Network Admission Control (NAC) protects data networks from computer viruses by assessing the health of client workstations, ensuring that they receive the latest available virus signature updates, and controlling their access to the network.

NAC works with antivirus software to assess the condition of a client, called the client’s *posture*, before allowing the client access to the network. NAC ensures that a network client has an up-to-date virus signature set which has not been infected. If the client requires a signature update, NAC directs it to complete the update. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment until disinfection is completed.

For more information on NAC, click the following links:


Create NAC Tab

You use the Create NAC tab and NAC wizard to create a NAC policy and associate it with an interface. After you create the NAC policy, you can edit it by clicking *Edit NAC* and choosing it in the policy list.
Create NAC Tab

The NAC configuration on the router is only one part of a complete NAC implementation. Click Other Tasks in a NAC Implementation to learn the tasks that must be performed on other devices in order to implement NAC.

Enable AAA Button

Authentication, authorization, and accounting (AAA) must be enabled on the router before you can configure NAC. If AAA is not enabled, click the Enable AAA button. If AAA has already been configured on the router, this button is not displayed.

Launch NAC Wizard Button

Click this button to launch the NAC wizard. The wizard divides NAC configuration into a series of screens in which you complete a single configuration task.

How Do I List

If you want to create a configuration that this wizard does not guide you through, click the button next to this list. It lists other types of configurations that you might want to perform. If you want to learn how to create one of the configurations listed, choose the configuration and click Go.

Other Tasks in a NAC Implementation

A full NAC implementation includes the following configuration steps:

**Step 1** Install and configure the Cisco Trust Agent (CTA) software on network hosts. This provides hosts with a posture agent capable of responding to EAPoUDP queries by the router. See the links after these steps to obtain the CTA software and learn how to install and configure it.

**Step 2** Install and configure an AAA authentication EAPoUDP server. This server must be a Cisco Secure Access Control Server (ACS) using the RADIUS protocol. Cisco Secure Access Control Server software version 3.3 is required. See the links after these steps to learn more about installing and configuring ACS.
Welcome

The NAC wizard enables you to do the following:

- Choose the interface on which NAC is to be enabled—Hosts attempting access to the network through this interface must undergo the NAC validation process.
- Configure NAC Policy Servers—Admission control polices are configured on these servers, and the router contacts them when a network host attempts to access the network. You can specify information for multiple servers. NAC policy servers use the RADIUS protocol.
Configure a NAC exception list—Hosts such as printers, IP phones, and hosts without NAC posture agents installed may need to bypass the NAC process. Hosts with static IP addresses and other devices can be identified in an exception list, and be handled using an associated exception policy. Hosts can also be identified by their MAC address, or by their device type.

Configure an agentless host policy—If you want to use a policy residing on a Cisco Secure ACS server to handle hosts without an installed posture agent, you can do so. When the Cisco Secure ACS server receives a packet from an agentless host, it responds by sending the agentless host policy. Configuring an agentless host policy is useful when there are agentless hosts that are dynamically addressed, such as DHCP clients.

Configuring NAC for remote access—Hosts using Cisco SDM to manage the router must be allowed access. The wizard lets you specify IP addresses for remote management so that Cisco SDM can modify the NAC ACL to allow the hosts with those addresses access to the router.

Configuring NAC on the router is the last step in a NAC configuration. Before you configure the router with this feature, complete the steps described in the following link: Other Tasks in a NAC Implementation.

NAC Policy Servers

NAC admission control policies are configured and stored in a policy database residing on RADIUS servers running Cisco Secure ACS version 3.3. The router must validate the credentials of network hosts by communicating with the RADIUS server. Use this window to provide the information the router needs to contact the RADIUS servers. Each RADIUS server that you specify must have Cisco Secure Cisco Access Control Server (ACS) software version 3.3 installed and configured.

Choose the RADIUS client source

Configuring the RADIUS source allows you to specify the source IP address to be sent in RADIUS packets bound for the RADIUS server. If you need more information about an interface, choose the interface and click the Details button. The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco ACS version 3.3 or later.
If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of the interface through which the RADIUS packets exit the router.

