

# **Intelligent Application Gateway**

## **User Guide**

December 2006

Version 3.7

© 2006 Whale Communications, a Microsoft subsidiary. All rights reserved.

This manual and the information contained herein are confidential and proprietary to Whale Communications, a Microsoft subsidiary, its affiliates and subsidiaries (hereinafter, the “Company”). All intellectual property rights (including, without limitation, copyrights, trade secrets, trademarks, etc.) evidenced by or embodied in and/or attached/connected/related to this manual, information contained herein and the Product, is and shall be owned solely by the Company. The Company does not convey to you an interest in or to this manual, information contained herein and the Product, but only a limited right of use. Any unauthorized use, disclosure or reproduction is a violation of the licenses and/or the Company’s proprietary rights and will be prosecuted to the full extent of the Law.

## TRADEMARKS

---

Application Aware, and Attachment Wiper are service marks, trademarks or registered trademarks of Whale Communications or its subsidiaries in the United States and other countries, or both.

---

Netscape, and Netscape Navigator are service marks, trademarks or registered trademarks of America Online, Inc. or its subsidiaries in the United States and other countries, or both.

---

Carbon, Macintosh, Mac OS, and Safari are service marks, trademarks or registered trademarks of Apple Computer, Inc. or its subsidiaries in the United States and other countries, or both.

---

Citrix , Citrix NFuse, Citrix Presentation Server, Citrix MetaFrame, Citrix SecureGateway, and ICA, are service marks, trademarks or registered trademarks of Citrix Systems, Inc. or its subsidiaries in the United States and other countries, or both.

---

Debian is a service mark, trademark or registered trademark of Software in the Public Interest, Inc. or its subsidiaries in the United States and other countries, or both.

---

GNU, and GZip are service marks, trademarks or registered trademarks of Free Software Foundation, Inc. or its subsidiaries in the United States and other countries, or both.

---

Domino, Lotus, IBM Lotus, iNotes, Lotus iNotes, Lotus Domino, Notes, Sametime, and WebSphere are service marks, trademarks or registered trademarks of IBM Corporation or its subsidiaries in the United States and other countries, or both.

---

Linux is a service mark, trademark or registered trademark of Linus Torvalds or its subsidiaries in the United States and other countries, or both.

---

Active Directory, ActiveSync, ActiveX, Excel, Microsoft, Outlook, SharePoint, Visual Basic, Windows Mobile, Windows NT, Windows Server are service marks, trademarks or registered trademarks of Microsoft Corporation or its subsidiaries in the United States and other countries, or both.

---

Camino, Firefox and Mozilla are service marks, trademarks or registered trademarks of Mozilla Foundation or its subsidiaries in the United States and other countries, or both.

---

Novell, Novell Directory Services, Novell NetWare, and SUSE are service marks, trademarks or registered trademarks of Novell, Inc. or its subsidiaries in the United States and other countries, or both.

---

PGP is a service mark, trademark or registered trademark of PGP Corporation or its subsidiaries in the United States and other countries, or both.

---

Red Hat is a service mark, trademark or registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries, or both.

---

Resonate is a registered trademark of Resonate, Inc. The Resonate logo and Resonate Central Dispatch are trademarks of Resonate, Inc. Resonate Central Dispatch contains technology protected under U.S. Patent 5,774,660.

---

ACE SecurID, RC4, and RSA SecurID, are service marks, trademarks or registered trademarks of RSA Security Inc. or its subsidiaries in the United States and other countries, or both.

---

---

SAP is a service mark, trademark or registered trademark of SAP AG or its subsidiaries in the United States and other countries, or both.

---

Java, JavaScript, JRE, and Sun are service marks, trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the United States and other countries, or both. Enhanced HAT owned by Sun Microsystems, Inc.

---

Norton and Symantec are service marks, trademarks or registered trademarks of Symantec Corporation or its subsidiaries in the United States and other countries, or both.

---

Apache is a service mark, trademark or registered trademark of The Apache Software Foundation or its subsidiaries in the United States and other countries, or both.

---

Terminal Services is a service mark, trademark or registered trademark of The Regents of the University of California or its subsidiaries in the United States and other countries, or both.

---

Unix is a service mark, trademark or registered trademark of The Open Group or its subsidiaries in the United States and other countries, or both.

---

XCompress is a service mark, trademark or registered trademark of XCache Technologies, Inc. or its subsidiaries in the United States and other countries, or both.

---

All other trademarks, copyrights, product and or service marks mentioned in this manual, whether claimed or registered, are the exclusive property of their respective owners.

## **DISCLAIMER**

The Company has reviewed this manual thoroughly. All statements, technical information, and recommendations in this manual and in any guides or related documents are believed reliable, but the accuracy and completeness thereof are not guaranteed or warranted, and they are not intended to be, nor should they be understood to be, representations or warranties concerning the products described. Further, the Company reserves the right to make changes to the information described in this manual at any time without notice and without obligation to notify any person of such changes.

## **LIMITATION OF LIABILITY**

Neither the Company nor any of its worldwide subsidiaries or distributors or management or employees grants any warranties in respect to any damages or deficiencies resulting from accident, alteration, modification, foreign attachments, misuse, tampering, negligence, improper maintenance, abuse or failure to implement any updates furnished. The Products must be used and maintained in strict compliance with the instructions and safety precautions of the Company contained herein in all supplements thereto or in any other written documents of the Company. The products must not be altered without prior written consent of the Company.

The Company grants no warranties with respect to the Products, either express or implied, including any implied warranties of merchantability or fitness for a particular purpose. The Company will have no liability for any damages whatsoever arising out of or in connection with the delivery, installation, use or performance of the product. In no event shall the Company be liable under any legal theory (including but not limited to contract, negligence, misrepresentation, strict liability in tort or warranty of any kind) for any indirect, special, incidental or consequential damages (including but not limited to loss of profits), even if the Company has notice of the possibility of damages.

Without limiting the effect of the preceding clauses, the Company's maximum liability, if any, for damages (including but not limited to liability arising out of contract, negligence, misrepresentation, strict liability in tort or warranty of any kind) shall not exceed the consideration paid to the Company for the product. The Company shall under no circumstances be liable for damages arising out of any claim (including but not limited to a claim for personal injury or property damage) made by any third person or party.

Document Name	Intelligent Application Gateway User Guide
Document Revision	3.7
Date	December 2006
Software Version No.	3.7

# Contents

## **Chapter 1: Introduction..... 15**

Overview .....	15
Control Access .....	15
Protect Assets .....	16
Safeguard Information .....	16
Intelligent Application Gateway Architecture .....	16
Broad Set of Connectivity Options .....	17
Integrated Application Firewall .....	18
Application Aware™ .....	18
Supported Applications .....	18
Trunks: the IAG Transfer Channels .....	19
Supported Browsers .....	19
Security Management Tools .....	20
Monitoring and Control Tools and Interfaces .....	21
Encryption .....	21
Encryption Passphrase .....	22
High Availability Array .....	23
About This Guide .....	23
Conventions Used in This Guide .....	25

## **Chapter 2: SSL VPN Portals ..... 27**

Creating an SSL VPN Portal .....	28
Users Setup .....	32
Defining Authorization Repositories .....	33
User/Group Servers.....	33
Local Groups.....	35

Defining Authorization for Portal Applications .....	38
Selecting Users and Groups .....	43
Optional Configuration .....	46
Configuring Global Host Address Translation .....	46
Configuring Application Subnets .....	48
Changing the Application Access Portal Port Number .....	49
Where To Go From Here .....	49
<b>Chapter 3: Single Application Sites.....</b>	<b>51</b>
Optional Pre-configuration of the Services .....	52
Creating a Webmail or a Basic Trunk .....	54
Where To Go From Here .....	57
Creating a Redirect Trunk .....	58
Editing Trunks .....	59
Editing in the Configuration Pane .....	59
Editing in the General Tab .....	61
Editing Webmail Trunk Server Settings .....	64
Domino iNotes (Single Server) .....	65
Domino iNotes (Multiple Servers) .....	66
<b>Chapter 4: Application Settings.....</b>	<b>67</b>
Editing Application Properties .....	67
Accessing the Application Properties Dialog Box .....	68
General Tab .....	68
Web Servers Tab .....	71
Web Settings Tab .....	73
Application Authentication .....	74
General Web Settings .....	75
User Authorization Data .....	77
Web Server Security Tab .....	78

Cookie Encryption Tab .....	80
Global Exclude List .....	82
Download/Upload Tab .....	82
Server Settings Tab .....	85
Client Settings Tab .....	86
Portal Link Tab .....	87
Authorization Tab .....	91
Duplicating an Application .....	91
<b>Chapter 5: Endpoint Security .....</b>	<b>93</b>
Endpoint Policies .....	93
Endpoint Detection .....	95
Session Endpoint Policies .....	95
What Information is Collected from the End User's Computer? .....	97
Application Endpoint Policies .....	99
Defining Application Endpoint Policies .....	99
Editing Application Policies .....	100
Default Policies .....	101
Basic Policy Configuration .....	103
Advanced Policy Configuration .....	104
Advanced Configuration Overview .....	105
Configuration in the Advanced Policy Editor.....	106
Variable Formats .....	107
Endpoint Settings .....	108
Attachment Wiper .....	110
Configuring the Attachment Wiper .....	112
Cleanup of Items That Are Saved Outside the Cache .....	113
Configuring a Scheduled Cleanup .....	115
Enabling the Attachment Wiper on a Custom Logoff Message Page .....	116
When Encrypted Pages Are Saved to a Location Other Than "Temp Files" .....	117

Certified Endpoints .....	118
Certified Endpoint Configuration Overview .....	118
Enabling Certified Endpoint Using Microsoft CA Locally .....	119
Enabling Certified Endpoints Using a Remote CA .....	122
Certified Endpoint Configuration Steps .....	123
Installing a Microsoft Certificate Authority (Local CA Only) .....	124
Defining a Certification Authority Policy (Local CA Only) .....	128
Editing the Default Configuration (Local CA Only) .....	131
Preparing Endpoint Computers that Use Internet Explorer (Local CA Only) .....	134
Adding Certified Endpoint Enrollment to the Trunk (Local CA Only) .....	135
Adding the CA to the Certificate Trust List (All CAs) .....	136
Backing Up the Certificate Settings (All CAs) .....	140
End-User Interaction (Local CA Only) .....	140
Requesting Certified Endpoint Status .....	142
Checking the Certified Endpoint Request Status .....	144
Installing the Certificate and Logging In as a Certified Endpoint User .....	144
Viewing and Processing Certificate Requests (Local CA Only) .....	146
Whale Client Components .....	147
Installing and Running the Components on Endpoint Computers .....	150
Prerequisites for Installing the Whale Client Components .....	151
Online Whale Client Components Installation .....	152
Whale Client Components Installer .....	154
Offline Whale Client Components Installation .....	157
Prerequisites for Running the Whale Client Components .....	159
IAG Trusted Sites .....	160
Remote Configuration of Users' Trusted Sites Lists .....	162
Restoring the Whale Client Components Defaults .....	165
Uninstalling the Whale Client Components .....	167



## **Chapter 6: SSL Wrapper..... 171**

Technology Overview .....	172
Socket Forwarding Activation Modes.....	174
Enabling Access to SSL Wrapper Applications .....	175
SSL Wrapper Java Applet Prerequisites .....	176
Uninstalling the SSL Wrapper Java Applet .....	178
Socket Forwarding Component Installation .....	178
LSP Conflict Detection .....	179
Supported Applications .....	181
Generic Applications .....	182
Configuration Overview .....	183
Remote User Interaction with the SSL Wrapper .....	183
Portal Activity Window .....	184
Connections Area.....	186
Applications Area .....	187
Portal Activity Window Buttons .....	188

## **Chapter 7: Network Connector ..... 189**

Network Connector Technology Highlights .....	189
Configuring the Network Connector .....	190
Configuring the Network Connector Server .....	190
Network Segment Tab.....	192
IP Provisioning Tab.....	193
Access Control Tab .....	196
Additional Networks Tab.....	197
Advanced Tab .....	199
Remote User Interaction with the Network Connector .....	200
Interaction on Computers Running the SSL Wrapper ActiveX Component .....	201
Interaction on Computers Running the SSL Wrapper Java Applet .....	202

