Manuals+ — User Manuals Simplified.

Dell EMC EMC Secured Component Verification Reference User Guide

Contents

Dell EMC EMC Secured Component Verification Reference

Secured Component Verification

SCV Process
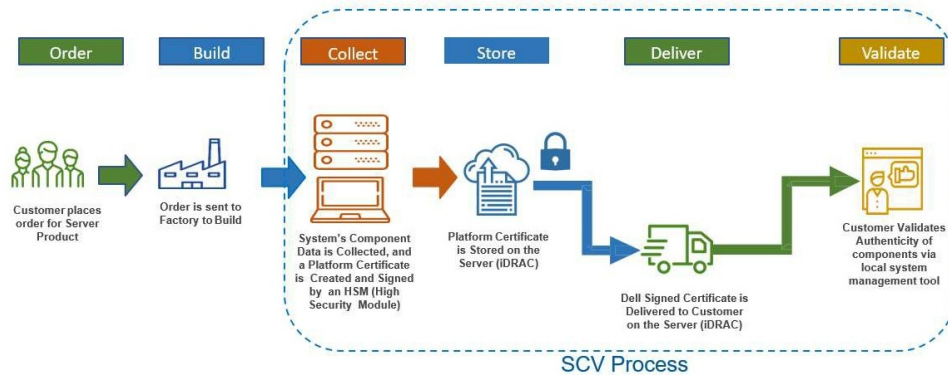
Product Information

- **Product Name:** Secured Component Verification Reference Guide for Servers
- **Version:** 10 2020 Rev. A00

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.

This section provides an overview about Secured Component Verification (SCV) and the system requirements for running the application on the system.

Topics:

- Secured Component Verification
- System Requirements

Overview

This section provides an overview about Secured Component Verification (SCV) and the system requirements for running the application on the system.

Secured Component Verification:
Secured Component Verification (SCV) is a supply chain assurance offering that enables you to verify that the PowerEdge server you have received matches what was manufactured in the factory. In order to validate components in a certificate containing the unique system component IDs is generated during factory assembly process. This certificate is signed in the Dell factory and is stored in iDRAC9, later used by the SCV application. The SCV application validates the system inventory against the SCV certificate. The application generates a validation report detailing the inventory match and mismatches against the SCV certificate. It also verifies the certificate and Chain of Trust along with the Proof of Possession of the SCV Private key for iDRAC9. Current implementation supports direct ship customers and does not include VAR or Part Replacement scenarios.

Secure Component Verification (SCV) Application performs the following functions:

- Downloads the SCV Certificate that is stored in iDRAC via RACADM and verifies the SCV certificate and issuer.

- Validates the SCV private key that is paired to the SCV public key in SCV certificate.
- Collects the current inventory of the system including the TPM EK Certificate Serial Number.
- Compares current system inventory against the inventory in the SCV certificate, including TPM EK Serial.
- Any swapping or removal of the components that are captured in the certificate will be identified as a "Mismatch". NOTE: SCV validates the virtual network ports as well. In systems with NPAR/NPAReP cards, run the SCV application before enabling them.
- **NOTE:** Ensure that any drive which is removed from the system registers in iDRAC or any other iDRAC interface, before running the SCV validation, or it will report incorrect data in the SCV output.
- SCV validates the virtual network ports as well. In systems with NPAR/NPAReP cards, run the SCV application before enabling them.
- Ensure that the TPM is enabled before running the SCV application.
- SCV does not support InfiniBand and Fibre Channel (FC).
- SCV application must be run before mapping any storage devices to the system.
- Flex Address should be disabled in modular systems, before running the SCV application.
- If internal and iDRAC USB ports are disabled, the SCV validation will fail.
- Ensure that any drive which is removed from the system registers in iDRAC or any other iDRAC interface, before running the SCV validation, or it will report incorrect data in the SCV output.

System Requirements:

- **Category:** Supported Operating Systems
- **Requirement:** WinPE 10.x and Red Hat Enterprise Linux 7.x
- **iDRAC Tools version:** iDRAC Tools 9.5.1 and above.

