

## Configuring 802.1X Authentication (NSM Procedure)

---

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from denial-of-service (DoS) attacks and preventing unauthorized user access.

802.1X works by using an *Authenticator Port Access Entity* (the device) to block all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking and opens the interface to the supplicant.

To configure 802.1X authentication:

- Specify 802.1X interface settings on the switch.
  - Specify the 802.1X exclusion list, used to specify which supplicants can bypass 802.1X authentication and be automatically connected to the LAN.
1. Configuring 802.1X Interface Settings on page 1
  2. Configuring Static MAC Bypass on page 2

### Configuring 802.1X Interface Settings

To configure 802.1X interface settings:

1. In the navigation tree, select Device Manager > Devices. In Device Manager, select the device for which you want to configure 802.1X settings.
2. In the Configuration tree, expand **Protocols** > **Dot1x**.
4. Select **Authenticator** > **Interface**.
5. Click the Add icon.
6. Add/modify member settings for the interface as specified in Table 1.



**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See Updating Devices for more information.

---

**Table 1: 802/1X Authentication for an Interface**

Option	Function	Your Action
Authentication Profile Name	Specifies the name for the profile.	Enter the name
Interface	Specifies the interface for which 802.1X authentication is being configured.	Select <b>Interface</b> . Click the Add icon.
Name	Specifies the interface name.	Enter the interface name.

**Table 1: 802.1X Authentication for an Interface** (continued)

Option	Function	Your Action
Disable	Disables 802.1X authentication on the interface.	Select to disable authentication.
Supplicant	Specifies the mode to be adopted for supplicants: <ul style="list-style-type: none"> <li>■ Single — allows only one host for authentication.</li> <li>■ Multiple — allows multiple hosts for authentication. Each host is checked before being admitted to the network.</li> <li>■ Single authentication for multiple hosts — Allows multiple hosts but only the first is authenticated.</li> </ul>	Select the required mode.
Retries	Maximum number of retries	Select a value from the list.
Quiet Period	Specifies the port waiting time after an authentication failure.	Select a value from the list.
Transmit Period	Specifies the retransmit interval.	Select a value from the list.
Supplicant Timeout	Port timeout value for the response from the supplicant.	Select a value from the list.
Server Timeout	Port timeout value for the response from the RADIUS server	Select a value from the list.
Maximum Requests	Specifies the maximum number of authentication requests to be made to the server.	Select a value from the list.
Guest Vlan	Specifies the guest VLAN to move the interface to in case of an authentication failure.	Enter the VLAN name.
Reauthentication	Specifies enabling reauthentication on the selected interface.	Select <b>Reauthentication</b> .  Select one: <ul style="list-style-type: none"> <li>■ none</li> <li>■ reauthentication</li> <li>■ no-reauthentication</li> </ul>

## Configuring Static MAC Bypass

Configure any MAC addresses, supplicants, or interfaces to be excluded from 802.1X authentication—that is, they will be authenticated.

To configure the 802.1X exclusion:

1. Specify a MAC address to be excluded from 802.1X authentication in the field **Name**.
2. Specify the interface for the supplicant to bypass authentication if connected through that interface.
3. Specify the VLAN to move the supplicant to once it is authenticated.



**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See [Updating Devices](#) for more information.

---

Published: 2009-08-21