

# Cisco Security Agent FAQ

Document ID: 63902

---

## Questions

### Introduction

**Where can I find CSA documentation and product support information?**

**Where can I download the latest versions and patches for CSA?**

**Where can I find information on bugs that exist for CSA?**

**What versions of Linux does a 4.5 agent support?**

**Which versions of Solaris does a 4.5 agent support?**

**Which versions of Microsoft Windows does a 4.5 agent support?**

**Besides English, what languages does the CSA 4.5 support?**

**What is the network bandwidth that the CSA takes in version 4.5?**

**On a UNIX system, a file access control list (FACL) denies writing the symbolic link, but not the target file of the symbolic link. What protection applies with a write to the target via the symbolic link?**

**How does the 4.5 agent GUI work with terminal services?**

**How do I get user state information?**

**The network worm heuristic sometimes triggers false positives. How does the 4.5 system address this?**

**Is the rule ordering, or the way in which rules are processed, the same in version 4.5 as in version 4.0x?**

**I created a network access control rule in order to block Network Basic Input/Output System (NetBIOS), ports 137–139. But, traffic still passed. What have I done wrong?**

**How do I configure a silent installation to an agent without user interaction or intervention?**

**CSA does not support dual network interface cards (NICs) with teaming enabled. Is there a workaround?**

**How do I disable individual shims on CSA for UNIX?**

**How do I uninstall CSA on UNIX?**

**How do I disable shims in CSA in Microsoft Windows?**

**Why is the CSA unable to communicate with the CSA MC?**

**Can CSA or the CSA MC be installed on a 64-bit Windows Operating System?**

**Can CSA 6.0.1 support Windows 2008/Windows 7 Operating Systems?**

**Can the CSA 5.x host application be installed on a Symantec Ghost image?**

**I reinstalled the agent on the exact same machine but it does not register. Why is this?**

**Why do all the CSA agents appear as parent devices and not as children after I add the CSA Management Center to MARS?**

### Related Information

---

## Introduction

This document contains Frequently Asked Questions (FAQ) about Cisco Security Agent (CSA). Refer to the *CiscoWorks Management Center for Cisco Security Agents (CSA MC)* section of CiscoWorks VPN/Security Management Solution Frequently Asked Questions for CSA Management Center (MC) FAQ.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

**Q. Where can I find CSA documentation and product support information?**

A. Refer to Cisco Security Agent Product Support.

**Q. Where can I download the latest versions and patches for CSA?**

A. Refer to Software Download – Hotfixes for Cisco Security Agent ( registered customers only) .

**Q. Where can I find information on bugs that exist for CSA?**

A. You can find details on these bugs in the Bug Toolkit – Cisco Security Agent ( registered customers only) .

**Q. What versions of Linux does a 4.5 agent support?**

A. CSA 4.5 supports RedHat Enterprise Linux 3.0 WS, ES, or AS only.

**Q. Which versions of Solaris does a 4.5 agent support?**

A. The requirements for Solaris have not changed for the 4.5 release:

- ◆ Solaris 8 64-bit 12/02 Edition, or later, with SUNWlibCx libraries installed
- ◆ UltraSPARC single, dual, and quad processor systems

Refer to the Release Notes for Management Center for Cisco Security Agents 4.5 for more information.

**Q. Which versions of Microsoft Windows does a 4.5 agent support?**

A. CSA 4.5 supports these versions:

- ◆ Windows NT service pack 6a only

**Note:** The earlier service pack versions no longer have support.

- ◆ Windows XP service packs 0, 1, and 2
- ◆ Windows 2000 Professional, Server, or Advanced Server service packs 0, 1, 2, 3, and 4
- ◆ Windows 2003 Server Standard, Enterprise, Web, or Small Business Edition service pack 0

**Q. Besides English, what languages does the CSA 4.5 support?**

A. You can install the CSA on a machine that is localized for German, French, and Japanese. The CSA user interface (UI), help guide, and events appear in these languages.

**Q. What is the network bandwidth that the CSA takes in version 4.5?**

A. An agent poll can cost 2KB>KB, if there are no changes. An agent event can cost 3KB™0KB for an average event upload. An agent rule download can cost 50KB™00KB, which depends on the size of the rule set.

Agent rule downloads are cacheable. As such, the appropriate use of Cache Engines provide an environment in which there is no effect on bandwidth utilization. In such a case, only one agent download needs to take place for all other agents behind the Cache Engine.

