Dell Secured Component Verification Version 1.5,1.5.1,1.6,1.7,1.8, 1.9, 1.91.0, 1.92.0, and 1.93.0

Reference Guide for Servers and Chassis

June 2024
Rev. A08

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

Chapter 1: Overview **5**
New features added 5
SCV 1.93.0 5
SCV 1.92.0 5
SCV 1.91.0 5
SCV 1.9 5
SCV 1.8 6
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 8
URIs Supported 8

Chapter 2: Secured Component Verification on WinPE **10**
Creating an ISO image to run SCV using WinPE 10
Adding SCV to Custom ISO Image 11
Running SCV on WinPE 11
How to check SCV logs using WinPE 13

Chapter 3: Secured Component Verification on Linux **14**
Running SCV on Linux 14
View the SCV logs using Linux 17

Chapter 4: Secured Component Verification on Windows Server 2019 and 2022 ..... **18**
Installing SCVApp on Windows Server 2019 and 2022 18
Running SCV on Windows Server 2019 and 2022 21

Chapter 5: Running Secured Component Verification (SCV) remotely **25**
Running SCV remotely on Windows Server 2019 and 2022 25
Running SCV remotely on WinPE 25
Running SCV remotely on Linux 25

Chapter 6: SCV Command Details **27**
Get information on how to run SCV 27
Get information about scv validatesysteminventory command 27
Connecting remotely to a management console and validating inventory 28
Connecting remotely to a management console with a specific port and validating inventory 29
Ensuring component location match and validating inventory 29
Get SCV Version 29
Displaying certificate identifier value on console or redirecting it to a file 30

Chapter 7: SCVApp MARS feature **32**

Chapter 8: SPDM feature **34**

Chapter 9: SCV Root CA Certificate **35**

Chapter 10: Return Codes **36**

Chapter 11: Getting help **37**

Contacting Dell 37

Support documents and resources 37

Documentation feedback 37

1

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
- URIs Supported

New features added

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

- SCV 1.93.0
- 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 1.93.0

The following features were added or updated in this release:

- The latest version includes critical security fixes in the SCV application.

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 is identified as a "Mismatch".

Notes:

- SCV application can be launched directly from the iDRAC UI 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.
- Even when the USB-NIC is enabled from iDRAC, you must enable the network interface manually within the operating system. It should not be disabled as it is required for inband communication.
- 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. It is an expected behavior because 1.0 certificate does not include ECC information.
- SCV does not support 1.0 certificates starting from version 1.93.0.

System Requirements

Table 1. System requirements for running SCV

<table>
<tr><th>Category</th><th>Requirement</th></tr>
<tr><td>Supported operating platforms</td><td>WinPE 10.x, Red Hat Enterprise Linux 9.0, Red Hat Enterprise Linux 8.6, SUSE Linux Enterprise Server 15 SP4, Windows Server 2019, and Windows Server 2022.</td></tr>
<tr><td>Firmware versions</td><td>• iDRAC 5.10.30.00 and later versions
• OME-M 2.00.00 and later versions
• PowerEdge BIOS 2.14.2 and later versions</td></tr>
<tr><td>Licenses required</td><td>Secured Component Verification License</td></tr>
<tr><td>Compatible versions</td><td>
<table>
<tr><th>SCV Version</th><th>iDRAC Version</th></tr>
<tr><td>1.93.0</td><td>7.10.50.00</td></tr>
<tr><td>1.92.0</td><td>7.10.30.00</td></tr>
<tr><td>1.91.0</td><td>7.10.30.00</td></tr>
<tr><td>1.9.0</td><td>7.00.30.00</td></tr>
<tr><td>1.8.0</td><td>6.10.80.00</td></tr>
<tr><td>1.6.0</td><td>6.00.30.00</td></tr>
<tr><td>1.5.0</td><td>5.10.30.00</td></tr>
</table>
SCV 1.91.0 and later versions are backward compatible with any version of iDRAC. However, SCV 1.90.0 and earlier versions are compatible only with version 7.00.30.00 and earlier versions of iDRAC.
</td></tr>
</table>

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 running 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: 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. 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"
 }
```

2

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\Anirban_Dasgupta\Downloads\Dell-SCVTools-Web-WINPE10-1.93.0-360>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\Anirban_Dasgupta\Downloads\Dell-SCVTools-Web-WINPE10-1.93.0-360\WINPE10_x_20246-02_105200
=================================================
```

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.

