

# **Dell Secured Component Verification Version 1.5,1.5.1,1.6,1.7,1.8, 1.9, 1.91.0 and 1.92.0**

## Reference Guide for Servers and Chassis

## 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.

<b>Chapter 1: Overview.....</b>	<b>5</b>
New features added.....	5
SCV 1.92.0.....	5
SCV 1.91.0.....	5
SCV 1.9.....	5
SCV 1.8.....	5
SCV 1.7.....	6
SCV 1.6.....	6
SCV 1.5.1.....	6
SCV 1.5.....	6
Secured Component Verification.....	6
System Requirements.....	7
Components Supported.....	7
URIs Supported.....	8
<b>Chapter 2: Secured Component Verification on WinPE.....</b>	<b>9</b>
Creating an ISO image to run SCV using WinPE.....	9
Adding SCV to Custom ISO Image.....	10
Running SCV on WinPE.....	10
How to check SCV logs using WinPE.....	13
<b>Chapter 3: Secured Component Verification on Linux.....</b>	<b>14</b>
Running SCV on Linux.....	14
How to check SCV logs using Linux.....	17
<b>Chapter 4: Secured Component Verification on Windows Server 2019 and 2022.....</b>	<b>18</b>
Installing SCVApp on Windows Server 2019 and 2022.....	18
Running SCV on Windows Server 2019 and 2022.....	21
<b>Chapter 5: Running Secured Component Verification (SCV) remotely.....</b>	<b>26</b>
Running SCV remotely on Windows Server 2019 and 2022.....	26
Running SCV remotely on WinPE.....	26
Running SCV remotely on Linux.....	27
<b>Chapter 6: SCV Command Details.....</b>	<b>28</b>
Get information on how to run SCV.....	28
Get information about scv validatesysteminventory command.....	28
Connecting remotely to a management console and validating inventory.....	29
Connecting remotely to a management console with a specific port and validating inventory.....	30
Ensuring component location match and validating inventory.....	30
Get SCV Version.....	31
Displaying certificate identifier value on console or redirecting it to a file.....	31
<b>Chapter 7: SCVApp MARS feature.....</b>	<b>33</b>

<b>Chapter 8: SPDM feature.....</b>	<b>35</b>
<b>Chapter 9: SCV Root CA Certificate.....</b>	<b>36</b>
<b>Chapter 10: Return Codes.....</b>	<b>37</b>
<b>Chapter 11: Getting help.....</b>	<b>38</b>
Contacting Dell.....	38
Support documents and resources.....	38
Documentation feedback.....	38

# Overview

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

## Topics:

- [New features added](#)
- [Secured Component Verification](#)
- [System Requirements](#)
- [Components Supported](#)
- [URLs Supported](#)

## New features added

This section provides the list of new features added in the following releases:

- [SCV 1.92.0](#)
- [SCV 1.91.0](#)
- [SCV 1.9](#)
- [SCV 1.8](#)
- [SCV 1.7](#)
- [SCV 1.6](#)
- [SCV 1.5.1](#)
- [SCV 1.5](#)

### SCV 1.92.0


The following features were added or updated in this release:

- Support for debug option for `scv extractcert` command.

### SCV 1.91.0

The following features were added or updated in this release:


- Support for MARS Feature.
- Added SPDM support for NIC Emulex Card and PERC 12.

 **NOTE:** To get the supported systems list for this release, see the release notes.

### SCV 1.9

Following features were added or updated in this release:

- Added support for new PowerEdge servers.

 **NOTE:** To get the supported systems list for this release, see the release notes.

### SCV 1.8

Following features were added or updated in this release:

- Support for new profile for cloud platforms that do not share hard drives.

- Support for `extractcert` command.

## SCV 1.7

Following features were added or updated in this release:

- Support for SLES 15 SP4.
- Support for 16th generation PowerEdge servers.

## SCV 1.6

Following features were added or updated in this release:

- Support for Red Hat Enterprise Linux 9.0.

## SCV 1.5.1

Following features were added or updated in this release:

- Support for PowerEdge cloud servers.
- Support for PowerEdge Modular servers and Chassis (MX series).

## SCV 1.5

Following features were added or updated in this release:

- Support for SCVTools.
- Support for Red Hat Enterprise Linux 8.x.
- Support for SCVApp for Windows Server 2019 and 2022.

# 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, a certificate containing the unique system component IDs is generated during the factory assembly process. This certificate is signed in the Dell factory and is stored in the system, 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 matches 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. Current implementation supports direct ship customers and does not include VAR or Part Replacement scenarios.

SCV Application performs the following functions:

- Downloads the SCV Certificate that is stored in the system through Dell Technology APIs and verifies the SCV certificate and issuer.
- Validates the SCV private key that is paired to the SCV public key in the SCV certificate.
- Collects the current inventory of the system.

 **NOTE:** For the list of system components supported, see the section [Components Supported](#).

- Compares current system inventory against the inventory in the SCV certificate.
- Any modification of the components that are captured in the certificate will be identified as a "Mismatch".

### Notes:

- SCV application can be launched directly from the iDRAC GUI version 7.10.30.00 and later, but it is recommended to validate your components using the application for an optimal security validation experience.
- 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 supports TPM version 2.0.
- Ensure that you run the SCV application before mapping any storage devices to the system.
- In modular systems, ensure that the FlexAddress is disabled before running the SCV application.

- If internal and iDRAC USB ports are disabled, the SCV validation fails.
- 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 reports incorrect data in the SCV output.
- SCV requires USB NIC communication for in-band validation. Do not disable the USB NIC while running the SCV operation.
- In SCV 1.5 with 1.0 certificate, one of the TPM component(ECC) entry reports as 'Match' with expected details as 'Unknown', while the detected details display all the information. This is an expected behavior because 1.0 certificate does not include ECC information.

## System Requirements

**Table 1. System requirements for running SCV**

Category	Requirement
Supported Operating Systems	WinPE 10.x, Red Hat Enterprise Linux 9.0, Red Hat Enterprise Linux 8.6, Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 15 SP4, Windows Server 2019, and Windows Server 2022.
SCV Tools	SCV 1.5,1.5.1,1.6,1.7,1.8, 1.9,1.91.0 or 1.92.0
Firmware versions	<ul style="list-style-type: none"> <li>• iDRAC 5.10.30.00 and later versions</li> <li>• OME-M 2.00.00 and later versions</li> <li>• PowerEdge BIOS 2.14.2 and later versions</li> </ul>
Licenses required	Secured Component Verification License

**NOTE:** To get the supported systems list for an SCV version, see the Supported Systems section in the release notes.

**NOTE:** Red Hat Enterprise Linux 7.x is not supported by SCV 1.6 and later versions.

**NOTE:** In SCV version 1.5, TPM mismatch is displayed while validating components on a server with an older iDRAC and BIOS firmware. Before performing SCV, ensure that the iDRAC firmware is upgraded to version 5.10.30.00, and the BIOS firmware is upgraded to version 2.14.2 or any later versions.

