



# IAG Configuration Guide

nAppliance Networks

Release 01/22/2009

Version 1.0.7

Copyright © 2008,2009, nAppliance Networks

## NAPPLIANCE APPLIANCE PRODUCT END USER AGREEMENT

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY INSTALLING AND USING SOFTWARE AND HARDWARE INCLUDED WITH THE NAPPLIANCE PRODUCT, YOU (THE 'END USER') ARE AGREEING TO BE BOUND BY THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, IMMEDIATELY RETURN THE PRODUCT TO NAPPLIANCE INC.

### 1. CERTAIN DEFINITIONS

1. "nAppliance Appliance" means the nAppliance hardware and software that includes, without limitation: licensed software, hardware, support, and professional services.

2. "Open Source Software" means software included in the nAppliance Appliance which is licensed and made available under the terms and conditions of the GNU General Public License version 2.

3. "Licensed Software" means nAppliance Proprietary Software and Open Source Software together.

4. "nAppliance Proprietary Software" means nAppliance proprietary software that may be included in the nAppliance Appliance, including enhancements, updates, bug fixes and upgrades thereto that may be provided to End User from time to time.

### 2. LICENSE

**(a) License Grant.** Subject to full payment of all applicable fees and to the terms of this end user agreement (the "Agreement"), nAppliance hereby grants to End User, a non-transferable, non-exclusive license to use the Licensed Software and related product documentation (the "Documentation") with the nAppliance Appliance for the duration of the Agreement. This license allows the End User to install the nAppliance Appliance on a network supporting the number of active nodes specified by the nAppliance Appliance Purchase Agreement. nAppliance shall have the right to conduct audits periodically upon advance notice to verify compliance with the terms of this Agreement.

**(b) License Restrictions.** End User may use the Licensed Software solely with the nAppliance Appliance. Except as otherwise

permitted by the GNU General Public License version 2, End User agrees not to modify, translate, reverse engineer, de-compile or disassemble the Licensed Software; or to create derivative works based on the Licensed Software.

**(c) Other Restrictions.** End User agrees to safeguard copies of the Licensed Software against disclosure, copying or use by unauthorized persons. End User agrees that it will not use, or allow use of, the nAppliance Appliance for any improper purpose (including without limitation, testing the integrity of any network other than those it is authorized to test). End User agrees that it will not, and will not allow, reverse engineering of the hardware included in the nAppliance Appliance. End User shall ensure that the provisions of this Agreement are not violated by End User's employees, contractors or agents. End User agrees to indemnify nAppliance for any third party claims related to the breach of this or any other provision of this Agreement by End User, its agents, contractors, or employees.

**(d) Open Source Software.** The use distribution and modification of Open Source Software is governed by the terms and conditions of the GNU General Public License version 2 which can be viewed at <http://gnu.org> and which is hereby incorporated by reference. Copies of the source code for Open Source Software may be obtained by contacting nAppliance via email at [source@nAppliance.com](mailto:source@nAppliance.com). nAppliance may charge End User a fee equal to its cost for copying and distributing such source code. Nothing in this Agreement is meant to modify or supercede any terms and conditions of the GNU General Public License version 2 and if there is a conflict between the Agreement and the GNU General Public License version 2, the terms of the GNU General Public License version 2 shall control.

### 3. TITLE

End User acknowledges and agrees that all right, title and interest in the Licensed Software and Documentation, including all intellectual property rights therein, is retained by nAppliance or its suppliers, subject only to the license granted to End User hereunder. This license is not a sale and does not transfer to End User any title or ownership in or to the Licensed Software or the Documentation.

#### 4. MAINTENANCE

End User shall have the option of purchasing maintenance services from nAppliance for a fee. Maintenance may include the following:

**(a) Software Updates.** Software updates will be provided by nAppliance at its sole discretion to End User from time to time. Updates may include software enhancements, upgrades, minor updates, and bug fixes.

**(b) Hardware Repair or Replacement.** For End Users purchasing maintenance services, nAppliance will use commercially reasonable efforts to repair or replace defective hardware within two (2) business days in accordance with the terms of the hardware warranty set forth in Section 4 (b) of this Agreement. End User is responsible for returning defective hardware to nAppliance within seven (7) days of receipt of replacement hardware. If nAppliance does not receive returned defective hardware within seven days nAppliance may charge End User the cost of the replacement hardware, such charges to be invoiced by nAppliance to End User in accordance with Section 7.

**(c) Support.** nAppliance will provide phone and email support to End Users Monday-Friday between 7:00 a.m. and 5:00 p.m. Pacific Time. nAppliance will use commercially reasonable efforts to reply to support requests within one (1) business day.

**(d) Technical Support Incidents.** End Users who purchase maintenance are entitled to twelve (12) technical support incidents per year. Support for technical support incidents above twelve (12) per year will be provided on a time and materials basis.

**(e) Bug Fixes.** The discovery of errors in the nAppliance Appliance ("Bugs") by End user shall not be deemed a technical support incident. Bugs should be promptly reported via email by End User to nAppliance at [bugs@nAppliance.com](mailto:bugs@nAppliance.com). nAppliance will use commercially reasonable efforts to fix Bugs in a timely manner.

**(f) Other Technical Support.** Additional technical support services are available, at nAppliance's discretion, on a time and materials basis.



## 5. LIMITED WARRANTY

**(a) Software.** nAppliance warrants to End User only that the media on which the Licensed Software is recorded shall be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of shipment by nAppliance. End User's sole and exclusive remedy, and nAppliance's sole and exclusive liability, shall be replacement of the media in accordance with this limited warranty.

**(b) Hardware.**

(i) Limited Warranty. nAppliance warrants only to End User that hardware furnished to End User under this Agreement will be free from defects in materials and workmanship for a period of ninety (90) days following shipment by nAppliance. nAppliance's sole and exclusive liability and End User's sole and exclusive remedy under this section 5(b) is to, at nAppliance's sole discretion, repair or replace without charge any non-conforming hardware. nAppliance shall repair or replace such hardware within a reasonable time period. Returned hardware and parts shall become nAppliance's property. End User agrees to assist nAppliance in identifying the circumstances under which the hardware failed.

(ii) Warranty Exclusions. The warranty under this section 5(b) does not apply to any hardware that has been subjected by End User or a third party to: (a) operating or environmental conditions contrary to nAppliance's specifications, (b) damage, misuse or neglect, (c) improper installation, repair or alteration, (d) modifications, other than by nAppliance, or (e) third party software, firmware or hardware that interferes with operation of such hardware. This warranty also excludes expendable items, such as fuses or other similar parts that fail from normal use.

**(c) WARRANTY DISCLAIMER.**

(i) The licensed software and documentation is provided "as is." except for the limited warranties granted in sections 5 (a) and (b), nAppliance expressly disclaims and negates all warranties for the nAppliance appliance, whether expressed, implied, statutory or otherwise, and nAppliance specifically disclaims any implied warranties of merchantability, fitness for a particular purpose, non-infringement of intellectual property or other violation of rights. nAppliance does not warrant that the nAppliance appliance will meet end user's requirements or that the operation of the licensed software will be uninterrupted or error free.

(iii) Some states or countries do not allow exclusion or limitation of incidental or consequential damages or limitation on how long an implied warranty lasts, so the above limitations or exclusions may not apply to End User. This warranty gives End User specific legal rights and End User may also have other rights, which vary from state to state or country to country.

## 6. LIMITATION OF LIABILITY AND DAMAGES

(a) In no event shall nAppliance, its suppliers or its distributors be liable for any indirect, special, incidental or consequential damage, including without limitation, loss of data, lost profits or cost of cover arising from the use of the nAppliance appliance, or any defect in the nAppliance appliance, however caused and on any theory of liability. This limitation shall apply even if nAppliance, its suppliers or its distributor shall have been advised of the possibility of any such damage. In particular, but without limitation, nAppliance, its suppliers and its distributors shall have no liability for the loss of any information stored or communicated or attempted to be stored or communicated within any system using the licensed software.

(b) The maximum aggregate liability of nAppliance and its suppliers for any claim arising out of use of the nAppliance appliance, or any defect in the nAppliance appliance, on any and all theories of liability, including without limitation negligence by nAppliance, shall in all events be limited to return of the amounts actually paid to nAppliance for the defective licensed software or hardware, less depreciation of such amounts linearly over a three-year period, which the parties agree constitutes a reasonable rate of depreciation.

## 7. FEES

End User shall pay to nAppliance the fees for the nAppliance Appliance in effect at the applicable delivery date requested by End User in accordance with the nAppliance Appliance Purchase Agreement, and nAppliance shall invoice End User for all such fees. nAppliance may increase fees at its discretion, provided that fee increases will not be effective until 30 days after notice to End User. All payments due hereunder to nAppliance shall be paid to nAppliance not later than thirty (30) days following the date of the applicable invoice. In addition to the fees, End User will pay all charges, including without limitation transportation charges, insurance premiums, and shall be responsible for all taxes (except nAppliance's U.S. income taxes), duties, costs of compliance with

export and import controls and regulations, and other governmental assessments.

## 8. TERMINATION

This agreement shall continue in effect until terminated hereunder. This Agreement may be terminated by nAppliance upon 30 days notice to End User. This Agreement shall terminate automatically if End User fails to pay fees when due and such failure is not remedied within fifteen days of the original payment due date. In addition, this agreement shall terminate automatically on End User's failure to comply with any of the restrictions and provisions herein, including without limitation any attempt to transfer this license. Upon any termination of this agreement, End User agrees promptly to destroy or return to nAppliance all copies of the Licensed Software and Documentation, including without limitation all original and archival copies thereof. No refunds shall be given for such returned materials. Notwithstanding any termination of this License, the rights and obligations set forth in section 3 (Title), section 5 (Limited Warranty), section 6 (Limitation of Liability and Damages), section 7 (Fees), section 8 (Termination) and section 9 (Miscellaneous) shall survive such termination.

## 9. MISCELLANEOUS

End User may not assign this Agreement without the consent of nAppliance. Any attempted assignment by End User shall be null and void. nAppliance may freely assign this Agreement. No delay, failure or waiver by either party to exercise any right or remedy under this Agreement shall operate to limit, preclude, cancel or waive any exercise of such right or remedy or the exercise of any other right or remedy. This Agreement shall be governed by and construed in accordance with the laws of the State of California without regard to conflict of laws principles or the United Nations 1980 Convention on Contracts for the International Sale of Goods. The federal and state courts of California shall have exclusive jurisdiction and venue to adjudicate any dispute arising out of this Agreement, and End User expressly consents to the personal jurisdiction of the state and federal courts of California. If any provision in this Agreement shall be found or be held to be invalid or unenforceable in any jurisdiction in which this Agreement is being performed, it shall not affect the validity of the remaining portions of the Agreement. This Agreement constitutes the entire agreement between the parties and supercedes

any prior agreement, whether written or oral, relating to the subject matter of this Agreement.

# TABLE OF CONTENTS

<b>ABOUT THIS GUIDE.....</b>	<b>23</b>
DOCUMENT OBJECTIVES.....	23
AUDIENCE .....	23
FEEDBACK.....	23
ONLINE VERSION .....	23
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>24</b>
IMPORTANT POINTS - CONFIGURATION ISSUES .....	26
<i>Additional resources</i> .....	26
<b>CHAPTER 2 – NETWORK CONFIGURATION .....</b>	<b>27</b>
DEFAULT GATEWAY .....	29
JOIN IAG TO WINDOWS DOMAIN .....	29
DNS .....	
<b>CHAPTER 3 – FIRST TIME IAG CONFIGURATION.....</b>	<b>30</b>
GENERATE IAG KEYS .....	30
<b>CHAPTER 4: CONFIGURE SINGLE TRUNK.....</b>	<b>32</b>
IAG CONFIGURATION SCREEN.....	32
STEP 1 – SELECT TRUNK TYPE .....	33
STEP 2 – SETTING THE TRUNK .....	34
STEP 3 – AUTHENTICATION .....	
<i>Define Active Directory</i> .....	
<i>Test the Active Directory</i> .....	
STEP 3 – AUTHENTICATION .....	
STEP 4 – APPLICATION SERVER .....	
STEP 5 – APPLICATION LOGIN .....	42
STEP 6 – ENDPOINT POLICIES.....	43
NEW TRUNK CREATED .....	44
ACTIVATE THE CONFIGURATION .....	45
TESTING THE NEW CONFIGURATION .....	47
<i>Connect to the web application</i> .....	47
<i>ActiveX</i> .....	
<i>Login Process</i> .....	51
<i>IAG Login</i> .....	53
FINALLY THE WEB APPLICATION .....	54
<b>CHAPTER 5: CONFIGURE PORTAL TRUNK.....</b>	<b>55</b>

STEP 1 – SELECT TRUNK TYPE .....	57
STEP 2 – SETTING THE TRUNK .....	58
STEP 3 - AUTHENTICATION	
STEP 4 – CERTIFICATE .....	65
STEP 5 – ENDPOINT POLICIES .....	66
TEST THE NEW PORTAL .....	69
<b>CHAPTER 6: PUBLISH WEB APPLICATION - OWA.....</b>	<b>74</b>
STEP 2 – APPLICATION SETUP .....	75
STEP 3 – WEB SERVERS .....	76
STEP 4 – AUTHENTICATION	
STEP 5 – PORTAL LINK.....	79
TESTING THE APPLICATION .....	82
<b>CHAPTER 7: PUBLISH CLIENT/SERVER APPLICATION – TERMINAL SERVICES</b>	
STEP 1 – SELECT APPLICATION .....	85
STEP 2 – APPLICATION SETUP .....	86
STEP 3 – SERVER SETTINGS .....	87
STEP 4 – PORTAL LINK.....	88
STEP 1 – ACCESS THE IAG PORTAL PAGE .....	94
STEP 1 – SELECT APPLICATION .....	95
STEP 2 – APPLICATION SETUP .....	97
STEP 3 – SERVER SETTINGS .....	98
STEP 3 – PORTAL LINK.....	100
APPLICATION PUBLISHED.....	101
TEST APPLICATION .....	103
<b>CHAPTER 9: PUBLISH NETWORK SHARE AS LOCAL DRIVE. 106</b>	
STEP 1 – SELECT APPLICATION .....	107
STEP 2 – APPLICATION SETUP .....	108
STEP 3 – SERVER SETTINGS .....	109
STEP 4 – PORTAL LINK.....	110
TEST DRIVE CONNECTION .....	112
DRIVE MAPPED.....	113
<b>CHAPTER 10: SUMMARY .....</b>	<b>115</b>
<b>APPENDIX 1 – HARDWARE PORT CONFIGURATIONS .....</b>	<b>116</b>
<b>INDEX .....</b>	<b>116</b>

foundation of IAG configuration. The administrator can use this guide for basic IAG implementation. This should then provide a foundation for IAG and prepare the administrator for the more advanced concepts in the User Guide and the IAG Advanced User Guide.

## **Audience**

This guide is for IAG administrators who are managing IAG in configurations.

## **Feedback**

nAppliance Networks appreciates any comments, complaints or opinion on what is right or wrong with this document is very helpful. nAppliance directly via email at:

[support@nAppliance.com](mailto:support@nAppliance.com)

Please include the document name and version.

### **Online Version**

The latest release of this document can be retrieved via the nAppliance

**<http://www.nAppliance.com/support/library.asp>**

The Microsoft's Intelligent Application Gateway (IAG) is a network device which provides remote user access to corporate applications and performs application proxy services, which isolate the corporate network from external users.

IAG publishes applications via what is called a "trunk". This trunk

[Configuration](#) 29 can provide or publish a single application mapping to a single address, or it can publish multiple applications presented as an IAG trunk called an IAG Portal trunk.

IAG resides on the edge of the corporate network (often behind a firewall), communicating through port 443), and interacts with the external users via SSL.

36 VPN [Connection](#) 37 circuit, and interacts with internal corporate applications via native IP protocols. In this manner, only SSL traffic is exposed to the Internet, and external users interact with published applications or other services via SSL protocols.

Fat clients, such as Outlook

[Connection](#) 38, telnet 39 or the SAP41 client, run natively on the user's machine, and talk native IP protocols to an ActiveX [plugin install](#) on the user's machine. For Linux 59 clients, IAG provides a Java client. For ActiveX software wraps the native IP traffic with SSL 84 and connects to the IAG hardware system. The IAG gateway then translates this SSL traffic back to native IP protocols. In this fashion, IAG can publish almost any client application or product.

An incomplete list of services and features include:

1. Single Sign-on authentication. Once IAG authenticates user, subsequent authentication is managed automatically via IAG.
2. Access controls based on corporate policies. The end client system is audited for compliance and access is blocked or reduced based on system policies.
3. VPN like access without the routing or security issues of tunnel connections.
4. Generic VPN like functions similar to PPTP but using SSL VPN tunneling.
5. File access and drive emulation. IAG provides Drive mapping to local systems of server shares, or can present a web version of a network drive.



6. Attachment wiper. This is a process on the client machine, where when the client disconnects from the IAG gateway, all browser access evidence is wiped off the client machines.

## Important Points - Configuration Issues

- IAG runs on top of ISA. IAG automatically defines ISA access policies.
- IAG and ISA work together as a single system. These systems run on top of Windows. All of these components must be considered as components of an entire complex system.
- IP networking and routing is managed by Windows. Network configuration and routing is managed through the Windows environment.
- Do not use IP addresses as definitions for hostnames. IAG does not support IP addresses in the HTTP URL addresses. DNS definitions are necessary for each service published by IAG.

### Additional resources

IAG and ISA documentation is located on the nAppliance web site

<http://www.nappliance.com/support/library.asp>

Knowledge Base resources for configuration and troubleshooting is located on the nAppliance online support portal

<http://support.nappliance.com>

Additional resources include:

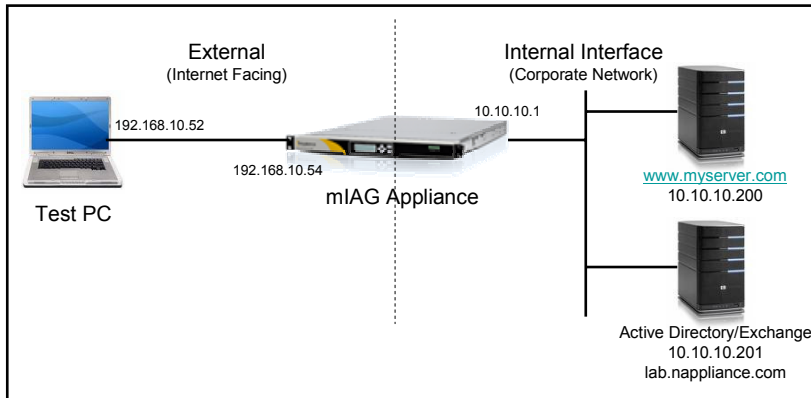
<http://www.iagserver.org>

<http://blogs.technet.com/yuridiogenes/default.aspx>

<http://www.ssl-vpn.de/wiki/default.aspx>

<http://www.isaserver.org>

## Chapter 2 – Network Configuration

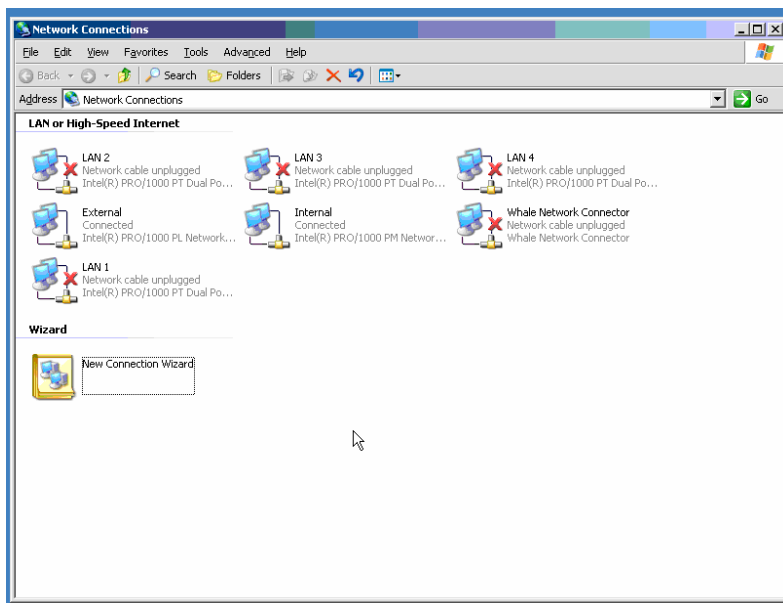


The example configurations for IAG will use a network configuration similar to the above. Sometimes the IP addresses will vary. The Test PC sits on the external network interface for IAG, which would typically be the Internet. The Internal interface is on the corporate network.

The Internal interface is the first NIC port, the port closest to the Mouse and Keyboard ports. The actual port layouts are described in the “Appliance User Guide”.

The External interface is the second NIC port, next to the Internal interface.

Configure the IAG network interfaces using either OneFace Web Console, or via the Windows interface via Control Panel -> Network Connections



Make sure the routing for the application servers (in this case the web server) routes back to the IAG server. In the above network, since both the IAG and the web server is on the same network, there are no routing concerns.

