Intel® Hybrid Cloud platform

Version 2.5

User Guide

Intel order number G34287-001

Revision 1.0

June, 2011

Intel® Hybrid Cloud, Data Center Group Marketing

Revision History

Date	Revision Number	Modifications
08-Jun-2011	1.0	Initial Release

Disclaimers

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. Intel products are not intended for use in medical, life saving, or life sustaining applications.

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 Intel® Hybrid Cloud platform 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.

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

List of Figures

List of Tables

1. About This Document

This User Guide describes in detail, the various features available for configuring and managing the Intel® Hybrid Cloud server. This user guide describes the features available on the latest version of the Intel® Hybrid Cloud platform.

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
Intel® AMT	Intel® Active Management Technology refers to Intel's management architecture with consistent cross platform capabilities, interfaces, and protocols. It 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.
OOB	Out of Band channel, can be used to access a system that is powered down and does not have OS running
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control. Intel® Hybrid Cloud server manager follows an RBAC mechanism. There are two roles supported by the Intel® Hybrid Cloud server manager. 1. "admin" with default password "admin" 2. "user" with default password "user"
Remote Administrator	Or a Managed Service provider (MSP) who will be Intel's interface to end customer and he/she will be providing remote manageability services to customers
SMB	Small and Medium Businesses
Virtualization	Refers to Intel's hardware implementation of Intel® Virtualization Technology (that is, Intel® VT), that enables multiple guest OSs and applications (together known as Virtual Machines or VMs) to co-exist on the same computer platform.
VMM*	Virtualization Machine Monitor, refers to third party ISV SW that uses Intel® VT and enables remote management of VMs.

1.3 Additional Information

The following table lists the other useful documents.

Table 2. List of documents

Topic	Link to the document
Intel® Hybrid Cloud Troubleshooting Guide	http://www.intel.com/support/motherboards/server/hybrid/sb/CS-031724.htm
Intel® Hybrid Cloud Software Log Guide	http://www.intel.com/support/motherboards/server/hybrid/sb/CS-031723.htm

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 the data on site.

The Intel Hybrid Cloud platform offers four key ingredients:

- Intel® Hybrid Cloud server that resides on the customer premises and hosts the customer appliances and data.
- Intel® Hybrid Cloud software stack which runs on the Intel® Hybrid Cloud server on top of a Virtual Machine Monitor (VMM).
- Intel® Hybrid Cloud server manager which an administrator can use to remotely manage the Intel® Hybrid Cloud server.
- Intel® Hybrid Cloud management portal which is an internet reachable management portal that allows a remote administrator to manage all his/her Intel® Hybrid Cloud servers, controls server registration, and manages expiry & activation of appliances on each of the server.

Each of these components is briefly described below:

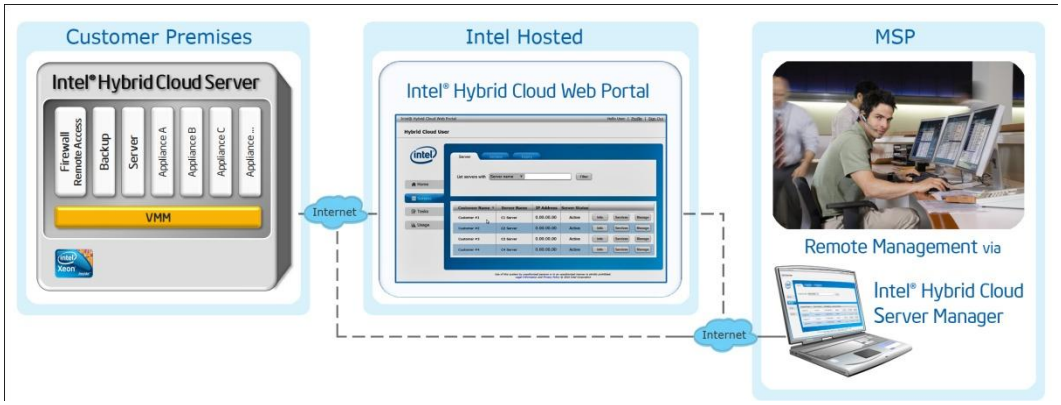

Figure 1: Components in Intel® Hybrid Cloud platform

2.1 Intel® Hybrid Cloud server

Intel® Hybrid Cloud server is a server that has the required technical ingredients to support the Intel Hybrid Cloud software stack, including Intel® Active Management Technology 6.0 for remote manageability and a Trusted Platform Module.

2.2 Intel® Hybrid Cloud software stack

Intel® Hybrid Cloud software stack is one of the core components of the Intel® Hybrid Cloud platform that runs on the Intel® Hybrid Cloud server on top of a Virtual Machine Monitor (VMM).

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 OSs are supported within the VMM, to run a variety of end-user applications.

2.3 Intel® Hybrid Cloud management portal

Registration and activation of Intel® Hybrid Cloud server and supported appliances will be controlled by an Internet reachable management portal named Intel® Hybrid Cloud management portal (will be referred to as management portal for the rest of this document). This portal requires a valid username and password for access and is available to authorized remote administrators. The management portal is described detail in chapter 5.

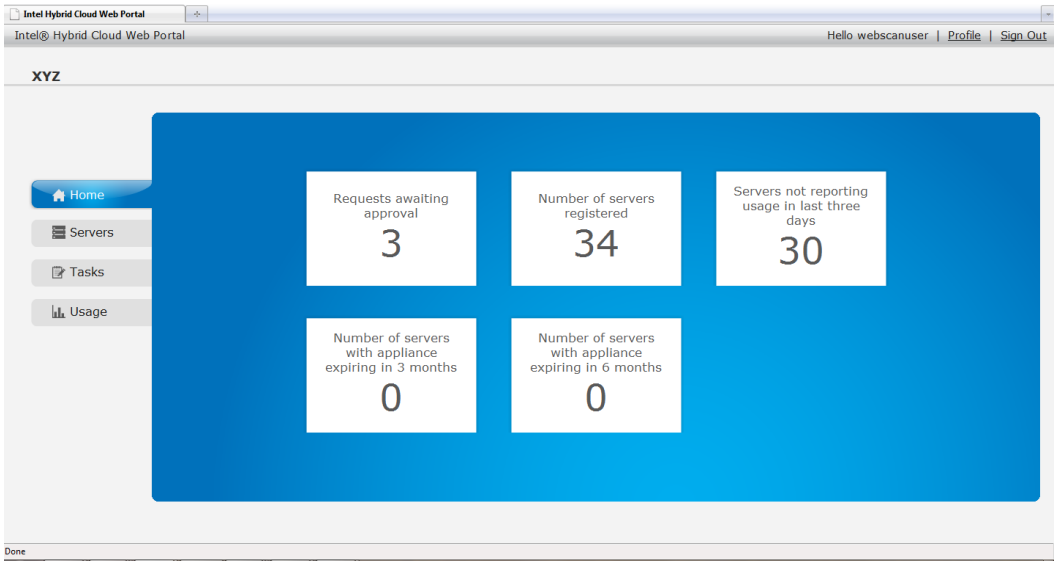

Figure 2. Intel® Hybrid Cloud management portal

2.4 Intel® Hybrid Cloud server manager

This simplified, UI-based application enables remote monitoring, management, and configuration of the server. Each software appliance runs on a separate virtual machine, allowing individual management of each appliance and isolation for reconfiguration or troubleshooting.

The details of Intel® Hybrid Cloud server manager (GUI) functionality are described in chapter 6 of the user guide.

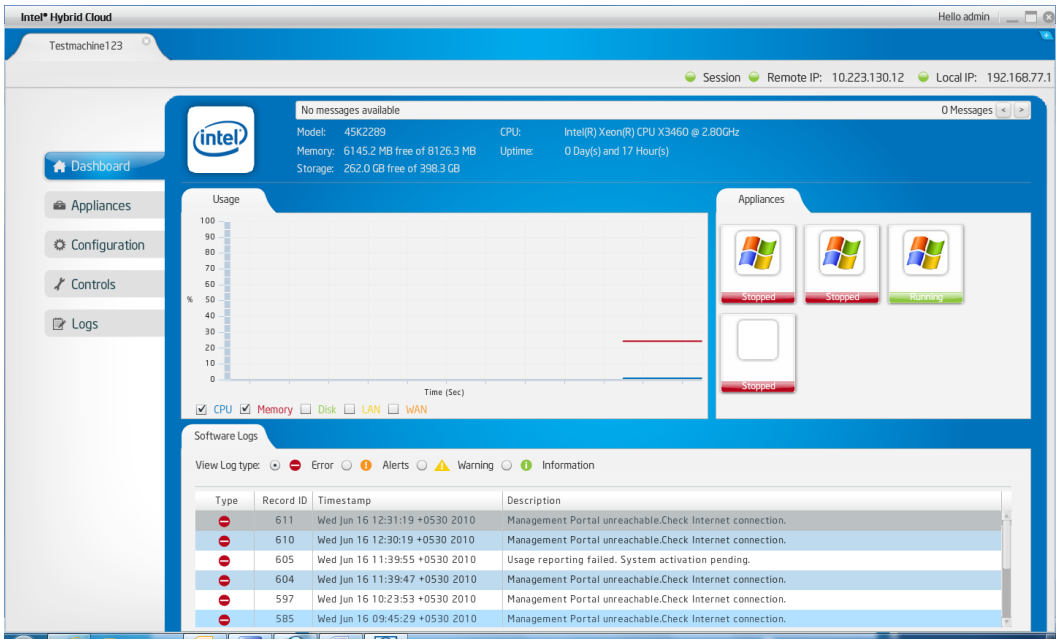

Figure 3. Intel® Hybrid Cloud server manager

There is also a command line utility (from here on referred to as IXE) available as part of Intel® Hybrid Cloud server manager and can be used for configuring and managing the Intel® Hybrid Cloud server. Details of IXE commands can be found in chapter 10 of the user guide.

3. System Requirements

3.1 Intel® Hybrid Cloud management portal

Intel® Hybrid Cloud management portal is accessed via a web browser. This release of Intel® Hybrid Cloud management portal supports the following browsers (minimum version is mentioned)

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

3.2 Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager runs on a client machine. Following is the recommended system requirement for the client machine running Intel® Hybrid Cloud server manager.

Minimum hardware Requirement - Pentium-4 2GHZ, 1GB RAM.

List of supported operating systems:

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

Intel® Hybrid Cloud server manager requires Adobe* AIR 2.5* for its operation. It is available for free download at http://get.adobe.com/air/. It can also be downloaded along with the Intel® Hybrid Cloud server manager. To know the details on how to download tools, please see Section 4.3 of this User Guide.

4. Getting Started

This section describes the steps to start using the Intel® Hybrid Cloud platform.

1. Setting up the Intel® Hybrid Cloud server.
2. Registering the Intel® Hybrid Cloud server.
3. Downloading Intel® Hybrid Cloud server manager.
4. Completing Registration process on management portal.

Each of these steps is described below.

4.1 Setting up the Intel® Hybrid Cloud server

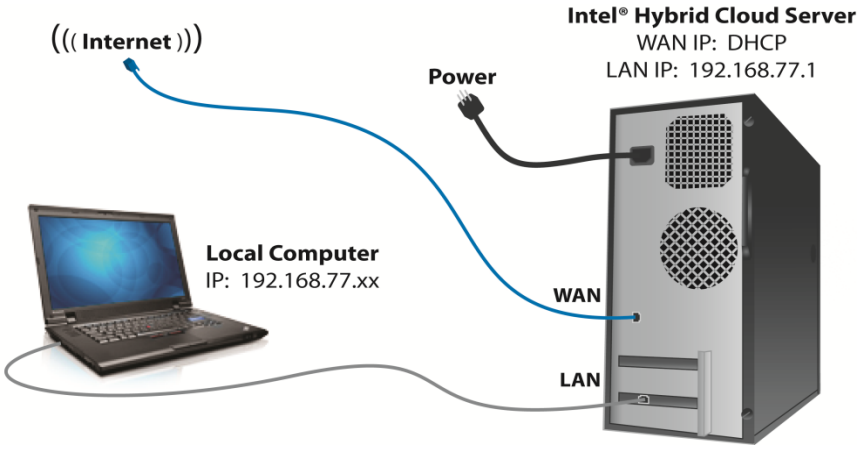

Figure 4. Basic Setup

1. Intel® Hybrid Cloud server has two Network interfaces – a WAN interface and a LAN interface. Both interfaces are provided via RJ45 jacks at the back of the system.
2. Connect the WAN port to the broadband access device (such as a cable modem, DSL modem etc).
3. Connect the LAN port to the Ethernet interface of a Windows* based client machine (such as a desktop or a laptop). Supported operating systems on client machine are Windows XP*, Windows Vista* and Windows 7*.
4. Configure the network interface of the client system to use a static IP address and use following settings for its network configuration:
   - IP address: 192.168.77.42
   - Subnet Mask: 255:255:255:0
   - Default Gateway: 192.168.77.1
5. Power up the Intel® Hybrid Client Server. Wait ~10 minutes for server to boot completely.

Note: If the Intel® Hybrid Cloud server is behind an external firewall, the initial configuration needs to be different from the above setup. Please follow the setup explained below.

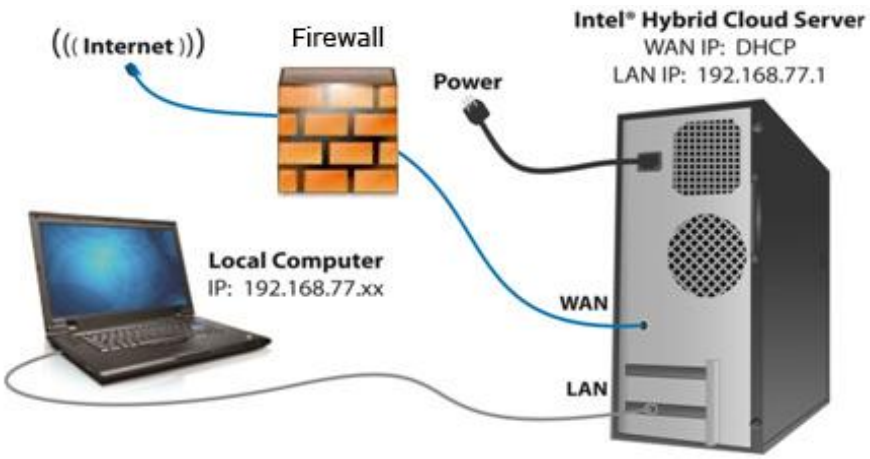

Figure 5. Setup if the Intel® Hybrid Cloud server is behind an external firewall

Default network settings for above setup are as follows (use the Intel® Hybrid Cloud server manager to change the settings as needed):

- The remote interface is configured for DHCP.
- The Local interface IP address is configured to 192.168.77.1 and subnet mask is configured to 255.255.255.0.
- Server can be accessed via https://<IP address>:64440/login

Intel® Hybrid Cloud server configuration has to follow the below steps:

- Server may not contain any Software Firewall appliance.
- All the client machines will be directly connected to the External Firewall.
- Move all the interfaces of the appliance on the server to WAN Link.

Manage the Intel® Hybrid Cloud server from external internet:

- Login to management portal and get the Internet IP Address of the server.
- Open the Intel® Hybrid Cloud server manager and connect to Internet IP with server username and password

Below are the ports that the Intel® Hybrid Cloud server uses to connect to the box externally and manage it. Please add appropriate entries in the external firewall.

Table 3. Ports

Port	Function	Forward to IP Address
64440	Management port used for the managing Intel® Hybrid Cloud server	Server IP Address
22	SSH to the Intel® Hybrid Cloud server	Server IP Address
65222	for the script engine that helps in debugging and executing some critical tasks	Server IP Address
16993	Intel® AMT Management port used for the managing Intel® Hybrid Cloud server “out of band” (OOB)	Server IP Address
16994-16995	Management port used for the managing Intel® Hybrid Cloud server via SOL	Server IP Address
5910-5920	VNC ports used for accessing the Appliance remotely	Server IP Address

Port	Function	Forward to IP Address
8282	BMC Management port used for the managing Intel® Hybrid Cloud server "out of band" (OOB)	BMC IP Address
443	RMM3	BMC IP Address

4.2 Initiating Registration for the Intel® Hybrid Cloud server

For the Intel® Hybrid server to be used for the first time, it needs to be registered first with the management portal.

Note: Registration for the Intel® Hybrid Cloud server can be done only by the Remote Administrator (that is, only by "admin" role).

1. Once Intel® Hybrid server box is accessible on the LAN interface, open one of the supported internet browsers from your Windows* client machine and type https://192.168.77.1:64440/login in the address field.
2. Enter the default User Name and Password in the "Connect to Server" login box.
   a. Default Username: admin
   b. Default password: admin

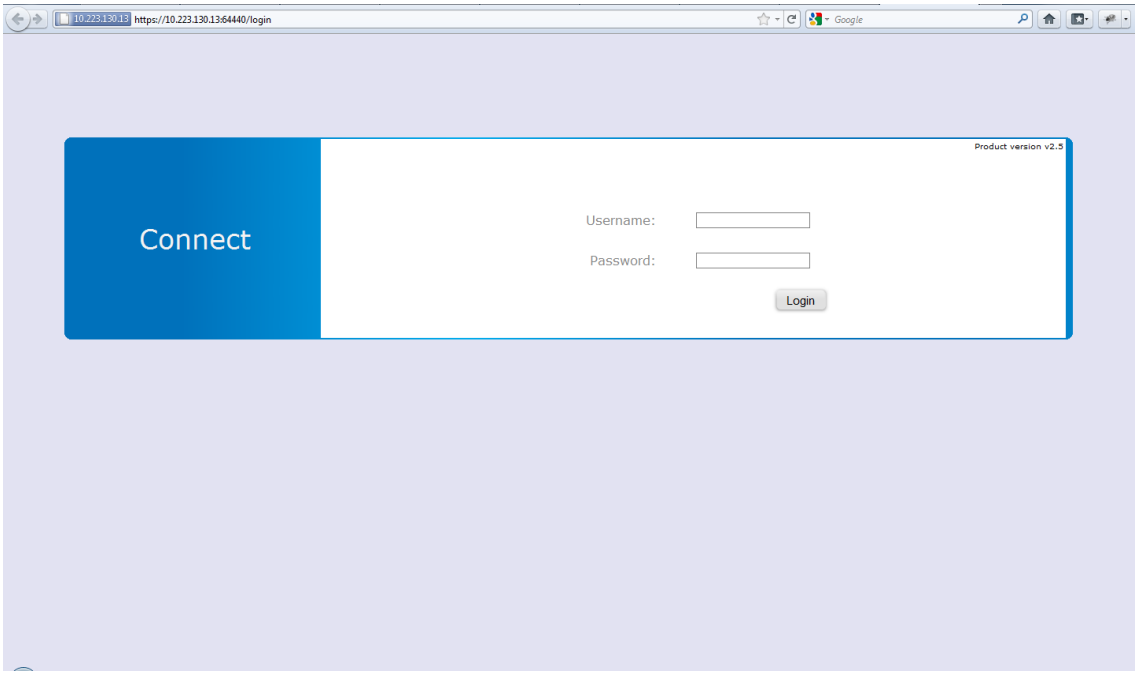

Figure 6. Registration for the Intel® Hybrid Cloud server – Connect Page (Username, Password)

3. You will be presented with an End User License Agreement. Remote Administrator must accept the end user license to proceed further.

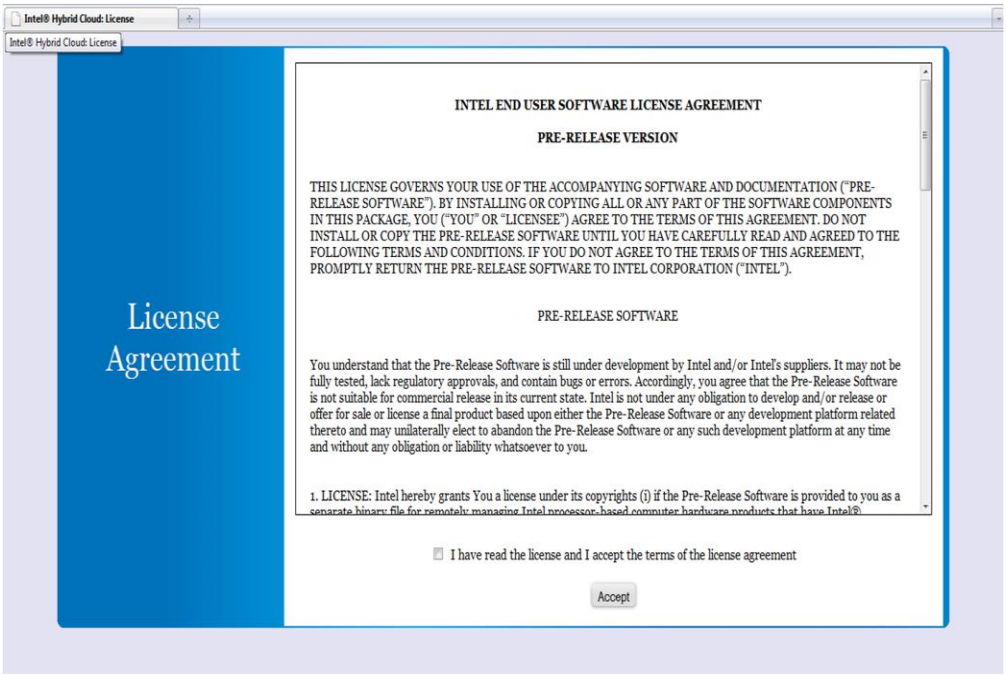

Figure 7. Registration for the Intel® Hybrid Cloud server – License Agreement Page

4. At this stage, Intel® Hybrid Cloud server will try to contact the management portal. It's possible that server is not able to reach the management portal because IP address settings used for WAN interface are not correct. If this happens then a web page to configure the Remote IP address appears (see screenshot below). Here the IP and other details can be provided.

