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

Reference Guide for Servers and Chassis

December 2023
Rev. A00

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

# 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

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



### 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 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 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 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 will report 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

| 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 or 1.91.0 |
| Firmware versions | iDRAC 5.10.30.00 and later versions<br>OME-M 2.00.00 and later versions<br>PowerEdge BIOS 2.14.2 and later versions |
| 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

| 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 |

| Components supported for Modular Chassis |
|---|
| Enclosure Controller |
| Fan |
| Open Manage Enterprise Modular |
| ChassisRCP |
| PowerSupply |

| Components supported for Modular Chassis |
|---|
| 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. 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

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`.

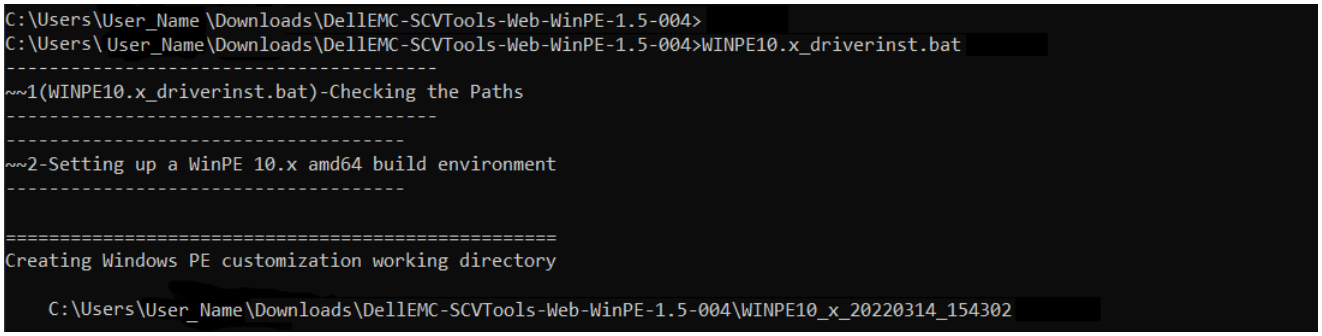


**Figure 1. Running the batch file through command prompt**

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

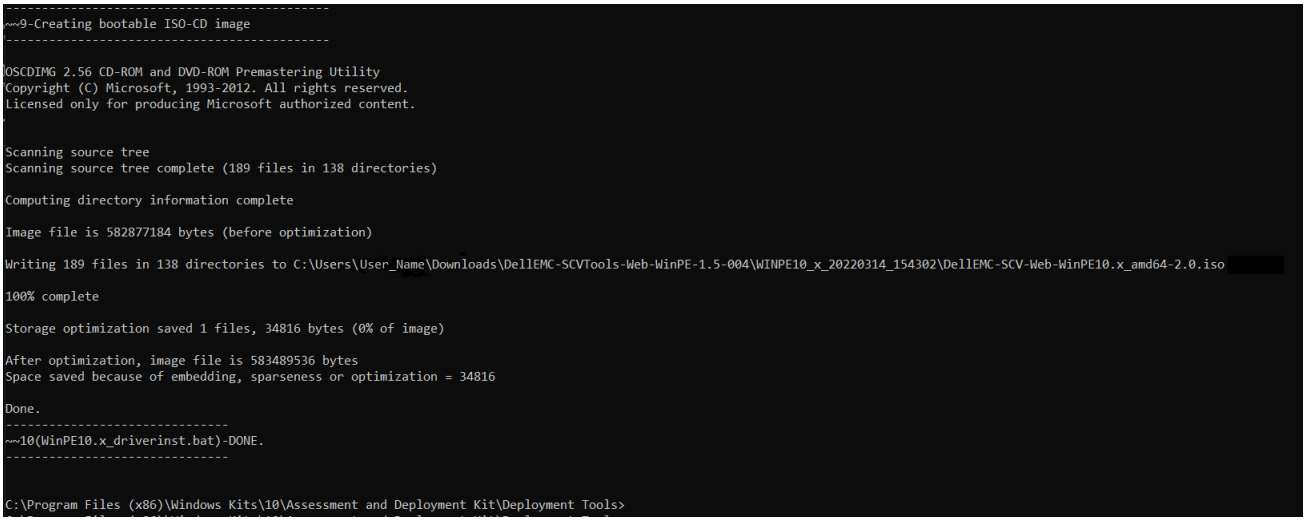


**Figure 2. Confirmation of the ISO image created successfully**

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\OpenSSL** to `X:\Dell\scv`
   c. **Toolkit\DLLs** to `X:\windows\system32`
5. After copying the files, set the path for the folder using the command `set PATH=%PATH%;X:\Dell\scv;X:\Dell\scv\openssl;`
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.