Network Connector Troubleshooting .....	203
Troubleshooting the Network Connector Server .....	203
Server Logs.....	204
Server Resources.....	205
Network Traffic Logs .....	205
Troubleshooting the Network Connector Client .....	206

## **Chapter 8: Providing Access to Internal File Systems ..... 209**

Local Drive Mapping .....	209
Mapping Shares .....	210
Windows 2003/XP Support .....	210
File Access .....	211
How File Access Works .....	212
Enabling Remote Access to the File Access Application .....	212
Windows Domain Settings .....	212
Novell NetWare Settings .....	220
Configuring File Access in the Configuration Program: Overview .....	220
File Access Administration Settings .....	221
Accessing the File Access Window .....	222
Configuring Home Directory, Mapped Drives, and Share Permissions.....	223
Novell Logon Settings.....	227
Configuring Access to Domains, Servers, and Shares.....	229
Configuring Authentication with the Novell Directory Service .....	231
Changing the Date Format of Files and Folders .....	234
Hiding the Folder Tree in the End-User Interface .....	234

## **Chapter 9: Monitoring and Control ..... 237**

Event Logging .....	237
Overview .....	238
Event Categories .....	238
Event Logging Reporters .....	238
Event Logging Messages.....	239

Optional Event Logging Configuration Steps .....	239
Configuring General Settings .....	240
Configuring the Built-In Reporter .....	242
Configuring the RADIUS Reporter .....	243
Configuring the Syslog Reporter .....	244
Configuring the Mail Reporter .....	245
Enabling the Mail Reporter to Send Messages.....	246
Configuring which Messages are Sent by the Mail Reporter.....	247
Message Configuration .....	249
Configuring Event Messages in the Message Definitions File.....	249
Event Logging Message Definitions File.....	250
Event Messages Application Interface.....	257
Disabling Event Logging and Reporting .....	258
Web Monitor .....	258
Accessing the Web Monitor .....	260
Enabling Web Monitor Access from Computers Other Than the IAG .....	261
Web Monitor Browser Support.....	264
Web Monitor Layout .....	264
Tips for Using the Web Monitor .....	265
Session Monitor - Current Status .....	266
Session Monitor Over Time.....	267
Session Monitor - Active Sessions .....	268
Session Details.....	270
Session Monitor - Statistics .....	271
Session Monitor - Statistics Window: Query Form .....	272
Session Monitor - Statistics Window: Query Results.....	273
Application Monitor - Current Status .....	275
Application Monitor Over Time .....	277
Application Monitor - Active Sessions .....	278

Application Monitor - Statistics .....	279
Application Monitor - Statistics Window: Query Form .....	279
Application Monitor - Statistics Window: Query Results View .....	281
Application Access Details .....	283
User Monitor - Current Status .....	285
User Monitor Over Time .....	286
User Monitor - Active Sessions .....	287
User Monitor - Statistics .....	288
User Monitor - Statistics Window: Query Form .....	289
User Monitor - Statistics Window: Query Results View.....	290
User's Application Access Statistics .....	291
Event Viewer .....	293
Event Query .....	295
Event Report .....	297
Web Monitor High Availability Support .....	298
Accessing IAG Servers in the Array .....	299
Analyzing History Reports Once an IAG Server is Removed from the Array .....	300
SSL Event Monitoring .....	301
<b>Chapter 10: Troubleshooting.....</b>	<b>303</b>
Backup & Restore Utility .....	303
Backing up the Configuration .....	304
Backing up the Configuration in the Configuration Program .....	304
Running the Backup Utility as a Console Application.....	305
Restoring the Configuration .....	305
Restoring the Configuration in the Configuration Program .....	306
Running the Restore Utility as a Console Application .....	306
Error Logging and Process Tracing .....	307
Error Server and Trace Configuration File .....	307
Individual Trace Sections .....	308
General Trace Configuration Section .....	310
Trace Activation .....	311

Error Server Trace and Log Files .....	311
File Location and Naming.....	311
Size and Quantity of Files .....	312
Log File Cleanup .....	313
Log File Cleanup Parameters .....	314
How the Log File Cleanup Process Works .....	314
Configuring Log File Cleanup Parameters .....	317
Excluding IIS Log Files from the Log File Cleanup Process .....	318
Support Utilities .....	319
Running Support Utilities Tests .....	320
Running the Data Collection Utility .....	321
Restarting the Web Service in the IIS .....	321
<b>Appendix A: Troubleshooting Event Logging Messages .....</b>	<b>325</b>



# Chapter I

## Introduction

### Overview

The Whale Communications Intelligent Application Gateway (IAG) is a Secure Socket Layer Virtual Private Network (SSL VPN) that provides employees and partners with policy-based secure access to applications and data from any PC or device and any location.

The IAG secure access solution enables remote access from diverse endpoints through a single point of entry to almost any business application and file share, while enforcing user authentication and authorization over a policy-defined application-layer connection. Endpoint security management enables granular access control and deep content inspection and application protection.

Running over Microsoft® Internet Security and Acceleration (ISA) Server 2006, the IAG enables users to access line-of-business, intranet, and client/server resources from a broad range of devices and locations, while providing infrastructure protection and information safeguards for corporate applications and data.

### Control Access

Secure, web-based access to business critical applications and data:

- Differentiated and policy-driven access to network, server, and data resources.
- Flexible application-intelligent SSL VPN from any device or location.
- Highly granular access and security policy enforced at the session, application, and functionality levels.
- Comprehensive basic and form-based authentication through Active Directory®, RADIUS, LDAP, and SecurID®.
- Customizable, identity-based web portal with single-sign-on (SSO).
- Handles embedded browser applications.
- Connectivity and control for client/server and legacy applications.

## Protect Assets

Integrated application protection helps ensure the integrity and safety of network and application infrastructure by blocking malicious traffic and attacks:

- Application-layer firewall blocks non-conformant requests, such as buffer overflow or SQL injection, on application protocols.
- Comprehensive protocol validation and deep content inspection with both positive and negative logic rulesets.
- URL cloaking and full functionality for remote users through dynamic URL rewrite and HTTP parameter filtering.
- Application Optimizers provide out-of-the-box protection for high-value applications such as SharePoint® Server, Microsoft® Outlook® Web Access, SAP®, and WebSphere®.
- Comprehensive monitoring and reporting; integrates with third-party risk and policy management platforms.
- Extensible infrastructure and tools for custom application publishing and scripting.

## Safeguard Information

Comprehensive policy enforcement helps drive compliance with legal and business guidelines that require information usage criteria to limit exposure and liability when accessing sensitive corporate data:

- Ensures network integrity by restricting client access based on endpoint security profile.
- Strong endpoint security management and verification helps ensure endpoint health compliance and session control.
- Enforces policy controls over actions within an application.
- Cache-cleanup tailored to specific applications removes downloaded files and pages, URLs, custom caches, cookies, history, and user credentials.
- Detects endpoint security state.

## Intelligent Application Gateway Architecture

The IAG consists of four elements:

- SSL VPN platform
- Endpoint security
- Application security
- Unified policy management framework



The IAG integrated approach rests on an architecture that functions across the client, proxy, and appliance tiers, and is managed through a single policy engine. The gateway functions at the application layer, terminating both inbound and outbound communications and parsing traffic through full inspection at the application layer.

The ability to understand traffic flows within the context of specific applications is the foundation for the IAG application-specific optimizers, and underpins the gateway's ability to enforce endpoint policy at the browser. This application intelligence allows the gateway to extend access to enterprise applications to unmanaged endpoints without creating risks to network integrity; it avoids having to resort to tunneling at the network layer and jeopardizing back-end resources. In addition, the gateway's underlying application intelligence provides the ability for administrators to create granular access control policies, to cordon off even parts of an application or network files, based on user profile.

The gateway incorporates a native host-checker engine that can be customized to detect third-party anti-virus software or personal firewalls, and supports integration with third-party inspection tools. This engine can also extend far further into the client-side and detect virtually any metric or watermark used by an organization to tag an asset.

## Broad Set of Connectivity Options

In order to support a wide variety of applications, the gateway supports the following connectivity options:

- Web proxy, for the support of web applications. The gateway's content translation engine removes the need for a client component, enabling pure browser access.
- The SSL Wrapper and the inherent Socket Forwarding component enable access to non-web applications, such as Native Outlook, Citrix®, and Telnet, based on specific application knowledge. It utilizes ActiveX® and Java™ applet controls for SSL tunneling.
- The Network Connector turns remote clients into part of the corporate network, supporting full connectivity over a virtual and secure transparent connection. It enables the gateway to support split tunneling configurations and afford greater network reliability and performance.

## Integrated Application Firewall

The gateway's deep application-level filtering, assessed through application behavior knowledge, prevents exploits that cause unexpected application responses. It blocks potentially malicious traffic using positive- and negative-logic rules that identify errant commands and syntax and reduces the immediacy of server software patches by providing protection from zero-day attacks.

## Application Aware™

Because the IAG is application aware, it can address application-specific issues, including security concerns and functionality requirements. This ability enables organizations to customize the behavior of specific applications when accessed remotely. The IAG provides out-of-the-box support for key applications, to allow for rapid optimization of most popular applications in use today. Out-of-the-box application support is optimized for each application-type, including features such as URL Inspection rulesets and character definitions, wiping out sensitive information possibly recorded by a web browser during an SSL VPN session, and more.

In addition, the application aware approach provides administrators with tools and interfaces that enable them to define features which are not supported out-of-the-box for each application individually.

## Supported Applications

The SSL VPN portal supports the following groups of applications:

- **Built-in Services** are services that are supplied with the IAG, such as File Access or Web Monitor.
- **Web Applications** are applications that use HTTP/HTTPS and a web interface, such as Microsoft Office SharePoint Server 2007 and Outlook Web Access.
- **Client/Server and Legacy Applications** are applications that use non-HTTP/HTTPS protocols and are handled by the SSL Wrapper. Examples of client/server and legacy applications include: Telnet; Citrix® MetaFrame® Program Neighborhood applications, Microsoft® Windows® Terminal Services Clients, Microsoft Outlook, and more.
- **Browser-Embedded Applications** are web initiated applications that use a web-based interface to create a non HTTP/HTTPS connection, and are handled by the SSL Wrapper. These include Citrix NFuse®, IBM WebSphere Host-on-Demand, Lotus® SameTime®, Terminal Services Web Client, and others.

In addition to the applications that are supported out-of-the-box, you can define your own generic applications, such as a generic web application, where you define all the application settings, rulesets, and definitions according to the application's requirements.

## Trunks: the IAG Transfer Channels

Data is transferred through the gateway via transfer channels, or trunks, where each trunk is related to the type of data being transferred: HTTP or HTTPS. Each trunk is divided into two channels, one incoming and one outgoing, allowing for bi-directional data flow.

You can configure three types of trunks:

- Portal trunk: a forked one-to-many connection, where the same IP address is used to access multiple applications. Use it to enable access to any number of web and non-web applications, for both out-of-the-box and generic applications.
- Webmail trunk: a one-to-one connection, enabling access to a single Webmail application. A Webmail trunk is automatically created with authentication, application customization, and URL inspection rules that are optimized for the Webmail application you are running.
- Basic trunk: a one-to-one straight line, where one IP address routes to a single web server, enabling access to any generic web application.

## Supported Browsers

On endpoint computers, the following browsers are supported:

**Table I. Supported Browsers**

Operating System	Supported Browsers
Windows 2000	<ul style="list-style-type: none"><li>• Internet Explorer 6.0</li><li>• Mozilla® family: Netscape® Navigator® 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox® 1.0.x and higher</li></ul>
Windows XP/2003	<ul style="list-style-type: none"><li>• Internet Explorer 6.0, 7.0</li><li>• Mozilla® family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox® 1.0.x and higher</li></ul>
Windows Mobile® 2003 for Pocket PC *	Pocket Internet Explorer

**Table I. Supported Browsers (Cont'd)**

Operating System	Supported Browsers
Mac® OS X	<ul style="list-style-type: none"><li>• Safari™ 1.2.4, 1.3 &amp; 2.0</li><li>• Mozilla family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox 1.0.x and higher; Camino® 0.83 and higher</li></ul>
Linux® (Red Hat®, SUSE®, Debian®)	Mozilla family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox 1.0.x and higher

\* Supports mobile Internet connectivity.

