

RSA

RSA NETWITNESS[®] PLATFORM

iDRAC

Configuration and Maintenance



iDRAC Configuration and Maintenance

Table of Contents

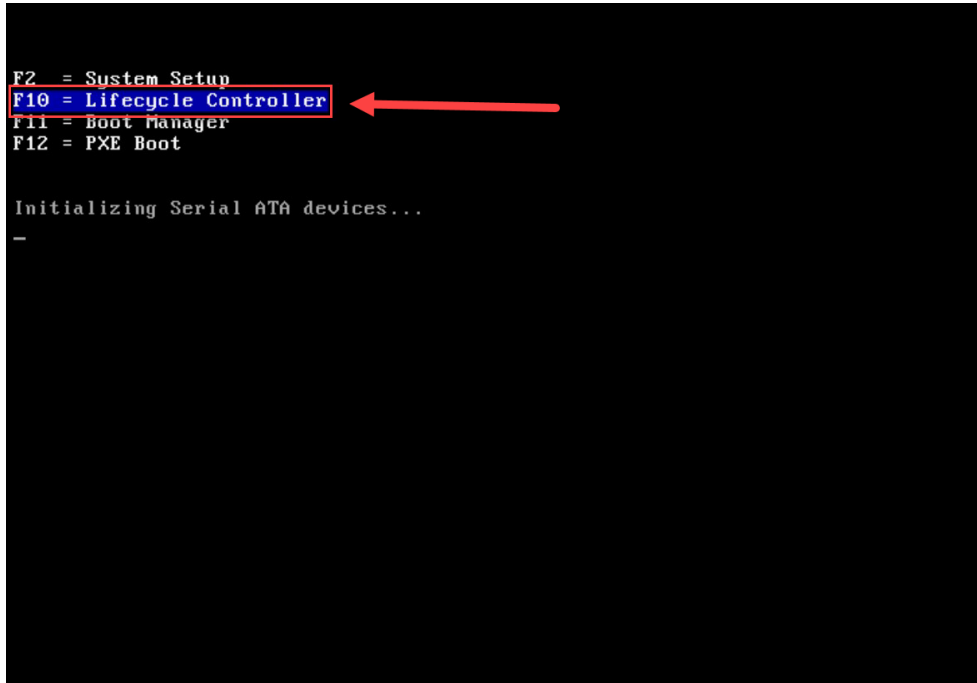
Setting IP Address First Time	2
<i>Console via Crash Cart</i>	<i>2</i>
Configuring iDRAC Settings Using Web UI.....	8
<i>Logging in to Web UI.....</i>	<i>8</i>
<i>Changing User Password</i>	<i>9</i>
<i>Changing IP V4 Settings</i>	<i>11</i>
<i>Setting iDRAC Name.....</i>	<i>13</i>
<i>Changing Browser Tab Name.....</i>	<i>14</i>
<i>Changing Time Zone.....</i>	<i>16</i>
<i>Enabling NTP.....</i>	<i>17</i>
Maintenance	18
<i>Checking iDRAC Firmware and System BIOS Versions</i>	<i>18</i>
<i>Checking iDRAC RAID Firmware Version</i>	<i>19</i>
<i>Updating Firmware/BIOS.....</i>	<i>20</i>
Locating Powervault Serial Number	25
SSL Certificate for Web UI.....	26
<i>Creating CSR.....</i>	<i>26</i>
<i>Uploading Certificate</i>	<i>28</i>
Configuring iDRAC Settings Using IPMITool	31
<i>Prerequisite</i>	<i>31</i>
<i>User Management</i>	<i>31</i>
Listing User Accounts.....	31
Changing Username.....	32
Changing User Password.....	32
Enable User Account.....	32
Disable User Account.....	33
Test User Credentials.....	33
List Available Commands for User Management.....	33
<i>Network Configuration Management.....</i>	<i>34</i>
Listing IP Address	34
Changing IP Address.....	35

iDRAC Configuration and Maintenance

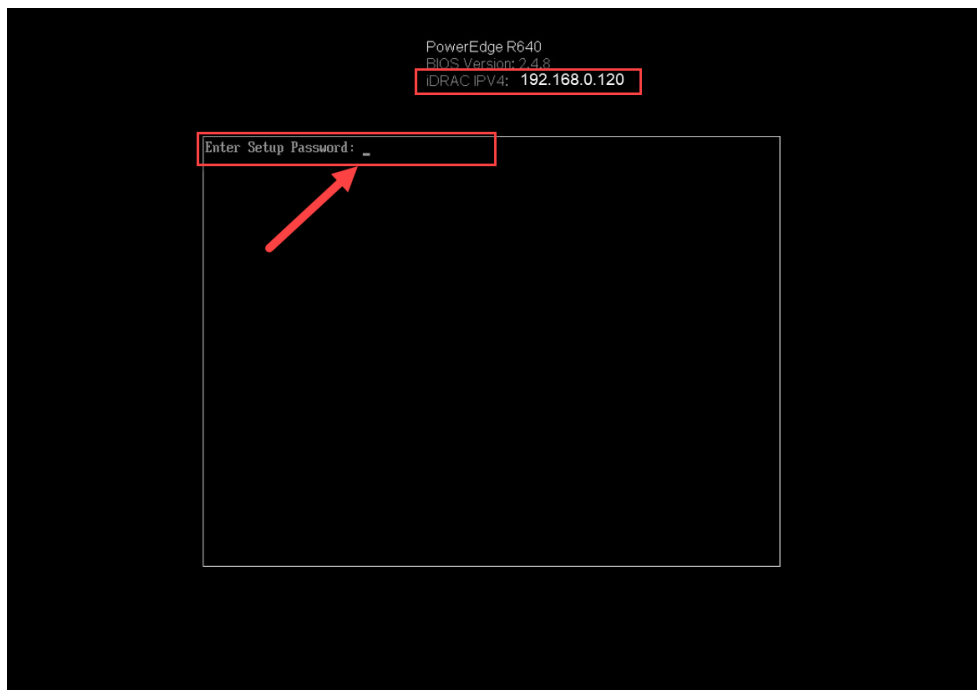
Setting IP Address First Time

Console via Crash Cart

1. Power on the system and Press "F10" to access the iDRAC.

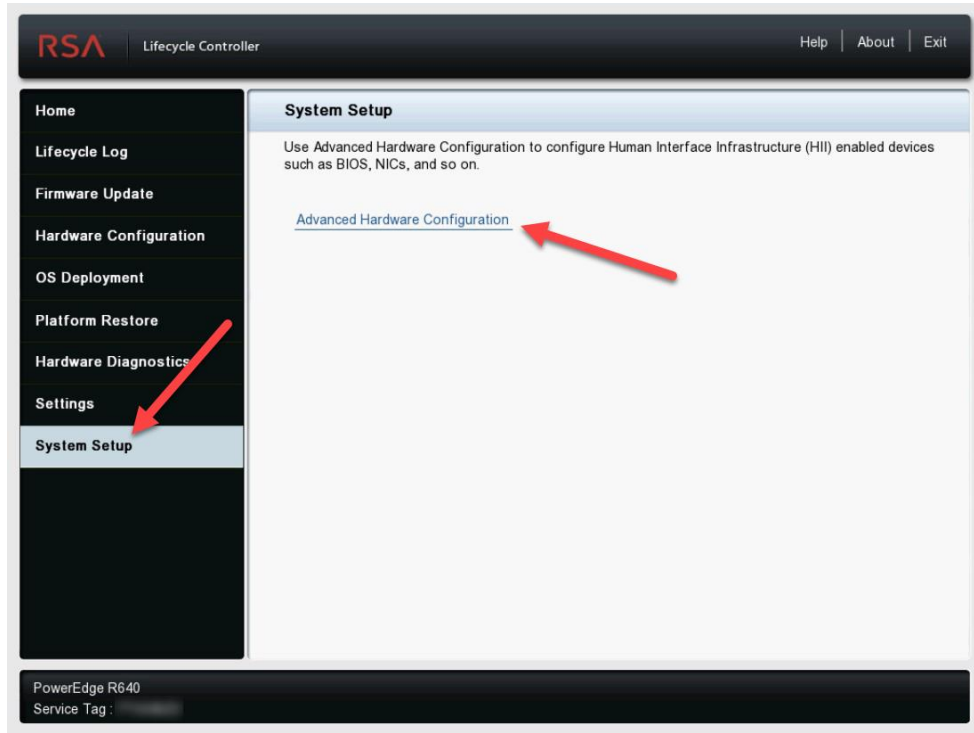


2. Enter the "Setup Password" of "rsabios"

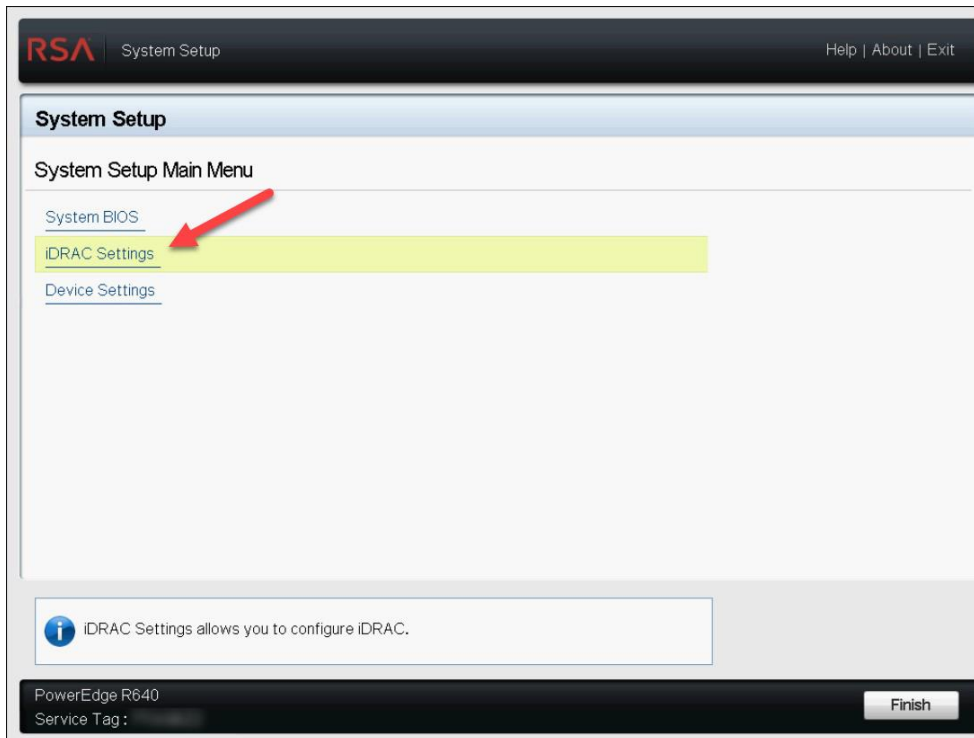


iDRAC Configuration and Maintenance

- Click on “System Setup”, then “Advanced Hardware Configuration”.

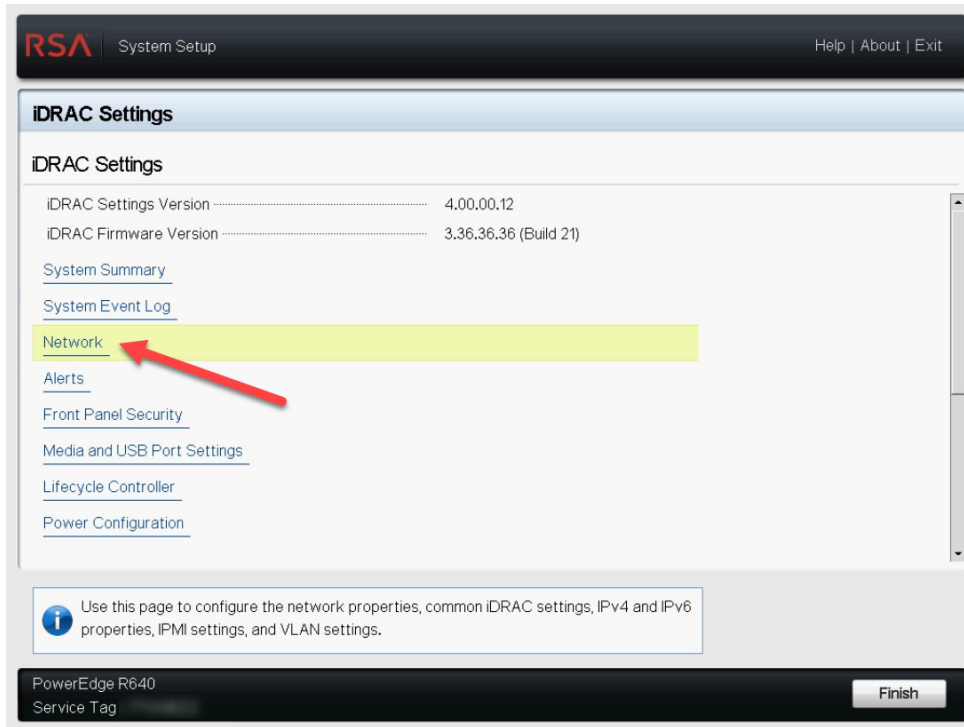


- Click on “iDRAC Settings”.

