Factory Generated Default Password for iDRAC9 for Dell EMC 14th Generation (14G) PowerEdge Servers

Guidance about adopting the Factory Generated Default Password feature for iDRAC9 on the Dell EMC 14G PowerEdge servers.

Dell Engineering
October 2017

Author

Doug Iler

A Dell EMC Technical White Paper

Revisions

Date	Description
July 2017	Initial release
October 2017	First revision

Contents

Executive Summary

This technical white paper explains the factors driving the introduction of the factory generated default password feature for iDRAC9 for Dell EMC 14th generation (14G) PowerEdge servers. Also, it provides guidance on how to adopt the feature in terms of best practices for provisioning, configuring, and maintaining. Each of the above practices have a strong influence on the secure operation and assurance of iDRAC9 for 14G PowerEdge Servers.

The feature has a major impact on the default user account password in terms of the factory-default or shipping value. Prior to this generation of servers, the password was a publically well-known value `calvin` used across all servers. This technical white paper introduces this new feature and attempts to cover the main aspects that are crucial in comprehending its impact on the system management processes and procedures.

1 Introduction

With iDRAC Systems Management, Dell EMC has been delivering solutions for generations of servers to make server management as simple as possible for the server administrator. The features offered embody simplicity, scalability, security, and convenience.

In terms of server security, the environment and landscape has been undergoing drastic transformation. For all previous generations, iDRACs have shipped with a static private IP-address for the iDRAC network management port as part of the default factory configuration. This default setting provided a level of security where any routine connection of the iDRAC network management port did not immediately provide network access. Further network configuration steps were required to make the port functional. As such having a well-known password for the administrator default user account did not pose a risk as no iDRAC access was possible without further purposeful configuration steps.

Although the above approach was secure, it was inconvenient for many users. Being forced to touch each and every server to provision the iDRAC network management port was a costly and time consuming effort. The users' desire was to have the DHCP client service enabled by default on the management port without requiring any at-the-box provisioning or special configuration ordering at the point of sale. The disadvantage of the special configuration ordering was that these settings were lost as soon as the iDRAC configuration was reset to factory defaults.

For iDRAC9, the DHCP Client Service is now enabled by default thereby providing the user with the desired convenience. As a trade-off with security in mind, the factory generated default password feature has been introduced. If the iDRAC network management port is now inadvertently hooked up and DHCP services are in operation in the user's network environment, the risk of unauthorized iDRAC access is mitigated as the password for the administrator default user account is now different for each server.

The following sections provide more introductory information on the factory generated default password feature.

2 Default factory password for iDRAC

2.1 Legacy default password

For previous generations, iDRAC shipped with a publically well-known password ‘calvin’ for the default user account. This default factory user account is named ‘root’ and the account is enabled will full administrator privileges. For the purposes of this discussion, we will refer to this default factory password (calvin) as the legacy factory default password for iDRAC.

2.2 Factory Generated Default Password

For the 14G PowerEdge servers and iDRAC9, a new option for the factory default password for iDRAC is offered. This option will be referred to as the factory generated default password for iDRAC.

The password consists of a string of alpha-numeric characters. The password is composed of a fixed length of 12 characters. The alpha characters are always capitalized. Some alpha-numeric characters will be omitted from the generation set. This has been done to reduce any ambiguity in recognizing the characters especially when they are translated to written text.

Each server will be programmed with the factory generated string. It should be noted that there is no guarantee that the password will be unique across all servers shipped.

Note: For iDRAC9 the factory generated default password option will be the default option. Meaning, all servers will ship with the factory generated default password option, unless legacy default password option is ordered.

3 Ordering information

It has been understood that some users may already have well established processes and procedures to manage the security implications of having a generally well-known password as the factory default password for iDRAC. To maintain the status-quo for these users, options have been put into place to allow these users to order their systems with the legacy default password.

Because the factory generated default password is the default option for iDRAC9, the following sections describe the various point-of-sale methods and how to override this default option during the ordering process.

3.1 Web sales

When purchasing from Dell EMC web-commerce sites, the following options will be presented:

- **Factory generated default password**: By default, all 14G PowerEdge servers will ship with a factory generated default password iDRAC password, to provide additional security. This password is generated at the factory and is located on the pull-out Information Tag located on the front of the chassis, adjacent to the server asset label. Users who choose this option must note this password and use it to log in to iDRAC for the first time. For security purposes, Dell EMC strongly recommends changing the default password.
- **Legacy Password**: Users who prefer known legacy password “calvin”, must choose this option. One reason to select this option would be to ensure conformance to current scripts. For security purposes, Dell EMC strongly recommends changing the legacy password.

Note: The factory generated default password is the default option. Ensure that the correct option is selected to ensure full preparedness for managing the iDRAC factory generated default password on the purchased systems.

3.2 Sales Representative

When placing an order with the assistance of a sales representative, make sure to explicitly state what choice of password for the iDRAC administrator default user account is required. If a choice is not stated, by default, the ordered system will ship with the factory generated default password. If the Legacy Default Password is better suited to your existing provisioning and deployments procedures and processes, make sure to inform the sales representative that you would like the ordered placed with the legacy default password option.

Note: If the sales representative places an order without being informed that the legacy password is desired, the systems will ship with the factory generated default password. Ensure that you are fully aware of the password option ordered so that you are fully prepared for managing the iDRAC factory generated default password on the purchased systems.

4 Un-Boxing the server

For many generations, all servers have come equipped with a fixture to house an Information Tag. The fixture is built into the chassis body and accessible by using a pull-out tab on the front panel that allows the tag to slide in and out of the slot housing it.

4.1 Information Tag

Figure 1 highlights the location of information tag on the front panel of a 14G rack server.

