802.1x Authentication

802.1x authentication allows a remote Cisco IOS router to connect authenticated VPN users to a secure network through a VPN tunnel that is up at all times. The Cisco IOS router will authenticate users through a RADIUS server on the secure network.

802.1x authentication is applied to switch ports or Ethernet (routed) ports, but not to both types of interfaces. If 802.1x authentication is applied to an Ethernet port, non-authenticated users can be routed outside the VPN tunnel to the Internet.

802.1x authentication is configured on interfaces by using the LAN wizard. However, before you can enable 802.1x on any interface, AAA must be enabled on your Cisco IOS router. If you attempt to use the LAN wizard before AAA is enabled, a window appears asking if you want to enable AAA. If you choose to enable AAA, then the 802.1x configuration screens will appear as part of the LAN wizard. If you choose to not enable AAA, then the 802.1x configuration screens will not appear.

LAN Wizard: 802.1x Authentication (Switch Ports)

This window allows you to enable 802.1x authentication on the switch port or ports you selected for configuration using the LAN wizard.

Enable 802.1x Authentication

Check Enable 802.1x Authentication to enable 802.1x authentication on the switch port.
Host Mode

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

**Note**

Ports on Cisco 85x and Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.

Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN form the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN form the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

Advanced Options

This window allows you to change the default values for a number of 802.1x authentication parameters.
Radius Server Timeout

Enter the time, in seconds, that your Cisco IOS router waits before timing out its connection to the RADIUS server. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Reply Timeout

Enter the time, in seconds, that your Cisco IOS router waits for a reply from an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Retries Timeout

Enter the time, in seconds, that your Cisco IOS router retries an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Quiet Period

Enter the time, in seconds, that your Cisco IOS router will wait between the initial connection to a client and when a login request is sent. Values must be in the range of 1–65535 seconds. The default setting is 60 seconds.

Ratelimit Period

Values must be in the range of 1–65535 seconds. However, the default setting is 0 seconds, which turns off Rate limit Period.

Maximum Reauthentication Attempts

Enter the maximum number of times your Cisco IOS router tries to reauthenticate an 802.1x client. Values must be in the range 1–10. The default setting is 2.

Maximum Retries

Enter the maximum number of login requests that can be sent to the client. Values must be in the range 1–10. The default setting is 2.
Reset to Defaults

Click **Reset to Defaults** to reset all advanced options to their default values.

LAN Wizard: RADIUS Servers for 802.1x Authentication

802.1x authentication information is 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 802.1x clients by communicating with a RADIUS server. Use this window to provide the information the router needs to contact one or more RADIUS servers. Each RADIUS server that you specify must have Cisco Secure ACS software version 3.3 installed and configured.

---

**Note**

All of your Cisco IOS router interfaces enabled with 802.1x authorization will use the RADIUS servers set up in this window. When you configure a new interface, you will see this screen again. Additions or changes to the RADIUS server information, however, do not have to be made.

---

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 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.
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

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 802.1x Check Box

Check this box if you want to use the listed RADIUS server for 802.1x. The server must have the required 802.1x authorization information configured if 802.1x is used successfully.

Add, Edit, and Ping

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.

Note

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.

**Edit 802.1x Authentication (Switch Ports)**

This window allows you to enable and configure 802.1x authentication parameters.

If the message “802.1x cannot be configured for a port operating in Trunk Mode.” appears instead of the 802.1x authentication parameters, then the switch cannot have 802.1x authentication enabled.

If the 802.1x authentication parameters appear but are disabled, then one of the following is true:

- **AAA has not been enabled.**
  
  To enable AAA, go to **Configure > Additional Tasks > AAA**.

- **AAA has been enabled, but an 802.1x authentication policy has not been configured.**
  
  To configure an 802.1x authentication policy, go to **Configure > Additional Tasks > AAA > Authentication Policies > 802.1x**.

**Enable 802.1x Authentication**

Check **Enable 802.1x Authentication** to enable 802.1x authentication on this switch port.

**Host Mode**

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

**Note**

Ports on Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.
Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN from the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN from the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

**LAN Wizard: 802.1x Authentication (VLAN or Ethernet)**

This window allows you to enable 802.1x authentication on the Ethernet port you selected for configuration using the LAN wizard. For Cisco 87x routers, this window is available for configuring a VLAN with 802.1x authentication.

