red Hat Linux version 6
- Red Hat Linux version 7
- SUSE Linux version 10
- SUSE Linux version 11
- SUSE Linux version 12
- VMware ESX Server 4.0
- VMware ESX Server 4.1
- VMware ESXi 4.0
- VMware ESXi 4.1
- VMware vSphere Hypervisor 5.0
- VMware vSphere Hypervisor 5.1
- VMware vSphere Hypervisor 5.5
- VMware vSphere Hypervisor 6.0

Note: For Linux distributions that do not install the compatibility libstdc++ library, the following message might be displayed:

```
 ./asu: error while loading shared libraries:
libstdc++-libc6.1-1.so.2: cannot open shared object file:
No such file or directory.
```

- You cannot use the ASU to configure:
  - Remote Supervisor Adapter II settings from Red Hat Enterprise Linux AS 2.1, because there is no Remote Supervisor Adapter II device driver for the Red Hat Enterprise Linux AS 2.1 operating system.
  - Remote Supervisor Adapter or Remote Supervisor Adapter II settings from PC-DOS, because there is no Remote Supervisor Adapter or Remote Supervisor Adapter II device driver for PC-DOS.
  - Baseboard management controller settings from PC-DOS, because there is no baseboard management controller device driver for PC-DOS.
- You can view or change settings on a local server only.
- The PC-DOS version of the ASU does not support:
  - A multi-node-capable server when it is configured as multi-node.
  - A server in which the BIOS settings are stored in the baseboard management controller (for example, an IBM System x3950 M2 server).
- You cannot unpack the Windows ASU packages on a server or workstation that is running a 64-bit version of WinPE. You can unpack the Windows ASU

packages on a server or workstation that is running any of the other Windows operating systems that support the ASU.

For the latest information about Lenovo servers, workstations, and the operating systems that are supported, see Compatibility for hardware, applications, and middleware.

WinPE support

Windows Preinstallation Environment (WinPE) requires some special considerations for the Advanced Settings Utility (ASU) to function correctly. These considerations are different for WinPE 1.6 or earlier and WinPE 2.0 (the version that is based on the Windows Vista operating system) or later.

WinPE 1.6 or earlier

ASU is not supported on WinPE 1.6 for IMM-based servers.

WinPE 1.6 or earlier (the WinPE versions that are based on Windows XP and Windows Server 2003) do not have temporary file storage, which affects how you extract the device driver from the ASU executable file.

WinPE 1.6 and earlier versions also cannot recognize new USB devices after startup, which affects the behavior of the Remote Supervisor Adapter II **Reset** and **Restart** commands.

Device driver extraction for read-only media

Windows operating-system support of the ASU requires that a helper device driver be loaded. This device driver is embedded in the ASU executable file and, under normal circumstances, is extracted automatically at run time to either a temporary directory or, if no *TEMP* environment variable is defined, the directory that contains the executable file, if it does not already exist. The device driver is then automatically loaded and used by the ASU.

In the case of WinPE, where no writeable temporary directory is defined, there must be an alternative way to load the device driver.

If the ASU is unable to extract the device driver to a temporary directory, it attempts to load the device driver from the directory where the executable file is located. If the device driver exists, it is loaded, and execution continues. If the ASU does not find the device driver and cannot extract it for loading, an error message is displayed, and execution is stopped.

If you are running the ASU from non-writeable media (such as a CD), the device driver must exist on the media. You can manually extract it from the ASU executable file (and then copy it onto the non-writeable media) by running the following command from writeable media that contains the ASU:

`ASU extractdriver` (32-bit Windows version)

`ASU64 extractdriver` (64-bit Windows version)

The device driver is extracted as `wflash.sys` into the directory that contains the executable file. From there, you can copy the device driver (together with the ASU executable file) to non-writeable media such as a bootable WinPE CD.

Remote Supervisor Adapter II reset and restart problem with WinPE

WinPE versions that are earlier than 2.0 recognize devices that are available only at startup and later. This causes a problem when you issue a **resetrsa** or **rebootrsa** command to the Remote Supervisor Adapter II using the ASU because it removes the Remote Supervisor Adapter II from the bus. This prevents further communication with the device before a subsequent server restart.

If the version of WinPE is earlier than 2.0, an information message is displayed indicating that the server must be restarted before you can run another ASU command for the Remote Supervisor Adapter II.

WinPE 2.0 or later

The standard WinPE 2.0 (based on the Windows Vista operating system) image is missing two packages that the ASU requires for operation: the WinPE-MDAC-Package and the WinPE-WMI-Package. To run the ASU, you must add these two packages. For instructions about adding WinPE packages to the image that you create, see the documentation that comes with the Windows Automated Installation Kit.

WinPE 2.0 has an integrated Microsoft IPMI device driver, and the ASU 2.3.0 or later has an embedded mapping layer that supports that driver. Therefore, no user-installed IPMI driver or mapping layer is required. For more information about the IPMI device-driver support in WinPE 2.0, see IPMI device driver support for Windows.

Windows Server 2008 support

The Microsoft Windows Server 2008 operating system supports ASU version 2.3.0 or later.

Windows Server 2008 has an integrated Microsoft IPMI device driver, and the ASU 2.3.0 or later version has an embedded mapping layer that supports that driver. Therefore, no user-installed IPMI driver or mapping layer is required. For more information about the IPMI device-driver support in Windows Server 2008, see “IPMI device driver support for Windows” on page 7.

Supported systems

The servers, blade servers, and computers supported by ASU are listed.

The ASU supports the following servers, blade servers, and computers:

- Lenovo Flex System x240 M4 Compute Node Type 7162, 2588
- Lenovo System x3850 X6 / x3950 X6 Type 6241
- Lenovo System x3750 M4 Type 8753
- Lenovo Flex System x280 X6/x480 X6/x880 X6 Compute Node Type 4258, 7196
- Lenovo System x3500 M5 Type 5464
- Lenovo System x3650 M5 Type 5462
- Lenovo System x3550 M5 Type 5463
- Lenovo NeXtScale nx360 M5 Type 5465
- Lenovo NeXtScale nx360 M5 DWC Type 5467
- Lenovo Flex System x240 M5 Compute Node Type 2591, 9532

- Lenovo Flex System x440 Compute Node Type 7167, 2590
- IBM eServer xSeries MXE 460 Type 8874
- IBM System x3100 Type 4348
- IBM System x3100 M4
- IBM System x3100 M5 Type 5457
- IBM System x3200 M2 Type 4367, 4368
- IBM System x3200 M3 Type 7327, 7328
- IBM System x3250 M2
- IBM System x3250 M3
- IBM System x3250 M4
- IBM System x3250 M5 Type 5458
- IBM System x3300 M4
- IBM System x3400 Type 7973, 7974
- IBM System x3400 Type 7975, 7976
- IBM System x3400 M2 Type 7836, 7837
- IBM System x3400 M3 Type 7378, 7379
- IBM System x3500 Type 7977
- IBM System x3550 Type 7978, 1913
- IBM System x3500 M2 Type 7839
- IBM System x3500 M3 Type 7380
- IBM System x3530 M4 Type 7160
- IBM System x3550 M2 Type 7946, 4198
- IBM System x3550 M3 Type 7944, 4254
- IBM System x3500 M4 Type 7383/*
- IBM System x3550 M4 Type 7914/*
- IBM System x3620 M3 Type 7376
- IBM System x3630 M3 Type 7377
- IBM System x3630 M4 Type 7158
- IBM System x3650 Type 7979, 1914
- IBM System x3650 M2 Type 7947, 4199
- IBM System x3650 M3 Type 7945, 4255, 5454
- IBM System x3650 M4 Type 7915/*
- IBM System x3650 M4 HD Type 5460
- IBM System x3650 M4 BD Type 5466
- IBM System x3690 X5 Type 7148, 7149
- IBM System x3690 X5 Type 7192, 7147
- IBM System x3750 M4 Type 8722, 8733
- IBM System x3750 M4 Type 8752, 8718
- IBM System x3755 M3 Type 7164
- IBM System x3850 M2 / x3950 M2 Type 7141, 7144
- IBM System x3850 M2 / x3950 M2 Type 7233, 7234
- IBM System x3850 X5 / x3950 X5 Type 7145, 7146
- IBM System x3850 X5 / x3950 X5 Type 7143, 7191
- IBM System x3850 X6 / x3950 X6 Type 3837, 3839
- IBM System x3950E Type 8874, 7364, 8879, 7367

- IBM System x iDataPlex dx320 Type 6388
- IBM System x iDataPlex dx360 M2 Type 7321, 6380, 7323
- IBM System x iDataPlex dx360 M3 Type 6391
- IBM System x iDataPlex Direct Water Cooled dx360 M4 server
- IBM BladeCenter® HS12 Type 8014, 8028, 1916
- IBM BladeCenter HS20 Type 1884, 8843
- IBM BladeCenter HS21 Type 8853, 1885
- IBM BladeCenter HS21 XM Type 7995, 1915
- IBM BladeCenter HS22 Type 7870, 1936, 7809, 1910
- IBM BladeCenter HS22V Type 7871, 1949
- IBM BladeCenter HS23 Type 7875, 1929
- IBM BladeCenter HS23E Type 8038, 8039
- IBM BladeCenter LS20 Type 8850
- IBM BladeCenter LS21/LS41 Type 7971, 7972
- IBM BladeCenter LS22/LS42 Type 7901, 7902
- IBM BladeCenter HX5 Type 7872, 1909
- IBM BladeCenter HX5 Type 7873, 1910
- IBM Flex System x440 Compute Node Type 7917
- IBM Flex System x220 Compute Node Type 7906,2585
- IBM Flex System x222 Compute Node Type 7916
- IBM Flex System x240 Compute Node Type 8737,7863,8956
- IBM Flex System x280 X6/x480 X6/x880 X6 Compute Node Type 4259, 7903
- IBM Smart Analytics System Type 7949
- IBM NeXtScale nx360 M4 Type 5455

IPMI device driver support for Windows

This section explains the Intelligent Platform Management Interface (IPMI) device driver support for Windows.

Microsoft Windows supports the Open Systems Adapter (OSA) and Microsoft Windows Installer (MSI)IPMI device drivers. If you are using Windows Server 2003 R2, Windows Server 2008, or Windows PE 2.0 or later, you do not have to install an external (OSA or MSI) IPMI device driver. Microsoft integrates the IPMI device driver with the operating system. The ASU 2.3.0 and later supports these operating systems. To support the integrated device driver, a new Lenovo mapping layer is required, which is embedded in the ASU 2.3.0 or later.

If you want to use the Microsoft IPMI device driver and you have previously installed the Lenovo mapping layer, you must remove the mapping layer. The mapping layer embedded within the ASU conflicts with the externally-installed mapping layer previously required to support the OSA and MSI IPMI device drivers.

The Microsoft IPMI device driver is automatically installed with Windows Server 2008 and Windows PE 2.0 or later. However, it is not installed by default with Microsoft Windows Server 2003 R2. For instructions about installing the Microsoft IPMI device driver on Microsoft Windows Server 2003 R2, see “Installing the Microsoft IPMI device driver” on page 8.

Installing the Microsoft IPMI device driver

The Microsoft IPMI device driver is not installed by default on Microsoft Windows Server 2003 R2.

Before you begin

The Microsoft Windows Server 2003 R2 installation disk is required for this procedure.

About this task

To install the Microsoft IPMI device driver on Windows Server 2003 R2, complete the following steps.

Procedure

1. Click **Start** > **Control Panel** > **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. From the component list, select **Management and Monitoring Tools**, and then click **Details**.
4. Select **Hardware Management**.
5. Click **Next**. The installation wizard opens and guides you through the installation.

What to do next

Verify that the installation was successful. For instructions, see "Verifying the installation."

Verifying the installation

This topic describes how to verify that the Microsoft IPMI device driver is installed correctly.

Procedure

1. Click **Start** > **Control Panel** > **System**.
2. Select the **Hardware** tab.
3. Click **Device Manager**.
4. Click **View** > **Show Hidden Devices**.
5. Expand **System devices**. If the Microsoft IPMI device driver is installed correctly, a device named Microsoft Generic IPMI Compliant Device is displayed under **System devices**. For a multi-node configuration, a device named Microsoft Generic IPMI Compliant Device is created for each node.

IPMI device driver support for Linux

To access baseboard management controller settings, use either the OSA or MSI device driver and its corresponding Lenovo IPMI mapping layer. You can also use the OpenIPMI device driver that comes in many Linux distributions.

Notes

1. Due to a timing issue, the ASU does not support the OpenIPMI device driver contained in Red Hat Enterprise Linux 3 Update 6 and Update 7. To use these versions of Linux, the OSA IPMI mapping layer is required.

2. For an IBM System x3950 M2 server (multi-node configuration), the OpenIPMI device driver is the only supported IPMI driver.

Obtaining the ASU and patch files

The ASU, patch files, and device drivers that you need are available from the Lenovo technical support web site. Patch files are not required for IMM-based servers.

The files you need to download from the Lenovo Advanced Settings Utility page at http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=LNVO-ASU include:

- ASU package. The package contains the ASU tool and the additional files that are required for IMM-based servers. The additional files for IMM-based servers are necessary for configuring and activating the IMM LAN over USB interface.
- For BIOS-based servers only, download the following:
  - BIOS patch file for the server, if required.
  - Remote Supervisor Adapter device drivers or Remote Supervisor Adapter II USB daemon (if you want to use the ASU to configure Remote Supervisor Adapter or Remote Supervisor Adapter II settings).
  - Baseboard management controller device drivers and, if required, mapping layer (if you want to use the ASU to configure baseboard management controller settings).

Downloading the Advanced Settings Utility

Use this topic to help you locate and download the required ASU files.

About this task

Changes are made periodically to the Lenovo web site. Procedures for locating firmware and documentation might vary slightly from what is described in this topic.

Procedure

1. To download the Lenovo Advanced Settings Utility, go to the Lenovo Support Portal or complete the following steps:
   a. In the navigation pane, click **Systems Management software**.
   b. Under Popular links, click **ToolsCenter**.
   c. Under Configuration, click **View ToolsCenter downloads**, then click **Advanced Settings Utility**.
2. For BIOS-based servers only, download the BIOS definition file:
   a. On the Support page for the server, select **Software and device drivers**.
   b. On the Software and device drivers page, click **BIOS**.
   c. Select **BIOS definition file for use with Lenovo Advanced Setting Utility**. The BIOS definition file must match the BIOS level that the server is running.
   d. Select the ASU BIOS definition `.exe` file.
   e. Follow the instructions that guide you through the download process.
3. For BIOS-based servers only, return to the software and device drivers page to install the device-driver software for the Remote Supervisor Adapter II and baseboard management controller.

4. If required, download the IPMI device driver by completing the following steps. The IPMI device driver is not required in Windows 2003 R2, Windows 2008, and Linux operating systems that support OpenIPMI. For more information, see “IPMI device driver support for Windows” on page 7 or “IPMI device driver support for Linux” on page 8.
   a. On the Software and device drivers page, click **OSA IPMI**, and then select the applicable device-driver file.
   b. Read the `.txt` file and follow the instructions that guide you through the download process.
5. After you have downloaded the OSA IPMI device driver file:
   a. Select the applicable mapping layer for OSA IPMI file.
   b. Read the `.txt` file, and follow the instructions that guide you through the download process.
6. (For BIOS-based servers only.) On the Software and device drivers page:
   a. Click **Remote Supervisor Adapter II**.
   b. Select the applicable RSA II daemon.
   c. Read the `.txt` file, and follow the instructions that guide you through the download process.

About ASU patch files

This topic explains how to use the ASU patch files, which contain the ASU configuration information. Patch files are not required for IMM-based servers.

Before you can perform ASU operations that are targeted to the selected device, you must provide configuration information to the ASUfor the baseboard management controller, BIOS, and Remote Supervisor Adapter II. This configuration information is contained in separate patches.

The patches for the baseboard management controller and Remote Supervisor Adapter II are included with the ASU. Depending on the server model and BIOS level, a BIOS code patch might be required. For the systems that do not require a BIOS patch file, the BIOS patch is embedded in the BIOS ROM. If the BIOS patch is required, you must download the BIOS patch (definition file) from the Lenovo web site and add it to the ASU (only if you are required to perform an ASU command by using the BIOS settings).

To determine whether the BIOS patch is already available for the ASU, enter the ASU **patchlist** command to display the current available patches. If the ASU determines that a BIOS patch file is embedded in the BIOS, it displays the BIOS patch files that are available.

The following example shows the ASU output that is generated when the **patchlist** command determines that no BIOS patch files are available:

```
Patch 1: <XX[00->99] (BMC)>
Patch 2: <XX[00->99] (RSA)>
```

The following example shows the ASU output that is generated when the **patchlist** command determines that a BIOS patch file is available:

```
Patch 1: <XX[00->99] (BMC)>
Patch 2: <XX[00->99] (RSA)>
Patch 3: <DO[14->14] (BIOS)>
```

If the BIOS patch is not listed, you must add the patch before you can change or view BIOS settings. You can add the patch from the ASU.

The following illustration shows how to add and remove patches in the ASU binary code. For each BIOS code and firmware type, the internal locations of the settings vary. A patch informs the ASU where the settings are located for a single BIOS code version.

If a BIOS patch is needed and is not listed when you use the **patchlist** command, download the selected BIOS definition file (patch file) from the Lenovo web site and add the patch by using the ASU.

When you run the ASU, it automatically scans the patches that are available and determines if the applicable patch exists for the setting that you want. If an applicable patch exists, the ASU applies the setting. If the patch does not exist, the ASU displays an error.

A patch that is added remains until you run the **patchremove** command on that patch.

Notes

1. You cannot remove the BIOS patches that are embedded in the BIOS ROM by running the **patchremove** command.
2. Only one patch is supported for any major version of BIOS. For example, if there are BIOS versions 19A and 19B, only one patch is supported for both.

Extracting the ASU files for Windows

This topic contains instructions for extracting the ASU files on a Windows operating system.

About this task

You must run the ASU commands from the directory in which the ASU files are located.

Procedure

From the directory that contains the downloaded ASU files, choose one of the following methods to extract the ASU files:

- In Windows, double-click *filename*.exe, where *filename* is the name for the Advanced Settings Utility file for Windows that you downloaded.

  The files are automatically extracted to the same directory.
- At a command prompt, type *filename*.exe, where *filename* is the name of the Advanced Settings Utility file for Windows that you downloaded.

What to do next

The ASU requires additional files for IMM-based servers, which are required to automatically configure and activate the LAN over USB interface. The ASU uses the LAN over USB interface as a connectivity option. For more information about connectivity options, see “Connectivity” on page 16.

Extracting the ASU files for Linux

This topic contains instructions for extracting the ASU files on a Linux operating system.

About this task

You must type the ASU commands from the directory in which the ASU files are located.

Procedure

1. Open an xterm or other terminal window.
2. Go to the directory that contains the downloaded ASU files.
3. From a shell command prompt, type one of the following commands and press **Enter**:
   - If the `.tgz` file for ASU was downloaded:

     Enter `tar -zxvf filename.tgz` where *filename* is the name of the Advanced Settings Utility file for Linux that you downloaded.

     The files are extracted to the same directory.
   - If the `.rpm` file for ASU was downloaded:

     Enter `rpm -Uvh filename.rpm` where *filename* is the name of the Advanced Settings Utility file for Linux that you downloaded.

     The files are extracted to the `/opt/IBM/toolscenter/asu` directory.

What to do next

The ASU requires additional files for IMM-based servers, which are required to automatically configure and activate the LAN over USB interface. The ASU uses the LAN over USB interface as a connectivity option. For more information about connectivity options, see "Connectivity" on page 16.

About using ASU commands

The ASU uses either the **asu** or **asu64** command. This topic explains how to use the commands and provides examples.

- To see all of the ASU command modes and options, type the following command: **asu**

  Note: For a 64-bit operating system, type **asu64**.
- To change a value, type the following command:

  ```
  asu set setting value
  ```
- To show the current value, type the following command:

  ```
  asu show setting
  ```
- To show all possible values, type the following command:

  ```
  asu showvalues setting
  ```
- To add a patch, type the following command:

  ```
  asu patchadd filename.def
  ```

  where *filename* is the file name of the definition file.

Explanation of variables

- In the commands, *setting* is the name of a setting that you want to view or change, and *value* is the value that you are placing on the setting.

- If *value* contains spaces, enclose the value string in quotation marks (").
- If you are using a Linux operating system, you must either add a period (.) to the path environment variable or type `./` before each ASU command. For example, type `./asu` or for a 64-bit operating system, type `./asu64`.

Configuration of Remote Supervisor Adapter settings through theASU

Use the ASU to directly configure a Remote Supervisor Adapter or Remote Supervisor Adapter II.

Before you use the ASU, be sure to install the Remote Supervisor Adapter device drivers or Remote Supervisor Adapter II USB daemon. To install the device drivers, see the LenovoRemote Supervisor Adapter II Installation Instructions for Microsoft Windows users or Lenovo Remote Supervisor Adapter II Installation Instructions for Linuxusers.

Setting up communication with the ASU

Before you can use the ASU to modify Remote Supervisor Adapter or Remote Supervisor Adapter II settings, you must configure the operating-system setting so that the ASU can communicate correctly with the Remote Supervisor Adapter or Remote Supervisor Adapter II.

About this task

Use the Configuration/Setup Utility program that is part of the system BIOS code to configure the operating system setting.

Procedure

To configure the operating system setting by using the Configuration/Setup Utility program, complete the following steps:

1. Turn on the system.
2. When the prompt **Press F1 for Configuration/Setup** is displayed, press **F1**.
3. On the Configuration/Setup Utility main menu, select **Advanced Setup**, and then select **RSA Settings**.
4. Select **Other OS** for a Windows operating system, or select **Linux OS** as the operating-system USB selection.
5. Select **Save the Values and Reboot RSA**, and then press **Enter**. Wait until the message `RSA Settings saved` is displayed.
6. Exit the Configuration/Setup Utility program and complete the startup of the operating system.

Configuring the Ethernet settings on a Remote Supervisor Adapter II

The Remote Supervisor Adapter II must be configured for it to remotely access the adapter through the adapter Ethernet and serial connectors. You can use the ASU to configure the Remote Supervisor Adapter II Ethernet settings.

For detailed information about using the Remote Supervisor Adapter II web interface for remote access, see the *LenovoRemote Supervisor Adapter II User's Guide*.

Note: If you have an accessible, active, and configured Dynamic Host Configuration Protocol (DHCP) server on your network, the host name, IP address,

gateway address, and subnet mask are set automatically. You can use the Configuration/Setup Utility program that is part of the server BIOS to select DHCP server settings. For more information, see the Lenovo Remote Supervisor Adapter II Installation Instructions for Microsoft Windows Users or Lenovo Remote Supervisor Adapter II Installation Instructions for Linux Users.

You can also configure the DHCP setting by using the ASU. To use the ASU, continue with the following procedure.

If you have an enabled DHCP server and you want to configure the serial connector, see "Configuring a serial connection on Remote Supervisor Adapter."

Configuring Ethernet settings without a DHCP server

If you do not have a DHCP server on your network, use this topic to help you configure the Ethernet settings.

About this task

If you are using Linux, be sure to type `./` before the **asu** command.

Procedure

1. If you have not already done so, extract the ASU files. For more information, see "Extracting the ASU files for Windows" on page 11 or "Extracting the ASU files for Linux" on page 12.
2. At a command prompt, change to the directory that contains the ASU files.
3. Extract the ASU files. For more information, see "Extracting the ASU files for Windows" on page 11 or "Extracting the ASU files for Linux" on page 12. Note: This step is not required if you are using ASU version 2.0 or later.
4. To view a list of all settings and their assigned values, type the command `asu show all` and press **Enter**.
5. From the following list, select the items that you want to set.

Option	Description
To set or enable the following:	Run this command and press **Enter**
network interface on Remote Supervisor Adapter II	asu set RSA_Network1 Enabled
IP address	asu set RSA_HostIPAddress1 192.169.70.140
subnet mask	asu set RSA_HostIPSubnet1 255.255.255.0
gateway IP address	asu set RSA_GatewayIPAddress1 192.168.70.1
DHCP	asu set RSA_DHCP1 Enabled
data-transfer rate	asu set RSA_LANDataRate1 "10M Ethernet"
duplex mode	asu set RSA_Duplex1 Full

6. Restart the system by entering `asu rebootrsa` and pressing **Enter**.

Configuring a serial connection on Remote Supervisor Adapter

Use the ASU to configure the Remote Supervisor Adapter II serial connection.

About this task

The serial connector connects to a modem for dial-out support only. To configure the Remote Supervisor Adapter II serial connection for access to a modem, complete the following steps.

Note: If you are using a Linux operating system, be sure to type `./` before the **asu** command.

Procedure

1. If you have not already done so, extract the ASU files. For more information, see either"Extracting the ASU files for Windows" on page 11 or "Extracting the ASU files for Linux" on page 12.
2. At the command prompt, change to the directory that contains the ASU files.
3. To view a list of all of the settings and assigned values, enter the `asu show all` command, and press **Enter**.
4. From the following list, select the items that you want to set.

Option	Description
To set	Use the following command and press **Enter**
modem baud rate	`asu set RSA_ModemBaudRate1 value` where *value* is a number from 2400 through 57600 in increments of 2400 (for example, 2400, 4800, 7200, 9600, and so on). The default is 57600. **Note:** Make sure that the baud rate matches the baud rate of the device that you are connecting to the serial connector on the Remote Supervisor Adapter II.
modem parity	`asu set RSA_ModemParity1 value` where *value* is None, Odd, Even, Mark, or Space. The default is None.
modem stop bits	`asu set RSA_ModemStopBits1 value` where *value* is either 1 or 2. The default is 1.

5. Restart the system by typing `asu rebootrsa` and pressing **Enter**.

Configuring IMM-based servers using the ASU

Use the Advanced Settings Utility to configure settings on IMM-based servers.

The most current version of the ASU uses the same set of commands and syntax used by previous versions of the ASU tool. Some commands are enhanced to manage and display groups of settings. New classes are used as filters if you display the supported settings by using the **show** command.

ASU can support certificate management of IMM-based servers. To use this function, the IMM firmware level must be yuoo71a or later.

For IMM-based servers, after you use the ASU to change settings, you must reset the IMM before you flash new firmware. If you do not reset the IMM, the changes you made to the settings might be lost. To reset the IMM, run the **asu rebootimm** command.

The following sections describe the functions that are available to support IMM-based servers with the ASU.

Connectivity

For IMM-based servers, all firmware settings are configured through the IMM.

The ASU can connect to the IMM locally (in-band) through the KCS interface or through the LAN over USB interface. The ASU can also connect remotely over the LAN.

The IMM comes with a LAN over USB interface that can be configured and activated on the running operating system. After you install and configure the corresponding information file, the ASU can be connected to the IMM. The local LAN over USB connection requires authentication. A new set of connectivity parameters are required when the ASU is connected over the LAN.

If the LAN over USB interface was disabled before an ASU command was run, ASU configures and activates it for the ASU connection. After running the command, ASU disables the interface. If the interface was enabled before, it remains enabled without changes so that ASU can keep the LAN over USB interface the same status as before and after the ASU command.

The local connection over the KCS interface does not require authentication and follows the online connecting model and command structure of BIOS-based servers, where no connectivity parameters are required. If you do not specify connectivity parameters, the ASU attempts to connect to the IMM by using the default LAN settings on the LAN over USB interface. If the ASU is unable to connect to the IMM over the LAN, it automatically connects over the KCS interface, provided that the correct IPMI device drivers or mapping layers are installed. For more information about the KCS interface, see the Intelligent Platform Management Interface Specification at: http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-specifications.html

asu show

You can request that the ASU connect locally, exclusively using the KCS interface, which avoids the automated connection over the LAN over USB interface (and the fallback to the KCS interface). If you use the `--kcs` option, the ASU communicates through the KCS interface only.