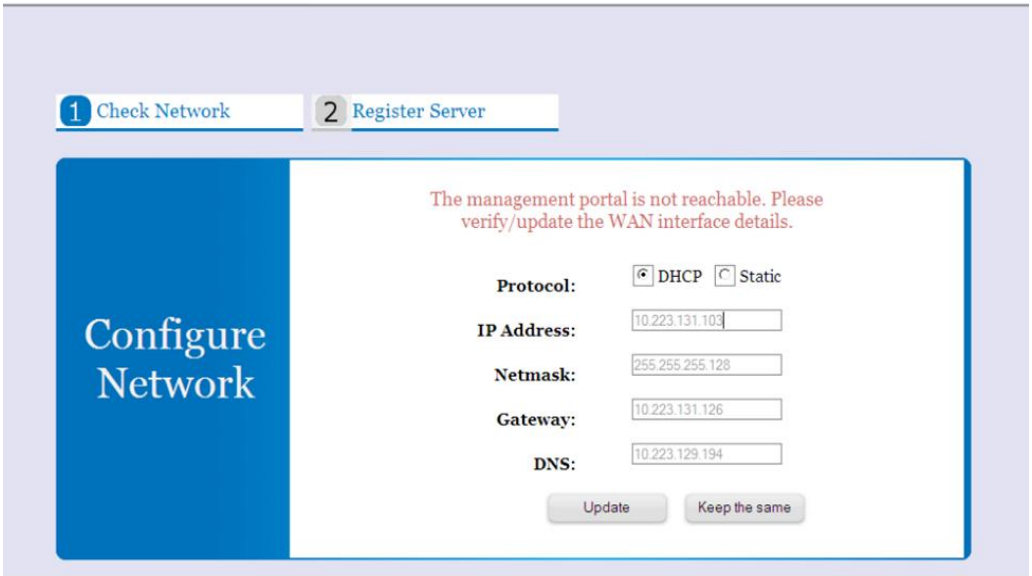

Figure 8. Registration for the Intel® Hybrid Cloud server – Configure Network Page

5. Once Intel® Hybrid Cloud server is successfully able to contact management portal, a web page to register this server with management portal is shown. You must enter following details to register this server with the management portal:
   - Server Name -- This is the name by which this server will be shown in the management portal
   - Remote Administrator ID – This is the login ID used by you to access management portal.
   - Click **Register**.

The status of the Intel® Hybrid Cloud server moves to Registration Pending. Now you can download available software tools (section 4.3) or skip the step, if you already have the software tools and move directly to completing registration process (section 4.4).

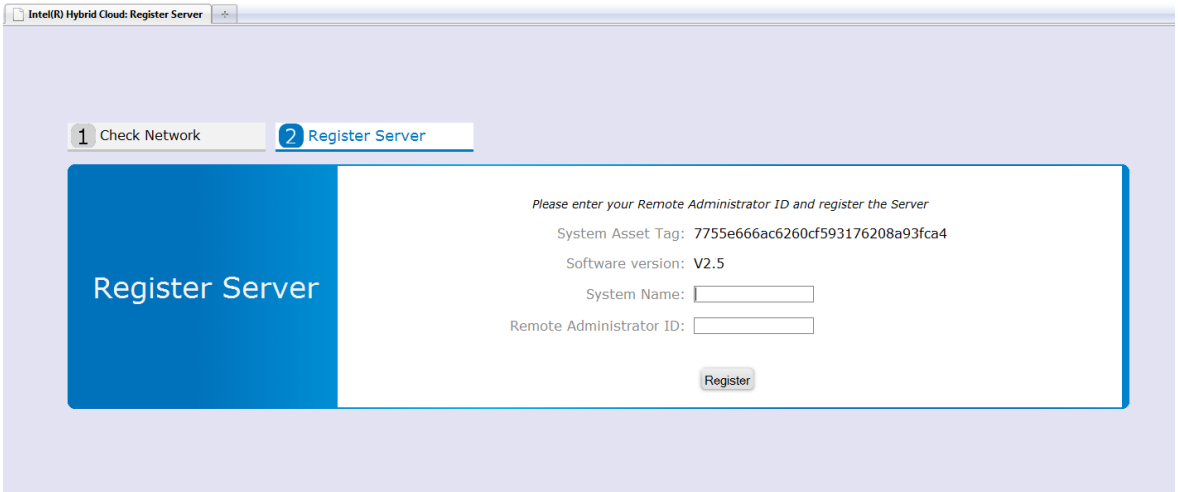

Figure 9. Registration for the Intel® Hybrid Cloud server – Register Server Page

4.3 Downloading Intel® Hybrid Cloud server manager.

Once the state of the Intel® Hybrid Cloud server is “Registration Pending” or “Registered”, a Remote Administrator or a user can download the management tools by accessing the Intel® Hybrid Cloud server at https://192.168.77.1:64440/login.

There are three ways to manage Intel® Hybrid Cloud server.

- Windows* based CLI tool (IXE)
- Linux* based CLI tool (IXE)
- Adobe AIR* based GUI tool (Intel® Hybrid Cloud server manager)

User can download the software tools from this page as shown below.

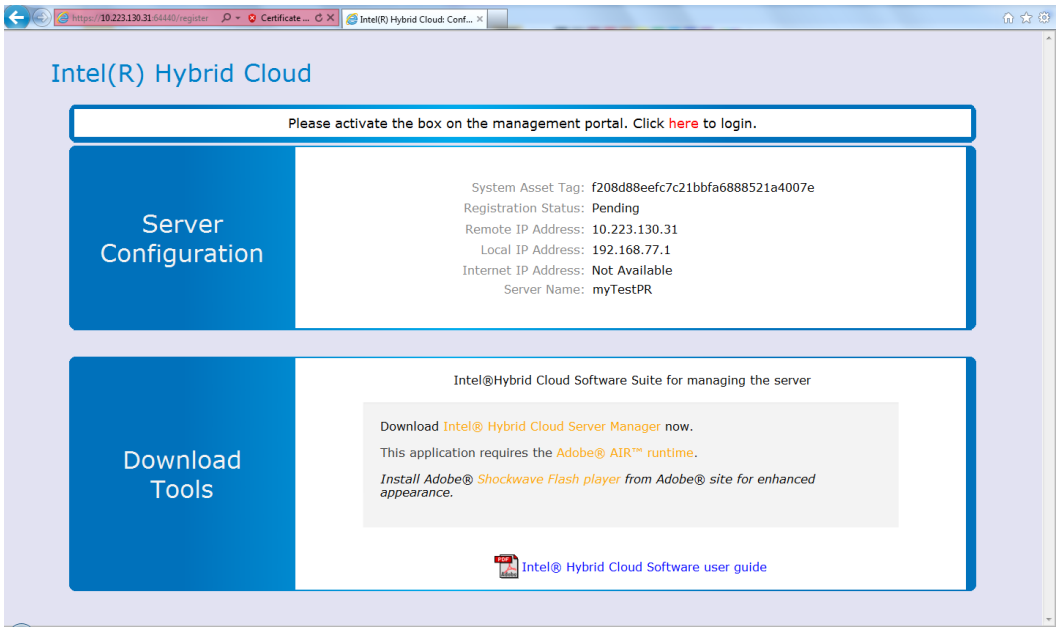

Figure 10. Registration for the Intel® Hybrid Cloud server - Configuration and Download Tools Page

Notes:

- No management operations via these tools are allowed till the Intel® Hybrid Cloud server moves to registered state.
- Download duration of the tools may take time as it primarily depends on the link bandwidth between the client and server.
- For Intel® Hybrid Cloud server manager Installation, make sure Adobe* AIR runtime v2.5 is already installed. If the client is connected to internet clicking “Install Now“ will download both Intel® Hybrid Cloud server manager and Adobe® AIR runtime v2.5 otherwise user has to download both tools separately.
- 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.

4.4 Completing Registration process on Intel® Hybrid Cloud management portal.

1. Remote Administrator (or MSPs) needs to log in to the management portal and confirm the registration of a particular Intel® Hybrid Cloud server.

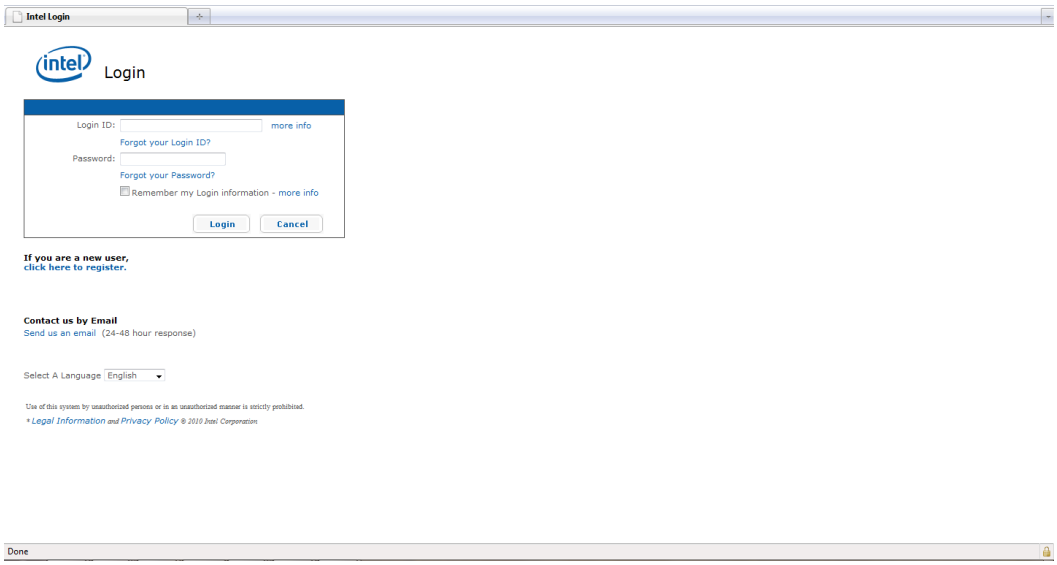

Figure 11. Intel® Hybrid Cloud management portal Login page

2. The list of registration activation appears in the pending task list. (See the screenshot below). Click Task tab in the left pane to view the list of pending registrations.

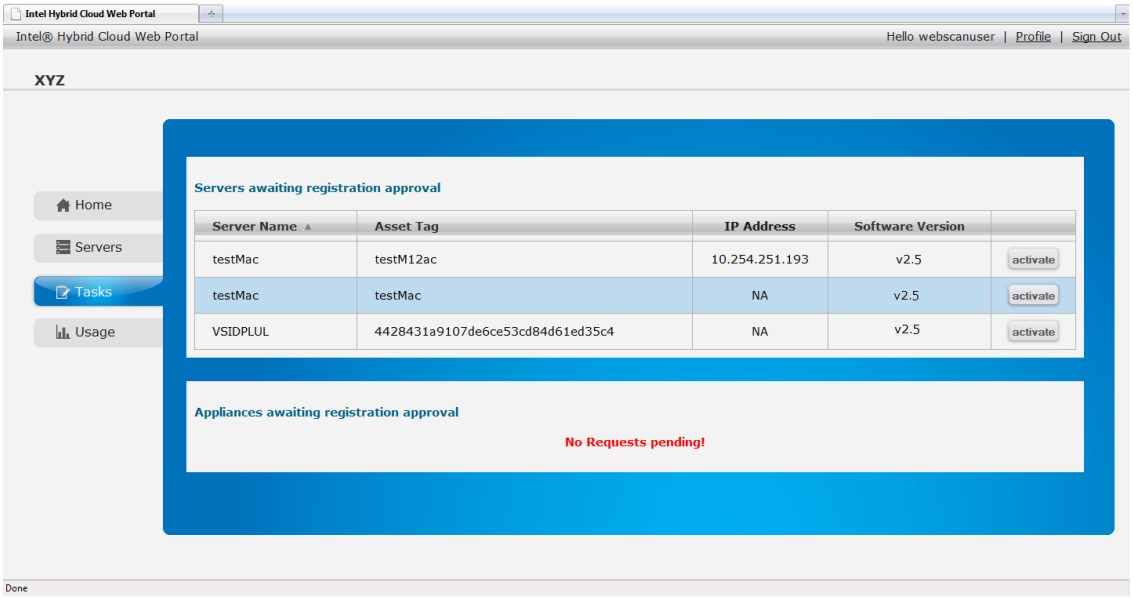

Figure 12. Intel® Hybrid Cloud management portal Task List

3. The Remote Administrator can click on the activate button which shows the details of the Intel® Hybrid Cloud server and a list of appliances installed on that server. Remote Administrator can choose to activate each of the appliances and confirm the registration. This confirmation activates the Intel® Hybrid Cloud server and the appliances. Expiry date for the appliances is set to a default of 3 years. Remote Administrator can also enter end customer name for the selected server.

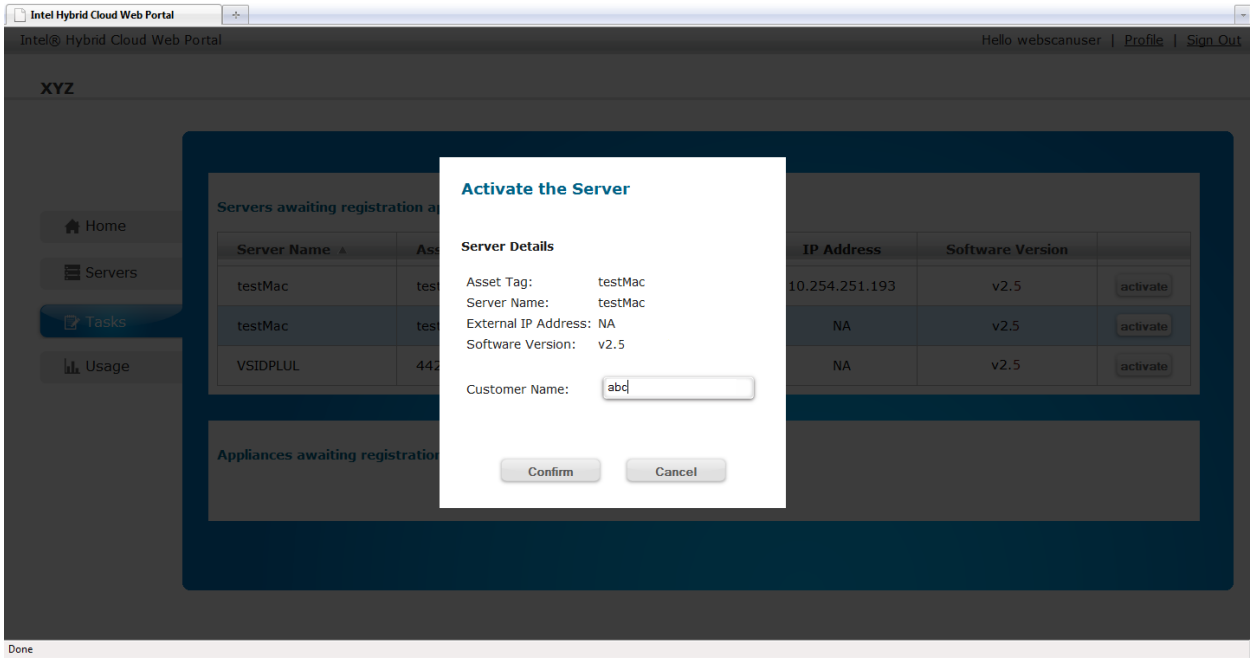

Figure 13. Intel® Hybrid Cloud management portal - Activating the Server and appliances

For details on more Intel® Hybrid Cloud management portal operations, please go to next section.

4. Your Intel® Hybrid Cloud server is now ready to use.

5. Intel® Hybrid Cloud management portal

Channel Partners/Remote administrators/MSPs can register, activate and monitor usage of various Intel® Hybrid Cloud servers that they deploy and manage for end users via an easy to use Intel® Hybrid Cloud management portal.

Various features available under this management portal are described in detail below.

5.1 Accessing Intel® Hybrid Cloud management portal

Remote Administrator needs to login to the management portal as a first step before he/she can start. Please use a supported Web Browser and type https://hybridcloud.intel.com in the address field.

Figure 14. Intel® Hybrid Cloud management portal Login Screen

Intel® Hybrid Cloud management portal has a timeout of five minutes. Inactivity of more than five minutes would automatically logout the logged in user. In case if administrator forgets the password, one can refer to “Recovering Password” of the *Troubleshooting Guide*.

5.2 management portal Dashboard

Following is the screenshot of the dashboard screen of the management portal with an overview of the servers that the administrator owns and some of the pending requests for the administrator.

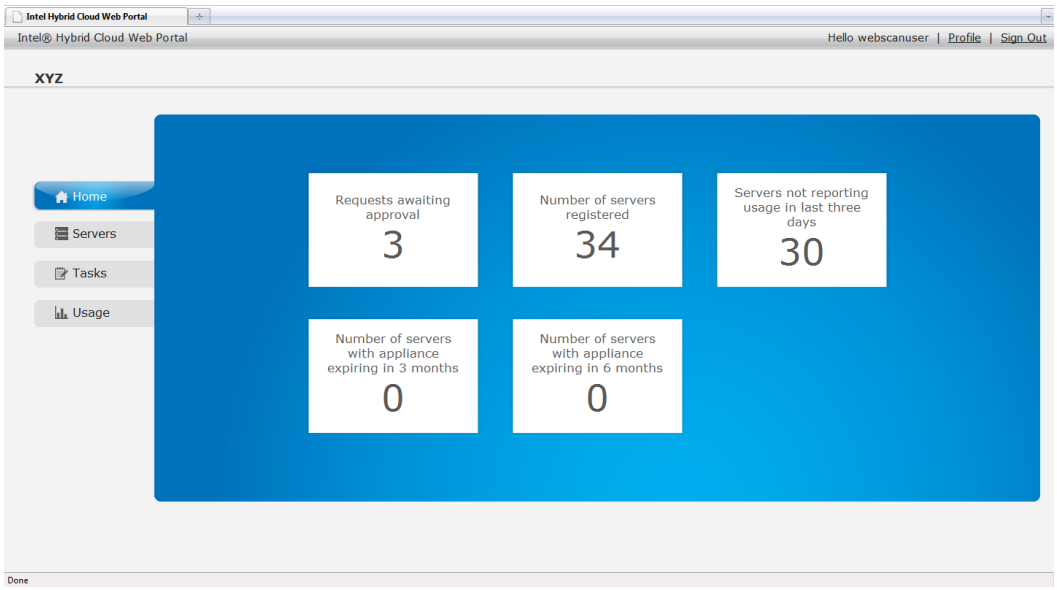

Figure 15. Intel® Hybrid Cloud management portal Dashboard

5.3 Managing Registered Servers

Once the server is registered and the administrator confirms the registration on the management portal, the server is listed in the “Manage Servers” list. Administrator can go to the Manage Servers page and modify the expiry date of appliance licenses or activate/deactivate the appliances. From the management portal, administrator will also be provided with a mechanism to launch the Intel® Hybrid Cloud server manager for each of the servers and can manage a specific server in detail using the same.

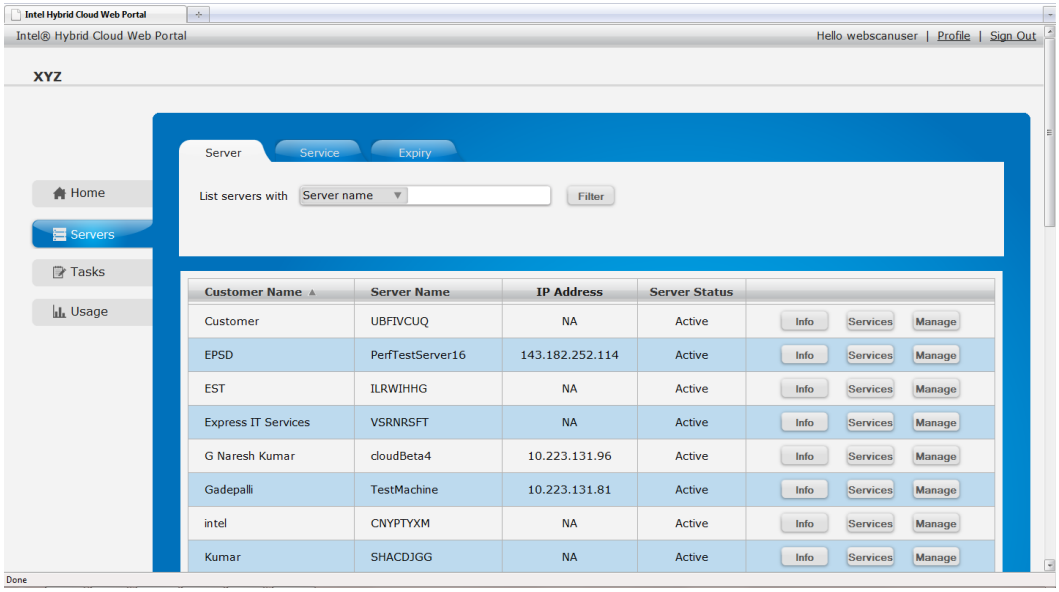

Figure 16. Intel® Hybrid Cloud management portal – Managing Registered Servers

In the above screen, following are the actions and corresponding details available:

- Click on **Info** for additional details about the deployed server (including VMM expiry, System Asset Tag, System HW serial number, Intel® Hybrid Cloud software stack version).
- Click on **Manage** to open the Intel® Hybrid Cloud server manager to manage the server.
- Click on the **Services** to view the list of appliance(s) installed on the server. Remote Administrator can activate/deactivate and change the expiry date of the appliance(s) license. Default appliance expiry is set to three years.