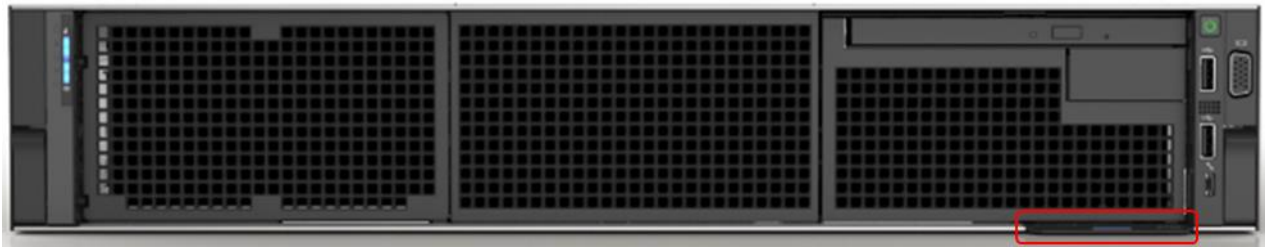

Figure 1 Location of Information Tag

Figure 2 shows the front or top-side on the Information Tag. The space is used to display labels for the following information:

- Service Information
- Reserved for other uses such as placing the Asset Tag

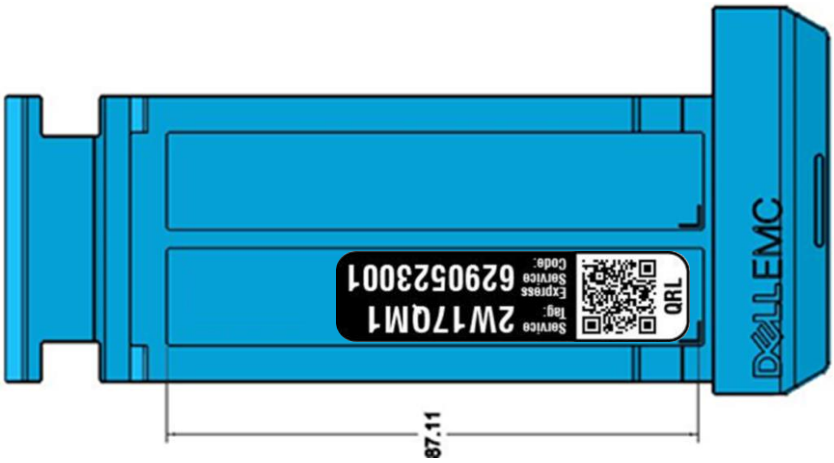

Figure 2 Front or top-side of Information Tag

Figure 3 depicts the back or underside on the Information Tag. The space is used to display labels for the following information:

- Part-Number Information
- QR (Quick Resource) Code for the OMM (Open-Manage Mobile) Application. Or, for scanning by using a general-purpose QR code scanner.
- MAC (Media-Access-Control) address Information
- iDRAC Default Password (option-based)

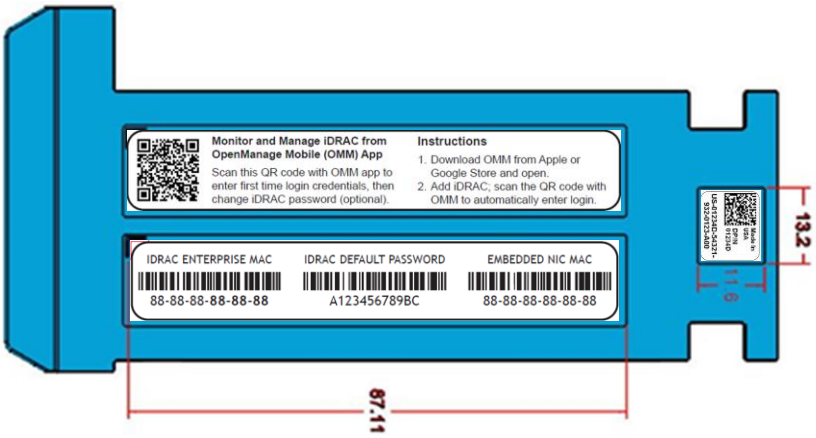

Figure 3 Back/Under-Side of Information Tag

4.2 Labels

The figures in this section provide close-up information about each of label.

Figure 4 depicts the following information:

- iDRAC Enterprise MAC address
  - This is the MAC address for the iDRAC Network Management Port.
- Embedded NIC MAC address
  - This is the MAC address for the NIC (Network Interface Card) that provides networks ports that can be accessed by the server host itself.
  - These network ports can also be shared by iDRAC to provide systems management network access. This option is not enabled by factory default and has to be configured.
- iDRAC default password
  - This is the location where the Default Password for iDRAC is placed when the server is shipped with this option.

Figure 4 Close-up of Label with factory generated default password

Figure 5 depicts similar information as that described in figure 4. The main point to note is the lack of the iDRAC default password on the label. This is what this label will appear as when the server is shipped with the Legacy Default Password option.

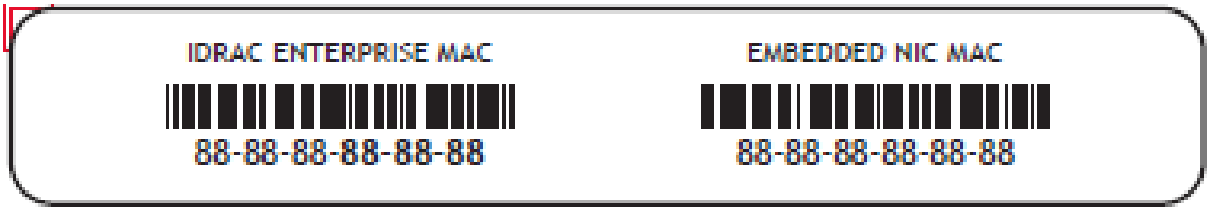

Figure 5 Close-up of Label without factory generated default password

Figure 6 depicts the following service information:

- Service Tag
  - Is a seven-character identifier that uniquely identifies the server.
- Express Service Code
  - Is a 10-digit numeric version of the Service Tag which can be typed into a telephone for call routing.
- QRL (Quick Resource Locator)
  - Using the Dell QRL mobile application, it allows enterprise Users to quickly get at-the-box videos and documentation supporting their Dell EMC products.

