Avaya Converged Platform 130 Series

iDRAC9 Best Practices

Release 4.0

May 2020

© 2018 Avaya Inc. All Rights Reserved

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Contents

Overview

The Integrated Dell Remote Access Controller (iDRAC) is designed to make system administrators more productive and improve the overall availability of Dell systems. The Dell iDRAC alerts administrators to system issues, help them perform remote system management and, reduce the need for physical access to the system.

iDRAC Implementation Rules

- iDRACs are intended to be on a separate management network; they are not designed nor intended to be placed on or connected to the internet. Doing so could expose the connected system to security and other risks for which Avaya is not responsible.
- Along with locating iDRACs on a separate management subnet, users should isolate the management subnet/VLAN with technologies such as firewalls, and limit access to the subnet/VLAN to authorized server administrators.

iDRAC9 Security Features

iDRAC provides a host of security features that should be utilized where applicable in accordance with your Corporation's Network Security Policy

- Custom signing certificate for Secure Socket Layer (SSL) certificate.
- User authentication through Microsoft Active Directory, generic Lightweight Directory Access Protocol (LDAP) Directory Service. (iDRAC9 Enterprise only)
- Two-factor authentication using the Smart–Card logon feature. The two-factor authentication is based on the physical smart card and the smart card PIN. (iDRAC9 Enterprise only)
- Single Sign-On and Public Key Authentication. (iDRAC9 Enterprise only)
- Role based authorization, to configure specific privileges for each user.
- SNMPv3 authentication for user accounts stored locally in the iDRAC. It is recommended to use this, but it is disabled by default.
- User ID and password configuration.
- Set user passwords and BIOS passwords using one-way hash format for improved security.
- FIPS 140-2 Level 1 capability.
- Support for TLS 1.2, 1.1, and 1.0. Avaya requires this setting be set to TLS 1.2.

Note: The base ACP 130 server comes with iDRAC9 Express. If the Enterprise license security features mentioned above are required, then the Enterprise license will need to be purchased. Additional Information about these security features can be found here: http://en.community.dell.com/techcenter/systems-management/w/wiki/3204.idrac9-home

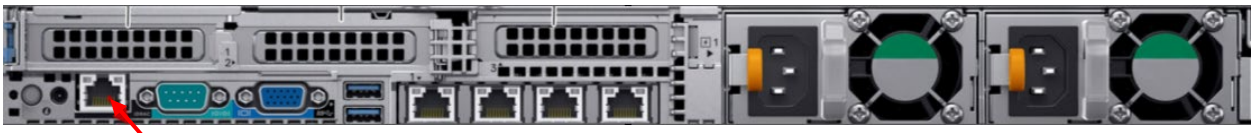
THE INFORMATION PROVIDED IN HEREIN IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. This document is intended to provide general information and is not part of any agreement you may have with Avaya related to your purchasing and/or licensing of Avaya products, services, warranty, maintenance and/or support. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Avaya ACP 130 Recommended

iDRAC9 Configuration Instructions

The following section describes how to configure an iDRAC9 interface using the iDRAC settings utilities. You must configure the initial network settings based on your network infrastructure to enable the communication to/from the iDRAC. As stated above ensure you are in accordance with your Corporation's Network Security Policies.

You can configure the iDRAC's IP address statically or assign an IP address via DHCP. By default, the iDRAC is set to use the dedicated iDRAC port of the server. Shared NIC is also supported, but not recommended. Avaya highly recommends use of the dedicated iDRAC interface for network security.



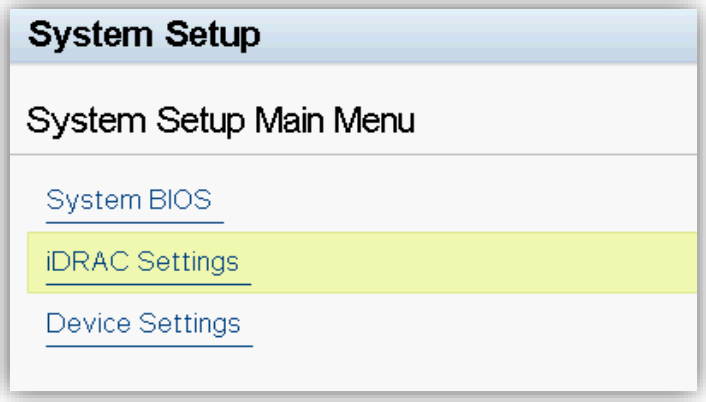
Dedicated iDRAC port

The iDRAC9 NIC port will come disabled and will require enablement before use.