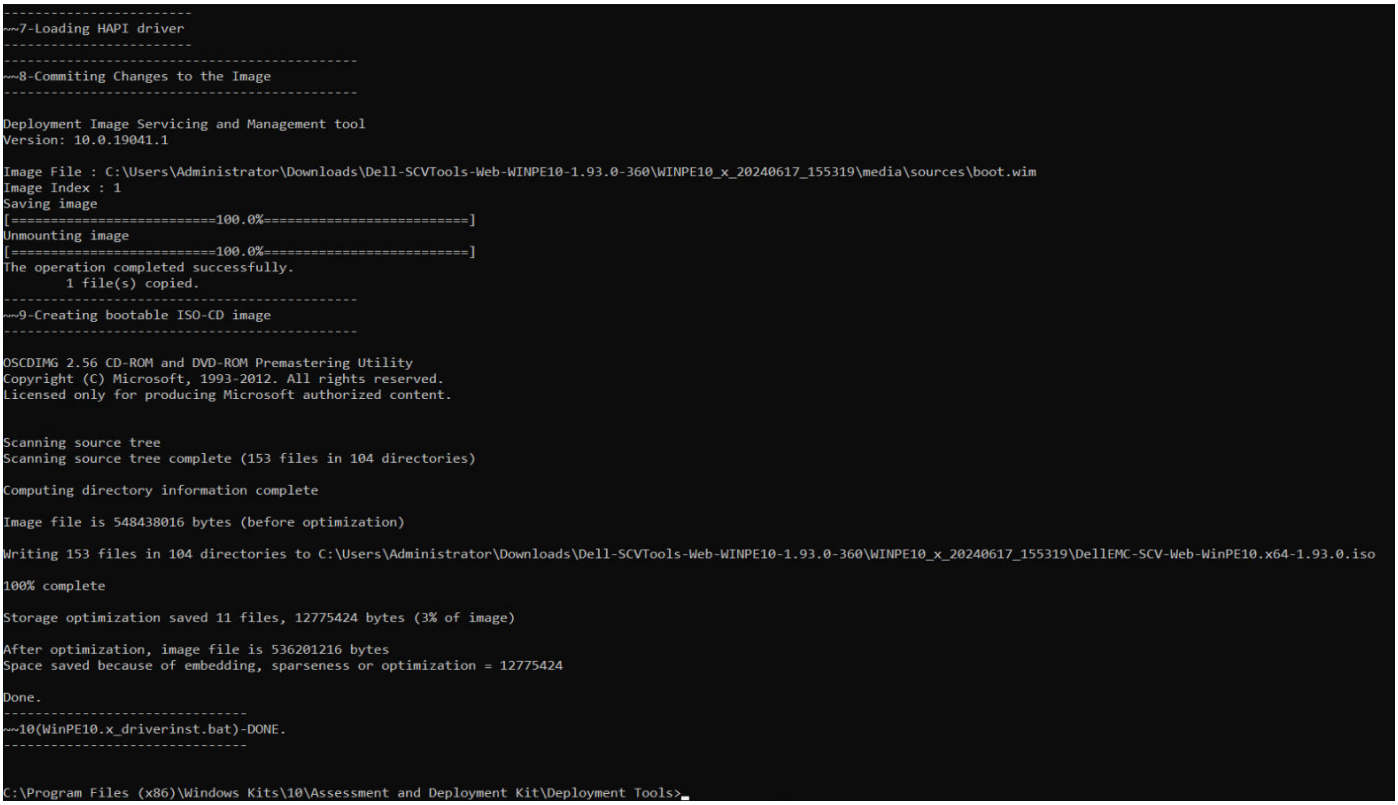

Figure 2. Confirmation of the ISO image created successfully

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 255 characters.

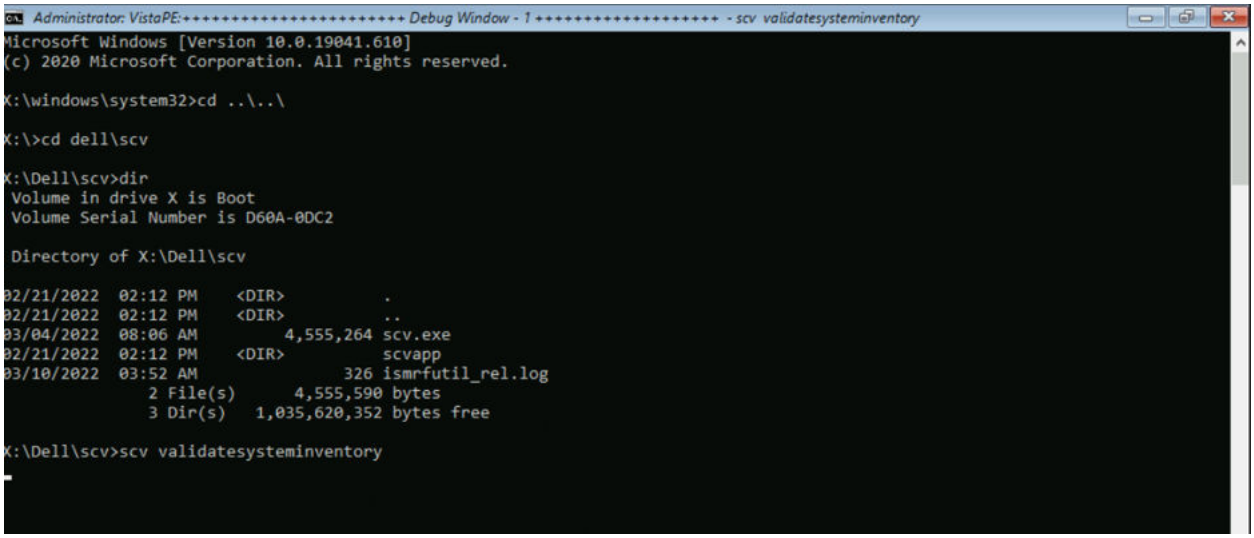

Figure 3. Running the validation command

8. Once the system runs the SCV application successfully, it should give the result of scv validatesysteminventory command as `Match`.