## Components Supported

**Table 2. Supported components for Rack, Tower and Cloud platforms**

Components supported for Rack, Tower and Cloud servers
Baseboard
Processor
Memory
Power supply
Hard drive
Network card
iDRAC
TPM
System Information
PCIe add-on cards

**Table 3. Supported components for Modular Chassis**

Components supported for Modular Chassis
Enclosure Controller
Fan
Open Manage Enterprise Modular
ChassisRCP
PowerSupply
IOModule
M2Drive

**NOTE:** Direct attached NVMe PCIe SSD will not be shown in PCIe slot. Check the HDD list to get the PCIe SSD.

**NOTE:** When there are no devices present for a component, the SCV inventory displays one 'Unknown' entry .

**NOTE:** The SCV inventory displays details only for those devices of a component that are present in the system.

## URIs Supported

SCV supports Application Programming Interfaces (API) to access information using an API client. For more information about using APIs, see the iDRAC9 Redfish API guide at [developer.dell.com](https://developer.dell.com). Following is the list of URIs and the supported methods:

- Download SCV certificates**

```
GET: /dtapi/rest/v1/x509-certificates
```

**Example response**

```
{
  "certificate": "<SCV_CERT_CONTENT>",
  "certificate_format": "PEM",
  "id": "scv_factory"
}
```

- Download SCV Inventory**

```
GET : /dtapi/rest/v1/scvs/0
```

**Example response on iDRAC**

```
{
  "description": "Dell Platform Certificate Profile for PowerEdge Servers",
  "hardware_inventory": [ <ARRAY OF COMPONENT DETAILS> ],
  "profile_version": "<Profile Version Number>",
  "profile_name": "PowerEdge"
}
```

**Example response on MX systems**

```
{
  "description": " Dell Platform Certificate Profile for PowerEdge Modular
Infrastructure",
  "hardware_inventory": [ <ARRAY OF COMPONENT DETAILS> ],
  "profile_version": "<Profile Version Number>",
  "profile_name": "PowerEdge MX"
}
```



# Secured Component Verification on WinPE

This section provides information for the following:

## Topics:

- [Creating an ISO image to run SCV using WinPE](#)
- [Adding SCV to Custom 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 SCVTools from the **Drivers & downloads** page at <https://www.dell.com/support>.
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 SCVTools 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.
  - NOTE:** Before running the WinPE batch file, ensure that you add the patch from <https://support.microsoft.com/en-us/help/5017380>. To add the patch, download the latest Servicing Stack Update (SSU) for the operating system with the Latest Cumulative Update (LCU), to the path mentioned in the batch file and rename the SSU file as `ssu-19041.1704-x64.msu` and LCU file as `windows10.0-kb5018410-x64.msu`.

```
C:\Users\User_Name\Downloads\DellEMC-SCVTools-Web-WinPE-1.5-004>
C:\Users\User_Name\Downloads\DellEMC-SCVTools-Web-WinPE-1.5-004>WINPE10.x_driverinst.bat
-----
~~1(WINPE10.x_driverinst.bat)-Checking the Paths
-----
~~2-Setting up a WinPE 10.x amd64 build environment
-----
=====
Creating Windows PE customization working directory
C:\Users\User_Name\Downloads\DellEMC-SCVTools-Web-WinPE-1.5-004\WINPE10_x_20220314_154302
```

**Figure 1. Running the batch file through command prompt**

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

```

-----
~~~9-Creating bootable ISO-CD image
-----
OSCDIMG 2.56 CD-ROM and DVD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2012. All rights reserved.
Licensed only for producing Microsoft authorized content.

Scanning source tree
Scanning source tree complete (189 files in 138 directories)

Computing directory information complete

Image file is 582877184 bytes (before optimization)

Writing 189 files in 138 directories to C:\Users\User_Name\Downloads\DellEMC-SCVTools-Web-WinPE-1.5-004\WINPE10_x_20220314_154302\DellEMC-SCV-Web-WinPE10_x_amd64-2.0.iso
100% complete

Storage optimization saved 1 files, 34816 bytes (0% of image)

After optimization, image file is 583489536 bytes
Space saved because of embedding, sparseness or optimization = 34816

Done.
-----
~~~10(WinPE10_x_driverinst.bat)-DONE.
-----
C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools>

```

**Figure 2. 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 a custom ISO image:

1. Download the SCVTools from the **Drivers & downloads** page at <https://www.dell.com/support>.
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 SCVTools 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:
  - a. **scv** to X:\Dell
  - b. **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;`
6. SCV can now be used to run validation.

## 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.
  - NOTE:** While running SCV on the host, ensure that the USB NIC IP Address in iDRAC is set to the default IP Address. Also, ensure that the first three octets of the IP address are '169.254.1'.
  - NOTE:** After getting 'Ready' state in `racadm getremoteservicesstatus` output, ensure that you wait for about 120 seconds before running the scv commands.
  - NOTE:** An error 'Collecting System Inventory: Fail' may be displayed while performing the `scv validatesysteminventory` command with `-d` option, if the directory path length exceeds 150 characters.

```

Administrator: VistaPE+***** Debug Window - 1***** - scv validatesysteminventory
Microsoft Windows [Version 10.0.19041.610]
(c) 2020 Microsoft Corporation. All rights reserved.

X:\windows\system32>cd ..\..\
X:\>cd dell\scv
X:\Dell\scv>dir
Volume in drive X is Boot
Volume Serial Number is D60A-0DC2

Directory of X:\Dell\scv

02/21/2022  02:12 PM    <DIR>          .
02/21/2022  02:12 PM    <DIR>          ..
03/04/2022  08:06 AM             4,555,264  scv.exe
02/21/2022  02:12 PM    <DIR>          scvapp
03/10/2022  03:52 AM             326 ismrfutil_rel.log
           2 File(s)          4,555,590 bytes
           3 Dir(s)       1,035,620,352 bytes free

X:\Dell\scv>scv validatesysteminventory

```

**Figure 3. Running the validation command**

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

```

X:\Dell\scv>scv validatesysteminventory
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----

Added Components Summary:
      HardDrive      23E0A08BTC88   Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75 PSU.Slot.2

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_03_17_46.txt

```

**Figure 4. Running the validation command and result is successful**

- If the result shows as Validating System Inventory: Mismatch it will specify which component has mismatched under Mismatch Inventory Summary.

```

-----
System Information
-----
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.
-----

Command Information
-----
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Not Enforced
-----

Command Execution Status
-----
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possion : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success
-----

Component Inventory Comparison Results
-----
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : MisMatch
OverAll Comparison Result : MisMatch
-----

Inventory MisMatch Summary
-----
Added Components Summary:
      HardDrive      23E0A08BTC88      Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75      PSU.Slot.2
-----

Added Components
-----
{
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000A0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A02",
      "Location": "PSU.Slot.2",
      "Manufacturer": "DELL",
      "Model": "PWR SPLY,1100W,RDNT,LTON",
      "SerialNumber": "CNL0D0034I2C75"
    }
  ]
}
-----

Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00030003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A01",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0NPR40",
      "SerialNumber": "CN1VC0036M0426"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.7:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A086TC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.3:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A08ETC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation ",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.2:Enclosure.Internal.0-1",
      "Manufacturer":
    }
  ]
}

```

Figure 5. Mismatched component expected and detected details

## How to check SCV logs using WinPE

1. After running SCV in WinPE, the logs that are 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
```

Figure 6. Checking logs using WinPE

# 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 SCVTools from the Drivers & downloads page at <https://www.dell.com/support>.
2. In the terminal, navigate to the directory where SCV package is downloaded and unzip the file using the command `tar -zxvf DelleMC-SCV-Web-LX-X.X.X-XXXX_XXX.tar.gz`