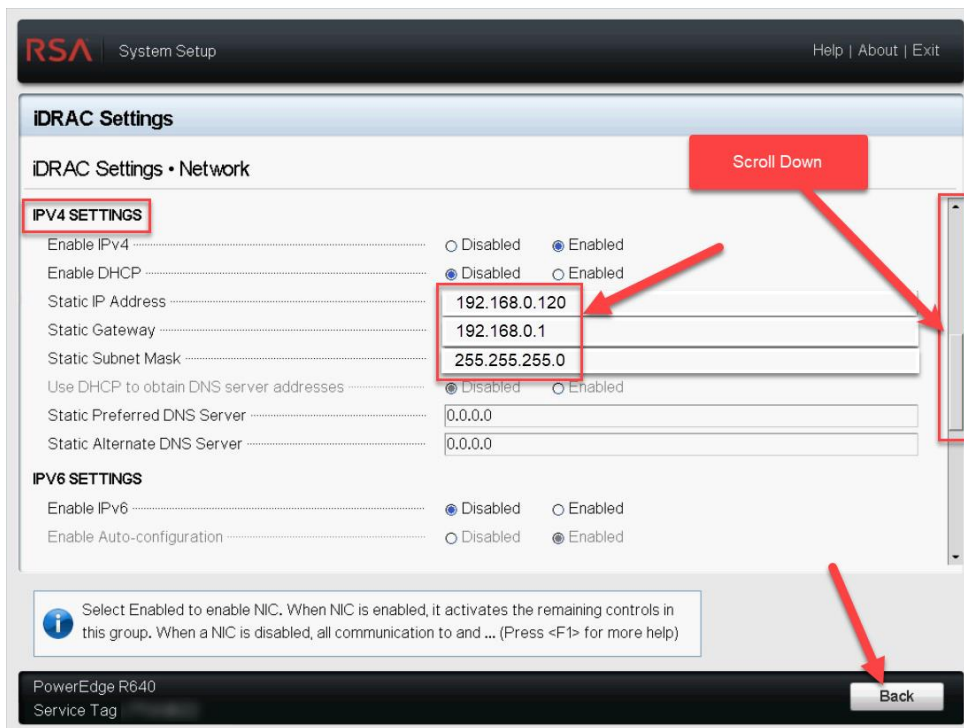


iDRAC Configuration and Maintenance

5. Click on “Network”.

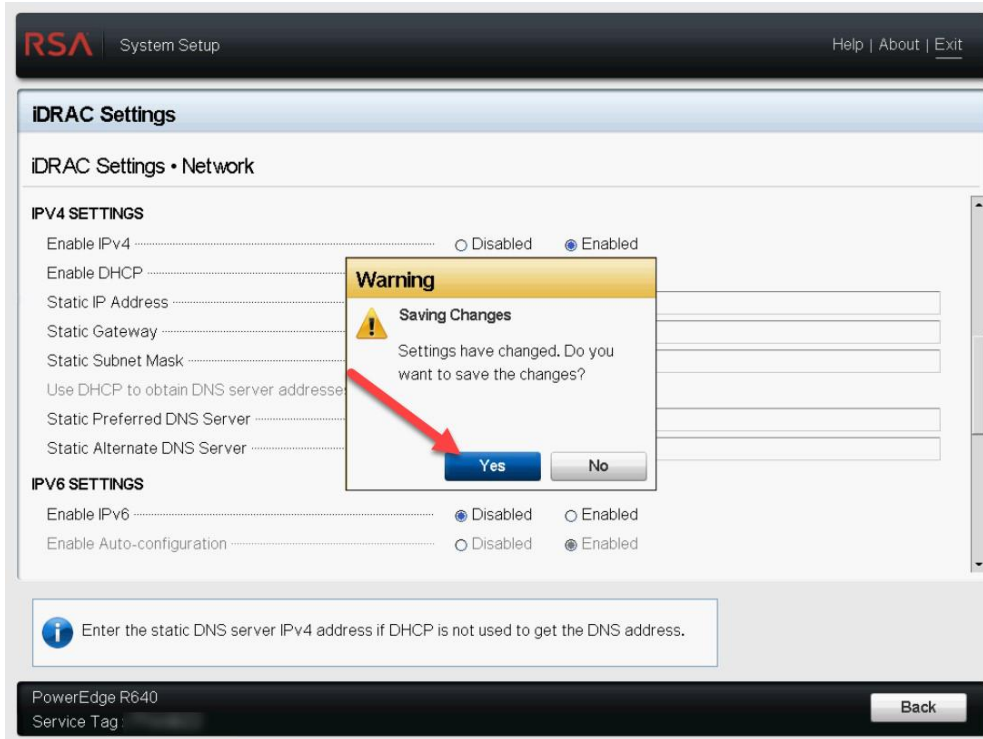


6. Scroll down to the IPV4 settings and enter your IP address information.

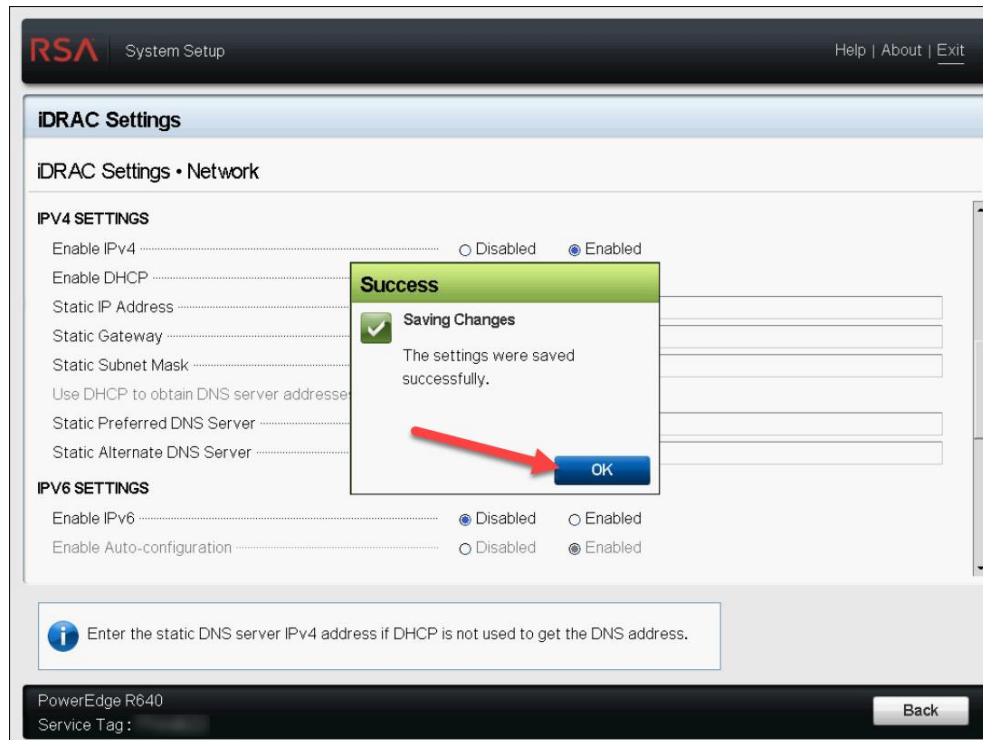


iDRAC Configuration and Maintenance

7. Click “Yes”.

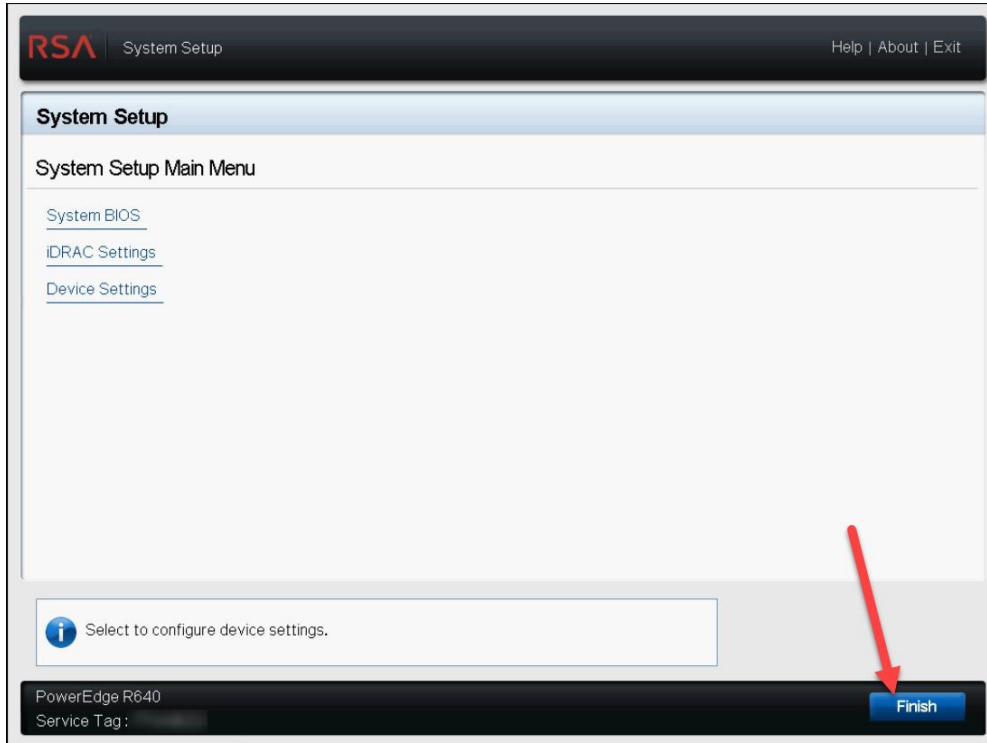


8. Click “OK”.

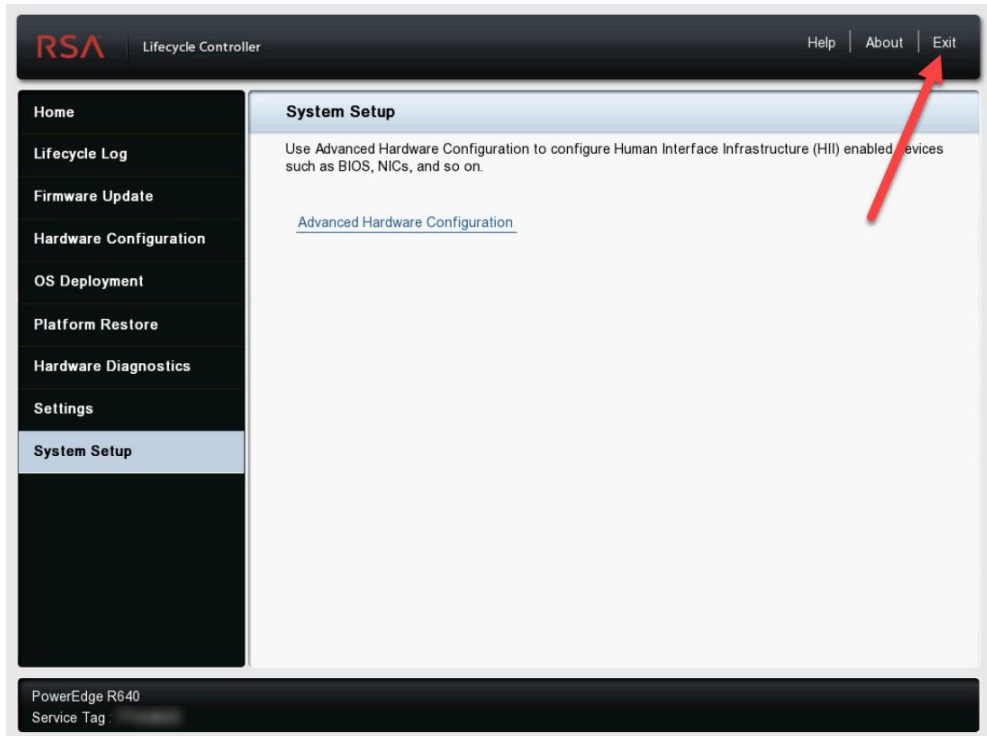


iDRAC Configuration and Maintenance

9. Click "Finish".

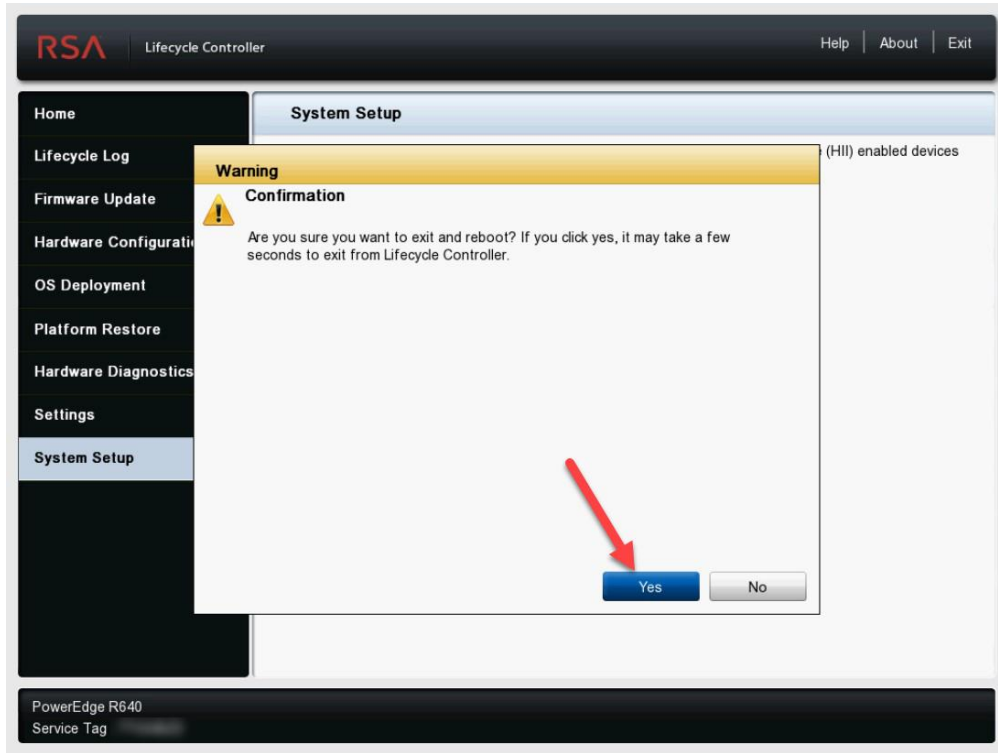


10. Click on "Exit".

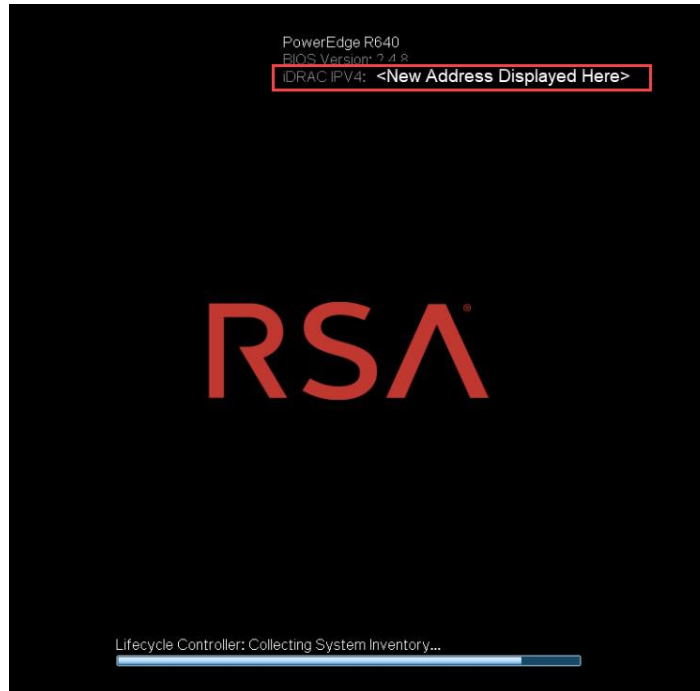


iDRAC Configuration and Maintenance

11. Click “Yes”. Be patient, it will not react immediately



12. During the reboot the new iDRAC IP address will be displayed at the top of the screen.



iDRAC Configuration and Maintenance

Configuring iDRAC Settings Using Web UI

Logging in to Web UI

1. Browse to <https://<your iDRAC IP Here>> using Chrome or Firefox Browser
2. Login to iDRAC Web UI using “**root**” and “**themaster01**” as the username and password and click on “Log In”.

