BROADCOM®

Symantec™ Data Center Security: Server Advanced 6.10.2 Release Notes

Table of Contents

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.

Release Notes of DCS:SA 6.10.2

The release notes of Data Center Security: Server Advanced 6.10.2 introduces you to the release items. The Release Notes contain the what's new features of Data Center Security: Server Advanced 6.10.2, 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:

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
  - Protect and harden your heterogeneous virtual and physical server environments
  - Restrict operating system behavior using policy-based least privilege access control
  - Pre-built 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 6.10.2

Review the new features and enhancements of Data Center Security: Server Advanced 6.10.2 before you start upgrading or installing the product.

The DCS:SA 6.10.2 release comprises the following features:

New Features of DCS:SA 6.10.2

The new features of Data Center Security: Server Advanced 6.10.2 are as follows:

- **Multiple Console Session Support**
  You can now launch multiple console sessions on one ore more computers for a specific user. This option to launch is configurable through the **application.properties** file.
  For more information, refer to the Online Help topic, **Management Console Login Options**.
- **Multiple Syslog Server Configuration**
  It is possible to add and configure multiple Syslog Servers from the **Integration > Syslog Server** page of the console for streaming events.
  For more information, refer to the Online Help topic, **Configuring a Syslog Server for Event Streaming**.
- **Quick and Custom Time Range Options for the Investigate Page**
  You can now configure the time range for filtering events using the newly added options such as **Quick** and **Custom**.
  For more information, refer to the Online Help topic, **Investigate Events**.

Enhancements in DCS:SA 6.10.2

- The **Version** column that is displayed on the grid of the **Assets > Agents** tab has been renamed to **Agent Version**.
- More OS options are added for the **Operating System** filter on the **Assets > Agents** page of the console.
- You can now double-click an activity row to view the activity details of a policy. Additionally, you can also copy the details into a clipboard for further analysis. This activity row is displayed for the **Activity History** tab on the policy details flyout pane.
- The search query text that you create using the **Custom Filters** option is now case-insensitive.
- Two new operators such as **Starts With** and **Ends With** are added to filter the strings using the **Custom Filters** option.
- The **Agent Actions** menu of the **Assets > Agent** page and the **Security Groups** page now displays menus that are specific to the operating system of the selected native agent.
- On the **Dashboard** page of the console, for the pie-chart widgets, you can now click at the number displayed at the center of the chart. The click directs you to the respective console page that contains the details. For example, on clicking the **Agent Status** widget, you are directed to the **Assets > Agents** page of the console.
- You can now right-click and **Copy** any individual cell data that is displayed on the **Assets > Agents** page grid.

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 refer to the Symantec Data Center Security: Server and Server Advanced 6.10.2 Platform Feature Matrix or 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 6.9.3 Agent

The supported Windows operating systems for Data Center Security: Server Advanced Windows 6.9.3 agent 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 6.10.0 Agent

The supported operating systems of Data Center Security: Server Advanced Linux 6.10.0 agent 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	x86_64	✓	✓	✓
RHEL /Rocky Linux /Oracle Linux 9.0 to 9.5	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 SP6	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.

Supported Linux Operating Systems for DCS:SA Linux 6.10.1 Agent

The supported operating systems of Data Center Security: Server Advanced Linux 6.10.1 agent 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	x86_64	✓	✓	✓
RHEL 10	aarch64	✓		

Operating System	Architecture	Support for IDS	Support for IPS	Antimalware support
RHEL /Rocky Linux /Oracle Linux 9.0 to 9.5	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 SP6	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.

Fixed Issues of DCS:SA 6.10.2

Review the issues that are fixed in Data Center Security: Server Advanced 6.10.2.

The fixed issues of Data Center Security: Server Advanced 6.10.2 are as follows:

Issue	Description
The **Device Control Rules** of the Prevention policies that are used by CSP cannot be edited after importing to the DCS:SA 6.10 Management Server.	This issue has been fixed
After migrating the CSP agents to DCS:SA 6.10 or later, the agent names are prefixed with **SESCSP_**.	This issue has been fixed. Now, all the new CSP agents that are deployed for DCS:SA 6.10.2 or later are not prefixed with SESCSP_.
After a CSP agent is registered with the DCS:SA 6.10 Management Server, the Prevention Device Control (PDEV) event type does not store the event type in the database. This activity resulted in an invalid error message for the event type.	This issue has been fixed.
The **Log Editor** of the Default Prevention Config does not list the **Device Access** event type.	This issue has been fixed.
The **Agent Actions** menu of the **Assets > Agent** page and the **Security Groups** page does not display menus specific to the operating system of the selected agent.	This issue has been fixed.
After migrating the CSP policies to DCS:SA 6.10 or 6.10.1, the Device Control Rules of certain policies cannot be edited on the console. This prevents upgrade to the latest Management Server of DCS:SA.	This issue has been fixed.
On exporting the assets from the **Assets > Agents** page of the console, all the columns are exported instead of the selected ones.	This issue has been fixed.

