



Symantec™ Data Center Security: Server Advanced 6.10.3 Release Notes



Table of Contents

Documentation Legal Notice.....	3
Release Notes of DCS:SA 6.10.3.....	4
About Data Center Security: Server Advanced 6.10 or later.....	4
What's new in DCS:SA 6.10.3.....	5
Supported OS Versions of DCS:SA Agent.....	6
About Firewalls in DCS:SA 6.10 or later.....	8
Fixed Issues of DCS:SA 6.10.3.....	9
Frequently Asked Questions.....	9
Symantec Information Resources.....	11
How to file a feature request.....	14
System Requirements for DCS:SA 6.10 or later.....	15
Hardware Requirements for Fresh Installation.....	15
Software Requirements for Fresh Installation.....	17
Hardware Requirements for the Agent.....	17
Hardware Requirements to Upgrade.....	18
Software Requirements to Upgrade.....	19

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Release Notes of DCS:SA 6.10.3

The release notes of Data Center Security: Server Advanced 6.10.3 introduces you to the release items. The Release Notes contain the what's new features of Data Center Security: Server Advanced 6.10.3, the system requirements required to install or upgrade, the supported agent OS versions, the known issues, the fixed issues, and the FAQs.

The release notes contains the following topics:

- [What's new in DCS:SA 6.10.3](#)
- [Supported OS Versions of DCS:SA Agent](#)
- [System Requirements for DCS:SA 6.10 or later](#)
- [Fixed Issues of DCS:SA 6.10.3](#)
- [Frequently Asked Questions](#)
- [Symantec Information Resources](#)
- [How to file a feature request](#)

About Data Center Security: Server Advanced 6.10 or later

Data Center Security: Server Advanced provides comprehensive runtime server monitoring and protection enabling micro-segmentation, administrator privilege de-escalation, patch mitigation, and protection against zero-day threats in private and public cloud data centers.

Data Center Security: Server Advanced also provides policy-based security and compliance to workloads and modern applications such as dockers, containers, and more. Policies such as the Intrusion Prevention policies (IPS) with hardening capabilities and the Intrusion Detection policies (IDS) operate across a broad range of platforms and applications.

Data Center Security: Server Advanced provides the following features:

- A policy-based host security agent for monitoring and protection.
- Proactive attack prevention using the least privilege containment approach.
- A centralized management environment for enterprise systems that contain Windows, UNIX, and Linux workloads.

The features of DCS:SA are as follows:

- Application control and isolation
 - Prevents zero-day attacks
 - Performs whitelisting of applications
 - Protects memory and processes
 - Mitigates vulnerabilities of the applications
- System Controls
 - Protects and hardens your heterogeneous virtual and physical server environments
 - Restricts operating system behavior using policy-based least privilege access control
 - Pre-builds security policies monitor and prevent tampering of critical system changes
 - Locks down binaries and operating system configuration settings
- Network Controls

-
- Reduces attack surface
 - Granular network controls help organizations control the flow of traffic at application or host level
 - Shares common network rules across diverse operating systems
 - Limits intruder presence
 - Malware Protection
 - Uses AI powered technologies such as file reputation and machine learning algorithms
 - Uses signature-based threat detection and sophisticated scanners
 - Audit and Alerting
 - Performs real-time monitoring of critical file changes
 - Identifies unauthorized configuration changes and system access
 - Notifies early visibility and response

What's new in DCS:SA 6.10.3

Review the new features and enhancements of Data Center Security: Server Advanced 6.10.3 before you start upgrading or installing the product.

The DCS:SA 6.10.3 release comprises the following features:

- [New Features of DCS:SA 6.10.3](#)
- [Enhancements in DCS:SA 6.10.3](#)

New Features of DCS:SA 6.10.3

- **Simplified Application Control Workflow of Discovered Applications**

Data Center Security: Server Advanced introduces a provision to manage and isolate discovered applications of an asset from the **Discovered Items > Applications** page of the Management Console. Isolation of applications is similar to sandboxing, which involves configuring the security levels of restrictions on the selected applications from the console. This configuration through the console inherently overrides the already existing application rules of the IPS policies that are applied on the applications. This feature is supported for both the Windows and Linux assets of DCS:SA.