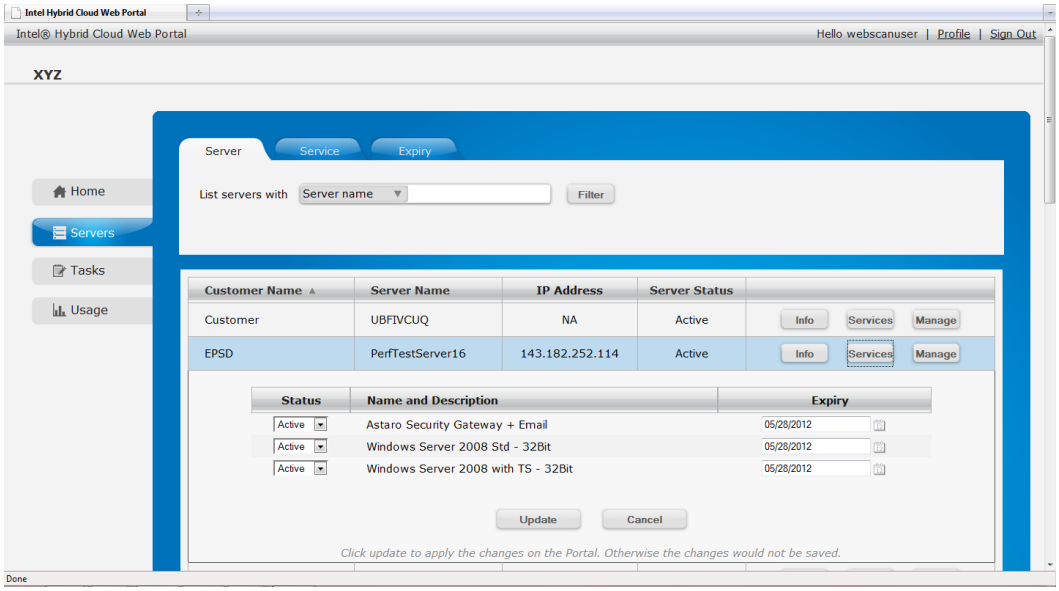

Figure 17. Intel® Hybrid Cloud management portal –Servers Screen (Services tab)

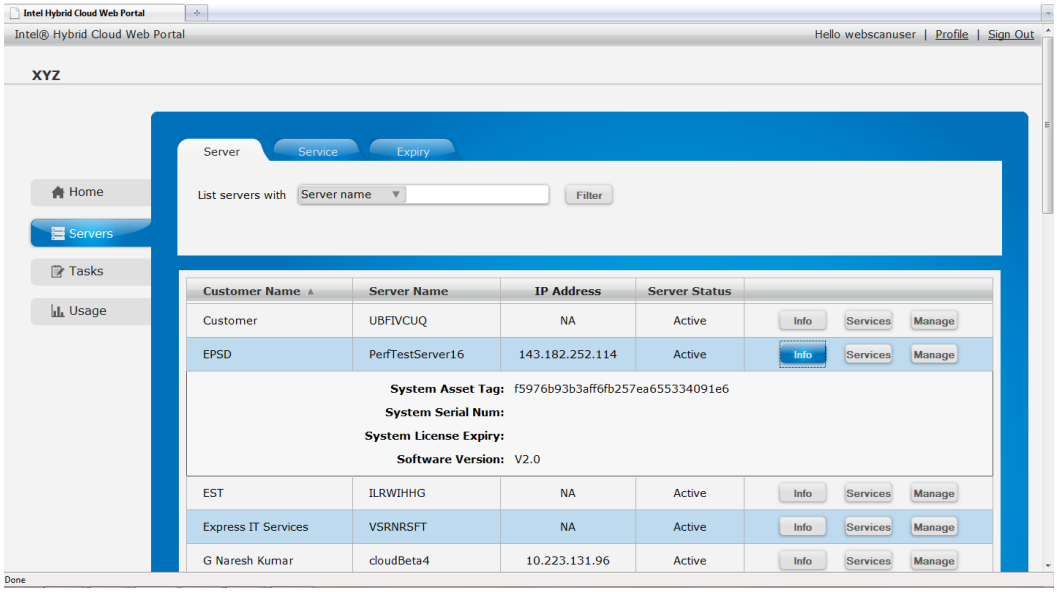

Figure 18. Intel® Hybrid Cloud management portal – Servers Screen (Info Tab)

5.4 Viewing Intel® Hybrid Cloud server Usage

The management portal also provides the option for the administrator to view the usage of all the appliances on a server. Each server reports the appliance-specific usage to the management portal on a daily basis which gets populated in the database. The Usage report display provides a graph-based and a text-based report of each of the appliances as shown in the following screenshot for usage reports.

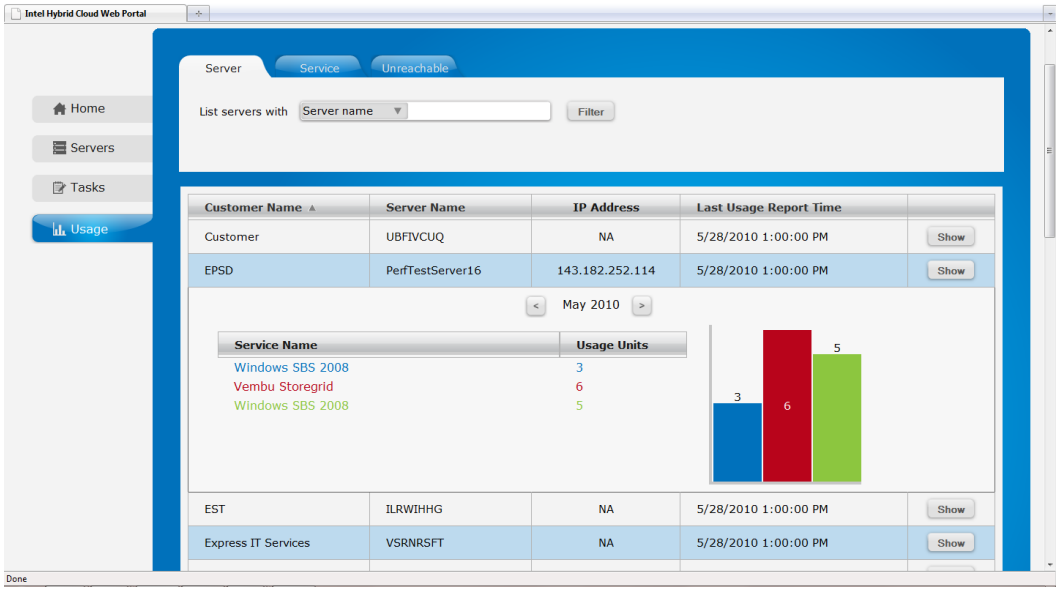

Figure 19. Intel® Hybrid Cloud management portal - Viewing Intel® Hybrid Cloud server Usage-1

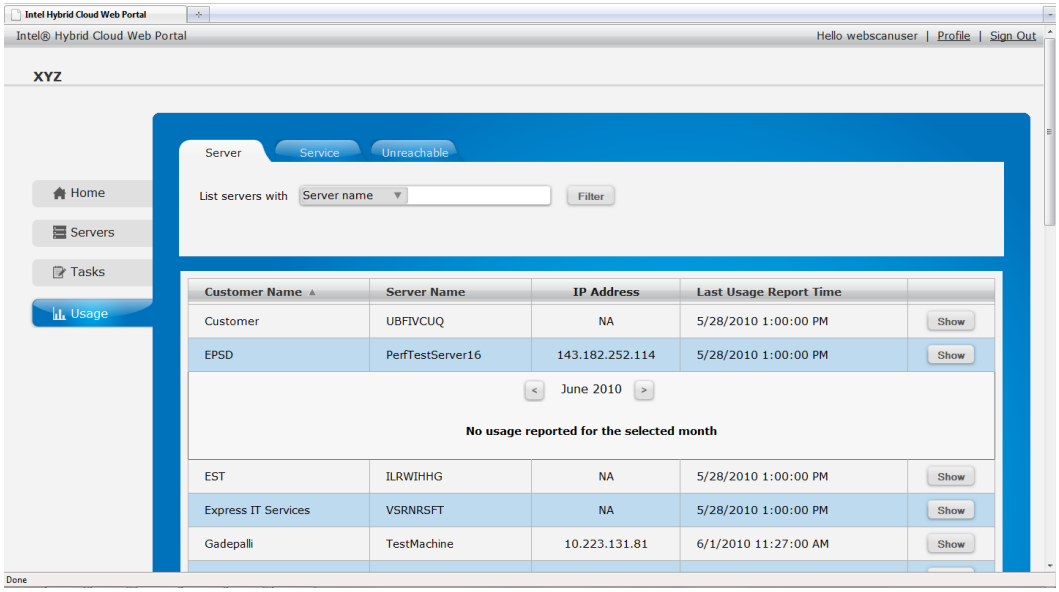

Figure 20. Intel® Hybrid Cloud management portal - Viewing Intel® Hybrid Cloud server Usage - 2

5.5 Viewing the Customer Profile

Management portal provides a read only access to the customer profile. Click on the **Profile** link on the top right corner to open the profile information as shown in following screen.

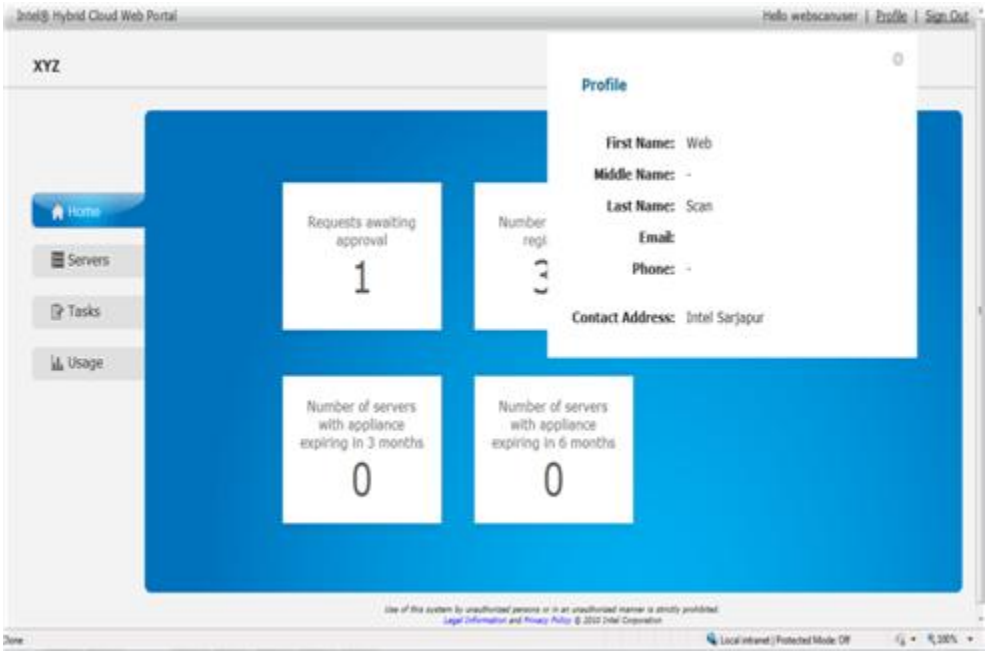

Figure 21. Intel® Hybrid Cloud management portal –Viewing Customer Profile

5.6 Reactivating the appliance

If the system has not connected to the management portal for consecutive 30 days, all the running appliances are stopped and appliances' licenses are revoked. Administrator needs to again activate those appliances using the management portal once the server comes online. Also, remote administrator should mange the expiry of appliance licenses from the management portal. Starting from 15 days prior to expiration of appliance licenses, warning messages are added on Intel® Hybrid Cloud server manager to indicate appliance license expiration. After expiration of licenses, user is allowed to use the appliance for 15 more days as grace period. Post the grace period, license for the corresponding appliance(s) is revoked and the appliance(s) is shutdown. Based on requirements of the end user, Remote Administrator can choose to extend the appliance license from the management portal.

6. Intel® Hybrid Cloud server manager

After the registration of Intel® Hybrid Cloud server, it can be managed using Intel® Hybrid Cloud server manager locally (via LAN link – add on card interface) or remotely (via WAN link– onboard NIC interface). Various management features will be available via both local and remote server manager depending on user role (admin/user)

Note: Maximum of 4 simultaneous remote connections (LAN + WAN) are allowed per Intel® Hybrid Cloud server.

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

Intel® Hybrid Cloud server manager follows a Role Based Access Control (RBAC) mechanism. There are two roles supported by the Intel® Hybrid Cloud server manager. A user can access the server with either of the following roles:

1. “admin” with default password “admin”
2. “user” with default password “user”

Once Intel® Hybrid Cloud server is configured for both local and remote access, end user and remote administrator can use Intel® Hybrid Cloud server manager to manage the server. In the sections hereafter, it is assumed that remote administrator is managing the server remotely with “admin” log in. User will have restricted view depending upon permissions given. The role with which the user has logged in determines the access control. However, “admin” has rights to modify the default access control for the “user” as needed. The rights can be modified using the Intel® Hybrid Cloud server manager.

Note: Intel® AMT features like HW inventory, HW events, Force shutdown, and Force restart are only available via the WAN interface. The admin/user must change the password after first login.

6.2 Login for managing multiple servers

Remote administrators can login to Intel® Hybrid Cloud server manager using Intel® Hybrid Cloud management portal login credentials and can see list of all active servers registered by them. They can then launch the Intel® Hybrid Cloud server manager for a specific Intel® Hybrid Cloud server.

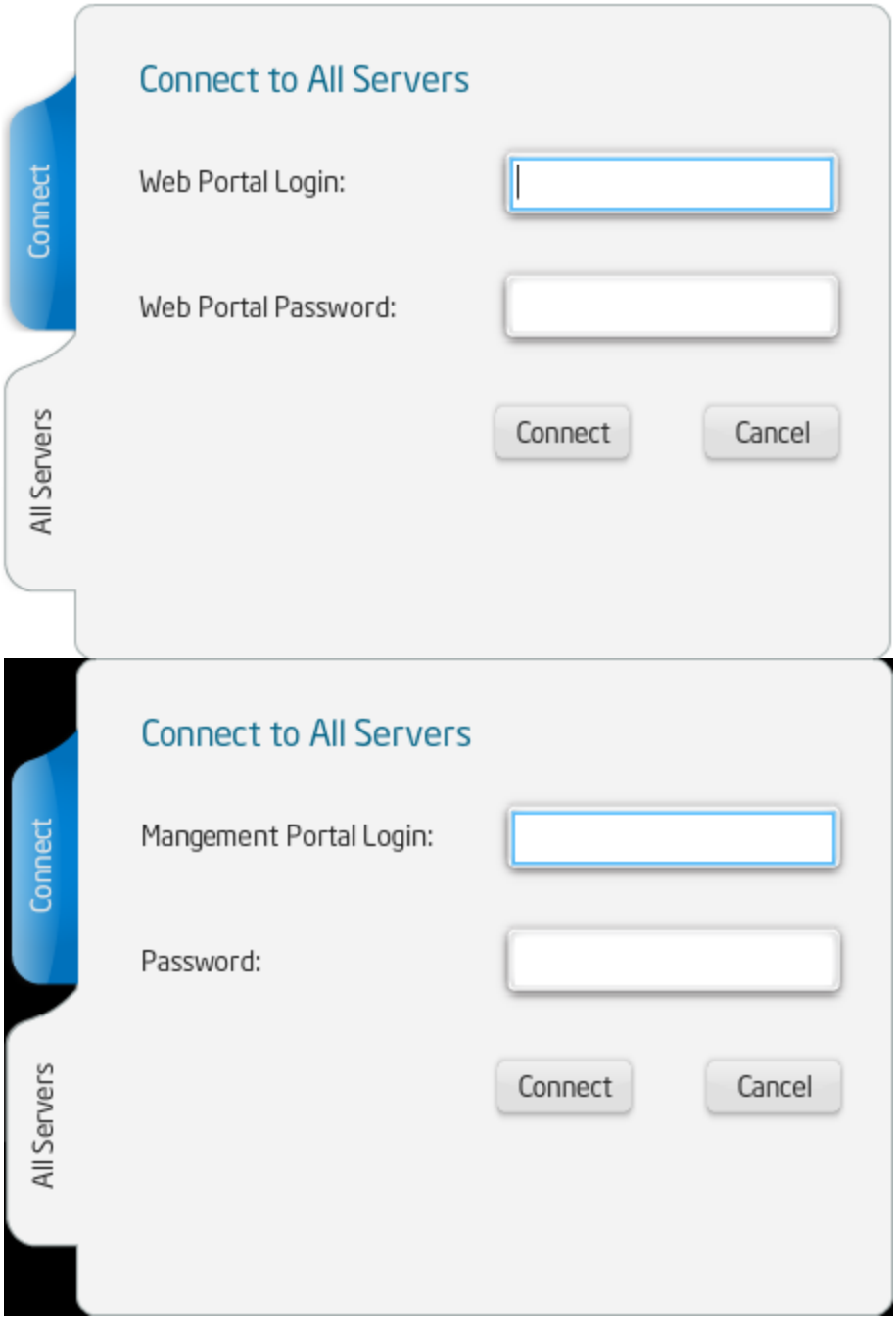

Figure 22. Intel® Hybrid Cloud server manager – Connecting to All Servers

6.3 Login to a specific Server

If the administrator/user chooses to connect to a particular server directly, the user will be asked to also provide IP address along with Server name.

Note: You can connect to a specific server only if it is already registered.

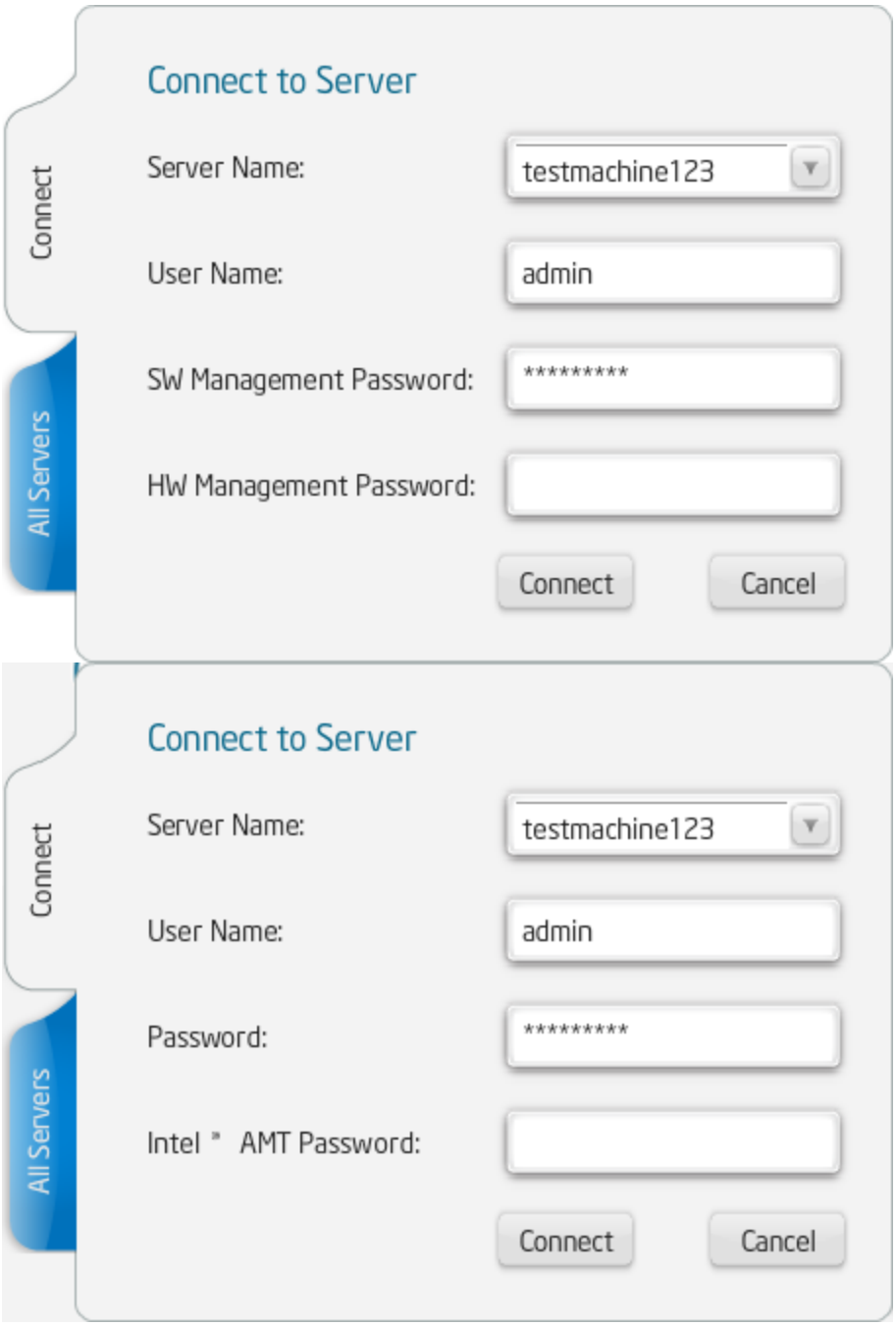

Figure 23. Intel® Hybrid Cloud server manager Login Window

When you access a server for the first time, you need to provide the IP address of the server. This information will be used to add the specific server to the hosts file.

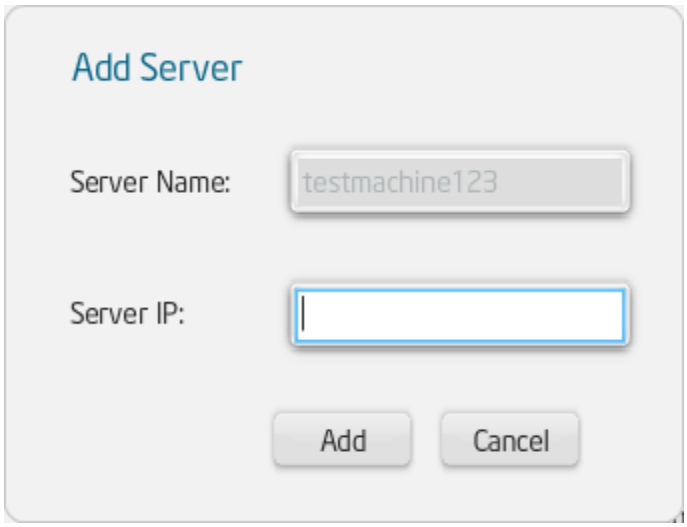

Figure 24. Intel® Hybrid Cloud server manager: Add server to hosts file

If the server is successfully registered and this is the first time Remote Administrator or user is logging in, they are required to change the default password and set a new password. Also, admin needs to give Intel® AMT password to access Intel® AMT features. If no password is given, Intel® AMT features will not be available in the UI. Login for user role will not have an option for accessing Intel® AMT features.

Notes**:**

- Entering IP address as the hostname is not allowed. User must enter hostname to connect to the server.
- User with Admin role can connect to server using Intel® AMT even when the server is powered off. In order to connect to Intel® AMT, it is necessary to give only hostname and Intel® AMT password. Using Intel® AMT, user can power on the system remotely. This feature is available only from remote connection (WAN IP) and only for admin role.

After clicking **Connect** to connect to the Intel® Hybrid Cloud server manager, the user is prompted to install an SSL server certificate (if not previously installed). This SSL certificate is presented every time the hostname of the server changes. User must install the certificate whenever prompted. Please refer to Troubleshooting guide if certificate prompts continue to appear even after installation of the certificate.