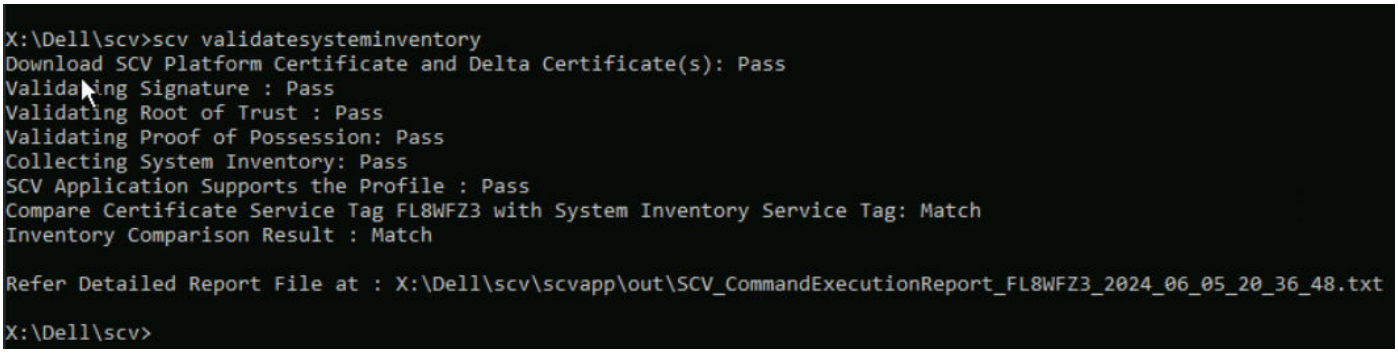

Figure 4. Running the validation command and result is successful

9. If the result of scv validatesysteminventory command is a `Mismatch`, it will specify which component has mismatched under `Mismatch Inventory Summary`.

```
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 Comparision Result : MisMatch


-----------------------------------------------------------------------
Inventory MisMatch Summary
-----------------------------------------------------------------------
Added Components Summary:
               HardDrive       23E0A08BTC88    Disk.Bay.5:Enclosure.Internal.0-1
               PowerSupply     CNLOD0034I2C75  PSU.Slot.2


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

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

3

Secured Component Verification on Linux

This section provides information for the following:

Topics:

- Running SCV on Linux
- View the 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@auvcetillem1m1 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@auvcetillem1m1 Downloads]# ls
COPYRIGHT.txt  DellEMC-SCV-Web-LX-2000-75.tar.gz  ismrfutil-el8-v0  license.txt  SCVTools
[root@auvcetillem1m1 Downloads]# cd SCVTools/
[root@auvcetillem1m1 SCVTools]# ls
install_scv.sh  readme.txt  RPMS  uninstall_scv.sh
[root@auvcetillem1m1 SCVTools]# sh uninstall_scv.sh
[root@auvcetillem1m1 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@auvcetillem1m1 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 as `scv validatesysteminventory: Match`

```
[root@localhost ~]# scv ValidateSystemInventory  -r [redacted] -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 : Match

Refer Detailed Report File at : /root/scvapp/out/SCV CommandExecutionReport FL8WFZ3 2024 06 17 20 07 36.txt
```

Figure 9. Running the validation command and result is match

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     CNLOD0034I2C75  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": "CNLOD0034I2C75"
        }
    ]
}
--------------------------------------------------------------------------------
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

View the SCV logs using Linux

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

