

Intel® Hybrid Cloud Platform 3.1 User Guide

Order Number: G56648-002

Rev2.0

February 16, 2012

Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>

Intel® Active Management Technology (Intel® AMT) requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. Results dependent upon hardware, setup and configuration. For more information, visit <http://www.intel.com/technology/platform-technology/intel-amt>.

Copyright © 2012 by Intel Corporation. All rights reserved. Intel, the Intel logo, Intel AppUp, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.

Table of Contents

1. About This Document	1
1.1 Intended Audience	1
1.2 Abbreviations	1
1.3 Additional Information.....	2
2. Intel® Hybrid Cloud platform Overview	3
2.1 Key Elements	3
2.1.1 Intel® Hybrid Cloud server	3
2.1.2 Intel® Hybrid Cloud software stack	4
2.1.3 Intel® Hybrid Cloud management portal.....	4
2.1.4 Intel® Hybrid Cloud server manager	5
2.2 Usage Reporting	5
3. Before You Get Started	6
3.1 Items you will Need	6
3.2 Local & Management Computer Requirements	6
4. Getting Started.....	7
4.1 External Firewall Settings	7
4.1.1 Port Forwarding.....	7
4.2 Connect the Cables.....	9
4.3 Establish Communication & Log In.....	10
4.4 Configure the Network.....	11
4.5 Register the Server	11
4.6 Record Data & Download Tools	12
4.7 Activate the Server	14
4.8 Connect to the Server	16
5. Intel® Hybrid Cloud management portal	18
5.1 Accessing Intel® Hybrid Cloud management portal.....	18
5.2 Management Portal - Dashboard.....	19
5.3 Managing Servers	19
5.4 Viewing Your Profile	21
5.5 Appliance & Application Installation.....	22
5.6 Reactivating an Expired Appliance	24
5.7 Appliance Expiration & Management.....	24
5.8 View the Applications on an Appliance.....	25
5.9 Activating or Deactivating an Appliance or Application	25
5.10 Server Patch Updates	26
6. Intel® Hybrid Cloud server manager.....	27
6.1 Installing Intel® Hybrid Cloud server manager	27
6.2 Accessing the Intel® Hybrid Cloud server manager	27
6.2.1 Role Based Access Control for Intel® Hybrid Cloud server manager	27

6.2.2	Login to Multiple Servers	28
6.2.3	Login to a Specific Server	28
6.3	Changing the Default SW Management Password	30
6.4	Dashboard	31
6.5	Hardware Inventory	31
6.6	Appliances	32
6.6.1	Appliances - Monitor.....	32
6.6.2	Appliances - Configure	33
6.6.3	Appliances - Control.....	34
6.6.4	Appliances - Console	34
6.6.5	Appliances - Application	36
6.6.6	Appliances - Services.....	37
6.6.7	Appliances - Restore.....	38
6.7	Configuration.....	38
6.7.1	Server Settings.....	38
6.7.2	Network Settings	39
6.7.3	Configuring Email Alerts.....	40
6.7.4	Rebrand Intel® Hybrid Cloud server.....	41
6.7.5	Configure Boot Settings	41
6.8	Disaster Recovery	42
6.8.1	Setup	42
6.8.2	Recover from Primary Server Failure	45
6.8.3	Repair – Re-Create the Disaster Recovery Setup	47
6.9	Controls.....	49
6.9.1	Permissions	51
6.9.2	Diagnostics (Controls → Scripts).....	51
6.10	Logs	52
6.10.1	Software and Hardware Logs Deletion:	53
6.10.2	Software Logs Download	54
6.11	Appliance and Application Download	55
6.12	Patching Mechanism	56
6.13	Multiple Server Management.....	58
6.14	Logging out of Intel® Hybrid Cloud server manager	59
7.	Saving & Restoring System Configuration.....	60
7.1	Saving the Server Configuration	60
7.2	Restoring the Server Configuration	60
8.	Activating Appliances	62
8.1	Activating Windows* Appliances.....	62
8.2	Activating Other Appliances	62
9.	Intel® AMT Configuration	63
9.1	Intel® AMT Password.....	63

10. Intel® Hybrid Cloud server BMC Configuration	64
10.1 Change the BMC IP Address	64
10.2 BMC Password	64
11. Intel® Hybrid Cloud command line tool (IXE).....	65
11.1 IXE command Line Format.....	65
11.2 List of IXE Commands.....	66
11.3 IXE AMT Commands.....	88
11.4 IXE Error Messages	90

List of Figures

Figure 1: Elements in the Intel® Hybrid Cloud platform.....	3
Figure 2. Intel® Hybrid Cloud management portal.....	4
Figure 3. Intel® Hybrid Cloud server manager.....	5
Figure 4. Initial Setup (server behind Firewall).....	9
Figure 5. Initial Setup (server as Edge Device).....	9
Figure 6. Connect screen.....	10
Figure 7. Software License Agreement.....	10
Figure 8. Configure Network screen.....	11
Figure 9. Register Server screen.....	12
Figure 10. Record the Server Data.....	12
Figure 11. Connect to the Internet (server Behind Firewall).....	13
Figure 12. Connect to the Internet (server as Edge Device).....	13
Figure 13. Download Tools.....	14
Figure 14. Click Here to Login.....	14
Figure 15. Login screen.....	15
Figure 16. Activate the Server.....	15
Figure 17. Enter the Customer’s Name.....	16
Figure 18. Connect to Server screen.....	17
Figure 19. Add Server screen.....	17
Figure 20. Management Portal - Login screen.....	18
Figure 21. Management Portal - Dashboard.....	19
Figure 22. Management Portal – Servers screen.....	19
Figure 23. Management Portal – Servers Screen – Info.....	20
Figure 24. Management Portal – Servers Screen - Services.....	20
Figure 25. Management Portal –Servers screen - Manage.....	21
Figure 26. Management Portal – Your Profile.....	21
Figure 27 Management Portal - Catalog.....	22
Figure 28 Management Portal – Catalog - Select a Server.....	22
Figure 29 Management Portal – Catalog - Select the Appliance.....	23
Figure 30 Management Portal – Catalog – Application EULA.....	23
Figure 31 Management Portal – Catalog - Download Confirmation.....	24
Figure 32. Management Portal – Applications on an Appliance.....	25
Figure 33. Management Portal – Applications Status Updates.....	25

Figure 34. Management Portal – Server Patch Updates.....	26
Figure 35. Server Manager – Connecting to All Servers	28
Figure 36. Server Manager - Login Window	28
Figure 37. Server Manager - Add server to hosts file	29
Figure 38. Server Manager – Change the Default Password	30
Figure 39. Server Manager - Default view (Dashboard)	31
Figure 40. Server Manager - Hardware Inventory - System Information window	32
Figure 41. Server Manager - Appliances Monitor window	33
Figure 42. Server Manager - Appliances Configure window.....	33
Figure 43. Server Manager - Appliances Control window	34
Figure 44. Server Manager - Appliances Console Screen	35
Figure 45. VNC Console.....	35
Figure 46. Server Manager – Appliance Services.....	36
Figure 47 Server Manager - Applications tab under Appliances	36
Figure 48 Server Manager - Services tab under Appliances	37
Figure 49. Server Manager - Appliances Restore Screen.....	38
Figure 50. Server Manager - Configure Server Settings window	39
Figure 51. Server Manager - Configure Network Settings Screen	40
Figure 52. Server Manager - Alerts (Email) Configuration window	41
Figure 53. Server Manager - Rebrand Server screen	41
Figure 54. Server Manager - Configure Boot Settings window.....	42
Figure 55. Secondary server details window	43
Figure 56. Server Manager - Configuring Disaster Recovery between servers	44
Figure 57. Server Manager - Waiting for Secondary systems to come up	44
Figure 58. Server Manager - Synchronization in progress.....	44
Figure 59. Server Manager - Synchronization complete	45
Figure 60. Server Manager - displaying usage of the mirror server	45
Figure 61. Server Manager - Server status message.....	46
Figure 62. Server Manager - Machine status.....	46
Figure 63. Server Manager - Recovery tab	47
Figure 64. Verify Network Connections for Secondary Server	47
Figure 65. Re-Create the Disaster Recovery Setup	48
Figure 66. Server Manager - Control - Maintenance Screen 1	50
Figure 67. Server Manager - Maintenance Screen 2	51
Figure 68. Server Manager - Permissions Screen	51

Figure 69. Server Manager - Diagnostics (Control > Scripts) window	52
Figure 70. Server Manager - Software Logs screen	53
Figure 71. Server Manager - Hardware Logs Screen.....	53
Figure 72. Server Manager - Software and Hardware Logs Deletion	54
Figure 73. Server Manager - Software Logs Download	54
Figure 74. Server Manager – Appliance Installing	55
Figure 75. Server Manager – Appliance Paused	56
Figure 76. Server Manager – Appliance Resuming	56
Figure 77. Server Manager – Installation Cancelling	56
Figure 81. Server Manager - Patch Message	57
Figure 82. Server Manager - Upgrade the Server Software.....	57
Figure 78. Server Manager - All Servers page.....	58
Figure 79. Server Manager - All servers → Connect to Server window	59
Figure 80. Server Manager - All servers → Connect to Server window (via Intel® AMT)	59
Figure 83. Server Manager - Log Out	60
Figure 84. Activating Microsoft Windows* Appliances - Customer Profile page	62

List of Tables

Table 1. Abbreviations	1
Table 2. Ports (AMT Configuration)	8
Table 3. Ports (BMC Configuration)	8
Table 4. IXE Error Messages	90

1. About This Document

This User Guide describes in detail, the various features available for configuring and managing the Intel® Hybrid Cloud platform Version 3.1.

1.1 Intended Audience

This User Guide is written for Remote Administrators and end users in the SMB segment, who may want to manage the Intel® Hybrid Cloud server, activate new virtual appliances on the server and monitor virtual appliances running on the server.

1.2 Abbreviations

The following table displays the abbreviations used in this document:

Table 1. Abbreviations

Term	Description
ARP	Address resolution protocol
BMC	Baseboard Management Controller
CLI	Command line interface
DDC	Display Data Channel
DHCP	Dynamic Host Configuration Protocol
DVC	Dambrackas Video Compression
DVO	Dynamic Visual Output
FPGA	Field Programable Gate Array
ICMP	Internet Control Message Protocol
Intel® AMT	Intel® Active Management Technology refers to Intel's management architecture with consistent cross platform capabilities, interfaces, and protocols. Intel® AMT offers a HW chipset based solution for remote out-of-band management, using a secondary processor on the motherboard, with embedded firmware that runs on the Manageability Engine (ME).
Intel® Hybrid Cloud platform	Intel® Hybrid Cloud platform is a unique Hardware and Software solution that is remotely managed and is targeted at small and medium businesses that have a business need for simplified IT functionality.
Intel® RMM3	Intel® Remote Management Module 3
IPMI	Intelligent Platform Management Interface
ITE	Information Technology Equipment
IXE	Intel® Hybrid Cloud Command Line Tool
KVM	Keyboard, video and mouse

Term	Description
LAS	Local Application Store is a local storage repository on the server that contains appliances.
MAC	Media Access Controller
OOB	Out of Band channel, can be used to access a system that is powered down and does not have an OS running.
PBDE	Polybrominated Biphenyls Diphenyl Ethers
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control.
Remote Administrator / MSP	A Managed Service provider (MSP) who interfaces between Intel and the End-User (to provide remote management services).
RMII	Reduced Media Independent Interface
RTC	Real-Time Clock
SMB	Small and Medium Businesses
TCP/IP	Transmission Control Protocol/Internet Protocol
TPS	Technical Product Specification
UART	Universal asynchronous receiver transmitter
UDP	User Datagram Protocol
Virtualization (Intel® VT)	The hardware implementation of Intel® Virtualization Technology (that is, Intel® VT), enables multiple guest OSs and applications (together known as Virtual Machines or VMs) to co-exist on the same computer platform.
VMM*	Virtual Machine Manager, refers to third party ISV SW that uses Intel® VT to enable remote management of VMs.

1.3 Additional Information

For additional information not covered in this guide, refer to our Support page:

<http://www.intelhybridcloud.com/support.html>

NOTE: You must be logged in to view confidential content.

2. Intel® Hybrid Cloud platform Overview

The Intel® Hybrid Cloud platform offers small business customers cloud-like flexibility, providing an innovative solution, which implements a subscription-based model for providing locally-hosted server software on a pay-as-you-go basis. Small businesses get all of the benefits of services in the cloud, with the responsiveness and consistency of local applications, plus the security of having data on site.

2.1 Key Elements

The Intel Hybrid Cloud platform is composed of four key elements:

- Intel® Hybrid Cloud server resides on the customer premises and hosts the customer appliances, applications and data locally.
- Intel® Hybrid Cloud software stack runs on the Intel® Hybrid Cloud server on top of a Virtual Machine Monitor (VMM).
- Intel® Hybrid Cloud management portal (Web Portal) is an internet accessible asset management site for all of your Intel® Hybrid Cloud Servers. This remotely accessible site allows you to register your servers and manage appliance activation and expiration for each of your customers from any location with an internet connection. Additional details about the Intel® Hybrid Cloud Web Portal are provided in Section 5.
- Intel® Hybrid Cloud server manager provides you with the power to manage your Intel® Hybrid Cloud Servers and users remotely.

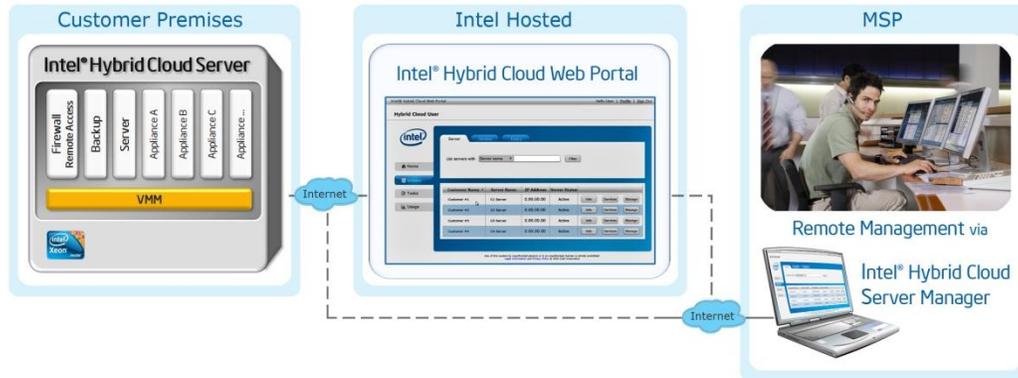


Figure 1: Elements in the Intel® Hybrid Cloud platform

2.1.1 Intel® Hybrid Cloud server

The Intel® Hybrid Cloud server is equipped with the technical ingredients required to support the Intel® Hybrid Cloud software stack, including Intel® Active Management Technology for remote manageability, Intel AMT/BMC and a Trusted Platform Module.

2.1.2 Intel® Hybrid Cloud software stack

The Intel® Hybrid Cloud software stack is a core component that runs on top of a Virtual Machine Monitor (VMM) on the Intel® Hybrid Cloud server. This software provides an abstraction layer over VMM, making it easy to deploy, configure and manage the Intel Hybrid Cloud server. Both Linux* and Microsoft Windows* guest operating systems are supported within the VMM, to run a variety of end-user applications.

2.1.3 Intel® Hybrid Cloud management portal

The Intel® Hybrid Cloud management portal (Web Portal) requires a valid username and password to access, and is available to authorized remote administrators. Through this portal, you can register your Intel® Hybrid Cloud Servers and activate appliances for your customers. Additional details about the Intel® Hybrid Cloud management portal are provided in Section 5 of this document.

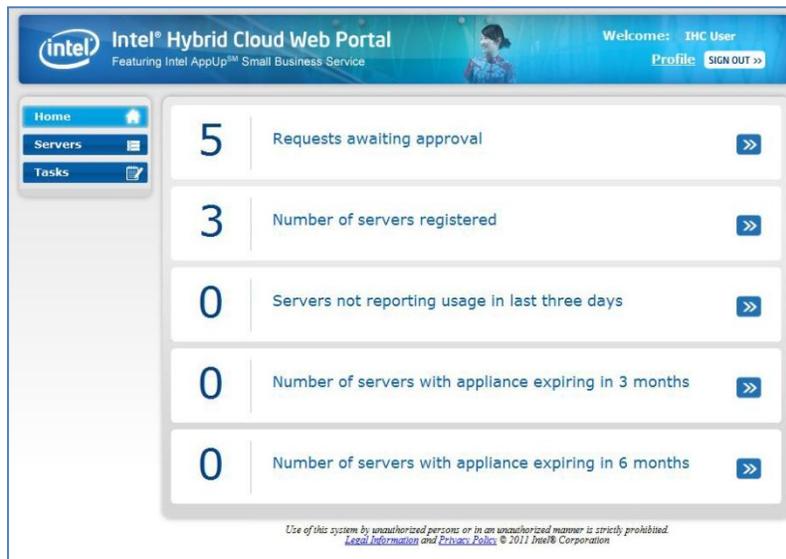


Figure 2. Intel® Hybrid Cloud management portal

2.1.4 Intel® Hybrid Cloud server manager

This user-friendly interface enables remote monitoring, server configuration and management. Since each software appliance runs on a separate virtual machine, you can manage and isolate appliances individually for reconfiguration or troubleshooting. Additional details are provided in Section 5 of this document.

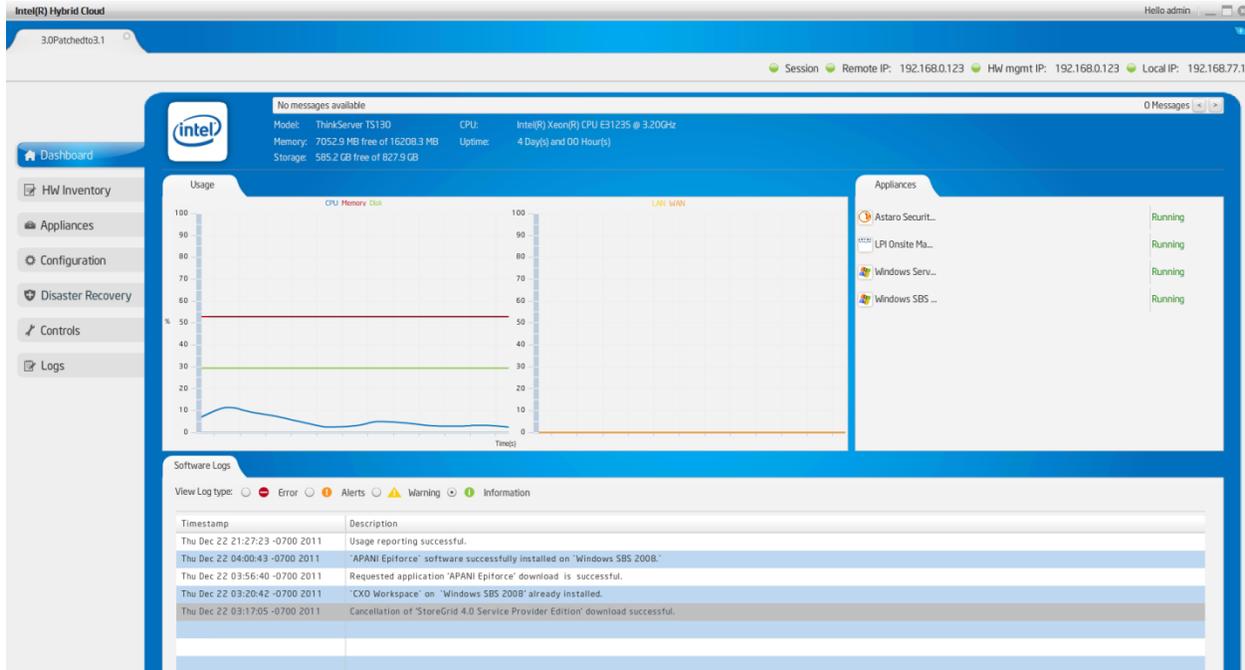


Figure 3. Intel® Hybrid Cloud server manager

Also available in the Intel® Hybrid Cloud Server Manager is a command line utility (called IXE). IXE is available as part of Intel® Hybrid Cloud server manager and can be used for configuring and managing Intel® Hybrid Cloud servers. Additional details for IXE commands are provided in Section 11 of this document.

2.2 Usage Reporting

A core feature of the Intel Hybrid Cloud platform is its ability to track usage of services, and to report those statistics to the Intel® Hybrid Cloud data center. Unique Client IDs are used to anonymously track and report software usage, so your customer's identity is never transmitted beyond the local server. Usage reports are provided to you on a monthly basis and include itemized details for the services used on each of the servers you manage. In turn, you can use this data to add margin to the monthly software subscriptions used by your customers.

The Intel® Hybrid Cloud Server must be connected to the internet (and communicating with the Intel® Hybrid Cloud data center) in order to provide accurate usage reports. Communication with the data center is also required for software downloads from the Intel® Hybrid Cloud catalog, and for patches to components of the Intel® Hybrid Cloud software stack.

NOTE: To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

3. Before You Get Started

3.1 Items you will Need

In addition to the Intel® Hybrid Cloud server, you will also need the following Items:

- Local Computer (see Section 3.2 for details)
- Internet Connection
- 2 CAT5 Ethernet Cables (for Remote & Local IP Connections)
- Your Login information (Intel® Hybrid Cloud user ID & PW)
- Password Guide (in the box with the hardware)
- Preliminary Setup Guide (in the box with the hardware)
- Password List (you must log in to <http://www.intelhybridcloud.com/> to download from the this document from the “**Support**” page)

3.2 Local & Management Computer Requirements

A local computer is required to setup and register your Intel® Hybrid Cloud server. You can use the same computer or a different computer to remotely manage your Intel® Hybrid Cloud servers. The system requirements are listed here:

Minimum Hardware Requirements

- Intel® Pentium® 4 Processor 2GHz
- 1GB RAM

Supported Operating Systems

Your management computer will need to run one of the following supported operating systems

- Microsoft Windows XP*
- Microsoft Windows 7*
- Microsoft Windows 2008*

Supported Web Browsers

A supported web browser is required to access the Intel® Hybrid Cloud management portal. The following browsers are currently supported (minimum version listed):

- Mozilla Firefox* 3.6
- Microsoft Internet Explorer* 7.0
- Google Chrome* 10.0

4. Getting Started

This section will help you set up and configure the Intel® Hybrid Cloud platform and management software.

IMPORTANT: Read all cautions and warnings (provided with the hardware) before powering-up the system.

4.1 External Firewall Settings

If an external firewall is used, ensure the following:

- The Intel® Hybrid Cloud server may not contain any Software Firewall appliance.
- All the client machines are to be directly connected to the external firewall.
- All the interfaces of the appliances on the server should use the remote interface (from “Appliances” select the Appliance, then select the Configure tab and scroll to Network section, and ensure the Network is using a remote interface).
- The appropriate Ports must be forwarded.

4.1.1 Port Forwarding

The following Ports should be forwarded when using an external firewall/router (i.e. a firewall that is not an appliance running on the Intel® Hybrid Cloud Server). Confirm that your external firewall is not blocking these ports. For details regarding your specific firewall/router, refer to the manufacturer’s documentation. Use the appropriate table below for your server:

Table 2. Ports (AMT Configuration)

Servers with Intel® Active Management Technology (Intel® AMT)		
Outbound TCP Port	Server IP Function	Requirement
443	Intel® Hybrid Cloud server - Usage Reporting	Must be Open
Inbound TCP Port	Server IP Function	Forward to IP Address
22	SSH to the Intel® Hybrid Cloud server	Server IP Address
16993	Used to manage the Intel® Hybrid Cloud server via Intel® AMT – out of band (OOB)	Server IP Address
16994-16995	Used to manage the Intel® Hybrid Cloud server via SOL	Server IP Address
5910-5920	VNC ports used to access virtual appliances remotely	Server IP Address
64440**	Used for server registration, management and IXE commands	Server IP Address
65222	Used by the script engine for debugging and executing critical tasks	Server IP Address

**If the external firewall device cannot open Port 64440, refer to the Intel® Hybrid Cloud - Release Notes to change the management port.

Table 3. Ports (BMC Configuration)

Servers with Baseboard Management Controller (BMC)		
Outbound TCP Port	Server IP Function	Requirement
443	Intel® Hybrid Cloud server - Usage Reporting	Must be Open
Inbound TCP Port	Server IP Function	Forward to IP Address
443	Intel® Remote Management Module 3 (RMM3)	BMC IP Address
8282	Used to manage the Intel® Hybrid Cloud server via BMC – out of band (OOB)	BMC IP Address
Inbound TCP Port	Server IP Function	Forward to IP Address
22	SSH to the Intel® Hybrid Cloud server	Server IP Address
5910-5920	VNC ports used to access virtual appliances remotely	Server IP Address
64440**	Used for server registration, management and IXE commands	Server IP Address
65222	Used by the script engine for debugging and executing critical tasks	Server IP Address

**If the external firewall device cannot open Port 64440, refer to the Intel® Hybrid Cloud - Release Notes to change the management port.

4.2 Connect the Cables

NOTE: Intel® Hybrid Cloud servers have more than one network interface port (for Remote and Local connections). These RJ45 jacks are labeled for easy identification:

- Port “**A**” - Remote Network Interface (Default: DHCP)
- Port “**B**” - Local Network Interface (Default IP: 192.168.77.1)

Perform the following steps (as shown in either “**Figure 4**” or “**Figure 5**”):

1. Connect the network port, labeled “**A**” on the Intel® Hybrid Cloud server, **to the broadband access device** (such as a cable modem, DSL modem etc).
2. Connect the power cable to the server, and to an appropriate power source.
3. Power-up the Intel® Hybrid Cloud server.
4. Before proceeding to the next step, **allow 8 to 10 minutes** for the server to boot completely.
5. Connect the network port, labeled “**B**” on the Intel® Hybrid Cloud server, directly **to your Local Computer’s network interface**.

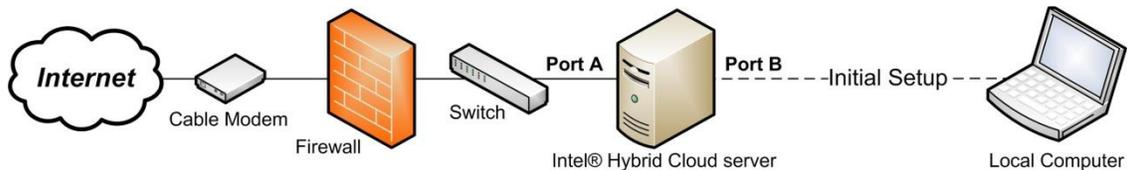


Figure 4. Initial Setup (server behind Firewall)

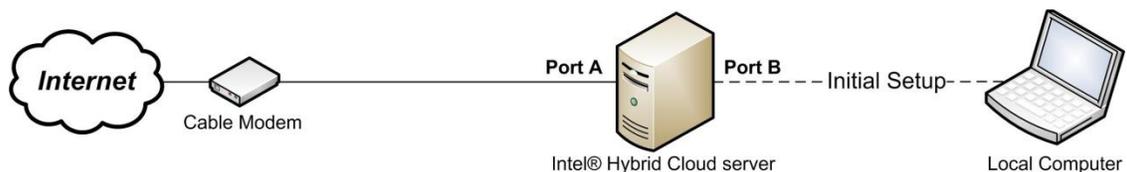


Figure 5. Initial Setup (server as Edge Device)

4.3 Establish Communication & Log In

1. Log into your local computer as the Administrator.
2. Change the network settings on your local computer to:

 IP: **192.168.77.42**
 Subnet Mask: **255.255.255.0**
3. Use a supported Internet browser to navigate to:

 <https://192.168.77.1:64440/login>
4. Choose “**Continue to this website**” at the Security Certificate warning. 
5. Enter the default User Name and Password in the “**Connect**” login box:

Username: **admin**
Password: **Hybr1dC!0ud**

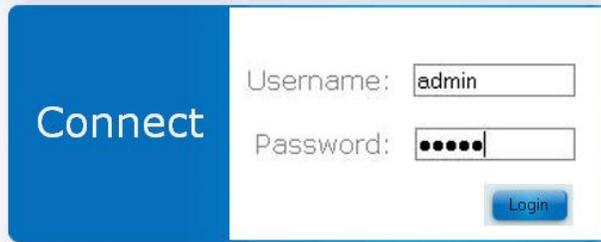


Figure 6. Connect screen

6. Click the “**Login**” button.
7. Read and Accept the “**Intel End User Software License Agreement.**”

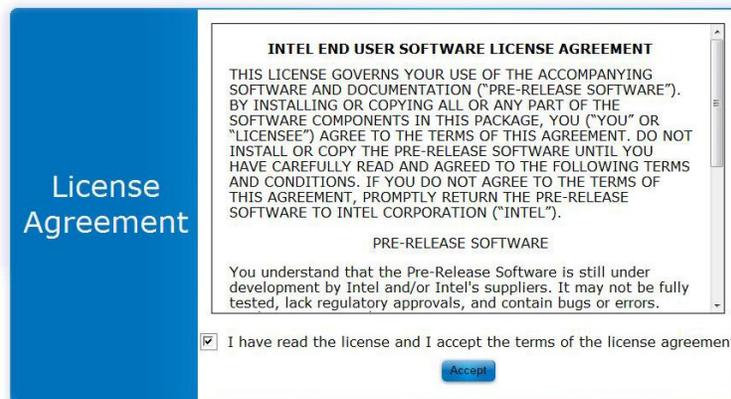


Figure 7. Software License Agreement

4.4 Configure the Network

Choose the appropriate network setting.