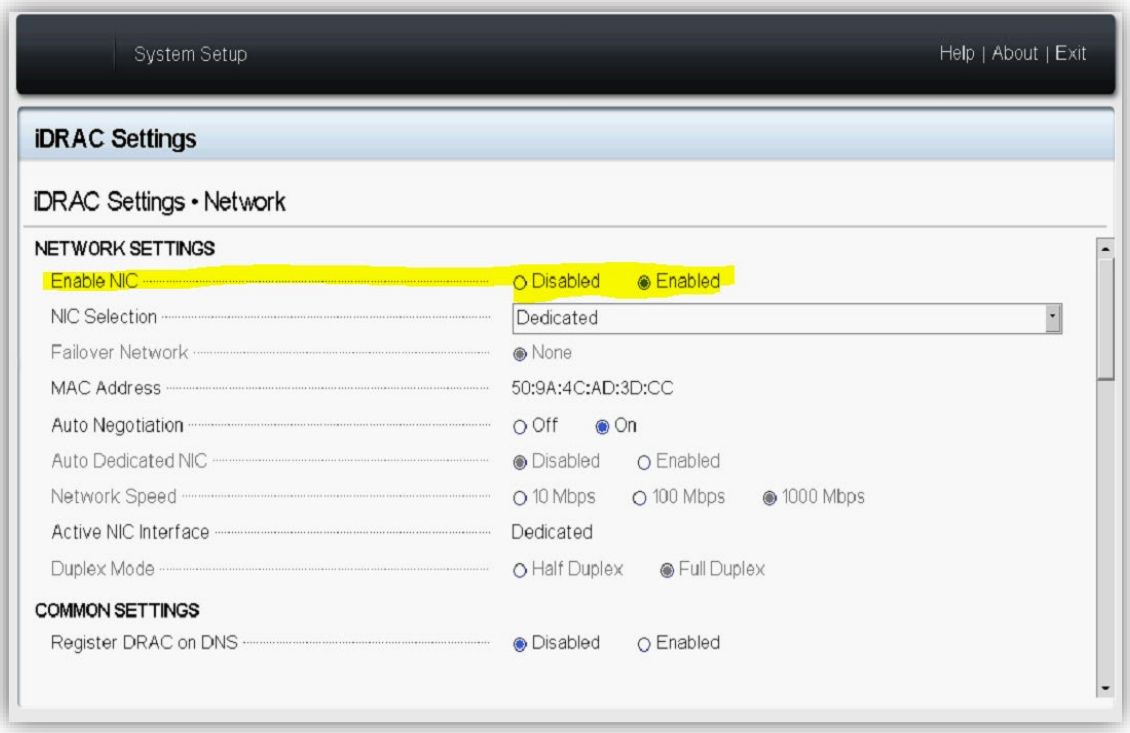
- How to enable and configure the iDRAC Network Interface using the iDRAC settings utility (F2 during server startup):
    1. Connect Monitor, USB keyboard and mouse to server.
    2. Power on the Dell R640.