In the following example, the ASU attempts to connect through the KCS interface only, without the need for authentication parameters.

asu show --kcs

You can also request that the ASU connect locally, exclusively using the LAN over USB interface, by specifying the `--host` connectivity option. The ASU does not attempt to fall back to use the KCS interface when this option is specified.

In the following example, the ASU attempts to connect through the LAN over USB interface only by using the default user ID and password account.

asu show

When the ASU runs any command on an IMM-based server, it attempts to connect and automatically configure the LAN over USB interface if it detects that this interface is not configured. The ASU provides a level of automatic and default settings. You can specify to skip the automatic configuration process if you have manually configured the IMM LAN over USB interface by using different settings than those used by the ASU application default settings.

Use the `--noimmlancfg` option to skip the automatic configuration process if you have manually configured the interface. For example, to show the IMM list of settings and avoid using the automatic configuration process when you attempt to connect through the LAN over USB interface, type the following command:

```
asu show IMM --noimmlancfg
```

If the ASU is connecting remotely to the IMM over the LAN, there is no requirement for the remote operating system of the targeted IMM to be online. The ASU can connect to the IMM remotely when the server is connected to power or is using standby power. Both IPv4 and IPv6 are supported remotely by the ASU. Before running the ASU, be sure that the IMM net configuration is correct.

To connect remotely, the `--host`, `--user` and `--password` options are all required. The following example indicates the minimum required parameter when the ASU connects remotely through the LAN to the IMM external port.

```
asu show --host target_IMM_external_IP_address --user target_IMM_User_ID
--password target_IMM_password
```

Enabling and disabling the LAN over USB interface

You can enable or disable the IMM LAN over USB interface by using the `IMM.LanOverUsb` setting in the ASU.

When you enable or disable the `IMM.LanOverUsb` setting, you must use the KCS interface because the LAN over USB interface is removed during the **set** command process. This prevents the ASU **set** command from terminating correctly. You must use the `--kcs` connectivity option to make sure that the **asu** command is completed correctly and relates status.

```
asu set IMM.LanOverUsb Disabled --kcs
```

To connect remotely to an IMM from a Windows client to display all available settings, type the following command; the IMM external IP address is 9.5.51.37.

```
asu show all --host 9.5.51.37 --user testid --password test
```

To connect locally to an IMM from a Windows operating system to display all available settings, type the following command; the ASU connects to the IMM through the LAN over USB interface.

```
asu show all --user testid --password test
```

To connect locally to an IMM from a Windows operating system to display all available settings, type the following command. The ASU attempts to connect over the LAN over USB interface by using the default IMM authentication credentials. If

the default settings do not match, the ASU attempts to use the KCS interface, provided that the IPMI device drivers and mapping layers are installed.

```
asu show all
```

To connect locally, forcing the ASU to use the KCS interface and avoid using the LAN over USB interface, type the following command:

```
asu show --kcs
```

For more information about connectivity parameters and usage, see "Connectivity" on page 16.

LAN over USB network configuration

You can configure the network interface of IMM LAN over USB by using the IMM.LanOverUsbIMMIP, IMM.LanOverUsbIMMNetmask, and IMM.LanOverUsbHostIP settings on IMMV2 with a build ID of 1AOO45F or later. IMMV1 is not supported.

The IMM.LanOverUsbIMMIP setting is used to set the in-band LAN over USB network IP address of the IMM. The IMM.LanOverUsbIMMNetmask setting is used to set the in-band LAN over USB network Netmask of the IMM. The IMM.LanOverUsbHostIP setting is not used to set the host IP address but rather is used to notify IMM that the host Lan-Over-Usb IP address has changed. So IMM watchdog can still work if the host side did not use the default IP address (169.254.95.120).

Before you set those three settings, you need to manually configure the host IP of the LAN over USB interface in your local operating system. If you are using a Linux operating system and LAN over USB is enabled, type `ifconfig` on the command line interface, and you will see a network interface named `usb0`.

The information for `usb0` may be displayed as follows:

```
usb0Link     encap:Ethernet  HWaddr E6:1F:13:95:1D:33
             inet addr:169.254.95.120  Bcast:169.254.95.255  Mask:255.255.255.0
             inet6 addr: fe80::e41f:13ff:fe95:1d33/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:755105 errors:0 dropped:0 overruns:0 frame:0
             TX packets:766670 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:63296929 (60.3 Mb)  TX bytes:74998936 (71.5 Mb)
```

The default host IP address of LAN over USB is 169.254.95.120. You can configure the host IP address by using network configuration commands on Linux. Then you can use the three commands below to configure the network interface for IMM LAN over USB:

- `asu set IMM.LanOverUsbIMMIP 169.254.95.110`
- `asu set IMM.LanOverUsbIMMNetmask 255.255.255.0`
- `asu set IMM.LanOverUsbHostIP 169.254.95.112`

The parameter for `IMM.LanOverUsbHostIP` should be the IP address of the LAN over USB interface (`usb0` in Linux) on the local operating system. You must set all three settings properly before the network configuration of LAN over USB takes effect.

Note: To avoid connection problems in multi-node server environments, do not configure the IMM LAN over USB IP into one subnetwork.

Settings syntax

All settings in IMM-based servers are configured through the IMM. The settings are classified into groups.

The following groups of settings or firmware settings are supported.

Note: The term "group" in this context refers to how the settings for a specific subsystem are organized.

- uEFI - uEFI (BIOS) settings
- BootOrder - Boot-order configuration in uEFI
- iSCSI - iSCSI-supported settings (Boot-over-iSCSI settings)
- SYSTEM_PROD_DATA - User-configurable vital product data (VPD) settings

In the setting syntax used to identify the corresponding group of settings, the setting name is preceded by the corresponding group name, as shown below:

```
group_name.setting_name
```

To set the external IP address in the IMM, type the following command:

```
asu set IMM.HostIPAddress 9.5.51.37
```

where *IMM.HostIPAddress* is the IMMsetting that is used to configure the IMM external IP address. The setting is part of the IMM group.

Some settings include an additional index, which is referred to in this document as an "instance." The index is used to identify and set different instances of the same setting when these are available.

To set the first instance of a number or login ID, type the following command:

```
asu set IMM.LoginId.1 testid
```

where *IMM.LoginId.1* is the IMM setting that is used to configure the first instance of a login account.

Instances of settings

This topic explains instances of settings on IMM-based servers.

The ASU extends the support of instances in several different ways. Commands have been created or modified to provide more information about instances and additional ways to create and delete them. Instances are denoted by adding a dot, followed by the instance number to the end of the setting name. For example, if the setting name is "IMM.LoginId," instance number 1 of the setting is "IMM.LoginId.1".

Note: There is an exception to the naming convention for single instances. Single instances do not have the dot followed by an instance number. The setting instead appears like a non-instance setting. Single instance settings are denoted in the output of the **showvalues** command by having a maximum number of instances of :"single." For example, the setting iSCSI.initiatorName is a “single instance.” The dot followed by an instance number is not used. If the single instance exists, the setting `iSCSI.initiatorName` is displayed in the **show** command output. If it does not exist, the setting is not displayed in the **show** command output.

Instance settings are defined to have a minimum and maximum number of allowed instances. To determine which settings can have instances and the minimum and maximum number of instances allowed, use the **showvalues** command with the **--instances** parameter. The output of this command is detailed in the“Showvalues command” on page 137 section.

Creating and deleting instances

This topic explains how to create and delete instances by using the Advanced Settings Utility.

Use the **set** command to create an instance. If the instance does not already exist, and the instance number is between 1 and the maximum number of allowed instances, the instance is automatically created and set to the value specified in the **set** command.

Use the **delete** command to delete an instance. This command deletes the instance if deleting the instance does not cause the number of instances for the setting to go below the minimum number of allowed instances for the setting.

Note: There are restrictions for creating and deleting instances of settings that are part of a record. For more information about the restrictions, see “Record management.”

Record management

This topic explains how instances can be part of a record and how to manage instances in a record.

Settings that have instances can be part of a record. A record is a group of settings that have dependencies on each other. For example, a user ID and a password are dependent on each other. A user ID must have a password, and a password must have a user ID. Therefore, they are grouped in the same record.

Each record has a setting that is defined as the "record key." It represents the primary setting for the record.

Determining if a setting is part of a record

To determine if a setting is part of a record, use the **showvalues** command with the **--instances** parameter. Settings that are part of a record are marked with the text "recordKey" (if the setting is the record key) or "recordKey=*key_name*" (if the setting is part of a record but is not the key), where *key_name* is the name of the setting that is the record key. See the “Showvalues command” on page 137 section for examples of the **showvalues** output for settings that are part of a record.

Creating an instance of a record

All settings in a record are created or deleted as a group. To create an instance of a record, you must first perform a "set" on the key setting of the record. This automatically causes an instance to be created and set to its default value for all other settings in the record. To see examples of how to create an instance of a setting, see the “Set command” on page 128 section.

Deleting an instance of a record

To delete an instance of a record, the delete command is performed on the "record key" setting. This automatically deletes all other instances for the settings in the

record. For examples of deleting an instance of a setting, see the “Delete command” on page 100 section.

Using the Remote Disk Command Line Interface

Use the Remote Disk Command Line Interface (RDCLI) to mount an image to a remote IMM-based server.

RDCLI is available in an ASU release package. Use it to mount an ISO, DVD, or CD to a remote IMM-based system so that it can be accessed like a local hardware device.

Considerations

Note the following points before using the RDCLI:

- To use the RDCLI mount image to connect to a remote IMM-based system, the system must be installed with the remote present key and remote present function enabled.
- The RDCLI does not work if there is a session started with the remote present function through the IMM web user interface.
- RDCLI is supported both in rack IMM-based and NGP servers. RDCLI does not support AMM blade servers.

Supported operating systems

The RDCLI supports the following operating systems:

- SUSE Linux version 9
- SUSE Linux Enterprise Server 10 (32 / 64 bit)
- SUSE Linux Enterprise Server 11 (32 / 64 bit)
- Red Hat Enterprise Linux version 3
- Red Hat Enterprise Linux version 4 (32 / 64 bit)
- Red Hat Enterprise Linux version 5 (32 / 64 bit)
- Red Hat Enterprise Linux version 6 with Xen added
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Small Business Server 2011
- Windows 2012
- Windows 2012 R2

Package

RDCLI contents include the following binary files:

`rdmount` -- Performs authentication and spawns new file server processes that allow access to the virtual disk. It can also query the existing file server processes.

`rdumount` -- Binary file to unmount an ISO, DVD, or CD from a remote IMM-based server

These two binary files are packaged under the `rdcli32` and `rdcli64` directories within ASU Linux distribution.

Supported command line parameters

RDCLI supports the following command line parameters:

-s <*address or hostname*> Address or hostname of the remote SP

-d <*path*> Image or local optical drive directory path

-l <*login*> Authorized login user to SP.

-p <*password*> Password of the authorized login user.

-w <*port*> Authentication port used to communicate to SP

Using the ASU to configure settings for VMware vSphere Hypervisor (ESXi)

This topic describes how to use the ASU to configure settings for VMware vSphere Hypervisor (ESXi) with Lenovo customization in IMM-based servers.

The VMware vSphere Hypervisor (ESXi) supports the ASU. Because the ESXi image has no console and individual tools cannot run directly on this operating system, theASU configures the ESXi image based on the CIM stack. The ASU only supports IMMv1 or IMM2 systems that have the CIM stack. Make sure that the CIM server is available on the operating system before running the **ASU** command.

ESXi with Lenovo customization must synchronize the schema from IMM either after the operating system starts or after the IMM firmware is updated. The update takes approximately 15 minutes. Do not run the ASU until the schema synchronization is finished.

Using the command-line interface

Enter the following command:

```
asu command <setting_name> <connection_options>
```

Supported commands

For the VMware vSphere Hypervisor (ESXi) operating system, ASU supports only three basic commands for configuration:

show gets the current setting value

set modifies the current setting value

showvalues presents the values that the setting supports

Note: The <*setting_name*> is the setting that refers to IMM, uEFI, and BootOrder. A group name such as IMM, uEFI, or all is not supported.

Supported settings

This topic describes the supported settings for VMware vSphere Hypervisor (ESXi) with Lenovo customization in IMM-based servers.

ASU supports three kinds of settings for VMware vSphere Hypervisor (ESXi): BootOrder settings, IMM settings, and uEFI settings.

BootOrder settings

BootOrder.BootOrder

BootOrder.WolBootOrder

IMM settings

IMM.ShutdownAndPowerOff

IMM.PowerOnServer

IMM.ShutdownAndRestart

IMM.LoginId.1

IMM.AuthorityLevel.1

IMM.Password.1

IMM.UserAccountManagementPriv.1

IMM.RemoteConsolePriv.1

IMM.RemoteConsoleDiskPriv.1

IMM.RemotePowerPriv.1

IMM.ClearEventLogPriv.1

IMM.BasicAdapterConfigPriv.1

IMM.AdapterConfigNetworkSecurityPriv.1

IMM.AdvancedAdapterConfigPriv.1

IMM.SNMPv3_AuthenticationProtocol.1

IMM.SNMPv3_PrivacyProtocol.1

IMM.SNMPv3_PrivacyPassword.1

IMM.SNMPv3_AccessType.1

IMM.SNMPv3_TrapHostname.1

IMM.User_Authentication_Method

IMM.LockoutPeriod

IMM.WebTimeout

IMM.AccountSecurity

IMM.LoginPassword

IMM.RemoteAlertRecipient_Status.1

IMM.RemoteAlertRecipient_Name.1

IMM.RemoteAlertRecipient_Email.1

IMM.RemoteAlertRecipient_IncludeEventLog.1

IMM.RetryLimit

IMM.EntriesDelay

IMM.RetryDelay

IMM.SerialRedirectionCLIMode1

IMM.SerialBaudRate

IMM.CIMOverHTTPPort

IMM.CIMOverHTTPSPort

IMM.HTTPPort

IMM.SSLPort

IMM.TelnetPort

IMM.SSHPort

IMM.SNMP_AgentPort

IMM.SNMP_TrapPort

IMM.SNMPTraps

IMM.Community_Name.1

IMM.SSL_Server_Enable

IMM.CIMXMLOverHTTPS_Enable

IMM.SSL_Client_Enable

IMM.SSH_Enable

The following settings are performed by the Chassis Management Module on Flex System, so they are not supported on Flex System.

IMM.User_Authentication_Method

IMM.LockoutPeriod

IMM.WebTimeout

IMM.AccountSecurity

IMM.LoginPassword

IMM.SSL_Server_Enable

IMM.CIMXMLOverHTTPS_Enable

IMM.SSL_Client_Enable

IMM.SSH_Enable

uEFI settings in an IMMv1 system

The uEFI settings that you can use for an IMMv1 system are listed here.

uEFI.TurboModeEnable

uEFI.ProcessorEistEnable

uEFI.ProcessorCcxEnable

uEFI.PackageCState

uEFI.ProcessorC1eEnable

uEFI.ProcessorHyperThreading

uEFI.ProcessorVmxEnable

uEFI.DdrSpeed

uEFI.MemoryChannelMode

uEFI.SpareErrorThreshold

uEFI.SocketInterleave

uEFI.PatrolScrub

uEFI.DemandScrub

uEFI.IdeMode

uEFI.VideoSelect

uEFI.RomOrder

uEFI.OnboardDeviceEnable.1

uEFI.LegacyRomExecution.1

uEFI.PCIeGenSelection.1

uEFI.SerialCOMPort1

uEFI.RemoteConsoleRedirection

uEFI.SerialPortSharing

uEFI.SerialPortAccessMode

uEFI.SPRedirection

uEFI.LegacyOptionRomPort

uEFI.Com1BaudRate

uEFI.Com1DataBits

uEFI.Com1Parity

uEFI.Com1StopBits

uEFI.Com1TextEmul

uEFI.Com1ActiveAfterBoot

uEFI.Com1FlowControl

uEFI.EnergyManager

uEFI.PerformanceStates

uEFI.WatchdogTimerUefi

uEFI.WatchdogTimerUefiValue

uEFI.RebootOnNMI

uEFI.ForceLegacyVideo

uEFI.Rehook19

uEFI.ThunkSupport

uEFI.EnableLegacyPxe

uEFI.Usb20_1

uEFI settings in an IMM2 system

This section provides information about the uEFI settings that you can use on an IMM2 system.

In the IMM2 system, ASU supports the uEFI group for VMware vSphere Hypervisor (ESXi) with Lenovo customization. To get the uEFIsetting list, use the following ASU command: `asu.exe showvalues uefi --host <OS_ip> --user root --password <OS_password> --vmware-esxi`

You can also get the list by using the command `asu show uefi <connection_options>` in a Windows or Linux operating system of your current IMM2 system. uEFI setting interdependencies are supported for VMware vSphere Hypervisor (ESXi) with Lenovo customization on ASU version 9.50, IMM version 1A0045V or later.

Notes

1. The settings previously listed are all supported through the ESXi CIM stack. However, some IMMv1 or IMM2 systems might not have all of these settings. Some settings might not be supported by different systems.
2. ASU ESXi support is limited:
   - Only three commands are supported. Other ASU commands like **showdefault**, **loaddefault**, and **showgroups** are not supported.
   - ASU only supports a uEFI group on IMM2-based systems; no other groups or subgroups are supported.
3. Some of the previously-listed settings have instance IDs, for example, IMM.LoginId.1, where 1 is a positive integer instance ID. Typically, the instance ID "1" is the default, and you can configure it.

Table 1. Connection options for VMware vSphere Hypervisor (ESXi) image

Parameter	Required	Description
--host <*OS ip*>	Yes	VMware vSphere Hypervisor (ESXi) image IP address. Both IPv4 and IPv6 are supported.
--user root	Yes	VMware vSphere Hypervisor (ESXi) image user. The root is needed here.
--password <*OS_password*>	Yes	Password for the root user.
--vmware-esxi *[http]*	**--vmware-esxi** is required, while *[http]* is optional	If *[http]* is not specified, ASU uses https to connect to the VMware vSphere Hypervisor (ESXi) image.
--port <*port*>	Optional	The connection port. The default port for https is 5989.

Command example

The following examples show how to view a setting by using the **asu show** command, configure a setting by using the **asu set** command, and list possible values by using the **asu showvalues** command.

```
asu.exe show <setting_name> --host <OS_ip> --user root  --password <OS_password>
--vmware-esxi

asu.exe set <setting_name> <setting_value> --host <OS_ip> --user root
--password <OS_password> --vmware-esxi

asu.exe showvalues <setting_name> --host <OS_ip> --user root
--password <OS_password> --vmware-esxi
```

Known limitations

This topic lists all of the known limitations with Advanced Settings Utility.

1. RDCLI supports only ISO/CDROM/DVDROM as the mount source.
2. RDCLI does not support non-IMM systems.

3. ASU does not support the **loaddefault** value for the boot order on IMM-based systems. The **loaddefault** command does not change the boot order to the default value.
4. In Flex system, there are two types of user accounts due to the security design: CMM user (LDAP user) and IMM2 user (local user). CMM users are available for Web, CLI, and CIM interfaces. IMM2 users are available for IPMI and SNMPv3 interfaces. Generally, ASU needs a IMM2 user to work on IMM, but it needs a CMM user in FoD key management if **--device CMM** or **--interface CIM** is specified.
5. ASU failed to set uEFI.LegacyRomExecution through ESXi, although uEFI rebooted.
6. On ESXi, ASU does not support the creation of iSCSI by setting iSCSI.AttemptName.x. You must create iSCSI by using the **F1** menu first, then using ASU to modify the iSCSI attribute.
7. On ESXi on the IMMv1 platform and IMMv2 platform earlier than 1AOO49Z, ASU does not support changes to the syslog status by setting IMM.RemoteAlertRecipient_Status.x. You might be able to change the setting, but the new value will neither be shown by ASU nor take effect.
8. After ASU sets some IMM network settings, which might lead to an IMM IP address change or ASU connection close, ASU might fail to get the set result.
9. On ESXi, if the CIM ports have been changed on IMM (the default is http 5988 https 5989), you must manually disable the ESXi5.x firewall by using the command `esxcli network firewall set -e false`, or ASU will not connect to ESXi.
10. In Flex System, the settings IMM.IMMInfo_Contact, IMM.IMMInfo_Location, and IMMInfo_RoomId cannot be set with the value of `null string`.
11. On ESXi4.1, ESXi5.0 and ESXi5.1, OpenSSL can only support TLS level 1.0; therefore, if you set the IMM TLS min level to 1.1 or 1.2, ASU will fail to get and set IMM configuration through those ESXi systems.
12. When using the **comparedefault** command, some settings might not match their default values, even though the **loaddefault** command was run before the **comparedefault** command.
13. On VMware ESXi with Lenovo Customized Image 5.0, ASU cannot set bootorder (and wolbootorder) settings. This is a permanent limitation on VMware ESXi with Lenovo Customized Image 5.0, and the workaround in limitation 14.does not work for it.
14. On VMware ESXi with Lenovo Customized Image 5.1 and 5.5u1, ASU cannot set bootorder (and wolbootorder) settings. This is caused by a conflict of the class name for bootorder in the Broadcom CIM Provider and IMM. The Broadcom CIM Provider must be disabled for ASU to set the bootorder (and wolbootorder) settings.

    To disable the Broadcom CIM Provider, run the following commands on theESXi command terminal:

    a. `. esxcli system settings advanced list | grep brcm`

       The following example illustrates what the output might look like:

       ```
       Path: /UserVars/CIMvmw_brcmProviderEnabled
                 Description: Enable or disable the CIM vmw_brcm provider
       ```

    b. `. esxcli system settings advanced set -o` *`[PATH]`* `-i 0`

       Where *[PATH]* is the path of the Broadcom CIM Provider listed in the output of the command run in step a. In the previous example, it is `/UserVars/CIMvmw_brcmProviderEnabled`

    c. `. /etc/init.d/sfcbd-watchdog restart`

Note: This issue has been fixed on VMware ESXi with Lenovo Customized Image 5.5u2 and later version.

15. There is a rebranding issue in all VMware ESXi with Lenovo Customized Image. Ensure that you have installed `patch2.1` or later into VMware ESXi with Lenovo Customized Image. To obtain the latest patch for ESXi, go to http://www-933.ibm.com/support/fixcentral/.

Chapter 2. Using the command-line interface

This section describes how to use the Advanced Settings Utility (ASU) command-line interface.

Command syntax

Before using the command-line interface, read the following guidelines.

- Each command has the following format:

  ```
  asu [application] [command [command_modifier] | [class]]
  [options] [connect_options]
  ```

- Each command starts with either asu or asu64.
- The optional configuration application can be either of the following options (see "Command configuration applications"):
  - savestat
  - immcfg
  - fodcfg
  - cmmcfg
  - immapp
  - secureboot
  - cmmvpd
- **command** is one of the commands that is listed in the command reference.
- command_modifier is one or more options that apply only to a certain command. These are considered command modifiers or extensions. Each command modifier must be preceded by a double hyphen (--). (See "Command modifiers" on page 70 for more information.)
- class is a filter that acts on a list of settings (settings display filters). A class is not considered a modifier or option. Classes are also used to operate a command upon a group or class of settings. A class does not require the double hyphen (--) as part of the syntax. For more information about a class, see "Classes of settings" on page 67.
- option is one or more general options that apply globally to the operation. Each option requires the preceding double hyphen (--) as part of its syntax. (See "General command options" on page 76.)
- **connect_option** is one or more parameters that are related to the ASU connection to the IMM. Connect options are defined as options. Each requires the double hyphen (--) as part of its syntax. (See "Command connectivity options" on page 72.)
- Brackets ([ ]) indicate that an application, option, or class is optional. Brackets are not part of the command that you type.

Command configuration applications

This topic explains the additional configuration applications integrated into the ASU.

The following applications are included in the ASU:

- savestat

- immcfg
- fodcfg
- cmmcfg
- immapp
- secureboot
- cmmvpd

The following sections describe each of the applications and outline the command syntax and structure.

Savestat

The savestat application is used by the ServerGuide Scripting Toolkit to save and restore the state information about the system. This function is supported for both IMM-based servers and some BIOS-based servers. The use cases for these are the same, with some exceptions:

- A file called `savestat.def` is used for BIOS-based servers. It is supplied in the ServerGuide Scripting Toolkit run time environment.
- Using savestat on IMM-based servers might require additional connectivity parameters, because the data is in the IMM on the server.

savestat write data example:

```
asu savestat write datafile
```

This command uses the contents of the `datafile` file to update the persistent storage contents.

savestat read data example:

```
asu savestat read datafile
```

This command reads the contents of the persistent storage and writes the results to the `datafile` file. If the file does not already exist, it is created. If the file already exists, it is overwritten.

Configuring the IMM LAN over USB interface

This topic describes how to install and configure the LAN over USB interface that is used to communicate with the IMM.

The ASU provides the ability to install and configure the LAN over USB interface that is used to communicate with the IMM as an add-on configuration application called immcfg. The command syntax is:

```
asu immcfg [application_commands]
```

The supported commands and the operating systems for which they are available are listed in Table 1.

The additional files that are required to perform these commands are included with the ASU package. The following required files must be in the directory from which the ASU is run.

Windows:

```
Lenovo_rndis_server_os.inf
device.cat
```

Linux:

```
cdc_interface.sh
```

Table 2. IMM LAN over USB configuration application commands

Configuration application command	Description	Operating system support	Command syntax to set the command
setip	Sets the operating system IP address for the LAN over USB interface	Windows only	`asu immcfg --setip`
detectdevice	Detects whether the IMM LAN over USB interface is activated	Windows only	`asu immcfg --detectdevice`
installdriver	Installs the IMM LAN over USB device driver	Windows only	`asu immcfg --installdriver [--inf inf_path/name]`
detectdriver	Detects whether the device driver for the IMM LAN over USB interface is installed in the operating system	Windows only	`asu immcfg --detectdriver`
autocfgdhcp	Automatically detects the presence of the IMM LAN/USB device, installs the required device driver, and delegates to IMM to assign an IP address to the OS USB-LAN interface.	WindowsLinux VMware	`asu immcfg --autocfgdhcp`
autocfgstatic	Automatically configures the IMM LAN/USB device using all default settings. Default settings include: Packaged INF/CAT and .SH files. Default IP addresses: 169.254.95.120 for the OS IP address. Note: It assumes that 169.254.95.118 is the IMM IP address. For multi-node, the primary node is always assigned 169.254.95.120, the secondary node is 169.254.96.120, and all others must follow this pattern.	WindowsLinux VMware	`asu immcfg --autocfgstatic`

Table 2. IMM LAN over USB configuration application commands (continued)

Configuration application command	Description	Operating system support	Command syntax to set the command
disable-imm-lan	Takes down the IMM USB LAN. For Windows it disables the LAN interface with Windows API, unsets IP(SetupDiChangeState). For Linux/VMware, it calls the ifdown and unset IP, and removes the configuration file in the Linux cdc_interface.sh.	WindowsLinux VMware	`asu immcfg --disable-imm-lan` **Note:** This case is for inband only. This parameter is also available when you try to operate a normal ASU command like `asu show all --disable-imm-lan`. It also disables the LAN interface after the command is done.

Note: On the Windows platform, ASU can automatically install a LAN over USB device driver or install the driver by using `Lenovo_rndis_server_os.inf`, which supports only these operating systems: Windows XP SP2, Windows XP x64, Windows Server 2003 SP1, and Windows Vista.

Feature on Demand configuration

This topic describes Feature on Demand configuration (fodcfg) management, which is supported by the ASU.