```
[root@auvcetilleml1 Downloads]# tar -xvf DelleMC-SCV-Web-LX-2000-75.tar.gz
COPYRIGHT.txt
license.txt
SCVTools/
SCVTools/RPMS/
SCVTools/RPMS/supportRPMS/
SCVTools/RPMS/supportRPMS/srvadmin/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/x86_64/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL7/x86_64/scv-2.0.0-136.el7.x86_64.rpm
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/x86_64/
SCVTools/RPMS/supportRPMS/srvadmin/RHEL8/x86_64/scv-2.0.0-136.el8.x86_64.rpm
SCVTools/install_scv.sh
SCVTools/uninstall_scv.sh
SCVTools/readme.txt
```

**Figure 7. Extracting SCV tools on Linux**

3. Navigate to the directory `SCVTools` 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@auvcetilleml1 Downloads]# ls
COPYRIGHT.txt  DelleMC-SCV-Web-LX-2000-75.tar.gz  ismrfutil-el8-v0  license.txt  SCVTools
[root@auvcetilleml1 Downloads]# cd SCVTools/
[root@auvcetilleml1 SCVTools]# ls
install_scv.sh  readme.txt  RPMS  uninstall_scv.sh
[root@auvcetilleml1 SCVTools]# sh uninstall_scv.sh
[root@auvcetilleml1 SCVTools]# sh install_scv.sh
warning: scv-2.0.0-136.el8.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID 34d8786f: NOKEY
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
 1:scv-2.0.0-136.el8 ##### [100%]
[root@auvcetilleml1 SCVTools]#
```

**Figure 8. Executing the SCV installation script**

4. Once SCV is installed, run the command `scv validateSystemInventory` to start the validation process.
  - NOTE:** While running SCV on the host, ensure that the USB NIC IP Address in iDRAC is set to the default IP Address. Also, ensure that the first three octets of the IP address are '169.254.1'.
  - NOTE:** Use the command `scv help` to get more information on SCV and how to run it.

**NOTE:** After getting 'Ready' state in `racadm getremoteservicesstatus` output, ensure that you wait for about 120 seconds before running the `scv` commands.

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

```
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag CL04506 with System Inventory Service Tag: Match
Inventory Comparison Result : Match
```

Refer Detailed Report File at : `./scvapp/out/SCV_CommandExecutionReport_CL04506_2023_11_28_10_30_58.txt`

**Figure 9. Running the validation command and result is successful**

6. If the result shows as `Validating System Inventory: Mismatch` it will specify which component has mismatched under `Mismatch Inventory Summary`.

```

-----
System Information
-----
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.
-----
Command Information
-----
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Not Enforced
-----
Command Execution Status
-----
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possion : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success
-----
Component Inventory Comparison Results
-----
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : MisMatch
OverAll Comparison Result : MisMatch
-----
Inventory MisMatch Summary
-----
Added Components Summary:
      HardDrive      23E0A08BTC88      Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75      PSU.Slot.2
-----
Added Components
-----
{
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000A0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A02",
      "Location": "PSU.Slot.2",
      "Manufacturer": "DELL",
      "Model": "PWR_SPLY,1100W,RDNT,LTON",
      "SerialNumber": "CNL0D0034I2C75"
    }
  ]
}
-----
Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00030003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A01",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0NPR40",
      "SerialNumber": "CNIVC0036M0426"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.7:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A086TC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.3:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A08ETC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.5:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA Corporation",
      "Model": "Unknown",
      "SerialNumber": "23E0A08BTC88"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.2:Enclosure.Internal.0-1",
      "Manufacturer": "KIOXIA"
    }
  ]
}

```

Figure 10. Mismatched component expected and detected details



## How to check SCV logs using Linux

1. After running SCV in Linux, the logs created are stored under `scvapp\logs`
2. To check logs, navigate to the logs folder and use the command `vi SCVLog_%service-tag%_%timestamp%.log`  

```
[root@localhost scv]# vi ./scvapp/logs/SCVLog_RTSTC21_2020_09_15_05_55_28.log
```

**Figure 11. Checking logs in Linux**

# Secured Component Verification on Windows Server 2019 and 2022

This section provides information about installing and running SCVApp:

**Topics:**

- [Installing SCVApp on Windows Server 2019 and 2022](#)
- [Running SCV on Windows Server 2019 and 2022](#)

## Installing SCVApp on Windows Server 2019 and 2022

To install SCVApp on Windows Server 2019 and 2022:

1. Download the SCV installer from the **Drivers & downloads** page at <https://www.dell.com/support>.
2. Extract the SCV installer.

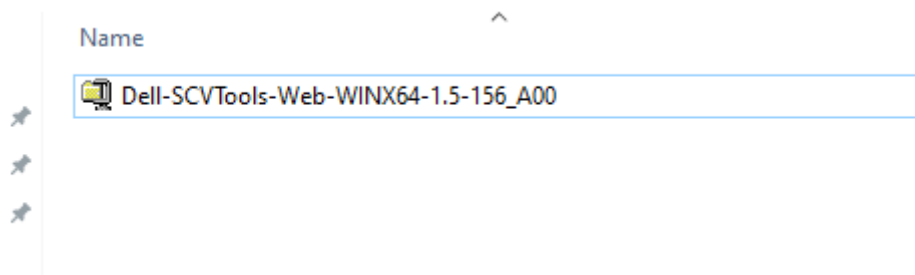


Figure 12. SCV installer zip file

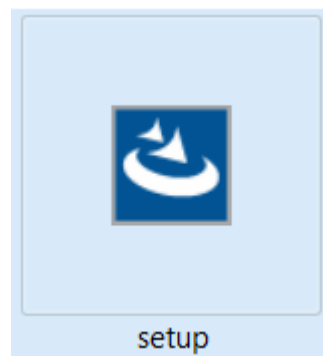
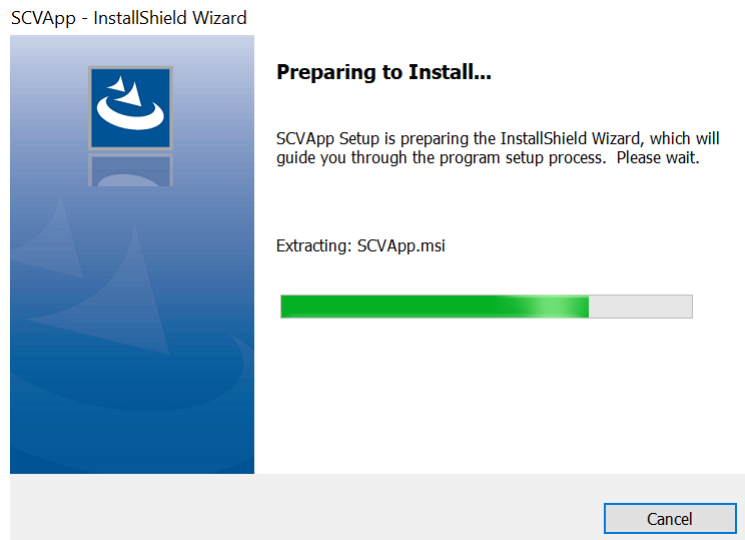


