iDRAC10 Security Configuration Guide

1.10.xx Series

December 2024
Rev. A00

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Overview

Dell PowerEdge servers have featured robust security for several generations, including the innovation of using silicon-based data security. As a key management component in Dell PowerEdge servers, the integrated Dell Remote Access Controller (iDRAC) offers industry-leading security features that adhere to and are certified against well-known NIST standards and Common Criteria.

For more information about iDRAC certifications and standards, see the white paper - Managing Web Server Certificates on iDRAC.

The iDRAC development team focuses on providing best in class server management capabilities and ensures that these can be exercised to meet a user's security requirements. The purpose of this document is to describe the security features offered by iDRAC10 that can be configured by the end user and provide the recommended settings and procedures that are required to maximize the security posture of the system.

The intended audience for this document includes system administrators who are responsible for maintaining and deploying servers and ensuring that network and infrastructure security best practices are followed.

NOTE: The information in this publication is provided "as-is." Dell Technologies makes no representations or warranties of any kind about the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

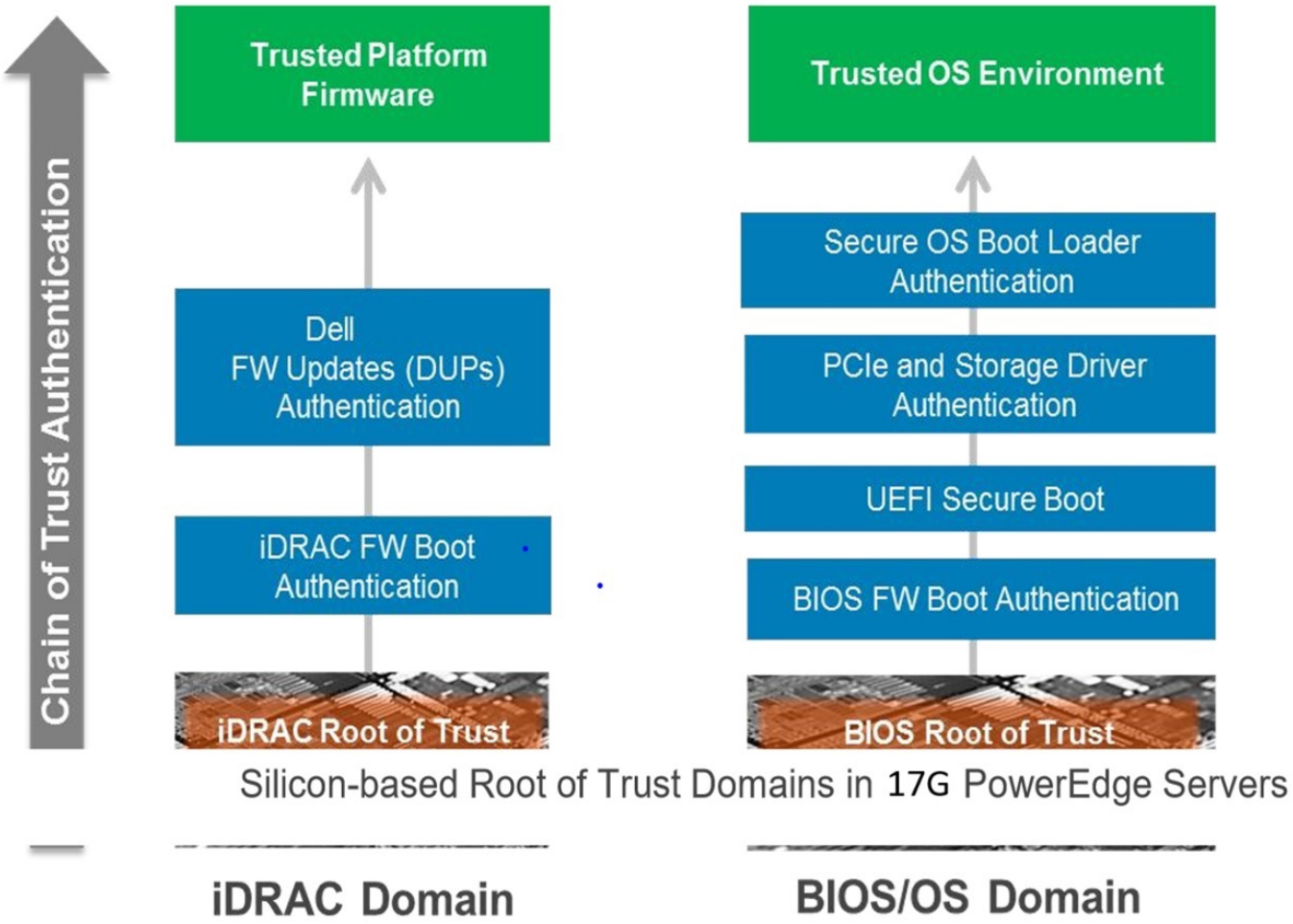
The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information that is contained in this document or materials that are linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

NOTE: For a list of features that are not supported in iDRAC10 version 1.10.17.00, see the section **Features not supported in this release** in the iDRAC10 User's Guide.

2

Built in iDRAC and PowerEdge Security

The iDRAC boot process uses its own independent silicon-based Root-of-Trust that verifies the iDRAC firmware image. The iDRAC Root-of-Trust also provides a critical trust anchor for authenticating the signatures of Dell firmware update packages (DUPs).



Topics:

- Silicon-based Root-of-Trust
- Cryptographically Verified Trusted Booting
- Signed Firmware Updates
- Non-Root Support
- SELinux
- iDRAC Credential Vault
- BIOS Recovery and Hardware Root of Trust (RoT)
- Live Scanning

Silicon-based Root-of-Trust

PowerEdge servers that are enabled with iDRAC use an immutable, silicon-based Root-of-Trust (RoT) to cryptographically attest to the integrity of BIOS and iDRAC firmware. This Root-of-trust is based on one-time programmable, read-only public keys that provide protection against malware tampering. iDRAC provides enhanced security with the use of a new dedicated security processor with no external interfaces to store all authentication keys and perform iDRAC secure boot. The BIOS boot process leverages Intel Boot Guard technology along with SPDM measurement verification by iDRAC to verify the digital signature of the cryptographic hash of the boot image. A failure to verify the boot image results in a shutdown of the server and a user notification in the Lifecycle Controller Log. If Boot Guard validates the boot image successfully, the rest of the BIOS modules are validated by using a chain of trust procedure until control is handed off to the operating system or hypervisor.

With chain of trust, each BIOS module contains a hash of the next module in the chain. The key modules in BIOS are the Initial Boot Block (IBB), Security (SEC), Pre-EFI Initialization (PEI), Memory Reference Code (MRC), Driver Execution Environment (DXE), and Boot Device Selection (BDS). If Intel Boots Guard authenticates IBB, then IBB validates SEC+PEI before handing control to it. SEC+PEI then validates PEI+MRC which further validates the DXE+BDS modules. At this point, control is handed over to UEFI Secure Boot as explained in later sections.

Cryptographically Verified Trusted Booting

One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an OS or updating firmware. The iDRAC boot process is verified using a silicon-based Root-of-Trust to meet recommendations in NIST SP 800-147B ("BIOS Protection Guidelines for Servers") and NIST SP 800-155 ("BIOS Integrity Measurement Guidelines").

Signed Firmware Updates

Enhanced firmware authentication is embedded within many third-party devices which provide signature validation using their own Root-of-Trust mechanisms. This prevents the possible use of a compromised third-party update tool from being used to load malicious firmware into devices like NIC or storage drive (and bypassing the use of signed Dell update packages). Many of the third-party PCIe and storage devices that are shipped with PowerEdge servers use a hardware Root-of-Trust to validate their respective firmware updates.

PowerEdge servers have digitally signed firmware updates for several generations to assure that only authentic firmware is running on the server platform. The firmware packages are digitally signed using SHA-512 hashing with ECDSA-384 encryption for the signature for all key server components including firmware for iDRAC, BIOS, PERC, I/O adapters and LOMs, PSUs, storage drives, FPGA, and backplane controllers. iDRAC scans firmware updates. To verify the authenticity of the firmware running on the system, the silicon-based Root-of-Trust is employed, and current signatures are compared to expected signatures. Any firmware package that fails validation is aborted and an error message is logged into the Lifecycle Controller Log (LCL) to alert IT administrators.

If any firmware in any device is suspected of malicious tampering, IT administrators can rollback many of the platform firmware images to a prior trusted version stored in iDRAC. Retain two versions of device firmware on the server - the existing production version (N) and a prior trusted version (N-1).

Non-Root Support

iDRAC10 firmware ensures that all internal iDRAC processes only grant access according to the principle of least privilege access, a core security concept. This approach provides protection against programming flaws, intrusion attempts, and malware. The protection ensures that access is only granted to those who need it and that systems or users cannot access files or hardware that are outside the scope of their defined roles. For example, the process that provides Virtual KVM support should not be able to change fan speeds. If Virtual KVM Support user roles have different access privileges from Fan Speed Controls roles, it becomes easier for the system to prevent attacks from propagating from one process to another.

SELinux

SELinux is based on defense-in-depth design, with multiple layers of protection and functionality to help secure this critical system component. SELinux is a core Linux security technology that is merged in the standard Linux kernel. SELinux has gained

adoption within many Linux distributions. Red Hat Enterprise Linux (RHEL) was one of the first adopters other Linux users followed. SELinux is now maintained in the core Linux kernel by a dedicated group including Red Hat, Network Associates, Secure Computing Corporation, Tresys Technology, among others. This security technology uses a method referred to as Mandatory Access Control. This method enables you to specify all the privileges that internal processes must complete their tasks and limits the access to only those tasks. This is important because most attempts to hack a system modify processes to perform actions that are not intended in the original product design.

Dell wrote comprehensive security policies in SELinux for every task that runs on the iDRAC. Dell conducts comprehensive tests to ensure that no features are affected by the applied policies. SELinux operates at the core kernel level on the iDRAC and cannot be disabled or modified by the users. SELinux adds a mitigation factor that prevents many programming flaws from being further exploited to gain elevated access to the system. Moreover, SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to users enrolled in this feature. In a future release of iDRAC, these logs are made available in the Lifecycle Controller Logs.

iDRAC Credential Vault

The iDRAC service processor provides a secure storage memory that protects various sensitive data such as iDRAC user credentials and private keys for default self-signed TLS/SSL certificates. Secure storage memory, a type of silicon-based security, is encrypted with a unique immutable root key that is programmed into each chip during the manufacturing process. Immutable keys protect against physical attacks from hackers who desolder or removes the chip to gain access to the data stored.

BIOS Recovery and Hardware Root of Trust (RoT)

Recovery from corrupted or damaged BIOS images due to malicious modification of data, power surges, damages, or other unforeseeable events is imperative. A recovery BIOS image is stored in the 2nd serial peripheral interface (SPI) to facilitate server recovery from an unbootable state.

The recovery sequence can be initiated through any of the following approaches with iDRAC as the main orchestrator of the BIOS recovery task:

1. Auto recovery of BIOS primary image / recovery image - BIOS image is recovered automatically during the host boot process after the BIOS corruption is detected by BIOS itself.
2. Forced recovery of BIOS Primary/recovery image - User initiates an out-of-band (OOB) request to update BIOS either because they have a new updated BIOS or BIOS fails to boot or crashes.
3. Primary BIOS ROM update - The single Primary ROM is split into Data ROM and Code ROM. iDRAC has full access/control over Code ROM. It switches MUX to access Code ROM whenever needed.
4. BIOS Hardware Root of Trust (RoT) - During every host boot (only cold boot or A/C cycle, not on a warm reboot), iDRAC ensures that the Root-of-Trust (RoT) verifies the authenticity of BIOS. The RoT automatically initiates during a host boot only. The RoT BIOS authentication process cannot be initiated through other interfaces .The iDRAC **Boot first** policy verifies the host BIOS ROM contents on every AC cycle and host DC cycle, ensuring that the BIOS and the host both shall boot securely.

Live Scanning

BIOS live scanning verifies the integrity and authenticity of the BIOS image in the BIOS primary ROM when the host is powered ON but not in POST.

NOTE:

- This feature requires iDRAC Datacenter license.
- A user must have Debug privilege for operating this feature.

iDRAC performs verification of immutable sections of BIOS image automatically at the following scenarios:

- At AC power cycle/Cold boot
- On a schedule determined by user
- On demand (initiated by user)

Successful result of live scanning is logged to Lifecycle Controller Log (LCL). Failure result is logged to both LCL and system event logs (SEL).

Table 1. Platforms, iDRAC Versions, and Feature Support

Platforms	Supported Versions	Features
All 17G platforms	1.10.05.00	BIOS Integrity check at host boot and live scanning of BIOS image

3

Securely Configuring iDRAC Web Server

One of the most widely used interfaces offered in iDRAC is a web server that supports remote RACADM, Redfish, and iDRAC GUI communication. The web server includes various configurable security settings to meet user security requirements such as HTTPS redirection, encryption strength, TLS protocol, and filtering the available TLS cipher suites. Below are the recommended configurations to maximize security for iDRAC's webserver.

- Redirecting all HTTP requests to HTTPS
- Configure TLS 1.3
- Enable 256-bit encryption strength
- Limit cipher suites to strongest available
- Use CA Signed TLS/ SSL Certificates
- Enable Simple Certificate Enrollment Protocol (SCEP)

Topics:

Webserver Information

The following information is available and read-only to the end user without authentication. This is useful to identify and provision a server within a datacenter. If this information must be protected, it is recommended to follow the Best Practices listed in the Appendix.

- Service Tag
- Host Name
- Firmware Version
- MAC Address
- Server Model
- Server Generation
- Manufacturer Name
- Product License

Certain URIs and files on the iDRAC are available unauthenticated. These are required for loading the GUI login page and for discovery of Redfish endpoints.

- /restgui/ - These contain Javascripts, CSS files, and font files required for the iDRAC GUI. These are static by nature and do not contain any information specific to the system.
- /software/ - These contain downloadable applications that are required to launch virtual console. These are precompiled binaries and do not contain any information specific to the system.

Enabling HTTPS Redirection

HTTP to HTTPS redirection redirects webserver communication from HTTP port (default is 80) to HTTPS port (default is 443). This ensures that only secure encrypted connections are established when clients connect to iDRAC using remote RACADM, Redfish, or iDRAC GUI. HTTPS redirection is enabled by default.

NOTE: This setting does not affect established connections. A user must have Configure iDRAC privilege to enable or disable HTTPS redirection and the user must log out and log in to iDRAC for this setting to take effect. When you disable

this feature, a warning message is displayed, and an event is recorded in the Lifecycle Controller log file when this feature is enabled or disabled.

