

Clean Access Manager FAQ 2

Document ID: 63593

Questions

Introduction

I would like to change the initial web page that comes up when I first try to access a web site before I am logged into Cisco. How do I do this?

When the number of entries in the event logs passes the number configured in the Cisco Clean Access Manager, are the entries removed from the database, or does the GUI only show the number specified?

When you try to upgrade NAC with 4.6.1 to 4.7.1 version, it is possible that you get the PCI: BIOS Bug: MCFG area at e0000000 is not E820-reserved PCI: Not using MMCONFIG error message. Why does this error occur and how can this be resolved?

I see the "500 Internal Server Error" message when the primary (active) Cisco Clean Access Manager fails over to the standby (inactive) manager. The manager GUI never displays. How do I fix this?

In virtual gateway mode, can I re-tag all machines in a role (for example, Xboxes) and have them appear to be on one network?

Failover Clean Access Servers do not appear to failover correctly. Both Cisco Clean Access Servers indicate that the other is down. The primary tries to failover to the secondary but does not succeed. No new logins are authenticated during this time. Why does this problem occur?

I need to develop a page where the helpdesk technicians can enter MAC addresses into the 'exclusion' table for things such as printers, routers, game systems, and so forth. Is there a utility to accomplish this?

If the session timer is set to 0 for a role, and a user in that role shuts down the machine and goes home, comes back in the morning and turns the machine on, is the user required to logon again?

I have ensured that the Nessus scan plugin 11011 SMB on port 445 is unchecked but still shows up in the user scan report. Why is this?

When I perform a failover, I see the DROP DATABASE, CREATE DATABASE, and pg_restore: [archiver (db)] could not execute query: ERROR: Cannot create unique values log messages in /var/log/messages or /var/log/ha-log. Why is this?

Can the Cisco Clean Access Manager database be queried remotely through SQL?

How do I perform a manual database backup?

How do I recreate the database?

How do tell if the services are running?

What filters do I need to configure for Xbox Live?

I uploaded some jpgs and html pages to be used for the right frame of the Login Page using frames.

Where are the files and how do I reference them?

I configured bandwidth management for the unauthenticated role, and my connection (or the Cisco Clean Access Manager) to the Cisco Clean Access Server is now very slow and it occasionally times out. Why is this?

How do I find the number of users per OS logged on?

Does CAM support EAP-TLS or EAP-TTLS authentication?

What does this [Failure] Error:"SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]:No such name" error message occur in switch?

How do I add a Clean Access Server (CAS) into Clean Access Manager (CAM)?

Why does the "unable to read cert found in /root/.chain.crt NAC only handles RSA keys <= 2048 ...java.io.IOException: subject key, Unknown key spec: Invalid RSA modulus size." error message appear?

When I try to save the running-config of the switch through SNMP, I get the failed to save the running configuration error message. Why does this error occur and how can this be resolved?

Related Information

Introduction

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

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 Cisco Technical Tips Conventions for more information on document conventions.

Q. I would like to change the initial web page that comes up when I first try to access a web site before I am logged into Cisco. How do I do this?

A. The initial page that appears states, "You are being redirected to the network authentication page." This page is currently not editable because it is a CGI script. In addition, the page is shown only a couple of seconds. Users are not able to read extended text display beyond the two lines.

Q. When the number of entries in the event logs passes the number configured in the Cisco Clean Access Manager, are the entries removed from the database, or does the GUI only show the number specified?

A. The event log threshold is the number of events that are stored in the database. The maximum number of log events kept on the server, by default, is 100,000. The event log threshold must be smaller than 200,000. The event log is a circular log. The oldest entries are over-written when the log passes the threshold.

Q. When you try to upgrade NAC with 4.6.1 to 4.7.1 version, it is possible that you get the PCI: BIOS Bug: MCFG area at e0000000 is not E820-reserved PCI: Not using MMCONFIG error message. Why does this error occur and how can this be resolved?

A. This error occurs if you upgrade through monitor/keyboard and not through console port.

Q. I see the "500 Internal Server Error" message when the primary (active) Cisco Clean Access Manager fails over to the standby (inactive) manager. The manager GUI never displays. How do I fix this?

