RSA NETWITNESS® PLATFORM

iDRAC
Configuration and Maintenance

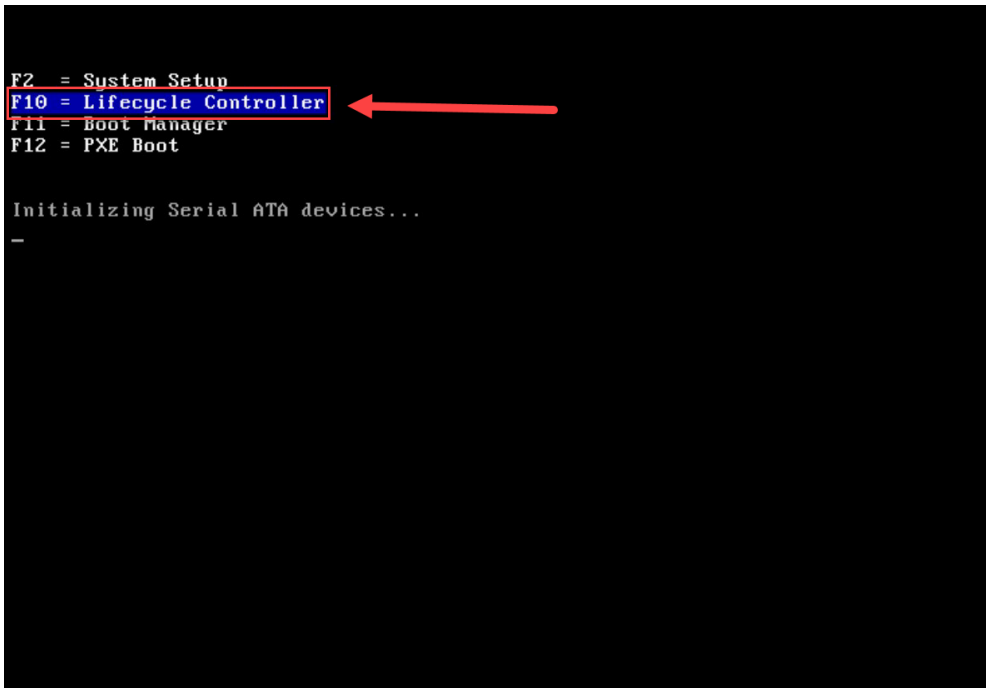
iDRAC Configuration and Maintenance

Table of Contents

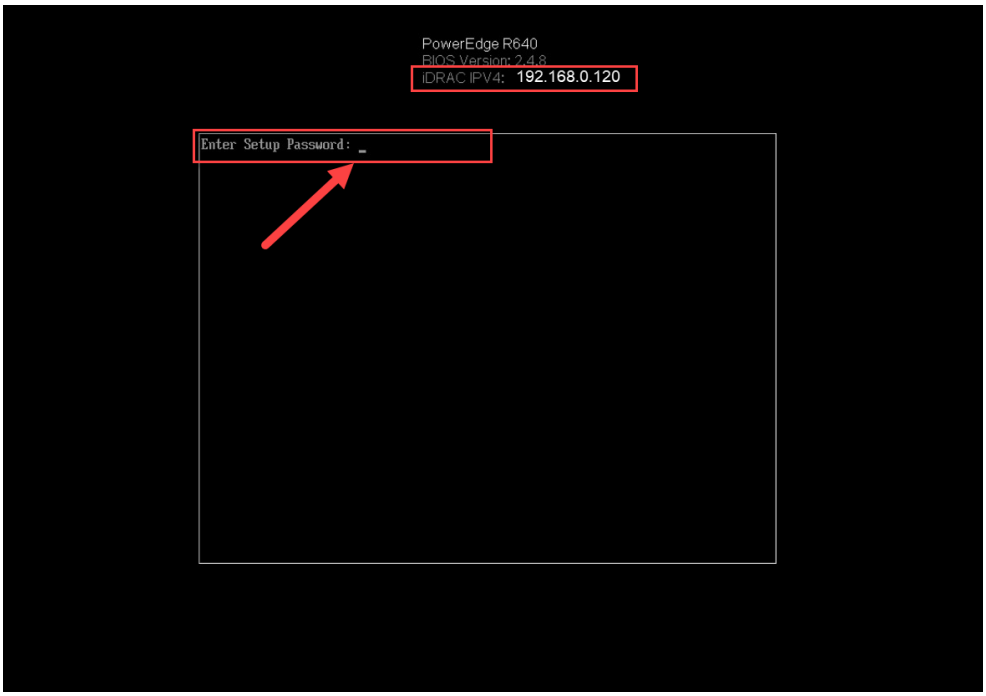
Setting IP Address First Time

Console via Crash Cart

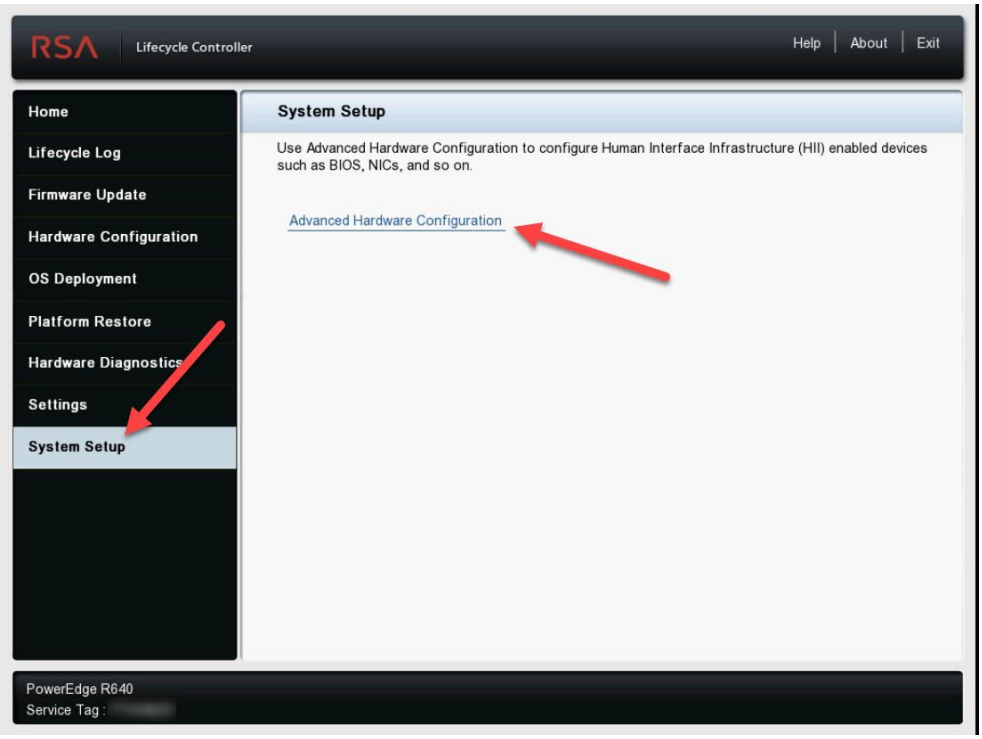
1. Power on the system and Press “F10” to access the iDRAC.



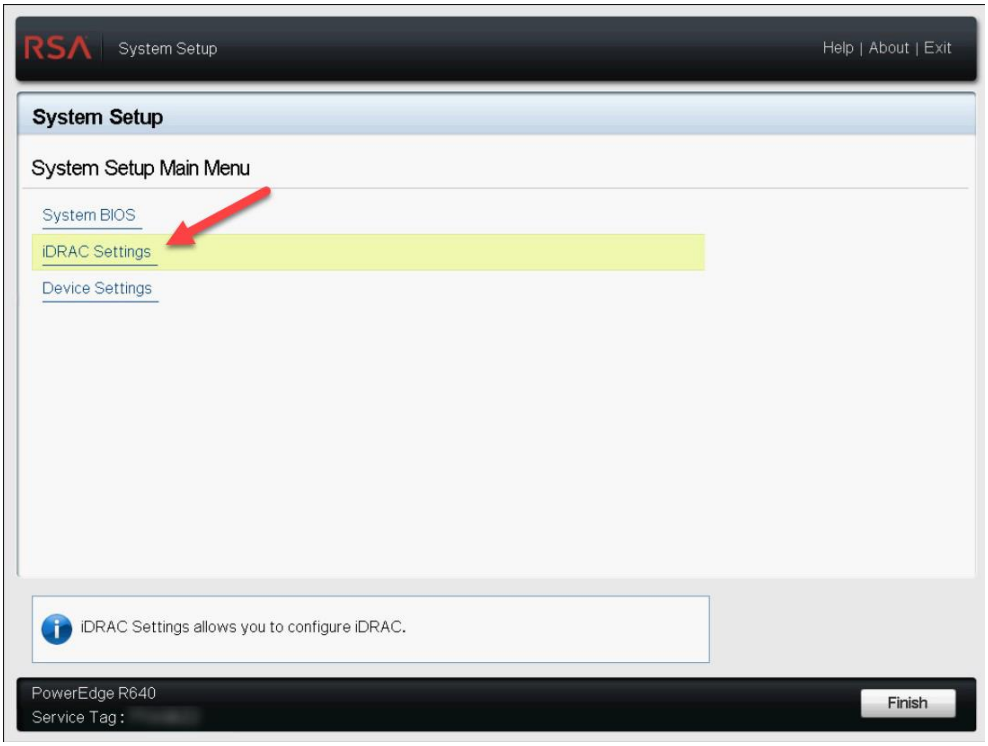
2. Enter the “Setup Password” of “***rsabios***”



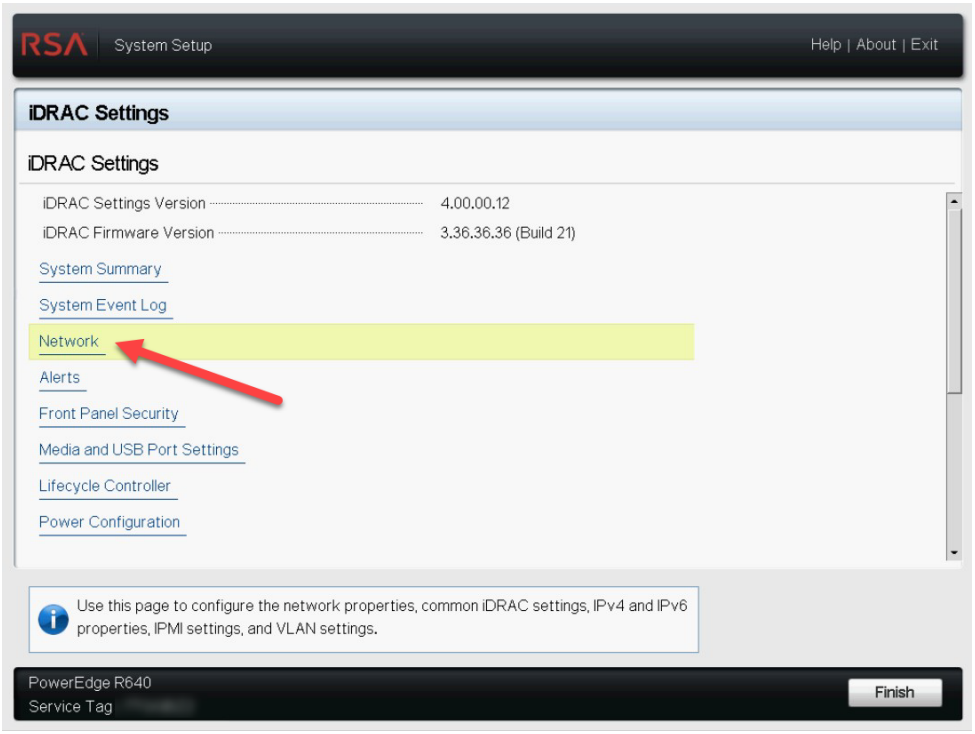
3. Click on “System Setup”, then “Advanced Hardware Configuration”.



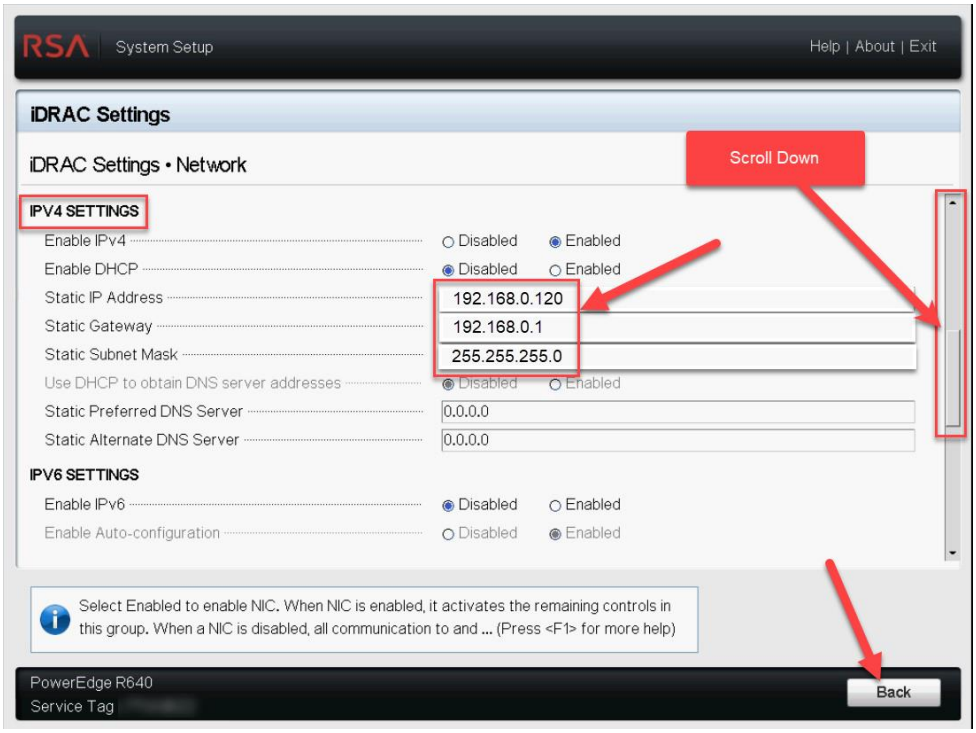
4. Click on “iDRAC Settings”.



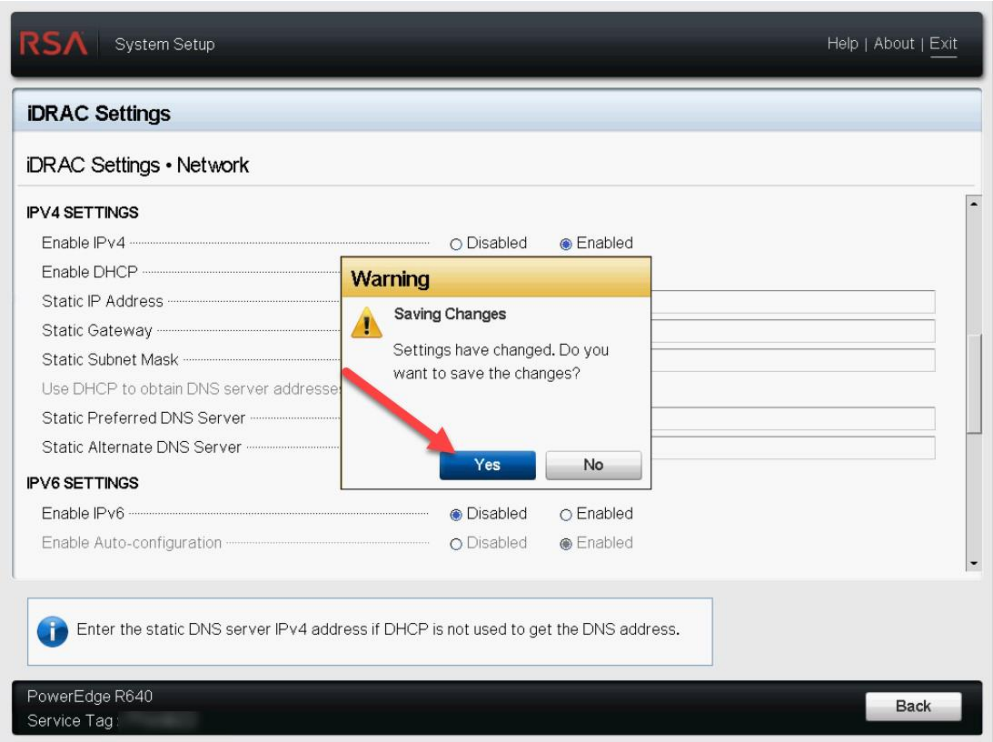
5. Click on “Network”.