NOTE: If the Intel® Hybrid Cloud server can access the internet, this screen may not appear.

- **DHCP** - The values will automatically populate:
 1. Click the “**Keep the Same**” button.
- **Static IP:**
 1. Enter the appropriate network configuration values.
 2. Click the “**Update**” button.

The screenshot shows a web interface for network configuration. At the top, there are two tabs: '1 Check Network' (highlighted in blue) and '2 Register Server'. On the left, a blue vertical bar contains the text 'Configure Network'. The main content area has a red error message: 'The web portal is not reachable. Please verify/update the WAN interface details.' Below the message, there are several configuration fields: 'Protocol' with radio buttons for 'DHCP' and 'Static' (the 'Static' button is selected); 'IP Address' with a text box containing 'XXX.XXX.XXX.XXX'; 'Netmask' with a text box containing '255.255.255.0'; 'Gateway' with a text box containing 'XXX.XXX.XXX.XXX'; and 'DNS' with a text box containing 'XXX.XXX.XXX.XXX'. At the bottom of the form, there are two buttons: 'Update' (highlighted in blue) and 'Keep the same' (greyed out).

Figure 8. Configure Network screen

4.5 Register the Server

1. Enter a “**System Name**” allowed characters are:
 - A-Z (uppercase letters) a-z (lowercase letters) 0-9 (numeric digits) . (period)
 - (dash) _ (underscore)

NOTE: The System Name (Server Name) will differentiate this server from your other servers in the Intel® Hybrid Cloud management portal.
2. Enter your “**Remote Administrator ID**” (i.e. same as your Intel® Channel account).

ATTENTION: Management of this server will be limited to this Administrator ID.
3. Click the “**Register**” button.

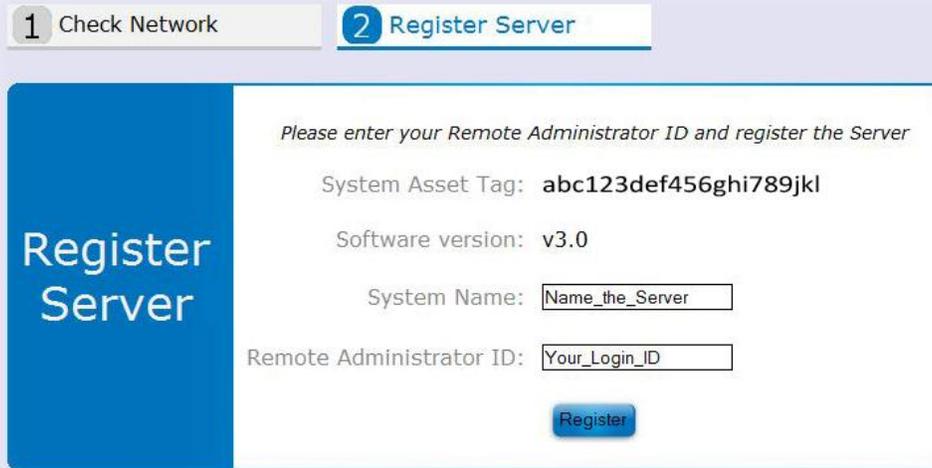


Figure 9. Register Server screen

4.6 Record Data & Download Tools

ATTENTION: Leave the browser open for Steps 4.6 & 4.7 (to install the software and activate the server).

1. Record the data from the Server Configuration box to corresponding spaces on the Intel® Hybrid Cloud - Server Management Info form (required for Step 4.8).

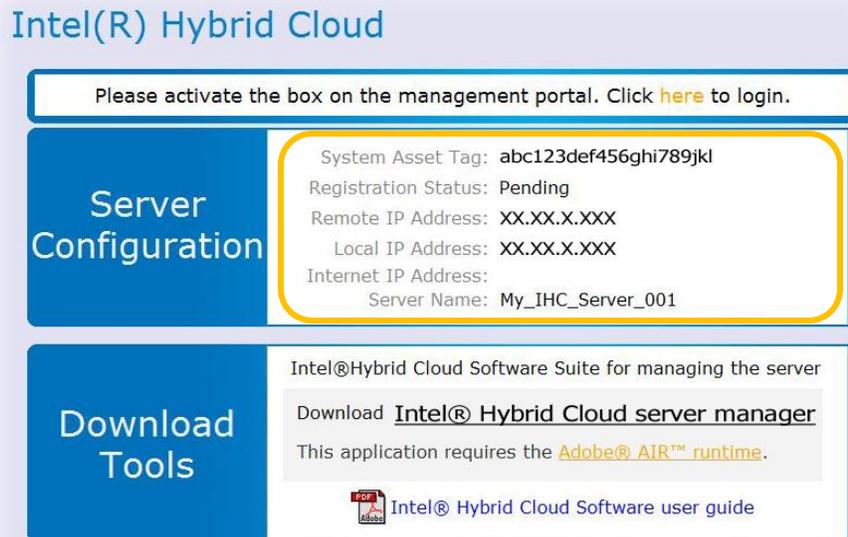


Figure 10. Record the Server Data

2. Disconnect the local computer's network interface from the Intel® Hybrid Cloud server.

3. Connect the local computer to the internet.

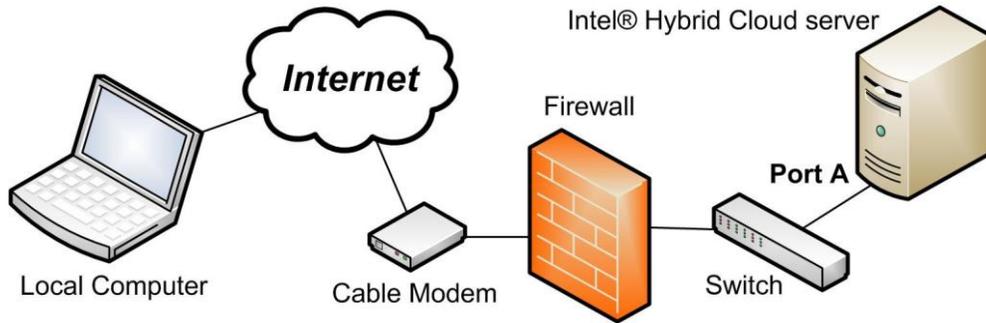


Figure 11. Connect to the Internet (server Behind Firewall)

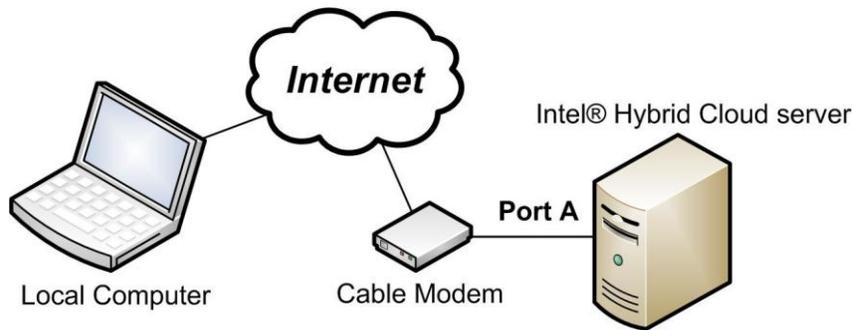


Figure 12. Connect to the Internet (server as Edge Device)

4. Reconfigure the local computer’s network settings to access the internet.
5. Under the “**Download Tools**” heading, click the “**Intel® Hybrid Cloud server manager**” link.

Intel(R) Hybrid Cloud

Please activate the box on the management portal. Click [here](#) to login.

Server Configuration	System Asset Tag: abc123def456ghi789jkl Registration Status: Pending Remote IP Address: XX.XX.X.XXX Local IP Address: XX.XX.X.XXX Internet IP Address: Server Name: My_IHC_Server_001
Download Tools	Intel®Hybrid Cloud Software Suite for managing the server Download Intel® Hybrid Cloud server manager This application requires the Adobe® AIR™ runtime . Intel® Hybrid Cloud Software user guide

Figure 13. Download Tools

6. Install the Certificates in the store titled "**Trusted Root Certification Authorities.**"

IMPORTANT: Adobe* Air Version is required, and will install with the Intel® Hybrid Cloud server manager software.

NOTES:

- Even if you have previously downloaded the software tools, you may not have the current versions of the tools. If you have already downloaded the current tools, you can skip this step.
 - When you download Intel® Hybrid Cloud server manager, IXE command line tools are automatically downloaded to the client machine. Please refer to chapter 10 for more details on IXE tool usage.
 - If the Adobe Shockwave Flash Player* plugin is installed, an “**Install Now**” button will be provided
7. Return to the browser window and continue to the next step.

4.7 Activate the Server

1. In the upper box, follow the "**Click here to login**" link (or go to <https://hybridcloud.intel.com> in a web browser).

Intel(R) Hybrid Cloud

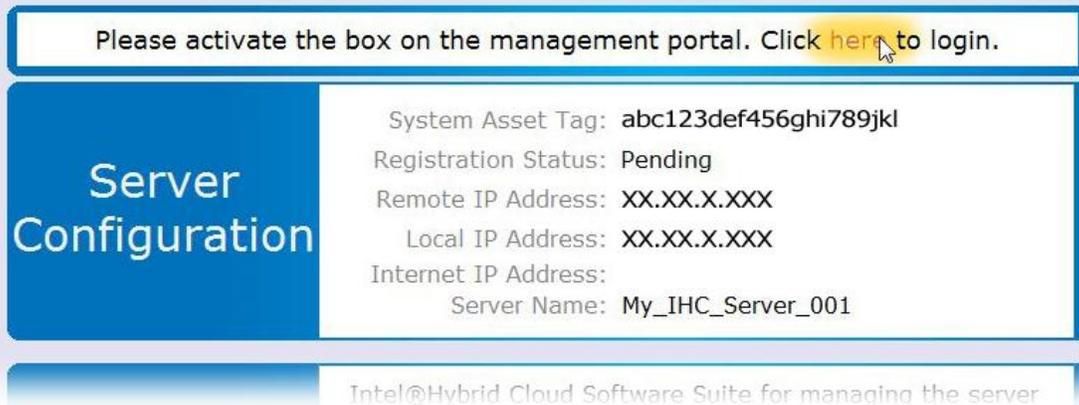


Figure 14. Click Here to Login

2. Enter your Remote Administrator ID ("**Login ID**") and Password.

3. Click the **"Login"** button.



Figure 15. Login screen

4. Select the **"Tasks"** menu bar (on the left).
5. Click the **"Activate"** link (for the new server).



Figure 16. Activate the Server

6. Enter a name for your customer in the **"Customer Name"** space.

7. Click the "**Confirm**" button.



Activate the Server

Asset Tag: abc123def456ghi789jkl

Server Name: My_IHC_Server_001

Internet IP Address: XXX.XXX.XXX.XXX

Software Version: v3.0

Customer Name:

Confirm **Reject** **Cancel**

Figure 17. Enter the Customer's Name

NOTE: If you have additional pending registrations, you can activate the servers by repeating the steps above.

4.8 Connect to the Server

1. Open "Intel® Hybrid Cloud server manager" as Administrator, using the shortcut on your desktop (or from your Start menu).

- a. Right-Click the Icon (or menu item).
- b. Select "Run as administrator."



2. Select the "**Connect**" tab.
3. Enter the remote login information in the "**Connect to Server**" screen:
 - Server Name..... (created in Step 4.5)
 - User Name..... **admin**
 - SW Management Password..... **Hybr1dC!0ud**

4. Click the "**Connect**" button.

TIP: If you are experiencing difficulty with the server connection, refer to Section 4.1 for external firewall and Port Forwarding details.



The image shows a dialog box titled "Connect to Server". On the left side, there is a vertical blue bar with the text "All Servers" and a "Connect" button. The main area of the dialog has the following fields and buttons:

- Server Name: A dropdown menu showing "My_IHC_Server_001".
- User Name: A text input field containing "admin".
- SW Management Password: A text input field containing "*****".
- Buttons: "Connect" and "Cancel".

Figure 18. Connect to Server screen

5. Enter the Remote IP address.
6. Press the **"Add"** button.



The image shows a dialog box titled "Add Server". It contains the following fields and buttons:

- Server Name: A text input field containing "My_IHC_Server_001".
- Server IP: A text input field containing "XXX.XXX.XXX.XXX".
- Buttons: "Add" and "Cancel".

Figure 19. Add Server screen

7. Install the Certificate in the store titled "**Trusted Root Certification Authorities.**"
8. At the prompt, change the SW Management Password.

Password Requirements:

- a minimum of 8 characters
- at least one uppercase character
- at least one numeric character
- at least one special character @ \$ % ^ ! () * # &

5. Intel® Hybrid Cloud management portal

The internet accessible Intel® Hybrid Cloud management portal features a user friendly interface to register, activate and remotely manage your Intel Hybrid Cloud servers. Through the management portal, you can also download new applications, manage users, and monitor subscription usage.

5.1 Accessing Intel® Hybrid Cloud management portal

1. From your Local Computer, use one of the supported web browsers (identified in Section 3.2) to navigate to the following address:

<https://hybridcloud.intel.com>

2. Login to the Intel® Hybrid Cloud management portal using your Remote Administrator ID (Intel® Channel ID).



Figure 20. Management Portal - Login screen

Inactivity of more than five minutes on the Intel® Hybrid Cloud management portal will automatically log the user (or administrator) out. For password recovery information, refer to the “**Password**” section of the “**Intel® Hybrid Cloud - Troubleshooting Guide.**”

5.2 Management Portal - Dashboard

The dashboard in the Intel® Hybrid Cloud management portal (Figure 21) shows an overview of the servers you manage and pending requests (for servers to be approved), as well as, some additional management alert links. Also displayed are the menu buttons (on the left) that allow you to navigate to various functional screens throughout the management portal.

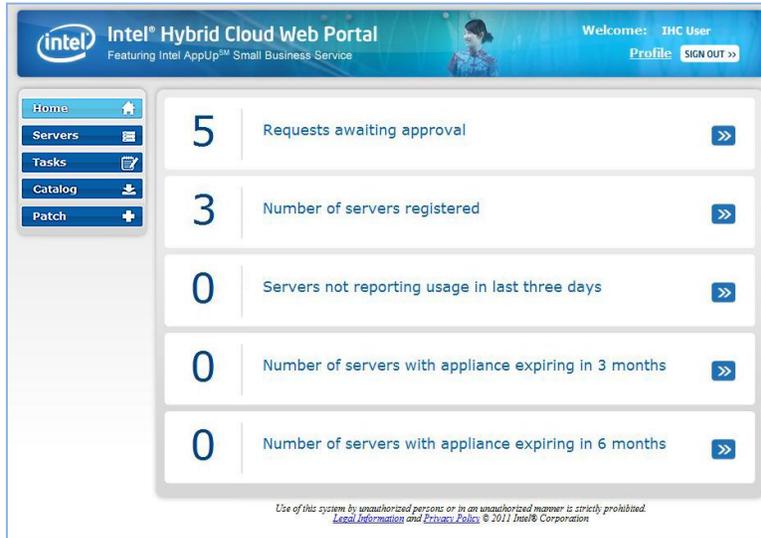


Figure 21. Management Portal - Dashboard

5.3 Managing Servers

Select the “**Servers**” menu button to access the “**Servers**” screen where you can view and modify the expiration dates for appliance licenses, or activate and deactivate the appliances for all of your registered servers. You can also launch the Intel® Hybrid Cloud server manager to monitor or perform maintenance on individual servers.

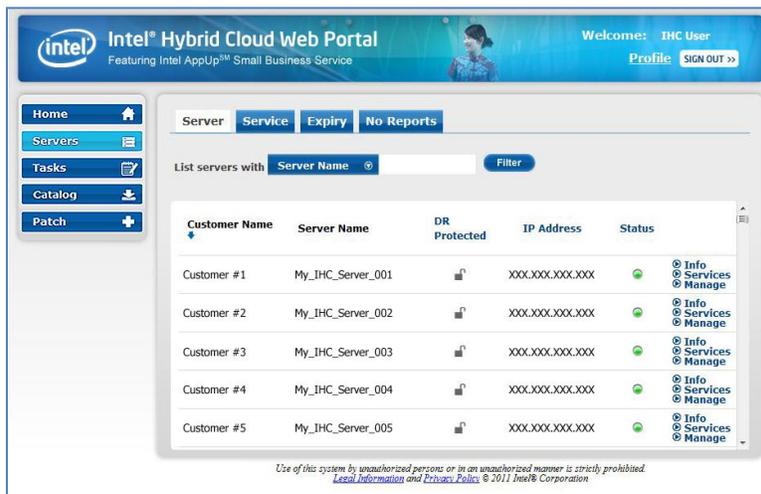


Figure 22. Management Portal – Servers screen

In the “**Servers**” tab on the “**Servers**” screen (Figure 22 above), the following items are available:

- ▶ **Info** - Provides details about the server (including VMM expiry, System Asset Tag, System HW serial number, Intel® Hybrid Cloud software stack version).
- ▶ **Services** - Displays a list of appliances installed on the server. You can activate/deactivate and change the expiry date of the appliance licenses. Default appliance expiry is set to three years.
- ▶ **Manage** – Provides a link to open the Intel® Hybrid Cloud server manager where you can perform additional server manage functions. Refer to Section 6 for details.

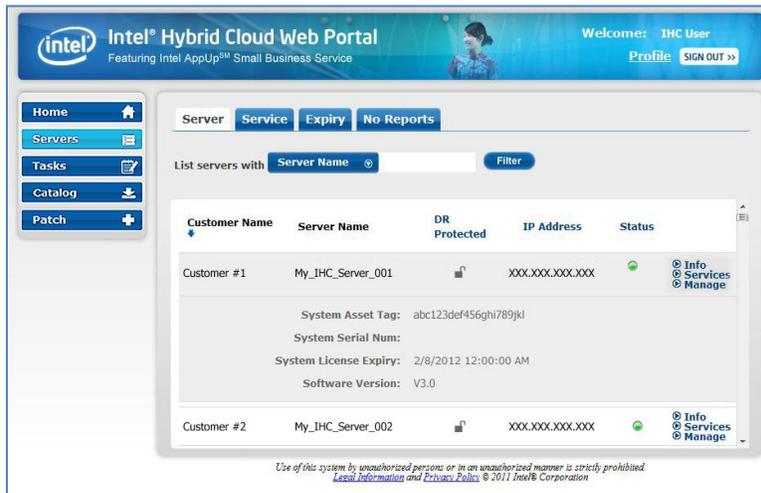


Figure 23. Management Portal – Servers Screen – Info

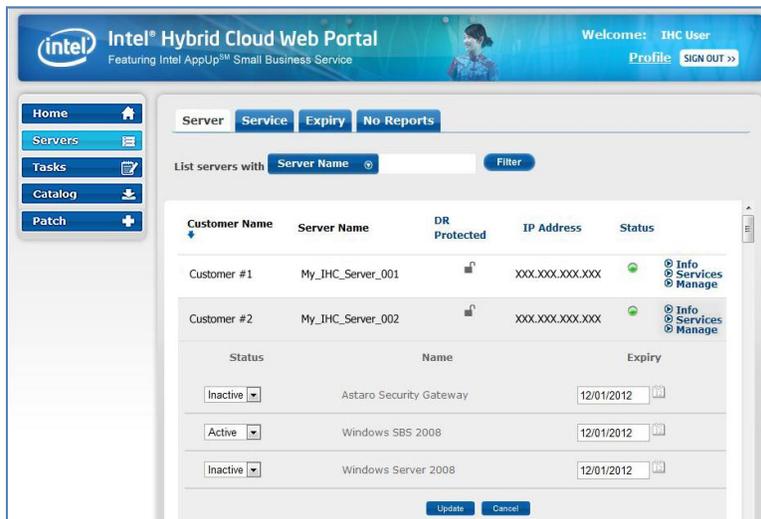


Figure 24. Management Portal – Servers Screen - Services



Figure 25. Management Portal –Servers screen - Manage

5.4 Viewing Your Profile

The “**Profile**” link (next to the “**SIGN OUT**” button on the top right) allows you to view your contact information (note: You cannot edit this information here).

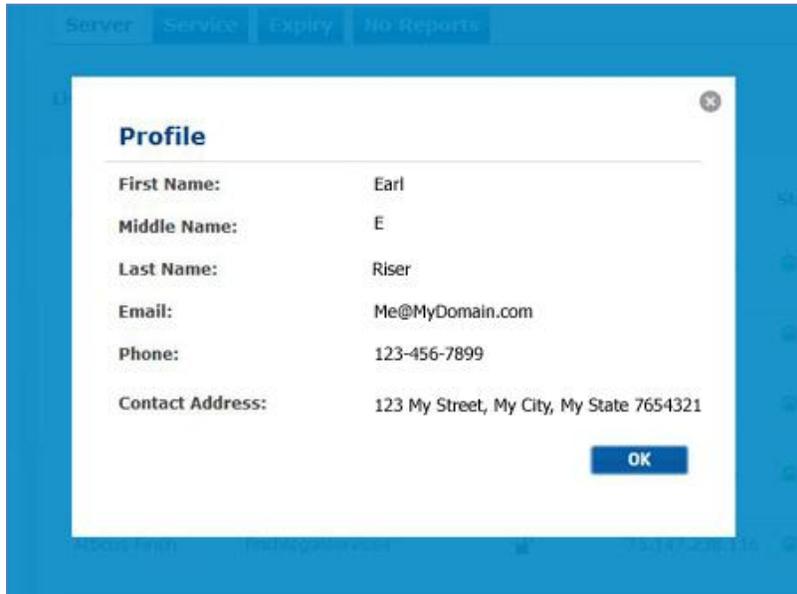


Figure 26. Management Portal – Your Profile

5.5 Appliance & Application Installation

This feature allows you to choose and install appliances and applications directly from the Intel AppUpSM Small Business Service catalog.

NOTE: Appliance and application installation can also be managed through Intel® Hybrid Cloud server manager. Refer to Section 6.2 to access the Intel® Hybrid Cloud server manager, and Section 6.11 for appliance and application installation details.

1. Select the “**Catalog**” tab on the left side of the management portal.
2. Click the “**Install**” button for the desired appliance or application.

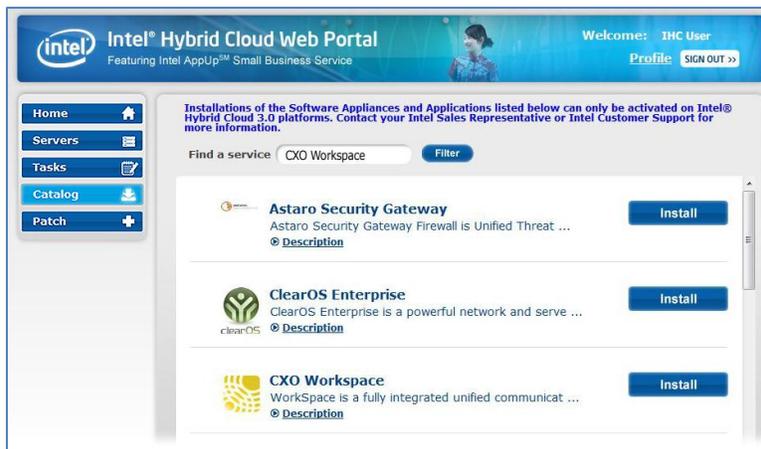


Figure 27 Management Portal - Catalog

NOTE: A search function is provided to quickly find a particular appliance or application. Some software is not compatible with servers running older versions of the Intel® Hybrid Cloud software stack.

1. Select the appropriate server from the list.
2. Click the “**Next**” button.

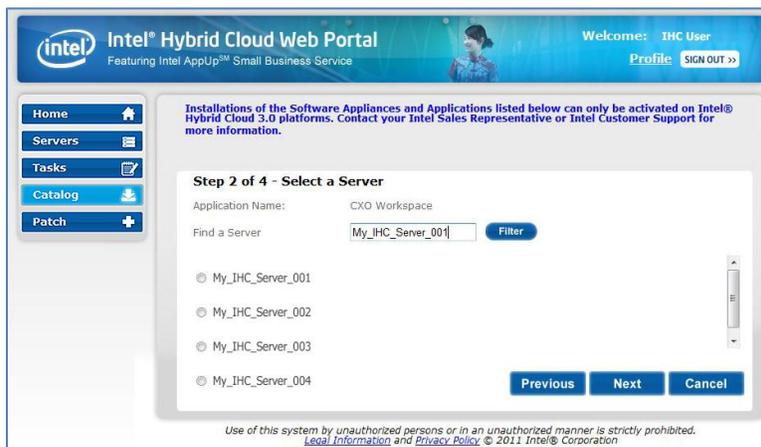


Figure 28 Management Portal – Catalog - Select a Server

- If you are installing an Application, select the appropriate Appliance (for the installation).
NOTE: If installing an appliance, this screen will not appear.



Figure 29 Management Portal – Catalog - Select the Appliance

- If you are installing an Application, read the End User License Agreement (EULA), and accept the terms and conditions by checking the corresponding box.
- Click the “**Confirm**” button to proceed.