```
[root@localhost scv] # vi ./scvapp/logs/SCVLog_RtSTC21_2020_09_15_05_55_28.log
```

4

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.

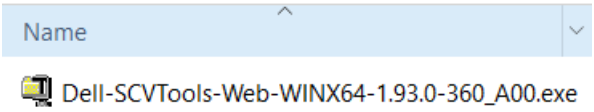

Figure 11. SCV installer zip file

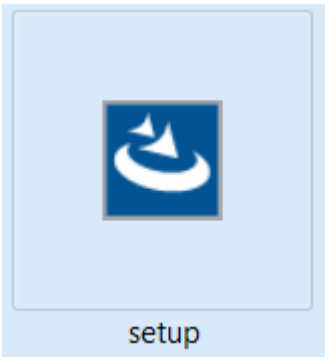

Figure 12. SCV installer

3. Run the application to start the InstallShield Wizard.

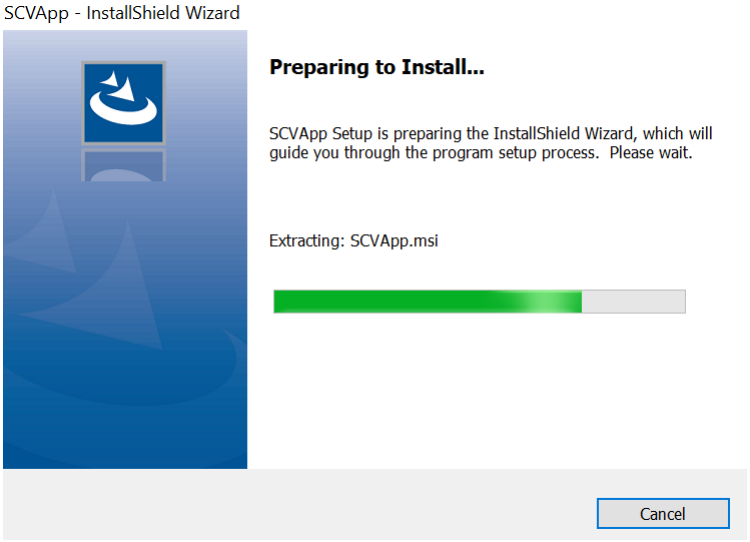

Figure 13. Running SCV installer

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.

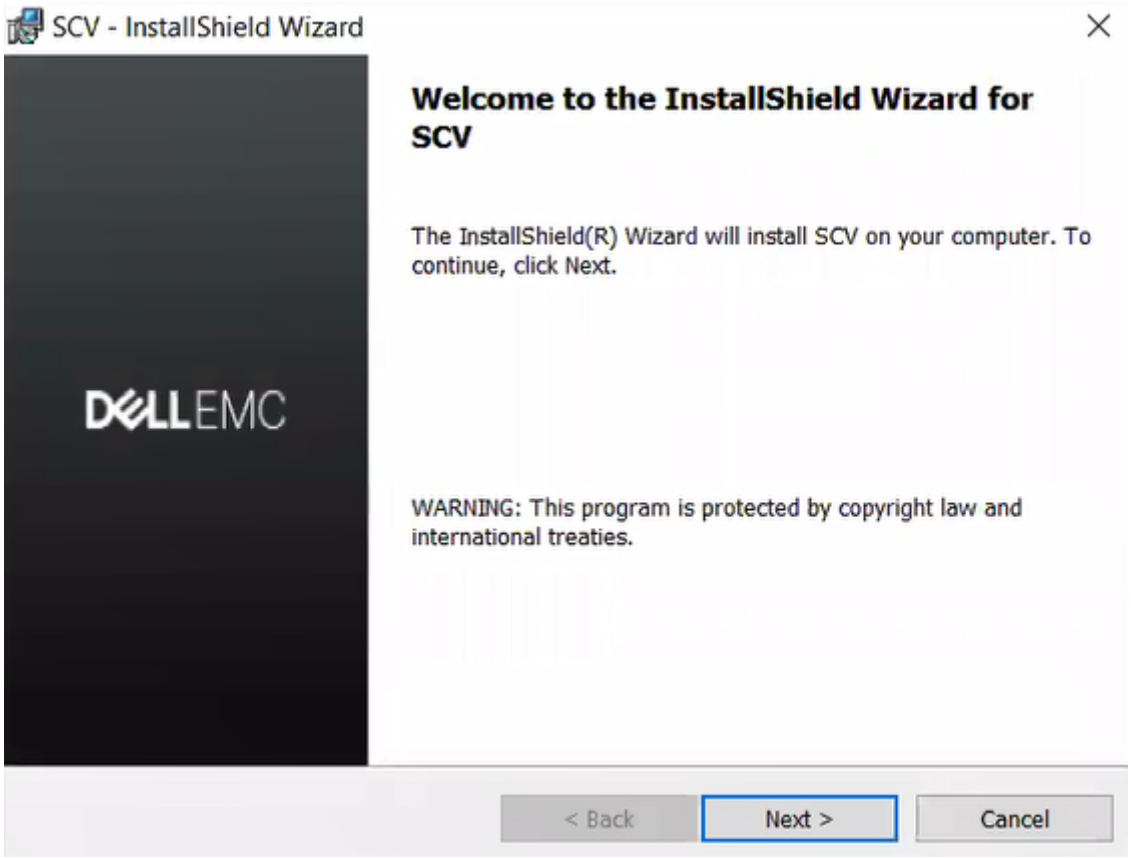

Figure 14. InstallShield Wizard for SCVApp

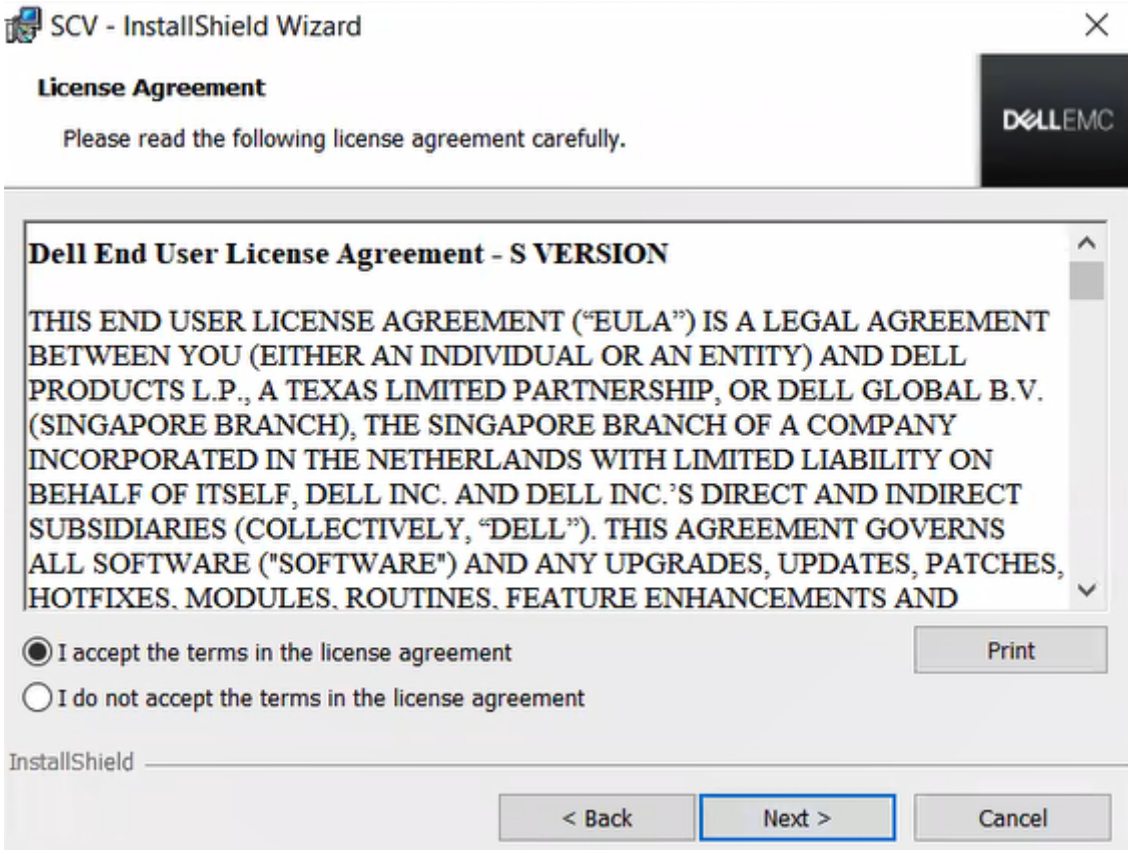

Figure 15. License Agreement for SCVApp

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