The Whale Network Connector is a virtual interface which is linked to the Internal interface. This is used when IAG creates a traditional VPN circuit from clients to the IAG system, and the traffic is tunneled through this virtual interface. This interface will require it's own range of IP addresses.

When the network is configured, both the PC and the web server should be pingable from the IAG system. The IAG system by default is not pingable by other

systems. The IAG system should also be able to ping remote nodes on the Internet. If this is not working, troubleshoot the Windows Network configuration.

## **Default Gateway**

There should be only one default gateway. This is typically defined on the External interface.

## **Join IAG to Windows Domain**

With the IAG system on the corporate network, the system can be joined to the corporate Windows Domain. This is optional, but is convenient for managing system accounts, security groups, access and passwords. Joining the IAG system to the domain does not have any consequence for authenticating external users access to applications via the IAG portal.

## **DNS Configuration**

The DNS server is typically defined on only one interface. This is usually on the Internal interface, using your Internal DNS servers.

IAG requires hostnames in application URLs instead of IP addresses. When defining published applications, each application published should have it's own IP address, and each IP address requires a DNS definition available to all users accessing the application.

IAG supports host files for hostname definitions, typically this would be used for testing purposes.

# Chapter 3 – First Time IAG Configuration

## Generate IAG Keys

To start IAG configuration manager, run

Start -> All Programs -> Whale Communications IAG -> Configuration

The first time IAG Configuration is run, IAG displays a form to define an internal encryption key. The seed field is used to define the random seed number. Type randomly in this field to define your seed number.

The screenshot shows a Windows-style dialog box titled "Intelligent Application Gateway Encryption Keys". It has two tabs: "Generate Keys" (selected) and "Import Keys". The "Generate Keys" tab contains the following elements:

- A "Seed:" label followed by a text input field.
- A "Passphrase:" label followed by a text input field.
- A "Retype Passphrase:" label followed by a text input field.
- "Create Keys" and "Export Keys" buttons.
- A "Show keys" checkbox.
- Three text input fields labeled "Part 1:", "Part 2:", and "Part 3:".
- "Next >" and "Cancel" buttons at the bottom right.

The left side of the dialog features a decorative vertical strip with a blue and black background, displaying binary code (0s and 1s) in a stylized font.

Once this field is defined, enter your passphrase. This will be the password used to access and manage IAG. Press the Create Keys button to generate the key. The system will insist you save this keyfile on the server, select a directory location and save this file.

Once the encryption keys are defined, you are ready to access the IAG application.

When you first log into IAG after creating the encryption key, IAG will then prompt you to define a password. The passphrase password is used when changing the IAG configuration. The password is used to access the IAG application. As this might be confusing, most users define the passphrase and password using the same code.

The password requires a complex code using numbers, characters and special characters. Be aware of this when creating the passphrase as the passphrase creation does not have this requirement.

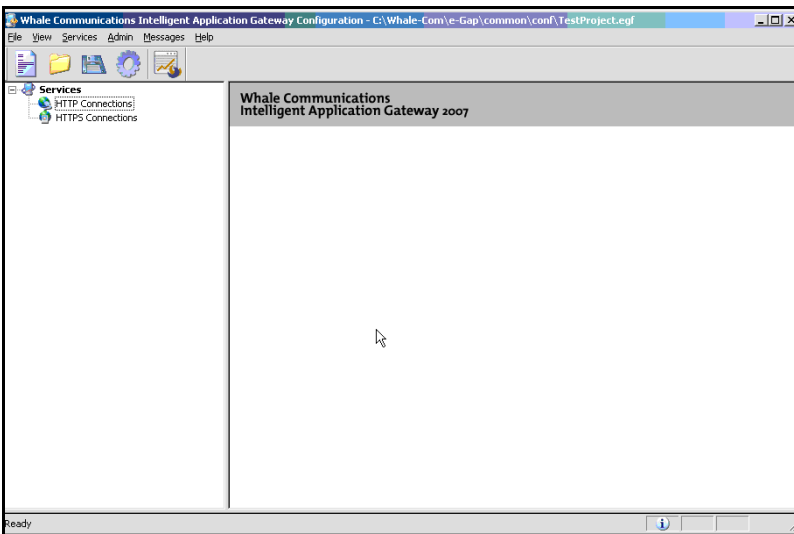
## Chapter 4 – Configure Single Trunk

The primary interface for IAG is the Configuration program. This can be started from the start menu at:

START -> All Programs -> Whale Communications IAG->  
> Configuration

### IAG Configuration Screen

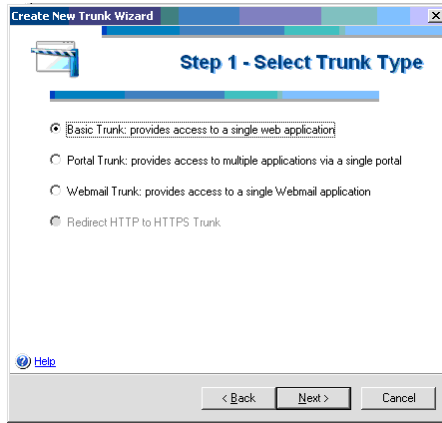
This should bring up the following screen:





## Step 1 – Select Trunk Type

Next, define a new HTTP trunk. Right click on the HTTP Connection option in the left pane. Then select the “New Trunk” pulldown menu item. The IAG configuration program will start a New Trunk wizard.



## Step 2 – Setting the Trunk

Select the Basic Trunk option and press Next.

The screenshot shows a window titled "Create New Trunk Wizard" with a progress bar at the top. The main heading is "Step 2 - Setting the Trunk". Below this, there is a yellow warning icon and the following fields:

- Trunk Name:
- Public Hostname/IP Address:
- External Website section (indicated by a minus sign):
  - IP Address:
  - HTTP Port:
  - HTTPS Port:

At the bottom left is a "Help" link. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

The Trunk Name should not contain special characters nor spaces.

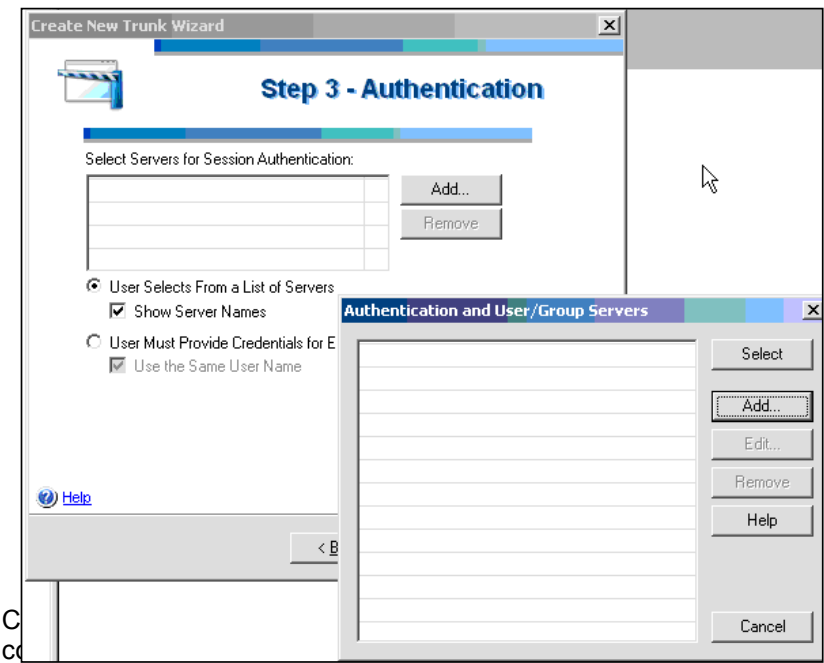
The Public Hostname must contain a hostname and not an IP address. Using an IP address in this field causes stability problems. Future releases of IAG will not support an IP address at all.

External Website is the IP address that IAG will use and respond to for IP connections for the web application. In

this case, we are using the External IP address of the IAG system.

# Step 3 – Authentication

Authentication requires the inbound user to give his username and password to be allowed access to an application. IAG queries Active Directory in this case for this information.



# Define Active Directory Connection

A form will appear allowing the administrator to define a connection to an Active Directory server.

Application Gateway Configuration

Create New Trunk Wizard

Select Servers for Session

User Selects From

☒ Show Server Names

☐ User Must Provide Credentials

☒ Use the Same Credentials

[Help](#)

Add Server

Type: Active Directory

Name: Corporate Domain Controller 1

IP/Host: lab.nappliance.com

Port: 389

☐ Secure Port

Alternate IP/Host:

Alternate Port: 389

☐ Secure Port

Domain: lab

Groups/Users Search

Base:

☐ Include Subfolders

Fetch

Level of Groups Nesting: 0

Server Access Credentials

User: administrator

Password: xxxxxxxx

Confirm Password: xxxxxxxx

Domain: lab

☐ Anonymous Logon

Help

OK

Cancel

Select

Add...

Edit...

Remove

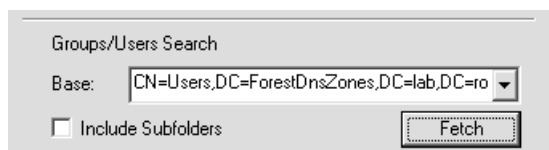
Help

Cancel

Fill in this form with the details and credentials from the local environment.

## Test the Active Directory Connection

Press the “Fetch” button to query the Active Directory server.

A screenshot of a 'Groups/Users Search' dialog box. It has a title bar with the text 'Groups/Users Search'. Below the title bar, there is a 'Base:' label followed by a dropdown menu containing the text 'CN=Users,DC=ForestDnsZones,DC=lab,DC=ro'. Below the dropdown menu, there is a checkbox labeled 'Include Subfolders' which is currently unchecked. To the right of the checkbox is a button labeled 'Fetch'.

If the Base field should return the LDAP parameters from the Active Directory server. If this fails, correct the parameters or user credentials. The IAG system should have IP connectivity with the Active Directory server for this to work.

Click OK to save this authentication record.

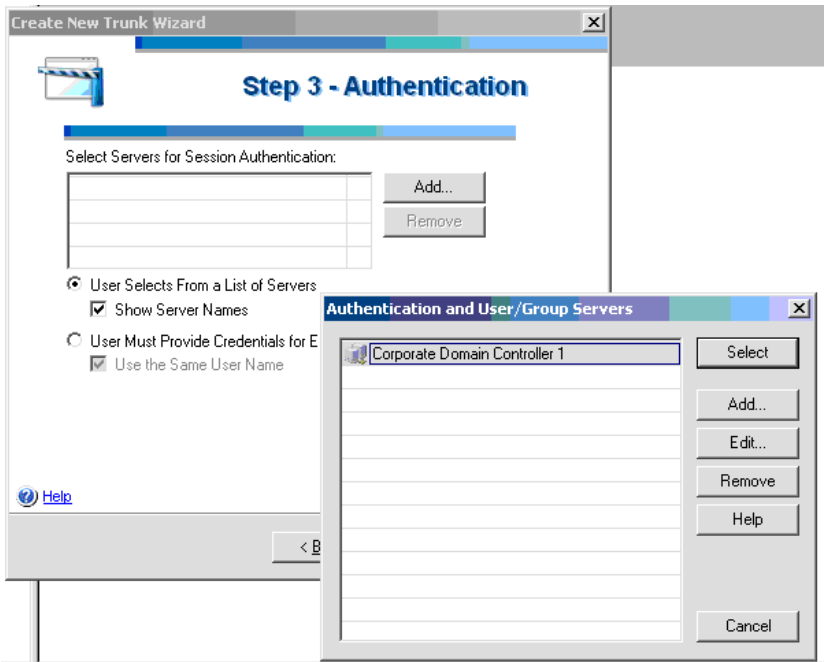
The Active Directory server should be listed in the servers list.

To troubleshoot this connection, make sure the IAG system can communicate with the Active Directory server using port 389. This can be tested from the IAG console via a console command:

```
telnet ADserver 389
```

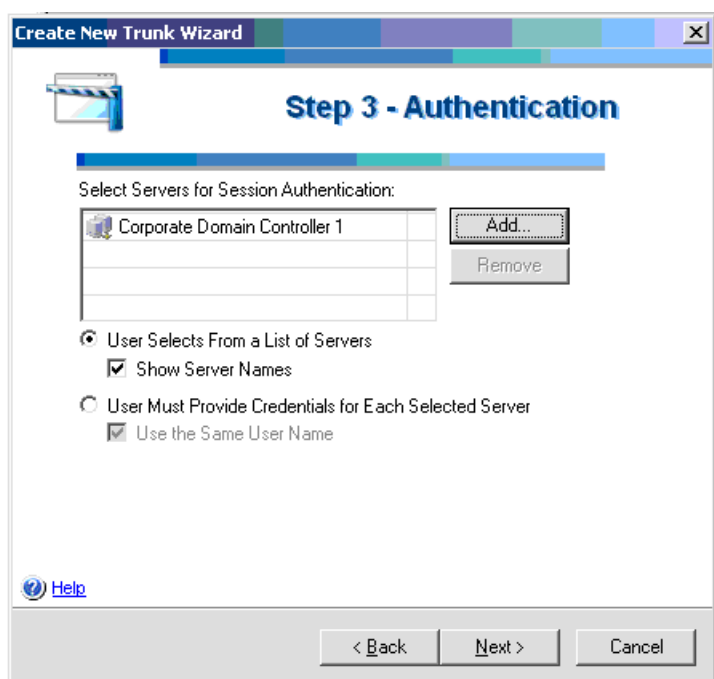
If you can access the Active Directory server, this telnet command will connect. If this fails, you will need to address the network connection issues between the IAG server and the Active Directory servers.

# Step 3 – Authentication



Highlight the new Active Directory server and press the Select button.

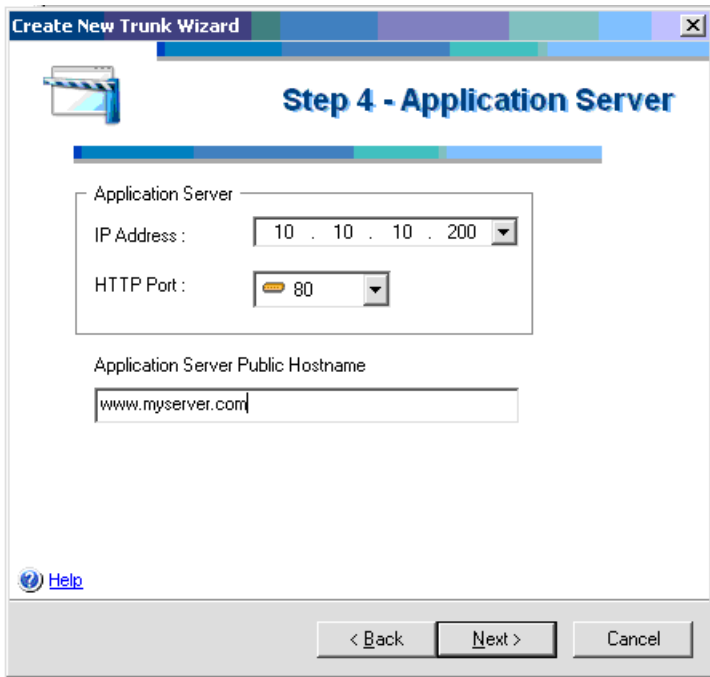
The Active Directory server will show up in the Authentication list of servers.



Click on the Next button to continue.



## Step 4 – Application Server

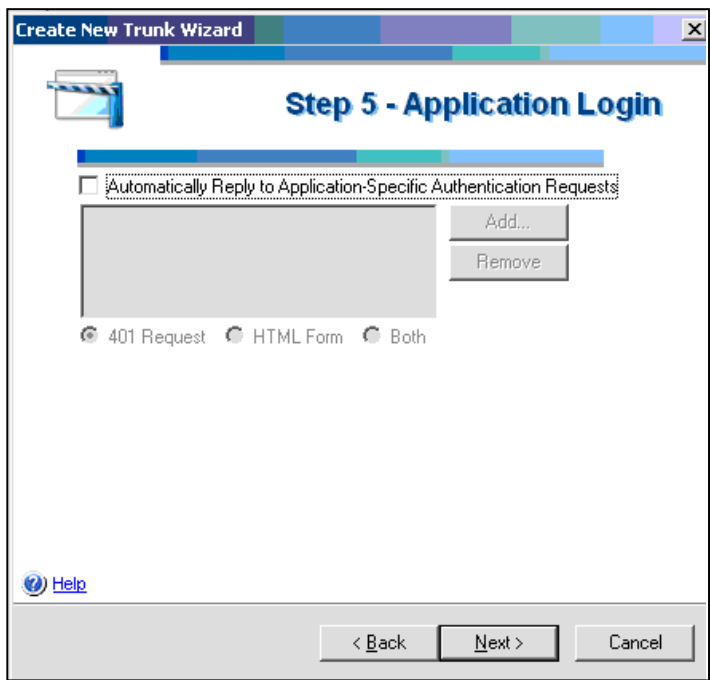


The screenshot shows a window titled "Create New Trunk Wizard" with a progress bar at the top. The current step is "Step 4 - Application Server". Inside the window, there is a section labeled "Application Server" containing two input fields: "IP Address" with a dropdown menu showing "10 . 10 . 10 . 200" and "HTTP Port" with a dropdown menu showing "80". Below these fields is a text input field for "Application Server Public Hostname" containing the text "www.myserver.com". At the bottom left, there is a "Help" link. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

The next step defines the Application Server, or in this case the web server. Enter the IP address of the web server on the network on the Internal IAG network.

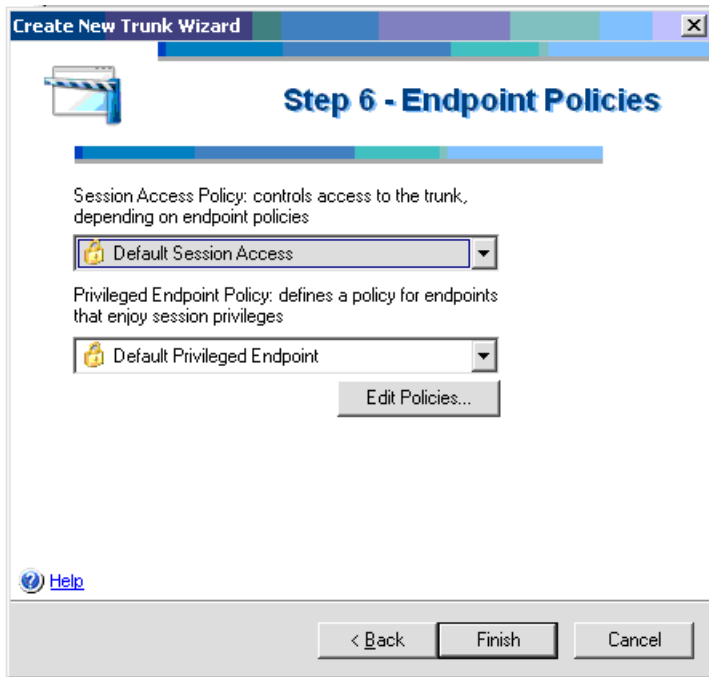
Make sure to enter a host name instead of an IP address for the Server Public Hostname.

# Step 5 – Application Login



Take the defaults for the application login. This section provides a mechanism for single sign-on by automatically logging into the application.

## Step 6 – Endpoint Policies



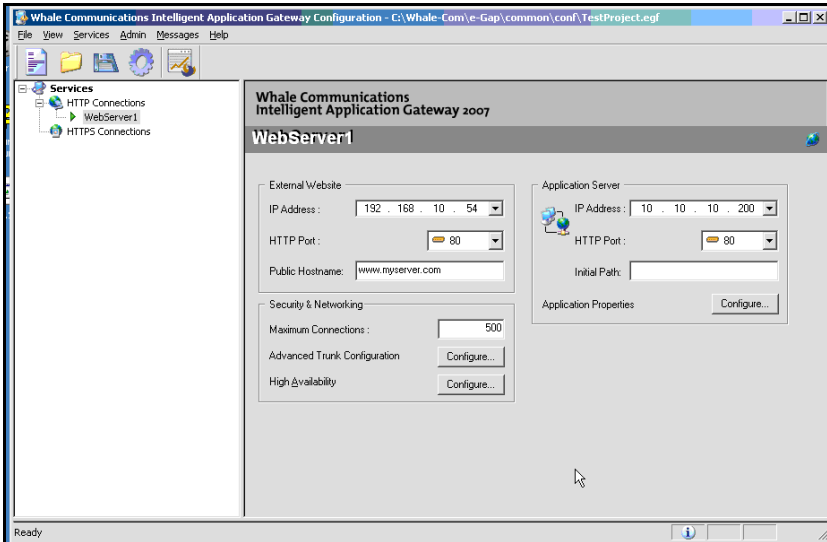
Take the defaults here and press the Finish Button.

The endpoint policies provide a mechanism to test the client for a variety of conditions which must be met before IAG will allow a connection. These conditions include patch levels, the existence of virus scanners, etc.