Integrated Dell Remote Access Controller 9
PowerEdge R640 | Enterprise

Type the User Name and Password and click Log In.

Username: Password:

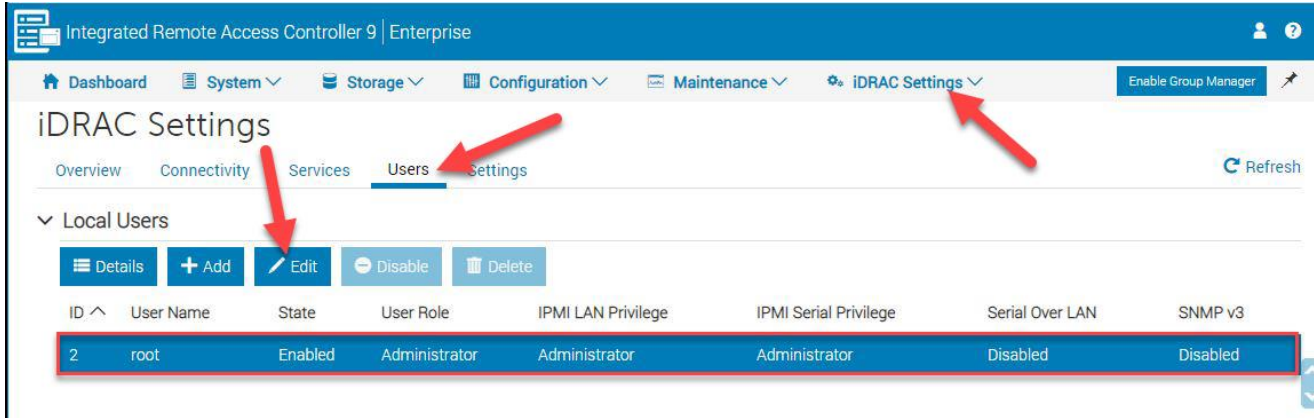
Domain:

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

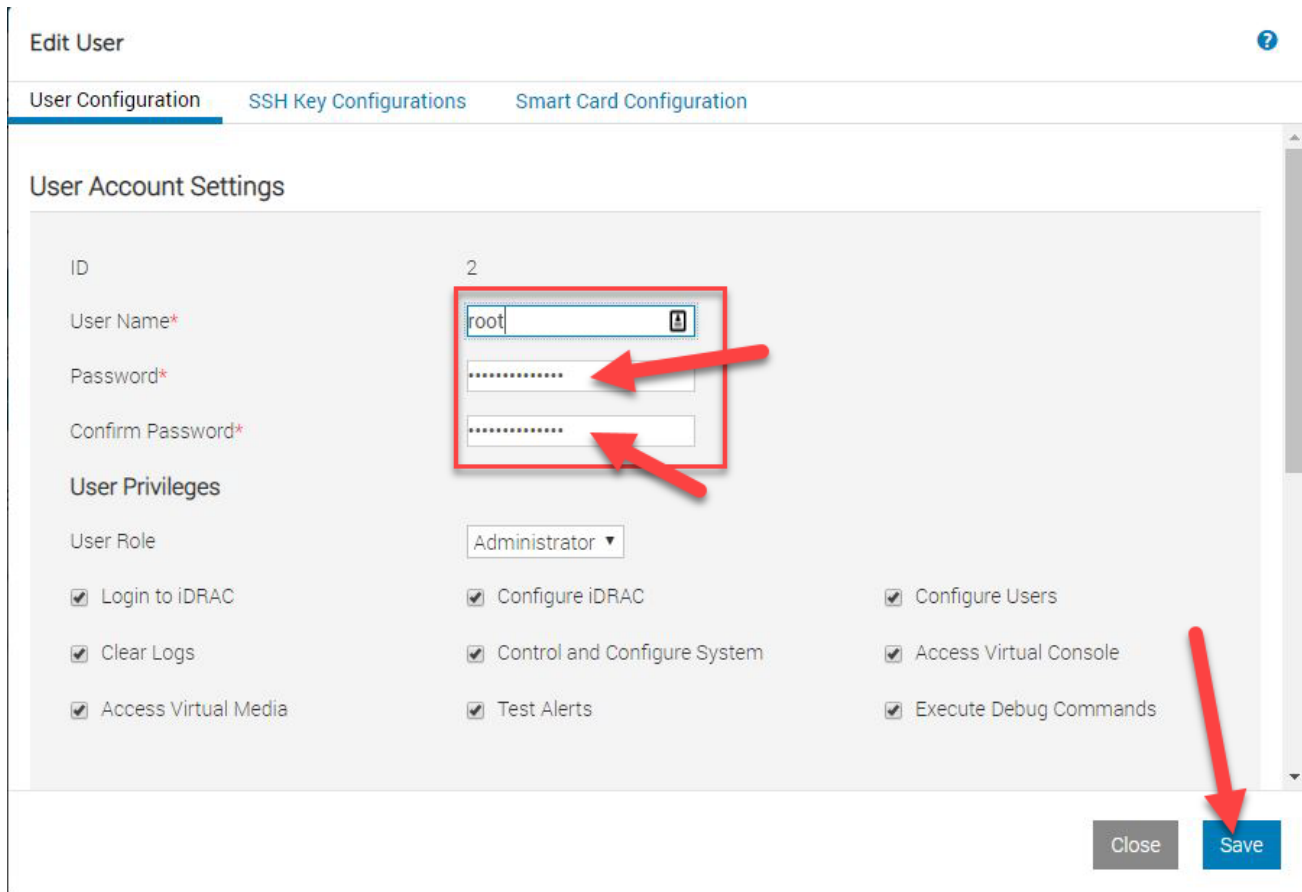
iDRAC Configuration and Maintenance

Changing User Password

1. Navigate to “iDRAC Settings→Users”, click on “Edit”.

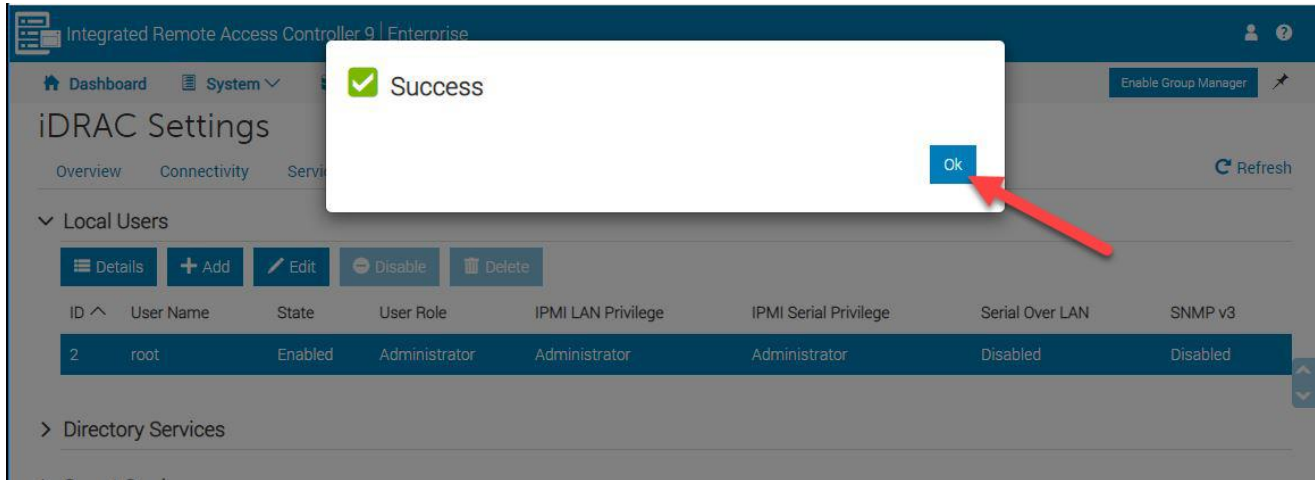


2. Type in password twice and click “Save”.



iDRAC Configuration and Maintenance

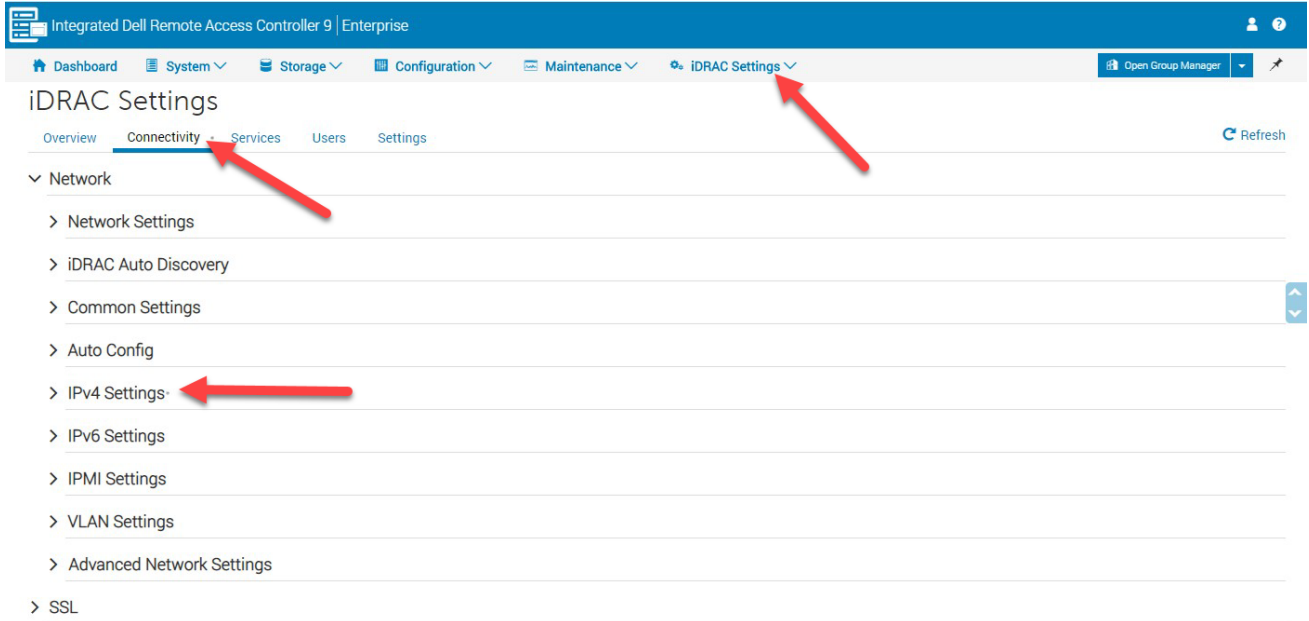
3. Click “Ok”.