Fodcfg is used to acquire, install, uninstall, report, and export activation keys from the key repository. Fodcfg supports the hardware devices as key repositories:

- IMM2 based systems, includingSystem x Server
- CMM
- IOM (I/O Module) switches

For different devices, fodcfg supports three different interfaces: IPMI, CIM, and SNMP. The following table shows the supported devices and interfaces. The checkmark means that the device supports the interface. The term "IPMI interface" here means IPMI through LAN or LAN over USB. KCS is the IPMI interface using local Keyboard Controller Style (KCS).

Table 3. Supported devices and interfaces

	IPMI	KCS	CIM	SNMP
IMM	√	√	√	
CMM			√	
Switch				√

Command syntax

```
asu fodcfg <command> [options] [command options] [device&interface] [connection options]
```

Commands

Table 4. Commands

Command	Description
acquirekey	Acquire and download the activation key from the Lenovo web site.
installkey	Install activation keys from the user-specified location to the key repository.
uninstallkey	Uninstall activation keys from the device.
reportkey	Inventory information of a specified key repository.
exportkey	Export activation keys from a specific key store.
replacekey	Replace activation key or keys from the original unique identifier with a new key or keys.
getsysinfo	Get FoD supported system and feature information from theLenovo website.

Table 5. Options

Option	Description
--help	Display help for this command in the console window and exit. This command is the same as running with no parameters.
--disable-imm-lan	Disable the USB LAN interface on an IMM system.
[command options]: Acquirekey command	
--ibmid <userid:pwd>	Lenovo ID credential for the interactive Lenovo web site.
--auth <code>	Lenovo authorization code.
-u <unique id>	Unique identifier information.
-m <MT/DC>	For the system/option feature, specify the system machine type (MT) here. For the IOM switch, specify device code (DC).
-d <dir>	Download the key file to the <dir> location.
-r	Install the downloaded activation key.
--installin <MT+SN>	System MT and serial number (SN) in which the key is installed
--all	Acquire the key for the specified machine and install it in the specified machine. All keys tied to the server are searched.
--proxy <proxy-info>	Set proxy information, for example: user:password@host:port
Installkey command	
-f <keyfilename|dir>	A single activation key file. Fodcfg installs a single activation key file.
Uninstallkey command	
--keyid <keyid>	Activation key ID is returned from the report command. If keyid is "all," then all keys are uninstalled.
Note: Some devices must follow rules to install and uninstall activation keys; `--keyid all` might not work correctly. Uninstall the key of upgrade 2 and then the key of upgrade 1. See device documents for the key management operation rules.	
Reportkey command	

Table 5. Options (continued)

Option	Description
None	Report activation key or keys from IMM, AMM, CMM and Switch. In IMM and CMM, the output format is `No, Key ID, Status, Description, User Reminding, Expired Date.` For AMM and Switch, the output format is `No, Key ID, Status, Description`.
Exportkey command	
--keyid <keyid>	Activation key ID is returned from the report command. If keyid is "all", then all keys are exported.
-d <dir>	Download the key file to the <*dir*> location. The default value is the current folder.
Replacekey command	
--ibmid <userid:pwd>	Lenovo ID credential for interactive Lenovo website.
--olduid <unique id>	Old unique identifier information.
-u <unique id>	Replace existing unique identifier with a new one.
-d <dir>	Download the key file to the <*dir*> location. The default value is the current folder.
--installin <MT+SN>	System machine type (MT) and SN, which the key is installed in.
--featurecode <featurecode>	Feature code.
--proxy <proxy-info>	Set proxy information, for example: *user:password@host:port*
Getsysinfo command	
--ibmid<userid:pwd>	Lenovo ID credential for interactive Lenovo website.
--proxy<proxy-info>	Set proxy information, for example: `user:password@host:port`
-f <dir>	Download the information file to the <*dir*> location. The default value is the current folder.
[device&interface]:	
--device <device>	Support device: IMM, CMM, Switch.
--interface <interface>	Support interface: IPMI, KCS, CIM, SNMP.
Note: If a device is specified, the default interface value is all supported interfaces by the device. If an interface is specified, the default device value is the device that supports this interface. If neither are specified, the default device is IMM.	
[connection options]:	
--host <IP>	Remote key repository. The default is the local IMM device.
--user <userid>	Key repository credential user name.
--password <password>	Password of the key repository.
--cimhttp	Use HTTP for the CIM interface.
--port <port>	Port for the CIM interface. The default is `5989`.
--sftp <IP:port>	SFTP server for the SNMP interface.
--tftp <IP:port>	TFTP server for the SNMP interface.
--ftpid <user:password>	FTP credential ID for the SNMP interface.

Table 5. Options (continued)

Option	Description
--community <community>	Community for snmpv1v2. The default is `public`.
--authproto <MD5/SHA>	Authorization protocol for snmpv3. The default is `no auth`.
--privproto <DES/AES>	Privacy protocol for snmpv3. The default is `No privacy`.
--privpasswd <password>	Privacy password. The default is `None`.

Command sample

```
asu.exe fodcfg installkey -f .\Lenovo_fod_7870abcdefg_anyos.key --host 10.10.10.1
--user USERID --password PASSW0RD
```

Using the address 10.10.10.1, install the activation key ibm_fod_7870abcdefg_anyos.key on the default device IMM. If you do not provide the `--host` parameter, ASU will try to install the activation key on the local IMM.

```
asu.exe fodcfg uninstallkey --keyid b2e61a48881917af --host 10.10.10.1
 --user USERID --password PASSW0RD --device cmm --interface cim
```

Using the address 10.10.10.1 through the CIM interface, uninstall the activation key b2e61a48881917af in CMM.

```
asu64.exe fodcfg uninstallkey --keyid all --device switch --interface snmp
 --host 9.125.90.190 --sftp 9.115.234.76:69 --ftpid 1234:1234 --community private
```

Using the address 9.125.90.190 through the SNMP interface, uninstall all the activation keys in the switch.

```
asu.exe fodcfg reportkey --device imm --interface cim --host 9.125.90.158
--user USERID --password PASSW0RD
```

Using the address 9.125.90.58 through the CIM interface, report all the activation keys in the IMM.

```
asu.exe fodcfg exportkey --keyid all -d ./fodkey --device imm
 --interface ipmi --host 9.125.90.158 --user USERID --password PASSW0RD
```

Using the address 9.125.90.58 through the IPMI interface, export all the activation keys in the IMM to file folder `./fodkey`.

Note: The ASU fodcfg application needs an extra tftp/sftp server to run on switches using the SNMP interface. Make sure that you have both write and read access for the tftp/sftp server. The ASU fodcfg application supports both snmp v1v2 and snmp v3. Make sure that the switch is properly configured and that you have the authority to perform operations on the switch.

FoD key management on different devices

This topic explains how to manage Feature on Demand (FoD) keys that are installed on different devices.

IMM2-based systems, including System x Server

Multiple interfaces are supported for the IMM-based system. If no interface (`--interface`) is specified, ASU tries to run by the CIM interface first. If the CIM

interface fails, ASU will try to run by IPMI LAN interface. If the IPMI LAN interface fails, ASU will try to run by the IPMI KCS interface.

ASU supports FoD key management out-of-band when `--host`, `--user`, and `--password` are all specified. In this out-of-band situation, if `--host` is specified, `--user` and `--password` both should be provided. However, if `--host`, `--user`, and `--password` are all specified, ASU will not try the IPMI KCS interface.

ASU supports FoD key management in-band when `--host` is not specified. First, ASU tries to get the IP address for the LAN over USB. The default values for `--user` and `--password` are `USERID` and `PASSW0RD`, respectively. ASU defaults to KCS if LAN over USB fails.

ASU supports work on the CIM interface by connecting with HTTP and HTTPS. By default, the ASU tries to connect with HTTPS, and the default port is 5989. You can specify `--cimhttp` to try the connection with HTTP, and then also specify `--port 5988`, which is the port for HTTP. Before running the ASU, configure the IMM correctly.

CMM

Only the CIM interface is supported on CMM; no in-band methods are available. You must enter `--host`, `--user` and `--password` for CMM management.

The ASU supports both HTTP and HTTPS. You can use the CIM interface on a CMM device the same as on an IMM device. Before running ASU, make sure that the CMM CIM interface is configured correctly.

IOM switches

The IOM switch is designed to use SNMP for FoD activation key management and needs an additional TFTP or SFTP server for key file transactions. You must prepare TFTP or SFTP before running the **ASU** command for FoD management on the IOM switch. In the command line, `--tftp <IP:port>` is for TFTP, while `--sftp <IP:port>` and `--ftpid <user:password>` are for SFTP. Make sure that you have both read and write access for TFTP/SFTP. You do not need to do operations on the TFTP/SFTP server directory; ASU automatically uploads and downloads keys and files.

ASU supports both SNMPv1v2 and SNMPv3. You do not need to specify `--user` and `--password` for SNMPv1v2. However, if `--user` and `--password` are specified, ASU will try to run SNMPv3 with the SNMP user and authorization password. `--privproto` and `--privpasswd` are for SNMPv3 privacy encryption. Before running ASU, make sure that the configuration on the IOM switch for the SNMP interface is correct.

Note: The ASU supports both SNMPv1v2 and SNMPv3. To use the correct one, make sure that both the interface and the IOM switch are supported.

Getting the key from the Lenovo website

This topic explains how to use the ASU command line utility to generate and download activation keys from the Lenovo website without logging onto the website.

From the ASU command line, specify your activation key information as necessary–see the command options parameters in the following table. Then you can download activation keys from the Lenovo website by using a command such as the following:

```
asu fodcfg acquirekey --ibmid restuser@invalid.domain:pasword --auth DEBAAAAAAAAA1654810000
-u 78704bc1234
```

Table 6. Command options parameters

Parameter	Required	Description
--ibmid <userid:pwd>	Yes	The Lenovo ID credential for the interactive Lenovo website.
-u <unique id>	Yes	Unique identifier information.
-m <MT/DC>	Yes	The machine type and device code. For the system/option feature, specify the system machine type (MT). For the IOM switch, specify the device code (DC).
--auth <code>	Optional	The Lenovo authorization code. If no `authcode` is provided, ASU gets the key without generating it.
-d <dir>	Optional	Download the key file to the <*dir*> location. The default value is the current folder.
-r	Optional	Install the downloaded activation key.

Values `-u` and `-m` specify the system information. Value `-u` is a unique identifier and `-m` is the system server type or switch device code. To get the keys that are installed on the IMM/CMM, enter the server type `-m`. For the switch keys, enter the device code. The available switch device codes are shown below.

When no authorization code is entered, ASUdownloads the keys for that system directly. If `--auth` is specified, ASU tries to generate and then download the keys for that system using the authorization code.

You can specify `-r` by using the **`acquirekey`** command to generate and download keys and install them automatically. If `-r` is not specified, ASU gets the key and puts it in the local folder without installing it. To install the key automatically, you must specify every element (except for `-f`), as shown in the following example: `asu fodcfg installkey`.

Table 7. Available switch device codes

Feature description	Install on system	Device code	Unique ID format
Lenovo Flex System Fabric EN4093 10 Gb Scalable Switch (Upgrade 1)	Lenovo Flex System Enterprise Chassis [8721]	FCA1EL	Lenovo Switch Serial Number (12 characters)
	Lenovo Flex System Enterprise Chassis [7893]	FC3597	

Table 7. Available switch device codes (continued)

Feature description	Install on system	Device code	Unique ID format
Lenovo Flex System Fabric EN4093 10 Gb Scalable Switch (Upgrade 2)	Lenovo Flex System Enterprise Chassis [8721]	FCA1EM	Lenovo Switch Serial Number (12 characters)
	Lenovo Flex System Enterprise Chassis [7893]	FC3597	
Lenovo Flex System EN2092 1 Gb Ethernet Scalable Switch (Upgrade 1)	Lenovo Flex System Enterprise Chassis [7893]	FC3599	Lenovo Switch Serial Number (12 characters)
	Lenovo Flex System Enterprise Chassis [8721]	FCA1QW	
Lenovo Flex System EN2092 1 Gb Ethernet Scalable Switch (10Gb Uplinks)	Lenovo Flex System Enterprise Chassis [8721]	FCA1EN	Lenovo Switch Serial Number (12 characters)
	Lenovo Flex System Enterprise Chassis [7893]	FC3594	
Lenovo Flex SystemIB6131 Infiniband Switch (FDR Upgrade)	Lenovo Flex System Enterprise Chassis [8721]	FCA1QX	Lenovo Switch Serial Number (19 characters)

Chassis Management Module configuration

This topic describes the Chassis Management Module (CMM) configuration management that is supported by ASU.

CMM is the management module for the Flex System chassis. ASU supports CMM configuration in ASU version 9.40 or later.

Command syntax

```
asu cmmcfg <command>[setting name] [setting options] [options] [connection options]
```

Commands

Table 8. Commands

Command	Description
list	Show all subsettings of the specified setting, and the support operation commands for each setting in list view. If the setting name is not specified, show all the setting names and the support commands for each setting name.
showtree	Show all subsettings of the specified setting and the support operation commands for each setting in tree view. If the setting name is not specified, show all the setting names and the support commands for each setting name.
help	Display detailed information about the specified setting.
show	Show the value of the specified setting.
set	Set the value for the specified setting.
showvalues	Show all the possible values for the specified setting.

Table 8. Commands (continued)

Command	Description
showdefault	Show the default value for the specified setting.
loaddefault	Load default values for the specified setting.
delete	Delete the specified setting.
import	Import local file to CMM.
export	Export file from CMM to local.
reboot	Restart the CMM.
reset	Reset the CMM to defaults and reboot.
enum	Enumerate all attached CMM.
Note: The **list**, **showtree**, and **help** commands are used to display supported setting information. You can run them to get the format and description from all the settings, so every setting supports these three commands. These commands are not operation commands for CMM, so you do not need to connect to CMM while running them. Connection options are also not required.	

```
<setting name>
```

The setting name takes the format of `CMM<0x>.xx.xx`, which can be shown by either the **list** or the **showtree** command. Options are provided in the tables below.

Table 9. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 10. Connection options

Connection option	Description
--host <ip>	Address of the CMM server to operate on.
--user <userid>	CMM user name for authentication. The default is `USERID`.
--password <password>	CMM password for authentication. The default is `PASSWORD`.
--port <port>	Port for the CIM interface. The default is `5989`.

CMM settings and commands supported

```
CMM<xx>:[Reboot,Reset]
CMM<xx>.Account:[Show]
CMM<xx>.Account.@<UserID>:[Delete]
CMM<xx>.Account.@<UserID>.Password:[Set,ShowValues]
CMM<xx>.Configuration:[Export,Import,ShowValues]
CMM<xx>.Firmware:[Show]
CMM<xx>.Network
CMM<xx>.Network.HostName:[Set,Show,ShowValues]
CMM<xx>.Network.DomainName:[Set,Show,ShowValues]
CMM<xx>.Network.DNS
CMM<xx>.Network.DNS.DDNS:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.State:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.IPv4Address:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.IPv6Address:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.IPv6Preferred:[Set,Show,ShowValues]
CMM<xx>.Network.IPv4:[Show]
CMM<xx>.Network.IPv4.StaticAddress:[Set,Show,ShowValues]
CMM<xx>.Network.IPv4.StaticSubnetMask:[Set,Show,ShowValues]
CMM<xx>.Network.IPv4.StaticDefaultGateway:[Set,Show,ShowValues]
CMM<xx>.Network.IPv4.AssignAddressMethod:[Set,Show,ShowValues,ShowDefault,LoadDefault]
```

```
CMM<xx>.Network.IPv6:[Show]
CMM<xx>.Network.IPv6.State:[Show,ShowValues]
CMM<xx>.Network.IPv6.Auto:[Set,Show,ShowValues]
CMM<xx>.Network.IPv6.DHCP:[Set,Show,ShowValues]
CMM<xx>.Network.IPv6.Static:[Set,Show,ShowValues]
CMM<xx>.Network.IPv6.StaticAddress:[Set,Show,ShowValues]
CMM<xx>.Network.IPv6.StaticDefaultGateway:[Set,Show,ShowValues]
CMM<xx>.Network.IPv6.StaticSubnetPrefixLength:[Set,Show,ShowValues]
CMM<xx>.Network.Ethernet:[Show]
CMM<xx>.Security
CMM<xx>.Security.Policy:[Set,Show,ShowValues]
CMM<xx>.Security.LdapClient:[Set,Show,ShowValues]
CMM<xx>.Security.SshServer:[Show,ShowValues]
CMM<xx>.Security.LdapTrustedCert:[Show,Delete,Import,Export,ShowValues]
CMM<xx>.Chassis:[Show]
CMM<xx>.Chassis.Name:[Set,Show,ShowValues]
CMM<xx>.Chassis.Room:[Set,Show,ShowValues]
CMM<xx>.Chassis.Rack:[Set,Show,ShowValues]
CMM<xx>.Chassis.Location:[Set,Show,ShowValues]
CMM<xx>.Chassis.UnitHeight:[Show,ShowValues]
CMM<xx>.Chassis.LowestRackUnit:[Set,Show,ShowValues]
CMM<xx>.Properties
CMM<xx>.Properties.General
CMM<xx>.Properties.General.ModuleName:[Show,ShowValues]
CMM<xx>.Properties.DateTime
CMM<xx>.Properties.DateTime.AutoDST:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.SyncMethod:[Set,Show,ShowValues,ShowDefault,LoadDefault]
CMM<xx>.Properties.DateTime.Date:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.Time:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.SyncFrequency:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.NTPServer:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.NTPv3Auth:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.NTPv3KeyIndex:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.NTPv3KeyData:[Set,Show,ShowValues]
CMM<xx>.Properties.DateTime.GMTOffset:[Set,Show,ShowValues,ShowDefault,LoadDefault]
```

Note: The setting name is composed of the node name separated by a comma. You do not need to type the <> tag in the node name, and the value within the brackets can be a number from 0 to 9 or a user ID like USERID. The *xx* represents the numbers required for input. For example: cmm01.account.@user.password. All of the settings support these three commands: **list**, **showtree**, and **help**.

List CMM settings

You use the ASU to list all subsettings of the specified CMM setting and the support operation commands for each setting. If the setting name is not specified, the **list** command lists all the setting names and support commands.

The **list** command is not an operation command. You do not need to connect CMM to run it. All the settings are supported by this command.

Command syntax

```
asu cmmcfg list [setting name] [options]
```

Command

```
<setting name>
```

Setting name is an option parameter for the list comment. It takes the format of CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 11. Options

Option	Description
--help	Display help for this command in the console window and exit.

Command example

```
C:\asu>asu.exe cmmcfg list cmm01 --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Discription:
  Setting name is composed by node name below separated by '.'
Example:
  cmm01.account.@user.password
  cmm01.network.dns.ipv4address1
Using 'enum' command to show all attched cmm.
   The <> tag in node name doesn't need to be typed, and the value between it
   needs user input which means number form '0' to '9' or userid like 'USERID'.
   The count of char 'x' stand for how many numbers need to input.
********************************************************************************
CMM<xx>:[Reboot,Reset]
CMM<xx>.Account:[Show]
CMM<xx>.Account.@UserID:[Delete]
CMM<xx>.Account.@UserID.Password:[Set,ShowValues]
CMM<xx>.Configuration:[Export,Import,ShowValues]
CMM<xx>.Firmware:[Show]
CMM<xx>.Network
CMM<xx>.Network.HostName:[Set,Show,ShowValues]
CMM<xx>.Network.DomainName:[Set,Show,ShowValues]
CMM<xx>.Network.DNS
CMM<xx>.Network.DNS.DDNS:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.State:[Set,Show,ShowValues]
CMM<xx>.Network.DNS.IPv4Address<x>:[Set,Show,ShowValues]
......
Command executed successfully
```

List CMM settings in a tree-like format

With ASU you can list all subsettings of the specified CMM setting and the support operation commands for each setting in a tree-like format. If the setting name is not specified, the **list** command lists all the setting names and support commands.

The **showtree** command is not an operation command. You do not need to connect CMM to run it. All the settings are supported by this command.

Command syntax

```
asu cmmcfg showtree [setting name] [options]
```

Command

```
<setting name>
```

`Setting name` is an option parameter for the list comment. It takes the format of `xx.xx.xx`, which can be shown by either the **list** or **showtree** command.

Table 12. Options

Option	Description
--help	Display help for this command in the console window and exit.

Command example

```
C:\asu>asu.exe cmmcfg showtree cmm01 --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Discription:
  Setting name is composed by node name below separated by '.'
Example:
  cmm01.account.@user.password
  cmm01.network.dns.ipv4address1
Using 'enum' command to show all attched cmm.
   The <> tag in node name doesn't need to be typed, and the value between it
   needs user input which means number form '0' to '9' or userid like 'USERID'.
   The count of char 'x' stand for how many numbers need to input.
********************************************************************************
|-CMM<xx>:[Reboot,Reset]
     |-Account:[Show]
              |-@<UserID>:[Delete]
                         |-Password:[Set,ShowValues]
     |-Configuration:[Export,Import,ShowValues]
     |-Firmware:[Show]
     |-Network
             |-HostName:[Set,Show,ShowValues]
             |-DomainName:[Set,Show,ShowValues]
             |-DNS
               |-DDNS:[Set,Show,ShowValues]
               |-State:[Set,Show,ShowValues]
               |-IPv4Address<x>:[Set,Show,ShowValues]
               |-IPv6Address<x>:[Set,Show,ShowValues]
               |-IPv6Preferred:[Set,Show,ShowValues]
             |-IPv4:[Show]
               |-StaticAddress:[Set,Show,ShowValues]
 ......
Command executed successfully.
```

Display help information for CMM setting

You can use the ASU to display detailed information about the specific CMM setting.

The **Help** command is not an operation command. You do not need to connect CMM to run it. All the settings are supported by this command.

Command syntax

```
asu cmmcfg help <setting name> [options]
```

Command

```
<setting name>
```

Setting name takes the format xx.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 13. Options

Option	Description
--help	Display help for this command in the console window and exit.

Command example

```
C:\asu>asu.exe cmmcfg help cmm01
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
```

```
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
 Description:
   This setting name is used to config the CMM.
 Supported commands for this setting name:
   help        Display this help message
   list        Show all subsettings of the specified setting name in list view
   showtree    Show all subsettings of this setting group in tree view
   enum       Enumerate all attached CMM
   reboot      Reboot the CMM
   reset       Reset the CMM to defaults and reboot
```

Show CMM setting

You can use the ASU to show the current value for the specified CMM setting.

Command syntax

```
asu cmmcfg show <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 14. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 15. Connection options

Connection option	Description
--host <ip>	Address of the CMM server to operate on.
--user <userid>	CMM user name to authenticate. The default is USERID.
--password <password>	CMM password to authenticate. The default is PASSWORD.
--port <port>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg show cmm01.network.ipv4.staticaddress --host 10.10.10.1
--user USERID
--password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.network.ipv4.staticaddress=9.1115.252.27
```

Set CMM setting

You can use the ASU to apply a value to a CMM setting.

Command syntax

```
asu cmmcfg set <setting name> <value> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

<value>

Specify the value to set.

Table 16. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 17. Connection options

Connection option	Description
--host <ip>	Address of the CMM server to operate on.
--user <userid>	CMM user name to authenticate. The default is USERID.
--password <password>	CMM password to authenticate. The default is PASSWORD.
--port <port>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg set cmm01.network.ipv4.staticaddress 9.115.252.27
--host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.network.ipv4.staticaddress=9.115.252.27
This setting will take effect after the CMM restart.
```

Show possible values for CMM setting

You can use the ASU to show the possible values for the specified CMM setting.

Command syntax

```
asu cmmcfg showvalues <setting name> [options] [connection options]
```

Command

<setting name>

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 18. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 19. Connection options

Connection option	Description
--host <ip>	Address of the CMM server to operate on.
--user <userid>	CMM user name to authenticate. The default is USERID.
--password <password>	CMM password to authenticate. The default is PASSWORD.
--port <port>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg showvalues cmm01.Network.DNS.State --host 10.10.10.1
 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.Network.DNS.State=Enabled=Disabled
```

Show default value for CMM setting

You can use the ASU to show the default value for the specified CMM setting.

Command syntax

```
asu cmmcfg showdefault <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format xx.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 20. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 21. Connection options

Connection option	Description
--host <ip>	Address of the CMM server to operate on.
--user <userid>	Key repository credential user name. The default is USERID.
--password <password>	CMM user name to authenticate. The default is PASSWORD.
--port <port>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg showdefault cmm01.Network.IPv4.AssignAddressMethod --host 10.10.10.1
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.Network.IPv4.AssignAddressMethod=DHCP Then Static
```

Load default value for CMM setting

You can use the ASU to load the default value for the specified CMM setting.

Command syntax

```
asu cmmcfg loaddefault <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 22. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 23. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is `USERID`.
--password <*password*>	CMM password to authenticate. The default is `PASSWORD`.
--port <*port*>	Port for the CIM interface. The default is `5989`.

Command example

```
C:\asu>asu.exe cmmcfg loaddefault cmm01.Network.IPv4.AssignAddressMethod--host 10.10.10.1
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.Network.IPv4.AssignAddressMethod=DHCP Then Static
```

Delete CMM setting

You can use the ASU to delete a specified CMM setting.

Command syntax

```
asu cmmcfg delete <setting name> [options] [connection options]
```

Command

```
<setting name>
```

`Setting name` takes the format `CMM<0x>.xx.xx`, which can be shown by either the **`list`** or **`showtree`** command.

Table 24. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 25. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is `USERID`.
--password <*password*>	CMM password to authenticate. The default is `PASSWORD`.
--port <*port*>	Port for the CIM interface. The default is `5989`.

Command example

```
C:\asu>asu.exe cmmcfg delete cmm01.Account.@ASUTEST --host 10.10.10.1
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
```

```
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
cmm01.Account.@ASUTEST is deleted.
Command executed successfully.
```

Import local file to CMM

You can use the ASU to import a local file to CMM.

Command syntax

```
asu cmmcfg import <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 26. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 27. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is USERID.
--password <*password*>	CMM password to authenticate. The default is PASSWORD.
--port <*port*>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg import
cmm01.configuration sftp://user:password@9.115.234.91:63/cfgabc.txt@Passw0rd
--host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
Started to import configuration file from
sftp://user:password@9.115.234.91:63/cfgabc.txt@Passw0rd
Still running 0......
Still running 1......
Still running 2......
Still running 3......
Finished to import configuration file to
sftp:// user: password@9.115.234.91:63/cfgabc.txt@Passw0rd
```

Export file from CMM

You can use the ASU to export a file from CMM to your local system. Refer to the **help** command to check a setting support export command and what the type of file it might be exporting.

Command syntax

```
asu cmmcfg export <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 28. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 29. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is USERID.
--password <*password*>	CMM password to authenticate. The default is PASSWORD.
--port <*port*>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg export cmm01.configuration
sftp://user:password@9.115.234.91:63/cfgabc.txt@Passw0rd --host 10.10.10.1
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
Started to export configuration file to
sftp://user:password@9.115.234.91:63/cfgabc.txt@Passw0rd
Still running 0......
Still running 1......
Still running 2......
Finished to export configuration file to
sftp://user:password@9.115.234.91:63/cfgabc.txt@Passw0rd
```

Reboot CMM

You can use the ASU to reboot the CMM.

Command syntax

```
asu cmmcfg reboot <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 30. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 31. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.

Table 31. Connection options (continued)

Connection option	Description
--user <*userid*>	CMM user name to authenticate. The default is USERID.
--password <*password*>	CMM password to authenticate. The default is PASSWORD.
--port <*port*>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg reboot cmm01 --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
Issuing reboot command to CMM.
Checking if the CMM has reboot yet. (attempt 0)
CMM has started the reboot.
Disconnect from CMM
Wait for about x mins to let the CMM complete reboots.
Checking if CMM CIM interface is ready. (attempt 0)
Connected to CMM at IP address 10.10.10.1
Reboot  completed successfully.
```

Reset CMM to default

You can use the ASU to reset the CMM to the default setting and reboot.

