

Clean Access Server FAQ

Document ID: 63594

Questions

Introduction

Clean Access Server DHCP Service does not restart or occasionally stops. What needs to be done?

How do I set the duplex and speed on the Cisco Clean Access Server network interface cards?

How do I set the duplex/speed on the Cisco Clean Access Interface "bnx2" ?

I configured the Heartbeat timer so that a device is logged off the system after some inactive time. In the event log, it states that it cannot ping the device but the device continues to pass traffic back and forth. How do I fix this?

How do I check to see the duplex and speed on the Cisco Clean Access Server network interface cards (NICs)?

How long does it take the Cisco Clean Access Manager (formerly SmartManager) to time out the Cisco Clean Access Server and for the `SecureSmart 2004-08-26 12:26:42 192.168.1.1 is inaccessible!` message to display?

I configured the Heartbeat timer so that a device logs off the system after some period of inactivity. In the event log, it states that it cannot ping the device but the device still passes traffic back and forth. How do I fix this?

What is the impact of changing the network interface card (NIC) on Cisco Clean Access Server?

How do I install the LSI SCSI drivers for Dell 1750 or others?

How do I configure the Broadcom drivers?

How do I configure the Cisco Clean Access Server behind a NAT gateway?

In the `/var/log/messages` or the `/var/log/ha-log` messages I see several heartbeat messages for Failover. Why is this and how do I fix it?

I am able to get an IP address from the Clean Access DHCP server, but after that, I continue to see a "Page Not Found" message when I try to open a browser to an outside address. I was never redirected to the web login page. Why is this?

Why do I receive the `cannot add Clean Access server error` message.

Why do I receive the `CAS Network Error: Clean Access Server could not establish a secure connection to Clean Access Manager at null.` error message?

Why do I receive the `Encountered error while building X509 certificate chain ..` error message?

Do I need to update anything after I replace a faulty Cisco Clean Access Server?

What is the number of VPN connections supported per Cisco Clean Access Server?

How do I change the IP address of the Cisco Clean Access Server? Do I need to delete and re-add the Cisco Clean Access Server?

How do I limit SSH access to the Cisco Clean Access Server?

How does the Bandwidth Burst setting work?

I recently read in the Clean Access Server Installation and Administration Guide Release 3.3BETA on page 68 that the recommended maximum number of subnets per Clean Access Server is 1000. I need to create more than 1000. What is the limit?

How do I manage a batch of access points that I have on a specific VLAN that is managed by the Clean Access Server. I have added them in the Access Point Device Management?

I have secondary (sometimes multiple secondary) subnets on each VLAN. The 150

subnet is for clients, and the 172 subnet is for the management of our networking gear in the building. Is the Clean Access Server able to deal with multiple subnets on a single VLAN?

I see the Clean Access Server 2004-08-30 11:30:28 192.168.151.60 System Stats: Load factor 0 (max since reboot: 3) Mem: 261160960 237854720 23306240 212992 47259648 99737600 cpu 188552 153 91405324 194183 messages in my event logs. What do they mean?

I get the Authentication 2004-11-01 15:53:40 Server communication error, [00:0E:35:5F:F9:91 ## 172.19.168.42] bart and Authentication 2004-11-01 15:53:13 Server communication error, [00:0E:35:5F:F9:91 ## 172.19.168.42] bart errors on the event logs. How do I fix this?

I get the TCP/IP Stack Signature: UNKNOWN UNKNOWN [65535:64:1:64:M1460,N,W2,N,N,T0,S,E:P] { } message. How do I fix this and how can I disable install of the client for iPhones?

Why am I unable to add the Clean Access Server to the Clean Access Manager (CAM)? You might receive this error message: Error: Upload Failed. This CA-signed Certificate doesn't match the private key in the key database. How can I resolve this?

Should I generate a new CSR to renew the certificate on the Clean Access Server?

Is it possible to pass through multicast traffic through CCA?

