DELL EMC

iDRAC9 Cipher Select – Improved Security for Dell EMC PowerEdge Servers

Cipher Select is an advanced user setting where the user can choose to block undesired ciphers negotiated by iDRAC, providing increased security.

May 2019

Revisions

Date	Description
May 2019	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC team:

Alaric Silveira

Chris Sumers

Doug Iler

Traci Knipp

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of contents

Executive summary

The Cipher Suite Selection can be used to limit the ciphers the web browser can use to communicate with iDRAC. Also, it can determine how secure the connection is. These settings can be configured through iDRAC web interface, RACADM, Redfish, and WSMan.

This functionality is available across several iDRAC releases – iDRAC7, iDRAC8, and the current iDRAC9. However, this technical brief will focus on iDRAC9.

1 Introduction

Security is crucial to the daily operation of your data center. IT administrators are continually implementing new methods to buttress their security efforts. The integrated Dell Remote Access Controller (iDRAC) offers several many tools and security solutions. iDRAC9 is built on a foundation of SELinux and offers new features such as Lockdown Mode alongside standard tools like Active Directory and LDAP integration.

One key area of focus is at a different layer – the access to the iDRAC itself. Many IT administrators are locking down access to the iDRAC by enabling browsers to connect using TLS 1.2 and enforcing 256-bit encryption strength.

1.1 Taking the next step – Advanced control using Cipher Select

Let us say you are already using these settings – TLS 1.2-bit and 256-bit encryption. At this point, you are left with a few ciphers at your disposal to connect from the browser to the iDRAC. But what if you want to limit those choices even further?

First step is to check the firmware on your iDRAC. For iDRAC7/8, version 2.60.60.60 or higher is required. And for iDRAC9 version 3.30.30.30 or higher is required.
Note: If the firmware is rolled back to a previous version where the newly added attribute is not supported, the behavior reverts to that of the rolled back firmware version.

1.2 The ciphers available with TLS1.2 Bit and 256 Bit Encryption

The following chart shows which ciphers are available when the above settings are enforced. For most Admins this is the preferred starting point. This quickly shortens the list of ciphers that are negotiated by iDRAC.
To see what ciphers are available you can use some tools such as testssl, sslscan, or ssldigger.