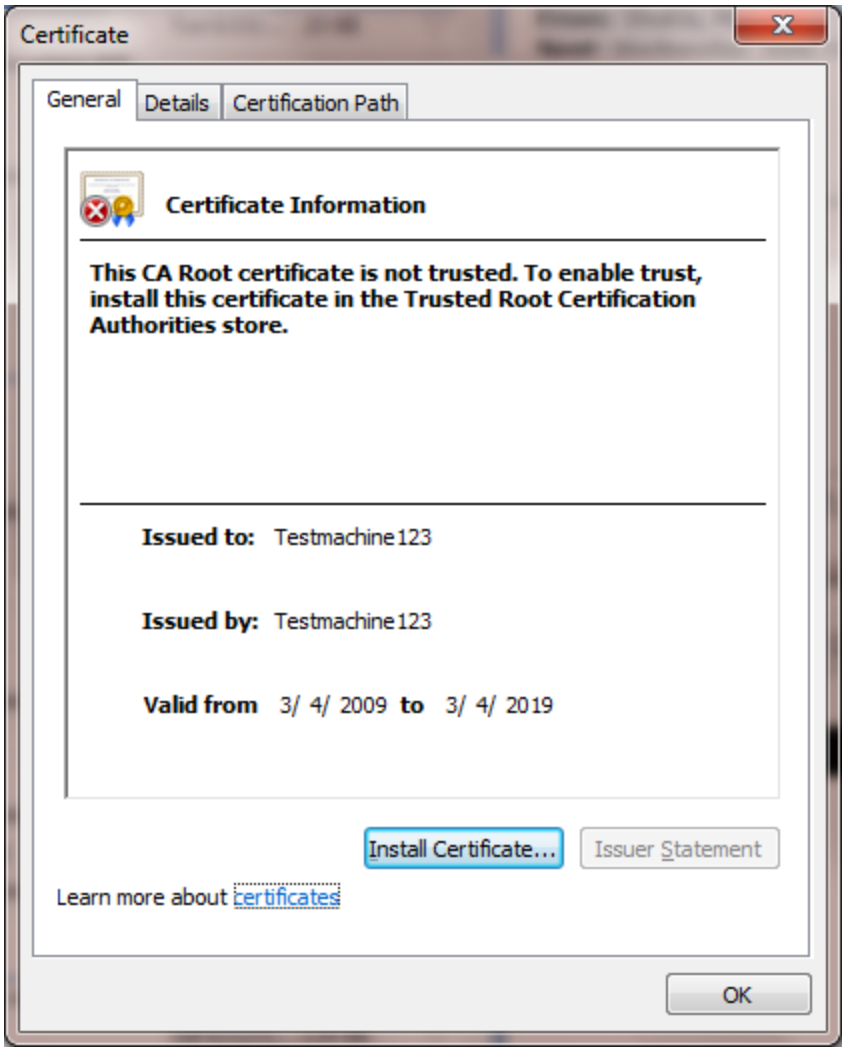

Figure 25. SSL Server Certificate

6.4 Windows 7*/Vista* Certificate Install process

6.4.1 Adding server name to the hosts file

When connecting to an Intel® Hybrid Cloud server, the Intel® Hybrid Cloud server manager first adds the IP Server name combination to the Windows* hosts file. In Windows 7* and Windows Vista*, special privileges needs to be set to enable Intel® Hybrid Cloud server manager to update the hosts file. The following command needs to be run in command prompt logged in as Administrator:

```
attrib –h –s c:\windows\system32\drivers\etc\hosts
```

Note: One needs to log in to Server Management console as an administrator for the first login to enable adding server name to hosts file.

6.4.2 Installing SSL server Certificate

In Microsoft Windows 7* and Vista*, user has to install the server certificate in a specific location in order to avoid the repeated certificate that popup when the admin/user logs in.

When the user tries to login to the server, the certificate window displays a pop-up message as shown below":

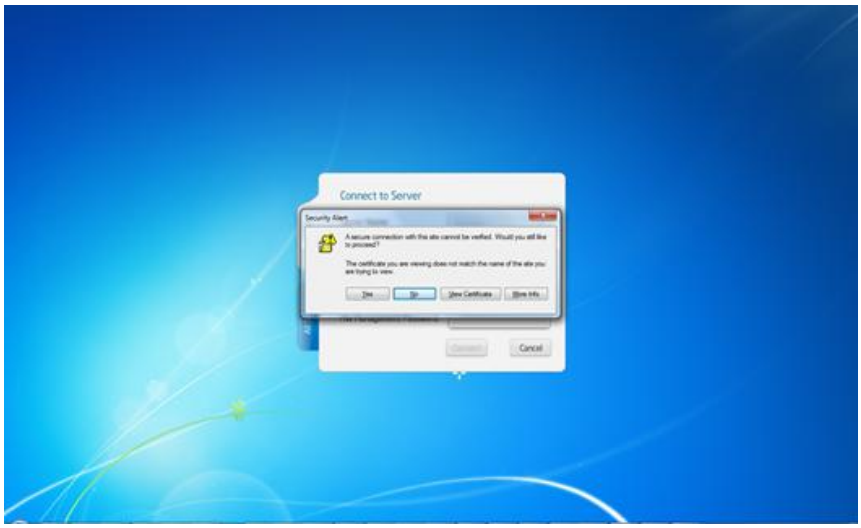

Figure 26. Certificate pop-up window

User has to follow these steps:

1. Click on **View Certificate**.

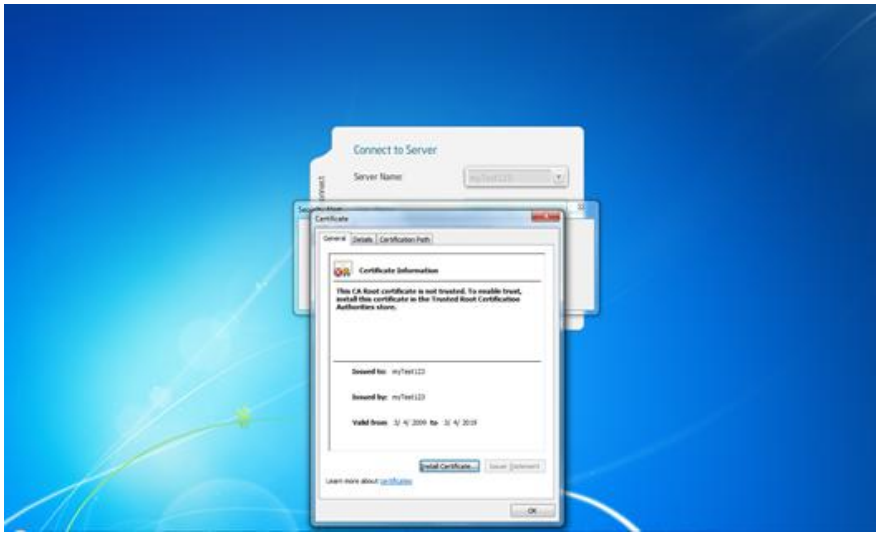

Figure 27. Installing the certificate

2. Click on **Install Certificate**.

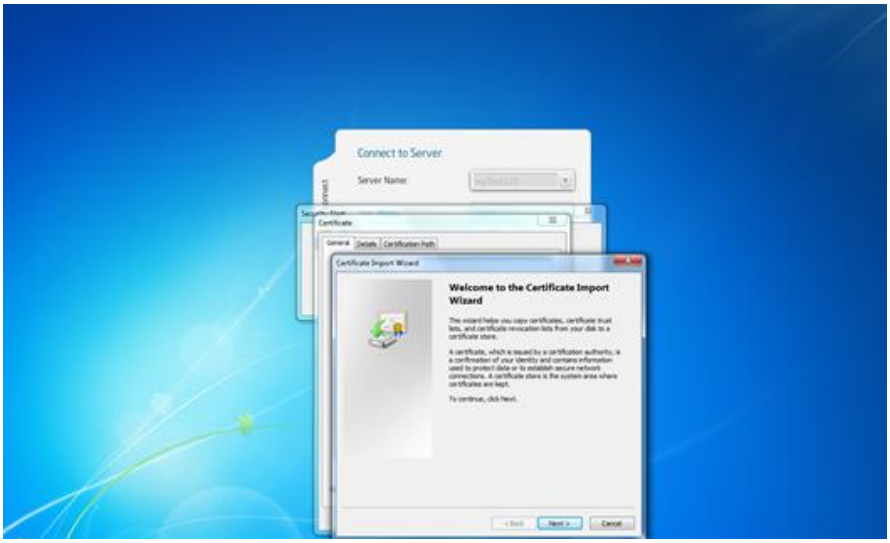

Figure 28. Certificate Import Wizard window

3. Click on **Next** till the Certificate Store selection window is displayed.

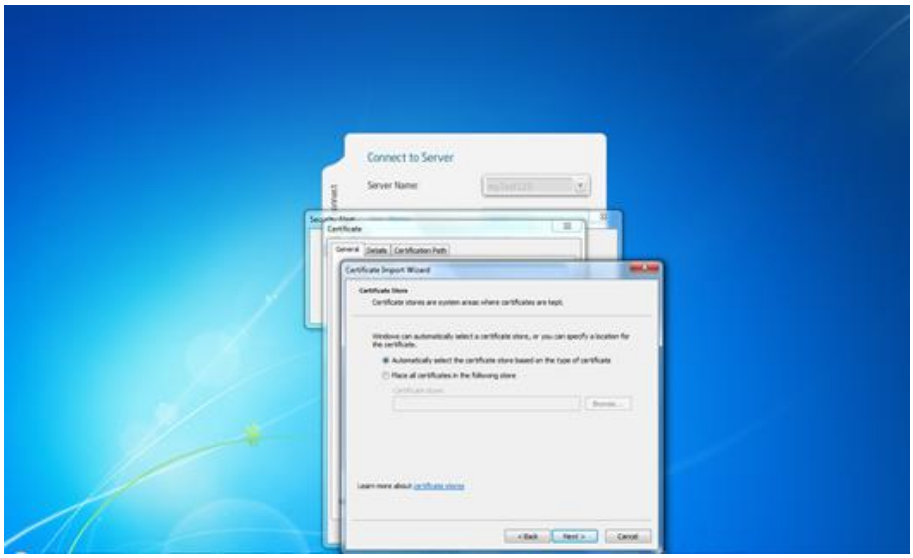

Figure 29. Browsing the Certificate Wizard window

4. Select **Place all certificates in the following store** and click on **Browse**.

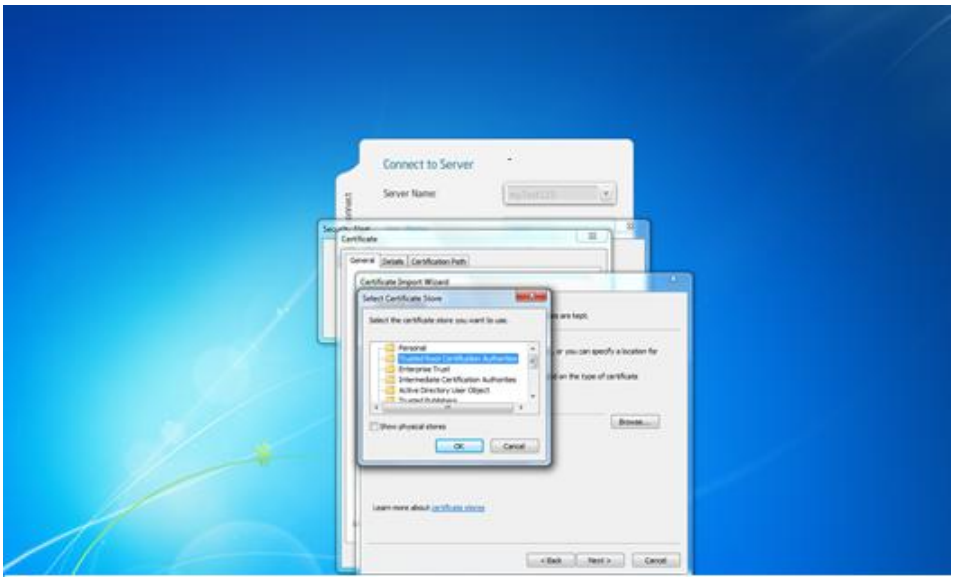

Figure 30. Completing the Certificate installation

5. Select the **Trusted Root Certification Authorities** store and click **Next** and **Finish** to complete the certificate installation.

The above process will ensure that certification prompts are not repeated once installed for a specific server.

6.5 Dashboard

Once connected to an the Intel® Hybrid Cloud server, Intel® Hybrid Cloud server manager "Default" 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 indicating the installed appliances on Intel® Hybrid Cloud server and their current power state (Starting/Stopping/suspending/halted/Suspended/Importing/Running)
- **Software Logs** — Log table that can show latest five logs of information, warning, alert and error categories. Each entry has a record ID, timestamp and description

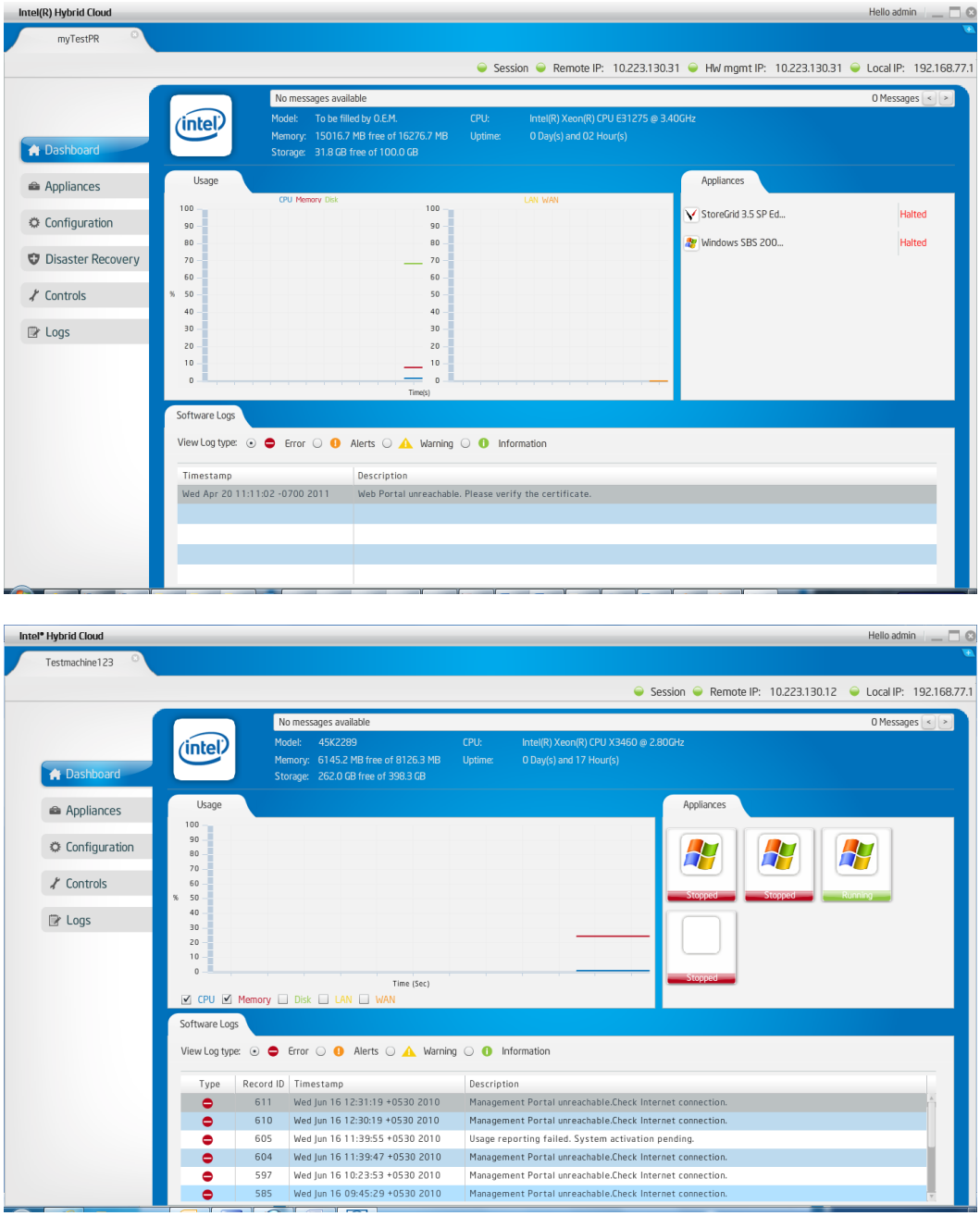

Figure 31. Intel® Hybrid Cloud server manager Default view (Dashboard)

6.6 Hardware Inventory

This tab provides detailed HW information of the Intel® Hybrid Cloud server via Intel® AMT. This option is available only on “admin” role when connected through the remote interface and Intel ® AMT password is provided. Following is a sample screen for system information. Similar data is available for processor, memory, and disk.

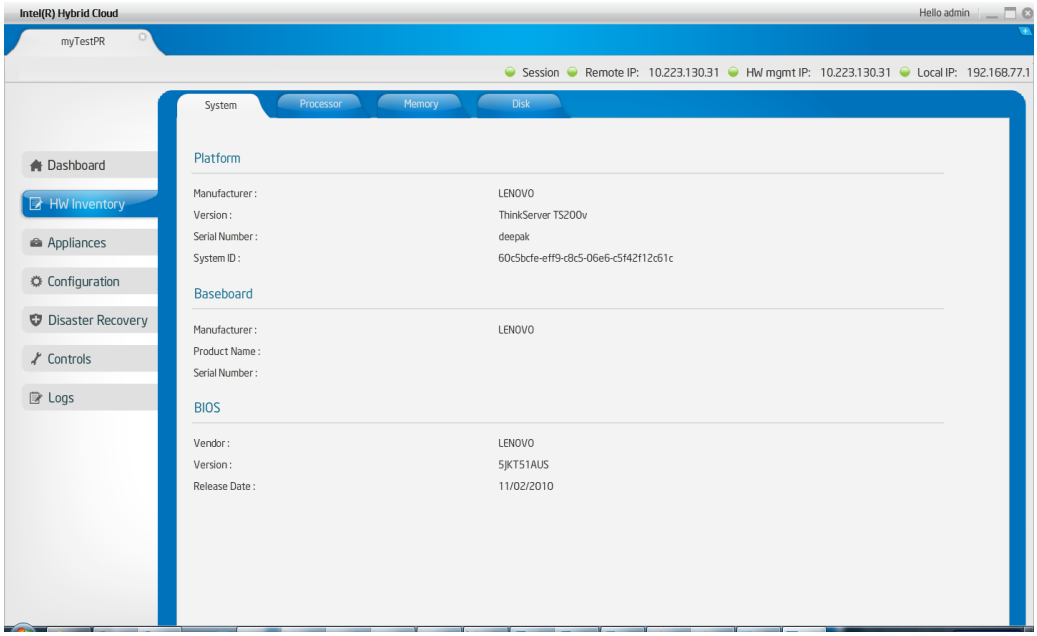

Figure 32. Intel® Hybrid Cloud server manager- Hardware Inventory: System Information window

6.7 Managing Appliances

Appliances installed on Intel® Hybrid Cloud server can be managed using the **Appliance** tab on the default screen. Default view under this option consists of icons for all the appliances available on top along with status of each of these appliances. User can select any appliance and manage it. Appliance details like Appliances name, vendor, and version are shown along with an option to either start/stop/suspend/resume the appliance depending upon its current state. For example, if an appliance is already started, the option to “stop” and “suspend” it and vice versa are available. Also, after installing the appliance, the default state is stopped. When the appliance is in this Stopped state, there is also an option to uninstall the appliance.

An appliance can be started or resumed (based on its current state) only when the license state of the appliance is activated via the Intel® Hybrid Cloud management portal. If the license of an appliance is inactive and Remote Administrator/user tries to start the appliance, the appliance license query is sent to the management portal. Only if the license is marked “active” on the management portal is the appliance allowed to start and license is marked “Active” on the Intel® Hybrid Cloud server manager. Else, an error message is displayed.

Likewise, an appliance can be remotely deactivated via the Intel® Hybrid Cloud management portal. However, this information is retrieved by the server only once in 24 hours (when usage information is reported to the management portal) or Remote Administrator can force the usage reporting (via IXE command) and thereby, the appliance state information is updated on the server. For details on IXE commands, please refer chapter 10.

If the appliance license has expired, the user is allowed to use the appliance for a grace period of 15 days post license expiry date, after which the appliance is suspended /shutdown (if suspend operation is not possible) Warning messages are logged in 15 days prior to expiry of the appliance license and error messages are logged in the grace period.

In addition to appliance details, there are four options available in this view:

6.7.1 Appliance Monitor

Usage details of resources like Memory, CPU, Disk, LAN, and WAN allocated to an appliance can be monitored via the graph available here. Also, allocated values to memory, CPU & disk are shown.

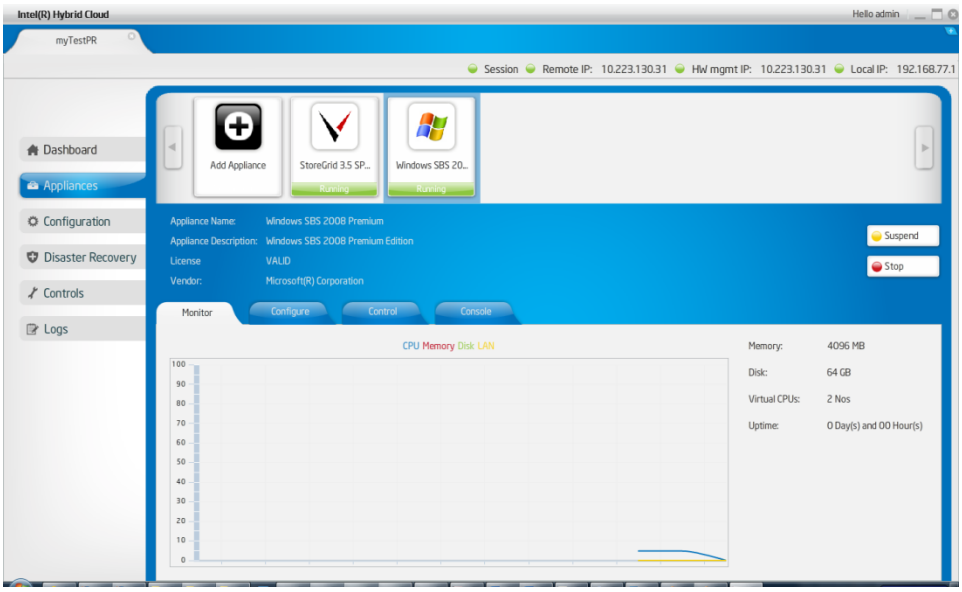

Figure 33. Intel® Hybrid Cloud server manager - Appliances Monitor window

6.7.2 Appliance Configure

This tab provides user the option to configure appliance specific parameters. These are similar to the ones required to be configured while installing the appliance. The user can update the appliance name, change the number of virtual CPUs, set the memory, add/delete HDD and add/delete network interfaces.