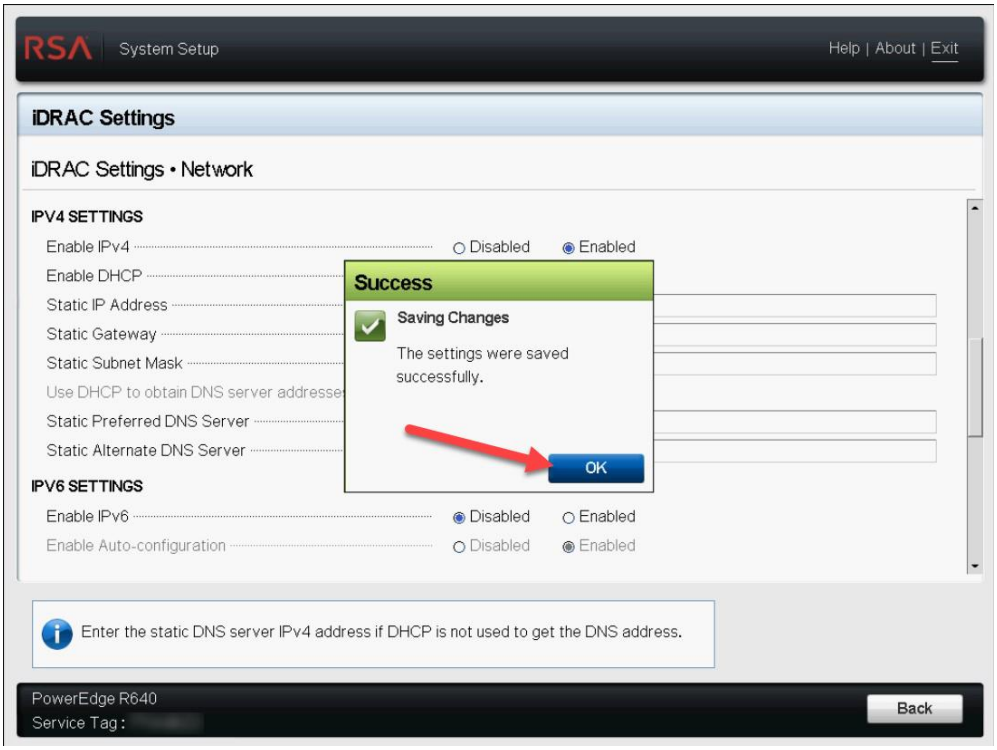
6. Scroll down to the IPV4 settings and enter your IP address information.



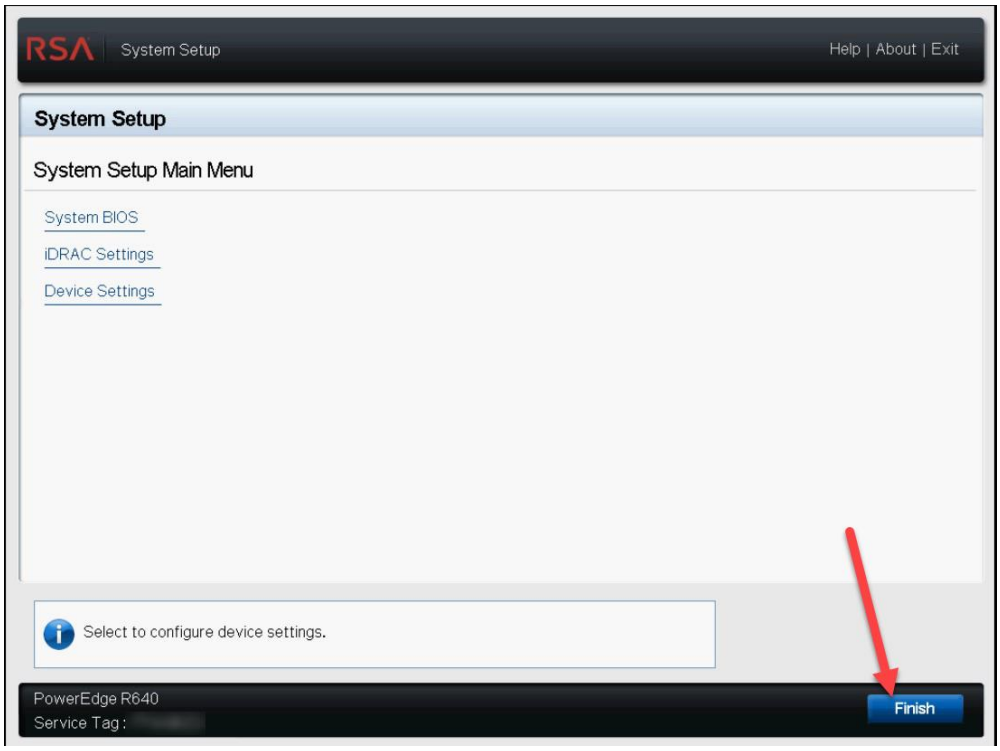
7. Click “Yes”.



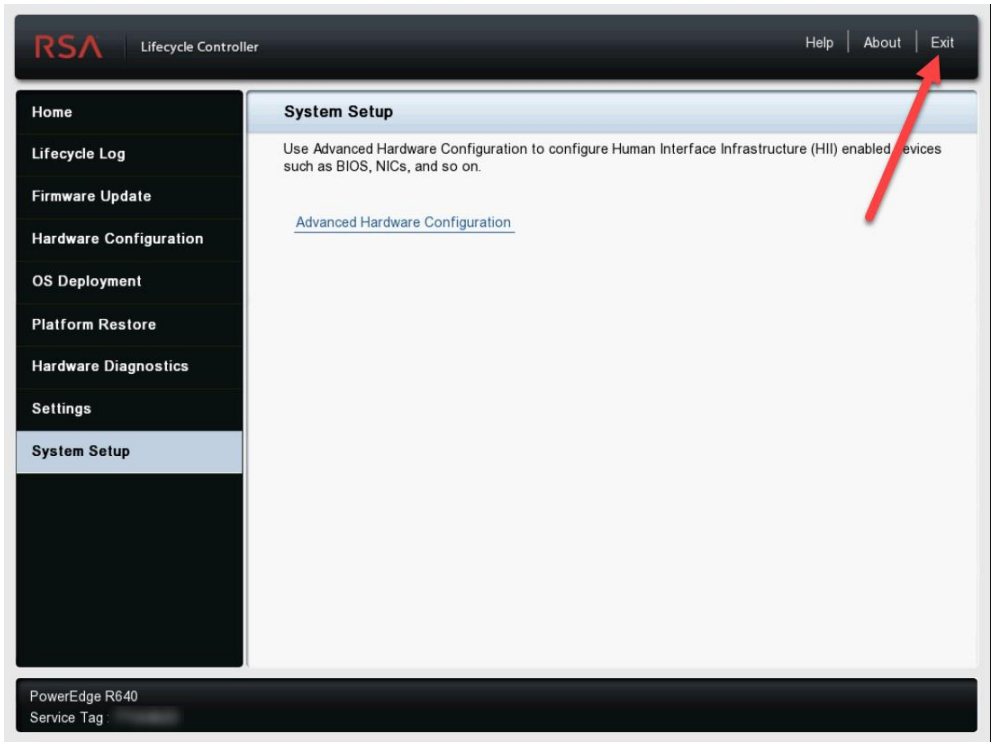
8. Click “OK”.



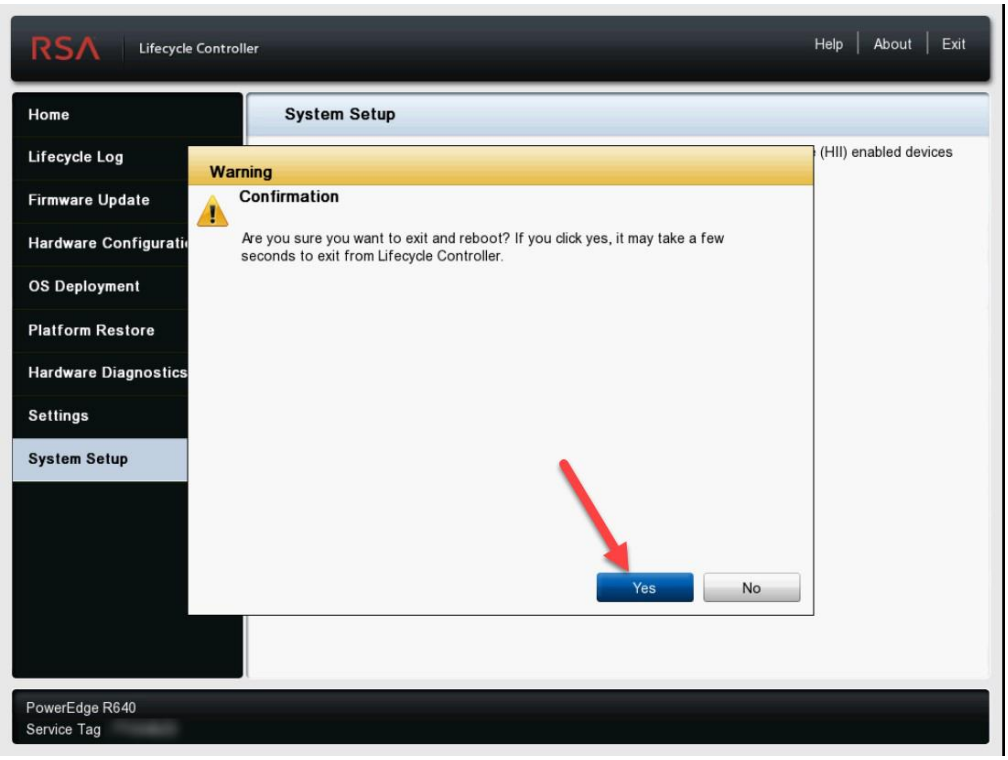
9. Click “Finish”.



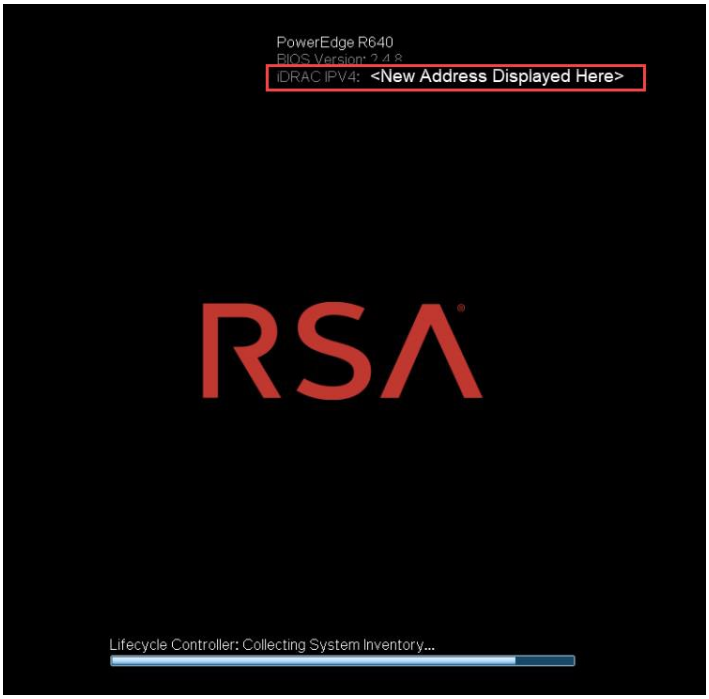
10. Click on “Exit”.



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



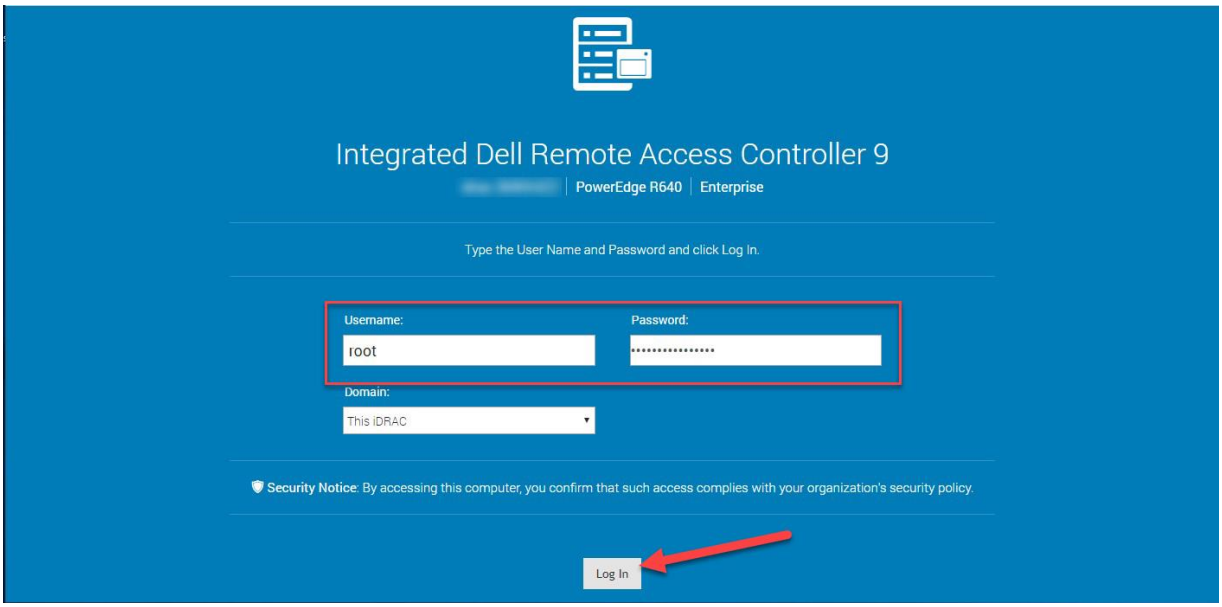
12. During the reboot the new iDRAC IP address will be displayed at the top of the screen.