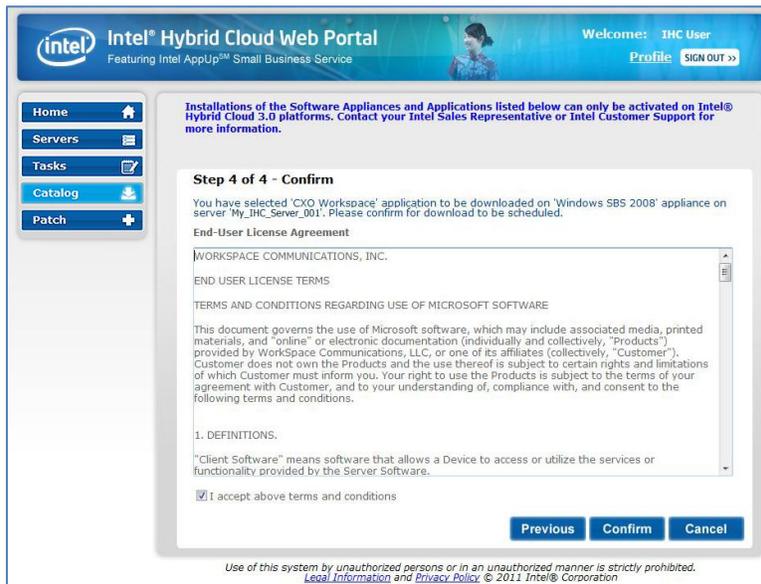


Figure 30 Management Portal – Catalog – Application EULA

6. Click the “**Finish**” button to initiate the download.

NOTE: The software download request will be added to the queue. Downloading and installation will proceed after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

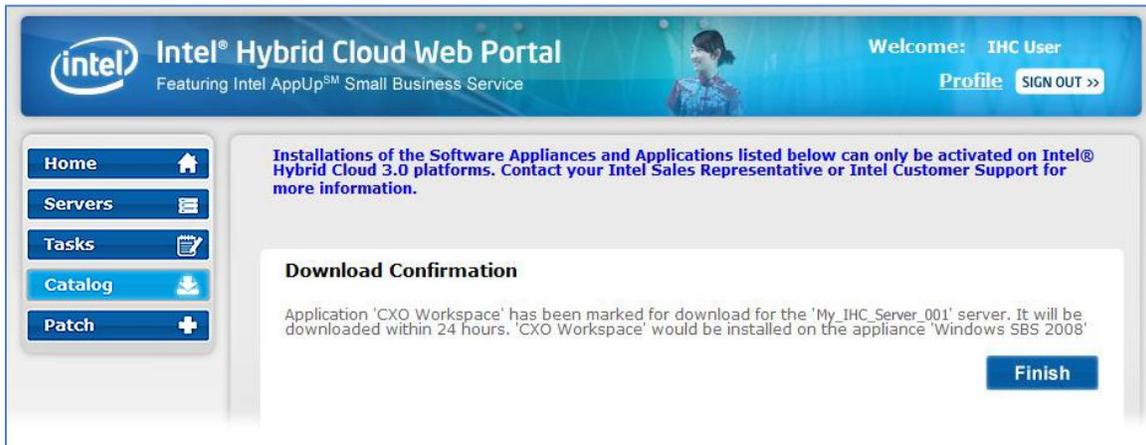


Figure 31 Management Portal – Catalog - Download Confirmation

5.6 Reactivating an Expired Appliance

If the system has not communicated with the Intel® Hybrid Cloud data center for 30 consecutive days, all the running appliances will stop and the appliance licenses will be revoked. The Administrator can use the management portal to re-activate the appliances, re-establishes communication with the management portal.

5.7 Appliance Expiration & Management

Appliance expiration must be managed by the administrator. Starting 15 days prior to the expiration of an appliance license, warning messages will be displayed in the Intel® Hybrid Cloud server manager to indicate the pending appliance license expiration. Email notifications will also be sent to the MSP warning of the pending appliance license expiration. NOTE: The appropriate settings must be entered in the Server Manager in order for email notifications to work properly (Refer to Section 6.7.3 to configure email alerts). After license expiration, there is a 15 day grace period (to use the appliance). Upon expiration of the grace period, the license for the corresponding appliance will be revoked and the appliance will shut down. The Remote Administrator can choose to extend the appliance license from the management portal (to meet end-user requirements).

5.8 View the Applications on an Appliance

The Management Portal allows you to view a list of applications installed on each appliance on any of the servers you manage. To view the applications, select the “**Servers**” screen, the “**Servers**” tab, and the “**Services**” link for a particular server. Appliances with installed applications will display an arrow to the left of the “**Status**” dropdown options. Click the arrow to view the applications on the corresponding appliance (as shown in the following screen).

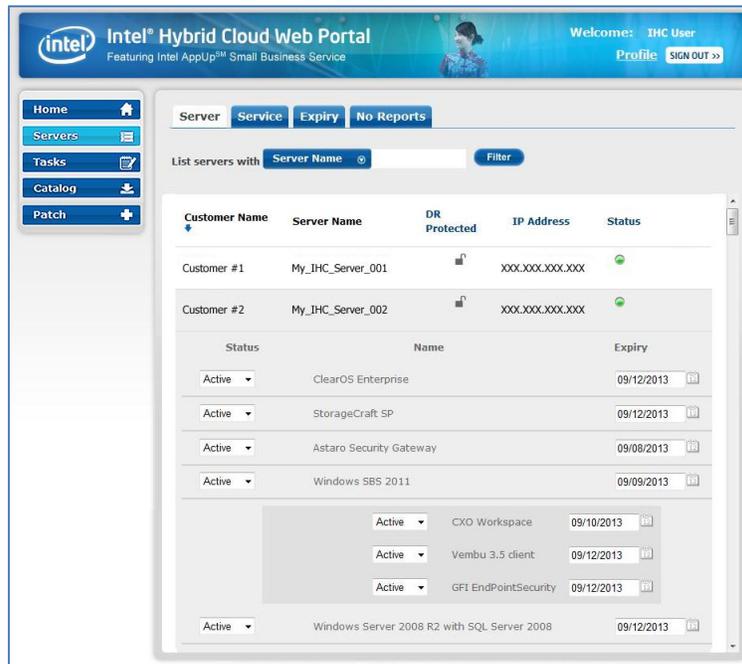


Figure 32. Management Portal – Applications on an Appliance

5.9 Activating or Deactivating an Appliance or Application

The Intel Hybrid Cloud management portal allows you to activate and deactivate appliances and applications. Status change requests will be added to the queue and will take effect after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List on Page 79, (Command: initiate-usage-reporting).

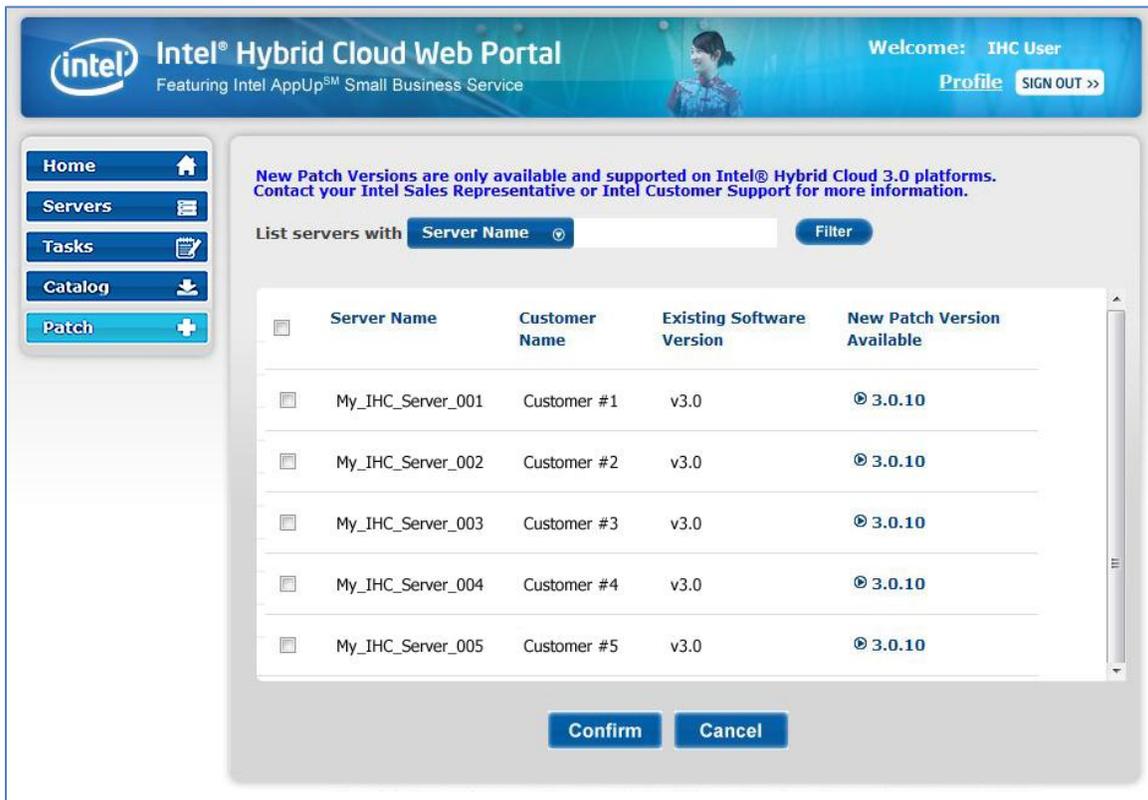


Figure 33. Management Portal – Applications Status Updates

5.10 Server Patch Updates

Select the **"Patch"** button from the navigation menu to view available upgrades for the servers you manage. If an upgrade is available, the servers will be listed along with the available upgrade (i.e. Patch). To apply a patch, select the server (check box) and click the **"Confirm"** button.

NOTE: Patch download requests are added to the queue. Downloading will proceed after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List in Section 11.2, (Command: initiate-usage-reporting, page 79).



The screenshot shows the Intel Hybrid Cloud Web Portal interface. The top navigation bar includes the Intel logo, the text "Intel® Hybrid Cloud Web Portal" with "Featuring Intel AppUp™ Small Business Service" below it, and a user profile section for "IHC User" with "Profile" and "SIGN OUT >>" links. A left-hand navigation menu contains buttons for "Home", "Servers", "Tasks", "Catalog", and "Patch" (which is highlighted in blue). The main content area features a message: "New Patch Versions are only available and supported on Intel® Hybrid Cloud 3.0 platforms. Contact your Intel Sales Representative or Intel Customer Support for more information." Below this is a search bar labeled "List servers with" containing a dropdown menu set to "Server Name" and a "Filter" button. A table lists five servers, each with a checkbox, a "Server Name", "Customer Name", "Existing Software Version", and "New Patch Version Available". At the bottom of the table area are "Confirm" and "Cancel" buttons.

<input type="checkbox"/>	Server Name	Customer Name	Existing Software Version	New Patch Version Available
<input type="checkbox"/>	My_IHC_Server_001	Customer #1	v3.0	3.0.10
<input type="checkbox"/>	My_IHC_Server_002	Customer #2	v3.0	3.0.10
<input type="checkbox"/>	My_IHC_Server_003	Customer #3	v3.0	3.0.10
<input type="checkbox"/>	My_IHC_Server_004	Customer #4	v3.0	3.0.10
<input type="checkbox"/>	My_IHC_Server_005	Customer #5	v3.0	3.0.10

Figure 34. Management Portal – Server Patch Updates

6. Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager provides remote and local access to a variety of management functions. A maximum of 4 simultaneous remote connections are allowed for each Intel® Hybrid Cloud server.

6.1 Installing Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager can be installed in 2 ways.

- Intel® Hybrid Cloud server manager is installed when you setup and register a new server as described in Sections 3 and 4.
- Intel® Hybrid Cloud server manager can also be downloaded and installed from the “**Support**” page on the Intel Hybrid Cloud web site (Login required):
 - a. Use a web browser go to: www.intelhybridcloud.com/
 - b. Click the “**LOGIN**” button and enter your login information.
 - c. Select the “**Support**” link from the menu on the left.
 - d. Select the “**Server Manager**” download link.

6.2 Accessing the Intel® Hybrid Cloud server manager

- After you have installed Intel® Hybrid Cloud server manager, you can access it via the icon on your desktop (or via your Windows* programs menu).
- You may also access the Intel Hybrid Cloud server manager through the Intel® Hybrid Cloud management portal (refer to Section 5.3 for details).



6.2.1 Role Based Access Control for Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager follows a Role Based Access Control (RBAC) mechanism. Two roles are supported by the Intel® Hybrid Cloud server manager:

Role (User ID)	Password
admin	Hybr1dC!0ud
User	Hybr1dC!0ud

The content in this section describes functions and features that can be performed or accessed when logged in as the administrator ("admin" role). The administrator can set privileges for the "User" role.

NOTE: Upon initial login, you will be prompted to change the SW Management password. This is generally done during server setup.

6.2.2 Login to Multiple Servers

You can login to Intel® Hybrid Cloud server manager using Intel® Hybrid Cloud management portal login credentials and see list of all active servers. You can then launch the Intel® Hybrid Cloud server manager for a specific Intel® Hybrid Cloud server.

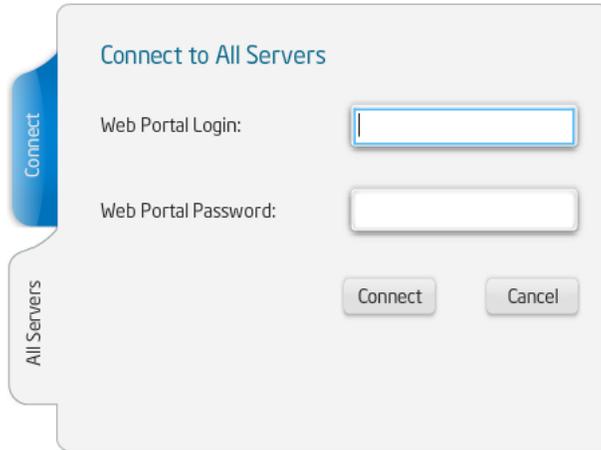


Figure 35. Server Manager – Connecting to All Servers

6.2.3 Login to a Specific Server

In contrast to the "All Servers" tab, the "Connect" tab allows you to connect directly to a particular server. However, you can only connect to servers that you have already registered.

NOTE: If you do not know the Server Name, use the "All Servers" tab (Section 6.2.2) to see a list of your servers.



Figure 36. Server Manager - Login Window

When you access a server for the first time, you need to provide the IP address of the server. After the initial connection, Intel® Hybrid Cloud server manager will remember the server name and IP address, so you will not need to enter it the next time.



The image shows a dialog box titled "Add Server". It has two input fields: "Server Name" with the value "My_IHC_Server_001" and "Server IP" with the value "XXX.XXX.XXX.XXX". Below the input fields are two buttons: "Add" and "Cancel".

Figure 37. Server Manager - Add server to hosts file

NOTES:

- If you are logging into the server for the first time, you will be prompted to change the default password. The SW management password is automatically synchronized with the HW management password (either the Intel® ME/Intel® AMT, or Baseboard Management Controller). Using any other method to change the Intel® AMT password or BMC password will break the synchronization.
- Entering IP address as the Server Name is not allowed. You must enter Server Name to connect to the server.
- On Windows 7, the server manager must be invoked with “administrator” privileges.
- If the server is equipped with Intel® AMT, you can use AMT to connect even if the server is powered down. This feature is available only through Remote Network Interface (Port A). Refer to Section 4.2 for details. In order to connect with AMT, you must provide the Server Name (hostname), and login with the “Admin” role. For details, refer to Section 9.
- If the server is equipped with Baseboard Management Controller (BMC), you can use BMC to connect even if the server is powered down. For details, refer to Section 10.

6.3 Changing the Default SW Management Password

In order to change the “admin” and “user” passwords, you will need to login separately for each role (the default passwords for each are shown below).

1. Open Intel Hybrid Cloud server manager (Run as administrator).
 2. Select the “Connect” tab.
 3. Enter the Server Name and login information:
 - Server Name (created during server setup, Section 4.5)
 - User Name **admin** (or **user**)
 - Default SW Management Password **Hybr1dC!0ud**

NOTE: The SW management password is automatically synchronized with the HW management password (Intel® ME / Intel® AMT / BMC). Using any other method to change the Intel® AMT password or BMC password will break the synchronization.
 4. Press the “Connect” button.
 5. Select the “Configuration” menu and the “Server Settings” tab.
 6. Enter the “Old Password,” and new password information.
 7. Click the “Change password” button.
- NOTE:** Perform the steps above for each role (i.e. “user” and “admin”).

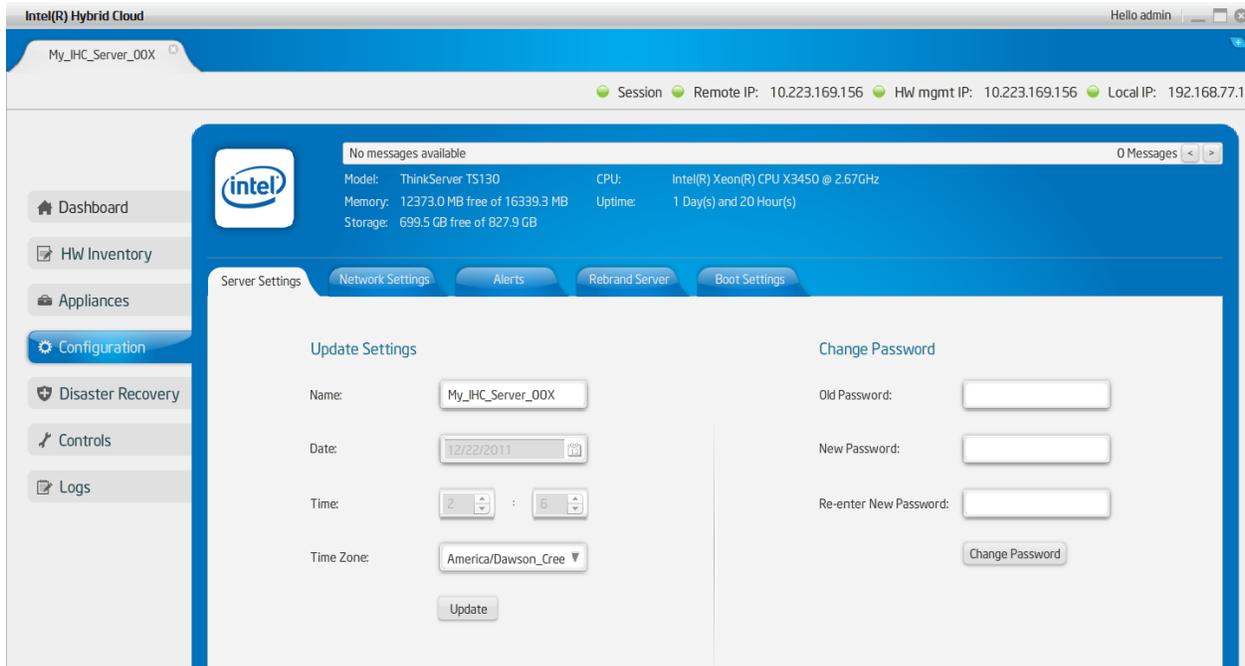


Figure 38. Server Manager – Change the Default Password

6.4 Dashboard

Once connected to an the Intel® Hybrid Cloud server, Intel® Hybrid Cloud server manager “Dashboard” view consists of Intel® Hybrid Cloud server details, main menu, log-in details and a dashboard view. Dashboard consists of three sections as shown in following screen:

- **Usage** — Displays usage graph of Memory, CPU, Disk, LAN, WAN of the server
- **Appliances** — Appliance status listing the installed appliances on Intel® Hybrid Cloud server and their current power state (Starting/Stopping/suspending/halted/Suspended/Importing/Running)
- **Software Logs** — A table of logs that show the last five log entries which could be information, warning, alert or error messages. Each entry has a record ID, timestamp and description. By default, messages that indicate “Errors” are displayed. By choosing the appropriate radio button on top of the messages, different categories of error messages can be viewed.

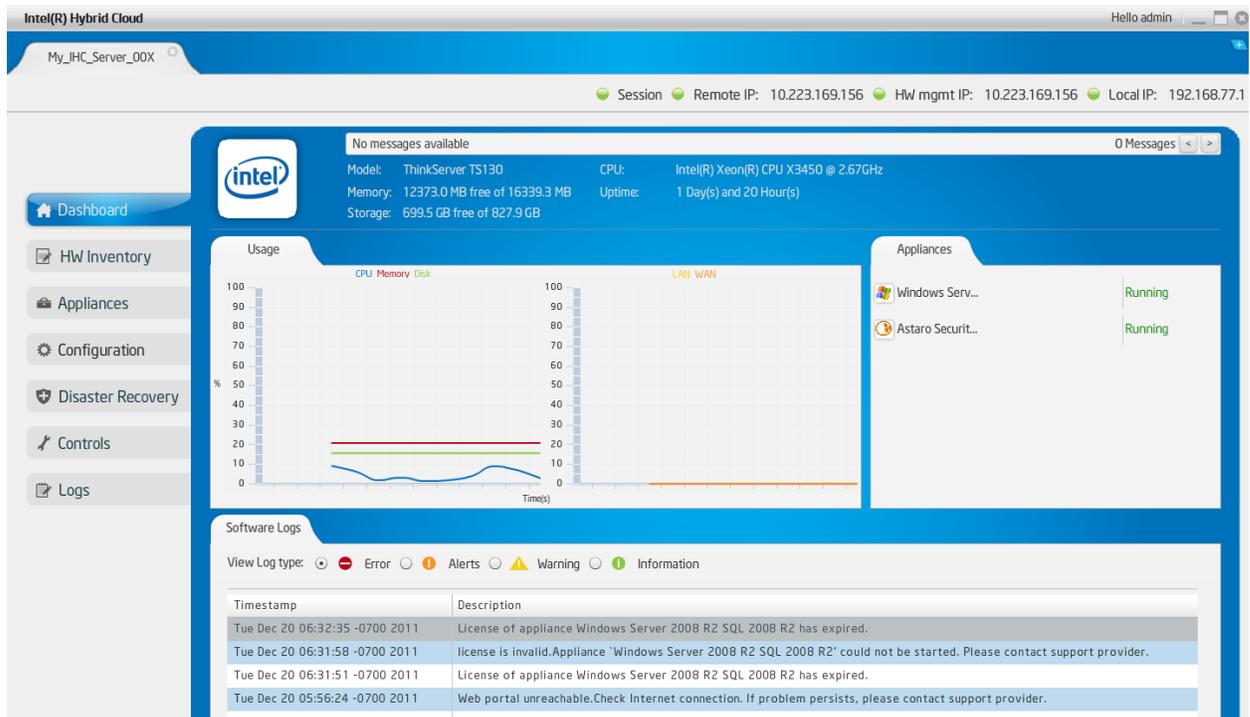


Figure 39. Server Manager - Default view (Dashboard)

A **Message Ticker** also appears at the top of the screen. This ticker will display important messages about any failures that may have occurred or if patches are available for install.

6.5 Hardware Inventory

The "Hardware Inventory" screens provide detailed HW information for the Intel® Hybrid Cloud server via Intel® AMT or Baseboard Management Controller (BMC). This option is available only for the “admin” role when connected through the remote interface. A sample screenshot for system information is shown below. Similar data is available for processors, memory, and disk.

NOTE: AMT and BMC features like HW inventory, HW events, force shutdown, and force restart are ONLY available through Remote Network Interface (Port A). Refer to Section 4.2 for details. BMC systems do not support disk data.

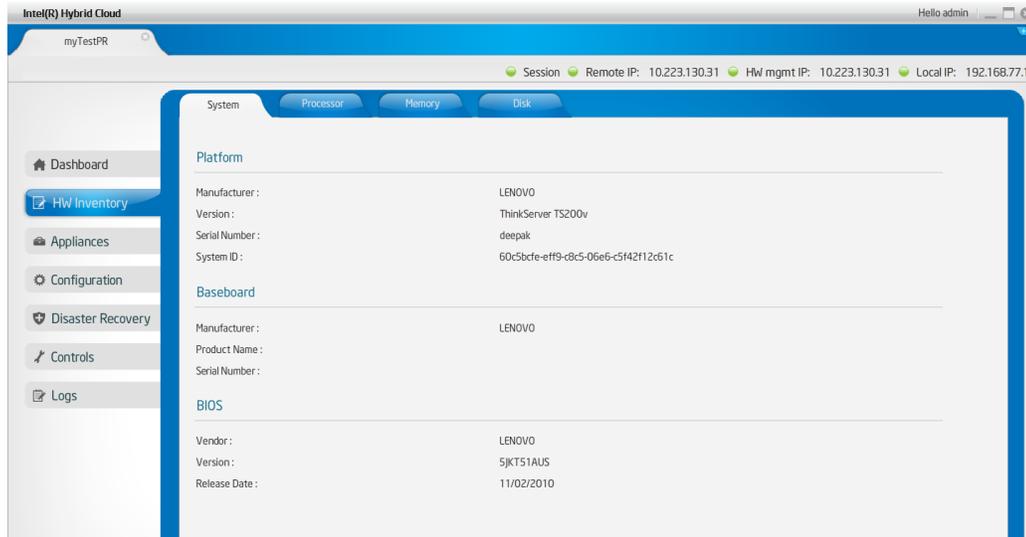


Figure 40. Server Manager - Hardware Inventory - System Information window

6.6 Appliances

Appliances installed on Intel® Hybrid Cloud server can be managed using the “Appliance” menu. The default (“Monitor” tab) view under this menu option displays icons for all available appliances, along with the respective power status of each. You can select any appliance to manage it. Appliance details (i.e. name, vendor, and version) are shown along with buttons to start, stop, suspend, or resume the appliance (depending upon its current state). For example, if an appliance is already started, the option to “stop” and “suspend” it are available. After installing an appliance, it will default to the “Stopped” state. Appliances can also be uninstalled only in the “Stopped” state.

An appliance can be “Started” or “Resumed” only when the license is set to the “Active” state in the Intel® Hybrid Cloud management portal (see Section 5.9). When you attempt to start an appliance, a license query is sent to the management portal. If the license is “Active,” the appliance will be permitted to start. If the license is not active, an error message will be displayed. Appliances may also be started or stopped using the management portal (see Section 5.9).

If the appliance license has expired, you are allowed to use the appliance for a grace period of 15 days post license expiry date, after which the appliance will be suspended (and non-operational). Warning messages will be displayed 15 days prior to the expiry of the appliance license and error messages will be logged during the grace period.

6.6.1 Appliances - Monitor

The “Monitor” tab provides access to view resource details such as, Memory, Disk, and CPU.

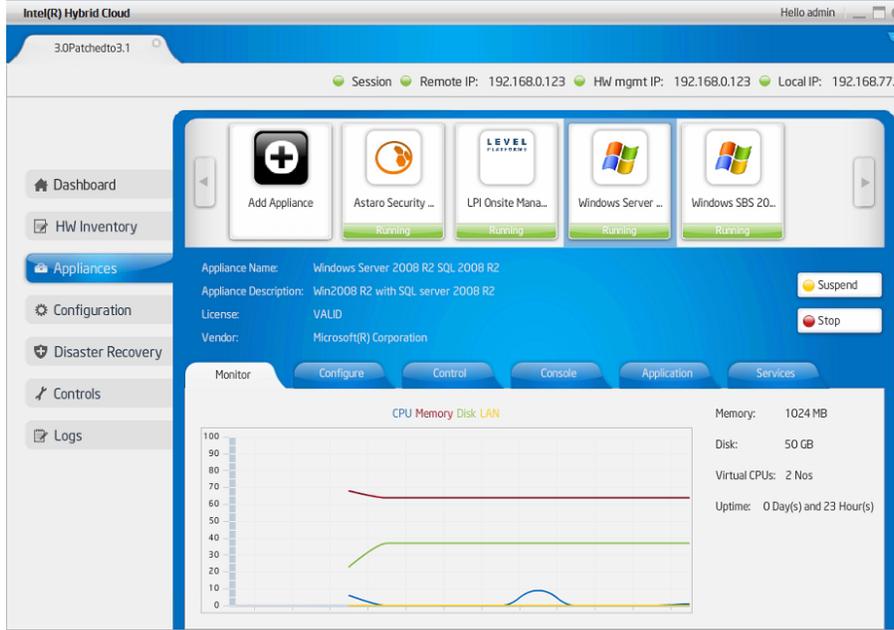


Figure 41. Server Manager - Appliances Monitor window

6.6.1.1 Appliance and Application Download

6.6.2 Appliances - Configure

The "Configure" tab allows you to manage the variables that you initially set when installing your appliances. These variables include Appliance Name, number of Virtual CPUs, total Memory allocated, add or delete storage devices and network interfaces.

