



CHAPTER 12

Local Certified and Floating Devices

This chapter describes local Clean Access settings that can be configured for a particular CAS. For complete information on Clean Access configuration in the CAM web console, see the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(2\)](#). Topics in this chapter include:

- [Overview, page 12-1](#)
- [Clear Certified Devices, page 12-3](#)
- [Add Exempt Devices, page 12-2](#)
- [Clear Exempt Devices, page 12-2](#)
- [Specify Floating Devices, page 12-4](#)

Overview

Most elements of Clean Access, such as login pages, Nessus scan plugin behavior, Clean Access Agent requirements, and Clean Access user roles, are configured at the global level for all CASes. However, certain tasks can also be performed at the local level for an individual CAS. These include the following.

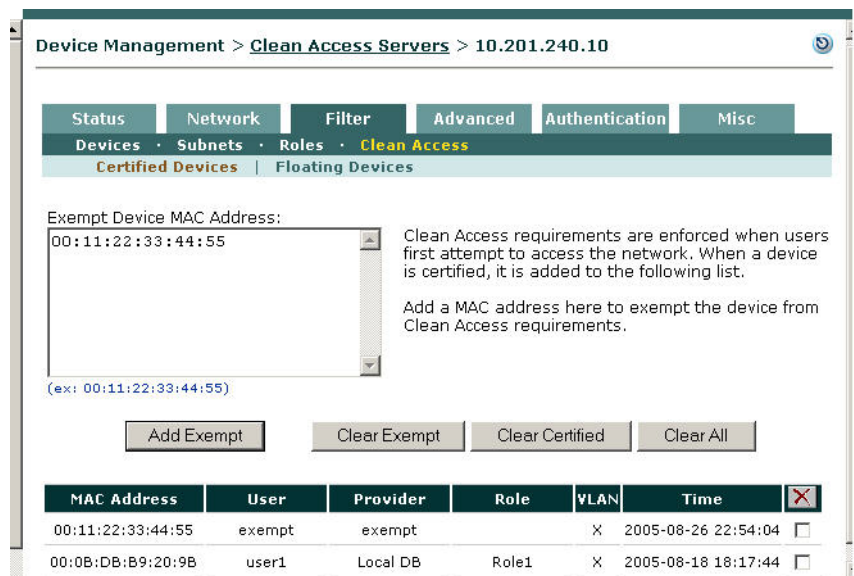
- Clearing certified devices
The Clean Access module on each Clean Access Server **automatically** adds devices to the Certified Devices list after the user authenticates and the device passes network scanning with no vulnerabilities found and/or meets Clean Access Agent requirements. Certified devices are considered clean until removed from the list. You can remove devices at a specified time or interval from the Certified Devices list in order to force them to repeat network scanning/Agent checking. Note that devices for Clean Access Agent users are always scanned for requirements at each login.
- Adding/clearing exempt devices
An exempt device is one which is never subject to Clean Access requirements. You can specify a device as exempt to allow it to bypass Clean Access requirements, or you can clear an exempt device to force it to meet Clean Access requirements. Adding or clearing exempt devices is always done **manually**.
- Specifying floating devices
A floating device requires Clean Access certification at every login and is certified only for the duration of a user session. Floating devices are always added manually.

Add Exempt Devices

Designating a device as exempt is the way a device can be **manually** added to the automatically-generated Certified Devices list. The CAS only adds a device to the Certified Devices list if the device has passed network scanning with no vulnerabilities found, or met Clean Access Agent system requirements, or both. Once added to the list, the device is considered clean and therefore exempt from having to go through certification while its MAC address remains on the Certified Devices list. Adding an exempt device in effect bypasses the automated Clean Access process to certify that the device you are adding to the list is clean.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**.

Figure 12-1 Certified Devices (Local)



2. Type the MAC address of the exempt device in the text field. Use line breaks to separate multiple addresses.
3. Click **Add Exempt**.

Clear Exempt Devices

Clearing an exempt device means you are removing it from the Certified Devices list and forcing it to go through Clean Access certification. Because exempt devices are manually added to the list, they must also be manually removed. This also means that an exempt device on the Certified Devices list is protected from being automatically removed when the global Certified Devices Timer is used to clear the list at regularly scheduled intervals.

To manually clear exempt devices from the list:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see [Figure 12-1](#)).
2. Click **Clear Exempt**. All exempt devices for this Clean Access Server will be cleared from the list.

Clear Certified Devices

Devices are added to the Certified Devices list by the Clean Access Server and are considered clean until removed from the list.

If a certified device is moved from one CAS to another, it must go through Clean Access certification again for the new CAS unless it has been manually added as an exempt device at the global level for all CASes. This allows for the case where one CAS has more restrictive Clean Access requirements than another.

The CAM maintains the central Certified Devices list, which stores device information according to the certifying Clean Access Server. The CAM then publishes each Clean Access Server's certified devices to the appropriate CAS as well as any globally exempt devices to all Clean Access Servers.