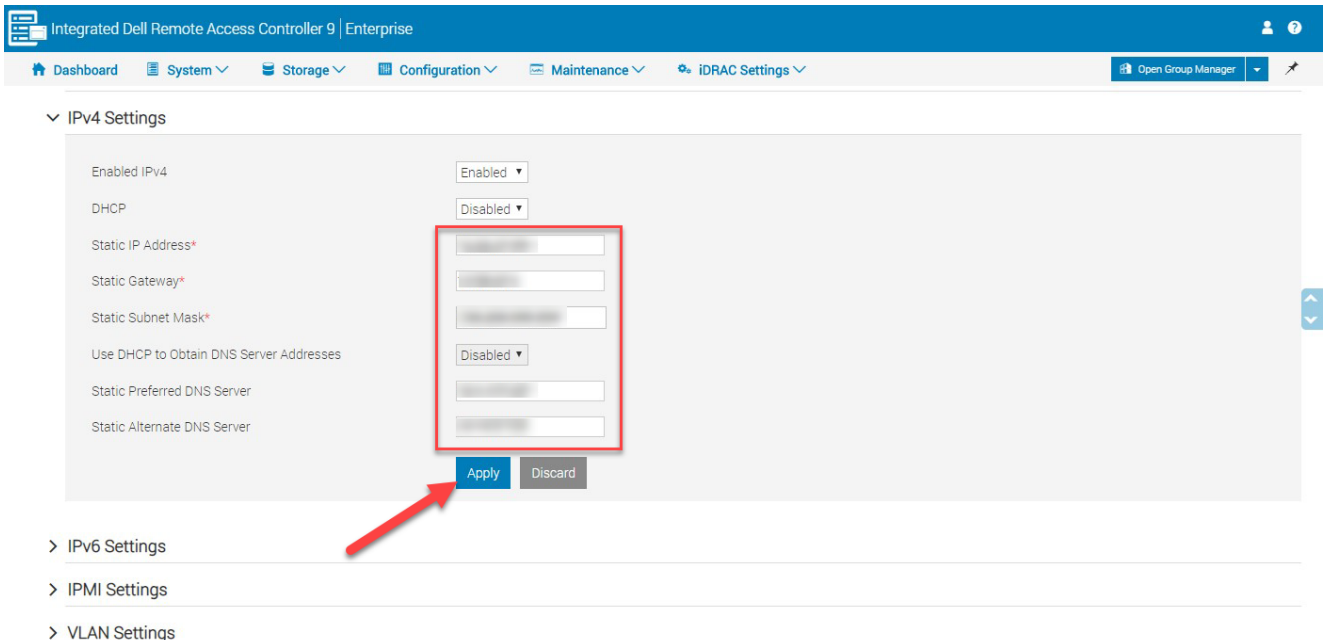
iDRAC Configuration and Maintenance

Changing IP V4 Settings

1. Click on “iDRAC Settings-->Connectivity→IPv4 Settings”.

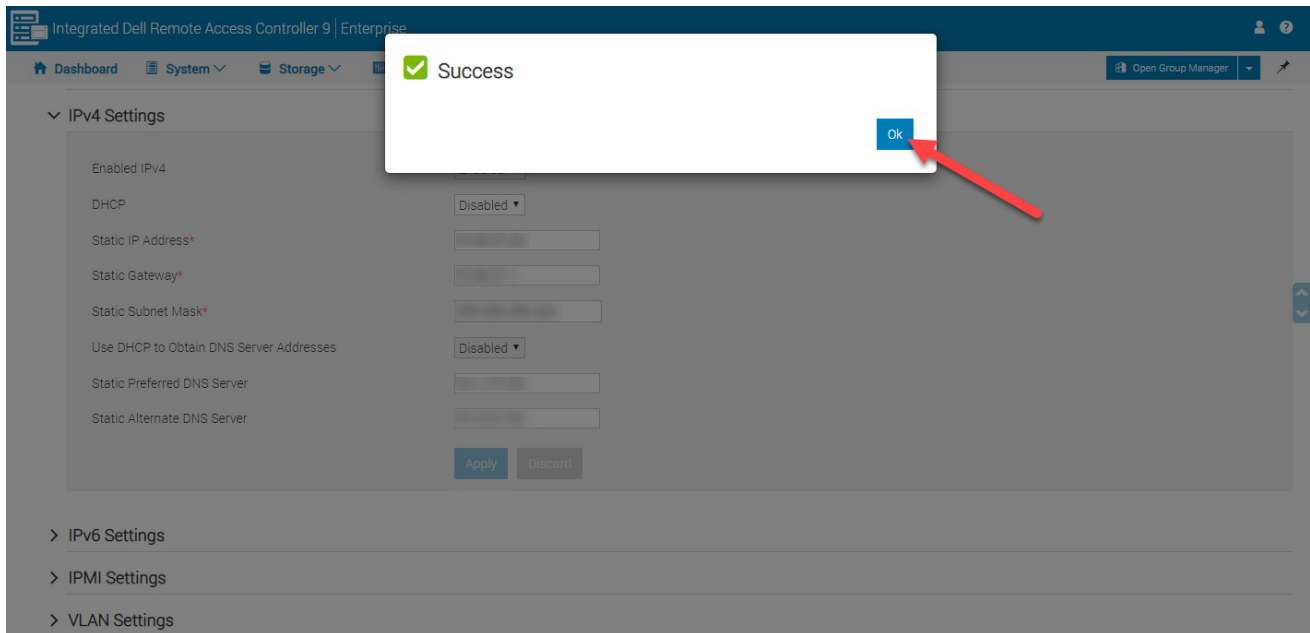


2. Fill in the IP address information, then click on “Apply”. (DNS is required for External Authentication).



iDRAC Configuration and Maintenance

3. Click on “OK”.



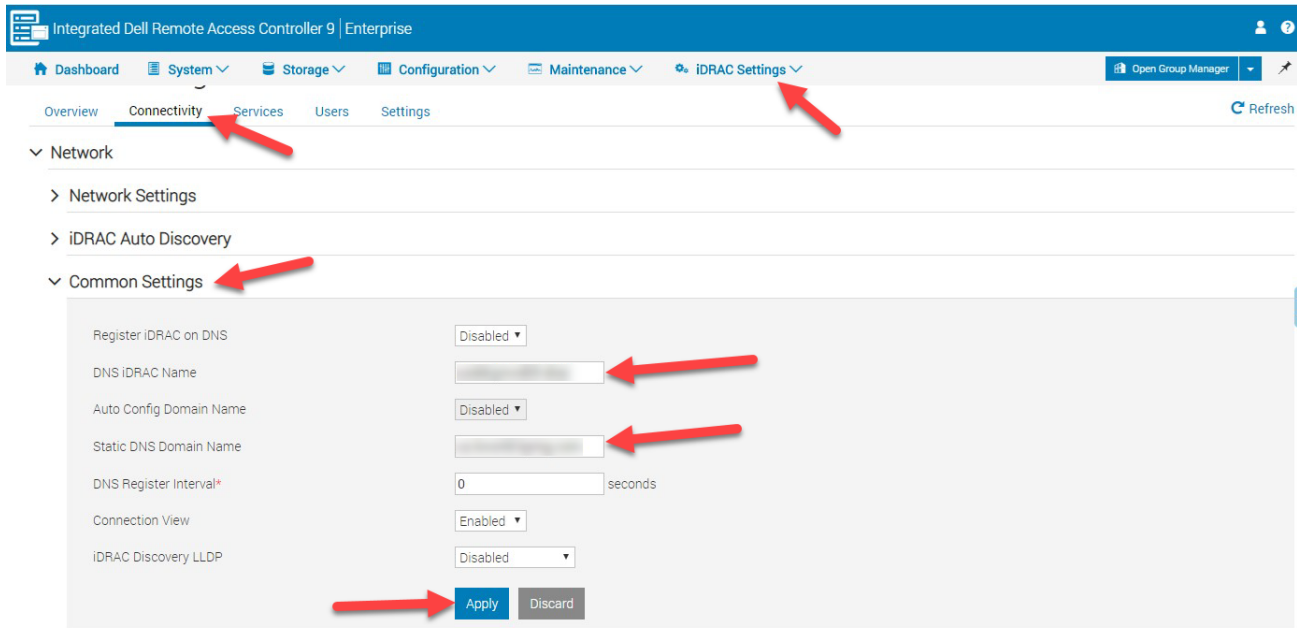
iDRAC Configuration and Maintenance

Setting iDRAC Name

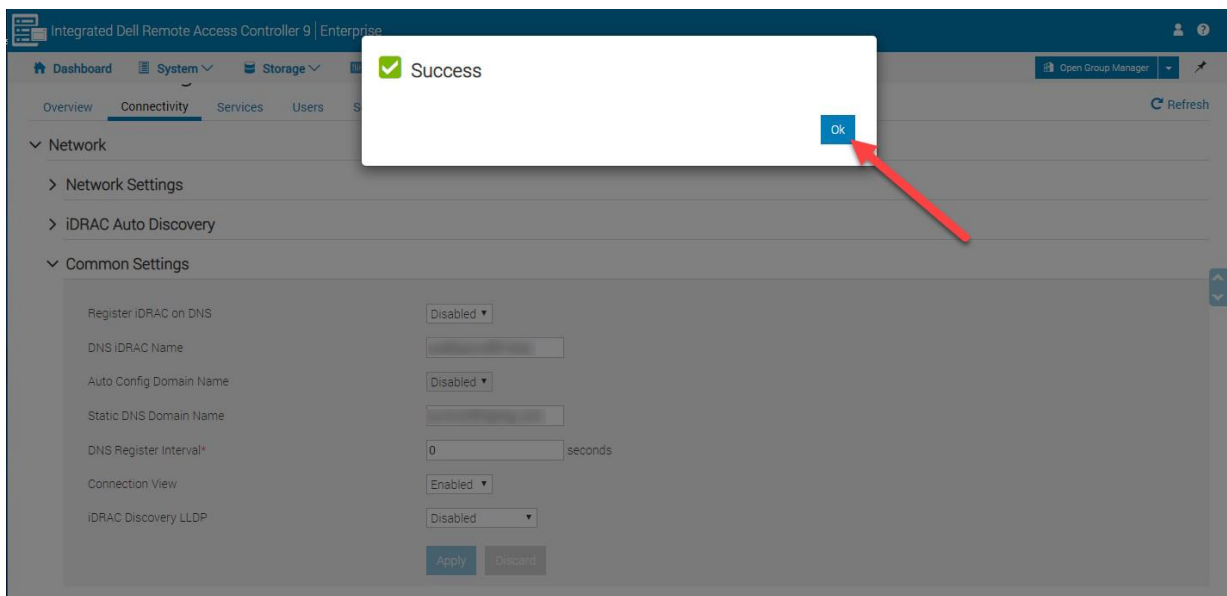
This is the name that will show up in the browser tab while using the iDRAC.

1. Click on “iDRAC Settings→Connectivity→Common Settings”, change the “DNS iDRAC Name” and the Static DNS Domain Name. Then click “Apply”.

NOTE: There can be NO underscores “_” in hostnames or the hostname portion of fully qualified DNS names. Only numbers, letters and dashes “-” in hostnames.



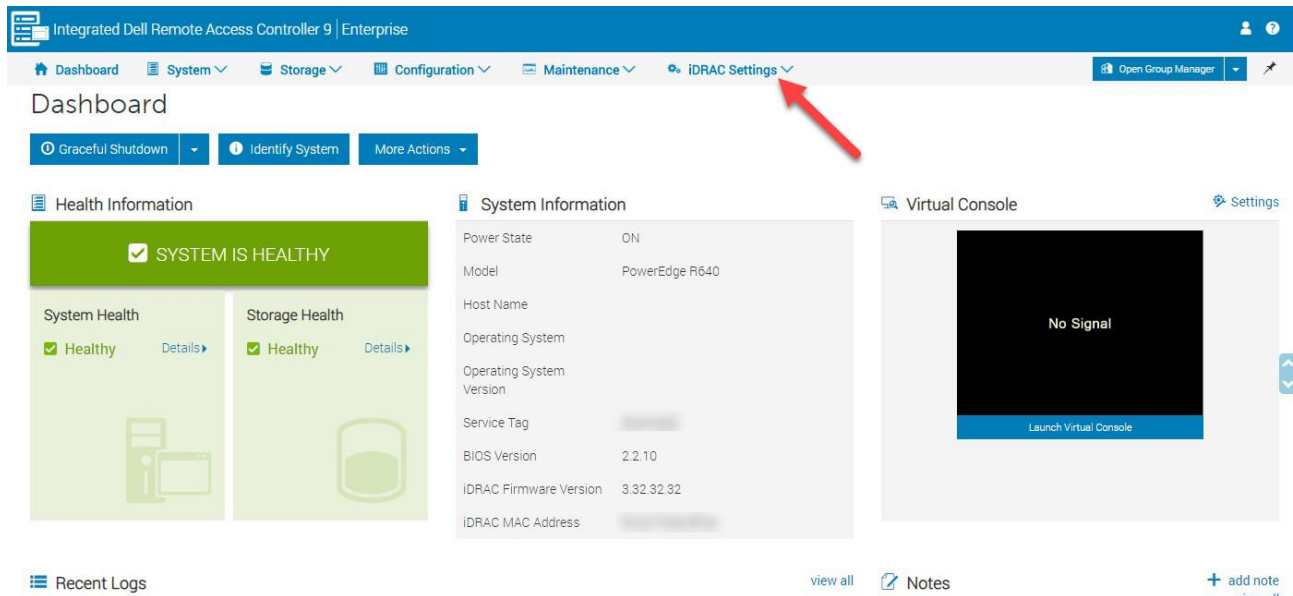
2. Click “Ok”.