Related Information

Introduction

This document addresses the most frequently asked questions (FAQs) related to Cisco Clean Access Server (formerly Perfigo SecureSmart Server).

The product names have changed. This table lists both the old and new names:

Old Name	New Name
SmartManager	Clean Access Manager
SecureSmart Server	Clean Access Server
SmartEnforcer	Clean Access Agent
CleanMachinesAPIs	Clean Access APIs

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

Q. Clean Access Server DHCP Service does not restart or occasionally stops. What needs to be done?

A. The DHCP settings are *compiled* on the Clean Access Server. Sometimes these compiled settings can become corrupted, especially after an upgrade to the Clean Access Server software. The solution is to force the Clean Access Server to recompile the settings. In order to do this, make a change, and click **update**.

Symptoms:

The DHCP server does not start, or it occasionally fails on the Clean Access Server.

Instructions:

1. If the DHCP daemon of the server does not start, go to the manager, open that particular server, and click **Manage**.
2. Select **Network > DHCP > Subnet List**, and click **Edit** for one of the subnet lists.
3. Make any change to the subnet (for example, increase the lease time by 1 minute), and click **Update**.
4. Go back to the status page and see if the DHCP service has started. At this point the DHCP settings should be compiled again.

Note: Another situation that can cause the DHCP server not to start is overlapping subnet configurations. Check for this as well.

Q. How do I set the duplex and speed on the Cisco Clean Access Server network interface cards?

A. Use this as a guide to set up appropriate network interface cards in the `/etc/modules.conf` file.

Note: Append the options parameter at the end for the `/etc/modules.conf` file with the use of the vi editor.

- ◆ Set broadcom 5700 cards to 100 Mbps full duplex:

```
options bcm5700 line_speed=100,100 auto_speed=0,0 duplex=1,1
```

- ◆ Set broadcom 5700 cards to 1000 Mbps full duplex:

```
options bcm5700 line_speed=1000,1000 auto_speed=0,0 duplex=1,1
```

- ◆ Set e1000 cards to 100 Mbps full duplex:

```
options e1000 Speed=100,100 Duplex=2,2
```

- ◆ Set e1000 cards to 1000 Mbps full duplex:

```
options e1000 Speed=1000,1000 Duplex=2,2
```

- ◆ Set eepr100 cards to 100 Mbps full duplex:

```
options eepr100 option="0x30,0x30"
```

Q. How do I set the duplex/speed on the Cisco Clean Access Interface "bnx2" ?

A. On Cisco Clean Access Server devices (even on CAM), there are files for each network interface that describe the properties and speed/duplex settings.

Here are the steps how to perform it manually:

1. Change the directory to `/etc/sysconfig/network-scripts`. For each interface there is a file in this directory named `ifcfg-ethX`, where X can be 0, 1, 2, etc.
2. Add this line for whichever interface you want to hardcode the settings for:

```
ETHSTOOL_OPTS="speed 100 duplex full autoneg off"
```

3. After saving the file, perform a "service network restart".
4. Make sure the switch settings are set manually. Check your settings by issuing the `eth-tool ethX` command on the shell, where X can be 0 or 1 to confirm the duplex settings are hardcoded.

Note: This interrupts the service momentarily. Keep this in consideration if you have to schedule a downtime.

Q. I configured the Heartbeat timer so that a device is logged off the system after some inactive time. In the event log, it states that it cannot ping the device but the device continues to pass traffic back and forth. How do I fix this?

A. This is an example of the error:

```
Authentication 2004-08-26 12:13:48
Unable to ping 149.151.206.251, going to logout user user1
```

Check to see if the device has any built-in firewalls that block ARP packets from the Cisco Clean Access Server. The Cisco Clean Access Server performs ARP ping. This is an ARP message and should not be blocked.

Q. How do I check to see the duplex and speed on the Cisco Clean Access Server network interface cards (NICs)?

A. Run the **mii-tool** utility from the command line. It works for the on-board NIC, but does not support fiber NICs.

For fiber NICs, use the **grep 'eth0'** command on `/var/log/messages`.