Enhancements in DCS:SA 6.10.3

- On the **Investigate** page, for the Custom Filter, a new field called **Event ID** has been added.
- On exporting a policy as a zip, the associated policy tag is also exported. If you import the policy to a server that already contains the same policy tag, the tag is reapplied to the policy. However, if you import the policy to a server that does not contain the tag, then no tag is applied to the policy.
- The newly imported policies are now highlighted on the **Policies** grid of the console. The scroll bar navigates automatically to the highlighted new policies of the grid.
- A new filter called the **Security Group Categories** has been added for the Quick Filter of the **Assets > Agents** page.
- A new column called the **Local Address** has been added on the **Assets > Agents** page of the console that displays the local IP address of an asset.
- It is now possible to export more than one policies from the **Policies** page using the **Export as Zip** option.
- The **Investigate** page has the provision to display up to **40000** events on the grid if selected in the drop-down that displays at the bottom-right corner of the page.
However, the loading time of the events can increase due to the large volume of data that is processed to display.
- A search box has been added in the **Assign Security Group** dialog box for the **Assets** and **Policies** pages of the console.
- In the **Investigate > Events** page of the console, a new operator called **Is one of** has been added for the **Custom Filter**.

Supported OS Versions of DCS:SA Agent

Learn about the supported OS versions of DCS:SA agents in Data Center Security: Server Advanced 6.10 or later.

Data Center Security: Server Advanced supports DCS:SA agents of the following operating systems:

- Windows Agent
- Linux Agent
- AIX Agent
- Solaris Agent

For the latest supported OS versions and flavors of Windows, AIX, Solaris, and Linux agents download the Platform Feature Matrix from the **Related Documents** section of the [Online Help](#).

Latest Supported OS Kernel Versions

For the latest OS kernels supported by the Data Center Security: Server Advanced agents, refer to the [Online Linux kernel support portal](#).

Supported Windows Operating Systems for DCS:SA Windows Agent 6.10.1

The supported Windows operating systems for Data Center Security: Server Advanced Windows agent 6.10.1 are as follows:

Operating System	Architecture	Support for IDS	Support for IPS
Windows 2025	x86_64	✓	✓
Windows 2022	x86_64	✓	✓
Windows 2019	x86_64	✓	✓
Windows 2016	x86_64	✓	✓
Windows 2012 R2	x86_64	✓	✓
Windows 2012	x86_64	✓	✓
Windows 10	x86 x86_64	✓	✓
Windows 11	x86_64	✓	✓

Supported Windows Operating Systems for DCS:SA Windows Agent 6.9.3

The supported Windows operating systems for Data Center Security: Server Advanced Windows agent 6.9.3 are as follows:

Operating System	Architecture	Support for IDS	Support for IPS
Windows 2025	x86_64	✓	✓
Windows 2022	x86_64	✓	✓
Windows 2019	x86_64	✓	✓
Windows 2016	x86_64	✓	✓
Windows 2012 R2	x86_64	✓	✓
Windows 2012	x86_64	✓	✓
Windows 2008 R2	x86_64	✓	✓
Windows 2008	x86 x86_64	✓	✓

Operating System	Architecture	Support for IDS	Support for IPS
Windows 10	x86 x86_64	✓	✓
Windows 11	x86_64	✓	✓

Supported Linux Operating Systems for DCS:SA Linux Agent 6.10.1

The supported operating systems of Data Center Security: Server Advanced Linux agent 6.10.1 are as follows:

Operating System	Architecture	Support for IDS	Support for IPS	Antimalware support
Alma Linux 8 .5 to 8.10	x86_64	✓	✓	✓
Amazon Linux 2023	x86_64	✓	✓	✓
Amazon Linux 2	x86_64	✓	✓	✓
Amazon Linux 2023	aarch64	✓		
RHEL 10 to RHEL 10.1	x86_64	✓	✓	✓
RHEL 10	aarch64	✓		
RHEL /Rocky Linux /Oracle Linux 9.0 to 9.7	x86_64	✓	✓	✓
RHEL 9.0 to 9.3	aarch64	✓		
RHEL /Rocky Linux /Oracle Linux 8.0 to 8.10	x86_64	✓	✓	✓
RHEL 8.4 to 8.10	aarch64	✓		
CentOS /RHEL /Rocky Linux/ Oracle Linux 7.0 to 7.9	x86_64	✓	✓	✓
SLES 15 SP0 to SP7	x86_64	✓	✓	✓
Ubuntu 24.04 LTS	x86_64	✓	✓	✓
Ubuntu 22.04 LTS	x86_64	✓	✓	✓
Ubuntu 20.04 LTS	x86_64	✓	✓	✓
Ubuntu 18.04 LTS	x86_64	✓	✓	✓

NOTE

Make sure that you download the latest policy pack.