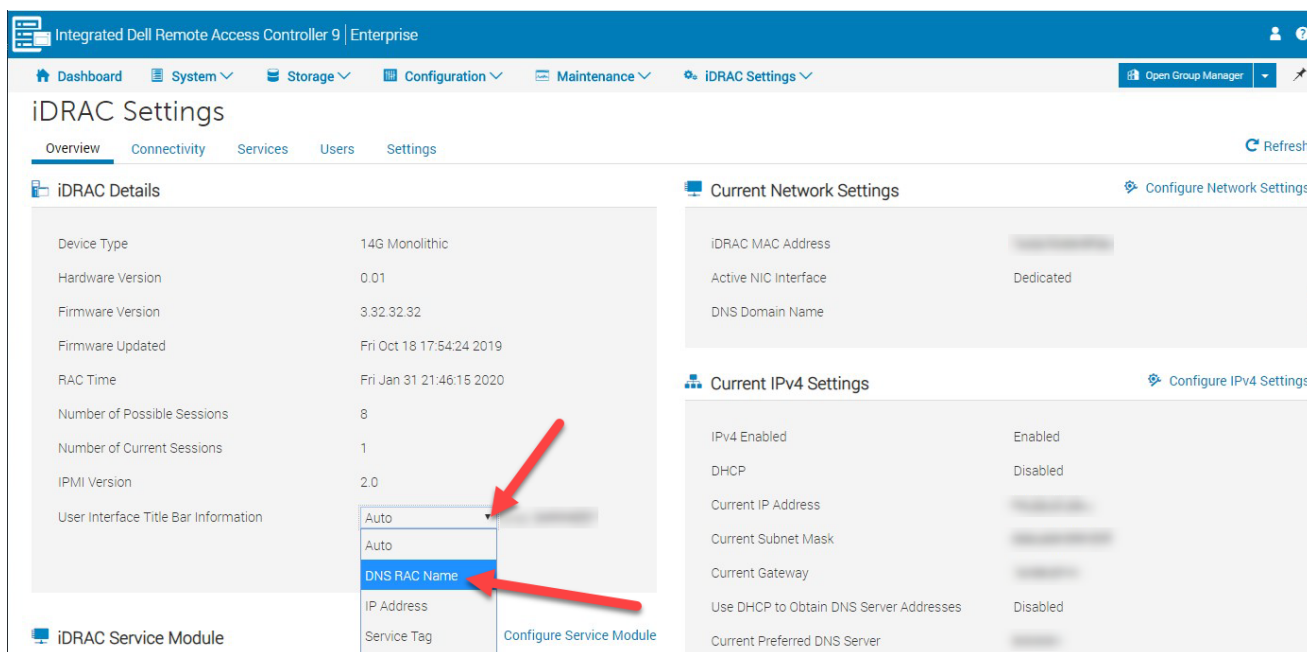
iDRAC Configuration and Maintenance

Changing Browser Tab Name

1. Click on “iDRAC Settings”.

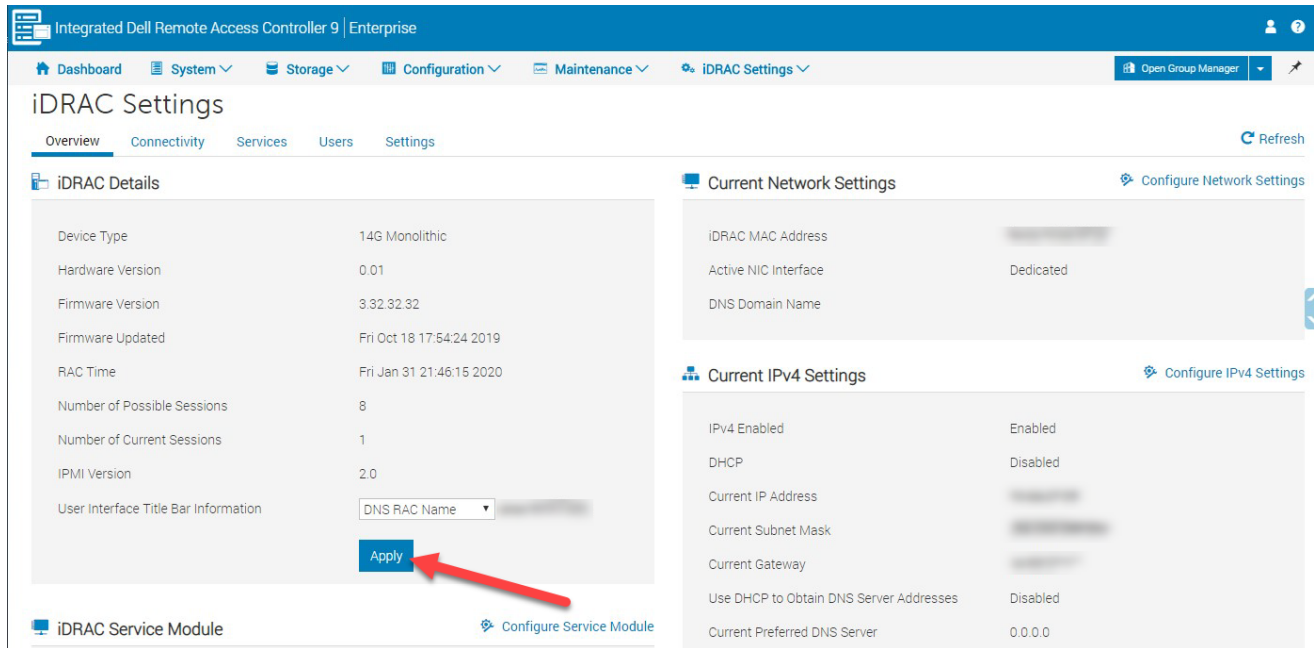


2. Change the “User interface Title Bar Information” to “DNS RAC Name”.

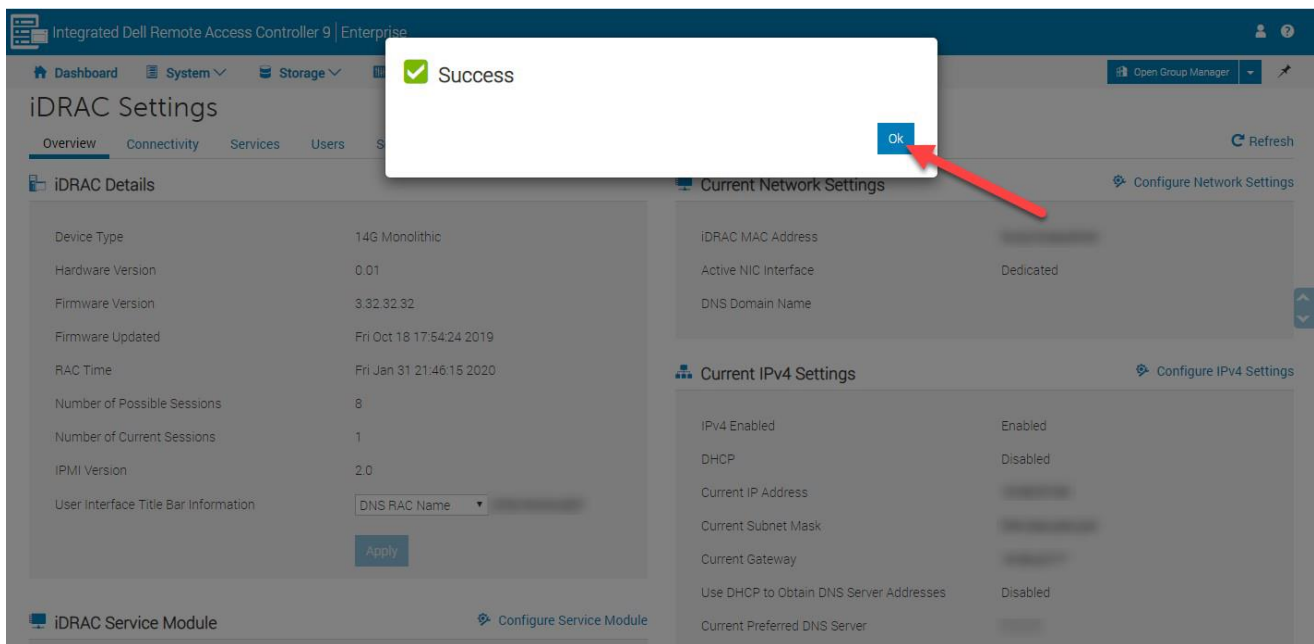


iDRAC Configuration and Maintenance

3. Click “Apply”.



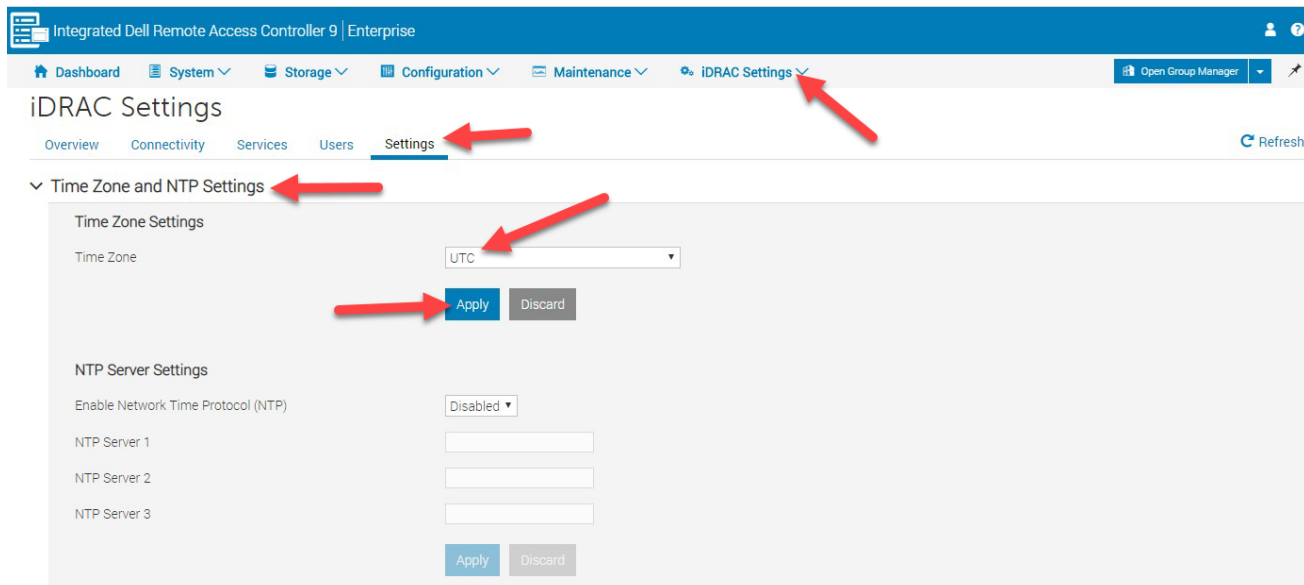
4. Click on “Ok”.



iDRAC Configuration and Maintenance

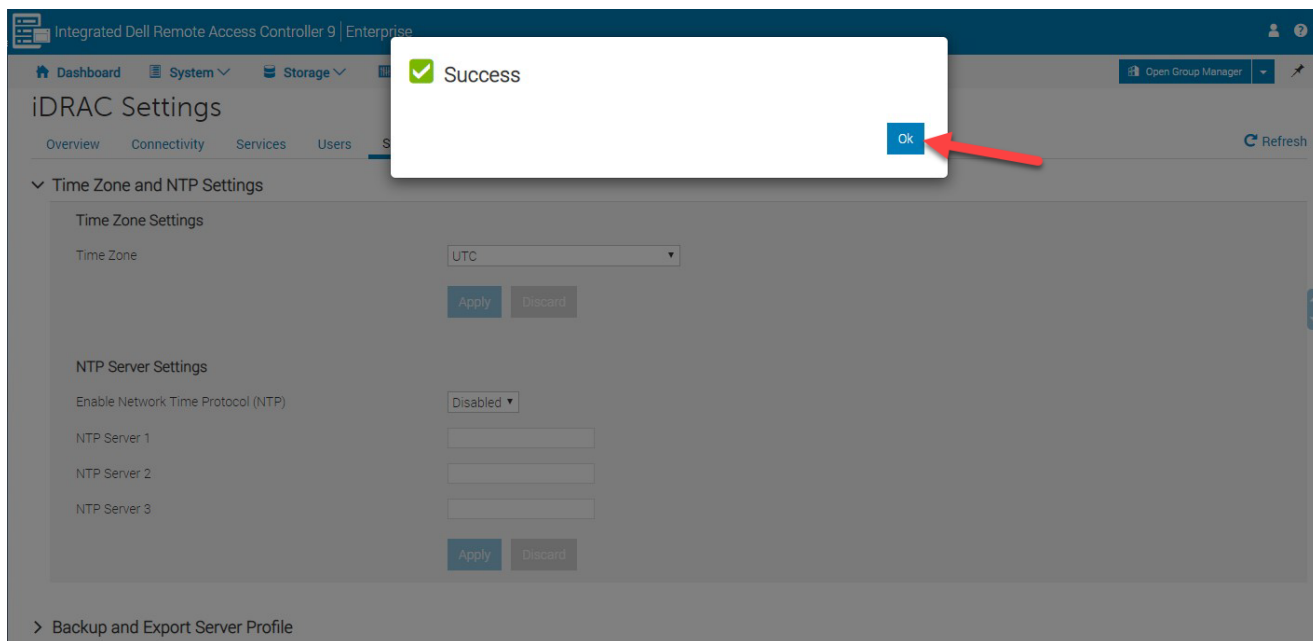
Changing Time Zone

1. Navigate to the “iDRAC Settings→Settings→Time Zone and NTP Settings”. Change the “Time Zone” and click “Apply”.



> Backup and Export Server Profile

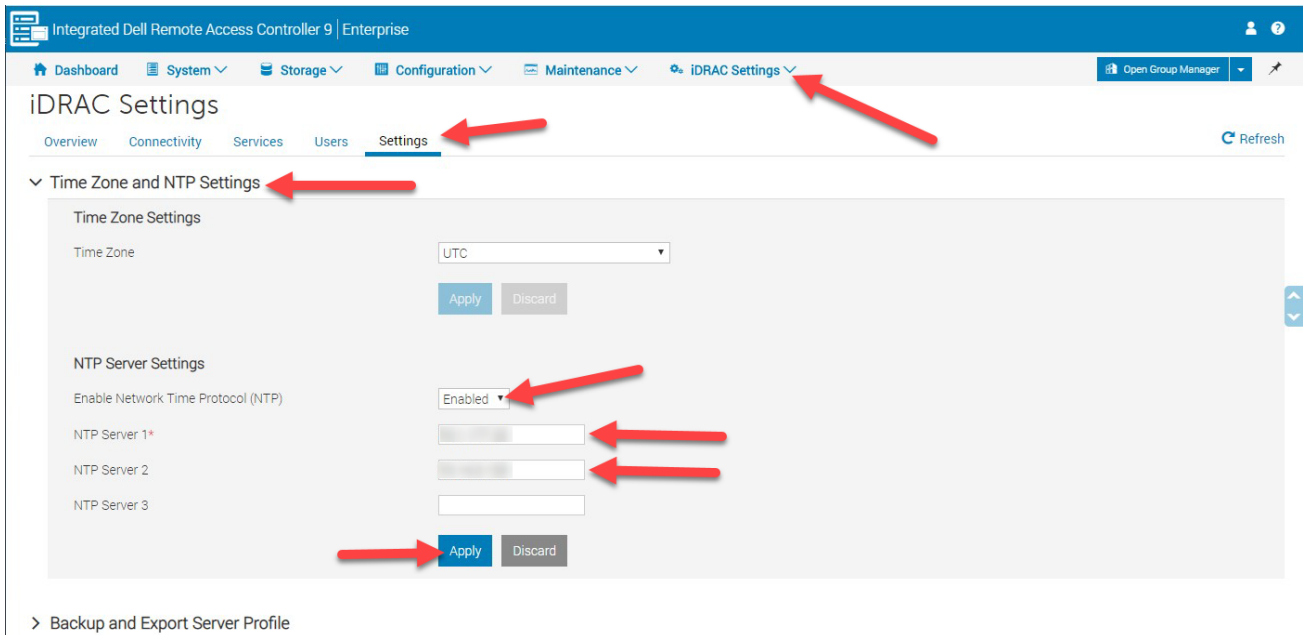
2. Click “Ok”.



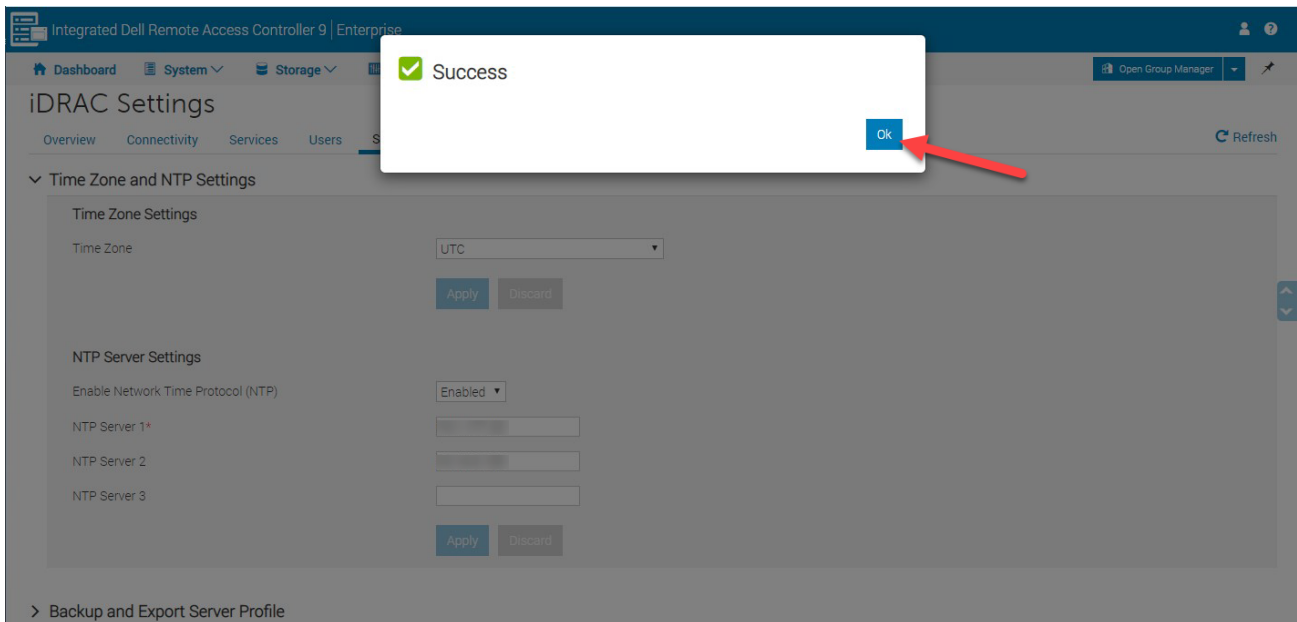
iDRAC Configuration and Maintenance

Enabling NTP

1. Navigate to the “iDRAC Settings→Settings→Time Zone and NTP Settings”. Change the “Enable Network Time Protocol” to “Enabled”, add the “NTP Server(s)” and click “Apply”.



2. Click “Ok”



iDRAC Configuration and Maintenance

Maintenance

Checking iDRAC Firmware and System BIOS Versions

1. Click on “Dashboard”, the BIOS and iDRAC firmware versions are in the middle pane on the page.

The screenshot displays the iDRAC Enterprise web interface for 'Integrated Remote Access Controller 9 | Enterprise'. The navigation menu includes Dashboard, System, Storage, Configuration, Maintenance, and iDRAC Settings. The 'Dashboard' tab is selected, and a red arrow points to it. The main content area is divided into three panes:

- Health Information:** Shows 'SYSTEM IS HEALTHY' with a green checkmark. Below this are 'System Health' and 'Storage Health', both marked as 'Healthy'.
- System Information:** A table of system details:

Power State	ON
Model	PowerEdge R640
Host Name	
Operating System	
Operating System Version	
Service Tag	
BIOS Version	2.4.8
iDRAC Firmware Version	3.36.36.36
iDRAC MAC Address	
License	Enterprise Edit

 The 'BIOS Version' and 'iDRAC Firmware Version' rows are highlighted with a red box.
- Virtual Console:** Shows a black screen with 'No Signal' and a 'Launch Virtual Console' button.