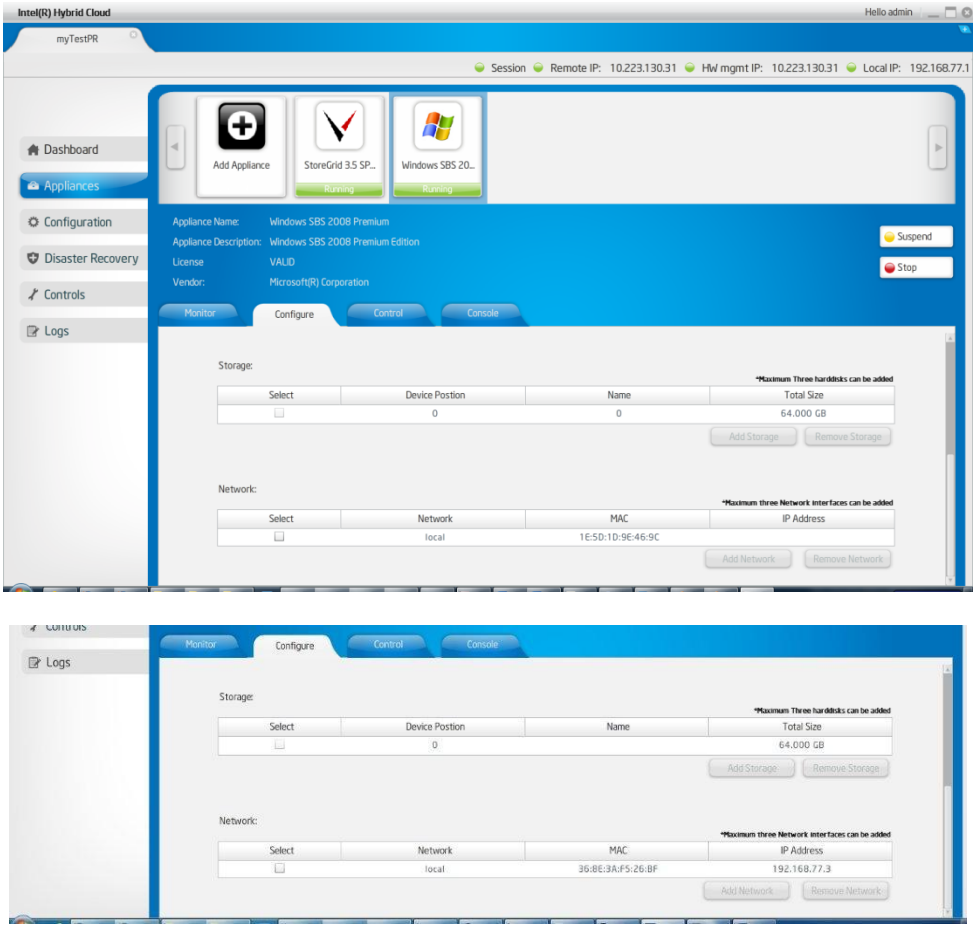

Figure 34. Intel® Hybrid Cloud server manager - Appliances Configure window

Note: User can perform the actions like Add/remove network/hard disk only when the appliance is in stop state.

6.7.3 Appliance Control

The user can take a backup of an appliance from this view onto a USB disk directly connected to server. USB disk should have free space equal or greater than the size of the appliance to be backed up and must be formatted in NTFS format. The backed up appliance can then be restored back from the USB disk at a later time.

To know how to restore appliance go to section 6.8. Along with the backup, any appliances can be deleted from this view. The uninstall button (option) will uninstall the appliances selected.

Figure 35. Intel® Hybrid Cloud server manager -Appliances Control window

6.7.4 Appliance Console

Under this tab, user can launch the VNC console of the selected appliance (only for appliances that are running). User can open only one console per appliance & the same can be closed only from the session that started it.

The Server Manager will display the port it is using for launching the VNC console.

Users have the option of launching VNC console of their choice. To do so, one needs to connect to it using the “Server IP address”:”Port Number” format.

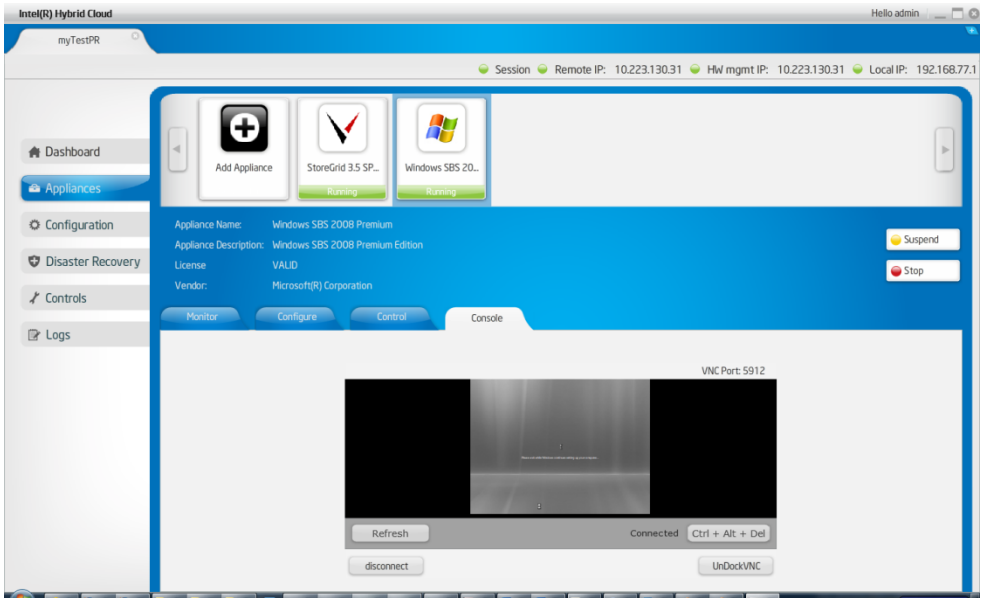

Figure 36. Intel® Hybrid Cloud server manager -Appliances Console Screen

6.8 Appliance 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 appliances 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. 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. Please refer section 6.7.3 to see how to delete an appliance.

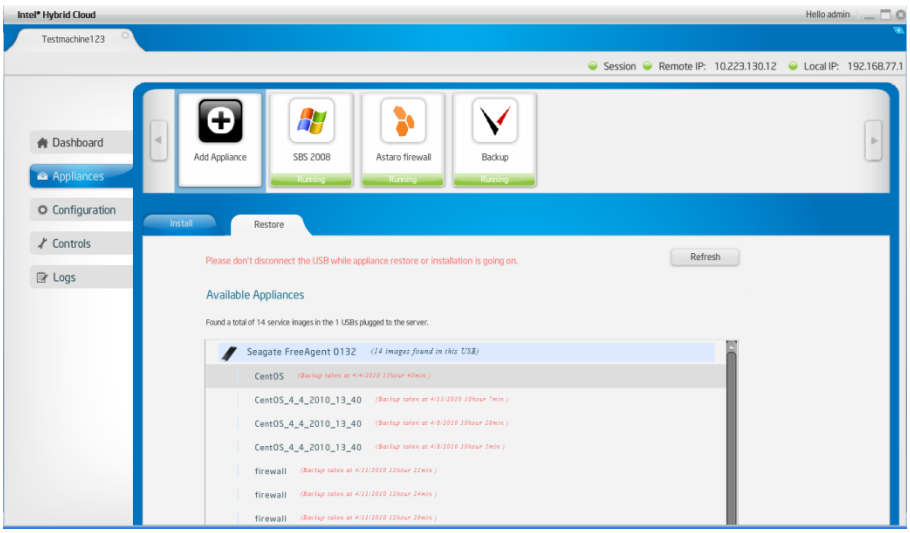

Figure 37. Intel® Hybrid Cloud server manager –Appliances Restore Screen

6.9 Configuring Intel® Hybrid Cloud server

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

6.9.1 Server Details

This tab can be used to configure System name, update time zone and change password. Both system and Intel® AMT password can be changed. Upon successful update of the password, are login screen opens in which user must login again with a new password.

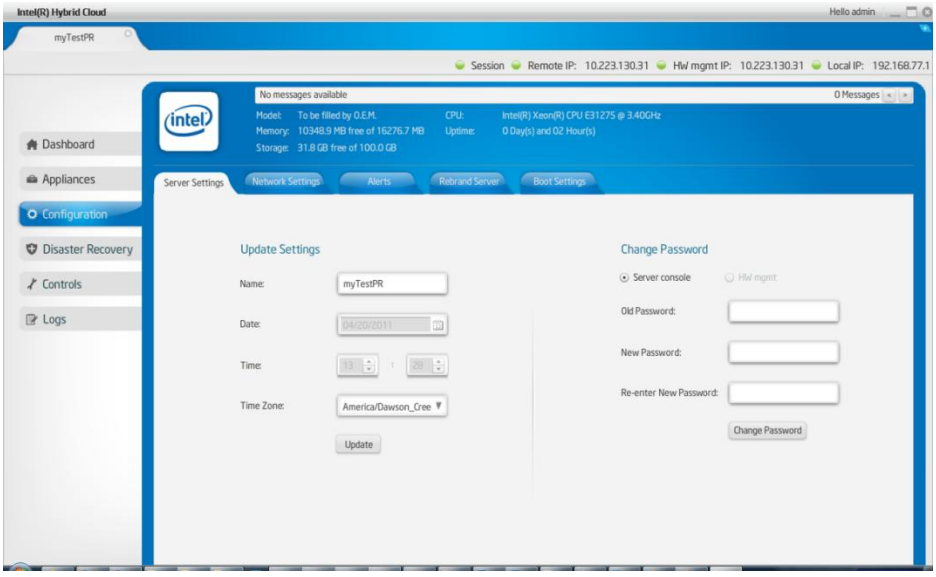

Figure 38. Intel® Hybrid Cloud server manager -Configure Server Settings window

6.9.2 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 shows a warning message before it proceeds.

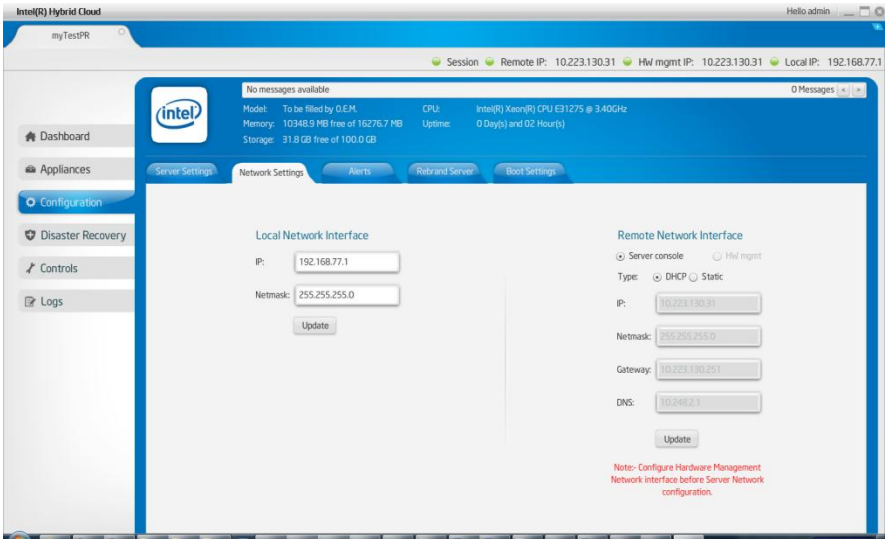

Figure 39. Intel® Hybrid Cloud server manager -Configure Network Settings Screen

6.9.3 Configuring Email Alerts

This tab lets the admin and user to 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. IP address for 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.

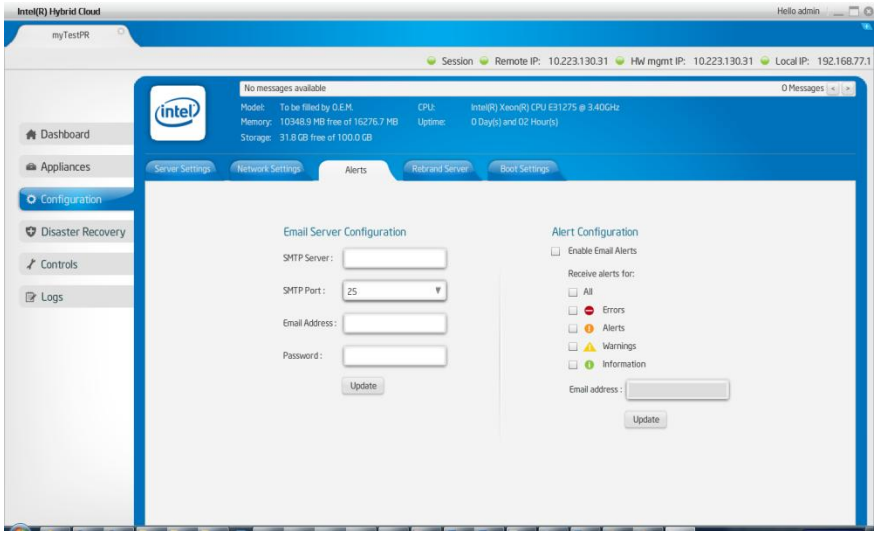

Figure 40. Intel® Hybrid Cloud server manager -Alerts (Email) Configuration window

6.9.4 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.

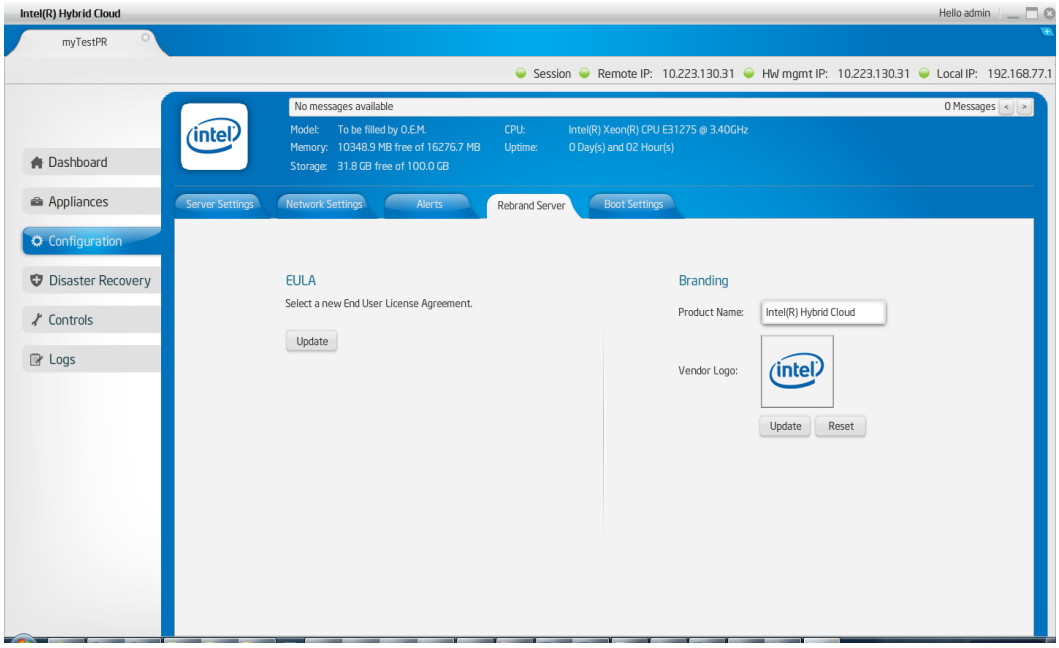

Figure 41. Intel® Hybrid Cloud server manager - Rebrand Server screen

6.9.5 Configure Boot Settings

This tab can be used to change the order in which appliances should automatically boot up post boot. User can do drag and drop to change the order. This order is 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.

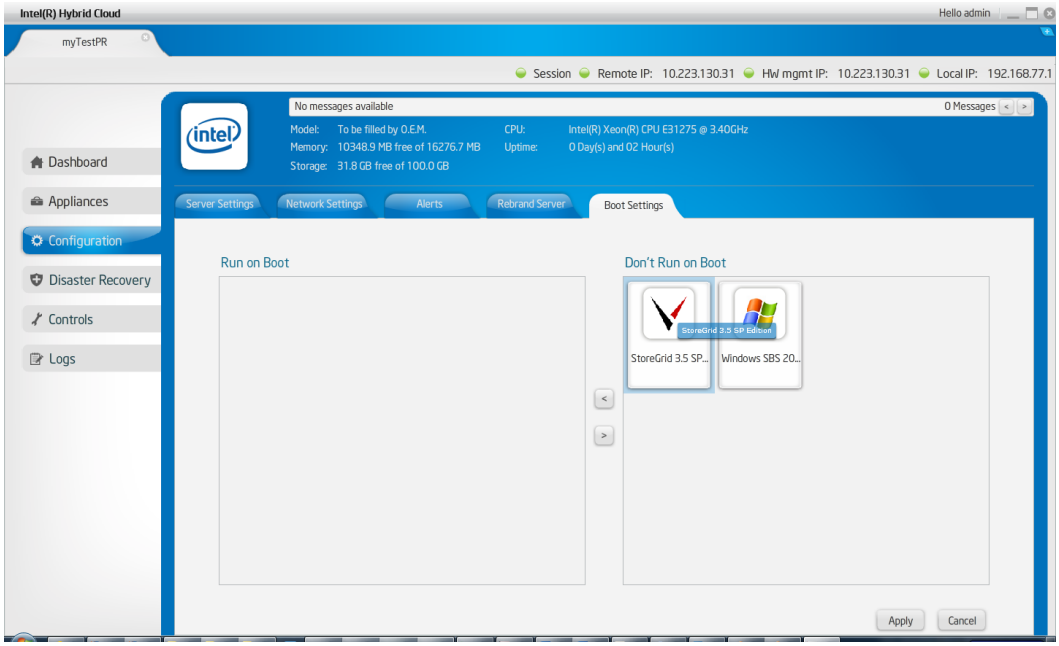

Figure 42. Intel® Hybrid Cloud server manager -Configure Boot Settings window

6.10 Disaster Recovery

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

6.10.1 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 of the primary server and navigate to the Disaster Recovery tab. This view provides a DR Setup option as given in the screenshot below.

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 same network but must be reachable via a router or gateway. Both machines must be on the same LAN.

Additionally, a server should be set to factory defaults prior to being configured as secondary server.

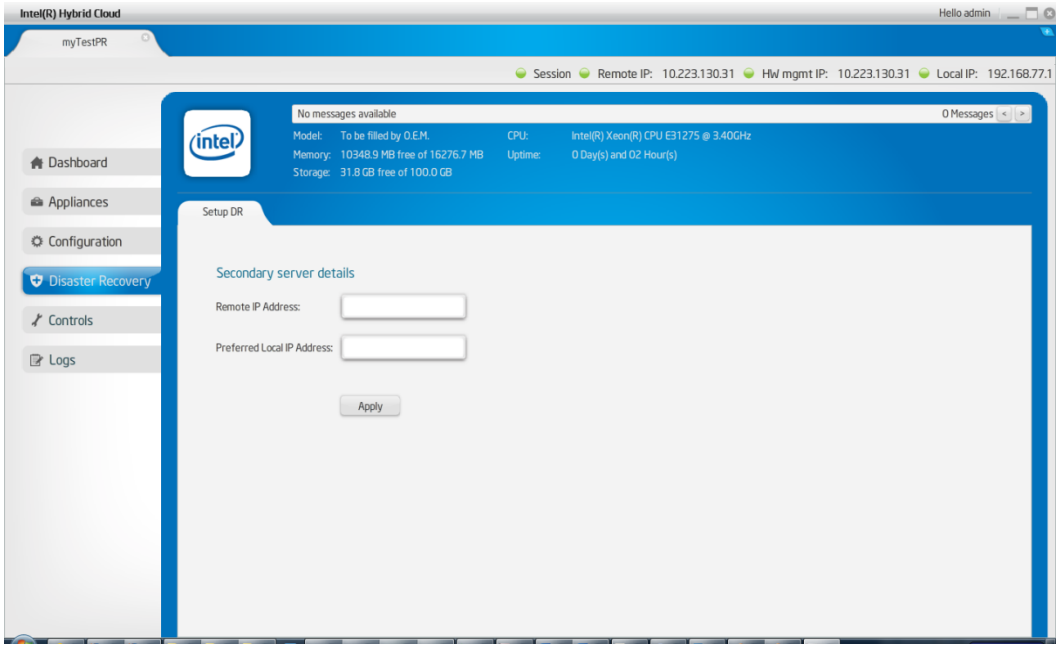

Figure 43. Secondary server details window

Once the details are provided, 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.