3. Select <F2> when prompted from the Dell Splash screen to enter System Setup.

4. In the System Setup Main Menu page, select iDRAC Settings. The iDRAC Settings page is displayed.

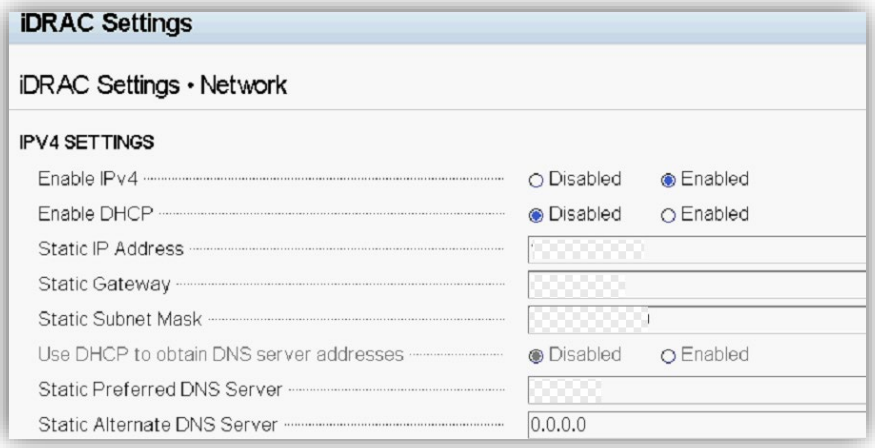


5. Select Network. The Network page is displayed.
6. Enable the NIC if set to disabled.
7. Ensure NIC selection is set to Dedicated. If shared NIC is preferred, make the change in this field. Avaya highly recommends keeping the iDRAC NIC interface on a separate, dedicated secure network(not shared).



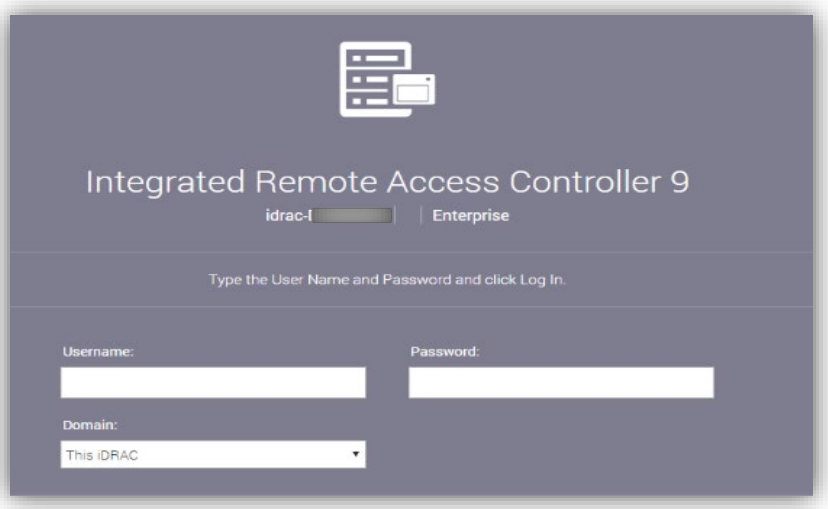
8. Scroll down and set Enable IPV4 to Enabled and then select either DHCP enabled or disabled. If DHCP is disabled, then the iDRAC static IP address can be populated. Fill in the details for iDRAC static IP Address, subnet mask, and gateway. Alternatively, if DHCP is enabled for the iDRAC network interface the IP address will be assigned automatically. Ensure that DHCP is enabled in your network environment if iDRAC DHCP is enabled.

Below is an example screen of the iDRAC9 IP Static address assignment.



9. Select Back, click Finish, and then click Yes. The network information is saved, and the system will reboot.

iDRAC9 IP address configuration is now complete. The iDRAC Web User Interface can now be reached with any supported browser (IE, Firefox, Chrome, Safari). Web interface GUI is shown below.