If you choose an interface, the source IP address in the RADIUS packets will be the address of the interface that you chose as the RADIUS client source.

---

**Note**

Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.

---

**Details Button**

If you need a quick snapshot of the information about an interface before choosing it, click **Details**. The screen shows you the IP address and subnet mask, the access rules and inspection rules applied to the interface, the IPSec policy and QoS policy applied, and whether there is an Easy VPN configuration on the interface.

---

**Server IP, Timeout, and Parameters Columns**

The Server IP, Timeout, and Parameters columns contain the information that the router uses to contact a RADIUS server. If no RADIUS server information is associated with the chosen interface, these columns are blank.

---

**Use for NAC Check Box**

Check this box if you want to use the listed RADIUS server for NAC. The server must have the required admissions control policies configured if NAC is to be able to use the server.

---

**Add, Edit, and Ping Buttons**

To provide information for a RADIUS server, click the **Add** button and enter the information in the screen displayed. Choose a row and click **Edit** to modify the information for a RADIUS server. Choose a row and click **Ping** to test the connection between the router and a RADIUS server.
When performing a ping test, enter the IP address of the RADIUS source interface in the source field in the ping dialog. If you chose Router chooses source, you need not provide any value in the ping dialog source field.

The Edit and Ping buttons are disabled when no RADIUS server information is available for the chosen interface.

**Interface Selection**

Choose the interface on which to enable NAC in this window. Choose the interface through which network hosts connect to the network.

Click the Details button to display the policies and rules associated with the interface you choose. The window displays the names of the ACLs applied to inbound and to outbound traffic on this interface.

If an inbound ACL is already present on the interface, Cisco SDM uses that ACL for NAC by adding appropriate permit statements for EAPoUDP traffic. If the IP address of the interface on which NAC is being applied were 192.55.22.33, a sample permit statement might be the following:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

The permit statement that Cisco SDM adds uses the port number 21862 for the EAPoUDP protocol. If the network hosts run EAPoUDP on a custom port number, you must modify this ACL entry to use the port number that the hosts use.

If no inbound ACL is configured on the interface you specify, you can have Cisco SDM apply an ACL to the interface. You can choose a recommended policy, or a policy that simply monitors reported NAC postures.

- **Strict Validation (Recommended)**—Cisco SDM applies an ACL that denies all traffic (deny ip any any). Admission to the network is determined by the NAC validation process. By default, all traffic is denied except the traffic found to be valid based on the policy configured on the NAC policy server.

- **Monitor NAC Postures**—Cisco SDM applies an ACL that permits all traffic (permit ip any any). After the NAC validation process, the router may receive policies from the NAC server that deny access to certain hosts. You can use the Monitor NAC Postures setting to determine the impact of NAC configuration on the network. After you have done so, you can modify the
policies on the NAC policy server, and then reconfigure NAC on the router to use **Strict Validation**, by changing the ACL applied to the interface to **deny ip any any** using the Cisco SDM Firewall Policy feature.

## NAC Exception List

You can identify hosts that must be allowed to bypass the NAC validation process. Typically, hosts such as printers, IP phones, and hosts without NAC posture agent software installed are added to the exception list.

If there are hosts without static addresses on your network it is recommended that they be entered in the agentless host policy, and not in the NAC exception list. The NAC exception policy may not work properly if host IP addresses change.

If you are using the NAC wizard and you do not need to configure a NAC exception list, you can click **Next** without entering information in this window. As an alternative or as a complement to the NAC exception list, the wizard allows you to configure an agentless host policy in another window.

### IP Address/MAC Address/Device Type, Address/Device, and Policy Columns

These columns contain information about a host in the exception list. A host can be identified by its IP address, MAC address, or the type of device it is. If it is identified by an address, the IP address or MAC address is shown in the row along with the name of the policy that governs the host access to the network.

### Add, Edit, and Delete Buttons

Build the exception list by clicking **Add** and entering information about a host. You can use the **Add** button as many times as you need to.

