



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

*Note: Because current Access Points (AP) do not forward EAP messages, 802.1x on the Nomadix is only for wired connections. To support 802.1x on a wireless network behind the Nomadix Radius Proxy will need to be utilized.*

**Step 1: Under Configuration -> AAA -> Options Enable 802.1x Authentication and optionally set an 802.1x Reauth period.**

**Authentication Authorization and Accounting Settings**

AAA Services  Enable

Options Internal Web Server External Web Server

Logout IP: 198.51.100.10

XML Interface [Configure](#)

Print Billing Command  Enabled

Print Server URL

AAA Passthrough Port  Enabled

Port  [i](#)

802.1X Authentication Support  Enabled [i](#)

802.1X Reauth Period (secs)

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

Failover to Internal Web Server Authentication if Portal Page/External Web Server is not reachable  Enabled

Port-based billing policies  Enabled

HTTPS Redirection  Enabled

Facebook Login  [Enable](#)

[Save](#) [Save then Reboot](#) [Restore](#)



## 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

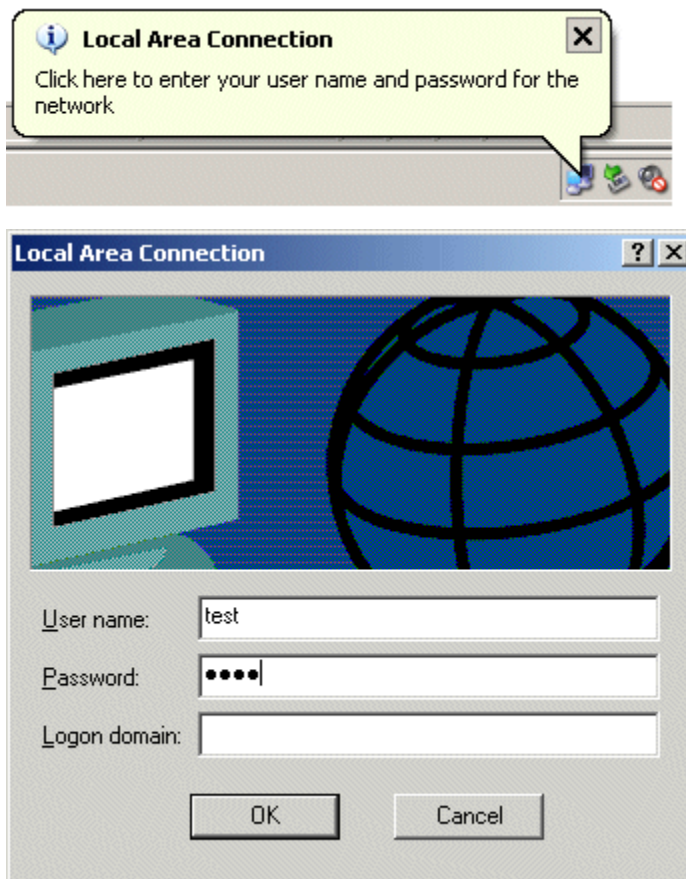
Enable charging for idle time

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.