Use the following RACADM command to enable HTTP to HTTPS redirection, in case it has been disabled:

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

Configuring the TLS Protocol

iDRAC offers two TLS protocol versions for secure webserver connections. TLS 1.3 is the most secure configuration and should be used whenever possible. TLS 1.0 is discouraged and is available only for backward compatibility.

By default, iDRAC is configured to use TLS 1.2 and higher. You can configure iDRAC to use any of the following:

- TLS 1.2 only
- TLS 1.2 and higher
- TLS 1.3 only

To configure the TLS protocol to TLS 1.3:

1. Go to **iDRAC Settings** > **Services**.
2. Click the **Services** tab and then click **Web Server**.
3. In the **TLS Protocol** drop-down, select TLS 1.3 version and click **Apply**.

Configuring Encryption Strength

iDRAC offers four encryption strength configurations. By default, iDRAC is configured to use an encryption strength of 128-bit or higher. The recommended secure configuration is 256-bit or higher.

- Auto negotiate
- 128-bit or higher
- 168-bit or higher
- 256-bit or higher

To configure Web Server Encryption to 256-bit or higher

1. Go to **iDRAC Settings** > **Services**.
2. Click the **Services** tab and then click **Web Server**.
3. In the **SSL Encryption** drop-down, select 256-bit or higher and click **Apply**.

Configuring Cipher Suite Selection

Cipher Suite Selection can be used to limit the ciphers that are offered by iDRAC's web server for client communications allowing the user to determine how secure the connection should be. It provides another level of filtering for the effective in-use TLS Cipher Suite. These settings can be configured through iDRAC web interface and RACADM command-line interface. While there are no weak ciphers suites enabled on iDRAC, the most secure available in iDRAC is TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and all others can be removed using this feature to maximize security. The cipherlist format is defined in the OpenSSL documentation.

CAUTION: Using OpenSSL Cipher Command to parse strings with invalid syntax may lead to unexpected errors.

NOTE: This is an advanced security option. Before you configure this option, ensure that you have thorough knowledge of the following:

- The OpenSSL Cipher String Syntax and its use
- Tools and Procedures to validate the resultant Cipher Suite Configuration to ensure that the results align with the expectations and requirements

NOTE: For more information about cipher strings, see the OpenSSL documentation.

The TLS 1.3 Ciphers supported by iDRAC are:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

When TLS 1.3 is used, Set Cipher string functionality is not supported.

Remote Syslog with TLS

The default setting in iDRAC is unencrypted RSyslog which is required for backward compatibility. Supporting TLS based Remote Syslog requires uploading trust certificates between the client device (iDRAC) and the server (Syslog server). Multiple steps are required to set up this configuration with external inputs.

With encrypted Remote Syslog, the devices and syslog servers share the same CA certificate. iDRAC supports up to three Remote Syslog servers in the existing cleartext UDP Remote Syslog implementation. But with encrypted Remote Syslog, the usage is normally just one target Syslog server. The open-source software used to implement the Remote Syslog protocol also has limitations to support only one secure target server, and does not allow combining multiple CA certificates. Hence iDRAC provides option to select only one secure Remote Syslog target.

The existing unencrypted Remote Syslog feature uses UDP port, the default port is 514.

A new iDRAC attribute `SecurePort` is used to specify the secure Remote Sylog port number, default port being 6514. Secure Syslog uses TCP port.

Simultaneous encrypted and unencrypted targets are not supported. iDRAC user must select either of the options by changing the value of the iDRAC attribute `SysLogEnable`.

TLS based Remote Syslog servers and clients use the same CA certificate in the configuration settings, which is obtained from a CA server. iDRAC provides a user interface to upload this CA certificate and add it to its configuration file and restart the Remote Sylog service.

By default, iDRAC uses anonymous identity for the encrypted Remote Syslog communication. This can be overridden by generating a signed trust certificate to prove iDRAC's authenticity. iDRAC provides a user interface to create a certificate signing request and an option to upload and view the iDRAC trust certificate.

The existing telemetry feature allows only anonymous identity for iDRAC as a syslog client.

iDRAC has user interfaces as part of the Telemetry features to upload CA certificate, and the web server feature has options to generate certificate signing request (CSR) and upload the signed certificate. These user interface templates could be reused in the context of the TLS Remote Syslog feature.

iDRAC web certificate can be used as the iDRAC identity certificate, but normal customer usage is to use separate certificates for web server and Remote syslog. Often, a Remote Syslog identity certificate can be generated within the company's internal certificate signing server setup. iDRAC does not provide option to reuse the web server certificate.

NOTE: Initial iDRAC versions included the Telemetry feature using Syslog code. Later versions of iDRAC changed the Telemetry feature to a different open-source code which no longer has any dependency to the Remote Syslog feature. The Telemetry feature also uses a different configuration of iDRAC attributes.

Setting Cipher Suite Selection using the iDRAC GUI

To set ciphers in the iDRAC GUI go to **iDRAC Setting** > **Services** > **Web Server**.

If you would like to block more than one cipher use a colon, space, or comma as a separator.

4

Secure Connection Using TLS/SSL Certificate

The iDRAC web server uses a TLS/SSL certificate to establish and maintain secure communications with remote clients. Web browsers and command-line utilities, such as RACADM and Redfish, use this TLS/SSL certificate for server authentication and establishing an encrypted connection.

There are several options available to secure the network connection using a TLS/SSL certificate. iDRAC web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Whichever method is chosen, once iDRAC is configured and the TLS/SSL certificate is installed on the management stations, TLS/SSL enabled clients can access iDRAC securely and without certificate warnings.

For more information, see the white paper - Managing Web Server Certificates on iDRAC.

Certificate upload can be automated by using Redfish (ImportSSLCertificate action) (or RACADM (sslcertupload command) scripts. For details, see:

- iDRAC Redfish API Documentation on Developer portal.
- iDRAC RACADM CLI Guide on the iDRAC page.

Table 2. TLS/SSL Certificate Analysis

Certificate	Description	Advantages	Disadvantages
Self-Signed TLS/SSL Certificate	This certificate is auto generated and self-signed by the iDRAC. Each iDRAC has a unique self-signed certificate by default.	• Do not have to maintain a Certificate Authority. • Certificates are auto generated by the iDRAC.	• The certificate for each iDRAC must be added to the trusted certificates store on each management station. (Every iDRAC is its own Certificate Authority which must be trusted.)
CA Signed TLS/SSL Certificate with common Public/Private key pair	A certificate signing request (CSR) is generated and submitted to your in-house Certificate Authority or by a third-party Certificate Authority such as VeriSign, Thawte, Go Daddy, and so on, for signing.	• Can use a commercial Certificate authority. Can use a commercial Certificate authority. • If a commercial CA is used, it is likely to be already trusted on your management stations and can be trusted for all iDRACs.	• Must either purchase commercial certificates or maintain your own Certificate Authority • Each iDRAC has same public/private key pair unless user can manage multiple key pairs.
CA Signed TLS/SSL Certificate	A certificate signing request (CSR) is generated by iDRAC and submitted to your in-house Certificate Authority or by a third-party Certificate Authority such as VeriSign, Thawte, Go Daddy, etc. for signing.	• Can use a commercial Certificate authority. • Only must trust one Certificate Authority for all iDRAC. If a commercial CA is used, it is likely to be already trusted on your management stations. • Each iDRAC has a unique public/private key.	• Must either purchase commercial certificates or maintain your own Certificate Authority. • A CSR must be generated and submitted for every iDRAC.
Custom Signing TLS/SSL Certificate (CSC)	The certificate is auto generated and signed using a signing certificate that is uploaded from your in-house Certificate Authority.	• Only must trust one Certificate Authority for all iDRAC. It is possible that your in-house	• Must maintain your own Certificate Authority.

Table 2. TLS/SSL Certificate Analysis (continued)

Certificate	Description	Advantages	Disadvantages
		Certificate Authority is already trusted on your management stations. • Certificates are auto generated by the iDRAC.	

See the Managing Web Server Certificates on iDRACwhitepaper.

Topics:

- Secure Connection Using TLS/SSL Certificate

Secure Connection Using TLS/SSL Certificate

The iDRAC web server uses a TLS/SSL certificate to establish and maintain secure communications with remote clients. Web browsers and command-line utilities, such as RACADM and Redfish, use this TLS/SSL certificate for server authentication and establishing an encrypted connection.

There are several options available to secure the network connection using a TLS/SSL certificate. iDRAC web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Whichever method is chosen, once iDRAC is configured and the TLS/SSL certificate is installed on the management stations, TLS/SSL enabled clients can access iDRAC securely and without certificate warnings.

For more information, see the white paper - Managing Web Server Certificates on iDRAC.

Certificate upload can be automated by using Redfish (ImportSSLCertificate action) (or RACADM (sslcertupload command) scripts. For details, see:

- iDRAC Redfish API Documentation on Developer portal.
- iDRAC RACADM CLI Guide on the iDRAC page.

Table 3. TLS/SSL Certificate Analysis

Certificate	Description	Advantages	Disadvantages
Self-Signed TLS/SSL Certificate	This certificate is auto that is generated and self-signed by the iDRAC. Each iDRAC has a unique self-signed certificate by default.	• Do not have to maintain a Certificate Authority. • Certificates are auto that is generated by the iDRAC.	• The certificate for each iDRAC must be added to the trusted certificates store on each management station. (Every iDRAC is its own Certificate Authority which must be trusted.)
CA Signed TLS/SSL Certificate with common Public/Private key pair	A certificate signing request (CSR) is generated and submitted to your in-house Certificate Authority or by a third-party Certificate Authority such as VeriSign, Thawte, Go Daddy, and so on, for signing.	• Can use a commercial Certificate authority. Can use a commercial Certificate authority. • If a commercial CA is used, it is likely to be already trusted on your management stations and can be trusted for all iDRACs.	• Purchase commercial certificates or maintain your own Certificate Authority. • Each iDRAC has same public/private key pair unless the user can manage multiple key pairs.
CA Signed TLS/SSL Certificate	A certificate signing request (CSR) is generated by iDRAC and submitted to your in-house Certificate Authority or by a third-party Certificate Authority such as VeriSign, Thawte, Go Daddy, so on for signing.	• Can use a commercial Certificate authority. • Only must trust one Certificate Authority for all iDRAC. If a commercial CA is used, it is likely to be	• Purchase commercial certificates or maintain your own Certificate Authority. • A CSR must be generated and submitted for every iDRAC.

Table 3. TLS/SSL Certificate Analysis (continued)

Certificate	Description	Advantages	Disadvantages
		already trusted on your management stations. • Each iDRAC has a unique public/private key.	
Custom Signing TLS/SSL Certificate (CSC)	The certificate is auto that is generated and signed using a signing certificate that is uploaded from your in-house Certificate Authority.	• Only must trust one Certificate Authority for all iDRAC. It is possible that your in-house Certificate Authority is already trusted on your management stations. • Certificates are auto that is generated by the iDRAC.	• Maintain your own Certificate Authority.

See the Managing Web Server Certificates on iDRACwhitepaper.

5

Automatic Certificate Enrollment

iDRAC offers two protocol standards - ACME (Automated Certificate Management Environment) and SCEP (Simple Certificate Enrollment Protocol). ACME and SCEP are used for managing certificates to large number of network devices using an automatic enrollment process. iDRAC can now integrate with SCEP-compatible servers like Microsoft Server's NDES service to maintain SSL/TLS Certificates automatically. This feature can be used to enroll and refresh a soon-to-be-expired web server certificate.

With a Datacenter license, iDRAC offers Automatic Certificate Enrollment.

iDRAC's Automatic Certificate enrollment feature automatically assures SSL/TLS certificates are in place and up to date for both bare-metal and previously installed systems. This security feature keeps iDRAC SSL/TLS certificates current.

iDRAC Web User Interface can be reached with any supported browser. It uses an SSL/TLS certificate to authenticate itself to web browsers and command-line utilities running on management stations thereby establishing an encrypted link. If the Certificate Authority that issued the certificate is not trusted by the management station, warning messages are displayed on the management station. Having an iDRAC SSL/TLS certificate in place ensures a validated and secure connection.

6

Secure Shell (SSH)

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution. On iDRAC, SSH can be used to run RACADM commands. The SSH service is enabled by default on iDRAC.

The security settings that are recommended for SSH are:.

- Enable PKI
- Do not use DSA keys
- Enable only elliptic curve key exchanges
- Enable only ciphers with 256-bit key strength or higher

Topics:

SSH Cryptography Configuration

iDRAC provides user control over the cryptographic settings for the SSH daemon such that the user can determine the ideal settings for their environment. The control given to the user is not a relaxation of the settings in any manner. Instead, the feature allows the user the ability to modify the value set for each option to achieve a narrower and stringent cryptographic policy. In other words, the user can only remove values from the options but is not able to add any values other than those that have been defined/allowed in the default value-set.

The cryptographic policies are configured using the following options:

- Ciphers—Ciphers
- Host-Key-Algorithms—HostKeyAlgorithms
- Key-Exchange Algorithms—KeyExchangeAlgorithms
- MACs—MACs

Typically, the values for each of these options are set to prudent settings that reflect the best security practices that cater to a wide variety of environments. As such the iDRAC default settings for these options are the same as those described by the SSH package open-source community. These settings can be configured using RACADM command-line interface. Values can only be removed from the options and cannot add any values other than those that have been defined/allowed in the default value-set. See iDRAC RACADM CLI User's Guide.

Following are the commands to view the current set of cryptographic algorithms:

```
racadm>>get idrac.sshcrypto.ciphers

[Key=idrac.Embedded.1#SSHCrypto.1]

Ciphers=chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com

racadm>>

racadm>>get idrac.sshcrypto.hostkeyalgorithms

[Key=idrac.Embedded.1#SSHCrypto.1]

HostKeyAlgorithms=rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519

racadm>>

racadm>>get idrac.sshcrypto.kexalgorithms

[Key=idrac.Embedded.1#SSHCrypto.1]
```

```
KexAlgorithms=curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

racadm>>

racadm>>get idrac.sshcrypto.macs

[Key=idrac.Embedded.1#SSHCrypto.1]

MACs=umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512

racadm>>
```

Following are the steps to remove unwanted or deprecated values. First query the default set and then identify values to remove.

```
racadm>>get idrac.sshcrypto.hostkeyalgorithms

[Key=idrac.Embedded.1#SSHCrypto.1]

HostKeyAlgorithms=rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519

racadm>>
```

Then, run the set command with a subset of values.

```
racadm>>set idrac.sshcrypto.hostkeyalgorithms rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519

[Key=idrac.Embedded.1#SSHCrypto.1]
```

Object value modified successfully

```
racadm>>

racadm>>get idrac.sshcrypto.hostkeyalgorithms

[Key=idrac.Embedded.1#SSHCrypto.1]

HostKeyAlgorithms=rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519

racadm>>
```

Supported SSH Cryptography Schemes

To communicate with iDRAC using SSH protocol, it supports multiple cryptography schemes that are listed in the following table.