Figure 6 Close-up of Label for Service Information

Figure 7 below depicts the following QR Code information:

- QR Code for OMM Application
  - Using the OMM application, it allows the QR code to be scanned for touchless login into the application to manage the iDRAC.

- This feature requires other optional hardware. This QR code can be scanned and captured by any general-purpose QR reader. This data can then be used in automatically provisioning the server as part of scripting.

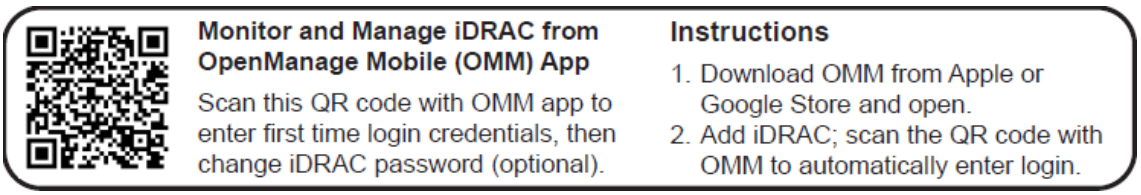

Figure 7 Close-up of Label for QR Code for OMM Application

Figure 8 depicts the following part number information:

- The PPID (Piece Part Identification) number is used as a means to identify and track.
- The number contains several sets of information:
  - Country of Origin
  - Dell EMC five-digit Part Number
  - Manufacture Identification
  - Date Code
  - Alpha-numeric Manufacture Sequence identification Number

Figure 8 Close-up of Label for Part-Number Information

5 Asset management

The iDRAC 9 for the 14th Generation PowerEdge servers has greatly improved the convenience for deploying the systems. New for 14G, all PowerEdge servers ship with the DHCP Client Service on iDRAC enabled as the factory default, there is virtually no at-the-box pre-provisioning required. With a network environment where DHCP services are prevalent, the installation of the systems would mainly consist of 'racking-n-stacking' the systems and hooking them up for network access. All further deployment actions and other systems management activities could be undertaken through remote network access to the systems.

Note: Dell EMC Systems Management best practices for networking recommends that all network interfaces on managed servers use Virtual LANs (VLANS), Access Control Lists (ACLs), or physical separation to isolate the management network from the rest of the data network.

However, for Users who receive systems with the iDRAC configured with the factory generated default password option for the default administrator user account, it is important that they have a best practice for asset management. Because the factory generated default password for iDRAC will be different by design for each system, knowledge of the password for each system will be a requisite for ongoing deployment actions and other systems management activities, especially if these are to be undertaken by using remote network access.

At best, the asset collection procedure should capture all the pertinent information located on the system's information tag. At a minimum, assuming that the systems are configured with the factory generated default password option and that DHCP Services are being utilized, and then capturing the iDRAC Network Management Port MAC address and the iDRAC Default Password would be very well advised. By capturing this information, the Systems Administrator can easily locate an iDRAC on the systems management network.

5.1 Barcodes

Figure 9 depicts information that has been covered in the sections above. The key point highlighted here are the barcodes associated with the various information.

The information of special interest for minimal asset collection are:

- iDRAC Network Management Port MAC addresses
- iDRAC Default Password

Figure 9 Close-up of Label highlighting the Barcodes

To be able to correlate a MAC address with the current IP address lease, the following sections provide some hints on the types of tools that can be used.

If your systems management network subnet is served by a Linux DHCP Server, the DHCP leases of all the iDRACs are listed in the file `/var/lib/dhcpd/dhcpd.lease` assuming the ISC DHCP Server is in use. For example, the following command line provides a simple formatted output:

```
egrep "lease|hostname|hardware|\}" /var/lib/dhcpd/dhcpd.leases
```

If your systems management network subnet is served by a Windows DHCP Server, the DHCP leases of all the iDRACs can be listed from the Windows Server as follows:

```
netsh dhcp server scope <IP-Address> show clients
```

Lastly, if you have a desktop client for Linux or Windows directly (no network router involved) connected to the same systems management network subnet that all the iDRACs are connected to, the DHCP leases for all the iDRACs can be listed by executing the following utility at command line:

```
arp -a
```

6 Pre-provisioning

If the user has not established processes for asset management, there will be instances where the system requires to have some level of pre-provisioning. This pre-provisioning procedure could involve configuring all systems to have some level of a common base configuration.

One example of a specific common setting for the common base configuration is the password for the default administrator user account. Because the iDRAC 14G PowerEdge servers will by default ship with the factory generated default password option, it may be prudent to change the password to an internal privately known password to ease remote network access to the systems for further provisioning and other systems management activities. The following sections describe features that could be used to pre-provision the password of the default administrator user account.

6.1 iDRAC Direct SCP feature

The SCP (Server Configuration Profile) feature provides a facility to import or export the system's configuration profile. The iDRAC Configuration is part of this profile. As mentioned, a possible pre-provision procedure that may be required is the procedure to change the password for the default administrator user account to an internal privately-known common password for the case where the systems are shipped with the factory generated default password option.

Again, it is assumed that this pre-provisioning exercise is required because the user does not have an adequate process for asset collection as described in the previous section. With a network environment with operational DHCP Services and by changing the password to an internal privately known password, later remote network access to the systems for further provisioning and other systems management activities can be easily undertaken.