Figure 13. SCV installer

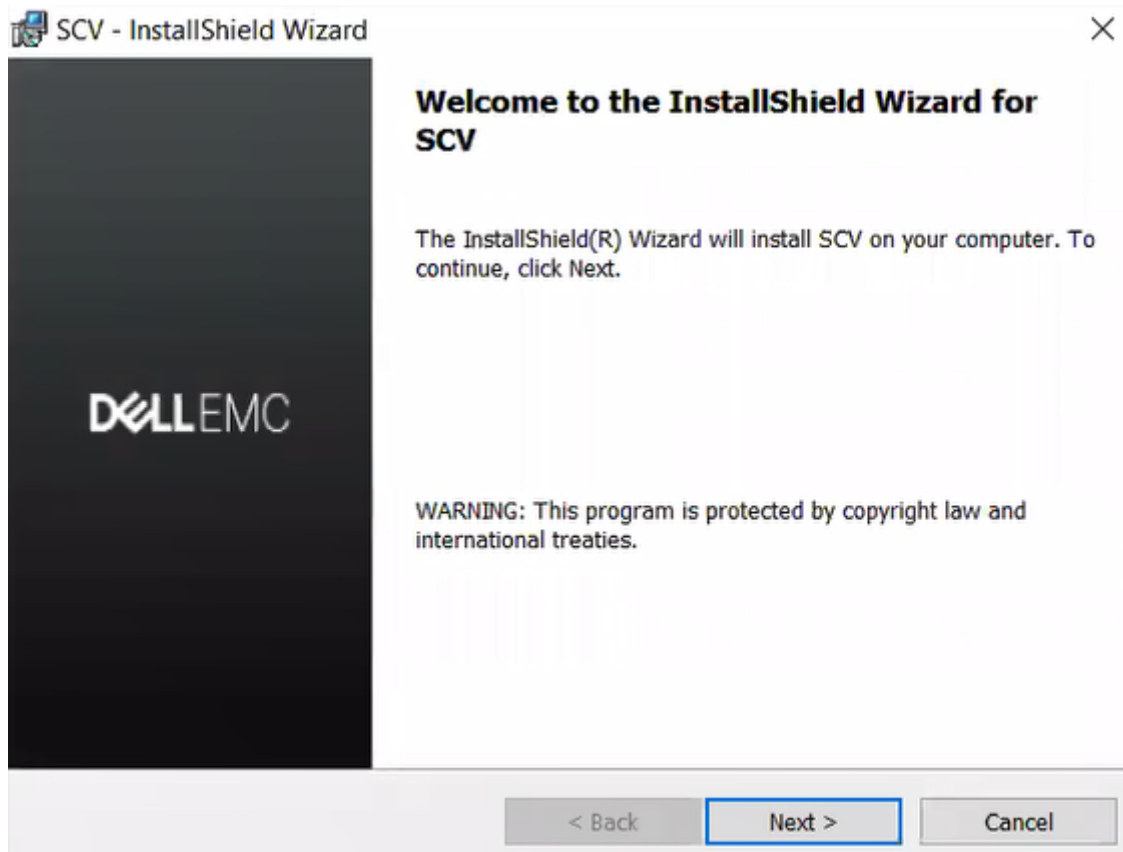
3. Run the application to start the InstallShield Wizard.



**Figure 14. Running SCV installer**

4. Click **Next** and accept the License Agreement.

**NOTE:** While installing the SCV application, ensure that you change the installation file path location to " C: \ProgramFiles\Dell\SCVTools" in the installation wizard.



