Secureboot certificate management using RACADM CLI

RACADM supports Secure Boot certificate management by using a new command **`bioscert`**. Following is the list of operations supported by using `bioscret`.

Secure boot certificate management operations	Role/Privilege required for iDRAC Users	Value/Setting required for "SecureBootPolicy" attribute
View	Login	`Standard/Custom`
Export	Login	`Custom`
Import	Login & System/Server Control	`Custom`
Restore	Login & System/Server Control	`Custom`
Delete	Login & System/Server Control	`Custom`

RACADM supports the following Secure Boot attribute configurations:

Attributes	Legal Values	Default Value	RACADM command to read value
`SecureBoot`	`Enabled,` `Disabled`	`Disabled`	`racadm get BIOS.SysSecurity.SecureBoot`
`SecureBootPolicy`	`Standard,` `Custom`	`Standard`	`racadm get BIOS.SysSecurity.SecureBootPolicy`

`SecureBootMode`	`UserMode,`
	`SetupMode, AuditMode,`
	`DeployedMode`
		`UserMode`	`racadm get BIOS.SysSecurity.SecureBootMode`

To modify settings of the above attributes, `racadm set` can be used as shown in the screen shot. After modification, change goes to pending state. Therefore, to apply the modified value, a configuration job must be created with the help of `racadm jobqueue create BIOS.Setup.1-1` and then a Host restart.

```
/admin1-> racadm set BIOS.SysSecurity.SecureBootMode "DeployedMode"
[Key=BIOS.Setup.1-1#SysSecurity]
RAC1017: Successfully modified the object value and the change is in
       pending state.
       To apply modified value, create a configuration job and reboot
       the system. To create the commit and reboot jobs, use "jobqueue"
       command. For more information about the "jobqueue" command, see RACADM
       help.
/admin1-> racadm jobqueue create BIOS.Setup.1-1
RAC1024: Successfully scheduled a job.
Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.
Commit JID = JID_930656581647
```

Firmware and remote racadm allow certificate management operations irrespective of the SecureBootMode settings. However, Local RACADM (Inband tool) does not allow Secure Boot certificate management operations when “SecureBootMode” is set to DeployedMode

Currently, the Secure Boot Certificate management by using RACADM is not a licensed feature. Therefore, RACADM allows certificate management operations irrespective of the license installed on your iDRAC.

Certificate management operations

Allowed operations and their syntaxes can be retrieved by running `racadm help bioscert` as shown in the screen shot. Generic syntax of **`bioscert`** operations which act on individual certificate or hash is:

`racadm bioscert <sub-command/operation> -t <KeyType> -k <KeySubType> -v <Hashvalue or Thumbprintvalue>`

```
/admin1-> racadm help bioscert

bioscert -- UEFI Secure Boot Certificate Management operations.

bioscert has multiple subcommands, view the help as shown below.

Usage:

racadm bioscert help import
racadm bioscert help export
racadm bioscert help restore
racadm bioscert help delete
racadm bioscert help view

--------------------------------------------------------------------------------
```

```
-t: <keyType>   : Key Type of the Secure Boot Certificate to be viewed.
                  0       : PK(Platform Key)
                  1       : KEK(Key Exchange Key)
                  2       : DB(Signature Database)
                  3       : DBX(Forbidden Signatures Database)
-k: <KeySubType>: Certificate type or Hash Type of
          Secure Boot Certificate file to be viewed.
                  0       : Certificate type
                  1       : Hash Type(SHA-256)
                  2       : Hash Type(SHA-384)
                  3       : Hash Type(SHA-512)
-v: <ThumbPrint/Hash Value>       : ThumbPrint value or Hash Value of
    Secure Boot Certificate file to be viewed.
```

Bioscert View Operation

Based on the “SecureBootPolicy” settings, it retrieves data from respective certificate store and displays. If the request is to view a certificate record, the output will list details of the certificate attributes such as subject information, issuer details, valid from, valid to, and thumb print etc. If the request is to view a hash record then the output lists the details of the record along with the hash value of the record.

racadm bioscert view --all

racadm bioscert view -t <keyType> -k <KeySubType> -v <HashValue or ThumbPrintValue>

