



Purpose: To enable the NSE to respond to Smart Client and GIS Client authentication.

Step 1: Enable AAA Internal Web Server and Smart Client and GIS Client Support

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

Username Enable

Note: Username option is enabled if any of the following are true: Relogin After Timeout, Relogin after Migration, XoverY billing, or Group Accounts.

New Subscribers Enable

Relogin After Timeout Enable

Credit Card Service Enable

Credit Card Server

Credit Card Server URL

Credit Card Server IP

Merchant ID

Use NSE's hostname and DNS domain name Enable

Authorize.net:
SIM Compliant Enable

Change Transaction Key

Verify Transaction Key

Chainfusion:
Credit Card Transaction Time minutes

Smart Client Support Enable

Note: To enable, make sure your license includes Smart Client support.



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: Port: Secret Key:

Secondary IP / DNS: Port: Secret Key:

Accounting

Enable RADIUS Accounting Service

Primary IP / DNS: Port: Secret Key:

Secondary IP / DNS: Port: Secret Key:

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

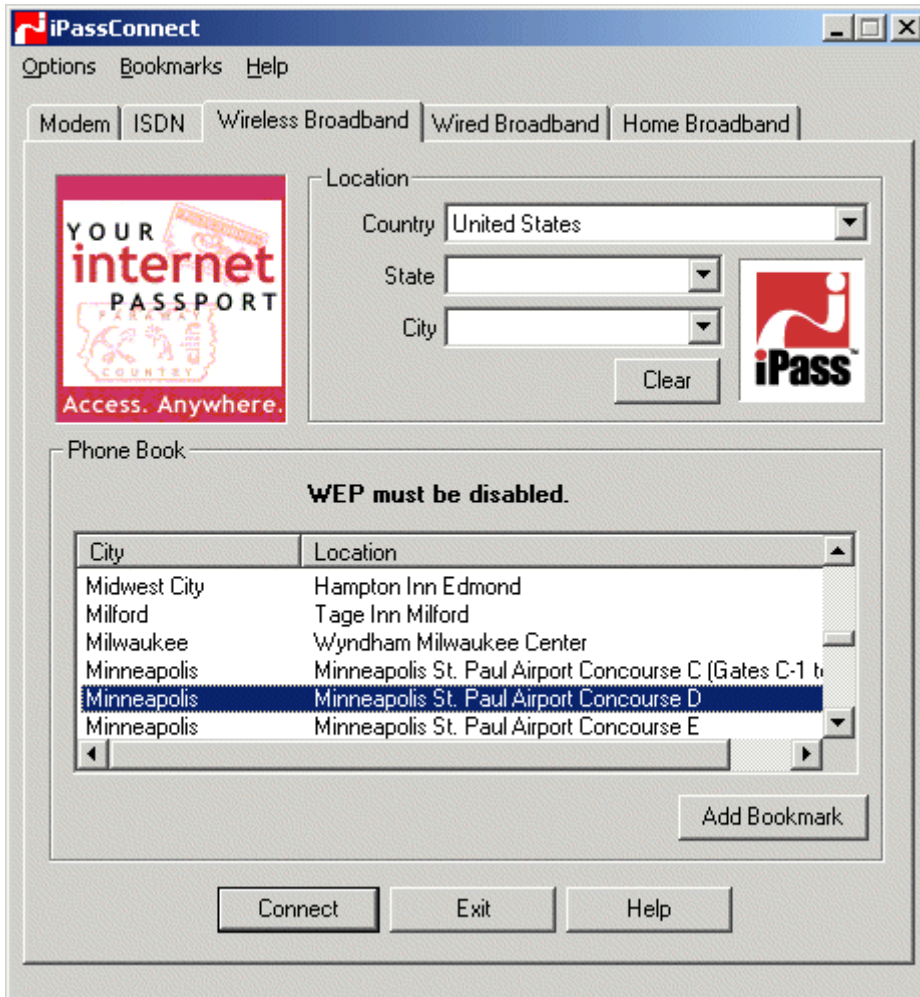
Note: When connecting to a roaming provider such as Ipass or Boingo, you will need to enable the Realm Routing Policy for the provider as well as configure the radius server settings for the policy. The roaming provider should provide you with the radius server details.