At the bottom, there are sections for 'Recent Logs', 'Notes', and 'add note view all'.

iDRAC Configuration and Maintenance

Checking iDRAC RAID Firmware Version

1. Click on “Storage→Overview→Controllers”, the “Firmware Version” is in the table.

The screenshot shows the iDRAC web interface for an Integrated Remote Access Controller 9 Enterprise. The navigation menu includes Dashboard, System, Storage, Configuration, Maintenance, and iDRAC Settings. The Storage Overview page is active, with sub-tabs for Summary, Controllers, Physical Disks, Virtual Disks, and Enclosures. The Controllers table lists two RAID controllers: PERC H740P Mini (Embedded) and PERC H840 Adapter. The Firmware Version column for both is 50.5.0-2819. Below the Controllers table is the Controller Battery section, which shows two batteries: Battery on Integrated RAID Controller 1 and Battery on RAID Controller in Slot 1, both in a Ready state.

Rollup Status	Name	Device Description	PCI Slot	Firmware Version	Driver Version	Cache Memory Size
+ <input checked="" type="checkbox"/>	PERC H740P Mini (Embedded)	Integrated RAID Controller 1	Not Applicable	50.5.0-2819	--NA--	8192 MB
+ <input checked="" type="checkbox"/>	PERC H840 Adapter	RAID Controller in Slot 1	1	50.5.0-2819	--NA--	8192 MB

Status	Battery Name	Device Description	State	Controller Name
<input checked="" type="checkbox"/>	Battery	Battery on Integrated RAID Controller 1	Ready	PERC H740P Mini (Embedded)
<input checked="" type="checkbox"/>	Battery	Battery on RAID Controller in Slot 1	Ready	PERC H840 Adapter

iDRAC Configuration and Maintenance

Updating Firmware/BIOS

1. Download Firmware/BIOS from the RSA Link Website.
<https://community.rsa.com/docs/DOC-79266>

RSA NetWitness Availability of BIOS & iDRAC Firmware Updates

Like • 0 Comment • 0

Document created by RSA Product Team [RSA](#) on Jul 24, 2017 • Last modified by RSA Product Team on Jan 7, 2020

Version 19

Summary:

The latest supported BIOS and iDRAC firmware version for Series 4, 4S, 5, and 6 appliances are available to download and apply. To obtain the latest security fixes and firmware enhancements, RSA strongly recommends updating systems with the updates provided below.

RSA has qualified these firmware versions and have verified it will NOT affect operation of the NW. Server, Decoder, Concentrator, Broker, Archiver, ESA, Malware, AIO and Hybrid hosts once applied. Reboot is required after applying iDRAC and BIOS updates.

Important: Please use the following instructions for updating Series 4S, 5, and 6 and PowerVault

firmware: <http://www.dell.com/support/article/us/en/04/sln292363/poweredge-server-updating-firmware-through-the-idrac?lang=en#idrac78>

PowerVault updates are performed through the iDRAC interface of the connected host system.

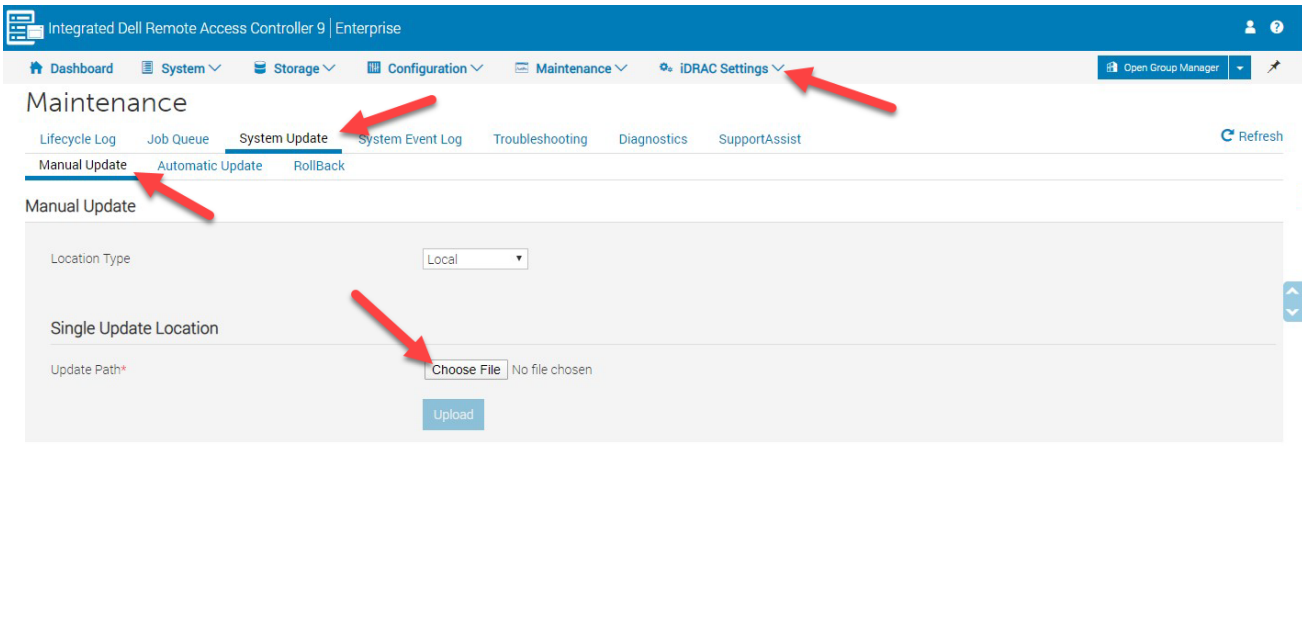
For S4s, S5, and S6 driver downloads, select the Update Package for Microsoft® Windows® 64-Bit. This file will be used to update the appliance via the iDRAC update and rollback feature identified in the link above.

For S4, download the Update Package for Red Hat Linux and perform the update via the Operating System

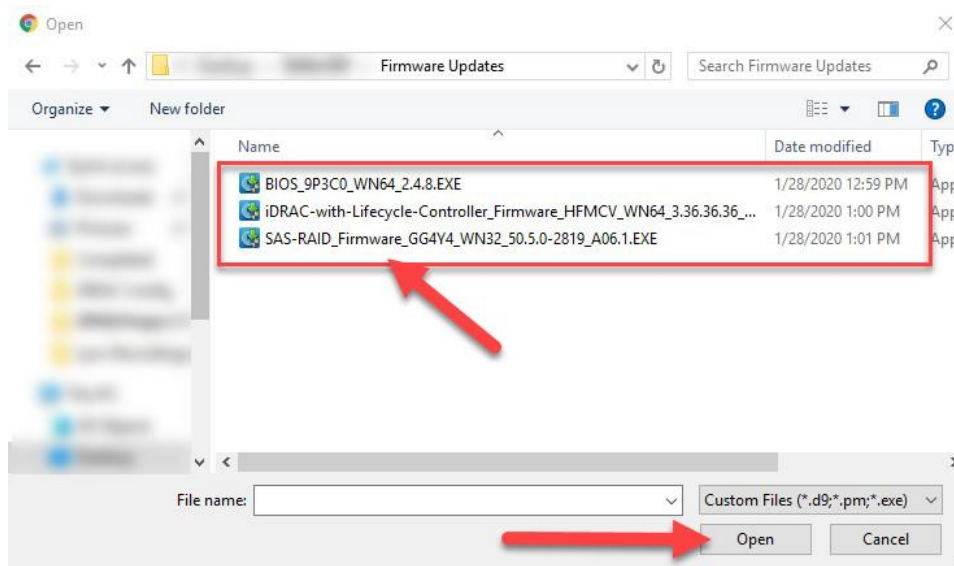
Hardware	BIOS	iDRAC	PERC	CPLD
Series 6	Dell EMC Server PowerEdge BIOS R740/R740xd/R640/R940/7920R Version 2.4.8 Download and Release Notes	iDRAC with Lifecycle Controller v. 3.36.36.36 Download and Release Notes	PERC H740P Mini/ H740P Adapter/ H840 Adapter RAID Controllers firmware version 50.5.0-2819 Download and Release Notes	CPLD Version 1.0.8 for Dell EMC PowerEdge R740 and R740 XDServers Download and Release Notes
Series 5	Dell Server PowerEdge BIOS R630/R730/R730XD Version 2.10.5 Download and Release Notes	iDRAC with Lifecycle Controller 2.70.70.70 Download and Release Notes	Dell PERC H730/H730P/H830/FD33xS/FD33xD Mini/Adapter RAID Controllers firmware 25.5.3.0005 Download and Release Notes	

iDRAC Configuration and Maintenance

- Navigate to the “iDRAC Settings→System Update→Manual Update” and click “Choose File”.



- Select a file and choose “Open”.



iDRAC Configuration and Maintenance

- Select the firmware/BIOS and click on “Install Next Reboot”.

The screenshot shows the 'Maintenance' page in the iDRAC interface. Under the 'Manual Update' section, there is a table with the following data:

Contents	Criticality	Prerequisites	Status
<input checked="" type="checkbox"/> BIOS_9P3C0_WN64_2.4.8.EXE	Recommended	None	Package successfully downloaded

Below the table are three buttons: 'Cancel', 'Install and Reboot', and 'Install Next Reboot'. A red arrow points from the 'Install Next Reboot' button back to the update row.

- Click on “Job Queue”.

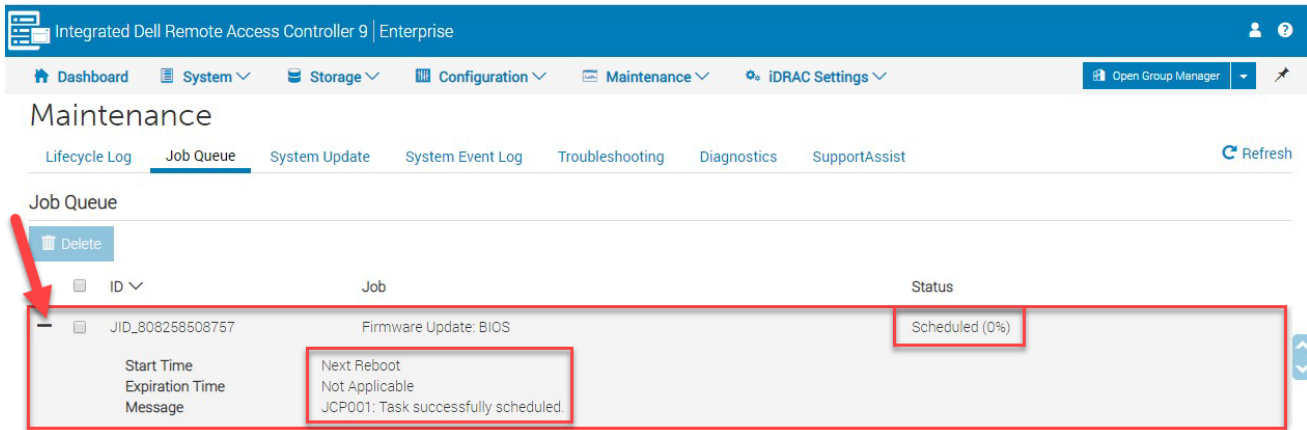
The screenshot shows the same 'Maintenance' page, but with an 'Information' dialog box overlaid. The dialog box contains the following text:

Information
 RAC0603: Updating Job Queue. Status of the update jobs can be viewed and managed within the Job Queue page.
 Click Job Queue button to view the status of the update jobs.

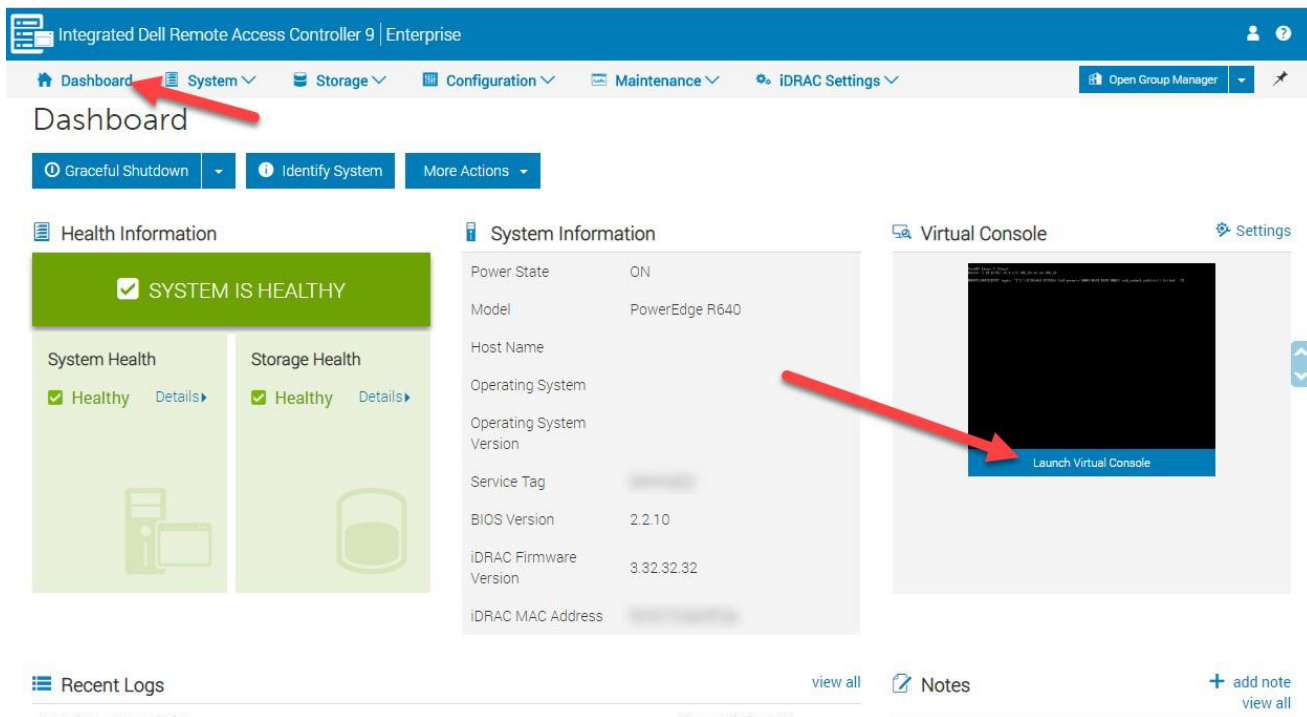
At the bottom of the dialog box are two buttons: 'Job Queue' and 'Cancel'. A red arrow points to the 'Job Queue' button.

iDRAC Configuration and Maintenance

6. Verify that the job is scheduled for next reboot.



7. Click on "Dashboard" and "Launch Virtual Console".



iDRAC Configuration and Maintenance

8. Login as “root” and type “reboot” to restart the system and start the update.

```

CentOS Linux 7 (Core)
Kernel 3.10.0-862.14.4.el7.x86_64 on an x86_64

NWAPPLIANCE18747 login: root
Password:
Last login: Tue Feb  4 14:59:08 on tty1
[root@NWAPPLIANCE18747 ~]# reboot_
    
```

9. After update completes you can check your “Job Queue”.

The screenshot shows the iDRAC Maintenance interface. The 'Job Queue' tab is selected, displaying a table with the following data:

ID	Job	Status
JID_808258508757	Firmware Update: BIOS	Completed (100%)

Below the table, the 'Message' field contains the text: "PR19: The specified job has completed successfully." A red arrow points to the 'Delete' button on the left, and red boxes highlight the 'Status' and 'Message' fields.

iDRAC Configuration and Maintenance

Locating Powervault Serial Number

1. Click on “Storage”, “Enclosures”, and then locate your Powervault. Click on the “+” to expand your view and the Service tag will be visible at the bottom of the display for that Powervault.