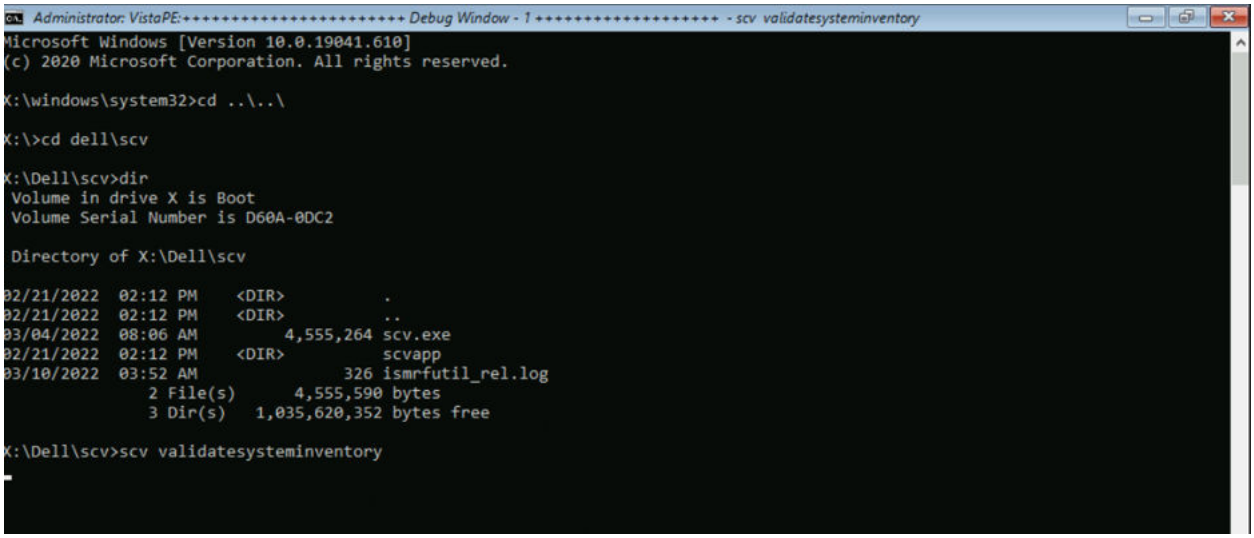


**Figure 3. Running the validation command**

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

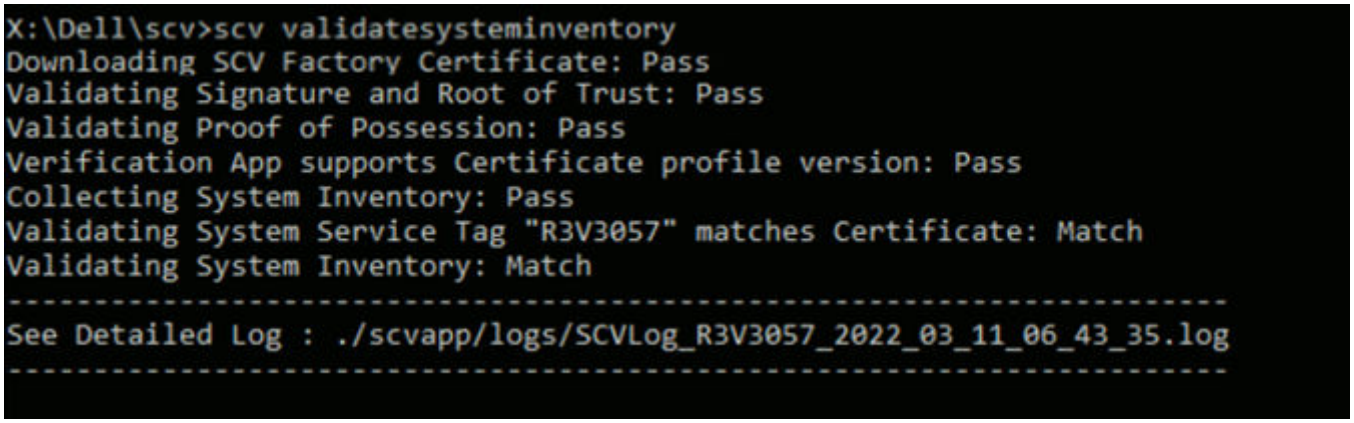


**Figure 4. Running the validation command and result is successful**

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

```
Mismatch Inventory Summary
---------------------------------------------------------------------------
Baseboard 1: Mismatch
---------------------------------------------------------------------------
Checking Component: Baseboard
---------------------------------------------------------------------------
Baseboard 1: Mismatch
Expected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "A02",
        "location" : "1",
        "manufacturer" : "Dell Inc.",
        "model" : "0HDV4Y",
        "serial_number" : "CNFCP0015V004L"
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown",
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown"
}
---------------------------------------------------------------------------
Overall Baseboard check Status: Mismatch
---------------------------------------------------------------------------
```