A. Check `/etc/ha.d/perfigo.conf` to ensure that the `peerhostname` and `ha_serial` are correctly set.

```
[root@smb root]# cat /etc/ha.d/perfigo.conf
#linux-ha
#Wed Sep 01 16:20:25 EDT 2004
WIRELESS_SERVICEIP=
HOSTNAME=
HA_DEAD=
PEERGUSSK=
PEERHOSTNAME=sma
HAMODE=STANDBY
PEERHOSTIP=
HA_UDP=
WIRED_SERVICEIP=207.206.230.27
HA_SERIAL=ttyS0
[root@smb root]#
```

Q. In virtual gateway mode, can I re-tag all machines in a role (for example, Xboxes) and have them appear to be on one network?

A. A VLAN is not retagged in Virtual Gateway mode.

Q. Failover Clean Access Servers do not appear to failover correctly. Both Cisco Clean Access Servers indicate that the other is down. The primary tries to failover to the secondary but does not succeed. No new logins are authenticated during this time. Why does this problem occur?

A. The cause of the problem can be in the configuration of `/etc/lilo.conf` and `/etc/inittab`. Modify `/etc/lilo.conf` and `/etc/inittab` to stop console redirection to the serial ttyS0 output.

Complete these steps to re-configure ttyS0 as the heartbeat connection:

1. From an SSH client, access the Cisco Clean Access Server and/or Cisco Clean Access Manager 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 be started 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 these steps on the failover peer Cisco Clean Access Manager.

Q. I need to develop a page where the helpdesk technicians can enter MAC addresses into the 'exclusion' table for things such as printers, routers, game systems, and so forth. Is there a utility to accomplish

this?

A. Cisco Clean Access provides a utility script called **cisco_api.jsp** (or **perfigo_api.jsp** for prior releases 3.2 and 3.3) that allows you to perform certain operations through HTTPS POST. Here is the URL for the Clean Access API description page for your Clean Access Manager that you can access from a web browser:

- ◆ https://<ccam-ip-or-name>/admin/cisco_api.jsp

The section tells you what the functions are and how to access them.

Important: Usage Requirements

- ◆ You or someone in your organization must know and be comfortable with scripting languages such as Perl.
- ◆ Only HTTPS, POST and AUTH are supported. HTTP, GET, and No Authentication APIs are not supported.
- ◆ You need to install Perl packages (or something similar) on the machine that runs these scripts.
- ◆ Cisco Technical Support does not support debugging of your Perl or scripting packages.

Authentication Requirements (3.5.4+)

The API requires authentication over SSL for access to the API, through these two authentication methods:

◆ **Authentication by Session**

In this method, as an administrator, you can use the **adminlogin** and **adminlogout** functions. These functions enable you to create an authentication shell script that sets a cookie with the session ID to be accessed for the rest of the admin session. If a session ID cookie is not set, the user receives a login prompt. The **adminlogin** (administrator login) function returns a session ID, which must be set as a cookie for usage of any API. You must then use the **adminlogout** function to terminate the session. However, if you do not use **adminlogout**, the session still terminates when the admin session times out.

◆ **Authentication by Function**

If you do not want to use cookies to create a shell script, you can instead perform authentication every time a function is used. If you authenticate by function, you need to add the admin and password parameters to all functions that you use in your existing script. In this case, you do not use the **adminlogin** and **adminlogout** functions.

Guest Access Support (3.5.8+)

The **getlocaluserlist**, **addlocaluser**, and **deletelocaluser** APIs are intended to support guest access for dynamic token user access generation, and provide the ability to:

- ◆ Use a webpage to access Cisco Clean Access API to insert a visitor username or password (for example, jdoe@visitor.com, jdoe112805), and assign a role (for example, guest1day).
- ◆ Delete all guest users associated with that role for that day (for example, guest1day).
- ◆ List all usernames associated with that role (for example, all users for guest1day).

These APIs support most implementations of guest user access dynamic token/password generation and allow the removal of those users for a guest role. This provides you the ability

to create your own customized login or subscription pages and then call the CCA API.

Note: You still need to create the front-end generation password/token. For accounting purposes, Cisco Clean Access provides RADIUS accounting functionality only.

Example

Here is a sample (right-click, download) of the Perl test script for the 'addmac' operation.

You must install these modules on your Linux server for this script to run. You can download them from Comprehensive Perl Archive Network .

- ◆ MIME-Base64-3.05.tar.gz
- ◆ URI-1.33.tar.gz
- ◆ HTML-Tagset-3.03.tar.gz
- ◆ HTML-Parser-3.36.tar.gz
- ◆ Crypt-SSLeay-0.51.tar.gz (requires openssl installed)
- ◆ libwww-perl-5.77.tar.gz

Refer to What To Do Once You have Downloaded a Module From The CPAN for module installation instructions.