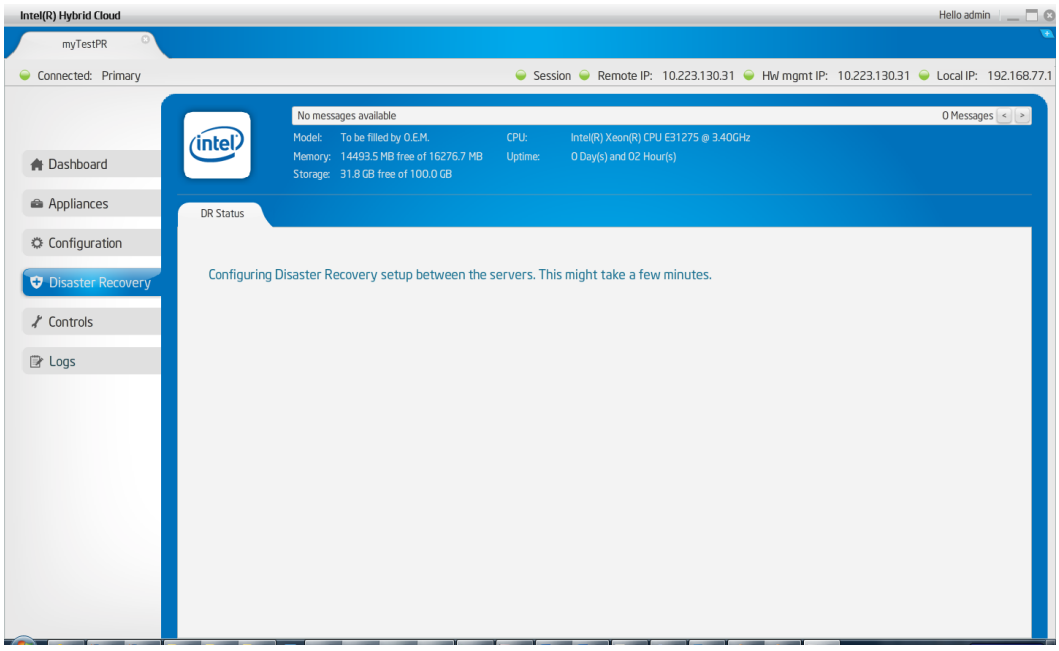

Figure 44. Configuring Disaster Recovery between servers

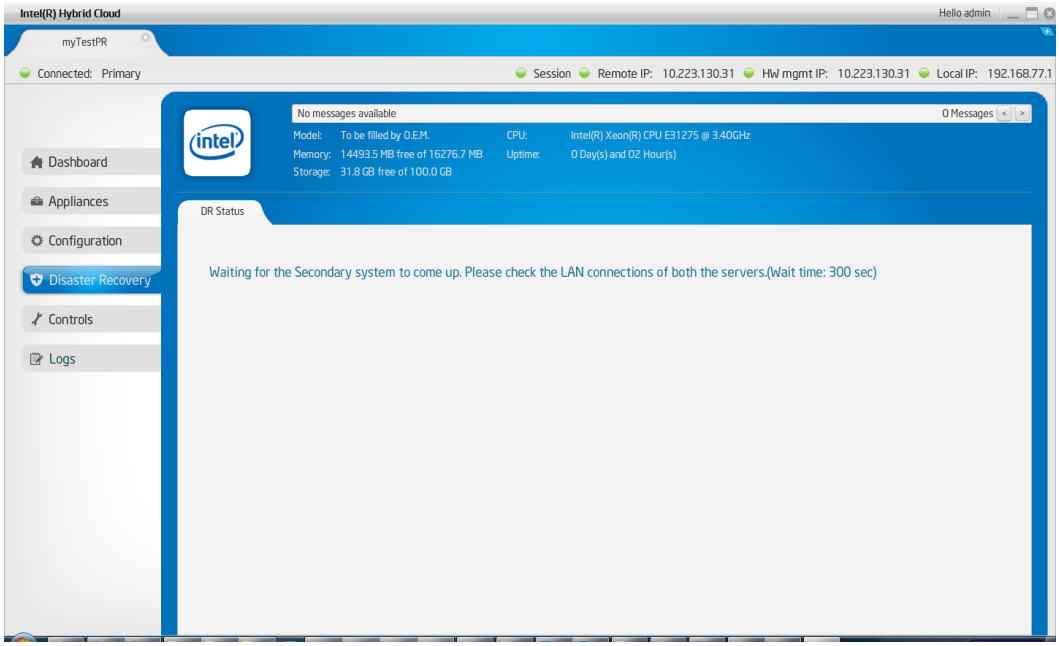

Figure 45. Waiting for Secondary systems to come up

Once the communication between the machines is enabled, 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.

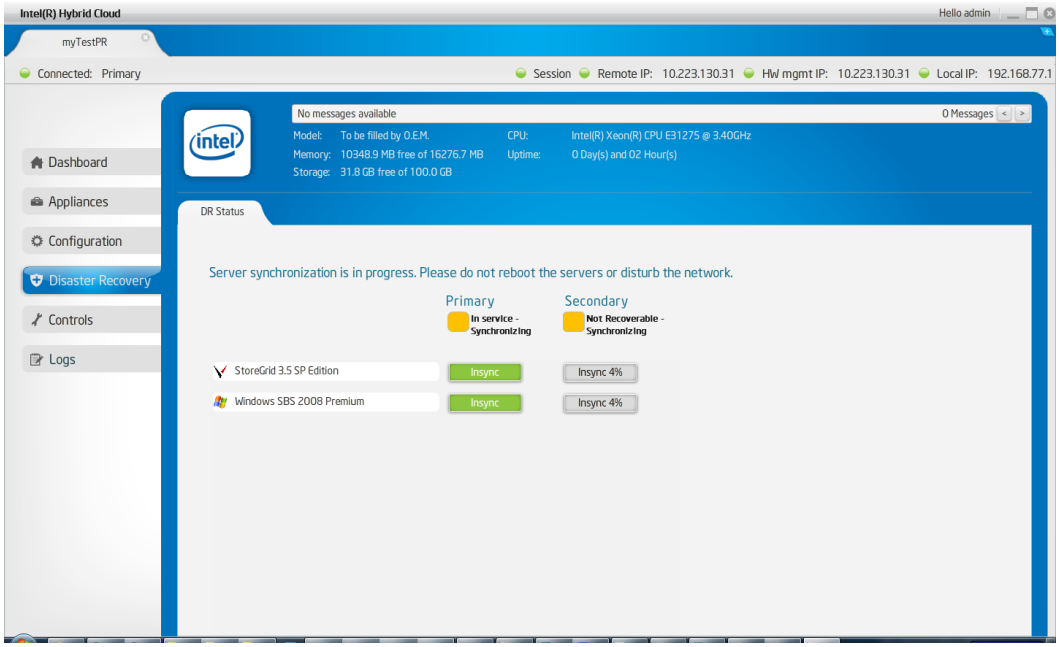

Figure 46. Server synchronization in progress

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.

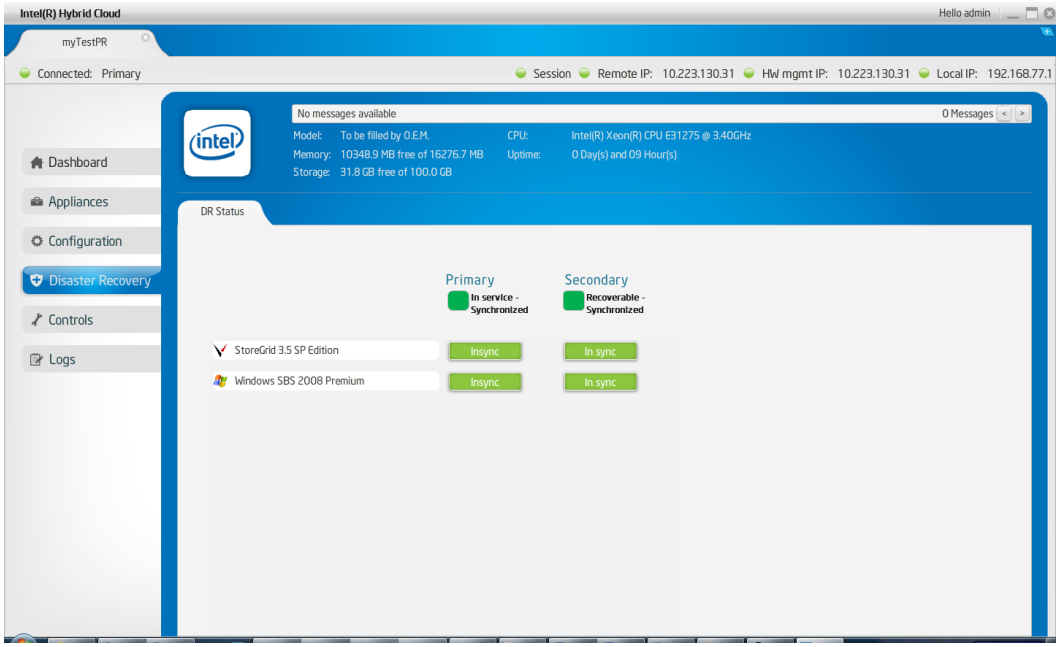

Figure 47. Synchronization complete

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.

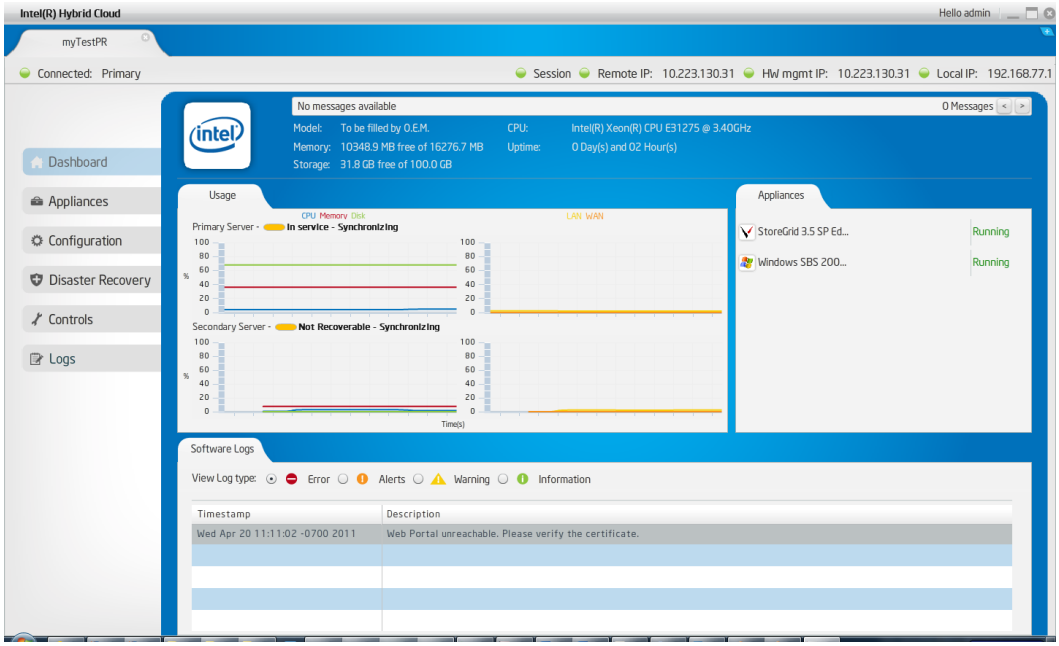

Figure 48. Server Management console displaying the usage of the mirror server

6.10.2 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.

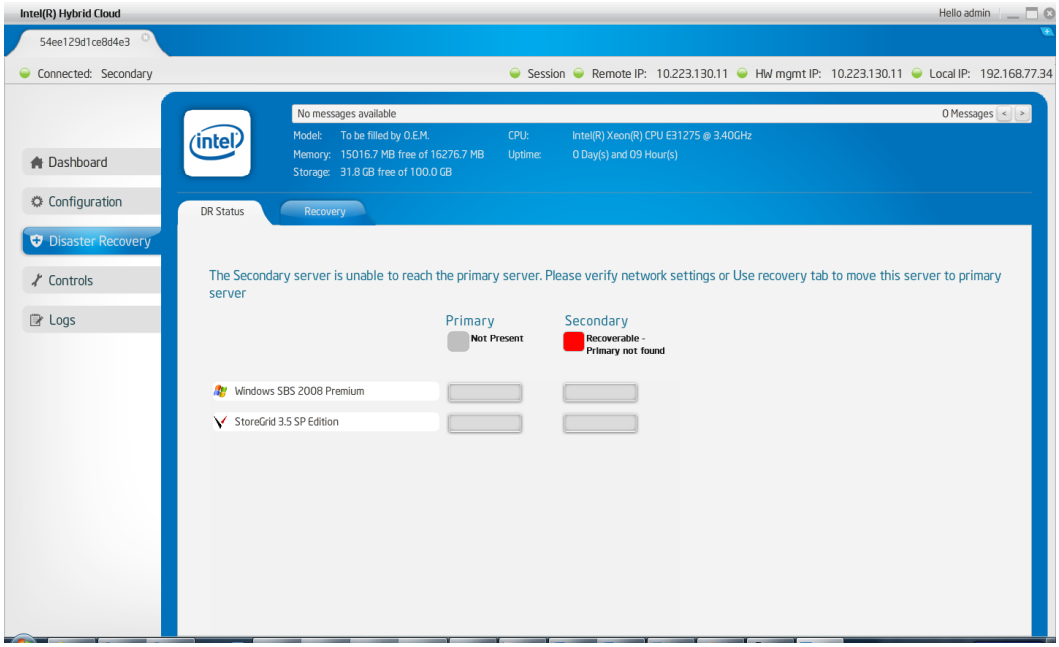

Figure 49. Server status message

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

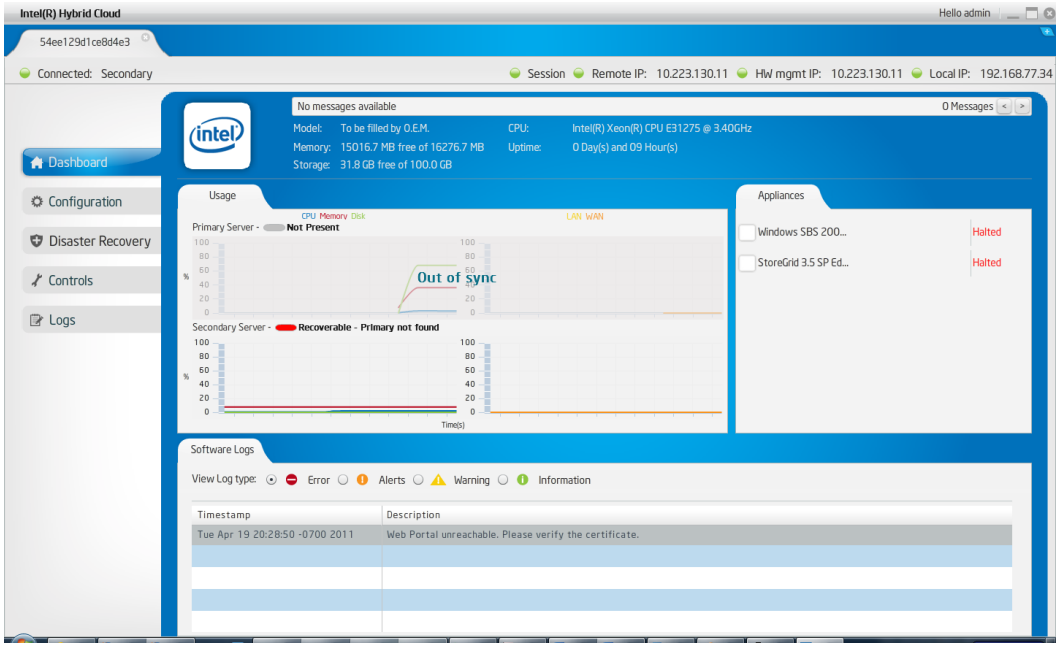

Figure 50. Machine status

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.

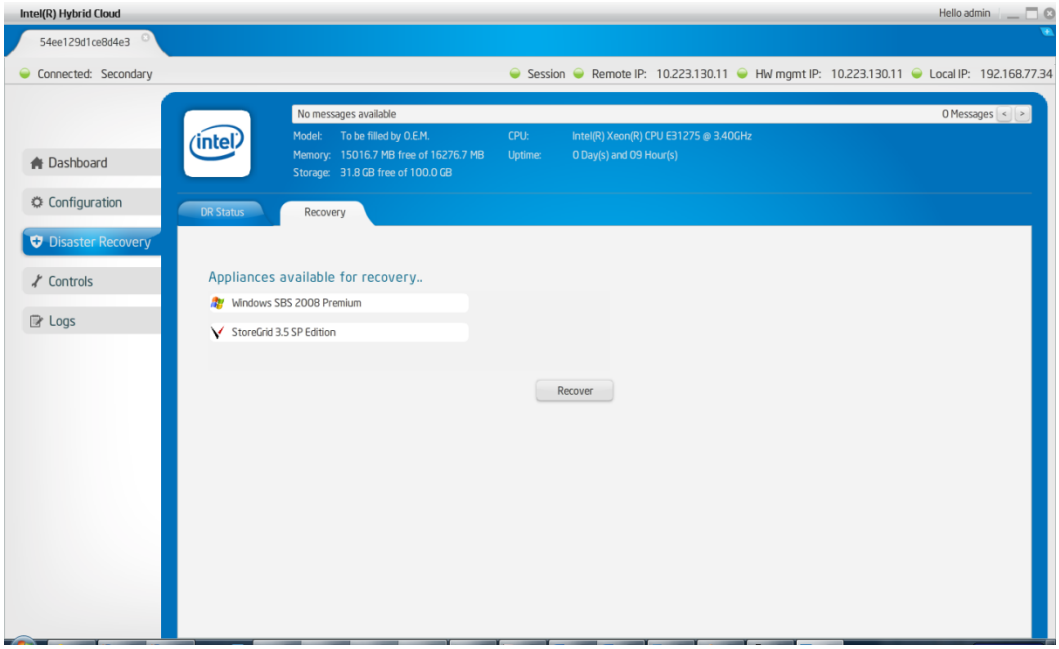

Figure 51. Recovery tab

6.10.3 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.

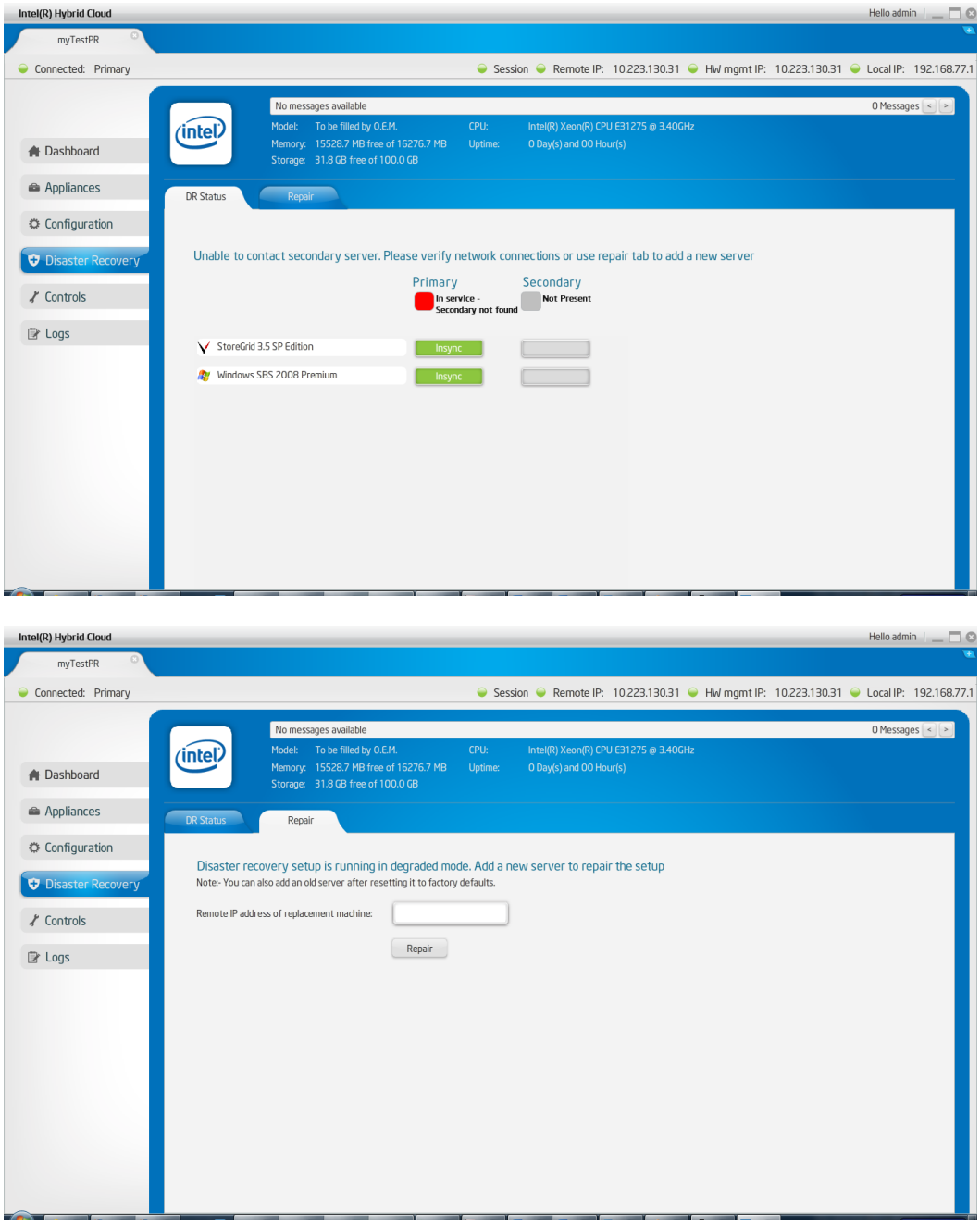

Figure 52. Re-Create the Disaster Recovery Setup

Just like in the first-time DR setup case, 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. Prior to setting up a server as secondary server, the server must be set to factory defaults, if not a new server.

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

6.11 Intel® Hybrid Cloud management controls

Various actions can be taken on the Intel® Hybrid Cloud server manager using this tab like System restart, shutdown. Force restart and shutdown can be done OOB using Intel® AMT. These Intel® AMT commands are available only on admin role. For others, admin can grant permission to user role.

There are four options available for software:

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

Set System Defaults — Resets the Intel® Hybrid Cloud software stack configuration to initial default settings. This sets the user permissions to default permission levels for all the XML-RPC APIs 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 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.

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 network. Post diagnostics, he/she can put these networks 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.