Choose a row and click **Edit** to change information about a host. Click **Delete** to remove information about a host from this window. The Edit and Delete buttons are disabled when there is no information in this list.

### Add or Edit an Exception List Entry

Add or edit the information in an exception list entry in this window.
**Type List**

Hosts are chosen by the way they are identified. This list contains the following selections:

- **IP Address**—Choose this if you want to identify the host by its IP address.
- **MAC Address**—Choose this if you want to identify the host by its MAC address.
- **Cisco IP Phone**—Choose this if you want to include the Cisco IP phones on the network in the exception list.

**Specify Address Field**

If you choose IP Address or MAC Address as the host type, enter the address in this field. If you choose a device type, this field is disabled.

**Policy Field**

If you know the name of the exception policy, enter it in this field. Click the button with three dots to the right of the Policy field to choose an existing policy or to display a dialog box in which you can create a new policy.

**Choose an Exception Policy**

Choose the policy that you want to apply to the host. When you choose a policy, the redirect URL specified for the policy appears in a read-only field, and the access rule entries for the policy are displayed.

If no policies are available in the list, click **Cancel** to return to the wizard screen, and then choose the option that allows you to add a policy.

Choose the policy that you want to apply to the excepted host from the list. If there are no policies in the list, click **Cancel** to return to the wizard. Then choose **Create a new policy** and choose it in the Add to the Exception List window.

**Redirect URL: URL Field**

This read-only field displays the redirect URL associated with the policy that you choose. Hosts to which this policy is applied are redirected to this URL when the attempt to access the network.
**Preview of Access Rule**

The Action, Source, Destination, and Service columns show the ACL entries in the access rule associated with the policy. These columns are empty if no ACL is configured for this policy.

**Add Exception Policy**

Create a new exception policy in this window.

To create a new exception policy, enter a name for the policy, and either specify an access rule that defines the IP addresses that hosts in the exception list can access, or enter a redirect URL. The redirect URL should contain remediation information that enables users to update their virus definition files. You must provide either an access rule name or a redirect URL. You can specify both.

**Name Field**

Enter the name for the policy in this field. Do not use question mark (?) characters or space characters in policy names. Limit each policy name to no more than 256 characters.

**Access Rule Field**

Enter the name of the access rule that you want to use, or click the button to the right of this field to browse for an access rule or create a new access rule. The access rule must contain permit entries that specify the IP addresses that hosts on the exception list can connect to. The access rule must be a named ACL; numbered ACLs are not supported.

**Redirect URL Field**

Enter a URL that contains the remediation information for your network. This information might contain instructions for downloading virus definition files.

A remediation URL might look like the following:

http://172.23.44.9/update

Redirect URLs are usually of the form http://URL, or https://URL.
Agentless Host Policy

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used as an alternative or as a complement to a NAC exception list. If you are using the NAC wizard and you do not need to configure an agentless host policy, you can click Next without entering information in this window.

Authenticate Agentless Hosts Check Box

Check this box to indicate that you want to use the agentless hosts policy on the Cisco Secure ACS server.

Username and Password Fields

Some Cisco IOS software images require that a username and password be supplied along with the request to the Cisco Secure ACS server. If this is required, enter the username and password configured on the Cisco Secure ACS server for this purpose. If the Cisco IOS software image does not require this information, these fields do not appear.

Configuring NAC for Remote Access

Configuring NAC for remote access allows you to modify the ACLs that NAC configuration creates so that they will permit Cisco SDM traffic. Specify the hosts that must be able to use Cisco SDM to access the router.

Enable Cisco SDM Remote Management

Check this box to enable Cisco SDM remote management on the named interface.

Host/Network Address Fields

If you want Cisco SDM to modify the ACL to allow Cisco SDM traffic from a single host, choose Host Address and enter the IP address of a host. Choose Network Address and enter the address of a network and a subnet mask to allow
Cisco SDM traffic from hosts on that network. The host or network must be accessible from the interfaces that you specified. Choose **Any** to allow Cisco SDM traffic from any host connected to the specified interfaces.

