



DELL PowerEdge C4140 Secured Component Verification User Guide

[Home](#) » [Dell](#) » DELL PowerEdge C4140 Secured Component Verification User Guide 



Rev. A00
November 2022
SCV 1.6 Release Notes

Contents

- [1 Product Description](#)
- [2 Important notes](#)
- [3 Environment and System Requirements](#)
- [4 Documents / Resources](#)
 - [4.1 References](#)

Product Description

Topics:

- Revision History
- New features
- Resolved Issues
- Known issues—To be fixed in future releases
- Limitations
- Environment and System Requirements
- Installation and Upgrade considerations
- Where to Get Help

Secured Component Verification (SCV) is a supply chain assurance offering that enables you to verify that the Power Edge 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.

Release date

November 2022

Revision History

- SCV 1.0
- SCV 1.5.0
- SCV 1.5.1

New features

- Support for RHEL 9.0

Resolved Issues

Known issues—To be fixed in future releases

Table 1. SCV displays generic message for missing License and Invalid credentials

Description	SCV operation may fail with the generic error message “Unable to complete the requested operation because of internal issues. Wait for sometime and retry the operation.”, if credentials provided are invalid or the required license is missing.
Workaround	N/A
Systems Affected	All systems supported by this release.
Tracking number	243773

Important 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 Flex Address 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.
- When there are no devices present for a component, the SCV inventory displays one ‘Unknown’ entry .

Limitations

- 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.

Environment and System Requirements

License Requirements

- Secured Component Verification License

Supported systems

- PowerEdge C4140
- PowerEdge C6420
- PowerEdge C6520
- PowerEdge C6525
- PowerEdge M640
- PowerEdge MX7000 Chassis
- PowerEdge MX740c
- PowerEdge MX750c
- PowerEdge MX840c
- PowerEdge R240
- PowerEdge R250
- PowerEdge R340
- PowerEdge R350
- PowerEdge R440
- PowerEdge R450
- PowerEdge R540
- PowerEdge R550
- PowerEdge R640
- PowerEdge R6415
- PowerEdge R650
- PowerEdge R6515
- PowerEdge R6525
- PowerEdge R740
- PowerEdge R740xd
- PowerEdge R740xd2
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge R750
- PowerEdge R750xa
- PowerEdge R7515
- PowerEdge R7525
- PowerEdge R940
- PowerEdge R940xa

- PowerEdge T140
- PowerEdge T150
- PowerEdge T340
- PowerEdge T350
- PowerEdge T440
- PowerEdge T550
- PowerEdge T640
- PowerEdge XE2420
- PowerEdge XE8545
- PowerEdge XR11
- PowerEdge XR12
- PowerEdge XR2
- Dell EMC XC Core XC450
- Dell EMC XC Core XC650
- Dell EMC XC Core XC6520
- Dell EMC XC Core XC740xd2
- Dell EMC XC Core XC750
- Dell EMC XC Core XC750xa
- Dell EMC XC Core XC7525
- Dell EMC XC Core XC940 System
- Dell EMC XC Series XC940 Appliance
- Dell EMC XC Core XCXR2
- OEMR R240
- OEMR R340
- OEMR R440
- OEMR R450
- OEMR R540
- OEMR R550
- OEMR XL R640
- OEMR R650
- OEMR R650xs
- OEMR R6515
- OEMR R6525
- OEMR R740xd
- OEMR R740xd2
- OEMR R750
- OEMR R750xa
- OEMR R750xs
- OEMR R7515
- OEMR R7525
- OEMR R840
- OEMR R940xa
- OEMR T140

- OEMR T150
- OEMR T340
- OEMR T350
- OEMR T440
- OEMR T550
- OEMR XL T640
- OEMR XR11
- OEMR XR12
- VxRail E660F
- VxRail S670

Supported managed server operating systems

- Microsoft Windows
 - Server 2022 Essentials
 - Server 2022 Standard
 - Server 2022 Datacenter
 - Server 2019 Essentials
 - Server 2019 Standard
 - Server 2019 Datacenter
 - WinPE 10
- Linux
 - RHEL 9.0
 - RHEL 8.6

Installation and Upgrade considerations

For information about installing SCV, see the SCV Reference Guide available at <https://www.dell.com/scvmanuals>

Where to Get Help


Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues, see <https://www.dell.com/contactdell>.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.

Copyright

© 2022 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc.

or its subsidiaries. Other trademarks may be trademarks of their respective owners.

	<p>DELL PowerEdge C4140 Secured Component Verification [pdf] User Guide</p> <p>PowerEdge C4140 Secured Component Verification, PowerEdge C4140, Secured Component Verification, Component Verification, Verification</p>
--	--

References

- [Support | Dell US](#)
- [Support for Secured Component Verification \(SCV\) | Documentation | Dell US](#)