When you have enabled the hint message, the MC sends User Datagram Protocol (UDP) packets to the agents. This action only affects bandwidth utilization if Network Address Translation (NAT) has not occurred for the address. The MC detects the hosts that are translated with NAT, and does not hint these hosts.

The cost of polling and events is not expected to increase significantly in version 4.5. But, for fair margin, double them.

In an environment in which bandwidth utilization is high, polling intervals can save bandwidth if you configure them for only once a day or so.

**Q. On a UNIX system, a file access control list (FACL) denies writing the symbolic link, but not the target file of the symbolic link. What protection applies with a write to the target via the symbolic link?**

A. The behavior is operating system–dependent. For example, on Solaris 8, a write to a file via a symbolic link opens the link file for writing. Thus, the FACL rule denies the write. On Linux 2.4, a similar write opens the symbolic link for reading only. Thus, there is no trigger of the FACL rule.

**Q. How does the 4.5 agent GUI work with terminal services?**

A. All terminal services users see an agent GUI and agent popups.

If multiple users have logged in via terminal services at the same time, each user agent GUI dynamically updates with the user responses. For example, assume that a terminal services user logs in as admin1, and another terminal services user logs in to the same machine as admin2. Whatever queries that admin1 answered also show up in the event log and agent GUI of admin2 instantly. These users share the same agent GUI and see what the other terminal service users see for the actual events. But, query popups and popup messages are visible only to the user that triggered the query and not to all the terminal service users.

**Note:** If you have two terminal service sessions that use exactly the same login credentials, both the users are treated as separate users. Both instances refer to the common agent GUI. But, even though these users have logged in with terminal services as the exact same user, only the person who triggers popups sees the popups. For example, Joe logged in as admin1 and sees the query popup that a rule triggered. But Mike, who also logged in as admin1, does not see the query popup.

**Q. How do I get user state information?**

A. You can use the Win32 application programming interface (API) in order to get user information from the operating system.

**Q. The network worm heuristic sometimes triggers false positives. How does the 4.5 system address this?**

A. The 4.5 system *replaces* the network worm heuristic with a user-configurable rule module. You can configure this worm rule module in order to display a query popup, a straight deny, or an allow.

**Note:** These options are similar to other configurable rule types.

## Q. Is the rule ordering, or the way in which rules are processed, the same in version 4.5 as in version 4.0x?

A. The rule precedence has changed in version 4.5 because of the introduction of the terminate option. Prior to 4.5, query (default allow) had a higher precedence than the query (default deny) precedence.

Version 4.5 reverses this precedence. The query (default deny) has higher precedence than the query (default allow). Therefore, rule sets that migrate into version 4.5 may function differently than in previous versions.

## Q. I created a network access control rule in order to block Network Basic Input/Output System (NetBIOS), ports 137–139. But, traffic still passed. What have I done wrong?

A. You need to create two rules in order to block the NetBIOS broadcast:

1. Deny any connection for TCP/137–139 and User Datagram Protocol (UDP)/137–139 as a server.
2. Deny any connection for TCP/137–139 and UDP/137–139 as a client.

**Note:** If your CSA received those rules after the machine booted, these rules do block the NetBIOS ports. This is because the NetBIOS ports open at boot time and remain open. After reboot of the machine, the agent rules that deny the connection of NetBIOS ports are in effect, and this blocks the ports. This is a Microsoft Windows limitation.

## Q. How do I configure a silent installation to an agent without user interaction or intervention?

A. Extract the agent kit in a local directory, and run setup.exe from the command line with a switch.

The syntax is:

```
[extracted directory]:\setup.exe /s --autolevel=n --noreboot=1
```

**Note:** n is the desired automation level. Also, note the double dash (--).

There is support for these levels:

- ◆ 0 No automation; standard mode. This is the default level.
- ◆ 1 No confirmations. Setup does not prompt the user for any confirmation and takes default actions.
- ◆ 2 No warnings. Setup does not pop up warning messages and proceeds silently.
- ◆ 3 No errors. Setup does not pop up error messages and aborts silently when an error occurs.

If you do not want the machine to reboot, you need to add the noreboot switch. Otherwise, the

machine reboots. The end user sees one popup that says the CSA is installing.