Configuring iDRAC Settings Using Web UI

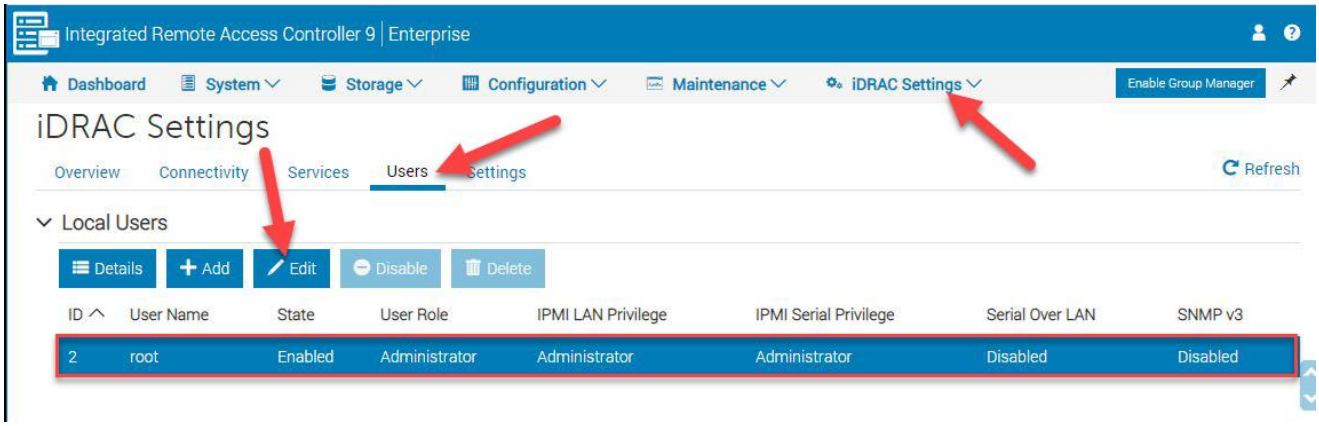
Logging in to Web UI

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".

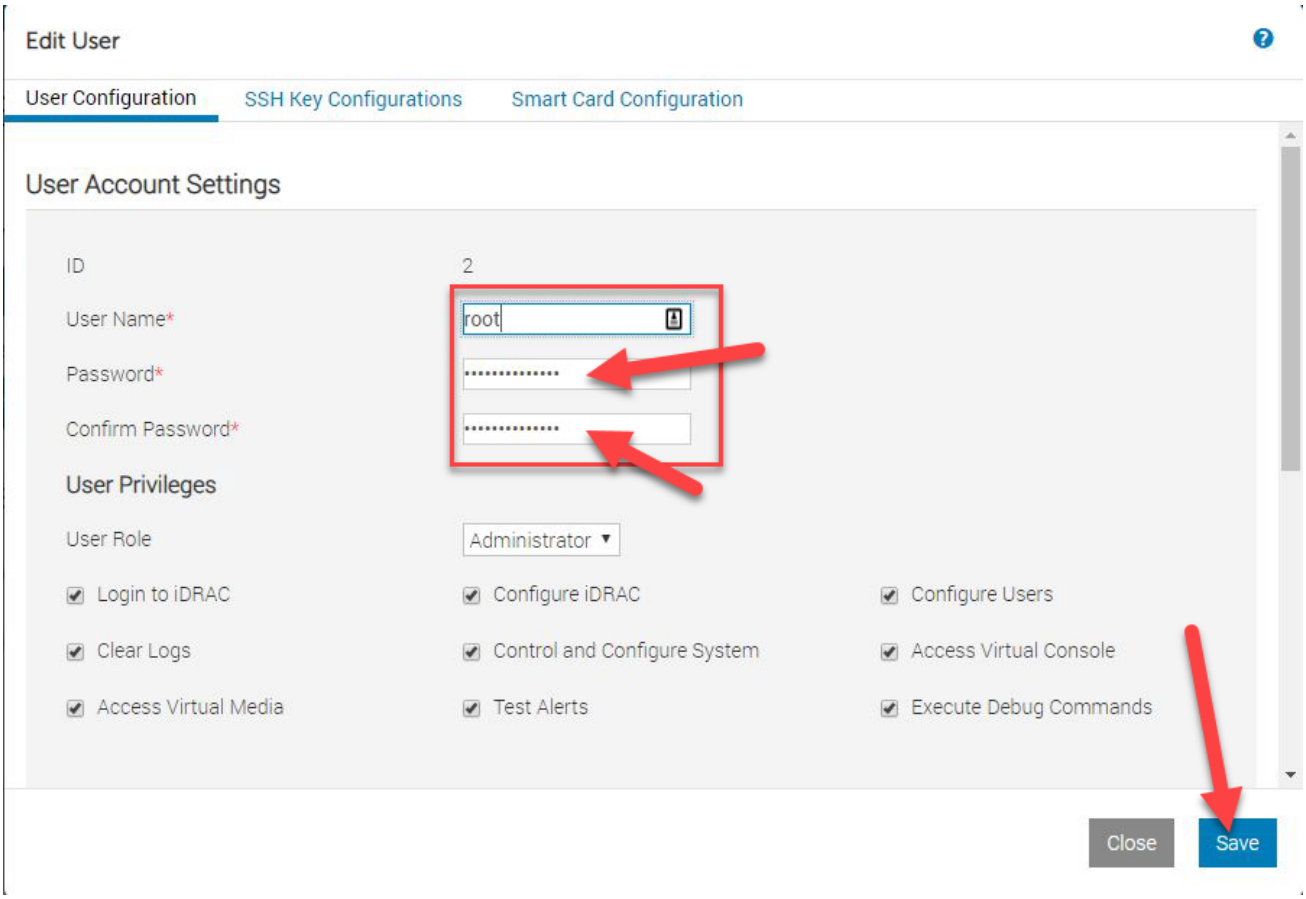


Changing User Password

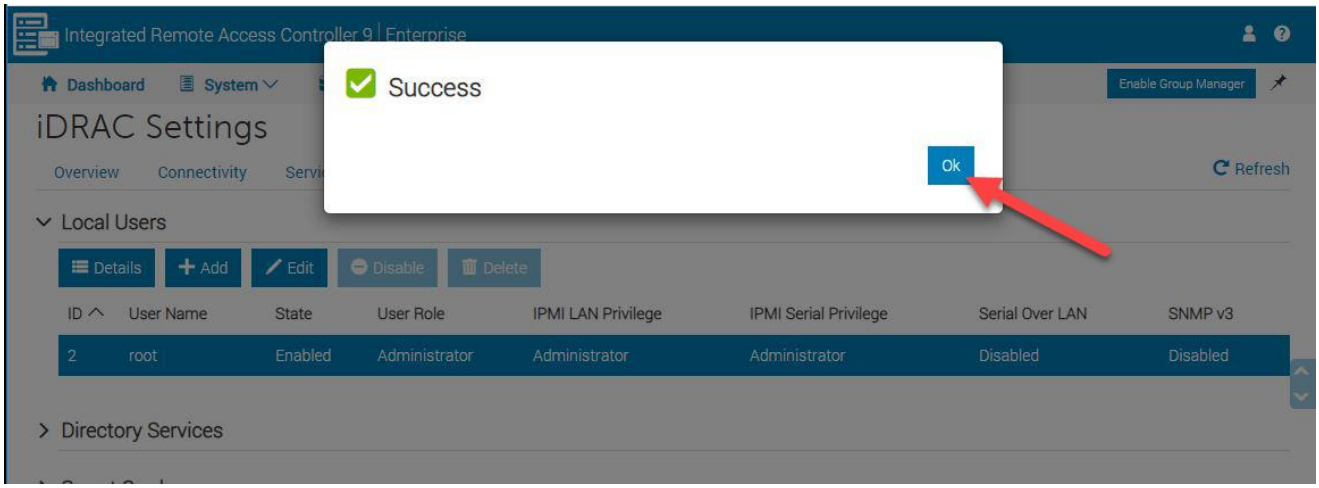
1. Navigate to "iDRAC Settings→Users", click on "Edit".



2. Type in password twice and click "Save".

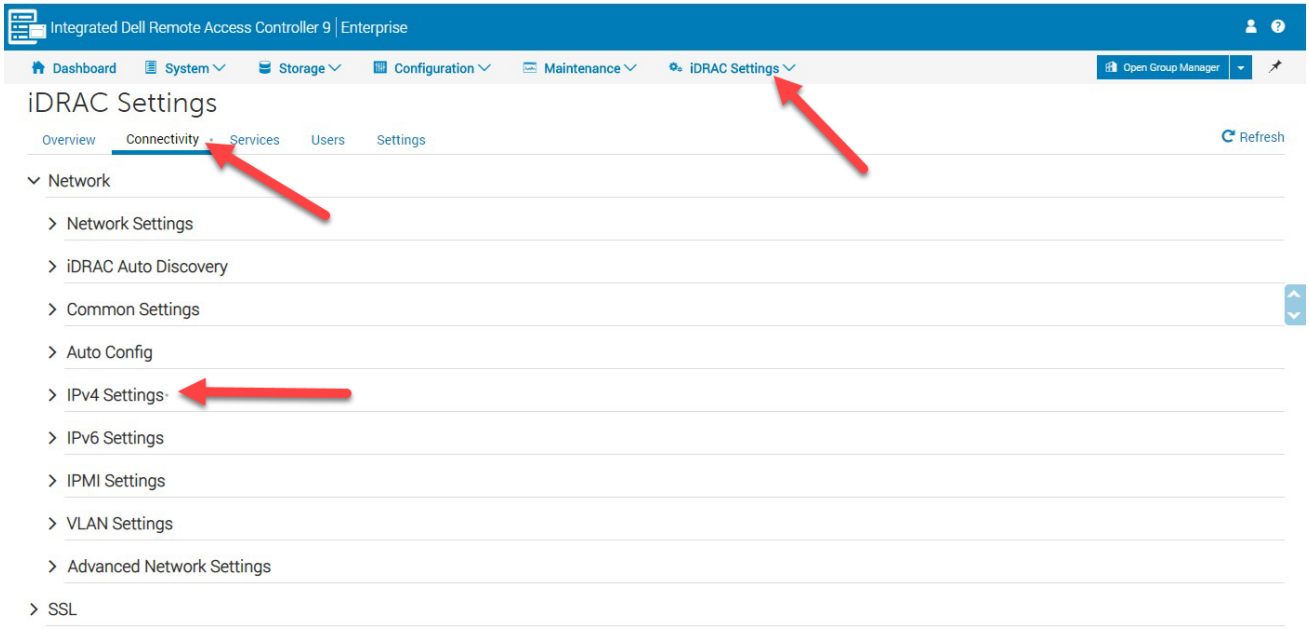


3. Click “Ok”.

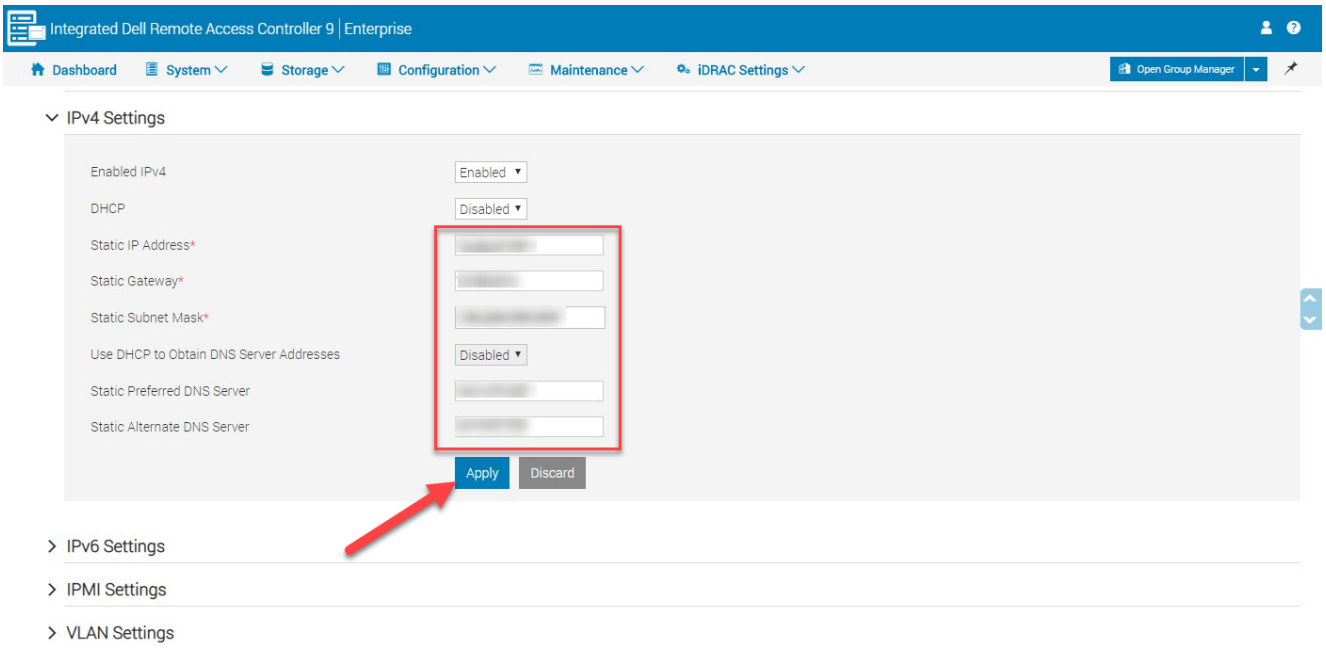


Changing IP V4 Settings

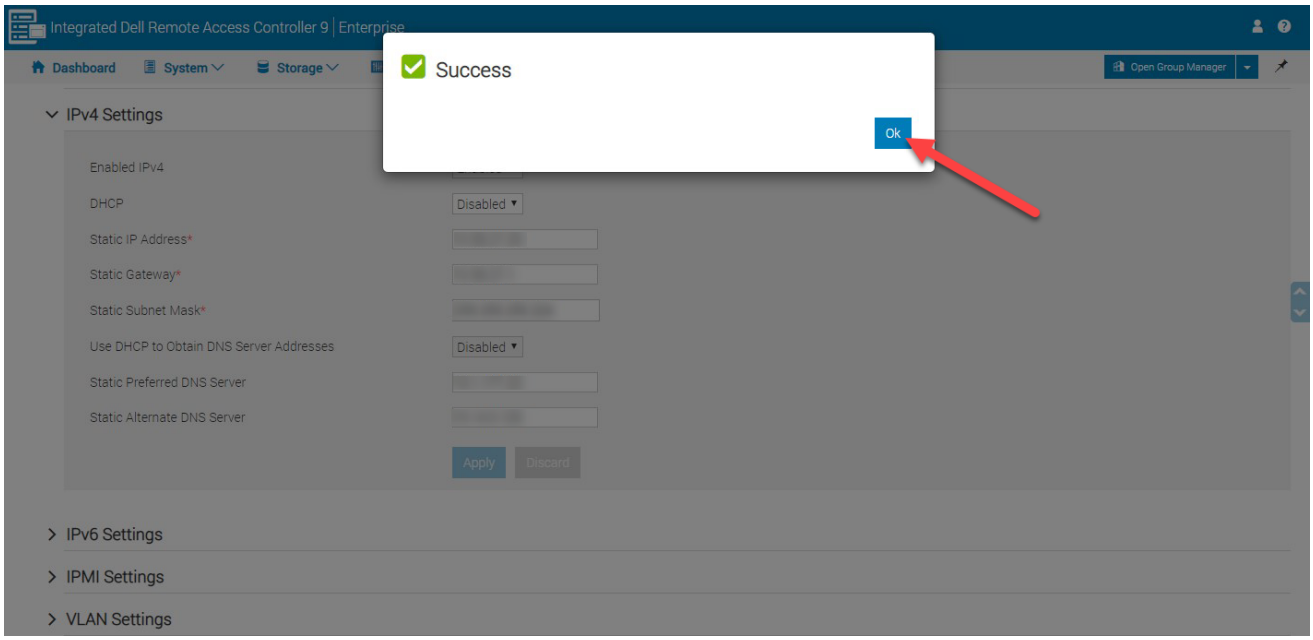
1. Click on “iDRAC Settings-->Connectivity→IPv4 Settings”.