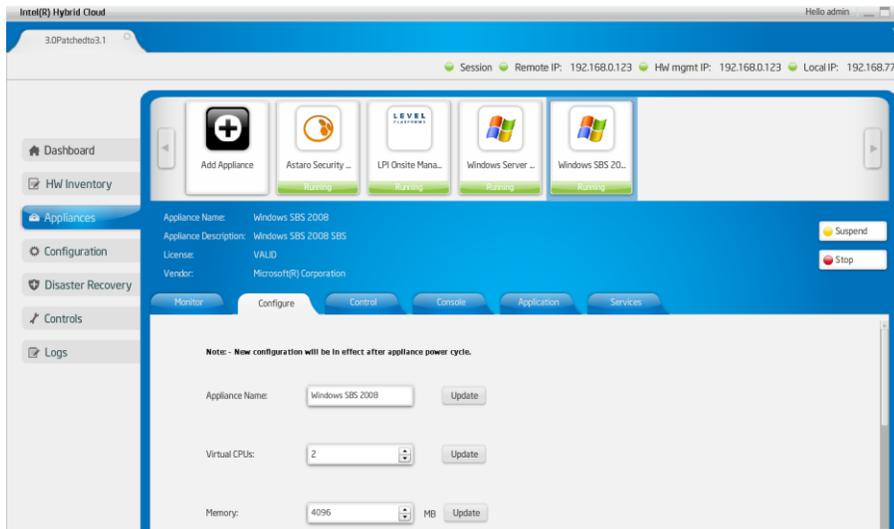


Figure 42. Server Manager - Appliances Configure window

NOTE: You can add or remove storage devices and network interfaces when the appliance is in stopped. Configuration changes take effect only when the appliance is restarted.

6.6.3 Appliances - Control

The "Control" tab allows you to backup an appliance to a USB drive that is directly connected to the server. The USB drive must have free space equal or greater than the size of the appliance you are backing up, and must be formatted in NTFS. Use the "USB Storage" button or the "CD/DVD ROM" button to attach or detach drives to an appliance for backup and restore functions. Once backed up, the appliance can be restored from the USB disk at a later time. For appliance restoration details, refer to Section 6.6.7.

The "Control" tab also allows you to remove appliances with the "Uninstall" button. Additionally, a CD/DVD ROM can be attached as virtual device inside an appliance (e.g. to copy data).

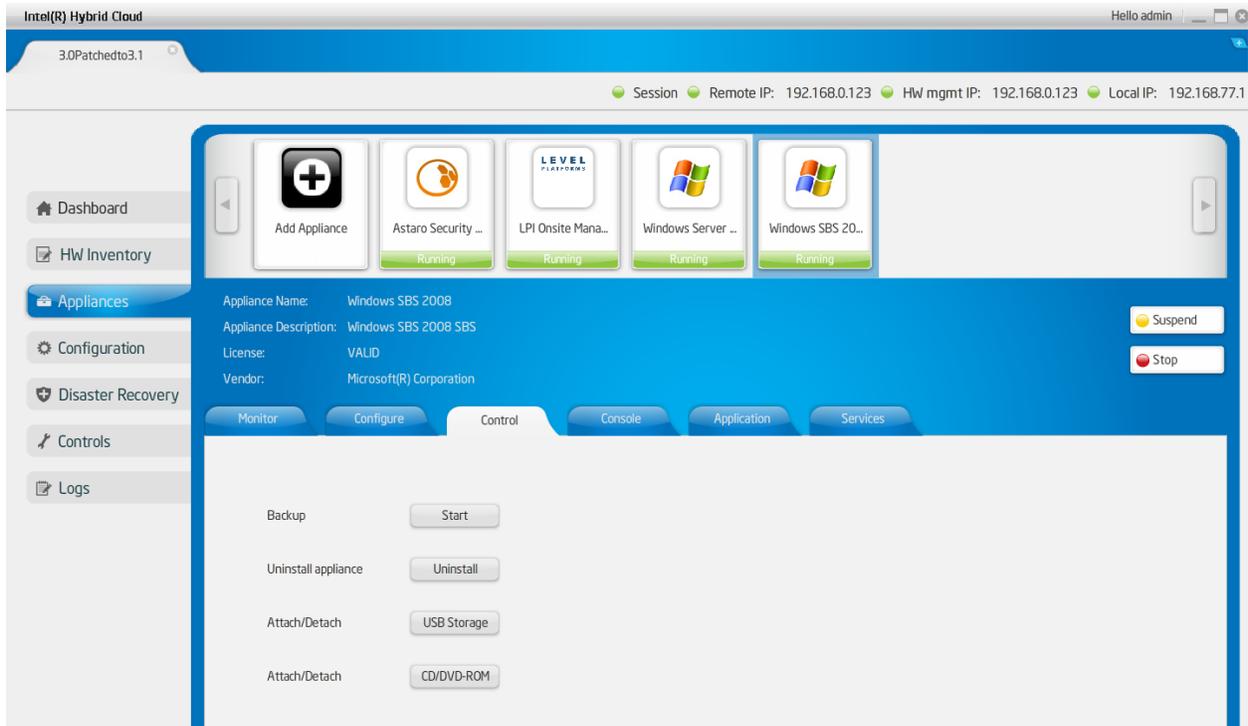


Figure 43. Server Manager - Appliances Control window

6.6.4 Appliances - Console

The "Console" tab allows you to launch the VNC console for an appliance that is running. You can open only one console per appliance. Each console can be closed only from the original session. You may also use Remote Desktop to view the console of an appliance (note: RDP protocol must be supported and configured properly).

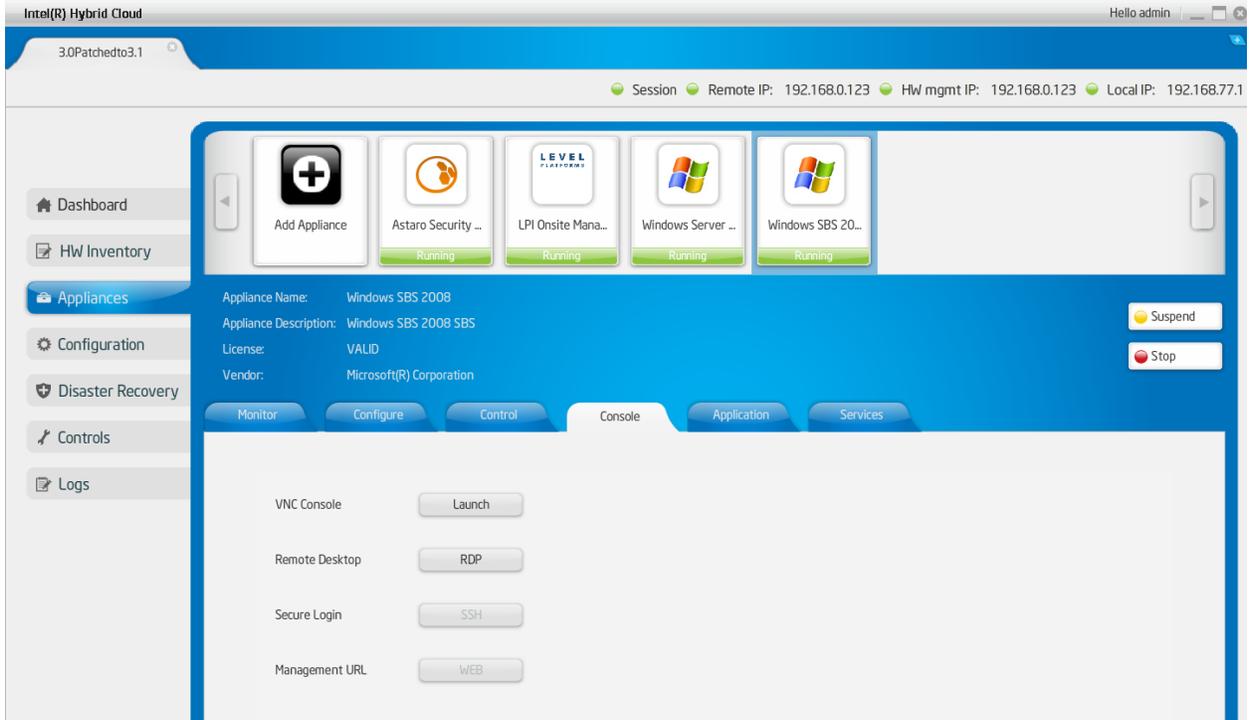


Figure 44. Server Manager - Appliances Console Screen

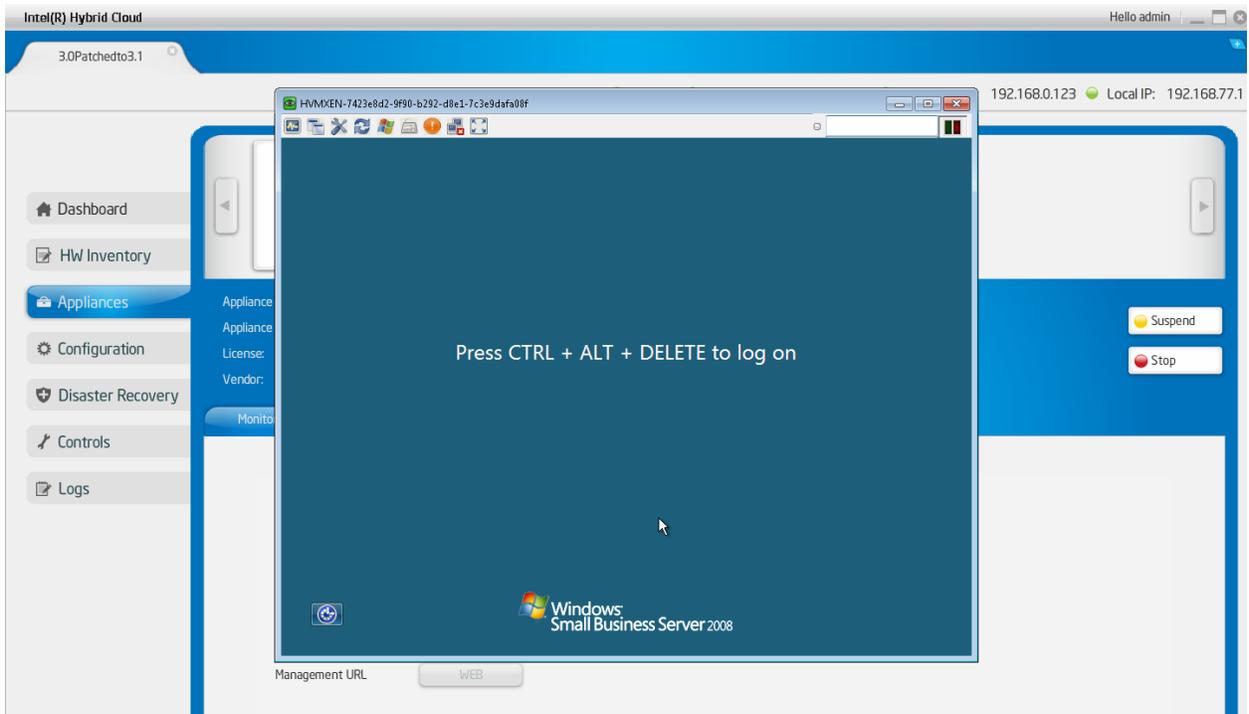


Figure 45. VNC Console

6.6.5 Appliances - Application

The "Application" tab provides access to the applications within each appliance. Select the appliance icon at the top of the screen to view the corresponding applications.

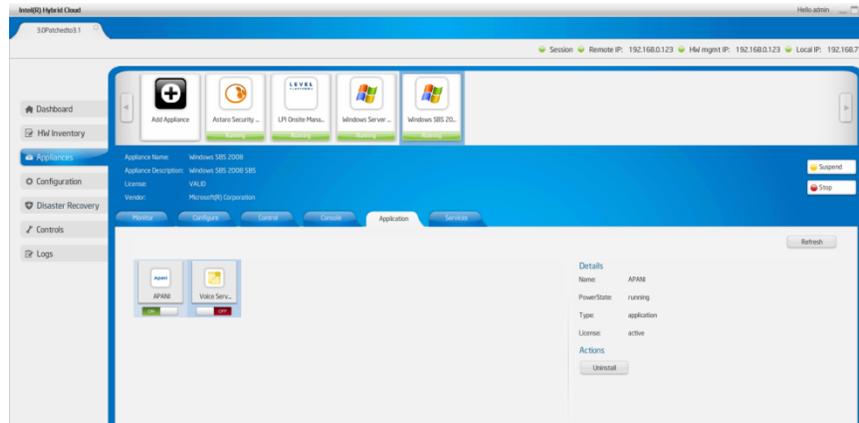


Figure 46. Server Manager – Appliance Services

Following controls are provided for each application:

Start

To start the application, right click the application icon and select the "Start" option. If the application requires a EULA, it will be displayed. When you accept the agreement, a license key will be retrieved from the portal; the application will be activated and allowed to start.

Stop

To stop the application, right click the application icon and select the "Stop" option.

Uninstall

An "Uninstall" button is available under the "Actions" section. Choose the appropriate application and click the "Uninstall" button.

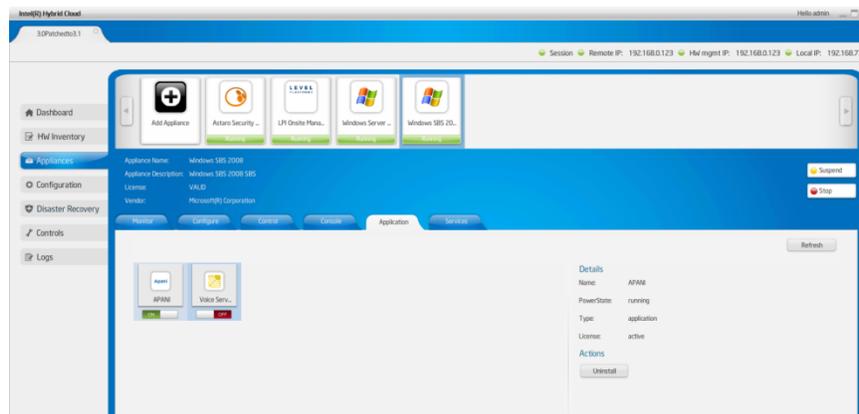


Figure 47 Server Manager - Applications tab under Appliances

6.6.6 Appliances - Services

The "Services" tab provides access to the services within each appliance. Select the appliance icon at the top of the screen to view the corresponding services.

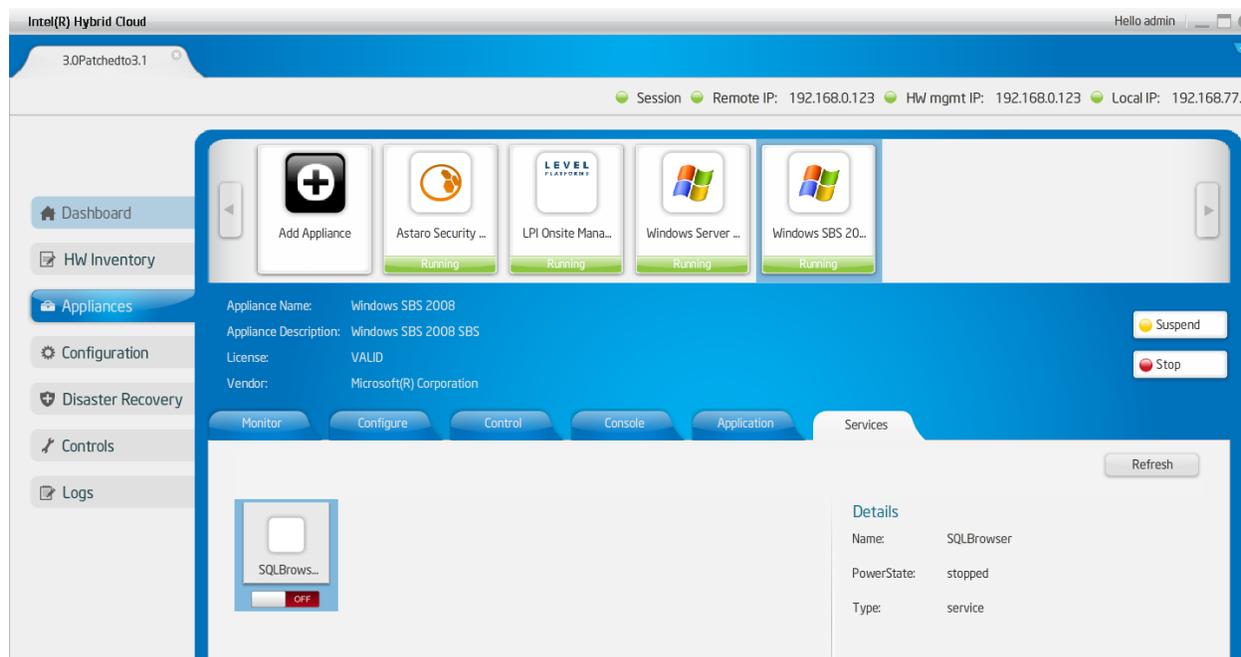


Figure 48 Server Manager - Services tab under Appliances

Following controls are provided for each service:

Start

To start the service, right click the service icon and select the "Start" option. If the service requires a EULA, it will be displayed. When you accept the agreement, a license key will be retrieved from the portal; the service will be activated and allowed to start.

Stop

To stop the service, right click the service icon and select the "Stop" option.

Uninstall

An "Uninstall" button is available under the "Actions" section. Choose the appropriate service and click the "Uninstall" button.

6.6.7 Appliances - Restore

The appliances that were backed up on to a USB disk can be restored via this tab. Once the user connects the USB disk containing backed up appliance images, this tab will show a list of all the backed up appliances. User can select any appliance and click on the restore button provided. The restored appliance needs to be activated again via the management portal before it can be used (see Section 5.9). The restore operation will install the previously backed-up appliance. The older appliance will still be present and has to be deleted manually if required. Refer to Section 6.6.3 to see how to delete an appliance. Also note that images backed up on a machine can be restored on any other IHC server, provided the hardware configuration of the machines match.

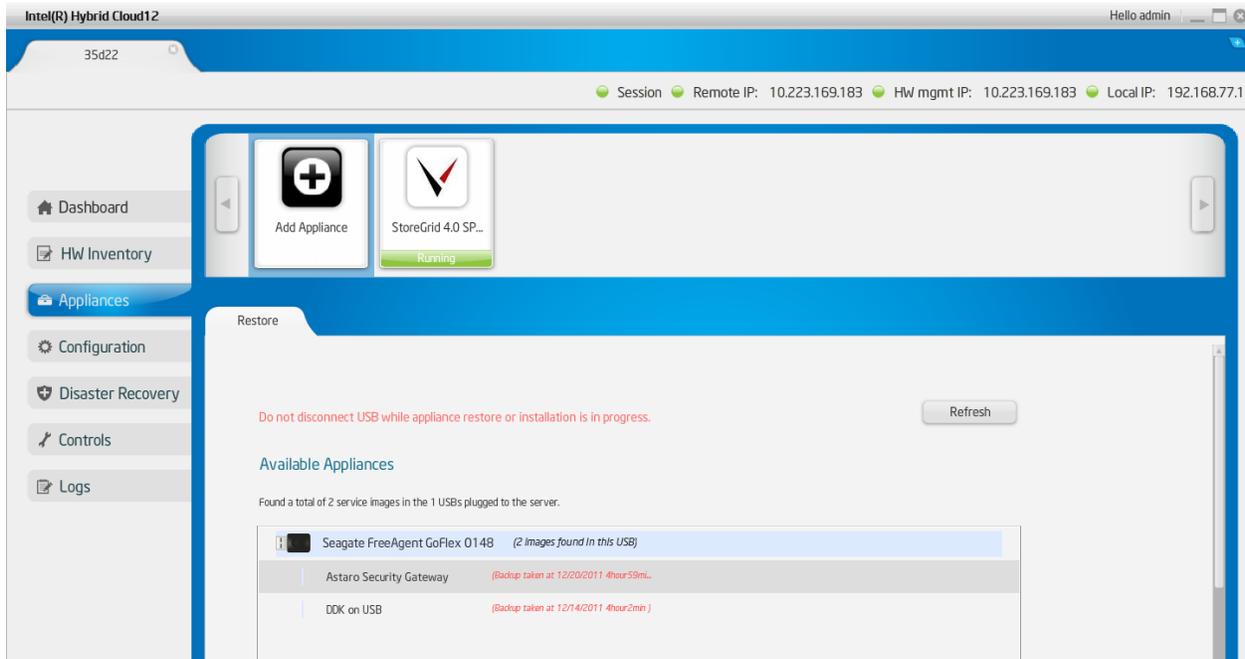


Figure 49. Server Manager - Appliances Restore Screen

6.7 Configuration

This feature can be used to configure Intel® Hybrid Cloud server and also to perform few other tasks like changing password, appliance boot settings, etc. Functionality of these features is explained in the following sections.

6.7.1 Server Settings

This tab can be used to configure System name, update time zone and change password will sync both system and Intel® AMT or BMC password.

NOTE: allowed characters for System name are:

A-Z (uppercase letters) a-z (lowercase letters) 0-9 (numeric digits) . (period) – (dash)
_ (underscore)

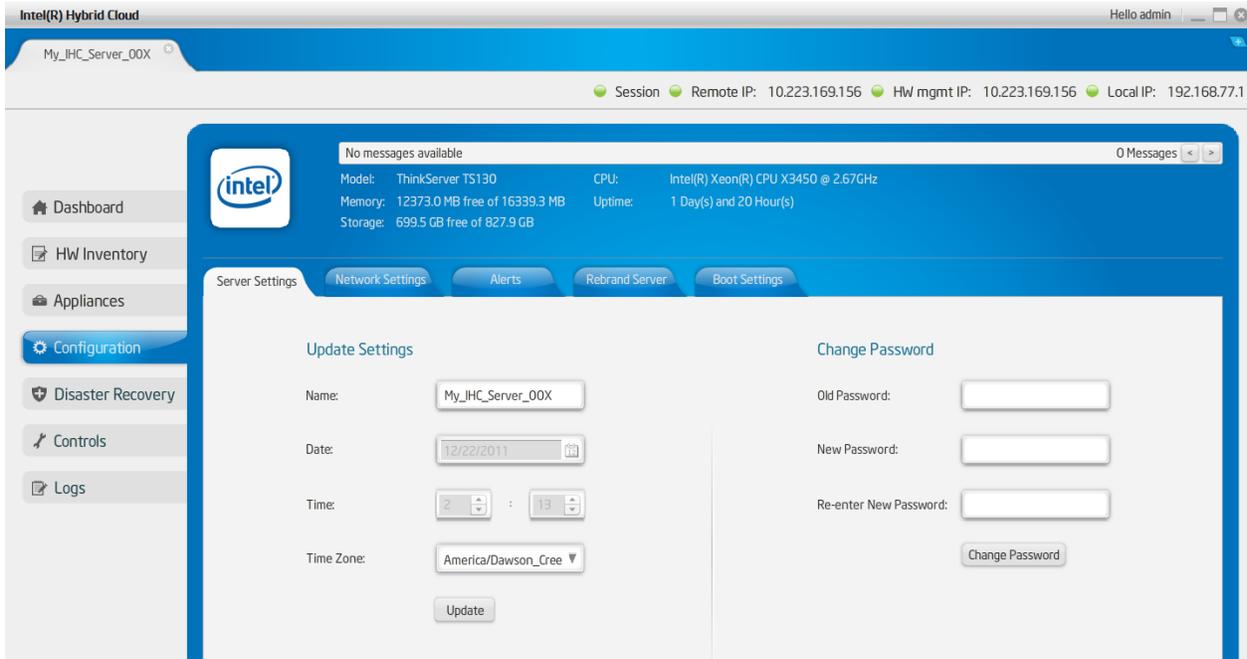


Figure 50. Server Manager - Configure Server Settings window

6.7.2 Network Settings

This tab can be used to configure local and remote interfaces of the Intel® Hybrid Cloud server. If one updates the interface through which the user is connected, it displays a warning message before it proceeds.

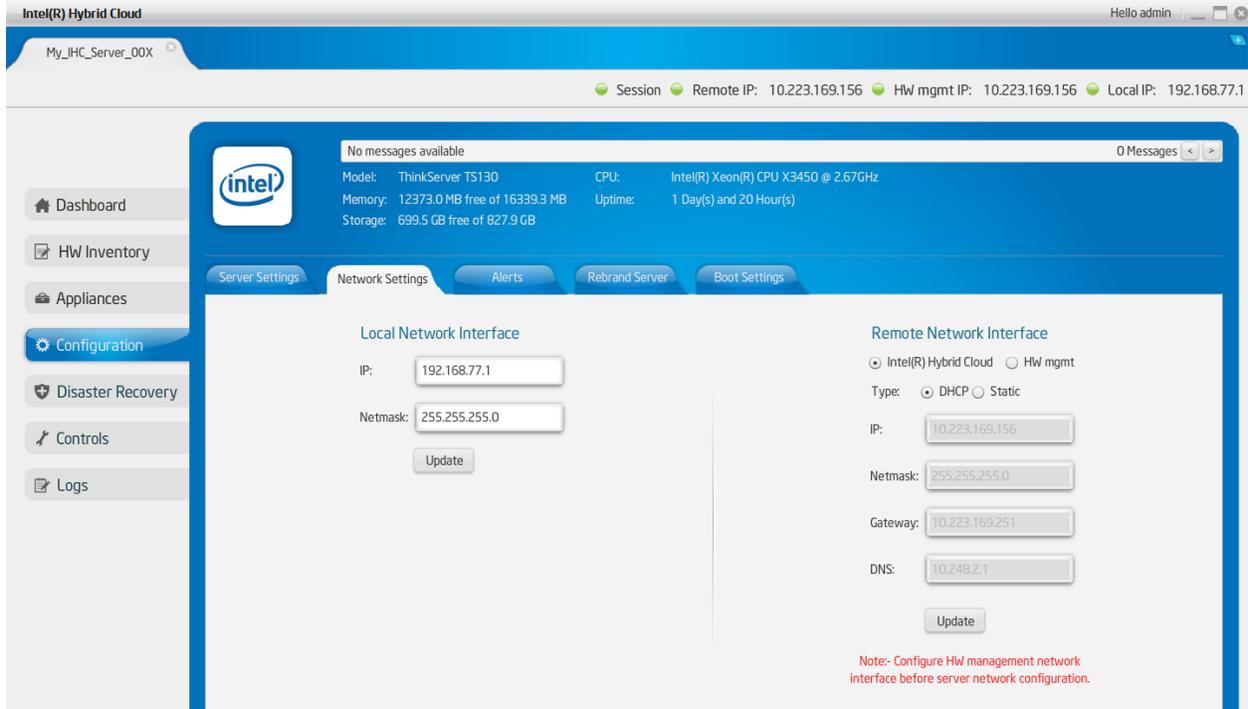


Figure 51. Server Manager - Configure Network Settings Screen

6.7.3 Configuring Email Alerts

This tab lets the admin and user configure the email settings and select the software alerts that can be received from the Intel® Hybrid Cloud server by email. The Server email/SMTP configuration can be updated only by admin. The DNS name of the SMTP server needs to be configured. The user and admin can configure their email addresses to which the alerts are sent and also the specific type of logs for which Intel® Hybrid Cloud server should send the alert emails.

Note: Currently, under the “Server email configuration” option, support is provided only for TLS/STARTTLS Ports. Therefore add only such SMTP mail servers. The most popular example of such a qualifying email service is Google’s Gmail* (smtp.gmail.com). Refer to the technical documentation of your email provider to check if it provides TLS/STARTTLS ports.