Table 4. SSH cryptography schemes

Scheme Type	Algorithms
Asymmetric Cryptography	
Public Key	• rsa-sha2-512 • rsa-sha2-256 • ecdsa-sha2-nistp256 • ssh-ed25519
Symmetric Cryptography	
Key Exchange	• curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
Encryption	• chacha20-poly1305@openssh.com • aes128-ctr • aes192-ctr • aes256-ctr

Table 4. SSH cryptography schemes (continued)

Scheme Type	Algorithms
	• aes128-gcm@openssh.com • aes256-gcm@openssh.com
MAC	• umac-128-etm@openssh.com • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128@openssh.com • hmac-sha2-256 • hmac-sha2-512
Compression	None

Using Public Key Authentication for SSH

iDRAC supports Public Key Authentication (PKA) over SSH as a licensed feature.. When the PKA over SSH is set up and used correctly, you must enter the username while logging into iDRAC. This is useful for setting up automated scripts that perform various functions. The uploaded keys must be in RFC 4716 or OpenSSH format. Else, you must convert the keys into that format. In any scenario, a pair of private and public keys must be generated on the management station. The public key is uploaded to iDRAC local user, and private key is used by the SSH client to establish the trust relationship between the management station and iDRAC. Public Key Authentication is recommended as a security feature because it cryptographically verifies authentication and eliminates the need for password credentials. To achieve the highest level of security, it is recommended to generate an RSA key with a 4096-bit key size which is the maximum that is supported on iDRAC.

You can generate the public or private key pair using:

- PuTTY Key Generator application for clients running Windows
- ssh-keygen CLI for clients running Linux.

The public key can be uploaded using iDRAC Web interface or RACADM command-line interface.

CAUTION: This privilege is reserved for users who are members of the Administrator user group on iDRAC. However, users in the Custom user group can be assigned this privilege. A user with this privilege can modify any user's configuration. This includes creation or deletion of any user, SSH Key management for users, and so on. For these reasons, assign this privilege carefully.

Disable SSH in iDRAC

To avoid or mitigate security risks, disable SSH in iDRAC.

Steps

1. Log in to iDRAC UI.
2. Go to **iDRAC Settings** > **Services** > **SSH**
3. In the **Enabled** list, select **Disabled**.
4. Click **Apply**.

7

Network Security Configuration

iDRAC provides optional networking interfaces that can be used for connection and management. As a security best practice, it is recommended to disable networking interfaces that are unused.

The following configurations are recommended for network security:

- iDRAC NIC Select – Dedicated
- iDRAC VLAN – enabled
- USB Management Port — Disabled
- iDRAC Managed: USB SCP — Disabled
- Pass-through State — Disabled
- Pass-through Mode — USB NIC
- IP Blocking Enabled
- IP Filtering Enabled
- Auto Discovery Disabled or if Auto Discovery is necessary set to DNS

Table 5. Network Configurations from Web Interface and RACADM

Feature	iDRAC Web Interface	RACADM
NIC Selection	**iDRAC Settings** > **Connectivity** > **Network** > **Network Settings** > **NIC Selection - Dedicated**	racadm set idrac.nic.selection 1
VLAN	• **iDRAC Settings** > **Connectivity** > **Network** > **VLAN Settings** > **Enable VLAN ID - Enabled** • **iDRAC Settings** > **Connectivity** > **Network** > **VLAN Settings** > **VLAN ID - <ID Number>**	• racadm set idrac.nic.vlanenable 1 • racadm set idrac.nic.vlanID <ID Number>
USB Management Port	**iDRAC Settings** > **Settings** > **Management USB Settings - Disabled**	• racadm set • idrac.usb.PortStatus 0
Pass-through State	**iDRAC Settings** > **Connectivity** > **OS to iDRAC Pass-through - Disabled**	racadm set idrac.OS-BMC.AdminState 0
Pass-through Mode	**iDRAC Settings** > **Connectivity** > **OS to iDRAC Pass-through - USB NIC**	racadm set idrac.OS-BMC.PTMode 1
IP Blocking	**iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Blocking Enabled – Enabled**	racadm set idrac.IPBlocking.BlockEnable 1
IP Blocking Fail Count	**iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Blocking Fail Count – 3**	racadm set iDRAC.IPBlocking.FailCount 3
IP Blocking Fail Window	**iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Blocking Fail Window – 60**	racadm set iDRAC.IPBlocking.FailWindow 60
IP Blocking Penalty Time	**iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Blocking Penalty Time – 60**	racadm set iDRAC.IPBlocking.PenaltyTime 60
IP Range Filtering	• **iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Ranges** > **IP Range Enabled - Enabled iDRAC Settings** > **Connectivity**	• racadm set idrac.IPBlocking.RangeEnable 1

Table 5. Network Configurations from Web Interface and RACADM (continued)

Feature	iDRAC Web Interface	RACADM
	> **Advanced Network Settings** > **IP Ranges** > **IP Range Address – <IP of Management Station>** • **iDRAC Settings** > **Connectivity** > **Advanced Network Settings** > **IP Ranges** > **IP Range Subnet – <Management Subnet Mask>**	• racadm set idrac.IPBlocking.RangeAddr <IP of Management Station> • racadm set idrac.IPBlocking.RangeMask < Management Subnet Mask>
Auto Discovery	**iDRAC Settings** > **Connectivity** > **Network** > **iDRAC Auto Discovery** > **Auto Discovery – Disabled**	racadm set idrac.autodiscovery.EnableIPChangeAnnounce 0

Topics:

Dedicated NIC and Shared LOM

The most secure network connection is the iDRAC's Dedicated NIC because it can be connected to a network that is physically separated from the production network. This physically segregates the iDRAC management traffic from the production network traffic.

If use of the iDRAC's Dedicated NIC is not feasible for any reason, the iDRAC can be run in Shared LOM mode with a VLAN enabled. But the iDRAC's management traffic is sent across the same wire as the production network. Alternatively, if the use of a VLAN is not possible while in Shared LOM mode, access to the iDRAC must be secured using strong passwords and other security measures described in this document.

OS to iDRAC Pass-through

In servers that have Open Compute Project (OCP) or embedded LAN On Motherboard (LOM) devices, you can enable the OS to iDRAC Pass-through feature. This feature provides a high-speed bi-directional in-band communication between iDRAC and the host operating system through a shared LOM, a dedicated NIC, or through the USB NIC. The OS-BMC lom-p2p (i.e., "LOM-PT") interface uses the OS-to-BMC passthrough capability of the Shared OCP or LOM hardware. This feature only must be enabled if the iDRAC is in Shared LOM mode and the external switch does not support "hairpin" mode. When the iDRAC has LOM-PT enabled, traffic between the server and iDRAC is not sent externally to the network.

The OS-BMC usb-p2p (i.e. "USB-NIC") interface uses hardware on the server motherboard to enable point-to-point connectivity between the server and the iDRAC. This interface can be used to isolate host-to iDRAC traffic from external networks. If server to iDRAC connectivity is needed, USB-NIC is a preferred secure method because it can be used in combination with iDRAC's dedicated NIC. However, as a security best practice, unused interfaces should be disabled if they are not needed. Disable USB-NIC if host-to-iDRAC communication is not needed and iDRAC Service Module (iSM) software is not installed on the server.

VLAN Usage

A VLAN can be configured on the iDRAC if iDRAC management traffic must be separated from production traffic. A VLAN is recommended as a best security practice when iDRAC is in Shared LOM mode or in Dedicated mode to isolate network access to iDRAC's management interfaces. Technologies such as VLANs and firewalls help ensure that only authorized users can access network resources.

IP Blocking

You can use IP blocking to dynamically determine when excessive login failures occur from an IP address and block or prevent the IP address from logging into the iDRAC10 for a preselected time span. IP blocking includes:

- The number of allowable login failures
- The timeframe in seconds when these failures must occur
- The amount of time, in seconds, when the IP address is prevented from establishing a session after the total allowable number of failures is exceeded

As consecutive login failures accumulate from a specific IP address, they are tracked by an internal counter. When the user logs in successfully, the failure history is cleared, and the internal counter is reset. These settings can be edited in the GUI, RACADM, and Redfish.

Enabling this feature is a recommended security best practice. By automatically detecting potential malicious actions being performed and preventing unauthorized access to iDRAC through brute force attacks, IP blocking hardens iDRAC network security resilience.

IP Range Filtering

In addition to IP Blocking, iDRAC offers IP Range filtering options to provide additional security.

- IP filtering limits the IP address range of the clients accessing iDRAC. It compares the IP address of an incoming login to the specified range and allows iDRAC access only from a management station whose IP address is within the range. All other login requests are denied.
- Users can specify up to five (5) different IP ranges to allow more granularity for multi-site or global datacenters.
- This feature can be viewed/edited in the GUI, or by RACADM or Redfish.

Auto-Discovery

The Auto-discovery feature allows newly installed servers to automatically discover the remote management console that hosts the provisioning server. The provisioning server provides custom administrative user credentials to iDRAC so that the un-provisioned server can be discovered and managed from the management console.

Provisioning server works with a static IP address. Auto-discovery feature on the iDRAC is used to find the provisioning server using DHCP/Unicast DNS/mDNS.

- When iDRAC has the console address, it sends its own service tag, IP address, Redfish port number, Web certificate etc.
- This information is periodically published to consoles.

DHCP, DNS server, or the default DNS hostname discovers the provisioning server. If DNS is specified, the provisioning server IP is retrieved from DNS and the DHCP settings are not required. If the provisioning server is specified, discovery is skipped so neither DHCP nor DNS is required.

Since auto-discovery relies on iDRAC, publishing unencrypted information for discovery purposes should only be required in initial provisioning. As a security best practice, this feature should be disabled unless needed. If auto-discovery is necessary, DNS is the preferred method.

Auto Config

The Auto Config feature configures and provisions all the components in a server in a single operation. These components include BIOS, iDRAC, and PERC. Auto Config automatically imports a Server Configuration Profile (SCP) XML or JSON file containing all configurable parameters. The DHCP server that assigns the IP address also provides the details for accessing the SCP file.

SCP files are created by configuring a gold configuration server. This configuration is then exported to a shared NFS, CIFS, HTTP, or HTTPS network location that is accessible by the DHCP server and the iDRAC of the server being configured. The SCP file name can be based on the Service Tag or model number of the target server or can be given as a generic name. The DHCP server uses a DHCP server option to specify the SCP file name (optionally), SCP file location, and the user credentials to access the file location.

NOTE: The user credentials to the network share are sent in plaintext as part of the DHCP response message, so care must be taken when using this Auto Config on an unsecure network that the credentials cannot be used for anything other than accessing the network share.

When the iDRAC obtains an IP address from the DHCP server that is configured for Auto Config, iDRAC uses the SCP to configure the server's devices. Auto Config is invoked only after the iDRAC gets its IP address from the DHCP server. If it does not get a response or an IP address from the DHCP server, then Auto Config is not invoked. HTTP and HTTPS file sharing options are supported for all iDRAC10 firmware. Details of the HTTP or HTTPS address must be provided. In case the proxy is enabled on the server, the user must provide further proxy settings to allow HTTP or HTTPS to transfer information.

If autoconfig is not needed, it is a recommended security configuration to disable this feature to limit the potential attack surface. If required, auto config should use HTTPS as a security best practice.

To configure Auto Config using iDRAC UI: **iDRAC Settings** > **Connectivity** > **iDRAC Auto Config.**

iDRAC USB Interfaces

For increased security, you can completely disable USB ports. You also have the option of disabling only the USB ports on the front. For example, USB ports can be disabled for production use and then temporarily enabled to grant access to a crash cart for debugging purposes.

iDRAC direct feature allows you to directly connect your laptop or PC USB port to the iDRAC USB port. This allows you to interact directly with iDRAC interfaces (such as Web interface and RACADM) for advanced server management and servicing.

iDRAC Direct is a special USB port that is hardwired to the iDRAC service processor for at-the-server debugging and management from the front of the server (cold aisle). It allows a user to attach a standard Micro-AB USB cable to this port and the other end (Type A) to a laptop. A standard web browser can then access iDRAC GUI for extensive debugging and management of the server. If iDRAC Enterprise license is installed, the user can even access the OS desktop over iDRAC's Virtual Console feature. Since normal iDRAC credentials are used for logging in, iDRAC Direct works as a secure "crash cart" with the additional advantage of extensive hardware management and service diagnostics. This can be an attractive option for securing physical access to the server in remote locations (host USB ports and VGA outputs can be disabled in this case).

As a security best practice, it is recommended to disable any unused interface including USB Interfaces.

Configuring iDRAC Direct USB Connection Using the Webserver

To configure the USB port:

1. In the iDRAC Web interface, go to **iDRAC Settings** > **Settings** > **Management USB Settings**. The **Configure USB Management Port** page is displayed.
2. From the **USB Management Port Mode** drop-down menu, select any of the following options:
   - **Automatic**—USB Port is used by iDRAC or the server's operating system.
   - **Standard OS Use**—USB port is used by the server OS.
   - **iDRAC Direct only**—USB port is used by iDRAC.
3. From the iDRAC Managed: USB SCP drop-down menu, select options to configure a server by importing SCP configuration files stored on a USB drive:
   - **Disabled**
   - **Enabled only when server has default credential settings**
   - **Enabled**

   For information about the fields, see the iDRAC Online Help.
4. Click **Apply** to apply the settings.