If this endpoint policy causes problems, select “Always” as the endpoint policy. “Always” disables endpoint checks and allows users to connect for these exercises. This policy can be tightened up after the rest of the system is working correctly.

## New Trunk Created

Once the new trunk is created, it shows up in the Services tree in the left pane.

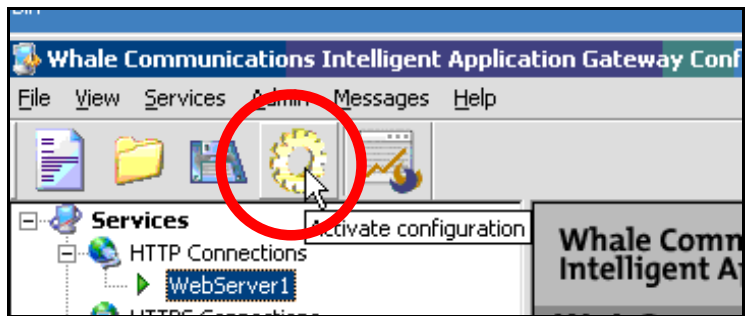


The configuration must now be activated. This saves the configuration in the permanent configuration file. The new trunk will not work until it has been activated.

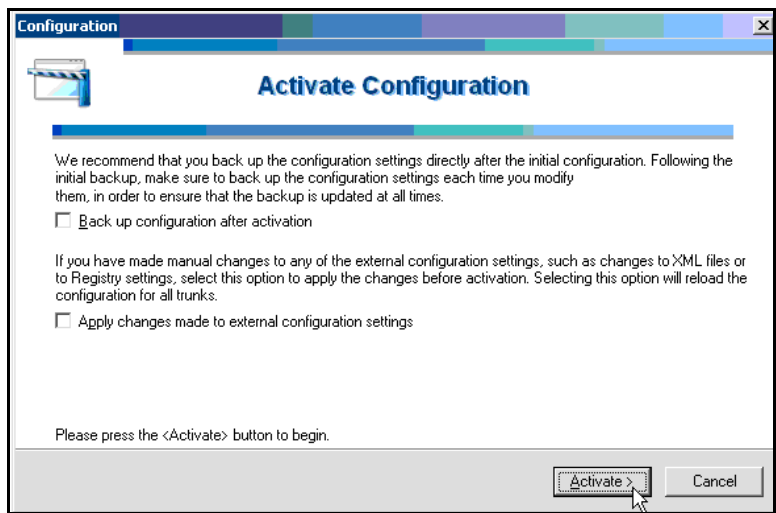
Activate the configuration by clicking on the sprocket ICON at the top left.

# Activate the Configuration

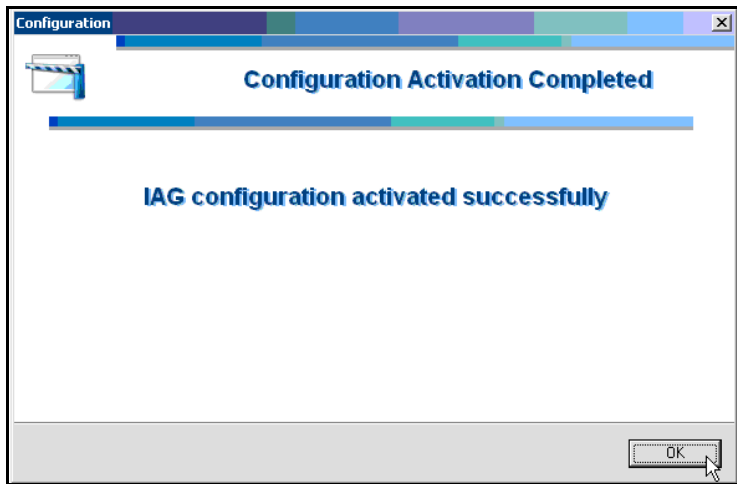
Then press the “Activate” button.



Then press the “Activate” button.



Once the configuration is activated, you will receive a confirmation screen.



And the configuration is complete and the published website is ready to use. This activation process processes the underlying XML configurations and compiles these XML files into the final application definition XML files.

Since IAG is still in the network path between the user and the application, IAG can provide extended functionality such as:

- Session timeout – the administrator can define how long a session will remain inactive before timing out the session.
- Application authentication via multiple authentication schemes. Applications do not have to provide front-end security as this is not provided by IAG.
- SSL – IAG can provide the SSL connection, without requiring every application to provide its own SSL mechanisms.

## Testing the new configuration

To test the new configuration, open the web application with a browser on a PC connected to the network on the External port of the IAG system.

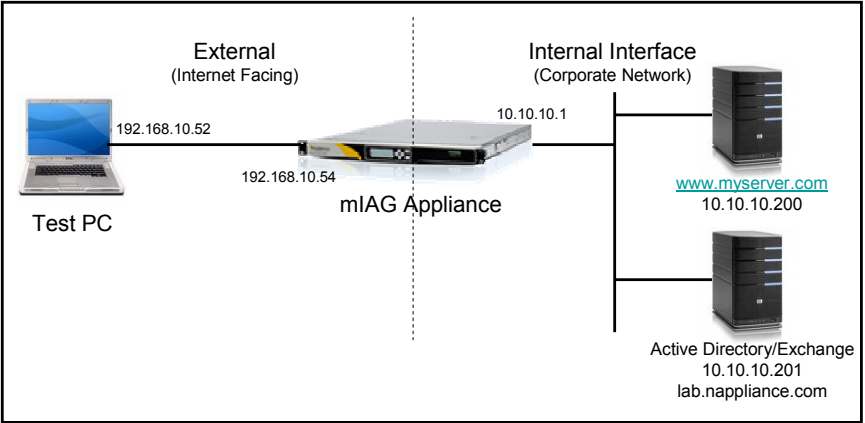
The connection process:

- The PC should connect with the IAG system on the External connection
- The IAG system will require an ActiveX plugin
- If the plugin does not exist, the browser will be prompted to download and install the plugin
- The IAG system will then present a login screen to the user via a web screen
- When the user logs in, the IAG system will interrogate the user PC and reject the connection if the user PC does not meet
- Once the PC passes the connection policy, the web application will be presented on the user browser.

## Connect to the web application

Point the browser at <http://www.myserver.com/>

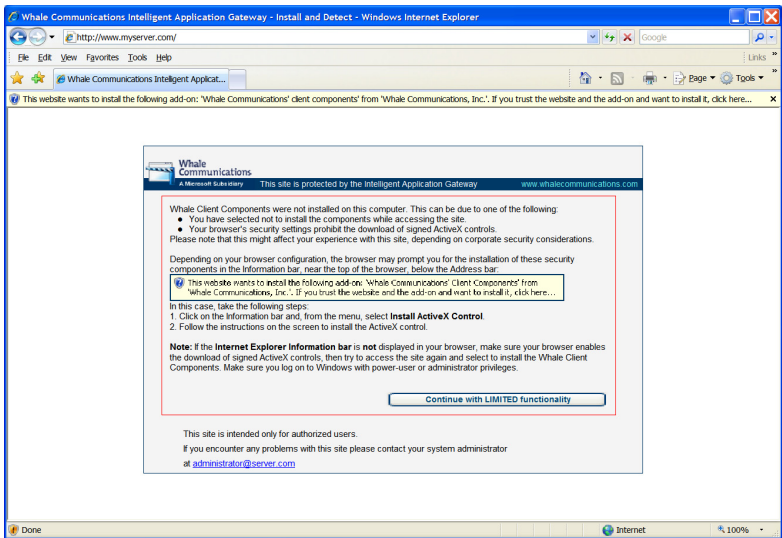
The hostname should point at the External interface on the IAG system which is IP 192.168.10.54.





# ActiveX plugin install

The IAG system will present a page describing the ActiveX installation process.



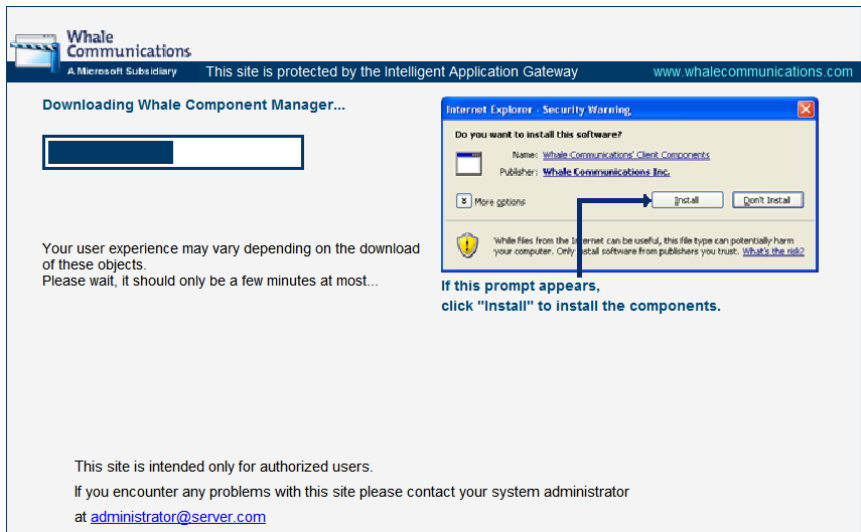
Notice the yellow bar at the top requesting the user allow an ActiveX plugin install.



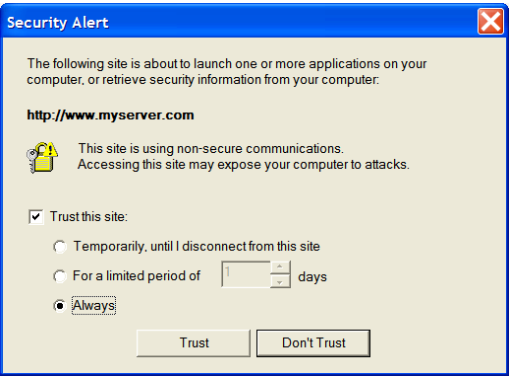
Click on the Install button and install the ActiveX module.

# Login Process

IAG will display an ActiveX installation page with a progress bar.



Since there is not signed certificate installed on the IAG system yet, the browser will present a warning message. Allow this connection by pressing the “Trust” button.

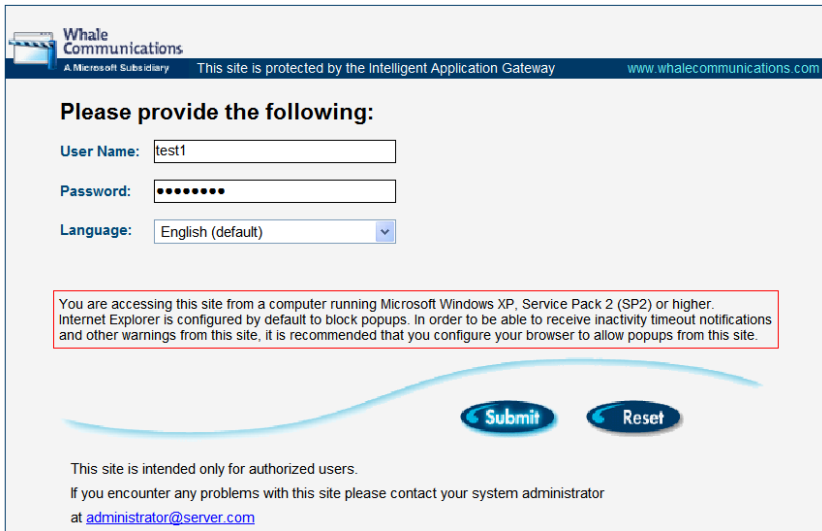




## IAG Login

The IAG system will then present a login screen.

The user id and password will be an account existing on the Active Directory server which was defined earlier.



The screenshot shows a web browser window displaying the IAG Login page for Whale Communications. The page has a blue header bar with the Whale Communications logo on the left, the text "A Microsoft Subsidiary" below it, "This site is protected by the Intelligent Application Gateway" in the center, and the URL "www.whalecommunications.com" on the right. Below the header, the main content area is light gray. It starts with the heading "Please provide the following:". Below this heading are three form fields: "User Name:" with a text box containing "test1", "Password:" with a text box containing seven dots, and "Language:" with a dropdown menu showing "English (default)". Below these fields is a red-bordered box containing a warning message about Internet Explorer's pop-up blocking. At the bottom of the form area are two blue buttons labeled "Submit" and "Reset". Below the buttons, there is a line of text stating the site is for authorized users only, followed by contact information for the system administrator.

Whale Communications  
A Microsoft Subsidiary    This site is protected by the Intelligent Application Gateway    www.whalecommunications.com

**Please provide the following:**

User Name:

Password:

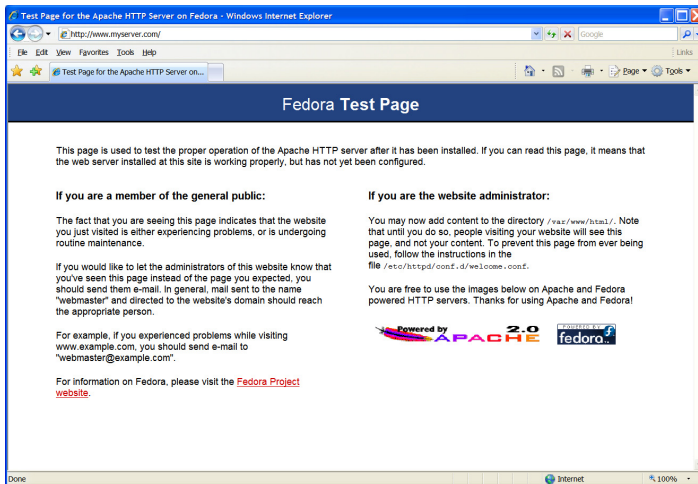
Language:

You are accessing this site from a computer running Microsoft Windows XP, Service Pack 2 (SP2) or higher. Internet Explorer is configured by default to block popups. In order to be able to receive inactivity timeout notifications and other warnings from this site, it is recommended that you configure your browser to allow popups from this site.

This site is intended only for authorized users.  
If you encounter any problems with this site please contact your system administrator  
at [administrator@server.com](mailto:administrator@server.com)

## Finally the Web Application

If the correct user name and password are entered, and after the “Submit” button is pressed, the final web application will be displayed.



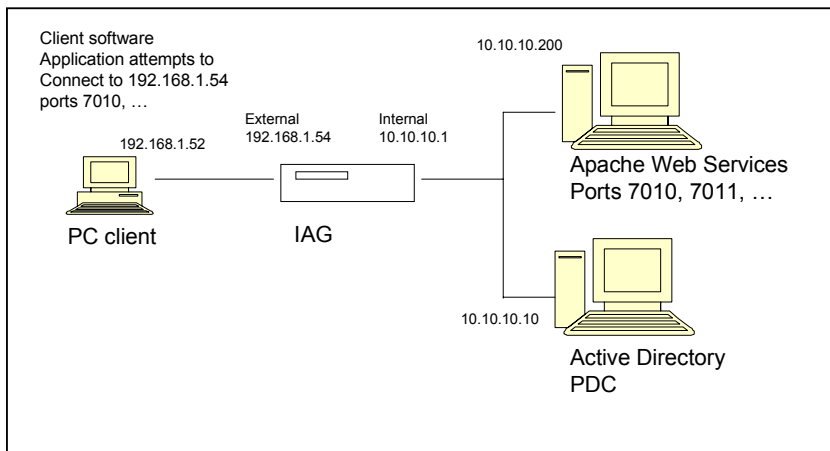
In this exercise, we published a simple web site or web application. IAG added the following services to this web application:

1. User Authentication – the user must be a valid domain user to access this application
2. SSL, the web application is HTTP on the corporate network, but HTTPS for external users
3. Endpoint policy, IAG can require an end user system to meet corporate policies to connect to this application
4. Application Wiping – users accessing this application can have all browser trace history removed when disconnecting from the application

## Chapter 5 – Configure Portal Trunk

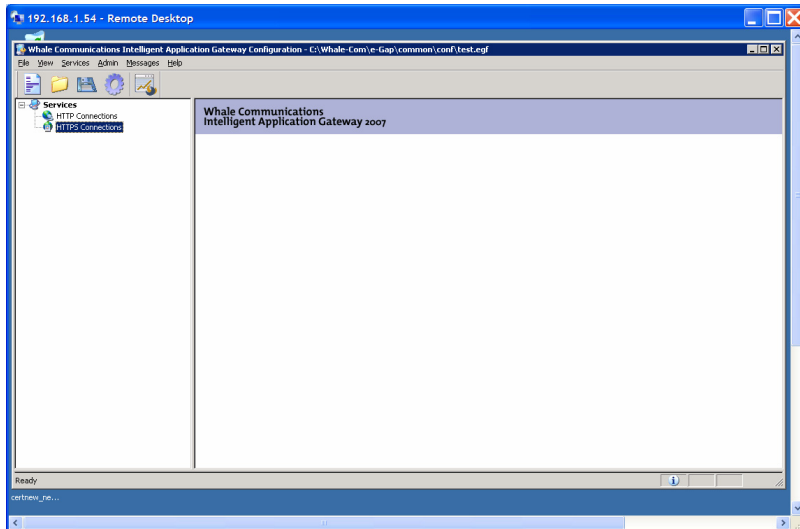
An IAG portal is presented to the user as a webpage created by the IAG server and has one or multiple published applications. These applications may be Web applications, Web Services or Client/Server applications.

For this exercise, we will be using a laboratory configuration such as:



To create a new IAG Portal, start the IAG Configuration application. Connect to the IAG server desktop and run:

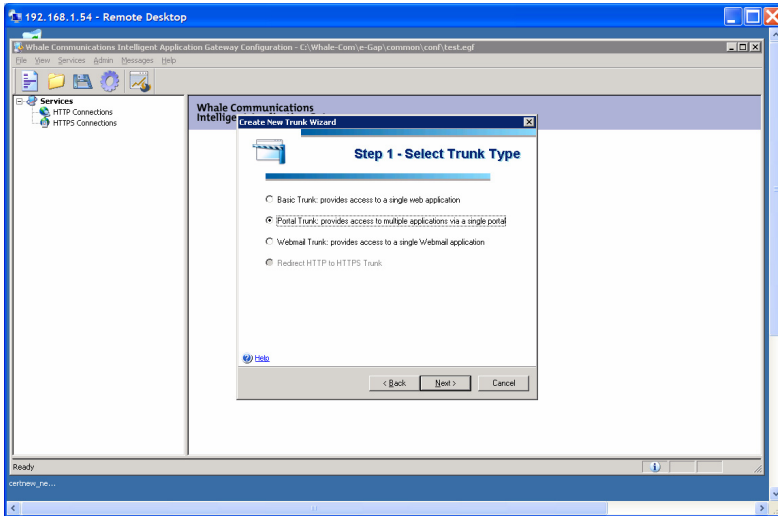
Start -> All Programs -> Whale Communications IAG -> Configuration



To create a new Portal, write click on the “HTTPS Connections” on the left pane. Then select “New Trunk”.

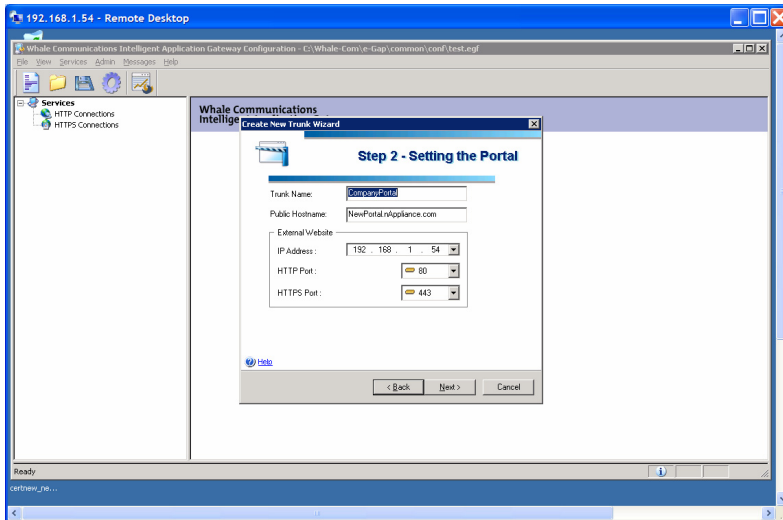


## Step 1 – Select Trunk Type



Select the Second Option, “Portal Trunk...” and press Next.

## Step 2 – Setting the Trunk



Fill in the form.