Although other browsers might also be functional, for optimal performance, Whale Communications extends support to these versions only.



**Note**

Some of the Whale Client Components are supported only on Windows operating systems running Internet Explorer. For details, refer to “Whale Client Components” on page 147.

For those users running other operating systems or other browser-versions, our portal homepage has been reworked to present a stripped-down page for browsers that do not support the rich environment necessary to support the entire range of IAG features, such as scheduled logoffs and session timeouts. The limited portal presents users with a page containing links to all applications; when a user clicks a link, the application opens in a new window. The limited portal does not, however, include the Whale toolbar, which enables additional IAG features such as credentials management and system information.

## Security Management Tools

The IAG provides you with security management tools that ensure strict security administration and enforcement:

- The **Service Policy Manager** is where you can optionally pre-configure security policies to which the configuration settings are enforced to conform.
- The **Configuration** program enables robust, granular configuration of all aspects of the gateway, including network management, content management, and application control. From within the Configuration

program, the **Create New Trunk Wizard** streamlines trunk creation and configuration. Application-sensitive predefined rulesets and out-of-the-box dangerous-character definitions are automatically applied to the filtering mechanism as part of the configuration process.

- The **Editor** enables you to easily edit, sort and convert any text file, including encrypted files and base64-encoded text.

All the tools are described in detail in the *Intelligent Application Gateway Advanced Configuration* guide, in Chapter 2: “Security Management Tools”.

## Monitoring and Control Tools and Interfaces

The IAG monitoring and control tools enable network management and auditing at both the network and application levels:

- The **Event Logging** mechanism logs IAG-related events to a variety of tools and output formats, including information about usage, user activities, and potential security risks.
- The **Web Monitor** is a monitoring and reporting web application that enables anywhere, anytime snapshot viewing of events, as well as event filtering and analyzing.

## Encryption

In order to prevent unauthorized access to the IAG, the IAG’s configuration files are encrypted. You generate an encryption key when you first access the IAG, and this key is used to encrypt and decrypt the IAG configuration data. This process is described in the *Intelligent Application Gateway Advanced Configuration* guide, in the section “Creating Encryption Keys” on page 20.

In setups where more than one IAG server is used, the IAG servers have to be configured with an identical encryption key in order to:

- Export and import configuration files between IAG servers.
- Export and import URL inspection and File Access rulesets.
- Use High Availability arrays.



### Tip

If you need to encrypt and decrypt any of the IAG files, use the Editor. For details, refer to the *IAG Advanced Configuration* guide, to “Editor” on page 40.

## Encryption Passphrase

Once the encryption key is generated, every time you carry out operations that write to the disk, such as saving or activating configuration files, or when you import a configuration file or a set of rules into the IAG, the IAG prompts you to enter the encryption passphrase. You must always enter a valid passphrase; this ensures that only authorized users can access the IAG's configuration files.

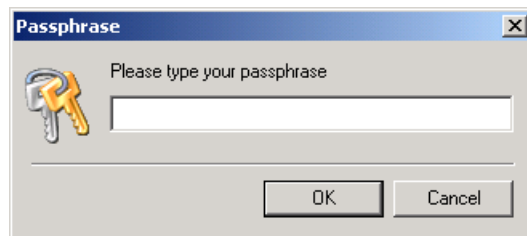


### Tip

In order to change the passphrase any time after the initial installation, run the following command in a Command prompt:

```
changepassphrase
```

The Passphrase prompt is shown below:



When prompted, enter the passphrase and click **OK**. You can then securely carry on the operation you have started.

In sites where a number of IAG servers use the same encryption keys—such as a High Availability array—the same encryption passphrase is used for all the IAG servers at the site.



### Tip

When using the Configuration program, the encryption passphrase you enter is valid for 10 minutes. That is, during the 10 minutes following an operation that requires access to the configuration files, you can access the files again without having to re-enter the passphrase.

## High Availability Array

For high-traffic sites, with applications supporting a large number of simultaneous connections, the IAG provides a powerful performance enhancement and traffic control solution—the High Availability array. Implementing central management and supporting a variety of load balancing tools, the High Availability array enables you to run a server array, consisting of two or more IAG servers, while controlling high traffic volumes through the system. The High Availability array is configured to route traffic so that it maximizes resource utilization and supports uptime.

For a detailed description of the High Availability array, including step-by-step instructions on how to configure it, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to Chapter 9: “Configuring the High Availability Array”.

## About This Guide

This Guide is intended for the system administrator of the IAG. It provides you with in-depth information about the IAG’s functionality and how you can best use its various components and options. It includes step-by-step instructions on how to configure, maintain, monitor and control any number of IAG servers, either locally or over the network.

This Guide provides information on the following topics:

- Chapter 2: “**SSL VPN Portals**” explains how you use the Create New Trunk and Add Application Wizards to create SSL VPN portals, to secure access to multiple applications from remote locations, anywhere, anytime.
- Chapter 3: “**Single Application Sites**” describes how you can use the Service Policy Manager to pre-configure the HTTP and HTTPS Connections services, how you create Webmail and Basic trunks, and how you use the Configuration program to edit trunks once they are created.
- Chapter 4: “**Application Settings**” describes application-specific settings you can edit and control after you add the application to the trunk, or create a Webmail trunk, such as the application’s web and non-web servers, application authentication, and more.
- Chapter 5: “**Endpoint Security**” describes features that help to protect your internal network against access from non-secure endpoint computers, including the definition of endpoint security policies, and the Attachment Wiper™ and Certified Endpoint options.

- Chapter 6: **“SSL Wrapper”** describes how you can provide users with secured SSL connectivity, via the portal homepage, to various TCP/IP client/server applications, such as native messaging applications, standard email applications, collaboration tools, connectivity products, and more. It also describes how you provide users with secured SSL connectivity to Domino® iNotes™ servers via a Webmail trunk.
- Chapter 7: **“Network Connector”** describes the Network Connector feature, which enables you to install, run, and manage remote connections as if they were part of the corporate network, supporting full connectivity over a virtual and secure transparent connection.
- Chapter 8: **“Providing Access to Internal File Systems”** describes how you can provide remote users with access to the organization’s internal file systems, including:
  - Local Drive Mapping, which provides access to Windows shared network folders.
  - File Access, which provides web access to the internal Windows Network and Novell® NetWare® file servers.
- Chapter 9: **“Monitoring and Control”** familiarizes you with the IAG’s monitoring and control tools and interfaces and provides detailed instructions on how to access and use them.
- Chapter 10: **“Troubleshooting”** describes how you use the Backup & Restore utility, and how you use various diagnostics tools such as support utilities tests and error and trace logs. It also provides information on how log files are cleaned up, and how to restart the Web service in the Windows Server® IIS (Internet Information Server).
- Appendix A: **“Troubleshooting Event Logging Messages”** provides troubleshooting guidelines and instructions for Warning and Error messages that are reported by the Event Logging mechanism.



#### Tip

For a description of additional, advanced features and configuration settings, refer to the *Intelligent Application Gateway Advanced Configuration* guide.



## Conventions Used in This Guide

This section explains the conventions used throughout this Guide.

**Menu Item**

Menu names and menu items.

**Button**

Buttons that you select with the mouse.



Icons that you select with the mouse are represented graphically.

***Procedure***

Title of an operating procedure.

`Computer text`

System files and information that you type in.



**Caution**

A note advising you that failure to take or avoid a specific action could result in loss of data.



**Note**

Important information you should note.



**Tip**

Helpful tips for working with the e-Gap Appliance.



## Chapter 2

# SSL VPN Portals

An Intelligent Application Gateway (IAG) SSL VPN Portal enables you to provide employees and partners with browser-based remote access to multiple corporate applications and file systems. In order to create an SSL VPN Portal, you go through the following stages:

- Portal session setup, which includes the lifecycle of a session, such as: access IP, authentication, access endpoint policies, and more.
- Application setup, where you set up the applications you enable through the trunk.

Once you set up the portal and applications, the SSL VPN Portal is operational; remote users can access the portal and the applications that are enabled through it. Portal session setup and initial application setup are described in “Creating an SSL VPN Portal” on page 28.

- Users setup (optional), to determine which users are authorized to view and access each of the applications enabled through the portal. By default, all authenticated users are allowed access to all applications. You can, however, configure a more granular setup, and determine which users can view and access each of the applications you enable through the portal, as described in “Users Setup” on page 32.
- Additional portal configuration options you may require are described in “Optional Configuration” on page 46, including:
  - “Configuring Global Host Address Translation” on page 46
  - “Configuring Application Subnets” on page 48
  - “Changing the Application Access Portal Port Number” on page 49
- If you need to make adjustments to the look-and-feel of the portal homepage, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Portal Homepage Configuration” on page 54.
- Some of the applications you can enable through the portal require additional configuration. For details, refer to the *Intelligent Application Gateway Application Aware Settings* guide.

Additional, advanced configuration options, which are not covered in this chapter are described in “Where To Go From Here” on page 49.

# Creating an SSL VPN Portal



## Note


- Before you start the configuration process, log on to Windows with full administrator privileges.
- The first time you access either the Configuration program or the Service Policy Manager, you are required to create an encryption key and passphrase for the IAG. The key and passphrase serve both IAG applications, so that this action is only required once; when you subsequently access either application, you use the same passphrase. Additional information is available as follows:
  - For an overview of the encryption mechanism, see “Encryption” on page 21.
  - For details on how to create the encryption keys and passphrase, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Creating Encryption Keys” on page 20.

You create an SSL VPN Portal in these stages:

- You can optionally use the Service Policy Manager to pre-configure the IAG HTTP Connections and HTTPS Connections services, as described in “Optional Pre-configuration of the Services” on page 52.
- In the Configuration program, set up the portal session using the Create New Trunk Wizard. The wizard facilitates a quick auto-completion of the initial portal session setup, including basic portal settings, session authentication, setup of the website that is created on the IAG, and session endpoint policies that control access to the site.
- In the trunk you defined, use the Add Application Wizard to set up the applications that will be enabled to remote users through the portal, including basic application attributes such as application servers, application authentication, endpoint policies, portal page links, and more. The IAG Application Aware approach insures that, for the supported applications, out-of-the-box settings such as replying to application authentication requests, URL inspection rulesets, and more, are automatically applied.

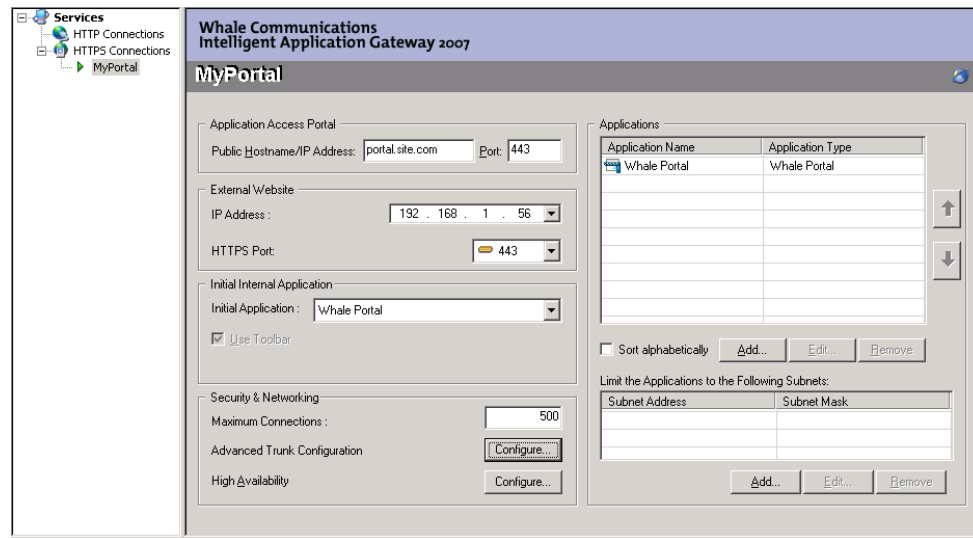
### *To create an SSL VPN Portal:*

1. In the Windows desktop of the IAG, click **Start**, then point to **Programs > Whale Communications IAG** and click **Configuration**. Enter your password, as required.
2. In the Configuration program, in the List pane, select and right-click **HTTP Connections** or **HTTPS Connections**, then select **New Trunk**.  
*The Create New Trunk Wizard is displayed.*

3. Follow the instructions on the screen to complete the wizard; for details, click  [Help](#).

When you complete the wizard, click **Finish**.