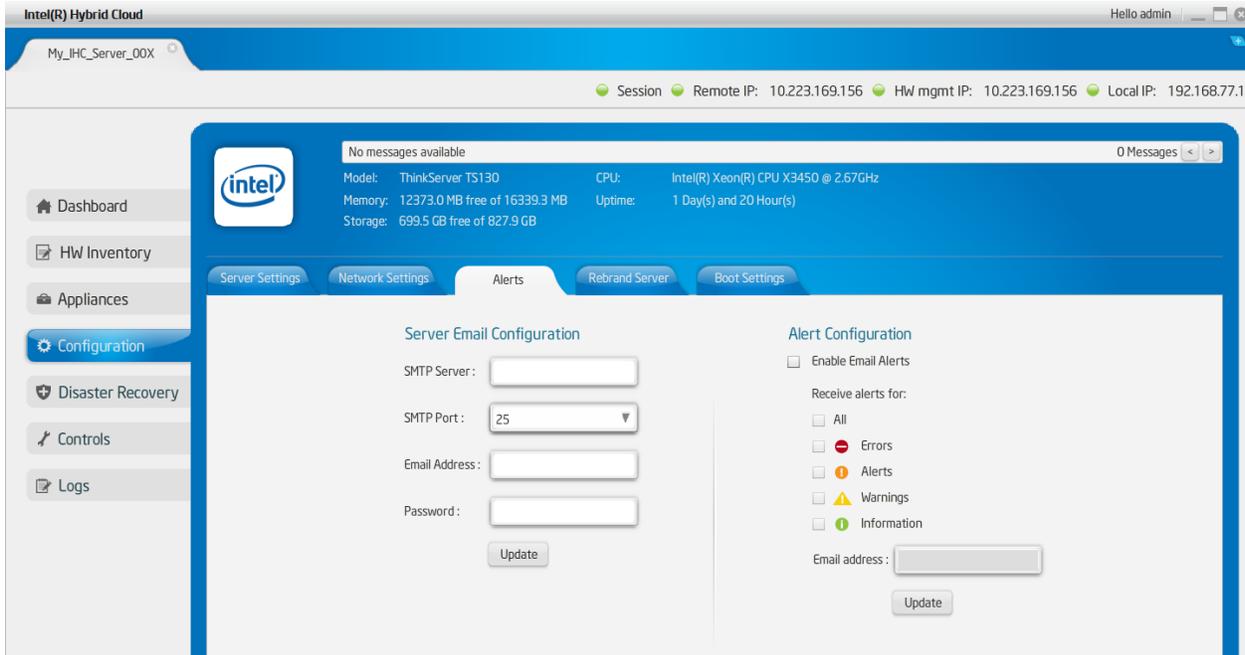


Figure 52. Server Manager - Alerts (Email) Configuration window

6.7.4 Rebrand Intel® Hybrid Cloud server

This option helps OEM/ Remote Administrator/MSPs to rebrand server by changing Vendor name, Client name, logo, and EULA. This option is available only for “Admin” role.

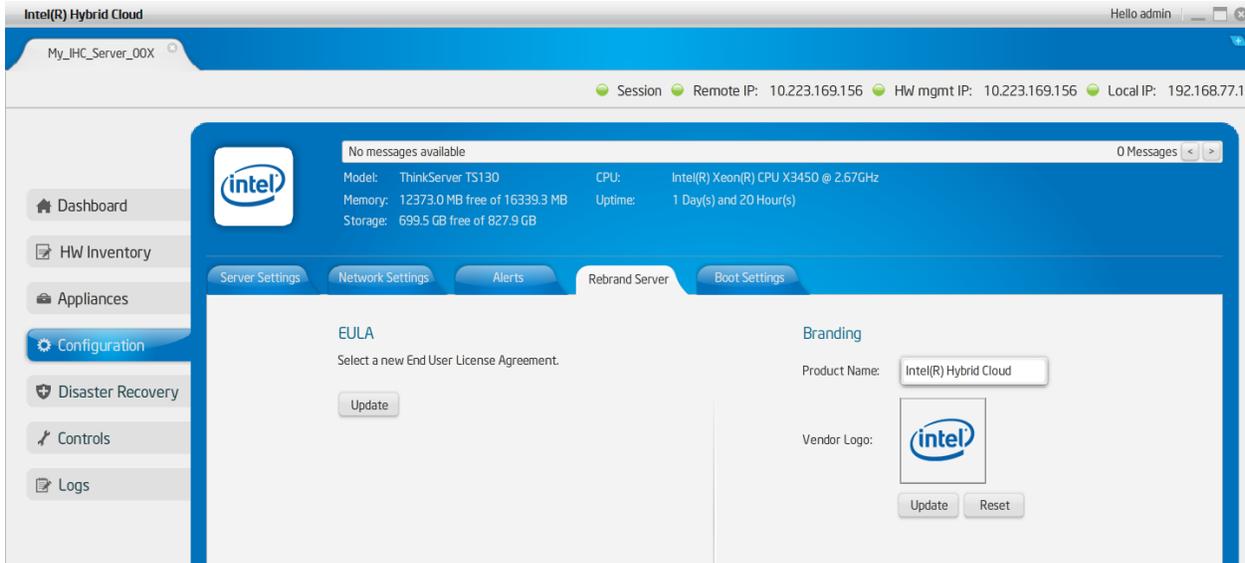


Figure 53. Server Manager - Rebrand Server screen

6.7.5 Configure Boot Settings

This tab can be used to change the order in which appliances should automatically start up post server boot. User can drag and drop to change the order. This order is only applicable on the subsequent boot.

Note: Reorder option for appliances is available only for admin role. Appliances marked to run on boot should have valid licenses installed. Without a valid license, appliance will not be started automatically or otherwise.

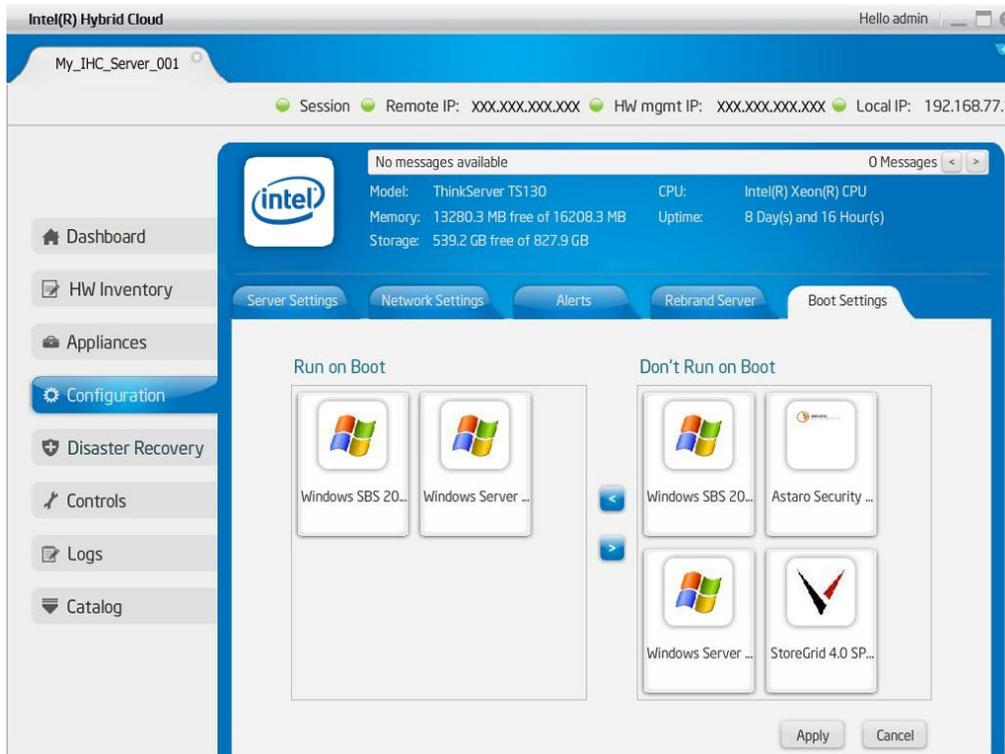


Figure 54. Server Manager - Configure Boot Settings window

6.8 Disaster Recovery

As the Intel® Hybrid Cloud platform works as a one-stop solution for all IT requirements of an SMB, the Intel® Hybrid Cloud server will be the backbone of IT in the SMB premises. Intel® Hybrid Cloud provides an option to subscribe for Disaster Recovery capability wherein the customer will get two Intel® Hybrid Cloud servers. One of the servers acts as a primary server and this server will run the customer applications and IT services. The second server is the secondary server and will mirror the primary server. In the event of the primary server failing, the secondary server can be activated, and the customer can have their business up and running with very minimal downtime.

6.8.1 Setup

Setting up Disaster Recovery is a single step process. Once both the primary and secondary servers are booted, launch the Intel® Hybrid Cloud server manager and connect to the primary server and navigate to the Disaster Recovery screen. This view provides a DR Setup option as given in the screenshot below.

When using a new secondary server that has not yet been registered or activated, follow steps 1-6 of the Quick Start Guide (e.g., configure network in the web interface, register, activate, connect port A and port B accordingly), but do not connect to the secondary server via the Intel Hybrid Cloud server manager. The Quick Start Guide is available here:

<http://www.intel.com/support/motherboards/server/hybrid/sb/CS-031725.htm>

When using a secondary server that has been registered and activated previously, login to the secondary server via Intel Hybrid Cloud server manager, ensure the network settings for both remote and local networks are correctly configured, and change the password to the default (Go to Configuration → Server Settings → Change Password. The password should be changed to the default password: **Hybr1dC!0ud**

Log out of Intel Hybrid Cloud server manager on the secondary server, and continue with the Disaster Recovery setup on the primary server (via Intel Hybrid Cloud server manager).

The MSP must enter the Remote/WAN IP address of the secondary server and the Local/LAN IP address that the MSP wants to configure as the secondary server. Both machines must be able to reach each other on the Remote/WAN interface. They need not be on the same network but must be reachable via a router or gateway. Both machines, though, must be on the same LAN.

The name of this secondary server is set, by default, as the “<primary-server-name>_clone”. This can be modified if the secondary server has been named differently.

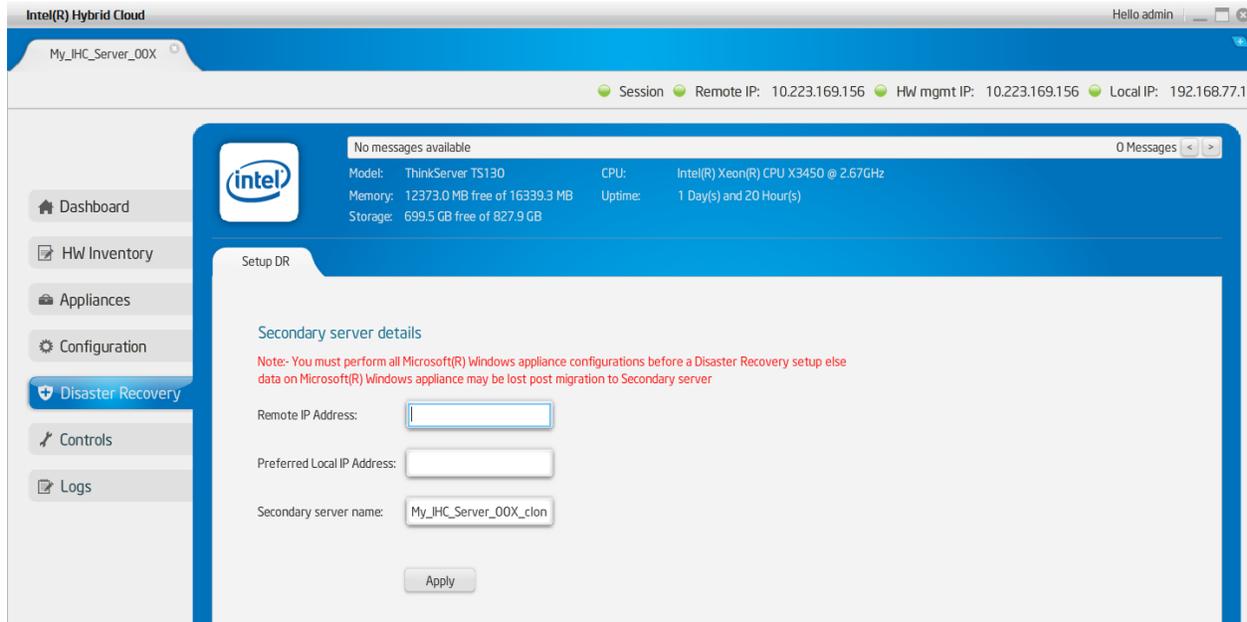


Figure 55. Secondary server details window

Once these details are entered, Intel® Hybrid Cloud software stack configures LAN interfaces of the machines to enable the communication between the servers. Once the LAN is configured, Intel® Hybrid Cloud software stack waits for 5 minutes to connect the LAN interfaces of the two machines and thus enables the communication between machines.

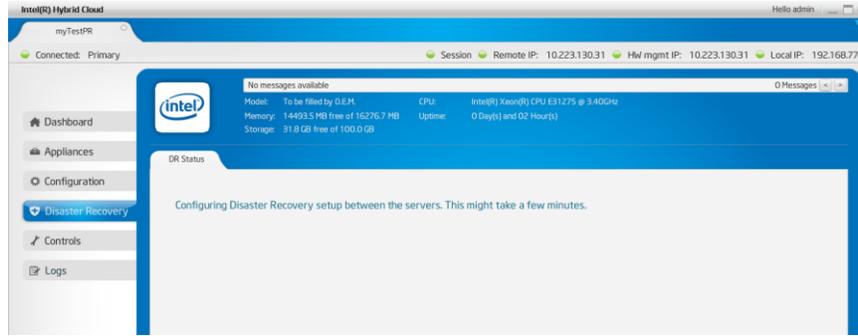


Figure 56. Server Manager - Configuring Disaster Recovery between servers

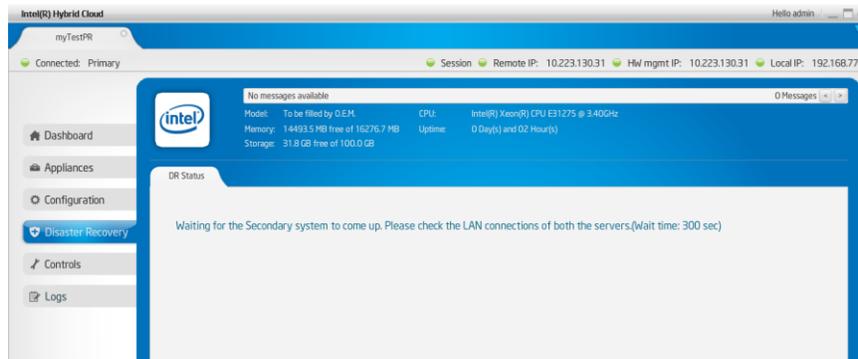


Figure 57. Server Manager - Waiting for Secondary systems to come up

Once the communication between the machines is enabled, the DR sync process starts.

After the DR setup is done, this view shows the present state of the servers for Disaster Recovery setup. It shows the DR Sync percentage for each appliance. Please refer the following screenshot.

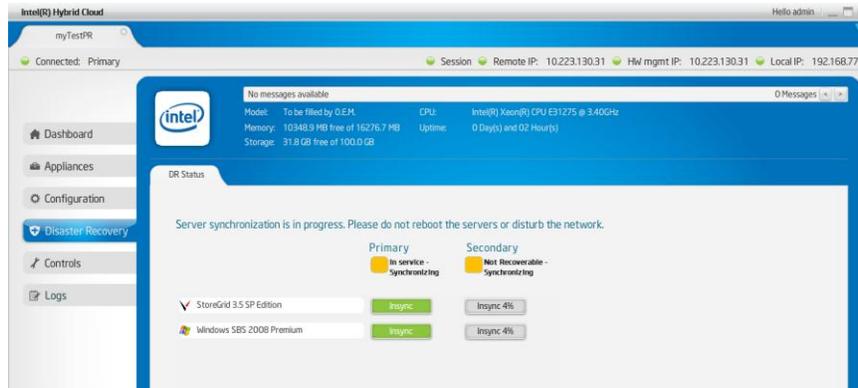


Figure 58. Server Manager - Synchronization in progress

During Sync, the resource on the mirror server would be in a non-recoverable state. Please refer to the screenshot above.

Once the complete sync is done, the view would show the state of each of the servers. Please refer the following screenshot.

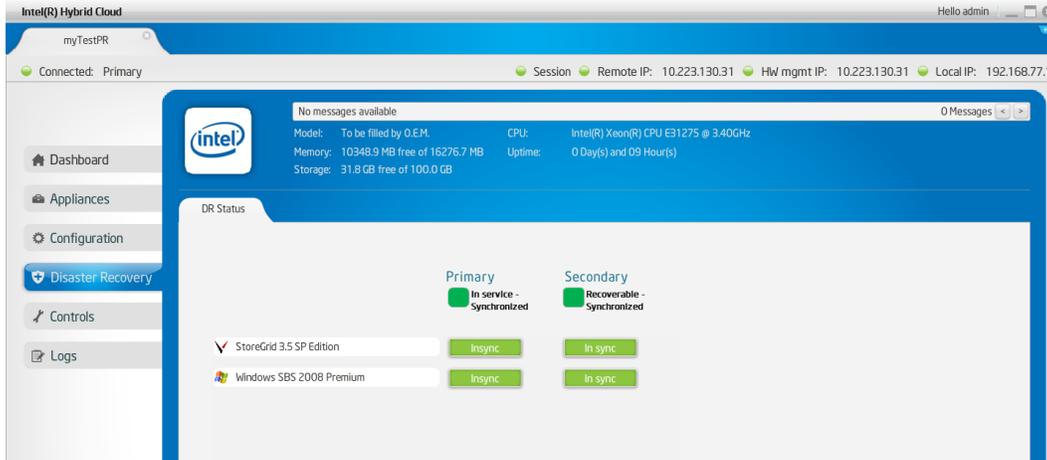


Figure 59. Server Manager - Synchronization complete

Intel® Hybrid Cloud software stack keeps syncing the VM metadata and various other system details (network details, API ACL, SMTP) between the servers so that the switch over during a failure would be as easy as possible for the MSP.

Once the DR setup is done, the dashboard of the Server Management console shows the usage of the mirror server too. Please refer to the following screenshot.

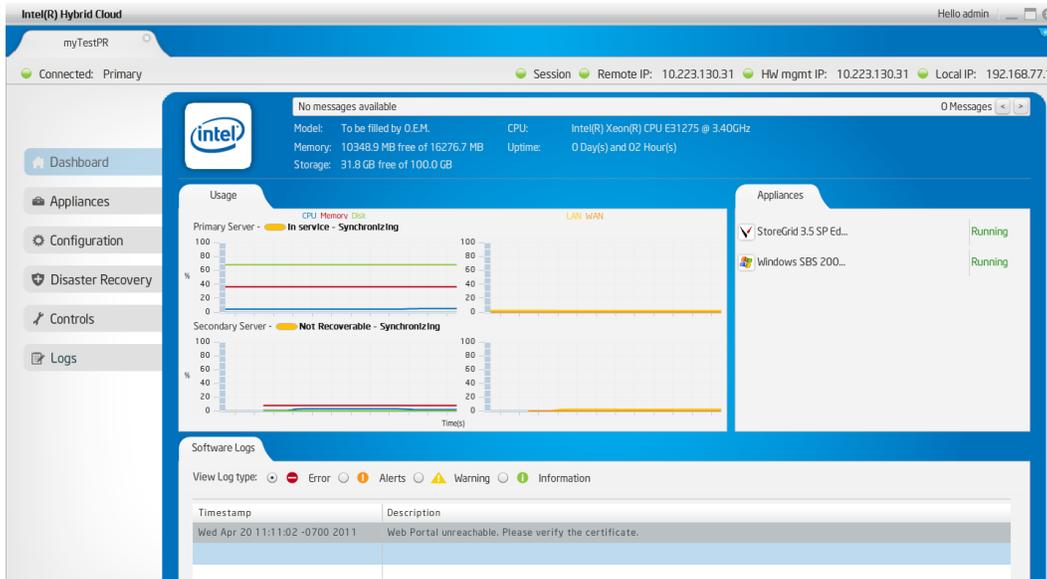


Figure 60. Server Manager - displaying usage of the mirror server

6.8.2 Recover from Primary Server Failure

Once the DR Setup is done, and, if at some point, the Primary server encounters a hardware/software failure, the secondary machine can be brought into service. This would bring back the IT infrastructure of the SMB in a matter of few minutes. When a user/MSP connects to

the secondary server while the primary server is down, the following is displayed as the server status.

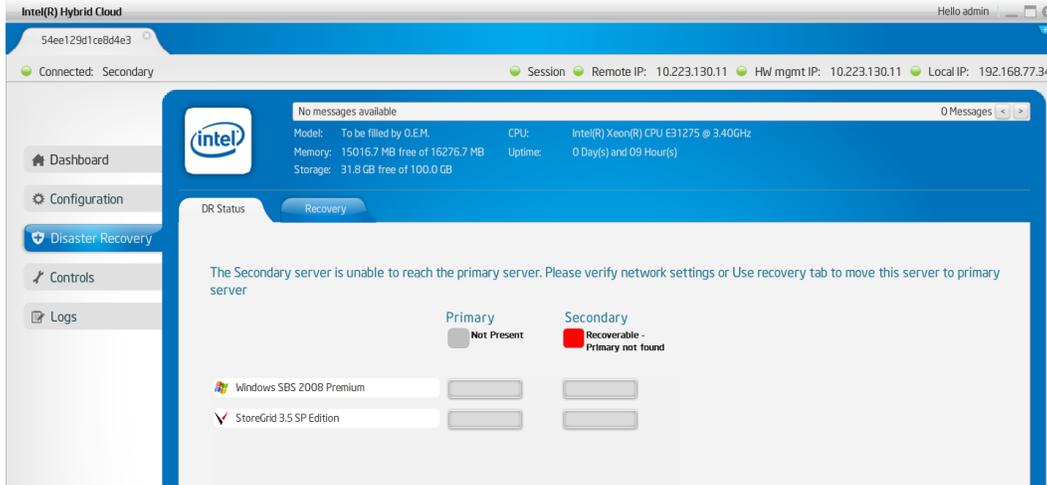


Figure 61. Server Manager - Server status message

Also, the dashboard shows the appropriate status of the machines. Please refer to the screenshot below.

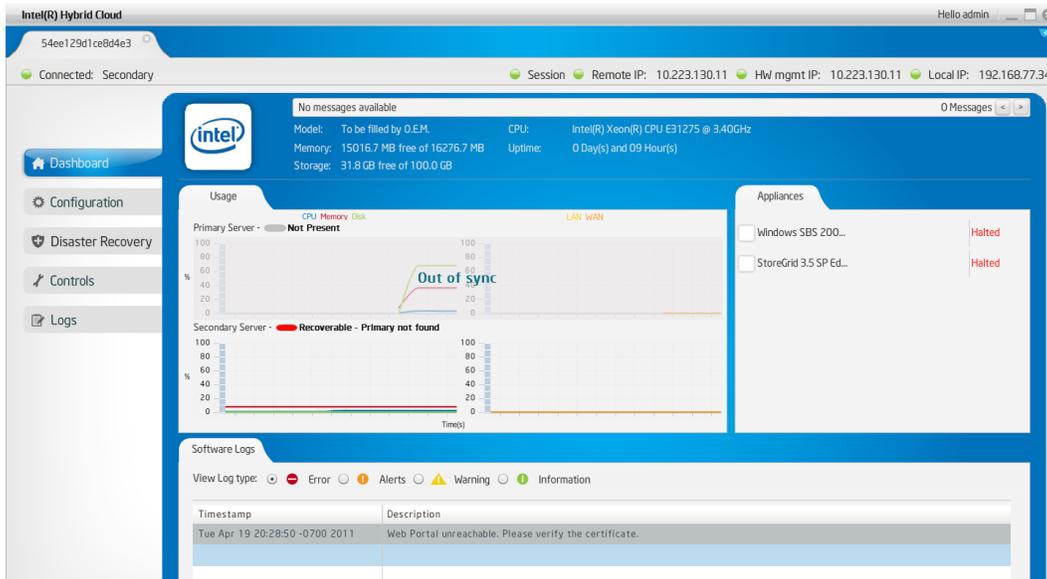


Figure 62. Server Manager - Machine status

MSP can use the Recovery tab to bring the appliance in service on this secondary server which will be the new Primary server post recovery. Please refer the screenshot below for the Recovery tab.

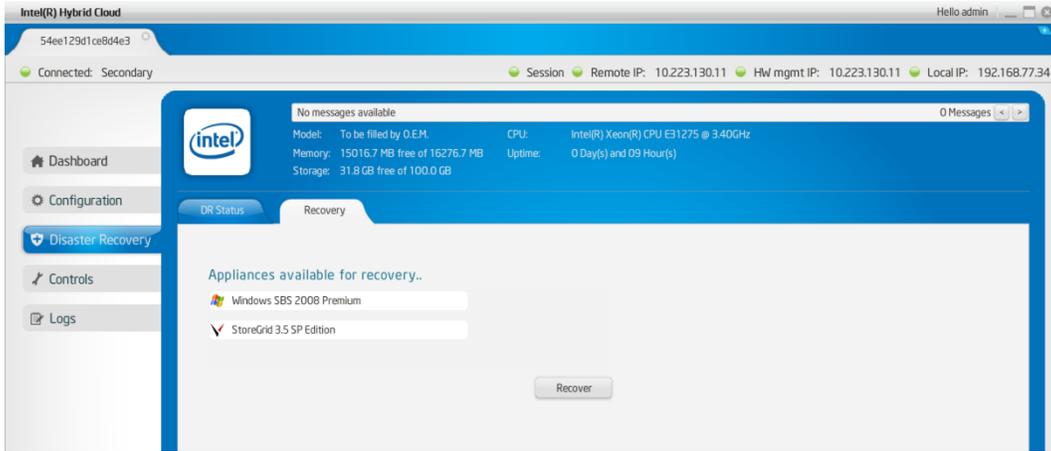


Figure 63. Server Manager - Recovery tab

6.8.3 Repair – Re-Create the Disaster Recovery Setup

Once the appliances are recovered, the original secondary server becomes the primary server. Now MSP can add a new secondary server and repair the setup to have disaster recovery capability once again. Repairing is a single step process where the MSP has to provide the WAN IP address of the new server. Please refer the screenshot below.

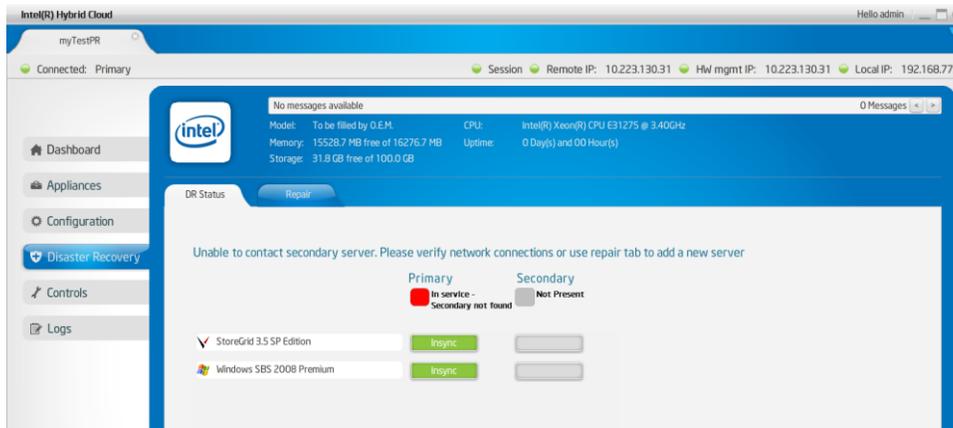


Figure 64. Verify Network Connections for Secondary Server

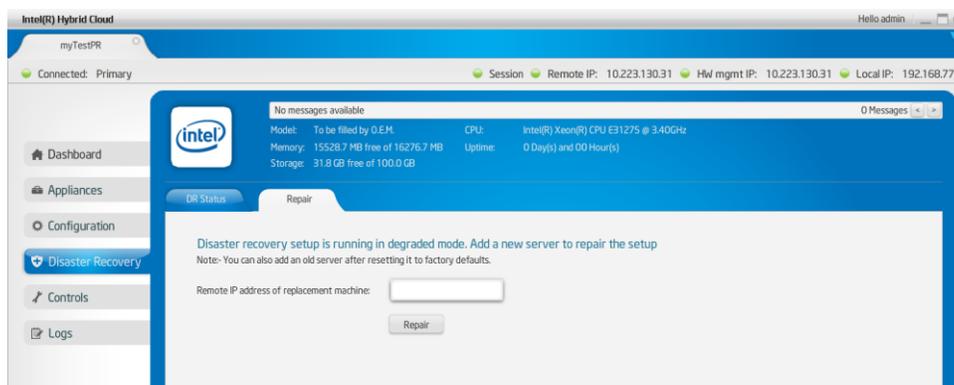


Figure 65. Re-Create the Disaster Recovery Setup

Just like in the case of the first-time DR setup, both the servers must be reachable on the Remote/WAN interface, and on the Local/LAN side both servers have to be connected to the same network. Refer to section **6.8.1 Setup** above to re-create the Disaster Recovery setup.