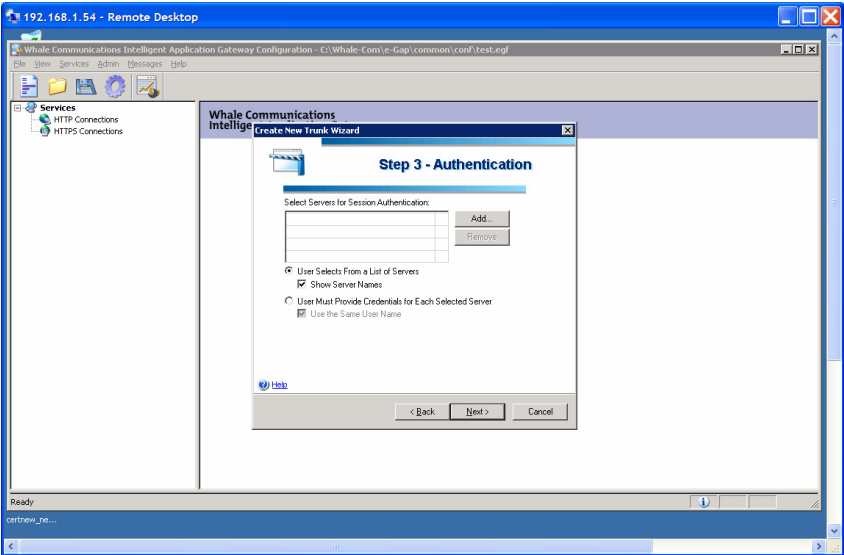
The Trunk Name will be the description to the IT Administrator. Do not use spaces or special characters for this name.

Public Hostname: is the FQDN hostname of the portal, which will be the External IP hostname of the IAG system. Do not use an IP address here; make sure there is a valid DNS entry for this name and this DNS entry is valid on the Internet.

IP Address: The External interface IP address. (The example uses a private IP address, when used on the Internet this would never be the case).

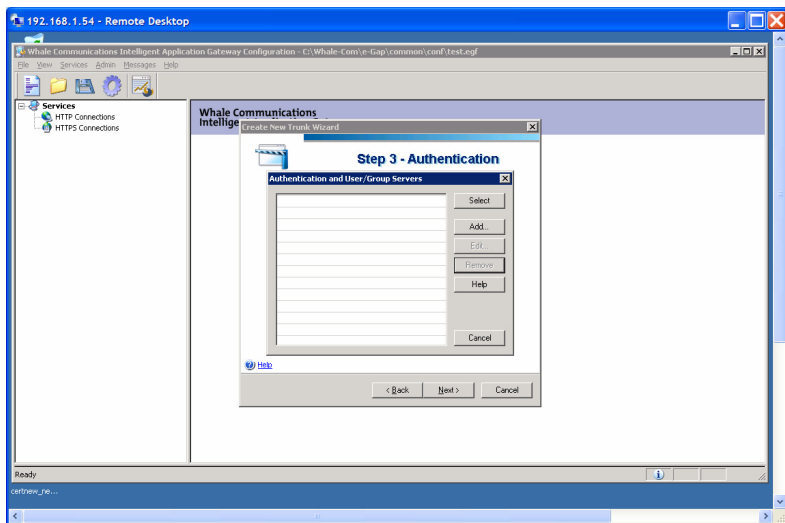
HTTP Port, HTTPS Port, leave these as defaults except for exceptional cases.

### Step 3 - Authentication

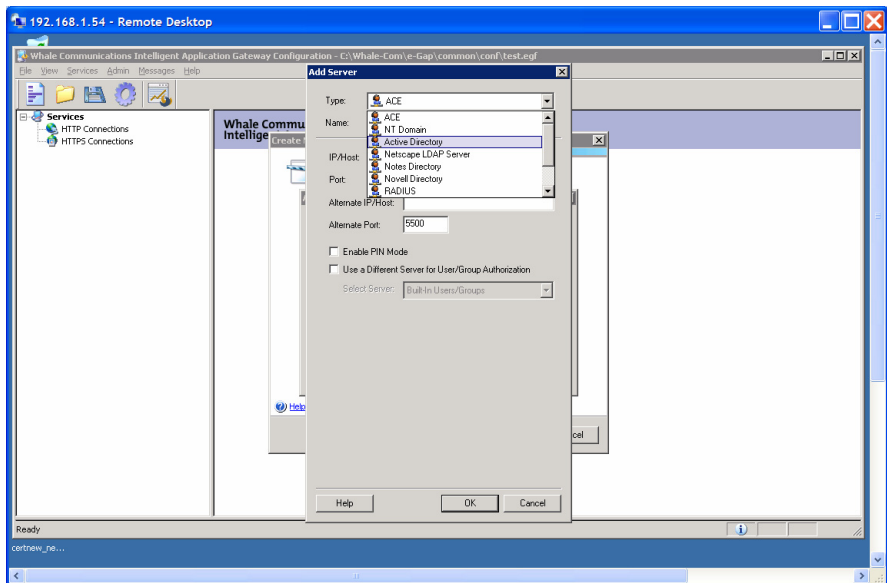


Add the Authentication Server. In this case, we will be authenticating against an Active Directory server.

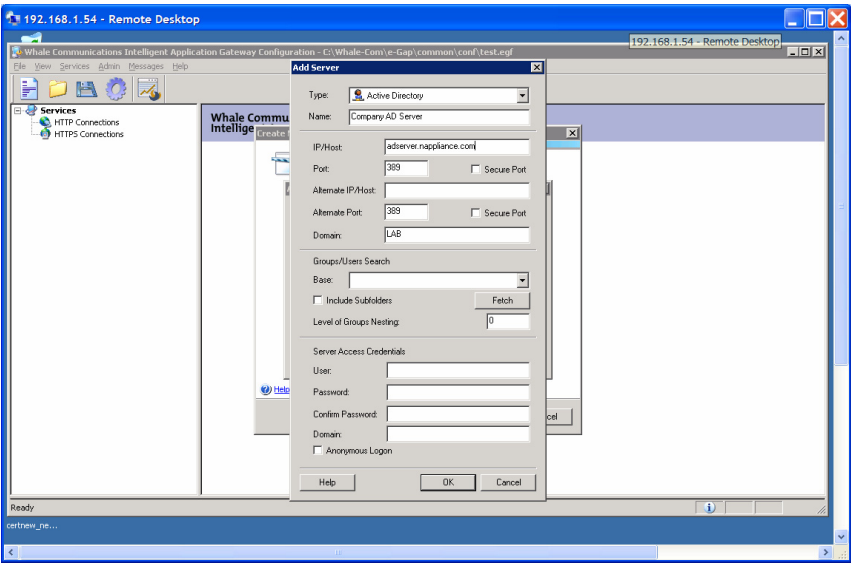
Click on the Add button.



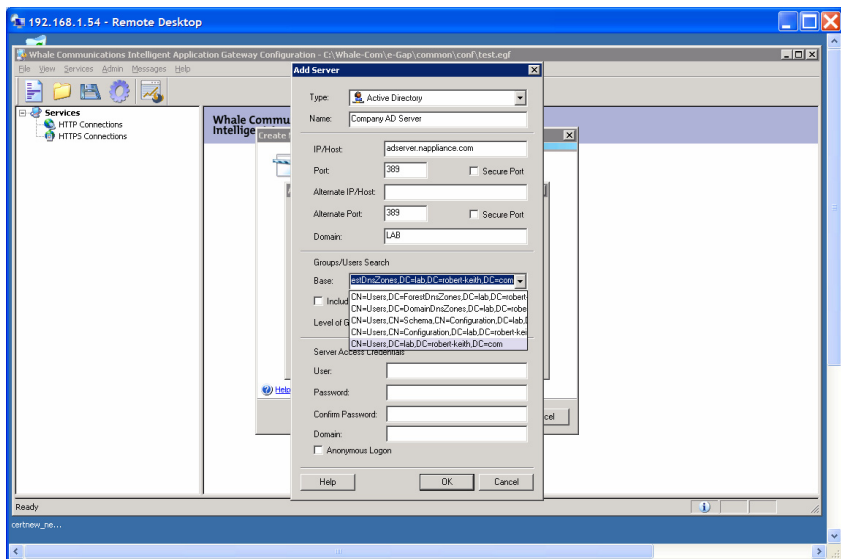
Click on the Add button to create a new Authentication Server object.



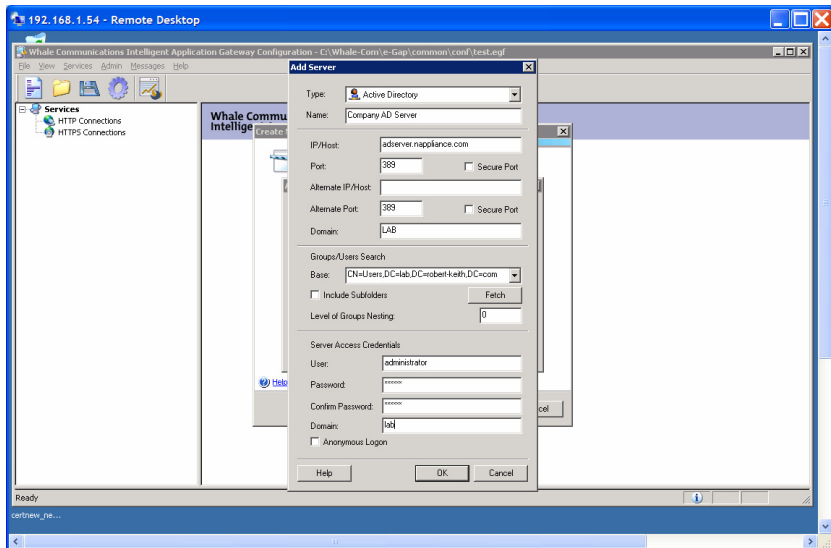
For the type of Authentication Servers, select the “Active Directory” selection in the pulldown.



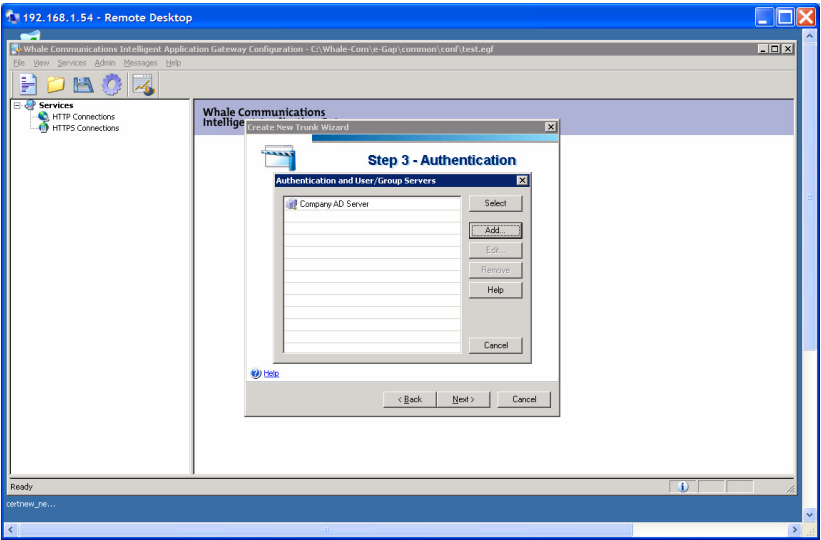
Fill in the Active Directory server information like above. To fill in the LDAP Base field, press the fetch button. The fetch function will use the filled in data for the Active Directory server and automatically fill in the LDAP query information.



Select the simplest connect string.

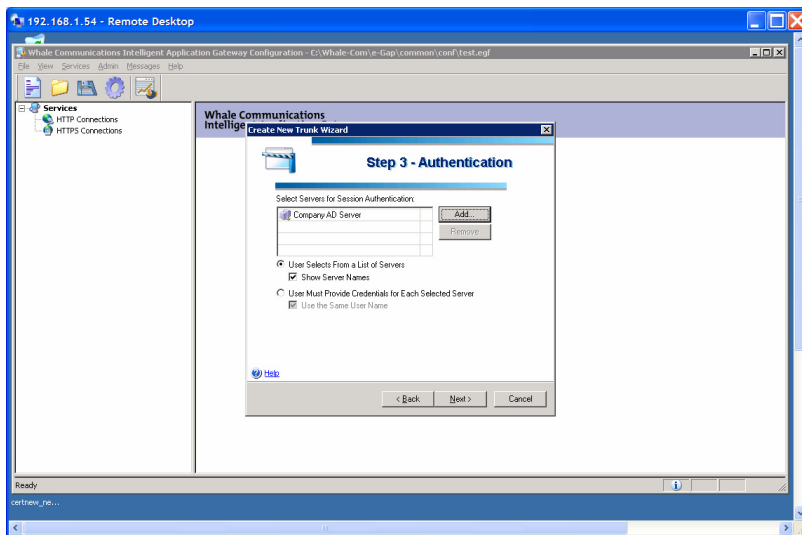


Then fill in the credentials for a domain user with access to query any user and password. This will be used to authenticate user logins.



When successful, the new authentication object will be created. This will be available for other application access when connecting through the portal.

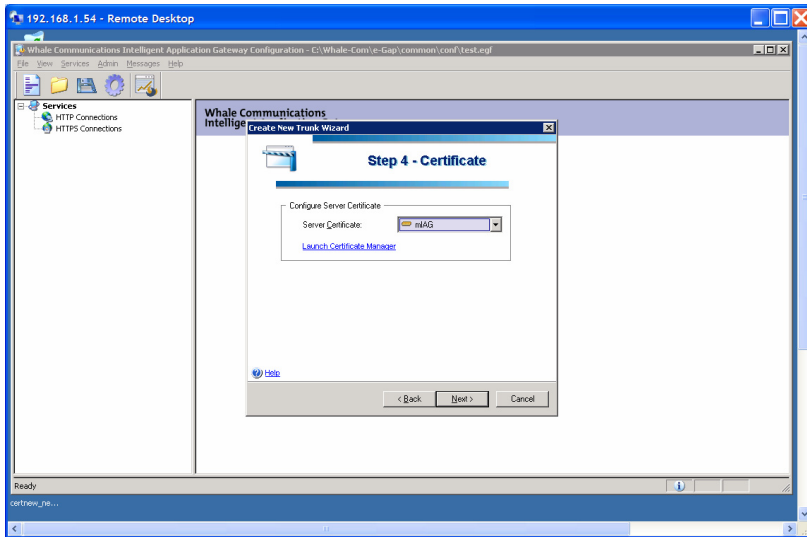
Now click on this authentication object and click on the Select button.



Press Next.



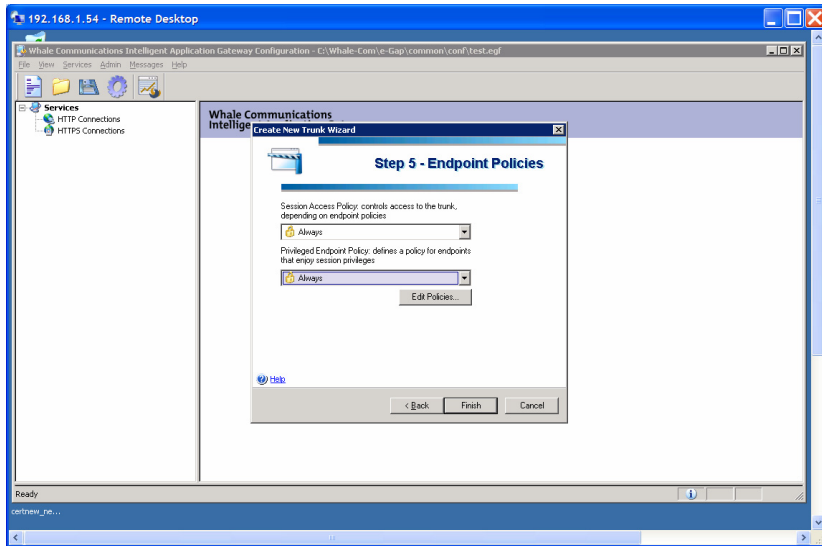
## Step 4 – Certificate



For correct user access to the portal, a valid certificate should be installed. This certificate should be created by a certificate authority. The nAppliance IAG system has default certificates available, but these are not authorized, and browsers connecting to the IAG portal will be presented with a certificate warning message.

Click on Next for this exercise. A new certificate can be installed later.

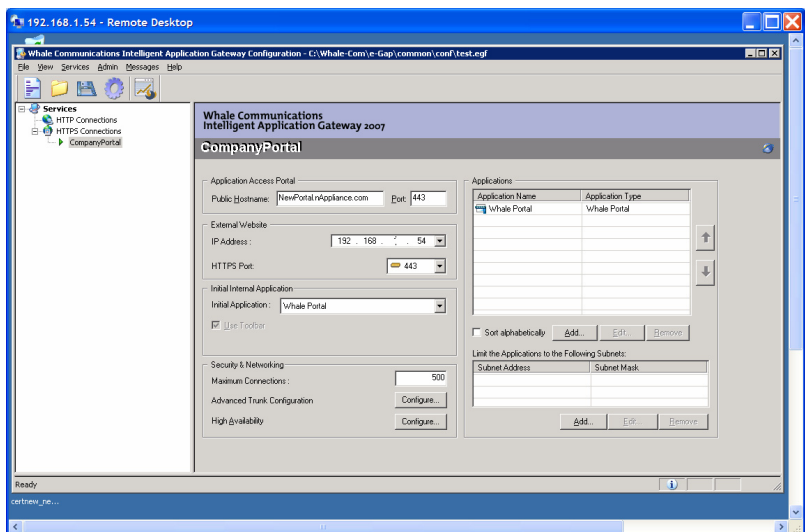
## Step 5 – Endpoint Policies



Select “Always” for the Session and Endpoint policies. Always does no filtering and allows users to connect to the portal regardless of the state of the user computer.

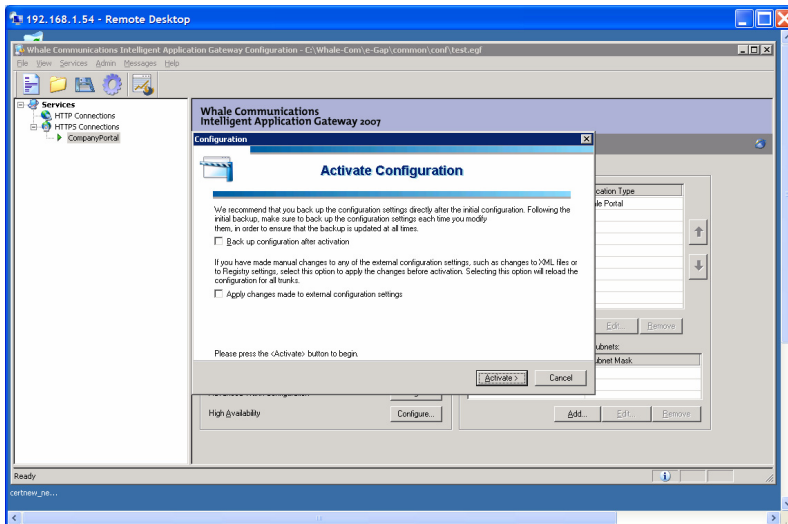
Users still have to authenticate with valid domain username and passwords. Uses this relaxed access policy for now to make the initial connections, then you can tighten access as desired to meet corporate access policies.

Click on Finish to create the portal configuration.

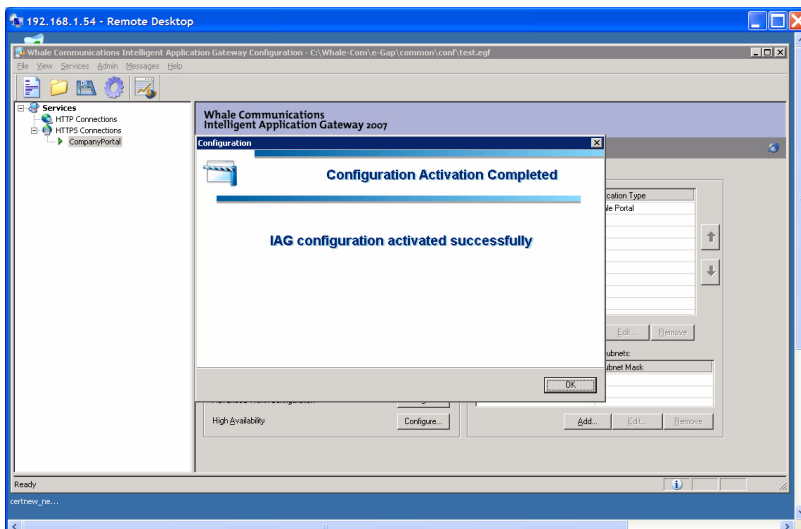


Now, activate the configuration to save the newly defined portal. Click on the sprocket ICON at the top left of the screen.

Enter your passphrase, then...



Click on the Activate button to complete the configuration.