*The wizard closes. The new Portal trunk you created now appears in the List pane, and the Configuration pane displays the trunk's parameters.*




#### Note

By default, the Initial Internal Application is the Whale Portal application, used in conjunction with the Whale toolbar. If you wish to use a different portal homepage, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Using a Custom Portal Homepage” on page 61.

4. In the List pane, right-click the trunk and select **Add**;  
Or,

In the “Applications” area of the Configuration pane, under the Application List, click **Add...**, or double-click an empty line.

*The Add Application Wizard is displayed.*

5. Follow the instructions on the screen to complete the wizard; for details, click  [Help](#).

When you complete the wizard, click **Finish**.

*The Add Application Wizard closes, and the application you defined appears in the Applications list. Once you activate the configuration, the application will be accessible to remote users.*

Applications

Application Name	Application Type
Whale Portal	Whale Portal
File Access	File Access

☐ Sort alphabetically

Limit the Applications to the Following Subnets:

Subnet Address	Subnet Mask




### Note

Some applications require additional setup. For those applications, when you finish adding the application to the trunk, a help screen pops up, informing you of the application-specific requirements, and providing step-by-step setup instructions where applicable. The help is also available to you any time thereafter, in the General tab of the Application Properties dialog box, via the following link:

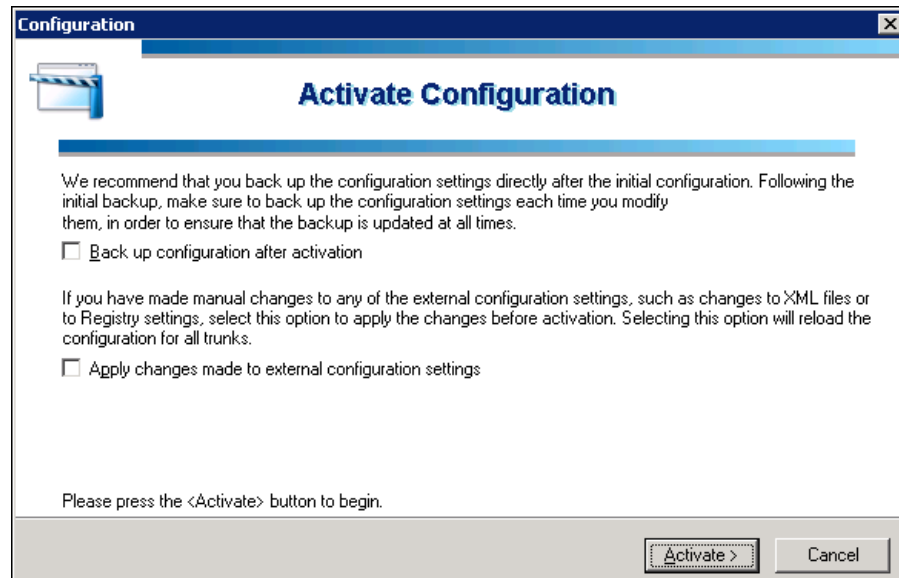
[Application Aware Settings](#)

You can find a description of all the IAG application-specific requirements in the *Intelligent Application Gateway Application Aware Settings* guide.

6. Repeat steps 4–5 to add more applications to the SSL VPN Portal. You can also quickly add a new application to the trunk, based on the definitions of an existing application, as described in “Duplicating an Application” on page 91.
7. Determine in what order you wish the applications to be displayed on the portal page, as follows:
  - If you want the applications to be displayed in alphabetical order, activate the option “Sort alphabetically”.
  - If you want to arrange the applications in any other order, leave the “Sort alphabetically” option unchecked, and use the up/down arrows to arrange the order of the applications in the list. They will be displayed on the portal page in the order by which they are arranged in the list of applications.

8. In the main window of the Configuration program, click  to save and activate the configuration.

*The following is displayed:*



9. Click **Activate >**.



#### Note

We recommend that you activate the option “Back up configuration after activation”, so that the configuration settings are backed up. For more details refer to “Backup & Restore Utility” on page 303.

*Once the configuration is activated, the following message is displayed:*

IAG configuration activated successfully.

*The trunk is operational. All authenticated users will be able to access the applications enabled through the portal. If you wish to configure authorization for any of the applications you enable through the trunk, proceed to “Users Setup” on page 32.*



#### Note

- You can duplicate a trunk, including all application definitions, changing only the name, and the external website’s IP address and port numbers. Right-click the trunk you wish to duplicate, and select **Duplicate**.
- Delete a trunk by right-clicking the trunk name and selecting **Delete**.

## Users Setup

Users setup determines which users are authorized to view and access each of the applications enabled through the portal. When you set an application up, by default, all authenticated users are allowed to view and access the application. If required, you can change the default settings, and determine which users can view and access the application.

Users setup affects the following:

- **Authorization:** the process by which authenticated users are given access to the portal applications.
- **Personalization:** the process by which different users view different application links on the same portal homepage, depending on their authorization permissions.



### Note

Personalization only works when you use the default portal homepage supplied with the IAG. However, even if you are using a custom portal homepage, authorization works, enabling users to access only those applications for which they have access permissions.

When you add an application to a Portal trunk using the Add Application Wizard, the option “All Users Are Authorized”, in the “Application Setup” step, is enabled by default. You can disable this option while adding the application to the trunk, or at any time after the initial application configuration, in the Application Properties dialog box, in the Authorization tab.

If you disable the “All Users Are Authorized” option for an application, you must configure authorization in order to enable access to the application through the portal. Using authorization, you can grant access permissions to an application to selected users and user groups, while blocking access from users that should not be accessing the application.

In order to configure authorization, you take the following steps:

- Define the users and groups of users to which you can grant authorization permissions, as described in “Defining Authorization Repositories” on page 33.
- Define authorization and personalization per application, as described in “Defining Authorization for Portal Applications” on page 38.



## Defining Authorization Repositories

Repositories are databases containing user and group information; a user can be defined as an individual unit or associated with a group. This section describes how you define repositories of users and user groups, which you can then use in order to define authorization for portal applications, including:

- “User/Group Servers” on page 33.
- Optional configuration of local groups, described in “Local Groups” on page 35.

### User/Group Servers

This section describes how you define a third-party user/group server. The servers are used as user/group repositories for application authorization, and can also be used to define local groups.

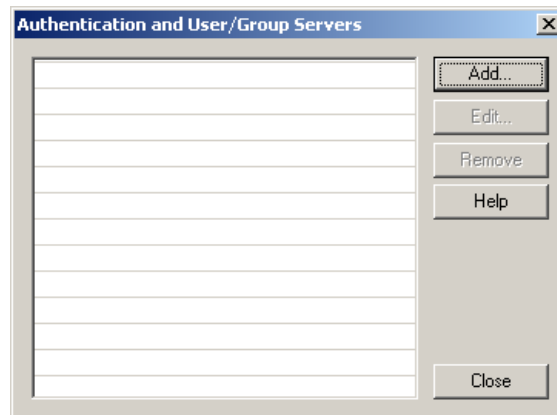


#### Note

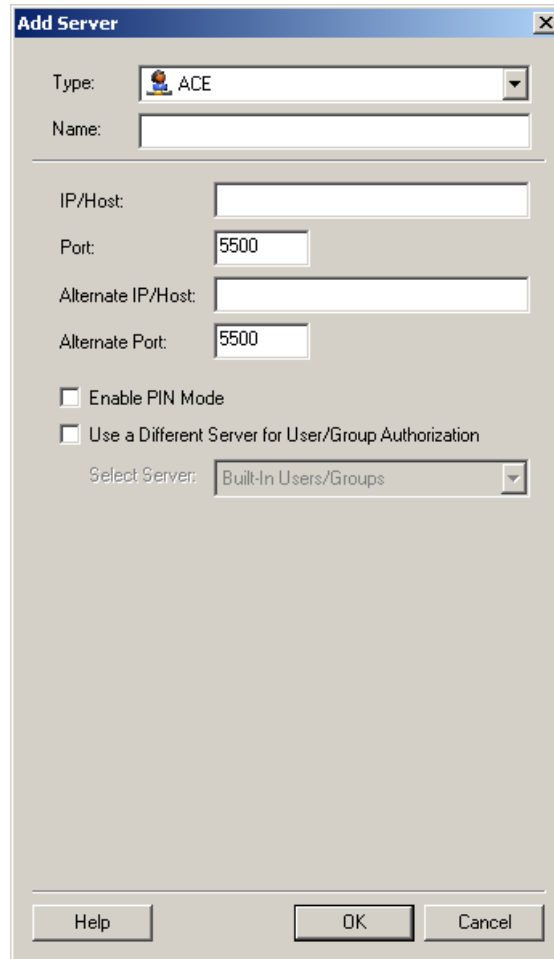
User/group servers are also used for session authentication, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Authentication” on page 81.

#### To define a user/group server:

1. In the Configuration program, on the **Admin** menu, click **Authentication and User/Group Servers...**  
*The Authentication and User/Group Servers dialog box is displayed.*



2. In the Authentication and User/Group Servers dialog box, click **Add...**.  
*The Add Server dialog box is displayed.*



The 'Add Server' dialog box is shown with the following fields and options:

- Type:** A dropdown menu with 'ACE' selected.
- Name:** An empty text field.
- IP/Host:** An empty text field.
- Port:** A text field containing '5500'.
- Alternate IP/Host:** An empty text field.
- Alternate Port:** A text field containing '5500'.
- ☐ **Enable PIN Mode**
- ☐ **Use a Different Server for User/Group Authorization**
- Select Server:** A dropdown menu with 'Built-In Users/Groups' selected.

At the bottom are three buttons: 'Help', 'OK', and 'Cancel'.

3. Use the Add Server dialog box to define the server. For details regarding each server-type, click [Help](#).



### Tip

For a description of the types of authentication and user/group servers you can use with the IAG, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Authentication Schemes” on page 104.

4. Repeat steps 2–3 to define all the required servers.  
*You can now use the servers you defined in order to:*
  - *Define local groups, as described in “Local Groups” on page 35.*
  - *Define application authorization, as described in “Defining Authorization for Portal Applications” on page 38.*

## Local Groups

A local group is a repository of users that you define once, and can then reuse as many times as required when defining authorization for portal applications. A local group can contain users and groups from various user/group servers; it can also contain other local groups. An include/exclude mechanism enables you to select individual users and groups that will be included in or excluded from the local group.

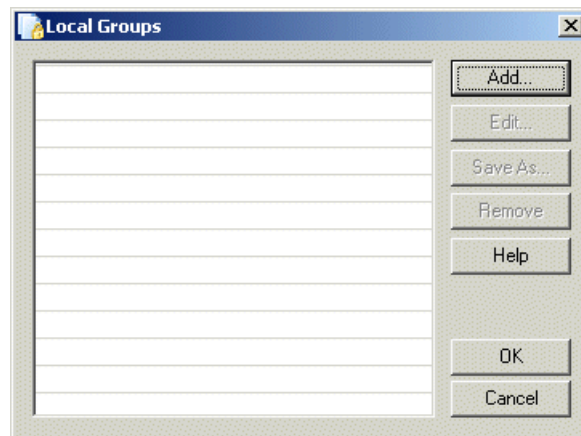
**For example:** you can create a local group that includes selected users from three different user/group servers, then use this group repeatedly, to define authorization for all the portal's non-web applications.

You can use the Configuration program to define local groups in one of two ways:

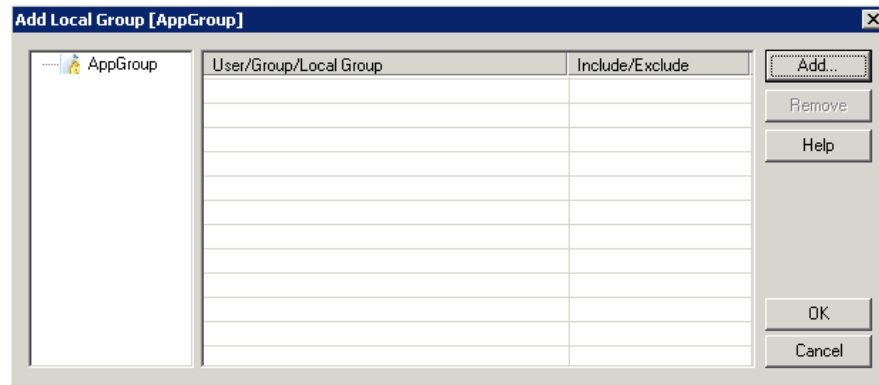
- Via the **Local Groups** menu item, as described in this section.
- Via the Authorization tab of the Application Properties dialog box, as described in “Defining Authorization for Portal Applications” on page 38.

