



Purpose: To enable authentication using a Radius Server

Step 1: Enable AAA, Internal Web Server and Usernames

Authentication Authorization and Accounting Settings

AAA Services Enable

Options	Internal Web Server <input checked="" type="radio"/>	External Web Server <input type="radio"/>
SSL Support	<input type="checkbox"/> Enabled ?	
Encrypt only Sensitive Data	<input checked="" type="checkbox"/> Enabled	
Certificate DNS Name	<input type="text" value="ssl.certificate.com"/>	
Portal Page	<input type="checkbox"/> Enable »	
Portal XML POST URL	<input type="text"/>	⚠ Caution
Portal XML Post Port	<input type="text" value="80"/>	
Usernames	<input checked="" type="checkbox"/> Enabled ?	<div style="border: 1px solid blue; padding: 5px; color: blue;">Operates with <i>Relogin After Timeout</i>, <i>Relogin after Migration</i>, <i>XoverY billing</i>, or <i>Group Accounts</i>.</div>
New Subscribers	<input type="checkbox"/> Enabled	
Relogin After Timeout	<input type="checkbox"/> Enabled	
Credit Card Service	<input type="checkbox"/> Enabled »	
Smart Client Support	<input type="checkbox"/> Enabled	



Step 2: Create a Radius profile – Go to Configuration/Realm-Based Routing and select Add to create a new Radius Service profile.

RADIUS Server and Realm-Based Routing Settings
How AG connects to RADIUS servers, and how it routes AAA requests

RADIUS Service Profiles (up to 10 may be created)

No RADIUS service profiles are defined.

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="192.168.1.10"/>	Port:	<input type="text" value="1645"/>	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="192.168.1.10"/>	Port:	<input type="text" value="1646"/>	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 Delay: (seconds)

Retransmission Attempts: (per server)



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

Setup AG as a RADIUS client

Server Selection and Communication

Default RADIUS Mode: Disabled Realm-Based Fixed

Default RADIUS Service Profile: (none) ▼
(none)

Local Authentication Port testradius port number will be selected dynamically)

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

Later login supersedes previous



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.

A screenshot of the NOMADIX login interface. At the top is the NOMADIX logo. Below it, the text reads: "Are you an existing user? Please enter your user ID and password:". There are two input fields: "Username:" and "Password:". Below the password field is a checkbox labeled "Remember my username and password.". A "Login" button is located to the right of the checkbox. At the bottom of the form, there is a note: "Please contact your Network Administrator in case of problems."/>

Are you an existing user?
Please enter your user ID and password:

Username:

Password:

Remember my username and password.

Login

Please contact your Network Administrator in case of problems.

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.