8

Interfaces and Protocols to Access iDRAC

Table 6. Interfaces and protocols to access iDRAC

Interface or Protocol	Description
iDRAC Settings Utility (F2)	Use the iDRAC Settings utility to perform pre-OS operations. It has a subset of the features that are available in the iDRAC web interface along with other features. To access the iDRAC Settings utility, press <F2> during boot and then click **iDRAC Settings** on the **System Setup Main Menu** page.
Lifecycle Controller (F10)	Use Lifecycle Controller to perform iDRAC configurations. To access Lifecycle Controller, press <F10> during boot and go to **System Setup** > **Advanced Hardware Configuration** > **iDRAC Settings**. For more information, see the Lifecycle Controller User's Guide..
iDRAC Web Interface	Use the iDRAC web interface to manage iDRAC and monitor the managed system. The browser connects to the web server through the HTTPS port. Data streams are encrypted using 128-bit/168-bit/256-bit TLS/SSL to provide privacy and integrity. Any connection to the HTTP port is redirected to HTTPS if the https redirect feature is enabled. Administrators can upload their own webserver certificate.
RACADM	Use this command-line utility to perform iDRAC and server management. You can use RACADM locally and remotely. ● The local RACADM command-line interface runs on the managed systems that have Server Administrator installed. Local RACADM communicates with iDRAC through its in-band IPMI host interface. Since it is installed on the local managed system, users are required to log in to the operating system to run this utility. A user must have a full administrator privilege or be a root user to use this utility. ● Remote RACADM is a client utility that runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed system and uses the HTTPs channel. The –r option runs the RACADM command over a network. ● Firmware RACADM is accessible by logging in to iDRAC using SSH. You can run the firmware RACADM commands without specifying the iDRAC IP, username, or password. You do not have to specify the iDRAC IP, username, or password to run the firmware RACADM commands. After you enter the RACADM prompt, you can directly run the commands without the RACADM prefix.
iDRAC RESTful API and Redfish	The Redfish Scalable Platforms Management API is a standard that is defined by the Distributed Management Task Force (DMTF). Redfish is a next-generation systems management interface standard, which enables scalable, secure, and open server management. It is a new interface that uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management. It is suitable for a wide range of servers ranging from stand-alone servers to rackmount and bladed environments and for large-scale cloud environments. Redfish provides the following benefits over existing server management methods: ● Increased simplicity and usability ● High data security ● Programmable interface that can be easily scripted. ● Follows widely used standards. ● For more information, see the **iDRAC Redfish API** Guide available on the iDRAC page.
Virtual Console and Virtual Media	Virtual Console provides a mechanism for iDRAC user to remotely view the host's console and perform operations such as power cycle, change boot order, attach virtual media, and so on.
SSH	Use SSH to run RACADM commands. It provides the same capabilities as the Telnet console using an encrypted transport layer for higher security. The SSH service is enabled by default on iDRAC. The SSH service can be disabled in iDRAC. iDRAC only supports SSH version 2 with the RSA host key algorithm.

Table 6. Interfaces and protocols to access iDRAC (continued)

Interface or Protocol	Description
	• A unique 1024-bit RSA host key is generated when you power-up iDRAC for the first time.
IPMITool	Use the IPMITool to access the remote system's basic management features through iDRAC. The interface includes local IPMI, IPMI over LAN, IPMI over Serial, and Serial over LAN. For more information about IPMITool, see the Dell OpenManage Baseboard Management Controller User's Guide available on the Baseboard Management Controller page. **NOTE:** IPMI version 1.5 is not supported.
NTLM	iDRAC10 allows NTLM to provide authentication, integrity, and confidentiality to the users. NT LAN Manager (**NTLM**) is a suite of Microsoft security protocols, and it works in a Windows network.
SMB	iDRAC10 supports the Server Message Block (SMB) Protocol. This is a network file sharing protocol and the default minimum SMB version supported is 2.0.
NFS	iDRAC10 supports **Network File System (NFS)**. This is a distributed file system protocol that enables users to **mount** remote directories on the servers.
SNMP	iDRAC10 supports Simple Network Management Protocol (SNMP) v2 and v3 for GETs and TRAPs.

9

iDRAC Port Configuration

The following table lists the ports that are required to remotely access iDRAC through firewall. These are the default ports iDRAC listens to for connections. Optionally, you can modify most of the ports. To modify ports, see Configuring services.

Table 7. Ports iDRAC listens for connections

Port number	Type	Function	Configurable Port	Maximum Encryption Level
22	TCP	SSH	Yes	256-bit SSL
80	TCP	HTTP	Yes	None
161	UDP	SNMP Agent	Yes	None
443	TCP	HTTPS	Yes	256-bit SSL
623	UDP	RMCP/RMCP+	No	128-bit SSL
5000	TCP	iDRAC to iSM	No	256-bit SSL
5901	TCP	VNC	Yes	128-bit SSL
NOTE: Port 5901 opens when the VNC feature is enabled.				

The following table lists the ports that iDRAC uses as a client:

Table 8. Ports iDRAC uses as client

Port Number	Type	Function	Configurable Port	Maximum Encryption Level
25	TCP	SMTP	Yes	None
53	UDP	DNS	No	None
68	UDP	DHCP-assigned IP address	No	None
69	TFTP	TFTP	No	None
123	UDP	Network Time Protocol (NTP)	No	None
162	UDP	SNMP trap	Yes	None
445	TCP	Common Internet File System (CIFS)	No	None
636	TCP	LDAP Over SSL (LDAPS)	No	256-bit SSL
2049	TCP	Network File System (NFS)	No	None
3269	TCP	LDAPS for global catalog (GC)	No	256-bit SSL
5353	UDP	mDNS	No	None
5696	TCP	Key Management Server (SEKM)	Yes	256-bit SSL

Table 8. Ports iDRAC uses as client (continued)

Port Number	Type	Function	Configurable Port	Maximum Encryption Level
NOTE: When node-initiated discovery is enabled, iDRAC uses mDNS to communicate through port 5353. However, when both are disabled, port 5353 is blocked by iDRAC's internal firewall and appears as open|filtered port in the port scans.				
514	UDP	Remote syslog	Yes	None
6514	TCP	Remote syslog	Yes	256-bit SSL
Ports Internally used by iDRAC (These cannot be changed by the end user and cannot be used for other purposes).				
• 4200 • 4201 • 4202 • 4203 • 4204 • 4205	TCP	Redfish Internal Ports	No	None
• 4300 • 4301 • 4400	TCP	Authorizer Internal Ports	No	None
• 5200 • 5201	TCP	UI and RACADM Internal Ports	No	None
• 5555 • 5556	TCP	Internal Ports for IPC	No	None
199	UDP	SNMP daemon	No	None
• 5905 • 5951	TCP	VNC Vmedia/Vconsole	No	None

Topics:

- Security Recommendations for Interfaces, Protocols, and Services
- Disabling IPMI over LAN using Web Interface
- Disabling Serial Over LAN using Web Interface
- Configuring Services using Web Interface

Security Recommendations for Interfaces, Protocols, and Services

Similarly, to iDRAC network interfaces, iDRAC protocols, and modes of communication should be disabled if they are not needed as a security best practice. In addition to disabling all unused features and methods of communication, below are the security recommendations for interfaces to disable based on known security limitations inherent in the protocols.

1. IPMI over LAN disabled
2. Serial Over LAN disabled
3. SNMP Disabled

Disabling IPMI over LAN using Web Interface

To configure IPMI over LAN:

1. In the iDRAC Web interface, go to **iDRAC Settings** > **Connectivity** . The **Network** page is displayed.
2. Under **IPMI Settings**, specify **Disabled** in the **Enable IPMI Over LAN** drop-down.
3. Click **Apply**.

Disabling Serial Over LAN using Web Interface

To disable Serial Over LAN:

1. In the iDRAC Web interface, go to **iDRAC Settings** > **Connectivity** . The **Serial Over LAN** page is displayed.
2. Under **Serial Over LAN**, specify **Disabled** in the **Enable Serial Over LAN** drop-down.
3. Click **Apply**.

Configuring Services using Web Interface

You can configure and enable the following services on iDRAC:

- Local Configuration
- Web Server
- SEKM Configuration
- SSH
- Remote RACADM
- SNMP Agent
- Automated System Recovery Agent

To configure the services using iDRAC Web interface:

1. In the iDRAC Web interface, go to **iDRAC Settings> Services**. The **Services** page appears.
2. Enter the required information and disable all unused services.
3. Click **Apply**.

10

IPMI and SNMP Security Best Practices

iDRAC has multiple options for secure connection and management. Users can configure IPMI and SNMP which are protocols that have known security limitations. If these protocols are necessary, below are the security recommendations to minimize potential risk:

Topics:

SNMP Security Best Practices

iDRAC supports SNMP 2/3 for information gathering, alerting, and configuration. The SNMP protocol can potentially leak sensitive information if configured improperly. If SNMP is not needed, Dell Technologies recommends disabling this service. If SNMP is required, below are recommendations for how to configure the service as securely as possible.

1. Enable SNMPv3 only if possible.
2. Segment SNMP interfaces on managed servers using virtual LANs (VLANS), access control lists (ACLs), or physical separation to isolate the management network from the rest of the network.
3. Ensure that all devices using SNMP to communicate with ITA are in the same segment as the ITA system. Do not bind SNMP to public or internal networks.
4. Avoid using "public", "private," or an easily guessable string as the SNMP community name.
5. Set a separate SNMPv3 Authentication Passphrase & Privacy Passphrase.

The following are the additional Security Considerations for SNMP:

- SNMP security lockout feature
  - iDRAC supports a simple, nonconfigurable SNMP security lockout feature. If more than six SNMPv3 USM authentication failures occur within a 2-minute window, then the iDRAC SNMP Agent blocks all subsequent SNMPv3 requests/queries for 10 minutes.
- Restriction of access to sensitive data
  - Some of the MIB data that iDRAC supports can only be accessed using SNMPv3 queries. Access to such data is blocked for SNMPv1 and SNMPv2c queries.
  - Currently, the following attributes and table are considered to be “sensitive” data and have this restriction:
    - numLCLogEntries (which has an SNMP OID of 1.3.6.1.4.1.674.10892.5.4.300.2.0)
    - lcLogTable (which has an SNMP OID of 1.3.6.1.4.1.674.10892.5.4.300.90)

IPMI Security Best Practices

IPMI is an iDRAC management interface that allows users to monitor and configure iDRAC. The IPMI protocol has inherent security concerns that potentially allow malicious actors to discover user credentials resulting in unauthorized actions being performed. If IPMI over LAN is not required, Dell Technologies recommends disabling this service. If IPMI over LAN is required, below are recommendations for how to configure the service as securely as possible.

1. Segment IPMI traffic (UDP and stateless) from the rest of the network.
2. Do not allow IPMI traffic from outside the network.
3. If using IPMI 1.5-capable BMCs, use ACLs and strict source routing to help ensure that the IPMI traffic is secure. IPMI 2.0 uses stronger encryption than IPMI 1.5.
4. Disable Cipher 0 - Cipher 0 is an option that is usually enabled by default that can allow authentication to be bypassed. Disabling Cipher 0 can prevent attackers from bypassing authentication and sending arbitrary IPMI commands.

Secure NTP

NTP is a protocol that is designed to synchronize the clocks of systems over a network. As part of its secure NTP implementation, iDRAC has added options to upload security keys from external time servers. Secure NTP servers append a hash to the time information packet. The iDRAC compares a locally generated hash for the same data packet with its locally stored key corresponding to that time-server. If the locally computed hash matches the received hash, then the time packet is accepted.

iDRAC secure NTP implementation uses symmetric key approach, since that is the only option that is supported as per the government agency NIST National Institute of Standards and Technology (NIST). Details can be found on the NIST site. NIST only guarantees time accuracy up to 50 milliseconds according to their documentation.

MD5 and SHA1 are the most commonly used key types, since they meet basic security and provides time accuracy in millisecond level with timeservers within the company infrastructure. In theory, any encryption type that is supported by openssl can be used for symmetric keys, but higher encryption can result in high CPU usage and high latency in processing the time data.

Secure NTP Configuration

iDRAC group and property name to enable NTP is `NTPConfigGroup.NTPEnable`. When this property is set to `Enabled`, iDRAC uses the properties NTP1, NTP2, NTP3 to set up to three timeserver FQDN or IP addresses (IPv4 or IPv6).

The new additions in iDRAC NTPConfigGroup to support secure NTP are:

1. NTP1SecurityType
2. NTP1SecurityKeyNumber
3. NTP1SecurityKey
4. NTP2SecurityType
5. NTP2SecurityKeyNumber
6. NTP2SecurityKey
7. NTP3SecurityType
8. NTP3SecurityKeyNumber
9. NTP3SecurityKey

- `SecurityType` is an enumeration with options Disabled, MD5, SHA1. Higher encryption options could be supported in the future.
- `SecurityKeyNumber` is a number between 1 to 65534. It should be the same key number that is used in the NTP server corresponding to the selected key.
- `SecurityKey` is the key that is configured in the NTP server corresponding to the `SecurityKeyNumber`.

The key number, type and key value should match in the NTP server and iDRAC, for secure NTP to work.

The NTP configuration has a limitation that the key numbers must be unique. Hence NTP1SecurityKeyNumber, NTP2SecurityKeyNumber and NTP3SecurityKeyNumber should be different values. This limitation comes from open-source ntpd code usage on iDRAC, even though in theory, different NTP servers could issue the same key number. If the same key number is repeated in a configuration, the second instance of the key number is ignored.

Even though iDRAC can support up to three secure NTP server addresses, the guidance is to use only one secure NTP server and leave the other two entries as nonpopulated for best iDRAC performance. It is a common practice to use multiple timeservers when using plain unencrypted NTP, however the present secure NTP installations mostly use a single secure NTP server.

iDRAC allows mixing secure and unsecure NTP servers in the configuration. However, this is not advised, since unencrypted NTP packets always become the primary NTP source, with the current ntpd implementation.

For security reasons, the SecurityKey attribute is write only. If SecurityType is set to Disabled (default setting), the corresponding key entry is ignored.

Example showing RACADM script to set security configuration in NTP group:

```
racadm set idrac.ntpconfiggroup.NTPEnable 1

racadm set idrac.ntpconfiggroup.ntp1 100.64.25.20

racadm set idrac.ntpconfiggroup.NTP1SecurityKey calvin

racadm set idrac.ntpconfiggroup.NTP1SecurityType 1

racadm set idrac.ntpconfiggroup.NTP1SecurityKeyNumber 65

racadm set idrac.ntpconfiggroup.ntp2 100.64.24.202

racadm set idrac.ntpconfiggroup.NTP2SecurityKey da39a3ee5e6b4b0d3255bfef95601890afd80709

racadm set idrac.ntpconfiggroup.NTP2SecurityType 2

racadm set idrac.ntpconfiggroup.NTP2SecurityKeyNumber 17

racadm set idrac.ntpconfiggroup.ntp3 100.64.24.26

racadm set idrac.ntpconfiggroup.NTP3SecurityKey carlos

racadm set idrac.ntpconfiggroup.NTP3SecurityType MD5

racadm set idrac.ntpconfiggroup.NTP3SecurityKeyNumber 13

Example showing RACADM script to disable secure NTP (default configuration in iDRAC)

racadm set idrac.ntpconfiggroup.NTPEnable 0

racadm set idrac.ntpconfiggroup.ntp1 ""

racadm set idrac.ntpconfiggroup.NTP1SecurityKey ""

racadm set idrac.ntpconfiggroup.NTP1SecurityType 0

racadm set idrac.ntpconfiggroup.NTP1SecurityKeyNumber 1

racadm set idrac.ntpconfiggroup.ntp2 ""

racadm set idrac.ntpconfiggroup.NTP2SecurityKey ""
```

```
racadm set idrac.ntpconfiggroup.NTP2SecurityType 0
```

```
racadm set idrac.ntpconfiggroup.NTP2SecurityKeyNumber 1
```

```
racadm set idrac.ntpconfiggroup.ntp3 ""
```

```
racadm set idrac.ntpconfiggroup.NTP3SecurityKey ""
```

```
racadm set idrac.ntpconfiggroup.NTP3SecurityType 0
```

```
racadm set idrac.ntpconfiggroup.NTP3SecurityKeyNumber 1
```

Redfish Session Login Authentication

Redfish is a DMTF standard that provides a secure replacement for IPMI in the datacenter. Redfish provides options for secure authentication:

- Basic authentication: In this method, username and password are provided for each Redfish API request.
- Session-based authentication: This method is used while issuing multiple Redfish operation requests.
  - Session login is initiated by accessing the Create session URI. The response for this request includes an X-Auth-Token header with a session token. Authentication for subsequent requests is made using the X-Auth-Token header.
  - Session logout is performed by issuing a DELETE of the Session resource that is provided by the Login operation including the X-Auth-Token header.

