



Purpose: To enable authentication using a Radius Server

Step 1: Enable AAA, Internal Web Server and Usernames

Authentication Authorization and Accounting Settings

AAA Services	<input checked="" type="checkbox"/> Enable	
XML Interface	<input type="checkbox"/> Enable	
	XML SERVER 1 IP	<input type="text" value="0.0.0.0"/>
	XML SERVER 2 IP	<input type="text" value="0.0.0.0"/>
Print Billing Command	<input type="checkbox"/> Enable	
	Print Server URL	<input type="text"/>
AAA Passthrough Port	<input type="checkbox"/> Enable	
	Port	<input type="text" value="0"/> Port must be different from 80, 2111, 1111, and 1112.
802.1X Authentication Support	<input type="checkbox"/> Enable	
	Note: 802.1x requires that both AAA and RADIUS Authentication be enabled.	
Enable Origin Server (OS) parameter encoding for Portal Page and EWS	<input type="checkbox"/> Enable	
Enable failover to Internal Web Server Authentication if Portal Page/External Web Server is not reachable	<input type="checkbox"/> Enable	
Port-based billing policies	<input type="checkbox"/> Enable	

Select one of the following:

Internal Web Server

SSL Support	<input type="checkbox"/> Enable	You must reboot the NSE after turning it on/off.
	Note: To enable, make sure your license includes SSL support and you have all the certificate files on the flash.	
	Certificate DNS Name	<input type="text" value="ssl.certificate.com"/>
Portal Page	<input type="checkbox"/> Enable	
	Portal Page URL	<input type="text"/>
	Parameter Passing	<input type="checkbox"/> Enable
	Portal XML POST URL	<input type="text"/>
	Portal XML Post Port	<input type="text" value="80"/>
	Supports GIS Clients	<input type="checkbox"/> Yes
	Block IWS Login Page	<input type="checkbox"/> Yes
Usenames	<input checked="" type="checkbox"/> Enable	



Step 2: Create Radius settings

a) Add a Radius Service profile

Add RADIUS Service Profile

Unique Name:

Authentication

Enable RADIUS Authentication Service

Protocol:

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

Accounting

Enable RADIUS Accounting Service

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

[Back to Main RADIUS Routing Settings page](#)



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

Routing Mode: Disabled Realm-Based Fixed

Default RADIUS Service Profile: testradius

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)

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

Enable Default 802.1q Tag for System Traffic: **Note: Changing this setting could result in loss of connectivity.**

Submit

Reset



The User Experience

When the user launches their browser they will be redirected to the Login screen where they will be prompted to enter in their User name and Password.

The login form is a rectangular box with a light green background and a thin border. At the top center, it features the NOMADIX logo (a green circular icon above the text 'NOMADIX' with a 'TM' symbol). Below the logo, the text 'Are you an existing user?' is followed by 'Please enter your user ID and password:'. There are two input fields: 'Username:' followed by a white text box, and 'Password:' followed by a white text box. Below these fields is a checkbox with the label 'Remember my username and password.'. To the right of the checkbox is a 'Login' button with a grey gradient and rounded corners. At the bottom of the form, the text 'Please contact your Network Administrator in case of problems.' is centered.

The NSE will send the user name and password to the Radius server and grant access to user based on the information received from the Radius server.