This section lists the steps required to use this feature to change the password for default administrator user account. To use this feature, physical presence at-the server is required.

Pre-requisites

There are three (3) pre-requisites involved.

1. USB drive

   Option 1.

   - USB storage drive with dual connectors: USB 2.0/3.0 male connector and Micro-USB male connector (recommended). See the example image.

   Option 2.

- USB storage drive with USB 2.0/3.0 Connector plus converter/adapter cable with USB 2.0/3.0 female connector and Micro-USB male connector. See the example image.

2. Identify iDRAC Direct micro-USB port on system front panel (Right Control Panel – RCP)
   - The port is located on the 'right-rack-ear' of the front panel which is referred to as the Right-Control-Panel (RCP).
   - There is a green status LED associated with this port (not visible when the LED is off). See the example image.

3. The password for the default administrator user account has not been changed and is still set at the factory default or shipping value.

Pre-Provisioning Steps

1. Select a suitable password
   - For this example, we will use `BlueDi@mond7777777`.
2. Obtain a SHA256 hash code for the password
   - For the above example password, the SHA256 hash code will be: `220A86AF58EA9D9D3C50353054F31BE6F01E9F872323755FEAF7E48D7988659E`
   - By using this procedure, the actual password can remain as a secret, especially if the pre-provisioning of the servers will be conducted by personnel not authorized to manage the servers.
3. Create a file named `config.xml`.
   - The file must be named exactly as shown.
4. Place the following XML-formatted text into the file and insert the hash code as shown:

```
<SystemConfiguration>
        <Component FQDD="iDRAC.Embedded.1">
                <Attribute Name="Users.2#SHA256Password">
                        220A86AF58EA9D9D3C50353054F31BE6F01E9F872323755FEAF7E48D7988659E
                </Attribute>
                <Attribute Name="Users.2#SHA256PasswordSalt"></Attribute>
        </Component>
</SystemConfiguration>
```

5. Create a folder named `System_Configuration_XML`.
   - The folder must be named exactly as shown

6. Place the file `config.xml` in the `System_Configuration_XML` folder.
7. Place the `System_Configuration_XML` folder in the top-level or root folder of the USB drive.
    - It does not matter if the USB drive contains other folders or files.
8. Insert the USB drive into the iDRAC-Direct Micro-USB Port.
    - The green status LED will illuminate, blinks a few times, and then stops blinking. At this point, it implies that the configuration import is complete. The import takes about 15 seconds.
    - **Important**: If Option 2 for the USB drive is used, ensure the USB drive and cable are first assembled, insert the micro USB connector end of the cable into the iDRAC Direct Micro-USB port.
    - The power state of the server is not relevant.
9. This USB Drive Setup can be used to pre-provision multiple servers
   The USB drive will accumulate for audit purposes a results folder for each server that was pre-provisioned using this setup. The results folder will contain a XML formatted file which will record the Service-Tag of the Server, the date and time the action was performed and finally the identification of the job performed by the iDRAC doing the import. This job-ID will also be recorded in lifecycle logs of the acting iDRAC. The iDRAC Direct SCP feature is disabled after this first operation unless it is explicitly re-enabled by the user.

6.2 Host: PXE Boot with CLI commands

This section describes how Microsoft Windows Pre-installation Environment can be combined with the Dell OpenManage Deployment Toolkit (DTK) to help deploy a minimal operating system (OS) and run an automated RACADM script to change the password for the administrator default user account. The steps are as follows:

1. Obtain the DTK WINPE executable image available at **www.dell.com/support**.
2. Extract DTK WINPE executable.
3. Go to the extracted path and edit `WINPE10.x.driverinst.bat`.
4. Add the following command for modifying the password after the `8-Loading HAPI driver` section:

```
echo racadm set iDRAC.Users.2.Password BlueDi@mond7777777 >>
WINPEPATH%\mount\windows\system32\STARTNET.CMD
```

5. Create a bootable media:

    a) Click **Start → → All Programs Microsoft Windows ADK**.
    b) Click **Windows PE Tools Command Prompt** to open the command line interface (CLI).
    c) Navigate to `C:\Program Files\Windows AIK\Tools\amd64` directory on the system.
    d) Run the script: `WINPE10_driverinst.bat` <*WIMPATH*> <*DTKPATH*>
        a. *Where,* <*WIMPATH*> is the destination path to create the directory structure for Windows PE, and <DTKPATH> is the path for the Dell drivers in the extracted DTK toolkit. For example:
            i. `WINPE10_driverinst.bat C:\winpe10 C:\DELL\x64\DRIVERS`
            This pre-installs the Dell drivers into Windows PE image.
    e) The successful execution of the above commands creates a bootable ISO image for Windows PE 10 at <*WIMPATH*>.

6. Boot the DTK ISO image created above with the PXE configuration.
   The password for the administrator default user account is now set as part of WINPE startup.

7 Managing password—At-the-box access

The following sections provide a short summary of the various at-the-box access features and functions available to manage the password for the administrator-default user account.

7.1 Host: System Setup

If the system is connected to a VGA monitor and keyboard, the system BIOS boot screen is another way to access the System Setup interfaces, where it is possible to manage the password for the iDRAC administrator default user account.

Figure 10 shows the sequence of screen shots to help navigate to the screen where the password can be modified.

1. After turning on the system, press the F2 key as soon as the boot screen prompts to press F2.
2. After the **System Setup** page is displayed, select **iDRAC Settings.**
3. Select **User Configuration**.
4. On the **User Configuration** page, type the new password.
5. Also, change the user name.
   The default username for the administrator default user account is ‘root’. As indicated by the warning message on the screen, changing both the default password and the default username is a best practice to reduce the security risk of managing the administrator default user account.