## Q. CSA does not support dual network interface cards (NICs) with teaming enabled. Is there a workaround?

A. Teaming is an advanced network feature that is difficult for CSA to work with because the feature inserts a network shim between the NIC level and the TCP/IP stack. Teaming creates virtual NICs and can do load balancing, which may or may not use the NIC on which the shim is installed.

Disable the teaming feature and install the CSA, without the netshim, in order to make the feature work. After everything works properly, enable the teaming feature.

## Q. How do I disable individual shims on CSA for UNIX?

A. Use this configuration:

```
Net shim:
cd /opt/CSCOcsa/drv
./r.csanet net shim

File shim:
./r.csafilter file shim

etc.
```

## Q. How do I uninstall CSA on UNIX?

A. Complete these steps:

1. Enter into single user mode.
2. Log in as root.
3. Move the file csamanager to csamanager.old.
4. Reboot the machine.
5. Log in as root.
6. Issue the **pkgrm CSCOcsa** command.

## Q. How do I disable shims in CSA in Microsoft Windows?

A. Complete these steps:

1. Issue the **regedit** command from a command prompt.

**Note:** Be sure to save your registry and back it up appropriately before you make any changes.

2. Navigate to HKLM\SYSTEM\CurrentControlSet\Services\ . You see several entries that relate to CSA:

```
csafilter - File Interceptor
csafilter - HTTP interceptor
csahook - System call interpreter
csanet - Network traffic interceptor
csreg - Registry interceptor
csatdi - Network application interceptor
```

3. Highlight the shim that you want to disable, and look for a key called Enable. If this

- key does not exist, create a new value and name it Enable.
4. Set the value of the Enable key from 1 to 0. This setting disables the shim.
  5. Reboot the machine.

## Q. Why is the CSA unable to communicate with the CSA MC?

A. The CSA machine must contact the CSA MC machine via Domain Name System (DNS) or Windows Internet Naming Service (WINS). The CSA machine must be able to resolve the CSA MC host name.

Complete these steps if the CSA is unable to communicate with the CSA MC:

1. Use **nslookup** in order to resolve the host name.
  - a. Get the exact name of the MC from the CSA. Verify that the CSA can resolve the host name. Also, verify if DNS suffixes are configured for the network adapter.
  - b. If this step fails, ping via IP address, and add an entry into the etc/hosts file.
2. Choose **Maintenance > License Information** in order to verify this license information:
  - ◇ Do you have enough licenses?
  - ◇ Can you verify the licenses that you use?
  - ◇ How many desktop and server machines do your licenses cover?You can also check the csalog.txt file from one of the agents that fails in order to search for errors. This is an example:

```
(indicate license problems) [2003-09-02 16:51:56.131]
[PID=672] [Csamanager]: Registration failed without message Error
?code=2035'.
```

3. Determine if ports 5401 and 443 are allowed between the CSA and the MC. Port 5402 is for profiler. Use the **icpping** utility in order to ping the MC on that port.
4. Check the time on the machines.

## Q. Can CSA or the CSA MC be installed on a 64-bit Windows Operating System?

A. Not at this time. Refer to the Cisco Security Agent Product Support area for the latest support information on CSA.

## Q. Can CSA 6.0.1 support Windows 2008/Windows 7 Operating Systems?

A. No. CSA 6.0.2 can start to provide support for Windows 2008/Windows 7 (32 bit and 64 bit) Operating Systems.

## Q. Can the CSA 5.x host application be installed on a Symantec Ghost image?

A. Yes, but, once the image is installed on the PC, you must change the IP address and hostname **before** you connect the PC to the network.

## **Q. I reinstalled the agent on the exact same machine but it does not register. Why is this?**

**A.** Once you un-install your CSA agent, the Hostname of your machine remains in the host page of the CSA MC for at least one hour before it is marked as Inactive. If you need to install the CSA agent again, you need to delete the Hostname from the Host page in the CSA MC before you can re-install. If you do not wait, the CSA agent is not able to register to the CSA MC and you see the = 2037 (backoff registration) error message in the csalog file. This is in order to prevent an attack where someone tries to register unauthorized agents over and over again.

## **Q. Why do all the CSA agents appear as parent devices and not as children after I add the CSA Management Center to MARS?**

**A.** This behavior is expected. Because each agent is considered a separate reporting device, each individual CSA agent appears as a parent and not as a child.

---

## **Related Information**

- **Cisco Security Agent Product Support**
- **Technical Support & Documentation – Cisco Systems**

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 22, 2009

Document ID: 63902

---