**Figure 15. InstallShield Wizard for SCVApp**

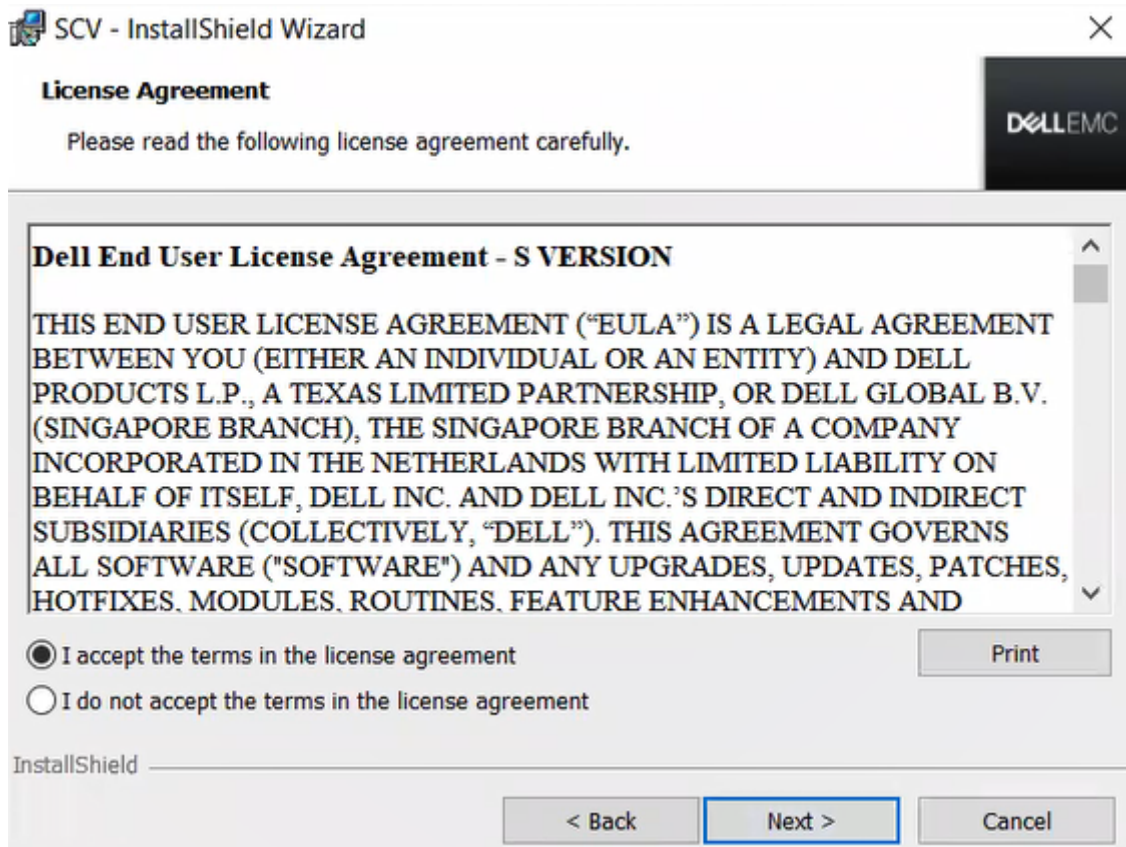


Figure 16. License Agreement for SCVApp

5. Click **Install** to begin the installation.

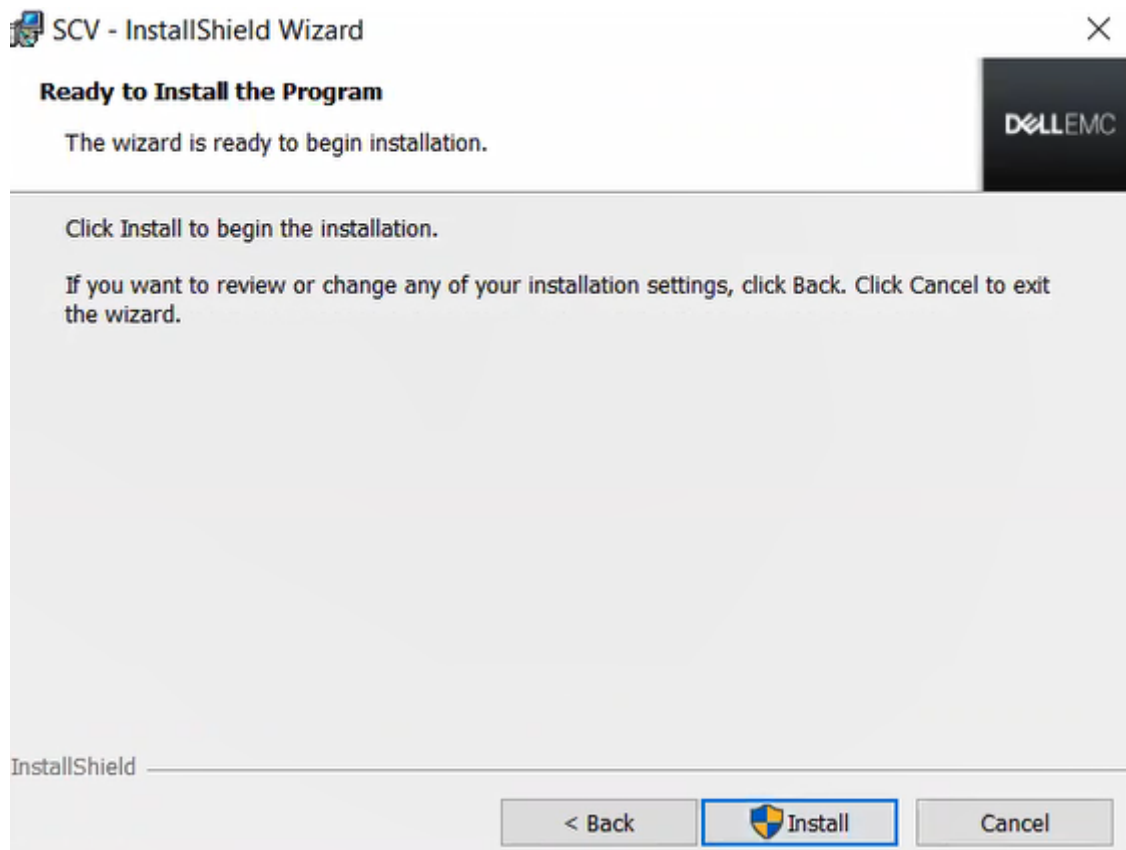
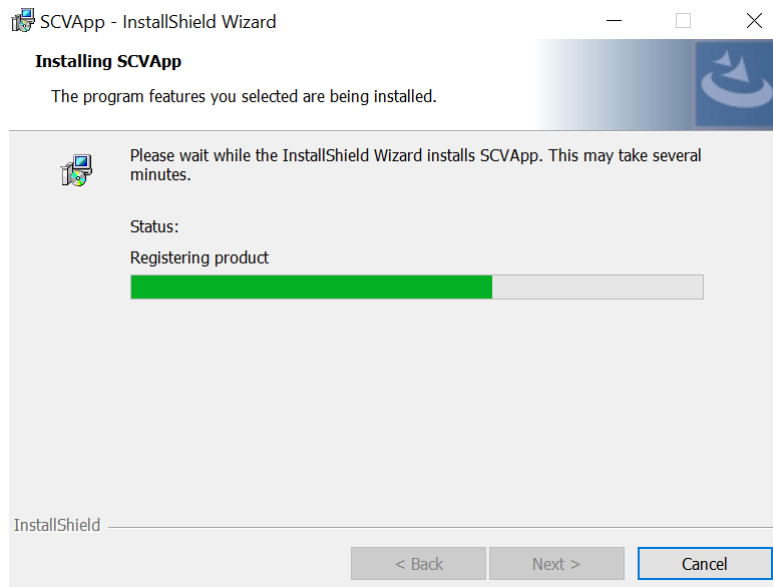
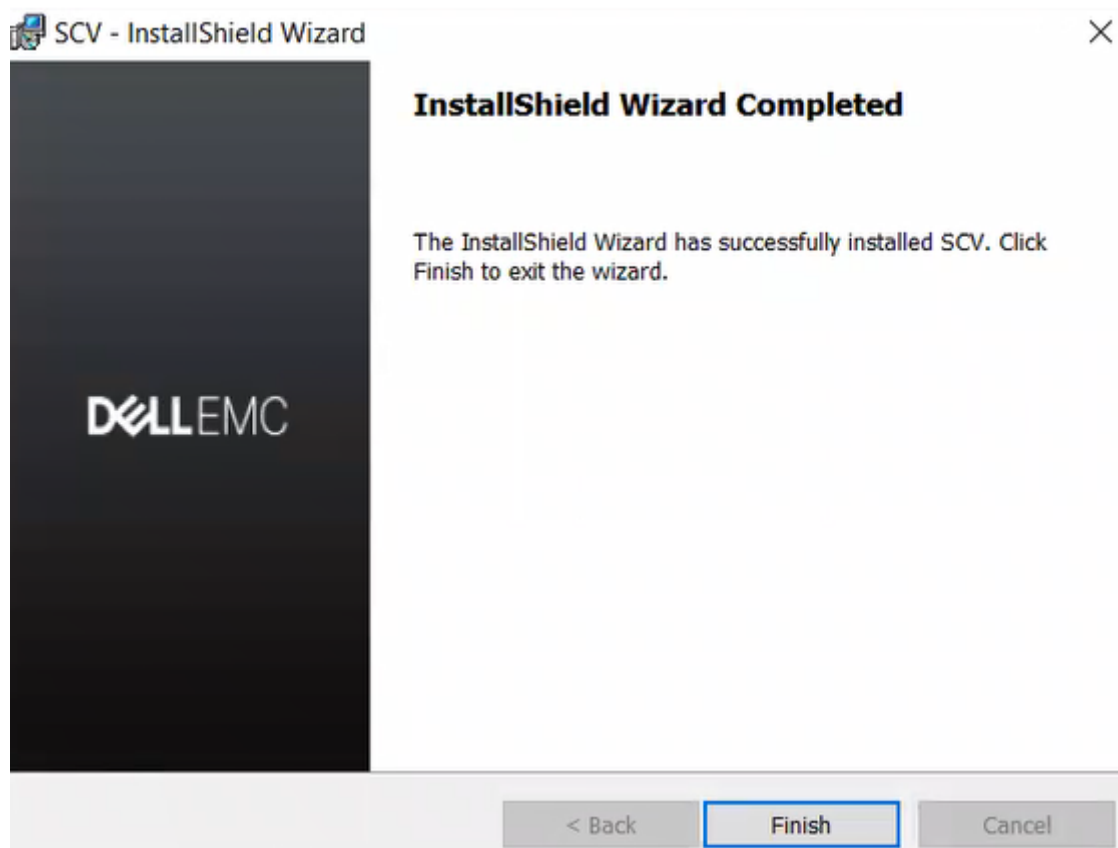


Figure 17. Ready to install SCVApp



**Figure 18. Installing SCVApp**

6. After the installation is complete, click **Finish** to exit the InstallShield Wizard.



**Figure 19. SCVApp installation complete**

## Running SCV on Windows Server 2019 and 2022

1. Open the command prompt and navigate to the `SCVTools` directory/folder.
2. Run the `scv validatesysteminventory` command to start the validation process.
  - NOTE:** While running SCV on the host, ensure that the USB NIC IP Address in iDRAC is set to the default IP Address. Also, ensure that the first three octets of the IP address are '169.254.1.'

- ① **NOTE:** 'Unable to create the scvapp directory : Failed' error is displayed when the `scv validatesysteminventory` command is performed on any directory other than the directory that hosts the application.
- ① **NOTE:** 'Downloading SCV Factory Certificate: Fail' error is displayed when `scv validatesysteminventory` command is performed while the host firewall is enabled. To run the command successfully, ensure that you create an outbound rule for I.P. address 169.254.1.1.
- ① **NOTE:** After getting the Overall Status as 'Ready' in `racadm getremoteservicesstatus` output, ensure that you wait for about 120 seconds before running the `scv` commands.
- ① **NOTE:** An error 'Collecting System Inventory: Fail' may be displayed while performing the `scv validatesysteminventory` command with `-d` option, if the directory path length exceeds 150 characters.

```
X:\Dell\scv>scv validatesysteminventory
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Added Components Summary:
      HardDrive      23E0A08BTC88   Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75 PSU.Slot.2

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_03_17_46.txt
```