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



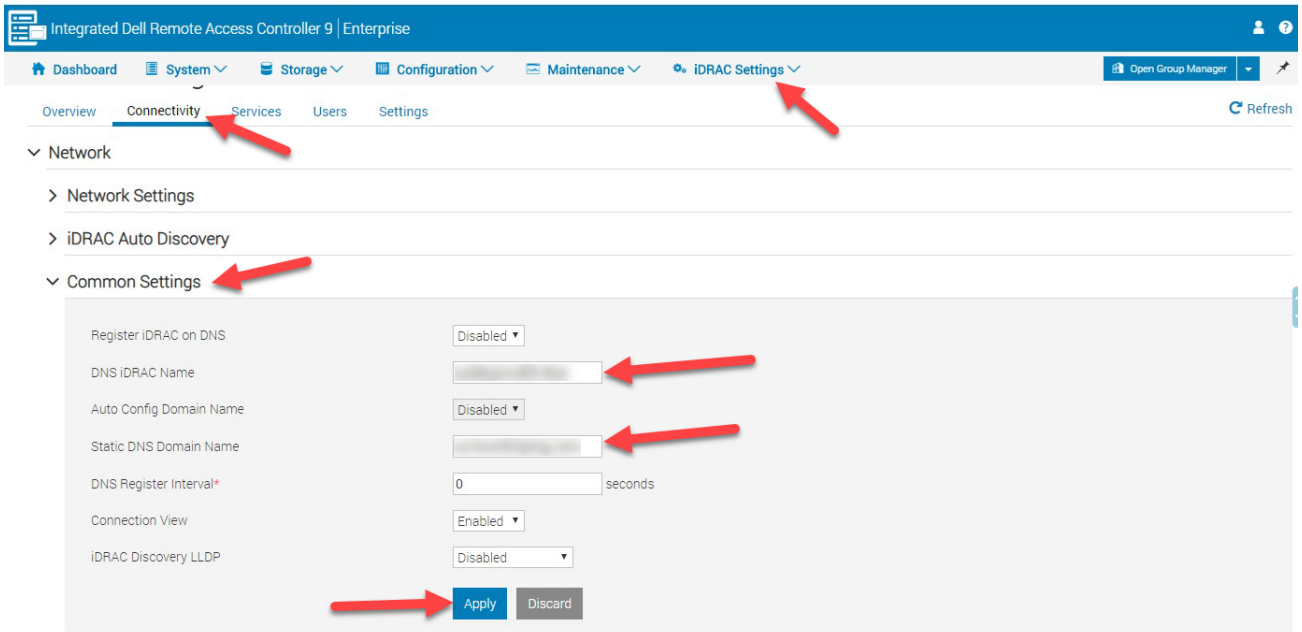
3. Click on “OK”.



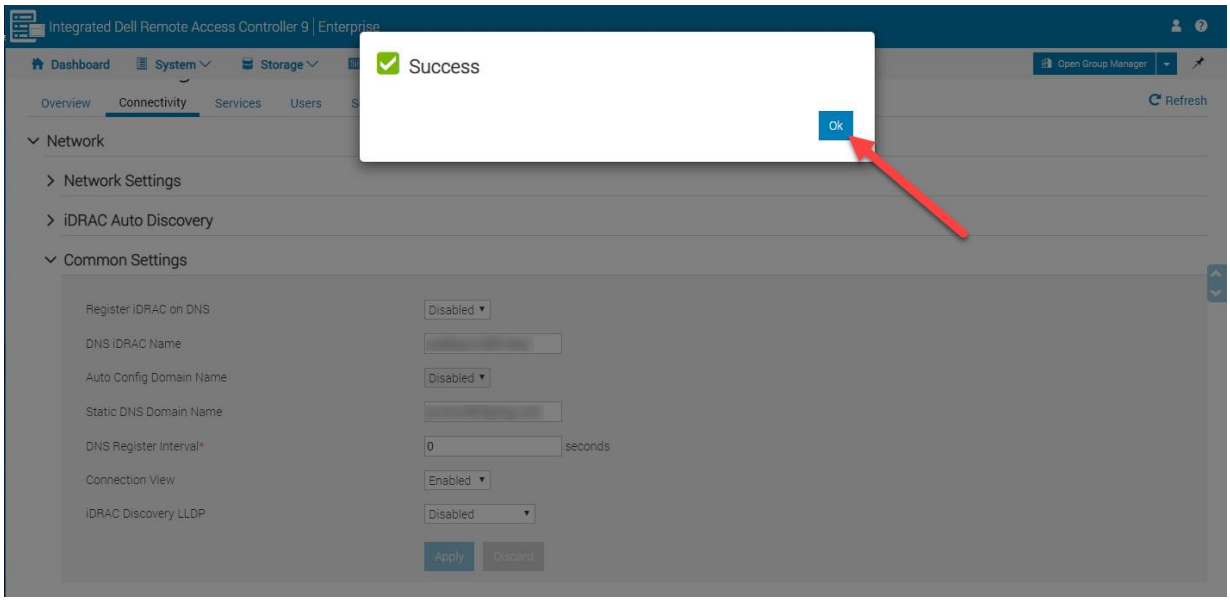
Setting iDRAC Name

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.

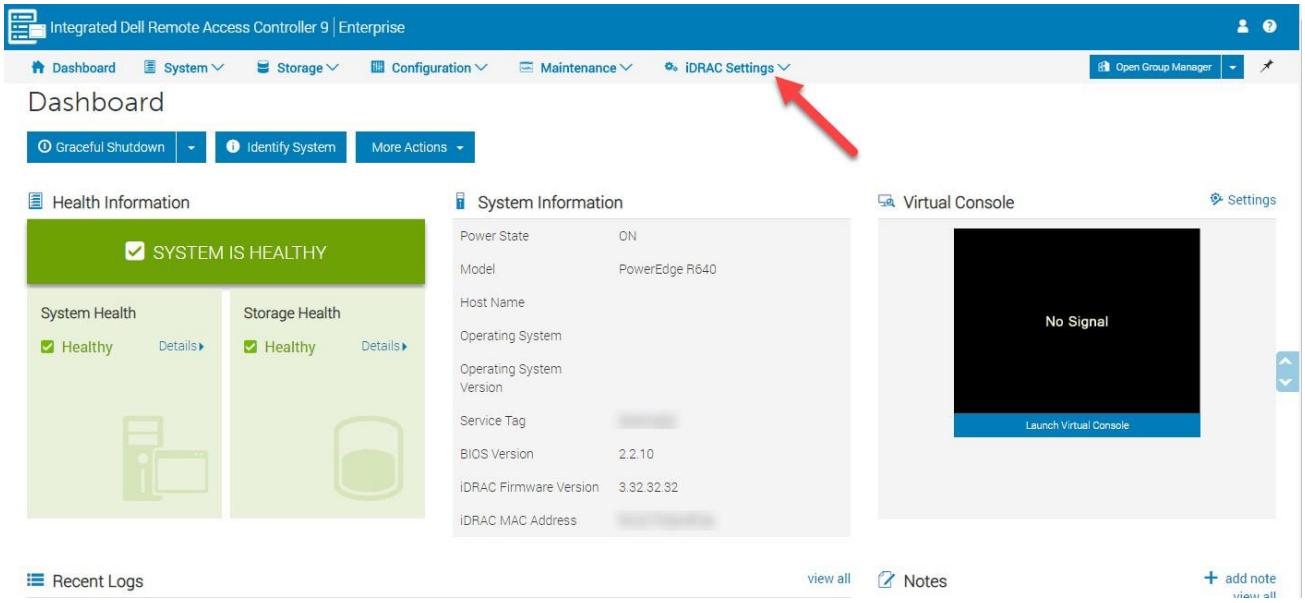


2. Click “Ok”.

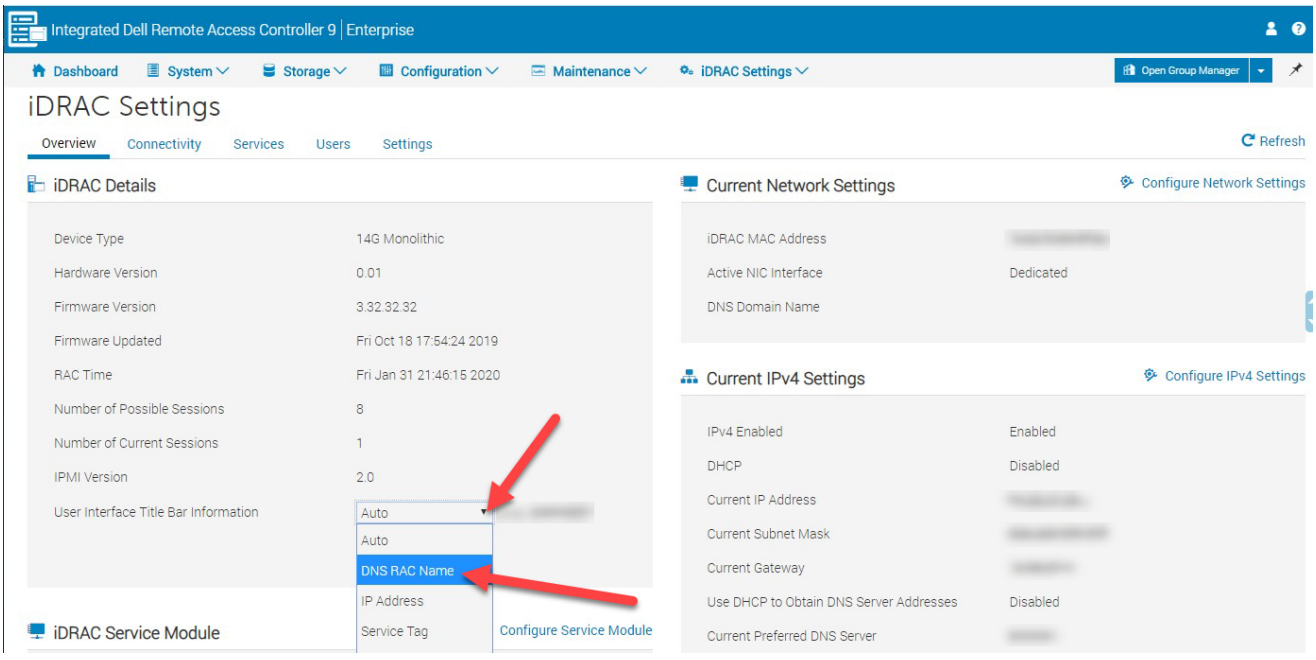


Changing Browser Tab Name

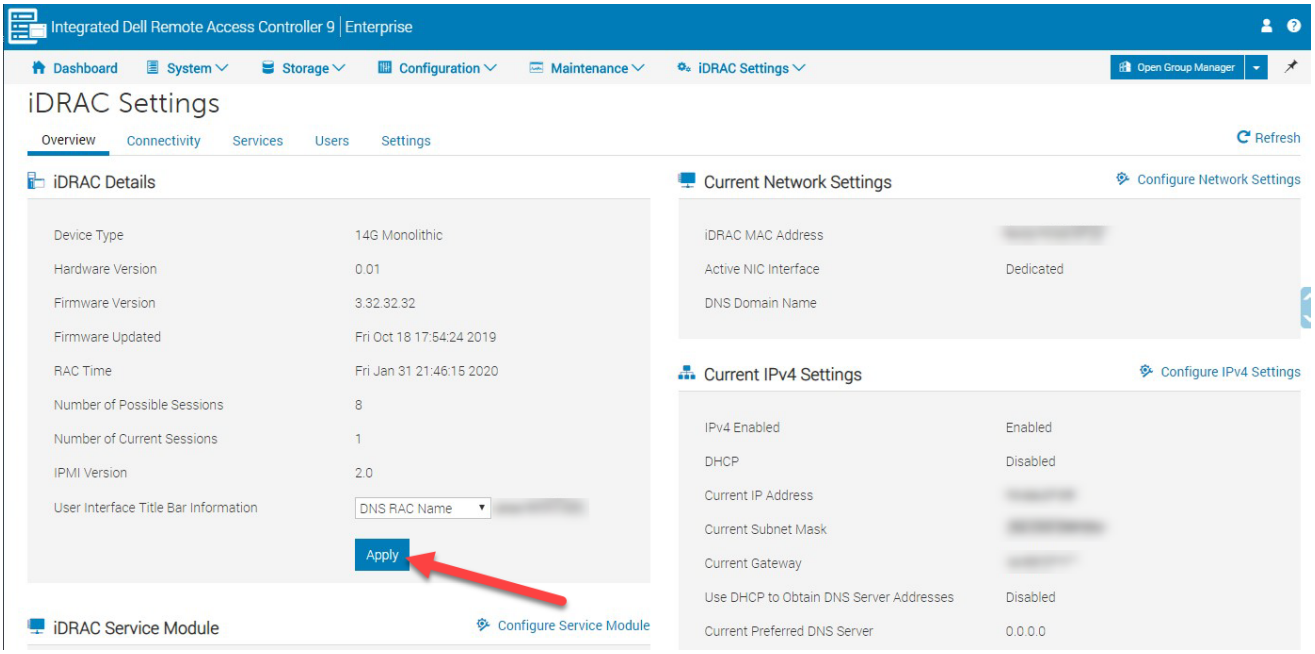
1. Click on “iDRAC Settings”.



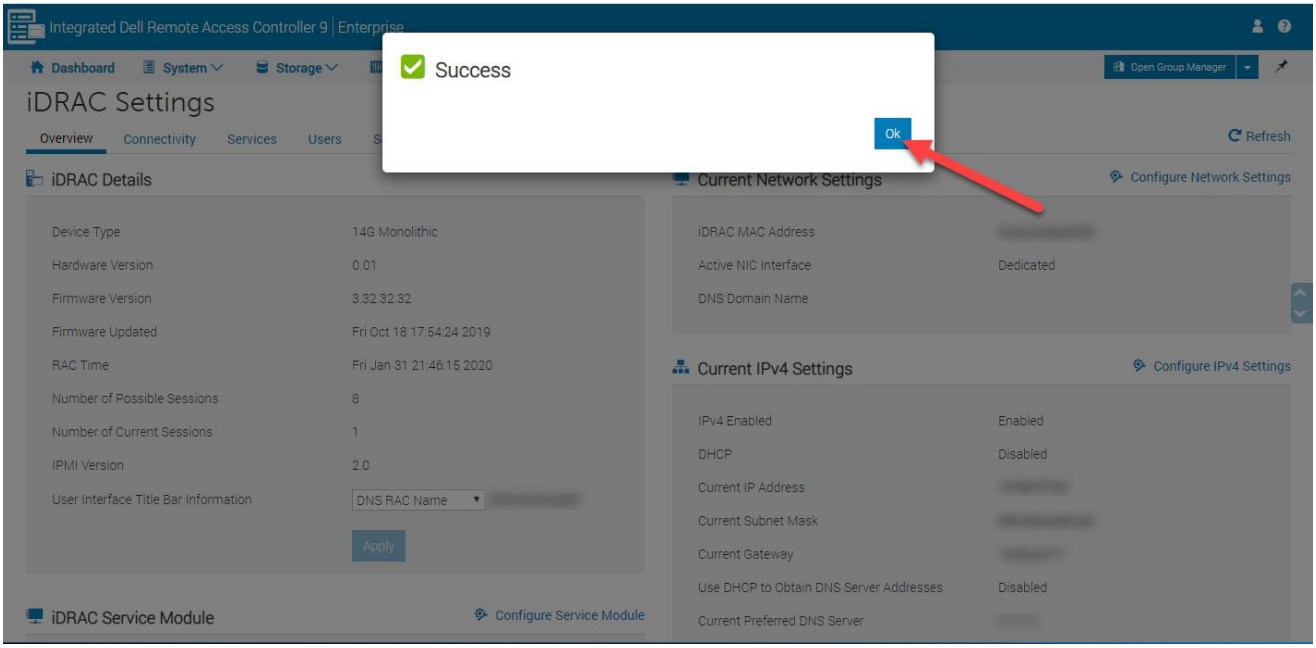
2. Change the “User interface Title Bar Information” to “DNS RAC Name”.