You can also issue a **tail -f** command on `/var/log/messages`. This displays messages whenever a NIC becomes active or inactive.

Q. How long does it take the Cisco Clean Access Manager (formerly SmartManager) to time out the Cisco Clean Access Server and for the SecureSmart 2004-08-26 12:26:42 192.168.1.1 is inaccessible! message to display?

A. The Cisco Clean Access Manager takes three minutes to timeout each Cisco Clean Access Server before it displays the Not Connected status.

Q. I configured the Heartbeat timer so that a device logs off the system after some period of inactivity. In the event log, it states that it cannot ping the device but the device still passes traffic back and forth. How do I fix this?

A. Make sure that you configure a serial port for failover connection.

If the computer that runs the Cisco Clean Access Server software has two serial ports, you can use the additional port for the serial cable connection. By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access). If the computer has only one serial port (ttyS0) and you do not intend to use it for administrative access, you can reconfigure the port to serve as the failover connection.

Complete these steps in order to reconfigure ttyS0 as the heartbeat connection:

1. From an SSH client, access the Cisco Clean Access Server as root user.
2. Edit **/etc/lilo.conf** and remove or comment out the last line:

```
append="console=ttyS0....."
```

This line causes console output to be redirected to the serial port.

Note: Add a **#** character to the start of the line in order to comment out a line. Lines that start with this character are ignored.

3. Edit **/etc/inittab** and remove or comment out the last line:

```
co:2345:respawn . . . vt100
```

This line causes a login terminal to start on the serial port.

4. Type **lilo** and press **enter** at the command prompt. This starts Lilo, the Linux boot loader.
5. Enter the **reboot** command to reboot the computer.
6. Repeat the steps on the failover peer Cisco Clean Access Server.

Q. What is the impact of changing the network interface card (NIC) on Cisco Clean Access Server?

A. If you have a non-site license, you do not need to inform Cisco Technical Support of the change on the MAC address. You only need to inform Cisco Technical Support when your number of Clean Access Servers changes. If you have a site license, you do not need to inform Cisco Technical Support.

Q. How do I install the LSI SCSI drivers for Dell 1750 or others?

A. Complete these steps:

1. Save the rawrite file to C:\ and the LSI Driver. Update files in the same directory.
2. Open a command prompt and enter **C:\rawrite**.
3. Enter the full name of the source file(s) and the destination on to two floppy disks.
4. Insert the Clean Access Manager Machines (formerly CleanMachines) Installation CD into Cisco Clean Access Server or Cisco Clean Access Manager.
5. Enter **custom** at the **boot>** prompt.
6. Follow the instructions to enter the Update disk, and then the Driver disk.

Q. How do I configure the Broadcom drivers?

A. Complete these steps:

1. Console into the box:

```
cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700  
insmod ./bcm5700.o
```

2. If step 1 results in no errors, enter the **vi /etc/modules.conf** command and add these two lines:

```
alias eth0 bcm5700  
alias eth1 bcm5700
```

Q. How do I configure the Cisco Clean Access Server behind a NAT gateway?

A. Complete these steps for each Cisco Clean Access Server deployed behind a NAT gateway.

1. SSH to the SecureSmart server or use a serial console to login as root.
2. Edit the `/perfigo/access/bin/starttomcat` file.
3. Append `-Djava.rmi.server.hostname=<CAS_hostname>` to the `CATALINA_OPTS` variable line.
4. Restart **service perfigo restart**.
5. SSH to SmartManager or use a serial console to login as root.
6. Edit the `/etc/hosts` file and append this line:

```
<public_IP_address> <seuresmart_hostname> <seuresmart_hostname>
```

Q. In the `/var/log/messages` or the `/var/log/ha-log` messages I see several heartbeat messages for Failover. Why is this and how do I fix it?