### *To define a local group via the menu bar:*

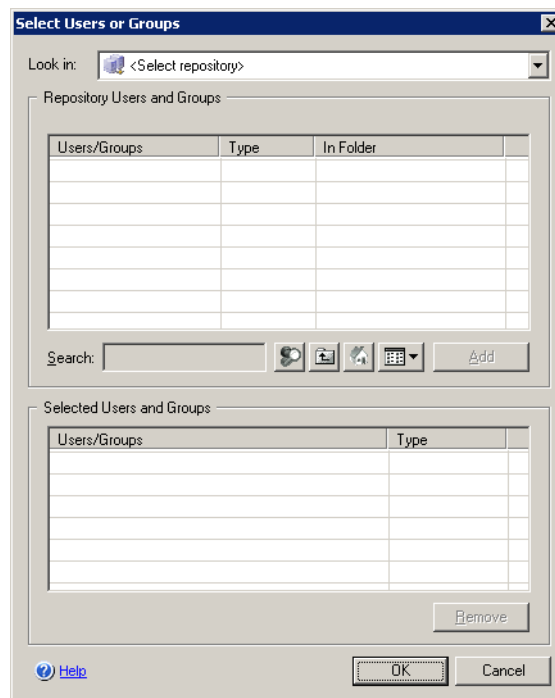
1. In the Configuration program, on the **Admin** menu, click **Local Groups...**  
*The Local Groups dialog box is displayed.*



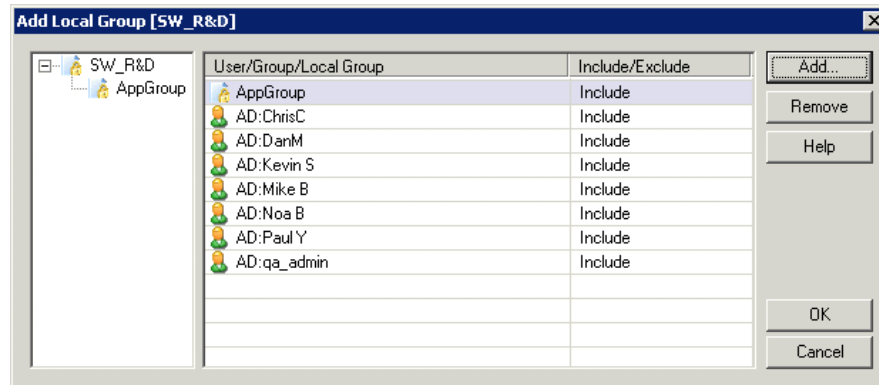
2. In the Local Groups dialog box, click **Add...**.  
*The Name Local Group dialog box is displayed.*
3. Name the group, then click **OK**.  
*The Add Local Group dialog box is displayed. The name you assigned to the group is displayed in the title bar and in the left pane of the dialog box.*



4. In the Add Local Group dialog box, click **Add...**.  
*The Select Users or Groups dialog box is displayed.*



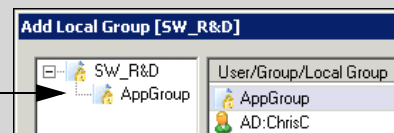
5. Use the Select Users or Groups dialog box to select the users and groups that will be included in the local group. If other local groups are already defined, they can also be selected as part of the current group. For a description of how you use the Select Users or Groups dialog box, refer to “Selecting Users and Groups” on page 43.
6. Once you select the users and groups you wish to assign to the local group, close the Select Users or Groups dialog box.  
*The selected users and groups are added in the Add Local Group dialog box.*



### Tip

If the local group you created includes other local groups, the nested local groups are displayed in the left pane of the Add Local Group dialog box:

“AppGroup” local group is nested under “SW\_R&D”



7. If required, use the “Include/Exclude” column to refine the definition. By default, when you add a user or group to the local group, their status is “Include”; double-clicking an entry in the “Include/Exclude” column toggles the status of the user or group.

**For example:** if you wish to include most of the users of an Active Directory user/group server in the local group, but exclude three individual users from that group, take the following steps:

- a) Use the Select Users or Groups dialog box to select from the Active Directory repository both the “Authenticated Users” group, and the three users you wish to exclude from the local group.
  - b) Use the Add Local Group dialog box to exclude the three users from the local group.
8. Click **OK** to close the Add Local Group dialog box.
  9. Repeat steps 2–8 to define additional groups, as required.



### Tip

You can use the **Save As...** button in the Local Groups dialog box to duplicate an existing local group.

*You can now use the groups you created to define application authorization, as described in “Defining Authorization for Portal Applications” on page 38. You can also use the local groups as building-blocks when defining additional local groups.*

## Defining Authorization for Portal Applications

You can define authorization for any of the applications enabled through an SSL VPN Portal. To define authorization for an application, take the following steps:

- **Assign users and groups to the application.** In this step, you select the users and user groups from any of the defined authorization repositories, and assign them to the application. By default, the users and groups you select here have Allow and View permissions for the application.
- **Assign authorization permissions** to the users and groups you selected for the application. For each user or group, you can assign Allow, View, or Deny authorization permissions.

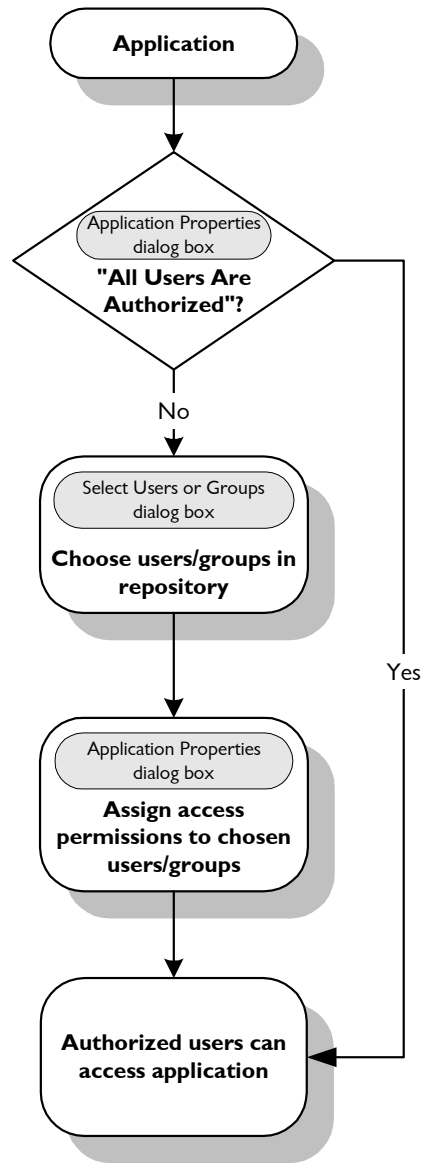


### Note

If, at any time after the initial configuration, there are changes in the authorization repository, such as a user is removed or added from the repository, or user permissions are changed, you need to change the permissions you assign to users and groups in this repository, correspondingly.

Figure 1 on page 39 illustrates the process of configuring users authorization permissions for an application.

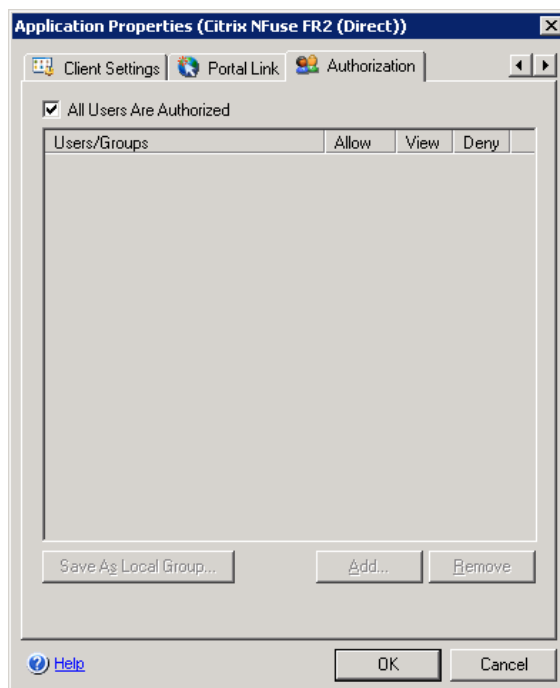
**Figure 1. Flow of Configuring Application Authorization**



***To assign authorization for an application:***

1. In the Configuration program, from the List pane, select the trunk that enables the application you wish to edit.
2. In the Configuration pane, in the "Applications" area, select the application and click **Edit...**, or double-click the application.  
*The Application Properties dialog box is displayed.*
3. Select the Authorization tab.

*In the Authorization tab, the option “All Users Are Authorized” is checked.*



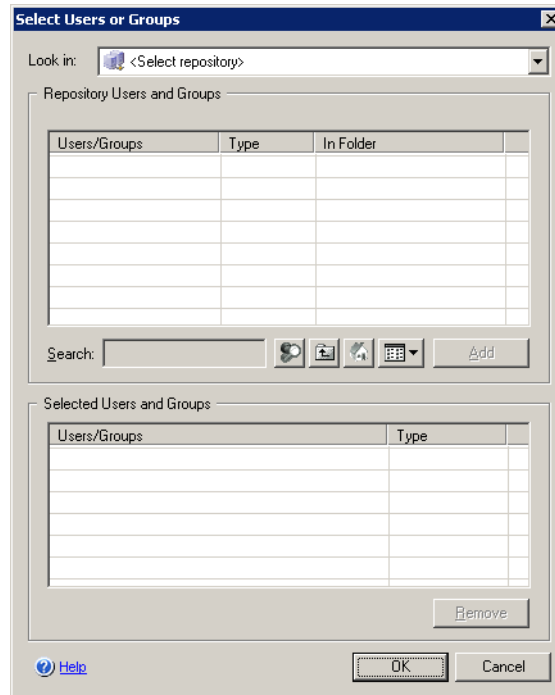
4. Uncheck the option “All Users Are Authorized” and click **Add...**.  
*The Select Users or Groups dialog box is displayed.*



#### **Note**

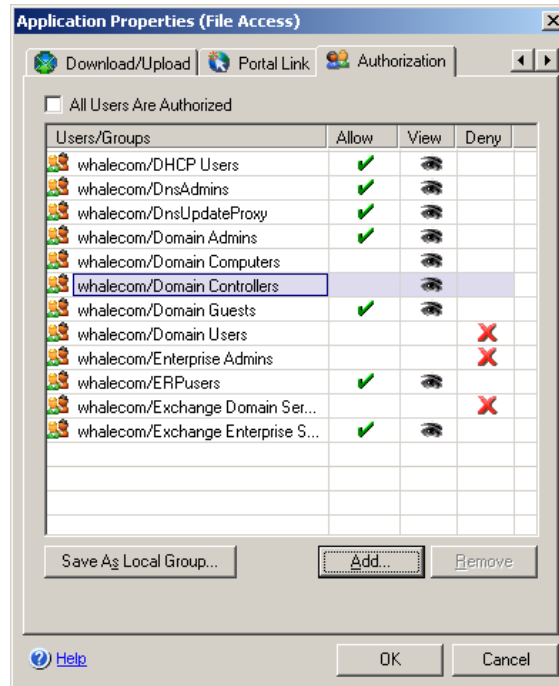
If the option “All Users Are Authorized” is unchecked, and you do not define the users and groups that are authorized to access and view the application, as described in the steps that follow, all users are blocked from using the application.





5. Use the Select Users or Groups dialog box to select the users and groups to which you wish to define authorization permissions for the application. For a description of how you use the Select Users or Groups dialog box, refer to “Selecting Users and Groups” on page 43.
6. Once you select the users and groups you wish to assign to the application, close the Select Users or Groups dialog box.