3. Click “Apply”.

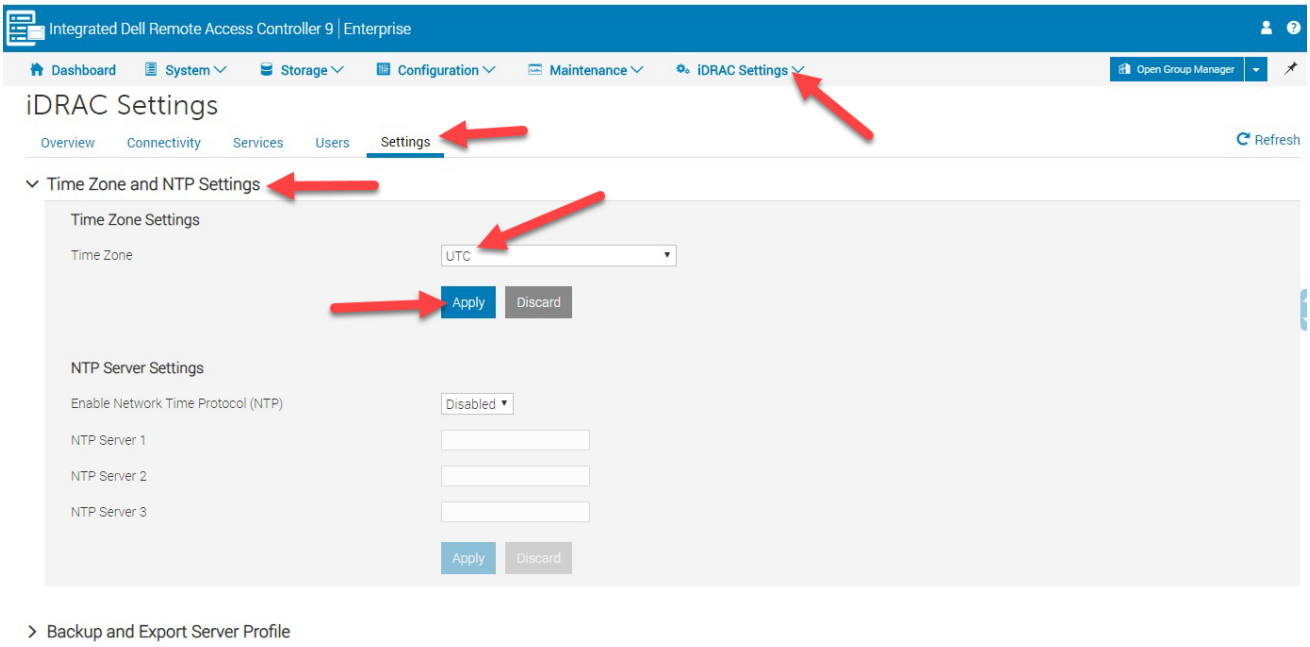


4. Click on “Ok”.

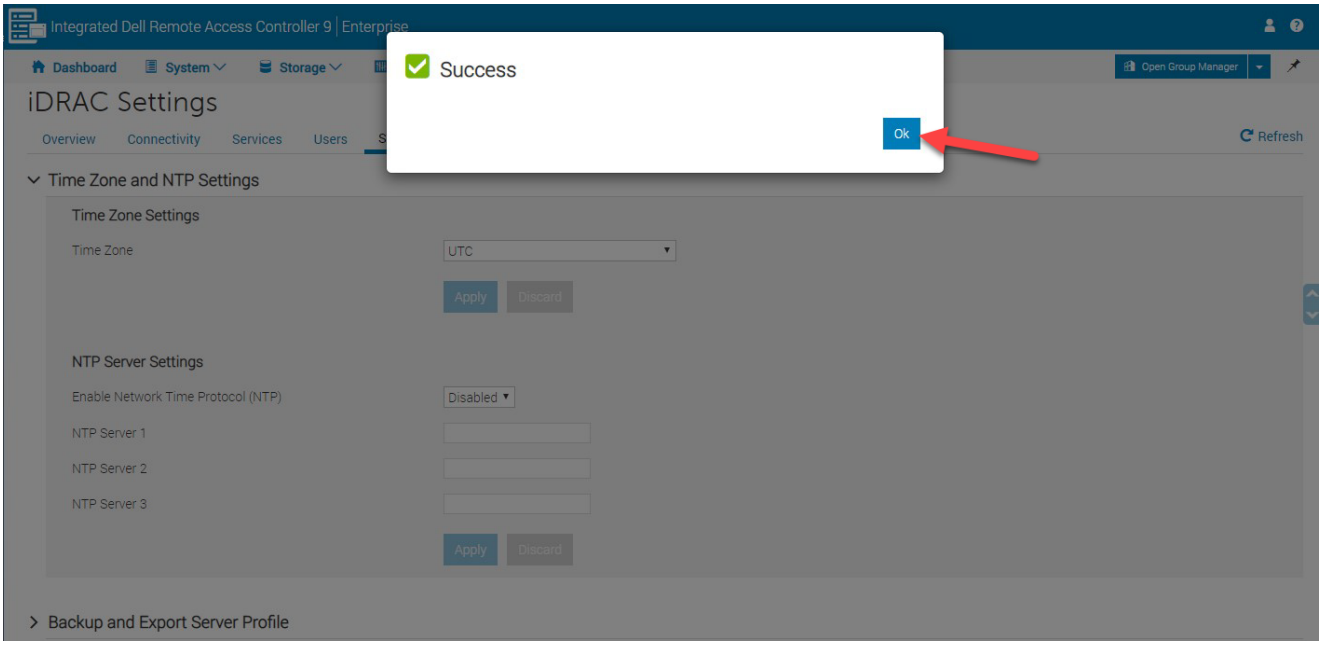


Changing Time Zone

1. Navigate to the "IDRAC Settings→Settings→Time Zone and NTP Settings". Change the "Time Zone" and click "Apply".

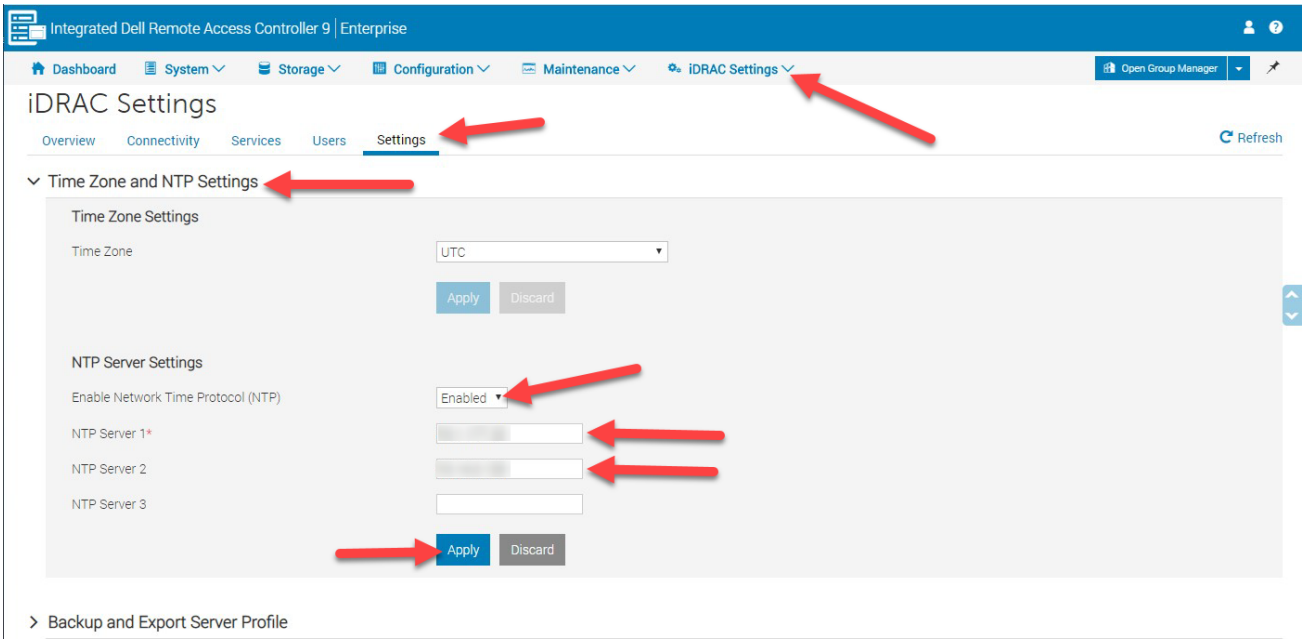


2. Click "Ok".

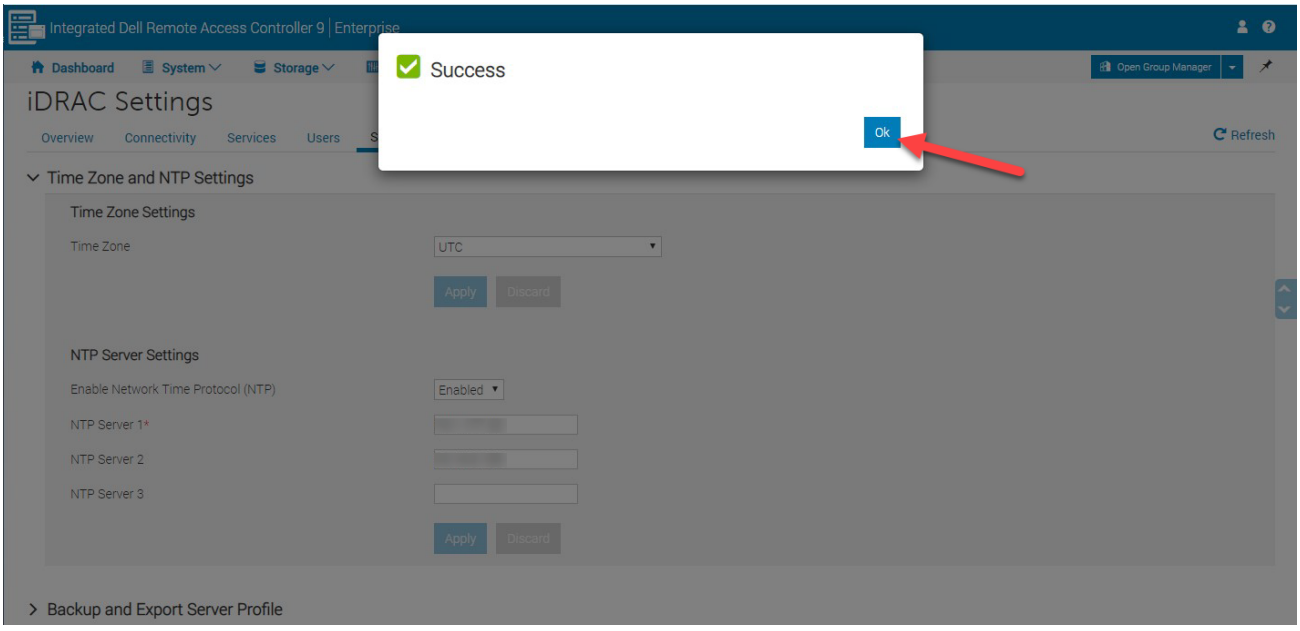


Enabling NTP

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".



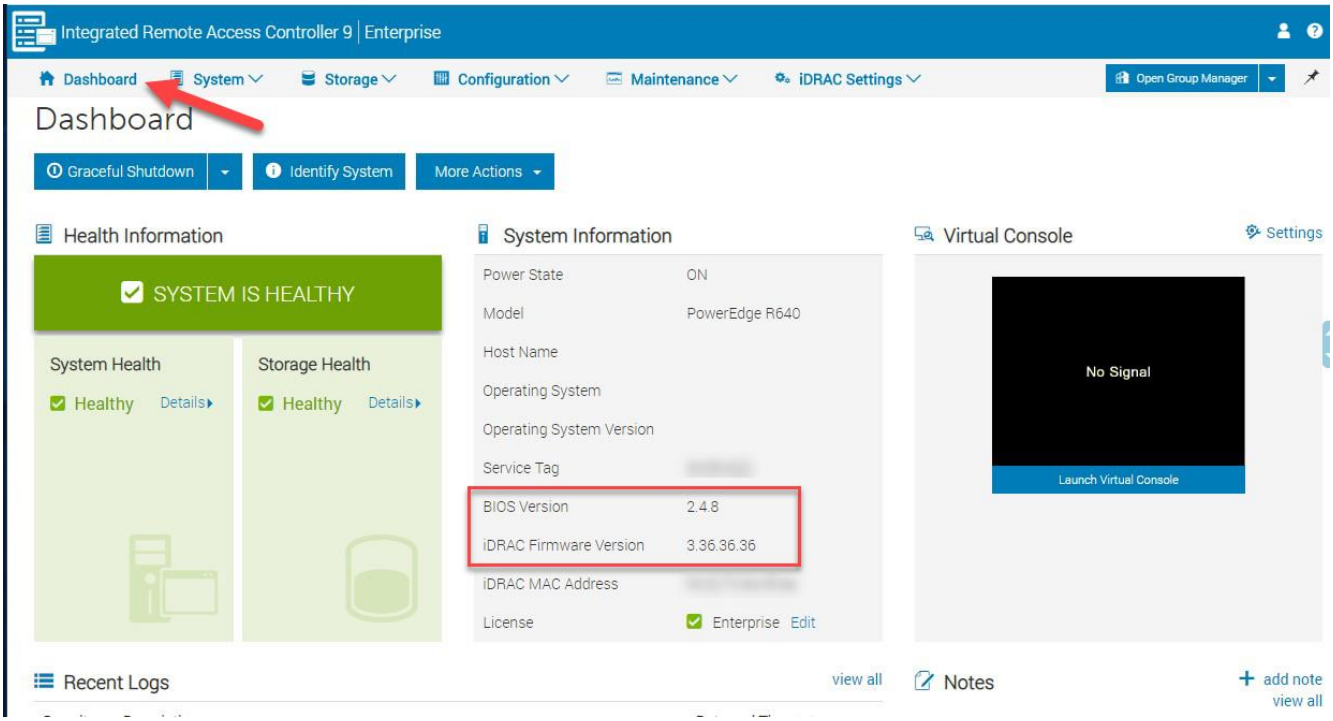
2. Click "Ok"



Maintenance

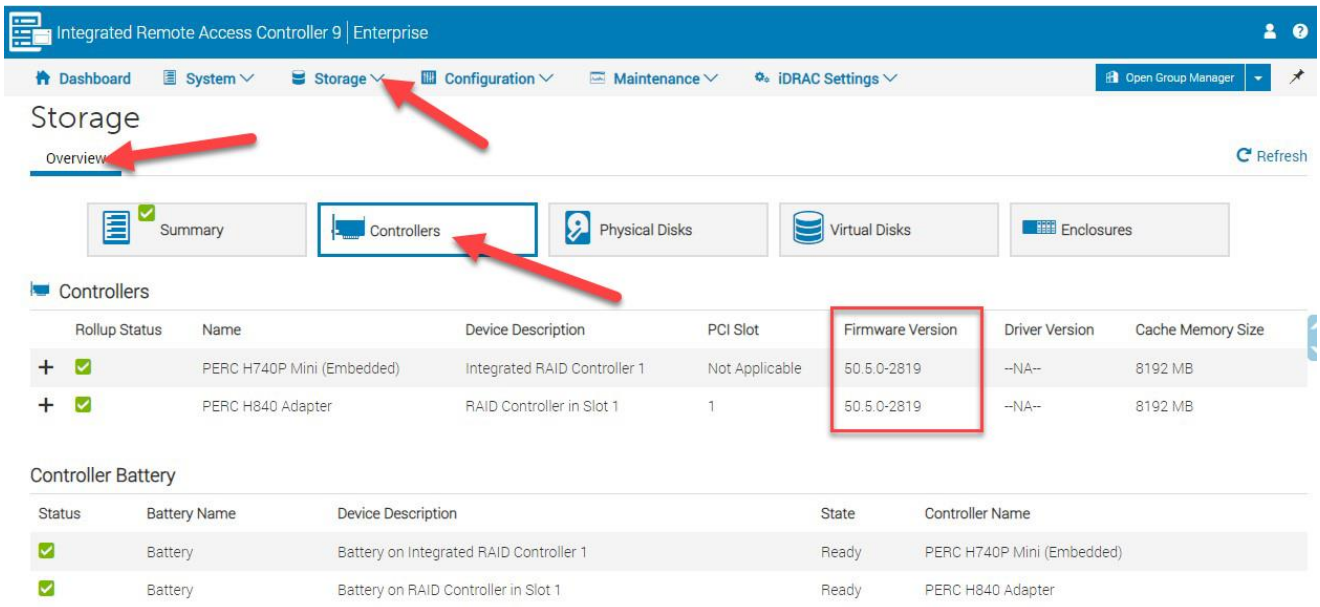
Checking iDRAC Firmware and System BIOS Versions

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



Checking iDRAC RAID Firmware Version

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



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 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.

