



CHAPTER 3

Device Management: Adding Clean Access Servers, Adding Filters

This chapter describes how to add and manage Clean Access Servers from the Clean Access Manager and configure device and/or subnet filters. It contains the following sections.

- [Working with Clean Access Servers, page 3-1](#)
- [Global and Local Administration Settings, page 3-6](#)
- [Global Device and Subnet Filtering, page 3-7](#)

The first step in implementing Cisco NAC Appliance is configuring devices in the Clean Access Manager (CAM)'s administrative domain. Clean Access Servers must be added to the CAM in order to manage them directly in the web console.

By default, Cisco NAC Appliance forces user devices on the untrusted side of the CAS to authenticate when attempting to access the network.

User roles, user authentication, user web pages, and traffic policies for in-band user traffic must be configured for users on the untrusted network as described in the following chapters:

- [Chapter 6, “User Management: Configuring User Roles and Local Users”](#)
- [Chapter 7, “User Management: Configuring Auth Servers”](#)
- [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#)

If deploying Cisco NAC Appliance for out-of-band, you will also need to configure the CAM as described in [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment”](#).

After Cisco NAC Appliance is configured for user traffic on the untrusted side of your network, you may need to allow devices on the untrusted side to **bypass** authentication and Clean Access certification (for example printers or VPN boxes). See [Global Device and Subnet Filtering, page 3-7](#) for how to configure filters in the Clean Access Manager for these kinds of devices.

Working with Clean Access Servers

The Clean Access Server gets its runtime parameters from the Clean Access Manager and cannot operate until it is added to the CAM's domain. Once the CAS is installed and added to the CAM, you can configure local parameters in the CAS and monitor it through the web admin console.

This section describes the following:

- [Add Clean Access Servers to the Managed Domain](#)
- [Troubleshooting when Adding the Clean Access Server](#)

- [Manage the Clean Access Server](#)
- [Check Clean Access Server Status](#)
- [Disconnect a Clean Access Server](#)
- [Reboot the Clean Access Server](#)
- [Remove the Clean Access Server from the Managed Domain](#)

For details on configuring local CAS-specific settings, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)*.

Add Clean Access Servers to the Managed Domain

The Clean Access Server must be running to be added to the Clean Access Manager.



Note

If intending to configure the Clean Access Server in Virtual Gateway mode (IB or OOB), you must disable or unplug the untrusted interface (eth1) of the CAS until after you have added the CAS to the CAM from the web admin console. Keeping the eth1 interface connected while performing initial installation and configuration of the CAS for Virtual Gateway mode can result in network connectivity issues.

For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**.

See the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)* for details.

To add a Clean Access Server:

1. From **Device Management**, click the **CCA Servers** link on the navigation menu.

Admin Name	Group Name	Description	Edit	Delete
admin	Full-Control Admin	Primary admin account		
testadmin	Full-Control Admin			

2. Click the **New Server** tab.

Figure 3-1 Add New Server

3. In the **Server IP address** field, type the IP address of the Clean Access Server's eth0 trusted interface.



Note The eth0 IP address of the CAS is the same as the Management IP address.

4. Optionally, in the **Server Location** field, type a description of the Clean Access Server's location or other identifying information.
5. For in-band operation, choose one of the following operating modes for the Clean Access Server from the **Server Type** list:
 - **Virtual Gateway** – Operates as an L2 transparent bridge, while providing IPSec, filtering, virus protection, and other services.
 - **Real-IP Gateway** – Acts as the default gateway for the untrusted network.
 - **NAT Gateway** – Acts as an IP router/default gateway and also provides NAT (Network Address Translation) services for the untrusted network.



Note NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because NAT Gateway is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is not supported for production deployment. Cisco NAC Appliance versions 4.1/4.0/3.6 use ports 20000-65535 (45536 connections) for NAT Gateway mode.

6. For out-of-band operation, you must choose one of the following out-of-band operating types:
 - **Out-of-Band Virtual Gateway** — Operates as a Virtual Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).
 - **Out-of-Band Real-IP Gateway** — Operates as a Real-IP Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).
 - **Out-of-Band NAT Gateway** — Operates as a NAT Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).



Note NAT Gateway (in-band or out-of-band) is not supported for production deployment.

The CAM can control both in-band and out-of-band Clean Access Servers in its domain. However, the CAS itself must be *either* in-band or out-of-band.

For more information on out-of-band deployment, see [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment.”](#)

See the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(1\)](#) for further details on the CAS operating modes and **NAT session throttling** for NAT gateways.

- Click **Add Clean Access Server**. The Clean Access Manager looks for the Clean Access Server on the network, and adds it to its list of managed Servers ([Figure 3-2](#)).

The Clean Access Server is now in the Clean Access Manager’s administrative domain.

Troubleshooting when Adding the Clean Access Server

See the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(1\)](#) for troubleshooting details.