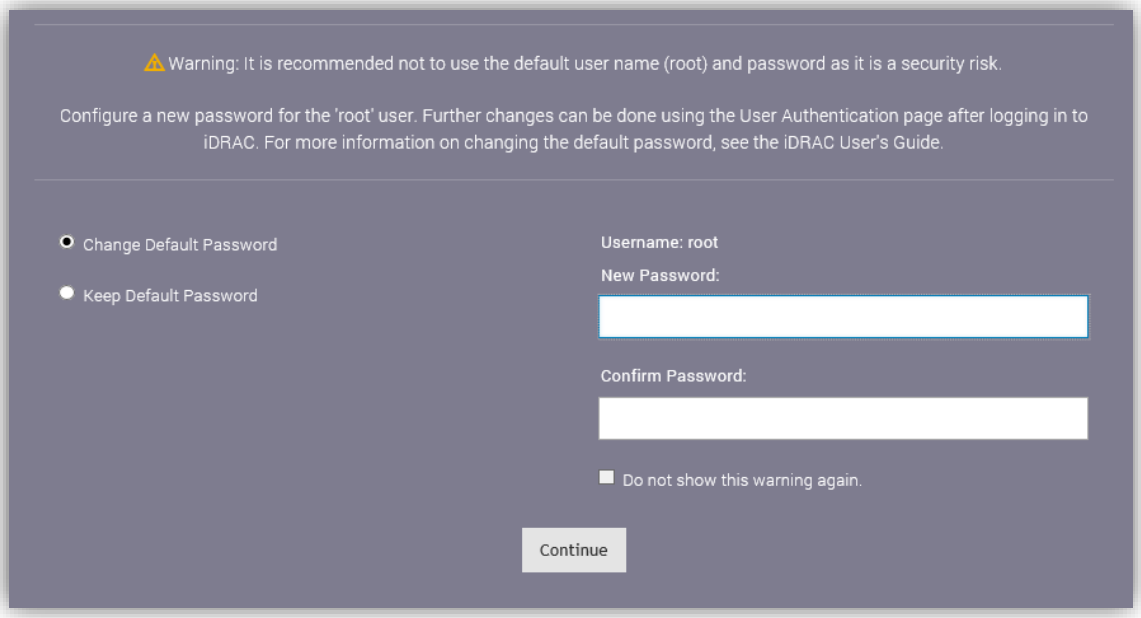


iDRAC User Configuration

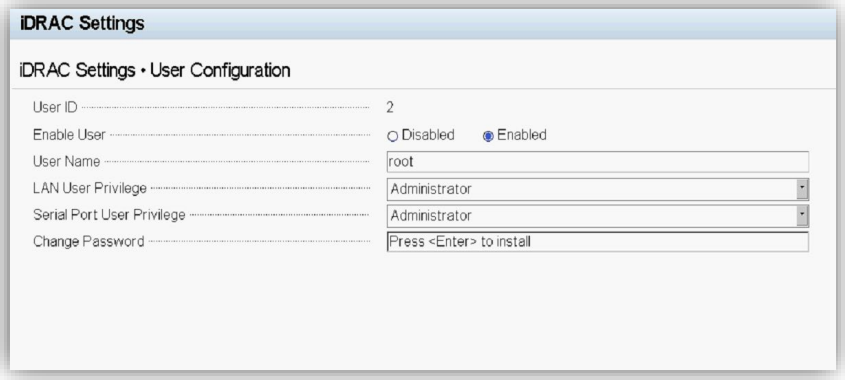
Follow these steps to configure iDRAC user accounts:

Important: Ensure that you change the default user name and password when initially logging into iDRAC web interface.

- Avaya servers ship with a unique factory generated password. It is displayed on the pull-out label on the front of the server. The default username will be root.
- Open a browser window and type in the iDRAC9 IP address in the address field to log into the server. Using the credentials of Login: root and Password:<Factory Generated Password>
- At the first login, the user will be prompted to change the password. Avaya recommends setting a complex password which would contain at least 8 characters and have each of the following:
  1. One special character
  2. One upper case letter
  3. One digit



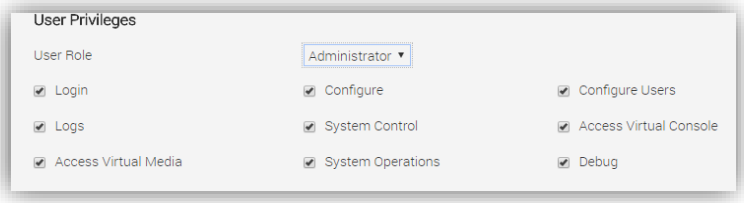
- The iDRAC password can also be set through direct console. The location to change the iDRAC password is located at System setup – iDRAC settings – User Configuration.



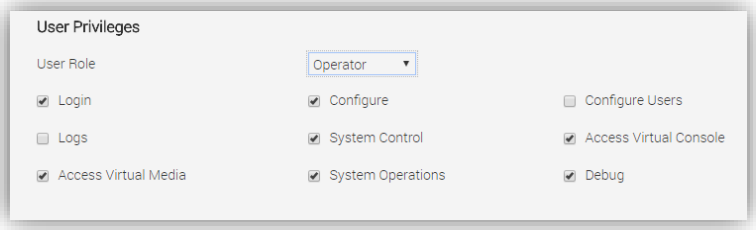
Recommended Role Based Access Control:

Initially, there should be only one user(root) account with admin privileges. Avaya recommends not to use the root account other than for initial user configuration. Avaya recommends having only 2 user accounts with admin privileges to minimize malicious behavior. Multiple users can be added with different user roles. Only create user accounts with the minimum permission requirements needed for the user. There are 4 types of user roles available, they can be customized to a finer granularity using individual check box selections. See below.