Issue	Description
The **Hostname** and the **Description** fields are missing from the Custom Filter option on the **Assets > Agents** page of the console.	This issue has been fixed.
The **Agent Description** field for the Custom Filter option on the **Assets > Agents** page is non-functional. This issue prevents filtering of agents based on the agent description.	This issue has been fixed.
A custom policy called the Windows Heartbeat policy contains a spelling error for the **Description** field.	This issue has been fixed.
A file watch rule of the Intrusion Detection policy, containing "." in the rule name does not generate an event when a file is deleted.	This issue has been fixed.

Known Issues of DCS:SA 6.10.2

Know the DCS:SA known issues before you install or upgrade to Data Center Security: Server Advanced 6.10.2.

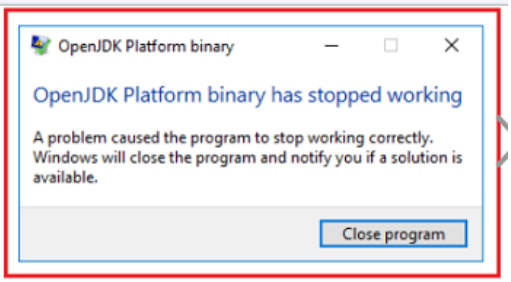
The known issues of Data Center Security: Server Advanced 6.10.2 are as follows:

Table 1: Known issues of Data Center Security: Server Advanced 6.10.2

Issue description	Workaround
Custom controls for multiple policies cannot be copied to a single target policy on the Policies page of the console. DCSM-259	You can copy the custom controls of one policy at a time from the **More Actions > Add Controls** menu that is displayed on the policy details flyout pane.
Multiple policies cannot be exported from the Policies page of the console. DCSM-577	You can export one policy at a time from the **More Actions > Export as Zip or Export as XML** menu that is displayed on the policy details flyout pane.
After upgrade, on applying the real-time events filter on the **Investigate** page of the console, the Management events are also displayed along with the real-time events. DCSM-1814	The Management events generated before the upgrade will be purged as per the **Event Purge** setting after which only the real-time events are displayed.
While remediating individual events, hash values cannot be imported to the **Add Rule** dialog boxes on the **Investigate** page of the console. DCSM-1845	You can manually add the MD5 and SHA hash values in the **Policy Editor** dialog boxes of the Prevention Policy to add rules for files, registries, or processes.
MD5 hashes cannot be added in the **Add Rule** dialog box while remediating events. DCSM-1862	As an Administrator, you can add MD5 value manually to the Prevention Policy. Edit the policy to add the MD5 value for the **Settings > Global Policy Options** of the Prevention Policy.
A **Custom Prevention** Policy cannot be created from the Management Console. DCSM-481	You can duplicate an existing **Custom Prevention** policy and edit as per your requirement.
Searching for tunable or benign Prevention events results in an exception error.	Before you search for tunable or benign Prevention events using the Simple Search option, you must first enter values in the agent and policy filters. Otherwise, attempting to do a Simple Search results in the following error: `* Machine Name and Policy Name are mandatory fields.`

Issue description	Workaround
On demand and scheduled scan jobs scan external drives twice.	When you enable **Scan External Drive option** in the Detection Configuration Policy and then apply the policy to the Data Center Security: Server Advanced 6.9.3 Linux agent or the 6.10 Linux agent, the on-demand and scheduled scan jobs scans the external drives (USB, CDROM (read/write only), floppies) twice.
Disabling Filewatch collector from IDS configuration is not honored by the agent.	Applying an IDS configuration to the Data Center Security: Server Advanced agent with **Filewatch collector** disabled does not disable the **Filewatch collector** on the agent. This issue existed since the 5.2.8 release of DCS:SA. There is no workaround available currently.

When using the sisipsconfig tool to move your system to another security group, certain steps must be followed if the target security group contains special characters.	• When "!" or any other special character is part of a security group name, with the exception of "$", you must use a single quoted string for the sisipsconfig command.
	`~# su - sisips -c './sisipsconfig.sh -g test-group!@'`
	• When "$" is in the security group name, escape "$" with a backslash:
	`~# su - sisips -c './sisipsconfig.sh -g \$\$'`
	– When both "$" and "!" are present in the security group name, you should use a single quoted string in the sispsconfig command along with a backslash for "$"
	`~# su - sisips -c './sisipsconfig.sh -g !\$\$'`

Sometimes, the following OpenJDK error message can display for the DCS:SA Management Console 6.10.1 or later versions. 	Make sure that the Management Console computer is installed with the latest **Microsoft Visual C++ Redistributable (Both x64, x86)** package. For more information, refer to the Microsoft article.

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 **SISPISService.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**.