Manage the Clean Access Server

After adding the Clean Access Server, you can configure CAS-specific settings such as VLAN Mapping or DHCP configuration. For some parameters, such as traffic control policies, the settings in the CAS can override the CAM’s global settings.

Once you add the CAS to the Clean Access Manager, the CAS appears in the **List of Servers** tab as one of the managed Servers, as shown in [Figure 3-2](#).

Figure 3-2 List of Servers Tab

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.10	Out-of-Band NAT Gateway	Dell350	Connected				
10.201.240.12	NAT Gateway	DellPowerEdge750	Connected				

Each Clean Access Server entry lists the IP address, server type, location, and connection status of the CAS. In addition four management control icons are displayed: **Manage**, **Disconnect**, **Reboot**, and **Delete**.

Click the **Manage** icon to administer the Clean Access Server.

**Note**

For further specifics on configuring Clean Access Servers (such as DHCP or high availability) see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(1\)](#).

Check Clean Access Server Status

The operational status of each Clean Access Server appears in the **Status** column:

- **Connected**—The CAM can reach the CAS successfully.
- **Not connected**—The CAS is rebooting, or the network connection between the CAM and CAS is broken.

If the Clean Access Server has a status of **Not connected** unexpectedly (that is, it is not down for standard maintenance, for example), try clicking the **Manage** button to force a connection attempt. If successful, the status changes to **Connected**. Otherwise, check for a connection problem between the CAM and CAS and make sure the CAS is running. If necessary, try rebooting the CAS.

**Note**

The Clean Access Manager monitors the connection status of all configured Clean Access Servers. The CAM will try to connect a disconnected CAS every 5 minutes.

Disconnect a Clean Access Server

When a Clean Access Server is disconnected, it displays **Not Connected** status but remains in the Clean Access Manager domain. You can always click **Manage** to connect the CAS and configure it.

Using the disconnect option is useful if you need to keep a Clean Access Server offline for maintenance work. Additionally, if at any point the Clean Access Server is out of sync with the Clean Access Manager, you can disconnect the Clean Access Server then reconnect it. The Clean Access Manager will again publish the data configured for the Clean Access Server and keep the CAS in sync.

In contrast, if you delete the Clean Access Server, all secondary configuration settings are lost.

Reboot the Clean Access Server

You can perform a graceful reboot of a Clean Access Server by clicking the **Reboot** button in the **List of Servers** tab. In a graceful reboot, the Clean Access Server performs all normal shutdown procedures before restarting, such as writing logging data to disk.

Remove the Clean Access Server from the Managed Domain

Deleting a Clean Access Server in the **List of Servers** tab removes it from the List of Servers and the system. To remove a Clean Access Server, click the **Delete** button next to the CAS. In order to reuse a Clean Access Server that you have deleted, you have to re-add it to the Clean Access Manager.

Note that when the Clean Access Server is removed, any secondary configuration settings specific to the CAS are deleted. Secondary settings are settings that are *not* configured at installation time or through the `service perfigo config` script, and include policy filters, traffic routing, and encryption parameters.

Settings that *are* configured at installation time, such as interface addresses, are kept on the Clean Access Server and are restored if the CAS is later re-added to the CAM's administrative domain.

Removing an active CAS has the following effect on users accessing the network through the CAS at the time it is deleted:

- If the CAS and CAM are connected when the CAS is deleted, the network connections for active users are immediately dropped. Users are no longer able to access the network. (This is because the CAM is able to delete the CAS's configuration immediately, so that the IP addresses assigned to active users are no longer valid in relation to any security policies applicable to the CASes.) New users will be unable to log into the network.
- If the connection between the CAS and CAM is broken at the time the CAS is deleted, active users will be able to continue accessing the network until the connection is reestablished. This is because the CAM cannot delete the CAS's configuration immediately. New users will be unable to log into the network.

Global and Local Administration Settings

The CAM web admin console has the following types of settings:

- **Clean Access Manager administration settings** are relevant only to the CAM itself. These include its IP address and host name, SSL certificate information, and High-Availability (failover) settings.
- **Global administration settings** are set in the Clean Access Manager and pushed from the CAM to all Clean Access Servers. These include authentication server information, global device/subnet filter policies, user roles, and Clean Access configuration.
- **Local administration settings** are set in the CAS management pages for a Clean Access Server and apply only to that CAS. These include CAS network settings, SSL certificates, DHCP and 1:1 NAT configuration, VPN concentrator configuration, IPSec key changes, local traffic control policies, and local device/subnet filter policies.

The global or local scope of a setting is indicated in the **Clean Access Server** column in the web admin console, as shown in [Figure 3-3](#).