**Modify Firewall**

Cisco SDM checks each **ACL** applied to the interface specified in this configuration to determine if it blocks any traffic that should be allowed through the firewall so that the feature you are configuring will work.

Each interface is listed, along with the service currently being blocked on that interface, and the ACL that is blocking it. If you want Cisco SDM to modify the ACL to allow the traffic listed, check the **Modify** box in the appropriate row. If you want to see the entry that Cisco SDM will add to the ACL, click the **Details** button.

In the following table, FastEthernet0/0 has been configured for **NAC**. This interface is configured with the services shown in the Service column.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Service</th>
<th>ACL</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>RADIUS Server</td>
<td>101 (INBOUND)</td>
<td>[ ] Modify</td>
</tr>
<tr>
<td>FastEthernet0/0</td>
<td>DNS</td>
<td>100 (INBOUND)</td>
<td>[ ] Modify</td>
</tr>
<tr>
<td>FastEthernet0/0</td>
<td>DHCP</td>
<td>100 (INBOUND)</td>
<td>[ ] Modify</td>
</tr>
<tr>
<td>FastEthernet0/0</td>
<td>NTP</td>
<td>101 (INBOUND)</td>
<td>[ ] Modify</td>
</tr>
<tr>
<td>FastEthernet0/0</td>
<td>VPN</td>
<td>190 (INBOUND)</td>
<td>[ ] Modify</td>
</tr>
</tbody>
</table>

**Details Window**

This window displays the entries that Cisco SDM will add to ACLs to allow services needed for the service you are configuring. The window might contain an entry like the following:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

In this case, web traffic whose port number is greater than 1024 is permitted from the host 10.77.158.84 on the local network to the host 10.77.158.1.
Summary of the configuration

This window summarizes the information you entered, and allows you to review it in a single window. You can use the Back button to return to any wizard screen to change information. Click **Finish** to deliver the configuration to the router.
Here is an example of a NAC configuration summary:

NAC Interface: FastEthernet0/1.42
Admission Name:: SDM_EOU_3

AAA Client Source Interface: FastEthernet0/1.40
NAC Policy Server 1: 10.77.158.54

Exception List

<table>
<thead>
<tr>
<th>Address/Device</th>
<th>IP Address</th>
<th>(22.22.22.2) newly added</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Details:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Name:</td>
<td>P55</td>
<td></td>
</tr>
<tr>
<td>Redirect URL:</td>
<td><a href="http://www.fix.com">http://www.fix.com</a></td>
<td></td>
</tr>
<tr>
<td>Access Rule:</td>
<td>test11</td>
<td></td>
</tr>
</tbody>
</table>

Enabled agentless host policy
Username: bill
Password: ******

In this example, RADIUS packets will have the IP address of FastEthernet 0/1.40. NAC is enabled on FastEthernet 0/1.42, and the NAC policy that the wizard applied is SDM_EOU_3. One host has been named in the exception list, and its access to the network is controlled by the exception policy P55.

**Edit NAC Tab**

The Edit NAC tab lists the NAC policies configured on the router and enables you to configure other NAC settings. A NAC policy must be configured for each interface on which posture validation is to be performed.

**NAC Timeouts Button**

The router and the client use Extensible Authentication Protocol over Unformatted Data Protocol (EAPoUDP) to exchange posture information. Default values for EAPoUDP timeout settings are preconfigured, but you can change the settings. This button is disabled if there is no NAC policy configured on the router.
Agentless Host Policy Button

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used when such hosts do not have static IP addresses. This button is disabled if there is no NAC policy configured on the router.

Add, Edit, and Delete Buttons

These buttons allow you to manage the NAC policy list. Click Add to create a new NAC policy. Use the Edit and Delete buttons to modify and remove NAC policies. The Edit and Delete buttons are disabled when no NAC policies have been configured on the router.

Only the Add button is enabled when there is no NAC policy configured on the router. The Add button is disabled when all router interfaces are configured with a NAC policy.

NAC Policies List

The name, the interface to which the NAC policy is applied, and the access rule that defines the policy are included in the list. If you enabled NAC on an interface using the Create NAC wizard, the default NAC policy SDM_EOU_1 appears in this list.