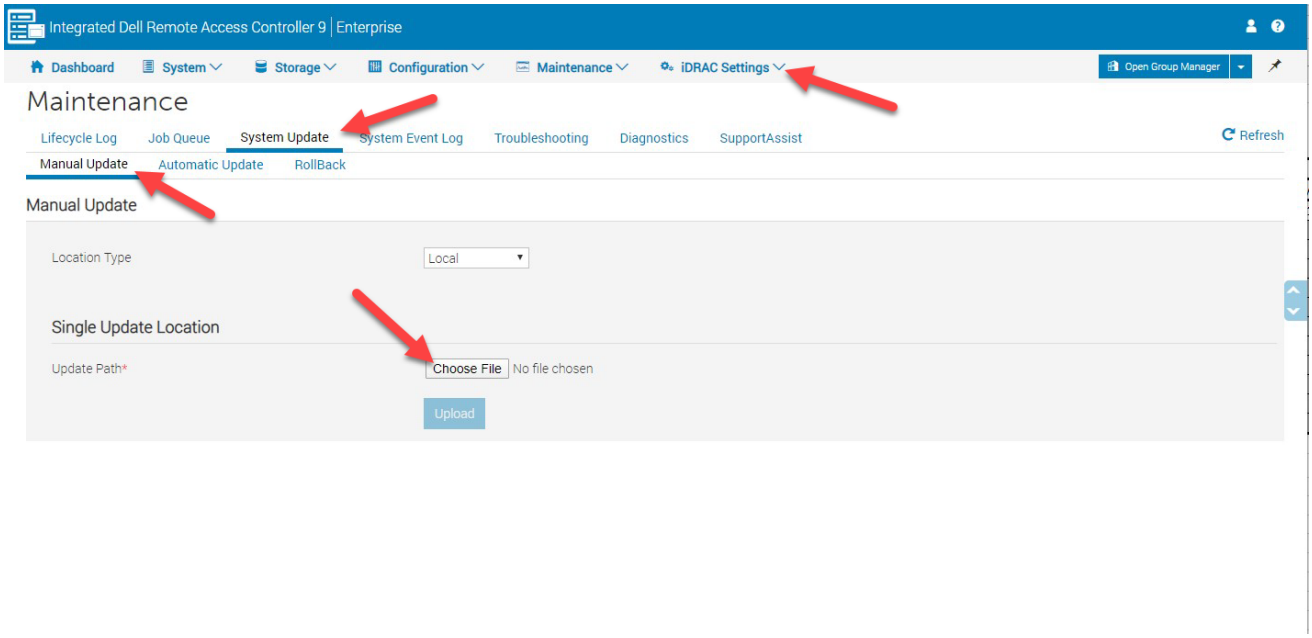
Important: Please use the following instructions for updating Series 4S, 5, and 6 and PowerVault firmware: http://www.dell.com/support/article/us/en/04/sln292363/poweredge-server-updating-firmware-through-the-idrac?lang=en#idrac78
PowerVault updates are performed through the iDRAC interface of the connected 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.

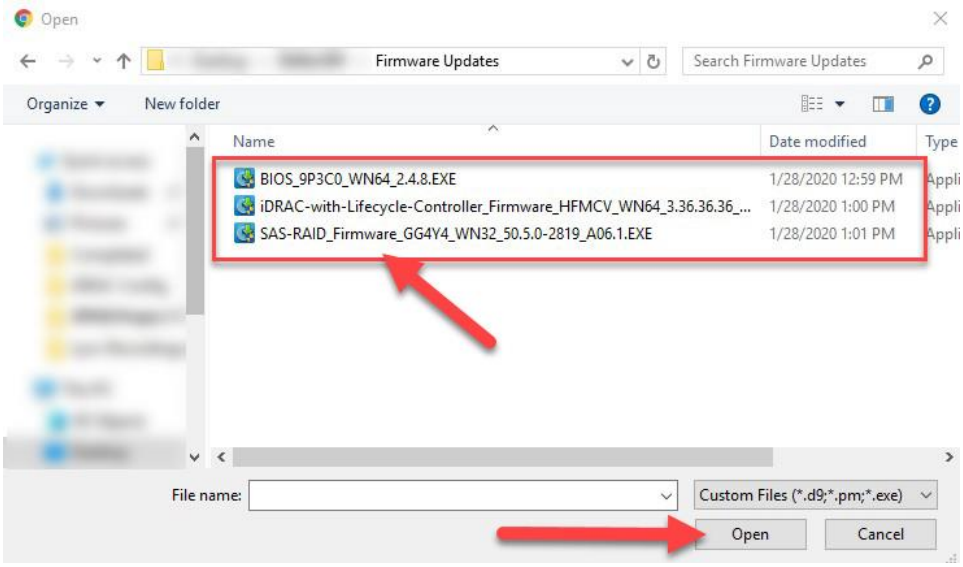
For S4, download the Update Package for Red Hat Linux and perform the update via the Operating System

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	

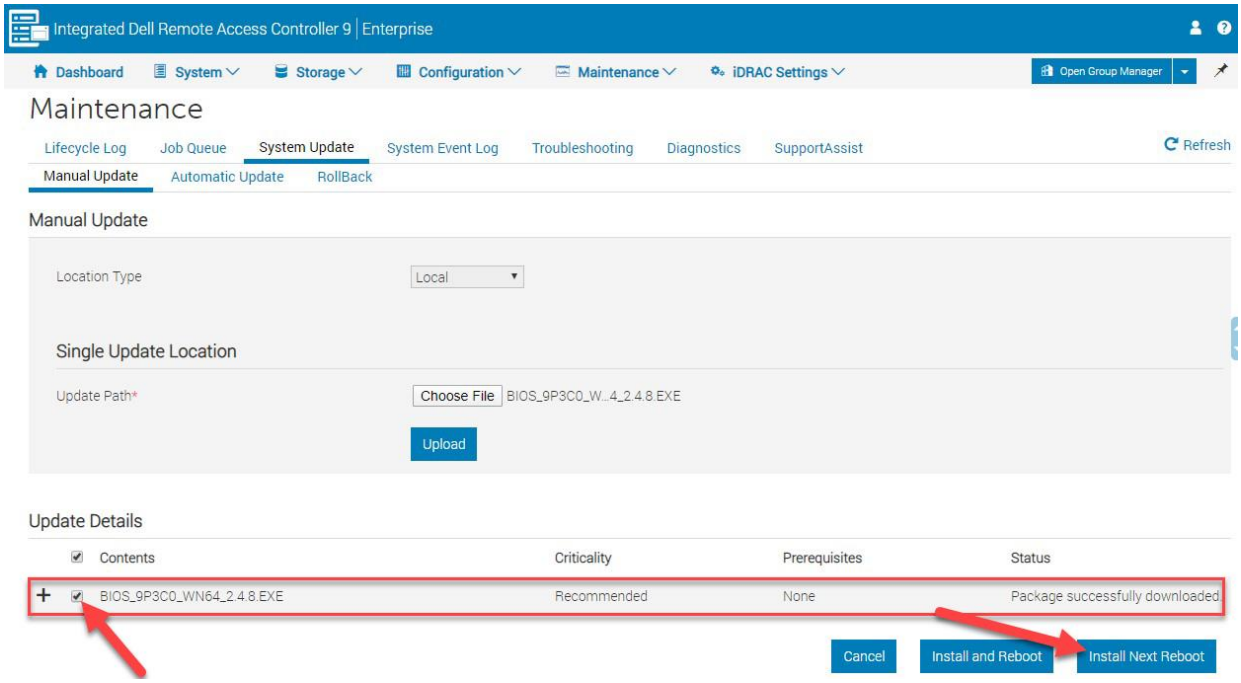
2. Navigate to the “iDRAC Settings→System Update→Manual Update” and click “Choose File”.



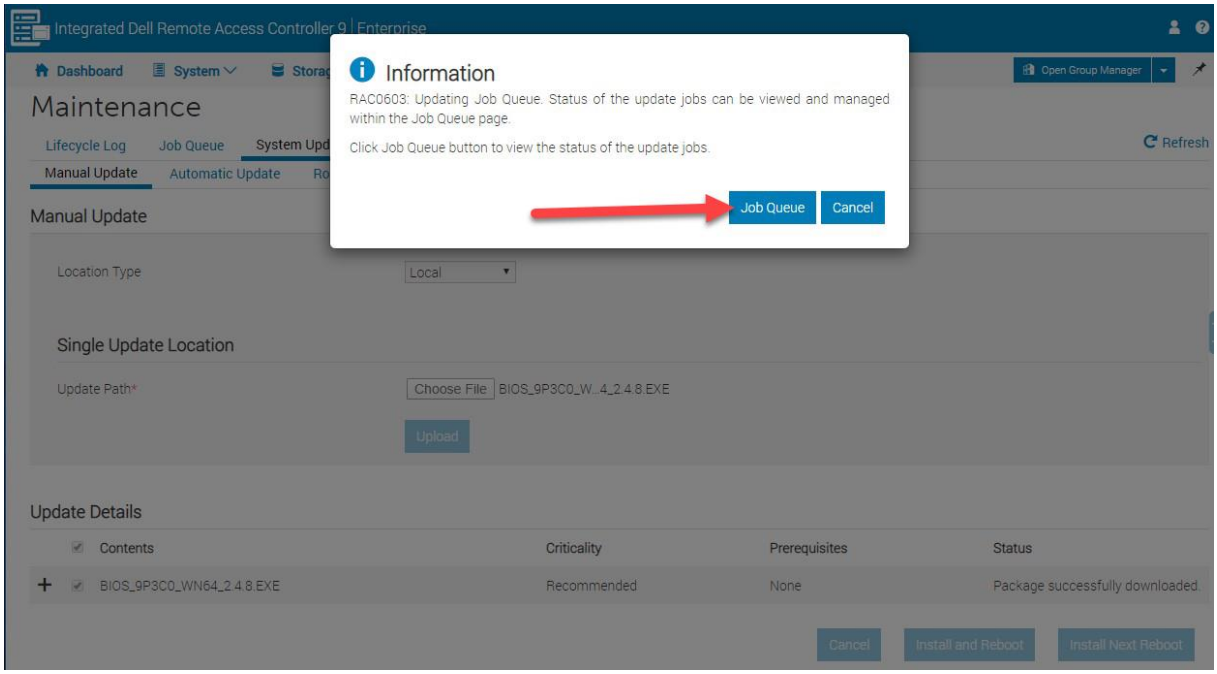
3. Select a file and choose “Open”.



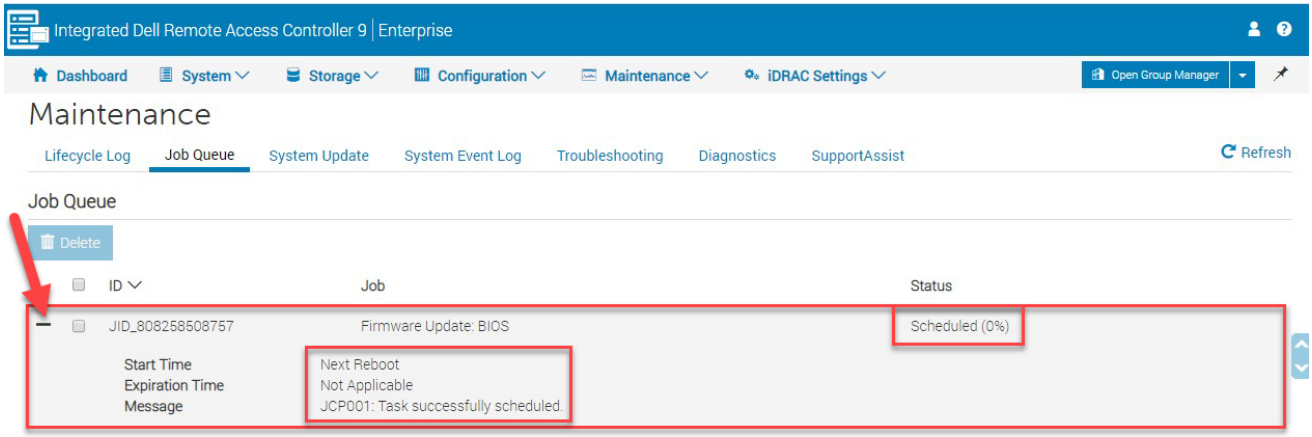
4. Select the firmware/BIOS and click on “Install Next Reboot”.