Figure 3-3 Scope of Settings

Clean Access Server	MAC Address	User	Provi
GLOBAL	00:11:5B:22:27:CF	exempt	exempt
GLOBAL	00:0F:1F:1E:CS:28	exempt	exempt
GLOBAL	00:0C:76:0E:1E:28	exempt	exempt
192.168.0.100	00:0B:DB:DC:8F:A5	user1	Local

- **GLOBAL**—The entry was created using a global form in the CAM web admin console and applies to all Clean Access Servers in the CAM's domain.
- **<IP Address>**—The entry was created using a local form from the CAS management pages and applies only for the CAS with this IP address.

In general, pages that display global settings (referenced by GLOBAL) also display local settings (referenced by CAS IP address) for convenience. These local settings can usually be edited or deleted from global pages; however, they can only be **added** from the local CAS management pages for a particular Clean Access Server.

Global and Local Settings

Global (defined in CAM for all CASes) and local (CAS-specific) settings often coexist on the same CAS. If a global and local setting conflict, the local setting always overrides the global setting. Note the following:

- For device/subnet filter policies (which bypass authentication/certification requirements), local (CAS-specific) settings override global (CAM) settings.
- For other settings, such as traffic control policies, the priority of the policy (higher or lower) determines which global or local policy is enforced.
- Some features must be enabled both on the CAS (via the CAS management pages) and/or configured in the CAM console, for example:
 - L3 support (for multi-hop L3 deployments) is enabled per CAS, but may require login page/Agent configuration on CAM
 - Bandwidth Management is enabled per CAS but can be configured for all roles on the CAM
 - Active Directory SSO is configured per CAS but requires Auth Provider on CAM
 - Cisco VPN Concentrator SSO is configured per CAS but requires Auth Provider on CAM
- Clean Access requirements and network scanning plugins are configured globally from the CAM and apply to all CASes.

Global Device and Subnet Filtering

This section describes the following:

- [Overview](#)
- [Device Filters and User Count License Limits](#)
- [Adding Multiple Entries](#)
- [Corporate Asset Authentication and Posture Assessment by MAC Address](#)
- [Device Filters for In-Band Deployment](#)
- [Device Filters for Out-of-Band Deployment](#)
- [Device Filters for Out-of-Band Deployment Using VoIP Phones](#)
- [Device Filters and IPSec/L2TP/PPTP Connections to CAS](#)
- [Device Filters and Gaming Ports](#)
- [Global vs. Local \(CAS-Specific\) Filters](#)
- [Configure Device Filters](#)
- [Configure Subnet Filters](#)

Overview

By default, Cisco NAC Appliance forces user devices on the untrusted side of the CAS to authenticate when attempting to access the network.

If you need to allow devices on the untrusted side to **bypass** authentication and posture assessment (referred to as “Clean Access certification” in this document), you can configure device or subnet filters.

There are two ways to bypass Clean Access: Filter lists and Exempt list:

- Filter lists (configured under **Device Management > Filters**) can be set by MAC, IP or subnet, and can auto-set role assignment. Filters allow users (or devices) to bypass **both authentication and Clean Access certification (posture assessment)**. This section describes how to configure device and subnet filters.
- The Exempt list is set by MAC address (under **Device Management > Clean Access > Certified Devices > Add Exempt Device**) and allows users to bypass **Clean Access certification (posture assessment) only**. See [Add Exempt Device, page 9-27](#) for further details on the Exempt list.

Device filters are specified by MAC address (and optionally IP) of the device, and can be configured for either in-band (IB) or out-of-band (OOB) deployments. The MAC addresses are input and authenticated through the CAM, but the CAS is the device that performs the actual filtering action. For OOB, the use of device filters must also be enabled in the Port Profile (see [Add Port Profile, page 4-25](#)). For both IB and OOB, authentication and certification is bypassed for the devices put in the filter list.

Subnet filters can be configured for IB deployments only and are specified by subnet address and subnet mask (in CIDR format).

You can configure device or subnet filters to do the following:

- IB: Bypass login/certification and allow all traffic for the device/subnet.
OOB: Bypass login/certification and assign the Default Access VLAN to the device.
- IB: Block network access to the device/subnet.
OOB: Block network access and assign the Auth VLAN to the device.
- IB: Bypass login/certification and assign a user role to the device/subnet.
OOB: Bypass login/certification and assign the Out-of-Band User Role VLAN to the device (the Access VLAN configured in the user role).



Note

Because a device in a Filter entry is allowed/denied access without authentication, the device will not appear on the Online Users list (see [Online Users List, page 13-3](#) for details).

Some uses of device filters include:

- For printers on user VLANs, you can set up an “allow” device filter for the printer's MAC address to allow the printer to communicate with Windows servers. Cisco recommends configuring device filters for printers in OOB deployment also. This prevents a user from connecting to a printer port in order to bypass authentication.
- For in-band Cisco NAC Appliance L3/VPN concentrator deployment, you can configure a device or subnet filter to allow traffic from an authentication server on the trusted network to communicate with the VPN concentrator on the untrusted network.