- Administrator



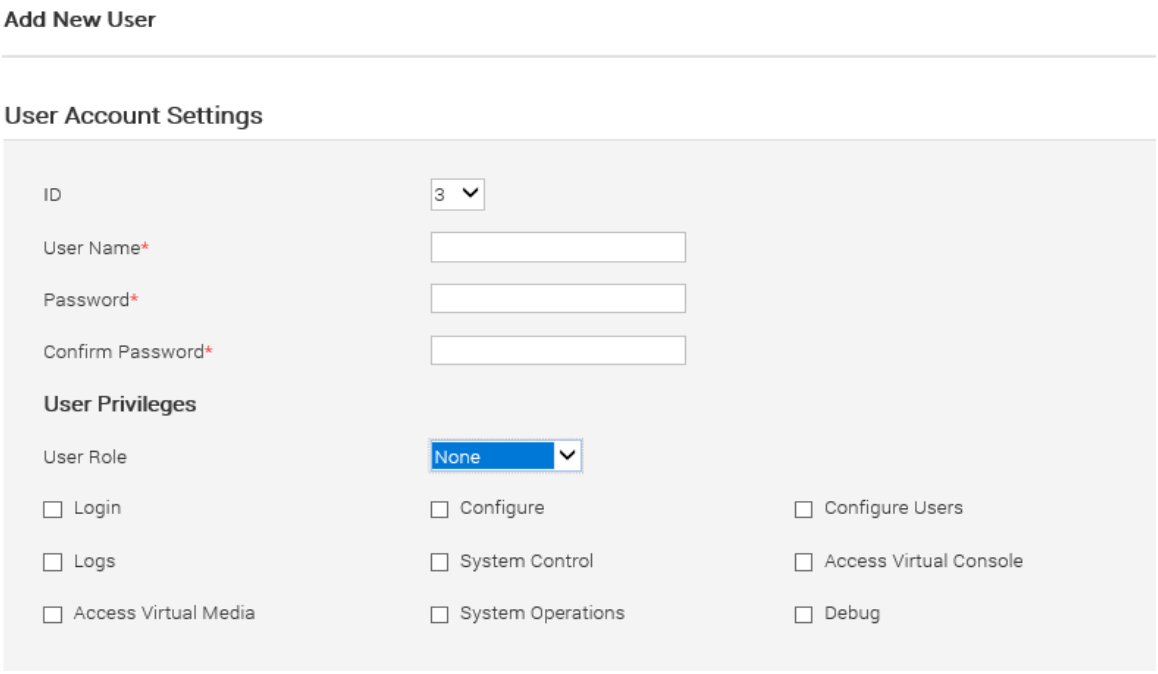
- Operator



- Read-Only – Only login access
- None – no access

How to Add a User

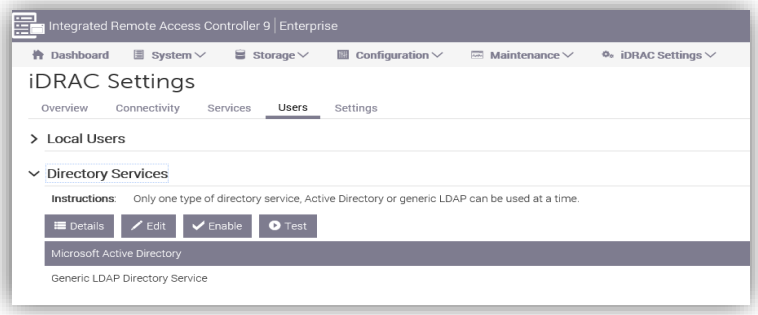
A new user can be added based on their role. The setting can be found at iDRAC Settings – Users – Add.



As per requirements, a new user can be added with different privilege levels. User role of None can be created with User privileges adjusted for that individual's needs.