Supported Linux Operating Systems for DCS:SA Linux Agent 6.10.0

The supported operating systems of Data Center Security: Server Advanced Linux agent 6.10.0 are as follows:

Operating System	Architecture	Support for IDS	Support for IPS	Antimalware support
Alma Linux 8 .5 to 8.10	x86_64	✓	✓	✓
Amazon Linux 2023	x86_64	✓	✓	✓
Amazon Linux 2	x86_64	✓	✓	✓
Amazon Linux 2023	aarch64	✓		
RHEL 10 to RHEL 10.1	x86_64	✓	✓	✓
RHEL /Rocky Linux /Oracle Linux 9.0 to 9.7	x86_64	✓	✓	✓

Operating System	Architecture	Support for IDS	Support for IPS	Antimalware support
RHEL 9.0 to 9.3	aarch64	✓		
RHEL /Rocky Linux /Oracle Linux 8.0 to 8.10	x86_64	✓	✓	✓
RHEL 8.4 to 8.10	aarch64	✓		
CentOS /RHEL /Rocky Linux/ Oracle Linux 7.0 to 7.9	x86_64	✓	✓	✓
SLES 15 SP0 to SP7	x86_64	✓	✓	✓
Ubuntu 24.04 LTS	x86_64	✓	✓	✓
Ubuntu 22.04 LTS	x86_64	✓	✓	✓
Ubuntu 20.04 LTS	x86_64	✓	✓	✓
Ubuntu 18.04 LTS	x86_64	✓	✓	✓
Ubuntu 16.04 LTS	x86_64	✓	✓	✓

NOTE

Make sure that you download the latest policy pack.

About Firewalls in DCS:SA 6.10 or later

Configure the firewall settings to support communications in Data Center Security: Server Advanced by opening ports or by specifying the trusted services.

NOTE

All the ports have default settings that you can change during installation.

You should note the following about using firewalls with Data Center Security: Server Advanced:

- Make sure your firewall allows traffic from the Management Server to the MS SQL Server computer on the UDP port **1434**. The default database TCP port that is used by the Data Center Security: Server Advanced instance is **1433**. The Management Server uses the UDP port to query MS SQL Server and finds the port used by the Data Center Security: Server Advanced instance. Once the MS SQL Server computer returns the port for the Data Center Security: Server Advanced instance, the Management Server then connects to the MS SQL instance using that port.
- If you are using the bulk log transfer feature and have host-based firewall that allows specific programs, then allow the **bulklogger.exe** and **SISIPSService.exe** to access the Internet. The Data Center Security: Server Advanced agent is provided by the bulklogger.exe. The bulklogger.exe program uses the same ports as SISIPSService.exe. If you do not use the bulk log transfer feature, bulklogger.exe will not run.

The following table lists the services that you can permit to send and receive traffic through your firewalls:

Component	Service	Traffic
Management Console	sdcs-management-console- <buildnum>.msi	Communicates with the Management Server using remote TCP ports 4443 .
Management Server	sdcs-management-server- <buildnum>.msi	Communicates with the database by using local TCP ports 4443 . Communicates with remote production SQL servers using the remote TCP port that the SQL server uses for the server instance.
Communication Server	sdcs-communication-server- <buildnum>.msi	Port 443 The Communication Server communicates with the agent through the port 443 .

Agent	sisipsdaemonbulklogger.exe	Communicates with the Communication Server using local TCP port 2222, and remote TCP port 443 .
-------	----------------------------	--

Fixed Issues of DCS:SA 6.10.3

Review the issues that are fixed in Data Center Security: Server Advanced 6.10.3.

The fixed issues of Data Center Security: Server Advanced 6.10.3 are as follows:

Table 1: Fixed issues of Data Center Security: Server Advanced 6.10.3

Issue Description	Status
The Edit Rules window of the IPS policies displays partial UI elements.	This issue has been fixed.
It is not possible to save the Windows App Control policy after entering a PowerShell argument.	This issue has been fixed.
For the Process Assignment events displayed on the Investigate > Events page, if Host Name is used as a filter, the arguments field under the parent process is blank. The arguments field is populated when the Host Name is not used as a filter.	This issue has been fixed.
An alert rule configured with more than one email address when imported to DCS:SA 6.10 or later allows you to edit only one email address and grays out the other email addresses.	This issue has been fixed.
The option to export more than one policy at a given time as a zip from the Policies page of the console is missing.	This issue has been fixed.
An empty string displays in the "--" format indicating the delay between the event generation and the event display or posting time.	This issue has been fixed.
The calendar in the Policy Violations wizard for the Retrieve violations from custom date range setting of an IPS policy displays an incorrect day of the week in the date picker.	This issue has been fixed.
After the description of a policy is modified and saved, the Activity History for the policy does not display the full text due to character limitation in the Description column.	This issue has been fixed.
The syslog events data does not display in the JSON format for Splunk.	This issue has been fixed.
On deploying the IPS policy on 6.10.2 Windows standalone agent with <i>sisipsconfig -P</i> , the policy fails with status code 200.	This issue has been fixed.

Frequently Asked Questions

Get answers for the FAQs on Data Center Security: Server Advanced 6.10.

- Can I enroll the existing Data Center Security: Server Advanced 6.9.3 Agents or earlier versions with the Data Center Security: Server Advanced 6.10 Management Server?
Yes, Data Center Security: Server Advanced 6.9.3 Agents can be enrolled with the Management Server of Data Center Security: Server Advanced 6.10. You must execute the following commands to ensure that the communication is established successfully:
 - Connect to the Communication Server

```
su - sisips -c "./sisipsconfig.sh -h <FQDN or IP address of the CommunicationServer >"
```

- Copy and import your certificate

```
su - sisips -c"./sisipsconfig.sh -c <certificate path>"
```

- Test the Symantec Agent connection with the Communication Server

```
su - sisips -c"./sisipsconfig.sh -t" to test connection
```

2. Will the Data Center Security: Server Advanced 6.9.3 or earlier versions of Java Console communicate with the Data Center Security: Server Advanced 6.10 Management Server?

No. The Java Console is deprecated in Data Center Security: Server Advanced 6.10, and replaced with the new Management Console.

3. What token does DCS:SA 6.10 Management Server use for authentication?

The Data Center Security: Server Advanced 6.10 Management Server uses the JWT authentication token. You must update the existing automation scripts to work with the latest Management Server.

4. In Data Center Security: Server Advanced 6.10 I cannot see separate tabs for Prevention, Detection, and the Config policies. How can I find my policies now?

In Data Center Security: Server Advanced 6.10, you can use the policy filters displayed for the **Quick Filters > Policy Type** option on the **Policies** page of the console.

5. What will happen to DCS:SA 6.9.x policy folder hierarchical structure after upgrading to DCS:SA 6.10?

After the successful upgrade to 6.10, every folder in the folder structure becomes a tag. The policy is automatically tagged with every tag that represents the folder in the policies hierarchy.

For example, you have a folder called **Windows\Manufacturing – Platform\EAST** and a policy called **sym_win_hardended_policy** in DCS:SA 6.9.3. You then upgrade to Data Center Security: Server Advanced 6.10.

After you upgrade, three tags will be created, and applied to the **sym_win_hardended_policy**, which are as follows:

- Windows
- Manufacturing – Platform
- EAST

6. Can I use my existing Data Center Security: Server Advanced 6.9.x policies in Data Center Security: Server Advanced 6.10?

Yes, you can view and use all the IDS and IPS policies of Data Center Security: Server Advanced 6.9.3 or 6.9.2 after upgrading to the Data Center Security: Server Advanced 6.10 setup. However, if you want to protect the Management Server or the Communication Server then you must use the following policies of the Data Center Security: Server Advanced 6.10 only.

- SDCSS Manager Workload Protection policy
- SDCSS Monitor IDS policy

7. Can I search for a specific custom rule in my policies?

Yes, you can search for specific custom rules by their name, settings, values used, or section names when editing the IDS or IPS policies. Add or edit custom rules on the **Advanced Policy Settings > My Custom Rules** option of the policy on the **Policies** page of the console.

8. How can I add and view additional columns on the Assets, Policies, and the Events grid?

A **Column Chooser** icon displays on the right-most corner of the Assets, Policies, and Events page. Select the columns that you want to display on the Assets, Policies, or Events grid from the **Column Chooser**.

9. Can Quick Filter and Custom Filter be combined for search operation?

Yes, you can create and run queries combining the fields selected from the Quick Filter and the Custom Filter.