Note: It must noted that there is no challenge for the original password before changing the password. This behavior has been provided as a convenience measure, especially in the case where the password for the administrator default user account has been forgotten. Use this method to change the password under such circumstances.

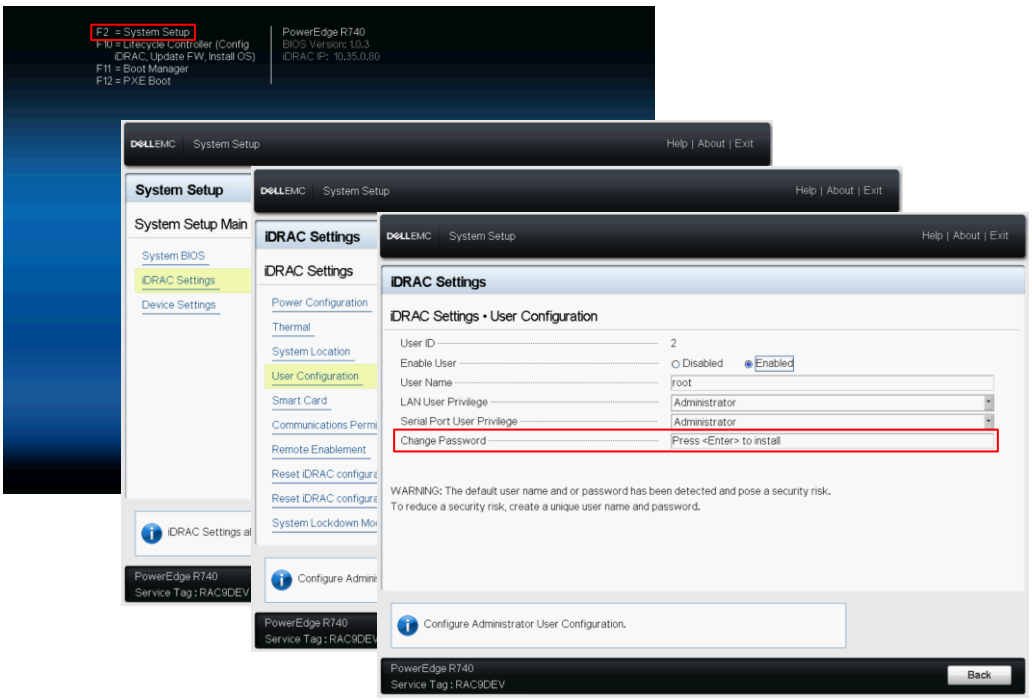

Figure 10 System Setup to manage the password for iDRAC administrator default user account

7.2 iDRAC Direct USB-NIC feature

This feature allows direct access to the iDRAC web-interface without requiring network connectivity by using the iDRAC Network Systems Management port. Instead, local connectivity can be managed by using a Micro-USB 2.0 cable as shown in Figure 11.

Figure 11 Micro-USB 2.0 Cable

1. Connect the micro-USB male connector end of the cable to iDRAC Direct Micro-USB port on the System Front Panel (Right Control Panel).
2. Connect the USB 2.0 male connector end of the cable to the USB port of the laptop computer. Assuming that the Microsoft Windows operating system is running on the laptop, an Ethernet-over-USB connection will be automatically established and the laptop will be configured with a static-IP address. The static-IP address is https://169.254.0.3.
3. Point the web browser on the laptop to this address.
   The login web-pages will be presented as described in section 8.1 of this document.
4. Follow the directions presented in that section.

8 Managing password—Remote network access

The following sections provide a short summary of the various remote network access features and functions available to manage the password for administrator default user account.

8.1 Web interface

When logging in to the iDRAC web interface for the very first time and if an incorrect password is entered for the administrator default user account, the message highlighted Figure 12 is displayed. This message provides a clue that the factory generated default password option is in place for the default user account. That is, the factory default or shipping value is the factory generated default password. As such, the message directs you to check the pull-out Information Tag located on the front panel of the chassis.