The security recommendation is to use session-based authentication.

11

Secure Enterprise Key Manager (SEKM) Security

The OpenManage SEKM enables you to use an external Key Management Server (KMS) to manage keys that can then be used by iDRAC to lock and unlock storage devices on a Dell PowerEdge server. iDRAC requests the KMS to create a key for each storage controller, and then fetches and provides that key to the storage controller on every host boot so that the storage controller can then unlock the SEDs. The advantages of using SEKM over Local Key Management (LKM) are:

- In addition to the LKM–supported "Theft of an SED" use case, SEKM protects from a "Theft of a server" use case. Because the keys used to lock and unlock the SEDs are not stored on the server, attackers cannot access data even if they steal a server.
- Centralized key management at the external Key Management Server.
- SEKM supports the industry standard OASIS KMIP protocol thus enabling use of any external third-party KMIP server.

For more information, see Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers

You can configure SEKM from iDRAC Settings page. Click **iDRAC Settings** > **Services** > **SEKM Configuration**.

NOTE: When Security (Encryption) mode is changed from None to SEKM, Real-Time job is not available. But it is added to Staged job list. However, Real-Time job is successful when the mode is changed from SEKM to None.

Verify the following when changing the value of the **Username** Field in Client Certificate section on the KeySecure server (for ex: Changing the value from **Common Name (CN)** to **User ID (UID)**)

1. While using an existing account:
   - Verify in the iDRAC TLS/SSL certificate that instead of the Common Name field, the Username field now matches the existing username on the KMS. If they do not, then you must set the username field and regenerate the TLS/SSL certificate again, get it signed on the KMS, and reupload to iDRAC.
2. While using a new user account:
   - Ensure the Username string matches the username field in the iDRAC TLS/SSL certificate.
   - If they do not match, then you must reconfigure the iDRAC KMS attributes Username and Password.
   - Once the certificate is verified to contain the username, then the only change that must be made is to change the key ownership from the old user to the new user to match the newly created KMS username.

While using Vormetric Data Security Manager as KMS, ensure that the Common Name (CN) field in iDRAC TLS/SSL certificate matches with the hostname added to Vormetric Data Security Manager. Otherwise, the certificate may not import successfully.

NOTE: Rekey option is disabled when racadm sekm getstatus reports as Failed.

NOTE: SEKM only supports Common name, User ID, or Organization Unit for Username field under Client certificate.

NOTE: If you are using a third-party CA to sign the iDRAC CSR, ensure that the third-party CA supports the value UID for Username field in Client certificate. If it is not supported, use Common Name as the value for Username field.

NOTE: If you are using Username and Password fields, ensure that KMS server supports those attributes.

Topics:

Create or Change SEKM Security Keys

When configuring the controller properties, you can create or change the security keys. The controller uses the encryption key to lock or unlock access to SED. You can create only one encryption key for each encryption-capable controller. The security key is managed using the following features:

1. Local Key Management (LKM) System - LKM is used to generate the key ID and the password or key that is required to secure the virtual disk. If you are using LKM, you must create the encryption key by providing the Security Key Identifier and the Passphrase.
2. Secure Enterprise Key Manager (SEKM) - This feature is used to generate the key using the Key Management Server (KMS). If you are using SEKM, you must configure iDRAC with KMS information and TLS/SSL related configuration.

NOTE: This task is not supported on PERC hardware controllers running in eHBA mode.

If you create the security key in 'Add to Pending Operation' mode and a job is not created, and then if you delete the security key, the create security key pending operation is cleared.

NOTE: For enabling SEKM, ensure that the supported PERC firmware is installed.

- Only TLS 1.2 is supported for SEKM.
- You cannot downgrade the PERC firmware to the previous version if SEKM is enabled. Downgrading of other PERC controller firmware in the same system which is not in SEKM mode may also fail. To downgrade the firmware for the PERC controllers that are not in SEKM mode, you can use OS DUP update method, or disable SEKM on the controllers and then retry the downgrade from iDRAC.

NOTE: When importing a hot plugged locked volume from one server to another, you see CTL entries for Controller attributes being applied in the LC Log.

12

Virtual Console and Virtual Media Security

You can use the virtual console to manage a remote system using the keyboard, video, and mouse on your management station to control the corresponding devices on a managed server. This is a licensed feature for rack and tower servers. You can launch a virtual console in a supported web browser by using eHTML5 plug-in. A maximum of six simultaneous Virtual Console sessions are supported. All the sessions view the same managed server console simultaneously.

Virtual media allows the managed server to access media devices on the management station or ISO CD/DVD images on a network share as if they were devices on the managed server. This is a licensed feature for rack and tower servers.

TLS 1.2 and TLS 1.3 are enabled for VConsole communication by default. VConsoles and VMedia can be configured to redirect internally to the iDRAC web server. If this option is selected, then the configurable web server encryption settings are used for VConsole and VMedia.

The following configurations are recommended for VConsole Security. The settings can be made by navigating to **Configuration** > **Virtual Console** in the GUI.

- Plugin Type - eHTML5 (Enabled by Default)
- Video Encryption – Enabled

The following web server settings are recommended and can be configured from **iDRAC Settings** > **Services** > **Web Server** > **Settings**.

- TLS Protocol - TLS 1.3
- SSL Encryption - 256-bit or higher

The following configurations are recommended for vMedia Security. The settings can be made by navigating to **Configuration** > **Virtual Media** in the UI.

- Virtual Media Encryption – Enabled.

13

VNC Security

The VNC feature can be enabled and configured on iDRAC to manage the remote server using both desktop and mobile devices such as Dell Wyse PocketCloud. The VNC viewer can connect to OS/Hypervisor on the server and provide access to keyboard, video, and mouse of the host server. Before launching the VNC client, you must enable the VNC server and configure the VNC server settings in iDRAC such as password, VNC port number, SSL encryption, and the time-out value. You can configure these settings using iDRAC Web interface or RACADM.

The below configuration options are recommended when using VNC server to maximize secure communication. The settings can be configured by navigating to **Configuration** > **Virtual Console** in the GUI.

- Set SSL encryption to 256-bit or higher
- Set a strong password. The VNC password must be exactly 8 characters long.
- Configure an acceptable Timeout value based on VNC use case.

Topics:

Setting up VNC Viewer with SSL Encryption

While configuring the VNC server settings in iDRAC, if the **SSL Encryption** option was enabled, then the SSL tunnel application must be used along with the VNC Viewer to establish the SSL encrypted connection with iDRAC VNC server.

NOTE: Most of the VNC clients do not have integrated SSL encryption support.

To configure the SSL/SSH tunnel application:

1. Configure SSL/SSH tunnel to connect to <iDRAC IP address>:<VNC server port Number>. For example, 192.168.0.120:5901.
2. Start the tunnel application.

To establish connection with the iDRAC VNC server over the SSL encrypted channel, connect the VNC viewer to the localhost (link local IP address) and the local port number (127.0.0.1:<local port number>).

14

User Configuration and Access Control

You can setup user accounts with specific privileges (role-based authority) to manage your system using iDRAC and maintain system security. By default, iDRAC is configured with a local administrator account. The default iDRAC username and unique password are provided with the system badge unless default credentials were specified at time of purchase. If default credentials were specified at the time of purchase, iDRAC is configured with the default password. As an administrator, you can setup user accounts to allow other users to access iDRAC. The defined user roles are administrator, operator, read-only, or none. There are 9 different privileges that can be configured separately from these roles. For more information, see the iDRAC10 User Guide.

You can also use directory services such as Microsoft Active Directory or LDAP to setup user accounts. Using a directory service provides a central location for managing authorized user accounts.

Topics:

Configuring Local Users

You can configure up to 32 local users in iDRAC with specific access permissions. Before you create an iDRAC user, verify if any current users exist. You can set usernames, passwords, and roles with the privileges for these users. The usernames and passwords can be changed using any of the iDRAC secured interfaces (that is, web interface, RACADM or Redfish). You can also enable or disable SNMPv3 authentication and IPMI User Privileges for each user.

As a security best practice when configuring users, an iDRAC administrator should apply a least privilege approach where only the required set of permissions are provided to each user. Any user who has been configured with the “Configure Users” privilege can modify the privilege level of any other iDRAC user including themselves. Users that do not have the Configure Users privilege cannot modify their own passwords.

Recommended Security Configuration for users:

- Provide iDRAC users with the least privileges required.
- Strong passwords
- Disable IPMI User Privileges for all user.
- If SNMPv3 is needed set Authentication Type to SHA and Privacy Type to AES.
- Enable 2 -Factor Authentication.
- Configure SSH Key for PKI authentication.

Disabling Access to Modify iDRAC Configuration Settings on Host System

Host administrators and users with access to F2 during POST can modify iDRAC configurations through Local RACADM and the iDRAC Settings Utility without being configured as an iDRAC user.

You can disable access to modify the iDRAC configuration settings from these interfaces. However, you can still view these configuration settings when this access is disabled.

If access is disabled, you cannot use Server Administrator, iDRAC Service Module, or IPMITool to perform iDRAC configurations. As a security best practice, it is recommended to disable all management functionality that is not required.

To do this:

1. In iDRAC Web interface, go to **iDRAC Settings** > **Services** > **Local Configurations**.
2. Select one or both of the following:
   - Disable the iDRAC Local Configuration using iDRAC Settings — Disables access to modify the configuration settings in iDRAC Settings utility.
   - Disable the iDRAC Local Configuration using RACADM — Disables access to modify the configuration settings in Local RACADM.
3. Click **Apply**.

iDRAC User Roles and Privileges

The iDRAC role and privilege names have changed from earlier generation of servers. You can create custom roles in iDRAC10.

Table 9. iDRAC roles

Current Generation	Privileges
Administrator	Login, Configure, Configure Users, Logs, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug
Operator	Login, Configure, System Control, Access Virtual Console, Access Virtual Media, System Operations, Debug, Firmware Update
Read Only	Login
Login	Enables the user to log in to iDRAC.
Configure	Enables the user to configure iDRAC. With this privilege, a user can also configure power management, virtual console, virtual media, licenses, system settings, storage devices, BIOS settings, SCP, and so on.
NOTE: The administrator role overrides all the privileges from the other components such as BIOS setup password.	
Configure Users	Enables the user to allow specific users to access the system.
Logs	Enables the user to clear only the System Event Log (SEL).
System Control	Allows power cycling the host system.
Access Virtual Console	Enables the user to run Virtual Console.
Access Virtual Media	Enables the user to run and use Virtual Media.
System Operations	Allows user initiated and generated events, and information is sent as an asynchronous notification and logged.
Debug	Enables the user to run diagnostic commands.

Creating user roles

You can create user roles with the required privileges so that you can delegate the tasks to the users efficiently. Only users with the Administrator role can create user roles.

Steps

1. Go to **iDRAC Settings** > **Users** > **Local Users** > **User Roles**.
2. Click **+Add**.
   The **Add New Role** dialog box is displayed.
3. Select the **User ID**.
4. Enter the **User Role Name**.
5. Select the **User Privileges**.
6. Click **Save**.
   The user role is listed in the **User Roles** list.

Recommended Characters in Usernames and Passwords

This section provides details about the recommended characters while creating and using usernames and passwords.

NOTE: This section provides details about the recommended characters while creating and using usernames and passwords.

Use the following characters while creating usernames and passwords:

Table 10. Recommended characters for usernames

Characters	Length
• 0-9 • A-Z • a-z - ! # $ % & ( ) * ; ? [\ ] ^ _ ` { | } ~ + < = >	1-16

Table 11. Recommended characters for passwords

Characters	Length
• 0-9 • A-Z • a-z ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1-40

NOTE: You may be able to create usernames and passwords that include other characters. However, to ensure compatibility with all interfaces, Dell Technologies recommends using only the characters that are listed here.

NOTE: The characters that are allowed in usernames and passwords for network shares are determined by the network-share type. iDRAC supports valid characters for network share credentials as defined by the share type, except <, >, and, (comma).

NOTE: To improve security, it is recommended to use complex passwords that have eight or more characters and include lowercase alphabets, uppercase alphabets, numbers, and special characters. It is also recommended to regularly change the passwords.

Password Strength Policy

Using iDRAC interface, you can check the password strength policy and check any errors if the policy is not met. The password policy cannot be applied to previously saved passwords, Server Configuration Profiles (SCP) copied from other servers, and embedded passwords in the profile.

iDRAC offers two password policy options:

- Simple Policy — Simple Policy is based on LUDS, i.e., lower- and uppercase letters, digits, and symbols.
- Regular Expression — Regular Expression Password Policy Enforcement is a based on the POSIX definition.

To access Password settings, go to **iDRAC Settings** > **Users** > **Password Settings**.

Following fields are available in this section:

- **Minimum Score** — Specifies the minimum password strength policy score. The values in this field are:
  - 0 — No protection
  - 1 — Weak protection
  - 2 — Medium protection
  - 3 — Strong protection

  Scoring is based on zxcvbn's entropy value and map to the following values:
  - 0 - No Protection; too easy to guess: risky password
  - 1 - Weak Protection; very easy to guess: protection from throttled online attacks
  - 2 - Moderate Protection; somewhat able to guess: protection from un-throttled online attacks
  - 3 - Strong Protection; safely to very not able to guess: moderate protection from offline slow-hash scenario
- **Simple Policy** — Specifies the required characters in a secure password. It has the following options:
  - Upper Case Letters
  - Numbers
  - Symbols
  - Minimum Length
- **Regular Expression** — The Regular expression along with the Minimum score is used for password enforcement.

Secure Default Password

All supported systems are shipped with a unique default password for iDRAC, unless you choose to set calvin as the password while ordering the system. The unique password helps improve the security of iDRAC and your server. To further enhance security, it is recommended that you change the default password.