10. What will happen to DCS:SA 6.9.x policy folder hierarchical structure after upgrading to DCS:SA 6.10?

After the successful upgrade to 6.10, every folder in the folder structure becomes a tag. The policy is automatically tagged with every tag that represents the folder in the policies hierarchy.

For example, you have a folder called **Windows\Manufacturing – Platform\EAST** and a policy called **sym_win_hardended_policy** in DCS:SA 6.9.3. You then upgrade to Data Center Security: Server Advanced 6.10.

After you upgrade, three tags will be created, and applied to the **sym_win_hardended_policy**, which are as follows:

- Windows
- Manufacturing – Platform
- EAST

11. Can I save my filters to access them later?

In Data Center Security: Server Advanced 6.10 you cannot save the filters, but this functionality will be available in the future release.

Symantec Information Resources

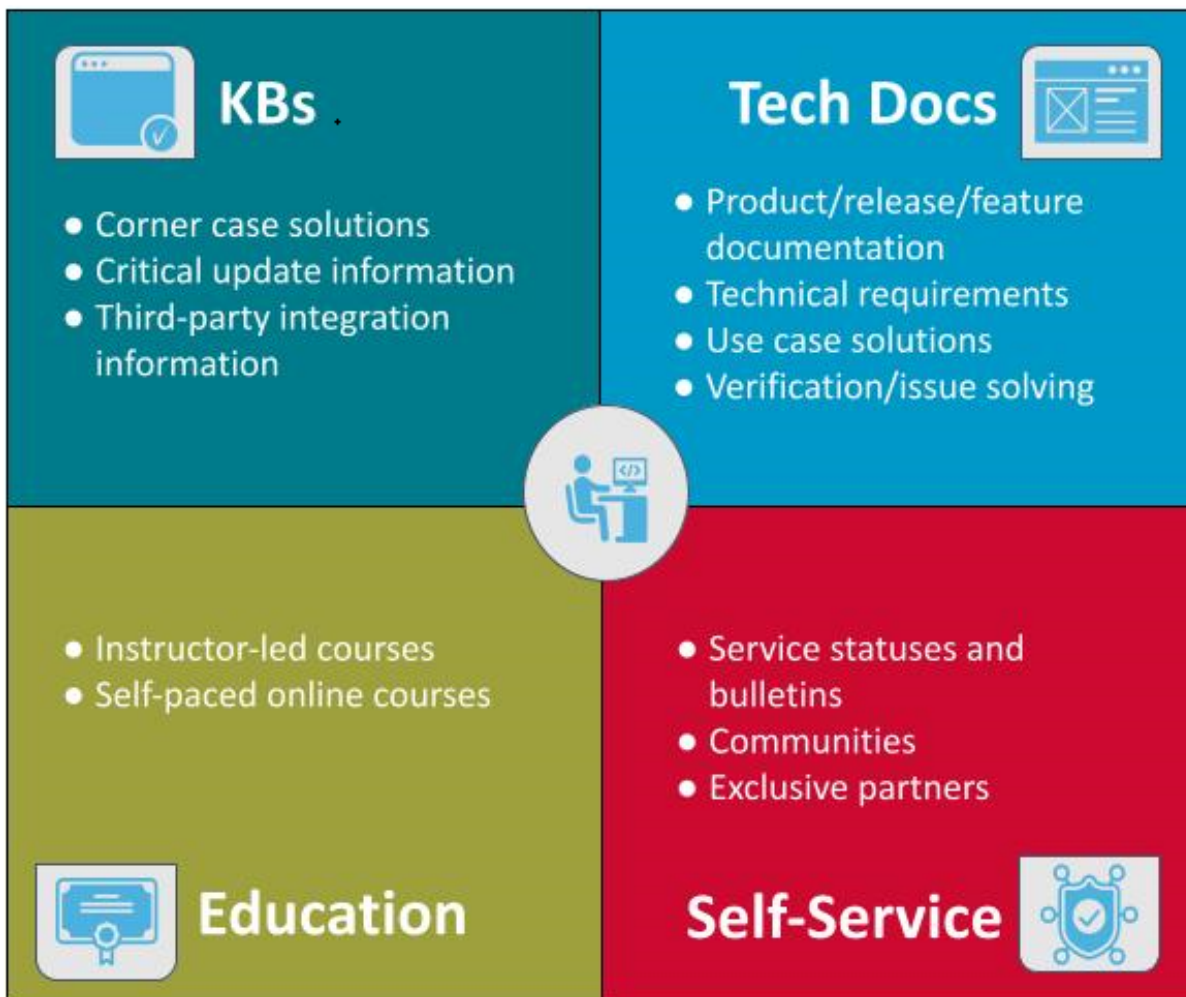
Access information, self-help, and support resources for Broadcom Software and Data Center Security: Server Advanced.