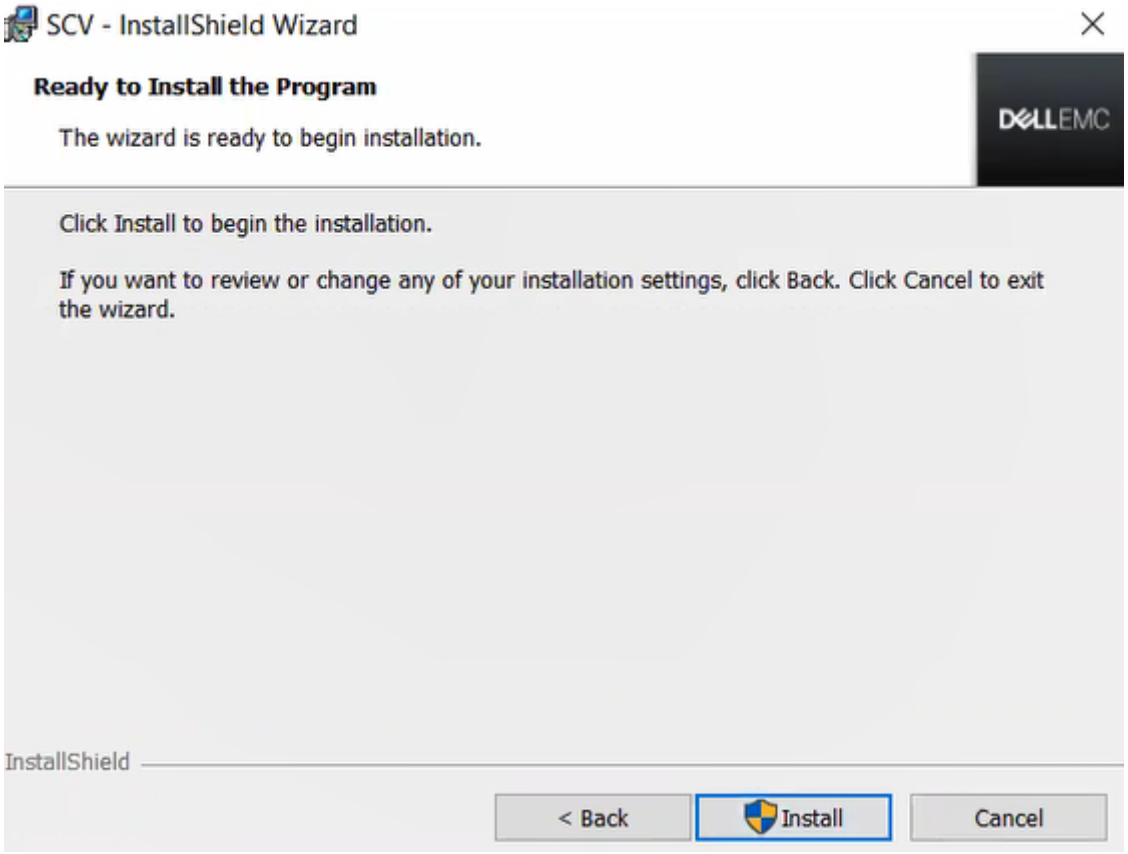

Figure 16. Ready to install SCVApp

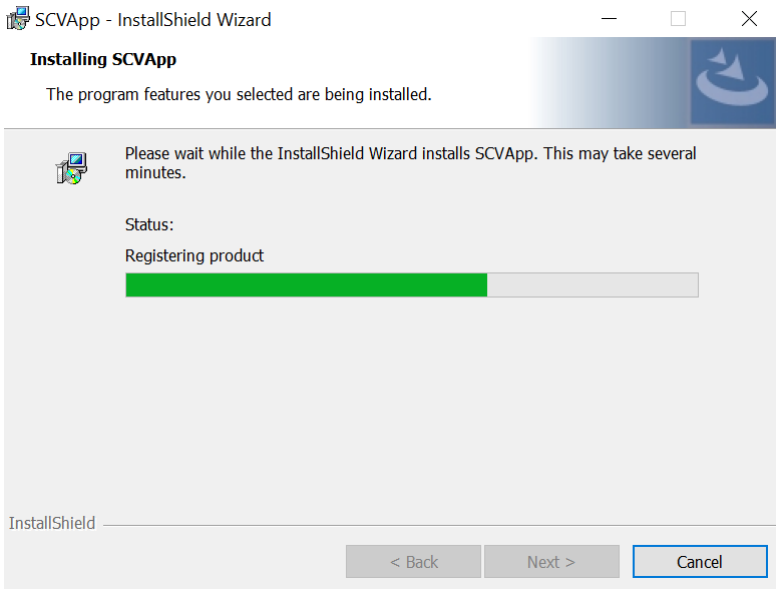

Figure 17. Installing SCVApp

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

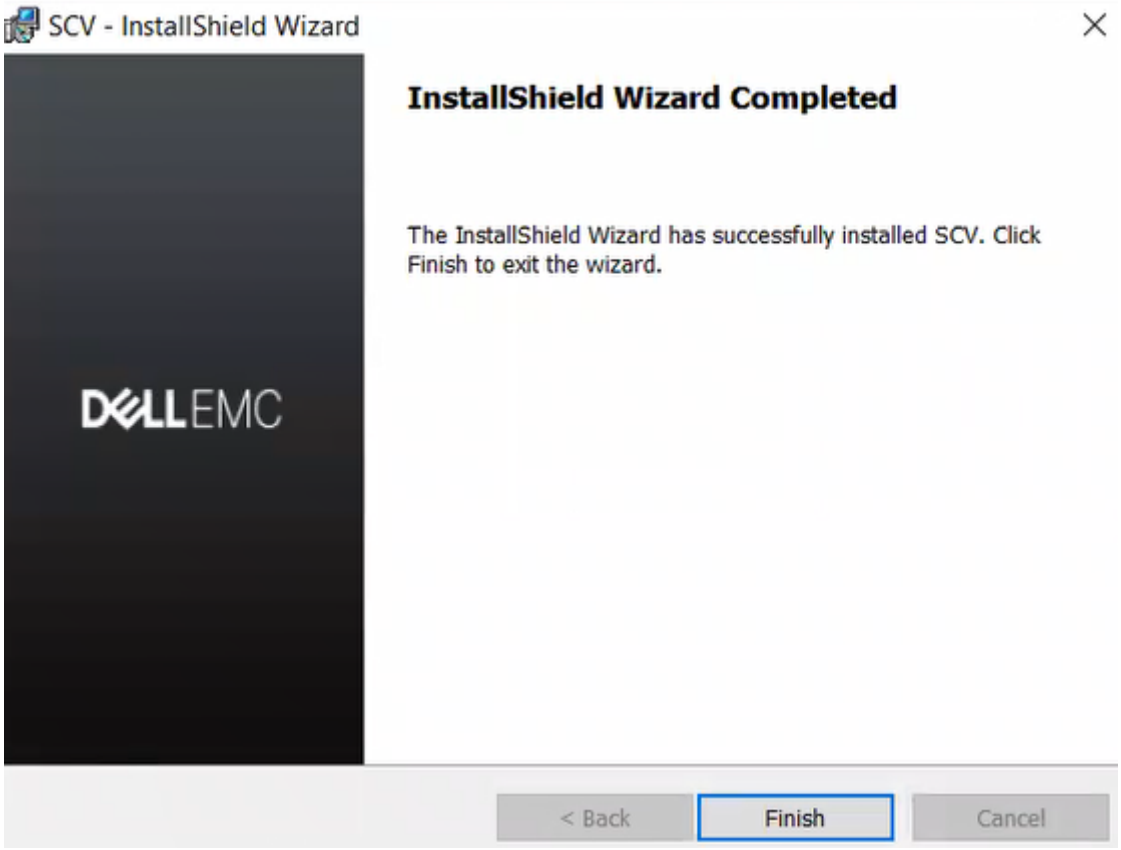

Figure 18. SCVApp installation complete

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.' .

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.

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.

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.

NOTE: An error 'Collecting System Inventory: Fail' may be displayed while executing the `scv validatesysteminventory` command with `-d <path of the directory>` option, if the directory path length exceeds 255 characters.