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
```

At this point, you can use the advanced settings to block undesired ciphers that are negotiated by iDRAC. Note, it is not possible to enable the weak ciphers that are already blocked by the TLS protocol and encryption strength set. For example, you cannot reenable a TLS 1.1 cipher if you have already enforced TLS 1.2 or higher.

The syntax of the Cipher List string needs to be consistent with the specifications that are provided in the manual located https://www.openssl.org/docs/man1.0.2/man1/ciphers

The feature may not behave in the manner that is described in this document when FIPS Mode has been ENABLED. When FIPS Mode is enabled, the TLS Cipher Suite may be filtered/reduced to a much smaller subset as governed by the NIST FIPS 140-2 Specification since FIPS Mode makes changes to the underlying capability of the Standard OpenSSL Library.

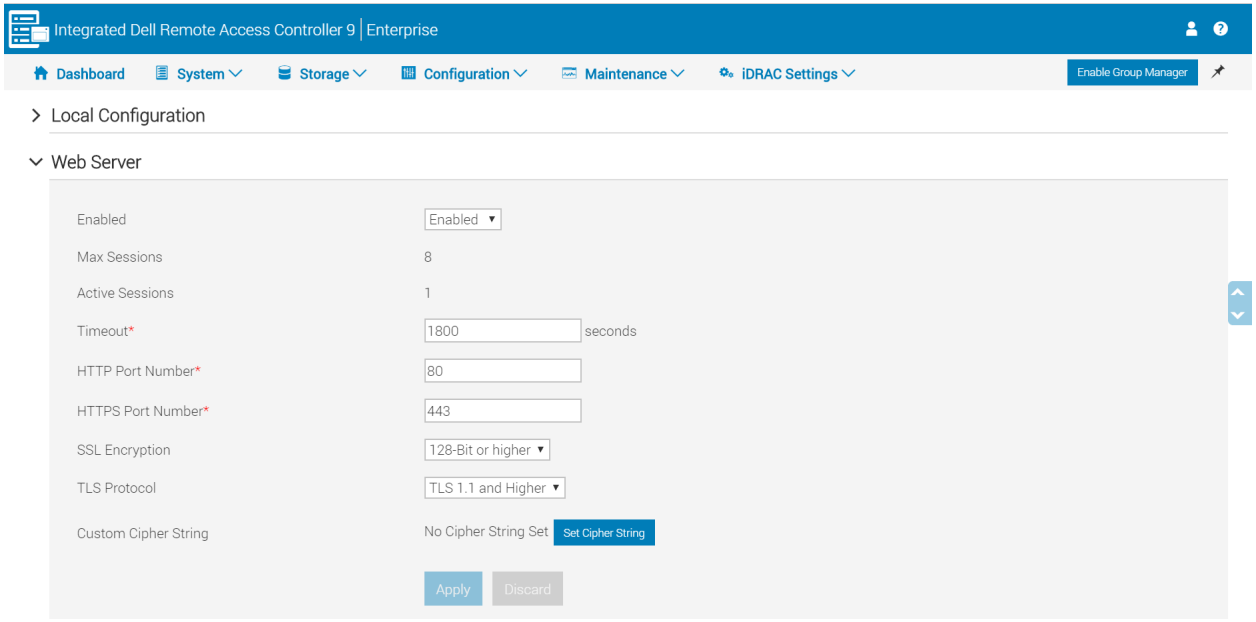
User’s should be aware of the browsers that supports the Cipher Suites. To see what ciphers your browser supports go to the following links using different browsers: https://cc.dcsec.uni-hannover.de/ or https://www.ssllabs.com/ssltest/viewMyClient.html

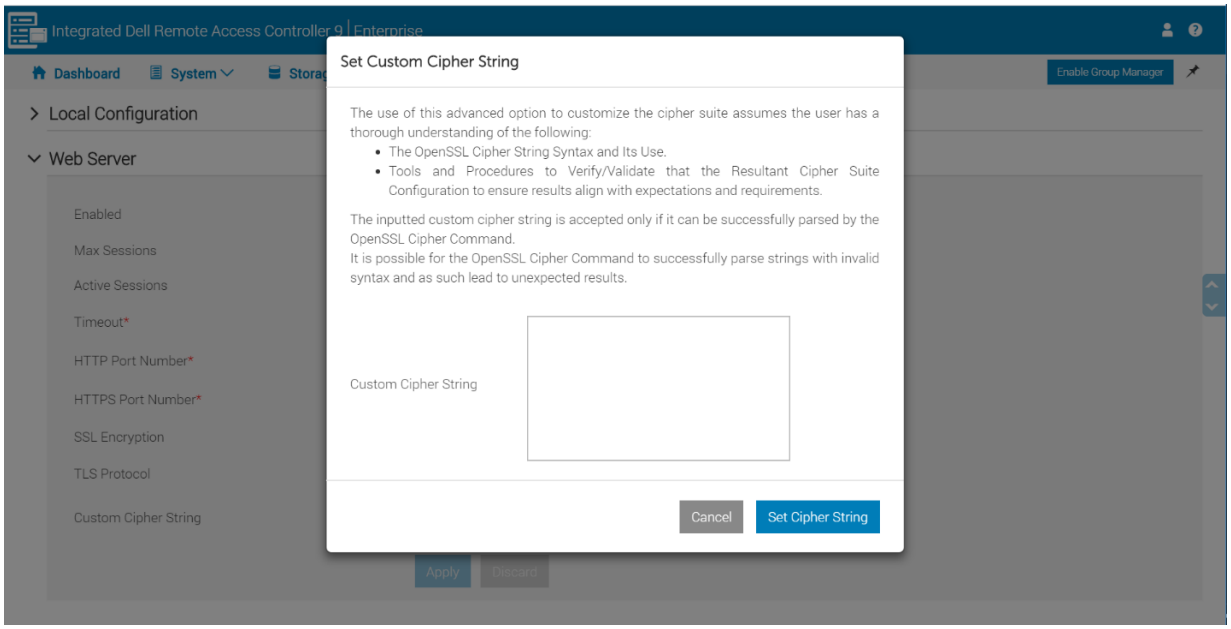
2 Setting Cipher Select policies

There are several methods in which IT admins can set Cipher Select rules. GUI, RACADM, and Redfish will be covered.

2.1 Setting using the iDRAC GUI

To set ciphers in 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.

2.2 Setting via RACADM commands

To set custom cipher using RACADM use the command:
“racadm set idrac.webserver.CustomCipherString <cipher>”

Note that RACADM does not allow you to set a cipher string that is separated by space so use comma or colon.

To set multiple ciphers, see the following example:

racadm set idrac.webserver.CustomCipherString ALL:!DHE-RSA-AES128-SHA256:!ECHE-RSA-AE256-SHA384

/admin1-> racadm set idrac.webserver.CustomCipherString ALL:!DHE-RSA-AES256-GCM