This topic provides the following information:

- Describes information types that Broadcom Enterprise Security Software (Carbon Black and Symantec products) provides.
- Provides Data Center Security: Server Advanced- specific information resource descriptions and link.

Broadcom Information Resources

Broadcom strives to provide detailed solution information to partners and customers. The following quadrant diagram defines the high-level information types.



Broadcom Information Resource Links to High-level Pages

Table 2: Broadcom Websites

Type of information	Web Address
Support Knowledge Base Articles	Create cases and find knowledge base articles, downloads and trial software, entitlement and licensing information, Security Advisories, and announcements and legal notices. https://support.broadcom.com/
Trainings Instructor-led Training	Access the training courses, the eLibrary, and more. Education Services
Community Forums	Check the catalog for the recent Broadcom Enterprise Security Group course offering. Community Forum

Type of information	Web Address
Virus and other threat information and updates	Provides access to the Virus Encyclopedia, which contains information about all known threats, information about hoaxes, and access to white papers about threats Symantec Security Center
Product Details Page	Data Center Security: Server Advanced Product Page
Information on product updates for Partners	Partner Portal
Related Documents	The list of PDFs of Data Center Security: Server Advanced is available as a zip in the Related Documents section of the Online Help .

About Tech Docs

What Are Tech Docs?

- The Broadcom Tech Docs Portal provides product documentation, including deployment/installation, use cases, how-to solutions, reference, and troubleshooting information.
- The documentation is intended to describe and explain the functionality, usage, and configuration steps for Data Center Security: Server Advanced solutions. A few topics include integration information with other Symantec or third-party technologies.
- Tech Docs are updated with every new and enhanced feature releases of Data Center Security: Server Advanced.
- Tech Doc search queries do include results for KB articles.

Provide Feedback

At the bottom of each Tech Doc topic, you can enter feedback using the Content feedback and comments link. The link is intended only for help content feedback. For technical issues, contact Broadcom Support. The link displays a form. Submitted forms go to the Broadcom Information and Courseware Development team. If you request a response, you receive a reply when your feedback is addressed.

NOTE

The feedback form is intended for customer and Catalyst/Partners use. Broadcom personnel who have feedback are asked to complete a different form. Contact ICD.

About the Knowledge Base

What is a KB?

- A KB is intended to provide problem-solving steps for customer issues and to address questions about time-sensitive problems or critical service updates.
- KB articles are typically updated more frequently than Tech Docs. KB articles are often removed when an issue is resolved through product or Tech Doc updates.
- The KB search does not include Tech Docs. However, in the Support Portal you can optionally search multiple sources, including KB articles and Tech Docs.

To search the **Support** site:

1. Access the [site](#)
2. In the Knowledge section, click **View All**.
3. On the search page, use the filters to search for the specific product.
4. Enter terms in the field and click **Search**.
5. Refer to the [Broadcom Article](#) for more details about advanced and customized searches.

-
6. Save searches.
 - Click the **Save Bookmark** (star) icon to save the current search filters. In the dialog, enter a name for the search and click **Save**.
 - Click the **Saved Bookmarks and Results** (bookmark) icon to access your saved bookmarks. To load a search, click the search name in the dialog.
 7. To search the KB with Google, limit the search by using site: *knowledge.broadcom.com*

How to file a feature request

File a feature request or create a support case for Data Center Security: Server Advanced 6.10 if you want to.

Do the following tasks to raise a feature request:

- [Open a Support case](#).
- Contact your [Broadcom partner](#). If you do not know your account manager, see the partner list.
- Call the [hotline](#) for your country.

Keep your Support Identifier or Contact ID available. When you open a case, add the following information:

- A clear description of the issue.
- Full text of any error messages.
- Screenshots capturing the issue.
- When the issue started.

System Requirements for DCS:SA 6.10 or later

Review the supported hardware and software requirements for the components and database of Data Center Security: Server Advanced 6.10 or later.

For the latest supported OS versions and flavors of Windows, AIX, Solaris, and Linux agents, download the latest **Platform Feature Matrix** from the **Related Documents** section of the [Online Help](#).

Hardware Requirements for Fresh Installation

Know the minimum hardware requirements and the recommended hardware requirements for different setups to install the Data Center Security: Server Advanced 6.10 components.