Category	Requirement
Supported Operating Systems	WinPE 10.x and Red Hat Enterprise Linux 7.x
iDRAC Tools version	iDRAC Tools 9.5.1 and above. **NOTE:** In iDRAC Tools, SCV is an independent application apart from RACADM and IPMI tool.

iDRAC9 version	4.32.10.00 and above
Software dependencies	Python 2.7 and OpenSSL
iDRAC licenses required	Secured Component Verification License

NOTE: SCV support is enabled only with local Redfish interface.

Components supported
Baseboard
Processor
OEM
Memory
Power supply
Harddrive
Network card
iDRAC
TPM
System Information

NOTE: In iDRAC Tools, SCV is an independent application apart from RACADM and IPMI tool.

Secured Component Verification on Linux

This section provides information on running SCV on Linux and how to check SCV logs using Linux.

This section provides information for the following:
Topics:

- Creating an ISO image to run SCV using WinPE
- Adding SCV to Custom ISO Image
- Adding RACADM to an ISO image
- Running SCV on WinPE
- How to check SCV logs using WinPE

Creating an ISO image to run SCV using WinPE
To create an ISO image to run SCV using WinPE:

1. Download the iDRAC tools from the Drivers & downloads page for your system at
   https://www.dell.com/support.
   NOTE: SCV is supported on iDRAC Tools version 9.5.1 or later.
2. Ensure that Windows ADK and Windows PE add-on for ADK is installed in the system for WinPE 10.x. To
   download and install the files, go to
   https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.
3. Run the self-extractor file for iDRAC tools and click Unzip to extract the files to the default location.
   NOTE: To extract the files to a specified location, click on Browse and select the folder where the files need to
   be extracted and click OK and then Unzip.
4. Launch command prompt and change directory to the location where the files were extracted. Run the batch
   file (WinPE10.x_driverinst.bat) using command prompt to create a bootable ISO image.

5. Once the ISO image is created successfully, open the folder created with the name "WINPE10.x-%timestamp%", to find the ISO image.

Confirmation of the ISO image created successfully

6. Use this ISO image to boot the SCV environment in the server.

Adding SCV to Custom ISO Image
To add SCV to your custom ISO image:

1. Download the iDRAC tools from the Drivers & downloads page for your system at
   https://www.dell.com/support.
   NOTE: SCV is supported on iDRAC Tools version 9.5.1 or later.
2. Ensure that Windows ADK and Windows PE add-on for ADK is installed in the system for WinPE 10.x. To download and install the files, go to
   https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.
3. Run the self-extractor file for iDRAC tools and click Unzip to extract the files to the default location.
   NOTE: To extract the files to a specified location, click on Browse and select the folder where the files need to

be extracted and click OK and then Unzip.

4. Copy the following folders into the corresponding folder path in the Custom ISO image:

   - scv to X:\Dell
   - Toolkit\Python27, Toolkit\TPM, Toolkit\OpenSSL to X:\Dell\scv
   - Toolkit\DLLs to X:\windows\system32

5. After copying the files, set the path for the folder using the command set
   PATH=%PATH%;X:\Dell\scv;X:\Dell\scv\Python27;X:\Dell\scv\openssl;X:\Dell\scv\tpm;

6. SCV can now be used to run validation.

Adding RACADM to an ISO image
To copy RACADM files into an ISO image:

1. Download the iDRAC tools from the Drivers & downloads page for your system at
   https://www.dell.com/support.
   NOTE: SCV is supported on iDRAC Tools version 9.5.1 or later.

2. Run the self-extractor file for iDRAC tools and click Unzip to extract the files to the default location.
   NOTE: To extract the files to a specified location, click on Browse and select the folder where the files need to
   be extracted and click OK and then Unzip.

3. Copy the Racadm folder into directory X:\Dell and set the path for the folder using the command set
   PATH=%PATH%;X:\Dell\Racadm.