A. These are the heartbeat messages that you see:

```
heartbeat: 2004/09/15_11:23:27 info: Heartbeat restart on node ss1
heartbeat: 2004/09/15_14:19:17 info: Heartbeat restart on node ss1
heartbeat: 2004/09/15_18:59:53 info: Heartbeat restart on node ss1
heartbeat: 2004/09/15_19:36:18 info: Heartbeat restart on node ss1
```

You see these messages when the peer server is up after a reboot. You can also see it in the log on the primary server when:

- ◆ You issue **service perfigo stop** and then **service perfigo start** on the peer or standby machine.

or

- ◆ Reboot a peer or standby machine.

Note: When you issue the **service perfigo restart** command, it does not trigger this log.

Q. I am able to get an IP address from the Clean Access DHCP server, but after that, I continue to see a "Page Not Found" message when I try to open a browser to an outside address. I was never redirected to the web login page. Why is this?

A. You can be experiencing one of these issues:

- ◆ The DNS of the Cisco Clean Access Server is not set in the DNS server.

You are redirected to the DNS name for the web login page. You may not have associated `seuresmart.company.com` with `192.168.0.1` in your DNS entry.

- ◆ The certificate uses the DNS name.

The certificate uses `seuresmart.company.com` but the DNS server has not been

associated with the name. The certification validation fails.

- ◆ The certificate is improperly created or is not valid. Check to see `/perfigo/access/apache/logs/error_log`. If you see these errors, recreate your SSL certificate.

```
[root@securesmart logs]# cat error_log
```

```
[Thu Sep 16 18:00:04 2004] [error] Unable to configure RSA
server private key
```

```
[Thu Sep 16 18:00:04 2004] [error] SSL Library Error:
185073780 error:0B080074:x509 certificate routines:
X509_check_private_key:key values mismatch
```

Note: Refer to `Where are the log files in the Clean Access Manager?` for all log files.

- ◆ The httpd is not started. Check to see if http is started with the `netstat -al | grep http` command. You should see this listing. If not, issue the `service perfigo restart` command.

```
tcp        0      0  *:http          :::*           LISTEN
tcp        0      0  *:https         :::*           LISTEN
```

Q. Why do I receive the cannot add Clean Access server error message.

A. Check these items:

- ◆ The shared secret is the same on the Cisco Clean Access Server and the Cisco Clean Access Manager.
- ◆ The certificates are correct.
- ◆ The connectivity between the Cisco Clean Access Server and Cisco Clean Access Manager and that there are not any firewall rules that block the RMI ports.

Q. Why do I receive the CAS Network Error: Clean Access Server could not establish a secure connection to Clean Access Manager at null. error message?

A. You might receive this error if the Clean Access Manager has expired, cannot be trusted, or cannot be reached. The error is basically due to CAS or CAM communication issues.

In order to resolve this issue, verify these items:

- ◆ Make sure both CAS and CAM are the same version.
- ◆ If you use a name for the certificate, make sure the name can be resolved using `nslookup`.
- ◆ Use the service IP for failover certificate.
- ◆ Make sure they are time synced before generating certificate.
- ◆ Make sure shared secrets match.
- ◆ CAS/CAM should not ACL block any SSL communication.

Q. Why do I receive the Encountered error while building X509 certificate chain .. error message?

A. You must use the correct root certificate. If Microsoft Certificate Authority (CA) is used, save the certificate in Base64 rather than default encoded.

Q. Do I need to update anything after I replace a faulty Cisco Clean Access Server?

A. In some instances, the `ss_key` is no longer the same. Complete these steps.

1. SSH to the Cisco Clean Access Manager and obtain the `ss_key`.
2. Issue the `psql -h 127.0.0.1 -U postgres controlsmartdb` command.
3. Select `*` from `securesmart_info`.

```
ss_key | ss_group | ss_type | ss_ip | ss_loc
00_40_33_60_43_D2_04_54_48_55_66_D5 | | standard_gateway | 10.0.0.1 |
```

4. SSH to the Cisco Clean Access Server and obtain/update the `ss_key`.
5. Issue the `[root@securesmart etc]# cat /etc/.GUSSK` command.

```
[root@securesmart etc]# cat /etc/.GUSSK
00_30_48_80_43_D6_00_30_48_80_43_D5
```

6. Edit `/etc/.GUSSK` and update it with the `ss_key` from the Clean Access Manager.
7. Perform a reboot.

Q. What is the number of VPN connections supported per Cisco Clean Access Server?

A. No limit is placed for IPsec.

PPTP and L2TP are currently set to 32 tunnels each.