**Figure 5. Mismatched component expected and detected details**

# How to check SCV logs using WinPE

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

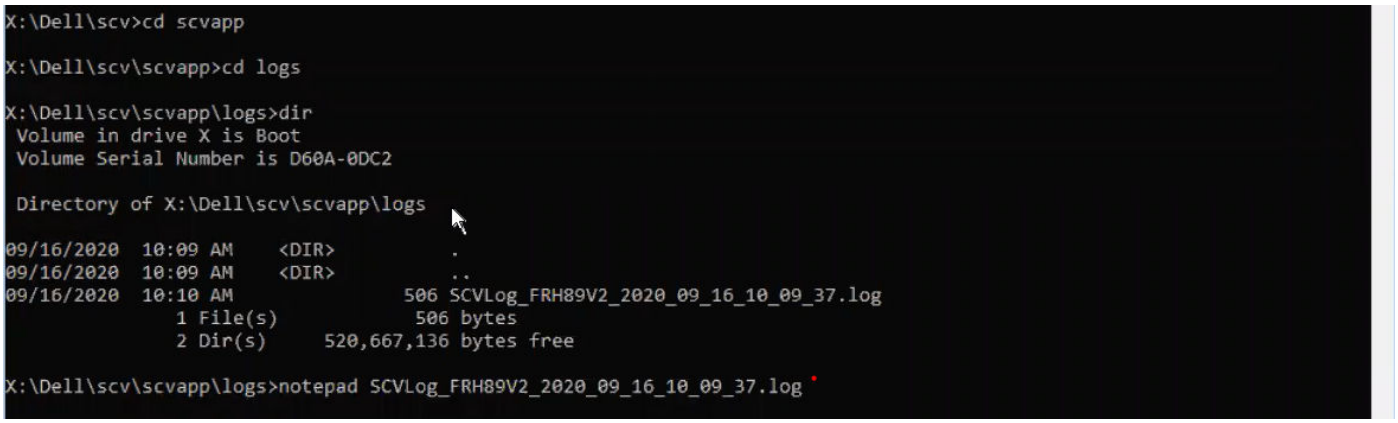


**Figure 6. Checking logs using WinPE**

# 3

# Secured Component Verification on Linux

This section provides information for the following:

**Topics:**



## 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 `Validating System Inventory: Match`

```
C:\SecureComponentVerification>scv validatesysteminventory
Downloading SCV Certificate: Pass
Downloading SCV Delta Certificate(s): No Cert Present
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "887NYX3" matches Certificate: Match
Validating System Inventory: Match
--------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_887NYX3_2023_10_26_03_27_13.log
--------------------------------------------------------------------------
```

**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`.

```
Mismatch Inventory Summary
--------------------------------------------------------------------------
Baseboard 1: Mismatch
--------------------------------------------------------------------------
Checking Component: Baseboard
--------------------------------------------------------------------------
Baseboard 1: Mismatch
Expected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "A02",
        "location" : "1",
        "manufacturer" : "Dell Inc.",
        "model" : "0HDV4Y",
        "serial_number" : "CNFCP0015V004L"
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown",
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown"
}
--------------------------------------------------------------------------
Overall Baseboard check Status: Mismatch
--------------------------------------------------------------------------
```

**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**

# 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

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.

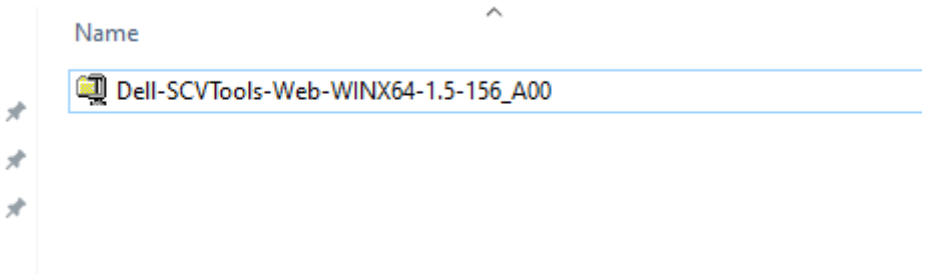


**Figure 12. SCV installer zip file**

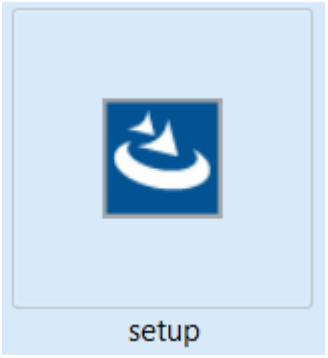


**Figure 13. SCV installer**

3. Run the application to start the InstallShield Wizard.

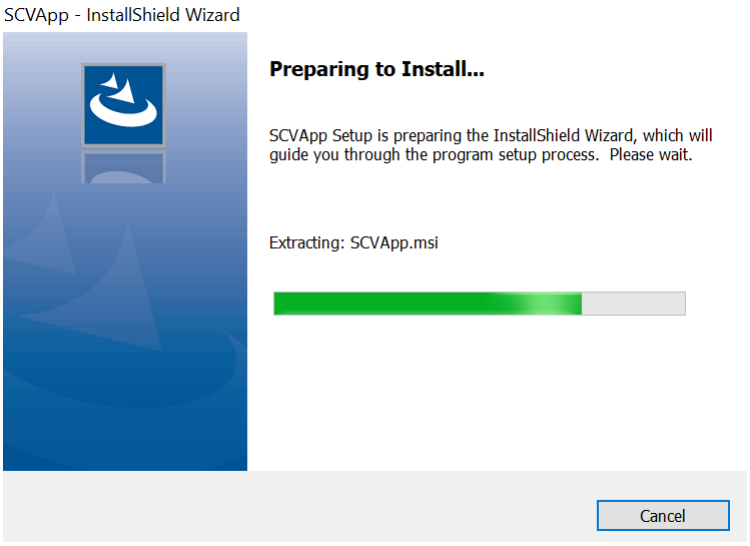


**Figure 14. Running SCV installer**

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.