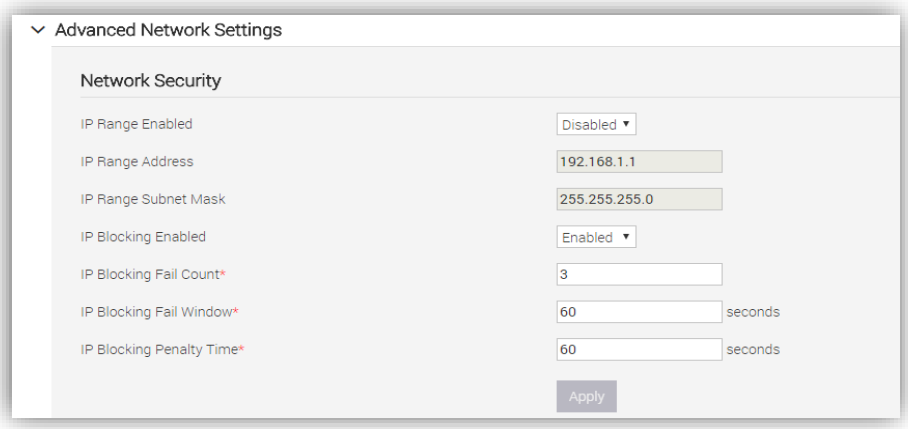
Caution: Avaya recommends having 2 users with admin level privileges with a complex password set for those accounts. Moreover, Microsoft AD or LDAP can also be integrated to make the iDRAC interface more secure. Please refer to Dell's documentation to access iDRAC using Microsoft AD or LDAP. The link provides a Dell document describing the steps on how to integrate iDRAC with Microsoft's AD.

LDAP or Active Directory Services can be accessed at iDRAC Settings -> Users -> Directory Services

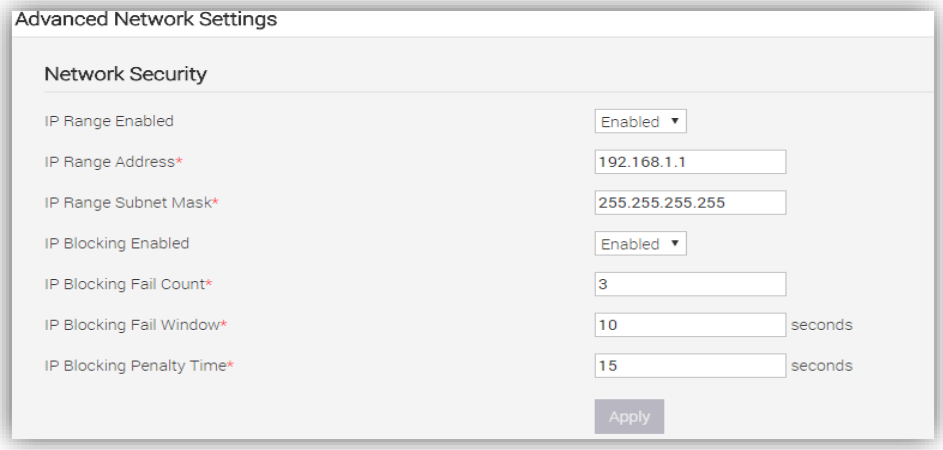


Network Security

Additional security can be added to the iDRAC interface by allowing only a specific range of IP addresses to access the iDRAC. Administrators can specify the range of IP addresses using the IP address and IP Range Subnet Mask. This can be done through the iDRAC settings listed under Advanced Network Settings. These settings can be found at iDRAC Settings -> Connectivity -> Network -> Advanced Network Settings.



If you opt to use this setting, then change the IP range enabled button to “enabled” and restrict the network range that you want to allow by setting the IP address and Subnet Mask. Administrators can specify a single, multiple or range of IP addresses using the IP Range Subnet Mask. Avaya encourages use of this feature if possible to strictly contain access to the iDRAC.



To allow only one IP to access the iDRAC9 interface, set an IP in the IP Range Address field and set the IP Range Subnet Mask as 255.255.255.255. See above.

IP Blocking Feature:

The IP Blocking feature allows for penalty time blocking out of IP addresses that have a failed number of login attempts. Failed count is also settable.