*The users and groups you selected are added to the Users/Groups list in the Authorization tab of the Application Properties dialog box.*



### Tip

You can save your selection of users and groups as a local group, using the **Save As Local Group...** button. For details on local groups, refer to “Local Groups” on page 35.

7. For each user or group, click the appropriate boxes to select one of the access permission levels:
  - **Allow:** users can view and access the application via the portal homepage.
  - **View:** the link is displayed on the portal homepage. However, when users click the link, they are prompted to enter additional credentials in order to access the application.
  - **Deny:** the effect of this option depends on the type of portal homepage used with the site:
    - In sites that use the default portal homepage supplied with the IAG, the link is not displayed on the portal homepage and users cannot access the application.
    - In sites that use a custom portal homepage, the link is displayed on the portal homepage. However, when users click the link, access to the application is denied.

In both types of portal homepages, if users attempt to access the application, either directly or via a different link, they are denied access.

8. Click **OK**.

*The Application Properties dialog box closes. Once the trunk is activated, the application is accessible to users according to the authorization permissions you defined in this procedure. If you use the default portal homepage, the portal is personalized according to each user's access permissions.*

## Selecting Users and Groups

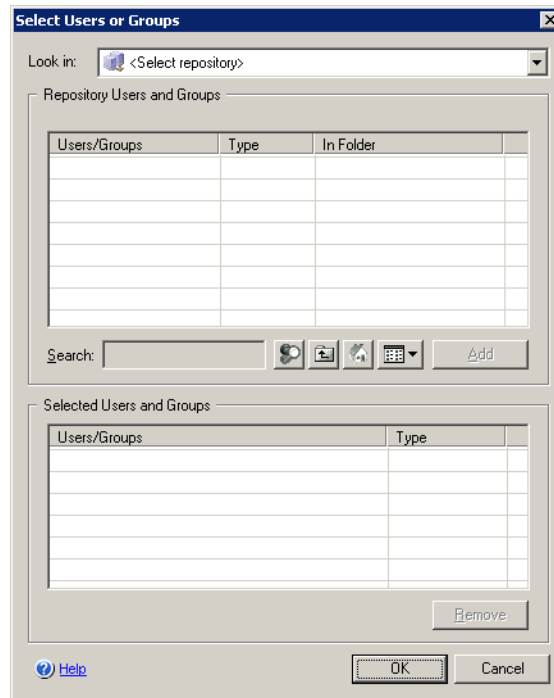
This section describes how you use the Select Users or Groups dialog box to select users and groups of users when you:

- Define local groups, as described in “Local Groups” on page 35.
- Define authorization for an application, as described in “Defining Authorization for Portal Applications” on page 38.

The dialog box is divided into two main areas:

- The “Repository Users and Groups” area changes according to the type of item selected in the “Look in” drop-down list:
  - If a users/groups server is selected in the “Look in” drop-down list, all the users and groups in the selected repository are listed in the “Repository Users and Groups” area.
  - If “Local Groups” is selected in the “Look in” drop-down list, all the defined local groups are listed in the “Repository Users and Groups” area.
- The “Selected Users and Groups” area lists the users and groups that you selected in the “Repository Users and Groups” area. These are the users and groups that will be added to the local group or to the application's Authorization tab, as applicable.

**Figure 2. Sample Select Users or Groups Dialog Box**



***To use the Select Users or Groups dialog box:***

1. In the **Look in** drop-down list, select the repository you wish to use. You can select from two types of user/group repositories:
  - Repositories of users and user-groups, based on the definition of a third-party user/group server, described in “User/Group Servers” on page 33.  
*All the users and user groups in the selected repository are listed in the “Repository Users and Groups” list.*
  - Local groups, described in “Local Groups” on page 35.  
*All the defined local groups are listed in the “Local Groups” list.*
2. To add users and groups to the “Selected Users and Groups” list, double-click a user or a group in the “Repository Users and Groups” list or the “Local Groups” list, respectively, or select one or more users and groups and click **Add**.

For Active Directory and LDAP servers, the “Repository Users and Groups” list contains groups and individual users; groups are listed first, then users. If the option “Include Subfolders” is activated for this user/group server (when you configure the server in the Add Server dialog box), subfolders are listed as well; the path of the selected folder is shown above the “Users/Groups” list. In order to facilitate the search for a user or a group, use any of the buttons described in Table 2 on page 45.

**Tip**

- To add all the users and groups in a users/groups server, select “Authenticated Users”.
- When you add a local group, all the users and groups that are part of the local group are selected.




*The selected users and groups are moved to the “Selected Users and Groups” list.*

3. Repeat steps 1–2 to add users and groups from other repositories, if required.


4. Click **OK** at the bottom of the Select Users or Groups dialog box.

*The dialog box closes. The users and groups you selected are added to the local group or to the application’s Authorization tab, as applicable.*

**Table 2. Select Users or Groups—User/Group Search Buttons**

Button		Description
	Search	Enter a string in the Search text-box then click the Search button. The search is affected by the selected View setting, described in “View Menu”, below. <b>Tip:</b> You can also select an entry in the list, then start typing the user/group string. The display automatically moves to the relevant letter or string.
	Up One Level	Moves the display one level up in the folder-tree.
	Home	Returns the display to the top level folder.

**Table 2. Select Users or Groups—User/Group Search Buttons (Cont'd)**

Button	Description
 View Menu	<p>Enables you to filter the view in the “Repository Users and Groups” list:</p> <ul style="list-style-type: none"><li>• Show all: displays all users and groups in the selected folder. If the option “Include Subfolders” is activated for the selected server, subfolders are also displayed.</li><li>• Show users only: displays all users in the selected folder.</li><li>• Show groups only: displays all groups in the selected folder.</li><li>• Show users &amp; groups: displays all users and groups in the selected folder. Subfolders are not displayed.</li><li>• Show users &amp; groups, including subfolders: displays all users and groups in the selected folder. If the option “Include Subfolders” is activated for the selected server, subfolders are also displayed, as well all users and groups in all subfolders.</li></ul>

## Optional Configuration

In certain cases, you may want to configure additional parameters, such as:

- Define the global Host Address Translation (HAT) parameters, which are applied to all the trunks configured in the IAG. For details, refer to “Configuring Global Host Address Translation” on page 46.
- Restrict the applications in the SSL VPN Portal so that only servers within the defined subnets are enabled, as described in “Configuring Application Subnets” on page 48.

## Configuring Global Host Address Translation

This section describes the optional configuration of HAT parameters. The parameters you configure here are global, and are used during link manipulation for all the Portal trunks configured in the IAG.



### Note

- Link manipulation is described in the *Intelligent Application Gateway Advanced Configuration* guide, in Chapter 8: “Optimizing Portal Performance”.
- If you do not configure HAT parameters here, the IAG automatically assigns the required parameters the first time you configure a Portal trunk. You can change the configuration settings any time after the initial configuration.

### To configure global HAT parameters:

1. In the Configuration program, on the **Admin** menu, click **Advanced Configuration...**

*The Advanced Configuration window is displayed.*

2. In the Host Address Translation area, enter the following:
  - **Unique Identifier:** a sign that will be added to manipulated links in responses, and by which the IAG will recognize the URL in the request.



### Note

- The unique identifier must contain only alphanumeric values.
- Make sure the identifier is not a string that is contained within one of the server names in your organization. For example, if one of the servers in your organization is named “appserver”, do not use the string “app” or “ser” as the unique identifier.

- **Encryption Key:** a key that will be used for internal encryption. Click **OK**.

*The Advanced Configuration window closes.*

3. In the Configuration program, click  to save and activate the configuration.  
*The IAG will use the unique identifier and encryption key you entered here during link manipulation, for all Portal trunks.*

## Configuring Application Subnets

You can restrict any of the applications in your SSL VPN Portal so that only servers within the defined subnets are enabled.

Once the trunk is operative, when a user requests a URL, the filter first checks the URL against the Application List; if the application is listed here, the filter goes on to check the URL against the Subnet List. Only URLs that pass both checks are enabled to the user.



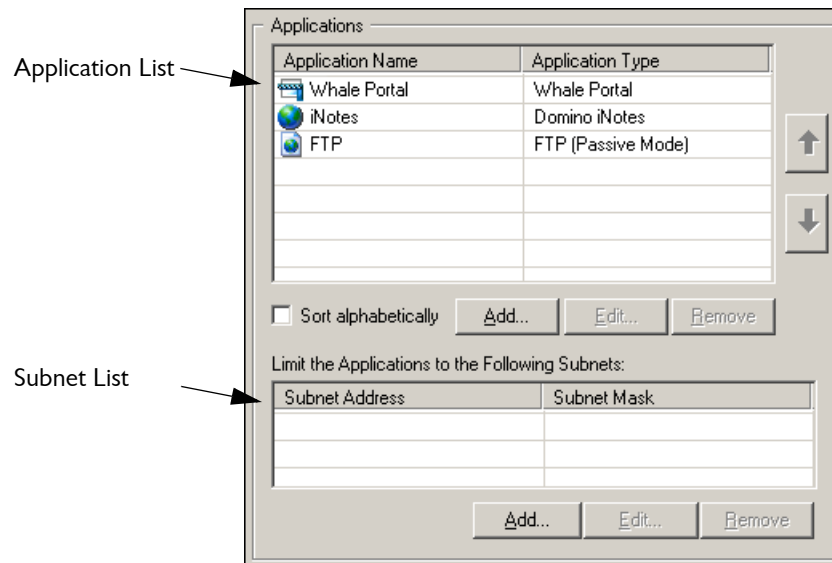
### Note

For each application you add, make sure that the application is listed in the IAG's DNS or Hosts file.

You configure subnets in the main window of the Configuration program, in the “Applications” area, as described in this procedure.

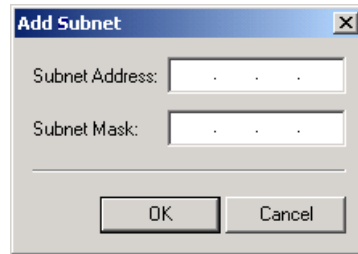
### To configure application subnets:

1. In the “Applications” area, under the Subnets list, click **Add...**.

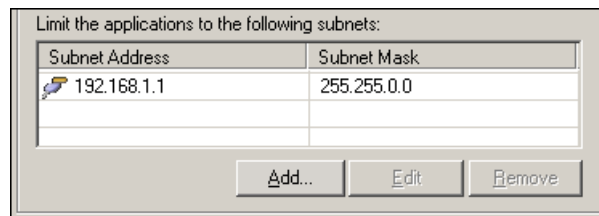


*The Add subnet dialog box is displayed.*





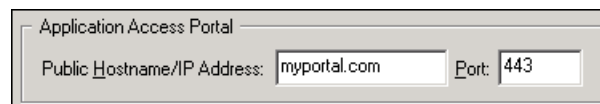
2. Enter the subnet address and mask, then click **OK**.  
*The Add subnet dialog box closes. The subnet you configured is added to the Subnet list.*



3. Repeat steps 1–2 to define additional subnets.  
*The applications will be restricted to the defined subnets.*

## Changing the Application Access Portal Port Number

The port number that is assigned to the Application Access Portal when you create the trunk in the Create New Trunk Wizard is the port number of the external website. In setups where remote users access a machine other than the IAG, such as a load balancer, enter the port number of the actual machine that is accessible to the users, at the top left side of the Configuration pane, in the Application Access Portal area:



## Where To Go From Here

Once the SSL VPN Portal is created, you can edit it using the Configuration program. You can configure any of the following:

- Options that are described in this Guide include:
  - Editing any of the applications' properties in the Application Properties dialog box, as described in "Editing Application Properties" on page 67.

**Tip**

- For information on the Network Connector application, see Chapter 7: “Network Connector”.
- For information on the Local Drive Mapping and File Access applications, see Chapter 8: “Providing Access to Internal File Systems”.