```
C:\Users\Administrator>scv validatesysteminventory
Download SCV Platform Certificate and Delta Certificate(s): 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 CLDBZR3 with System Inventory Service Tag: Match
Inventory Comparison Result : Match

Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_CLDBZR3_2024_06_17_16_44_42.txt
```

Figure 19. Running the validation command and result is match

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

```
C:\Users\Administrator>scv validatesysteminventory
Download SCV Platform Certificate and Delta Certificate(s): 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 CLDBZR3 with System Inventory Service Tag: Match
Inventory Comparison Result : MisMatch


--------------------------------------------------------------------------
Inventory MisMatch Summary
--------------------------------------------------------------------------
Added Components Summary:
                HardDrive       SJB5N7040I2405V33       Disk.Bay.4:Enclosure.Internal.0-1
                HardDrive       SJB5N7040I2405V2Z       Disk.Bay.5:Enclosure.Internal.0-1
                HardDrive       PHLN1142018X1P6AGN      Disk.Bay.3:Enclosure.Internal.0-1
                HardDrive       PHLN1142015J1P6AGN      Disk.Bay.2:Enclosure.Internal.0-1
                HardDrive       PHLN1142018Z1P6AGN      Disk.Bay.1:Enclosure.Internal.0-1
                HardDrive       PHLN114201751P6AGN      Disk.Bay.0:Enclosure.Internal.0-1
```

Figure 20. Running the validation command and result is a mismatch