After installation, you can try it out through SSH to the Cisco Clean Access Manager. Go to `/root/perl` (assuming you installed here) and execute the **https-auth-post** script. A MAC entry is added to 192.168.151.156 global filters.

Operation Name: adminlogin

Description Administrator login returns a session ID which has to be set as a cookie for usage of any API.

Use **adminlogin** and **adminlogout** to create a shell script if you use authentication by session with cookies. Otherwise, use the admin and password parameters in each function.

In Params:

- ◆ op (required) adminlogin
- ◆ admin (required) Admin account user name
- ◆ passwd (required) Admin account password

Out Params:

- ◆ A comment of the form `<!--error=msg-->` is returned. If the msg value is 0 then the operation is a success or else there is an error string.
- ◆ If the msg value is 0, another comment of form `<!--session_id=SESSION_ID_STRING-->` is returned

Operation Name: adminlogout

Description Administrator is logged out. The cookie identifies the session.

Use **adminlogin** and **adminlogout** to create a shell script if you use authentication by session with cookies. Otherwise, use the admin and password parameters in each function.

In Params:

- ◆ op (required) adminlogout

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: addmac

Description Adds MAC address to the Devices list.

In Params:

- ◆ op (required) addmac
- ◆ mac (required) Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445
- ◆ ip (optional) Supported formats 192.168.0.10
- ◆ type (optional) One of the Strings [deny, allow, userole]. Default is deny.
- ◆ role (optional) Specify role name. Default is unauthenticated. Required if type=userole.
- ◆ desc (optional) Any description string.
- ◆ ssip (optional) Default is global. Provide the IP address used to configure Clean Access Server to Clean Access Manager.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: removemac

Description Removes the MAC address from the Device Filters list.

In Params:

- ◆ op (required) removemac
- ◆ mac (required) Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445
- ◆ ssip (optional) The default is global. Provide the IP address used for the configuration of Clean Access Server to Clean Access Manager.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: addcleanmac

Description Adds a MAC address to the Cisco Clean Access certified devices list as an exempted device.

In Params:

- ◆ op (required) addcleanmac
- ◆ mac (required) Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445
- ◆ ssid (optional) The default is global. Provide the IP address used to configure the Clean Access Server to the Clean Access Manager.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: removecleanmac

Description Removes the MAC address from the Clean Access certified devices list.

In Params:

- ◆ op (required) removecleanmac
- ◆ mac (required) Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445
- ◆ ssid (optional) The default is global. Provide the IP address used to configure the Clean Access Server to Clean Access Manager.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

You can have more than one error comment if SSIP is not provided and MAC cannot be deleted from more than one Clean Access Server.

Operation Name: clearcertified

Description Clears the Clean Access certified devices list.

In Params:

- ◆ op (required) clearcertified
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.

- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: kickuser

Description Kicks out logged in user

In Params:

- ◆ op (required) kickuser
- ◆ ip (required) Provides the IP address of the user to be removed.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: kickoobuser

Description Kicks out a logged in out of band user.

In Params:

- ◆ op (required) kickoobuser
- ◆ mac (required) Provides the MAC address of the user to be removed.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

Operation Name: queryuserstime

Description Queries logged in users remaining time in the session. Only users logged into session timeout roles are returned.

In Params:

- ◆ op (required) queryuserstime
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.

- ◆ If the mesg value is 0, another comment of the form <!--list=iplist--> is returned. The iplist format is 10.1.10.10=23345,10.1.10.11=23001,10.1.10.12.....,IP=Time_Remaining(milliseconds).

Operation Name: renewuserstime

Description Renew logged in users session timeout by a session.

In Params:

- ◆ op (required) renewuserstime
- ◆ list (required) Format of the list is 10.1.10.10, 10.1.10.11, 10.1.10.12.....IP, IP.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the mesg value is 0 then the operation is a success or else there is an error string.

Operation Name: changeuserrole

Description Changes the role of the logged in user.

In Params:

- ◆ op (required) changeuserrole
- ◆ ip (required) The IP address of the logged in user.
- ◆ role (required) The role this user has to be placed in.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the mesg value is 0 then the operation is a success or else there is an error string.

Operation Name: getuserinfo

Description Given one of IP, MAC or Name, the logged in user(s) information is returned. If there are multiple users that match the criteria, a list of users is returned.