Examples are shown in the screen shot here:

```
/admin1-> racadm bioscert view --all

 -------------------- SECURE BOOT CERTIFICATE DETAILS --------------------

SecureBootCert Policy  :Custom
Certificate Type       :PK
Certificate SubType    :Certificate
Serial Number          :18E0E033DB57CD984ABB23689D61BE4D

Subject Information:
Country Code (CC)      :US
State (S)              :Texas
Locality (L)           :Round Rock
Organization (O)       :Dell Inc.
Organizational Unit(OU):
Common Name (CN)       :Dell Inc. Platform Key

Issuer Information:
Country Code (CC)      :US
State (S)              :Texas
Locality (L)           :Round Rock
Organization (O)       :Dell Inc.
Organizational Unit(OU):
Common Name (CN)       :Dell Inc. Platform Key

ThumbPrint             :A8:52:14:A3:BA:23:C1:CE:98:5A:C2:F6:52:11:C3:54:7B:C4:0A:FC

Valid From             :Feb  2 17:17:37 2016 GMT
Valid To               :Feb  2 17:27:36 2031 GMT

--------------------------------------------------------------------------------

SecureBootCert Policy  :Custom
Certificate Type       :KEK
Certificate SubType    :Certificate
Serial Number          :610AD188000000000003
```

The `View --all` command lists all the certificates and image digests present on the system at that point in time. If you want to view information about a specific record (certificate or image digest) then the command must specify the certificate type, subtype, and identifier of the record as shown in the screen shot here:

```
/admin1-> racadm bioscert view -t 0 -k 0 -v A8:52:14:A3:BA:23:C1:CE:98:5A:C2:F6:52:11:C3:54:7B:C4:0A:FC

 -------------------- SECURE BOOT CERTIFICATE DETAILS --------------------

SecureBootCert Policy  :Custom
Certificate Type       :PK
Certificate SubType    :Certificate
Serial Number          :18E0E033DB57CD984ABB23689D61BE4D

Subject Information:
Country Code (CC)      :US
State (S)              :Texas
Locality (L)           :Round Rock
Organization (O)       :Dell Inc.
Organizational Unit(OU):
Common Name (CN)       :Dell Inc. Platform Key

Issuer Information:
Country Code (CC)      :US
State (S)              :Texas
Locality (L)           :Round Rock
Organization (O)       :Dell Inc.
Organizational Unit(OU):
Common Name (CN)       :Dell Inc. Platform Key

ThumbPrint             :A8:52:14:A3:BA:23:C1:CE:98:5A:C2:F6:52:11:C3:54:7B:C4:0A:FC

Valid From             :Feb  2 17:17:37 2016 GMT
Valid To               :Feb  2 17:27:36 2031 GMT

--------------------------------------------------------------------------

/admin1-> racadm bioscert view -t 3 -k 1 -v 45C7C8AE750ACFBB48FC37527D6412DD644DAED8913CCD8A24C94D856967DF8E

 -------------------- SECURE BOOT CERTIFICATE DETAILS --------------------

SecureBootCert Policy  :Custom
Certificate Type       :DBX
Certificate SubType    :SHA-256

Hash                   :45C7C8AE750ACFBB48FC37527D6412DD644DAED8913CCD8A24C94D856967DF8E

--------------------------------------------------------------------------
```

Bioscert Export Operation

Export the Secure Boot Certificate to a remote share (CIFS, NFS, HTTP, and HTTPS) or local share:

racadm bioscert export -t <keyType> -k <KeySubType> -v <HashValue or ThumbPrintValue> -f <filename> [-l <CIFS/NFS/HTTP/HTTPS share path>] [-u <username>] [-p <password>]

Example

Export DB key to CIFS share by using the local or firmware RACADM

```
$ racadm bioscert export -t 1 -k 0 -v
31:59:0B:FD:89:C9:D7:4E:D0:87:DF:AC:66:33:4B:39:31:25:4B:30 -f kek_cer.der -l
//100.97.161.33/sambashare/ -u root -p dell_123
```

The Event and Error Message RAC1202: The Secure Boot Certificate is successfully exported.

```
Usage Examples:

- Export the KEK certificate to a remote CIFS share:
 racadm bioscert export -t 1 -k 0 -v AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E
 -f kek_cert.der -l //10.94.161.103/share -u admin -p mypass

- Export the DBX(Hash Type SHA-256) to a remote NFS share:
 racadm bioscert export -t 3 -k 1 -v 416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
 -f kek_cert.der -l 192.168.2.14:/share

- Export the KEK certificate to a local share using local racadm:
  racadm bioscert export -t 1 -k 0 -v AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E
  -f kek_cert.der

- Export the KEK certificate to a local share using remote racadm:
  racadm -r 10.94.161.119 -u root -p calvin bioscert export -t 1 -k 0
  -v AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E -f kek_cert.der
```

```
/admin1->
/admin1-> racadm bioscert export -t 1 -k 0 -v 31:59:0B:FD:89:C9:D7:4E:D0:87:DF:AC:66:33:4B:3
9:31:25:4B:30 -f kek_cer.der -l //100.97.161.33/sambashare/ -u root -p dell_123
RAC1202: The Secure Boot Certificate is successfully exported.
/admin1->
```