NAC Components

This window provides a brief description of the EAPoUDP components that Cisco SDM allows you to configure.

Exception List Window

This placeholder topic will be removed when the help system for NAC is built. This help topic has already been written for wizard mode. To view it, click the following link:

NAC Exception List
Exception Policies Window

NAC exception policies control the network access of hosts in the exception list. A NAC exception policy consists of a name, an access rule, and/or a redirect URL. The access rule specifies the destinations to which hosts governed by the policy have access. If a redirect URL is specified in the policy, the policy can point web clients to sites that contain information on how to obtain the latest available virus protection.

An example of a NAC policy entry is shown in the following table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Access Rule</th>
<th>Redirect URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>NACLess</td>
<td>nac-rule</td>
<td><a href="http://172.30.10/update">http://172.30.10/update</a></td>
</tr>
</tbody>
</table>

Access rules associated with NAC policies must be extended ACLs, and must be named. An example of an access rule that might be used in a NAC policy is shown in the following table:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Log</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>any</td>
<td>172.30.2.10</td>
<td>ip</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This rule permits any host governed by the policy to send IP traffic to the IP address 172.30.2.10.

Add, Edit, and Delete Buttons

Click the Add button to create a new exception policy. Use the Edit button to modify existing exception policies, and the Delete button to remove exception policies. The Edit and Delete buttons are disabled when there are no exception policies in the list.

NAC Timeouts

Configure the timeout values the router is to use for EAPoUDP communication with network hosts. The default, minimum, and maximum values for all settings are shown in the following table.
Interface Selection

Choose the interface to which the NAC timeout settings are to apply.

Hold Period Timeout Field

Enter the number of seconds that the router is to ignore packets from clients that have just failed authentication.

Retransmit Timeout Field

Enter the number of seconds that the router is to wait before retransmitting EAPoUDP messages to clients.

Revalidation Timeout Field

The router periodically queries the posture agent on the client to determine the client’s adherence to security policy. Enter the number of seconds that the router should wait between queries.

Status Query Timeout Field

Enter the number of seconds that the router should wait between queries to the posture agent on the host.

Reset to Defaults Button

Click this button to reset all NAC timeouts to their default values.
Configure these timeout values globally Check Box

Click this check box to have these values apply to all interfaces.

Configure a NAC Policy

A NAC policy enables the posture validation process on a router interface, and can be used to specify the types of traffic that are to be exempt from posture validation in the admission control process.

Name Field

Enter a name for the policy.

Select an Interface List

Choose the interface to which you want to apply the NAC policy. Choose an interface that connects network clients to the router.

Admission Rule Field

You can use an access rule to exempt specific traffic from triggering the admission control process. It is not required. Enter the name or the number of the access rule that you want to use for the admission rule. You can also click the button to the right of this field and browse for the access rule, or create a new access rule.

The access rule must contain deny statements that specify the traffic that is to be exempted from the admission control process. No posture validation triggering occurs if the access rule contains only deny statements.

An example of ACL entries for a NAC admission rule follows:

deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any

The first deny statement exempts traffic with a destination of port 53 (domain), and the second statement exempts traffic with a destination of port 80 (www). The permit statement ending the ACL ensures that posture validation occurs.
How Do I...

The following topics contain procedures for performing tasks that the Create NAC wizard does not help you to do.

How Do I Configure a NAC Policy Server?

The router must have a connection to a Cisco Secure Access Control Server (ACS) running ACS software version 3.3. The ACS must be configured to use the RADIUS protocol in order to implement NAC. The document at the following link contains an overview of the configuration process.


Documents at the following link explain how to install and configure Cisco Secure ACS for Windows Servers version 3.3.


How Do I Install and Configure a Posture Agent on a Host?

If you are a registered Cisco.com user, you can download Cisco Trust Agent (CTA) software from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

The document at the following link explains how to install and configure CTA software on a host.


The specific installation procedures required to install third-party posture agent software and the optional remediation server vary depending on the software in use. Consult the vendor documentation for complete details.