Post-repair, disaster recovery is setup again, and it ensures high availability for the customer's IT infrastructure.

6.8.4 Disabling Disaster Recovery Mode

Primary Server Procedure

1. Shut down the primary server's appliances (under "Appliances" select "Stop" or perform a shutdown within the OS itself via RDP or VNC).
2. Disconnect the primary server from the local network interface (network port "B" on the primary server).
3. On the primary server, do a system reset to default (refer to section **6.9 Controls – Restore Defaults**).
4. Login to the primary server again with Intel Hybrid Cloud server manager and re-configure the Remote Network Interface to the correct settings for your network if needed; the remote network interface will be configured for DHCP after a Restore Defaults is issued (Configuration → Network Settings: Remote Network Interface). Keep the local network interface configured to the 192.168.77.1/255.255.255.0 IP configuration.

Secondary Server Procedure

1. On the secondary server, connect with Intel Hybrid Cloud server manager using the secondary server's IP address (either local or remote interface).
2. Click "Disaster Recovery" in the left panel, then click the "Recovery" tab.
3. Click the "repair/restore" button.

After clicking on "repair/restore", the backup state changes to active state. The secondary server is now in standalone mode and the appliances can be uninstalled. This server can now be repurposed as a standalone server. Additionally, you may now reconnect the primary server to the local network interface (network port "B") and continue using as a standalone server.

6.9 Controls

Various actions can be taken on the Intel® Hybrid Cloud server manager using the “Controls” menu option and the “Maintenance” tab (e.g. system restart, shutdown, etc.). Forced restart and shutdown can be done OOB using Intel® AMT. These Intel® AMT commands are available only for the admin role. For others, admin can grant permission to the user role.

Software Reset — Resets the Intel® Hybrid Cloud software stack on the server.

Restore Defaults — Resets the Intel® Hybrid Cloud software stack configuration to initial default settings. This sets the user permissions to default permission levels and disables SSH for the user. It also configures the remote interface to ‘dhcp’ and sets local interface to 192.168.77.1/255.255.255.0 IP configuration. All Email alert configurations are removed. The boot orders of the appliances are also removed. There is no effect on the server registration and appliance activation state.

Upgrade — The Intel® Hybrid Cloud software stack can be patched using the upgrade option. There is an option to patch both Intel® Hybrid Cloud server manager and Intel® Hybrid Cloud software stack. User needs to copy the patch to the client system and then using the upgrade feature, remotely patch the software stack, or patch the server manager on the client system.

Sync – The Sync with Web Portal is used to start appliance and application downloads.

Appliance network — There is also a provision for taking appliances off the network. This could be used in scenarios where a network threat is detected and admin may want to put appliances off the network. Post diagnostics, he/she can put these appliances back on the network. Remote Administrator logged in as “admin” can also allow user role to perform this action.

Note: A power cycle on an appliance after detaching it from network automatically brings the appliance back on the network.

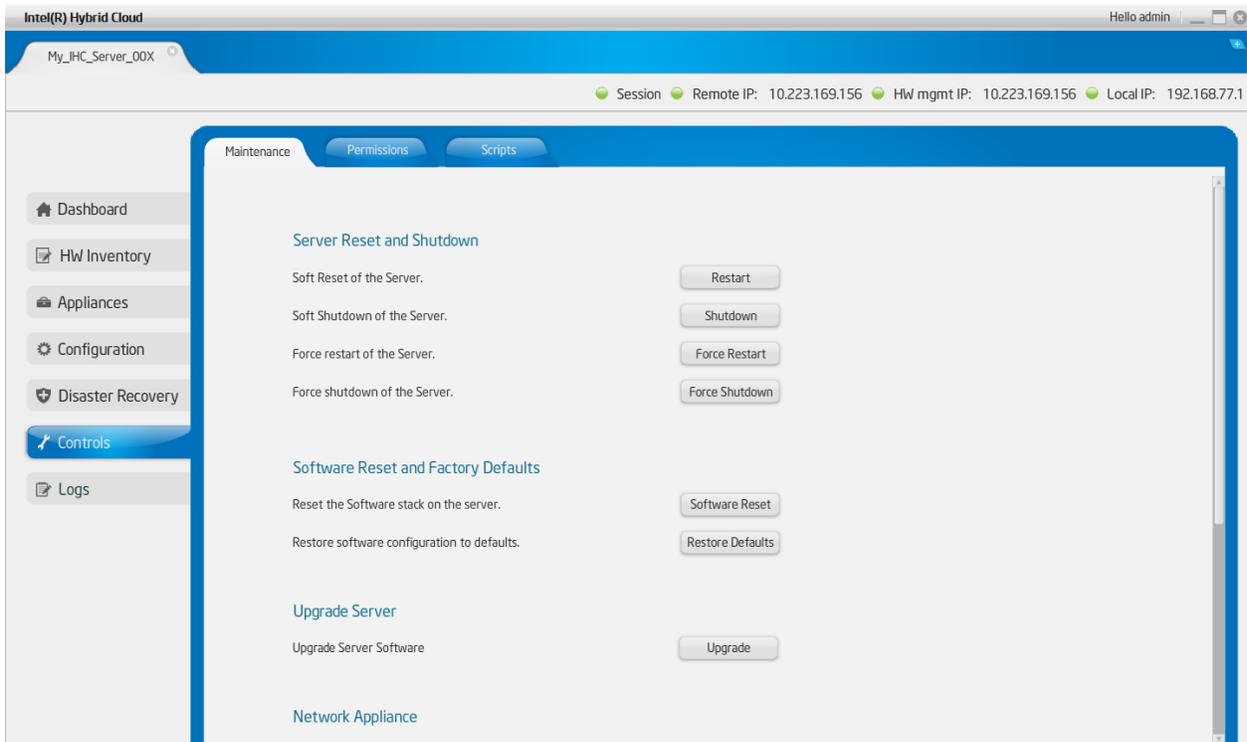


Figure 66. Server Manager - Control - Maintenance Screen 1

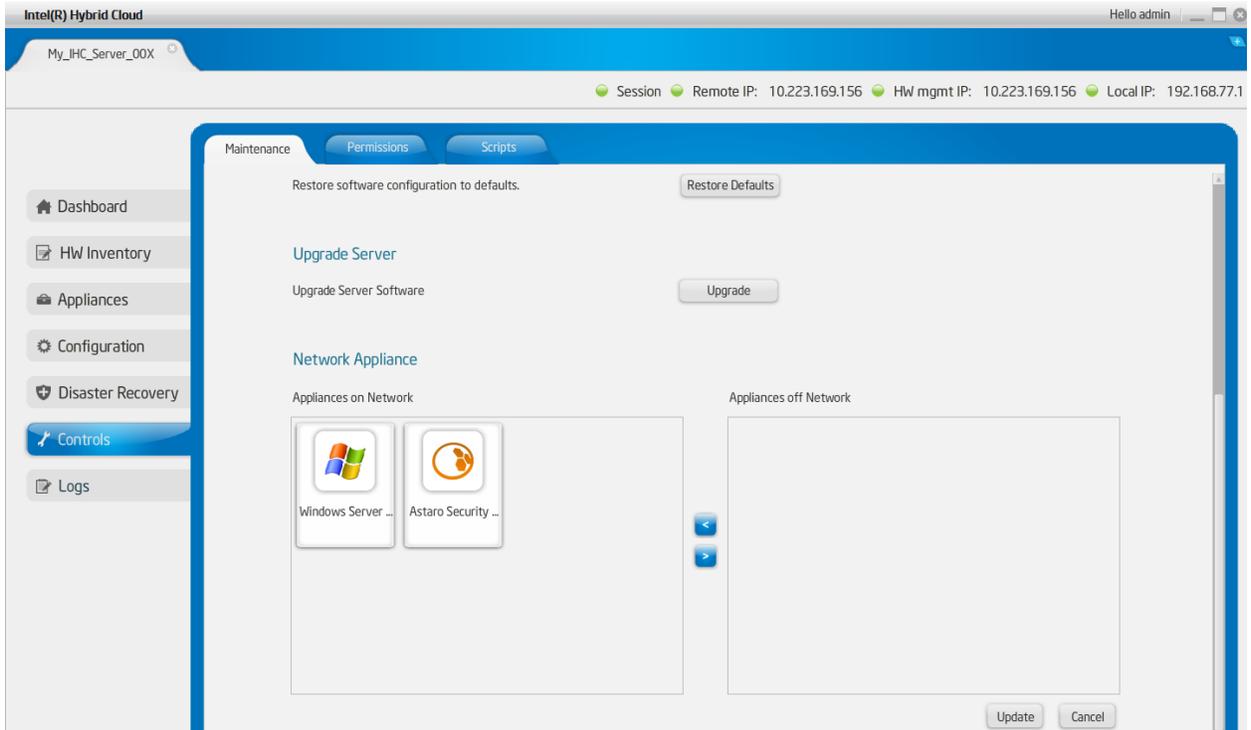


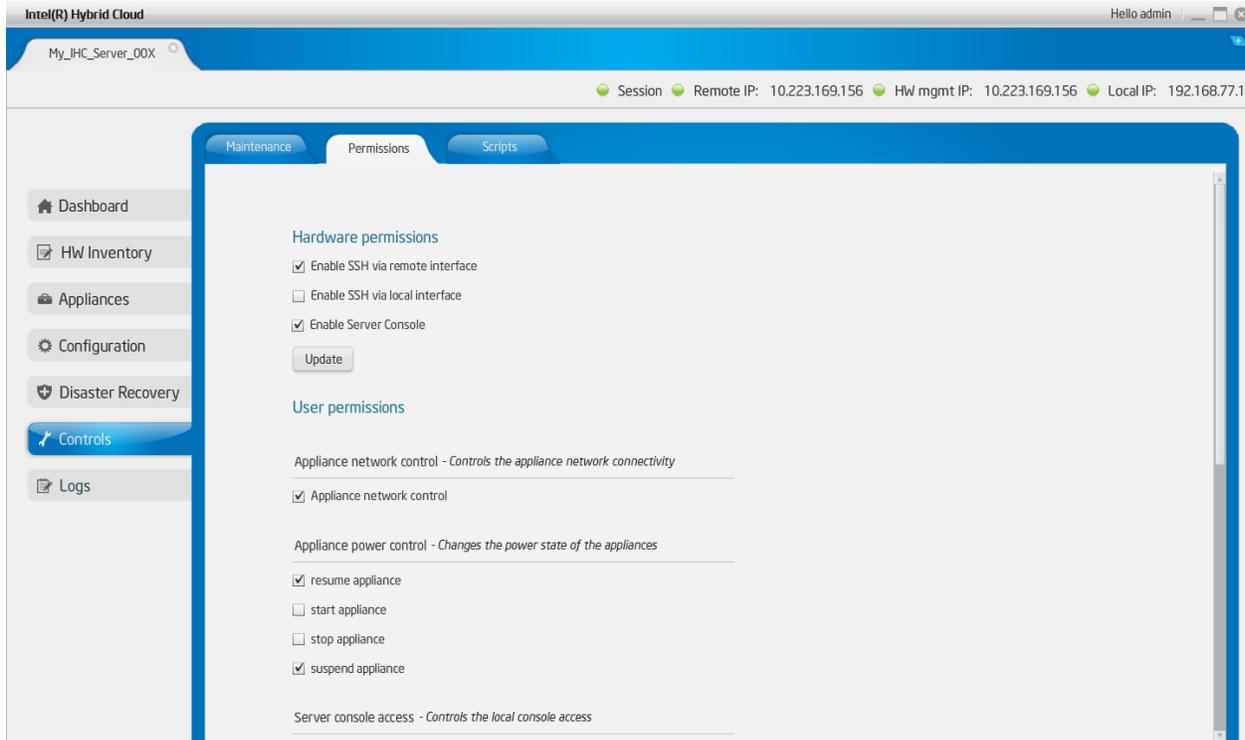
Figure 67. Server Manager - Maintenance Screen 2

6.9.1 Permissions

This screen is divided into 2 groups; system or hardware permissions and User permissions.

System permissions allow “Admin” to enable/disable SSH and System Console.

User permissions allow “Admin” set permissions for user role. Once logged in as “admin”, the Remote Administrator can change the default access permissions for the “user”. The access permissions are limited to “allowed” or “denied” for various operations supported.

**Figure 68. Server Manager - Permissions Screen**

6.9.2 Diagnostics (Controls → Scripts)

This tab provides a window to execute scripts to perform operations on the server. The script engine is designed in such a way that the user can add customized scripts. Default scripts available include:

1. Deleting ISO attached to appliance/VM.
2. Manage software RAID on this system.

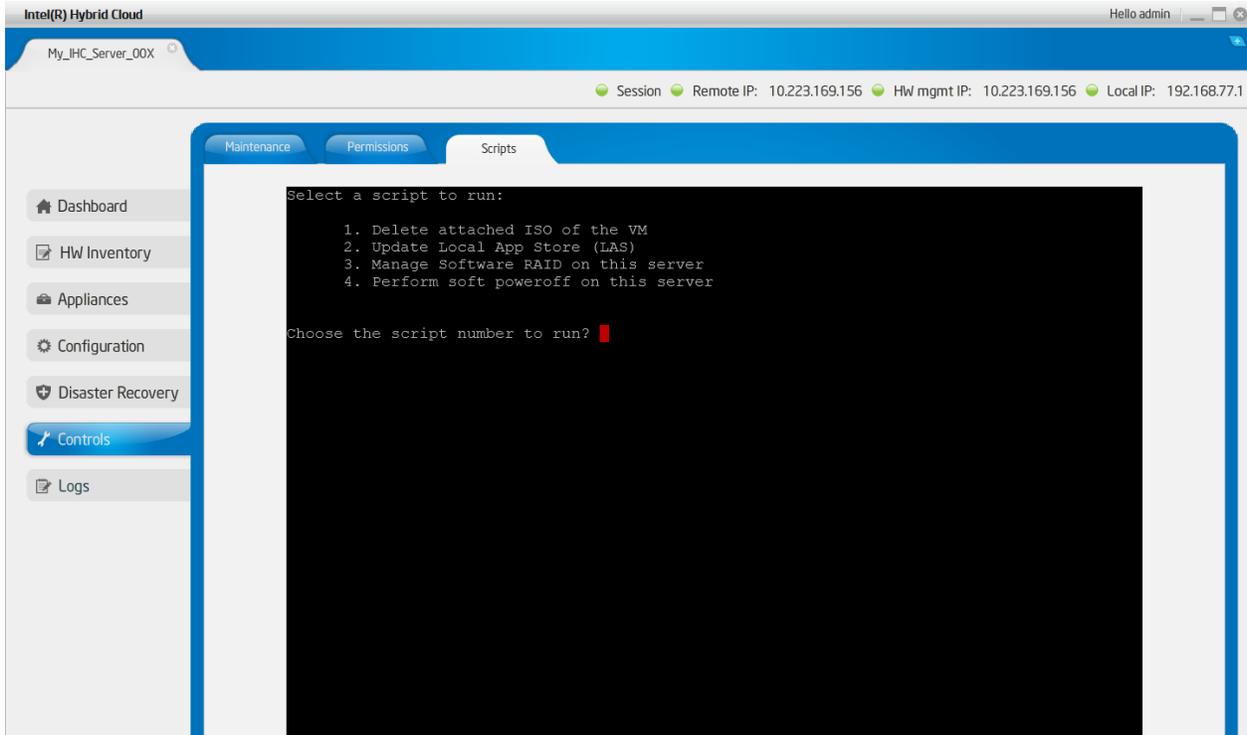


Figure 69. Server Manager - Diagnostics (Control > Scripts) window

6.10 Logs

This tab shows detailed logs on Intel® Hybrid Cloud server. The log entries fall under various categories: information, warning, alerts, and errors. A filtering mechanism is available by which any subset of these categories of messages can be viewed. The log messages are also classified into three “event” types.

- Software events that are captured by Intel® Hybrid Cloud software stack and RAID Controller.
- Hardware events that are captured by Intel® AMT.
- System events that are captured by Citrix* XenServer*.

Intel® Hybrid Cloud software stack supports both Hardware and Software RAID to be configured on the server to provide maximum availability for the services installed on the server. RAID drives would be used as the default storage for installing all the appliances. Intel® Hybrid Cloud software stack collects the logs generated by RAID and adds them to the Intel® Hybrid Cloud software logs.

The user also has the option of marking a particular log entry, or a set of log entries, as “closed”. The default response of the server manager is to not display the closed log entries any more. Using a drop down, the user can select and view closed log entries as well.

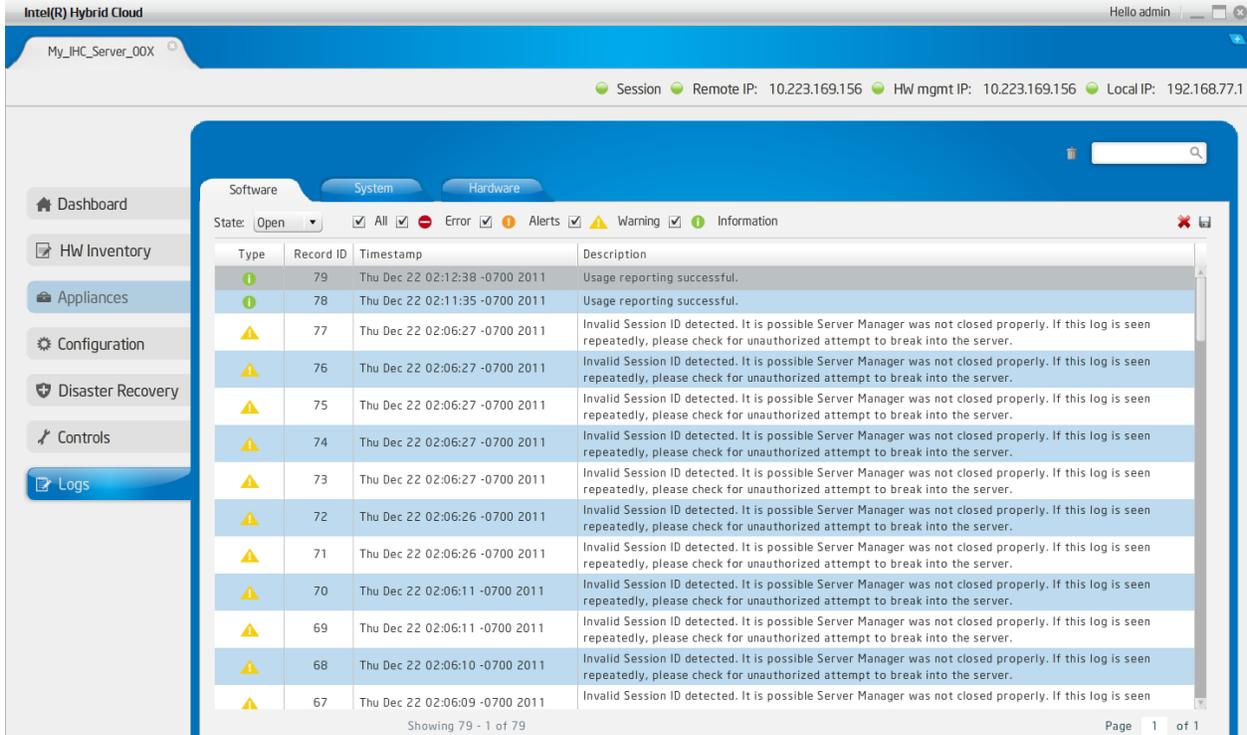


Figure 70. Server Manager - Software Logs screen

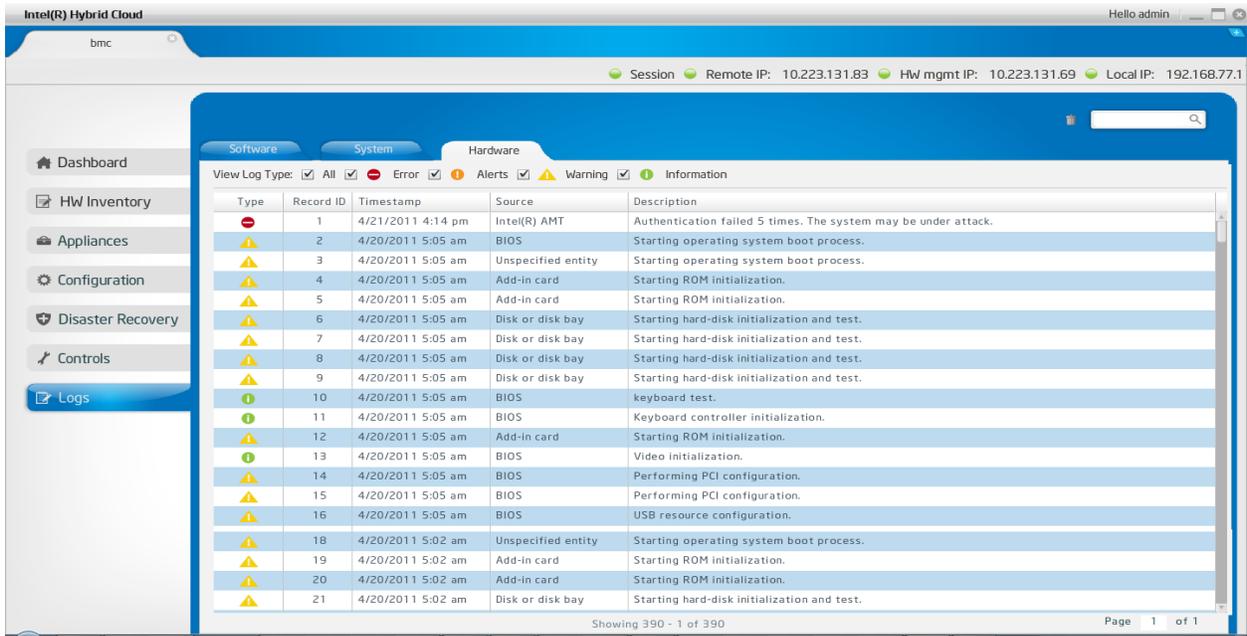


Figure 71. Server Manager - Hardware Logs Screen

6.10.1 Software and Hardware Logs Deletion:

Clicking on the **Trash Bin** icon highlighted below will delete all software or hardware logs. There is no option to delete specific set of logs. Also, system logs cannot be deleted.

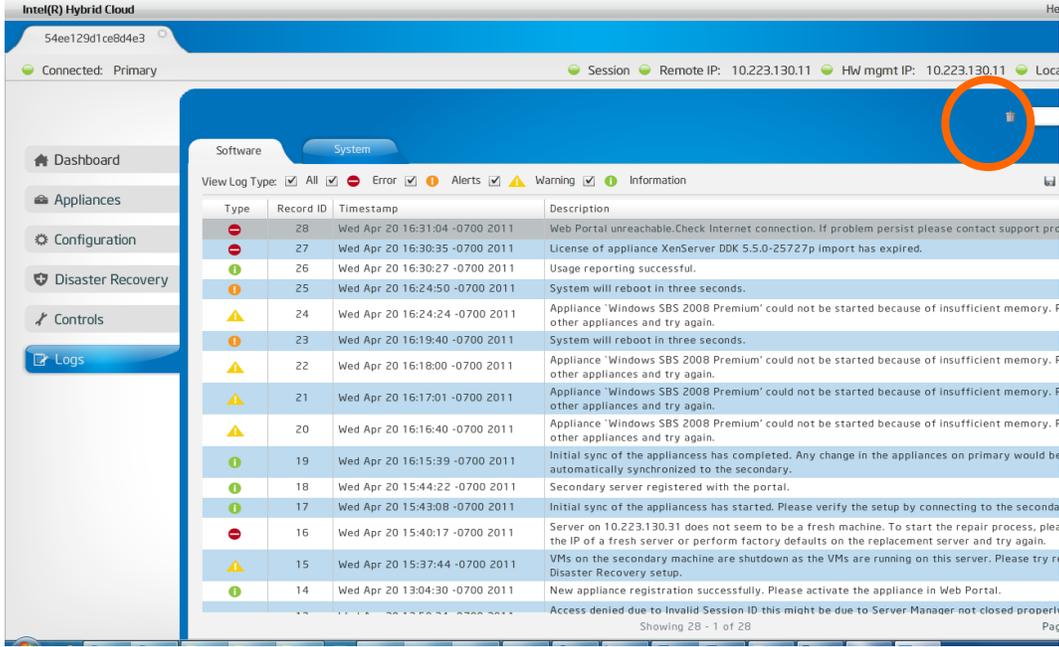


Figure 72. Server Manager - Software and Hardware Logs Deletion

6.10.2 Software Logs Download

The entire software log set can be exported to a CSV (Comma Separated Values) file. This file can also be used to import data to an excel sheet. This feature is available only for software logs. Clicking on the icon highlighted below can download software logs.

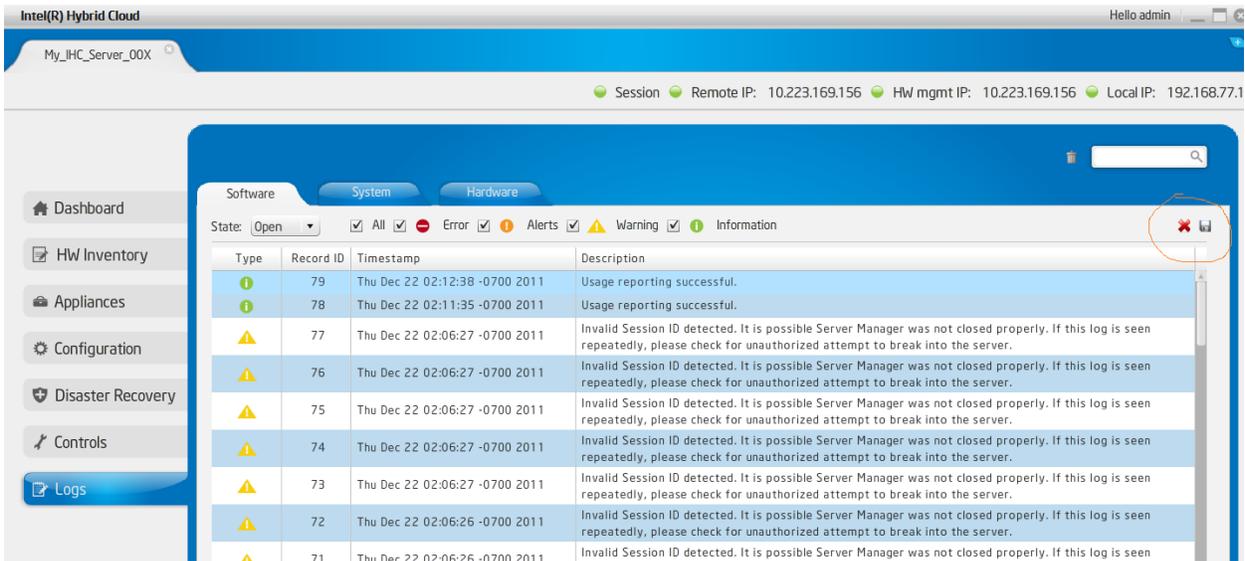


Figure 73. Server Manager - Software Logs Download

6.11 Appliance and Application Download

Appliance and application installation can be performed through Intel® Hybrid Cloud management portal. Refer to Section 5.1 to access the Intel® Hybrid Cloud management portal, and Section 5.5 for appliance and application installation details.

After the download has been initiated, the software package will automatically install and appear in the "Appliance" tab as shown in Figure 1: Elements in the Intel® Hybrid Cloud platform.