Command syntax

```
asu cmmcfg reset <setting name> [options] [connection options]
```

Command

```
<setting name>
```

Setting name takes the format CMM<0x>.xx.xx, which can be shown by either the **list** or **showtree** command.

Table 32. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 33. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is USERID.
--password <*password*>	CMM password to authenticate. The default is PASSWORD.
--port <*port*>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg reset cm01 --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
Issuing reset command to CMM.
```

```
Checking if the CMM has reset yet. (attempt 0)
CMM has started the reset.
Disconnect from CMM
Wait for about x mins to let the CMM complete reset.
Checking if CMM CIM interface is ready. (attempt 0)
Connected to CMM at IP address 10.10.10.1
Reset  completed successfully.
```

Enumerate attached CMMs

You can use the ASU to enumerate all attached CMMs.

Command syntax

```
asu cmmcfg enum [options] [connection options]
```

Command

Table 34. Options

Option	Description
--help	Display help for this command in the console window and exit.

Table 35. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate. The default is USERID.
--password <*password*>	CMM password to authenticate. The default is PASSWORD.
--port <*port*>	Port for the CIM interface. The default is 5989.

Command example

```
C:\asu>asu.exe cmmcfg enum --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20xx All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
CMM[1]=cmm01
Name=SN#Y030BG16802L
Role=Primary
```

Note: The **enum** (enumerate) command also describes which CMM is primary and which one is secondary.

IMM application configuration

This topic describes IMM application configuration (immapp) that is supported by theASU.

Immapp is the application for IMM configuration, which is supported by ASU version 9.40 or later. It is used to power on, power off, and reboot the operating system (OS). You can also use immapp to report the OS status and show and clear the OS event log and IMM log.

Note: Immapp only supports IMM based systems. For the CIM interface, both HTTP and HTTPS are supported.

Command syntax

```
asu immapp <command> [options] [command options] [connection options]
```

Commands

Table 36. Commands

Command	Description
powerstate	Display the current host OS power state of the server.
poweronos	Power on the server host OS.
poweroffos	Power off the server host OS.
rebootos	Reboot the server host OS.
clearsel	Clear the system event log.
showsel	Display the system event log.
clearimmlog	Clear the IMM event log.
showimmlog	Display the IMM event log.
clearalllog	Clear the IMM event log and system event log.

Table 37. Command options

Option	Description
--help	Display help for this command and exit without executing the command.

Table 38. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force to use IPMI over KCS local interface.
--cimhttp	Use HTTP for the CIM interface. The default is `HTTP`.
--port <*port*>	Port for the IMM interface. The default is `5989`.

Display the host operating system power status

You can use the ASU command line to display the power state of the remote system host operating system.

Command syntax

```
asu immapp powerstate [command options] [connection options]
```

Command

Table 39. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 40. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force to use IPMI over the KCS local interface.

Command example

```
C:\asu>asu.exe immapp powerstate --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 10.10.10.1
Server Power is currently On!
```

Power on the host OS

You can use the ASU command line to power on the remote system host OS.

Command syntax

```
asu immapp poweronos [command options] [connection options]
```

Command

Table 41. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 42. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force the use of IPMI over the KCS local interface.

Command example

```
C:\asu>asu.exe immapp poweronos --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to IMM at IP address:10.10.10.1
Server is powered on.
```

Power off the host OS

You can use the ASU command line to power off the remote system host OS.

Command syntax

```
asu immapp poweroffos [command options] [connection options]
```

Command

Table 43. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 44. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force the use of IPMI over the KCS local interface.

Command example

```
C:\asu>asu.exe immapp poweroffos --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to IMM at IP address:10.10.10.1
Server is powered off.
```

Clear the system event log

You can use the ASU command line to clear the remote system IMM system event log.

Command syntax

```
asu immapp clearsel [command options] [connection options]
```

Command

Table 45. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 46. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force the use of IPMI over the KCS local interface.

Command example

```
C:\asu>asu.exe immapp clearsel --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to IMM at IP address:10.10.10.1
Successfully clear the system event log.
```

Show the system event log

You can use the ASU command line to show the IMM system event log for the remote system.

Command syntax

```
asu immapp showsel [command options] [connection options]
```

Command

Table 47. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 48. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--kcs	Force the use of IPMI over the KCS local interface.

Command example

```
C:\asu>asu.exe immapp showsel --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to IMM at IP address:10.10.10.1
SEL Information
Version          : 1.5 (v1.5, v2 compliant)
Entries          : 512
Free Space       : 0 bytes
Percent Used     : 100%
Last Add Time    : 02/26/2002 08:58:55
Last Del Time    : 02/19/2002 03:43:34
Overflow         : true
Supported Cmds   : 'Reserve'
   1 | 07/03/2012 | 09:38:35 | Event Logging Disabled #0xb6 | Log area reset/cle
ared | Asserted
   2 | 07/03/2012 | 09:39:54 | System Firmware Progress #0xb4 | System boot init
iated | Asserted
   3 | 07/04/2012 | 07:00:27 | Power Unit #0x01 | Power off/down | Asserted
   4 | 07/04/2012 | 07:01:25 | Power Unit #0x01 | Power off/down | Deasserted
   5 | 07/04/2012 | 07:01:25 | System Firmware Progress #0xb4 | Unspecified | As
serted
   6 | 07/04/2012 | 07:03:21 | System Firmware Progress #0xb4 | System boot init
iated | Asserted
   7 | 07/04/2012 | 07:24:06 | Power Unit #0x01 | Power off/down | Asserted
   8 | 07/04/2012 | 07:35:48 | Power Unit #0x01 | Power off/down | Deasserted
   9 | 07/04/2012 | 07:35:59 | System Firmware Progress #0xb4 | Unspecified | As
serted
   10 | 07/04/2012 | 07:38:06 | System Firmware Progress #0xb4 | System boot init
iated | Asserted
```

Clear the IMM event log

You can use the ASU command line to clear the remote IMM event log.

Command syntax

```
asu immapp clearimmlog [command options] [connection options]
```

Command

Table 49. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 50. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--cimhttp	Use HTTP for CIM interface. The default is `https`.
--port <*port*>	Port for CIM interface. The default is `5989`.

Command example

```
C:\asu>asu.exe immapp clearimmlog --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to CIMOM at IP address:10.10.10.1 on Port:5989
Successfully clear the IMM log.
```

Show the IMM event log

You can use the ASU command line to display the remote IMM event log.

Command syntax

```
asu immapp showimmlog [command options] [connection options]
```

Command

Table 51. Options

Option	Description
--help	Display help information for commands and exit without running the command.

Table 52. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--cimhttp	Use HTTP for CIM interface. The default is `https`.
--port <*port*>	Port for CIM interface. The default is `5989`.

Command example

```
C:\asu>asu.exe immapp showimmlog --host 10.10.10.1 --port 5988 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to CIMOM at IP address: 10.10.10.1 on Port:5988
0 | Severity:2 | Message:The Chassis Event Log on system SN#2329269 cleared by user USERID
1 | Severity:2 | Message:The ComponentActivity Log on system SN#2329269 cleared by user USERID
2 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP address 9.123.236.180
3 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP address 9.125.90.77
4 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP address 9.125.90.77
5 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP address 9.111.30.227
6 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP address 9.111.30.227
7 | Severity:2 | Message:Management Controller SN# 2329269 reset was initiated by user USERID
8 | Severity:2 | Message:LAN: Ethernet[eth1] interface is now active
9 | Severity:2 | Message:ENET[sp-ethernetport]IP-Cfg:HstName=IMM-00215E5E118D,IP@=9.125.90.89,
NetMsk=255.255.255.0,GW@=9.125.90.1
10 | Severity:2 | Message:ENET[sp-ethernetport] IPv6-LinkLocal:HstName=IMM-00215E5E118D,
IP@=fe80::221:5eff:fe5e:118d, Pref=64
11 | Severity:2 | Message:Remote Login Successful. Login ID: USERID from Web at IP
address 9.111.30.227
12 | Severity:2 | Message:"Host Power" has been turned off
13 | Severity:2 | Message:"Host Power" has been turned on
```

Clear the IMM event log and system event log

You can use the ASU command line to clear the remote IMM event log and system log.

Command syntax

```
asu immapp clearalllog [command options] [connection options]
```

Command

Table 53. Options

Option	Description
--help	Display help information for the command and exit without running it.

Table 54. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name to authenticate. The default is `USERID`.
--password <*password*>	IMM password to authenticate. The default is `PASSWORD`.
--cimhttp	Use HTTP for the CIM interface. The default is `https`.
--port <*port*>	Port for the CIM interface. The default is `5989`.

Command example

```
C:\asu>asu.exe immapp clearalllog --host 10.10.10.1 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 10.0.87F
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to IMM at IP address:10.10.10.1
Successfully clear the system event log.
Connected to CIMOM at IP address: 10.10.10.1 on Port:5989
Successfully clear the IMM log.
```

Secureboot configuration

This topic describes the secureboot configuration that is supported by ASU.

Secureboot is the application for secureboot configuration, which is supported by ASU 9.51 or later. It is used to manage secureboot related keys and signatures in uEFI.

Note: The secureboot application in ASU supports Lenovo System x servers from Brickland only.

Command syntax

```
asu secureboot <operation> [keytype] [owner] [-f keyfile] [connection
options]
```

Operations

Table 55. Operations

Operation	Description
--help	Display the help information for secureboot usage.
enrollkek	Enroll a key to kek in uEFI.
enrolldb	Enroll a signature to db in uEFI.
enrolldbx	Enroll a signature to dbx in uEFI.
queryinfo	Query the secureboot status in uEFI.
queryret	Query the results of the secureboot operations.

Table 56. Connection options

Connection option	Description
--host <*ip*>	Address of the IMM server to operate on.
--user <*userid*>	IMM user name for authentication.
--password <*password*>	IMM password for authentication.

Secureboot policy update

You can use the ASU to enroll keys and signatures to a related key and signature database in uEFI. The **enroll** command will fail if the secureboot of the target uEFI is not in custom mode.

Command syntax

```
asu secureboot <operation> [keytype] [owner] [-f keyfile] [connection
options]
```

Command

<operation> Can be: `enrollkek`, `enrolldb`, `enrolldbx`

`[keytype]` Can be: `SHA256`, `RSA2048`, `RSA2048SHA256`, `SHA1`, `RSA2048SHA1`, `X509`, `SHA224`, `SHA348`, `SHA512`, `PKCS7`

`keytype` Refers to key and signature types, not just the key type. For kek, only three key types are supported for enrollment: `rsa2048`, `x509`, and `pkcs7`.

For db and dbx, those 10 key types are all supported for enrollment.

[owner] A GUID identifier of the key or signature.

- Valid format is 45678-9012-3456-7890-12345678aaaa
- Valid length is 32 characters, excluding the separator "-"
- Valid characters are 0-9, A/a-F/f

[-f keyfile] Key or signature file path

Command example

```
c:\asu\asu.exe   secureboot enrollkey x509
"12345678-9012-3456-7890-12345678aaaa"  -f  KeyFile.cer --host
9.111.68.20 --user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 9.51.xxx
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2014 All Rights Reserved
Start to update policy of SecureBoot
Connected to IMM at IP address 9.111.68.20
Command has been sent successfully, and will take effect after reboot uefi.
```

After the previous command is executed successfully, the key file is transferred to the IMM datastore. When uEFI reboots, it updates the key file from the IMM datastore to the uEFI key database. Because of this, you must reboot uEFI for the ASU enroll key command to take effect.

Secureboot query

You can use the ASU **query** command to get the secureboot status and the results of the ASU **secureboot** command.

Command syntax

- asu secureboot <queryinfo> [connection options]
- asu secureboot <queryret> [connection options]

Command

queryinfo is used to query the secureboot configuration status and key list. The command **queryret** is used to query the results of those secureboot commands that executed before the last uEFI reboot.

Command example

```
c:\asu\asu.exe   secureboot queryinfo --host 9.111.68.20 --user
USERID --password PASSW0RD
c:\asu\asu.exe   secureboot queryinret --host 9.111.68.20 --user
USERID --password PASSW0RD
```

CMM VPD configuration

This topic describes CMM VPD configuration that is supported by the ASU. CMMVPD is the application for CMM VPD configuration, which is supported by ASU 9.60 or later. It is used to manage VPD of the Chassis Management Module.

Command syntax

`asu cmmvpd <command> [setting name][command options] [connection options]`

Table 57. Commands

Command	Description
enum	Displays the topology path in CMM.
show	Displays the VPD information.
set	Changes the VPD information.
revert	Reverts from OEM VPD to Lenovo VPD and cleans the OEM VPD block.
help	Displays detailed information about the setting.

Table 58. Command options

Command option	Description
--help	Displays information about this command in the console window and exits.

Table 59. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name for authentication.
--password <*password*>	CMM password for authentication.
--port <*port*>	CMM port; the default is `6091`.

Supported settings

The following table provides a list of settings that can be modified with the CMMVPD tool.

Table 60. OEM VPD setting list

Setting type	Description
--machine-type-model	Machine type and model number in the OEM VPD base block
--machine-serial	Machine serial number in the OEM VPD base block
--comp-part	Component part number in the OEM VPD base block
--comp-serial	Component serial number in the OEM VPD base block
--hw-revision	Hardware revision level in the OEM VPD base block
--company	Company name in the OEM VPD base block
--service-tag	Service tag in the OEM VPD extended block
--oem-part	OEM part number in the OEM VPD extended block
--oem-string1	OEM component text string description 1
--oem-string2	OEM component text string description 2

Enum CMM topology

You can use the ASU to obtain all available supported modules in the CMM chassis by using the **--host** parameter and CMM user account in the **--user** and **--password** parameters.

Command syntax

```
asu cmmvpd enum [command options] [connection options]
```

Table 61. Command options

Command option	Description
--help	Displays information about the command and exits without executing it.

Table 62. Connection options

Connection option	Description
--host <*ip*>	Address of the CMM server to operate on.
--user <*userid*>	CMM user name to authenticate; the default is USERID
--password <*password*>	CMM password used to authenticate; the default is PASSW0RD
--port <*port*>	CMM port; the default is 6091.

Command sample

```
C:\ASU>asu.exe cmmvpd enum --host xxx.xxx.xxx.xxx --user xxx --password xxx
    Lenovo Advanced Settings Utility version 9.nn.nn
    Licensed Materials - Property of Lenovo
    (C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
    Chassis
    Chassis.Blade[10]
    Chassis.Blade[11]
    Chassis.Blade[12]
    Chassis.Blade[13]
    Chassis.Blade[1]
    Chassis.Blade[4]
    Chassis.Blade[5]
    Chassis.Blade[7]
    Chassis.Blade[8]
    Chassis.Blade[9]
    Chassis.CMM[1]
```

Show CMM VPD settings

You can use the ASU to display the current value of the VPD settings on CMM-based servers.

Specify the CMM IP address in the **--host** parameter and the CMM user account in the **--user** and **--password** parameters.

Command syntax

```
asu cmmvpd show <setting> [command options] [connection options]
```

<setting>: The setting name and format is *[Module]*.vpdsetting. You can obtain the available module by using the **enum** command. The value for vpdsetting is defined in the definition file.

[command options]:

--help Displays information about the command.

Command sample

```
C:\ASU>asu.exe cmmvpd show Chassis.Blade[1].oem-string1 --host
xx.xx.xx.xx --user xxx --password xxx
     Lenovo Advanced Settings Utility version 9.nn.nn
     Licensed Materials - Property of Lenovo
     (C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
     Connected to CMM at IP address:xx.xx.xx.xx
     Chassis.Blade[1].oem-string1=xxx
```

Set CMM VPD settings

You can use the ASU to modify VPD information on CMM-based servers.

You can use the ASU command line to modify the VPD information of certain devices on a CMM chassis by specifying the address in the **--host** parameter and the CMM user account in the **--user** and **--password** parameters.

Command syntax

asu cmmvpd set *<setting> <setting value> [command options] [connection options]*

<setting>:

The setting name and format is *[Module]*.vpdsetting. You can obtain the available module by using the **enum** command. You can locate the setting for vpdsetting in the definition file.

<setting value>:

The VPD string you want to set.

[command options]:

--help Displays information about the command and exits without executing it.

Command sample

```
C:\ASU>asu.exe CMMVPD set Chassis.Blade[1].oem-string1 "value"
--host xxx.xxx.xxx.xxx --user xxx --password xxx
     Lenovo Advanced Settings Utility version 9.nn.nn
     Licensed Materials - Property of Lenovo
     (C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
     Connected to CMM at IP address:xx.xx.xx.xx
     Chassis.blade[1].oem-string1=xxx
     Waiting for command completion status.
     Command completed successfully.
```

Revert CMM module

You can use the ASU to revert OEM VPD to Lenovo VPD and clean all data fields of the OEM VPD block for a specific module.

If it is Lenovo VPD, ASU will return the following settings empty if you try to show them:

- service-tag
- oem-part
- oem-string1
- oem-string2

For the following settings, ASU can only show those that can be seen in the CMM web GUI. Otherwise, ASU returns an empty string.

- machine-type-model
- machine-serial
- comp-part
- comp-serial
- hw-revision
- company

Note: Different modules may have different settings that can been shown in the CMM web GUI.

Specify the CMM IP address in the **--host** parameter and the CMM user account in the **--user** and **--password** parameters.

Command syntax

```
asu cmmvpd revert <module> [command options] [connection options]
```

<*module*>:

You can obtain available modules by using the **enum** command, for example: `Chassis.Blade[1]`

`[command options]`

`--help` displays information about the **revert** command.

Command sample

```
C:\ASU>asu.exe CMMVPD revert Chassis.Blade[1] --host
xx.xx.xx.xx --user xxx --password xxx
Lenovo Advanced Settings Utility version 9.nn.nn
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Connected to CMM at IP address:xx.xx.xx.xx
Revert Chassis.Blade[1] Successful!
```

help command

This command provides a detailed description about the setting.

You do not need an Internet connection between ASU and CMM to use the **help** command.

Command syntax

```
ASU cmmvpd help <setting> [command option]
```

<*setting*>:

The setting name and format is *[Module]*.vpdsetting. You can locate an available module by using the **enum** command; vpdsetting is defined in the definition file.

<*Module*>:

Use the **enum** command to obtain available modules, such as Chassis.Power[1].

[command options]:

--help displays information about the command and exits without executing it.

Command sample

```
C:\ASU>ASU.exe cmmvpd help Chassis.Power[2].machine-type-model
Lenovo Advanced Settings Utility version 9.nn.nn
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-20nn All Rights Reserved
Detail description for the setting Chassis.Power[n].machine-type-model
---------------------------------
This setting is used to set or show the oem vpd setting:machine type.
```

Supported modules and devices

This topic lists the modules and devices that are supported by the ASU CMMVPD tool.

The following modules are supported by the ASU CMMVPD tool:

- Blade (including xITE, Storage Blades, ITME)
- Power
- Fan/cooling
- IO module
- Chassis
- Fan Mux/Fan Logic Module
- LED card (and module)
- Chassis Management Module
- Blade Expansion (for example, SME and PME)
- Card expansion

Generic OEM product names

To have the FRU or CRU display the original generic Next Generation Product (NGP) Flex OEM product name to match the original part VPD data set by the manufacturing system build process, use the **set** command to enter the generic NGP Flex OEM product name into the extended VPD data field (the **Text1** field).

Refer to the following table for a list of the approved NGP Flex GA4/GA4.1/GA5 OEM product names.

After using the **set** command, to verify that the product name was entered correctly, use the **show** command to ensure that the name displays as expected.

If you want to default to the original Lenovo product name, use the **revert** command, which clears the **Text1** field and displays the default product name.

Note: If the extended OEM data field **Text1** is set to the default value of NULLs, the common FRU product name shown in the Lenovo name column is used, as shown in the following table.

Table 63. NGP Flex OEM product names

Category (FRU/CRU)	STD base name	Bytes (length)	Generic OEM name	Bytes (length)
New Lenovo offerings (no legacy support required)				
Compute Node	Lenovo Flex System x240 M5 Compute Node	41	x86 2S M5 EP Node	17
Legacy rebranded (new Lenovo MTMs, Lenovo website)				
Chassis	Lenovo Flex System Enterprise Chassis	39	Chassis	7
Management	Lenovo Flex System Chassis Management Module	45	Chassis Mgt Module	18
Compute Node	Lenovo Flex System x280 X6 (2S Only) Compute Node	49	x86 2S EX Node	14
	Lenovo Flex System x480 X6 (Scalable to 4S) Compute Node	56	x86 4S Scalable EX Node	23
	Lenovo Flex System x880 X6 (Scalable to 8S) Compute Node	56	x86 8S Scalable EX Node	23
Compute Node	Lenovo Flex System x440 Compute Node	38	x86 4S EP Node	14
Compute Node	Lenovo Flex System x240 Compute Node	38	x86 2S EP Node	14
Legacy (original IBM MTMs, IBM code support/website)				
Chassis	IBM Flex System Enterprise Chassis	36	Chassis	7
Management	IBM Flex System Chassis Management Module	43	Chassis Mgt Module	18

Table 63. NGP Flex OEM product names (continued)

Category (FRU/CRU)	STD base name	Bytes (length)	Generic OEM name	Bytes (length)
Compute Node	IBM Flex System x280 X6 (2S Only) Compute Node	46	x86 2S EX Node	14
	IBM Flex System x480 X6 (Scalable to 4S) Compute Node	53	x86 4S Scalable EX Node	23
	IBM Flex System x880 X6 (Scalable to 8S) Compute Node	53	x86 8S Scalable EX Node	23
Compute Node	IBM Flex System x440 Compute Node	35	x86 4S EP Node	14
Compute Node	IBM Flex System x240 Compute Node	35	x86 2S EP Node	14
Compute Node	IBM Flex System x220 Compute Node	35	x86 2S EN Node	14
Compute Node	IBM Flex System x222 Compute Node	35	x86 Dense 2S EN Node	20

Classes of settings

This topic explains classes and how they are used in the Advanced Settings Utility ASU.

For commands that support operating on multiple settings, classes are used to indicate groups of settings. The commands that support classes are **comparedefault**, **help**, **loaddefault**, **show**, **showdefault**, **showlocation**, and **showvalues**.

Classes

The ASU classes of settings are described in the following list:

all
This class includes all settings that are listed in the ASU for the Remote Supervisor Adapter or Remote Supervisor Adapter II, baseboard management controller, and BIOS.

authentication
This class includes all settings that are classified as authentication settings, such as passwords, user IDs, and authority-related settings.

The **save** and **restore** commands do not save or restore this class of settings.

You can list the user IDs and authority-related settings by using the **show** command.

You cannot list the password settings by using the show command. To list the password settings, use the **showvalues** command.

Example:

List the settings defined as authentication, including the password settings. Password settings are normally not displayed when you use the **show** command. To display the available password, use the **showvalues** command with the password class:

```
asu showvalues authentication
```

backupctl
This class lists all settings that are not restored when you run the **restore** command. An additional flag is required for these settings to be included during a restore operation. For more information, see the "Restore command" on page 124.

The class is used as a filter for the **show**, **showvalues**, **showdefault**, and **showlocation** commands.

To list the settings that are not restored if saved, type the following command:`asu show backupctl`

bios
This class includes all settings that match the installed BIOS code level.

bmc
This class includes all settings that are identified as baseboard management controller settings.

change
This class includes all settings that are not in the reboot class that can be changed safely and changed back before the system is restarted.

critical
This class includes all settings that you cannot change safely before a restart but that must be tested.

group
This class includes all settings that belong to the specified group. To view the supported groups, use the **showgroups** command.

Settings in BIOS-based servers and IMM-based servers are cataloged into classes or groups. If specified, the class is used as a filter for the command that is displaying or operating on the settings.

The class is used as a filter for the **show**, **showvalues**, **showdefault**, **showlocation**, **save**, **restore**, and **replicate** commands.

Examples:

To list the settings that are part of the IMM group (IMM-based servers), use:`asu show IMM`

To list the settings that are part of the BIOS group (BIOS-based servers), use:`asu show bios`

nochange
This class includes all changeable settings that are not in the reboot and change classes.

noreplicate
This class lists all settings that are not replicated when you run the **replicate** command. These settings are usually unique to each system.

The class is used as a filter for the **show**, **showvalues**, **showdefault**, and **showlocation** commands.

Example:

To list the settings that are not replicated, use:`asu show noreplicate`

password
This class lists all settings that are classified as password settings.

Password setting values are not displayed with the **show** command.

This class filter can be used with the following commands to list the settings classified as password: **showvalues**, **showdefault**, and **showlocation** (BIOS-based servers only) commands.

Example:

List the settings that are defined as password settings. Password settings are normally not displayed when you use the **show** command. To display the available password, use the **showvalues** command with the password class: `asu showvalues password`

rsa
This class includes all settings that are identified as Remote Supervisor Adapter and Remote Supervisor Adapter II settings.

readonly
This class includes all settings that are read-only (for example, settings that you cannot change).

reboot
This class includes all settings that can be changed safely before a restart. If changing a setting does not preclude starting from the hard disk drive on the next startup, the setting is in this class.

writeonly
This class includes all settings that are write-only (for example, settings that you can change but that cannot be read, such as passwords).

Setting interdependencies support on an IMM2-based system

Settings are now interdependencies that are supported on IMM2-based systems.

When you run the **show** and **set** commands, some settings are hidden or read-only because they are dependent on other settings. You can view the dependency information by using the **showvalues** command.

Example:

The setting BootModes.OptimizedBoot is hidden (suppressed) if the value of the setting BootModes.SystemBootMode is `Legacy Only`. If the value of the setting BootModes.SystemBootMode changes, the value is displayed. The dependency information is described in this **showvalues** command:

```
D:\asu>asu showvalues BootModes.OptimizedBoot --host 9.119.41.101 --user USERID
--password PASSW0RD
Lenovo Advanced Settings Utility version 9.00.76N
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 9.119.41.101
BootModes.OptimizedBoot=Disable=<Enable>
This setting is suppressed if the result of the following expression is true:
" BootModes.SystemBootMode == Legacy Only "
```

After modifying the setting BootModes.SystemBootMode to `Legacy Only`, you cannot display or set it. The output of the **show** command might look like the following:

```
D:\asu>asu show BootModes.OptimizedBoot --host 9.119.41.101 --user USERID
--password PASSW0RD
Lenovo Advanced Settings Utility version 9.00.76N
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 9.119.41.101
This setting cannot be shown because it is hidden!
```

The setting SystemRecovery.POSTWatchdogTimerValue is read-only if the setting SystemRecovery.POSTWatchdogTimer is disabled. The dependency information is shown here:

```
D:\asu>asu showvalues SystemRecovery.POSTWatchdogTimerValue --host 9.119.41.101
--user USERID --password PASSW0RD
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 9.119.41.101
SystemRecovery.POSTWatchdogTimerValue= numeric min=5 max=20 step=1 default=5
```

This setting is read-only if the result of the following expression is set to `true`:

```
SystemRecovery.POSTWatchdogTimer == Disable "
```

If you try to modify the value, the following output is displayed:

```
D:\asu>asu set SystemRecovery.POSTWatchdogTimerValue 7 --host 9.119.41.101
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 9.00.76N
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 9.119.41.101
This setting cannot be set because it is read-only!
```

Setting groups and setting values also have internal independencies. You cannot display or change them because they are hidden. When you use the **showvalues** command, some settings are marked with an asterisk. An asterisk means that the settings are not only dependent on other internal settings, but are also dependent on the system environment. You can modify these settings by using the uEFI **F1** menu. The following example shows sample output for the **showvalues** command:

```
D:\asu>asu showvalues Power.PowerPerformanceBias --host 9.125.90.191 --user USERID
--password PASSW0RD
Lenovo Advanced Settings Utility version 9.00.76N
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2012 All Rights Reserved
Connected to IMM at IP address 9.125.90.191
(*)Power.PowerPerformanceBias=<Platform Controlled>=OS Controlled
For more information about the settings marked with an asterisk (*),
refer to the ASU User's Guide.
```

Note: Only the **show** and **set** commands support setting interdependencies. Use the **showvalues** command to see the values of the dependency information. Other commands like **save**, **replicate**, **restore**, and **batch** ignore the dependencies restriction.

Command modifiers

This topic describes the command modifiers and the commands to which they apply.

Purpose

Command modifiers are optional. Use command modifiers to modify the default operation of specific commands.

Table 64. Command modifiers

Command modifier	Description	Syntax LAN over USB
--group	Optional command modifier for the **show**, **showdefault**, **showvalues**, **showlocation**,and **save** commands. When used with a supporting command, the modifier specifies the name of a group section. The group_name is obtained by running the **showgroups** command.	asu show [--group group_name] asu save [--group group_name] Obtain the group_name by running the following **showgroups** command: `asu showgroups`
--setlist	Optional command modifier for the **show**, **showdefault**, **showvalues**, **showlocation**, and **save** commands. When used with a supporting command, it is used to specify a list of settings on which the command operates.	asu show [--setlist name1 name2 nameN] asu save [--setlist name1 name 2 nameN]
--excbackupctl	Optional command modifier for the **save** command. Use this command modifier with the **save** command to exclude saving the backup control settings in a file. The default in a **save** command is to include all backupctl settings. To review the backupctl settings, use the `asu show backupctl` command. This command is mutually exclusive to the incbackupctl command modifier.	asu save file_name [--excbackupctl]

Table 64. Command modifiers (continued)

Command modifier	Description	Syntax LAN over USB
--incbackupctl	Optional command modifier for the **restore** command. Use this command modifier with the **restore** command to include the backup control settings. The backupctl settings are not restored by default. To review the backupctl settings, use the `asu show backupctl` command. This command is mutually exclusive to the excbackupctl command modifier.	asu save file_name [--incbackupctl]
--instances	Optional command modifier for the **showvalues** command. Use this command modifier with the **showvalues** command to show the names of settings that can have instances. This command is mutually exclusive to the group command modifier.	asu showvalues [--instances]
--help	Optional command modifier for all commands and applications. Use this command modifier to show the help text for an ASU command or application.	asu command | application --help

Command connectivity options

This topic describes the command connectivity options, which are a set of parameters that relate to the ASU connection on the IMM.

The connectivity options might be required when you connect the ASU to a local IMM. When you attempt to connect the ASU to a local IMM and none of the connectivity parameters are specified, the ASU attempts to connect to the IMM by using the default LAN over USB interface settings.

The default settings include user ID, password, and host. The values for these settings are defined by the IMM hardware. If none of these settings are specified on a local connection and the default LAN over USB interface settings fail, the ASU attempts to connect over the KCS interface. The KCS interface does not require any of these parameters.

To connect the ASU remotely to the IMM, also referred to as out-of-band way, the “host,” "user,” and ”password” must all be specified. Beginning with version 9.41, ASU will not provide a default user and password in out-of-band way.

ASU also supports connecting the ASU remotely to the IMM with the **mtsn** parameter, which is a string composed with “machine type and model” and “serial number” if the server running ASU and the IMM are in one LAN.

When **mtsn** is specified, the **net** parameter is optional. The **net** parameter is used to specify the network interface through which the ASU sends messages to a LAN.

If the **mtsn** and **net** parameters are specified, the ASU tries to search the target IMM whose machine type, model, and serial number are equal to the **mtsn** parameter in the LAN the network interface specified by the **net** parameter is in. If the **mtsn** parameter is specified and the **net** parameter is not specified, the ASU will try to search the target IMM whose machine type, model, and serial number are equal to the **mtsn** parameter in the LAN to which the server running ASU is linked.

If the server running ASU has more than one network interface that is linked to different LANs, ASU tries to search the target IMM in the LANs one by one. After the target IMM is found, ASU obtains the host IP address from the target IMM and tries to use it to connect to the IMM.

In the Linux version of ASU, the **net** parameter should be the name of the network interface, such as eth0, eth1, lo, and so on.

In the Windows version of ASU, the **net** parameter should be an integer that indicates the index of the network interface. You can use the command `arp -a` to get all of the indexes of the network interfaces that exist. For example, the information in the following table may be shown when you use the command: `arp -a`:

Table 65. Show network interface

Interface : 9.111.23.166 --- 0xc		
Internet address	**Physical address**	**Type**
9.111.23.1	00-00-0c-07-ac-01	dynamic
9.111.23.3	d4-d7-48-bc-82-40	dynamic
9.111.23.4	d4-d7-48-bc-a1-c0	dynamic
9.111.23.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.253	01-00-5e-7f-ff-fd	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static
Interface: 9.111.30.161 --- 0xf		
Internet address	**Physical address**	**Type**
9.111.30.1	00-00-0c-07-ac-01	dynamic
9.111.30.255	ff-ff-ff-ff-ff-ff	static
224.0.0.252	01-00-5e-00-00-fc	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Table 56 shows two interfaces whose indexes are 0xc and 0xf and whose IP addresses are 9.111.23.166 and 9.111.30.161, respectively. The indexes shown in Table 56 are in hexadecimal format. Before being input to ASU as the **--net** parameter, they should be transferred to decimal integers.

In the following example, the two decimal integers should be 12(0xc) and 15(0xf). If you want ASU to scan IMMs in the LAN to which the network interface 12 is linked, add `--net 12` to the list of parameters for the ASU command.

Command Example:

```
C:\asu>asu.exe show BootOrder.BootOrder --mtsn  791525Z06CNZ14 --net 10
--user USERID --password PASSW0RD
Lenovo Advanced Settings Utility version 9.41.__
Licensed Materials - Property of Lenovo
(C) Copyright Lenovo Corp. 2007-2013 All Rights Reserved
Searching for IMM's IP Address...
Round: 1
Round: 2
The Target IMM's IP Address is:9.111.66.95
Connected to IMM at IP address 9.111.66.95
BootOrder.BootOrder=Legacy Only=CD/DVD Rom=Hard Disk 0=Hard Disk 1=Hard Disk 2
```

The **mtsn** and **net** parameters are only suitable for IMM-based servers, not CMM, AMM, and Blade servers. They are also not suitable for ESXi. ASU supports the **mtsn** and **net** parameters in ASU version 9.41 and later. The commands supported by the **mtsn** and **net** parameters are listed below.

Command	Description
show	Display IMM server setting
set	Update IMM server setting
showdefault	Display IMM default server setting
showvalues	Display IMM values server setting
showgroups	Display IMM setting for server groups
batch	Execute several ASUcommands simultaneously
createuuid	Generate a UUID value and set it
Comparedefault	Compare the default value with the current value
delete	Delete an instance of a setting
deletecert	Delete an IMM certificate
export	Export an IMM certificate
generate	Generate a selected certificate
help	Show description for selected settings
import	Import a certificate into the IMM
loaddefault	Load the default value
rebootimm	Reboot IMM
replicate	Replicate settings saved in a settings file
restore	Restore settings saved in a settings file
save	Save all or some settings to a settings file
setenc	Apply an encrypted value to a setting

Any local or remote LAN over USB connection requires authentication. The default authentication parameters are the default user ID and password that come configured with each IMM. For the default authentication settings, see the documentation that comes with the server or optional devices.

Table 66. Command connectivity options

Connectivity option	**Description**	**Syntax**
host	Specifies the host name or IP address of the IMM to which the ASU should connect.	asu cmd [command_modifier] options --host host_name|ip asu cmd [command_modifier] options --host=host_name | ip
mtsn	Specifies the machine type and model and serial number of the IMM to which the ASU should connect	asu cmd [command_modifier] options --mtsn machinetype_model_ serialnumber asu cmd [command_modifier] options --mtsn=machinetype_model_serailnumber
net	When the **mtsn** parameter is specified, the **net** parameter is optional to specify the network interface of the server running ASU.	asu cmd [command_modifier] options --net network_interface asu cmd [command_modifier] options --net=network_interface
user	Specifies the user name to use when you are authenticating with the IMM.	asu cmd [command_modifier] options --user user_id asu cmd [command_modifier] options --user=user_id
password	Specifies the password to use when you are authenticating with the IMM.	asu cmd [command_modifier] options --password password asu cmd [command_modifier] options --password=password
password-file	Specifies the name of a file that contains the password to use when you are authenticating with the IMM.	asu cmd [command_modifier] options --password-file file_name asu cmd [command_modifier] options --password-file=file_name

Table 66. Command connectivity options (continued)

Connectivity option	Description	Syntax
kcs	Specifies to send commands by using the KCS IPMI interface only. This option requires the IPMI device driver. For more information, see "IPMI device driver support for Windows" on page 7 or "IPMI device driver support for Linux" on page 8. This option does not require authentication.	asu cmd [command_modifier] options --kcs

General command options

This section describes general command options, including bypass, dumptofile, -nx node, showsptraffic, silent, and help.

Bypass command option

Note: The bypass command option is not available for IMM-based servers.

If you try to run the **patchadd** command on a system on which a BIOS CMOS patch file is already installed in the BIOS ROM, and the definition file that you use has the same BIOS code level as the system, an error message is generated and the ASU is not modified. Also, if you issue the **patchremove** command and select the BIOS CMOS patch, an error message is generated, and the ASU does not remove this patch.

To add and use a BIOS CMOS definition patch file on a system in which the BIOS ROM has a BIOS CMOS patch with the same BIOS code level, use the bypass option (`--bypass`) at the end of the **asu** command.

```
asu  patchadd  GG16A.def --bypass
asu patchlist  --bypass
asu show all --bypass
```

When you run the **asu** command with the bypass option, the ASU ignores the BIOS CMOS patch information in the BIOS ROM.

dumptofile command option

Use the dumptofile option to redirect all output that is produced by the ASU to a log file.

Using the dumptofile command

The **dumptofile** option is inserted at the end of any ASU command.

The **dumptofile** option complements and is mutually exclusive with the silent option. When the **dumptofile** option is specified, the ASUruns in silent mode. All output that is produced by the ASU, whether informational or error logging, is redirected to a predefined log file. For Linux, the log file is `/asulog/asuout.log`. For Windows, the log file is `c:\asulog\asuout.log`, where `c` is the system drive as defined in Windows.

Output

The dumptofile option does not produce any additional output or filter any output that is normally produced by the ASU. It is a simple redirect to the predefined file.

Every time the ASU runs, the predefined file is initialized. All content from a previous ASU run is lost. There are no appends to the existing file from a previous run.

The predefined log file has no maximum file size. If during an ASU run the file reaches the maximum file system available space, any additional output is lost.

Examples

The following examples show the **asu** command with the dumptofile option.

Command	Description
`asu show all dumptofile`	This ASU command shows the current value for all settings and redirects the output to a predefined log file.
`asu set CMOS_CRTRequired Disabled dumptofile`	This ASU command sets the value, and all output is redirected to the predefined log file.

-nx node option

The -nx option supports multi-node systems. A multi-node system has multiple BIOS CMOS settings, Remote Supervisor Adapter settings, baseboard management controller settings for legacy systems, multiple uEFI settings, and IMM settings for IMM-based systems. The ASU enables you to access any node settings by adding the **-nx** parameter to the command (where *x* is the selected node).

Before you use the **-nx** option with a multi-node system that is running a Windows operating system, see “IPMI device driver support for Windows” on page 7. If the multi-node system is running a Linux operating system, see “IPMI device driver support for Linux” on page 8.

Syntax

If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system and is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1). The -nx option must be at the end of the command. If the --bypass option is also specified, the --bypass option must follow the node option. See the following examples.

```
asu show all -n3
```

This command shows the current value for all settings for node 3.

```
asu set CMOSCRTRequired Disabled
```

This command sets the CMOS setting to disabled for node 1.

```
asu rebootrsa -n1
```

This command restarts theRemote Supervisor Adapter node 1, which is the primary node.

```
asu patchadd GG16A.def -nx 2 --bypass
```

This command forces adding a patch to node 2.

When you run the **asu** command with the **--bypass** option, the ASU ignores the BIOS CMOS patch information in BIOS ROM.

showsptraffic command option

Note: The showsptraffic command option is not available for IMM-based servers.

Use the **showsptraffic** command option (--showsptraffic) to show raw traffic to and from the service processor (SP). Use this option for debugging.

Usage

The showsptraffic option can be inserted anywhere in any **asu** command. Any communication with the service processor is shown.

Output

When the showsptraffic option is specified on the command line, the following lines are interspersed with normal output:

```
SP Sent: <byte 1> <byte 2> ... <byte n>
SP Recv: <byte 1> <byte 2> ... <byte n>
```

Or

```
SP6 Sent: <byte 1> <byte 2> ... <byte n>
SP6 Recv: <byte 1> <byte 2> ... <byte n>
```

Examples

The showsptraffic option and corresponding output are shown in the following example.

Command line:

```
asu show RSA_SSL_Server_Enable --showsptraffic
```

Output:

```
SP Sent: 02 06 00 00 00 00 04 09 05 01 01 01
SP Recv: 04 06 01 00 00 00 04 09 05 01 01 01 00
RSA_SSL_Server_Enable=Disabled
```

Command line:

```
asu set RSA_SSH_Enable Enabled --showsptraffic
```

Output:

```
SP Sent: 00 06 01 00 00 00 04 09 05 01 04 01 01
SP Recv: 04 06 00 00 00 00 04 09 05 01 04 01
SP Sent: 02 06 00 00 00 00 04 09 05 01 04 01
SP Recv: 04 06 01 00 00 00 04 09 05 01 04 01 01
RSA_SSH_Enable=Enabled
```

silent command option

Use the silent command option to suppress all output.

Usage

The silent option can be inserted at the end of any ASU command. Any output that is produced by the ASU as either informational or error logging to screen is suppressed. To determine whether the command was successful, see the command return code.

Output

If the ASU command is successful, the return code is zero (0). If the ASU command is not successful, the return code is a positive number greater than zero. For information about the return codes, see "Return codes" on page 81.

Examples

In the following example, the ASU sets the value, and no output is produced to the screen or to a file.

```
asu set CMOS_CRTRequired Disabled --silent
```

--help command option

Use the **--help** command option to show command-line help.

Usage

The **--help** option can be used to give a full description of an ASU application (for example, savestat, immcfg or fodcfg) or ASU command (for example, **batch**, **set**, or **loaddefault**).

Output

The output is a full description of the ASU application or command, including available options and the description of those options. By running the command `asu --help` you can obtain details about the **--help** command option.

Examples

In the following command example, the ASU displays the full description of the **asu show** command.

Command line:

```
asu show --help
```

Output

Description:

You can view the current value for one or all settings. If <*setting*> is specified, the current value is shown for the setting only. If `--group all` is specified, current values are shown for all settings. If --group <*group*> is specified, then values are shown for settings in that group only. If `--setlist <setting1>...<settingN>` is specified, the list of settings from <*setting1*> to <*settingN*> are specified.

Syntax:

```
show [<setting>][<cmdmod>] [<options>] [<connect_opts>]
```

where

```
<cmd_mod>
```

Note: Use the command **`asu showgroups`** to find available variable classes.

Option	Description
--setlist <name 1>...<name n>	Operate commands on list of settings.
--group <variableclass>	Operate commands on the group of setting options.
--silent	Silent execution. Use the return code to retrieve status.
--dumptofile	Run silently and send output to `asuout .log` file.
-n<node>	Node number node in a multinode system.
-v	If the optional **`-v`** parameter is specified, the output is verbose.

Note: These connectivity options apply to IMM-based servers only:

Option	Description
--host <*ip*>	Address of the IMM to operate on.
--user <*user*>	User name used to authenticate to the IMM.
--password <*password*>	Password used to authenticate to the IMM.
--password-file <*file name*>	File containing password to authenticate with IMM.

ASU log file

This section provides information about the ASU log file.

Every time ASU is run, it generates a new log file in the log file directory.

On the Windows platform, the ASU log file directory is in `Lenovo_Support` under `system drive device`. On theLinux platform, the ASU log file directory is `/var/log/Lenovo_Support/`.

The ASU log file is named with the running time as `asu_%runningtime%.log`. Running time is formatted as *%Year%% Month%%Day%%Hour%%Minute %%Second%% Microsecond%% Timezone*%.

```
asu_20120827161042.593000+480.log
```

Return codes

This section lists and explains the return codes for both the ASU and RDCLI.

ASU return codes

The ASU categorizes failure return codes. This topic explains the ASU return codes and categories.

When the ASU completes a request successfully, it returns a return code of zero (`0`). If a failure is detected, the ASU return code is a positive number greater than zero.

The ASU assigns a specific failure return code for each type of error. Although a failure return code signals that a failure has been detected, it does not indicate a specific failure. To determine the specific error, refer to the return code explanation in the error message that is displayed.

The error codes are listed in the following table, along with brief descriptions of the possible reasons for the failure.

Table 67. ASU return codes

Return code value	Description	Explanation
0	Successful command	The ASU command has been completed successfully.
5	Input error	The input that was provided to the ASU has an error. The error can be related to either user input or the provided definition file.
10	Software error	An error occurred with the software being used.
15	Hardware error	An error occurred when the ASU tried to communicate with or find specific hardware.
20	Data error	An error occurred in the data that the ASU reads or sets.
25	Program error	An error occurred in the ASU program execution flow.
30	Invalid or missing patch detected	Either an ASU patch is missing or an ASU patch does not match the required level.
35	The command is not supported.	The command is not supported by ASU.
40	Invalid value input error	The input value that is provided to the ASU has a syntax error.
45	Batch command error	One or more of the commands that were specified in the batch file has failed.
80	32-bit version running on 64-bit operating system	The ASU application is a 32-bit version, and you are attempting to run it on a 64-bit operating system.

RDCLI return codes

This topic lists and describes the RDCLI return codes.

Table 68. RDCLI return codes

Return code value	Description	Explanation
0	Success.	The ASU command has been completed successfully.
1	Parameter is lacking.	The input parameters provided to the RDCLI are not enough for RDCLI.
2	Could not allocate memory.	The operating system failed to allocate enough memory for RDCLI to run.
6	Unknown option.	The input parameters provided to RDCLI have unknown options.
7	Unknown option character.	The input parameters contain some unknown characters.
10	No target path specified.	The input parameters do not provide the file path that you wanted to mount onto the IMM.
13	Error from ending the previous RDCLI process.	An existing RDCLI process on the current local machine failed to end.
14	Error from system call.	An error occurred while invoking an operation system call.
22	Invalid token.	An invalid token ended the process.
34	You failed to authenticate. Check your login information, IMM setting, and firewall status.	You did not pass authentication because either the information is incorrect or the wrong IMM configuration or an improper firewall status was entered. Check that they are all correct.
37	Socket error, socket connection failed.	A socket connection error occurred.
38	Could not reach the Service Processor IMM authentication site-check, hostname/IP/ports/the installation, of IMM remote disk key.	Some unknown errors occurred during the authentication process. Check all configurations and input.
44	Indicate a target IMM by hostname or IP address.	Provide a target IMM host name or IP address when issuing the RDCLI command.
59	You failed to mount remote disk. Check to see if others have already used the remote disk, and unmount their disk before mounting yours.	The local file was not mounted onto the IMM remote disk because the disk is occupied by another user.
60	The remote disk session stopped.	The connect session between the local computer and IMM are broken.
62	Specify a port argument to connect to the IMM Virtual Disk port.	Provide a port number to connect to IMM if you do not want to use the default port number.
63	No virtual drives found. Try again later.	No virtual drive on IMM is currently available.

Table 68. RDCLI return codes (continued)

Return code value	Description	Explanation
64	Local drive to remote drive attach failed.	The local file could not be mapped to the IMM remote disk.
65	Could not open target file.	The local file that you want to mount could not be opened.
66	Lack remote key. Install the key to activate the remote disk function.	The remote presence key has not been installed on IMM. You must install the key now.
67	There is already a link on that machine, so unmount first.	There is already a session mounting file on the same IMM as the local machine. Unmount the previous session before you issue a new RDCLI command.

Baseboard management controller startup sequence (boot order) settings

This topic describes the startup sequence settings for the baseboard management controller.

Note: The baseboard management controller startup sequence setting is not available for IMM-based servers.

If the startup sequence (boot order) settings for your LenovoSystem x Server are contained in the baseboard management controller and not in the BIOS CMOS memory, you must use the baseboard management controller settings when you use the **asu** commands (such as the **set** and **show** command).

To determine whether the startup sequence settings for your System x Server are contained in the baseboard management controller, use the ASU **patchextract** command. The **patchextract** command syntax is:`asu patchextract` *`patch_number patch_ filename`* where

the *patch_number* is the patch number for the BIOS code and *patch_ filename* is the generated extracted BIOS definition file.

Command line

`asu patchlist` - to determine which patch is the BIOS patch.

Output

```
Patch 1: <XX[00->99] <BMC>
Patch 2: <XX[00->99] <RSA>
Patch 3: <DY[14->14] <BIOS>
```

Command line

`asu patchextract 3 bios.def` - `bios.def` contains the bios definitions.

Output

```
Extracted patch 3: <DY[14->14] <BIOS>> to bios.def
```

Open the `bios.def` file and review the contents. If any of the settings start with BMCSetting (for example, BMCSetting BMC_PrimaryBootDevice2, "Second Primary Boot Device", critical,.....), the server startup sequence settings are contained in the baseboard management controller, and you must use the BMCSetting when you access the server startup sequence settings.

Note: Before you can access the baseboard management controller settings, the baseboard management controller device driver must be installed. For information about obtaining the device driver, see "Obtaining the ASU and patch files" on page 9.

Boot order settings for IMM-based servers

The boot order settings on IMM-based servers are a special group of settings. This topic describes those settings.

The boot order sequence is stored in the IMM and used by the server firmware during the startup process.

The following examples illustrate how to view the current settings and to set the boot order sequence. Each example shows a different connectivity option to illustrate the different methods of connectivity.

To determine the current boot order sequence, start by listing the settings that belong to the special boot-order group. The special group or class is currently defined as BootOrder.

To list the boot order settings using a local connection to an IMM:

```
asu show BootOrder
```

A sample output of the command:

```
BootOrder.BootOrder=CD/DVD Rom=Floppy Disk=Hard Disk
0=Network=Hard Disk 1=Hard Disk 2=Hard Disk 3
```

The setting that contains the boot order is called BootOrder.BootOrder. This output represents an ordered list. The syntax of an ordered list is:

```
value1=value2=valueN
```

The values that are separated by the equal sign (=) represent each of the items in the list. Therefore, this is the list of devices in the boot order.

The listed values are those devices that are currently set in the boot order. Additional devices might be available to be included in the boot order. To learn about all the available devices, use the **showvalues** command.

To list the devices that are available to be set by using the remote connection to an IMM and the default authentication for the BootOrder.BootOrder setting, type the following command:

```
asu showvalues BootOrder.BootOrder --host 9.5.51.207 --user USERID --password PASSW0RD
```

Sample output for this command:

```
BootOrder.BootOrder==CD/DVD Rom=Floppy Disk=Hard Disk
0=Network=Hard Disk 1=Hard Disk 2=Hard Disk 3=Hard Disk
4=USB Storage=Diagnostics=iSCSI=iSCSI Critical=Legacy
Only=Embedded Hypervisor
```

The list of devices is much larger than what is shown in the previous example. Note the double equal sign (==). It represents the values in an ordered list. You can select any of these values to build a new ordered list.

After all the possible values are known, you can build a new ordered list of values by using the **set** command.

To build a new boot order sequence by using the **set** command on a local IMM through the LAN over USB connection:

```
asu set BootOrder.BootOrder "Network=Hard Disk 1=USB
Storage=Diagnostics=iSCSI=iSCSI Critical=Legacy
Only=Embedded Hypervisor" --user testuser --password
testpwd
```

Each of the devices in the list in the specified order constitutes the new boot order sequence.

Sample output for this command:

```
BootOrder.BootOrder=Network=Hard Disk 1=USB
Storage=Diagnostics=iSCSI=iSCSI Critical=Legacy
Only=Embedded Hypervisor --user testuser --password
testpwd
```

Configuring iSCSI

The ASU supports setting iSCSI boot parameters. This section describes how to configure iSCSI settings.

The ASU is designed to configure iSCSI settings, which do not initially exist. This section describes the steps for creating and configuring the iSCSI settings.

Before you configure iSCSI boot parameters, read the following information:

- The iSCSI settings are grouped into a record. The record key for the record is the iSCSI.AttemptName setting. Each record represents an attempt. The term "attempt" is equivalent to the term "instance" that is defined for other settings.
- More than one attempt can be defined. In the examples in this section, all the settings that end with **.1** belong to the "first" attempt. The iSCSI.AttemptName.1 setting defines the name of the attempt group of settings.
- If more than one attempt is defined, the same setting names that define the attempt group are used, but each attempt contains a different instance number sequence.
- The iSCSI settings can be created by using the ASU **set** command on an instance of the iSCSI.AttemptName setting that does not already exist.
- The iSCSI settings can be deleted by using the ASU **delete** command on an instance of the iSCSIAttemptName setting. This command deletes all iSCSI settings for that instance because iSCSI instance settings are grouped as a record.
- The **iSCSI.InitiatorName** parameter is the only one defined as a global iSCSI setting to all attempts and does not require an instance index. This setting does not require the attempt index that all the other settings require. The initiator name is always defined as iSCSI.InitiatorName.
- The iSCSI parameters are defined in the iSCSI group of settings. To list the available iSCSI settings, type the following command:

  ```
  asu show iscsi
  ```

Single attempt group

The following example shows the list of settings if a single attempt group is defined. All setting names with the same instance .1 belong to the same attempt group:

```
iSCSI.InitiatorName

iSCSI.MacAddress.1
iSCSI.AttemptName.1
iSCSI.IscsiMode.1
iSCSI.ConnectRetryCount.1
iSCSI.ConnectTimeout.1
iSCSI.InitiatorInfoFromDhcp.1
iSCSI.LocalIp.1
iSCSI.SubnetMask.1
iSCSI.Gateway.1
iSCSI.TargetInfoFromDhcp.1
iSCSI.TargetName.1
iSCSI.TargetIp.1
iSCSI.TargetPort.1
iSCSI.BootLun.1
iSCSI.CHAPType.1
iSCSI.CHAPName.1
iSCSI.CHAPSecret.1
iSCSI.ReverseCHAPName.1
iSCSI.ReverseCHAPSecret.1

iSCSI.MacAddress.2
```

Two attempt groups

The following example shows the list of settings if two attempts are defined:

```
iSCSI.InitiatorName

iSCSI.MacAddress.1
iSCSI.AttemptName.1
iSCSI.IscsiMode.1
iSCSI.ConnectRetryCount.1
iSCSI.ConnectTimeout.1
iSCSI.InitiatorInfoFromDhcp.1
iSCSI.LocalIp.1
iSCSI.SubnetMask.1
iSCSI.Gateway.1
iSCSI.TargetInfoFromDhcp.1
iSCSI.TargetName.1
iSCSI.TargetIp.1
iSCSI.TargetPort.1
iSCSI.BootLun.1
iSCSI.CHAPType.1
iSCSI.CHAPName.1
iSCSI.CHAPSecret.1
iSCSI.ReverseCHAPName.1
iSCSI.ReverseCHAPSecret.1

iSCSI.MacAddress.2
iSCSI.AttemptName.2
iSCSI.IscsiMode.2
iSCSI.ConnectRetryCount.2
iSCSI.ConnectTimeout.2
iSCSI.InitiatorInfoFromDhcp.2
iSCSI.LocalIp.2
iSCSI.SubnetMask.2
iSCSI.Gateway.2
iSCSI.TargetInfoFromDhcp.2
iSCSI.TargetName.2
```

```
iSCSI.TargetIp.2
iSCSI.TargetPort.2
iSCSI.BootLun.2
iSCSI.CHAPType.2
iSCSI.CHAPName.2
iSCSI.CHAPSecret.2
iSCSI.ReverseCHAPName.2
iSCSI.ReverseCHAPSecret.2
```

IPv6 related settings in IMM

To be consistent with the web user interface, ASU requires that you enter a prefix for the IPv6 address.

The following is an example:

```
IMM.IPv6HostIPAddressWithPrefix1= 2002:325b:1000::097D:5AF5/64
```

where *64* is the address prefix for an IPv6 address.

You must enter a slash (/) in the setting string between the address and prefix.

Managing certificates for IMM-based systems

ASU can manage either the Certificate Authority (CA) or Certificate Sign Request (CSR) file on an IMM-based system. This section explains how to set up certificates for both Linux and Windows.

Signing a certificate sign request by using certificate authority

This topic describes how to use certificate authority to sign a certificate.

About this task

As an example, this topic uses `asu_csr.der` as your certificate sign request file.

Procedure

1. Export the certificate sign request file by issuing the following ASU command: `asu export SSL_LDAP_CLIENT_CSR asu_crs.der --host xx.xx.xx.xx --user USERID --password PASSW0RD`
2. Convert the certificate sign request format from `.der` to `.pem`. The following example uses the **openssl** command: `openssl req -in asu_csr.der -inform DER -out asu_csr.pem -outform PEM`
3. Sign the certificate sign request by using the certificate authority you just set up. The following example uses the **openssl** command: `openssl ca -policy policy_anything -out asu_cert.pem -infiles asu_csr.pem`
4. Convert the certificate format from `.pem` to `.der`. The following example uses the **openssl** command: `openssl x509 -in asu_cert.pem -inform PEM -out asu_cert.der –outform DER` The certificate sign request file is ready to import.
5. Import the certificate sign request file by using the ASU command `asu import SSH_SERVER_KEY asu_cert.der --host xx.xx.xx.xx --user USERID --password PASSW0RD`
6. Enter the command `Openssl x509 -in asu_cert.pem -inform PEM -out asu_cert.der –outform DER`. You receive the signed certificate`asu_cert.der` for your certificate sign request file `asu_csr.der`.

Revoking a certificate

This topic provides information about the command that you enter to revoke a signed certificate.

You cannot sign the same certificate sign request twice. You must revoke it before signing it again. Use the following command to revoke a certificate signed by this certificate authority.