Data Center Security: Server Advanced provides workload and server security to enterprises of all sizes. You must consider multiple variables to determine your sizing and deployment needs. Careful consideration can help you to create optimum protection and serviceability.

The minimum hardware recommendations for you to plan the installation, and the hardware recommendations for different setups are as follows:

- [Minimum hardware requirements](#)
- [Hardware Recommendation for a Small Scale Setup](#)
- [Hardware Recommendation for a Medium Scale Setup](#)
- [Hardware Recommendation for a Large Scale Setup](#)
- [Failover or High Availability Recommendations](#)

The hardware requirements for the **Management Console** for all setups are as follows:

DCS Management Component	Free Disk Space	Number of CPU	Memory
Management Console	2 GB	1	2 GB

Minimum Hardware Requirements

The minimum hardware requirements to install DCS:SA 6.10 are as follows:

Installer Component	Free Disk Space	Memory	CPU
Management Server	60 GB	8 GB	4
Communication Server	60 GB	8 GB	4

Hardware Recommendation for a Small Scale Setup (50-10,000 agents)

The recommended hardware requirements to install DCS:SA 6.10 for a small scale setup is as follows:

DCS Management Components	Free Disk Space	Number of CPU	Memory	Recommended Failover Communication Servers (Optional)
Management Server	500 GB	8	16 GB	One
Communication Server	500 GB	8	32 GB	
SQL Database Server	1 TB	8	32 GB	

NOTE

The recommendation is that you deploy **one** Communication Server for a small scale setup.

Hardware Recommendation for a Medium Scale Setup (10,001 - 20,000 agents)

The recommended hardware requirements to install DCS:SA 6.10 for a medium scale setup is as follows:

DCS Management Components	Free Disk Space	Number of CPU	Memory	Recommended Failover Communication Servers (Optional)
Management Server	500 GB	8	32 GB	One
Communication Server	500 GB	8	32 GB	
SQL Database Server	1 TB	16	64 GB	

NOTE

The recommendation is that you deploy **two** Communication Servers for a medium scale setup.

Hardware Recommendation for a Large Scale Setup (20,001 - 40,000 agents)

The recommended hardware requirements to install DCS:SA 6.10 for a large scale setup is as follows:

DCS Management Components	Free Disk Space	Number of CPU	Memory	Recommended Failover Communication Servers (Optional)
Management Server	500 GB	8	32 GB	One
Communication Server	500 GB	8	32 GB	
SQL Database Server	1 TB	32	128 GB	

NOTE

The recommendation is that you deploy **four** Communication Servers for a large scale setup.

Failover or High Availability Recommendations**• API Console Failover or Redundancy**

The recommendation is to deploy a second Management Server to meet the API Server failover use case scenarios.

• Agents Failover or Redundancy

Add an additional Communication Server to the recommended setup. For example, if you are in a small scale setup, then the recommendation is to use two Communication Servers. Similarly, if you are in a medium scale setup, then you need one additional Communication Server, which is a total of two Communication Servers to cover failover use case scenarios.

NOTE

The architecture, designs, and recommendations that are provided in documentation are based on metrics from internal testing of the product. These tests are performed in an isolated environment. Implementations in production environments may result in some performance metrics that vary from the testing scenarios. These variations can alter the recommended sizing and architecture. This documentation references possible changes and modifications to Data Center Security: Server Advanced capability, functions, metrics, and features. These changes are subject to continuous evaluation and must not be considered as firm commitments by Broadcom.

Software Requirements for Fresh Installation

Data Center Security: Server Advanced 6.10 or later supports specific operating systems for installing the Management Server, Communication Server, and the Management Console.

The software requirements to install the DCS:SA components for the Production mode or the Evaluation mode are as follows:

Operating System	Management Server	Communication Server	Management Console
Windows 2016	Yes	Yes	Yes
Windows 2019	Yes	Yes	Yes
Windows 2022	Yes	Yes	Yes
Windows 2025	Yes	Yes	Yes
Windows 11	No	No	Yes

Additional software requirements for the **Production** and **Evaluation** modes of installations are as follows:

Production Mode Installation	Evaluation Mode Installation
<ul style="list-style-type: none">Microsoft SQL Server 2016 Standard with Service Pack 1 or higherWindows Installer 2.0 or higher	<ul style="list-style-type: none">Microsoft SQL Server 2022 Express.NET Framework 4.7.1Windows Installer 2.0 or higher

Hardware Requirements for the Agent

Know the minimum hardware requirements and the recommended hardware requirements for installing the Data Center Security: Server Advanced agents of different operating systems.