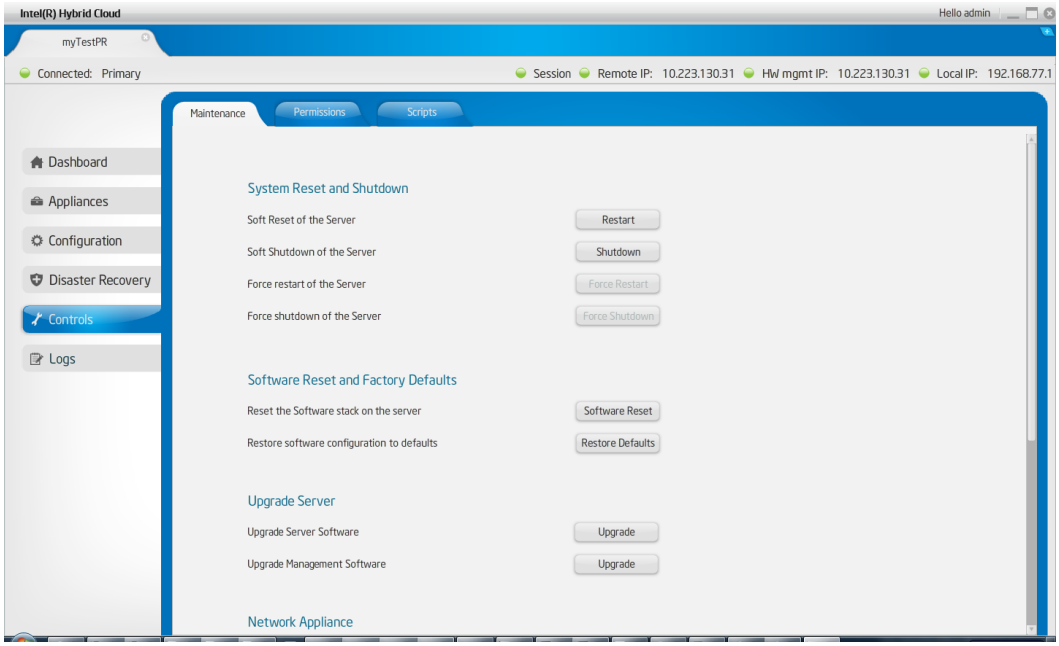

Figure 53. Intel® Hybrid Cloud server manager Control - Maintenance Screen 1

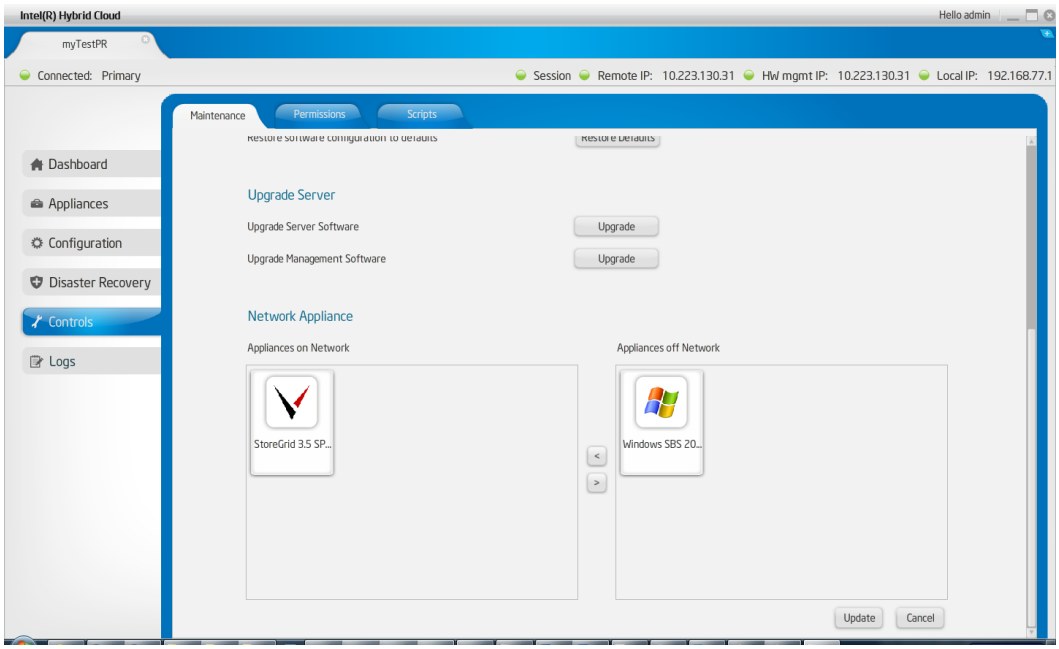

Figure 54. Intel® Hybrid Cloud server manager - Maintenance Screen 2

6.11.1 Permissions

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

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

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.

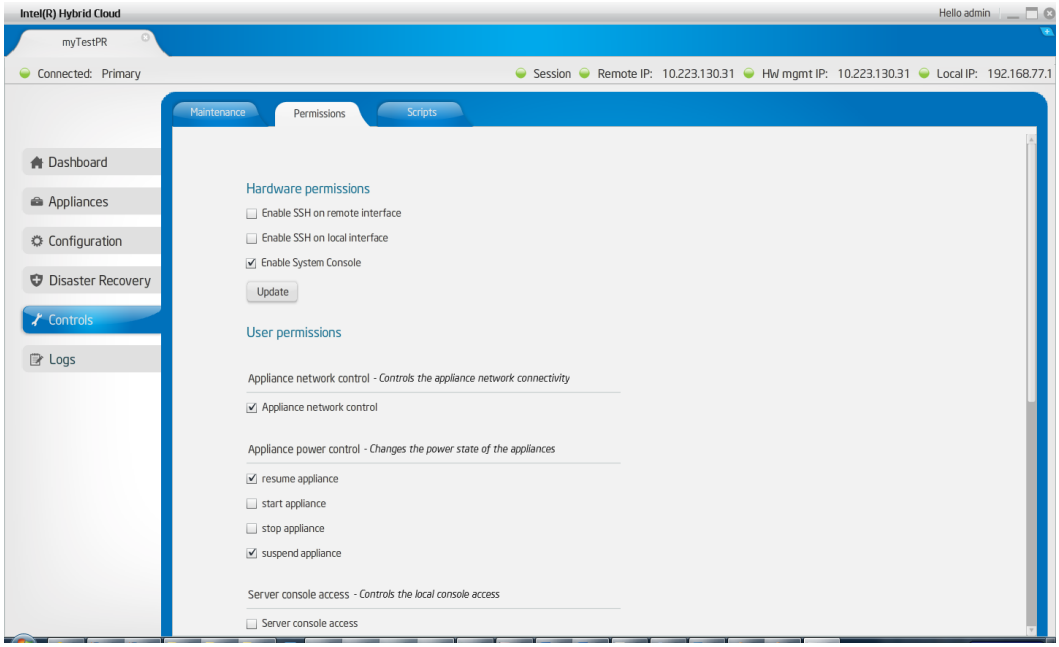

Figure 55. Intel® Hybrid Cloud server manager - Permissions Screen

6.11.2 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. Attaching a USB to an appliance/VM.
2. Detaching a USB from appliance/VM.
3. Deleting ISO attached to appliance/VM.

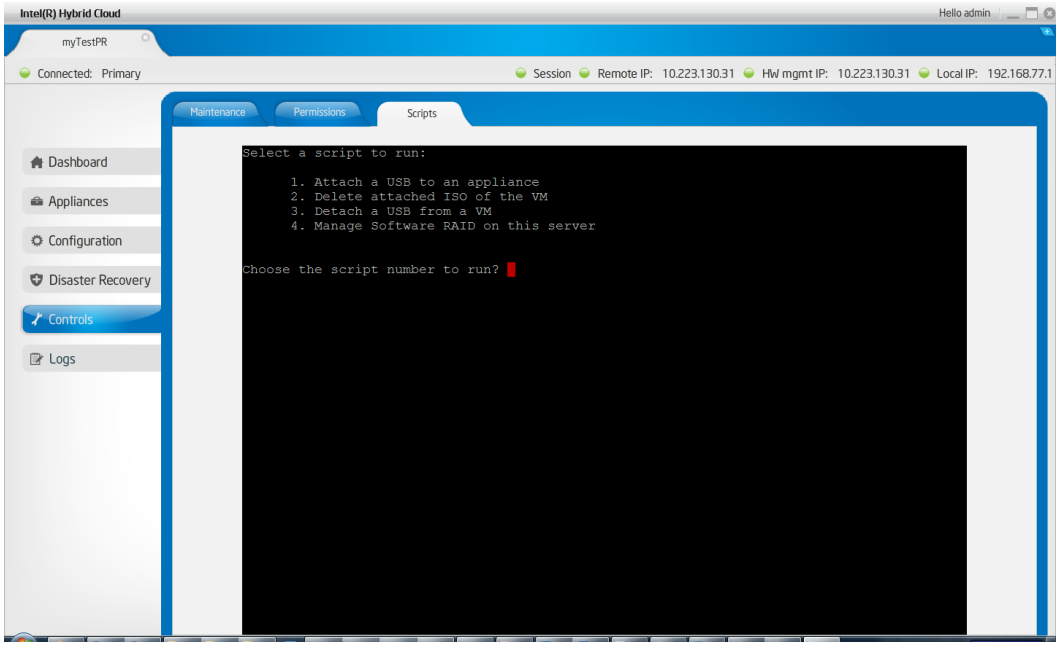

Figure 56. Intel® Hybrid Cloud server manager - Diagnostics (Control > Scripts) window

6.12 Intel® Hybrid Cloud software logs

This tab shows detailed logs on Intel® Hybrid Cloud server. One can choose to see logs in any of these categories: information, warning, alerts, and errors.
There are three types of events:

- 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.

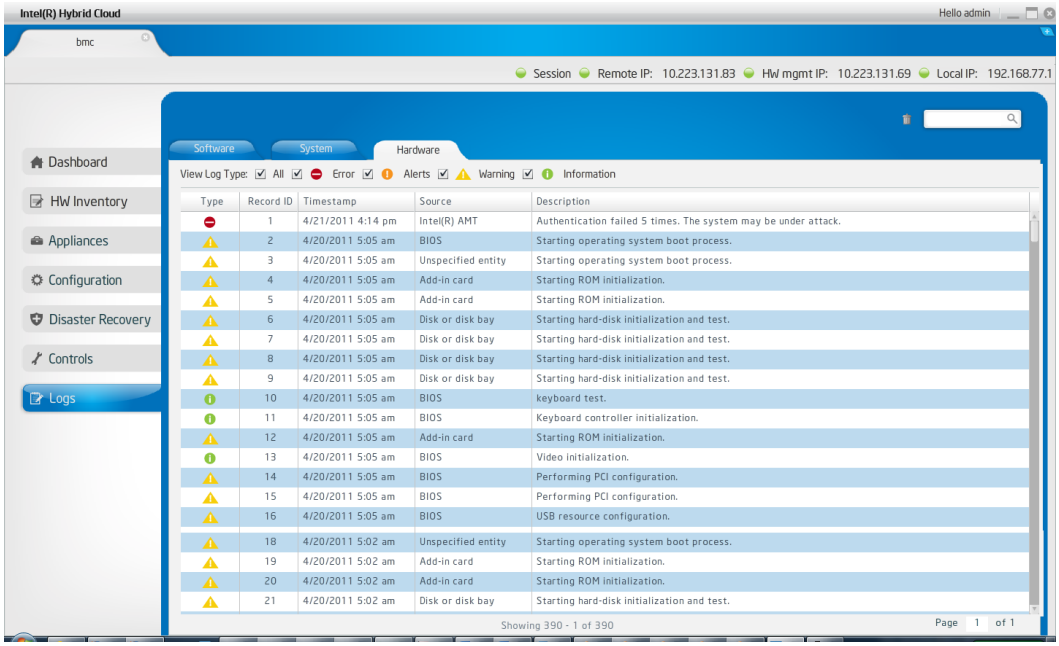

Figure 57. Intel® Hybrid Cloud server manager Logs Screen

6.12.1 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.

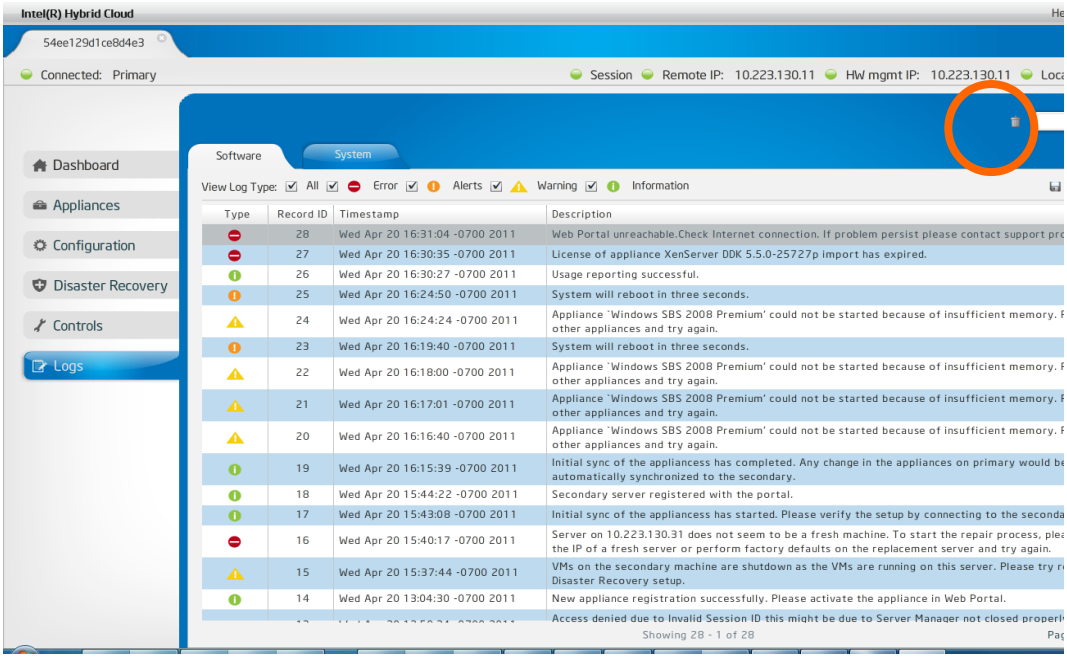

Figure 58. Software and Hardware Logs Deletion

6.12.2 Software Logs Download

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

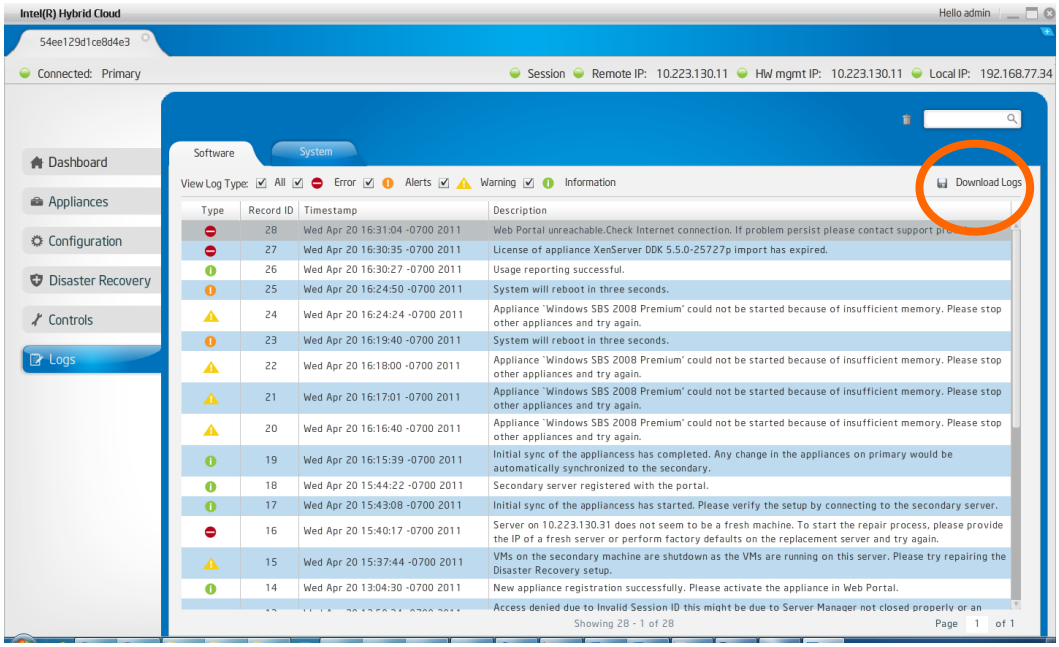

Figure 59. Software Logs Download

6.13 Intel® Hybrid Cloud server manager Multiple Servers Management

The **All Servers** tab of the Intel® Hybrid Cloud server manager lists all the registered and active servers for the connected Remote Administrator. Remote Administrator needs to provide management portal login credentials for this server list to be populated on this page. The **All Servers** window is displayed below.

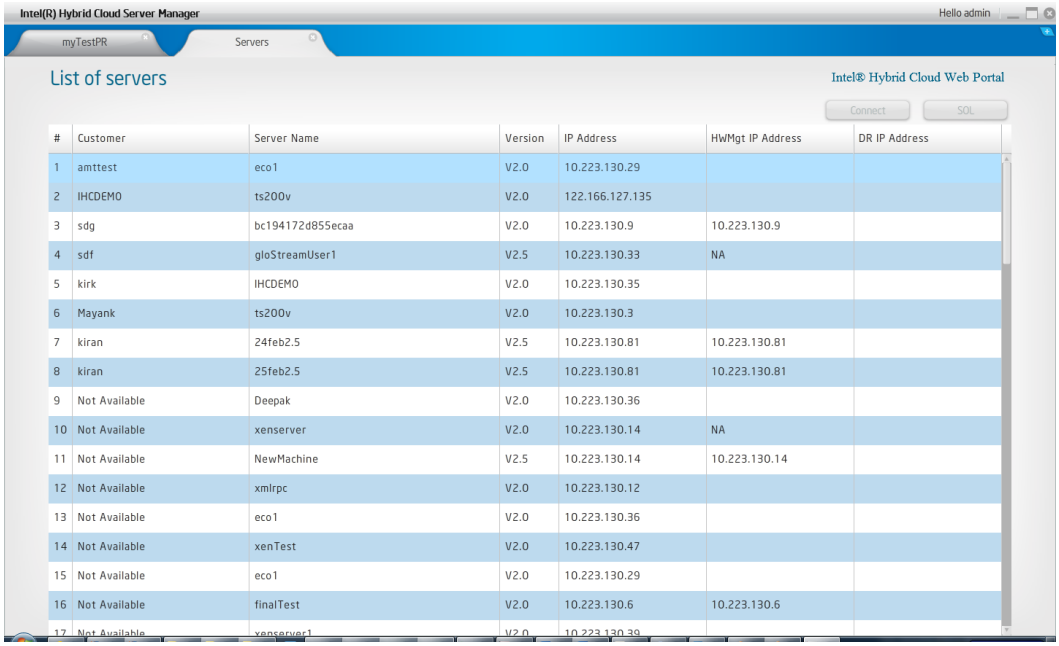

Figure 60. Intel® Hybrid Cloud server manager - All Servers page

Remote Administrator can then connect to any of the servers listed by clicking **Connect** and entering user credentials of the specific server in the **Connect to Server** dialog that appears as follows:

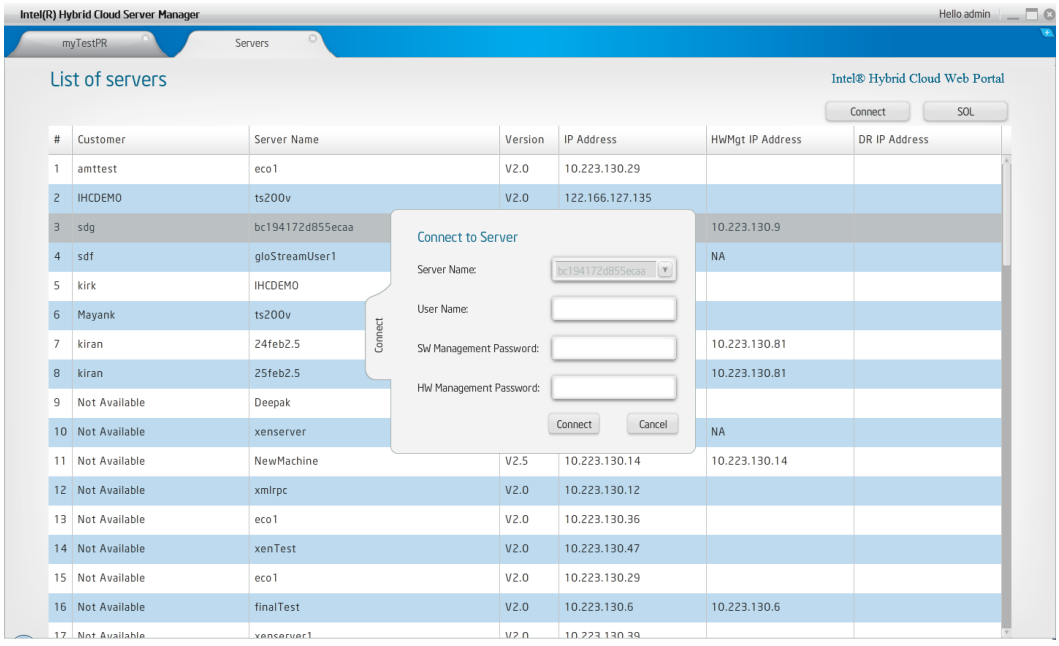

Figure 61. Intel® Hybrid Cloud server manager - All servers → Connect to Server window

A new tab opens within the existing Intel® Hybrid Cloud server manager UI for the specified server.

- 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 need Intel ® AMT login credentials. One can use this for recovering a server remotely via Intel ® AMT.
- If the Configured system is a BMC supported, on clicking SOL RMM3 (Remote management module) we page will open. This allows user to perform all other kvm and out of band other actions
- Click **Remote** on the **All Servers** page to open Intel® AMT password dialog; enter password to open a new tab with Intel ® AMT features like Hardware Inventory, Intel® AMT logs and system force restart/shutdown options. One can use this for restarting server when the server software is not reachable.

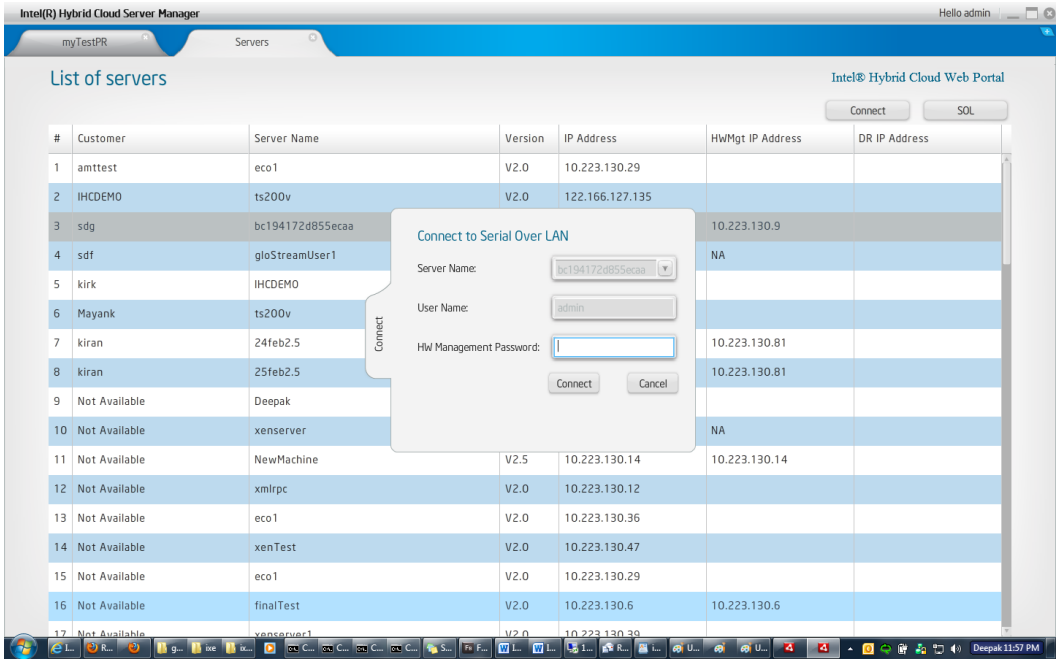

Figure 62. Intel® Hybrid Cloud server manager - All servers → Connect to Server window (via Intel® AMT)

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.