```
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": "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": "CNLOD0024635D4"
        }
    ],
------------------------------
------------------------------
 "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": "1BFCF11FD1C1E363"
        }
    ],
    "iDRAC": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060003",
            "CertificateIdentifier": "MIICVTCCAfugAwIBAgIIAwAAAAAxE+QwCgYIKoZIzj0EAwIwdTEL
             MAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREw
        }
```

Figure 21. 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": "0x00030003",
            "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": "CNLOD0024635D4"
        }
    ],
    "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": "1BFCF11FD1C1E363"
        }
    ],
    "iDRAC": [
        {
            "ComponentRegistryOID": "2.23.133.18.3.1",
            "ComponentClass": "0x00060003",
            "CertificateIdentifier": "MIICVTCCAfugAwIBAgIIAwAAAAAxE+QwCgYIKoZIzj0EAwIwdTELMAkGA
             1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTa
        }
```

Figure 22. Mismatched component expected and detected details

5

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.

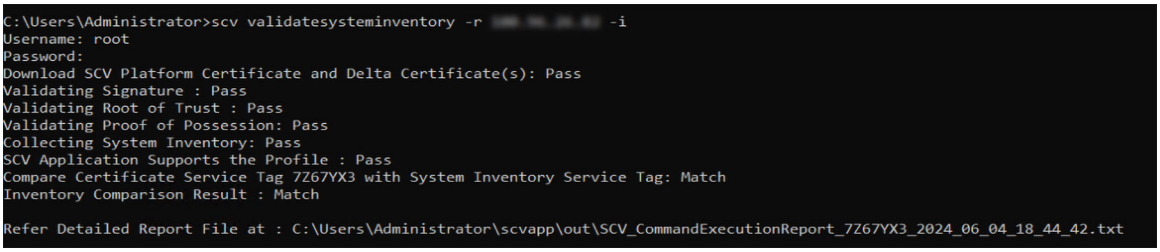

Figure 23. Running the validation command remotely on Windows and result is match

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.

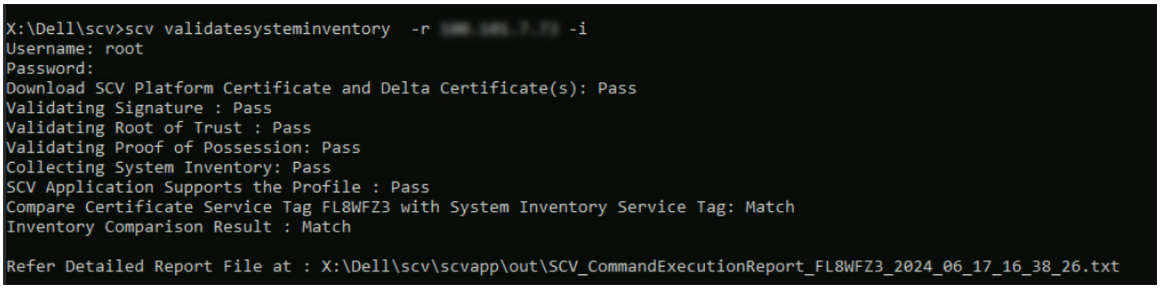

Figure 24. Running the validation command remotely on WinPE and result is match

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 ~]# scv ValidateSystemInventory  -r  [redacted] -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 : Match

Refer Detailed Report File at : /root/scvapp/out/SCV CommandExecutionReport FL8WFZ3 2024 06 17 20 07 36.txt
```

Figure 25. Running the validation command remotely on Linux and result is match

6

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	
Description	Use the following command to get more information about SCV and how to run it.
Synopsis	`scv help`

Output

```
C:\Users\Administrator>scv help

SCV -- Secured Component Verification

Usage: scv.exe help <subcommand> [options]...

List of supported subcommands:
        - validatesysteminventory
        - deltacert
        - extractcert
        - getcertinfo
        - version
        - mars
```

Get information about scv validatesysteminventory command

Table 5. Get more information about SCV validatesysteminventory command

scv help validatesysteminventory	
Description	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)

scv help validatesysteminventory	
Synopsis	`scv help validatesysteminventory`

Output

```
localhost:~/SCVTools # scv help validatesysteminventory

SCV -- Secured Component Verification

Usage: scv validatesysteminventory [options]...