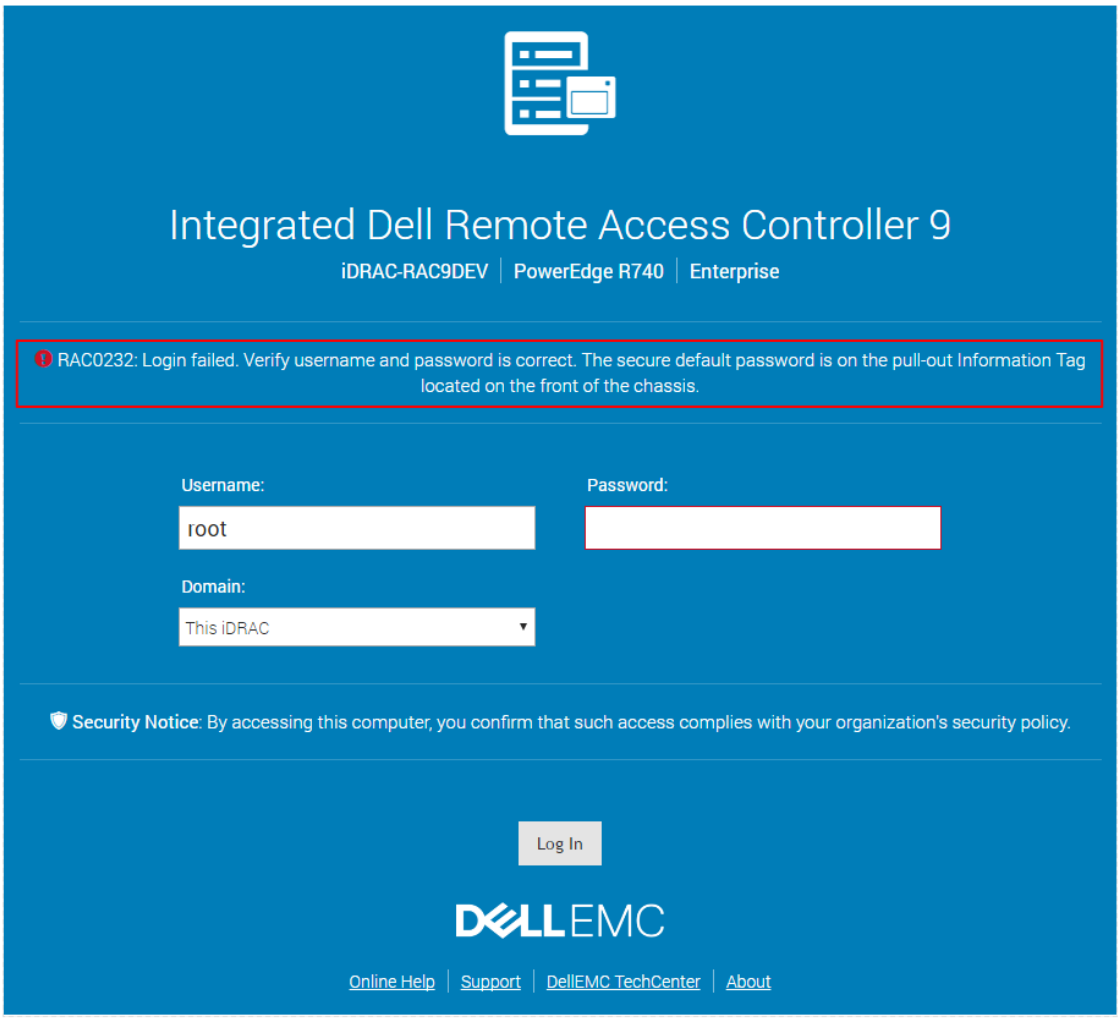

Figure 12 Message about where to locate the factory generated default password

- After successfully logging in, the web page is the first convenient opportunity to change the password for the administrator default user account.
- Messages prompt you to change the default factory settings.
- Options are displayed to prevent the display of this warning and also keep the factory default password.
- Do not select these options unless there are strong organizational security policies and robust networking security policies in place.
- Also, by not selecting these options, further reminders will provided to change the factory default password at the next login if it was not possible to change the password at the earlier opportunity.

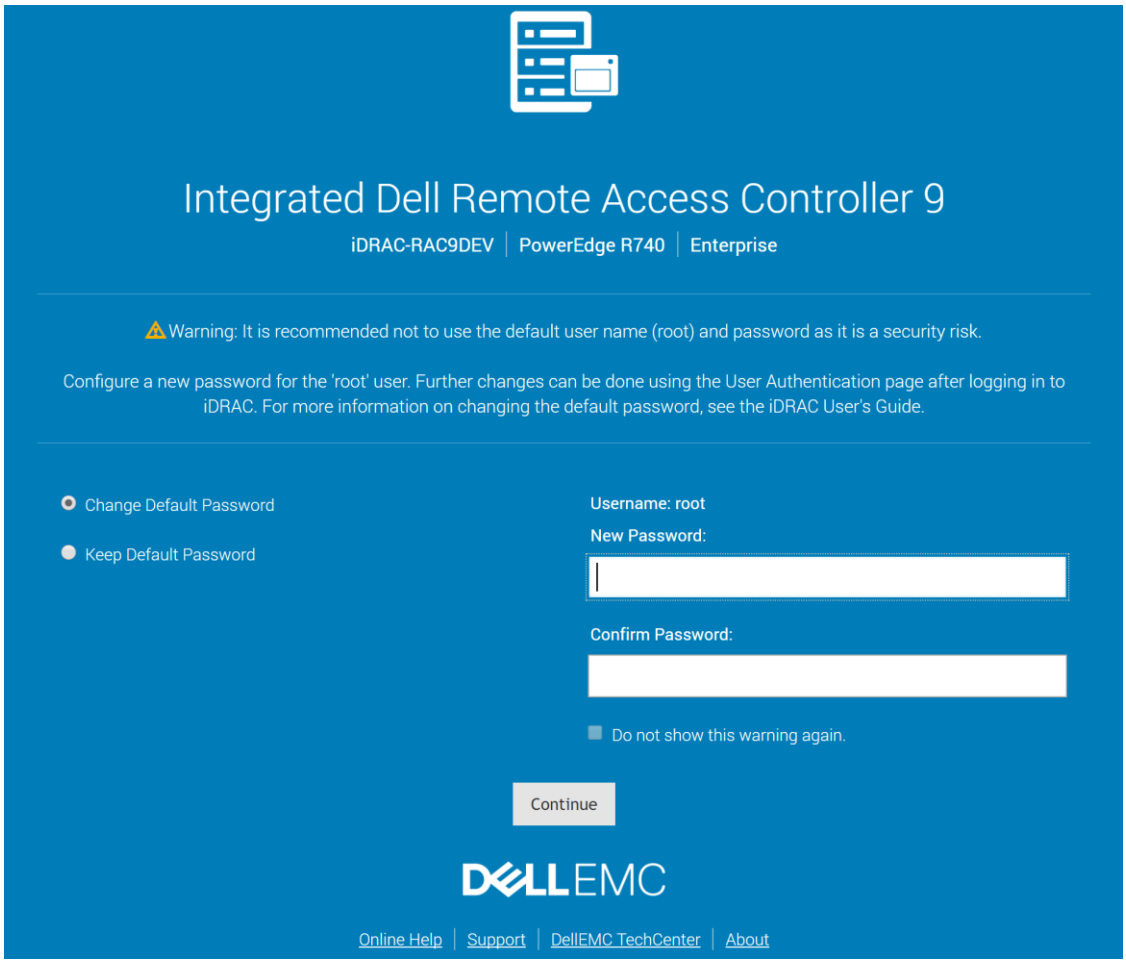

Figure 13 Warning and prompts to change the factory default password

If the administrator default user account credentials were either left unmodified or were changed, it is possible to manage the details by navigating to the **iDRAC Settings** page. On the **Users** tab, there will be listing of the user accounts. See figure 14. Note that the username for the administrator default user account can also be changed. As a reminder, the default username for the factory default user account is 'root'. If this username is changed, make a note that ID for the factory default user account is two (2). Therefore, in future, if details for the administrator user account need to be altered, you must select ID 2.