Note:

- In case “SecureBootPolicy” is set to `Standard`, RACADM will not allow export operation, but the following Event and Error Message is displayed: `RAC1212: Unable to complete the operation because the Secure Boot policy is set to Standard.`
- If the remote share does not have enough space during export, the following Event and Error Message is displayed: `RAC1219: Unable to export the Secure Boot certificate data to remote share because of insufficient storage space.`
- Local file share support is allowed only from Remote and Local RACADM.
- To know more about export command, enter the `racadm bioscert help export` command at the RACADM CLI.

Bioscert Import Operation

This feature enables you to import a Secure Boot Certificate to iDRAC from remote share (CIFS, NFS, HTTP, and HTTPS) or local share. If you want to enroll a certificate to authenticate a firmware or driver or Option ROM, which is likely to get executed during the POST, the Import feature enables you to add the certificate to the iDRAC Secure Boot certificate store. Subcommand to be used for import operation is “import”. The command must provide details of certificate type, subtype, path to the file to import, and share details.

racadm bioscert import -t <keyType> -k <KeySubType> -f <filename> [-l <CIFS/NFS/HTTP/HTTPS share path>] [-u <username>] [-p <password>]

Example

Import KEK Key from CIFS share using local RACADM

$ racadm bioscert import -t 1 -k 0 -f kek_cer.der -l //100.97.161.33/sambashare -u root -p dell_123

The Event and Error Message RAC1203: The Secure Boot Certificate Import operation is successfully scheduled. For the changes to become effective, restart the host server.

```
Usage Examples:

- Import KEK Certificate from CIFS share to Embedded iDrac:
  racadm bioscert import -t 1 -k 0 -f kek_cert.der
 -l //10.94.161.103/share -u admin -p mypass

- Import KEK(Hash Type SHA-256) from CIFS share to Embedded iDrac:
  racadm bioscert import -t 1 -k 1 -f kek_cert.der
  -l //192.168.2.140/licshare -u admin -p passwd

- Import KEK Certificate from a NFS share to Embedded iDrac:
  racadm bioscert import -t 1 -k 0 -f kek_cert.der -l 192.168.2.14:/share

- Import KEK Certificate from a local share using Local RACADM:
  racadm bioscert import -t 1 -k 0 -f kek_cert.der

- Import KEK Certificate from a local share using remote RACADM:
  racadm -r 10.94.161.119 -u root -p calvin bioscert import -t 1 -k 0 -f kek_cert.der
```

After the import request is successfully serviced, a pending task is added to the pending list in iDRAC which gets serviced during the next restart of the host server. Therefore, to apply the changes of requested Secure Boot certificate management operations, the host server must be restarted.

```
/admin1-> racadm bioscert import -t 1 -k 0 -f kek_cer.der -l //100.97.161.33/sam
bashare -u root -p dell_123
RAC1203: The Secure Boot Certificate Import operation is successfully scheduled.
       For the changes to become effective, restart the host server.
/admin1->
```

Note

- If “SecureBootPolicy” is set to `Standard`, RACADM will not allow export operation, but the following Event and Error Message is displayed: `RAC1212: Unable to complete the operation because the Secure Boot policy is set to Standard.`
- If “SystemLockDownMode” is enabled, RACADM does not allow import operation and the following Event and Error Message is displayed: `RAC1201: Unable to complete the operation because the server is in the lockdown mode.` “SystemLockDownMode” must be disabled before trying the import operation.
- After importing a new PK, if a PK already exists, RACADM displays the following Event and Error Message: `RAC1213: Unable to import the Public Key (PK) because a PK already exists`. Therefore, before importing the new PK, the existing PK must be deleted.
- Local file share support is allowed only from Remote and Local RACADM.
- To know more about import command, enter the `racadm bioscert help import` command at the RACADM CLI.