Q. How do I change the IP address of the Cisco Clean Access Server? Do I need to delete and re-add the Cisco Clean Access Server?

A. Cisco recommends that you change the IP address of the Cisco Clean Access Server via the Manager UI. When the IP address of the Cisco Clean Access Server is changed from the Manager UI, reboot the Cisco Clean Access Server. It automatically tries to connect to the Cisco Clean Access Manager upon reboot. The Cisco Clean Access Manager changes the IP address of the Cisco Clean Access Server in the database and the SSKEY remains the same.

Note: If you delete and re-add the Cisco Clean Access Server, you lose all the configuration settings of the Cisco Clean Access Server.

Q. How do I limit SSH access to the Cisco Clean Access Server?

A. Add a line similar to this example in order to change the `/etc/ssh/sshd_config` file:

```
ListenAddress IP_address_of_where_you_want_ssh_to_allow_connections
```

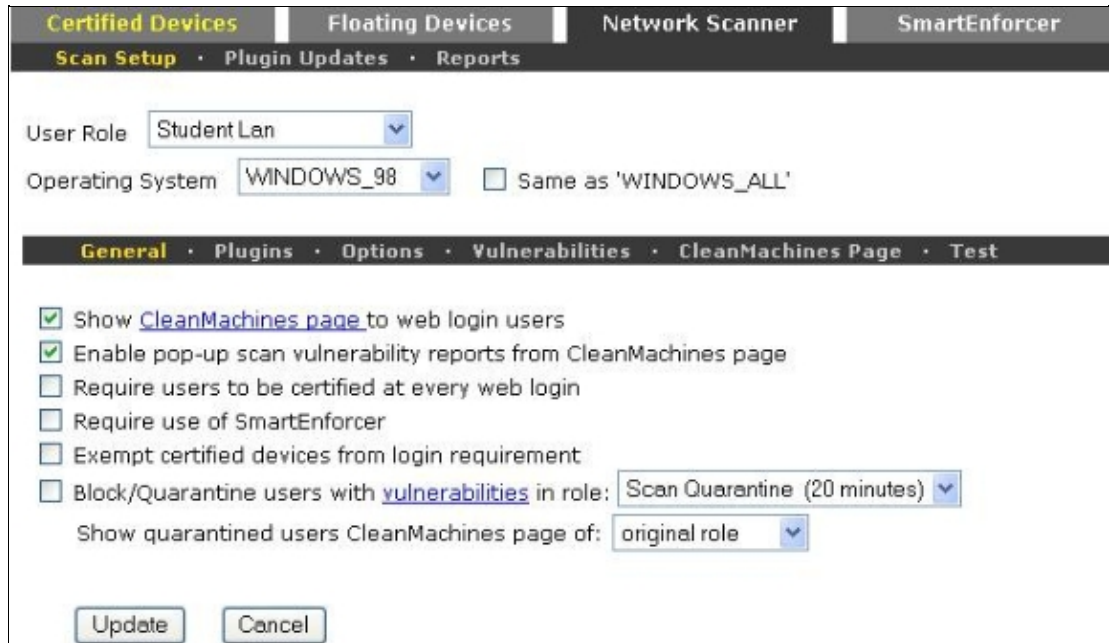
For example:

```
ListenAddress 192.168.151.60
```

Issue the `service sshd restart` command in order to restart the SSHD process.