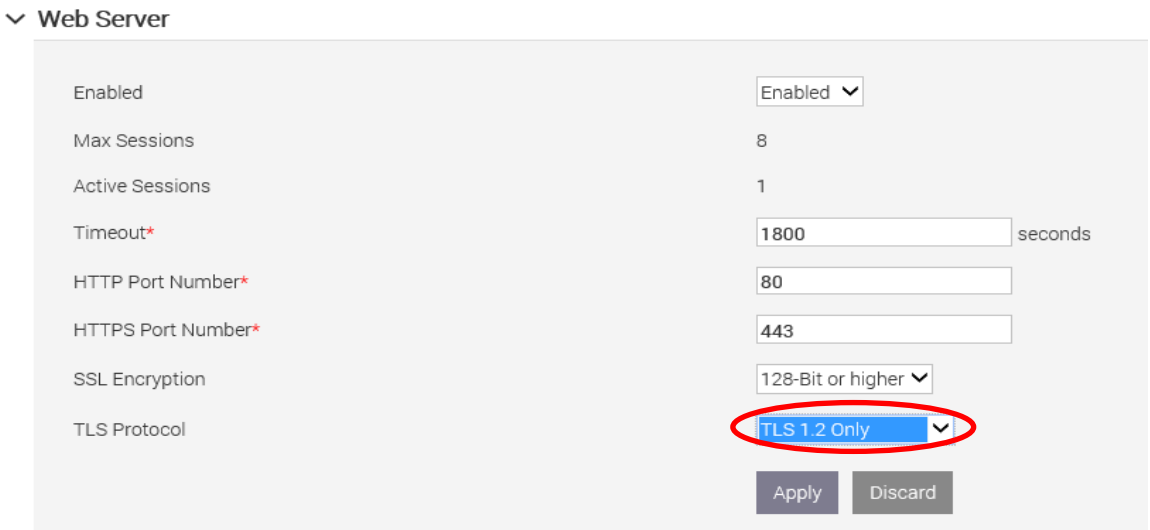
IP Blocking Fail Count: Max no. of failed attempts allowed before the user is blocked.

IP Blocking Fail Window: The time in seconds for which the user can't login to iDRAC.

iDRAC9 Web Server Settings

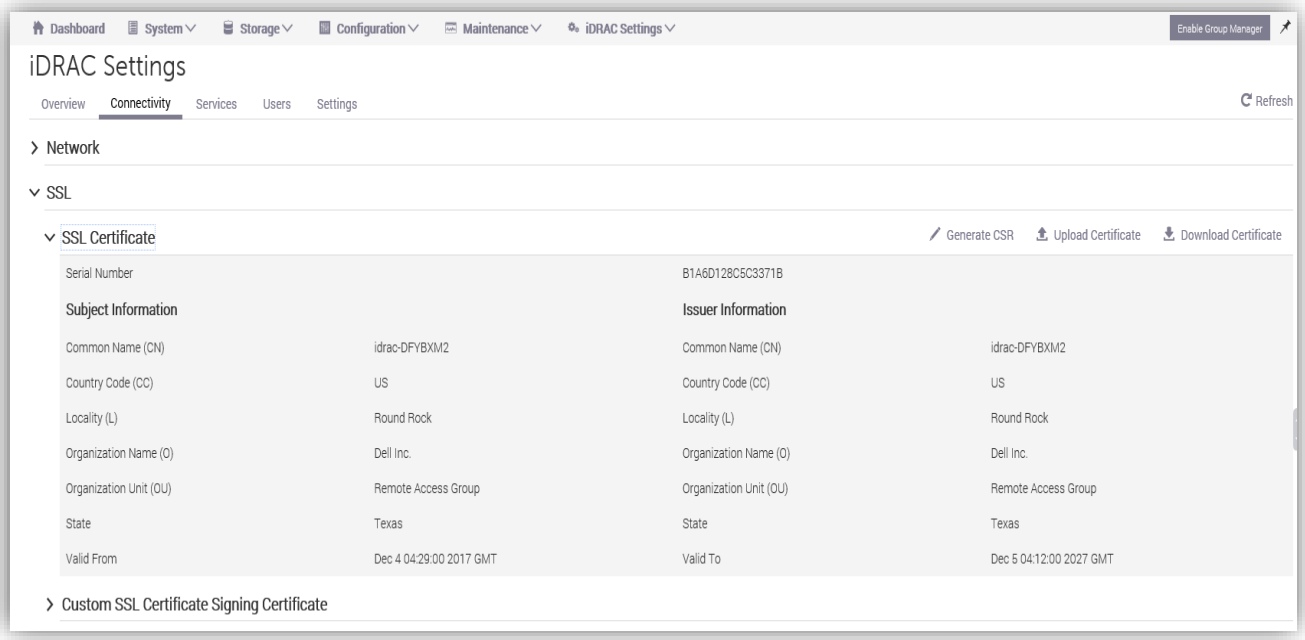
The SSL encryption and TLS protocol settings can also be changed to make the iDRAC web interface more secure. The options to change these settings are found at iDRAC Settings > Services > Web Server. Set the **TLS Protocol** to **TLS 1.2 Only** as shown in the following image.