**Figure 20. Running the validation command and result is successful**

3. If the result is `Validating System Inventory: Mismatch`, it will specify which component has mismatched under `Mismatch Inventory Summary`.

```
C:\Users\Anirban_Dasgupta>scv.exe ValidateSystemInventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8MFZ3 with System Inventory Service Tag: Match
Inventory Comparision Result : MisMatch

-----
Inventory MisMatch Summary
-----

Added Components Summary:
    PowerSupply    CNL00003412C75    PSU.Slot.2
    HardDrive      23E0A088TC88     Disk.Bay.5:Enclosure.Internal.0-1

Refer Detailed Report File at : C:\Users\Anirban_Dasgupta\scvapp\out\SCV_CommandExecutionReport_FL8MFZ3_2023_12_24_03_43_10.txt
```

Figure 21. Validation and result is unsuccessful

```

System Information
-----
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.
-----

Command Information
-----
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Enforced
-----

Command Execution Status
-----
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possession : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success
-----

Component Inventory Comparison Results
-----
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : Match
OverAll Comparison Result : Match
-----

Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00030003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "X31",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0M1CC5",
      "SerialNumber": "CN1VC0026T0065"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "Location": "Disk Bay:0:Enclosure.Internal.0-1",
      "Manufacturer": "Samsung Electronics Co Ltd",
      "Model": "Unknown",
      "SerialNumber": "S6CSNA0RA02805"
    }
  ],
  "Memory": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060001",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "A1",
      "Manufacturer": "Micron Technology",
      "Model": "DDR5 DIMM",
      "SerialNumber": "3169944A"
    }
  ],
  "Network": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.2-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:17"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.1-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:16"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000a0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A04",
      "Location": "PSU.Slot.1",
      "Manufacturer": "DELL",
      "Model": "PWR_SPLY,800W,RDNT,LTGN",
      "SerialNumber": "CNL0D0024635D4"
    }
  ],
  "Processor": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00010002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Intel(R) Xeon(R) Platinum 8452Y",
      "Location": "CPU1",
      "Manufacturer": "Intel",
      "Model": "B3",
      "SerialNumber": "1BF0F11FD1C1E363"
    }
  ],
  "iDRAC": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060003",
      "CertificateIdentifier": "MIICVCCAfulAwIBAgIIAwAAAAAAE+QkYIKoZiZj0EAWIwdTELMAKGA1UEBHMCMQ04ETAPBgNVBAGMCFNoY5naGFpPjREw
    }
  ]
}

```

Figure 22. Mismatched component expected and detected details



```

-----
System Information
-----
ServiceTag: <Service Tag>
HostIP: <IP address>
PlatformModel: PowerEdge R660
Manufacturer: Dell Inc.
-----
Command Information
-----
Command : ValidateSystemInventory
Execution Mode : Remote
Enforce Order : Enforced
-----
Command Execution Status
-----
Download SCV Platform Certificate : Success
Validate SCV Platform Certificate Signature : Success
Validate SCV Platform Certificate Root Of Trust : Success
Validate SCV Platform Certificate Proof Of Possession : Success
Collect System Inventory : Success
Validate System Inventory : Success
SCV Application Support For System Inventory Profile : Supported
Validate Profile Data between SCV Platform Certificate and System Inventory : Success
Compare SCV Platform Certificate Against System Inventory : Success
-----
Component Inventory Comparison Results
-----
Service Tag Comparison Result : Match
Subject Alternate Name Comparison Result : Match
Inventory Comparison Result : Match
OverAll Comparison Result : Match
-----
Matched Components
-----
{
  "Baseboard": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090003",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "X31",
      "Location": "1",
      "Manufacturer": "Dell Inc.",
      "Model": "0M1CC5",
      "SerialNumber": "CNIVC0026T0065"
    }
  ],
  "HardDrive": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00070002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "Disk.Bay.0:Enclosure.Internal.0-1",
      "Manufacturer": "Samsung Electronics Co Ltd",
      "Model": "Unknown",
      "SerialNumber": "S6CSNA0RA02805"
    }
  ],
  "Memory": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060001",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "A1",
      "Manufacturer": "Micron Technology",
      "Model": "DDR5 DIMM",
      "SerialNumber": "3169944A"
    }
  ],
  "Network": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.2-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:17",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:17"
    },
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00090002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Unknown",
      "Location": "NIC.Embedded.1-1-1",
      "Manufacturer": "Broadcom",
      "Model": "Broadcom Gigabit Ethernet BCM5720 - EC:2A:72:33:06:16",
      "SerialNumber": "Unknown",
      "MacAddress": "EC:2A:72:33:06:16"
    }
  ],
  "PowerSupply": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x000a0002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "A04",
      "Location": "PSU.Slot.1",
      "Manufacturer": "DELL",
      "Model": "PWR SPLY,800W,RDNT,LTON",
      "SerialNumber": "CNL0D0024635D4"
    }
  ],
  "Processor": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00010002",
      "CertificateIdentifier": "Unknown",
      "HardwareVersionNumber": "Intel(R) Xeon(R) Platinum 8452Y",
      "Location": "CPU1",
      "Manufacturer": "Intel",
      "Model": "b3",
      "SerialNumber": "1BFCE11FD1C1E363"
    }
  ],
  "iDRAC": [
    {
      "ComponentRegistryOID": "2.23.133.18.3.1",
      "ComponentClass": "0x00060003",
      "CertificateIdentifier": "MIICVTCCAFugAwIBAgIIAwAAAAAxE+QwCYIKoZIzj0EAwIwdTFLMAKGA
      1UEBHQ0QxETAPBgNVBAMCFNoYw5uGfPmREwDwYDQQAHAhTa
    }
  ]
}

```

Figure 23. Mismatched component expected and detected details

# Running Secured Component Verification (SCV) remotely

This section provides information for the following:

## Topics:

- Running SCV remotely on Windows Server 2019 and 2022
- Running SCV remotely on WinPE
- Running SCV remotely on Linux

## Running SCV remotely on Windows Server 2019 and 2022

1. Open the command prompt and navigate to the `SCVTools` directory/folder.
2. Run the `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` command to start the validation process.

```
C:\Users\Anirban_Dasgupta>scv ValidateSystemInventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Added Components Summary:
      HardDrive      23E04888TC88      Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0003412C75    PSU.Slot.2

Refer Detailed Report File at : C:\Users\Anirban_Dasgupta\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_03_49_26.txt
```

Figure 24. Running the validation command remotely on Windows and result is successful

## Running SCV remotely on WinPE

1. Open the command prompt and go to the `SCVTools` directory/folder.
2. Run the `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` command to start the validation process.

```

X:\Dell\scv>scv validatesysteminventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag DL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : X:\Dell\scv\scvapp\out\SCV_CommandExecutionReport_DL8WFZ3_2024_01_24_22_33_43.txt

```

**Figure 25. Running the validation command remotely on WinPE and result is successful**

## Running SCV remotely on Linux

1. Open the command prompt and navigate to the SCVTools directory/folder.
2. Run the `scv validatesysteminventory -r <iDRAC IPv4/IPv6[] address> -i` command to start the validation process.

```

[root@localhost SCVTools]# scv validateSystemInventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag DL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Removed Components Summary:
      TPM      0096797170CFE773D5DA59  RSA
      TPM      00EAC1C8340E7E80FD0F77  ECC

Refer Detailed Report File at : /root/1.93/SCVTools/scvapp/out/SCV_CommandExecutionReport_DL8WFZ3_2024_01_24_09_06_27.txt

```

**Figure 26. Running the validation command remotely on Linux and result is successful**

## SCV Command Details

This section provides information on some additional scv commands.