The screenshot shows the iDRAC interface for an Integrated Remote Access Controller 9 Enterprise. The 'Storage' menu is selected, and the 'Enclosures' sub-menu is active. A table lists the enclosure details:

Status	Enclosure ID	Associated Controllers	State
+	MD1400 0:0	PERC H840 Adapter	Ready

Below the table, the 'Physical Disks Overview' shows a pie chart with 12 disks, all in a 'Ready' state. The 'Summary of Slots' table lists 8 slots, all with 'Ready' status and 'SAS' bus protocol:

Slot	Status	State	Capacity	Bus Protocol	Hot Spare	PCIe Capable
0	+	Ready	1787.88GB	SAS	No	No
1	+	Ready	1787.88GB	SAS	No	No
2	+	Ready	1787.88GB	SAS	No	No
3	+	Ready	7451.50GB	SAS	No	No
4	+	Ready	7451.50GB	SAS	No	No
5	+	Ready	7451.50GB	SAS	No	No
6	+	Ready	7451.50GB	SAS	No	No
7	+	Ready	7451.50GB	SAS	No	No

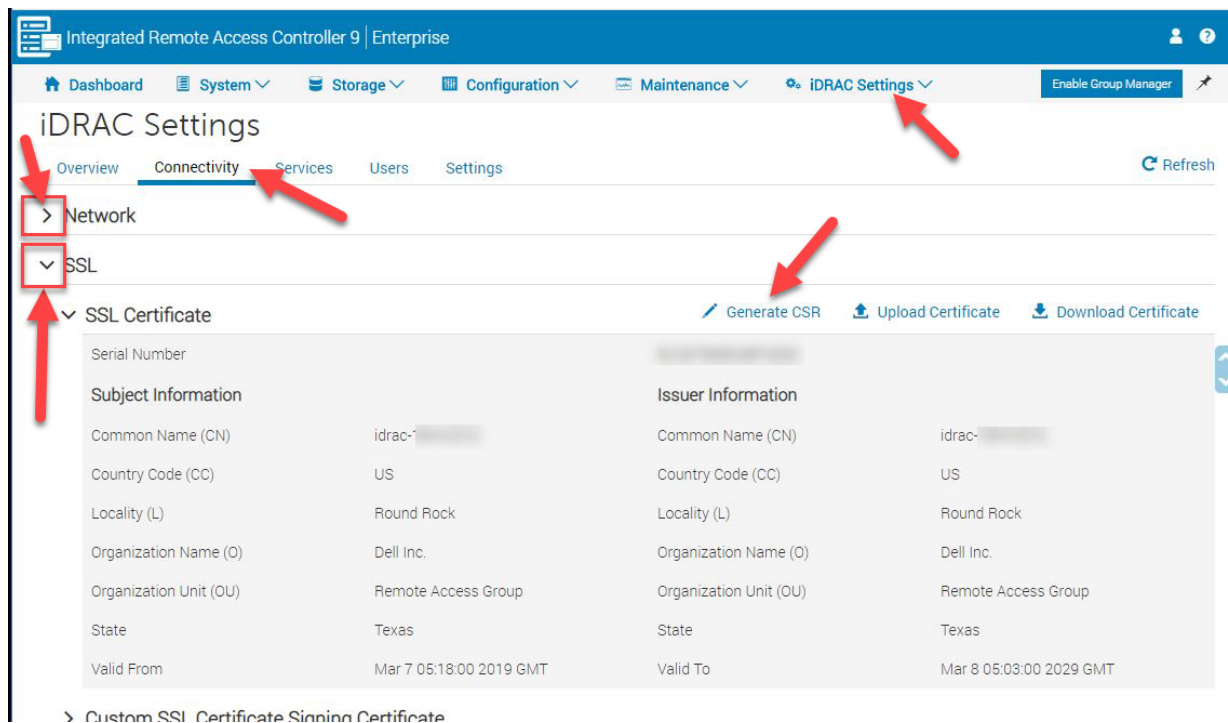
The 'Advanced Properties' section at the bottom includes fields for 'Device Description', 'Connector', 'Enclosure position', 'SAS Address', 'Redundant Path', and 'Service Tag'. The 'Service Tag' field is highlighted with a red box.

iDRAC Configuration and Maintenance

SSL Certificate for Web UI

Creating CSR

1. Navigate to the “SSL” section, “iDRAC Settings→Connectivity→SSL” and click on “Generate CSR”.



2. Fill out the CSR Form, then click “Generate”.

Generate Certificate Signing Request (CSR)

Instructions: Enter the information in the following fields and click Generate to create a new Certificate Signing Request (CSR). Generating a new CSR prevents certificates that are created with the previously generated CSR from being uploaded to iDRAC.

Common Name (CN)*

Country Code (CC)

Locality (L)*

Organization Name (O)*

Organization Unit (OU)*

State*

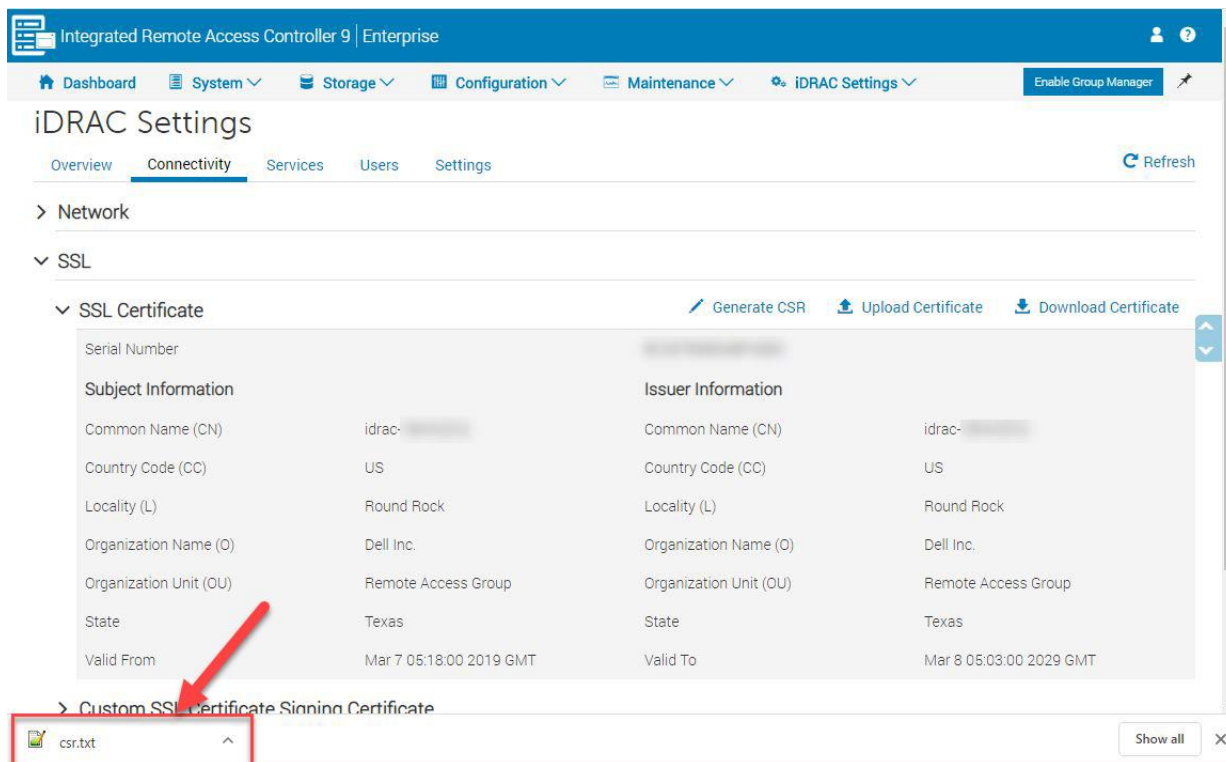
Email*

Subject Alternative Names

NOTE: The “Subject Alternate Names” allows you to put in the IP address of the host along with other possible alias hostnames that DNS might use to resolve this iDRAC’s IP address and still have the certificate to be valid. There can be NO underscores “_” in hostnames or the hostname portion of fully qualified DNS names. Only numbers, letters and dashes “-” in hostnames.

iDRAC Configuration and Maintenance

- The “csr.txt” file is downloaded to the local computer, typically in the “Downloads” folder.

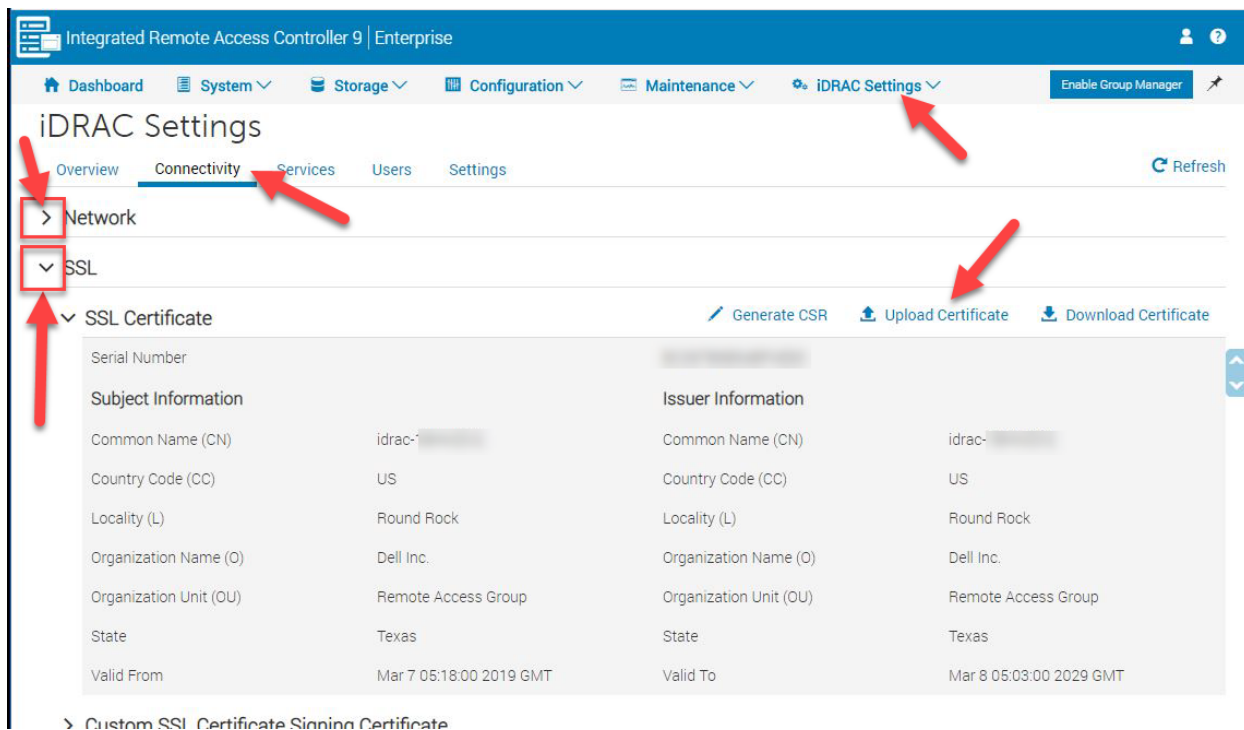


- Submit the “csr.txt” to the Certificate Authority.
NOTE: When retrieving/downloading the certificates they should be in a Base64 Encoded format.