The unique password for your system is available on the system information tag. To locate the tag, see the documentation for your server on the Support site.

NOTE: Resetting iDRAC to the factory default settings reverts the default password to the one that the server was shipped with.

Changing the Default Login Password using Web Interface

The warning message that allows you to change the default password is displayed if:

- You log in to iDRAC with Configure User privilege.
- The default password warning feature is enabled.
- The default iDRAC username and password are provided on the system information tag.

A warning message is also displayed when you log in to iDRAC using SSH, Telnet, remote RACADM, or the Web interface. For Web interface, SSH, and Telnet, a single warning message is displayed for each session. For remote RACADM, the warning message is displayed for each command.

When you log in to the iDRAC web interface, if the **Default Password Warning** page is displayed, you can change the password.

To do this:

1. Select the **Change Default Password** option.
2. In the **New Password** field, enter the new password.
3. In the **Confirm Password** field, enter the password again.
4. Click **Continue**.

The new password is configured, and you are logged in to iDRAC.

For information about the other fields, see the iDRAC Online Help

Force Change of Password (FCP)

The 'Force Change of Password' feature prompts you to change the factory default password of the device. The feature can be enabled as part of factory configuration.

The FCP screen appears after successful user authentication and cannot be skipped. Only after the user enters a password, normal access, and operation is allowed. The state of this attribute is not affected by a 'Reset Configuration to Defaults' operation.

NOTE: To set or reset the FCP attribute, you must have Login privilege and User configuration privilege.

NOTE: When FCP is enabled, 'Default Password Warning' setting is disabled after changing the default user password.

NOTE: When root user logs in using Public Key Authentication (PKA), FCP is bypassed.

When FCP is enabled, following actions are not allowed:

- Log in to iDRAC through any UI except IPMI over-LAN interface which uses CLI with default user credentials
- Log in to iDRAC through OMM app using Quick Sync-2

Simple 2-Factor Authentication (Simple 2FA)

iDRAC offers simple 2-factor authentication option to enhance the security to the local users for logging in. When you log in from a source IP address which is different from the last login, you are prompted to enter the second factor authentication details.

Simple two factor authentication has two steps of authentication:

- iDRAC Username and password
- Simple 6-digit code which is sent to the user by email. User must enter this 6-digit code when prompted at login.

NOTE:

- To receive 6-digit code, it is mandatory to configure 'Custom Sender Address' and have valid SMTP configuration.
- The 2FA code expires after 10 minutes or is invalidated if it is already consumed before expiry.
- If a user attempts to log in from another location with a different IP-Address while a pending 2FA challenge for the original IP-Address is still outstanding, the same token is sent for login attempt from the new IP address.
- The feature is supported with iDRAC Enterprise license.

You can set an interval that requires user to authenticate periodically regardless of IP change (requires 6.00 firmware or higher).

When 2FA is enabled, following actions are not allowed:

- Log in to iDRAC through any UI which uses CLI with default user credentials.
- Log in to iDRAC through OMM app using Quick Sync-2

NOTE: RACADM, Redfish, IPMI LAN, Serial, CLI from a source IP works only after successful login from supported interfaces such as iDRAC GUI and SSH.

RSA SecurID Two Factor Authentication (2FA) iDRAC10 Datacenter

RSA SecurID can be used as another means of authenticating a user on a system. The iDRAC10 with the Datacenter license and firmware support RSA SecurID as another two-factor authentication method.

- Using iDRAC10 RSA SecurID 2FA - This document goes through how to configure iDRAC10 to enable RSA SecurID 2FA on local users, and Active Directory and LDAP users.

Active Directory

If your company uses the Microsoft Active Directory software, you can configure the software to provide access to iDRAC, allowing you to add and control iDRAC user privileges to your existing users in your directory service. This is a licensed feature.

You can configure user authentication through Active Directory to log in to the iDRAC. You can also provide role-based authorizations, which enables an administrator to configure specific privileges for each user. For full instructions on configuring Active Directory, see iDRAC user's guide.

NOTE: StartTLS on Port 389 is supported. By default, LDAPS on Port 636 is configured. The connection protocol can be reconfigured to StartTLS using Redfish or the RACADM command `racadm set iDRAC.ActiveDirectory.Connection StartTLS`.

The Certificate Settings page in iDRAC GUI is used to configure the digital certificate that is used during initiation of TLS/SSL connections when communicating with the Active Directory (AD) server; these communications use LDAP over TLS/SSL (LDAPS). When certificate validation is enabled, it is necessary to upload the certificate of the Certificate Authority (CA) that issued the certificate that is used by the AD server during initiation of TLS/SSL connections. The CA's certificate is used to validate the authenticity of the certificate provided by the AD server during TLS/SSL initiation. For more information, see the Integrate iDRAC with Microsoft's Active Directory whitepaper.

Table 12. Certificate Validation

Certificate Validation	
Select **Enabled** to validate the SSL certificate of your Active Directory server.	iDRAC always uses LDAP over Secure Socket Layer (SSL) while connecting to Active Directory. By default, iDRAC uses the CA certificate available in iDRAC to validate the SSL server certificate of the domain controllers during SSL handshake and provides security. You can disable the certificate validation for testing purposes, or when you choose to trust the domain controllers in the security boundary without validating their SSL certificates.

LDAP

iDRAC provides a generic solution to support Lightweight Directory Access Protocol (LDAP)-based authentication. This feature does not require any schema extension on your directory services.

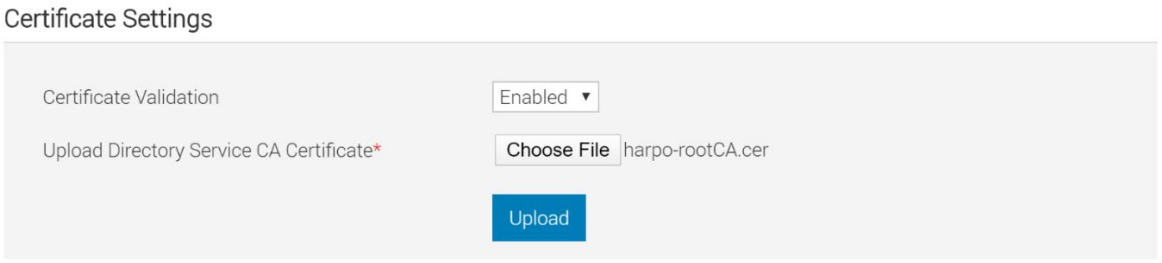
To make iDRAC LDAP implementation generic, the commonality between different directory services is used to group users and then map the user-group relationship. The directory service-specific action is the schema. For example, they may have different attribute names for the group, user, and the link between the user and the group. These actions can be configured in iDRAC.

NOTE: StartTLS on Port 389 is supported. By default, LDAPS on Port 636 is configured. The connection protocol can be reconfigured to StartTLS using Redfish or the RACADM command `racadm set iDRAC.ActiveDirectory.Connection StartTLS`.

The Certificate Settings page in iDRAC UI is used to configure the digital certificate that is used during initiation of SSL connections when communicating with a generic LDAP server; these communications use LDAP over SSL (LDAPS). Certificate validation is a recommended security configuration. When enabled, it is necessary to upload the certificate of the Certificate Authority (CA) that issued the certificate used by the LDAP server during initiation of SSL connections. The CA certificate is used to validate the authenticity of the certificate provided by the LDAP server during SSL initiation.

Table 13. Certificate Validation

Certificate Validation	
Select **Enabled** to enable certificate validation.	If enabled, iDRAC uses the CA certificate to validate the LDAP server certificate during the SSL handshake. If disabled, iDRAC skips the certificate validation step of the SSL handshake. You can disable the certificate validation for testing purposes or if you choose to trust the domain controllers in the security boundary without validating their SSL certificates.



Customizable Security Banner

You can customize the security notice that is displayed on the login page. You can use SSH, RACADM, or Redfish to customize the notice. Depending on the language you use, the notice can be either 1024 or 512 UTF-8 characters long.

15

System Lockdown Mode

System Lockdown mode helps in preventing unintended changes after a system is provisioned. This feature can help in protecting the system from unintentional or malicious changes. Lockdown mode is applicable to both configuration and firmware updates. When the system is locked down, any attempt to change the system configuration is blocked. If any attempts are made to change the critical system settings, an error message is displayed.

NOTE: After the System Lockdown mode is enabled, you cannot change any configuration settings. System Settings fields are disabled.

Lockdown mode can be enabled or disabled using the following interfaces:

- iDRAC web interface
- RACADM
- SCP (System Configuration Profile)
- Redfish
- Using F2 during POST and selecting iDRAC Settings

NOTE: To enable Lockdown mode, you must have iDRAC Enterprise or Datacenter license and Control and Configure system privileges.

The following tasks can be performed while the system is in Lockdown mode:

- Power cap setting
- System power operations (power on/off, reset)
- Power priority
- Identify operations (PERC)
- Part replacement
- Running diagnostics
- Modular operations (FlexAddress or Remote-Assigned Address)

NOTE: You may access vMedia while the system is in Lockdown Mode but configuring remote file share is not enabled.

The following table lists the functional and nonfunctional features, interfaces, and utilities affected by Lockdown mode:

NOTE: Changing the boot order using iDRAC is not supported when Lockdown mode is enabled. However, a boot-control option is available in the vConsole menu, which has no effect when iDRAC is in Lockdown mode.

Table 14. Items affected by Lockdown mode

Disabled	Remain Functional

• OMSA/OMSS
• IPMI
• DRAC/LC
• DTK-Syscfg
• Redfish
• OpenManage Essentials
• BIOS (F2 settings become read-only)
	• All Vendor tools that have direct access to the device.
	• PERC
	  ○ PERC CLI
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• NVMe
	  ○ DTK-RAIDCFG
	  ○ F2/Ctrl+R
	• BOSS-S1
	  ○ Marvell CLI
	  ○ F2/Ctrl+R
	• Part replacement, Easy Restore, and system board replacement
	• Power capping
	• System power operations (power on, off, reset)
	• Identify devices (PERC)

Table 14. Items affected by Lockdown mode

Disabled	Remain Functional
	• ISM/OMSA settings (operating system BMC enable, watchdog ping, operating system name, operating system version) • Modular operations (FlexAddress or Remote-Assigned Address)

NOTE: When lockdown mode is enabled, the OpenID Connect login option is not displayed in the iDRAC login page.

16

Securely Configuring BIOS System Security

iDRAC allows the user to configure the options under System Security in the BIOS such as power, system or setup passwords, and secure boot policies.

NOTE: This is a BIOS option. iDRAC can also configure BIOS settings.

To update System Security Settings:

1. Go to **Configuration** > **BIOS Settings** > **System Security**.
2. Select the necessary security configurations and set to required values.
3. Click **Apply**.

The following System Security settings can be configured:

Table 15. BIOS Security Settings

Menu Item	Option	Description
System Password	N/A	Enables you to set the system password which is the password that you must enter to allow the system to boot to an operating system. This option is read-only if the password switch (PWRD_DIS) is off. A password has up to a maximum of 32 characters. Enable a Setup Password using SHA256 hash and salt.
Setup Password	N/A	Enables you to set the Setup password. The Setup password is the one you must enter to change any BIOS settings, except for the System password, which can be changed without entering the correct Setup password. This option is read-only if the password switch (PWRD_DIS) is off. A password must have up to a maximum of 32 characters. Enable a System Password using SHA256 hash and salt.
Password Status	Unlocked/Locked	Locks the system password. To prevent the system password from being modified, set this option to locked and enable Setup password. This field also prevents the system password from being disabled by the user while the system is booting. Set the password status to “Locked”.
Power Button	Enabled/Disabled	When set to Disabled, this blocks someone from pressing the power button to shut down the system, however, the system can still be powered on. This is a security setting as it protects from accidental or malicious powering off the system.
UEFI Variable Access	Standard/Controlled	This field provides varying degrees of securing UEFI variables. When set to Standard, UEFI variables are accessible

Table 15. BIOS Security Settings (continued)

Menu Item	Option	Description
		in the operating system based on the UEFI specification. When set to Controlled, selected UEFI variables are protected in the environment and new UEFI boot option entries are forced to be appended to the end of the current boot order.
In-Band Manageability Interface	Enabled/Disabled	When set to Disabled, this setting hides the Management Engine's (ME) HECI devices and the system's IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access to all in-band management tools. All management functions must be managed by using the out-of-band techniques. **NOTE:** BIOS update requires HECI devices to be operational, and DUP updates require IPMI interface to be operational. This setting must be set to Enabled to avoid update errors.
Secure Boot	Enabled/Disabled	Allows you to enable Secure Boot, where the BIOS authenticates each component that is performed during the boot process using the certificates in the Secure Boot Policy. The following components are validated in the boot process: • UEFI drivers that are loaded from PCIe cards. • UEFI drivers and executables from mass storage devices • Operating System boot loaders **NOTE:** A Setup password is recommended to be enabled for Secure Boot.
Secure Boot Policy.	Standard/Custom	When Secure Boot Policy is Standard, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot Policy 33 Setting up BIOS on 14th Generation (14G) Dell PowerEdge Servers is set to Custom, the BIOS uses the user-customized key and certificates. **NOTE:** If Custom mode is selected, the Secure Boot Custom Policy Settings menu is displayed. **NOTE:** Changing the default security certificate may cause the system to fail booting from certain boot options.

Table 15. BIOS Security Settings (continued)

Menu Item	Option	Description
Secure Boot Mode.	User Mode/Deploy Mode	• Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, and dbx). In Setup Mode and Audit Mode, PK is not present, and BIOS does not authenticate programmatic updates to the policy objects. In User Mode and Deployed Mode, PK is present, and BIOS performs signature verification on programmatic attempts to update policy objects. • Deployed Mode is the most secure mode. Use Setup, Audit, or User Mode when provisioning the system, then use Deployed Mode for normal operation. Available mode transitions depend on the current mode and PK presence. For more information about transitions between the four modes, see Figure 77 in the UEFI 2.6 specification. • In Audit Mode, the BIOS performs signature verification on pre-boot images and logs the results in the Image Execution Information Table but performs the images whether they pass or fail verification. Audit Mode is useful for programmatically determining a working set of policy objects.
Secure Boot Policy Settings.	N/A	Enables you to configure the Secure Boot Custom Policy. A user can enroll and delete the PK, KEK, db, and dbx entries.

For a complete list of BIOS settings, see the Set up BIOS on 17th Generation Dell PowerEdge Servers whitepaper.

17

Secure Boot Configuration

UEFI Secure Boot is a technology that eliminates a major security void that may occur during a handoff between the UEFI firmware and UEFI operating system (OS). In UEFI Secure Boot, each component in the chain is validated and authorized against a specific certificate before it can load or run. Secure Boot removes the threat and provides software identity checking at every step of the boot— Platform firmware, Option Cards, and OS BootLoader.