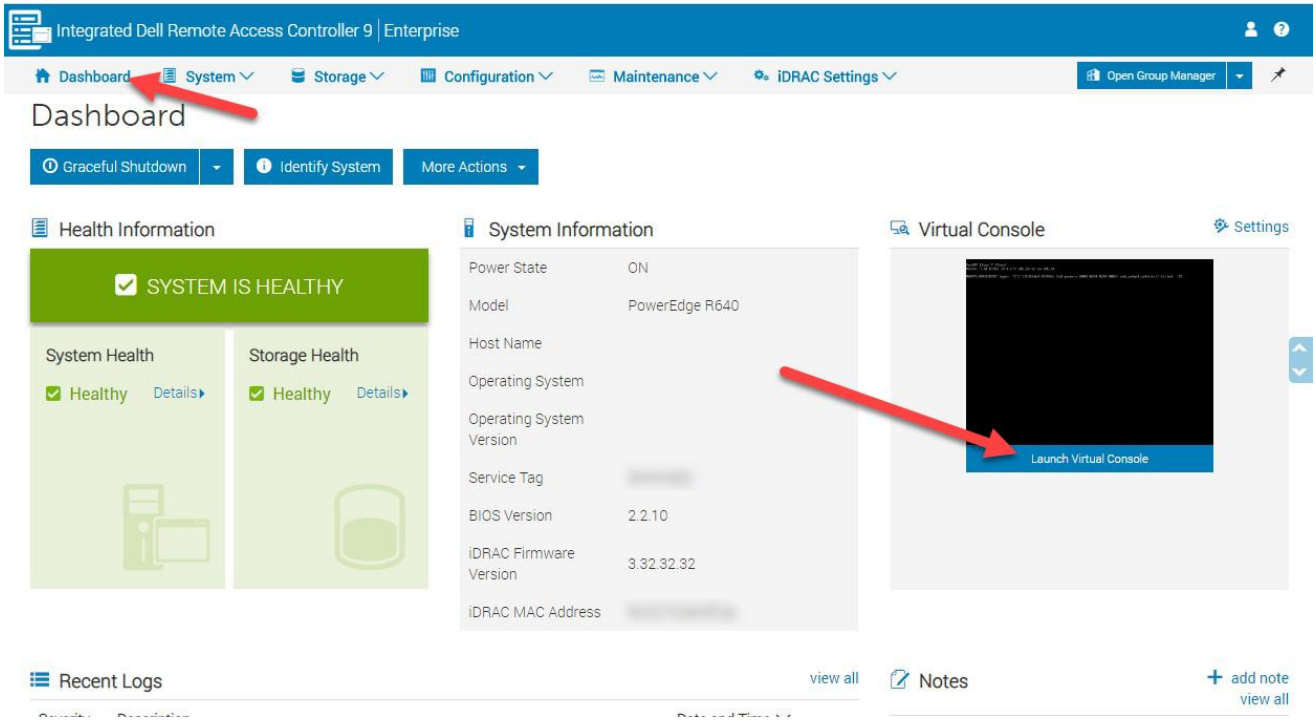
5. Click on “Job Queue”.



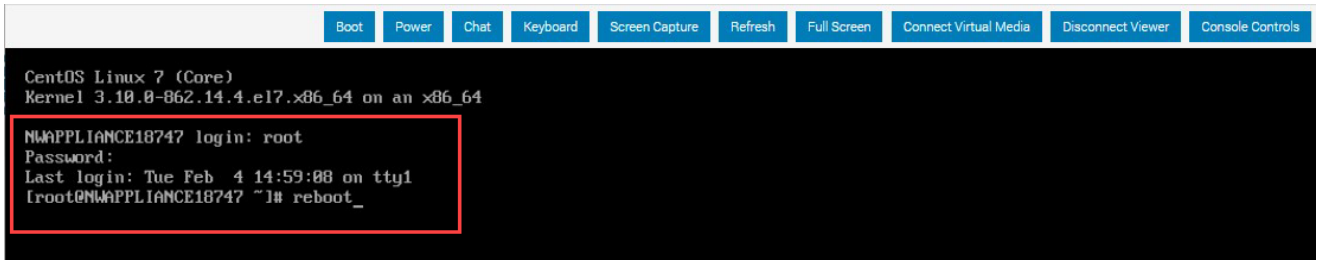
6. Verify that the job is scheduled for next reboot.



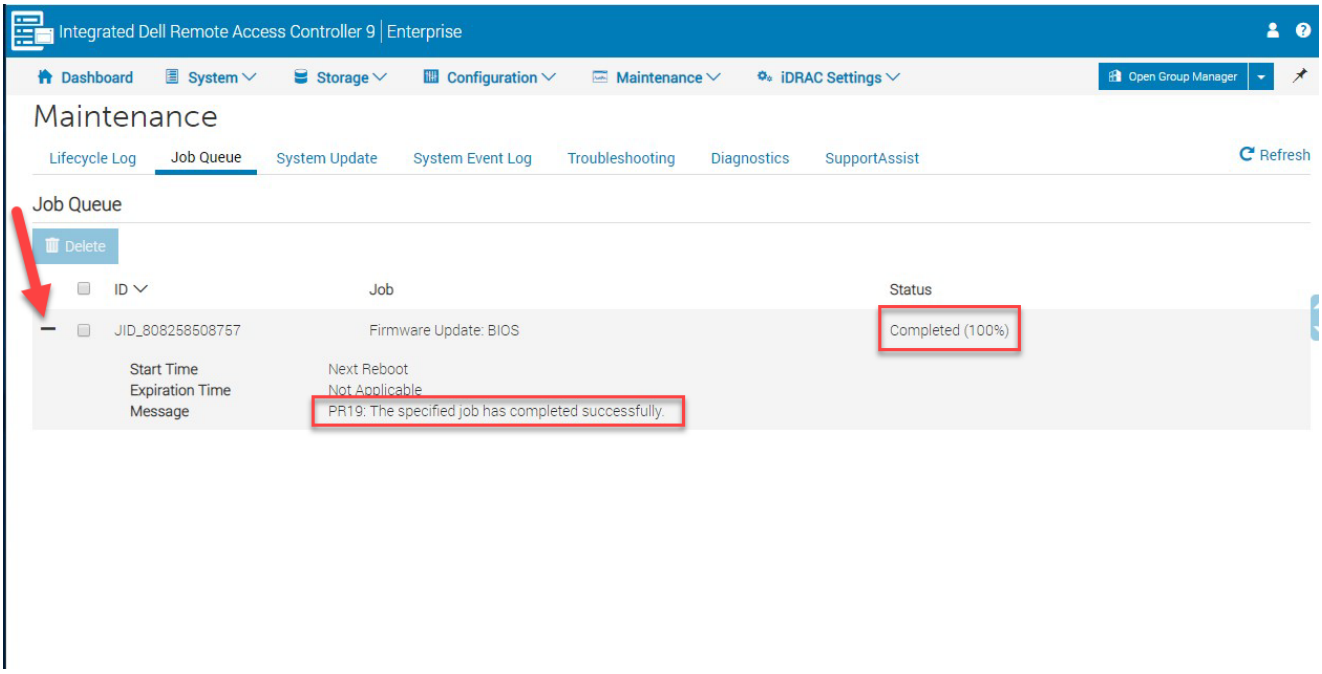
7. Click on “Dashboard” and “Launch Virtual Console”.



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

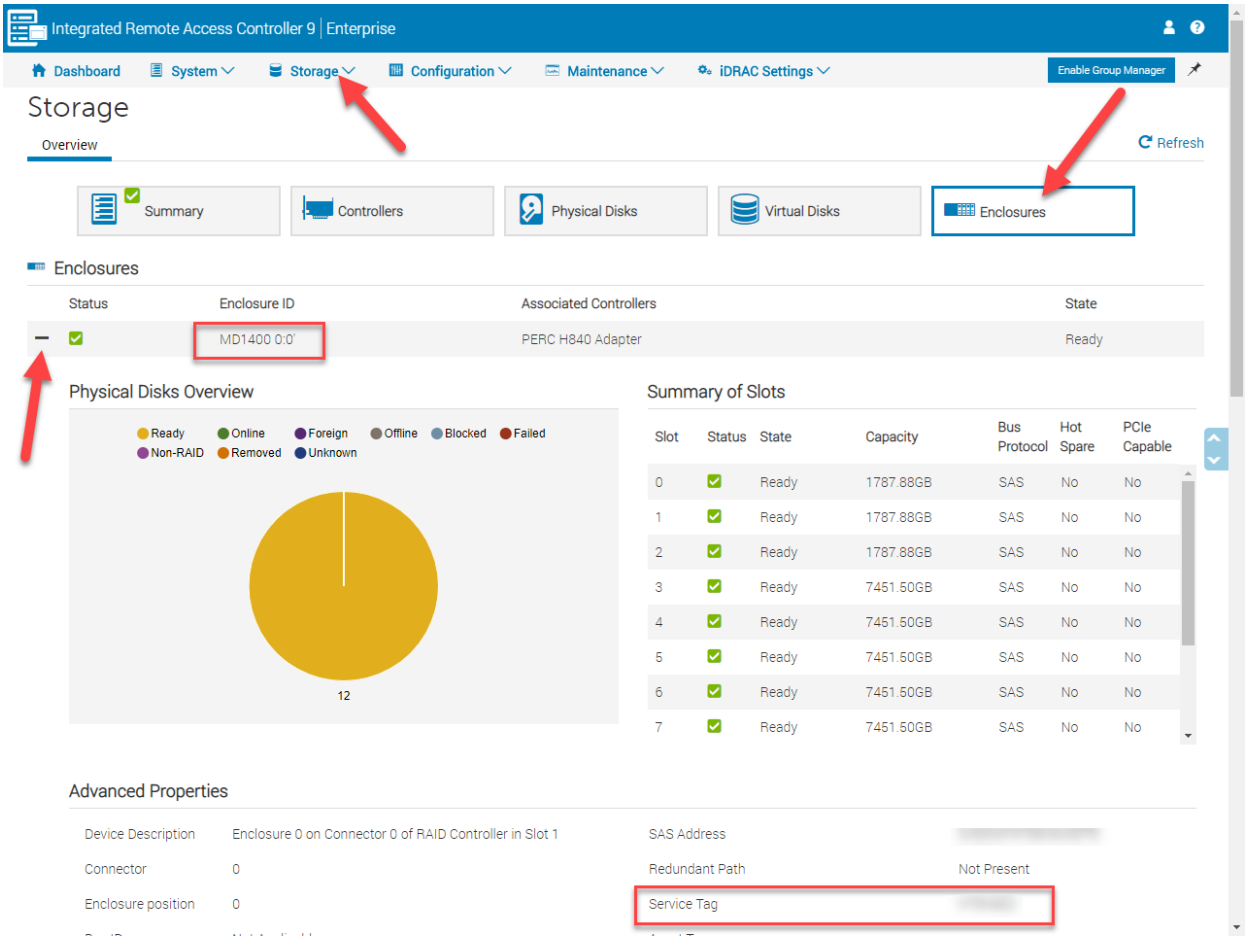


9. After update completes you can check your “Job Queue”.



Locating Powervault Serial Number

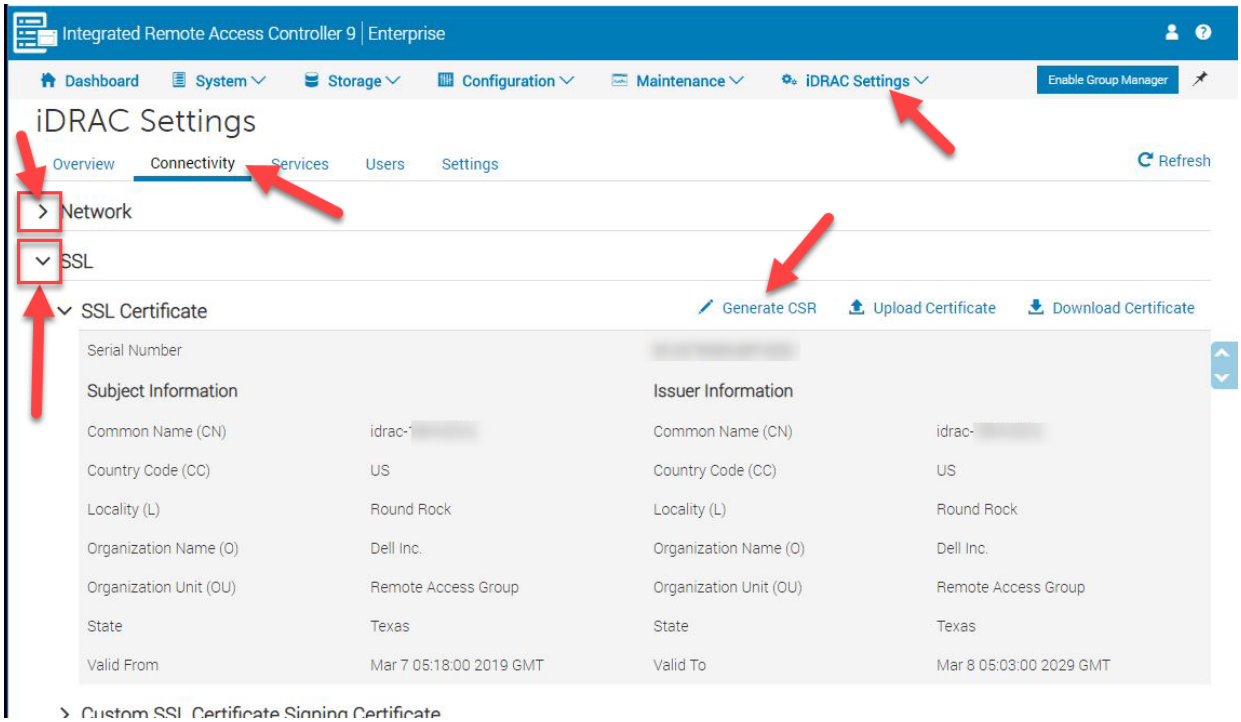
1. Click on “Storage”, “Enclosures”, and then locate your Powervault. Click on the “+” to expand your view and the Service tag will be visible at the bottom of the display for that Powervault.



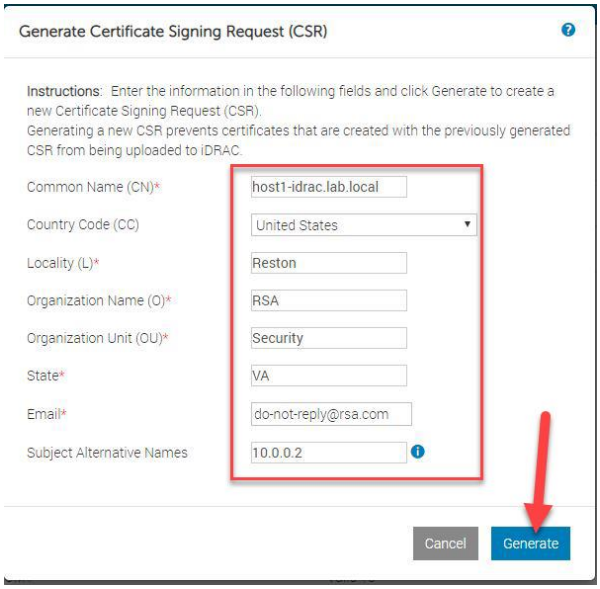
SSL Certificate for Web UI

Creating CSR

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

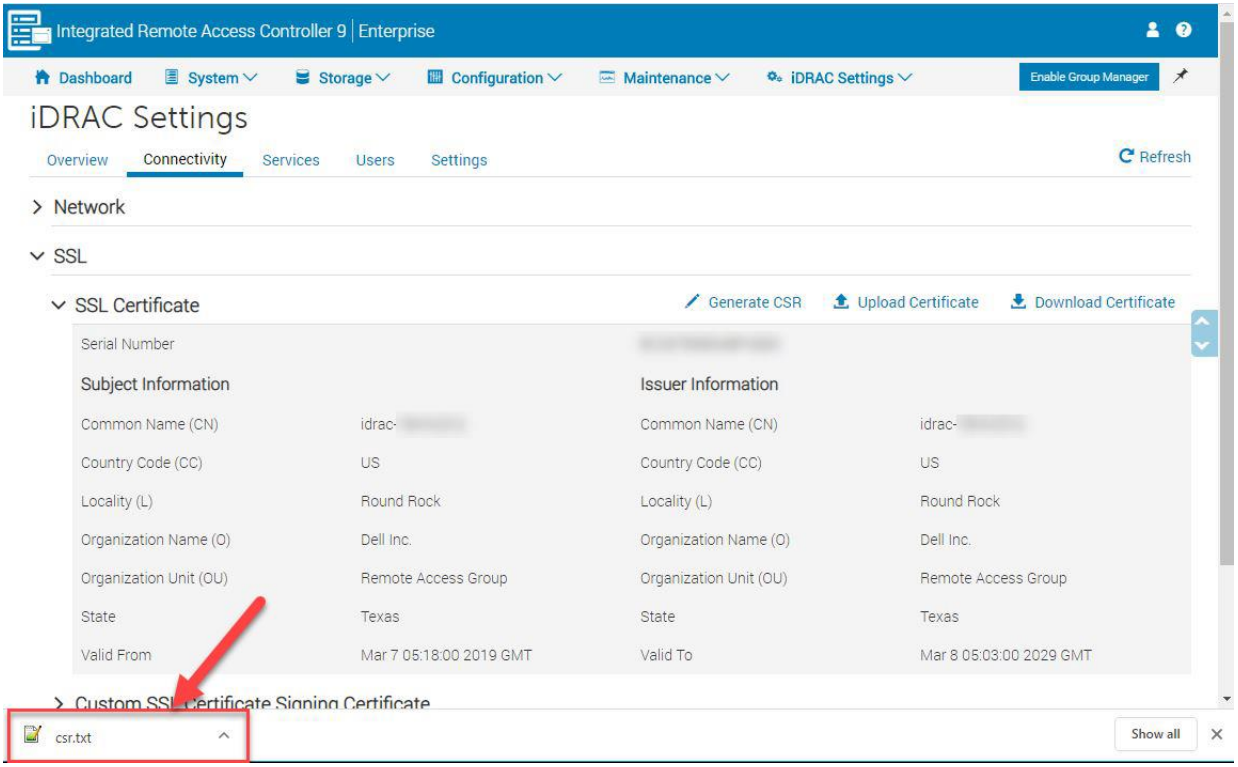


2. Fill out the CSR Form, then click "Generate".



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.