The hardware requirements of the DCS:SA agents of different versions are as follows:

- [Hardware Requirements of the DCS:SA Linux 6.10 Agent](#)
- [Hardware Requirements of the DCS:SA 6.9.3 Agent](#)

Hardware Requirements of the Linux Agent 6.10 or later and Windows Agent 6.10.1 or later

The hardware requirements to install a DCS:SA Linux 6.10 Agent are as follows:

- 1 GB free disk space (all Linux platforms)
- 256 MB RAM
- Sun SPARC™ 450 MHz
- SPARC64
- IBM PowerPC® (CHRP) 450 MHz
- x86
- AMD™64
- ARM support for RHEL 8 and RHEL 9
- Antimalware (AMD) feature on Linux systems
 - 4GB RAM
 - 4GB free disk space

NOTE

If the Antimalware feature is enabled, then Data Center Security: Server Advanced Linux 6.10 agent does not install on a computer with less than 4 GB RAM.

- 100 MB free disk space (Solaris).

-
- A Solaris 11 server might require additional 1.5 GB disk as per Network Publisher Configuration.

NOTE

Disk space for the new Image Packaging System package installation of the Symantec Solaris agent is 100 MB. When the agent is installed on a computer with additional package publishers configured to query network repositories, the Oracle package client reports an estimated disk space needed for the agent to be 1.5GB. Installation time of the new Solaris agent includes a dryrun to check for system prerequisites.

touch /etc/sdcss-check-bypass

NOTE

If there is a concern about issues with connecting to network repositories for other publishers on the computer, you can disable the publishers temporarily before installing the Solaris 11 agent and then reenable them once the agent is installed. Temporarily disabling other network based publishers also improves the time taken to install the Solaris agent. This is an optional step.

Hardware Requirements of the DCS:SA 6.9.3 Agent

The hardware requirements to install a DCS:SA 6.9.3 Agent are as follows:

- 100 MB free disk space (AIX, Linux, and Windows)
- 100 MB free disk space (Solaris).
- A Solaris 11 server might require additional 1.5 GB disk as per Network Publisher Configuration.

NOTE

Disk space for the new Image Packaging System package installation of the Symantec Solaris agent is 100 MB. When the agent is installed on a computer with additional package publishers configured to query network repositories, the Oracle package client reports an estimated disk space needed for the agent to be 1.5GB. Installation time of the new Solaris agent includes a dryrun to check for system prerequisites.

touch /etc/sdcss-check-bypass

NOTE

If there is a concern about issues with connecting to network repositories for other publishers on the computer, you can disable the publishers temporarily before installing the Solaris 11 agent and then reenable them once the agent is installed. Temporarily disabling other network based publishers also improves the time taken to install the Solaris agent. This is an optional step.

- 256 MB RAM
- Sun SPARC 450 MHz
- Sun SPARC32, SPARC64
- IBM PowerPC (CHRP) 450 MHz
- x86
- EM64T
- AMD 64
- Antimalware (AMD) feature on Linux systems
 - 4GB RAM
 - 4GB free disk space

Hardware Requirements to Upgrade

Your environment must meet the minimum hardware requirements to upgrade the components of Data Center Security: Server Advanced 6.9.2 or 6.9.3 to Data Center Security: Server Advanced 6.10 or later.

The minimum hardware requirements to upgrade to Data Center Security: Server Advanced 6.10 are as follows:

Free Disk Space	Memory	CPU	Installer Component
60GB	8GB	4	Management Server
60GB	8GB	4	Communication Server
2GB	1GB	1	Management Console

Software Requirements to Upgrade

Data Center Security: Server Advanced 6.10 supports specific operating systems for upgrading from Data Center Security: Server Advanced 6.9.2 or 6.9.3.

NOTE

If you are upgrading from DCS:SA 6.9.2 or 6.9.3, then the best practice is to upgrade first to DCS:SA 6.10, and then upgrade to the DCS:SA 6.10 Updates.

Upgrade the following components to the supported operating systems:

Management Server	Communication Server	Microsoft SQL Server
Windows 2016 or higher	Windows 2016 or higher	SQL Server 2016 SP1 or higher You must upgrade to SQL Server 2016 SP1 or higher before you upgrade the server components.