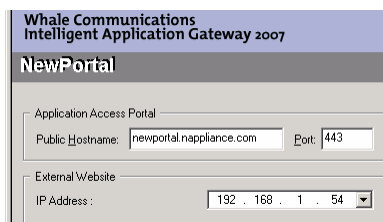


## Test the New Portal

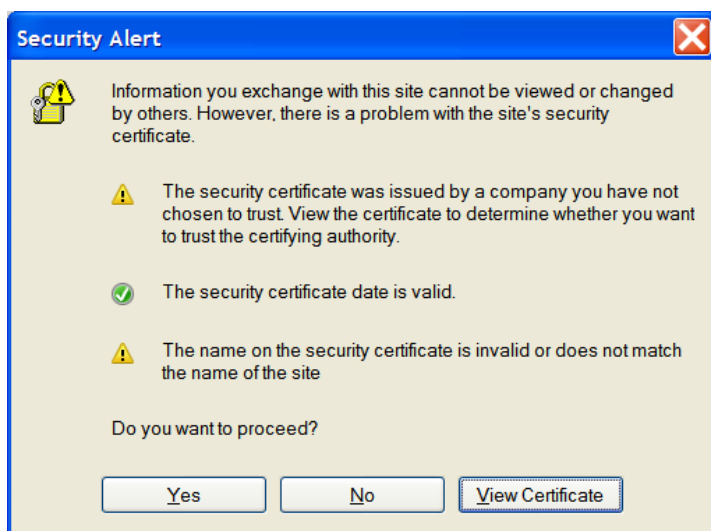
You can connect to this configuration by connecting to the URL

<https://NewPortal.nAppliance.com/>

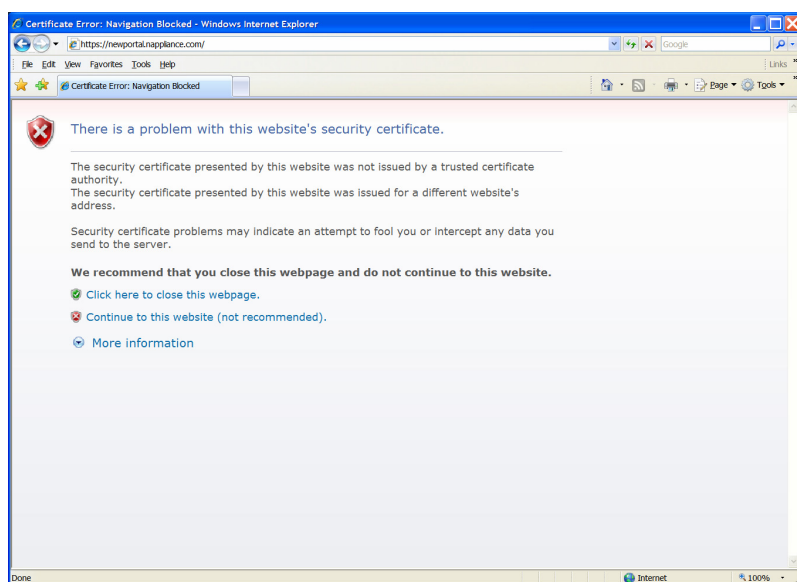
or whatever hostname you defined in your portal configuration.



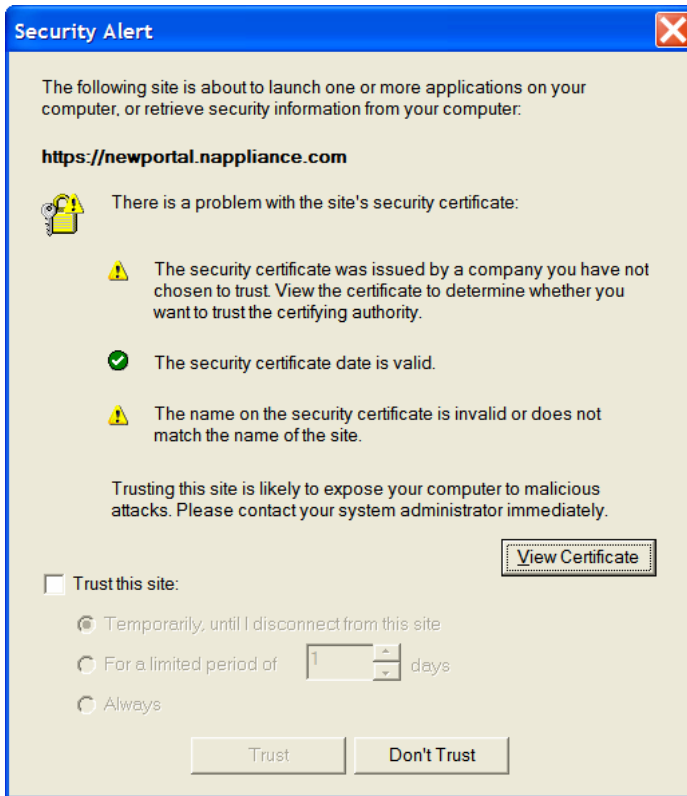
The screenshot shows a web interface titled "Whale Communications Intelligent Application Gateway 2007" with a sub-header "NewPortal". It contains two main sections: "Application Access Portal" and "External Website". The "Application Access Portal" section has a "Public Hostname" field with the value "newportal.nappliance.com" and a "Port" field with the value "443". The "External Website" section has an "IP Address" field with a dropdown menu showing "192 . 168 . 1 . 54".



You will see the security warning. Proceed anyway.

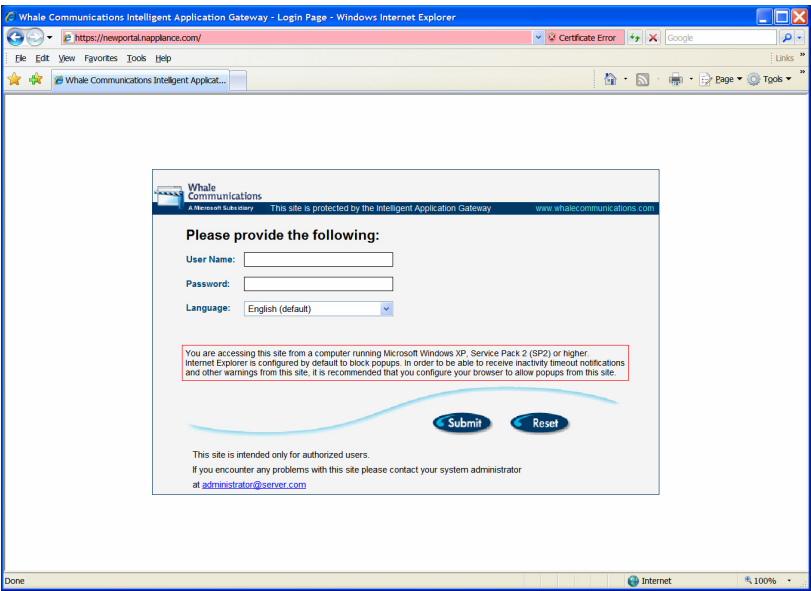


And this warning screen. Continue anyway.



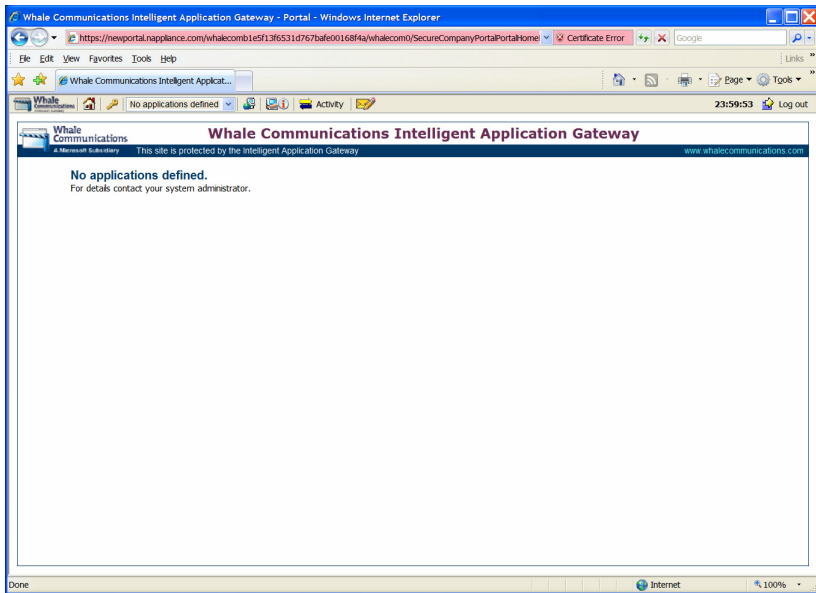
Click on “Trust this site” and continue anyway.

You should a portal login page.



Log in with a valid domain user existing on the Active Directory server. In this case, we will use the “Administrator” account and password. This is the Administrator account on the Active Directory, not on the IAG server.



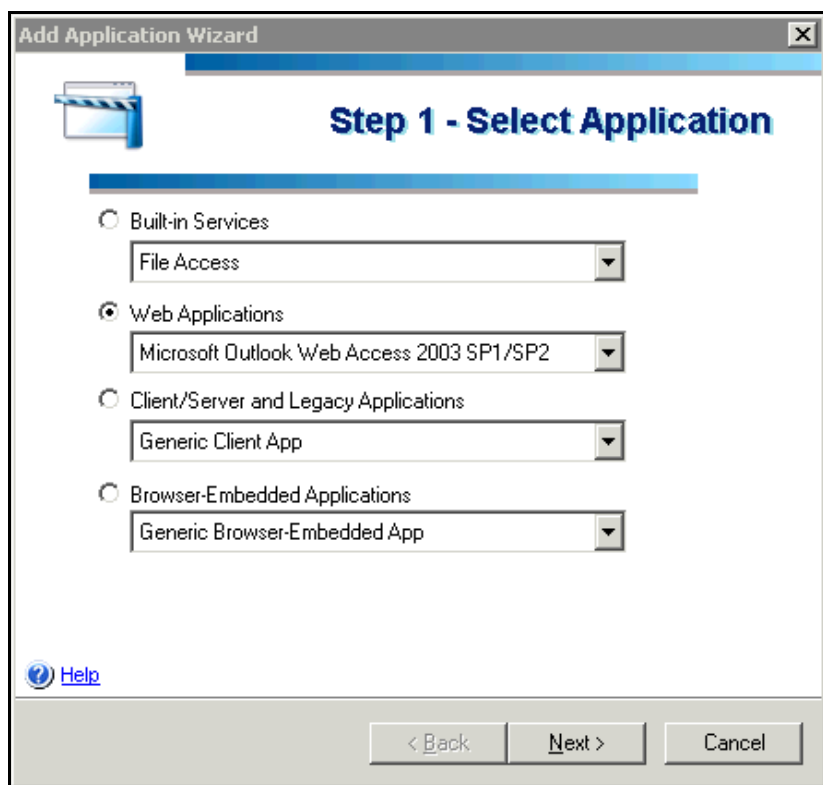


When successful, you will see an IAG portal webpage. This page shows a “No applicatinos...” message.

Next steps are to publish applications on this portal.

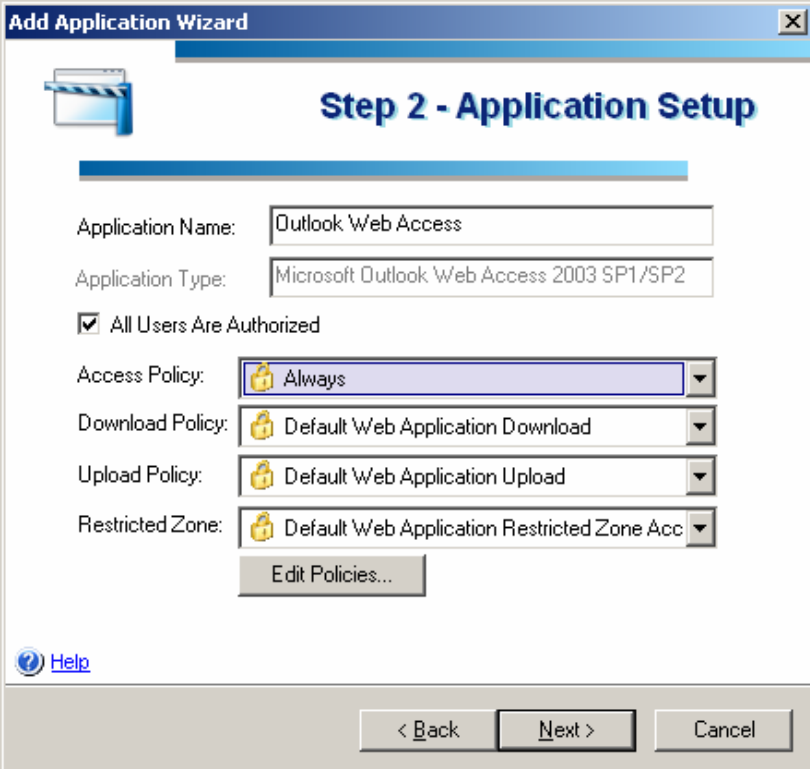
## Chapter 6 – Publish Web Application - OWA

In this exercise, we will publish Outlook Web Access through the IAG Portal.



Select the Web Application “Microsoft Outlook Web Access 2003 SP1/SP2” and click on “Next”.

## Step 2 – Application Setup

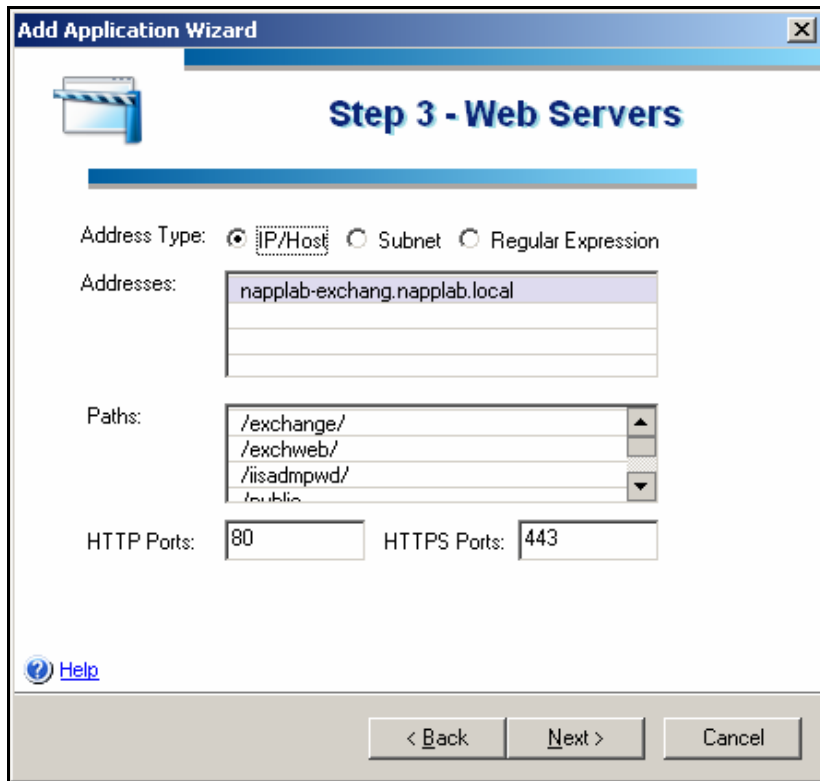


The screenshot shows the 'Add Application Wizard' window, specifically 'Step 2 - Application Setup'. The window has a title bar with the text 'Add Application Wizard' and a close button. Below the title bar is a blue header area with a folder icon and the text 'Step 2 - Application Setup'. The main content area contains the following fields and controls:

- Application Name:** A text box containing 'Outlook Web Access'.
- Application Type:** A text box containing 'Microsoft Outlook Web Access 2003 SP1/SP2'.
- Authorization:** A checkbox labeled 'All Users Are Authorized' which is checked.
- Access Policy:** A dropdown menu with a lock icon, currently set to 'Always'.
- Download Policy:** A dropdown menu with a lock icon, currently set to 'Default Web Application Download'.
- Upload Policy:** A dropdown menu with a lock icon, currently set to 'Default Web Application Upload'.
- Restricted Zone:** A dropdown menu with a lock icon, currently set to 'Default Web Application Restricted Zone Acc'.
- Edit Policies...:** A button located below the policy dropdowns.
- Help:** A blue question mark icon followed by the text 'Help'.
- Navigation Buttons:** At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Select a descriptive application name. Also select “Always” for the Access Policy. This endpoint policy can be tightened later.

## Step 3 – Web Servers



The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar is a blue header area with a folder icon and the text "Step 3 - Web Servers".

The main content area contains the following fields and controls:

- Address Type:** Three radio buttons are present: ☒ "P/Host", ☐ "Subnet", and ☐ "Regular Expression".
- Addresses:** A text box containing "napplab-exchang.napplab.local" with two empty rows below it.
- Paths:** A list box with four items: "/exchange/", "/exchweb/", "/iisadmpwd/", and "/public". The first three items are visible, and the last one is partially obscured. Up and down arrow buttons are on the right side of the list box.
- HTTP Ports:** A text box containing "80".
- HTTPS Ports:** A text box containing "443".

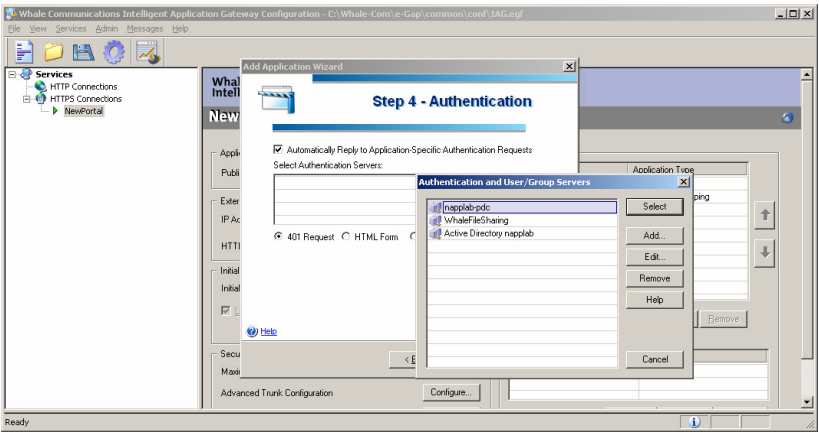
At the bottom left, there is a "Help" link with a question mark icon. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Select the host for the Exchange server.

Note: This must be a valid DNS name, and it must be a FQDN format. Also, this needs to use the 3 node format name, such as exchange.company.com.

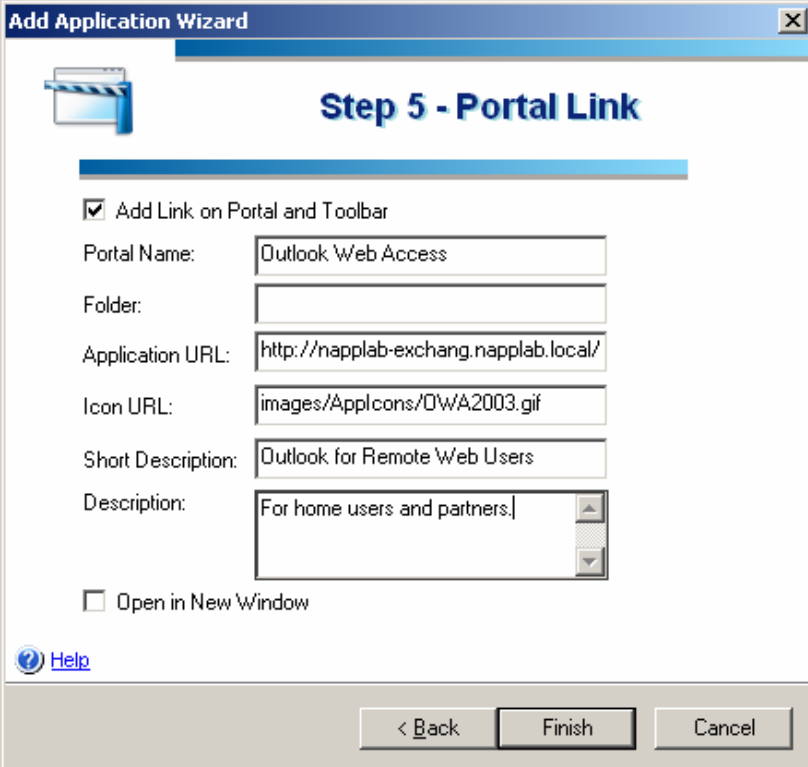
The Paths are defined for the default exchange OWA configuration. If you have modified this path, you have to include this path in the “Paths:” box.

# Step 4 – Authentication



Enter the Active Directory server defined earlier.

## Step 5 – Portal Link



**Add Application Wizard**

**Step 5 - Portal Link**

☒ Add Link on Portal and Toolbar

Portal Name:

Folder:

Application URL:

Icon URL:

Short Description:

Description:

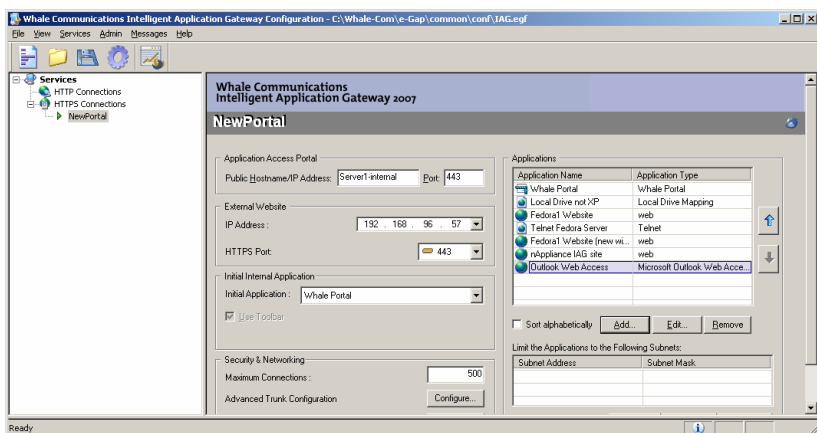
☐ Open in New Window

[Help](#)

< Back   Finish   Cancel

Define the text for the Portal page which describes this service to the user.