Though devices can only be certified and added to the list per CAS, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS. Clearing certified devices means you want to force the devices to repeat the Clean Access scanning/requirement checking.

- Global level (auto) — You can clear the list at regular intervals using the Certified Devices Timer form (**Device Management > Clean Access > Certified Devices > Timer**)
- Global level (manual) — You can manually clear the Certified Device list using the global form **Device Management > Clean Access > Certified Devices**.
- Local level (manual) — You can manually clear certified devices for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**



Note

- Clearing the Certified Device list either manually or automatically also logs the user off the network.
- Removing a user from **Monitoring > Online Users > View Online Users** does not remove the client from the Certified Devices list. This allows the user to log in again without forcing the client device to go through the Clean Access certification process when it is still considered clean.

To manually clear devices from the list for a specific Clean Access Server:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see [Figure 12-1](#)).
2. Click **Clear Exempt** to remove the devices that were added manually (using **Add Exempt**).
3. Click **Clear Certified** to remove the devices that were added to the list by meeting the Clean Access criteria.
4. Click **Clear All** to remove both types.
5. Remove individual users by selecting the checkbox next to the user's MAC address and clicking the **Kick Individual User** button.



Note

Only certified devices for the particular CAS will appear in the local list. To view certified devices for all Clean Access Servers, go to **Device Management > Clean Access**.

Specify Floating Devices

A floating device is certified only for the duration of a user session. Once the user logs out, the next user of the device needs to be certified again. Floating devices are useful for shared equipment, such as kiosk computers or wireless cards loaned out by a library.

You can also specify devices that are never exempt from certification requirements by MAC address. This is useful for multi-user devices, such as dialup routers that channel multi-user traffic from the untrusted (managed) network. In such cases, the Clean Access Server will see only the MAC address of that device as the source address of traffic from the trusted network. If the device is not configured as a floating device, this means that after the first user is certified, additional users will be unintentionally exempt from certification. By configuring the router's MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.

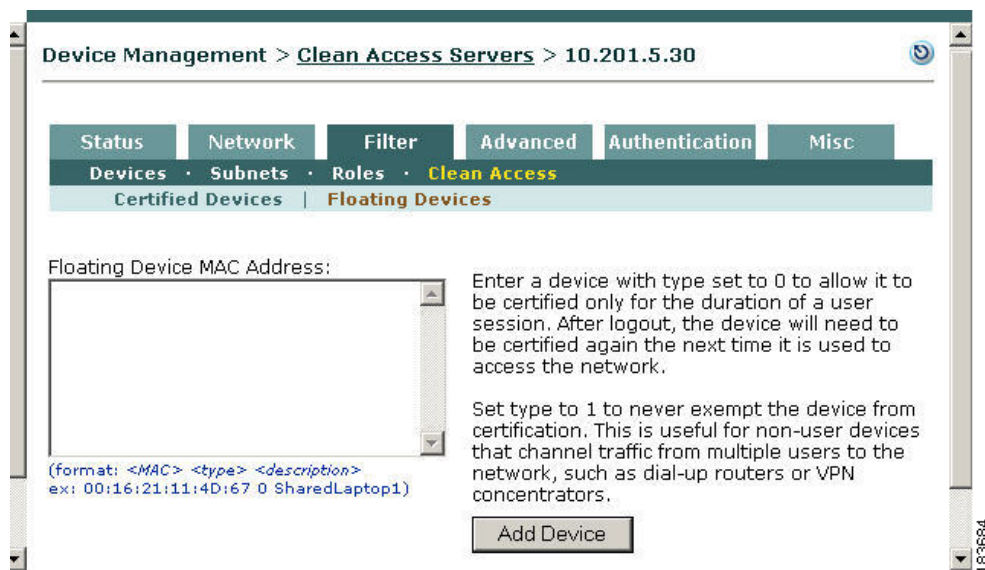
In this case, the users are distinguished by IP address. Note that users must have different IP addresses for this to work. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

See also [Add VPN Concentrator as a Floating Device](#), page 8-9.

To specify a local floating device:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Floating Devices**.

Figure 12-2 Floating Devices (Local)



2. Specify a floating device by MAC address in the form:

`<MAC> <type> <description>`

Where:

- *MAC* is the MAC address of the device (in standard hexadecimal MAC address format, e.g., 00:16:21:23:4D:00).
- *type* is either:
 - 0 - for session-scope certification, or

1 - if the device should never be considered certified

– *description* is an optional description of the device.

Be sure to include spaces between each element and use line breaks to separate multiple entries. For example:

```
00:16:21:23:4D:00 0 LibCard1
00:16:34:21:4C:00 0 LibCard2
00:16:11:12:4A:00 1 Router1
```

3. Click **Add Device** to save the setting.

To remove a floating MAC address, click the **Delete** icon next to the address.