In Params:

- ◆ op (required) getuserinfo
- ◆ qtype (required) One of the strings ('ip', 'mac', 'name', 'all').
- ◆ qval (required) The IP address or MAC address or User name or Empty String incase of 'all'.
- ◆ admin (optional) The admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) The password for the admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.
- ◆ If msg value is 0, A comment of form <!--count=10--> shows the number of users returned, followed by a corresponding number of comments of form <!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,ORIGROLE=Student,VLAN=1024,NEWVLAN=1024,OS=Windows XP--> are returned.

Operation Name: getoobuserinfo

Description: Given one of IP, MAC or Name, the logged in OOB user(s) information will be returned. If there are multiple users matching the criteria, a list of users will be returned

In Params:

- ◆ op (required) getoobuserinfo
- ◆ qtype (required) one of the strings ('ip', 'mac', 'name', 'all')
- ◆ qval (required) IP address or MAC address or User name or Empty String incase of 'all'
- ◆ admin (optional) admin account user name. This parameter is not needed if using authentication by session.
- ◆ passwd (optional) password for admin account. This parameter is not needed if using authentication by session.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.
- ◆ If the msg value is 0, a comment of the form <!--count=10--> shows the number of users returned, followed by a corresponding number of comments of the form <!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,AUTHVLAN=10,ACCESSVLAN=1024,OS=Windows XP,SWITCHIP=10.1.10.1,PORTNUM=18-->.

Operation Name: getcleanuserinfo

Description Given one of MAC or Name, the certified user(s) information is returned. If there are multiple users that match the criteria, a list of certified users is returned.

In Params:

- ◆ op (required) getcleanuserinfo
- ◆ qtype (required) One of the strings ('mac', 'name', 'all').
- ◆ qval (required) The MAC address or user name or Empty String incase of 'all'.

Out Params:

- ◆ A comment of the form <!--error=msg--> is returned. If the msg value is 0 then the operation is a success or else there is an error string.
- ◆ If the msg value is 0, a comment of the form <!--count=10--> shows the number of users returned, followed by the same number of comments of the form <!--MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,VLAN=10-->.

Operation Name: getlocaluserlist

Description Returns list of configured local user accounts with user name and role name.

In Params:

- ◆ op (required) getlocaluserlist
- ◆ admin (optional) admin account user name. This parameter is not needed if using authentication by session.
- ◆ passwd (optional) password for admin account. This parameter is not needed if using authentication by session.

Out Params:

- ◆ Comment of form `<!--error=msg-->` is returned. If *msg* value is 0 then operation is success or else there will be an error string.
- ◆ If *msg* value is 0, A comment of form `<!--count=10-->` shows the number of users returned, Following same number of comments of form `<!--NAME=jdoe,ROLE=Student-->` are returned.

Operation Name: addlocaluser

Description Adds a new local user account.

In Params:

- ◆ op (required) addlocaluser
- ◆ username (required) local user account user name.
- ◆ userpass (required) local user account user password.
- ◆ userrole (required) local user account user role name.
- ◆ admin (optional) admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) password for admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ Comment of the form `<!--error=msg-->` is returned. If *msg* value is 0, the operation is a success, otherwise, there is an error string.

Operation Name: deletelocaluser

Description Deletes a local user account.

In Params:

- ◆ op (required) deletelocaluser
- ◆ qtype (required) one of the strings ('name', 'all')
- ◆ qval (required) User name or Empty String incase of 'all'
- ◆ admin (optional) admin account user name. This parameter is not needed if you use authentication by session.
- ◆ passwd (optional) password for admin account. This parameter is not needed if you use authentication by session.

Out Params:

- ◆ Comment of the form <!--error=msg--> is returned. If *msg* value is 0, the operation is a success, otherwise, there is an error string.

Q. If the session timer is set to 0 for a role, and a user in that role shuts down the machine and goes home, comes back in the morning and turns the machine on, is the user required to logon again?

A. A user session persists until one of these occurs:

- ◆ The user logs off the network.
- ◆ An administrator manually kicks the user off the network.
- ◆ The session times out because of the session timer. Session timeout, in which the user is dropped regardless of connection status or activity. The setting applies to all users, whether locally or externally authenticated.
- ◆ The Cisco Clean Access Server determines that the user is no longer connected using the heartbeat timer.
- ◆ Heartbeat timer sets the number of minutes after which a user is logged off the network if unreachable by a connection attempt from the Cisco Clean Access Server.

Additional explanations:

- ◆ If the session timer is 0 *and* the heartbeat timer is not set, the user is not dropped from the online users and is not required to re-logon.
- ◆ If the session timer is 0 *and* the heartbeat timer is set, then the heartbeat timer takes effect.
- ◆ If the session timer is non-zero *and* the heartbeat is not set, then the session timer takes effect.
- ◆ If both timers are set, the first timer to be reached is activated first.
- ◆ If the user logs out and shuts down the machine, the user is dropped from the Online Users and is required to re-logon.