Device Filters and User Count License Limits

- MAC addresses specified with the “ALLOW” option in the Device Filter list (bypass authentication/posture assessment/remediation) **do not** count towards the user count license limit.
- MAC addresses specified with the “CHECK” option in the Device Filter list (bypass authentication but go through posture assessment/remediation) **do** count towards the user count license limit.

**Note**

The maximum number of (non-user) devices that can be filtered is based on memory limitations and is not directly connected to user count license restrictions. A CAS can safely support approximately 5,000 MAC addresses.

Adding Multiple Entries

You can enter a large number of MAC addresses into the device filter list by:

1. Specifying wildcards and MAC address ranges when configuring device filters.
2. Copying and pasting individual MAC addresses (one per line) into the New Device Filter form and adding all of them with one click.
3. Using the API (`cisco_api.jsp`) `addmac` function to add the MAC addresses programmatically. See [API Support, page 14-36](#) for details.

Corporate Asset Authentication and Posture Assessment by MAC Address

Cisco NAC Appliance can perform MAC-based authentication and posture assessment (Clean Access certification) of client machines without requiring the user to log into Cisco NAC Appliance. This feature is implemented through the “CHECK” device filter control for global and local device filters, and the Clean Access Agent (see [Clean Access Agent Sends IP/MAC for All Available Adapters, page 10-8](#) for additional details).

The following Device Filter configuration options are available:

- **CHECK** and **IGNORE** device filter options.
- **ROLE** and **CHECK** filters require choosing a **User Role** from the dropdown menu.
- **IGNORE** is for OOB only. For IB, checking this option has no effect.
- **IGNORE** is for global filters only. It does not appear on CAS New/Edit filter pages.
- **IGNORE** device filters are intended to replace “allow” device filters that were specified for IP phones in previous releases.

**Note**

Administrators should reconfigure their device filters for IP phones to use the **IGNORE** option in order to avoid creating unnecessary MAC-notification traps. For more information, see [Device Filters for Out-of-Band Deployment Using VoIP Phones, page 3-11](#).

Device filter policies have different applicability in L2 deployments (deployments where the CAS is in L2 proximity to the end points/user devices) versus L3 deployments (where the CAS may be one or more hops away from the end points/user devices). Note that in an L3 deployment, the endpoint needs to access the network using a web browser (Applet/ActiveX) or the Clean Access Agent for Clean Access to be able to obtain the end point's MAC address. The behavior in L2 and L3 deployments is different, as described in [Table 3-1](#).

Table 3-1 CAM L2/L3 Device Filter Options

Option	L2	L3
ALLOW	Allows all traffic from the end-point - no authentication or posture assessment is required	Allows all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role - no authentication or posture assessment is required
DENY	Denies all traffic from the end-point	Denies all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role
ROLE	Allows traffic from the end-point without any authentication or posture assessment as specified by role traffic policies (for backward compatibility with CCA 3.x, this will continue to behave the same way)	Once MAC address is known, posture assessment is performed if configured following which traffic is allowed as per role traffic policies
CHECK	Performs posture assessment as specified for the Role following which traffic is allowed as per role traffic policies	Same as above
IGNORE	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)

Device Filters for In-Band Deployment

Cisco NAC Appliance assigns user roles to users either by means of authentication attributes, or through device/subnet filter policies. As a result, a key feature of device/subnet filter policy configuration is the ability to assign a system user role to a specified MAC address or subnet. Cisco NAC Appliance processing uses the following order of priority for role assignment:

1. MAC address
2. Subnet / IP address
3. Login information (login ID, user attributes from auth server, VLAN ID of user machine, etc.)

Therefore, if a MAC address associates the client with “Role A,” but the user’s login ID associates him or her to “Role B,” “Role A” is used.

For complete details on user roles, see [Chapter 6, “User Management: Configuring User Roles and Local Users.”](#)



Note

- For management of Access Points (APs) from the trusted side, you can ensure the APs are reachable from the trusted side (i.e. through SNMP, HTTP, or whatever management protocol is used) by configuring a filter policy through **Device Management > Filters > Devices**.
- When upgrading to 4.1(x), device filters added by the EOled AP Management feature will not be lost.