The Unified Extensible Firmware Interface (UEFI) Forum—an industry body that develops standards for pre-boot software —defines Secure Boot in the UEFI specification. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability. As a portion of the UEFI specification, Secure Boot represents an industry-wide standard for security in the pre-boot environment.

When enabled, UEFI Secure Boot prevents the unsigned UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. You must disable Secure Boot to load the unsigned device drivers.

On the Dell 14th generation and later versions of PowerEdge servers, you can enable or disable the Secure Boot feature by using different interfaces (RACADM, REDFISH, and LC-UI).

The Secure Boot Settings feature can be accessed by clicking System Security under System BIOS Settings from the iDRAC web interface or by pressing <F2> when the company logo is displayed during POST and navigating to System BIOS Settings,

- By default, Secure Boot is Disabled, and the Secure Boot policy is set to Standard. To configure the Secure Boot Policy, you must enable Secure Boot.
- When the Secure Boot mode is set to Standard, it indicates that the system has default certificates and image digests, or hash loaded from the factory. This caters to the security of standard firmware, drivers, option-roms, and boot loaders.
- To support a new driver or firmware on a server, the respective certificate must be enrolled into the database of Secure Boot certificate store. Secure Boot Policy must be configured to Custom.

When the Secure Boot Policy is configured as Custom, it inherits the standard certificates and image digests that are loaded in the system by default, which you can modify. Secure Boot Policy configured as Custom allows you to perform operations such as View, Export, Import, Delete, Delete All, Reset, and Reset All. Using these operations, you can configure the Secure Boot Policies.

Configuring the Secure Boot Policy to Custom enables the options to manage the certificate store by using various actions such as Export, Import, Delete, Delete All, Reset, and Rest All on PK, KEK, DB, and DBX. You can select the policy (PK / KEK / DB / DBX) desired for changes and perform appropriate actions by clicking the respective link. Each section has links to perform the Import, Export, Delete, and Reset operations. Links are enabled based on what is applicable, which depends on the configuration at the time. Delete All and Reset All are the operations that have impact on all the policies. **Delete All** deletes every the certificate and image digest in the Custom policy. **Reset all** restores every certificate and image digest from Standard or Default certificate store.

Configuring Secure Boot is discussed in detail in the Secure boot management on Dell PowerEdge Servers whitepaper.

Table 16. Acceptable file formats

Policy Component	Acceptable File Formats	Acceptable File Extensions	Max records allowed
PK	X.509 Certificate (binary DER format only)	1. .cer 2. .der 3. .crt	1
KEK	• X.509 Certificate (binary DER format only) • Public Key Store	1. .cer 2. .der 3. .crt 4. .pbk	More than 1
DB and DBX	• X.509 Certificate (binary .DER format only) • EFI image (system BIOS calculates and imports the image digest)	1. .cer 2. .der 3. .crt 4. .efi	More than 1

18

Securely Erasing Data

Data security is a key consideration throughout the life cycle of a server, including when the server is repurposed or retired. Many servers are repurposed as they are transitioned from workload to workload, or as they change ownership from one organization to another. All servers are retired when they reach the end of their useful life. When such transitions occur, the best practice for data protection is to remove all data from the server to ensure that sensitive information is not inadvertently shared. Beyond best practices, often government regulations about privacy rights also necessitate complete data elimination when IT resources are transitioned.

System Erase simplifies the process of erasing server storage devices, and server nonvolatile stores such as caches and logs. To meet varying Systems Administrator needs for interactive and programmable operations, System Erase can be performed by the following methods: Lifecycle Controller UI, Redfish, and RACADM CLI.

Using one of these three methods, an administrator can selectively reset a PowerEdge server to its original state (factory settings), removing data from internal server nonvolatile stores and from storage devices within the server. System Erase can discover server-attached storage including hard disk drives (HDDs), self-encrypting drives (SEDs), Instant Secure Erase (ISE), and nonvolatile memory drives (NVMes). Data stored on ISE, SED, and NVMe devices can be made inaccessible using cryptographic erase while devices such as non-ISE SATA HDDs can be erased using data overwrite.

NVMe Sanitize Cryptographic Erase functionality is much faster and more efficient way than other methodologies. This feature destroys the key and creates a media encryption key. Data blocks are overwritten with zeros and rendered irretrievable. Data erases other user sensitive data such as debug logs and Personal Identifying Information (PII).

For information about the System Erase function within the Lifecycle Controller UI, see the Lifecycle Controller User's Guide available on the iDRAC page.

Table 17. System Erase methods

Drive Type	Connected to	Erase Method used	Notes
SAS/SATA SED	PERC	TCG Enterprise Extension (Dell Drive specification) RevertSP	Cryptographically erases all user data and returns the drive to factory secure state. PERC issues the command to the drives.
• SAS SED/SAS ISE • SATA SED/ SATA ISE	• PERC/HBA/SW RAID/ AHCI • PERC/BOSS/HBA/SW RAID/AHCI	• SCSI SANITIZE command(048h) with Service Action=Cryptographic erase • (03h) • ATA Sanitize Device command(0B4h) with Feature=Crypto Scramble • Ext(011h)	• PERC/SW RAID issues the command to the drive. For AHCI and HBA, LC issues the command using BIOS. SED and ISE drives behave identically since they are NOT secured behind these controllers. • PERC/BOSS/SW RAID issues the command to the drive. For AHCI and HBA, LC issues the command using BIOS.
SAS/SATA HDD	PERC/HBA/SW RAID/AHCI	SCSI Write Buffer(3Bh)/ATA Write Buffer	Dell only ships ISE/SED drives, this method is no longer in use.
NVMe	PERC/non-PERC	1. Sanitize NVM command with bits 00:02 set to 100b – Cryptographic erase) 2. Format NVM (Command DWORD 10 – bits 09:11 set to 010b – Cryptographic erase)	BIOS and PERC issue these commands to the drives. Sanitize is a new command and so is supported by newer drives – older drives support the Format NVM. BIOS/PERC checks if the drive supports

Table 17. System Erase methods (continued)

Drive Type	Connected to	Erase Method used	Notes
			Sanitize and use it – if not use the Format NVM command.
NVMe SED	PERC/BOSS/non-PERC	TCG Opal Revert	Cryptographically erases all user data and returns the drive to a factory secure state. PERC/BOSS issues the command to the drives. For direct attach, iDRAC issues the command. BOSS and iDRAC support for NVMe SED is not supported.

19

Server Inventory, Lifecycle Log, Server Profiles, and Licenses Import and Export

iDRAC10 with Lifecycle Controller firmware enables multiple protocols to perform export of server inventory, export of the Lifecycle Controller log, import and export of server profiles, and import of iDRAC with Lifecycle Controller licenses. These interfaces expand the options for network file share support with the Lifecycle Controller UI to include CIFS, NFS, HTTP, and HTTPS simplifying Lifecycle Controller UI operations. The recommended secure protocol for exports and imports of logs, profiles, and licenses is HTTPS.

To communicate using HTTPS, there is an existing iDRAC facility to upload and store certificates for various uses which have been expanded in iDRAC10 to allow the upload of the HTTPS server certificate. With the Apache server, for example, this is often the ca.crt file that is found in /etc/pki/tls/certs. This allows the uploaded certificate to be compared with the HTTPS server certificate at the time of a data transfer to validate the identity of the server.

NOTE: This is not the certificate that is used with the iDRAC UI for in-bound HTTPS connections to the iDRAC. It is the one used for iDRAC outbound connections from the iDRAC to an external HTTPS server. For example, using a web browser to connect to the iDRAC over HTTPS uses one certificate. When the iDRAC fetches a firmware update package from an HTTPS server, it uses this other different certificate.

Server Profile can be Exported or Imported by navigating to **Configuration** > **Server Configuration Profile** .

- It is recommended to use HTTP/HTTPS shares using a proxy.
- When using HTTPS:
  - Configure Expired or invalid certificate action to Show error.
  - Upload a valid certificate for outbound connection.

Topics:

Configuring Lifecycle Controller Logs Export using Web Interface and HTTPS

Lifecycle Controller Logs can be exported by navigating to **Maintenance** > **Lifecycle Logs** and clicking **Export**.

- It is recommended to use HTTP/HTTPS shares using a proxy.
- When using HTTPS:
  - Configure Expired or invalid certificate action to Show error.
  - Upload a valid certificate for outbound connection.

NOTE: Part of the process of certificate validation is the comparison of the CN name in the certificate with the IP address or DNS name that is used to connect to the server. If a DNS name was used in the certificate, then that name is required on the iDRAC. This requires DNS resolution be enabled on the iDRAC. DNS servers can be obtained by DHCP or can be set manually. These settings are off by default.

Certificates that are used with HTTPS are intended to be signed by a certificate authority. The certificate authorities publish public keys that allow the certificates to be validated. Software, such as web browsers, use a bundle of these public keys that is regularly updated to validate the certificates from websites that are visited.

It is possible to create self-signed certificates, but software such as web browsers would not be able to validate them by using the bundle of public keys. Self-signed keys can protect against eavesdropping but not man-in-the-middle attacks.

Using HTTPS with a Proxy Securely

When using HTTPS with a proxy, the connection between the iDRAC and the proxy is not as secure as the connection between the iDRAC and the HTTPS server. The connection between the iDRAC and the HTTPS server is encrypted, and credentials that are used to log in to the server (if any) are carried over the encrypted connection. The connection between the iDRAC and the proxy is not encrypted. The credentials used to log in to the proxy (if any) are transferred before the encrypted connection is started. Because of this, the credentials used to log in to the proxy should not be the same credentials that are used to log in to the server. With different credentials, If the proxy credentials are compromised, the HTTPS server credentials are not compromised also.

The following attributes are also used in interfaces other than the LC-UI. Attributes are available to allow values to be set when an interface is not able to set them itself. One set of these is for proxy settings.

LifeCycleController.LCAttributes.UserProxyPassword

LifeCycleController.LCAttributes.UserProxyPort

LifeCycleController.LCAttributes.UserProxyServer

LifeCycleController.LCAttributes.UserProxyType

LifeCycleController.LCAttributes.UserProxyUserName

These attributes are used with both HTTP and HTTPS.

The UserProxyServer is an important attribute. If it is not set, then the other attributes cannot be used, and the behavior is as if none of them are set.

The LifeCycleController.LCAttributes.IgnoreCertWarning attribute is used only with HTTPS. If the attribute is set to **ON**, the certificate warnings are ignored or the HTTPS server validation is not completed. Dell recommends that this configuration is set to **Off** so that certificate validation is performed as part of the HTTPS communication.

Security recommendations if a proxy is required:

1. Set IgnoreCertWarning to “Off”
2. If proxy credentials are used, they should be different than the remote HTTPS server
3. HTTP Proxy or socks4

20

Security Events Lifecycle Log

Security Events are logged in the Lifecycle Log for access-related security events such as new user creation, user password/ privilege modification, successful or failed login attempts so on Security events are also logged for encryption-related events on storage such as cryptographic erase, secure key encryption/decryption so on.

Table 18. Security Event Descriptions

Message ID	Detailed Description	Recommended Response Action
CTL136	A key exchange is required for the controller identified in the message.	No response action is required.
PDR118	The drive identified in the message is successfully unlocked.	No response action is required.
PDR208	The Cryptographic Erase operation is successfully completed on the physical disk drive that is identified in the message.	No response action is required.
PDR84	The Security key on a secure encrypted disk was activated.	No response action is required.
PDR85	Errors were detected with security-related operations on the disk. The data on the disk might not be retrieved or stored successfully. In addition, the security of the stored data might be at risk.	Verify that the disk is a Secure Encrypted Disk and is not locked. If it is not, replace the disk with a Secure Encrypted Disk. See the storage hardware documentation for more information.
CTL98	The security key provided as input has been assigned to the controller identified in the message.	No response action is required.
CTL131	The Key exchange process for the controller identified in the message is successfully completed.	No response action is required.
CTL81	The security key assigned to the controller identified in the message is modified.	No response action is required.
CTL132	The security key for the controller in the message cannot be changed.	Unable to change the security key for the <controller name>.
CTL117	The operation cannot be completed because an invalid passphrase is passed for the controller identified in the message.	Enter a valid passphrase and retry the operation.
CTL99	The security key assigned to the controller identified in the message is deleted.	No response action is required.
CTL117	The operation cannot be completed because an invalid passphrase is passed for the controller identified in the message.	Enter a valid passphrase and retry the operation.
CTL133	The security key for the controller identified in the message is successfully changed.	No response action is required.

Table 18. Security Event Descriptions (continued)

Message ID	Detailed Description	Recommended Response Action
CTL134	The controller identified in the message is in the Secure Enterprise Key Manager mode.	No response action is required.
CTL135	The Key exchange process for the controller identified in the message failed.	Ensure of the following and retry the operation: • The iDRAC can communicate to the Key Management Server. • The device for which the key is generated is online and responding. • The device for which the key exchange is required is in the same Key Management Server Domain.
PDR97	The controller detected drives that require security keys for access. Without providing security keys, the drives are unusable.	Provide the security key required to unlock the secure encrypted drives.
VDR104	The secure virtual disk operation was successful on the security capable virtual disk that is identified in the message. A security capable virtual disk is created using only Self-Encrypting Drives (SED).	No response action is required.
VDR130	The virtual drive identified in the message is partially secured.	No response action is required.
VDR59	This alert message occurs if virtual disk security has failed.	This alert message occurs if virtual disk security has failed. No response action is required.
PDR41	The clear command did not complete on the physical disk. This means that some data was not cleared and may be recoverable.	No response action is required.
PDR217	The cryptographic erase operation cannot be completed on the physical disk drive identified in the message.	No response action is required.
PDR38	A user has initiated a clear operation on a physical disk.	No response action is required.
PDR208	The Cryptographic Erase operation is successfully completed on the physical disk drive identified in the message.	No response action is required.
PDR82	Security on a secure encrypted disk was activated.	No response action is required.
PDR96	Security on a secure encrypted disk was disabled.	No response action is required.
USR0030	Successfully logged in using <username>, from <IP address> and <interface name>.	No response action is required.
USR0031	Unable to log in for <username> from <IP address> using <interface name>.	Ensure that the login credentials are valid and retry the operation.
USR0032	The session for <username> from <IP address> using <interface name> is logged off.	No response action is required.

