



Purpose: To enable IEEE 802.1x authentication using the NSE.

Step 1: Enable Usernames and 802.1x Authentication

Authentication Authorization and Accounting Settings

AAA Services Enable

Logout IP:

XML Interface Enable

XML SERVER 1 IP

XML SERVER 2 IP

XML SERVER 3 IP

Print Billing Command Enable

Print Server URL

AAA Passthrough Port Enable

Port Port must be different from 80, 2111, 1111, and 1112.

802.1X Authentication Support Enable

Note: 802.1x requires that both AAA and RADIUS Authentication be enabled.

802.1X Reauth Period (secs)

Enable Origin Server (OS) parameter encoding for Portal Page and EWS Enable

Enable failover to Internal Web Server Authentication if Portal Page/External Web Server is not reachable Enable

Port-based billing policies Enable

Select one of the following:

Internal Web Server

SSL Support Enable

Encrypt only Sensitive Data Enable

Note: To enable, make sure your license includes SSL support and you have all the certificate files on the flash.

Certificate DNS Name

Portal Page Enable

Portal Page URL

Parameter Passing Enable

Parameter Signing	
Method	<input checked="" type="radio"/> None <input type="radio"/> HASH-CRC32 <input type="radio"/> HMAC-MD5
Parameters	<input type="checkbox"/> UI <input type="checkbox"/> MA <input type="checkbox"/> RN <input type="checkbox"/> PORT <input type="checkbox"/> SIP
Shared Secret	<input type="text"/> (write-only)

Manual Passthrough Address Enable

Portal XML POST URL

Portal XML Post Port

Supports GIS Clients Yes

Block IWS Login Page Yes

Usernames Enable



Step 2: Create Radius settings

a) Add a Radius Service profile

Realm-Based Routing Settings

RADIUS Service Profiles (up to 10 may be created)

No RADIUS service profiles are defined.

Add Click here to add a new RADIUS service profile.

Add RADIUS Service Profile

Unique Name:

Authentication

Enable RADIUS Authentication Service

Protocol:

Primary IP / DNS:	<input type="text" value="10.10.10.10"/>	Port:	<input type="text" value="1812"/>	Secret Key:	<input type="text" value="secret"/>
Secondary IP / DNS:	<input type="text"/>	Port:	<input type="text" value="0"/>	Secret Key:	<input type="text"/>

Accounting

Enable RADIUS Accounting Service

Primary IP / DNS:	<input type="text" value="10.10.10.10"/>	Port:	<input type="text" value="1813"/>	Secret Key:	<input type="text" value="secret"/>
Secondary IP / DNS:	<input type="text"/>	Port:	<input type="text" value="0"/>	Secret Key:	<input type="text"/>

Retransmission Options

Retransmission Method: Failover Round-Robin

Retransmission Frequency: (seconds)

Retransmission Attempts: (per server)

Add



b) Set Radius Client Settings

For the Routing Mode select Fixed.

For the Default RADIUS Service Profile, select the one you just created from the drop down list.

RADIUS Client Settings

Server Selection and Communication

Default RADIUS Mode: Disabled Realm-Based Fixed

Default RADIUS Service Profile:

Reboot required to put changes of the following two parameters into effect.

Local Authentication Port: (0 means port number will be selected dynamically)

Local Accounting Port: (0 means port number will be selected dynamically)

Later login supersedes previous

Miscellaneous Options

Default User Idle Timeout: (seconds)

User Login Retry Timeout: (seconds)

Enable Automatic Subscriber Reauthentication

Enable URL Redirection

Send NAS identifier

NAS identifier:

Send NAS IP

Send NAS Port type

NAS Port Type:

Send Framed IP

Enable Termination-Action Radius Attribute

Enable Session-Terminate-End-Of-Day When Authorized

Enable Byte Count Reset On Account Start

Enable Radius Subnet Attribute

Enable Goodbye URL

Enable Forgot your Password

Forgot your Password URL:

(Note: This URL will be added to the passthrough address list)

Enable RADIUS Based WAN VLAN **Note: WAN 802.1Q headers for subscribers must be enabled in the Location page for this setting to be effective**

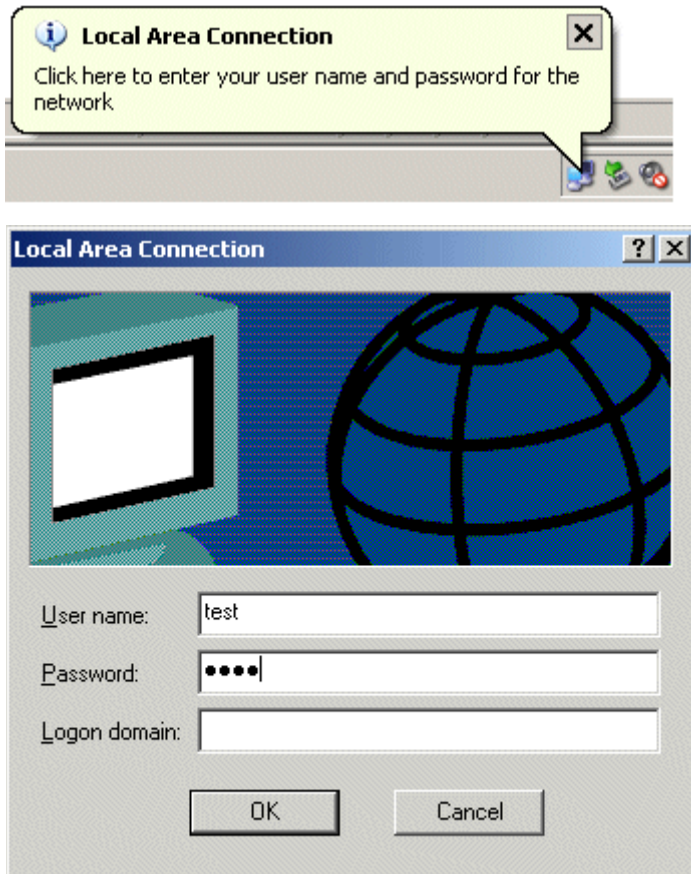
Enable user session time adjustment for NSE down time

Enable charging for idle time

Enable RADIUS QoS Policies

The User Experience.

When a 802.1x enabled user launches their browser, they will be prompted to login to the network.



When the user clicks OK, the user name and password is then sent to the Radius Server for authentication.

Note: IEEE 802.1x needs to be turned off in the Access Point and the Access Points used in the network must be able to bridge (pass-through) the EAP packets from the client computer (supplicant).