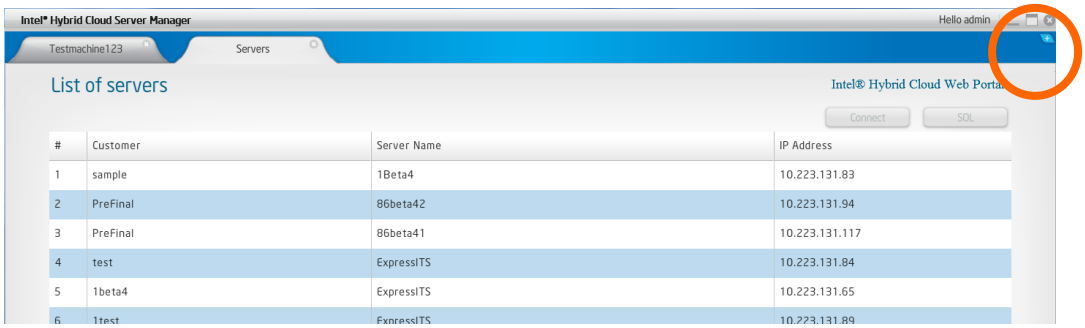

Figure 63. Intel® Hybrid Cloud server manager: Logging Out

7. Saving and Restoring System Configuration

Once the Intel® Hybrid Cloud server is configured, the system configuration can be saved and can be applied back to the same machine in case of Intel® Hybrid Cloud server stack or VMM crash. There is an IXE command to save a particular configuration. The saved software configuration can be applied back through another IXE command later. IXE command to restore software configuration does not require the server to be registered.

Following are the settings that can 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 configuration file can only be restored back to the same server for which it was originally saved after reinstalling the Intel® Hybrid Cloud software stack.

- User can save a specific server configuration to any location and apply the same later instead of applying an auto save configuration. Appliance metadata configuration save is not allowed and that is saved by system automatically as incorrect appliance metadata will result in unstable server state.
  - IXE commands for saving user-specified server configuration:

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

  - IXE commands for restoring user-specified server configuration:

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

The server will reboot after successfully restoring and applying the configuration.

Details of the IXE command are provided in chapter 10.

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.

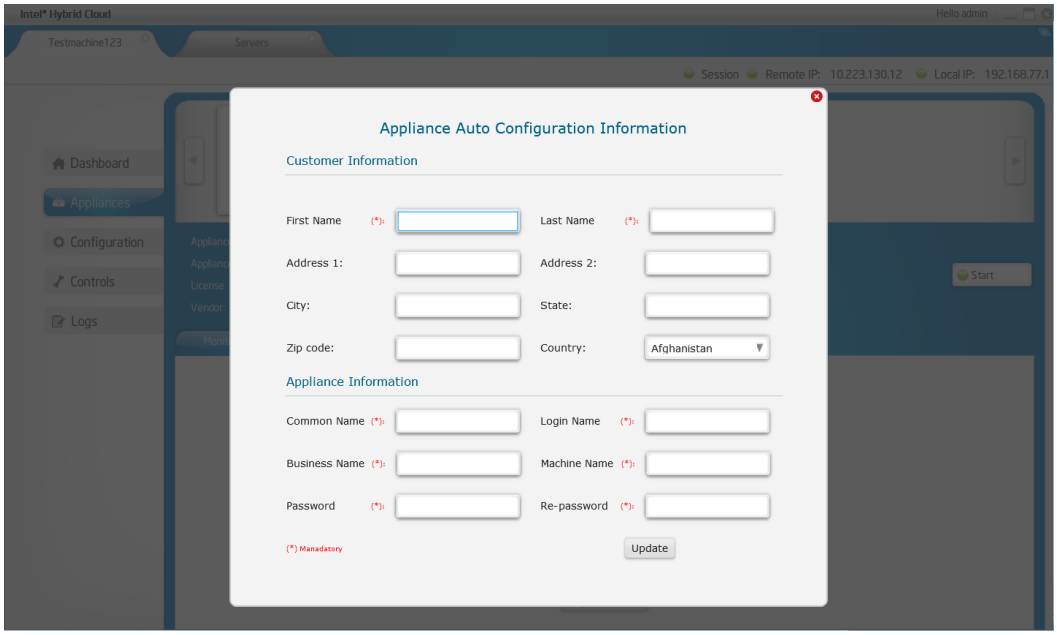

Figure 64. Activating Microsoft Windows* Appliances - Customer Profile page

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 Remote Administrator given information (like login name, password and so on).

8.2 Activating Other Appliances

All other appliances except Windows* appliances need to be simply activated through Intel® Hybrid Cloud management portal by remote administrator. If needed, a license is downloaded by Server manager from the management portal. License mechanism varies depending on the type of an 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 ® Hybrid Cloud server BMC Configuration

This section is applicable only for Intel® Hybrid Cloud servers that are BMC based and not applicable to those which are AMT-based.

A baseboard management controller (BMC) is a specialized service processor that monitors the physical state of a computer, network server or other hardware device using sensors and communicates with the system administrator through an independent connection. It provides remote management capability similar to Intel® AMT technology.

To access the hardware information via the BMC, please use the Intel® Hybrid Cloud server manager Configuration → Network Settings tab to change BMC IP ("HW mgmt") address from the default of "0.0.0.0" to the appropriate value. Both BMC ("HW mgmt") IP address and software stack ("Server console") IP address must be different. (**Configure → Network Settings → Hardware Mgmt → IP address**). Also, the BMC password needs to be configured using Change Password feature (**Configure → Server Settings → Hardware Mgmt → Change Password**)

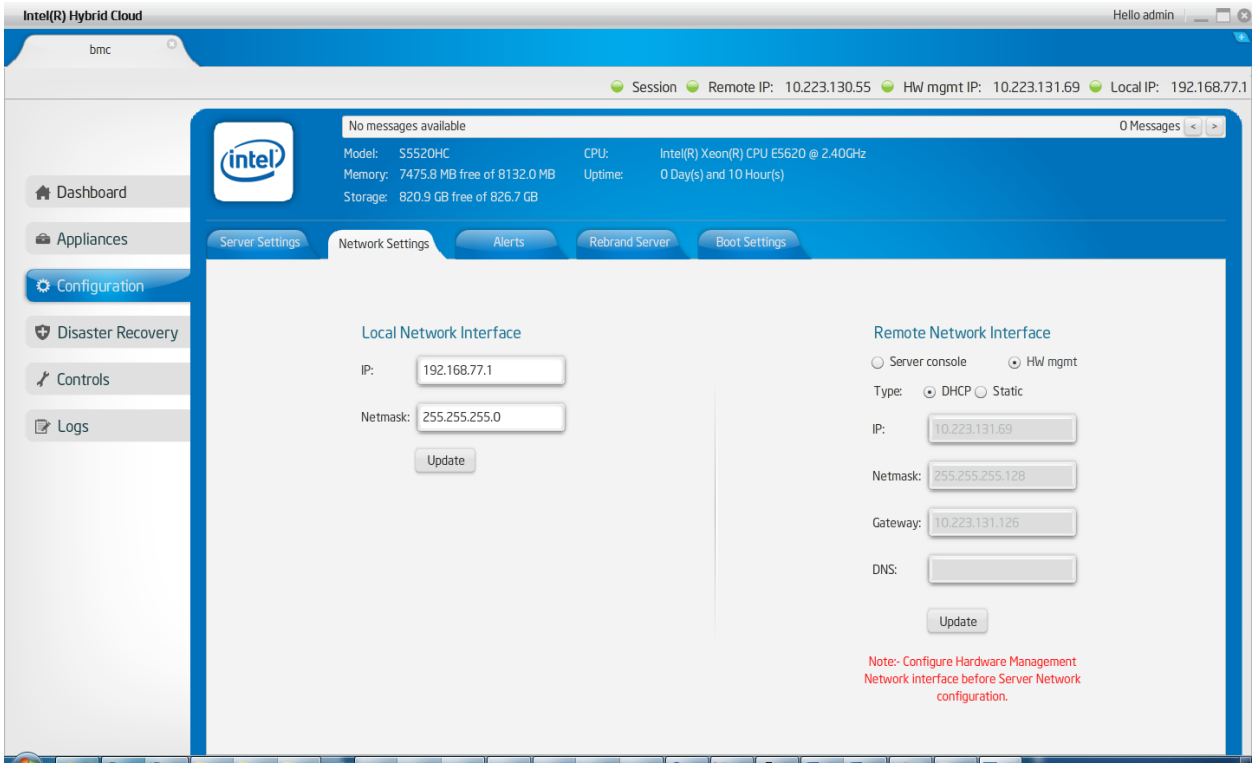

Figure 65. Intel® Hybrid Cloud server manager -- Configuration Page: Hardware Management Network Settings

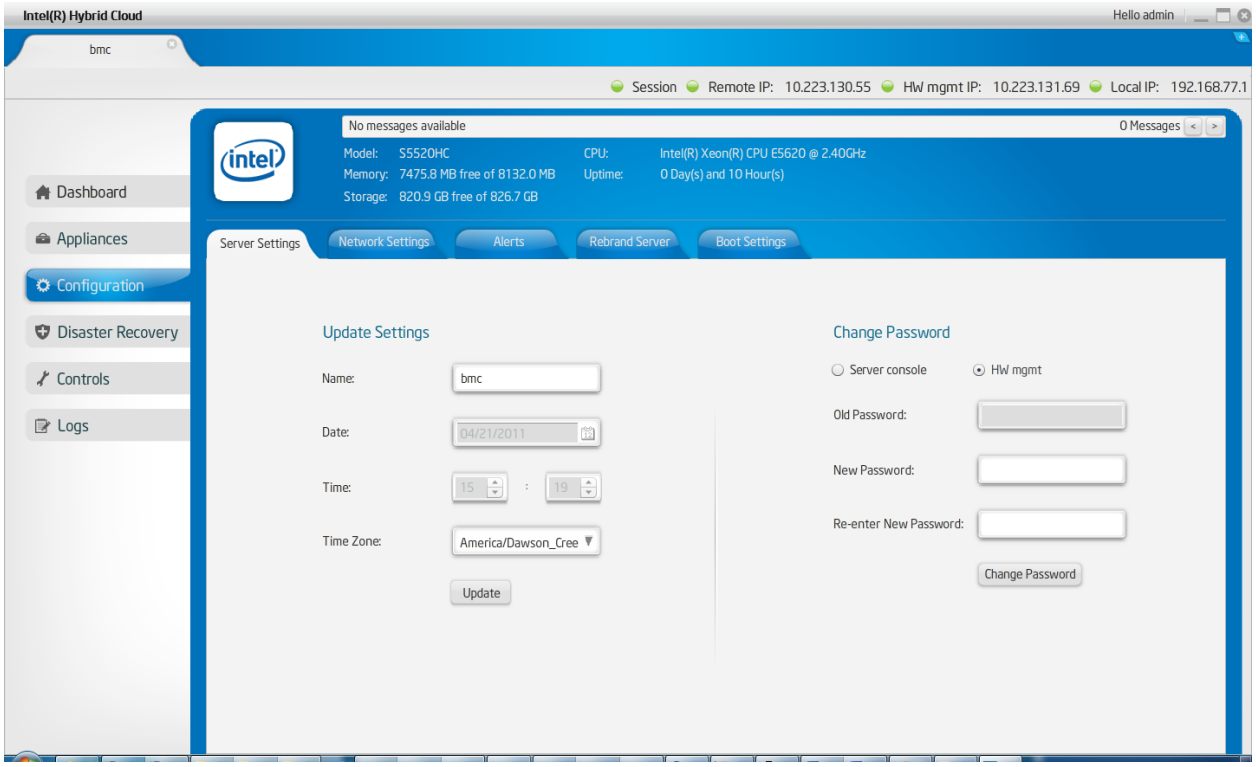

Figure 66. Intel® Hybrid Cloud server manager -- Configuration Page: Hardware Management password set

Note: After configuring the BMC, the user has to disconnect and connect to the server again with Hardware management credentials to access Hardware related information from the BMC.

.

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

Intel® Hybrid Cloud server can also be managed using `ixe` command line tool. The tool is a one-operation-at-a-time type 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.

10.1 IXE command Line Format

A number of operations are supported by `ixe`, and the syntax of each operation can be found 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>**

10.2 List of IXE Commands

Below in each table, all the supported Intel® Hybrid Cloud commands are explained. The error codes are explained at the end of this section separately.

For each command Description, Result, Supported User (Admin means Remote Administrator) and appropriate Examples are given. The result portion of each command shows the example on how the result may look like after executing the command. The result or output in your system may not be the same.

Command: `get-number-of-appliances`

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

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	ixe –h <*server ip*> –u <*user name*> –p <*password*> –o *get-installed-appliances*
Result	Appliance1 : 75d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: `get-appliance-power-state`

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

Command: `start-appliance`

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

Command: `stop-appliance`

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

Command: `change-password`

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

Command: `install-appliance-license`

Required Parameter	<Appliance license file Location >
Supported User	{ 'admin'}
Description	Install the license for the requested appliance. [Note :- File location both relative/absolute]
Usage	ixe –h <*server ip*> –u <*user name*> –p <*password*> –o *install-appliance-license <license file path>*
Result	Command successful

Command: `is-appliance-license-valid`

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

Command: `revoke-appliance-license`

Required Parameter	<Appliance Name>
Supported User	{ 'admin'}
Description	Uninstall (revoke) the license of the requested appliance
Usage	ixe –h <*server ip*> –u *admin* -p <password>–o *revoke-appliance-license* <Appliance Name>
Result	Command successful

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
Supported User	{'user', 'admin'}
Description	returns all logs for the requested level
Usage	ixe –h <*server ip*> –u <*user name*> -p <password>–o *get-event-log 1*
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: `delete-event-log`

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

Command: `system-reset`

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

Command: `system-poweroff`

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

Command: `software-reset`

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

Command: `update-system-name-label`

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

Command: `set-appliance-boot-order`

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

Command: `get-system-parameters`

Required Parameter	null
Supported User	{'user', 'admin'}
Description	Returns the system parameters
Example	ixe –h <*server ip*>-u <user name>-p <password> –o *get-system-parameters*
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-usage`

Required Parameter	null
Supported User	{'user', 'admin'}
Description	returns the system usage like wan, lan , cpu etc
Usage	ixe –h <*server ip*> -u <user name> -p <password> –o *get-system-usage*
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-network-parameters`

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

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)
Supported User	{'user', 'admin'}
Description	returns the network parameters for the requested interface
Usage	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]
Result	Command successful

Command: `get-appliance-boot-order`

Required Parameter	null
Supported User	{'user', 'admin'}
Description	Appliances name and the UUID are returned in the order they are set to boot
Example	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-activation-license-all`

Required Parameter	null
Supported User	{'admin'}
Description	Returns the activation license file for all the appliances installed on the Little Mountain server
Usage	ixe –h <*server ip*>-u <user name>-p <password> –o *get-appliance-activation-license-al*
Result	Appliance1-4abeacc3deeefa58620cc734607486ab.lic Appliance2-5aaec7eedefa47381ee734601234ab.lic

Command: `get-appliance-parameters`

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

Command: `get-appliance-usage`

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

Command: `detach-appliances-from-network`

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

Command: `attach-appliances-to-network`

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

Command: `get-network-detached-appliances`

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

Command: `block-remote-login`

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

Command: `allow-remote-login`

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

Command: `get-network-policy`

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

Command: `set-console-enable`

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

Command: `set-console-disable`

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

Command: `get-console-status`

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

Command: `suspend-appliance`

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

Command: `resume-appliance`

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

Command: `get-system-brand-info`

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

Command: `set-system-product-name`

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

Command: `set-system-client-name`

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

Command: `set-system-logo`

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

Command: `get-appliance-brand-info`

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

Command: `get-appliance-brand-info`

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

Command: `set-appliance-vendor-name`

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

Command: `set-appliance-client-name`

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

Command: `set-appliance-logo`

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

Command: `execute-xen-command`

Required Parameter	<xen command to be executed>
Supported User	{'admin'}
Description	Executes the requested XE command on the server and returns the value
Usage	ixe –h <*server ip*> -u <user name> -p <password> –o *execute-xen-command* <xen command to be executed>
Result	The requested xen command result

Command: `update-eula`

Required Parameter	<license file>
Supported user	{'admin' }
Description	Updates the eula on the Little Mountain System.
Usage	ixe –h <*server ip*> -u <user name> -p <password> –o *update-eula* <license file>
Result	Command successful

Command: `set-system-defaults`

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

Command: `upgrade-system-software`

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

Command : `upgrade-management-software`

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

Command: `get-system-timezones`

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

Command: `update-system-timezone`

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

Command: `get-system-time`

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

Command: `update-system-time`

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

Command: `get-command-permissions`

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

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

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

Command: `connect-appliance-console`

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

Command: `get-system-asset-tag`

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

Command: `install-system-license`

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

Command: `get-system-event-log`

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

Command: `configure-email-alerts`

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

Command : `configure-server-email-alerts`

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

Command: `get-email-alert-parameters`

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

Command: `delete-appliance-store-url`

Required Parameters	null
Supported user	{'admin'}
Description	Deletes the configured local ftp appliance store URL.
Usage	*ixe -h <server ip> -u <username> -p <password> -o delete-appliance-store-url*
Result	Command successful

Command: `update-appliance-store-url`

Required Parameters	null
Supported user	{'admin'}
Description	Updates the local ftp store URL.
Usage	*ixe -h <server ip> -u <username> -p <password> -o update-appliance-store-url* 10.223.130.10
Result	Command successful

Command: `destroy-appliacen-hdd`

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

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

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

Command: `delete-appliance-network-interface`

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

Command: `create-appliance-network-interface`

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

Command: `change-appliance-memory`

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

Command: `update-appliance-name`

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

Command: `set-appliance-cpu-number`

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

Command: `get-appliance-download-percentage`

Required Parameters	null
Supported user	{'user','admin'}
Description	*Returns the percentage of the appliance installation process*
Usage	*ixe -h <server ip> -u <username> -p <password> -o* get-appliance-download-percentage
Result	*NA(if no appliance is getting installed)| 29%(percentage of the appliance getting installed)*

Command: `start-appliance-backup`

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

Command: `appliance-backup-status`

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

Command: `appliance-uninstall`

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

Command: `set-oem-factory-defaults`

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

Command: `upgrade-host-server`

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

Command: `save-restore-configuration`

Required Parameters	<Path to Store the restore configuration file>
Supported user	{'user','admin'}
Description	Retrieves the current system configuration. This can be used by the
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o save-restore-configuration
Result	File Name of the system configuration

Command: `get-internet-ip-address`

Required Parameters	<>
Supported user	{'user','admin'}
Description	displays the internet accessable ip address which can be used to connect to the server.
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o get-internet-ip-address
Result	Internet accessible IP Address

Command: `change-default-password`

Required Parameters	<NewPassword>
Supported user	{'user','admin'}
Description	Resets the system password to new password this is a mandatory step before connecting to stack.
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o change-default-password <NewPassword>
Result	Command successful

Command: `get-alert-messages`

Required Parameters	< >
Supported user	{'user','admin'}
Description	This command provides the messages related to box and appliances.
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o get-alert-messages
Result	Returns the Stack messages for the User and MSP

Command: `get-system-serial-id`

Required Parameters	< >
Supported user	{'user','admin'}
Description	This command retrieves the unique serial number of the box.
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o get-system-serial-id
Result	Returns the system unique serial id

Command: `apply-restore-configuration`

Required Parameters	<system> | [<user> <restore file>]
Supported user	{'user','admin'}
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o apply-restore-configuration <system> | [<user> <restore file>]
Description	restore the system to old configurations.
Result	Command successful. (Restores the system to original configurations.)

Command: `apply-vm-metadata`

Required Parameters	<>
Supported user	{'user','admin'}
Description	apply the appliance metadata to the server host
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o apply-vm-metadata
Result	Command successful. (Restores the appliance metadata)

Command: `update-ntp-servers`

Required Parameters	<ntp server 1>[server2]… {max 3 serves}
Supported user	{'admin'}
Description	apply new ntp settings
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o update-ntp-server <ntp server IP>
Result	Command successful.

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

Required Parameters	<APP ID> <Vendor name> <vendor Logo>
Supported user	{'admin'}
Description	Updates the appliance brand information in the stack
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o set-appliance-default-brand-info <APP ID> <Vendor name> <vendor Logo>
Result	Command successful.

Command: `update-active-aeon-md5sum`

Required Parameters	< new active aeon md5sum>
Supported user	{'admin'}
Description	Updates active aeon md5sum for usage reporting
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o update-active-aeon-md5sum <active Aeon Md5sum>
Result	Command successful.

Command: `upload-system-scripts`

Required Parameters	<script location>
Supported user	{'admin'}
Description	Uploads script to script tabs to help user in diagnostics
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o upload-system-scripts <script>
Result	Command successful.

Command: `update-appliance-unattend-template`

Required Parameters	<unattended template>
Supported user	{'admin'}
Description	Uploads template for unattended installation.
Usage	ixe -h 192.168.1.1 -u <username> -p <password> -o update-appliance-unattend-template <unattended template>
Result	Command successful.

10.3 IXE AMT Commands

Command: `force-system-poweroff`

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

Command: `force-system-reset`

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

Command: `hw-system-information`

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

Command: `hw-processor-information`

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

Command: `hw-memory-information`

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

Command: `hw-disk-information`

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

Command: `hw-event-log`

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

Command: `force-system-poweron`

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

Command: `change-hw-management-password`

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

Command: `get-hw-network-parameters`

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

Command: `configure-hw-network-parameters`

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

Command: `get-hw-system-power-state`

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

10.4 IXE Error Messages

All the IXE commands explained in the previous section will return error messages in case there is a failure. A brief description of some of the error messages are provided here. For more information, please refer to the support site at: http://www.intel.com/p/en_US/support/highlights/server/hcserver.

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

Glossary

Word/Acronym	Definition
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® RMM3	Intel® Remote Management Module 3
IPMI	Intelligent Platform Management Interface
ITE	Information Technology Equipment
KVM	Keyboard, video and mouse
MAC	Media Access Controller
OOB	Out-Of-Band- No operating system interaction on Server
PBDE	Polybrominated Biphenyls Diphenyl Ethers
RMII	Reduced Media Independent Interface
RTC	Real-Time Clock
TCP/IP	Transmission Control Protocol/Internet Protocol
TPS	Technical Product Specification
UART	Universal asynchronous receiver transmitter
UDP	User Datagram Protocol