### Topics:

- [Get information on how to run SCV](#)
- [Get information about scv validatesysteminventory command](#)
- [Connecting remotely to a management console and validating inventory](#)
- [Connecting remotely to a management console with a specific port and validating inventory](#)
- [Ensuring component location match and validating inventory](#)
- [Get SCV Version](#)
- [Displaying certificate identifier value on console or redirecting it to a file](#)

## Get information on how to run SCV

**Table 4. Get more information about SCV**

scv help	
<b>Description</b>	Use the following command to get more information about SCV and how to run it.
<b>Synopsis</b>	scv help

### Output

```
C:\>scv help
SCV -- Secured Component Verification
Usage: scv.exe help <subcommand> [options]...
List of supported subcommands:
- validatesysteminventory
- extractcert
- getcertinfo
- version
- mars
Note:
  This is the SCV Help Command
```

## Get information about scv validatesysteminventory command

**Table 5. Get more information about SCV validatesysteminventory command**

scv help validatesysteminventory	
<b>Description</b>	Use the following command to get more information about SCV validatesysteminventory command and how to run it.

**Table 5. Get more information about SCV validatesysteminventory command (continued)**

<b>scv help validatesysteminventory</b>	
<b>Synopsis</b>	scv help validatesysteminventory

**Output**

```
PS C:\> scv help validatesysteminventory
SCV -- Secured Component Verification

Usage: scv.exe validatesysteminventory [options]...

List of supported options:
-r, --remotep=<Remote Target IP>      Target System IP. Not required when SCV is running on Host OS.
-u, --username=<UserName>            Username for Authenticating to target system. Not required when SCV is running on Host OS.
-p, --password=<Password>           Password for Authenticating to target system. Not required when SCV is running on Host OS.
-i, --interactive                    Enable interactive command execution Mode. UserName and Password will be accepted interactively from the use
r
-d, --directory=<Directory Path>     Output directory path (MAX 207 Characters). If not specified, Current Working directory will be the output d
irectory.
-e, --enforceorder                  force component slot location comparision along with the serial number comparision.
-D, --debug                          Enable Debug log level

List of Example Commands:
scv.exe validatesysteminventory [ -r|--remotep -u|--username -p|--password ] [ -e|--enforceorder ] [ -d|--directory ] [ -D|--debug ]
scv.exe validatesysteminventory [ -r|--remotep -i|--interactive ] [ -e|--enforceorder ] [ -d|--directory ] [ -D|--debug ]

Note:
The detailed logs collected are available in: directory->scvapp->logs folder.
Steps Performed:
  Downloads SCV Factory certificate and Delta certificate(s)
  Validates Signature and Root of Trust
  Validates Proof of Possession
  Verifies application supported certificate profile version
  Validates System service Tag
  Collects and validates system inventory.
```

## Connecting remotely to a management console and validating inventory

**Table 6. Validating a specific inventory remotely**

<b>scv validatesysteminventory -r &lt;IPv4/IPv6 address&gt; -i</b>	
<b>Description</b>	Use the following command to connect remotely to a specific management console IP and validate the inventory.
<b>Synopsis</b>	scv validatesysteminventory -r <IPv4/IPv6 address> -i
<b>Input</b>	<ul style="list-style-type: none"> <li>- r — IPv4/IPv6 address</li> </ul>

**Output**

```

C:\>scv ValidateSystemInventory -r <IP address> -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Added Components Summary:
      PowerSupply      CNL000034I2C75      PSU.Slot.2
      HardDrive        23E0A08BTC88       Disk.Bay.5:Enclosure.Internal.0-1

Refer Detailed Report File at : C:\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_04_53_26.txt

```

## Connecting remotely to a management console with a specific port and validating inventory

Table 7. Validating inventory by using a specific port

<b>scv validatesysteminventory -r &lt;IPv4/IPv6 address:Port&gt; -i</b>	
<b>Description</b>	Use the following command to connect to a management console IP using a specific port and validate the inventory.
<b>Synopsis</b>	<code>scv validatesysteminventory -r &lt;IPv4/IPv6 address:Port&gt; -i</code>
<b>Input</b>	<ul style="list-style-type: none"> <li>- r — IPv4/IPv6 address</li> </ul>

## Ensuring component location match and validating inventory

Table 8. Ensuring component location match

<b>scv validatesysteminventory --enforceorder</b>	
<b>Description</b>	Use the following command to ensure that the component location matches while validating the inventory. <span style="border-left: 1px solid black; padding-left: 5px;">NOTE:</span> Any component swapping will be identified as 'Mismatch' while using the <code>--enforceorder</code> command.
<b>Synopsis</b>	<code>scv validatesysteminventory --enforceorder</code>

### Output

```

PS C:\> scv.exe ValidateSystemInventory -r <IP address> -i --enforceorder
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Validating Proof of Possession: Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
Compare Certificate Service Tag FL8WFZ3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch

-----
Inventory MisMatch Summary
-----
Added Components Summary:
      HardDrive      23E0A08BTC88      Disk.Bay.5:Enclosure.Internal.0-1
      PowerSupply    CNL0D0034I2C75    PSU.Slot.2

Moved Components Summary:
      HardDrive      23E0A08BTC88      PCIeSSD.SL.3-2

Refer Detailed Report File at : C:\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2023_12_24_04_35_37.txt

```

## Get SCV Version

Table 9. Get version of SCV

scv version	
<b>Description</b>	Use the following command to display the current version of SCV application.
<b>Synopsis</b>	scv version

### Output

```

C:\Users\Administrator>scv version
SCV version 1.5 (Build 156)
Copyright(c) 2020 - 2022 Dell, Inc.
All Rights Reserved

C:\Users\Administrator>
C:\Users\Administrator>

```

## Displaying certificate identifier value on console or redirecting it to a file

Table 10. Displaying or redirecting certificate identifier value

scv extractcert	
<b>Description</b>	Use the following command to display certificate identifier value on the console or to redirect it to a file.
<b>Synopsis</b>	scv extractcert -r <IPv4/IPv6 address> -i -component <Component Name> -l <Location> -f <File Name> -D <Debug>
<b>Input</b>	<ul style="list-style-type: none"> <li>- r — IPv4/IPv6 address</li> <li>- component — Component Name</li> </ul>

**Table 10. Displaying or redirecting certificate identifier value (continued)**

scv extractcert	
	<ul style="list-style-type: none"> <li>- l— Location</li> <li>- f— File Name</li> <li>- D— Enable debug log level</li> </ul>

**Output**

```
PS C:\> scv.exe extractcert -r <IP address> --component IDRAC --location 1 -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICZCCAgmgAwIBAgIIAwAAAAA3LbowCgYIKoZIzj0EAwIwDTELMAkGA1UEBhMCQ04xETAPBgNVBAGMCFNoYXNaGFpMREwDwYDVQHDAAhTaGFuZ2ZhaTERMA8GA1UEC
gwISW52Zm50ZW50DzDTALBgNVBAQMBFBST0QxHjAcBgNVBAMMFTBjVWwMc1DRtBDL TEwNUUHNjgyNjAaFw0yMzA2MjYyMjM0MDJhFjA4MjYyMjM0MDJhMh8xCzAJBgNVBAYTA1VTMjQ4MDYDVQQIDAVUZ
XhhczETMBEGA1UEBmwwKUm91bmQgUm9jazEFMB0GA1UECgwWRGVsbCBUZWNoe9sb2dpZm95SjEJEDMAwGA1UECmwfSURSQUMxGjAYBgNVBAMMEM90mNi0mUx0mFh0jQz0jEYmFkEwYHkoZiZj0CAQYIK
oZiZj0DAQcDQgAEICw0gZp7SjwS9GXAHXwA SPANvtjjIPMFvMfBf0F5Bv+GCAMWdmIv0WygNva7Wqw0prFN3ziy50ebRpSi0giKNSMhcwCQYDVR0TBAlwADALBgVVHQ8EBANCBwAmHQYDVR0LBBYwFAYIK
wYBBQUHwEGCCSGAQUFBwMCM8BGA1UjDQgNBRRFE1ZnZgc+DAUUmiehz/9AVoU0DAFBgNVHSMGDAWgBTTQRLYLTKIV9I9he9zyVUcYtYNTAKBggqhkJOPQQAglJAD8GA1EA/pe51/eUULQwqbkYTr0ZG
EGTjuaZkN3RTRtGv4LNB8CIQ0S5R8t2JYvLEuSU24tb/mZjDRBkKNBAwMa/KZVs/YAA-----END CERTIFICATE-----
```

