



Purpose: To configure the NSE to authenticate a Radius user based on the realm in their login.

Step 1: Enable AAA, Internal Web Server and Usernames

Authentication Authorization and Accounting Settings

AAA Services Enable

Options Internal Web Server External Web Server

SSL Support Enabled ⓘ

Encrypt only Sensitive Data Enabled

Certificate DNS Name

Portal Page Enable »

Portal XML POST URL ⚠ Caution

Portal XML Post Port

Usernames Enabled ⓘ

Operates with *Relogin After Timeout*, *Relogin after Migration*, *XoverY billing*, or *Group Accounts*.

New Subscribers Enabled

Relogin After Timeout Enabled

Credit Card Service Enabled »

Smart Client Support 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)



Step 3: Create the Realm Policy - Go to Configuration/Realm-Based Routing and select Add to create a new Realm Routing Policy

Realm Routing Policies (up to 50 may be defined)

<u>Realm</u>	<u>Pre/Suf Match</u>	<u>RADIUS Profile</u>	<u>RadStrip</u>
* <u>BOINGO</u>	Prefix		no
* <u>IPASS</u>	Prefix		no

(* indicates policy configured as disabled)

Click here to add a new Realm Routing Policy.

Add Realm Routing Policy

Entry Active

Specific Realm Realm name:

Wildcard match

Prefix match only (Match characters preceding "/>")

Suffix match only (Match characters following "@", i.e., NAI realm)

Match either (Try prefix first, then try suffix if no prefix match)

RADIUS Service Profile:

Strip off routing information when sending to RADIUS server

In this example, user logging in with a user name ending in @nomadix.com will be authenticated against the server set as the Radius Service Profile.



Step 4: Create Client Settings – Go to Configuration/Radius Client Settings and enable Real-Based and select the radius server you wish to you as the default radius server.

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 0 testradius port number will be selected dynamically)

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