

Clean Access Manager FAQ

Document ID: 63592

Questions

Introduction

How can I re-direct to another registration page first and then get re-directed back to the Login page?

How can I configure the Quarantine Policy for access to various update sites such as Windows Update, Symantec LiveUpdate, and so forth?

Where are the log files in the Cisco Clean Access Manager?

When I log in from the web into a role that requires a VPN, I get a message that says I must use a VPN Client to connect. I want to edit it to add a link to download a VPN Client. Where is the VPN page located?

Where is the remote back up script that can take a snapshot and forward to a specific remote server using FTP?

The Cisco Clean Access Manager shows all MAC addresses as 00:00:00:00:00:00. Why is this?

I received a signed SSL certificate for our Cisco Clean Access Manager. I thought that this would stop the certificate warning from appearing when a client begins the authentication process. The certificate warning still appears. How do I fix this?

If I have a signed certificate for the Cisco Clean Access Manager, can I also import it in the Cisco Clean Access Servers and share it?

How do I turn the Certified Device clearing timer off?

I have two Failover Clean Access Managers. I added a license key to the primary Manager, then tried to go to the second via <http://<sm2>/admin/main.jsp> to add the same key to the secondary Manager. When I hit the "Apply License Key" button, I get an error. Why do I receive this error?

Do you have Authentication Server Failover support?

How does the Bandwidth Burst setting work?

What is the impact when you change the network interface card (NIC) on the Cisco Clean Access Manager?

The network interface cards (NICs) do not come up properly and do not pass traffic. What should I do?

How do I query user information from the database directly?

Related Information

Introduction

This document answers the most frequently asked questions (FAQs) related to Cisco Clean Access Manager. This document is part one of a two part documentation set. Refer to Cisco Clean Access Manager FAQ 2 for part two.

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. How can I re-direct to another registration page first and then get re-directed back to the Login page?

A. There are two solutions:

- ◆ Provide a link for unregistered or new users to click on from the Login page. The registration page can show up on the right frame. The user can register first, and then obtain their login credentials.
- ◆ Use attribute mapping in LDAP that indicates if the users are registered or not. If the users are not registered, put them in a particular role (based on the response from LDAP). Then redirect them to a registration web site in order to obtain their login credentials based on the role.

Q. How can I configure the Quarantine Policy for access to various update sites such as Windows Update, Symantec LiveUpdate, and so forth?

A. Cisco suggests that you set these rules in this order in order to mitigate the need to put individual Windows Update or antivirus update IP addresses:

1. Allow DNS (your DNS can be internal or external) to resolve the DNS of the update site.
2. Block all TCP/UDP/ICMP incoming traffic to your internal network.
3. Enable outbound port 80/443 so traffic can traverse to Windows Update and perform the update.

Quarantine Role		Untrusted -> Trusted	Select	Add Policy to All Roles					
Quarantine Role						Add Policy			
Action	Protocol	Port	Source	Destination	Enable	Edit	Del	Move	
Allow	UDP	53	*	*	<input checked="" type="checkbox"/>				
Block	ANY	*	*	192.168.0.0/255.255.0.0	<input checked="" type="checkbox"/>				
Allow	TCP	80	*	*	<input checked="" type="checkbox"/>				
Allow	TCP	443	*	*	<input checked="" type="checkbox"/>				
Block	ALL								

Cisco also recommends that you set the Quarantine session timer accordingly (for example, 20 minutes).

List of Roles	New Role	Traffic Control	Bandwidth	Schedule
Session Timer · Heartbeat Timer				
Role	Session Timeout	Description		Edit
Unauthenticated Role	Disabled			
Student Lan	Disabled			
Admin	Disabled			
Scan Quarantine	20	Network Scan Quarantine		
Client Scan Quarantine	20	SmartEnforcer Client Scan Quarantine		
Wireless	Disabled			

Note: domain-based policy filtering has been added in versions 3.2 and later (allows windowsupdate.microsoft.com in the policy permit).

Q. Where are the log files in the Cisco Clean Access Manager?

A. The event log is in the database table name as log_info table.

There are other logs in the Cisco Clean Access Manager:

- ◆ /var/log/messages – startup
- ◆ /var/log/dhcplog – dhcp relay, dhcp logs
- ◆ /tmp/perfigo-log0.log.? – service logs
- ◆ /perfigo/control/apache/logs/* – ssl, apache error logs
- ◆ /perfigo/control/tomcat/logs/localhost*. – tomcat, redirect, jsp logs

Q. When I log in from the web into a role that requires a VPN, I get a message that says I must use a VPN Client to connect. I want to edit it to add a link to download a VPN Client. Where is the VPN page located?

A. It is located in /perfigo/access/tomcat/webapps/auth/perfigo_ipsec_enforced.jsp on the Cisco Clean Access Server.

Q. Where is the remote back up script that can take a snapshot and forward to a specific remote server using FTP?

A. The remote back up script is on the Cisco Clean Access Manager in the /perfigo/control/bin directory named as pg_backup.