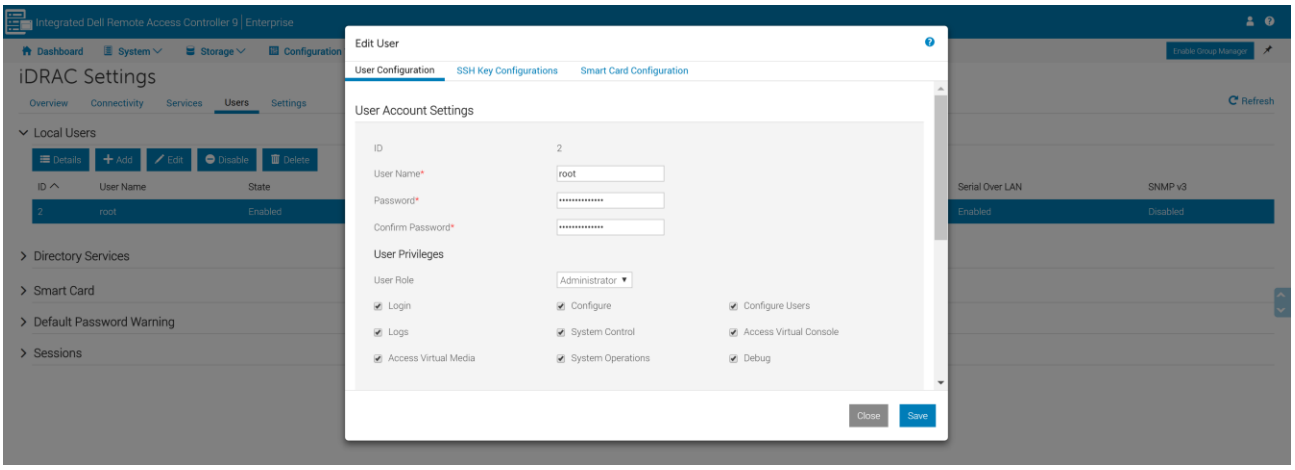

Figure 14 Web-page screen-shot showing the details to manage the user account passwords

8.2 Host: OS-based CLI commands

If the systems are already provisioned with OSs and the remote access facilities for these OSs are enabled, these facilities can be used to invoke a few methods for IDRAC CLI access on the managed system itself. These IDRAC CLI methods are:

- Local RACADM
- IPMI

Local RACADM CLI: is a utility that supports running RACADM commands from the managed system's OS. It is available on the latest *Dell Systems Management Tools and Documentation DVD ISO* which is available for download at dell.com/support. After installing, the following RACADM command can be used to change the password for the administrator default user account.

```
racadm set iDRAC.Users.2.Password BlueDi@mond7777777
```

IPMI CLI: is a utility that supports executing standards based IPMI commands from the managed system's operating system. The IPMI Specification provides a standard way to do both simple and complex server management functions. An open-source version of this utility for a number of operating systems is IPMIUTIL which is available at ipmiutil.sourceforge.net. After installing, the following IPMI command can be used to change the password for the administrator default user account.

```
ipmiutil user set 2 password BlueDi@mond7777777
```

Note: It must noted that there is no challenge for the original password before changing the password. This behavior is available as a convenience measure especially in the case where the password for the administrator default user account has been forgotten. Use this method to change the password under such circumstances.

9 Manage password—Reset configuration to factory default

When resetting the iDRAC configuration to factory default, there are various options to help you manage how the default user account and the associated default password are handled.

The shipping user name for the default user account is root. The associated shipping default password for this user account will either be the legacy default password or factory generated default password .

The options to reset the iDRAC configuration to factory defaults are as follows:

- Option 1: Discard all settings, but preserve user and network settings
- Option 2: Discard all settings and reset default username to root and password to the shipping value (root/shipping-value)
- Option 3: Discard all settings and reset default username to `root` and `password` to calvin (root/calvin)

Option 1 is recommended if you are performing the reset configuration to factory defaults from a remote network location. This option will preserve your user and network settings thereby allowing you to maintain your remote network access to the iDRAC after the reset.

Option 2 is provided to allow you to fully reset the iDRAC configuration to factory defaults where all settings are discarded. If you intend to use this option from a remote location, then make sure your network is set for DHCP operation and you have full knowledge of the shipping password for the default user account. Remember that shipping password may be the factory generated default password.

Option 3 can also be used if you are performing the reset configuration from a remote location. In this case, the assumption is that although your network settings are discarded, your network access will be restored by virtue of the DHCP setting being enabled by default as this is the shipping factory default for this setting and of course your network environment is provisioned for DHCP operation. If your network is not set for DHCP operation, then do not use this option. The other convenience aspect of this option is that although all your user settings are discarded, the default user account setting is reset to a known state. In this case, default username to root and password to ‘calvin’.

9.1 Using the web interface

Figure 15–16 depict the options available to help manage the administrator user account password when the feature to reset the iDRAC configuration to factory default or shipping values.