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

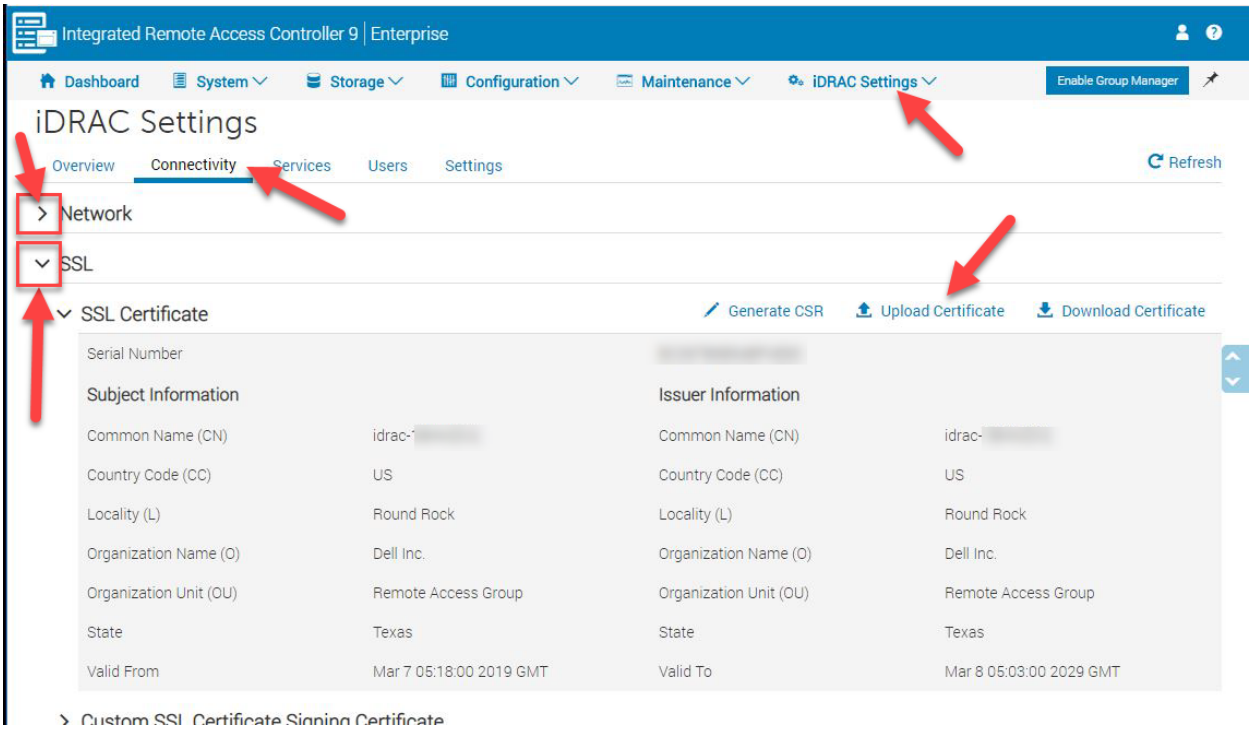


4. Submit the “csr.txt” to the Certificate Authority.

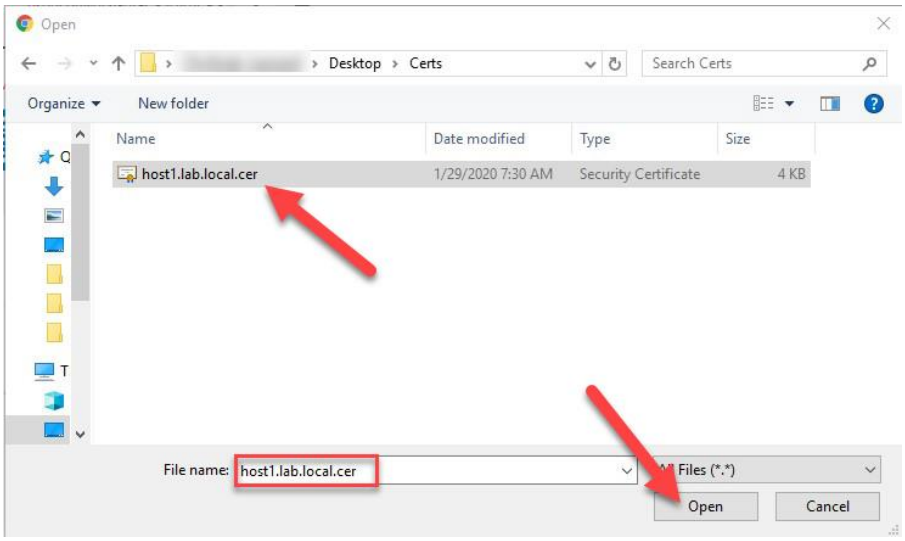
NOTE: When retrieving/downloading the certificates they should be in a Base64 Encoded format.

Uploading Certificate

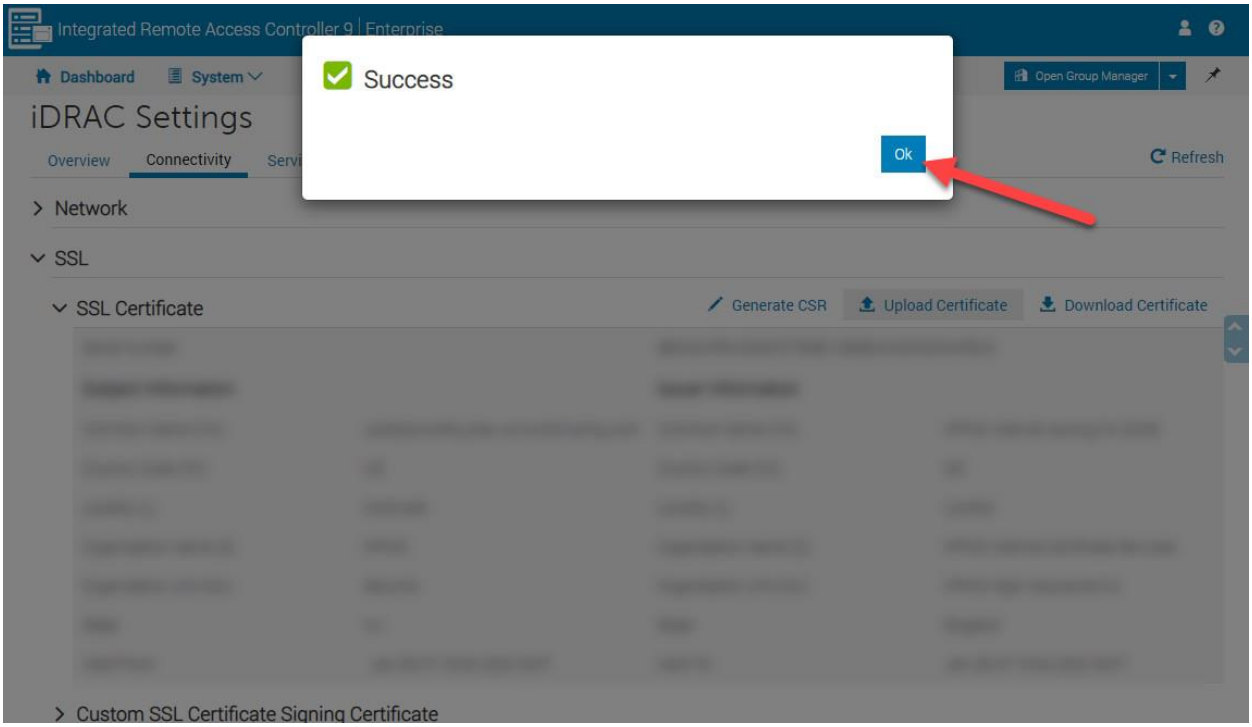
1. Navigate to the "SSL" section, "iDRAC Settings→Connectivity→SSL" and click on "Upload Certificate".



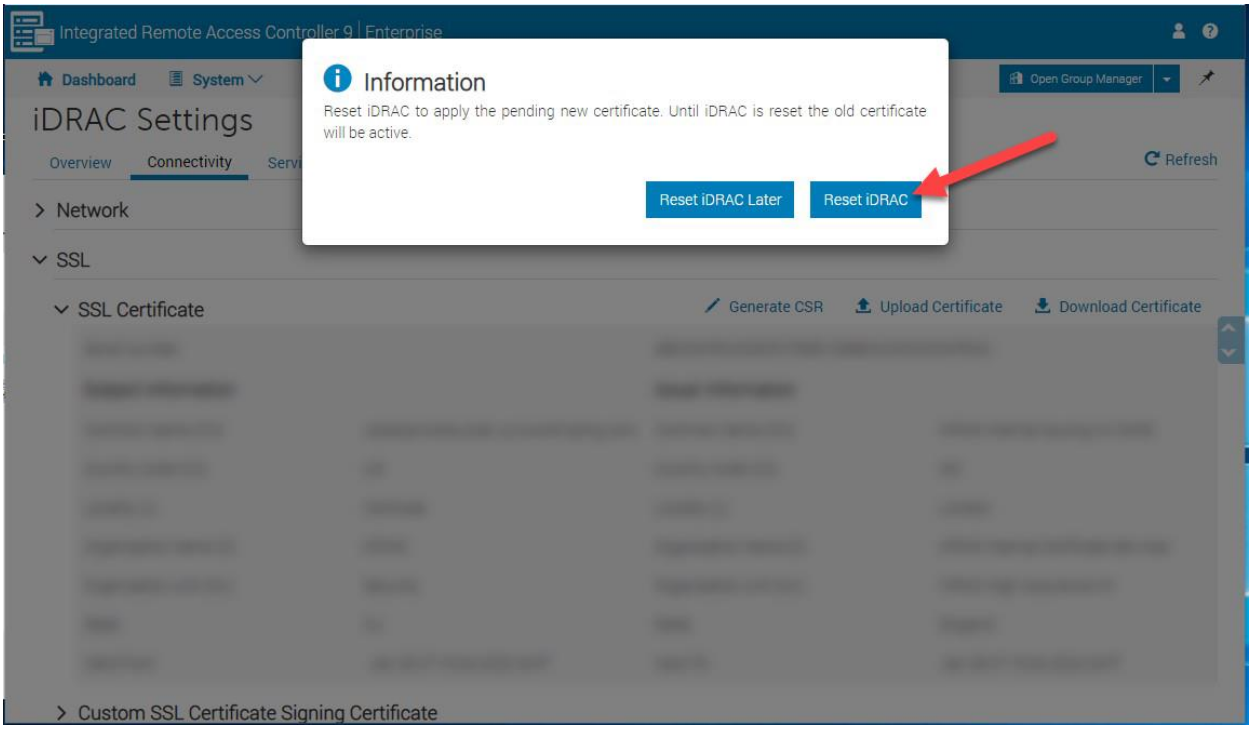
2. Choose the certificate file, click on "Open".



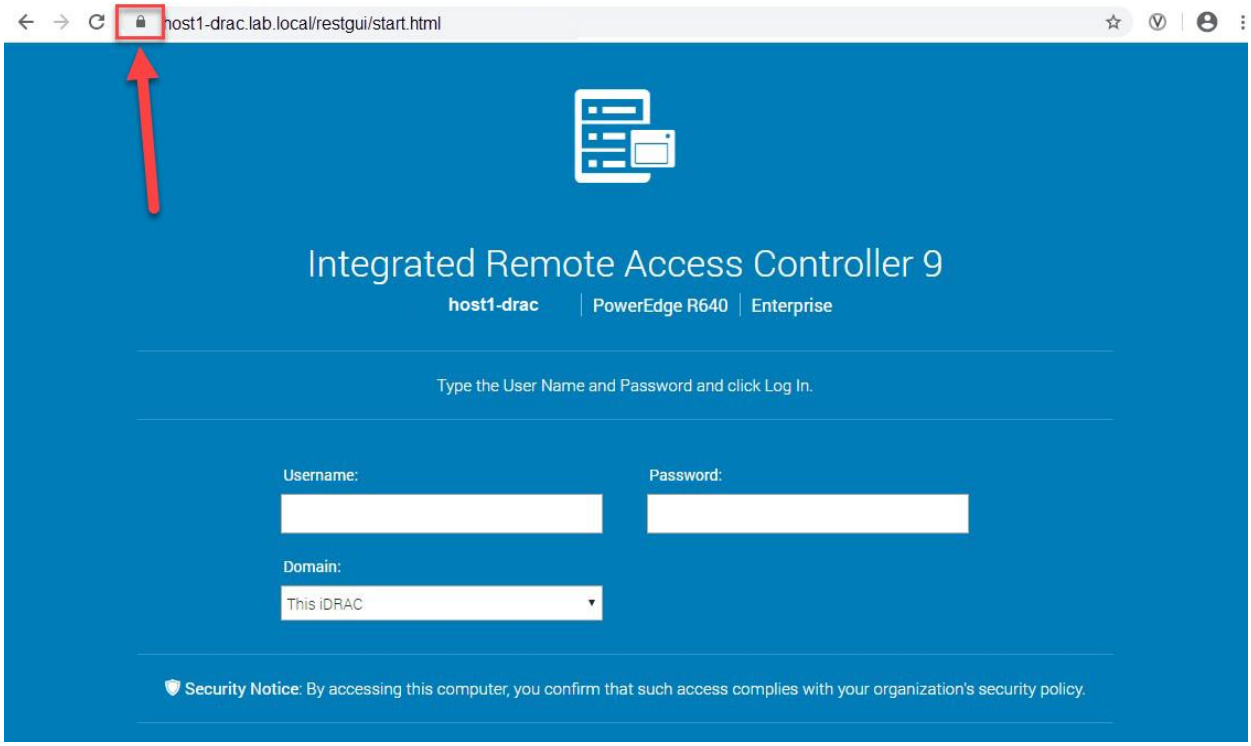
3. Click “Ok”.



4. Click “Reset iDRAC”.



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



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***

ID	*Name*	*Callin*	*Link Auth*	*IPMI Msg*	*Channel Priv Limit*
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@st3rO1"***

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***

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]>

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
Gratituous 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   : Xaaaaaaaaaaaaaa
Bad Password Threshold  : Not Available
```

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
Gratituous 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   : Xaaaaaaaaaaaaaa
Bad Password Threshold  : Not Available
```

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