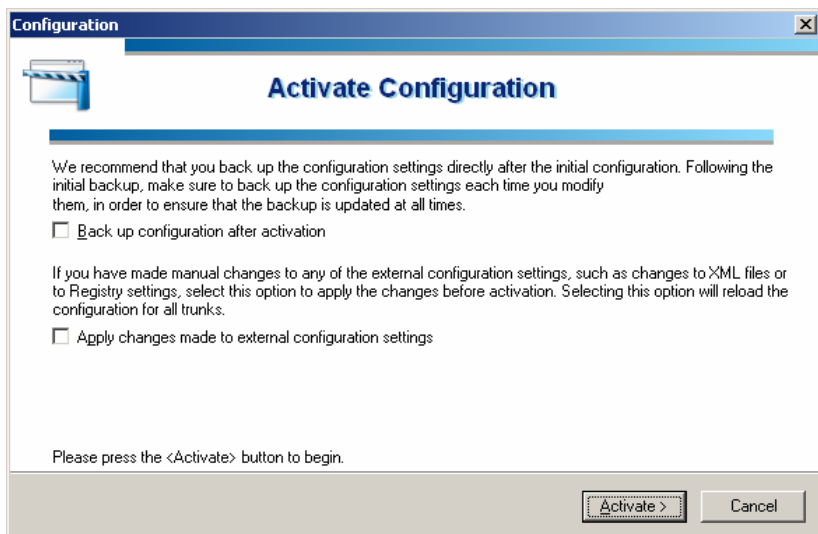
Note: if you select the “Open in New Window”, IAG will spawn a new browser window for Outlook. This exercise leaves outlook embedded inside the IAG web application window.



The new application for Outlook is defined in the IAG portal configuration.

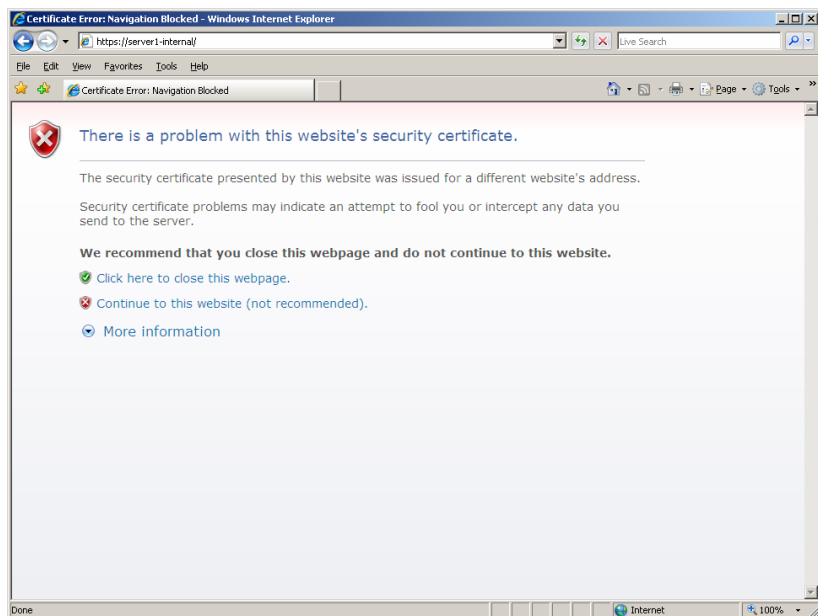
Remember to activate the IAG configuration





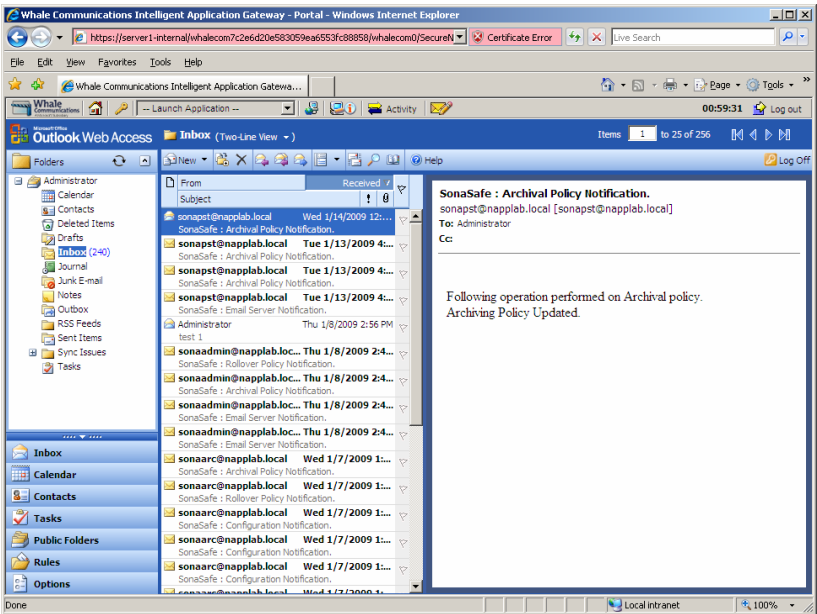
## Testing the Application

Connect to the IAG portal web application.

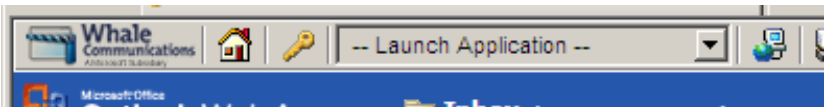


Click “Continue...”.

And when selecting the Outlook link on the IAG Portal, the Outlook Web Access application is displayed.



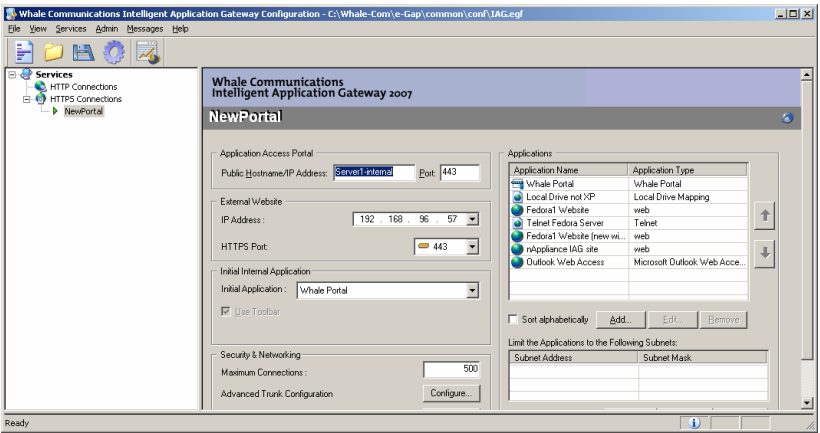
Notice that the IAG Portal toolbar is displayed above the Outlook web application. This allows the user to select other applications from the pulldown application launcher and perform other functions.



# Chapter 7 – Publish Client/Server Application – Terminal Services

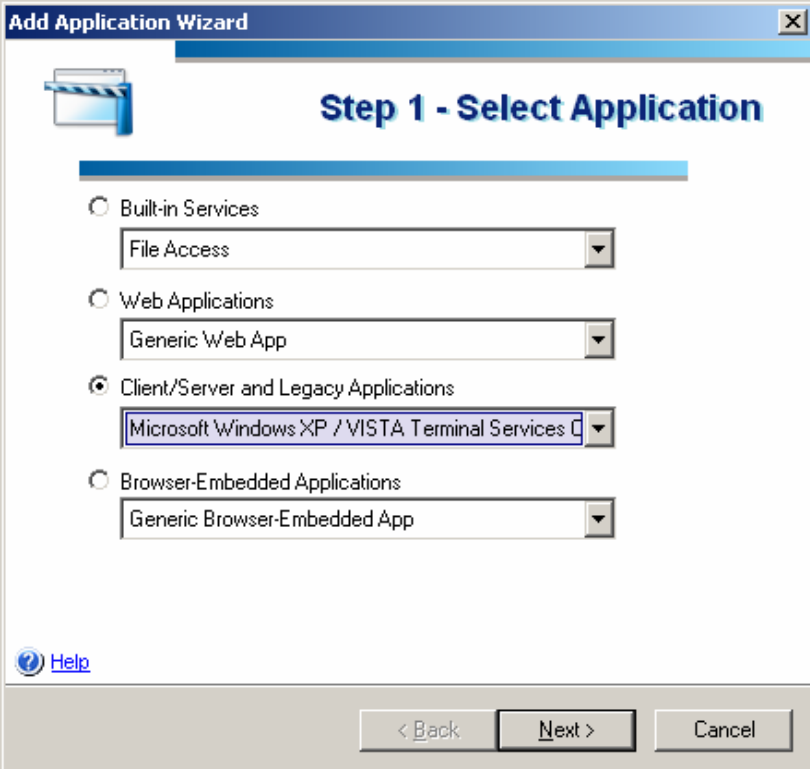
This example publishes the Microsoft Terminal Services application from an internal corporate server to remote users.

The Terminal Services application must reside on the client system.



Add a new application to the existing portal.

## Step 1 – Select Application



**Add Application Wizard**

**Step 1 - Select Application**

☐ Built-in Services  
File Access

☐ Web Applications  
Generic Web App

☒ Client/Server and Legacy Applications  
Microsoft Windows XP / VISTA Terminal Services

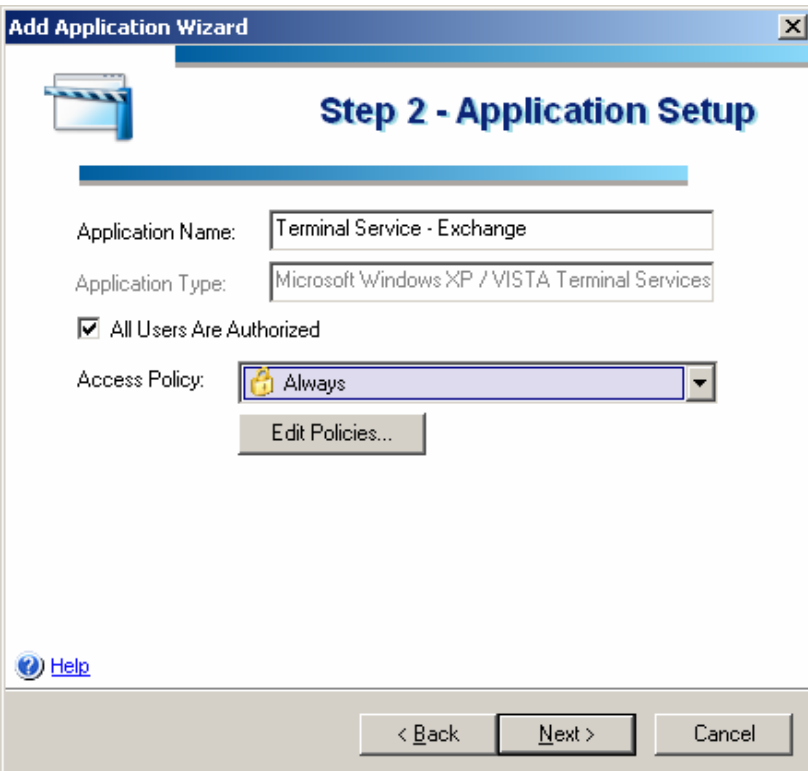
☐ Browser-Embedded Applications  
Generic Browser-Embedded App

[Help](#)

< Back   Next >   Cancel

Select the “Microsoft Windows XP/Vista Terminal Services Client” from the application list. There is an older version of this for Windows 2000 Terminal Services. Do not select this older version.

## Step 2 – Application Setup

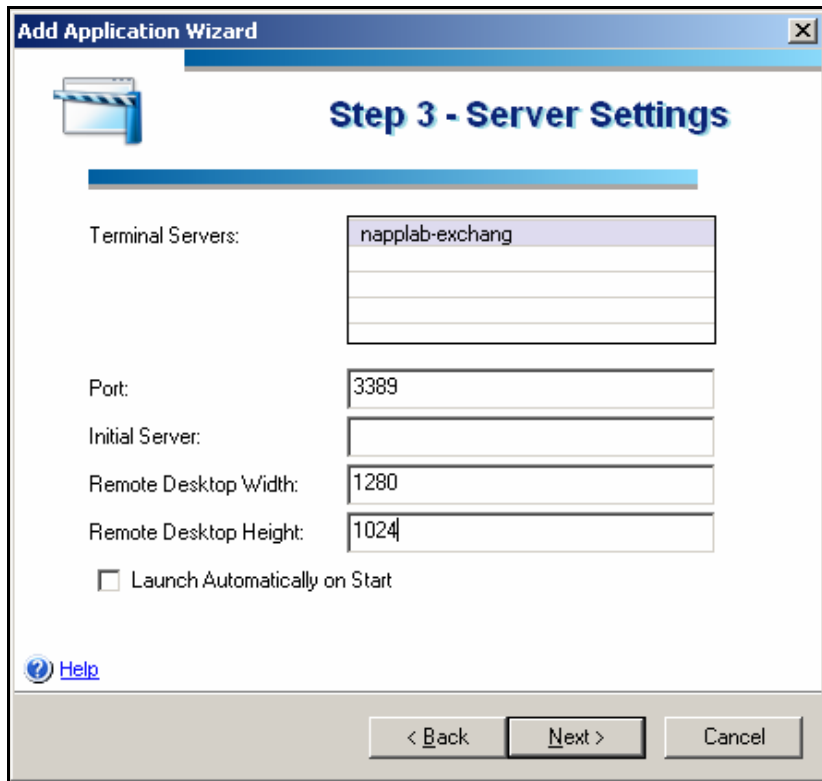


The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. The main heading inside is "Step 2 - Application Setup". Below the heading is a blue progress bar. The form contains the following fields and controls:

- Application Name:** A text box containing "Terminal Service - Exchange".
- Application Type:** A text box containing "Microsoft Windows XP / VISTA Terminal Services".
- Authorization:** A checkbox labeled "All Users Are Authorized" which is checked.
- Access Policy:** A dropdown menu showing "Always" with a lock icon on the left and a downward arrow on the right.
- Edit Policies...:** A button located below the Access Policy dropdown.
- Help:** A blue question mark icon followed by the text "Help" in the bottom left corner.
- Navigation Buttons:** Three buttons at the bottom right: "< Back", "Next >", and "Cancel".

Give the application a descriptive name. Include the server name.

## Step 3 – Server Settings



The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar is a blue header area with a folder icon and the text "Step 3 - Server Settings". The main area contains several input fields and a checkbox:

- Terminal Servers:** A list box containing "napplab-exchang" and two empty rows.
- Port:** A text box containing "3389".
- Initial Server:** An empty text box.
- Remote Desktop Width:** A text box containing "1280".
- Remote Desktop Height:** A text box containing "1024".
- Launch Automatically on Start:** An unchecked checkbox.

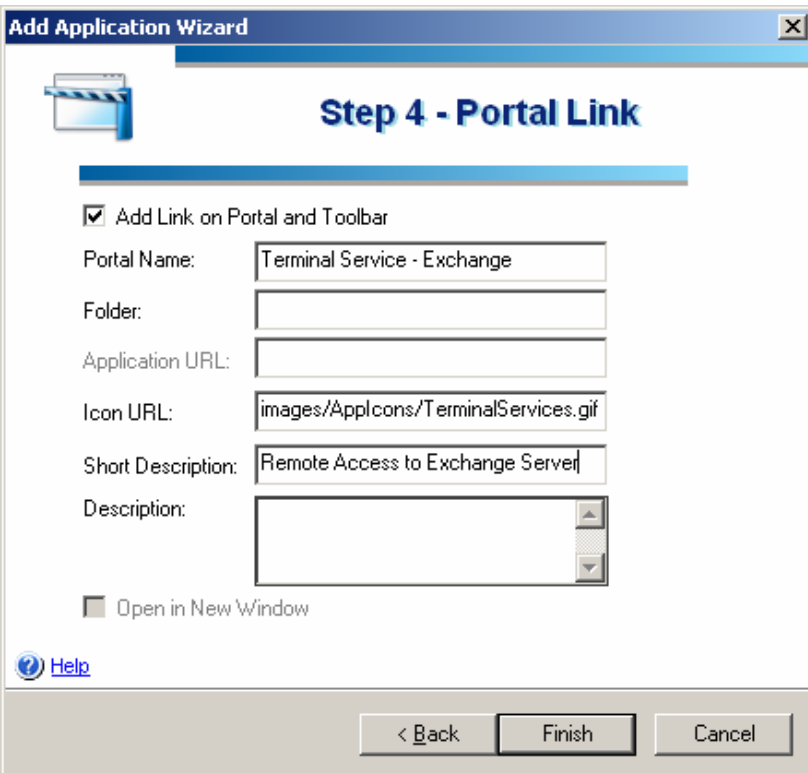
At the bottom left is a "Help" link with a question mark icon. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

Select the server which is serving as a Terminal Services server.

Be sure to select a reasonable screen Width and Height values. The defaults create a very small screen and will not allow the user to maximize the screen to full screen size.

Selecting the "Launch Automatically on Start" will launch this application as soon as the user logs into the IAG Portal.

## Step 4 – Portal Link



The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar is a blue header area with a folder icon and the text "Step 4 - Portal Link". The main content area has a light blue horizontal bar. Below this bar, there is a checked checkbox labeled "Add Link on Portal and Toolbar". Following this are several input fields: "Portal Name:" with the text "Terminal Service - Exchange", "Folder:" (empty), "Application URL:" (empty), "Icon URL:" with the text "images/AppIcons/TerminalServices.gif", "Short Description:" with the text "Remote Access to Exchange Server", and "Description:" (empty text area with scrollbars). At the bottom left of the main area is an unchecked checkbox labeled "Open in New Window". Below the main area is a "Help" link with a question mark icon. At the very bottom are three buttons: "< Back", "Finish", and "Cancel".

**Add Application Wizard**

**Step 4 - Portal Link**

☒ Add Link on Portal and Toolbar

Portal Name: Terminal Service - Exchange

Folder:

Application URL:

Icon URL: images/AppIcons/TerminalServices.gif

Short Description: Remote Access to Exchange Server

Description:

☐ Open in New Window

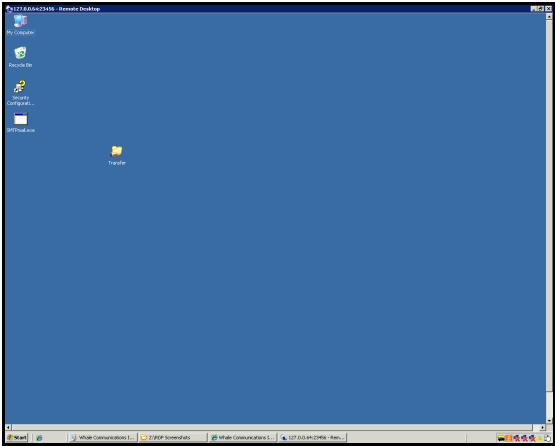
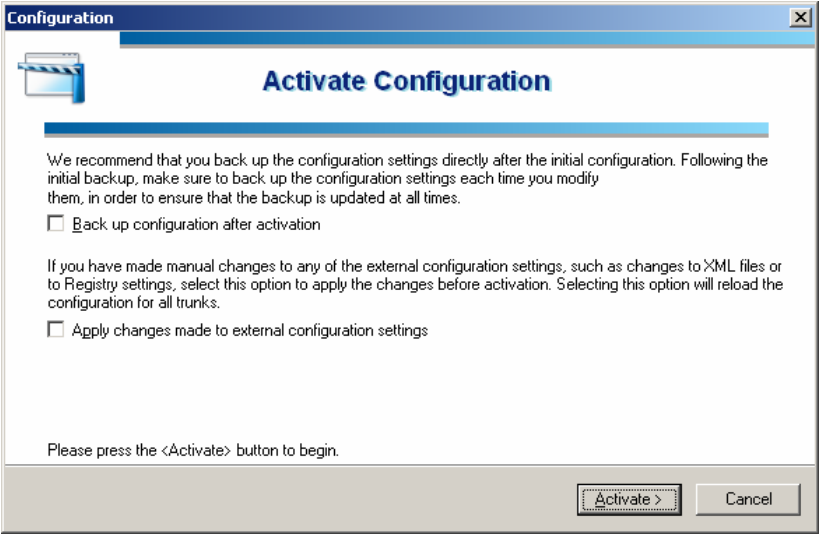
[Help](#)

< Back Finish Cancel

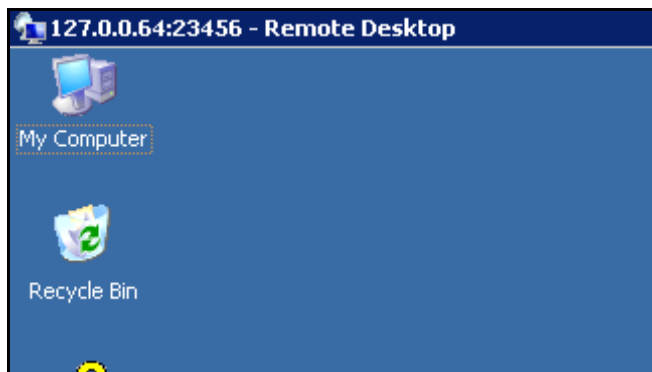
Describe the text for this application that explains to the user what service they are attaching to.