- For HTTPS Connections trunks: creating a Redirect trunk in order to redirect HTTP requests, as described in “Creating a Redirect Trunk” on page 58.
- Editing general trunk parameters, as described in “Editing in the General Tab” on page 61.
- Changing the event logging definitions, as described in “Event Logging” on page 237.
- Enabling access to the Web Monitor, as described in “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.
- Additional, advanced options, described in the *Intelligent Application Gateway Advanced Configuration* guide, including:
  - Customizing the look-and-feel and other aspects of the HTML pages the user interacts with, for example changing the company logo and the color scheme, described in Chapter 3: “Customizing Web Pages”. This chapter also describes how you can use your own, custom portal homepage, if you do not wish to use the default page supplied with the IAG.
  - Authentication, described in Chapter 4: “Access Control”.
  - Session settings, such as the maximum number of sessions that can be concurrently open through the trunk, and how you define default and privileged sessions, described in Chapter 5: “Session Settings”.
  - Content Inspection, described in Chapter 6: “Content Inspection”.
  - Application Customization, described in Chapter 7: “Application Customizers”.
  - Optimizing and troubleshooting portal performance, as described in Chapter 8: “Optimizing Portal Performance”.
  - Configuring a High Availability array, as described in Chapter 9: “Configuring the High Availability Array”.
  - Configure the Form Authentication engine. The engine handles HTML login and change password forms sent by the application, as described in Appendix C: “Form Authentication Engine”.

## Chapter 3

# Single Application Sites

In addition to Portal trunks, you can use the Intelligent Application Gateway (IAG) to create two different types of single application trunks: Webmail and Basic Trunks.

- **Webmail trunks** are dedicated trunks for a single Webmail application, and are automatically created with authentication, application customization, and URL inspection rules that are optimized for the specific Webmail application you are running on this trunk.
- **Basic trunks** enable you to establish a one-to-one connection, where one IP address routes to a single application server.

Each trunk is created with a combination of the parameters you enter in the Create New Trunk Wizard, and of default IAG parameters and settings. Once you create a trunk, you can use the Configuration program to edit the trunk.

You configure a Webmail or Basic trunk in the following stages:

- You can optionally use the Service Policy Manager to pre-configure the IAG HTTP Connections and HTTPS Connections services, as described in “Optional Pre-configuration of the Services” on page 52.
- In the Configuration program, you use the Create New Trunk Wizard to create a trunk under either the HTTP Connections or the HTTPS Connections service, as described in “Creating a Webmail or a Basic Trunk” on page 54.
- Options you can configure once the trunk is created are described in “Where To Go From Here” on page 57.



### Note

The first time you access either the Configuration program or the Service Policy Manager, you are required to create an encryption key and passphrase for the IAG. The key and passphrase serve both IAG applications, so that this action is only required once; when you subsequently access either application, you use the same passphrase. Additional information is available as follows:

- For an overview of the encryption mechanism, see “Encryption” on page 21.
- For details on how to create the encryption keys and passphrase, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Creating Encryption Keys” on page 20.

This chapter also describes how you:

- Create a Redirect trunk that will automatically redirect HTTP requests to an HTTPS trunk, as described in “Creating a Redirect Trunk” on page 58.
- Edit an existing trunk, as described in “Editing Trunks” on page 59.

## Optional Pre-configuration of the Services

This section describes how you can optionally pre-configure the HTTP Connections and HTTPS Connections services in the Service Policy Manager. During pre-configuration, you define lists of external websites and application servers that can be used in the configuration of the service; you can pre-configure only one of the services, or both service-types. Subsequently, these are available for selection during trunk creation in the Create New Trunk Wizard, and when editing the trunk in the Configuration program. The parameters you can define include:

- IP addresses and port numbers of the IAG external websites.
- IP addresses and port numbers of the application servers that will be accessed via the IAG.

You pre-configure these parameters separately for the HTTP Connections and the HTTPS Connections services.



### Note

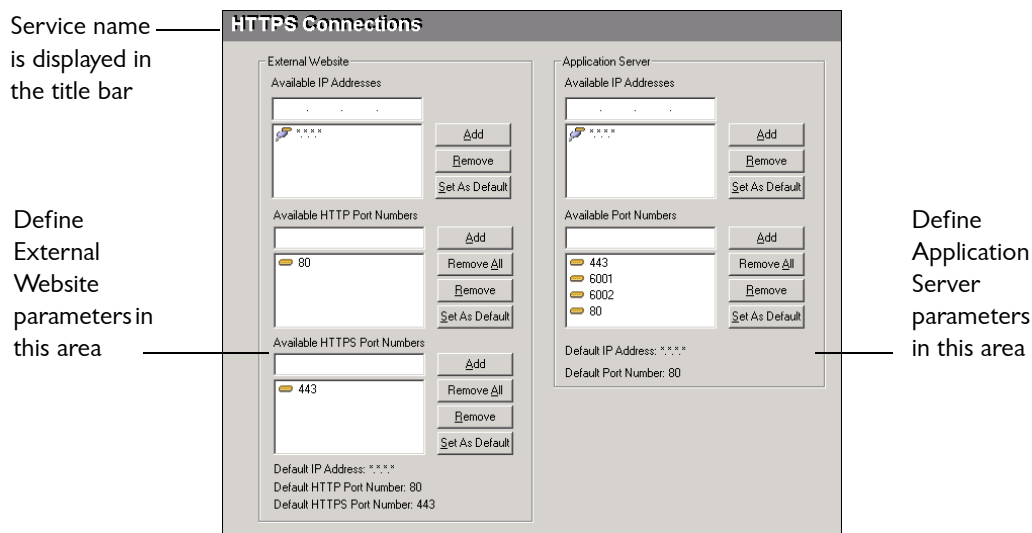
A detailed description of the Service Policy Manager, including detailed procedures, is available in the chapter titled “Security Management Tools” in the *Intelligent Application Gateway Advanced Configuration* guide.


***To pre-configure the services:***

1. At the IAG, click **[Start]**, and then point to **Programs > Whale Communications IAG > Additional Tools > Service Policy Manager**.
2. In the List pane of the Service Policy Manager, click the **+** sign next to **Built-In Services**, and then select the service you wish to configure—HTTP Connections or HTTPS Connections.

*The Configuration pane displays the parameters of the selected service.*

**Figure 3. Service Policy Manager—Configuration Pane**



3. Edit the parameters in the Configuration pane, as described in Table 3 on page 54.
4. When you finish configuring the services in the Service Policy Manager, click  to save and activate the Service Policy Manager configuration file.

*The parameters you defined here are available for selection during trunk creation and configuration in the Configuration program.*

*When the Configuration program is started, it reflects the parameters in the last activated Service Policy Manager configuration file. If the Configuration program is already running, once you activate the Service Policy Manager configuration file and return to the Configuration program, the IAG prompts you to apply the new parameters.*

**Table 3. Pre-configuration Trunk Parameters**

Parameter	Description
Available IP Addresses	Create lists of these IP addresses: <ul style="list-style-type: none"><li>• External Website</li><li>• Application Server</li></ul> <b>Tip:</b> If you want to restrict the list of IP addresses to those entered in the Service Policy Manager, delete the wildcard value: *.*.*.*
Available Port Numbers	Create lists of these port numbers: <ul style="list-style-type: none"><li>• External Website (HTTP and HTTPS)</li><li>• Application Server</li></ul> <b>Tip:</b> You can add a single port or a range of ports.
Default IP Address	Select the IP addresses that will be displayed by default in the Configuration program.
Default Port Numbers	Select the port numbers that will be displayed by default in the Configuration program.

## Creating a Webmail or a Basic Trunk


You create a Webmail or a Basic trunk using the Create New Trunk Wizard in the Configuration program. The trunk can be created under either of the services—HTTP or HTTPS.



### Tip

- You can pre-configure lists of IP addresses and port numbers that you will be able to assign to the services when creating and editing trunks, as described in “Optional Pre-configuration of the Services” on page 52.
- If you create an HTTPS trunk, you can later add a Redirect trunk to automatically direct HTTP requests to that trunk, as described in “Creating a Redirect Trunk” on page 58.
- The Create New Trunk Wizard is also used to create Portal trunks. For a description of Portal trunks, refer to Chapter 2: “SSL VPN Portals”.

**To create a Webmail or a Basic trunk:**

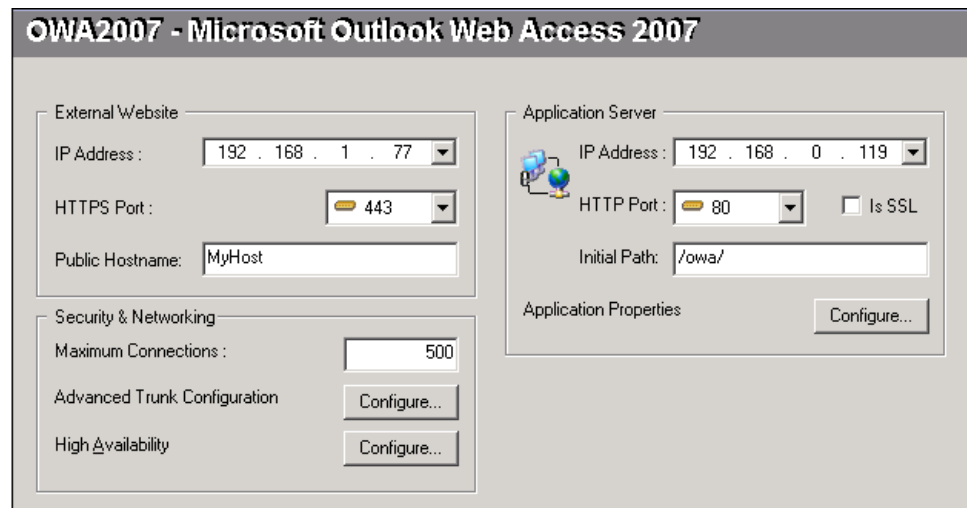
1. At the IAG, in the Windows desktop, click **Start**, and then point to **Programs > Whale Communications IAG > Configuration**.
2. In the List pane, select and right-click **HTTP Connections** or **HTTPS Connections**, and then select **New Trunk**.  
*The Create New Trunk Wizard is displayed.*
3. Depending on the type of trunk you are creating, select **Webmail Trunk** or **Basic Trunk**. Follow the instructions on the screen to complete the wizard; for details, click  [Help](#).



**Note**

When creating Webmail trunks, we recommend that you use the HTTPS Connections service.

4. When you complete the wizard, click **Finish**.  
*The Create New Trunk Wizard closes. The trunk you created now appears in the List pane, and the Configuration pane displays the trunk's parameters. In the following sample screen, a Webmail trunk was created, for the application Microsoft Outlook Web Access 2007.*



**OWA2007 - Microsoft Outlook Web Access 2007**

**External Website**

IP Address : 192 . 168 . 1 . 77

HTTPS Port : 443

Public Hostname: MyHost

**Application Server**

IP Address : 192 . 168 . 0 . 119

HTTP Port : 80 ☐ Is SSL

Initial Path: /owa/


Application Properties [Configure...](#)

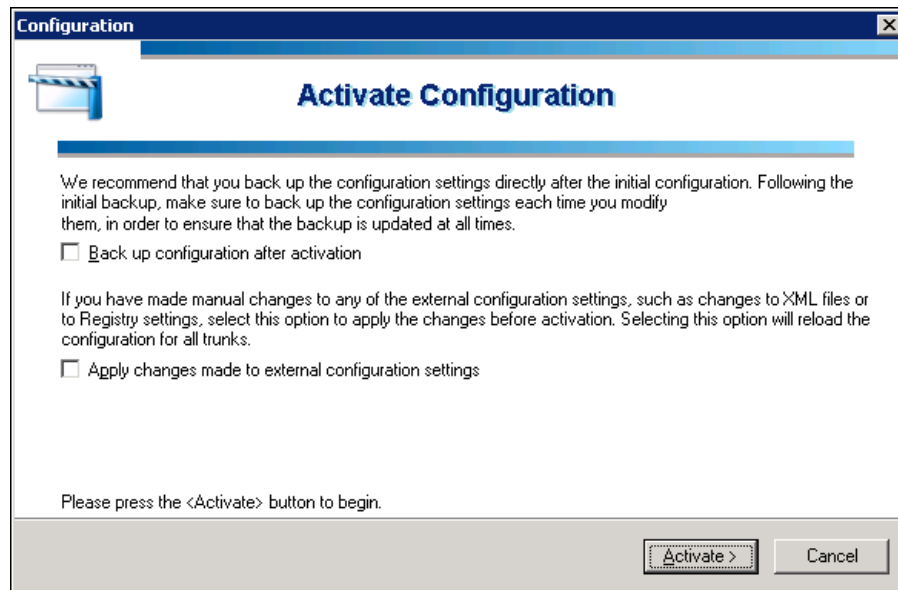
**Security & Networking**

Maximum Connections : 500

Advanced Trunk Configuration [Configure...](#)

High Availability [Configure...](#)

5. In the Configuration program, click  to save and activate the configuration.  
*The following is displayed.*



6. Click **Activate >**.



#### Note

We recommend that you activate the option “Back up configuration after activation”, so that the configuration settings are backed up. For more details, refer to “Backup & Restore Utility” on page 303.