Running SCV on WinPE

1. Login to iDRAC in the system where you want to run the SCV application.
2. Launch the Virtual Console and click Connect Virtual Media.
3. Click on Virtual Media and under Map CD/DVD click Browse and select the ISO image for SCV and click on
   Map Device and close the window.
4. In the Virtual Console window, click on Boot and select Virtual CD/DVD/ISO and click Yes on the prompt to
   confirm the new boot device.
5. Click on Power and power on the system and let it boot into the ISO image.
6. Once the system boots into the ISO image, wait for the command prompt window to load into the directory
   X:\Dell>
7. Navigate to X:\Dell\scv and run the command scv validateSystemInventory to start the validation process.

```
Administrator: X:\windows\system32\cmd.exe

X:\Dell\racadm>cd ..

X:\Dell>cd scv

X:\Dell\scv>dir
 Volume in drive X is Boot
 Volume Serial Number is D60A-0DC2

 Directory of X:\Dell\scv

09/09/2020  10:19 PM    <DIR>          .
09/09/2020  10:19 PM    <DIR>          ..
09/03/2020  10:08 AM         2,724,856 scv.exe
09/09/2020  10:19 PM    <DIR>          openssl
09/09/2020  10:19 PM    <DIR>          Python27
09/09/2020  10:19 PM    <DIR>          scvapp
09/09/2020  10:19 PM    <DIR>          tpm
               1 File(s)      2,724,856 bytes
               6 Dir(s)     523,595,776 bytes free

X:\Dell\scv>scv validateSystemInventory
```

8. Once the system runs the SCV application successfully, it should give the result Validating System Inventory: Match

```
X:\Dell\scv>scv validateSystemInventory
Downloading SCV Certificate from iDRAC: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "FRH89V2" matches Certificate: Match
Validating System Inventory: Match
-----------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_FRH89V2_2020_09_22_16_17_15.log
-----------------------------------------------------------------
```

9. If the result shows as Validating System Inventory: Mismatch it will specify which component has mismatched under Mismatch Inventory Summary. For more help contact Technical Support.

```
HardDrive 2: Mismatch
Expected:
{
        "Manufacturer" : "TOSHIBA",
        "Media Type" : "HDD",
        "Model" : "AL13SXB30EN",
        "Name" : "Physical Disk 0:1:2",
        "Part Number" : "PH00RVDT7557158TOR38A00",
        "Serial" : "85T0A1UVFHSC",
        "Size" : "278.88 GB",
        "Version" : "Unknown"
}
Detected:
{
        "Manufacturer" : "Unknown",
        "Media Type" : "Unknown",
        "Model" : "Unknown",
        "Name" : "Unknown",
        "Part Number" : "Unknown",
        "Serial" : "Unknown",
        "Size" : "Unknown",
        "Version" : "Unknown"
}
-----------------------------------------------------------------
-----
Overall HardDrive check Status: Mismatch
-----------------------------------------------------------------
```

How to check SCV logs using WinPE

1. After running SCV in WinPE, the logs created will be stored under X:\Dell\scv\scvapp\logs
2. To check logs, navigate to the logs folder and use the command notepad SCVLog_%service-tag%_%timestamp%.log

```
X:\Dell\scv>cd scvapp

X:\Dell\scv\scvapp>cd logs

X:\Dell\scv\scvapp\logs>dir
 Volume in drive X is Boot
 Volume Serial Number is D60A-0DC2

 Directory of X:\Dell\scv\scvapp\logs

09/16/2020  10:09 AM    <DIR>          .
09/16/2020  10:09 AM    <DIR>          ..
09/16/2020  10:10 AM               506 SCVLog_FRH89V2_2020_09_16_10_09_37.log
               1 File(s)            506 bytes
               2 Dir(s)     520,667,136 bytes free

X:\Dell\scv\scvapp\logs>notepad SCVLog_FRH89V2_2020_09_16_10_09_37.log
```

Secured Component Verification on Linux

This section provides information for the following:
Topics:

- Running SCV on Linux
- How to check SCV logs using Linux

Running SCV on Linux

1. Download the iDRAC tools from the Drivers & downloads page for your system at
   https://www.dell.com/support.
2. In the terminal, navigate to the directory where iDRAC Tools file is downloaded and unzip the file using the command tar

```
-zxvf DellEMC-iDRACTools-Web-LX-X.X.X-XXXX_XXX.tar.gz
        [root@localhost ~]# tar -xvf DellEMC-iDRACTools-Web-LX-9.5.1-4135.tar.gz
        iDRACTools/
        iDRACTools/license.txt
        iDRACTools/ipmitool/
        iDRACTools/ipmitool/RHEL7_x86_64/
        iDRACTools/ipmitool/RHEL7_x86_64/ipmitool-1.8.18-99.dell.4135.16999.el7.x86_64.rpm
        iDRACTools/readme.txt
        iDRACTools/racadm/
        iDRACTools/racadm/uninstall_racadm.sh
        iDRACTools/racadm/install_racadm.sh
        iDRACTools/racadm/RHEL7/
        iDRACTools/racadm/RHEL7/x86_64/
        iDRACTools/racadm/RHEL7/x86_64/srvadmin-idracadm7-9.5.1-4135.16999.el7.x86_64.rpm
        iDRACTools/racadm/RHEL7/x86_64/srvadmin-argtable2-9.5.1-4135.16999.el7.x86_64.rpm
        iDRACTools/racadm/RHEL7/x86_64/srvadmin-hapi-9.5.1-4135.16999.el7.x86_64.rpm
        iDRACTools/scv/
        iDRACTools/scv/install_scv.sh
        iDRACTools/scv/RHEL7/
        iDRACTools/scv/RHEL7/x86_64/
        iDRACTools/scv/RHEL7/x86_64/scv-9.5.1-4135.16999.el7.x86_64.rpm
        iDRACTools/scv/RHEL7/x86_64/tpm2-tss-1.4.0-3.el7.x86_64.rpm
        iDRACTools/scv/RHEL7/x86_64/tpm2-abrmd-1.1.0-11.el7.x86_64.rpm
        iDRACTools/scv/RHEL7/x86_64/tpm2-tools-3.0.4-3.el7.x86_64.rpm
        iDRACTools/scv/uninstall_scv.sh
        iDRACTools/gpl.txt
```

3. Navigate to the directory iDRACTools/scv after the files have been extracted and execute the install_scv.sh script using the command sh install_scv.sh.

   NOTE: To uninstall SCV you can use the command sh uninstall_scv.sh to execute the uninstall_scv.sh script.

```
[root@localhost iDRACTools]# cd scv/
[root@localhost scv]# ls -lrt
total 8
-rwxrwSrwx. 1 root root  130 Sep 11 01:49 uninstall_scv.sh
drwxrwxrwx. 3 root root   20 Sep 11 01:49 RHEL7
-rwxrwSrwx. 1 root root 3071 Sep 11 01:49 install_scv.sh
[root@localhost scv]# sh install_scv.sh
warning: srvadmin-argtable2-9.5.1-4135.16999.el7.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID 34d8786f: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:srvadmin-hapi-9.5.1-4135.16999.el#################################### [ 33%]
   2:srvadmin-argtable2-9.5.1-4135.169################################### [ 67%]
   3:srvadmin-idracadm7-9.5.1-4135.169################################### [100%]
   ***********************************************************
   After the install process completes, you may need
   to logout and then login again to reset the PATH
   variable to access the RACADM CLI utilities

   ***********************************************************
```

4. Once SCV is installed, run the command scv validate System Inventory to start the validation process.

   NOTE: Use the command scv help to get more information on SCV and how to run it.

5. Once the system runs the SCV application successfully, it should give the result Validating System Inventory: Match

```
[root@localhost scv]# scv validateSystemInventory
Downloading SCV Certificate from iDRAC: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "RTSTC21" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_RTSTC21_2020_09_15_05_55_28.log
--------------------------------------------------------------------
```