---

**Note**

Before configuring 802.1x on VLAN, be sure that 802.1x is not configured on any VLAN switch ports. Also be sure that the VLAN is configured for DHCP.
Use 802.1x Authentication to separate trusted and untrusted traffic on the interface

Check Use 802.1x Authentication to separate trusted and untrusted traffic on the interface to enable 802.1x authentication.

DHCP IP Address Pool for Untrusted 802.1x Clients

To enable an Internet connection for clients that fail 802.1x authentication, each untrusted client must be assigned a unique IP address. These IP addresses can come from a new or existing IP address pool, but the pools used cannot overlap with the IP addresses of any of your Cisco IOS router existing interfaces.

Note

The IP address pool can overlap the IP address used for a loopback interface. However, you will be asked to confirm such an overlap before it is allowed.

Choose Create a new pool to configure a new IP address pool for issuing IP addresses to untrusted clients. The following fields may already be populated from previously entered information, but you may change or fill them:

- **Network**: Enter the IP network address from which the pool of IP addresses is derived.
- **Subnet Mask**: Enter the subnet mask to define the network and host portions of the IP address entered in the Network field.
- **DNS Server 1**: The DNS server is a server that maps a known device name to its IP address. If a DNS server is configured for your network, enter the IP address for that server.
- **DNS Server 2**: If there is an additional DNS server on the network, enter the IP address for that server.
If there is an existing IP address pool you want use for issuing IP addresses to untrusted clients, choose **Select an existing pool**. Choose the existing pool from the drip-down menu. To see more information about an existing pool, click **Details**.

### Exception Lists

Click **Exception Lists** to create or edit an exception list. An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel.

### Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

### 802.1x Exception List

An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel. Exempt clients are identified by their MAC addresses.

### Add

Click **Add** to open a window where you can add the MAC address of a client. The MAC address must be in the format that matches one of these examples:

- 0030.6eb1.37e4
Cisco SDM rejects misformatted MAC addresses, except for MAC addresses shorter than the given examples. Shorter MAC addresses will be padded with a “0” (zero) for each missing digit.

**Note** Cisco SDM’s 802.1x feature does not support the CLI option that associates policies with MAC addresses and will not include in the exception list MAC addresses that have a policy associated with them.

**Delete**

Click **Delete** to remove a chosen client from the exception list.

### 802.1x Authentication on Layer 3 Interfaces

This window allows you to configure 802.1x authentication on a Layer 3 Interface. It lists Ethernet ports and VLAN interfaces that have or can be configured with 802.1x authentication, allows you to choose a Virtual Template interface for untrusted clients, and create an exception list for clients to bypass 802.1x authentication.

**Note** If policies have been set using the CLI, they will appear as read-only information in this window. In this case, only enabling or disabling 802.1x is allowed in this window.

**Prerequisite Tasks**

If a prerequisite task appears in the window, it must be completed before 802.1x authentication can be configured. A message explaining the prerequisite task is displayed, along with a link to the window where the task can be completed.

**Enable 802.1x Authentication Globally**

Check **Enable 802.1x Authentication Globally** to enable 802.1x authentication on all Ethernet ports.
Interfaces Table

The Interfaces table has the following columns:

**Interface**—Displays the name of the Ethernet or VLAN interface.

**802.1x Authentication**—Indicates whether 802.1x authentication is enabled for the Ethernet port.

Edit

Click **Edit** to open a window of editable 802.1x authentication parameters. The parameters are the 802.1x authentication settings for the interface chosen in the Interfaces table.

Policy for Untrusted Users

Choose a Virtual Template interface from the drop-down list. The chosen Virtual Template interface represents the policy applied to clients that fail 802.1x authentication.

Click the **Details** button to see more information about the chosen Virtual Template interface.

Exception List

For more information about the exception list, see **802.1x Exception List**.

Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

Apply Changes

Click **Apply Changes** for the changes you made to take effect.

Discard Changes

Click **Discard Changes** to erase the unapplied changes you made.
Edit 802.1x Authentication

This window allows you to enable and change the default values for a number of 802.1x authentication parameters.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the Ethernet port.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** for descriptions of the fields in the Advanced Options box.

How Do I ...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Configure 802.1x Authentication on More Than One Ethernet Port?

Once you configure 802.1x authentication on an interface, the LAN wizard will no longer display any 802.1x options for Ethernet ports because Cisco SDM uses the 802.1x configuration globally.
Note

For configuring switches, the LAN wizard will continue to display the 802.1x options.

If you want to edit the 802.1x authentication configuration on an Ethernet port, go to Configure > Additional Tasks > 802.1x.