List of supported options:
        -r, --remoteip=<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 user
        -d, --directory=<Directory Path>        Output directory path (MAX 247 Charactors). If not specified, Current Working directory will be the output directory.
        -e, --enforceorder                      force component slot location comparison along with the serial number comparison.
        -D, --debug                             Enable Debug log level


List of Example Commands:
        scv validatesysteminventory [ -r|--remoteip -u|--username -p|--password ] [ -e|--enforceorder ] [ -d|--directory ] [ -D|--debug ]
        scv validatesysteminventory [ -r|--remoteip -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

scv validatesysteminventory -r <IPv4/IPv6 address> -i	
Description	Use the following command to connect remotely to a specific management console IP and validate the inventory.
Synopsis	`scv validatesysteminventory -r <IPv4/IPv6 address> -i`
Input	• `-r <IPV4/IPV6 address>`

Output

```
C:\Users\Administrator>scv validatesysteminventory -r [redacted] -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 : Match
```

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

Table 7. Validating inventory by using a specific port

scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i	
Description	Use the following command to connect to a management console IP using a specific port and validate the inventory.
Synopsis	`scv validatesysteminventory -r <IPv4/IPv6 address:Port> -i`
Input	• `-r <IPV4/IPV6 address>`

Ensuring component location match and validating inventory

Table 8. Ensuring component location match

scv validatesysteminventory --enforceorder	
Description	Use the following command to ensure that the component location matches while validating the inventory. **NOTE:** Any component swapping will be identified as 'Mismatch' while using the `--enforceorder` command.
Synopsis	`scv validatesysteminventory --enforceorder`

Output

```
C:\Users\Administrator>scv validatesysteminventory -r [redacted] -i --enforceorder
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): 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 : Match

Refer Detailed Report File at : C:\Users\Administrator\scvapp\out\SCV_CommandExecutionReport_FL8WFZ3_2024_06_17_17_27_40.txt
```

Get SCV Version

Table 9. Get version of SCV

scv version	
Description	Use the following command to display the current version of SCV application.
Synopsis	`scv version`

Output

```
C:\Users\Administrator>scv version
SCV version 1.93.0 [redacted]
Copyright(c) 2020 - 2024 Dell Inc.
All Rights Reserved.
```

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

Table 10. Displaying or redirecting certificate identifier value

scv extractcert	
Description	Use the following command to display certificate identifier value on the console or to redirect it to a file.
Synopsis	`scv extractcert -r <IPv4/IPv6 address> -i -c <Component Name> -l <Location> -f <File Name>  -d <Directory Name>`
Input	• `--remoteip <IPV4/IPV6 address>` • `--component <Component_name>` • `--location <Location_name>` • `--file <File_name>` • `--directory <Directory_name>`

Output

```
X:\Dell\scv>scv extractcert -r [redacted] --component iDRAC --location 1 -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
-----BEGIN CERTIFICATE-----MIICXzCCAgagAwIBAgIIBAAAAAAighswCgYIKoZIzj0EAwIwcjELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB1RpYW5qaW4xEDAOBgN
VBAcMB1RpYW5qaW4xEDAOBgNVBAoMB0ZveGNvbm4xDTALBgNVBAsMBFBST0QxHjAcBgNVBAMMFTBGQ1AwMC05NzQxLTc0QkItMjMzNzAeFw0yMzA0MTIwMDI0MzJaF
w00MjA2MTEwMDI0MzJaMH8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEGA1UEBwwKUm91bmQgUm9jazEfMB0GA1UECgwWRGVsbCBUZWNobm9sb2dpZXM
gSW5jLjEOMAwGA1UECwwFSURSQUMxGjAYBgNVBAMMEWVjOjJhOjcyOmVkOjIzOmE4MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEX+zOMoLfbL7ArlFfIm5XKR4/m
c5L+7p2z1HmL5MDKU2eqFHcN6iO5KxKBrCGky0wVvxrhUATSSdbUrAEYYnS+6N5MHcwCQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwHQYDVR0lBBYwFAYIKwYBBQUHAwE
GCCsGAQUFBwMCMB0GA1UdDgQWBBQ/g68GL[illegible]PlReExQMNbYupAEk63lTAfBgNVHSMEGDAWgBRyuNpU7GgYOVwiMaBV8If/PxX/eTAKBggqhkjOPQQDAgNHADBEAiAyP
OFDJ2+nuJ1cZ2/W49RFpQUhBcXfVp6hAWhK[illegible]hLNtwIgNkWr48X5OlPmK47N09S1MwsUHF5OFQE7JihTSVtu6ow=-----END CERTIFICATE-----

X:\Dell\scv>
```

Figure 26. Displaying certificate identifier value on console

```
C:\Users\Administrator>scv extractcert -r [redacted] -C iDRAC -l 1 -f abc.crt -i
Username: root
Password:
Download SCV Platform Certificate and Delta Certificate(s): Pass
Validating Signature : Pass
Validating Root of Trust : Pass
Collecting System Inventory: Pass
SCV Application Supports the Profile : Pass
```

Figure 27. Writing certificate identifier value into a file

Figure 28. Displaying certificate identifier value on console using --debug or -D option

7

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

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

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

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

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

scv mars	
	`<ServiceTag>,iDRAC,c8:4b:d6:98:93:4c`

8

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 1.93.0 supports PERC 12.2.

9

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

10

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 is 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	The 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 or platform.
14	Syntax of the command is incorrect.
16	SCV does not have a required license installed.
17	iDRAC does not have enough resources (Example: Memory)
18	Service unavailable/busy.
19	File transfer issue (Inband).
20	Lockdown mode enabled or dependent attributes are invalid or 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 key, certificate, and signing error.
25	Certificate upload failed.

11

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 Dell Support page.
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
- iDRAC User Guide and other manuals:
  - www.dell.com/idracmanuals
- For information about PowerEdge servers, see the documentation at:
  - www.dell.com/poweredgemanuals
- Dell Technical Support:
  - 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.