Device Filters for Out-of-Band Deployment

The Clean Access Manager respects the global Device Filters list for out-of-band deployments. As is the case for In-Band deployments, for OOB, the rules configured for MAC addresses on the global Device Filter list will have the highest priority for user/device processing. For OOB, the order of priority for rule processing is as follows:

1. Device Filters (if configured with a MAC address, and if enabled for OOB)
2. Certified Devices List
3. Out-of-Band Online User List

MAC address device filters configured for OOB have the following options and behavior:

- **ALLOW**—bypass login and posture assessment (certification) and assign **Default Access VLAN** to the port
- **DENY**—bypass login and posture assessment (certification) and assign **Auth VLAN** to the port
- **ROLE**—bypass login and L2 posture assessment (certification) and assign **User Role VLAN** to the port
- **CHECK**—bypass login, apply posture assessment, and assign **User Role VLAN** to the port
- **IGNORE**—ignore SNMP traps from managed switches (IP Phones)



Note

- To use global device filters for OOB, you must enable the **Change VLAN according to global device filter list** option for the Port Profile (under **Switch Management > Profiles > Port > New or Edit**). See [Add Port Profile, page 4-25](#) for details.
- This feature applies to global device filters only (does not apply to CAS-specific device filters).
- See [Out-of-Band User Role VLAN, page 6-10](#) for details on VLAN assignment via the user role.

For further details, see [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment.”](#)

Device Filters for Out-of-Band Deployment Using VoIP Phones

You must create a Global Device filter list of MAC Addresses designed to *ignore* IP phones through which client machines connect to your network. You can define a list of MAC Addresses by compiling a collection of individual MAC addresses (Cisco recommends this method only for small deployments), specify a range of MAC addresses using range delimiters and/or wildcard characters, and you can also extract a list of MAC addressees from an existing IP phone management application like Cisco CallManager.

Once you build a list of the applicable IP phone MAC addresses, ensure that the Cisco NAC Appliance system *ignores* them by enabling the **Change VLAN according to global device filter list** option for the Port Profile (under **Switch Management > Profiles > Port > New or Edit**) **when you configure your Cisco Clean Access system for OOB**. This ensures that the IP phones MAC-notification behavior cannot initiate a switch from one VLAN to another (from Access to Authentication VLAN, for example), thus inadvertently terminating the associated client machine’s connection. See [Configure OOB Switch Management in the CAM, page 4-17](#) for details.

Device Filters and IPSec/L2TP/PPTP Connections to CAS

Devices allowed in the MAC filter list cannot establish IPSec/L2TP/PPTP connections to the Clean Access Server (CAS). Only users logging in via web login or Clean Access Agent can establish IPSec/L2TP/PPTP connections to the CAS.

See “User Traffic Encryption” in the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)* for how to configure secure connections between the Clean Access Server and the end user device.



Warning

IPSec/L2TP/PPTP and roaming are deprecated and will be removed in future releases.

Device Filters and Gaming Ports

To allow gaming services, such as Microsoft XBOX Live, Cisco recommends creating a gaming user role and to add a filter for the device MAC addresses (under **Device Management > Filters > Devices > New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports. For additional details, see:

- [Allowing Gaming Ports, page 8-24](#)
- <http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16>
- [Add New Role, page 6-6](#)

Global vs. Local (CAS-Specific) Filters

You can add device/subnet filter policies at a global level, for all Clean Access Servers in the Clean Access Manager **Filters** pages, or for a specific Clean Access Server through the CAS management pages. The CAM stores both types of access filters and distributes the global filter policies to all Clean Access Servers and the local filter policies to the relevant CAS.

Note that for device/subnet filter policies, if a global and local setting conflict, the *local* setting overrides any global settings. (Refer to [Global and Local Administration Settings, page 3-6](#).)

This section describes the forms and the steps to add global access filter policies. See the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)* for how to add a local access filter policies.



Note

The CAM respects the global Device Filters list (not CAS-specific filters) for OOB deployments.

Configure Device Filters

This section describes the following:

- [Add Global Device Filter](#)
- [Display / Search Device Filter Policies](#)
- [Edit Device Filter Policies](#)
- [Delete Device Filter Policies](#)

Add Global Device Filter

If there is a MAC address entry in the Device Filter list, the machine can also be checked per Clean Access policies (e.g. Agent-based checks, network scanner checks). The device is authenticated based on MAC address but will still have to go through scanning (network and/or Agent).

A device filter set up as described in the following steps applies across all Clean Access Servers in the CAM domain.

1. Go to **Device Management > Filters > Devices > New**.

Figure 3-4 New Device Filter

Device Management > Filters

Devices Subnets
List · New · Order · Test · Active

By default, Cisco Clean Access (CAS) forces user devices (identified by MAC address and IP address combination) on the untrusted side of the CAS to authenticate in order to access the network. This page allows you to specify options to bypass authentication and posture assessment on devices's MAC address (and/or IP address).

Note that for Out-of-Band (OOB) deployments, you must enable the use of device filters in the Port Profile section [Switch Management > Profiles > Port].

MAC Address/IP Address Description (per entry)

Type one entry per line using format: <MAC>/<optional_IP> <optional_entry_description>
(ex: "00:16:21:11:4D:67/10.1.12.9 pocket_pc", "00:16:21:12:* group 1", "00:16:21:13:4D:12-00:16:21:13:E4:04 group2")
Note: You can use wildcard "*" or range "-" for MAC. Client must match both MAC/IP if specifying IP.