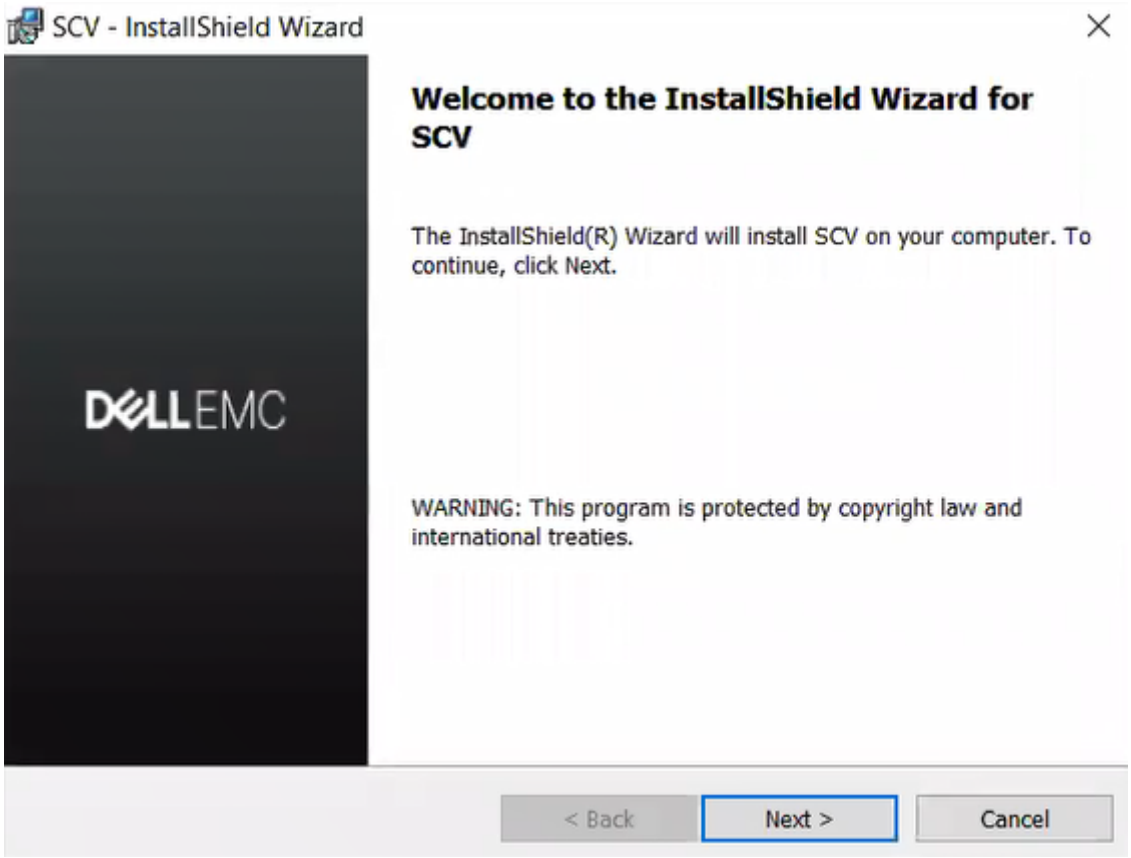


**Figure 15. InstallShield Wizard for SCVApp**

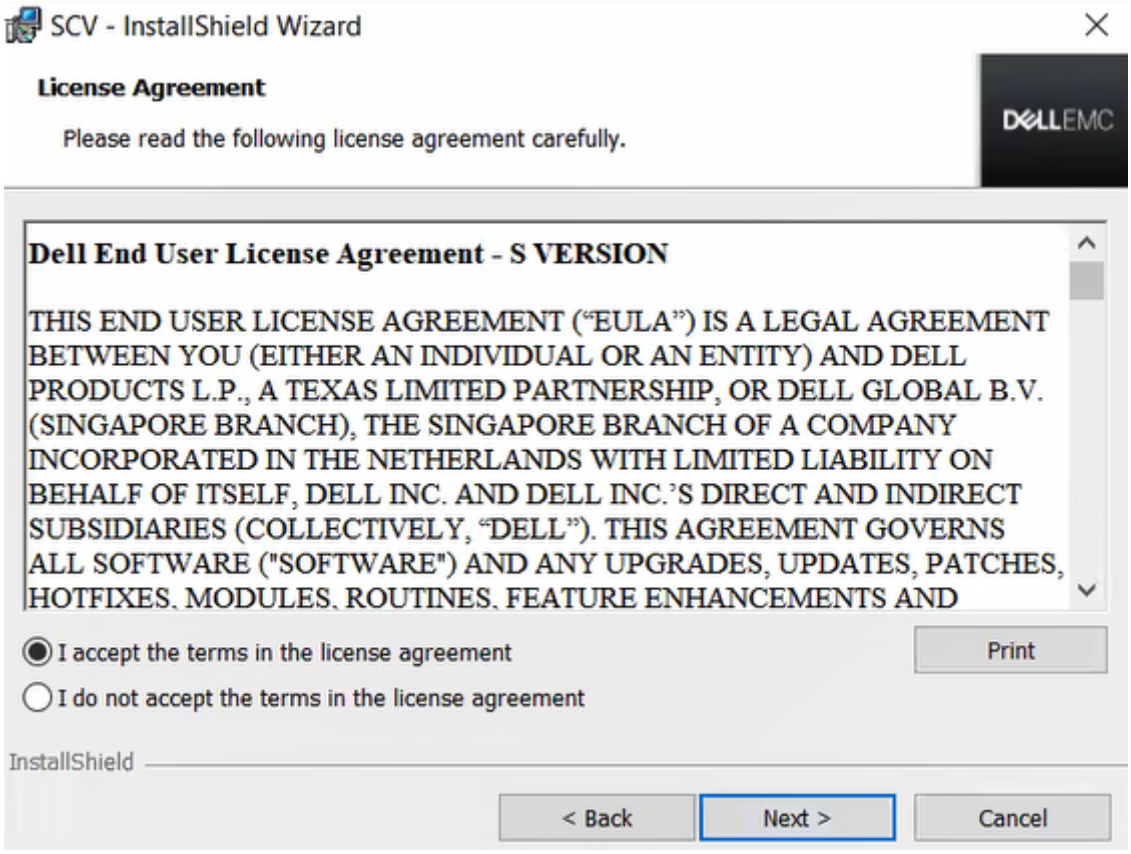


**Figure 16. License Agreement for SCVApp**

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

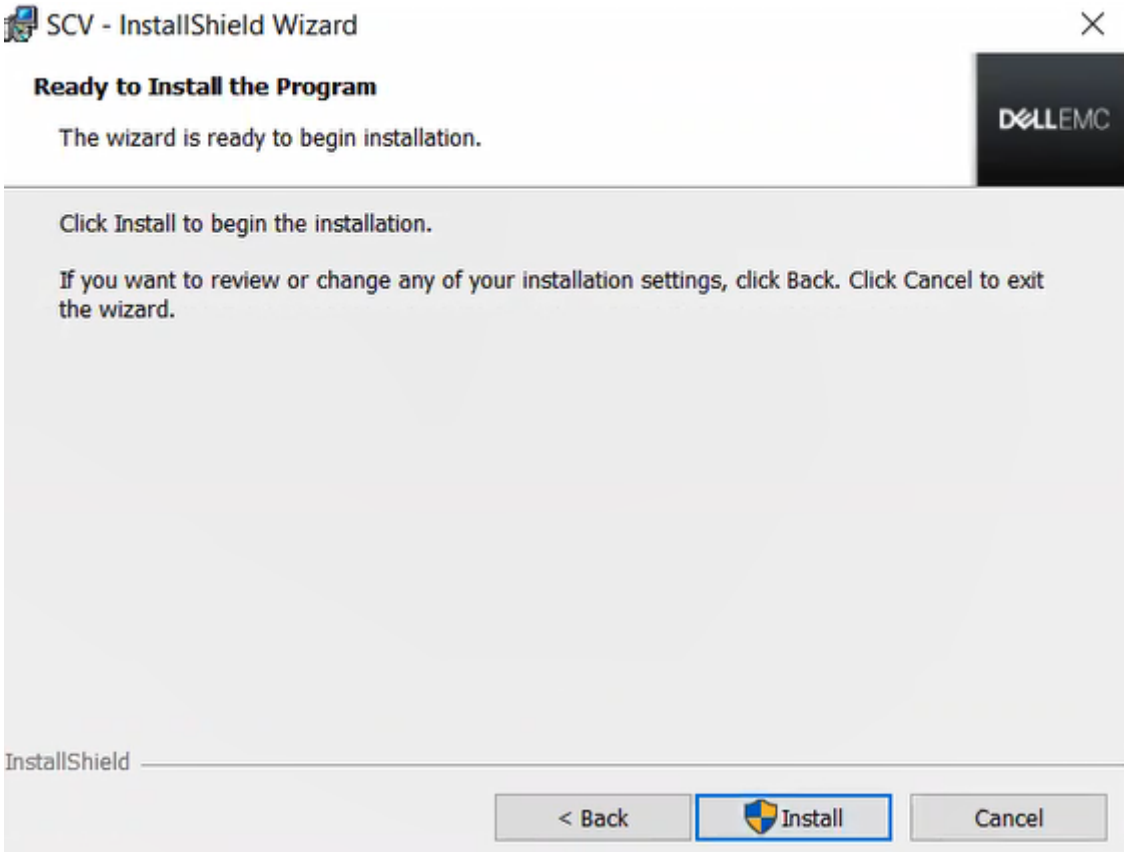


**Figure 17. Ready to install SCVApp**

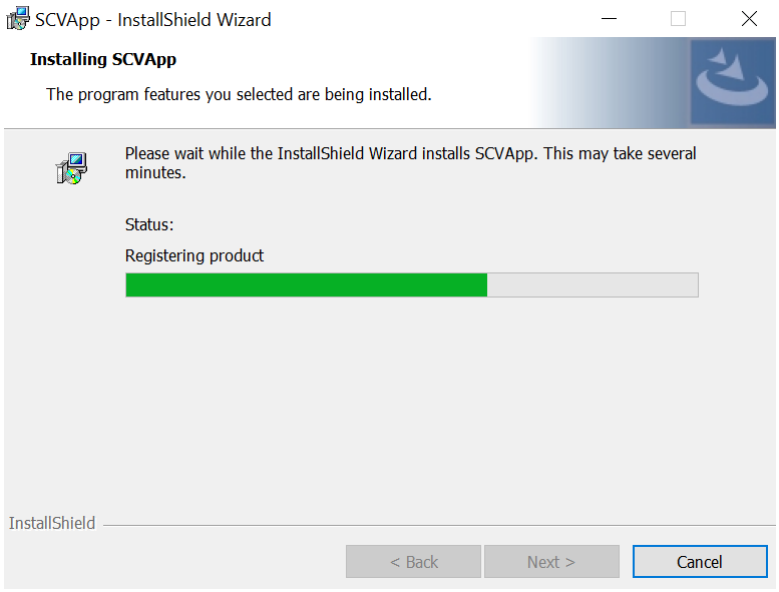


**Figure 18. Installing SCVApp**

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

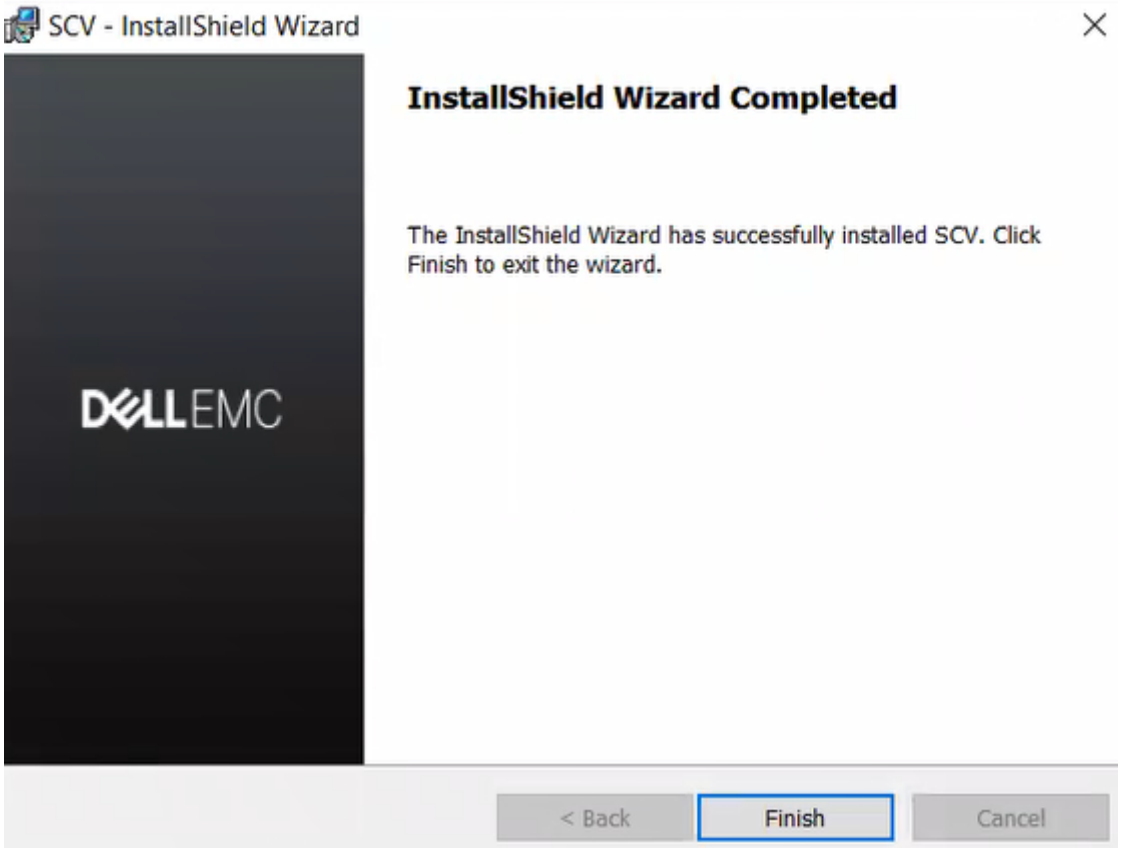


**Figure 19. SCVApp installation complete**

# 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.' .

**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 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 performing the `scv validatesysteminventory` command with `-d` option, if the directory path length exceeds 150 characters.

```
X:\Windows\System32>scv validatesysteminventory
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "R3V2040" matches Certificate: Match
Validating System Inventory: Match
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_R3V2040_2022_04_26_13_14_37.log
---------------------------------------------------------------------
```

**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:\Program Files\DELL\SCVTools>scv validatesysteminventory

Downloading SCV Factory Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "S3S5509" matches Certificate: Match
Validating System Inventory: Mismatch
---------------------------------------------------------------------
Mismatch Inventory Summary
---------------------------------------------------------------------
Network 12: Mismatch
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_S3S5509_2022_03_11_21_09_49.log
---------------------------------------------------------------------
```

**Figure 21. Validation and result is unsuccessful**