```
openssl ca -revoke  cert.pem
```

Supported commands for IMM-based certificate management

This topic lists all supported ASU commands for certificate settings.

Table 69. Supported ASU commands for settings

Setting	Generate	Import	Export	Deletecert
SSL_HTTPS_SERVER_CERT	Y	Y	Y	N/A
SSL_HTTPS_SERVER_CSR	Y	N/A	Y	N/A
SSL_SERVER_DIRECTOR_CERT	Y	Y	Y	N/A
SSL_SERVER_DIRECTOR_CSR	Y	N/A	Y	N/A
SSL_LDAP_CLIENT_CERT	Y	Y	Y	N/A
SSL_LDAP_CLIENT_CSR	Y	N/A	Y	N/A
SSL_CLIENT_TRUSTED_CERT1	N/A	Y	Y	Y
SSL_CLIENT_TRUSTED_CERT2	N/A	Y	Y	Y
SSL_CLIENT_TRUSTED_CERT3	N/A	Y	Y	Y
SSH_SERVER_KEY	Y	N/A	N/A	N/A

Note: You can also view the supported commands for certificate settings by running the **Showvalues** command. On a command line, enter the following information:

```
asu showvalues IMM.SSL_HTTPS_SERVER_CERT
```

The following output is displayed:

```
IMM.SSL_HTTPS_SERVER_CERT=*generate=import=export
```

Disabling the corresponding server

Before you can manage a certificate on IMM, you must disable the HTTPS server, the Lenovo Systems Director, and the SSL Client Configuration for the LDAP client.

Procedure

1. Before using HTTPS Server Certificate Management, disable the HTTPS server:
   a. On a command line, check to see if the IMM HTTPS server configuration for the web server is disabled. Enter the command:`asu show IMM.SSL_Server_Enable` . The following output is displayed: `IMM.SSL_Server_Enable=Disabled`.
   b. If the server is enabled, disable the IMM HTTPS server configuration for the web server by using the command: `asu set IMM.SSL_Server_Enable Disabled`. The following output is displayed: `IMM.SSL_Server_Enable=Disabled`.

c. Restart the IMM to enforce the change (either enable or disable) by entering the **asu rebootimm** command.

2. Before using Lenovo Systems Director over HTTPS Certificate Management, disable the director over the HTTPS server:
   a. On a command line, enter the `asu show IMM. CIMXMLOverHTTPS_Enable` command to see if theLenovo Systems Director Over HTTPS is disabled. The following output is displayed: `IMM.CIMXMLOverHTTPS_Enable=Disabled`.
   b. If the server is enabled, disable Lenovo Systems Director Over HTTPS by using the `asu set IMM.CIMXMLOverHTTPS_Enable Disabled` command. The following output is displayed: `IMM.CIMXMLOverHTTPS_Enable=Disabled`.
   c. Restart the IMM to enforce the change (either enable or disable) by entering the **asu rebootimm** command.
3. Before using SSL Client Certificate Management, disable the SSL Client Configuration for the LDAP client:
   a. On a command line, check to see if the SSL Client Configuration for LDAP client is disabled by entering the `asu show IMM.SSL_Client_Enable` command. The following output is displayed: `IMM.IMM.SSL_Client_Enable=Disabled`.
   b. If the server is enabled, disable the IMM SSL Client Configuration for LDAP by using the `asu set IMM.SSL_Client_Enable Disabled` command. The following output is displayed: `IMM.SSL_Client_Enable=Disabled`.

Sample commands for using ASU to manage certificates

This topic provides sample commands for using ASU to manage certificates and responses received.

Getting the current status of the certificate setting

To view the status of a particular certificate, use the **asu show** command.

At the command line, enter the following command:

```
asu show IMM.SSL_HTTPS_SERVER_CERT
```

The output is:

```
IMM.SSL_HTTPS_SERVER_CERT=Private Key and CA-signed cert installed, Private Key stored, CSR available for download.
```

Getting the available command for the setting

Get supported commands for the related certificate setting by either running the **asu showvalues** command or by consulting the table of supported commands in “Feature on Demand configuration” on page 34.

At the command line, enter:

```
asu showvalues IMM.SSL_HTTPS_SERVER_CSR
```

The output is:

```
IMM.SSL_HTTPS_SERVER_CSR=*generate=export
```

You can tell from the output that the **generate** and **export** commands are supported for the setting `IMM.SSL_HTTPS_SERVER_CSR`.

Generating a Certificate Sign Request (CSR)

Use the following command to generate a CSR.

At the command line, enter:

```
asu generate IMM.SSL_HTTPS_SERVER_CSR asu.xml
```

The output is:

```
Certificate was generated successfully!
```

An `.xml` file, like `asu.xml` in this command, is required in the `generate` command for all settings that support "generate," except `SSH_SERVER_KEY`. For instructions about creating this `.xml` file, refer to the “Generate command” on page 105 section.

A certificate sign request must be signed by an independent certificate authority to be a certificate.

Generating a self-signed certificate

You can also use the ASU to generate a self-signed certificate, which is one that is already signed.

At the command line, enter:

```
asu generate IMM.SSL_HTTPS_SERVER_CERT asu.xml
```

The output is:

```
Certificate was generated successfully!
```

Exporting a certificate sign request

At the command line, enter:

```
asu export IMM.SSL_HTTPS_SERVER_CSR asu_csr.der
```

The output is:

```
Certificate was exported successfully!
```

The `asu_csr.der` file is saved in the current directory.

You can export a certificate or a certificate sign request. If a certificate sign request is signed by an independent certificate authority (CA), it is a CA-signed certificate.

Importing a certificate

After you export a certificate, you can get the certificate sign request file `asu_csr.der`. You must sign it by using an independent certificate authority. You can only import the CA-signed certificate, which is different than a self_signed one, into HTTPS Server Certificate Management and Lenovo Systems Director over HTTPS Certificate Management.

The following two settings for SSL Client Certificate Management permit only CA-signed certificates to be imported:

- SSL_LDAP_CLIENT_CERT
- SSL_LDAP_CLIENT_CSR

The following three settings allow both self-signed and CA-signed certificates to be imported:

- SSL_CLIENT_TRUSTED_CERT1
- SSL_CLIENT_TRUSTED_CERT2
- SSL_CLIENT_TRUSTED_CERT3

For settings SSL_CLIENT_TRUSTED_CERT1, SSL_CLIENT_TRUSTED_CERT2, and SSL_CLIENT_TRUSTED_CERT3, if the certificate already exists, you must delete it before importing the certificate.

On a command line, enter:

```
asu import IMM.SSL_HTTPS_SERVER_CERT asu_cert.der
```

The output is:

```
Certificate was imported successfully!
```

Note: asu_cert.der is a CA-signed certificate after asu_csr.der is signed using your own certificate authority.

Deleting a certificate

In SSL Client Certificate Management, only three settings support the **deletecert** command:

- SSL_CLIENT_TRUSTED_CERT1
- SSL_CLIENT_TRUSTED_CERT2
- SSL_CLIENT_TRUSTED_CERT3

On a command line, enter:

```
asu deletecert IMM.SSL_CLIENT_TRUSTED_CERT1
```

The output is:

```
Certificate was deleted successfully!
```

Remote Disk Command Line Interface

This topic describes the Remote Disk Command Line Interface (RDCLI) and provides examples for how to use it.

The RDCLI is designed to mount an ISO/DVD/CD to a remote IMM-based server. Before you invoke the RDCLI, make sure that:

- The remote IMM has been connected to your network environment.
- There is no other remote session open through RDCLI or the IMM web interface.
- The remote key is installed on the server and the remote function is enabled.

To mount a CDROM/ISO to a remote IMM:

```
rdmount -s 192.168.1.12 –d /dev/cdrom -l USERID -p PASSW0RD
rdmount -s 192.168.1.12 –d /home/install.iso -l USERID -p PASSW0RD
rdmount –s 192.168.1.12 –d /dev/cdrom -l USERID –p PASSW0RD –w 90
```

If a remote IMM has an IPv6 address:

```
rdmount -s 2002:325b:1000::097D:5AF5 –d /dev/cdrom -l USERID -p PASSW0RD
rdmount -s 2002:325b:1000::097D:5AF5 –d /home/install.iso -l USERID -p PASSW0RD
rdmount –s 2002:325b:1000::097D:5AF5 –d /dev/cdrom -l USERID –p PASSW0RD –w 90
```

2002:325b:1000::097D:5AF5 is an IPv6 address of IMM.

If the mount is successful, a message displays that the mount operation completed without error. Otherwise, a message states that the mount operation failed and provides details about the failure.

In the examples, `-w 90` means that you can switch the authentication port to `90`, the default port number is `80`. If you do not provide the **-w** parameter, RDCLI will use a default port of `80`.

Query the existing mount sessions between the client operating system and the remote server:

```
rdmount –q
```

The output lists all available tokens on the client operating system in the following format:

```
"Token 507 mounted to SP 192.168.0.1"
```

Unmount an ISO/DVD/CD that is already mounted to the remote system. For this example, the remote mount session has the token 507: `rdumount 507`.

If the action was successful, a message displays saying that the present remote session has ended. If the action failed, an error message and reason for the failure is printed.

Out-of-band configuration for blades on the Advanced Management Module (AMM)

ASU supports the configuration of blade settings through the out-of-band (OOB) mode. This section describes how to use it to configure blades on AMM.

The OOB configuration is designed to configure settings of blades on AMM. Before you use this function, ensure that the following requirements are met:

- The remote blades on AMM are connected to your network environment.
- The blade is an IMM-based server.
- Add the *--slot* argument to force ASU to connect with the remote AMM. If not, ASU will try to establish a connection with the provided IP address in an IMM out-of-band mode by default. And the *--slot* argument also can identify the blade'sIMM node bay.
- Add the *--host*, *--user* and *--password* connectivity options because it is on out-of-band mode.
  - *--host* provides the IP address of the remote AMM where the blade is.
  - *--user* and *--password* authenticate to the AMM.

Command Examples:

To show a remote blade uEFI setting: `asu show uefi --host x.x.x.x --user xxx --password xxx --slot x`

To set a remote blade setting, use: `asu set SETTING_NAME xxx --host x.x.x.x --user xxx --password --slot x --port 6090`

In the examples, *-- host x.x.x.x* is the IP address of the remote AMM, *--user xxx* and *--password xxx* are used to authenticate the connection, *--slot x* refers to the IMM node bay of the blade, and *--port* provides the port number for AMM chassis interface; the default is `6090`.

The commands supported by OOB configuration for blades on AMM are listed below.

Command	Description
show	Display IMM server setting
set	Update IMM server setting
showdefault	Display IMM default server setting
showvalues	Display IMM values server setting
showgroups	Display IMM setting for server groups
batch	Execute several ASUcommands simultaneously
createuuid	Generate a UUID value and set it
comparedefault	Compare the default value with the current value
delete	Delete an instance of a setting
help	Show description for selected settings
loaddefault	Load the default value
replicate	Replicate settings saved in a settings file
restore	Restore settings saved in a settings file
save	Save all or some settings to a settings file
setenc	Apply an encrypted value to a setting

Chapter 3. Using the commands

This section describes the Lenovo Advanced Settings Utility (ASU) commands.

The following commands are explained in this reference:

Batch command

Use the **batch** command to queue ASU operations without any knowledge of the scripting capabilities of the operating system on which the ASU is running.

Syntax

The syntax of the **batch** command is

```
asu batch batch_filename [-nx] [connect_options]
```

where

batch_filename is the name of a file that contains a list of ASU commands.

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system and is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. Do not specify the **-nx** optional parameter in the batch file for any of the batched commands.
3. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.
4. All consecutive **set** commands in a batch file are set synchronously, and the inconsecutive **set** command parts are set one by one. If an error occurs in one **set** command, all consecutive **set** commands also work, and the commands above the error are set successfully; only those below the error stop working.

Output

When you use the **batch** command on a batch file, the output that is sent to `stdout`, and `stderr` is the collective output of all the commands in the batch file. The output of each command in the batch file is preceded by the command itself, surrounded by brackets ([ ]), as shown in the following example:

```
[command 1]
output of command 1
[command 2]
output of command 2
```

•

```
•
•
[command n]
output of command n
```

The **batch** command and corresponding output are shown in the following examples.

Example 1

Batch file:

```
set IMM.PowerRestorePolicy "Always on"
set IMM.PowerOnAtSpecifiedTime_Hour 05
set IMM.PowerOnAtSpecifiedTime_Minute 00
set IMM.PowerOnAtSpecifiedTime_Second 00
set IMM.ShutdownAndPowerOff_WeekDay Sunday
set IMM.HTTPPort 81
set IMM.SSLPort 441
set IMM.TelnetPort 21
set SYSTEM_PROD_DATA.SysEncloseAssetTag "Server Tag"
set iSCSI.InitiatorName "iqn.2009-01.com.ibm:InitiatorName"
set uEFI.Com1BaudRate 9600
```

Output:

```
[set IMM.PowerRestorePolicy "Always on"]
IMM.PowerRestorePolicy=Always on
[set IMM.PowerOnAtSpecifiedTime_Hour 05]
IMM.PowerOnAtSpecifiedTime_Hour=05
[set IMM.PowerOnAtSpecifiedTime_Minute 00]
IMM.PowerOnAtSpecifiedTime_Minute=00
[set IMM.PowerOnAtSpecifiedTime_Second 00]
IMM.PowerOnAtSpecifiedTime_Second=00
[set IMM.ShutdownAndPowerOff_WeekDay Sunday]
IMM.ShutdownAndPowerOff_WeekDay=Sunday
[set IMM.HTTPPort 81]
IMM.HTTPPort=81
[set IMM.SSLPort 441]
IMM.SSLPort=441
[set IMM.TelnetPort 21]
IMM.TelnetPort=21
[set SYSTEM_PROD_DATA.SysEncloseAssetTag "Server Tag"]
SYSTEM_PROD_DATA.SysEncloseAssetTag=Server Tag
[set iSCSI.InitiatorName "iqn.2009-01.com.ibm:InitiatorName"]
iSCSI.InitiatorName=iqn.2009-01.com.ibm:InitiatorName
[set uEFI.Com1BaudRate 9600]
uEFI.Com1BaudRate=9600
```

Example 2

Batch file:

```
show CMOS_PrimaryBootDevice1
show CMOS_PrimaryBootDevice2
show CMOS_PrimaryBootDevice3
show CMOS_PrimaryBootDevice4
```

Output:

```
[show CMOS_PrimaryBootDevice1]
CMOS_PrimaryBootDevice1=CD ROM
[show CMOS_PrimaryBootDevice2]
CMOS_PrimaryBootDevice2=Diskette Drive 0
```

```
[show CMOS_PrimaryBootDevice3]
CMOS_PrimaryBootDevice3=Hard Disk 0
[show CMOS_PrimaryBootDevice4]
CMOS_PrimaryBootDevice4=Network
```

Example 3

Batch file:

```
set CMOS_PrimaryBootDevice1 "Network"
set CMOS_PrimaryBootDevice2 "Hard Disk 0"
set CMOS_PrimaryBootDevice3 "Diskette Drive 0"
set CMOS_PrimaryBootDevice4 "CD ROM"
```

Output:

```
[set CMOS_PrimaryBootDevice1 "Network"]
CMOS_PrimaryBootDevice1=Network
[set CMOS_PrimaryBootDevice2 "Hard Disk 0"]
CMOS_PrimaryBootDevice2=Hard Disk 0
[set CMOS_PrimaryBootDevice3 "Diskette Drive 0"]
CMOS_PrimaryBootDevice3=Diskette Drive 0
[set CMOS_PrimaryBootDevice4]
CMOS_PrimaryBootDevice4=CD ROM
{set CMOS_PrimaryBootDevice1]
CMOS_PrimaryBootDevice1=CD ROM
[show CMOS_PrimaryBootDevice2]
CMOS_PrimaryBootDevice2=Diskette Drive 0
[show CMOS_PrimaryBootDevice3]
CMOS_PrimaryBootDevice3=Hard Disk 0
[show CMOS_PrimaryBootDevice4]
CMOS_PrimaryBootDevice4=Network
```

Comparedefault command

Use the **comparedefault** command to compare current values to default values for one or more settings.

Syntax

The syntax of the **comparedefault** command is

```
asu comparedefault [setting | class] [-v] [-nx] [connect_options]
```

where

where *setting* is the name of an ASU setting, and *class* is the name of an ASU class of settings.

Notes

1. If the optional **-v** parameter is specified, the output is verbose.
2. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system, represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
3. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the

server running ASU and the target IMM-based servers are in one LAN. The `--user` *`user_id`* and `--password` *`password`* connect options are not required if you are using the local KCS interface.

Output

The output of the **comparedefault** command shows the current and default values for one or all settings, without the **-v** parameter:

```
<setting 1>=<current value 1><<default value1>>
<setting 2>=<current value 2><<default value2>>

•
•
•<setting n>=<current value n><<default valuen>>
```

With the **-v** parameter:

```
<setting 1>: <setting 1 description> = <current value 1>,
<default value 1> (default)
<setting 2>: <setting 2 description> = <current value 2>,
<default value 2> (default)

•
•
•
<setting n>: <setting n description> = <current value n>,
<default value n> (default)
```

The **comparedefault** command and corresponding output are shown in the following examples.

Example 1

Command line:

```
asu comparedefault uefi.com1baudrate
```

Output:

```
uEFI.Com1BaudRate=115200<115200>
```

Example 2

Command line:

```
asu comparedefault CMOS_PrimaryBootDevice1
```

Output:

```
CMOS_PrimaryBootDevice1=Network<CD ROM>
```

Example 3

Command line:

```
asu comparedefault CMOS_PrimaryBootDevice2 -v
```

Output:

```
CMOS_PrimaryBootDevice2: Second Startup Device = Network, CD
ROM (default)
```

Example 4

Command line:

```
asu comparedefault bios
```

Output:

```
CMOS_DisketteA=1.44 MB 3.5"<1.44 MB 3.5">
CMOS_CRTRequired=Disabled<Enabled>
```

•
•
•

```
CMOS_OSUSBControl=Other OS<Other OS>
```

Createuuid command

Use the **createuuid** command to generate and set the Universally Unique Identifier (UUID). This command is for IMM-based servers only.

Syntax

Note: When you set the UUID, the command requires the setting name. You can use the **asu show** command to identify the setting.

The syntax of the **createuuid** command is:

```
asu createuuid UUID_setting_name [connect_options]
```

Notes

1. The *UUID_setting_name* is usually defined as SYSTEM_PROD_DATA.SysInfoUUID.
2. To view the actual setting name, which can vary from server to server, use the **show** command to list the setting name that belongs to the SYSTEM_PROD_DATA group. To view the available groups, use the **showgroups** command.
3. The connect options are defined for IMM-based servers only. The --host *ip_address*, --user *user_id*, and --password *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The --mtsn, --net, --user, and --password options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The --user *user_id* and --password *password* connect options are not required if you are using the local KCS interface.

Output

To see the value that is set by the **createuuid** command, use the **show** command.

```
asu show SYSTEM_PROD_DATA.SysInfoUUID
```

The output of the show command is the new randomly-generated UUID.

```
SYSTEM_PROD_DATA.SysInfoUUID=801a3b663e82b60104af001a64e50c94
```

The **createuuid** command and corresponding output are shown in the following examples.

Command line:

```
asu createuuid SYSTEM_PROD_DATA.SysInfoUUID
```

Output:

The command does not produce output. To see the generated UUID, use the **show** command.

```
asu show SYSTEM_PROD_DATA.SysInfoUUID
SYSTEM_PROD_DATA.SysInfoUUID=801a3b663e82b60104af001a64e50c94
```

Delete command

Use the **delete** command to delete an instance of a setting. This command is for IMM-based servers only.

Syntax

Note: If you use this command to delete the instance of a setting that is a record key, all other settings with the same instance number are deleted.

The syntax of the **delete** command is

```
asu delete setting_instance [-nx] [connect_options]
```

where

setting_instance is the name of an instance of a setting to delete. Use the command **asu show all** to show a list of available setting instances.

Use the **asu showvalues** setting command to show a list of all values that are available for the setting.

Limitations

Settings can have a minimum number of allowed instances. The **delete** command does not allow you to delete an instance if doing so causes the number of instances to drop below the minimum number of allowed instances. To determine the minimum number of instances allowed, use the command:

```
asu showvalues --instances
```

The output for each setting that can have instances will be displayed, along with the minimum and maximum number of allowed instances.

Also, deleting instances that are part of a record is allowed for only the record key setting. To determine whether or not a setting is part of a record, use the command:

```
asu showvalues --instances
```

The output for each setting that can have instances will be displayed, along with the record information. See the “Showvalues command” on page 137 topic for details about the record information.

Notes

1. Values that contain spaces must be enclosed in quotation marks (" "). If a value contains quotation marks, add a backslash (\ ) before each quotation mark in the value.
2. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a

number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

3. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The **delete** command and corresponding output are shown in the following examples.

Deleting an existing instance

Command line:

```
asu delete IMM.Community_Name.1
```

Output:

```
Deleting IMM.Community_Name.1
Waiting for command completion status
Command completed successfully
```

Deleting an instance that does not exist

Command line:

```
asu delete IMM.Community_Name.3
```

Output:

```
Could not find setting IMM.Community_Name.3
```

Deleting an instance that causes the number of instances to drop below the minimum allowed number of instances

Command line:

```
asu delete IMM.MacAddress.1
```

Output:

```
The setting IMM.MacAddress.1 cannot be deleted.  Too few instances.
```

Deleting an instance that is in a record but is not the record key

Command line:

```
asu delete iSCSI.ConnectTimeout.1
```

Output:

```
The setting iSCSI.ConnectTimeout.1 is part of a record and cannot be
deleted. To delete the entire instance of the record you must
delete the record's key setting, iSCSI.AttemptName.1.
```

Deletecert command

Use the **deletecert** command to delete a certificate on IMM. This command is for IMM-based servers only.

Syntax

Note: Only Client Trusted Certificate setting is supported for this command. See "Supported commands for IMM-based certificate management" on page 88 to learn more about supported commands of settings.

The syntax of the **deletecert** command is

```
asu deletecert setting_[-nx] [connect_options]
```

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Deleting SSL Client Trusted Certificate 1

The **delete** command and corresponding output are shown in the following example.

Command line:

```
asu deletecert IMM.SSL_CLIENT_TRUSTED_CERT1
```

Output:

```
Certificate was deleted successfully!
```

Dump command

To see the raw contents of CMOS memory, use the **dump** command. This command is for BIOS-based servers only.

Syntax

The syntax of the **dump** command is

```
asu dump [-nx]
```

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **dump** command is a table that contains the current raw hexadecimal contents of CMOS memory. The CMOS memory setting area is preceded by an angle bracket (<) and followed by an angle bracket (>). CMOS memory locations that are outside the CMOS memory setting area are denoted by an asterisk (*). The ASU uses information from the CMOS memory map to determine how to access the second bank of CMOS memory. It also uses CMOS memory limit information from the map to determine the CMOS memory setting area.

The **dump** command and corresponding output are shown in the following example.

Command line:

```
asu dump
```

Output:

```
0 1 2 3 4 5 6 7 8 9 A B C D E F
00: 38*00*14*00*10*00*01*07*07*03*26*02*50*80<00 00
10: 40 00 00 7e 01 80 02 ff ff 00 00 f2 00 86 c0 c8
20: 60 00 00 00 00 00 00 00 00 00 00 02 27 50 07 18
30: ff ff 20 05 0d 06 00 00 c0 00 f0 ff 00 ca 00 00
40: 00 00 00 00 00 00 00 00 00 00 00 20 52 00 00 60
50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24
70: 10 42 08 21 00 00 81 4a 2a 00 2e 28 00 30 00 00
80: 00 00 ff 01 00>00*00*00*00*00*00*00*00*00*00*00
90: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
a0: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
b0: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
c0: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
d0: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
e0: 00*00*00*00*00*00*00*00*00*00*00*00*00*00*00*00
f0: 00*00*00*32*08*9c*00*62*90*5c*cd*ff*4f*5f*ba*9f
```

Encrypt command

Use the **encrypt** command to encrypt a setting value.

Syntax

The value that you encrypt can be any valid string. If the value contains spaces, it must be enclosed in double quotation marks (" ") so that you can use the encrypted value in the **setenc** command.

The syntax of the **encrypt** command is

```
asu encrypt <value>
```

where

value is the valid value of an ASU setting.

Output

The output of the **encrypt** command shows the encrypted string of data that you enter. For example, if you enter `value`, the output is `s56RrL6`.

The **encrypt** command and corresponding output are shown in the following examples.

Command line:

```
asu encrypt "something to input"
```

Output:

```
pzMRbH7QfvsPWGtRWacRmL7T
```

Command line:

```
asu encrypt something_to_input
```

Output:

```
pzMRbH7QfvsPWGtRWacRmL7T
```

Export command

Use the **export** command to export a selected certificate or certificate sign request (CSR) file.

Syntax

This **export** command is only for the Remote Supervisor Adapter and Remote Supervisor Adapter II and IMM. Specially, out-of-band mode of the command is supported only for IMM. This command fails if the certificate or certificate sign request is not available in the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM.

The **export** command generates a binary file that is saved in the current directory.

The syntax of the **export** is