Remember to activate the IAG configuration.



Once the application is selected from the IAG portal, the normal Terminal Services application is launched. The user is not prompted to log in as IAG handles this automatically.



Notice the remote Terminal Server IP address is not exposed. The Terminal Service software client interacts with the local IAG ActiveX client which communicates with the IAG server using SSL, where the IAG server then communicates with the corporate Terminal Services server using TCP port 3389.



# **Chapter 8 – Publish Multi-Port Client/Server Application**

## **Publish IAG Multi-Port Client/Server Application**

This example will define a Multi-Port client/server application which is published on the IAG Portal. The IAG Portal is a web page which allows a single user login to grant access to multiple applications, each displayed and accessed from that web page.

The client/server application will talk with the server application using multiple IP ports. The application may talk over HTTP protocols, or over generic IP links.

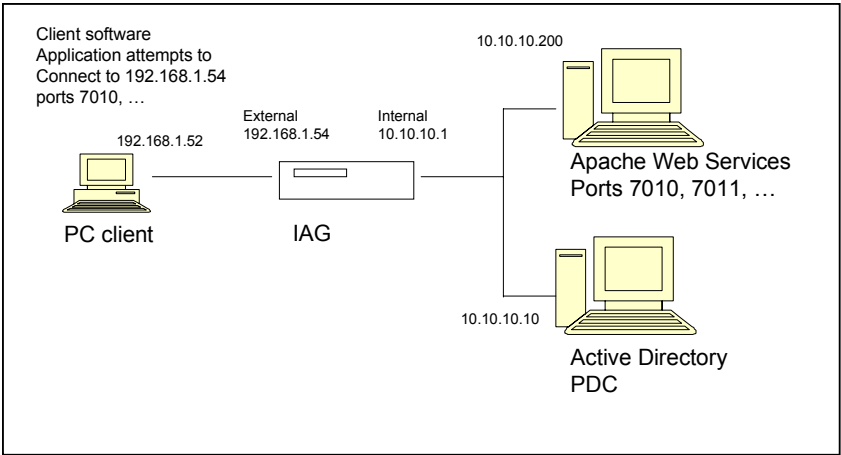
Examples of this kind of client/server environment includes SAP Fat Clients, Microsoft Outlook to Exchange via MAPI, various Web Services applications, etc.

This client/server application

Once configured, this published application defined by this example will

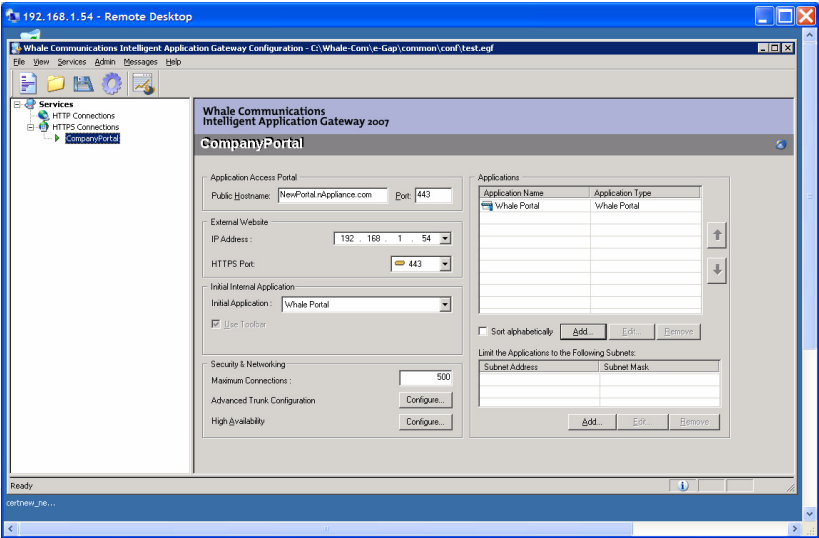
1. Allow the authenticated user to select this application from the portal page by a single click
2. Create a SSL VPN tunnel between the client application to the target server with no external routing nor VPN IP networks exposed outside of the IAG environment
3. Spawn the client application on the users desktop and link the application with the VPN tunnel

The lab environment used for this exercise will be defined as such:



# Step 1 – Access the IAG Portal page

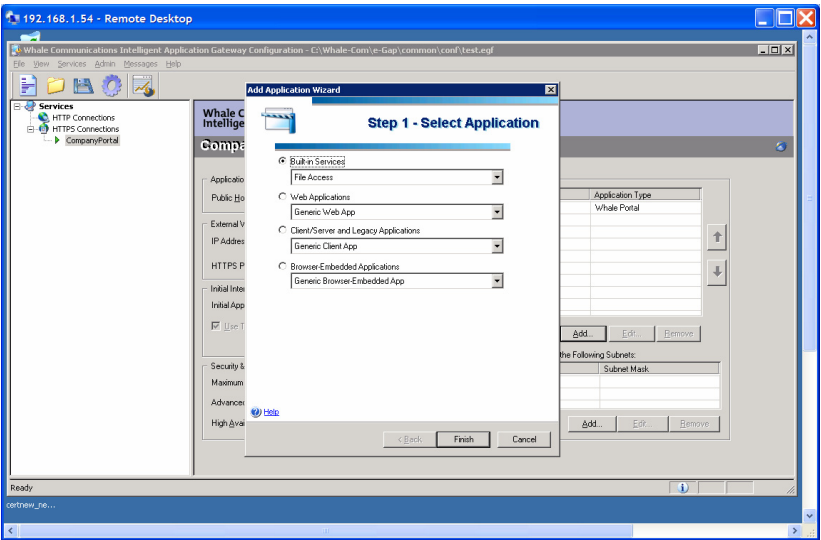
Click on the Portal link on the Services pane on the left side of the IAG Configuration application.



On the right side of the Portal form is the Application pane.

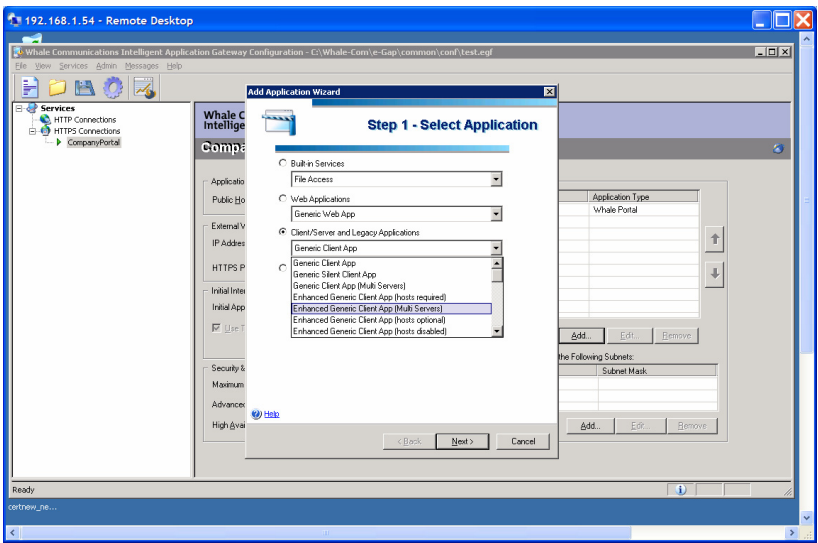
# Step 1 – Select Application

Click on the Add button.



Select the “Client/Server and Legacy Applications” pulldown option.

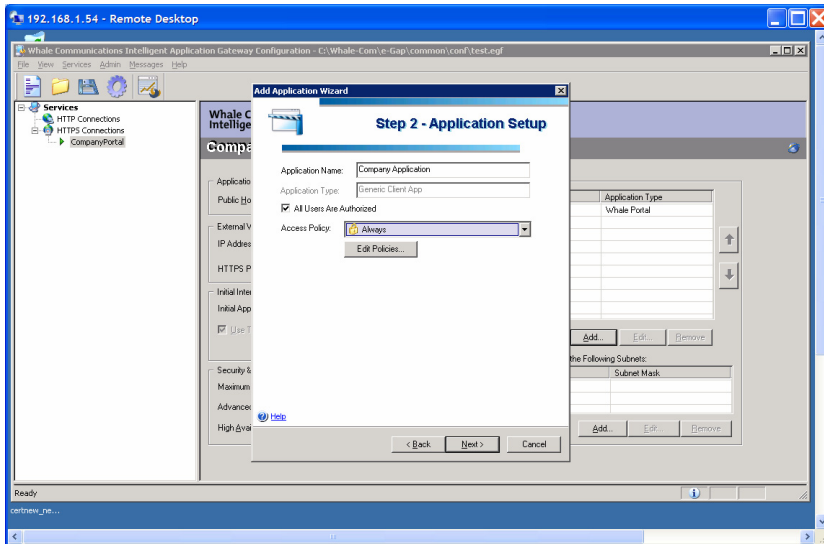
Then Select “Enhanced Generic Client App (Multi Servers)” option.



Once selected, then press Next.



## Step 2 – Application Setup

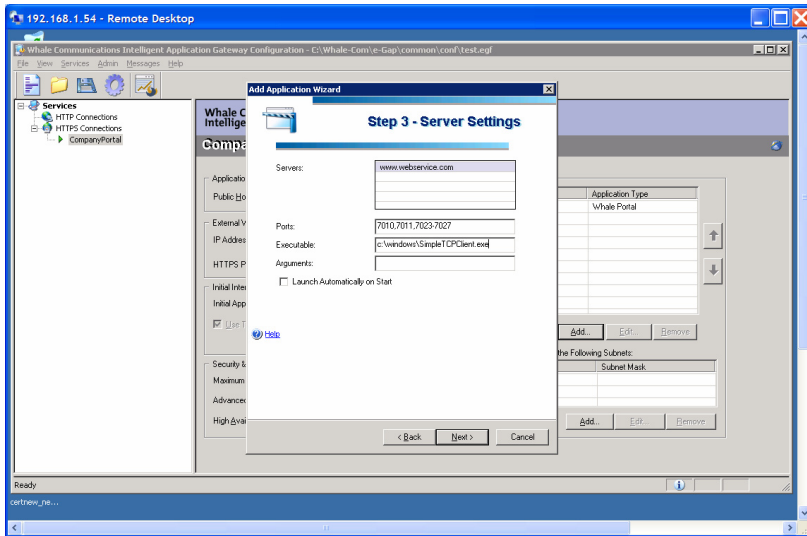


Define the application name, which is displayed to the user on the Portal Page.

Define the “Access Policy” as “Always”. This defines the Access Policy for the application to always allow access. This does not block user access regardless of the security condition of the client machine, and does not block access if the client environment does not conform to the corporate policies. This allows this environment to be defined in as simple a model as possible. This access can be further refined and constrained later.

Click on Next.

## Step 3 – Server Settings



Define the target server environment.

**Servers:** Define the Servers by double clicking on the Servers edit box. This will open up a data entry box within the Servers edit box form. Enter the server FQDN hostname. Make sure the DNS entry is defined inside the corporate network. The IAG System must be able to resolve this DNS name and have IP access to this server.

**\*Note:** Troubleshoot this configuration by insuring that the IAG system has unobstructed access to the target server. For HTTP and some other IP protocols, this can be tested using Telnet from a command prompt. (Running the command: "Telnet [www.webservice.com](http://www.webservice.com) 80" command from the IAG system attaches directly to a web service running on port 80. If this fails, then this

connection must be resolved. In this case, the port might be 7010, etc.).

**Ports:** Define the IP ports which will be opened by the client when communicating with the server. Multiple ports may be defined here. Each port must be comma delimited. A range of ports may be defined using the “-” character.

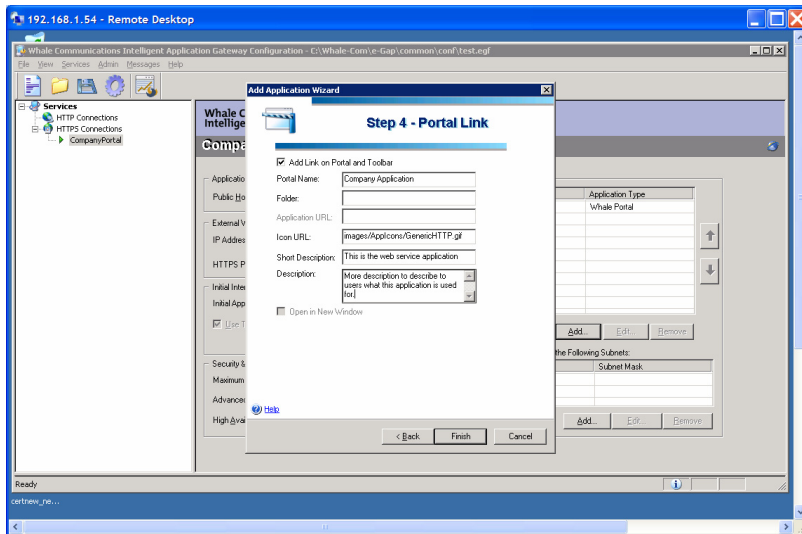
**Executable:** This may be the full path to the client application running on the client operating system. If the full path is not entered, the client application must be defined in the operating system command path.

The example used above is a utility application created by nAppliance for testing generic web services. The program will test connecting with multiple ports to multiple web servers, and display an IP connection trace. When there are connection problems within the network, these are displayed. This application is available to customers by request from nAppliance.

**Arguments:** Define any arguments required by the client application here.

Press the Next button.

## Step 3 – Portal Link



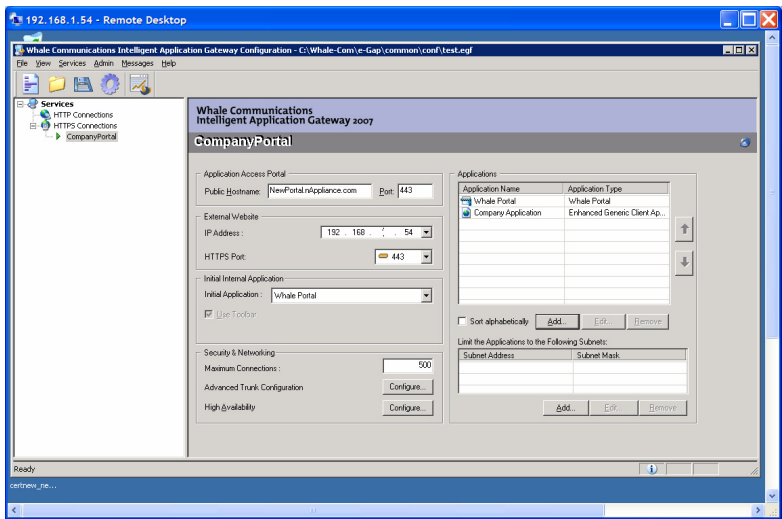
The Portal Link defines how this application looks to the user on the Portal Page.

The Folder allows the portal to group multiple applications inside a folder ICON on the portal page.

There are description fields and an ICON graphic to further customize the portal look.

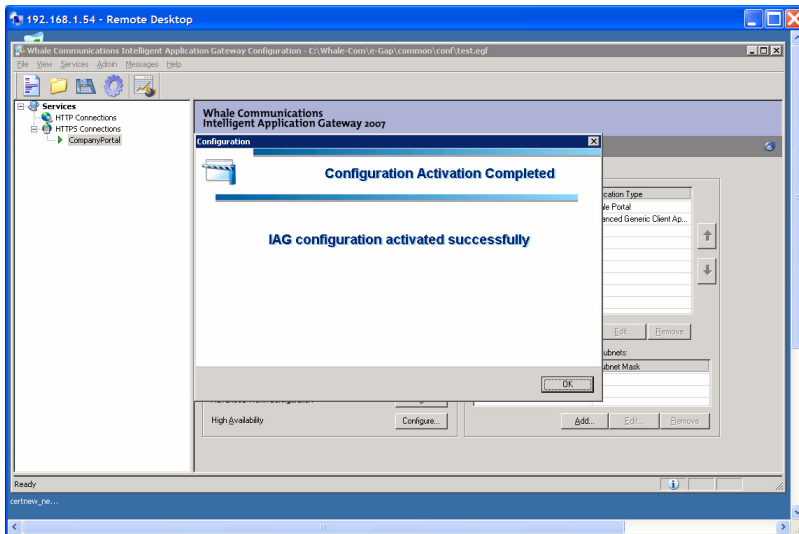
Fill in these fields as desired and press Next.

# Application Published



A simple version of this application is defined in the pane on the right. This application can be further configured with more advanced parameters. For now, lets test this application.

Activate the application by pressing the Sprocket ICON on the top left of the screen.

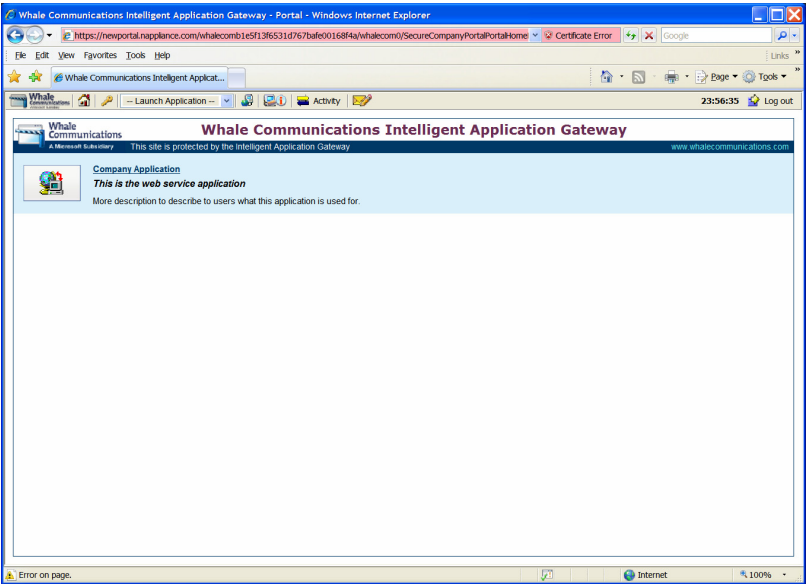


Once the application is activated, connect to the portal by pointing a browser to the URL:

<https://newportal.nappliance.com/>

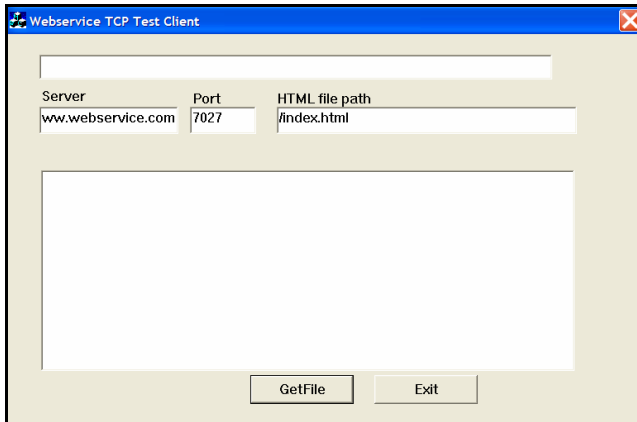
or the nodename you defined on the External interface of the IAG system.

# Test Application

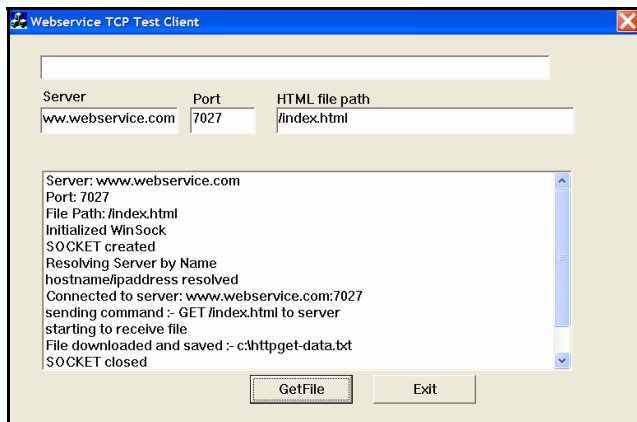


After you log into the portal with a valid username and password available on the Active Directory, you should see the portal page with a published application. The “Company Application” should be a more descriptive name which company users will recognize.

Click on the application link.