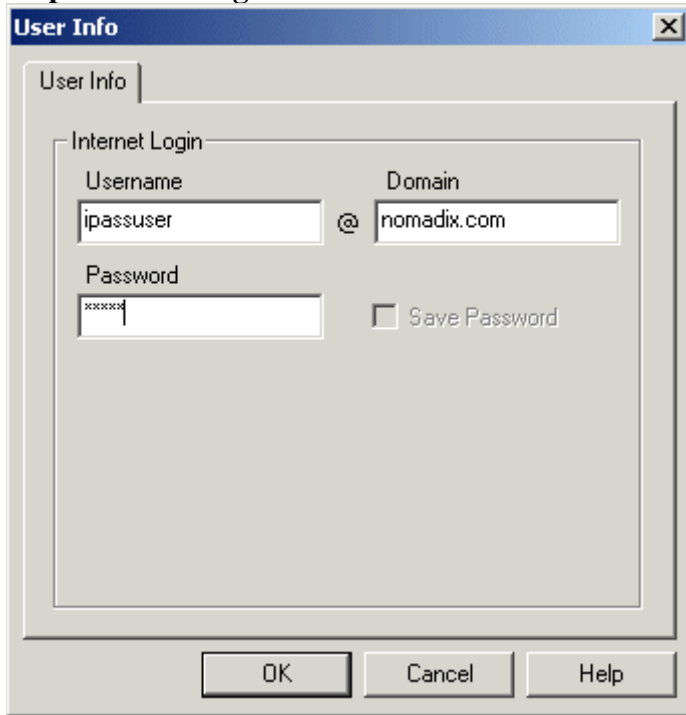
The User Experience

IPass Client

Step 1: Selecting the proper location.



Step 2: Enter Login information.



The image shows a Windows-style dialog box titled "User Info". It contains a tab labeled "User Info" and a section titled "Internet Login". Inside this section, there are two input fields: "Username" with the text "ipassuser" and "Domain" with the text "nomadix.com". An "@" symbol is positioned between these two fields. Below the "Username" field is a "Password" field containing "xxxxxx". To the right of the password field is a checkbox labeled "Save Password" which is currently unchecked. At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Confirmation that the IPass client is running.





GRIC Client

Step 1: Enter Login information.

A screenshot of a Windows-style dialog box titled 'Login Properties'. The dialog has four tabs: 'Access', 'Programs', 'Timeout', and 'Personal Firewall Settings'. The 'Access' tab is selected. Inside the dialog, there is a section titled 'Network Login Information' which contains a 'Login ID:' label followed by a text box containing 'gricuser' and an '@' symbol, and another text box containing 'nomadix.com'. Below this is a 'Password:' label followed by a text box containing '*****'. At the bottom of this section is a checked checkbox labeled 'Save password at exit'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.



Step 2: Select Location.

A screenshot of a Windows-style dialog box titled "Login Properties". It has four tabs: "Access", "Programs", "Timeout", and "Personal Firewall Settings". The "Access" tab is selected. Inside the dialog, there is a section titled "Network Login Information" which contains a "Login ID:" field with the text "gricuser" and an "@" symbol followed by a domain field containing "nomadix.com". Below this is a "Password:" field with six asterisks. A checkbox labeled "Save password at exit" is checked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".