Description (all entries)

Access Type

- ALLOW: IB - bypass login, bypass posture assessment, allow access
OOB - bypass login, bypass posture assessment, assign Default Access VLAN
- DENY: IB - bypass login, bypass posture assessment, deny access
OOB - bypass login, bypass posture assessment, assign Auth VLAN
- ROLE: IB - bypass login, bypass L2 posture assessment, assign role
OOB - bypass login, bypass L2 posture assessment, assign User Role VLAN
- CHECK: IB - bypass login, apply posture assessment, assign role
OOB - bypass login, apply posture assessment, assign User Role VLAN
- IGNORE: OOB - ignore SNMP traps from managed switches (IP Phones)

User Role: Role1

Add

Note: Device filter policies have different applicability in L2 deployments (deployments where the CAS is in L2 proximity to the end points/user devices) versus L3 deployments (where the CAS may be one or more hops away from the end points/user devices). Note that in an L3 deployment, the endpoint needs to access the network using a web browser (Applet/ActiveX) or the Clean Access Agent for Clean Access to be able to obtain the end point's MAC address. The behavior in L2 and L3 deployments is different as follows:

Option	L2	L3
ALLOW	Allows all traffic from the end-point - no authentication or posture assessment is required	Allows all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role - no authentication or posture assessment is required. Note: If MAC address of next hop router connected to the untrusted side of CAS is allowed, all clients going through that router are allowed!
DENY	Denies all traffic from the end-point	Denies all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role
ROLE	Allows traffic from the end-point without any authentication or posture assessment as specified by role traffic policies (for backward compatibility with CCA 3.x, this will continue to behave the same way)	Once MAC address is known, posture assessment is performed if configured following which traffic is allowed as per role traffic policies
CHECK	Performs posture assessment as specified for the Role following which traffic is allowed as per role traffic policies	Same as above
IGNORE	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)

183731

- In the **New Device Filter** form, enter the MAC address of the device(s) for which you want to create a policy in the text field. Type one entry per line using the following format:

```
<MAC>/<optional_IP> <optional_entry_description>
```

Note the following:

- You can use wildcards “*” or a range “-” to specify multiple MAC addresses.
 - Separate multiple devices with a return.
 - As an option, you can enter an IP address with the MAC to make sure no one spoofs the MAC address to gain network access. If you enter both a MAC and an IP address, the client must match both for the rule to apply.
 - You can specify a description by device or for all devices. A description specific to a particular device (in the MAC Address field) supersedes a description that applies all devices in the **Description (all entries)** field. There cannot be spaces within the description in the device entry (see [Figure 3-4](#)).
- Choose the policy for the device from the **Access Type** choices:
 - **ALLOW**
IB - bypass login, bypass posture assessment, allow access
OOB - bypass login, bypass posture assessment, assign Default Access VLAN
 - **DENY**
IB - bypass login, bypass posture assessment, deny access
OOB - bypass login, bypass posture assessment, assign Auth VLAN
 - **ROLE**
IB - bypass login, bypass L2 posture assessment, assign role
OOB - bypass login, bypass L2 posture assessment, assign User Role VLAN. The Out-of-Band User Role VLAN is the Access VLAN configured in the user role. See [Chapter 6, “User Management: Configuring User Roles and Local Users”](#) for details.
 - **CHECK**
IB - bypass login, apply posture assessment, assign role
OOB - bypass login, apply posture assessment, assign User Role VLAN
 - **IGNORE**
OOB (only) - ignore SNMP traps from managed switches (IP Phones)



Note

For OOB, you must also enable the use of global device filters at the Port Profile level under **Switch Management > Profiles > Port > New** or **Edit**. See [Add Port Profile, page 4-25](#) for details.

- Click **Add** to save the policy.
- The **List** page under the **Devices** tab appears.

The following examples are all valid entries (that can be entered at the same time):

```
00:16:21:11:4D:67/10.1.12.9 pocket_pc
00:16:21:12:* group1
00:16:21:13:4D:12-00:16:21:13:E4:04 group2
```



Note

If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See [Control Bandwidth Usage, page 8-13](#) for details.

**Note**

Troubleshooting Tip: If you see ERROR: “Adding device MAC failed” and you are unable to add any devices in the filter list (regardless of which option is checked, or whether an IP address/description is included), check the Event Logs. If you see “xx:xx:xx:xx:xx:xx could not be added to the MAC list”, this can indicate that one of the CASes is disconnected.