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

Object value modified successfully

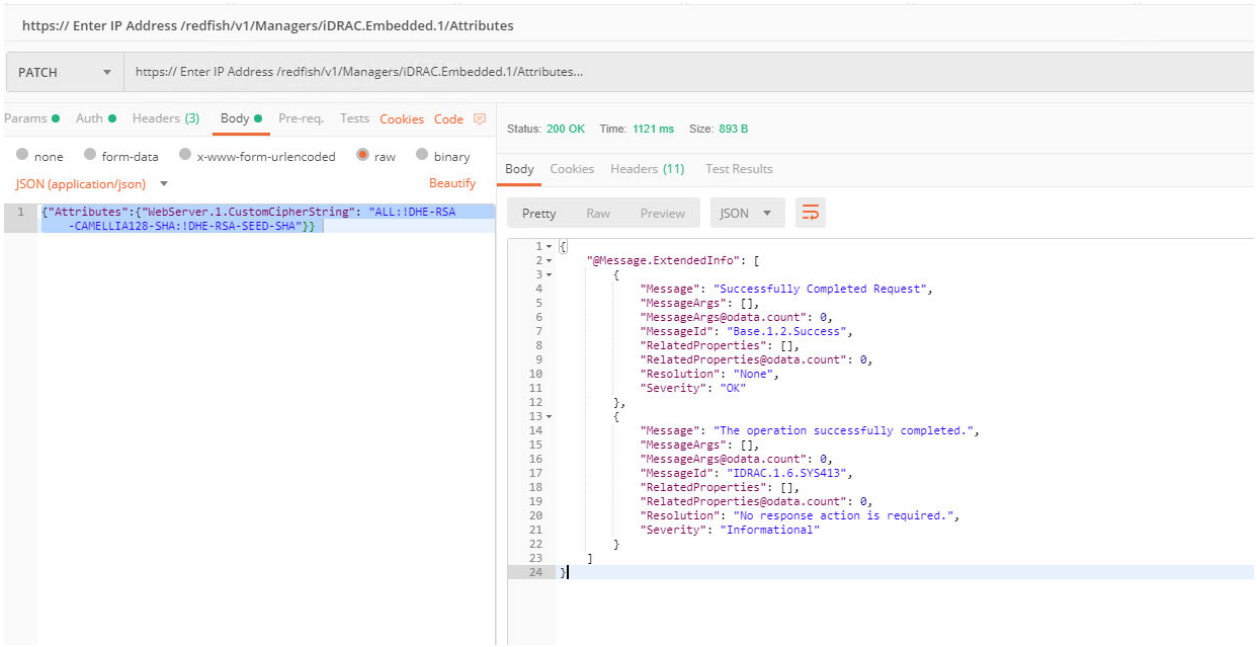
To set a NULL value to delete the Cipher String which is already set: Use “” as cipher string value.

2.3 To run the Redfish commands using an API Develop Environment such as Postman

- Enter GET request - https://IPAddress/redfish/v1/Managers/iDRAC.Embedded.1/Attributes

Now Perform PATCH operation with the supported cipher suite in proper format which can be seen in OPENSSL website. See example below.

- {"Attributes":{"WebServer.1.CustomCipherString": "ALL:!DHE-RSA-CAMELLIA128-SHA:!DHE-RSA-SEED-SHA"}}



To set NULL value, enter {"Attributes":{"WebServer.1.CustomCipherString": ""}} in the input section.

2.4 Setting ciphers using WSMan

Use the following command to set Ciphers using WSMan.

- winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCardService+Name=DCIM:iDRACCardService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:root -p:calvin -r:https://100.65.177.126/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="iDRAC.Embedded.1";AttributeName="WebServer.1#CustomCipherString";AttributeValue="ALL:!DHE-RSA-AES256-SHA"}

To set a NULL value to delete the Cipher String which is already set: Use “” as cipher string value, see example below:

- winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_iDRACCardService?CreationClassName=DCIM_iDRACCardService+Name=DCIM:iDRACCardService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:root -p:calvin -r:https://IPAddress/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="iDRAC.Embedded.1";AttributeName="WebServer.1#CustomCipherString";AttributeValue=""}

Conclusion

Dell is continually looking for areas to improve the overall security of iDRAC which in turn improves the security of your servers, your information, and your business. Cipher Select is available in the 3 current and previous generations of PowerEdge Servers, which means a secure policy you can enforce across your entire data center.