Q. How does the Bandwidth Burst setting work?

A. Under CleanMachines, uncheck **Windows All** and select each OS independently for Require Use of SmartEnforcer or not.



The screenshot shows the configuration interface for the Clean Access Server. The top navigation bar includes 'Certified Devices', 'Floating Devices', 'Network Scanner', and 'SmartEnforcer'. Below this, there are tabs for 'Scan Setup', 'Plugin Updates', and 'Reports'. The 'User Role' is set to 'Student Lan' and the 'Operating System' is set to 'WINDOWS_98'. There is a checkbox for 'Same as 'WINDOWS_ALL'' which is unchecked. The main configuration area is titled 'General' and includes several options: 'Show CleanMachines page to web login users' (checked), 'Enable pop-up scan vulnerability reports from CleanMachines page' (checked), 'Require users to be certified at every web login' (unchecked), 'Require use of SmartEnforcer' (unchecked), 'Exempt certified devices from login requirement' (unchecked), and 'Block/Quarantine users with vulnerabilities in role:' (unchecked). The 'Block/Quarantine' option has a dropdown menu set to 'Scan Quarantine (20 minutes)'. Below this, there is a dropdown for 'Show quarantined users CleanMachines page of:' set to 'original role'. At the bottom, there are 'Update' and 'Cancel' buttons.

Q. I recently read in the Clean Access Server Installation and Administration Guide Release 3.3BETA on page 68 that the recommended maximum number of subnets per Clean Access Server is 1000. I need to create more than 1000. What is the limit?

A. The limit of 1000 is a warning only. If the machine has enough memory (more than 1G), you can configure up to 2500 subnets.

Q. How do I manage a batch of access points that I have on a specific VLAN that is managed by the Clean Access Server. I have added them in the Access Point Device Management?

A. Add the MAC addresses of the Access Points to the **Filters >Devices** area as opposed to the Access Point Device Management section.

Q. I have secondary (sometimes multiple secondary) subnets on each VLAN. The 150 subnet is for clients, and the 172 subnet is for the management of our networking gear in the building. Is the Clean Access Server able to deal with multiple subnets on a single VLAN?

A. An example of this problem is:

```
!  
interface Vlan 106  
 ip address 150.135.47.1 255.255.255.0  
 ip address 172.16.10.1 255.255.255.192 secondary  
!
```

Clean Access Server is in the virtual gateway mode:

- ◆ In this case, the Clean Access Server does not care about the number of subnets or their associated VLAN tags. All of the VLAN information passes through with no exceptions.

Clean Access Server is in a gateway (real-ip or NAT) mode:

- ◆ In this case, the Clean Access Server also functions as either a DHCP relay or a DHCP server. In either situation, the range of IP addresses allocated depends on the VLAN tag or the gateway address which also depends on the VLAN tag.

Therefore, the Clean Access Server is not able to differentiate (from a DHCP point of view) between two subnets on the same VLAN. The one limitation is that one of the two subnets on the same VLAN should not use DHCP for address assignment. Instead, the IP addresses need to be statically assigned. This is most likely the case for the 172 subnet in the network since it consists of network gear.

Q. I see the Clean Access Server 2004-08-30 11:30:28 192.168.151.60 System Stats: Load factor 0 (max since reboot: 3) Mem: 261160960 237854720 23306240 212992 47259648 99737600 cpu 188552 153 91405324 194183 messages in my event logs. What do they mean?

A. System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default. Reported information includes the load factor of each server, maximum load since reboot, memory, and CPU usage.