Display / Search Device Filter Policies

- Priorities can be defined for ranges (via the Order page)
 - A single MAC address device filter (e.g. 00:14:6A:6B:6C:6D) always takes precedence on the filter List over a wildcard/range device filter (e.g. 00:14:6A:6B:*, or 00:14:6A:*).
 - New wildcard/range device filters are always put at the end of the **List** page. To change the priority, go to the **Order** page.
 - The role assignment for a single MAC address device filter always takes precedence over other filters. You can check the role assignment to be used for a MAC address using the **Test** page.
 - The **Test** page shows which filter will take effect for the MAC address entered.
1. You can narrow the number of devices displayed in the filter list (under **Device Management > Filters > Devices > List**) using the following search criteria:
 - Clean Access Server: Any CAS, GLOBAL, or <CAS IP address>
 - Access: Any Access, allow, deny, use role
 - MAC Address
 - IP Address
 - Description

For MAC Address, IP Address and Description searches, you can select **equals** (exact match), **starts with**, **ends with**, or **contains** operators for text entered in the search text field.

2. Click the **View** button after entering the search criteria to display the desired search.

Figure 3-5 Device Filters List

The screenshot shows the 'Device Management > Filters' interface. At the top, there are tabs for 'Devices' and 'Subnets', with 'Devices' selected. Below the tabs are navigation links: 'List', 'New', 'Order', 'Test', and 'Active'. There are two dropdown menus for 'Any CCA Server' and 'Any Access'. A search bar contains 'Search For: - Select Field - equals'. Below the search bar are 'Reset View', 'Delete List', and 'View' buttons. A table displays MAC filter addresses. The table has columns: MAC Address, IP Address, Clean Access Server, Description, Access Type, Priority, Edit, and a delete icon. The first two rows are highlighted in yellow. The first row has MAC Address 00:12:11:22:33:44, IP Address (empty), Clean Access Server GLOBAL, Description VoIP_1, Access Type ALLOW, Priority 0, and Edit icons. The second row has MAC Address 00:16:21:12:4D:68, IP Address 10.201.240.10, Clean Access Server (empty), Description (empty), Access Type DENY, Priority 0, and Edit icons. Below the table, there is a pagination bar: 'MAC Filter Addresses 1-2 of 2 | First | Previous | Next | Last |'. A red box highlights the '2' in this bar, with a red arrow pointing to it from the text 'filtered devices indicator' on the right.

MAC Address	IP Address	Clean Access Server	Description	Access Type	Priority	Edit	
00:12:11:22:33:44		GLOBAL	VoIP_1	ALLOW	0		
00:16:21:12:4D:68	10.201.240.10			DENY	0		

3. Clicking **Reset View** resets the list to display all entries (default). Use the **First**, **Previous**, **Next**, and **Last** links to navigate the pages. A maximum of 25 entries are shown per page.

183730

The **Clean Access Server** column in the list shows the scope of the policy. If the policy was configured locally in the CAS management pages, this field displays the IP address of the originating Clean Access Server. If the policy was configured globally for all Clean Access Servers in the **Device Management > Filters** module of the admin console, the field displays **GLOBAL**.

The filter list can be sorted by column by clicking on the column heading label (MAC Address, IP Address, Clean Access Server, Description, Access Type).

See [Global and Local Administration Settings, page 3-6](#) and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)* for further details.

Order Device Filter Wildcard/Range Policies

The **Order** page is for **wildcard/range** device filters **only**. The **Order** page is used to change the priority of wildcard/range device filters.

For example:

- If the **Order** page is configured with filters as follows:

- 00:14:6A:* — Access Type: DENY
- 00:14:6A:6B:* — Access Type: IGNORE

A device with MAC address 00:14:6A:6B:60:60 will be denied.

- If the **Order** page is configured as follows:

- 00:14:6A:6B:* — Access Type: IGNORE
- 00:14:6A:* — Access Type: DENY

A device with MAC address 00:14:6A:6B:60:60 will have access type IGNORE.

However, if a device filter exists for the exact MAC address 00:14:6A:6B:60:60, the rules of that filter apply instead, and any existing wildcard/range filters are not used.

- Go to **Device Management > Filters > Devices > Order**

Figure 3-6 Order

Device Management > Filters

Devices Subnets

List · New · Order · Test · Active

MAC filter entries with single MAC address have higher precedence over those with MAC address wildcard or range.

Commit: save changes; Reset: cancel changes.

MAC Address	IP Address	Clean Access Server	Description	Access Type	Priority
00:16:21:13:4D:12-00:16:21:13:E4:04		GLOBAL	group2	ALLOW	▲ ▼
00:16:21:12:*		GLOBAL	group1	ALLOW	▲ ▼

Commit Reset

- Click the arrows in the **Priority** column to move the priority of the wildcard/range filter up or down.
- Click **Commit** to apply the changes. (Click **Reset** to cancel the changes.)

Test Device Filter Policies

The **Test** page control allows administrators to determine which device filter and access type will be applied to the specified MAC address for a particular Clean Access Server.