```
asu export setting certificate_binary_file [-nx] [connect_options]
```

where

setting is the name of a valid ASU setting and *certificate_binary_file* is the name of a file that is generated with the valid certificate information that is provided by the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM.

Note: To learn more about supported commands of settings for IMM-based servers, see "Supported commands for IMM-based certificate management" on page 88.

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system and is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the

server runningASU and the target IMM-based servers are in one LAN. The `--user user_id` and `--password password` connect options are not required if you are using the local KCS interface.

Output

The output of the **export** command is a binary file and a message that indicates that the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM completed the command successfully.

The **export** command and corresponding output are shown in the following example.

Exporting a certificate from RSA

Command line:

```
asu export RSA_SSL_Client_PrivateKey_Export asu.cert
```

Output:

```
Certificate was exported to the file successfully!
( asu.cert file is saved in the current directory)
```

Exporting a certificate sign request file from IMM

The IMM external IP address is 9.5.51.37.

Command line:

```
asu export IMM.SSL_HTTPS_SERVER_CSR asu.cert --host 9.5.51.37 --user USERID
--password PASSW0RD
```

Output:

```
Certificate was exported successfully!
( asu.cert file in saved in the current directory)
```

Generate command

Use the **generate** command to generate a private key and public key pair with a self-signed certificate or a certificate sign request.

The **generate** command is targeted to only the Remote Supervisor Adapter, Remote Supervisor Adapter II, and IMM. Specially, out-of-band mode of the command is supported for IMM only. The **generate** command generates a private key and public key pair with a self-signed certificate or certificate sign request (CSR). The generation can take a few seconds to complete, depending on the state of the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM.

The **generate** command requires an Extensible Markup Language (XML) file that contains the certificate information that you want in the directory from which the ASU is running. When you extract the ASU files, a template file (`template.xml`) is extracted. This file provides an XML file with the correct syntax. Modify this XML file with the information you need to generate the selected certificate.

To learn more about supported commands of settings for IMM-based servers, see "Supported commands for IMM-based certificate management" on page 88.

Note: The XML file supports the self-signed certificate request and the certificate sign request (CSR). The start and end tag for the self-signed certificate is `new_key_and_self_signed_cert_info`. The start and end tag for a certificate sign request is `new_key_and_cert_sign_req_info`.

Template.xml

```
<?xml version="1.0" encoding="utf-8"?>
<asu version="2.1">
 <new_key_and_self_signed_cert_info>
   <item type="Required">
    <vectorID>0001</vectorID>
    <name>countryName</name>
    <value minlen="2" maxlen="2">xx</value>
   </item>
   <item type="Required">
    <vectorID>0001</vectorID>
    <name>stateOrProvinceName</name>
    <value minlen="1" maxlen="30">xx</value>
   </item>
   <item type="Required">
    <vectorID>0001</vectorID>
    <name>localityName</name>
    <value minlen="1" maxlen="50">xx</value>
   </item>
   <item type="Required">
    <vectorID>0001</vectorID>
    <name>organizationName</name>
    <value minlen="1" maxlen="60">xx</value>
   </item>
   <item type="Required">
    <vectorID>0001</vectorID>
    <name>commonName</name>
    <value minlen="1" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>Name</name>
    <value minlen="1" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>emailAddress</name>
    <value minlen="1" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>validityPeriod</name>
    <value minlen="0" maxlen="2">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>organizationalUnitName</name>
    <value minlen="0" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>Surname</name>
    <value minlen="0" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>givenName</name>
    <value minlen="0" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
```

```
   <name>Initials</name>
   <value minlen="0" maxlen="20">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>dnQualifier</name>
   <value minlen="0" maxlen="60">xx</value>
  </item>
</new_key_and_self_signed_cert_info>
<new_key_and_cert_sign_req_info>
  <item type="Required">
   <vectorID>0001</vectorID>
   <name>countryName</name>
   <value minlen="2" maxlen="2">xx</value>
  </item>
  <item type="Required">
   <vectorID>0001</vectorID>
   <name>stateOrProvinceName</name>
   <value minlen="1" maxlen="30">xx</value>
  </item>
  <item type="Required">
   <vectorID>0001</vectorID>
   <name>localityName</name>
   <value minlen="1" maxlen="50">xx</value>
  </item>
  <item type="Required">
   <vectorID>0001</vectorID>
   <name>organizationName</name>
   <value minlen="1" maxlen="60">xx</value>
  </item>
  <item type="Required">
   <vectorID>0001</vectorID>
   <name>commonName</name>
   <value minlen="1" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>Name</name>
   <value minlen="1" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>emailAddress</name>
   <value minlen="1" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>organizationalUnitName</name>
   <value minlen="0" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>Surname</name>
   <value minlen="0" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>givenName</name>
   <value minlen="0" maxlen="60">xx</value>
  </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
 </item>
  <item type="Optional">
   <vectorID>0001</vectorID>
   <name>Initials</name>
   <value minlen="0" maxlen="20">xx</value>
```

```
   </item>
   <item type="Optional">
    <vectorID>0001</vectorID>
    <name>dnQualifier</name>
    <value minlen="0" maxlen="60">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0002</vectorID>
    <name>challengePassword</name>
    <value minlen="6" maxlen="30">xx</value>
   </item>
   <item type="Optional">
    <vectorID>0002</vectorID>
    <name>unstructuredName</name>
    <value minlen="1" maxlen="60">xx</value>
   </item>
 </new_key_and_cert_sign_req_info>
</asu>
```

Table 70. Explanation of XML

Item	Description
Country name	The two-letter ISO abbreviation for your country.
State or Province name	The state or province where your organization is located. Do not abbreviate.
Locality name	The city where your organization is located.
Organization name	The exact legal name of your organization. Do not abbreviate.
Common name	A fully qualified domain name that resolves to the SSL VPN device. For example, to secure the URL `https://ssl.yourdomain.com`, the common name of the certificate sign request should be `ssl.yourdomain.com`.
Name	Optional field for entering a contact name.
Email address	Optional field for entering a contact email address.
Organization unit name	Optional field for the name of the unit in your organization.
Surname	Optional field for entering the surname of a contact person.
givenName	Optional field for entering the given name of a contact.
Initials	Optional field for entering the initials of a contact name.
dnQualifier	Optional field for entering the domain name qualifier.
Challenge password	Optional attribute. If you specify a challenge password in the certificate sign request, you must know the challenge password if you want to revoke the certificate later.
unstructuredName	Optional field for entering the unstructured name for a contact.

Notes

1. The *xx* field requires user input. The minimum length for each vector (item) is identified by `minlen=`, and the maximum length is identified by `maxlen=`. For example, for the vector named `stateOrProvinceName`, the `minlen` is 1, the `maxlen` is 30, and a valid *xx* value is `Vermont`.
2. Items that are identified as "Required" have to be updated with user data. Items that are identified as "Optional" do not have to be updated. If the optional items are not updated, remove them from the XML file.

3. The ASU requires that you provide the XML file with the correct data for the **generate** command to run correctly.

Syntax

The syntax of the generate command is

```
asu generate setting xml_file [-nx] [connect_options]
```

where

setting is the name of a valid Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM setting, and *xml_file* is the name of an XML file that contains valid information.

When generating a SSH key in IMM, the syntax of the **generate** command is

```
asu generate setting [-nx] [connect_options]
```

because the *xml_file* is not required for generating an SSH key.

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The output of the **generate** command is a message that indicates that the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM has completed the command successfully.

The **generate** command for a self-signed certificate and corresponding output are shown in the following example.

Command

Command line:

```
asu generate RSA_Generate_SSL_Client_Certificate asu.xml
```

Output:

```
Certificate was generated successfully!
```

Command line:

```
asu generate IMM.SSL_HTTPS_SERVER_CERT asu.xml
```

Output:

```
Certificate was generated successfully!
```

The **generate** command for a certificate sign request certificate and corresponding output are shown in the following example:

Command line:

```
asu generate IMM.SSL_HTTPS_SERVER_CSR asu.xml
```

Output:

```
Certificate was generated successfully!
```

The **generate** command for SSH Key and corresponding output are shown in the following example:

Command line:

```
asu generate IMM.SSH_SERVER_KEY
```

Output:

```
Certificate was generated successfully!
```

Help command

Use the **help** command to view help information for one or more settings. For BIOS settings, this command provides the same help that you access when you press **F1** during startup.

Syntax

The syntax of the **help** command is

```
asu help [setting | class] [connect_options]
```

where

setting is the name of an ASU setting and *class* is the name of an ASU class of settings.

Note: The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The output of the **help** command shows the help text for one or more settings. The name and description of the setting are followed by the help title and the help text.

```
<setting 1>: <setting description 1>
<help title 1>
--------------
<help text 1>
<setting 2>: <setting description 2>
<help title 2>
--------------
```

```
<help text 2>

•
•
•
<setting n>: <setting description n>
<help title n>
--------------
<help text n>
```

The **help** command and corresponding output are shown in the following examples.

Command line:

```
BootOrder.BootOrder: Boot Order
Help for Boot Order
-------------------
```

Output:

```
Specify, from the list of bootable devices, the desired order in which
to search for bootable media.  One or more items from the list may be
specified.
```

Command line:

```
 asu help CMOS_PrimaryBootDevice3
```

Output:

```
CMOS_PrimaryBootDevice3: Third Startup Device

Help for Startup Device
-----------------------
The system uses a startup sequence to determine which device
will be the startup device. The startup device is the
diskette drive, hard disk, or network adapter which will be used
to load the operating system. This field specifies the third
device for which a system start will be attempted. If the
start from this device fails, the system will attempt to
start from the fourth startup device.
```

Command line:

```
asu help bios
```

Output:

```
CMOS_DisketteA: Diskette Drive A

Help for Diskette Drive
-----------------------
If you change or add a diskette drive, you might need to
use this option to set the correct type.

CMOS_CRTRequired: Displayless Operation
Help for Displayless Operation
------------------------------
This option suppresses the error messages that
normally occur when no video device is present.

•
•
•
CMOS_OSUSBControl: OS USB Selection
```

```
Operating System USB Support
----------------------------
Choose which operating system you will be using
for RSA II USB support.
```

Import command

Use the **import** command to import a certificate into the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM.

Syntax

The **import** command is targeted to a Remote Supervisor Adapter, Remote Supervisor Adapter II or IMM. Use the command to import a certificate into the Remote Supervisor Adapteror Remote Supervisor Adapter II command or IMM. Out-of-band mode of the command is supported for IMM only. The **import** command requires a binary certificate file that is in the same directory from which the ASU is running.

You are only allowed to import the CA-signed certificate (it differs from self-signed) into the HTTPS Server Certificate Management and Lenovo Systems Director over HTTPS Certificate Management section.

For the section SSL Client Certificate Management, the first two settings `SSL_LDAP_CLIENT_CERT` and `SSL_LDAP_CLIENT_CSR`,

also only permit CA-signed certificates to be imported. But for the other three settings shown below, both self-signed and CA-signed certificates can be imported:

- SSL_CLIENT_TRUSTED_CERT1
- SSL_CLIENT_TRUSTED_CERT2
- SSL_CLIENT_TRUSTED_CERT3

The certificate to be imported should be in the `.der` format. If you want to set up your own independent certificate authority and sign your certificate sign request file, see “Managing certificates for IMM-based systems” on page 87 to set up a certificate authority and sign a certificate sign request.

Note: See “Supported commands for IMM-based certificate management” on page 88 to learn more about supported commands of settings for IMM-based servers. For the following settings, if the certificate already exists, you must delete it before you import the certificate:

```
SSL_CLIENT_TRUSTED_CERT1
SSL_CLIENT_TRUSTED_CERT2
SSL_CLIENT_TRUSTED_CERT3
```

The syntax of the **import** command is

```
asu import setting certificate_binary_file [-nx] [connect_options]
```

where

setting is the name of an ASU setting and *certificate_binary_file* is the name of a file that is generated with the valid certificate information.

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. It is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The output of the **import** command is a message that indicates that the Remote Supervisor Adapter, Remote Supervisor Adapter II, or IMM has completed the command successfully.

You can import the signed certificate in `.der` format only. See "Managing certificates for IMM-based systems" on page 87 to set up a certificate authority and sign a certificate sign request to learn about how to set up your own CA.

The **import** command and corresponding output are shown in the following examples.

Command line:

```
asu import RSA_Import_Trusted_Certificate_1 asu.cert
```

Output:

```
Certificate was imported successfully!
```

Command line:

```
 asu import IMM.SSL_HTTPS_SERVER_CERT asu.cert
```

Output:

```
Certificate was imported successfully!
```

Loaddefault command

Use the **loaddefault** command to load default values for one or more settings.

Limitations

Note the following limitations related to the **loaddefault** command.

- Not all settings in the definition or configuration file have assigned default values.
- The **loaddefault** command sets the default settings for only the settings that have defined default values in the configuration file.
- On BIOS-based servers, the **loaddefault** command should not be viewed or used as a general restore factory defaults command.

- On IMM-based servers, when the **loaddefault** command is run remotely (using the --host connectivity option) the authentication and password class settings are not applied.
- On IMM-based servers that are running the ASU 3.00, the **loaddefault** command is not functionally equivalent to the Restore Defaults function that is defined in the IMM web interface. You have to use the IMM web interface or the server Setup utility settings to restore the IMM settings to the factory defaults.
- On IMM-based servers that are running the ASU 3.01 or later (and have the required IMM firmware that is described in Chapter 1, "Using the Advanced Settings Utility," on page 1 to configure settings in IMM-based servers), the **loaddefault** command is now functionally equivalent to the Restore Defaults function that is defined in the IMM web interface. Settings from other groups are still not the equivalent of the Restore Factory Defaults function that is available through the server Setup utility (the **F1** option).

Note: For the ASU 3.01, some instances are deleted when you run the **loaddefault** command. To determine which instances are deleted, use the **showdefault** command. Instances that have a default value of remove are deleted.

The following example shows the**showdefault** command being used on a setting that has a default action of remove, and the **loaddefault** command then being used on the setting.

Command line:
```
asu showdefault IMM.LoginId.7
```

Output:
```
IMM.LoginId.7=<remove>
```

Command line:
```
 asu loaddefault IMM.LoginId.7
```

Output:
```
Could not find setting IMM.LoginId.7
```

Syntax

The syntax of the **loaddefault** command is
```
asu loaddefault [setting | class] [-v] [-nx] [connect_options]
```

where

setting is the name of an ASU setting and *class* is the name of an ASU class of settings.

Notes

1. If the optional **-v** parameter is specified, the output is verbose.
2. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
3. The connect options are defined for IMM-based servers only. The --host *ip_address*, --user *user_id*, and --password *password* connect options are all required if you connect remotely to the IMM. The default user and password

will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *`user_id`* and `--password` *`password`* connect options are not required if you are using the local KCS interface.

Output

The output of the **`loaddefault`** command is displayed if a setting is changed to the default value. If a setting is already set to the default value, no output is displayed. If a setting is not already set to the default value, the value is changed, and the output is shown as the output of the **`set`** command.

Note: Starting with the ASU 3.01, there are exceptions on IMM-based servers. Performing the **`loaddefault`** command on a group of settings (for example, `IMM`, `UEFI`, `SYSTEM_PROD_DATA`, `BOOT_ORDER`, and `all`) can trigger a reset to factory defaults. If the group is being reset to factory defaults, the setting names and their new values are not displayed. Instead, the ASU displays the message `Issuing reset of IMM`.

Without the *-v* parameter:

```
<setting 1>=<default value 1>
<setting 2>=<default value 2>

•
•
•
<setting n>=<default value n>
```

With the *-v* parameter:

```
<setting 1>: <setting 1 description> = <default value 1>
<setting 2>: <setting 2 description> = <default value 2>

•
•
•
<setting n>: <setting n description> = <default value n>
```

The **`loaddefault`** command and corresponding output are shown in the following examples.

Command line:

```
asu loaddefault uEFI.Com1BaudRate
```

Output:

```
uEFI.Com1BaudRate=115200
```

Command line:

```
asu loaddefault CMOS_CRTRequired
```

Output:

```
CMOS_CRTRequired=Enabled
```

Command line:

```
asu loaddefault CMOS_KbdRequired -v
```

Output:

```
CMOS_KbdRequired: Keyboardless Operation = Enabled
```

Command line:

```
asu loaddefault bios
```

Output:

```
CMOS_DisketteA=1.44 MB 3.5"
CMOS_CRTRequired= Enabled
CMOS_WakeOnLAN=Enabled
```

Command line (IMM-based servers with ASU 3.01 or later):

```
asu loaddefault IMM
```

Output:

```
Issuing reset of IMM
The IMM has started the reset. Waiting for the reset to complete.
Connected to IMM at IP address 169.254.95.118
Reset completed successfully
```

Command line (IMM-based servers with ASU 3.01 or later):

```
asu loaddefault all
```

Output:

```
Connected to IMM at IP address 9.5.107.158
SYSTEM_PROD_DATA.SysInfoProdName=
SYSTEM_PROD_DATA.SysInfoProdIdentifier=
SYSTEM_PROD_DATA.SysInfoSerialNum=
SYSTEM_PROD_DATA.SysInfoUUID=
SYSTEM_PROD_DATA.SysEncloseAssetTag=
uEFI.TurboModeEnable=Disable
uEFI.OperatingMode=Custom Mode
.
.
.
Issuing reset of IMM
The IMM has started the reset. Waiting for the reset to complete.
Connected to IMM at IP address 169.254.95.118
Reset completed successfully
```

Patchadd command

Use the **patchadd** command to add support for a particular firmware setting to the ASU. This command is for BIOS-based servers only.

Depending on the system from which you are running this command, a BIOS patch might not be added because the BIOS patch is already contained in the BIOS ROM.

Syntax

The syntax of the **patchadd** command is

```
asu patchadd patch_filename
```

where

patch_filename is the name of a patch file. For a description of the patch file format, see "About ASU patch files" on page 10.

Output

The output of the **patchadd** command shows the success or failure of adding a patch. If the patch is successfully added, a message is shown indicating that a new patch was written to the executable file, and information about the patch is provided. If the patch could not be added, a message is shown indicating why the patch failed.

If the patch command is successful, the output looks similar to this example:

```
Wrote new patch <<patch identification>> to <executable>
Wrote patch footer to <executable>
```

If the patch command is not successful, the output looks similar to this example:

```
<<patch identification>> already patched.
Wrote patch footer to <executable>
```

The **patchadd** command and corresponding output are shown in the following examples.

Successful patch

Command line:

```
asu patchadd T2C125A.def
```

Output:

```
Wrote new patch <T2[25->25] (BIOS)> to ./asu
Wrote patch footer to ./asu
```

System BIOS already has a patch

Command line:

```
asu patchadd T2C125A.def
```

Output:

```
BIOS def file already defined in BIOS ROM!
```

Patchextract command

Use the **patchextract** command to extract a patch from the ASU to a patch file. This command is for BIOS-based servers only.

You can patch the extracted patch file to another version of the ASU by using the **patchadd** command.

Syntax

The syntax of the **patchextract** command is

```
asu patchextract patch_number patch_filename
```

where

patch_number is the patch number to extract and *patch_filename* is the name of the patch file that is extracted.

To show the patch number for each patch, use the **patchlist** command.

Output

The output of the **patchextract** command shows the success or failure of the extraction operation. If the extraction is successful, a message is displayed indicating which patch was extracted and the name of the file to which it was extracted.

```
Extracted patch <patch number>: <<patch identification>> to <patch filename>
```

The **patchextract** command and corresponding output are shown in the following example.

Command line:

```
 asu patchextract 1 T2.def
```

Output:

```
Extracted patch 1: <T2[25->25] (BIOS)> to T2.def
```

Patchlist command

Use the **patchlist** command to display the patches that are applied to the ASU. This command is for BIOS-based servers only.

Syntax

The syntax of the **patchlist** command is

```
asu patchlist
```

Output

The output of the **patchlist** command is a list of patches. Each patch has a patch number and patch identification.

```
Patch <patch number 1>: <<patch identification 1>>
Patch <patch number 2>: <<patch identification 2>>
•
•
•
Patch <patch number n>: <<patch identification n>>
```

The **patchlist** command and corresponding output are shown in the following example.

Command line:

```
 asu patchlist
```

Output:

```
Patch 1: <T2[25->25] (BIOS)>
Patch 2: <GE[00->99] (RSA)>
Patch 3: <GE[46->46] (BIOS)>
```

Patchremove command

Use the **patchremove** command to remove a patch from the ASU. This command is for BIOS-based servers only.

Depending on the system from which you are running the **patchremove** command, the BIOS patch might not be removed because the patch is contained in the BIOS ROM.

Syntax

The syntax of the **patchremove** command is

```
asu patchremove patch_number
```

where

patch_number is the patch number to extract. Use the **patchlist** command to show the patch number for each patch.

Output

The output of the **patchremove** command shows the outcome of the removal operation. If the removal is successful, messages are displayed that indicate the removal of a patch and the copy of each patch to the temporary executable file.

```
Copied patch <<patch identification>> to <temporary executable>
Removing patch <<patch identification>> from <executable>
```

The **patchremove** command and corresponding output are shown in the following examples.

Command line:

```
 asu patchremove 2
```

Output:

```
Copied patch <T2[25->25] (BIOS)> to smep2tmp-9yFPOa
Removing patch <GE[00->99] (RSA)> from ./asu
```

The **patchremove** command is attempting to remove a BIOS patch that is in BIOS ROM, and the corresponding output is shown in the following example.

Command line:

```
asu patchremove 3
```

Output:

```
Cannot remove patch in BIOS ROM, patch <T2[25->25]. (BIOS)> is not removed.
```

Readraw command

Use the **redraw** command to read raw CMOS data and save it in a file to use on other systems by using the **writeraw** command. This command is for BIOS-based servers only.

Syntax

The syntax of the **redraw** command is

```
asu readraw filename [-nx]
```

where

filename is the name of a file to which the raw CMOS data is saved.

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **readraw** command is a message that indicates that the raw read operation is completed.

Command line:

```
asu readraw CMOSraw.dat
```

Output:

```
Raw CMOS read from CMOS, written to CMOSraw.dat
```

Rebootbmc command

Use the **rebootbmc** command to restart the baseboard management controller. This command is for BIOS-based servers only.

This command is useful because the system must be restarted after you make changes to baseboard management controller settings.

Syntax

The syntax of the **rebootbmc** command is

```
asu rebootbmc [-nx]
```

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **rebootbmc** command is a message that indicates that the restart of the baseboard management controller is completed.

The **rebootbmc** command and corresponding output are shown in the following example.

Command line:

```
asu rebootbmc
```

Output:

```
Rebooting BMC...done
```

Rebootimm command

Use the **rebootimm** command to restart the integrated management module (IMM). This command is for IMM-based servers only.

This command is useful because you must restart the IMM after making changes to IMM settings. This command takes approximately 4 minutes to complete.

Syntax

The syntax of the **rebootimm** command is

```
asu rebootimm [-nx] [connect_options] [-a]
```

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.
3. If the option **–a** parameter is specified, ASU restarts all nodes in the same partition. ASU does not support restarting multiple partitions.

Output

The output of the **rebootimm** command is a message that indicates that the restart of the IMM is completed.

The following example shows the **rebootimm** command and corresponding output.

Command line:

```
asu rebootimm
```

Output:

```
Connected to IMM at IP address 169.254.95.118
Issuing reset command to IMM.
The IMM has started the reset. Waiting for the reset to complete.
Connected to IMM at IP address 169.254.95.118
Reset completed successfully.
```

Rebootrsa command

Use the **rebootrsa** command to restart the Remote Supervisor Adapter and Remote Supervisor Adapter II. This command is for BIOS-based servers only.

This command is useful because you must restart a Remote Supervisor Adapter or Remote Supervisor Adapter II after you make changes to the Remote Supervisor Adapter settings. This command takes approximately 30 seconds to complete.

Syntax

The syntax of the **rebootrsa** command is

```
asu rebootrsa [-nx]
```

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **rebootrsa** command is a message that indicates that the restart of the Remote Supervisor Adapter is completed.

The following example shows the **rebootrsa** command and corresponding output.

Command line:

```
asu rebootrsa
```

Output:

```
Rebooting RSA/RSA2...done
```

Replicate command

Use the **replicate** command to replicate all settings in the update configuration file.

On IMM-based servers, the **replicate** command skips the settings that are defined as `noreplicate`. To see the settings that are defined as `noreplicate`, use the **show** command and specify the `noreplicate` class.

Syntax

The syntax of the **replicate** command is

```
asu replicate file_name [connect_options]
```

where

file_name is the name of the file that was created by a previous **asu save** command or by redirecting the output of a previous **asu show** command to a file.

Note: The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The output of the **replicate** command is a list of output from set commands.

```
<setting 1>=<value 1>
<setting 2>=<value 2>

•
•
•
<setting n>=<value n>
```

The **replicate** command and corresponding output are shown in the following examples.

Command line (IMM-based servers):

```
asu replicate rep.data
```

rep.data file (Show or save output file):

```
uEFI.Com1BaudRate=115200
uEFI.Com1DataBits=8
uEFI.Com1Parity=None
uEFI.Com1StopBits=1
uEFI.Com1TextEmul=VT100
uEFI.Com1ActiveAfterBoot=Enable
uEFI.Com1FlowControl=Disable
```

Output:

```
uEFI.Com1BaudRate=115200
uEFI.Com1DataBits=8
uEFI.Com1Parity=None
uEFI.Com1StopBits=1
uEFI.Com1TextEmul=VT100
uEFI.Com1ActiveAfterBoot=Enable
uEFI.Com1FlowControl=Disable
```

Command line (BIOS-based servers):

```
asu replicate rep.data
```

rep.data file (Show output file):

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled

•
•
•
CMOS_OSUSBControl=Other OS
```

Output:

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled

•
•
•
CMOS_OSUSBControl=Other OS
```

Note: The output is identical to the show output file that is used as input to the **replicate** command.

Resetrsa command

Use the **resetrsa** command to reset the Remote Supervisor Adapter or Remote Supervisor Adapter II to the default settings and then restart it. This command is for BIOS-based servers only.

This command takes approximately 30 seconds to complete.

Syntax

The syntax of the **resetrsa** command is

```
asu resetrsa [-nx]
```

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **resetrsa** command is a message that indicates that the restart of the Remote Supervisor Adapter is completed.

The following example shows the **resetrsa** command and corresponding output.

Command line:

```
 asu resetrsa
```

Output:

```
Rebooting RSA/RSA2...done
```

Restore command

Use the **restore** command to restore all settings that are defined in the update configuration file on the server.

On IMM-based servers, the backup control settings are not restored by default. To restore the backup control settings on an IMM-based server, you must specify the `-incbackupctl` modifier (refer to the section "Command modifiers" on page 70 for specific syntax.

Limitations

During a restore operation, settings that are defined in the password and authentication classes are not restored. To list the settings that belong to either the password or authentication class, use the following command:

```
asu showvalues authentication
```

To list only the password class settings, use the following command:

```
asu showvalues password
```

During a restore operation, the ASU does not delete settings that might exist on the target server that is being restored and that are not included in the restore file.

The **restore** command restores the values that are defined in the restore file for those settings that exist in the target system. Therefore, the restore operation should be viewed as restoring values and not as a system settings restore command.

Syntax

The syntax of the **restore** command is

```
asu restore file_name [--incbackupctl ] [-nx] [connect_options]
```

where

file_name is the name of the file that was created by a previous **asu save** command or by redirecting the output of a previous **asu show** command to a file.

Notes

1. The optional **-incbackupctl** parameter is used on a restore operation to specify whether the settings defined by the backupctl class are to be included. To list the backcupctl class, use the **show**, command and specify the backupctl class.
2. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

Each setting and the restored value are displayed.