6. If the result shows as Validating System Inventory: Mismatch it will specify which component has mismatched under Mismatch Inventory Summary. For more help contact Technical Support.

```
[root@localhost ~]# scv validateSystemInventory
Downloading SCV Certificate from iDRAC: Passed
Validating Signature and Root of Trust: Passed
Validating Proof of Possession: Passed
Verification App supports Certificate profile version: Passed
Collecting System Inventory: Passed
Validating System Service Tag "BLSTC25" matches Certificate: Match
Validating System Inventory: Mismatch
--------------------------------------------------------------------
Mismatch Inventory Summary
--------------------------------------------------------------------
HardDrive 2: Mismatch

        HardDrive 2: Mismatch
        Expected:
        {
              "Manufacturer" : "TOSHIBA",
              "Media Type" : "HDD",
              "Model" : "AL13SXB30EN",
              "Name" : "Physical Disk 0:1:2",
              "Part Number" : "PH00RVDT7557158TOR38A00",
              "Serial" : "85T0A1UVFHSC",
              "Size" : "278.88 GB",
              "Version" : "Unknown"
        }
        Detected:
        {
              "Manufacturer" : "Unknown",
              "Media Type" : "Unknown",
              "Model" : "Unknown",
              "Name" : "Unknown",
              "Part Number" : "Unknown",
              "Serial" : "Unknown",
              "Size" : "Unknown",
              "Version" : "Unknown"
        }
        --------------------------------------------------------------
        -----
        Overall HardDrive check Status: Mismatch
        --------------------------------------------------------------
        -----
```

How to check SCV logs using Linux

1. After running SCV in Linux, the logs created will be stored under scvapp\logs

2. To check logs. navigate to the logs folder and use the command vi SCVlog_&service-tag$_8timestamp8.10g

   [root@localhost scv)‡ vi ./scvapp/logs/SCVlog_RTSTC21_2020_09_15_05_55_28.10g

Return Codes

This section provides information on return codes related to Secured Component Verification.
Note: The above information is derived from the user manual of the Dell EMC Secured Component Verification Reference Guide for Servers. Please refer to the complete user manual for detailed instructions and additional information.

Following is the list of the return codes for SCV operation:
SCV return codes

Code	Description
0	All operations were successful and inventory matched.
1	Generic failure.
2	Another instance of SCV operation is running.
3	Permission is not appropriate for the user.
4	SCV operation failed to start, dependencies not met.
5	Certificate download failed from iDRAC.
6	Validating signature and Root of Trust Failed.
7	Validating proof of possession failed.
8	Profile not supported for the version details as specified in the certificate.
9	Profile, Subschema/utilities are tampered, profile signature mismatch.
10	Unable to collect data due to a utility failure.
11	Mismatch in the inventory.

Getting help

Topics:

- Contacting Dell EMC
- Support documents and resources
- Documentation feedback

Contacting Dell EMC

Dell EMC provides several online and telephone based support and service options. If you do not have an active internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell EMC product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical assistance, or customer service issues:

Steps

1. Go to **www.dell.com/support/home**.
2. Select your country from the drop-down menu on the lower right corner of the page.
3. For customized support:
    - Enter your system Service Tag in the Enter your Service Tag field.
    - Click Submit.

      The support page that lists the various support categories is displayed.
4. For general support:
    - Select your product category.
    - Select your product segment.
    - Select your product.

      The support page that lists the various support categories is displayed.

5. For contact details of Dell EMC Global Technical Support:
    - Click Global Technical Support.
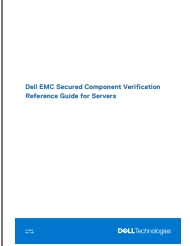   - Enter your system Service Tag in the Enter your Service Tag field on the Contact Us webpage.

Support documents and resources

- **The iDRAC support home page provides access to product documents, technical white papers, how-to videos, and more:**
    - **www.dell.com/support/idrac**
- **iDRAC User Guide and other manuals:**
    - **www.dell.com/idracmanuals**
- **Dell Technical Support:**
    - **www.dell.com/support**

Documentation feedback
You can rate the documentation or write your feedback on any of our Dell EMC documentation pages and click Send Feedback to send your feedback.

Documents / Resources

Dell EMC Secured Component Verification Reference Guide for Servers DELLTechnologies	**Dell EMC EMC Secured Component Verification Reference** [pdf] User Guide EMC Secured Component Verification Reference, EMC, Secured Component Verification Reference, Component Verification Reference, Verification Reference

References

- **Download and install the Windows ADK | Microsoft Learn**
- **Support | Dell US**
- **Support | Dell US**
- **Contact Technical Support | Dell US**