**Figure 27. Displaying certificate identifier value on console**

```
PS C:\> scv.exe extractcert -r <IP address> --component IDRAC --location 1 -f abc.crt -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
```

**Figure 28. Writing certificate identifier value into a file**

```
PS C:\Users\Raj_Bhawan\scvGo2.0\workspace\SCV\scv_go> ./scv extractcert -r <IP address> -C idrac -l 1 -D -i
Username: root
Password:
Download SCV Platform Certificate: Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICZCCAgmgAwIBAgIIAwAAAAA3La8wCgYIKoZIzj0EAwIwDTELMAkGA1UEBhMCQ04xETAPBgNVBAGMCFNoYXNaGFpMREwDwYDVQHDAAhTaGFuZ2ZhaTERMA8GA1UEC
gwISW52Zm50ZW50DzDTALBgNVBAQMBFBST0QxHjAcBgNVBAMMFTBjVWwMc1DRtBDL TEwNUUHNjgyNjAaFw0yMzA2MjYyMjM0MDJhFjA4MjYyMjM0MDJhMh8xCzAJBgNVBAYTA1VTMjQ4MDYDVQQIDAVUZ
XhhczETMBEGA1UEBmwwKUm91bmQgUm9jazEFMB0GA1UECgwWRGVsbCBUZWNoe9sb2dpZm95SjEJEDMAwGA1UECmwfSURSQUMxGjAYBgNVBAMMEM90mNi0mUx0mFh0jQz0jEYmFkEwYHkoZiZj0CAQYIK
oZiZj0DAQcDQgAEICw0gZp7SjwS9GXAHXwA SPANvtjjIPMFvMfBf0F5Bv+GCAMWdmIv0WygNva7Wqw0prFN3ziy50ebRpSi0giKNSMhcwCQYDVR0TBAlwADALBgVVHQ8EBANCBwAmHQYDVR0LBBYwFAYIK
wYBBQUHwEGCCSGAQUFBwMCM8BGA1UjDQgNBRRFE1ZnZgc+DAUUmiehz/9AVoU0DAFBgNVHSMGDAWgBTTQRLYLTKIV9I9he9zyVUcYtYNTAKBggqhkJOPQQAglJAD8GA1EA+w8RS3qvx/t4lp2Ww
iZU4t+DNSXqJEtIUL/sdR7UvrMCIQkhwPwNxf4ULcbBZ9m7EDTzWbrYs+dchzBgIRfoISQ-----END CERTIFICATE-----
```

**Figure 29. Displaying certificate identifier value on console using debug option**



## SCVApp MARS feature

MAC Address Reporting Service (MARS) is a new offering that provides MAC address for the iDRAC and LOM port 0 and the corresponding server service tag.

SCVApp extracts MAC address from the certificate inventory for the network and iDRAC component.

The following are the SCVApp commands:

**Table 11. Getting information about mars**

<b>scv help mars</b>	
Synopsis	scv help mars
Output	<pre> scv help mars  SCV -- Secured Component Verification  Usage: scv.exe mars [options]...  List of supported options:     -d, --directory=&lt;Directory Path&gt;         Output directory path (MAX 247 Characters). If not specified, Current Working directory will be the output directory.     -f, --file=&lt;File Path&gt;         Input or Output File Path.     -D, --debug         Enable Debug log level  List of Example Commands:     scv.exe mars -f --file [ -d --directory ] [ -D --debug ] </pre>

**Table 12. Running mars command to extract mars details and create the marsreport.csv file**

<b>scv mars</b>	
Synopsis	scv mars ./SCVTest.zip ./scvapp/out/marsreport.csv
Output	<pre> scv mars ./SCVTest.zip ./scvapp/out/marsreport.csv :  ServiceTags,Components,MacAddresses  FYRLCW3,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52  FYRLCW3,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53  FYRLCW3,iDRAC,c8:4b:d6:98:93:4c  FYRLCW3,NIC.Embedded.1-1-1,C8:4B:D6:98:93:52  FYRLCW3,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53 </pre>

**Table 12. Running mars command to extract mars details and create the marsreport.csv file (continued)**


<b>scv mars</b>	
	FYRLCW3,iDRAC,c8:4b:d6:98:93:4c

## SPDM feature

Security Protocol and Data Model (SPDM) is a protocol that is used for establishing security capabilities and authenticity between hardware components. SPDM allows message exchange between iDRAC and end devices such as storage controllers and NIC controllers. This includes hardware identity certificates.

SCV Application supports discovery of the hardware identity certificates for SPDM enabled end devices. SCV Application exports the hardware identity of the SPDM enabled devices into the SCV certificate.

# SCV Root CA Certificate

 **NOTE:** This section provides details for the SCV Root CA Certificate.

File Format: Extracts files directly to local disk

File Name: Certificate A00.zip

File Size: 929 Bytes

Format Description: This file format consists of an archive of files that may be decompressed to a directory on the hard drive. The installation can then be done from that directory.

Download Link: <https://dl.dell.com/FOLDER06748569M/1/Certificate A00.zip>

To ensure the integrity of your download, please verify the checksum value.

MD5: edb649dbf130e43aeaf5358f1186d312

SHA1: a92d23c8e9e61fd5c4e568cb23be3024df3f886f

SHA-256: c947162dc67f5d441ff22b063d7566c52db23cc0c51746455e492c60943f8165

## Return Codes

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

**Table 13. 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.
12	Value specified is out of range. The length of argument is larger or shorter than allowed.
13	Invalid or incorrect SCV command entered. Any command or option entered is not supported on the current interface/platform.
14	Syntax of command is incorrect.
15	Command to be executed in Factory(SSM) mode.
16	SCV doesn't have a required license installed.
17	iDRAC doesn't have enough resources (Ex:- Memory)
18	Service unavailable/busy.
19	File transfer issue (Inband).
20	Lockdown mode enabled or dependent attributes are invalid/not configured.
21	Unable to connect (Out of Band)
22	Dependency not met for a specification
23	Session related issues.
24	Failure due to invalid keys, certificate, and signing error.
25	Certificate upload failed.

# Getting help

## Topics:

- [Contacting Dell](#)
- [Support documents and resources](#)
- [Documentation feedback](#)

## Contacting Dell

Dell 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 product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical assistance, or customer service issues:

### Steps

1. Go to [www.dell.com/support/home](http://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:
  - a. Enter your system Service Tag in the **Enter your Service Tag** field.
  - b. Click **Submit**.  
The support page that lists the various support categories is displayed.
4. For general support:
  - a. Select your product category.
  - b. Select your product segment.
  - c. Select your product.  
The support page that lists the various support categories is displayed.
5. For contact details of Dell Global Technical Support:
  - a. Click [Contact Technical Support](#).
  - b. 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](http://www.dell.com/support/idrac)
- iDRAC User Guide and other manuals:
  - [www.dell.com/idracmanuals](http://www.dell.com/idracmanuals)
- For information about PowerEdge servers, see the documentation at:
  - [www.dell.com/poweredgemanuals](http://www.dell.com/poweredgemanuals)
- Dell Technical Support:
  - [www.dell.com/support](http://www.dell.com/support)

## Documentation feedback

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