```
Network 12: Mismatch
Expected:
{
        "certificate_identifier" : "NIC.Embedded.2-1-1",
        "hw_version_number" : "Unknown"
        "location" : "F4:02:70:BF:8F:F5",
        "manufacturer" : "Broadcom Corp",
        "model" : "Broadcom Gigabit Ethernet BCM5720",
        "serial_number" : "Unknown",
}
Detected:
{
        "certificate_identifier" : "Unknown",
        "hw_version_number" : "Unknown"
        "location" : "Unknown",
        "manufacturer" : "Unknown",
        "model" : "Unknown",
        "serial_number" : "Unknown",
}
--------------------------------------------------------------------------------
Overall Network check Status: Mismatch
--------------------------------------------------------------------------------
```

**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

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

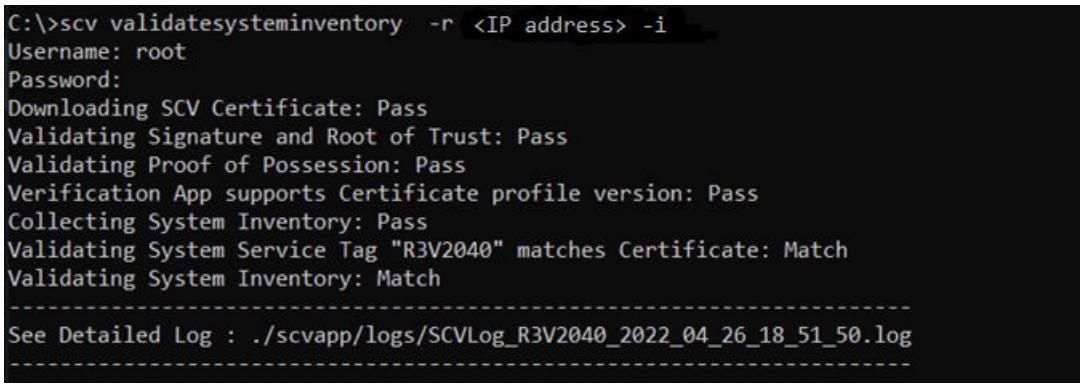


**Figure 23. Running the validation command remotely on Windows and result is successful**

**NOTE:** The above example is for running validation command in interactive mode, it does not require `-u` and `-p` parameters.

## 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> -u <iDRAC username> -p <iDRAC password>` command to start the validation process.

```
X:\Dell\scv>scv validatesysteminventory -r <IP address> -i
Username: root
Password:
Downloading SCV Factory Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "S3S5526" matches Certificate: Match
Validating System Inventory: Match
-------------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_S3S5526_2022_03_11_21_28_06.log
```

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

**NOTE:** The above example is for running validation command in interactive mode, it does not require `-u` and `-p` parameters.

# 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> -u <iDRAC username> -p <iDRAC password>` command to start the validation process.


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

**NOTE:** The above example is for running validation command in interactive mode, it does not require `-u` and `-p` parameters.

# 6

# SCV Command Details

This section provides information on some additional scv commands.

**Topics:**



## Get information on how to run SCV

**Table 1. Get more information about SCV**

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

**Output**

```
C:\SecureComponentVerification>scv help

SCV -- Secured Component Verification

Syntax:
scv <subcommand> <options> [-d <directory>]
scv <subcommand> <options> [-r <target IP> -u <username> -p <password>] [-d <directory>] [-component <component_name>] [-loca
tion <location>] [-f <file_name>]
scv <subcommand> <options> [-r <target IP> -i]

NOTE:
- "-r", "-u" and "-p" options are not required when scv is running on Host OS.
- Use the "-d" option to specify the output directory name. If not specified,
  by default the working directory is set as the output directory.
- The "-i" option allows you to interactively enter the username and password.

The detailed logs collected are available in: directory->scvapp->logs folder.
The list of available SCV subcommands:
- version
- ValidateSystemInventory
- deltaCert
- extractcert
- replacementCert
- mars
- getcertinfo

To display more information about a specific subcommand:
- scv help <subcommand>
```

# Get information about scv validatesysteminventory command

### Table 2. Get more information about SCV validatesysteminventory command

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

**Output**

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

SCV -- Secured Component Verification

Syntax:
scv ValidateSystemInventory [-r <target IP> -u <username> -p <password>] [-d <directory>] [--enforceorder]
scv ValidateSystemInventory [-d <directory>] [--enforceorder] [-r <target IP> -i]

NOTE:
- "-r", "-u" and "-p" options are not required when scv is running on Host OS.
- Use the "-d" option to specify the output directory name. If not specified,
  by default the working directory is set as the output directory.
- "--enforceorder" option indicates to additionally compare the component slot location along with the serial number.
- The "-i" option allows you to interactively enter the username and password.

The detailed logs collected are available in: directory->scvapp->logs folder.
Description:
Downloads SCV factory certificate,
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 3. Validating a specific inventory remotely

| | |
|---|---|
| **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> -u <UserName> -p <Password>` |
| **Input** | • `-r` — IPv4/IPv6 address<br>• `-u`— User name<br>• `-p`— Password |

**Output**