```
<setting 1>=<value 1>
<setting 2>=<value 2>

•
•
•
<setting n>=<value n>
```

The **restore** command and corresponding output are shown in the following example.

Command line (IMM-based servers):

```
 asu restore rep.data
```

rep.data file (Show or save output file):

```
uEFI.Com1BaudRate=115200
uEFI.Com1DataBits=8
uEFI.Com1Parity=None
uEFI.Com1StopBits=1
uEFI.Com1TextEmul=VT100
uEFI.Com1ActiveAfterBoot=Enable
uEFI.Com1FlowControl=Disable
```

Output:

```
uEFI.Com1BaudRate=115200
uEFI.Com1DataBits=8
uEFI.Com1Parity=None
uEFI.Com1StopBits=1
uEFI.Com1TextEmul=VT100
uEFI.Com1ActiveAfterBoot=Enable
uEFI.Com1FlowControl=Disable
```

Command line (BIOS-based servers):

```
asu restore rep.data
```

rep.data file (Show or save output file):

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled

•
•
•
CMOS_OSUSBControl=Other OS
```

Output:

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled

•
•
•
CMOS_OSUSBControl=Other OS
```

Note: The output is identical to the save or show output file that is used as input in the **restore** command.

Save command

Use the **save** command to save all settings to a file.

By default, backup control settings (settings in the class backupctl) are saved unless an optional modifier is specified. The supported modifiers include `--group`, `--setlist`, and `--excbackupctl` (refer to "Command modifiers" on page 70 for the specific syntax).

Limitations

Settings that are defined in the password class or authentication settings (user IDs) class settings are not saved during a **save** operation. To list the settings that belong to the password class, type the following command:

```
asu showvalues password
```

Syntax

The syntax of the **save** command is

```
asu save file_name [--group group_name | --setlist set_name1..set_nameN]
[--excbackupctl] [-nx] [connect_options]
```

where

file_name is the name of the file to which the saved settings are written.

Notes

1. If the optional **--group** parameter is specified, only settings that belong to the specified group are saved.
2. If the optional **--setlist** parameter is specified, only settings that belong to the specified list of settings are saved.
3. If the optional **--excbackupctl** parameter is specified, backup control settings (settings in the class backupctl) are not saved.
4. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

5. The connect options are defined for IMM-based servers only. The `--host` *`ip_address`*, `--user` *`user_id`*, and `--password` *`password`* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *`user_id`* and `--password` *`password`* connect options are not required if you are using the local KCS interface.

Output

The output of the **save** command is a message that indicates that the settings are saved to the file name that is specified in the command.

The **save** command and corresponding output are shown in the following examples.

Command line to save all settings:

```
asu save save.txt
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled
```

•
•
•

```
BMC_CRTRequired=Enabled
BMC_KbdRequired=Enabled
```

•
•
•

Command line to save all BIOS settings:

```
asu save save.txt --group bios
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled
```

•
•
•

Command line to save all IMM settings:

```
asu save save.txt --group IMM
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
IMM.PowerRestorePolicy=Last state
IMM.PowerOnAtSpecifiedTime_Year=0
```

-
-
-

Command line to save only the IMM.LockoutPeriod and UEFI.rehook19 settings:

```
asu save save.txt --setlist IMM.LockoutPeriod uEFI.rehook19
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
IMM.LockoutPeriod=2
uEFI.rehook19=CMOS_KbdRequired=Enabled
```

Command line to save all settings except those in the backupctl class:

```
asu save save.txt --excbackupctl
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
uEFI.TurboModeEnable=Enable
uEFI.ProcessorEistEnable=Enable
```

-
-
-

Command line to save all BIOS settings from node 2:

```
asu save save.txt --group bios -n2
```

Output:

```
Settings saved to save.txt
```

save.txt file (Save output file):

```
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled
```

-
-
-

Set command

Use the **set** command to either change the value of a setting or to list a setting.

The **set** command also creates an instance if the instance number does not exist, and if the instance value is less than or equal to the maximum allowed instances for the setting. For more information about instances, see “Instances of settings” on page 19.

Syntax

The syntax of the **set** command is either

```
asu set setting value [-v] [-nx] [connect_options]
```

where *setting* is the name of a setting to change. Use the command `asu show all` to show a list of available settings; *value* is the exact value string to set for the setting.

For settings with a single value, the **asu showvalues** command output is *setting_name=value*.

OR

```
asu set setting value1=value2=valueN [-v] [-nx] [connect_options]
```

where *setting* is the name of a setting to change that can accept a list of values. Use the **asu showvalues** setting command to show a list of all values that are available for the setting.

For settings that allow a list of values, the **asu showvalues** command output syntax is `setting_name==value1=value2=valueN`. The double equal sign (==) shows that the setting can accept either single or multiple values in an ordered list.

Notes

1. Values that contain spaces must be enclosed in quotation marks (" "). If a value contains quotation marks, add a backslash (\ ) before each quotation mark in the value.
2. If the optional **-v** parameter is specified, the output is verbose.
3. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
4. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.

Output

The output of the **set** command when the **-v** parameter is not specified is the setting name and the new value. When the **-v** parameter is specified, the description of the setting is also shown.

The setting with a single value without the **-v** parameter:

```
<setting>=<new value>
```

The setting with a single value with the **-v** parameter:

```
<setting>: <setting description> = <new value>
```

The setting with multiple values without the **-v** parameter:

```
<setting>=<new value1>=<new value2>=<new valueN>
```

The setting with multiple values with the **-v** parameter:

```
<setting>: <setting description>=<new value1>=<new value2>=<new valueN>
```

The **set** command and corresponding output are shown in the following examples.

Command line:

```
 asu set CMOS_CRTRequired Disabled
```

Output:

```
CMOS_CRTRequired=Disabled
```

Command line:

```
asu set CMOS_DisketteA "1.44 MB 3.5\""
```

Output:

```
CMOS_DisketteA=1.44 MB 3.5"
```

Command line:

```
asu set RSAIP_HostIPAddress1 192.168.0.100
```

Output:

```
RSAIP_HostIPAddress1=192.168.0.100
```

Command line:

```
asu set RSAString_LoginId2 rsauser
```

Output:

```
RSAString_LoginId2=rsauser
```

Command line to set the boot order to be CD/DVD ROM, then diskette, and then Hard Disk 0:

```
asu set BootOrder.BootOrder "CD/DVD Rom=Floppy Disk=Hard Disk 0"
```

Output:

```
BootOrder.BootOrder=CD/DVD Rom=Floppy Disk=Hard Disk 0
```

Create a new record instance and set the record key setting

Command line:

```
asu set iSCSI.AttemptName.2 "MyAttempt2Name"
```

Output:

```
iSCSI.AttempName.2=MyAttempt2Name
```

Note: All other settings in this record (for example, iSCSI.LocalIp.2 and iSCSI.SubnetMask.2) are set to default values.

To set the other settings for this instance in this record, refer to the following examples:

Command line:

```
asu set iSCSI.LocalIp.2 "9.5.107.170"
```

Output:

```
iSCSI.LocalIp.2=9.5.107.170
```

The output is followed by this command line:

```
asu set iSCSI.SubnetMask.2 "255.255.255.0"
```

Output:

```
iSCSI.SubnetMask.2="255.255.255.0"
```

Setenc command

Use the **setenc** command to change the value of a setting or to list a setting.

You can apply an encrypted value (<*encrypted value*>) to a setting. The encrypted value is a value returned by the **encrypt** command. If <*encrypted value*> contains spaces, it must be enclosed in double-quotation marks (" ").

Syntax

The syntax of the **setenc** command is either

```
asu setenc setting <encrypted value>
```

where *setting* is the name of a setting to change. Use the command **asu show all** to show a list of available settings; *value* is the exact encrypted value string to set for setting. For settings with a single value, the **asu showvalues** command output is *setting_name*=<*encrypted value*>.

OR

```
asu set setting value1=value2=valueN [-v] [-nx] [connect_options]
```

where *setting* is the name of a setting to change that can accept a list of values. Use the **asu showvalues** setting command to show a list of all values that are available for the setting.

Output

The output of the **setenc** command when the **-v** parameter is not specified is the setting name and the new value. When the **-v** parameter is specified, the description of the setting is also shown.

The setting with a single value without the **-v** parameter:

```
<setting>=<new value>
```

The setting with a single value with the **-v** parameter:

```
<setting>: <setting description> = <new value>
```

The setting with multiple values without the **-v** parameter:

```
<setting>=<new value1>=<new value2>=<new valueN>
```

The setting with multiple values with the **-v** parameter:

```
<setting>: <setting description>=<new value1>=<new value2>=<new valueN>
```

The **setenc** command and corresponding output are shown in the following example.

Command line:

```
 asu setenc CMOS_CRTRequired 5vMOYnMPa1
The "5vMOYnMPa1" equals "Enable" encrypted by command encrypt.
```

Output:

```
CMOS_CRTRequired=Disabled
```

Show command

Use the **show** command to see the current value of one or more settings.

Syntax

The syntax of the **show** command is either

```
asu show [all | --group group_name | setting_name |
--setlist name1..nameN | class] [-v] [-nx] [connect_options]
```

If no command modifier or class setting is specified, all settings and their current values are displayed.

Notes

1. If the optional **all** parameter is specified, all settings are displayed.
2. If the optional `--group` *group_name* is specified, only settings in the group *group_name* are displayed.
3. If the optional `--setlist` *name1..nameN* is specified, only the settings that are specified in *name1..nameN* are displayed.
4. If the optional class setting is specified, only settings that belong to the specific class are displayed.
5. If the optional **-v** parameter is specified, the output is verbose.
6. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
7. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not provide for out-of-band way now. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCSinterface.

Output

If the **-v** parameter is not specified, the setting and the current value are displayed. If the **-v** parameter is specified, the description of the setting is displayed as well as an indicator that the value is the default value.

The setting without the **-v** parameter:

```
<setting>=<current value>
```

The setting with the **-v** parameter:

```
<setting>: <setting description> = <current value> [(default)]
```

Command line:

```
asu show RSAIP_HostIPAddress1
```

Output:

```
RSAIP_HostIPAddress1=192.168.0.100
```

Command line:

```
asu show CMOS_WakeOnLAN -v
```

Output:

```
CMOS_WakeOnLAN: Wake On Lan = Enabled (default)
```

Command line:

```
asu show bios
```

Output:

```
CMOS_DisketteA=1.44 MB 3.5"
CMOS_CRTRequired=Disabled
•
•
•
CMOS_OSUSBControl=Other OS
```

Showdefault command

Use the **showdefault** command to show the default value for one or more settings.

Syntax

The syntax of the **showdefault** command is either

```
asu showdefault [all | --group group_name |  setting_name |
--setlist name1..nameN | class] [-v] [-nx] [connect_options]
```

If no setting command modifier or class setting is specified, all settings and their current values are displayed.

Notes

1. If the optional **all** parameter is specified, all settings are displayed.
2. If the optional `--group` *group_name* is specified, only settings in the group *group_name* are displayed.
3. If the optional `--setlist` *name1..nameN* is specified, only the settings that are specified in *name1..nameN* are displayed.
4. If the optional class setting is specified, only settings that belong to the specific class are displayed.
5. If the optional **-v** parameter is specified, the output is verbose.
6. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
7. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`,

and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *`user_id`* and `--password` *`password`* connect options are not required if you are using the local KCS interface.

Output

If the **-v** parameter is not specified, the setting and the default value are displayed. If the **-v** parameter is specified, the description of the setting is also displayed.

The setting without the **-v** parameter:

```
setting=default value
```

The setting with the **-v** parameter:

```
setting: setting description = default value
```

For instance settings, the default state can be that the instance does not exist. If this is the case, the default value that is displayed by the **showdefault** command is `delete`. This response indicates that all instances of the setting are deleted if the **loaddefault** command is performed on the setting. For more information about instances, see "Instances of settings" on page 19.

The **showdefault** command and corresponding output are shown in the following examples.

Command line:

```
asu showdefault CMOS_WakeOnLAN -v
```

Output:

```
CMOS_WakeOnLAN: Wake On Lan = Enabled
```

Command line:

```
asu showdefault bios
```

Output:

```
CMOS_DisketteA=1.44 MB 3.5"
CMOS_CRTRequired=Disabled
•
•
•
CMOS_OSUSBControl=Other OS
```

Command line:

```
asu showdefault iSCSI.AttemptName.1
```

Output:

```
iSCSI.AttemptName.1=<remove>
```

Showgroups command

Use the **showgroups** command to list the setting groups that are available on the server.

The settings are organized into groups. All uEFI settings belong to the uEFI group, and all BIOS settings belong to the BIOS group. The listed groups can be used as a

class of commands that support the class modifier, or they can be used with the `--group group` option on commands that support this option.

Syntax

The syntax of the **showgroups** command is

```
asu showgroups [-nx] [connect_options]
```

Notes

1. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* can be a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
2. The connect options are defined for IMM-based servers only. The `--host ip_address`, `--user user_id`, and `--password password` connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user user_id` and `--password password` connect options are not required if you are using the local KCS interface.

Output

The setting groups that are available on the server are displayed.

The **showgroups** command and corresponding output are shown in the following examples.

Command line:

```
asu showgroups
```

Output on an IMM-based server:

```
IMM
SYSTEM_PROD_DATA
uEFI
BootOrder
```

Output on a BIOS-based server:

```
bios
bmc
rsa
```

Showlocation command

Use the **showlocation** command to show the location of one or more settings. This command is for BIOS-based servers only.

This command shows where the actual data for the setting is stored.

Syntax

The syntax of the **showlocation** command is

```
asu showlocation [all | --group group_name | setting_name |
--setlist name1..nameN | class] [-v] [-nx] [connect_options]
```

If no setting command modifier or class setting is specified, all settings and their current values are displayed.

Notes

1. If the optional **all** parameter is specified, all settings are displayed.
2. If the optional `--group` *group_name* is specified, only settings in the group *group_name* are displayed.
3. If the optional `--setlist` *name1..nameN* is specified, only the settings that are specified in *name1..nameN* are displayed.
4. If the optional *class* setting is specified, only settings that belong to the specific class are displayed.
5. If the optional **-v** parameter is specified, the output is verbose.
6. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
7. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local Lenovointerface.

Output

If the **-v** parameter is not specified, the setting and its location are displayed. If the **-v** parameter is specified, the description of the setting is also displayed.

Without the **-v** parameter:

```
<setting>=<location>[<extra location info>]

if <location> is CMOS, <extra location info> is of the form
         <byte offset>","<bit offset>","<number of bits>
if <location> is SP, <extra location info> is of the form
         <SP dot byte 1>"."<SP dot byte 2>"," ... "."<SP dot byte n>
if <location> is SP6, <extra location info> is of the form
         ">"<write command info>  ">"<read command info> and <write command info>
         and <read command info> are of the form
         <read command byte>["@"<data offset>]
         ("."<command data>)*["|"<request data length>]
```

With the **-v** parameter:

```
<setting>: <setting description> {
           <location>[<extra location info>]
}

if <location> is CMOS, <extra location info> is of the form
          <byte offset>","<bit offset>","<number of bits>
if <location> is SP, <extra location info> is of the form
          <SP dot byte 1>"."<SP dot byte 2>"." ... "."<SP dot byte n>
if <location> is SP6, <extra location info> is of the form
          ">"<write command info>  "<"<read command info> and <write command info>
          and <read command info> are of the form
          <read command byte>["@"<data offset>]
          ("."<command data>)*["|"<request data length>]
```

The **showlocation** command and corresponding output are shown in the following examples.

Command line:

```
asu showlocation CMOS_SerialA
```

Output:

```
CMOS_SerialA=CMOS[70,00,03]
```

Command line:

```
asu showlocation CMOS_SerialA -v
```

Output:

```
CMOS_SerialA: Serial Port A {
     CMOS[70,00,03]
}
```

Command line:

```
asu showlocation RSA_Network1
```

Output:

```
RSA_Network1=SP[04.09.01.01.02]
```

Command line:

```
asu showlocation RSA_Network1 -v
```

Output:

```
RSA_Network1: Network Interface 1 {
      SP[04.09.01.01.02]
}
```

Showvalues command

Use the **showvalues** command to list all possible values for one or more settings.

This command is useful for finding the value parameter that is used for the **set** command. The **showvalues** command also describes the setting interdependencies information.

Syntax

The syntax of the **showvalues** command is

```
asu showdefault [all | --group group_name |  setting_name |
--setlist name1..nameN | class] [-v] [-nx] [connect_options]
```

asu showvalues [all | --group *group_name* | *setting_name* | --setlist *name1..nameN* | --instances | class] [-v | -t] [-nx] [connect_options]

Notes

1. If the optional **all** parameter is specified, all settings are displayed.
2. If the optional `--group` *group_name* is specified, only settings in the group *group_name* are displayed.
3. If the optional `--setlist` *name1..nameN* is specified, only the settings that are specified in *name1..nameN* are displayed.

4. If the optional *class* setting is specified, only settings that belong to the specific class are displayed.
5. If the optional **-v** parameter is specified, the output is verbose.
6. If the optional **-t** parameter is used, the output includes the raw values.
7. If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).
8. The connect options are defined for IMM-based servers only. The `--host` *ip_address*, `--user` *user_id*, and `--password` *password* connect options are all required if you connect remotely to the IMM. The default user and password will not support an out-of-band connection now. The `--mtsn`, `--net`, `--user`, and `--password` options can be used to connect to IMM-based servers if the server running ASU and the target IMM-based servers are in one LAN. The `--user` *user_id* and `--password` *password* connect options are not required if you are using the local KCS interface.
9. If the optional *--instances* parameter is specified, only settings that can have instances are displayed. The minimum and maximum number of instances allowed for the settings is also displayed. For more information about instances, see "Instances of settings" on page 19.

Output

If the **-v** parameter is not specified, the setting and its value are displayed. If the **-v** parameter is specified, the description of the setting is also displayed.

If the setting is an enumerated type:

```
-v and -t not specified:
          <setting>=<value 1>=<value 2>=...=<value n>
-v specified:
          <setting>: <setting description> {
                    <value 1>
                    <value 2>
                    .
                    .
                    .
                    <value n>
          }
-t specified:
<setting>=<value 1>[<raw 1>]=<value 2>[<raw 2>]=...=<value n>[<raw n>]
```

If the setting is a string type:

```
-v not specified:
           <setting>=char[<length>]
                    <length> is the max length string that can be entered.
                    If <length> is omitted, there is no maximum.
-v specified:
           <setting>: <setting description> {
                    char[<length>]
       }
                    <length> is the max length string that can be entered.
                    If <length> is omitted, there is no maximum.
```

If the setting is an IP address type:

```
-v not specified:
          <setting>= x.x.x.x where (0 <= x <= 255)
-v specified:
          <setting>: <setting description> {
                  A string formatted x.x.x.x, where x is an integer from 0 to 255
       }
```

If the setting is a MAC address type:

```
-v not specified:
          <setting>= x:x:x:x where (0 <= x <= FF)
-v specified:
          <setting>: <setting description> {
                  A string formatted x:x:x:x, where x is a hex integer from 0 to FF
       }
```

If the setting is a keystroke sequence type:

```
-v not specified:
          <setting>=(c )* where c in [0x01-0xFF, 'ESC', ^A-^Z, ^[-^_, ' '-'~']
-v specified:
         <setting>: <setting description> {
          A space-separated sequence of characters where each of the characters is:
                    0x01-0xFF, 'ESC', ^A-^Z, ^[-^_, ' ', '!', '#', '$', '%', '&',
                    '(', ')', '*', '+', ',', '-', '.', '/', '0'-'9', ':', ';', '<',
                    '=', '>', '?', '@', A'-'Z', '[', '\', ']', '^', '_', 'a'-'z',
                    '{', '|', '}', or '~'
```

If the **--instances** parameter is specified, the output for a setting that is not part of a record is:

```
-v not specified:
          <setting>= numeric type=dec min=0 max=65535 default=3260 [min=0, max=256]
                 The output for the setting indicates that it can have anywhere from
                 0 to 256 instances. This is indicated by '[min=0, max=256]'
-v specified:
<setting>: T <setting description> {
    numeric data
    numeric type = dec
    minimum value = 0
    maximum value = 65535
    default value = 3260
    min instances = 0
    max instances = 256
  }
```

The verbose output for the setting also indicates that it can have anywhere from 0 to 256 instances. This is indicated by `min instances = 0` and `max instances = 256`.

If the **--instances** parameter is specified, the output for settings that are part of a record is:

```
-v not specified:
setting1=char[] default="" [min=0, max=12] recordKey
setting2=char[] default="" [min=0, max=12] recordKey="setting1"
setting3=char[] default="" [min=0, max=12] recordKey="setting1"
```

The output for all of the settings indicate that they can have anywhere from 0 to 12 instances. Setting1 is the record key, and setting2 and setting3 are part of a record,

where

setting1 is the key setting.

For more information about records, see “Record management” on page 20.

```
-v specified:
<setting1>: <setting1 description> {
    char[]
    default =
    min instances = 0
    max instances = 12
    Record Key
}
<setting2>: <setting2 description> {
    char[]
    maximum characters = 16
    pattern = ^(.{4,16})?
    default =
    Record Key = <setting1>
}
<setting3>: <setting3 description> {
    char[]
    maximum characters = 16
    pattern = ^(.{4,16})?
    default =
    Record Key = <setting1>
}
```

The verbose output for setting1 also indicates that it can have anywhere from 0 to 256 instances. In this case, it is indicated by `min instances = 0` and `max instances = 256`. Setting1 is the recordKey, and setting2 and setting3 are part of the same record as setting1,

where

setting1 is the key setting.

For more information about records, see "Record management" on page 20.

If the setting is a certificate-related setting:

```
-v not specified:
  <setting>=*<generate>=<import>=...=<export>
-v specified:
<setting>:<setting long name> {
     generate
 import
 export
}
"generate, import, export" are methods supported by this certificate setting.
```

If the setting has interdependency information:

Setting 1 has clear dependency:

```
<setting 1>=<value 11>=<value 12>=...=<value 1n>
```

This setting is hidden if the result of the following expression is true:

```
" <setting 2>== <value 20> "
Refer to the ASU User's Guide for the settings which is marked as (*).
```

Setting 1 depends on both internal settings and system environment:

```
(*)<setting 1>=<value 11>=<value 12>=...=<value 1n>
See the ASU User's Guide for the settings marked as (*).
```

The **showvalues** command and corresponding output are shown in the following examples.

Command line:

```
asu showvalues CMOS_SerialA
```

Output:

```
CMOS_SerialA=PnP=Auto-configure=<Port 3F8, IRQ 4>=Port 2F8,
IRQ 3=Port 3E8, IRQ 4=Port 2E8, IRQ 3=Disabled
```

Command line:

```
asu showvalues CMOS_SerialA -v
```

Output:

```
CMOS_SerialA: Serial Port A {
PnP
Auto-configure
Port 3F8, IRQ 4 (default)
Port 2F8, IRQ 3
Port 3E8, IRQ 4
Port 2E8, IRQ 3
Disabled
}
```

Command line:

```
asu showvalues CMOS_SerialA -t
```

Output:

```
CMOS_SerialA=PnP=Auto-configure=<Port 3F8, IRQ 4>=Port 2F8,
IRQ 3=Port 3E8, IRQ 4=Port 2E8, IRQ 3=Disabled
```

Command line:

```
asu showvalues --instances
```

Output:

```
IMM.LoginId=char[] maxchars=16 pattern=^(.{4,16})? default=<remove>
[min=0, max=12] recordKey
IMM.Password=char[] default="" [min=0, max=12] recordKey="IMM.LoginId"
IMM.AuthorityLevel=<Supervisor>=ReadOnly=Custom [min=0, max=12]
recordKey="IMM.LoginId"
```

Command line:

```
asu showvalues IMM.SSL_HTTPS_SERVER_CERT
```

Output:

```
IMM.SSL_HTTPS_SERVER_CERT=*generate=import=export
```

Version command

Use the **version** command to show the version and build date of the ASU.

The version number uses the following standard format: *w.xy.zzz*

where

w is the major revision number (this value changes if there are major new features in the release), *x* is the minor revision number (this value changes if there are only minor new features in the release), *y* is the sub-minor revision number (this value changes if there are only fixes in the release), and *zzz* is the build number.

Syntax

The syntax of the **version** command is

```
asu version
```

Output

The output of the **version** command shows the current version and build date of the ASU.

The **version** command and corresponding output are shown in the following example.

Command line:

```
asu version
```

Output:

```
Advanced Settings Utility 3.00.65A Mar 12 2009
```

Writeraw command

Use the **writeraw** command to read and write CMOS data that is saved in a file through the **readraw** command. This command is for BIOS-based servers only.

Syntax

The syntax of the **writeraw** command is

```
asu writeraw filename [-nx]
```

where

filename is the name of a file in which the raw CMOS data is to be read.

Note: If the optional **-nx** parameter is specified, the ASU performs the operation for node *x*, where *x* is the selected node in a multi-node system. Node *x* is represented by a number from 1 through 8. If the **-nx** parameter is not specified, the operation is performed on the primary node (node 1).

Output

The output of the **writeraw** command is a file that is generated in the directory where the ASU is running and a message that indicates that the raw write operation is completed.

The **writeraw** command and corresponding output are shown in the following example.

Command line:

```
asu writeraw CMOSraw.dat
```

Output:

```
Raw CMOS read from CMOSraw.dat, written to CMOS
CMOSraw.dat file generated
```

Nodes command

Use the **nodes** command to detect the available nodes in current system. This command is for IMM and legacy servers.

Syntax

The syntax of the **nodes** command is

```
asu nodes
```

Note: You can use it on a either a multi-node system or a single node system. On a single node system, 1 is always reported.

Output

The output of the **nodes** command is a string with a number of nodes currently available on the system.

The **nodes** command and corresponding output are shown in the following example.

Command line:

```
asu nodes
```

Output:

```
System Nodes: 2
```

Appendix. Getting help and technical assistance

This section contains information about where to go for additional information about Lenovo and Lenovo products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

If you need help, service, or technical assistance or you simply want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Before you call

Before you call, take the following steps to try to solve the problem yourself:

- 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. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the Lenovo Documentation CD that comes with your system.
- Go to the Lenovo Support Portal to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the documentation that is provided with your Lenovo product. The documentation that comes with Lenovo 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, refer to its documentation.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, or optional device is available in the documentation that comes with the product.

The documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. You can get the latest technical information and download device drivers and updates from the Official Lenovo Support Home.

Also, some documents are available through the Lenovo Publications Center at IBM Publications Center.

Getting help and information from the Lenovo website

The Lenovo website has up-to-date information about Lenovo systems, optional devices, services, and support.

Refer to the following websites for Lenovo information and support:

- Lenovo System x and xSeries information, see IBM System x®
- Lenovo BladeCenter®, seeIBM BladeCenter
- Lenovo IntelliStation®, see IBM Workstations
- Service information for Lenovo systems and optional devices, see Official Lenovo Support Home
- Lenovo product documentation, see IBM Publications Center

Software service and support

Through Lenovo Support Line, you can get fee-based telephone assistance with usage, configuration, and software problems with System x and xSeries servers, IBM BladeCenter products, Lenovo IntelliStation workstations, and appliances.

For information about the products that are supported by Support Line in your country or region, see the Supported product list.

For more information about Support Line and other Lenovo services, see IT services, or see the Lenovo Support Phone List page for support telephone numbers.

Hardware service and support

You can receive hardware service through your Lenovo reseller or Lenovo Services.

To locate a reseller authorized by Lenovo to provide warranty service, go to IBM PartnerWorld® and click **Business Partner Locator** at the top of the page. For Lenovo support telephone numbers, see the Lenovo Support Phone List page.

Product services for Taiwan

This topic explains how to get product service in Taiwan.

For Lenovo Taiwan product service contact information:

Lenovo Taiwan Corporation

3F, No 7, Song Ren Rd.

Taipei, Taiwan

Telephone: 0800-016-888

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

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.

Printed in USA