Table 18. Security Event Descriptions (continued)

Message ID	Detailed Description	Recommended Response Action
USR0034	Login attempt alert for <username> from <IP Address> using <interface name>, IP is blocked for <seconds> seconds.	The account identified in the message is temporarily disabled because of consecutive unsuccessful Login attempts to iDRAC from the IP address identified in the message.
RAC1195	User requested state or configuration change using specified interface.	No response action is required.
SWC1910	User ID Name has been changed.	No response action is required.
SWC1911	User ID Password has been changed.	No response action is required.
SWC1912	User ID Access Right has been changed.	No response action is required.
SEL0014	The System Event Log (SEL) was cleared by the username identified in the message from the IP address identified in the message.	No response action is required.

21

Default Configuration Values

The table below includes the security configurations that are described in this document and the default values.

Table 19. Default Configuration Values

Configuration	Default Values
iDRAC.Webserver.HttpsRedirection	1 - Enabled
iDRAC.Webserver.TLSProtocol	1 -TLS 1.3 and higher
iDRAC.Webserver.SSLEncryptionBitLength	1- 128-Bit or higher
iDRAC.Webserver.CustomCipherString	None
TLS/ SSL Certificates	Self-signed certificate
iDRAC.Security.FIPSMode	0 - Disabled
iDRAC.Users.2.SSHPublicKey1	None
iDRAC.SSHCrypto.KexAlgorithms	curve25519-sha256,curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384,ecdh-sha2-nistp521
iDRAC.SSHCrypto.Ciphers	chacha20-poly1305@openssh.com,aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
iDRAC.NIC.Selection	1 - Dedicated
iDRAC.NIC.VlanEnable	0 – Disabled
iDRAC.USB.PortStatus	1 – Enabled
iDRAC.autodiscovery.EnableIPChangeAnnounce	1 – Enabled
iDRAC.IPMILan.Enable	0 – Disabled
iDAC.IPMISOL.Enable	1 – Enabled
iDRAC.SNMP.AgentEnable	0 – Disabled
iDRAC.NTPConfigGroupEnable.NTPEnable	0 – Disabled
iDRAC.GUI.SecurityPolicyMessage	By accessing this system, you confirm that such access complies with your organization's security policy.
iDRAC.VirtualConsole.Enable	1 – Enabled
iDRAC.VirtualConsole.EncryptEnable	1 – Enabled
iDRAC.VirtualConsole.WebRedirect	0 – Disabled
iDRAC.VNCServer.SSLEncryptionBitLength	1 – Auto Negotiate
iDRAC.VNCServer.Enable	0 – Disabled
iDRAC.VNCServer.Timeout	300
iDRAC.Users.2.IpmiLanPrivilege	15 – No Access
iDRAC.Users.2.ProtocolEnable. If SNMPv3 is needed set Authentication Type to SHA and Privacy Type to AES.	0 – Disabled
iDRAC.Users.2.AuthenticationProtocol	2 – SHA
iDRAC.Users.2.PrivacyProtocol	2 – AES

Table 19. Default Configuration Values (continued)

Configuration	Default Values
iDRAC.Users.2.Simple2FA	0 – Disabled
iDRAC.Security.MinimumPasswordScore	1 – Weak Protection
iDRAC.Security.PasswordRequireNumbers	0 – Disabled
iDRAC.Security.PasswordMinimumLength	0
iDRAC.Security.PasswordRequireSymbols	0 – Disabled
iDRAC.Security.PasswordRequireUpperCase	0 – Disabled
iDRAC.SecureDefaultPassword.ForceChangePassword	0 – False
iDRAC.ActiveDirectory.Enable	0 – Disabled
iDRAC.LDAP.Enable	0 – Disabled
iDRAC.Lockdown.SystemLockdown	0 – Disabled
BIOS.Syssecurity.PasswordStatus	Unlocked
BIOS.Syssecurity.PwrButton	Enabled
BIOS.Syssecurity.UefiVariableAccess	Standard
BIOS.Syssecurity.SecureBoot	Disabled
BIOS.Syssecurity.SecureBootPolicy	Standard
BIOS.Syssecurity.SecureBootMode	DeployedMode
LifeCycleController.LCAttributes.UserProxyPort	80
LifeCycleController.LCAttributes.UserProxyType	HTTP
LifeCycleController.LCAttributes.IgnoreCertWarning	1 – On

22

Network Vulnerability Scanning

Network vulnerability scanning is one of the many controls included as part of iDRAC's Security Design Lifecycle (SDL). Multiple industry-leading tools are used to verify that iDRAC maintains secure protocols and is not exposed to newly published CVEs and vulnerabilities. The table below outlines the known findings that may be highlighted when using these scanning tools and the Dell Response.

NOTE: Dell Technologies recommends configuring the iDRAC to secure settings that are recommended in the table below before running the scans.

Table 20. Network Vulnerability Scanning

Vulnerability	Port	Dell Response
1. Self-signed SSL certificate	443	This is a result of having self-signed SSL keys which cannot be verified by a certificate authority. To remove this finding, follow the steps that are outlined in the **Importing iDRAC Firmware SSL Certificate** section of the iDRAC10 User Guide.
2. SSL certificate cannot be trusted.	443	
3. The subject common name does not match the entity name (FQDN)	443	
4. Improper SSL certificate usage	443	
5. SSL signature verification failed	443	
6. SSL certificate invalid maximum validity date detected	443	
7. TLS/SSL Weak Message Authentication Code Cipher Suites	443	This is a result of the server using the following two cipher suites: • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA To remove this finding, disable the ciphers through iDRAC web interface or RACADM command-line interface.
8. Default/Guessable SNMP community names resulting in readable SNMP information (CVE-1999-0516, CVE-1999-0517)	161	This is a result of SNMP being enabled. To remove this finding, disable SNMP or update to SNMPv3 with an updated SNMP Community Agent Name. To update the Community Agent name, use the racadm command- `racadm set idrac.SNMP.CommunityAgent <name>`. To update to SNMP v3, use the racadm command- `racadm set idrac.SNMP.SNMPProtocol 1`.
9. SNMP credentials transmitted in cleartext	161	This is a result of SNMPv2 being enabled. To remove this finding, disable SNMP or enable SNMPv3 only. To update to SNMP v3, use the racadm command- `racadm set idrac.SNMP.SNMPProtocol 1`.
10. SNMP protocol version detected	161	
11. SNMP GETBULK reflected distributed DOS	161	
12. IPMIv2 Password Hash exposure (CVE-2013-4786, CVE-2013-4037)	623	This is a result of IPMI over LAN being enabled. To remove this finding disable IPMI over LAN. To disable IPMI over LAN, use the racadm command- `racadm set idrac.ipmilan.Enable 0`.
13. IPMIv1.5 GetChannelAuth response information disclosure	623	
14. IPMIv2 Authentication Username Disclosure	623	

Table 20. Network Vulnerability Scanning (continued)

Vulnerability	Port	Dell Response
15. SSH brute force login with default credentials	22	This is a result of a default password being used. To remove this finding, change the password. For more information about changing passwords, see the **Configuring User Accounts and Privileges** section of the iDRAC10 User Guide.
16. Dell Remote Access Controller default password for "root" account	N/A	
17. UDP constant IP identification field fingerprinting (CVE-2002-0510)	N/A	Dell does not consider this an issue and there are many ways to identify or fingerprint a Linux machine.
18. VNC remote control service detected	5901	This is a result of VNC being enabled. To remove this finding, disable VNC. To disable VNC, use the racadm command- `racadm set idrac.VNCServer.enable 0`.
19. Anonymous root login is allowed.	N/A	False positive. There is no root login or access to the iDRAC file system.
20. Nonabsolute directory entries found in the PATH variable	N/A	
21. TCP timestamp response	N/A	Dell does not consider the TCP timestamp response to be a security vulnerability given iDRAC's design and use. Knowledge of iDRAC's uptime is not considered a risk and its operating system is well-known and documented.
22. TCP sequence number approximation-based DOS (CVE-2004-0230)	N/A	Dell considers CVE-2004-0230 to be a vulnerability with minimal security risk, as it mainly effects long-lived connections, such as BGP routers. If the systems are installed according to Dell Best Practices, then the management network is separate from the host data network and can be isolated from the Internet over a firewall/VPN combination if connected at all. Access to the management network is limited to authorized administrative personnel, so security risks are minimized.
23. The host is vulnerable to the TLS Triple Handshake Vulnerability.	443	The TLS Triple Handshake attack is a false positive because iDRAC does not use client certificates or channel binding for authentication. Many scan tools are looking for this extension and are simply reporting that the extension is not present.
24. SSH Weak Key Exchange Algorithms Enabled	N/A	Use `racadm get idRAC.SSHCrypto.KexAlgorithms` to check the SSH algorithms in use. Remove the weaker SHA1 algorithm from the string and set it using `racadm set idRAC.SSHCrypto.KexAlgorithms`.
25. SSH Server CBC Mode Ciphers Enabled	N/A	Use `racadm get idRAC.SSHCrypto.Ciphers` to check the SSH ciphers in use. Remove the weaker CBC ciphers from the string and set it using `racadm set idRAC.SSHCrypto.Ciphers`.
26. OpenSSH remote code execution (CVE-2023-38408)	22	There is no impact for this OpenSSH Vulnerability because Dell does not enable `AllowAgentForwarding` on sshd configuration in iDRAC.
27. OpenSSH authentication bypass (CVE-2021-36368)	22	There is no impact for this OpenSSH Vulnerability because Dell does not support `Authentication type None` of OpenSSH in iDRAC.
28. OpenSSH row hammer attack (CVE-2023-51767)	22	There is no impact for this OpenSSH Vulnerability because of iDRAC's design and RACADM's restricted Shell.
29. OpenSSH command injection (CVE-2023-51385)	22	There is no impact for this OpenSSH Vulnerability as it only affects SSH client devices.

Table 20. Network Vulnerability Scanning (continued)

Vulnerability	Port	Dell Response
30. OpenSSH privilege escalation (CVE-2021-41617)	22	There is no impact for OpenSSH Vulnerability because Dell does not enable `AuthorizedKeysCommand` and `AuthorizedPrincipalsCommand` of OpenSSH in iDRAC.
34. OpenSSH sensitive information Disclosure (CVE-2023-28531)	22	There is no impact for OpenSSH Vulnerability because Dell does not support Smartcard keys or use `ssh-add` in iDRAC.
35. OpenSSH vulnerability (CVE-2023-51385)	22	Affects SSH clients and hence no impact on iDRAC.
36. OpenSSH vulnerability (CVE-2023-51767)	22	There is no impact on iDRAC because of its design and how it is deployed. The restricted Shell scripts of RACADM help to mitigate this vulnerability.
37. OpenSSH vulnerability (CVE-2024-39894)	22	Affects SSH clients and hence no impact on iDRAC.

23

Security Licensing

iDRAC offers various security features that require different licenses.

Table 21. Licensed security features in iDRAC10

Feature	iDRAC10 Core	iDRAC10 Enterprise	iDRAC10 Datacenter
Role-based authority	Yes	Yes	Yes
Local Users	Yes	Yes	Yes
SSL encryption	Yes	Yes	Yes
Secure Enterprise Key Manager	No	Yes (with SEKM license)	Yes (with SEKM license)
IP Blocking	Yes	Yes	Yes
Directory services (AD, LDAP)	No	Yes	Yes
Two-factor authentication (smart card)	No	Yes	Yes
Single sign-on	No	Yes	Yes
PK authentication (for SSH)	Yes	Yes	Yes
FIPS 140-2	No	No	No
Secure UEFI boot certificate management	Yes	Yes	Yes
Lockdown Mode	No	Yes	Yes
Unique iDRAC default password	Yes	Yes	Yes
Customizable Security Policy Banner - login page	Yes	Yes	Yes
Easy Multi Factor Authentication	No	No	Yes
Auto Certificate Enrollment (TLS/SSL Certs)	No	No	Yes
iDRAC Quick Sync 2 optional auth for read operations	Yes	Yes	Yes
iDRAC Quick Sync 2 - add mobile device number to LCL.	Yes	Yes	Yes
System Erase of internal storage devices.	Yes	Yes	Yes
RSA Secure ID	No	No	Yes
Delegated Authorization	No	No	Yes
Proof of Position Identity	No	No	Yes

24

Field Service Debug (FSD)

iDRAC10 Field Service Debugging (FSD) can be used when additional console debugging/support is needed to resolve system issues.

By using FSD, you can perform the following tasks:

- Allow enabling and copying of debug logs
- Allow copying of real-time logs
- Allow backing up or restoring of database to VM
- Enable debug access to Dell support team
- Allow flashing X-rev iDRAC, BIOS or FPGA

FSD is disabled by default. To initiate the FSD process, iDRAC administrators need to contact their Dell support representative.

25

Security Protocol and Data Model

The Integrated Dell Remote Controller (iDRAC) uses Security Protocol and Data Model (SPDM) to ensure that the components in the server assembly are genuine and from trusted device manufacturers.

SPDM from Distributed Management Task Force (DMTF), supports hardware identity verification to verify if the component is from a genuine manufacturer, and that the component is not tampered within the supply chain. iDRAC creates an inventory of devices and identifies if the devices are SPDM compatible or not. iDRAC provides details about the device SPDM capabilities in Redfish, RACADM, and GUI.

iDRAC verifies whether the device is genuine and if the validation fails, iDRAC logs an LC log message. For components that support SPDM, the device identity used in Secure Component Verification (SCV) is enhanced by using SPDM certificates.

26

Best Practices

Dell iDRAC Security Best Practices

Dell Best Practices regarding iDRAC:

- The iDRAC is intended to be on a separate management network. The iDRAC is not designed nor intended to be placed on, nor connected directly to the Internet. Doing so could expose the connected system to security and other risks for which Dell is not responsible.
- Dell Technologies recommends using the Dedicated Gigabit Ethernet port available on rack and tower servers to connect the iDRAC to a separate management network.
- Along with locating iDRAC on a separate management network, users should isolate the management subnet/vLAN with technologies such as firewalls, and limit access to the subnet/vLAN to authorized server administrators.
- Dell Technologies recommends using 256-bit encryption strength and TLS 1.2 or higher. For tighter control, additional ciphers may be removed using “Cipher Select” – see the iDRAC User Guide for more details.
- Dell Technologies recommends additional settings such as IP range filtering and System Lockdown Mode.
- Dell Technologies recommends using additional security authentication options such as Microsoft Active Directory or LDAP.
- Dell Technologies recommends keeping iDRAC firmware up to date.

Link to Firmware:

Users can download software, including the latest release of iDRAC firmware, from the Dell Support site.

Users can find the iDRAC documentation from the iDRAC page on the Dell Support site.

27

Appendix - References

- iDRAC Documentation—Dell support site
- iDRAC Redfish Scripts on GitHub—Redfish scripts
- Set up BIOS on 17th Generation Dell PowerEdge Sever—Set up BIOS on 17th Generation Dell PowerEdge Severs