Bioscert Delete Operation

The *Delete* operation deletes the installed Secure Boot certificate or an image digest in the iDRAC Secure Boot certificate store. *Delete* operation is applicable when you want to delete one or more of the standard certificates or image digests, and enroll your own customized certificates or image digests. *Delete* command must provide the record type, subtype, and identifier (Thumb print or hash) of the record.

```
racadm bioscert delete --all

racadm bioscert delete -t <keyType> -k <KeySubType> -v <HashValue or ThumbPrintValue>
```

Example

To delete an installed DBX Secure Boot Certificate of HASH type SHA-256

```
$ racadm bioscert delete -t 3 -k 1 -v
416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
```

The Event and Error Message RAC1204: The Secure Boot Certificate Delete operation is successfully scheduled. For the changes to become effective, restart the host server.

DeleteAll certificates

```
racadm bioscert Delete --all
```

The Event and Error Message RAC1206: The Secure Boot Certificate DeleteAll operation is successfully scheduled. For the changes to become effective, restart the host server.

```
Usage Examples:

- To Delete an installed KEK Secure Boot Certificate
  racadm bioscert delete -t 1 -k 0 -v 58:0A:6F:4C:C4:E4:B6:69:B9:EB:DC:1B:2B:3E:
08:7B:80:D0:67:8D

- To Delete an installed DBX Secure Boot Certificate of HASH type SHA-256
  racadm bioscert delete -t 3 -k 1 -v 416e3e4a6722a534afba9040b6d6a69cc313f1e48e
7959f57bf248d543d00245

- To Delete all the installed Secure Boot Certificates
  racadm bioscert delete --all
```

After the *Delete* request is successfully serviced, a pending task is added to the pending list in iDRAC which gets serviced during the next restart of the host server. Therefore, to apply the changes of requested Secure Boot certificate management operations, the host server must be restarted.

```
/admin1-> racadm bioscert delete -t 1 -k 0 -v 31:59:0B:FD:89:C9:D7:4E:D0:87:DF:A
C:66:33:4B:39:31:25:4B:30
RAC1204: The Secure Boot Certificate Delete operation is successfully scheduled.
       For the changes to become effective, restart the host server.
/admin1->
```

Note:

- If “SecureBootPolicy” is set to `Standard`, RACADM will not allow export operation, but the following Event and Error Message is displayed: `RAC1212: Unable to complete the operation because the Secure Boot policy is set to Standard.`
- If “SystemLockDownMode” is enabled, RACADM does not allow import operation and the following Event and Error Message is displayed: `RAC1201: Unable to complete the operation because the server is in the lockdown mode.` “SystemLockDownMode” must be disabled before trying the import operation.
- To know more about delete command, enter the `racadm bioscert help delete` command at the RACADM CLI.

Bioscert Restore Operation

The *Restore* operation resets the installed custom certificates to default standard certificates. Restore operation helps you to undo the changes you made on certificate store by replacing the customized certificates with standard default certificates. Restore operations can be performed on certificate store based on section (PK/KEK/DB/DBX) or as a whole.

RACADM does not support individual certificate Hash restore.

```
racadm bioscert restore –all

racadm bioscert restore -t <keyType>
```

Example

Restore DB section

racadm bioscert restore –t 2

The Event and Error Message RAC1205: The Secure Boot Certificate Restore operation is successfully scheduled. For the changes to become effective, restart the host server.

RestoreAll certificates

`racadm bioscert restore –all`

The Event and Error Message RAC1207: The Secure Boot Certificate RestoreAll operation is successfully scheduled. For the changes to become effective, restart the host server.

```
Usage Examples:

- To Restore the installed KEK Secure Boot Certificates
  racadm bioscert restore –t 1

- To Restore all the installed Secure Boot Certificates
  racadm bioscert restore --all
```

After the restore request is successfully serviced, a pending task is added to the pending list in iDRAC which gets serviced during the next restart of the host server. Therefore, to apply the changes of requested Secure Boot certificate management operations, the host machine should be rebooted.

```
/admin1-> racadm bioscert restore -t 1
RAC1205: The Secure Boot Certificate Restore operation is successfully
       scheduled.For the changes to become effective, restart the host server.
```

Note:

- If “SecureBootPolicy” is set to `Standard`, RACADM will not allow export operation, but the following Event and Error Message is displayed: `RAC1212: Unable to complete the operation because the Secure Boot policy is set to Standard.`
- If “SystemLockDownMode” is enabled, RACADM does not allow import operation and the following Event and Error Message is displayed: `RAC1201: Unable to complete the operation because the server is in the lockdown mode.` “SystemLockDownMode” must be disabled before trying the import operation.

1. To know more about restore command, enter the `racadm bioscert help restore` command at the RACADM CLI.