Note: A Cisco Clean Access Agent client does not send a logout request to the Cisco Clean Access Server when the client machine is shutdown based on Cisco Clean Access APIs (formerly CleanMachine's) session based connection setup.

Q. I have ensured that the Nessus scan plugin 11011 SMB on port 445 is unchecked but still shows up in the user scan report. Why is this?

Scan Report:			
Type	Plugin	Service	Description
INFO	11011	microsoft-ds (445/tcp)	A CIFS server is running on this port
INFO	11011	netbios-ssn (139/tcp)	An SMB server is running on this port
INFO	10150	netbios-ns (137/udp)	The following 4 NetBIOS names have been gathered : JSTOOPS COMPUTERS = Workgroup / Domain name JSTOOPS = This is the computer name COMPUTERS = Workgroup / Domain name (part of the Browser elections) The remote host has the following MAC address on its adapter : 00:03:47:fd:55:3c If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621

A. If you have turned on other plugins that check Windows NT LAN Manager (NTLM) such as 12054 ASN.1 Parsing Vulnerabilities (NTLM check), the 11011 scan is still activated as the base scan and the 11011 is reported as INFO type.

As long as you have not made 11011 a vulnerability, it does not trigger any response other than INFO in the report.

Note: Starting with version 3.2.13, users only see reports from selected plugins.

Q. When I perform a failover, I see the DROP DATABASE, CREATE DATABASE, and pg_restore: [archiver (db)] could not execute query: ERROR: Cannot create unique values log messages in /var/log/messages or /var/log/ha-log. Why is this?

A. The inconsistent database is likely due to an upgrade issue. If this happens after an upgrade, run the dbupgrade.sql again and report to Cisco Technical Support the error messages that you see.

Q. Can the Cisco Clean Access Manager database be queried remotely through SQL?

A. No, the server only allows local connections for security reasons.

Q. How do I perform a manual database backup?

A. Complete these steps.

1. Log in as root on the Cisco Clean Access Manager box.
2. Type **su postgres** to switch the user to postgres.
3. Type **pg_dump h 127.0.0.1 controlsmartdb D f sm_back_092004.sql** to create the dump of the database. This command creates a file called sm_back_092004.sql in the /var/lib/pgsql directory.
4. SCP this file.

Q. How do I recreate the database?

A. Issue these commands in this order.

1. **service perfigo stop**
2. **su postgres**
3. **dropdb h 127.0.0.1 controlsmartdb**
4. **createdb h 127.0.0.1 controlsmartdb**
5. **psql h 127.0.0.1 controlsmartdb < /perfigo/dbscripts/pg_createtable.sql**
6. **logout from postgres**
7. **service perfigo start**

Q. How do tell if the services are running?

A. Issue one of these commands:

- ◆ **netstat -an [to show all services running]**
- ◆ **netstat -al | grep http [to show web server listening]**
- ◆ **ps -ef | grep http [to show web services running]**
- ◆ **ps -ef | grep java [to show java services running]**

Q. What filters do I need to configure for Xbox Live?

A. First, setup Filters and put the MAC address(es) of the Xbox(es) in a role, for example, un-authenticated role. Then configure this policy for the role.

The Xbox Live service uses two standard ports that need to be configured in your role (for example, an un-authenticated role).

- ◆ Kerberos-Sec (UDP); Port 88; UDP; Send Receive
- ◆ DNS Query (UDP); Port 53; Send

The service also requires two custom protocol definitions be configured in your role (for example, an un-authenticated role)

- ◆ Port 3074 over UDP Send/Receive
- ◆ Port 3074 over TCP Outbound

The service also requires that you configure these ports:

- ◆ Game Server Port (TCP): 22042
- ◆ Voice Chat Port (TCP/UDP): 22043-22050
- ◆ Peer Ping Port (UDP): 13139
- ◆ Peer Query Port (UDP): 6500

Note: If you want to enable Xbox across VLANs, tunnel Xbox between the VLANs using one of these tools:

- ◆ GameSpy Tunnel
- ◆ XBCConnect

For GameCube (you may need to check specific games):

- ◆ Port 4000: both UDP and TCP

For Playstation 2 (you may need to check specific games):

- ◆ TCP Ports: 10070 – 10080
- ◆ UDP Ports: 10070

Q. I uploaded some jpgs and html pages to be used for the right frame of the Login Page using frames. Where are the files and how do I reference them?