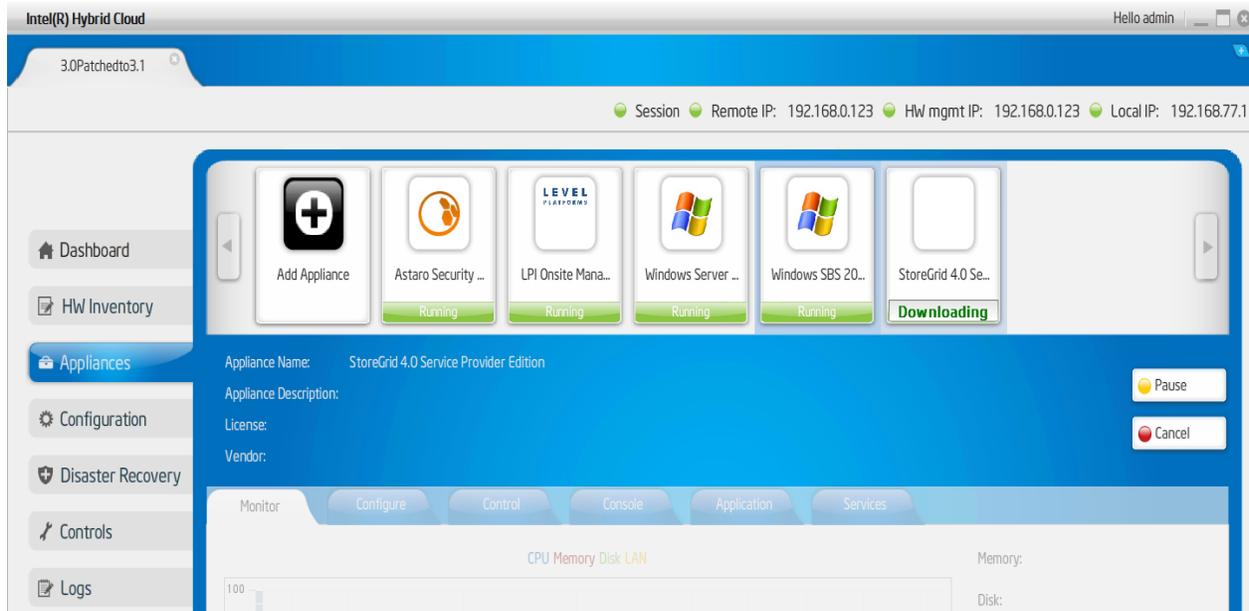


Figure 74. Server Manager – Appliance Installing

While the download is in progress, it can be paused, resumed, or cancelled by clicking the corresponding buttons (as shown in the following figures):

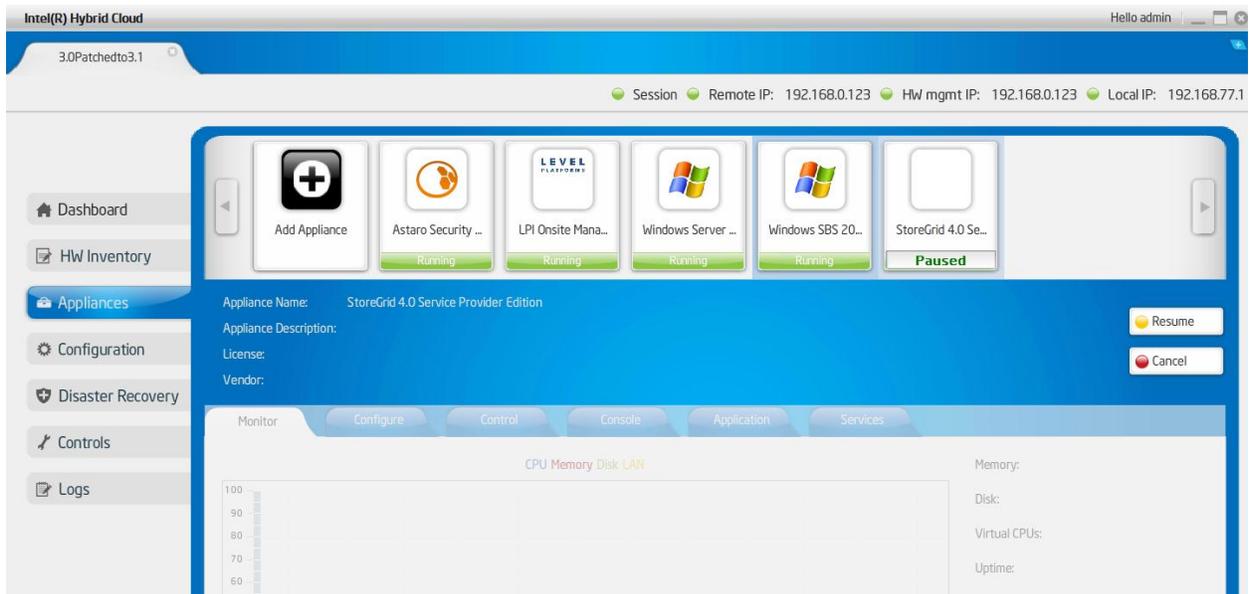


Figure 75. Server Manager – Appliance Paused

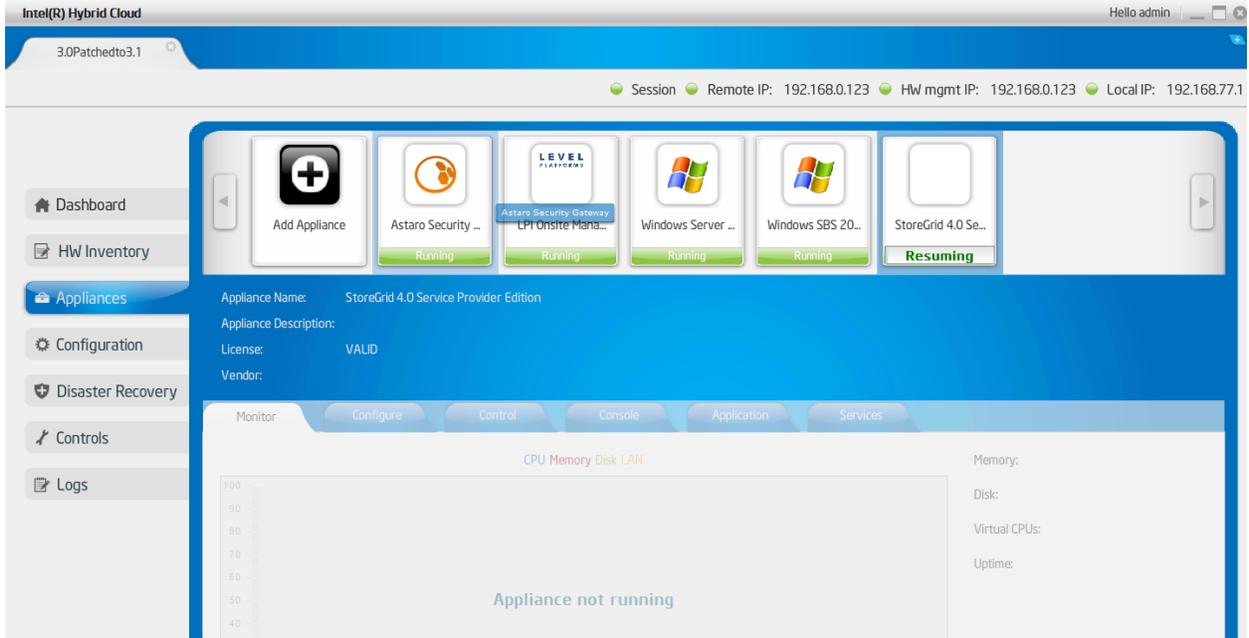


Figure 76. Server Manager – Appliance Resuming

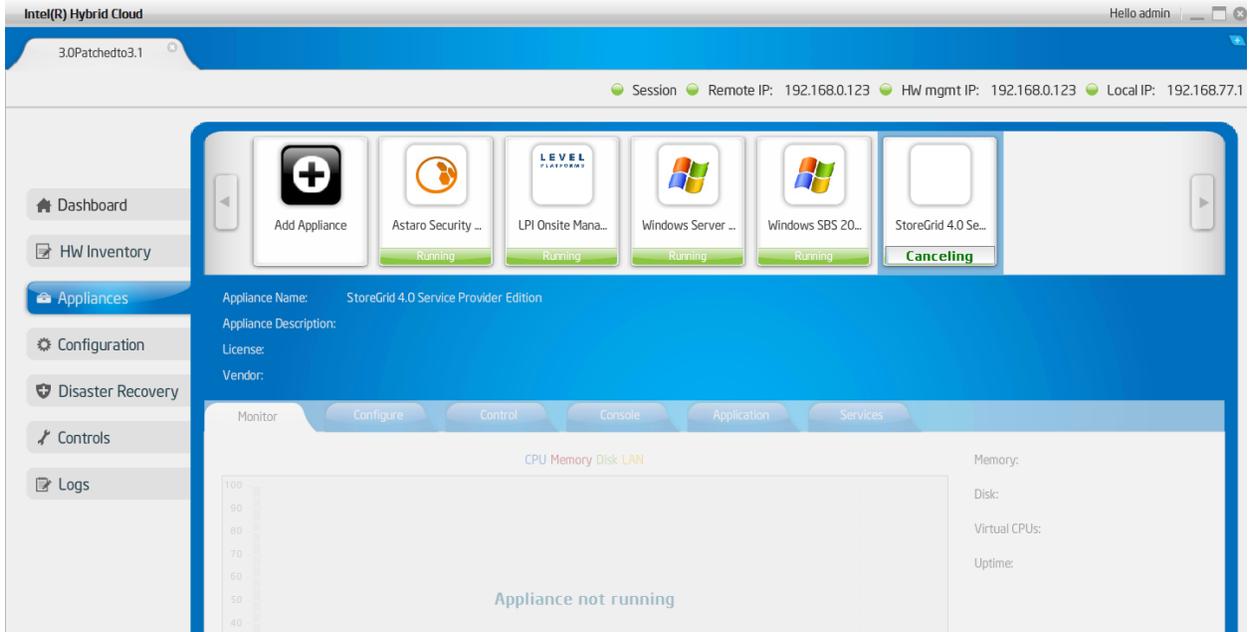


Figure 77. Server Manager – Installation Cancelling

6.12 Patching Mechanism

IHC software (Release 3.0 and above) supports patching the various components. The patching module handles deploying patches for any issues that are fixed once a release is made. During usage reporting, these patches get copied over to the portal and are ready to be applied.

Patches are version based and will be accompanied by a corresponding log entry to explain the reason for the patch.

Here is a brief explanation of the patching mechanism:

- Intel Admin uploads the patch to IHC web portal.
- The portal administrator initiates the download of the patch to the particular server from the management portal (refer to Section 5.10 for details).
- When any IHC server performs usage reporting, the portal checks for any patch availability and if a qualifying patch is found, the usage report response to the stack would contain the patch details.
- The stack downloads the patch and displays a ticker message on the server manager dashboard displaying “Patch is available. Please update”. Refer to screen shot below.



Figure 78. Server Manager - Patch Message

- Whenever user wishes to apply patch to stack, click on “Upgrade button in the server manager under Controls → Maintenance tab, in the “Upgrade Server” section. The following screenshot shows the location of this control.

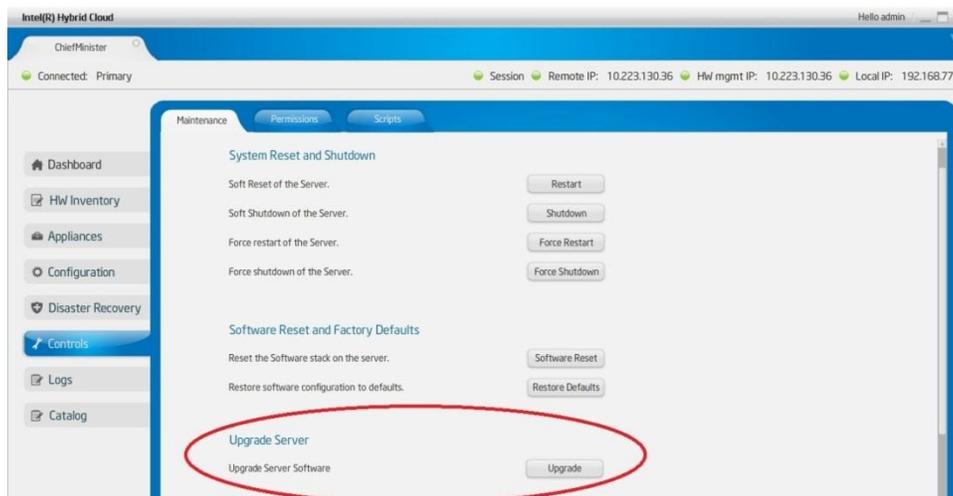


Figure 79. Server Manager - Upgrade the Server Software

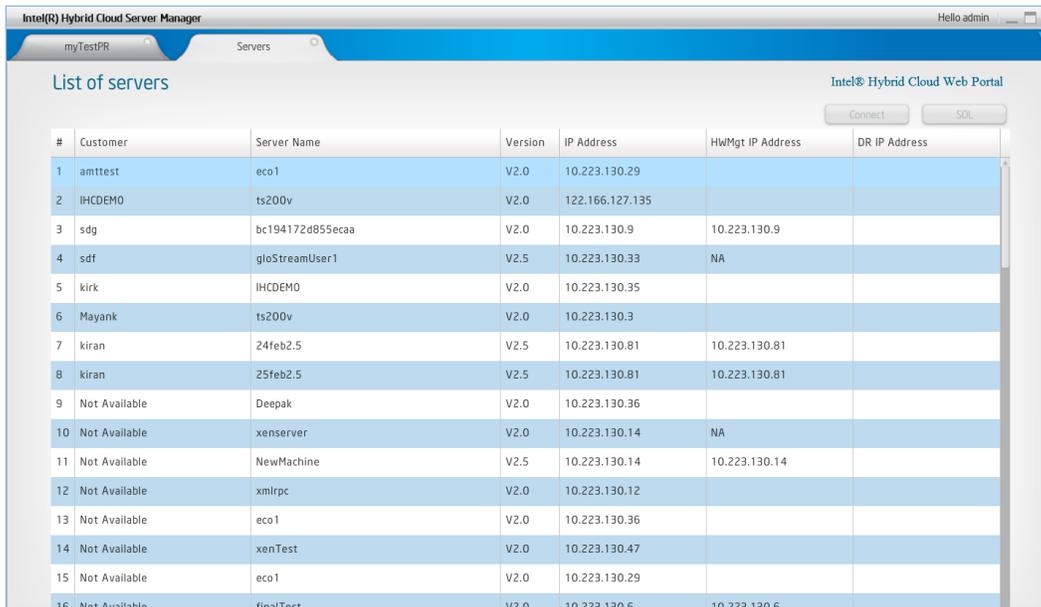
- If the current patch has a dependency on other patches, the patching mechanism automatically downloads those previous patches and installs them as well.

Upon successfully applying a patch a log message is recorded.

In a configuration where disaster recovery has been setup, if a patch is applied via the above steps on the primary machine, the patching module automatically takes care of applying the patch on to the secondary machine. Therefore, no additional steps are required to update the secondary machines.

6.13 Multiple Server Management

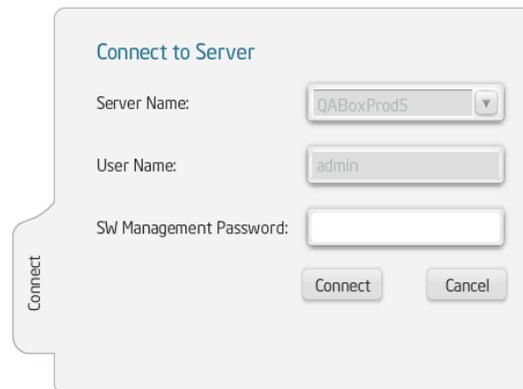
The “**Servers**” tab lists all of your registered and active servers. A sample **All Servers** window is displayed below.



#	Customer	Server Name	Version	IP Address	HW Mgt IP Address	DR IP Address
1	amtest	eco1	V2.0	10.223.130.29		
2	IHCDEMO	ts200v	V2.0	122.166.127.135		
3	sdg	bc194172d855ecaa	V2.0	10.223.130.9	10.223.130.9	
4	sdf	gloStreamUser1	V2.5	10.223.130.33	NA	
5	kirk	IHCDEMO	V2.0	10.223.130.35		
6	Mayank	ts200v	V2.0	10.223.130.3		
7	kiran	24feb2.5	V2.5	10.223.130.81	10.223.130.81	
8	kiran	25feb2.5	V2.5	10.223.130.81	10.223.130.81	
9	Not Available	Deepak	V2.0	10.223.130.36		
10	Not Available	xenserver	V2.0	10.223.130.14	NA	
11	Not Available	NewMachine	V2.5	10.223.130.14	10.223.130.14	
12	Not Available	xmlrpc	V2.0	10.223.130.12		
13	Not Available	eco1	V2.0	10.223.130.36		
14	Not Available	xenTest	V2.0	10.223.130.47		
15	Not Available	eco1	V2.0	10.223.130.29		
16	Not Available	finalTest	V2.0	10.223.130.6	10.223.130.6	

Figure 80. Server Manager - All Servers page

You can connect to any of the servers listed by selecting a server, clicking “**Connect**” button and entering the corresponding login credentials (in the “**Connect to Server**” box). A new tab will be added to the management screen (for each server connection).



Connect to Server

Server Name:

User Name:

SW Management Password:

Figure 81. Server Manager - All servers → Connect to Server window

NOTES:

- Click **Portal** button in the **All Servers** page to open the management portal page in the default browser of the client machine.
- Click **SOL** to open a Serial over LAN access to a specific server. This will require Intel® AMT or Baseboard Management Controller (BMC) login credentials. You can use this to recover a server remotely.
 - If the configured system has AMT support, upon clicking the SOL button, the user will be prompted to enter the SW Management Password prior to establishing the SOL session.
 - If the configured system has BMC support, upon clicking the SOL button, the Intel® BMC Integrated Web Console will open in a web browser. The user will login with Username: **root** and the SW Management Password. From the console, you can view system information, server health, and perform power actions and other out-of-band operations. Console redirect (IDE) and KVM management requires Intel® Remote Management Module (Intel® RMM) hardware (<http://www.intel.com/support/motherboards/server/sb/CS-032371.htm>).

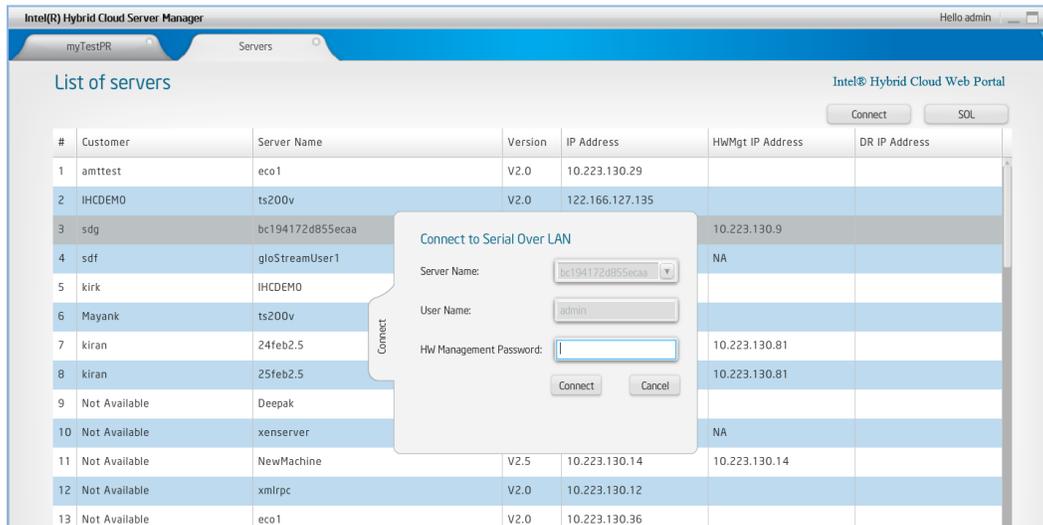


Figure 82. Server Manager - All servers → Connect to Server window (via Intel® AMT)

6.14 Logging out of Intel® Hybrid Cloud server manager

User can log out of the management console anytime by using the sign out option as highlighted in following screen OR clicking the UI close (X) button.

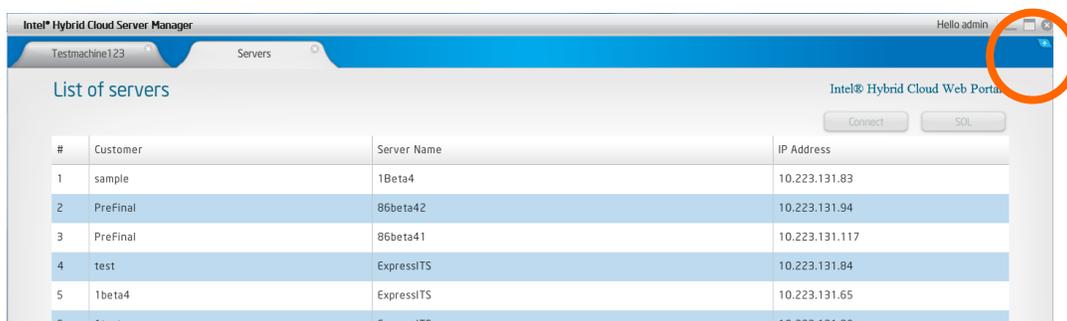


Figure 83. Server Manager - Log Out

7. Saving & Restoring System Configuration

Once the Intel® Hybrid Cloud server is configured, the system configuration can be saved and restored to the same machine (if needed due to a server stack or VMM crash). IXE commands are used to create the restore file, and to subsequently restore the configuration to the server.

The following items may be saved and restored:

- IP table settings: Secure Shell (SSH), Citrix XenServer* management
- Remote & Local IP configuration
- Email alerts configuration
- System Asset Tag
- Appliance store URL
- System brand info
- System name, time-zone
- User permissions
- User & Admin passwords
- System Host Name

NOTE: The restore file can only be applied to the server from which it was created. SMTP configuration can only be restored when using a DNS name. If SMTP is using a server IP address, it will not be restored.

7.1 Saving the Server Configuration

Use the following IXE commands to save the server configuration to a convenient location:

```
IXE -h <server IP> -u <user name> -p <password> -o save-restore-configuration <directory path>.
```

7.2 Restoring the Server Configuration

Use the following IXE commands to restore the server configuration:

```
IXE -h <server IP> -u <user name> -p <password> -o apply-restore-configuration user <file name>
```

NOTE: The server will reboot after successfully restoring and applying the configuration. Refer to Section 11 for additional IXE command information.

8. Activating Appliances

8.1 Activating Windows* Appliances

Once the Microsoft Windows* appliance is activated on the management portal and the Remote Administrator tries to start the appliance for the first time via the Intel® Hybrid Cloud server manager, the server manager opens a customer profile page giving an option to fill in appliance specific information (name, login name, business name, machine name, and password) as shown in following figure: This information is used for creating auto answer file for Windows* configuration and will vary from one version of Windows* OS to other.

Figure 84. Activating Microsoft Windows* Appliances - Customer Profile page

After the Remote Administrator fills the information and clicks **Update**, server manager gets the available appliance activation key from the management portal, activates the appliance with that key, and configures the appliance with the information entered by the Remote Administrator (like login name, password and so on).

8.2 Activating Other Appliances

All non-Windows* appliances need to be simply activated through the Intel® Hybrid Cloud management portal by the remote administrator. If needed, a license is downloaded by the server manager from the management portal. License mechanism varies depending on the type of appliance. In some cases, an appliance key is emailed to MSP/Remote administrator and remote administrator may have to apply the license key manually for fully activating the appliance functionality. Once the appliance is installed on the server, the information would be sent to the management portal. Remote administrator can login to the management portal and activate the appliance.

9. Intel® AMT Configuration

This section applies only to Intel® Hybrid Cloud servers with Intel® Active Management Technology (Intel® AMT), and does not apply to servers with Baseboard Management Controller (BMC).

Intel® AMT offers a HW chipset based solution for remote out-of-band management, using a secondary processor on the motherboard, with embedded firmware that runs on the Manageability Engine (ME). You can access Intel® AMT through the server remote IP port connection.

NOTE: If you are using an external firewall, refer to Section 4.1 for port forwarding details.

9.1 Intel® AMT Password

The Intel AMT password is automatically synchronized with the SW management password. Using any other method to change the Intel AMT password will break the synchronization. To change the SW management password (and the Intel AMT password), refer to Section 6.3.

IMPORTANT: Changing the Intel (R) ME Password (Intel AMT password) in the ME Configuration screen (BIOS) will break the synchronization with the SW management password. If an unsynchronized Intel AMT password is lost, cannot be recovered. A subsequent Intel AMT password reset would require returning the Intel® Hybrid Cloud server to the place of purchase.

If the Managed Services Provider (or its End-User) makes changes to the Intel AMT/ME configuration and/or provisioning on the Hardware that renders Intel AMT/ME unusable as designed and implemented with the Intel Hybrid Cloud platform, the Managed Services Provider agrees to be responsible for all costs associated with reimaging that Hardware, including shipping to and from the system builder.

10. Intel® Hybrid Cloud server BMC Configuration

This section applies only to Intel® Hybrid Cloud servers with Baseboard Management Controller (BMC), and does not apply to servers with Intel® Active Management Technology (Intel® AMT).

BMC is a specialized processor service that monitors the physical state of Intel® Hybrid Cloud server and provides remote management capabilities similar to Intel® AMT technology. You can access BMC through an independent IP port connection.

NOTE: If you are using an external firewall, refer to Section 4.1 for port forwarding details.

10.1 Change the BMC IP Address

IMPORTANT: The BMC IP address is initially set to 0.0.0.0 when shipped. You must follow the below steps in order to use HW mgmt, SOL, power actions, etc on BMC systems.

1. Open the Intel® Hybrid Cloud server manager and connect to a server (as described in Section 6.2).
2. Use the following path in the Intel® Hybrid Cloud server manager to access the hardware information for BMC:

"Configuration" menu button > **"Network Settings"** tab

3. Select the **"HW mgmt"** radio button.
4. Select the appropriate network type (i.e. DHCP or Static).
5. Change the default HW mgmt IP (BMC IP) to a suitable value.
NOTE: The BMC IP address must be different from the remote IP address of the Intel® Hybrid Cloud server.
6. Close the current connection, and reconnect to the server to access the BMC Hardware features.

10.2 BMC Password

The BMC password is automatically synchronized with the SW management password. Using any other method to change the BMC password will break the synchronization. To change the SW management password (and the BMC password), refer to Section 6.3.

11. Intel® Hybrid Cloud command line tool (IXE)

Intel® Hybrid Cloud server can also be managed using the “ixe” command line tool. The tool is a one-operation-at-a-time kind of tool that can be scripted using any of the scripting languages the user may want to use. Both Linux* & Windows* variants of the tool are supported.

11.1 IXE command Line Format

The syntax for each operation supported by ixe is provided below.

Command Line Format:

```
# ixe -h | --host <IP Address/Hostname of the target machine>
-u | --user <target machine username> -p | --pass <target machine
password> -o | --operation <command name> [ <arg1><arg2>...]
```

Intel® AMT command format:

```
# ixe -h | --host < Intel® AMT IP Address/HostName> -u | --
user < Intel® AMT username> <-p | --pass> < Intel® AMT password> -
o | --operation < Intel® AMT command>
```

[AMT Commands: force-system-poweroff, force-system-reset, force-system-poweron, hw-system-information, hw-processor-information, hw-memory-information, hw-disk-information, and hw-event-log, change-hw-management-password]

- [] → optional variable
- <> → compulsory variable
- or -- → is fixed and must

Command Time out: 3 minutes

Help : > **ixe help** or > **ixe help <command>**

11.2 List of IXE Commands

The following tables provide the IXE commands that are supported on the Intel® Hybrid Cloud platform. Error codes are displayed separately at the end of this section.

NOTE: The results are provided as examples only. The results you see may differ.