1. Go to **Device Management > Filters > Devices > Test**
2. Type the MAC address of the device in the **MAC Address** field.
3. Choose CAS to test against from the **Clean Access Server** dropdown menu.
4. Click **Submit**. The **Access Type** specified for the corresponding device filter appears in the list below.

Figure 3-7 Test

Device Management > Filters

Devices Subnets

List · New · Order · Test · Active

MAC Address: Clean Access Server:

Find out which MAC filter entry will be applied to the specified MAC address on the specified Clean Access Server.

MAC Address	IP Address	Clean Access Server	Description	Access Type	Priority
00:16:21:11:4D:67	10.1.12.9	GLOBAL	pocket_pc	ALLOW	

183729

View Active L2 Device Filter Policies

The Active L2 In-Band Device Filters list displays all clients currently connected to the CAS, sending packets, and with their MAC addresses in a device filter. This list is especially useful in cases where users are configured to bypass authentication (via device filters) and/or posture assessment (such as when no requirements are enforced). Though by definition these users will not appear in the Online Users List or Certified Device List, they can still be tracked on the in-band network through the Active L2 Device Filters List.

To view active L2 devices in filter policies across all Clean Access Servers

1. Go to **Device Management > Filters > Devices > Active**
2. Click the **Show All** button first to populate the **Active** page with the information from all clients currently connected to the CAS, sending packets, and with their MAC addresses in a device filter.

You can also perform a **Search** on a client IP or MAC address to populate the page with the result. By default, the **Search** parameter performed is equivalent to “contains” for the value entered in the **Search IP/MAC Address** field.



Note

For performance considerations, the **Active** page only displays the most current device information when you refresh the page by clicking **Show All** or **Search**.

Figure 3-8 Active

**Note**

To view active devices for an individual CAS, go **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Devices > Active**.

Edit Device Filter Policies

1. Clicking the **Edit** button next to device filter policy in the filter list. The **Edit** page appears.
2. You can edit the IP Address, Description, Access Type, and role used. Click **Save** to apply the changes.
3. Note that the MAC address is not an editable property of the filter policy. To modify a MAC address, create a new filter policy and delete the existing policy (as described below).

Delete Device Filter Policies

There are two ways to delete a device access policy or policies:

- Select the checkbox next to it in the List and click the delete button. Up to 25 device access policies per page can be selected and deleted in this way.
- Use the search criteria to select the desired device filter policies and click **Delete List**. This removes all devices filtered by the search criteria across the number of applicable pages. Devices can be selectively removed using any of the search criteria used to display devices. The “filtered devices indicator” shown in [Figure 3-5](#) displays the total number of filtered devices that will be removed when **Delete List** is clicked.

Configure Subnet Filters

The **Subnets** tab ([Figure 3-9](#)) allows you to specify authentication and access filter rules for an entire subnet. All devices accessing the network on the subnet are subject to the filter rule.

To set up subnet-based access controls:

1. Go to **Device Management > Filters > Subnets**.

Figure 3-9 Subnet Filters

By default, managed clients must log in to access the network. Set up alternate access policies by subnet here. You can permit access without authentication, block access, or permit access without authentication with a role. If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

Subnet Address/Netmask: /
(CIDR format, ex: 192.168.128.0/22)

Description:

Access Type: allow deny
 use role:

Subnet	Clean Access Server	Description	Access Type	Edit	Del
192.168.128.0 / 22	GLOBAL	admin	allow		
10.2.12.0 / 22	GLOBAL	building 2	allow		

- In the **Subnet Address/Netmask** fields, enter the subnet address and subnet mask in CIDR format.
- Optionally, type a **Description** of the policy or device.
- Choose the network **Access Type** for the subnet:
 - allow** – Enables devices on the subnet to access the network without authentication.
 - deny** – Blocks devices on the subnet from accessing the network.
 - use role** – Allows access without authentication and applies a role to users accessing the network from the specified subnet. If you select this option, also select the role to apply to these devices. See [Chapter 6, “User Management: Configuring User Roles and Local Users”](#) for details on user roles.
- Click **Add** to save the policy.

The policy takes effect immediately and appears at the top of the filter policy list.

**Note**

If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See [Control Bandwidth Usage, page 8-13](#) for details.

After a subnet filter is added, you can remove it using the **Delete** button or edit it by clicking the **Edit** button. Note that the subnet address is not an editable property of the filter policy. To modify a subnet address, you need to create a new filter policy and delete the existing one.

The **Clean Access Server** column in the list of policies shows the scope of the policy. If the policy was configured as a local setting in a Clean Access Server, this field identifies the CAS by IP address. If the policy was configured globally in the Clean Access Manager, the field displays GLOBAL.

The filter list can be sorted by column by clicking on the column heading label (Subnet, Clean Access Server, Description, Access Type).