A. The files uploaded to the Cisco Clean Access Manager using the File Upload tab are located at /perfigo/control/tomcat/normal-webapps/admin in the Cisco Clean Access Manager.

Enter **https://manageripaddress/admin/file_name.htm** (for url) or **** (for jpg) to reference the files on the Right Frame box.

The screenshot shows the 'Administration > User Pages' interface. At the top, there are three tabs: 'Login Page', 'CleanMachines Page', and 'File Upload'. Below the tabs, there are links for 'List', 'Add', and 'Edit'. Underneath, there are four sub-tabs: 'General', 'Content', 'Style', and 'Right Frame'. The 'Right Frame' tab is selected. Below the sub-tabs, there is a text input field labeled 'Right Frame Content (as URL or HTML source):'. The text entered in the field is 'https://192.168.151.100/admin/Whats_new.htm'. There is a small icon to the right of the input field.

Q. I configured bandwidth management for the unauthenticated role, and my connection (or the Cisco Clean Access Manager) to the Cisco Clean Access Server is now very slow and it occasionally times out. Why is this?

A. In release 3.2, the communication bandwidth between the Cisco Clean Access Manager and the Cisco Clean Access Server is governed by the Unauthenticated Role bandwidth settings. Based on what your settings are, it can affect the communication bandwidth and can occasionally affect configuration publishing.

Cisco recommends that you do not set bandwidth management for the unauthenticated role in version 3.2 per this example:

User Management > User Roles				
List of Roles	New Role	Traffic Control	Bandwidth	
Role	Up/Down Kbps	Mode	Burst	Desc
Unauthenticated Role	Unlimited	Shared	1	
Temporary Role	700/700	Non-Shared	1	
Quarantine Role	700/700	Non-Shared	1	
Student	1000/1000	Non-Shared	1	
Gaming	1000/1000	Non-Shared	1	
bandwidth hogs	200/200	Non-Shared	1	
Staff	Unlimited	Shared	10	

Q. How do I find the number of users per OS logged on?

A. This first command gets you to the database CLI only:

◆ [Manager root]# psql -h 127.0.0.1 controlsmartdb -U postgres [ENTER]

The second command(s) gets you the various OSes only (one at a time):

- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_ALL';
- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_XP';
- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_98';
- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_95';
- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_ME';
- ◆ select count(*) from user_info WHERE os_name = 'WINDOWS_2K';
- ◆ select count(*) from user_info WHERE os_name = 'MAC_ALL';
- ◆ select count(*) from user_info WHERE os_name = 'MAC_OSX';
- ◆ select count(*) from user_info WHERE os_name = 'LINUX';

Q. Does CAM support EAP-TLS or EAP-TTLS authentication?

A. No, CAM does not support EAP-TLS and EAP-TTLS authentication.

Q. What does this [Failure] Error:"SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]:No such name" error message occur in switch?

A. This issue usually occurs when you try to change settings in the **PORTS tab > Switch Management > Devices > Switch of the CAM**. Correct the snmp community strings in the CAM configuration in order to resolve this issue.

Q. How do I add a Clean Access Server (CAS) into Clean Access Manager (CAM)?

A. You have to configure the ACS on the CAM as an authorized server so that the CAM establishes a connection to the CAS. Now you are able to add CAS into CAM. Refer to **Configure Clean Access Manager-to-Clean Access Server Authorization** for more information on how to add CAS to CAM.

Q. Why does the "unable to read cert found in /root/.chain.crt NAC only handles RSA keys <= 2048 ...java.io.IOException: subject key, Unknown key spec: Invalid RSA modulus size." error message appear?

A. Check the certificate that is used. Cisco Clean Access only supports 1024- and 2048-bit RSA key lengths for SSL certificates.

Q. When I try to save the running-config of the switch through SNMP, I get the failed to save the running configuration error message. Why does this error occur and how can this be resolved?

A. The failed to save the running configuration error message occurs when the time taken to save the running-config is more than the timeout set, which causes the process to save the configuration to fail. Increase the time out value in order to resolve this error. In order to change the timeout, choose **OOB Management > Profiles > SNMP Receiver > Advanced Settings** and change **SNMP Timeout** to a higher value.

Related Information

- [Cisco Clean Access Agent FAQ](#)
- [Cisco Clean Access Manager FAQ](#)
- [Cisco Clean Access Server FAQ](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