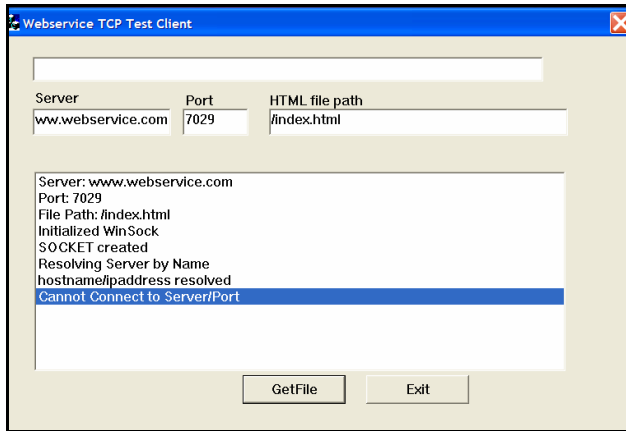


The application will be spawned, attached to a VPN tunnel which will tunnel traffic over ports 7010, 7011, and 7023 through 7027.



When using the application to test the server application, the client communicates with the server over the defined ports. When extending the range of ports on the server application, the client will still not communicate with the server over these ports until IAG is configured for the new ports.





After defining a web service on port 7029, the client will still not access the server until the IAG system is updated.

## **Chapter 9 – Publish Network Share as Local Drive**

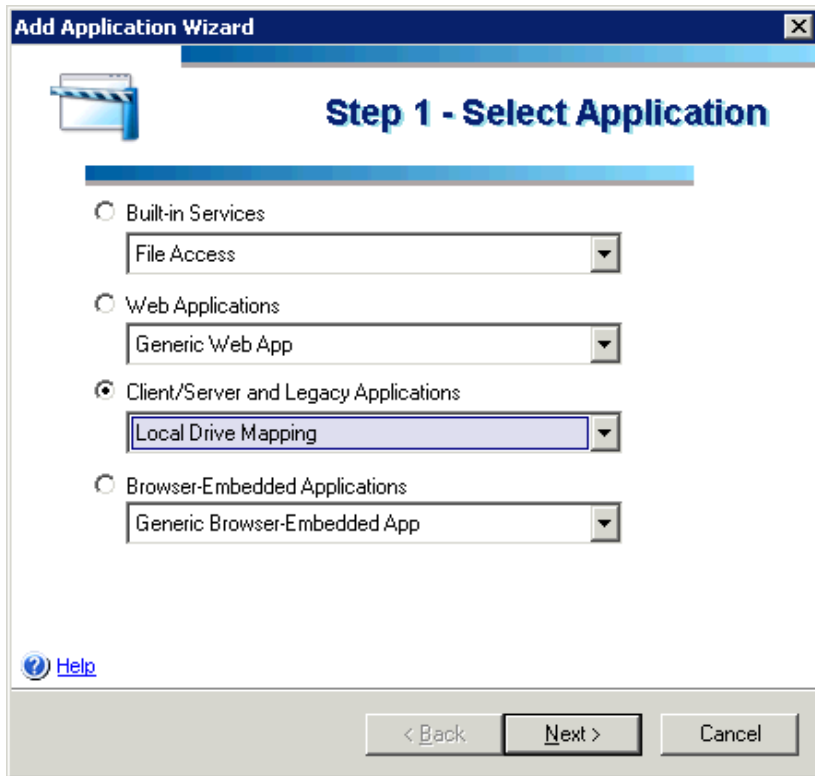
IAG can access a network share on an internal server, and publish this share as a remote drive on a users system. The network share could look like drive X: (for example) on an end users computer.

This requires IAG to download and install another ActiveX plugin module. Once this plugin is in place, all the configuration is done from the IAG system.

The internal share name and server attributes are not exposed to external users.

User access and control is managed by the network file privileges, and user access will be the same level of access as is granted by his domain group privileges. When the user logs into the IAG portal using his login credentials, his access is based on his domain privileges.

## Step 1 – Select Application



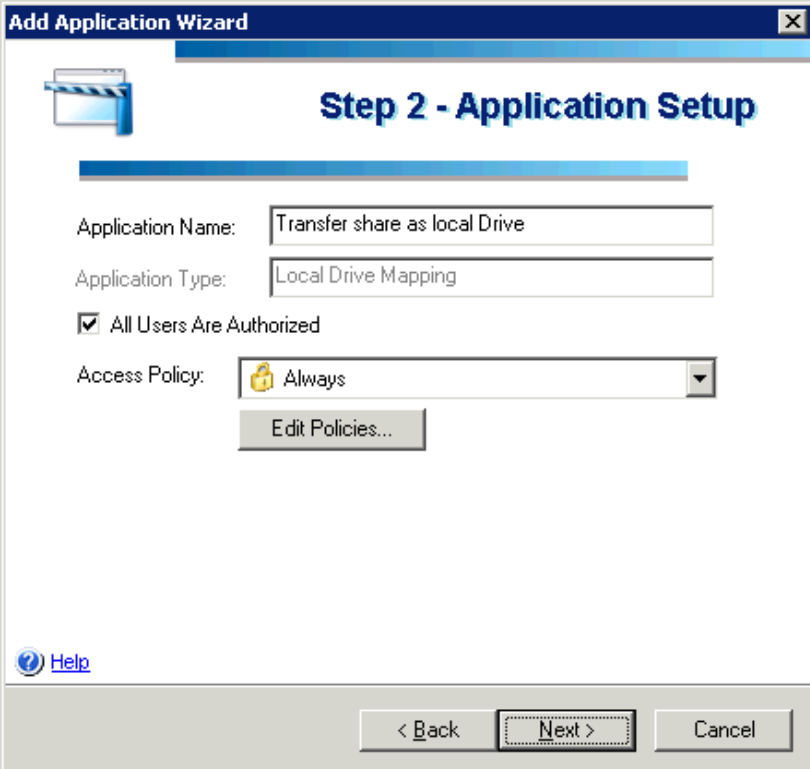
The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar is a blue header area with a folder icon and the text "Step 1 - Select Application". The main area contains four radio button options, each with a dropdown menu:

- ☐ Built-in Services  
File Access
- ☐ Web Applications  
Generic Web App
- ☒ Client/Server and Legacy Applications  
Local Drive Mapping
- ☐ Browser-Embedded Applications  
Generic Browser-Embedded App

At the bottom left is a "Help" link with a question mark icon. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

Select the “Local Drive Mapping” entry on the Client/Server and Legacy Applications application list.

## Step 2 – Application Setup

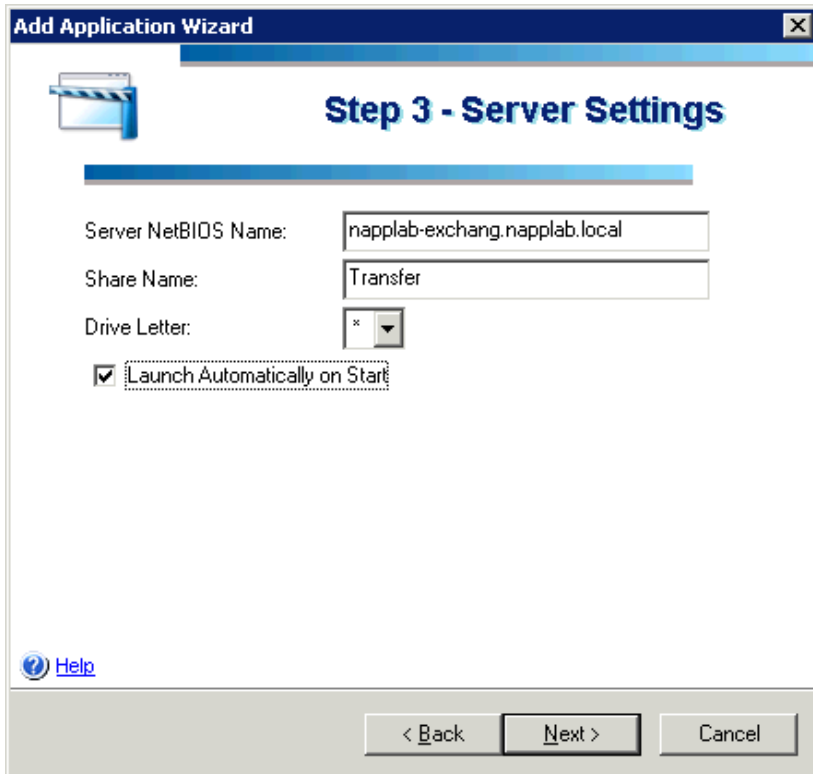


The screenshot shows a Windows-style dialog box titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar is a blue header area with a folder icon and the text "Step 2 - Application Setup". The main content area contains the following fields and controls:

- Application Name:** A text box containing "Transfer share as local Drive".
- Application Type:** A text box containing "Local Drive Mapping".
- Authorization:** A checked checkbox labeled "All Users Are Authorized".
- Access Policy:** A dropdown menu showing "Always" with a lock icon. Below it is a button labeled "Edit Policies...".
- Help:** A blue question mark icon followed by the text "Help".
- Navigation:** At the bottom are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

Select an Application Name. This should include a name for the share resource which is easily identifiable to the end user.

## Step 3 – Server Settings



**Add Application Wizard**

**Step 3 - Server Settings**

Server NetBIOS Name:

Share Name:

Drive Letter:

☒ Launch Automatically on Start

[Help](#)

< Back   Next >   Cancel

Select the server name, the share name and the drive letter to map on the end users machine. Selecting “\*” will select the next available drive on the user’s machine.

When selecting “Launch Automatically on Start”, this drive will be attached to the network share when the user logs into the IAG Portal.

## Step 4 – Portal Link

**Add Application Wizard**

**Step 4 - Portal Link**

☐ Add Link on Portal and Toolbar

Portal Name:

Folder:

Application URL:

Icon URL:

Short Description:

Description:

☐ Open in New Window

[Help](#)

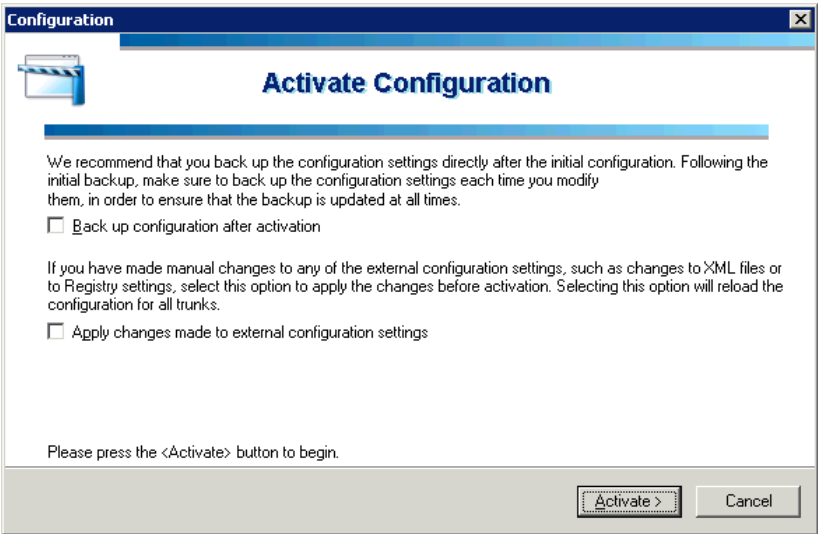
< Back   Finish   Cancel

This screen defines the what the user sees on the Portal screen.

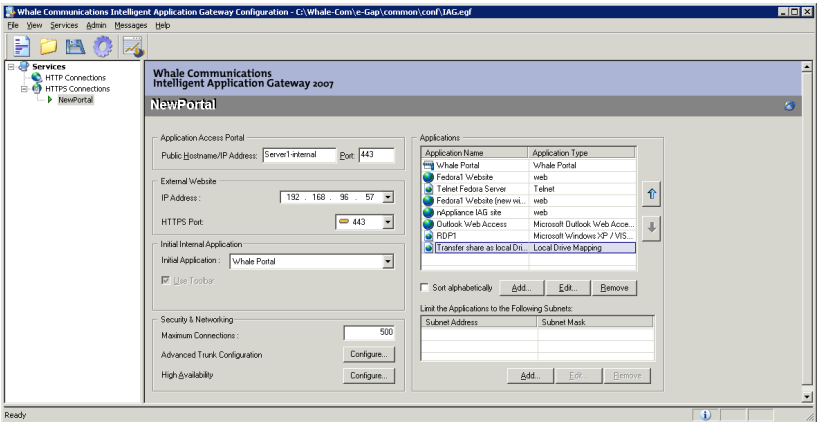
If the “Add Link on Portal and Toolbar” is select, then the user can connect to the network share manually from the portal screen. If this is not selected, then the the “Launch Automatically on Start” should be selected on the prior screen.

If the user has the option to connect manually, then the user could connect multiple times to the same share, each time connecting to a new drive letter.

Remember to activate the configuration.

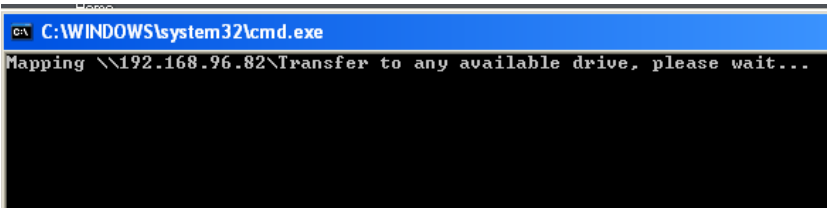
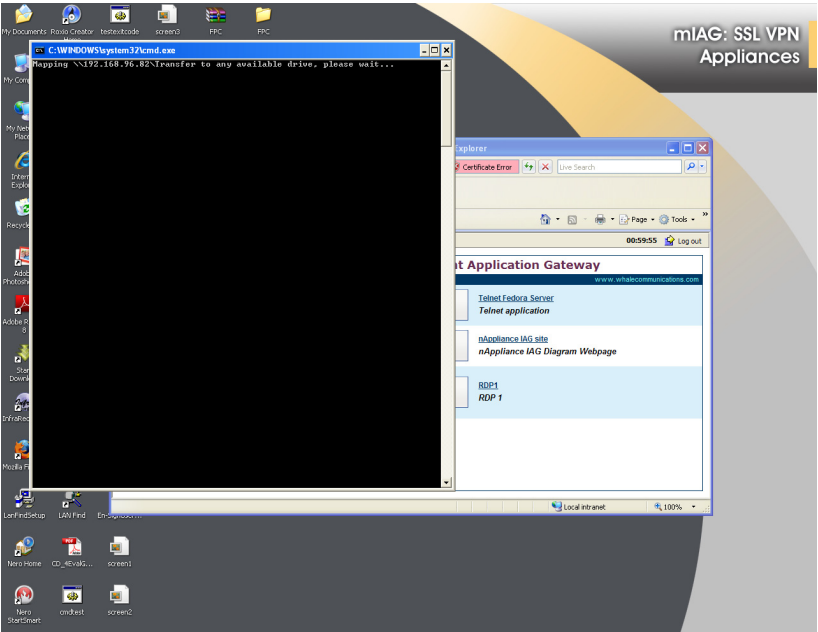


And the drive application is complete



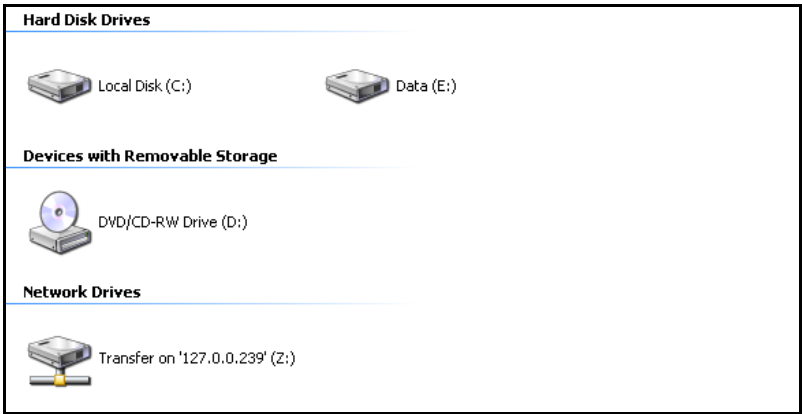
# Test Drive Connection

Once the user logs into the Portal, the drive will be connected automatically.

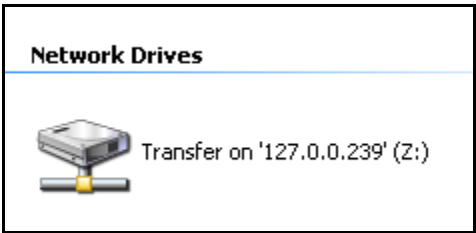




# Drive Mapped



Notice the drive is mapped to a local IP address on the user system. The internal corporate network is not exposed.



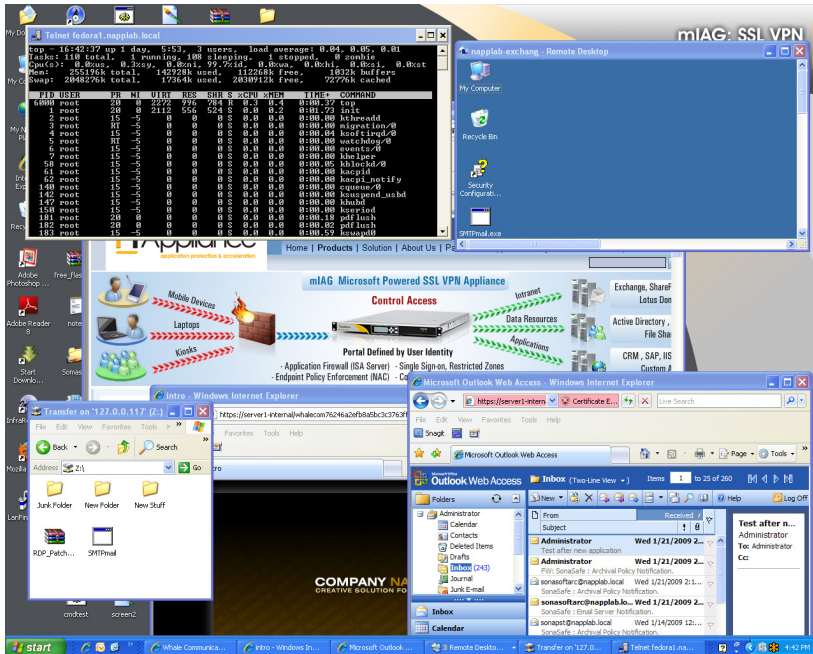
IAG's client application interacts directly with the user computer, and communicates via an internal SSL connection to the IAG system.

When troubleshooting this configuration, be sure the IAG system can communicate to the network share server via the SMB protocols. Any security blocks between the IAG

system and the network share server will cause this configuration to fail.

The administrator should be able to map a share directly from the IAG system. This connection can be simulated from the console of the IAG system

# Chapter 10 – Summary



The above screenshot shows five published applications running on a single desktop: Telnet connected to a remote Linux system, Terminal Services, a remote network share mounted locally, Outlook Web Access running as a separate application, and a website embedded with the IAG portal application.

IAG provides a platform for distributing application and network resources securely to remote users. Remote users can have the same rich environment securely without sacrificing performance or usability.

# Appendix 1 – Hardware Port Configurations

## Index

### A

Access Policy, 57, 79  
Active Directory, **21**, 15, 16, 17,  
19, 34, 41, 43, 54, 60, 85  
ActiveX, **21**, 2, 28, 30, 31, 32, 72,  
88  
Application authentication, 27  
Application Server, **21**, 21  
Application Wiping, 36  
Attachment wiper, 3  
Authentication, **21**, **22**, 15, 19,  
35, 41, 42, 43, 60

### B

Basic Trunk, 13

### C

certificate, 32, 47

### D

DNS, **21**, 4, 7, 40, 58, 80

### E

endpoint policies, 23  
Endpoint policy, 35  
External Website, 13

### F

FQDN, 40, 58, 80

### H

HTTP, 4, 12, 35, 41, 74, 80  
HTTP trunk, 12  
HTTPS, 35, 38, 41

### I

IAG Portal toolbar, 65  
ISA, 4

### J

Java client, 2

### L

Launch Automatically on Start,  
69, 91, 92  
LDAP, 17, 43  
Linux, 2, 97  
login screen, 28, 34

### M

MAPI, 74

### N

network share, 3, 88, 91, 92, 95, 97  
New Trunk wizard, 12

## O

Outlook, 2, 56, 61, 62, 65, 74, 97  
Outlook Web Access, 65

## P

password., 10, 45, 54  
Public Hostname, 13, 21, 40

## S

SAP, 2, 74  
Session timeout, 27  
single sign-on, 22  
Single Sign-on, 3  
SMB, 95  
SSL, 2, 3, 27, 35, 72, 74, 95  
SSL VPN, 2

## T

TCP port 3389, 72  
telnet, 2, 17  
Telnet, 80, 97  
Terminal Services, 22, 66, 67, 69,  
72, 97  
trunk, 2  
Trunk Name, 13, 40  
tunnel traffic, 86

## V

virus scanners, 23

## W

Web Console, 5, 9  
Whale Communications, 9, 11, 38

## X

XML configurations, 27

}