```
C:\Users\Administrator>scv validatesysteminventory -r <IP address> -u root -p calvin
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "GD3M8F3" matches Certificate: Match
Validating System Inventory: Match
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_GD3M8F3_2022_06_17_09_21_10.log
---------------------------------------------------------------------
```

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

**Table 4. Validating inventory by using a specific port**

| | |
|---|---|
| **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> -u <UserName> -p <Password>` |
| **Input** | • `-r` — IPv4/IPv6 address<br>• `-u`— User name<br>• `-p`— Password |

# Ensuring component location match and validating inventory

**Table 5. Ensuring component location match**

| | |
|---|---|
| **Description** | Use the following command to ensure that the component location matches while validating the inventory.<br>**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 <IP address> -u root -p calvin --enforceorder
Downloading SCV Certificate: Pass
Validating Signature and Root of Trust: Pass
Validating Proof of Possession: Pass
Verification App supports Certificate profile version: Pass
Collecting System Inventory: Pass
Validating System Service Tag "GD3M8F3" matches Certificate: Match
Validating System Inventory: Match
---------------------------------------------------------------------
See Detailed Log : ./scvapp/logs/SCVLog_GD3M8F3_2022_06_17_09_18_03.log
---------------------------------------------------------------------
```

# Get SCV Version

**Table 6. Get version of SCV**

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

**Output**

```
C:\Users\Administrator>scv version
SCV version 1.5 (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 7. Displaying or redirecting certificate identifier value**

| | |
|---|---|
| **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> -u <UserName> -p <Password> -component <Component Name> -l <Location> -f <File Name>` |
| **Input** | • `-r` — IPv4/IPv6 address<br>• `-u` — User name<br>• `-p` — Password<br>• `-component` — Component Name<br>• `-l` — Location<br>• `-f` — File Name |

**Output**

```
C:\Program Files\DELL\SCVTools>scv extractcert -r <IP address> -u root -p calvin -component iDRAC -location 1
Downloading SCV Certificate: Pass
Extracting Certificate Identifier: Pass
MIICVTCCAfugAwIBAgIIAwAAAAxQPMwCgYIKoZIzj0EAwIwdTELMAkGA1UEBhMCQ04xETAPBgNVBAgMCFNoYW5naGFpMREwDwYDVQQHDAhTaGFuZ2hhaTERMA8GA1UECgwISW52ZW50ZWMxDTALBgNVBAsMBFBST0QxHjAcBgNV
BAMMFTBJVkMwMC1DRTBDLTEwNUUtNjgyNjAeFw0yMjA3MDUxMzU2NDJaFw00MTA5MDMxMzU2NDJaMHExCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEGA1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMx
DjAMBgNVBAsMBUlEUkFDMRowGAYDVQQDDBFlYzoyYTo3MjozNjoxMjpkODBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABElv0GZsBbrNCmRwwHVbWXBhp13lmqPtiUOqIB0OVr/9rTN66pSZpuNeoeQH3INnuy/x95MML7rM5HOG
UBuG2xmjeTB3MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUYVqWFIGsWmAmri7T2UAx9QcnAu8wHwYDVR0jBBgwFoAU00ES2C0yiFfSPYXvc8lVHMrWGDEw
CgYIKoZIzj0EAwIDSAAwRQIgfcoqKl5UwmmPM5akHJXzz4UvQZye7wOS8+f49eD02TACIQDTyvuShyr4lI1YAWf9qqg88xmkJvuQ0C/yN5u7JinYFw==
```

**Figure 26. Displaying certificate identifier value on console**

```
C:\Program Files\DELL\SCVTools>scv extractcert -r <IP address> -u root -p calvin -component iDRAC -location 1 -f abc.crt
Downloading SCV Certificate: Pass
Extracting Certificate Identifier: Pass
```

**Figure 27. Writing certificate identifier value into a file**

# 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 8. Getting information about mars**

| Synopsis | scv help mars |
|---|---|
| Output | scv help mars<br><br>SCV -- Secured Component Verification<br><br>Syntax:<br><br>scv mars [certzipfile] [outputfolderpath]<br><br>Example : scv mars ./Marscert.zip ./ scvapp/out/<br><br>[certzipfile] : Is a path of zipfile which has contain the certificates .<br><br>[outputfolderpath] : Is optional, By default path will be ./scvapp/out/<br><br>Description:<br><br>Extract the mac addresses from the Network and iDRAC component .<br><br>Mars report will generate with file name mar_ + timestamp .<br><br>NOTE: By default the working directory is set as the output directory. |

**Table 9. Running mars command to extract mars details and create the marsreport.csv file**

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

**Table 9. Running mars command to extract mars details and create the marsreport.csv file (continued)**

| | |
|---|---|
| | FYRLCW3,NIC.Embedded.2-1-1,C8:4B:D6:98:93:53<br><br>FYRLCW3,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.

# 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%20A00.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 10. 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. |

# 11

# Getting help

**Topics:**



## 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.
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.