If you run it without any parameters, it tells you how it needs to be used. Usage for the script is:

- ◆ pg_backup [FTP-Server] [Username] [Password]

Q. The Cisco Clean Access Manager shows all MAC addresses as 00:00:00:00:00:00. Why is this?

A. This can be due to:

- ◆ If there is a router downstream, the Cisco Clean Access Manager shows the MAC address of the router, as long as the router is ARPing for the IP addresses in question (for example, user's IP). If the router is not (for some reason), then you have 00:00:00:00:00:00 as the MAC address of the user.

- ◆ If the user comes in from the trusted side (for example, there is no ARP entry for the user on the untrusted side), the Cisco Clean Access Manager shows all zeros.

Q. I received a signed SSL certificate for our Cisco Clean Access Manager. I thought that this would stop the certificate warning from appearing when a client begins the authentication process. The certificate warning still appears. How do I fix this?

A. If you do not want your end users to see the certificate warning, get a certificate for the Cisco Clean Access Server, not the Cisco Clean Access Manager.

Q. If I have a signed certificate for the Cisco Clean Access Manager, can I also import it in the Cisco Clean Access Servers and share it?

A. No, you cannot use a certificate that you bought for the Cisco Clean Access Manager on the Cisco Clean Access Server. You need to buy a separate certificate for each Cisco Clean Access Server.

Q. How do I turn the Certified Device clearing timer off?

A. Select a date in the future and click the **enable/disable** box in order to disable the certified timer.

Q. I have two Failover Clean Access Managers. I added a license key to the primary Manager, then tried to go to the second via <http://<sm2>/admin/main.jsp> to add the same key to the secondary Manager. When I hit the "Apply License Key" button, I get an error. Why do I receive this error?

A. You do not need to do this. The license key is kept in the database. It makes its way over to the secondary Manager through database replication.

Q. Do you have Authentication Server Failover support?

A. Cisco currently supports Authentication Server clustering and plans to look into Authentication Server Failover in future releases.

Q. How does the Bandwidth Burst setting work?

A. A bursty factor is used to determine the "capacity" of the bucket. As an example, assume the bandwidth is 100 Kbps and the factor is 2. Therefore, the capacity of the bucket is $100 \text{ Kb} * 2 = 200 \text{ Kb}$.

If a user does not send any packet for some time, they have at most 200 Kb tokens in the bucket. Once the user needs to send packets, the user is able to send out 200 Kb packets immediately. Thereafter, the user needs to wait for the tokens to come in at the rate of 100 Kbps to send out additional packets.

One way to think of the fit is that the average rate is 100 Kbps, and the peak rate is approximately 200 Kbps. Therefore, it is good for bursty applications such as web browsing.

Q. What is the impact when you change the network interface card (NIC) on the Cisco Clean Access Manager?

A. If you have a non-site license, inform Cisco Technical Support of the change on the MAC address for a new license key issuance. For a failover pair, provide both MAC addresses. If you have a site license, you do not need to inform Cisco Technical Support.

Q. The network interface cards (NICs) do not come up properly and do not pass traffic. What should I do?

A. This can be a case of the NICs not being recognized as Broadcom NICs. Try to:

- ◆ Console into the box.
- ◆ Issue the `cd /lib/modules/kernel-2.4.9-perfigo/drivers/addon/bcm5700` command.
- ◆ Issue the `insmod ./bcm5700.o` command.

If these commands result in no errors, issue the `vi /etc/modules.conf` command and add these two lines:

```
alias eth0 bcm5700

alias eth1 bcm5700
```

Q. How do I query user information from the database directly?

A. On the primary Cisco Clean Access Manager from the root prompt, enter this command:

```
root>psql h 127.0.0.1 U postgres controlsmartdb
```

You are now in the database shell – `controlsmartdb=#`.

Examples:

- ◆ Enter this command to get the number of users logged on per Cisco Clean Access Server:

```
select count(*) from user_info where ss_key=
(select ss_key from securesmart_info where ss_ip='x.x.x.x');
```

Note: Make sure you enter the trailing semi-colon. Change the IP address to get information for the other Cisco Clean Access Servers.

- ◆ Enter this command to get the number of users logged on per role:

```
select count(*) from user_info where role_id=
(select role_id from role_info where role_name='Wireless');
```

Note: Replace the role name for information related to the other roles.

- ◆ Enter this command to get the event logs:

```
select * from report_info;
```

Related Information

- [Cisco Clean Access Miscellaneous FAQ](#)
 - [Cisco Clean Access Agent FAQ](#)
 - [Cisco Clean Access Manager FAQ 2](#)
 - [Cisco Clean Access Server FAQ](#)
 - [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: Feb 02, 2006

Document ID: 63592