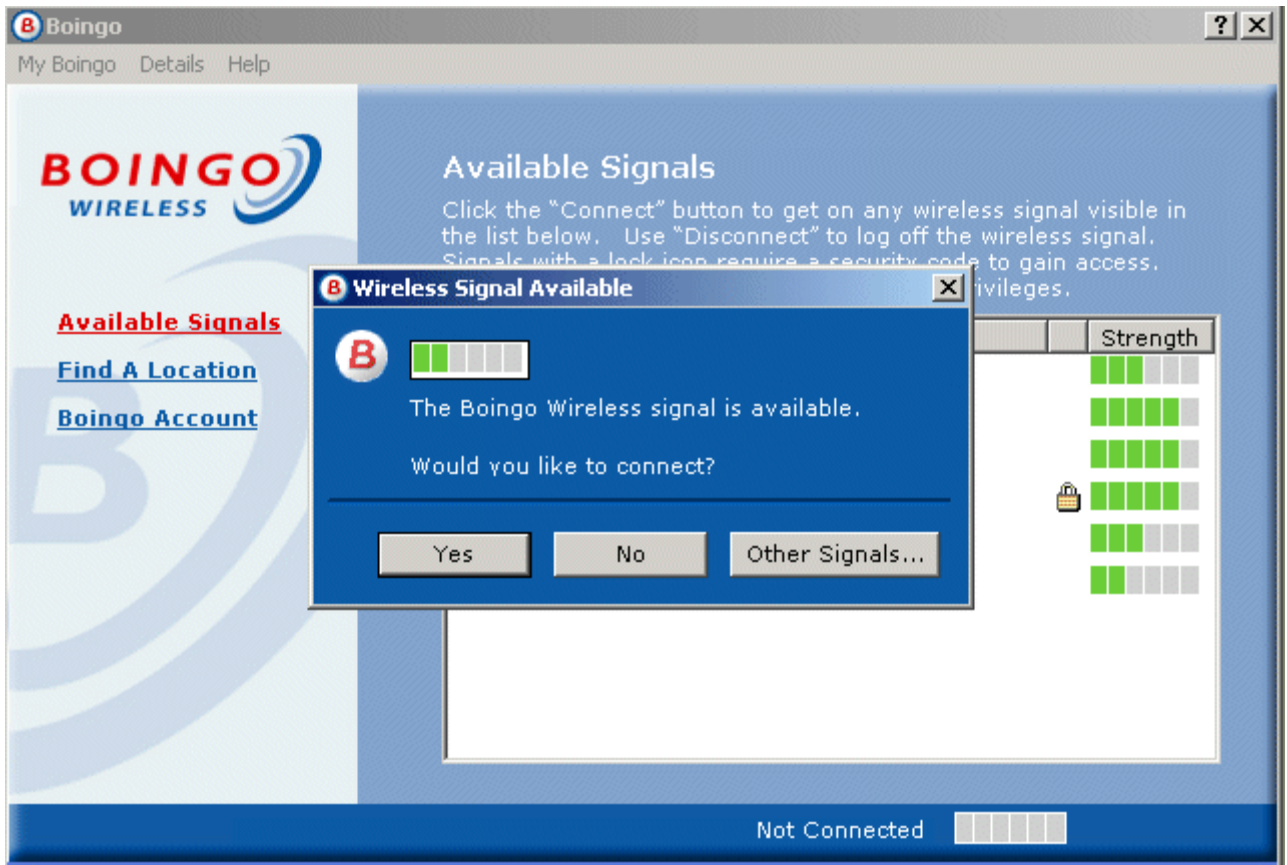
Step 3: Confirmation that the Login was successful.

Your request was successful

A screenshot of a web browser window displaying the GRIC website. The browser's title bar reads "Wireless Login from Westlake Village, CA, USA/Nomadix 1". The website header includes the GRIC logo, a navigation menu with links for "Phonebook", "Downloads", "Customer Care", "Contact Us", and "Member L...", and a secondary menu with "Company Info", "Products & Services", "TierOne Network", "Partners & Customers", and "Investor Relations". The main content area features a purple banner for "GRIC's Mobile Office" with sub-sections for "Access", "Applications", "Devices", and "Network Management". A sidebar on the right lists "Company Overview", "Webcast", "Stock Quote", "SEC Filings", "Press Release Request", "Annual Reports", "Printed Materials", and "Investor FAQs". Below the banner, there are sections for "TierOne" (with an AOL logo) and "Partners" (with a webex logo). The "GRIC's Vision" section describes the company's goal of providing an integrated mobile office solution. At the bottom, there is an "empowering the mobile office™" logo and a "Sign Up" button. The "Latest News" section contains several news items with blue hyperlinks, including "AT&T Enhances Dial Internet Access with Extended Roaming", "GRIC CEO Says Broadband Wireless Has A Bright Future Once Access Improves In Churchill Club Address", and "GRIC Beats First Call Estimates for 1st Quarter Net Loss Per Share".

Boingo Client

Step 1: Launch the Boingo Client.





Step 2: Enter in Login information.

A screenshot of a Windows-style dialog box titled 'Boingo Login'. The dialog has a blue background and a white border. At the top, it says 'You are connecting to a Boingo Wireless signal. Please log in.' Below this, there are two input fields. The first is labeled 'User Name' and contains the text 'jcook'. To the right of this field is a button labeled 'Change User...'. The second input field is labeled 'Password' and contains a series of asterisks. Below the password field is a checked checkbox labeled 'Remember my password'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Step 3: Confirmation that the Login was successful.



NOMADIX

Boingo My Boingo Details Help

BOINGO WIRELESS

[Available Signals](#)
[Find A Location](#)
[Boingo Account](#)

Available Signals

Click the "Connect" button to get on any wireless signal visible in the list below. Use "Disconnect" to log off the wireless signal. Signals with a lock icon require a security code to gain access. Some unlocked private signals require login privileges.

Status	Signal Name	Strength
CONNECTED	Boingo Wireless	██████
CONNECT	Nomadix2002	██████
CONNECT	nomadix-proxim-hotspot	██████
CONNECT	nomadix-agere-hotspot-1000	██████
CONNECT	default	██████
CONNECT	AP-2000-Testlab_A	██████

Connected to Boingo Wireless ██████ **DISCONNECT**