- ◆ **Load Factor** Load factor is a number that describes the number of packets that wait to be processed by the server (for example, the current load that is handled by the Clean Access Server). When the load factor grows, it is an indication that packets are waiting in the queue to be processed. If the load factor is greater than 500 for any consistent period of time (for example, 5 minutes), then it is indicative that the Clean Access Server has a steady high load of traffic/packets that come in. You need to be concerned if the number reaches 500 or higher.
- ◆ **Max since reboot** The maximum number of packets in the queue at any one time (for example, the maximum load handled by the Clean Access Server).
- ◆ **Mem** The memory usage statistics. There are six numbers (the unit is bytes). These numbers stand for the total, used, free, shared, buffers, and cached memory.
- ◆ **Cpu** The processor load on the hardware. There are four numbers that provide information about CPU usage (the unit is jiffies – on most systems, a jiffy is a 10 ms time unit). The numbers indicate the time spent by the system in user, nice, system, and idle processes.

For the example provided, $\text{system \%} = 91405324 * 100 / (188552 + 153 + 91405324 + 194183) = 99.58\%$. Similarly, you can calculate the others as well. However, on a Clean Access Server, system time is typically greater than 90 percent. This is the sign of a healthy system.

Q. I get the Authentication 2004-11-01 15:53:40 Server communication error, [00:0E:35:5F:F9:91 ## 172.19.168.42] bart and Authentication 2004-11-01 15:53:13 Server communication error, [00:0E:35:5F:F9:91 ## 172.19.168.42] bart errors on the event logs. How do I fix this?

A. If you run failover Clean Access Server in virtual gateway mode, then edit the vi /etc/hosts file and change the SS-1 (Clean Access Server) address to the Service IP (virtual address).

You need to change them on both Clean Access Servers, active and standby.

- ◆ 127.0.0.1 localhost localhost
- ◆ 192.168.1.2 SS-1 SS-1

Q. I get the TCP/IP Stack Signature: UNKNOWN UNKNOWN [65535:64:1:64:M1460,N,W2,N,N,T0,S,E:P] { } message. How do I fix this and how can I disable install of the client for iPhones?

A. Here are the instructions that should work for not requiring the agent for iPhones:

1. Choose the role under **Clean Access > General Setup > Agent Login**.
2. Choose **MAC_ALL** to configure the agent requirements for iPhone or iPod touch. Make sure the **Use ALL settings** for the MAC OS family if no version-specific settings are specified is unchecked, so it will not use the shared setting from "ALL". Also, make sure the Require agent downloading option is unchecked, so the Clean Access Server will not ask the client (iPhone/iPod touch) to download the agent.
3. Choose **MAC_OSX** to configure the agent requirements for MAC OS. You can check the **ALL settings** option or uncheck it to configure this specific OS. The Require agent downloading option must be checked if you want the regular MAC OS users to download the MAC agent.

Q. Why am I unable to add the Clean Access Server to the Clean Access Manager (CAM)?

A. If you are unable to add the Clean Access Server to the CAM, then this is a licensing issue. Make sure that the server licenses are generated based on the Primary CAM's ethernet 0 MAC address. The MAC addresses on the server license should match the (Primary) MAC address of the CAM.

1. Go to **CAM GUI > Administration > Clean Access Manager > Licensing**.
2. Perform a "Remove All Licenses".
3. Re-install the server license files again.

Q. You might receive this error message: Error: Upload Failed. This CA-Signed Certificate doesn't match the private key in the key database. How can I resolve this?

A. In order to resolve the issue, complete these steps:

1. Generate a CSR.
2. Save the private key.
3. Upload the new certificate with the saved private key.

Q. Should I generate a new CSR to renew the certificate on the Clean Access Server?

A. No. For renewal of the certificate on the Clean Access Server, do not generate a new CSR. However, if you are generating a new CSR, then you have to upload the private key in the Clean Access Server. After uploading the private key, reboot the Clean Access Server. This completes the renewal process.

Q. Is it possible to pass through multicast traffic through CCA?

A. No, multicast is not supported under the inband real gateway. However, it will work for out-of-band or virtual gateway.

Related Information

- **Cisco Clean Access Agent FAQ**
 - **Cisco Clean Access Manager FAQ**
 - **Cisco Clean Access Manager FAQ 2**
 - **Technical Support – 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: Oct 13, 2009

Document ID: 63594