Command: `activate-native-management`

Required Parameter	Null
Description	Enables xen center for the server to access
Supported User	{'admin'}
Usage	<code>ixe -h <server> -u admin -p <Password> -o activate-native-management</code>
Result	Command successful

Command: `active-aeon-md5sum`

Required Parameter	Null
Description	Updates active aeon
Supported User	{'admin'}
Usage	<code>ixe -h <server> -u admin -p <Password> -o active-aeon-md5sum <md5sum></code>
Result	Command successful

Command: `allow-remote-login`

Required Parameter	<remote local>
Description	Enable the remote login (SSH) option
Supported User	{'admin','user'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o allow-remote-login <remote/local></code>
Result	Command successful

Command: `add-appliance-hard-disk-drive`

Required Parameters	<Appliance name> <Hard disk size in GB>
Description	Attach new harddisk to appliance.
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o add-appliance-hard-disk-drive <Appliance name> <Hard disk size in GB></code>
Result	Command successful

Command: `appliance-attach-cdrom`

Required Parameters	<Appliance name> <CDROM name>
Description	Attach cd-rom to appliance.
Supported user	{'admin', 'user'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o appliance-attach-cdrom <Appliance name> <CDROM name></code>
Result	Command successful

Command: `appliance-attach-usb`

Required Parameters	<Appliance name> <usb>
Description	Attach usb to appliance.
Supported user	{'admin', 'user' }
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-attach-usb <Appliance name> <usb></i>
Result	Command successful

Command: `appliance-delete-hard-drive`

Required Parameters	<Appliance name> <Harddisk device position>
Description	Destroy harddisk connected to the appliance.
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-delete-hard-drive <Appliance name> <Harddisk device position></i>
Result	Command successful

Command: `appliance-detach-cdrom`

Required Parameters	<Appliance name> <CDROM name>
Description	Detach cd-rom to appliance.
Supported user	{'admin', 'user' }
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-detach-cdrom <Appliance name> <CDROM name></i>
Result	Command successful

Command: `appliance-detach-usb`

Required Parameters	<Appliance name> <usb>
Description	Detach usb to appliance.
Supported user	{'admin', 'user' }
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-detach-usb <Appliance name> <usb></i>
Result	Command successful

Command: `appliance-resize-hard-drive`

Required Parameters	<Appliance name> <hard-drive-position> <new hdd size>
Description	Increases HDD capacity which is already attached to appliance.
Supported user	{'admin', 'user' }
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-resize-hard-drive <Appliance name> <hard-drive-position> <new hdd size></i>
Result	Command successful

Command: `appliance-uninstall`

Required Parameters	<appliance name>
Description	<i>uninstalls the requested appliance from system</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o appliance-uninstall <appliance name></i>
Result	<i>Command successful</i>

Command: `apply-restore-configuration`

Required Parameters	<system> [<user> <restore file>]
Description	restore the system to old configurations.
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o apply-restore-configuration <system> [<user> <restore file>]</i>
Result	Command successful. (Restores the system to original configurations.)

Command: `apply-stack-patch`

Required Parameters	Null
Description	Applies patch to IHC server.
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o apply-stack-patch</i>
Result	Command successful

Command: `apply-vm-metadata`

Required Parameters	<>
Description	apply the appliance metadata to the server host
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o apply-vm-metadata</i>
Result	Command successful. (Restores the appliance metadata)

Command: `attach-appliances-to-network`

Required Parameter	<Appliance name>
Description	attaches the requested appliances to the network
Supported User	{'admin','user'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o attach-appliance-network <appliance name></i>
Result	Command successful

Command: `block-remote-login`

Required Parameter	<remote local>
Description	Disable the remote login (SSH) option for the requested interface.
Supported User	{'admin','user'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o <i>block-remote-login</i> <remote/local></code>
Result	Command successful

Command: `change-appliance-memory`

Required Parameters	<Appliance name> <Memory in MB>
Description	Create Increase or Decrease the appliance Memory.
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o change-appliance-memory <Appliance name> <Memory in MB></code>
Result	Command successful

Command: `change-default-password`

Required Parameters	<NewPassword>
Description	Resets the system password to new password this is a mandatory step before connecting to stack.
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o change-default-password <NewPassword></code>
Result	Command successful

Command: `change-password`

Required Parameter	<Appliance Name>
Description	Change the password for the requested user
Supported User	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o <i>change-password</i> <new password></code>
Result	Command successful

Command: `configure-box-expiry-grace-period`

Required Parameter	<expiry days> <grace period days>
Description	Sets box expiry period days and grace period days
Supported User	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o <i>configure-box-expiry-grace-period</i> <expiry period days number> <grace period days number></code>
Result	Command successful

Command: `configure-email-alerts`

Required Parameters	<disable enable <msp user email> <loglevels>>
Description	<i>Update the email parameters to which the alerts will be sent.</i>
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o configure-email-alerts <disable enable <msp user email> <loglevels>></code>
Result	Command successful

Command: `configure-network-parameters`

Required Parameter	<local remote> <static or dhcp> <IP Address > <Net mask> [gateway] [DNS server] (IP Address and Netmask is required for static and gateway is compulsory for remote for static)
Description	returns the network parameters for the requested interface
Supported User	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <user name>-p <password> -o configure-network-parameters <remote/local> <local remote> <static or dhcp> <IP Address > <Net mask> [gateway] [DNS server]</code>
Result	Command successful

Command: `configure-server-email-alerts`

Required Parameters	<smtp server IP address> <smtp port> <box username> <box password>
Description	<i>Update Update the server email parameters from which the alerts will be sent.</i>
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o configure-server-email-parameters <smtp server IP address> <smtp port> <box username> <box password></code>
Result	Command successful

Command: `connect-appliance-console`

Required Parameter	Null
Description	<i>Connect to the Appliance console</i>
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o connect-appliance-console</code>
Result	<i>Command Successful (launches the appliance console)</i>

Command: `create-appliance-network-interface`

Required Parameters	<Appliance name> <remote local>
Description	Create a new network interface for the appliance .
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o create-appliance-network-interface <Appliance name> <remote local></code>
Result	Command successful

Command: deactivate-native-management

Required Parameter	Null
Description	disables xen center for the server to access
Supported User	{'admin'}
Usage	<i>ixe -h <server> -u admin -p <Password> -o deactivate-native-management</i>
Result	Command successful

Command: delete-appliance-network-interface

Required Parameters	<Appliance name> <mac address of the network interface>
Description	Destory a network interface for the appliance
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o delete-appliance-network-interface <Appliance name> <mac address of the network interface></i>
Result	Command successful

Command: delete-event-log

Required Parameter	<Error level 0 (delete all logs in all level)>
Description	Deletes all logs from requested level.
Supported User	{'user'}
Usage	<i>ixe -h <server ip> -u <user name>-p <password> -o delete-event-log <Error level></i>
Result	Event log cleared

Command: detach-appliances-from-network

Required Parameter	<Appliance name>
Description	Detaches the requested appliances from the network
Supported User	{'admin','user'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o detach-appliance-network <appliance name></i>
Result	Command successful

Command: disable-patching

Required Parameter	Null
Description	Disables patch path
Supported User	{'admin','user'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o disable-patching</i>
Result	Command successful

Command: disconnect-appliance-console

Required Parameter	<appliance name>
Description	Closes console for the specified appliance
Supported User	{'admin','user'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o disconnect-appliance-console
Result	Command successful

Command: enable-patching

Required Parameter	Null
Description	Enables patch path
Supported User	{'admin','user'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o enable-patching
Result	Command successful

Command: get-alert-messages

Required Parameters	< >
Description	This command provides the messages related to box and appliances.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-alert-messages
Result	Returns the Stack messages for the User and MSP

Command: get-appliance-backup-status

Required Parameters	Null
Description	<i>returns the progress of the appliance backup</i>
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-appliance-backup-status
Result	<i>NA/NA-Success/NA-failure/percentage</i>

Command: get-appliance-boot-order

Required Parameter	null
Description	Appliances name and the UUID are returned in the order they are set to boot
Supported User	{'user', 'admin'}
Usage	ixe -h <server ip>-u <user name>-p <password> -o get-appliance-boot-order
Result	Appliance1 : 075d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: get-appliance-brand-info

Required Parameter	<Appliance name>
Description	Returns the appliances brand info set by the admin
Supported User	{'admin'}
Usage	ixe -h <server ip>-u <user name>-p <password> -o get-appliance-brand-info "appliance name"
Result	Command successful

Command: `get-appliance-license-configuration`

Required Parameter	<Appliance name>
Description	Returns the appliances configuration details
Supported User	{'admin'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-appliance-license-configuration "appliance name"</code>
Result	Configuration details

Command: `get-appliance-management-url`

Required Parameter	<Appliance name>
Description	Returns the appliance management url to connect
Supported User	{'admin'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-appliance-management-url "appliance name"</code>
Result	Management url

Command: `get-appliance-parameters`

Required Parameter	<Appliance name>
Description	returns all the appliances specific parameters
Supported User	{'admin','user'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-appliance-parameters "appliance name"</code>
Result	disktotal : 8.59 GB Numcpu : 1 Nos Memorytotal : 1.00 GB Uptime : 1 Day(s) 21:29:58

Command: `get-appliance-power-state`

Required Parameter	<Appliance Name>
Description	Returns the power state of the requested appliance
Supported User	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o get-appliance-power-state "appliance name"</code>
Result	name : Appliance1 uuid : 75d37ba0-40cb-d4cc-8adc-42de1d519487 powerstate : Halted

Command: `get-appliance-restore-status`

Required Parameters	Null
Description	<i>returns the progress of the appliance backup</i>
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o get-appliance-restore-status</code>
Result	<i>NA/NA-Success/NA-failure/percentage</i>

Command: get-appliance-usage

Required Parameter	<Appliance name>
Description	returns all the appliances specific usage [note :- ts -> time stamp Usage is in percentage]
Supported User	{'admin','user'}
Usage	ixe -h <server ip>-u <user name>-p <password> -o <i>get-appliance-usage</i> "appliance name"
Result	disktotal : 8.59 GB Numcpu : 1 Nos Memorytotal : 1.00 GB Uptime : 1 Day(s) 21:29:58

Command: get-cdrom-list

Required Parameter	Null
Description	Lists all cdroms attached to server
Supported User	{'admin','user'}
Usage	ixe -h <server ip>-u <user name>-p <password> -o <i>get-cdrom-list</i>
Result	name_label : SCSI 2:0:0:0 vdi_uuid : 9db06e24-0299-44a2-8a61-6e16395190d4 virtual_size : 1073741312

Command: get-close-logs

Required Parameter	<log level>
Description	Lists all closed logs
Supported User	{'admin','user'}
Usage	ixe -h <server ip>-u <user name>-p <password> -o <i>get-close-logs 1</i>
Result	1 : 233 : Mon Mar 09 06:16:48 +0530 2009 : Access granted 1 : 232 : Mon Mar 09 06:16:40 +0530 2009 : Session Successfully Disconnected

Command: get-command-permissions

Required Parameter	Null
Description	<i>returns the api and the permission status set by admin</i>
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o <i>get-command -permissions</i>
Result	<i>returns the api and the permission status set by admin</i>

Command: get-console-status

Required Parameter	Null
Description	Returns the Console(USB) status
Supported User	{'admin', 'user'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o <i>get-console-status</i>
Result	Command successful

Command: get-email-alert-parameters

Required Parameters	Null
Description	<i>Displays the email alert parameters configured for the requested user.</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-email-alert-parameters</i>
Result	Email aler configuration for the user requested

Command: get-event-log

Required Parameter	<Error level> (0 -> to get logs of all level) Level 1 -> Information Level 2 -> Warnings Level 3 -> Alerts Level 4 -> Error
Description	returns all logs for the requested level
Supported User	{'user', 'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o get-event-log 1</i>
Result	Detailed Logs for example 1,233, Mon Mar 09 06:16:48 +0530 2009, Access granted 1,232, Mon Mar 09 06:16:40 +0530 2009, Session Successfully Disconnected

Command: get-installed-appliances

Required Parameter	Null
Description	Returns the names and UUIDs of the appliances installed on the system.
Supported User	{'user', 'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o get-installed-appliances</i>
Result	Appliance1 : 75d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: get-internet-ip-address

Required Parameters	<>
Description	displays the internet accessible ip address which can be used to connect to the server.
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-internet-ip-address</i>
Result	Internet accessible IP Address

Command: get-log-size

Required Parameters	<log level>
Description	Returns log count for the level
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-log-size 1</i>
Result	20

Command: get-network-detached-appliances

Required Parameter	Null
Description	returns all the appliances that are detached from the network
Supported User	{'admin','user'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-network-detached-appliances</code>
Result	Appliance1 : 75d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: get-network-parameters

Required Parameter	<local remote>
Description	returns the network parameters for the requested interface
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-network-parameters local</code>
Result	netmask : 255.255.255.0 ip : 192.168.1.1 boot-protocol : static

Command: get-network-policy

Required Parameter	<remote local>
Description	List the Network policy of the requested Interface (remote local)
Supported User	{'admin','user'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o get-network-policy <remote/local></code>
Result	remote-management : enabled ssh : enabled xen-management : enabled

Command: get-number-of-appliances

Required Parameter	Null
Description	Returns the total number appliance installed on the system
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server> -u admin -p admin -o get-number-of-appliances</code>
Result	2

Command: get-open-logs

Required Parameter	<Log level>
Description	Lists all open logs
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server> -u <username> -p <password> -o get-open-logs 1</code>
Result	1 : 233 : Mon Mar 09 06:16:48 +0530 2009 : Access granted 1 : 232 : Mon Mar 09 06:16:40 +0530 2009 : Session Successfully Disconnected

Command: get-power-state-for-all-appliances

Required Parameter	Null
Description	<i>returns the power state of all the appliance installed in the System</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-power-state-for-all-appliances</i>
Result	<i>returns the power state of all the appliance installed in the System</i>

Command: get-restore-files

Required Parameter	Null
Description	<i>returns backed up image files from USB connected to server</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-restore-files</i>
Result	<i>Lists img files</i>

Command: get-service-list

Required Parameter	<appliance-name>
Description	<i>Lists all services available on particular appliance</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-sevice-list <appliance name></i>
Result	<i>Name: SamSs Power_state: running app_id: sam1 type: service</i>

Command: get-system-asset-tag

Required Parameters	Null
Description	<i>Display the System uniquely identified tag.</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-asset-tag</i>
Result	<i>System unique asset tag</i>

Command: get-system-brand-info

Required Parameter	Null
Description	Returns the Intel® Hybrid Cloud server Brand Info set by the admin
Supported User	{'admin','user'}
Example	<i>ixe -h <server ip>-u <user name>-p <password> -o get-system-brand-info</i>
Result	<i>product : Intel® Hybrid Cloud client : Client name logo : test.png</i>

Command: get-system-event-log

Required Parameters	Null
Description	<i>Displays xensource system event logs.</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-event-log</i>
Result	Xensource System event logs (only warning and error logs)

Command: get-system-log-size

Required Parameters	Null
Description	<i>Returns system log count.</i>
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-log-size</i>
Result	200

Command: get-system-parameters

Required Parameter	Null
Description	Returns the system parameters
Supported User	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o get-system-parameters</i>
Result	disktotal : 151 GB Name : system name cpumodel : Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz memorytotal : 3.90 GB version : 1.0 uptime : 1 Day(s) 12:09:47 systemmodel : DQ45CB

Command: get-system-serial-id

Required Parameters	< >
Description	This command retrieves the unique serial number of the box.
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-serial-id</i>
Result	Returns the system unique serial id

Command: get-system-time

Required Parameter	Null
Description	returns system time and time zone
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-time</i>
Result	returns the system time and time zone

Command: `get-system-timezones`

Required Parameter	Null
Description	returns list of time zone..
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-timezones</i>
Result	returns the list of time zone

Command: `get-system-tpm-key`

Required Parameter	Null
Description	returns tpm key for the server
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o get-system-tpm-key</i>
Result	returns 64 bytes tpm key

Command: `get-system-usage`

Required Parameter	Null
Description	returns the system usage like wan, lan , cpu etc
Supported User	{'user', 'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o get-system-usage</i>
Result	lan : 0.0 memory : 37.38 wan : 10.0 cpu : 12.8 ts : 03/09/2009 09:38:07 IST Disk : 92.93

Command: `get-usb-list`

Required Parameter	Null
Description	Lists all cdroms attached to server
Supported User	{'admin','user'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o get-usb-list</i>
Result	name_lable : USB 2:0:0:0 vdi_uuid : 9db06e24-0299-44a2-8a61-6e16395190d4 virtual_size : 1073741312

Command: `initiate-usage-reporting`

Required Parameter	Null
Description	Performs usage reporting of box to server and parses response from server
Supported User	{'admin','user'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o initiate-usage-reporting</i>
Result	<i>Command successful</i>

Command: `install-system-license`

Required Parameters	<System license>
Description	<i>Applies the system license for the xenserver</i>
Supported user	{admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o install-system-license <System license></i>
Result	<i>Command successful</i>

Command: `is-appliance-license-valid`

Required Parameter	<Appliance Name>
Description	Returns the status of the license installed on the requested appliance
Supported User	{'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o is-appliance-license-valid <appliance name></i>
Result	valid/invalid

Command: `resume-appliance`

Required Parameter	<Appliance Name>
Description	Resume the requested appliance
Supported User	{'admin','user'}
Example	<i>ixe -h <server ip>-u <user name>-p <password> -o resume-appliance <appliance name></i>
Result	Command successful

Command: `save-restore-configuration`

Required Parameters	<Path to Store the restore configuration file>
Description	Retrieves the current system configuration. This can be used by the
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o save-restore-configuration</i>
Result	File Name of the system configuration

Command: `set-appliance-boot-order`

Required Parameter	<Appliance name in order required separated by space>
Description	set the appliance to boot during the system reboot Note: - If the Arguments are Empty the Command Clears the Boot order set previously.
Supported User	{'admin'}
Example	<i>ixe -h <server ip>-u <user name> -p <password> -o set-appliance-boot-order Backup Windows</i>
Result	Command successful

Command: `set-appliance-client-name`

Required Parameter	<Appliance Name><client name>
Description	Updates the requested Appliance Client name.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o <i>get-appliance-client-name</i> <Appliance Name><client name></code>
Result	Command successful

Command: `set-appliance-default-brand-info`

Required Parameters	<APP ID> <Vendor name> <vendor Logo>
Description	Updates the appliance brand information in the stack
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o <i>set-appliance-default-brand-info</i> <APP ID> <Vendor name> <vendor Logo></code>
Result	Command successful.

Command: `set-appliance-logo`

Required Parameter	<Appliance name><logo location>
Description	Uploads the requested Appliance Logo.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o <i>set-appliance-logo</i> <Appliance name><logo location></code>
Result	Command successful

Command: `set-appliance-vcpu-number`

Required Parameters	<Appliance name> <number of Vcpu>
Description	Increase appliance virtual CPU numbers.
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o <i>set-appliance-vcpu-number</i> <Appliance name> <number of Vcpu></code>
Result	Command successful

Command: `set-appliance-vendor-name`

Required Parameter	<Appliance Name> <vendor name>
Description	Updates the requested Appliance Vendor name.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o <i>set-appliance-vendor-name</i> <Appliance Name> <vendor name></code>
Result	Command successful

Command: set-console-disable

Required Parameter	Null
Description	Disable the Console (USB) option
Supported User	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o set-console-disable
Result	Command successful

Command: set-console-enable

Required Parameter	Null
Description	Enable the Console (USB) option
Supported User	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o set-console-enable
Result	Command successful

Command: set-logs-close

Required Parameter	<log ID/s>
Description	Closes particular log IDs
Supported User	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o set-logs-close 200
Result	Command successful

Command: set-oem-factory-defaults

Required Parameters	<>
Description	Set the Server to OEM factory defaults(removes all VMS)
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o set-oem-factory-defaults
Result	Command successful

Command: set-system-client-name

Required Parameter	<Name>
Description	Updates the Intel® Hybrid Cloud server client name.
Supported User	{'admin'}
Example	ixe -h <server ip>-u <user name>-p <password> -o set-system-client-name <new client name>
Result	Command successful

Command: set-system-defaults

Required Parameter	Null
Description	Reset the system to factory defaults
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o set-system-defaults
Result	Command successful

Command: set-system-logo

Required Parameter	<logo file location>
Description	Updates the Intel® Hybrid Cloud server logo.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o set-system-logo <File location></code>
Result	Command successful

Command: set-system-product-name

Required Parameter	<Product Name>
Description	Updates the Intel® Hybrid Cloud system vendor name.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip>-u <user name>-p <password> -o set-system-product-name <product name></code>
Result	Command successful

Command: software-reset

Required Parameter	null
Description	Restarts the Intel® Hybrid Cloud software stack.
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password>-o software-reset</code>
Result	Command successful

Command: start-appliance

Required Parameter	<Appliance Name>
Description	Starts the requested appliance in the system.
Supported User	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o start-appliance Backup</code>
Result	Command successful

Command: start-appliance-backup

Required Parameters	<Appliance Name>
Description	<i>initiates the backup for the requested appliance.</i>
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o start-appliance-backup <Appliance Name></code>
Result	<i>Command successful</i>

Command: start-appliance-restore

Required Parameters	<path >
Description	<i>initiates the restore for the requested appliance.</i>
Supported user	{'user','admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o start-appliance-restore <path> </code>
Result	<i>Command successful</i>

Command: start-service

Required Parameters	<Appliance Name> <Service/Application Name>
Description	<i>Starts the requested service/application.</i>
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o start-service <Appliance Name> <Service/Application Name></i>
Result	<i>Command successful</i>

Command: stop-service

Required Parameters	<Appliance Name> <Service/Application Name>
Description	<i>Stops the requested service/application.</i>
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o stop-service <Appliance Name> <Service/Application Name></i>
Result	<i>Command successful</i>

Command: stop-appliance

Required Parameter	<Appliance Name>
Description	Stop the requested appliance in the system
Supported User	{'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password> -o stop-appliance <appliance name></i>
Result	Command successful

Command: suspend-appliance

Required Parameter	<Appliance Name>
Description	Suspends the requested appliance
Supported User	{'admin'}
Example	<i>ixe -h <server ip>-u <user name>-p <password> -o suspend-appliance <appliance name></i>
Result	Command successful

Command: sync-with-portal

Required Parameter	null
Description	It syncs client with portal.
Supported User	{'admin'}
Usage	<i>ixe -h <server ip> -u <user name> -p <password>-o sync-with-portal</i>
Result	Command successful

Command: `system-poweroff`

Required Parameter	null
Description	power off the system
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o system-poweroff</code>
Result	Command successful

Command: `system-reset`

Required Parameter	null
Description	Restarts the System.
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o system-reset</code>
Result	Command successful

Command: `update-appliance-name`

Required Parameters	<Appliance name> <New Appliance Name>
Description	Set new appliance name.
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o update-appliance-name <Appliance name> <New Appliance Name></code>
Result	Command successful

Command: `update-eula`

Required Parameter	<license file>
Description	Updates the eula on the Intel Hybrid cloud System.
Supported user	{'admin' }
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o update-eula <license file></code>
Result	Command successful

Command: `update-ntp-servers`

Required Parameters	<ntp server 1>[server2]... {max 3 serves}
Description	apply new ntp settings
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o update-ntp-server <ntp server IP></code>
Result	Command successful.

Command: `update-system-name-label`

Required Parameter	<system name>
Description	Update the system label with the requested name
Supported User	{'user', 'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o update-system-name-label <new name></code>
Result	Command successful

Command: update-system-timezone

Required Parameter	<time zone>
Description	Update the system time zone
Supported user	{'user','admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o update-system-timezone <time zone></i>
Result	<i>Command Successful</i>

Command: update-appliance-unattend-template

Required Parameters	<unattended template>
Description	Uploads template for unattended installation.
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o update-appliance-unattend-template <unattended template></i>
Result	Command successful.

Command: update-catalog-server-url

Required Parameters	<URL>
Description	Updates TC catalog server url
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o update-catalog-server-url <url></i>
Result	Command successful.

Command: update-custom-template

Required Parameters	<unattended template>
Description	Uploads template for unattended installation.
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o update-custom-template <unattended template></i>
Result	Command successful.

Command: update-reg-server-url

Required Parameters	<url>
Description	Updates registration server URL
Supported user	{'admin'}
Usage	<i>ixe -h <server ip> -u <username> -p <password> -o update-reg-server-url <url></i>
Result	Command successful.

Command: `update-reg-ssl-cert`

Required Parameters	<certificate pem file>
Description	Uploads certificate to box
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o update-reg-ssl-cert <pem file></code>
Result	Command successful.

Command: `upgrade-host-server`

Required Parameters	<Xen update patch file>
Description	<i>upgrade the server Software</i>
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o ,upgrade-host-server XenServer-5.5.0-Update2.xsupdate</code>
Result	<i>Command successful</i>

Command: `upgrade-management-software`

Required Parameter	<applications. zip>
Description	Upgrade the system software stack
Supported user	{'admin','user'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o upgrade- management-software <applications. zip></code>
Result	Command successful

Command: `upgrade-system-software`

Required Parameter	<System Stack File>
Description	Upgrade the system software stack
Supported user	{'admin','user'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o update-system-software <System Stack File></code>
Result	Command successful

Command: `upload-system-scripts`

Required Parameters	<script location>
Description	Uploads script to script tabs to help user in diagnostics
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <username> -p <password> -o upload-system-scripts <script></code>
Result	Command successful.

11.3 IXE AMT Commands

Command: `change-hardware-management-password`

Required Parameter	<new password>
Description	AMT password change
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o change-hardware-management-password <new password></code>
Result	Command successful

IMPORTANT: The Intel AMT password is automatically synchronized with the SW management password. To change the SW management (password and the Intel AMT password), refer to Section 0. Changing the Intel AMT password by any other method will break the synchronization. If an unsynchronized Intel AMT password is lost, it cannot be recovered. A subsequent Intel AMT password reset would require returning the Intel® Hybrid Cloud server to the place of purchase.

Command: `configure-hw-network-parameters`

Required Parameter	<dhcp static>[if static <ip> <netmask> <gateway> [dns]]
Description	Configure hardware management network details
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o configure-hw-network-parameters <dhcp static>[if static <ip> <netmask> <gateway> [dns]]</code>
Result	Command successful

Command: `force-system-poweroff`

Required Parameter	Null
Description	AMT system power off (force fully shutdowns the system)
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o force-system-poweroff</code>
Result	Command successful

Command: `force-system-poweron`

Required Parameter	Null
Description	AMT system power off (force fully shutdowns the system)
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o force-system-poweron</code>
Result	Command successful

Command: `force-system-reset`

Required Parameter	Null
Description	AMT system reboot (force fully reboot the system)
Supported user	{'admin'}
Usage	<code>ixe -h <server ip> -u <user name> -p <password> -o force-system-reset</code>
Result	Command successful

Command: get-hw-network-parameters

Required Parameter	Null
Description	AMT network details
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o get-hw-network-parameters
Result	AMT Network details {IP,Netmask,gateway etc}

Command: get-hw-system-power-state

Required Parameter	Null
Description	System power state.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o get-hw-system-power-state
Result	System state

Command: hardware-disk-information

Required Parameter	Null
Description	Returns Hardware Disk Information
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o hardware-disk-information
Result	returns hardware disk information

Command: hardware-event-log

Required Parameter	Null
Description	Returns Hardware event logs
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o hardware-event-log
Result	returns hardware event logs

Command: hardware-memory-information

Required Parameter	Null
Description	Returns Hardware memory Information
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o hardware-memory-information
Result	returns hardware memory information

Command: hardware-processor-information

Required Parameter	Null
Description	Returns Hardware Processor Information
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o hardware-processor-information
Result	returns hardware processor information

Command: hardware-system-information

Required Parameter	Null
Description	Returns system hardware Information
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <user name> -p <password> -o hardware-system-information
Result	returns hardware system information

11.4 IXE Error Messages

In the event of a error, IXE commands will provide an error message. For your convenience, some error descriptions are provided below.

Table 4. IXE Error Messages

Failure Messages	Description
Command failed	Command could not be executed successfully.
Invalid parameters	Wrong arguments are supplied to the command.
Invalid session	Session to the Intel® Hybrid Cloud server is lost.
Invalid server response	Invalid response received.
Authentication failed	User name or password provided is incorrect.
No appliance Installed	No appliance available in Intel® Hybrid Cloud server.
No response from server	Command has reached timeout