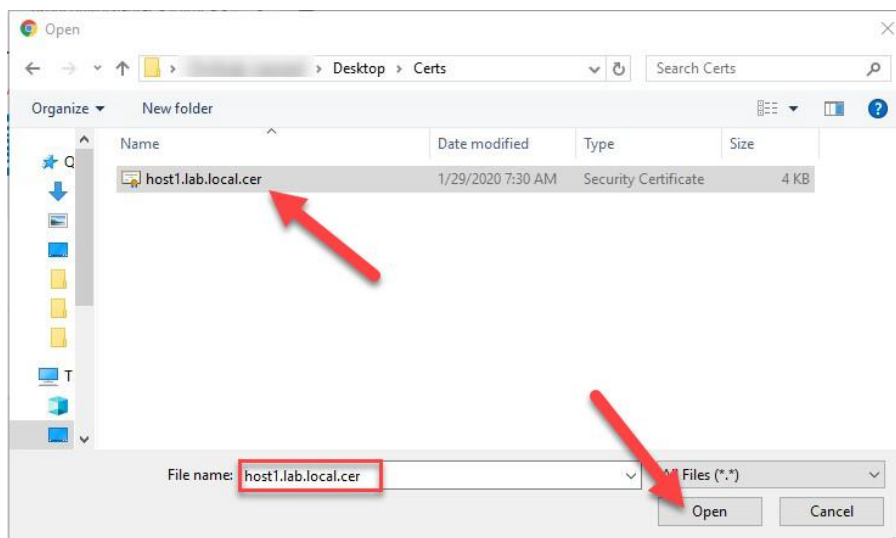
iDRAC Configuration and Maintenance

Uploading Certificate

1. Navigate to the “SSL” section, “iDRAC Settings→Connectivity→SSL” and click on “Upload Certificate”.

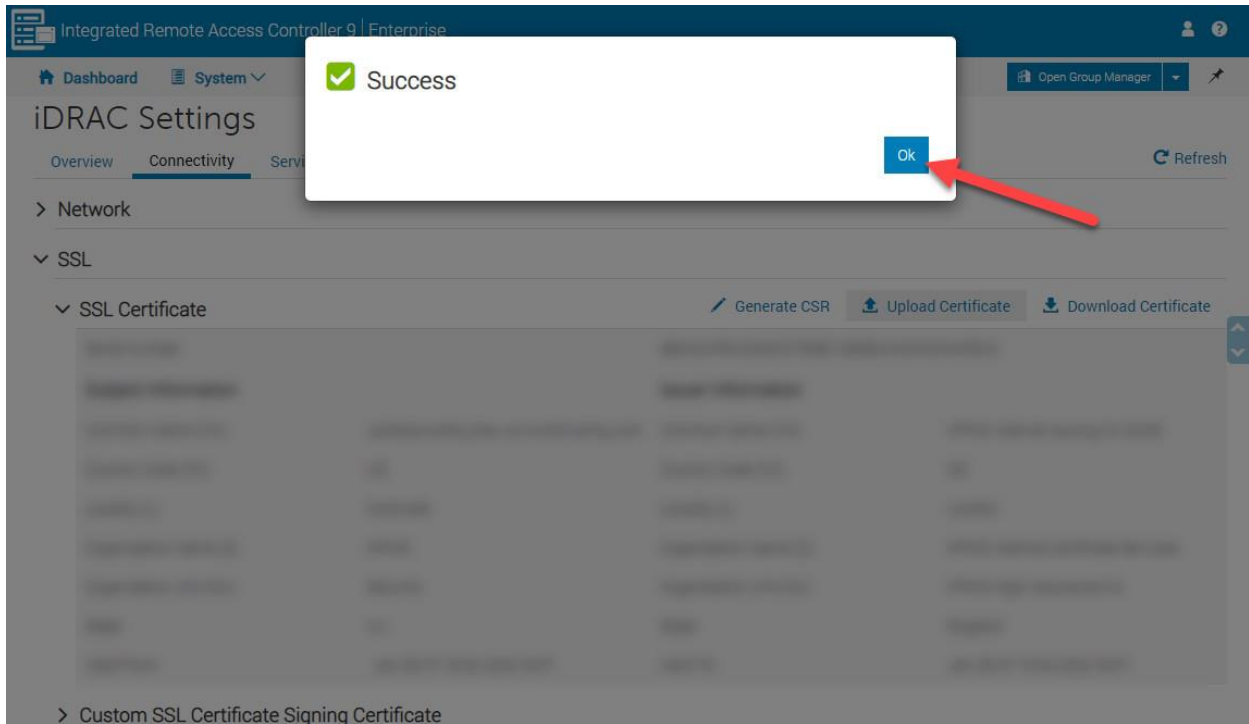


2. Choose the certificate file, click on “Open”.

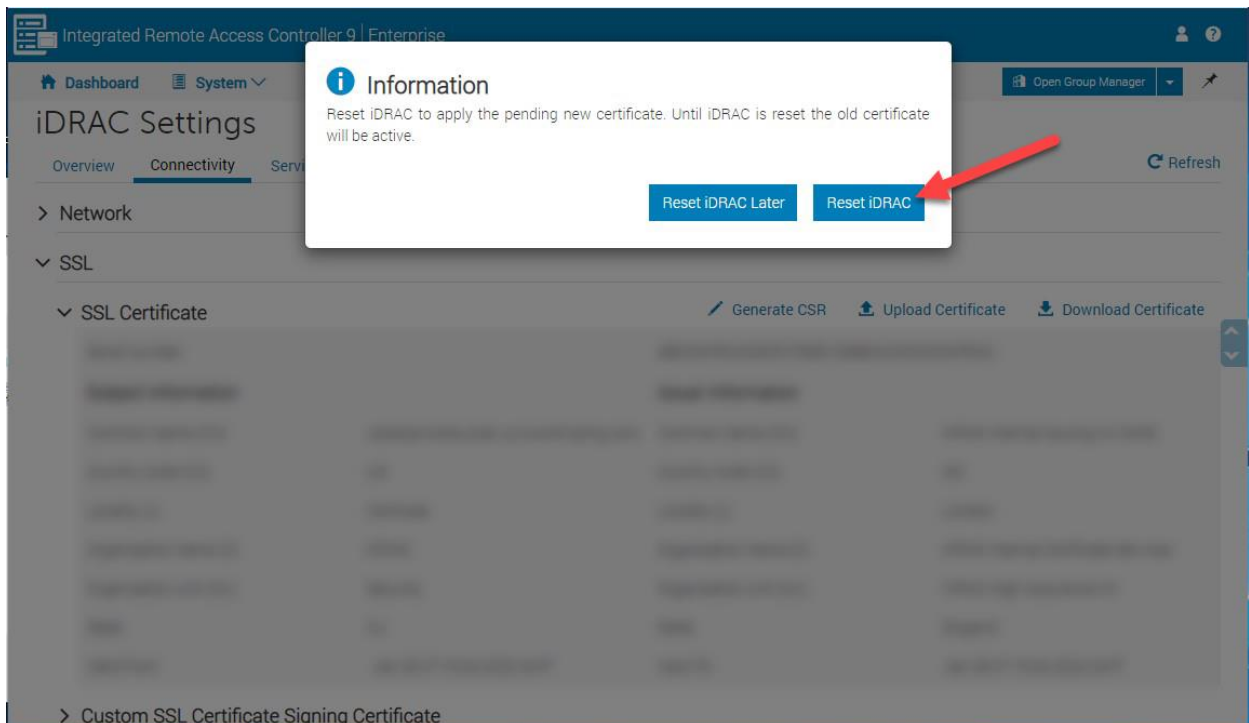


iDRAC Configuration and Maintenance

- Click "Ok".

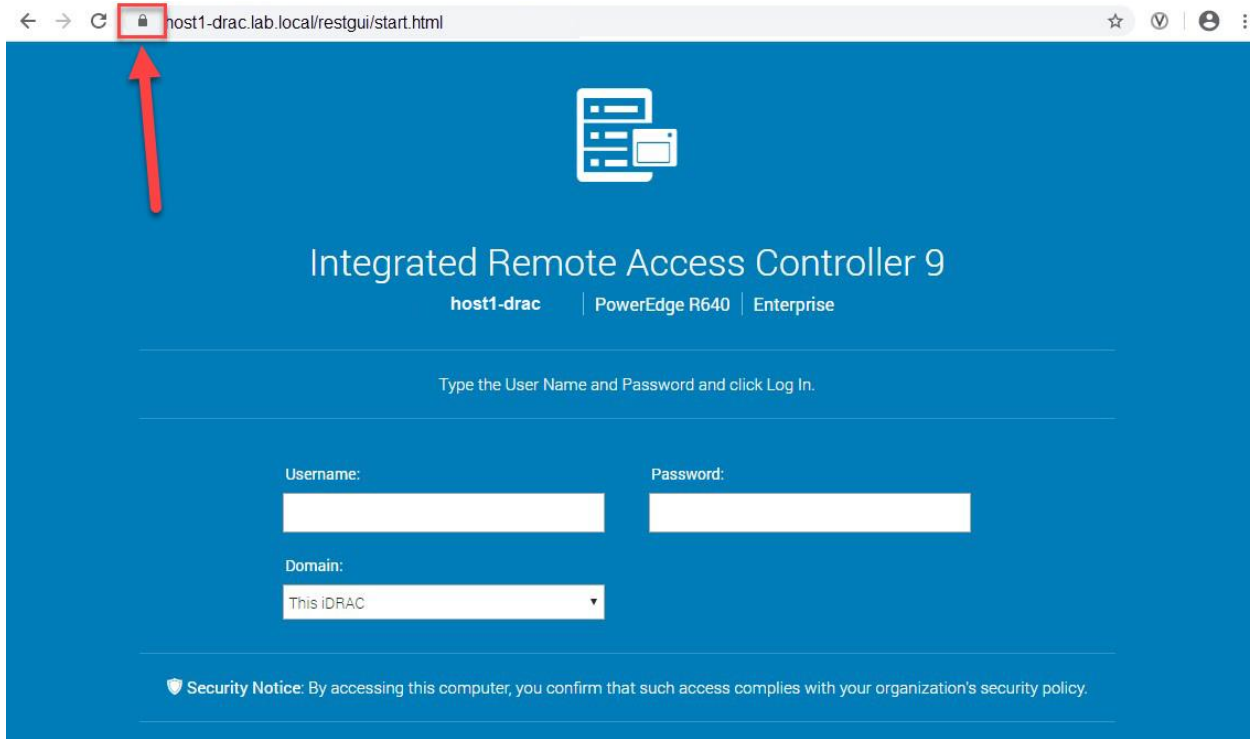


- Click "Reset iDRAC".



iDRAC Configuration and Maintenance

- After the iDRAC has reset the Web UI page should have the padlock and no longer show a “Not Secure”.



iDRAC Configuration and Maintenance

Configuring iDRAC Settings Using IPMITool

Prerequisite

The appliance must have the ipmitool installed (**yum install ipmitool**) and is orchestrated, this will not work from a NetWitness Base image without having the intended service installed (orchestrated).

User Management

Listing User Accounts

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool user list [1/2]

Example:

[root@node0 ~]# ipmitool user list 1

<i>ID</i>	<i>Name</i>	<i>Callin</i>	<i>Link Auth</i>	<i>IPMI Msg</i>	<i>Channel Priv Limit</i>
1		true	false	false	NO ACCESS
2	root	true	false	false	ADMINISTRATOR
3		true	false	false	NO ACCESS
4		true	false	false	NO ACCESS
5		true	false	false	NO ACCESS
6		true	false	false	NO ACCESS
7		true	false	false	NO ACCESS
8		true	false	false	NO ACCESS
9		true	false	false	NO ACCESS
10		true	false	false	NO ACCESS
11		true	false	false	NO ACCESS
12		true	false	false	NO ACCESS
13		true	false	false	NO ACCESS
14		true	false	false	NO ACCESS
15		true	false	false	NO ACCESS
16		true	false	false	NO ACCESS

iDRAC Configuration and Maintenance

Changing Username

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool set name <user id> <NewUserName>

Example:

```
[root@node0 ~]# ipmitool set name 2 not-root
```

```
[root@node0 ~]# ipmitool user list 1
```

ID	Name	Callin	Link Auth	IPMI Msg	Channel Priv Limit
1		true	false	false	NO ACCESS
2	not-root	true	false	false	ADMINISTRATOR
3		true	false	false	NO ACCESS
4		true	false	false	NO ACCESS
5		true	false	false	NO ACCESS
6		true	false	false	NO ACCESS
7		true	false	false	NO ACCESS
8		true	false	false	NO ACCESS
9		true	false	false	NO ACCESS
10		true	false	false	NO ACCESS
11		true	false	false	NO ACCESS
12		true	false	false	NO ACCESS
13		true	false	false	NO ACCESS
14		true	false	false	NO ACCESS
15		true	false	false	NO ACCESS
16		true	false	false	NO ACCESS

Changing User Password

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool set password <user id> <password>

Example:

```
[root@node0 ~]# ipmitool set password 2 "NOTthem@st3r01"
```

Enable User Account

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool enable <user id>

Example:

```
[root@node0 ~]# ipmitool enable 2
```

iDRAC Configuration and Maintenance

Disable User Account

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool disable <user id>

Example:

[root@node0 ~]# ipmitool disable 2

Test User Credentials

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool user test <user id> <16|20> [<password>]

Example:

[root@node0 ~]# ipmitool user test 2 20 <Press Enter>

Password for user 2:<Type Password Here><Press Enter>

[Success | Failure: password incorrect]

List Available Commands for User Management

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool user

Example:

[root@node0 ~]# ipmitool user

Not enough parameters given.

User Commands:

```
summary      [<channel number>]
list         [<channel number>]
set name     <user id> <username>
set password <user id> [<password> <16|20>]
disable     <user id>
enable      <user id>
priv        <user id> <privilege level> [<channel number>]
```

Privilege levels:

- * 0x1 - Callback
- * 0x2 - User
- * 0x3 - Operator
- * 0x4 - Administrator
- * 0x5 - OEM Proprietary
- * 0xF - No Access

```
test      <user id> <16|20> [<password>]
```

iDRAC Configuration and Maintenance

Network Configuration Management

Listing IP Address

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following command:

ipmitool lan print

Example:

[root@node0 ~]# ipmitool lan print

```

Set in Progress           : Set Complete
Auth Type Support         : MD5
Auth Type Enable          : Callback : MD5
                          : User    : MD5
                          : Operator : MD5
                          : Admin  : MD5
                          : OEM    :
IP Address Source         : Static Address
IP Address                 : 192.168.0.120
Subnet Mask                : 255.255.255.0
MAC Address                : f4:00:00:00:00:00
SNMP Community String     : public
IP Header                  : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control           : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl     : 2.0 seconds
Default Gateway IP         : 192.168.0.1
Default Gateway MAC        : 00:00:00:00:00:00
Backup Gateway IP         : 0.0.0.0
Backup Gateway MAC        : 00:00:00:00:00:00
802.1q VLAN ID            : Disabled
802.1q VLAN Priority       : 0
RMCP+ Cipher Suites       : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14
Cipher Suite Priv Max     : Xaaaaaaaaaaaaa
Bad Password Threshold     : Not Available
  
```

iDRAC Configuration and Maintenance

Changing IP Address

1. Login to the system using for SSH client of choice, like PuTTY.
2. Type the following commands:

```
ipmitool lan set 1 ipsrc [static/dhcp/bios]
ipmitool lan set 1 ipaddr <xxx.xxx.xxx.xxx>
ipmitool lan set 1 netmask <xxx.xxx.xxx.xxx>
ipmitool lan set 1 defgw ipaddr <xxx.xxx.xxx.xxx>
ipmitool mc reset [warm/cold]
```

Example:

```
[root@node0 ~]# ipmitool lan set 1 ipsrc static
[root@node0 ~]# ipmitool lan set 1 ipaddr 10.0.0.100
[root@node0 ~]# ipmitool lan set 1 netmask 255.255.255.0
[root@node0 ~]# ipmitool lan set 1 defgw ipaddr 10.0.0.1
[root@node0 ~]# ipmitool lan print
```

```
Set in Progress           : Set Complete
Auth Type Support         : MD5
Auth Type Enable         : Callback : MD5
                          : User      : MD5
                          : Operator : MD5
                          : Admin    : MD5
                          : OEM      :
IP Address Source        : Static Address
IP Address                : 10.0.0.100
Subnet Mask               : 255.255.255.0
MAC Address              : f4:00:00:00:00:00
SNMP Community String    : public
IP Header                : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control          : ARP Responses Enabled, Gratuitous ARP Disabled
Gratuitous ARP Intrvl    : 2.0 seconds
Default Gateway IP       : 10.0.0.1
Default Gateway MAC      : 00:00:00:00:00:00
Backup Gateway IP        : 0.0.0.0
Backup Gateway MAC       : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority     : 0
RMCP+ Cipher Suites     : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14
Cipher Suite Priv Max    : Xaaaaaaaaaaaaaaaa
Bad Password Threshold   : Not Available
```

```
[root@node0 ~]# ipmitool mc reset cold
```