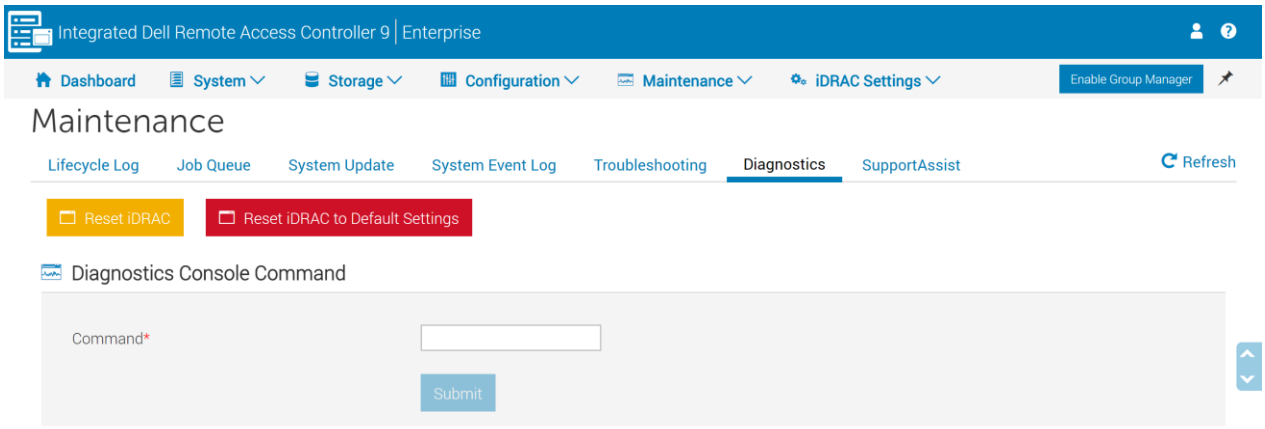

Figure 15 Navigating to the reset iDRAC Configuration page

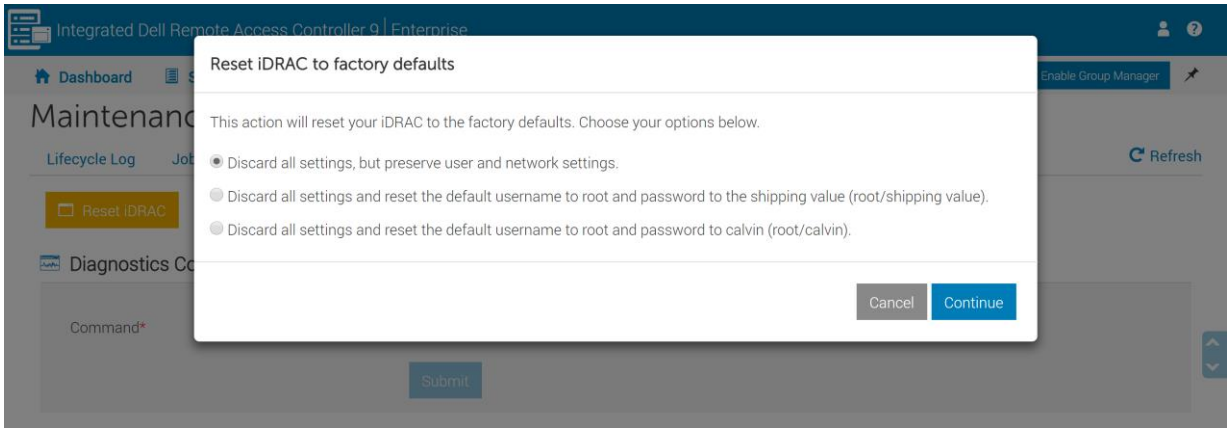

Figure 16 Options to reset iDRAC Configuration to factory default

9.2 Using RACADM CLI

The following CLI command examples show the options available to help manage the administrator user account password when the feature to reset iDRAC configuration to factory default or shipping values.

Following the description of the reset options described above, here are the reset options with the equivalent CLI commands and attributes.

Option 1 > `racadm racresetcfg`
Option 2 > `racadm racresetcfg -all`
Option 3 > `racadm racresetcfg –rc`

To access the RACADM CLI remotely by using the iDRAC system management network port, use any Secure Shell client.

10 Replacing the system board

The Easy Restore feature provides the functionality to back up and restore the iDRAC configuration data. The configuration data is automatically backed up on a non-volatile storage. The non-volatile storage is located on the chassis front panel so that it is independent of the system board. The configuration data includes all the user account information and factory-programmed default settings such as the factory generated default password.

10.1 Easy Restore feature

When the system-board is replaced and the system is turned on, the **BIOS boot-up** screen provides directions to restore all the backed up configuration data.

All the user account information is part of the configuration data and is backed up. The user account information will be restored to the same level prior to the system board replacement. For example, if the default administrator user account (root) had the password changed by the user to a private setting; say, **BlueJay97**, this will still be the user account information after the new system board has been installed and operationalized.

Similarly, all factory-programmed default settings such as the factory generated default password is also part of the configuration data and is backed up. So, if the system with the newly installed system board now has the iDRAC Configuration reset to factory or shipping default properties, the password for the administrator user account (root) will be set to the shipping password of the original system. If the shipping password was the factory generated default password, the password will be the same as that located on the information tag of the system.

Conclusion

The iDRAC9 for 14G PowerEdge Servers continues build on past generations with greater levels of security while continuing to provide better features and functions for systems management for greater ease and convenience. With the factory generated default password feature, all network access to the iDRAC is secured allowing the simplicity and convenience of DHCP network services to be utilized with minimal pre-provisioning requirements. Just rack-n-stack the systems and hookup the iDRACs to the systems management network allowing DHCP services to do the rest. Remember, with this greater convenience, comes the need for better best practices for asset management, especially to collect the factory generated default passwords for the systems to ease later remote network access for further deployment actions and other systems management activities.

A Technical Support and Resources

Dell.com/support is focused on meeting user needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure user success on Dell EMC Storage platforms.