Frequently Asked Questions

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

1. 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

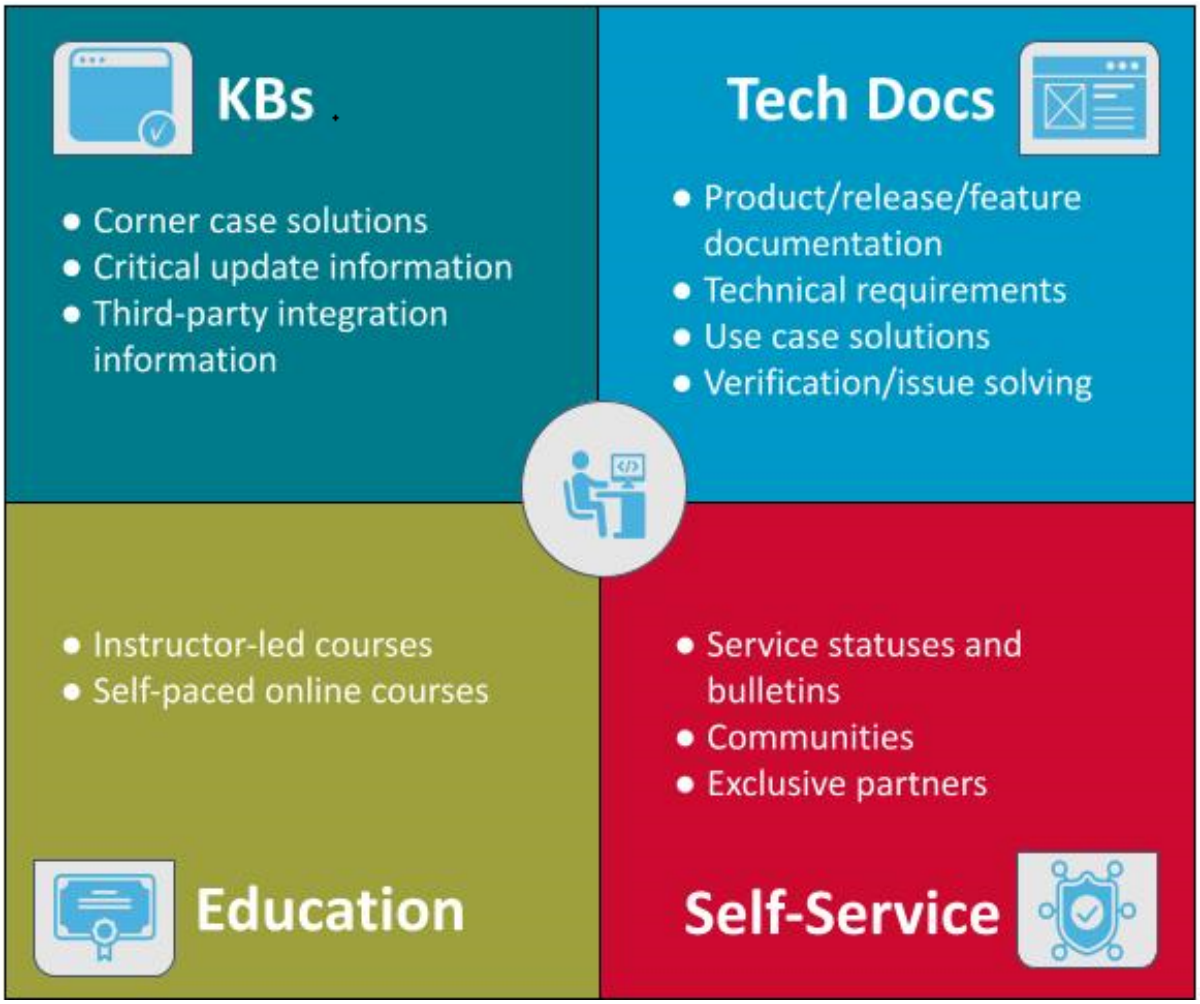
Access information, self-help, and support resources for Broadcom Software and Data Center Security: Server Advanced.

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.

Your environment must meet the following hardware and software requirements for Data Center Security: Server Advanced 6.10 or later versions:

- Hardware Requirements for Fresh Installation
- Software Requirements for Fresh Installation
- Hardware Requirements for the Agent
- Hardware Requirements to Upgrade
- Software Requirements to Upgrade
- Hardware Recommendation for a Large Scale Setup

For the latest supported OS versions and flavors of Windows, AIX, Solaris, and Linux agents refer to the Symantec Data Center Security: Server and Server Advanced 6.10 Platform Feature Matrix. Alternately, you can also download the latest Platform Feature Matrix of the specific DCS:SA version such as 6.10.1 or so 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
• Microsoft SQL Server 2016 Standard with Service Pack 1 or higher • Windows Installer 2.0 or higher	• Microsoft SQL Server 2022 Express • .NET Framework 4.7.1 • Windows 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 agent of different operating systems.

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

- Hardware Requirements of the DCS:SA 6.9.3 Agent
- Hardware Requirements of the DCS:SA Linux 6.10 Agent

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 of the DCS:SA Linux 6.10 Agent

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 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.


BROADCOM®