Web Server parameters can be adjusted on this page. The Web Server field is set to Enabled by default, but you can disable it. The web server timeout setting can be set in seconds in the Timeout field. An inactive web page will time out based on the value in the timeout setting. A re-login is required for the new setting to take effect.

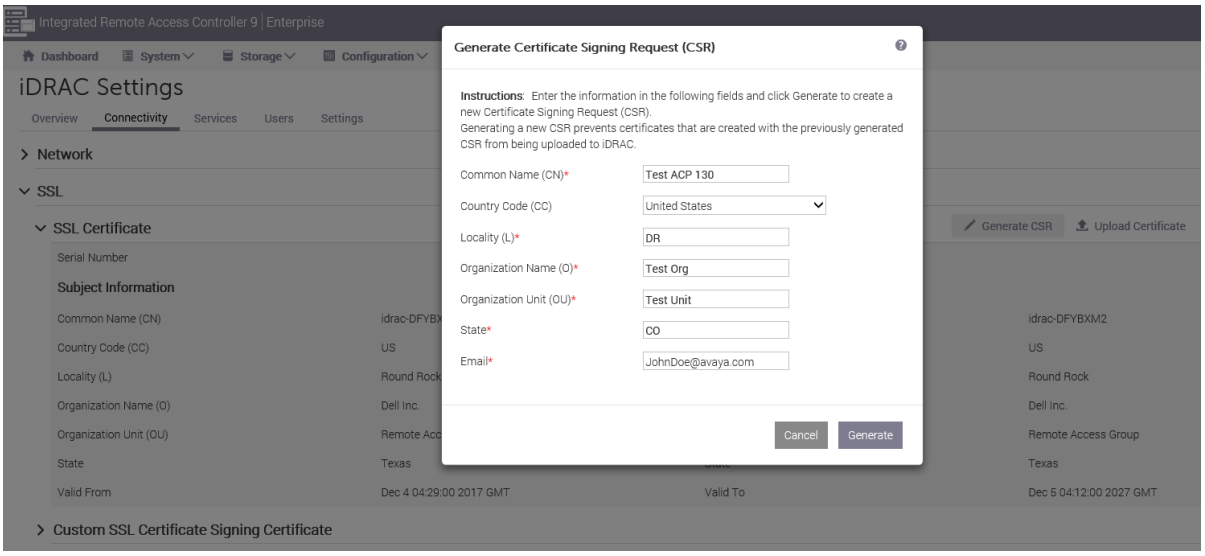


iDRAC9 Certificates

iDRAC9 SSL Certificate Uploading, Downloading, Generation and Custom Certificate Signing: The iDRAC SSL Certificate features are located here: iDRAC Settings -> Connectivity -> SSL -> SSL Certificate. Custom SSL Certificate Signing is also supported. See below



The iDRAC allows users to generate their own Certificate Signing Request if required.



Conclusion

The iDRAC9 interface is a powerful and valuable tool for managing and maintaining the Dell R640 server platform. Key measures must be taken to keep it secure. It is expected that users implement as many of the security measures cited in this document as possible. Even with a secure iDRAC interface, the user must also secure the network that it is utilizing. If iDRAC network security is compromised, user permissions are not properly assigned, user passwords are not complex, and/or the interface is breached then Avaya is not responsible.