*Once the configuration is activated, the following message is displayed:*

IAG configuration activated successfully.

*HTTP or HTTPS protocols that arrive at the port defined in the trunk will be transferred to and from the application server specified in the configuration. In addition, the Create New Trunk Wizard automatically creates an external website on the Internet Information Services (IIS), in the following location:*

...\Whale-Com\e-Gap\Von\Conf\WebSites\<site\_name>

*Where <site\_name> is the trunk name defined in the Setting the Trunk step in the Create New Trunk Wizard. The website's root folder—root—is created under this folder.*



## Where To Go From Here

Once a trunk is created, you can edit it in the Configuration program. The items you can edit and configure are as follows:

- Options that are described in this chapter include:
  - For HTTPS Connections trunks: creating a Redirect trunk in order to redirect HTTP requests, as described in “Creating a Redirect Trunk” on page 58.
  - Editing general trunk parameters, as described in “Editing Trunks” on page 59.
  - Editing the Server Settings in Webmail trunks that enable Domino iNotes (Single Server) and Domino iNotes (Multiple Servers) applications, as described in “Editing Webmail Trunk Server Settings” on page 64.

Options that are described in other chapters of this Guide include:

- Editing any of the applications’ properties in the Application Properties dialog box, as described in “Editing Application Properties” on page 67.
- Changing the event logging definitions, as described in “Event Logging” on page 237.
- Enabling access to the Web Monitor, as described in “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.
- Additional options are described in the *Intelligent Application Gateway Advanced Configuration* guide, including:
  - Customizing the look-and-feel and other aspects of the HTML pages the user interacts with, for example, changing the company logo and the color scheme, described in Chapter 3: “Customizing Web Pages”.
  - Authentication, Server Name Translation, and Initial Host Selection, described in Chapter 4: “Access Control”.
  - Session settings, such as the maximum number of sessions that can be concurrently open through the trunk, and how you define default and privileged sessions, described in Chapter 5: “Session Settings”.
  - Content Inspection, described in Chapter 6: “Content Inspection”.
  - Application Customization, described in Chapter 7: “Application Customizers”.
  - Configuring a High Availability array, as described in Chapter 9: “Configuring the High Availability Array”.

- Configuring the Form Authentication engine. The engine handles HTML login and change password forms sent by the application, as described in Appendix C: “Form Authentication Engine”.



#### Note

You can delete a trunk in the Configuration program by selecting the trunk in the List pane and selecting **Delete** from the right-click menu.

## Creating a Redirect Trunk

When you create an HTTPS trunk, only HTTPS requests that arrive at the IAG are handled by the trunk. If you want the IAG to automatically redirect HTTP requests to the HTTPS trunk, you can create an additional Redirect trunk, as described in the following procedure.

Before you create a Redirect trunk, please note the following:

- Make sure that you have already created the HTTPS trunk to which you wish to redirect HTTP requests:
  - For Webmail and Basic trunks, see “Creating a Webmail or a Basic Trunk” on page 54.
  - For Portal trunks, refer to Chapter 2: “SSL VPN Portals”.

Make sure to complete the definition of all the parameters of the HTTPS Connections trunk before you create the Redirect trunk, including definitions you make in the Configuration program after completing the New Trunk Wizard.

- If at a later stage you change the IP address or port number of the HTTPS Connections trunk, do one of the following:
  - Update the IP address/port number manually in the relevant Redirect trunk.
  - Delete the existing Redirect trunk and create a new one.
- Redirect trunks are not monitored by the Web Monitor.
- Sessions in Redirect trunks are not calculated in the session count of the IAG. When an HTTP session is redirected to HTTPS via a Redirect trunk, it is only counted as one HTTPS session.

#### **To create a Redirect trunk:**

1. In the List pane of the Configuration program, select and right-click **HTTP Connections**, and then select **New Trunk**.  
*The Create New Trunk Wizard is displayed.*
2. Select **Redirect HTTP to HTTPS Trunk** and click **Next >**.  
*All HTTPS trunks for which no Redirect trunk exists are listed.*

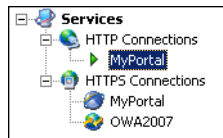
3. Select the HTTPS trunk to which you wish to redirect HTTP requests, and then click **Finish**.



#### Tip

For additional details, click  [Help](#) in any of the wizard screens.

*A new trunk with the same name as the HTTPS trunk you selected is created in the List Pane.*



*HTTP requests that arrive at the external website that is defined for this trunk are redirected to the HTTPS trunk you selected in the wizard.*

## Editing Trunks

Once you create a trunk with the Create New Trunk Wizard, the trunk values you defined in the wizard, and other IAG default values, are visible in the various fields of the Configuration program. This section describes the parameters that are visible and can be edited in two places:

- The main window of the Configuration program, as described in “Editing in the Configuration Pane” on page 59.
- The General tab of the Advanced Trunk Configuration window, as described in “Editing in the General Tab” on page 61.

### Editing in the Configuration Pane




#### Note

This section applies to Webmail and Basic trunks only; Portal trunks are described in Chapter 2: “SSL VPN Portals”.

This section describes the parameters that you can edit in the main pane of the Configuration program, as illustrated in Figure 4 on page 60. The fields are identical in both Basic and Webmail trunks, as described in Table 4 on page 60.



### Note

Once you finish editing the required parameters, click  to save and activate the configuration.

**Figure 4. Configuration Pane of an Outlook Web Access Webmail Trunk**

**OWA2007 - Microsoft Outlook Web Access 2007**

**External Website**

IP Address : 192 . 168 . 1 . 77

HTTPS Port : 443

Public Hostname: MyHost

**Application Server**

IP Address : 192 . 168 . 0 . 119

HTTP Port : 80 ☐ Is SSL

Initial Path: /owa/

**Security & Networking**

Maximum Connections : 500

Advanced Trunk Configuration [Configure...](#)

High Availability [Configure...](#)

**Application Properties** [Configure...](#)

**Table 4. Configuration Pane Parameters—Webmail and Basic Trunks**

Parameter	Description
IP Addresses*	<ul style="list-style-type: none"><li>External Website—IP address of the external website.</li><li>Application Server—IP address of the application server.</li></ul>
Ports*	<ul style="list-style-type: none"><li>External Website—port number of the external website. The type of port (HTTP or HTTPS) that is displayed and that can be edited here depends on the connection type. <b>Note:</b> The other port of the external website can be edited in the General tab of the Advanced Trunk Configuration window. For example, for an HTTP Connections trunk, the HTTP port is displayed and can be edited here, while the HTTPS port is displayed and can be edited only in the General tab of the Advanced Trunk Configuration window.</li><li>Application Server—HTTP port of the application server.</li></ul>

**Table 4. Configuration Pane Parameters—Webmail and Basic Trunks (Cont'd)**

Parameter	Description
Public Hostname*	Optional—applicable only if the application is accessed via a hostname.  The host through which remote users access the application enabled in this trunk (external website). You can enter either a domain name (effective hostname) or an IP address.
Maximum Connections	Maximal number of simultaneous connections that are permitted for this trunk.  Default: 500
Initial Path	Path of the application on the application server, as follows: <ul style="list-style-type: none"><li>• Basic trunks—required only if the application is not located in the root folder. For example, if the application is located under a subfolder named “MyApplication”, enter /MyApplication/ in this field.</li><li>• Webmail trunks—by default, the default installation path of the application, for example /exchange/ for Microsoft Outlook Web Access applications. If the application resides under a different path, change this field accordingly.</li></ul>

\* This parameter is defined during the creation of the trunk with the Create New Trunk Wizard.

## Editing in the General Tab

This section describes the parameters that you can edit in the General tab of the Advanced Configuration window, as illustrated in Figure 5 on page 62.

### *To edit parameters in the General tab:*

1. In the Configuration program, select the trunk in the List pane.
2. In the “Security & Networking” area, next to “Advanced Trunk Configuration”, click **Configure...**.

*The Advanced Trunk Configuration window is displayed.*

**Figure 5. Advanced Trunk Configuration—General Tab**

Advanced Trunk Configuration [OWA2007]

Server Name Translation | URL Inspection | Global URL Settings | URL Set

General | Authentication | Session | Application Customization

External Website

IP Address : 192 . 168 . 1 . 77

HTTP Port: 80

HTTPS Port: 443

Site Name : owa2007

Website Logging

☐ Enable Web Server Logging

☐ Include Username in Log

Debugging

☐ Debug Mode


Server Certificate

Server Certificate: edinburgh6

Certificate Hash: 85 A6 EA 9A 47 C4 9C 24 F4 68 7B 12 C0 62 C5 15 86 F4 CE 39

The Server Certificate parameters are applicable in HTTPS Connections trunks only; they do not appear in this tab in HTTP Connections trunks.

OK Cancel

3. Edit the parameters in the General tab as required, as described in “Advanced Trunk Configuration—General Tab” on page 63.
4. When you complete editing all the required options for the filter, click **OK**.  
*The Advanced Trunk Configuration window closes and you are returned to the main window of the Configuration program.*
5. In the main window of the Configuration program, click  to save and activate the configuration.  
*The trunk will function according to the configured settings.*

**Table 5. Advanced Trunk Configuration—General Tab**

Parameter	Description
IP Address*	(Read-only) IP address of the external website, on the IAG. <b>Tip:</b> You can edit the IP address of the external website in the main Configuration window.
HTTP/HTTPS Ports*	HTTP and HTTPS ports of the external website. <b>Note:</b> The port that corresponds with the Connections type of this trunk cannot be edited here. You edit it in the main Configuration window. For example, for an HTTP Connections trunk, you edit the HTTPS port here, and you edit the HTTP port in the main Configuration window. <b>Note:</b> <ul style="list-style-type: none"><li>Both HTTP and HTTPS ports are displayed in the General tab, since you can use the same IP address for two trunks sharing the same site name, one for HTTP sessions, and the other for HTTPS sessions.</li><li>Sites with the same IP address must have matching site names; sites with different IP addresses must have unique site names.</li></ul>
Site Name	Name of the external website folder; determined by the trunk name as defined in the Create New Trunk Wizard.
Enable Web Server Logging	Enable this option if you wish the IIS to record a log of the transactions through the trunk, including the source IP addresses. The log is created in the location that is defined in the Microsoft Management Console (MMC), in the filter site Properties dialog box, under the Web Site tab.
Include Username in Log	Select whether to add the username, which the user enters during login, to the IIS log you enabled in Enable Web Server Logging, above.
Debug Mode	This option disables all of the trunk's security features. <b>Caution:</b> This mode is intended for use only when so instructed by technical support. Whenever you use this option, be sure to disable it when you finish debugging the trunk.

**Table 5. Advanced Trunk Configuration—General Tab (Cont'd)**

Parameter	Description
Server Certificate (HTTPS Connections trunks only)*	Server certificate used for the external website. The certificate that is displayed here is selected during trunk configuration; you can use the drop-down list to select any of the certificates listed in the Certificate store installed on the IIS, on the default website.
Certificate Hash (HTTPS Connections trunks only)	Unique ID of the selected Server Certificate (displayed automatically).

\* This parameter is defined during the creation of the trunk with the Create New Trunk Wizard.

## Editing Webmail Trunk Server Settings



### Note

This section is only applicable for Webmail trunks that enable access to Domino iNotes (Single Server) and Domino iNotes (Multiple Servers) applications.

You initially configure the server settings for Domino iNotes applications when you create the trunk, in the Create New Trunk Wizard. In Webmail trunks, any time after the initial configuration, you can edit these settings in the Advanced Trunk Configuration window, in the Server Settings tab:

- The Server Settings tab of the Domino iNotes (Single Server) application is described on page 65.
- The Server Settings tab of the Domino iNotes (Multiple Servers) application is described on page 66.



## Domino iNotes (Single Server)

Figure 6. Server Settings Tab—Domino iNotes (Single Server)

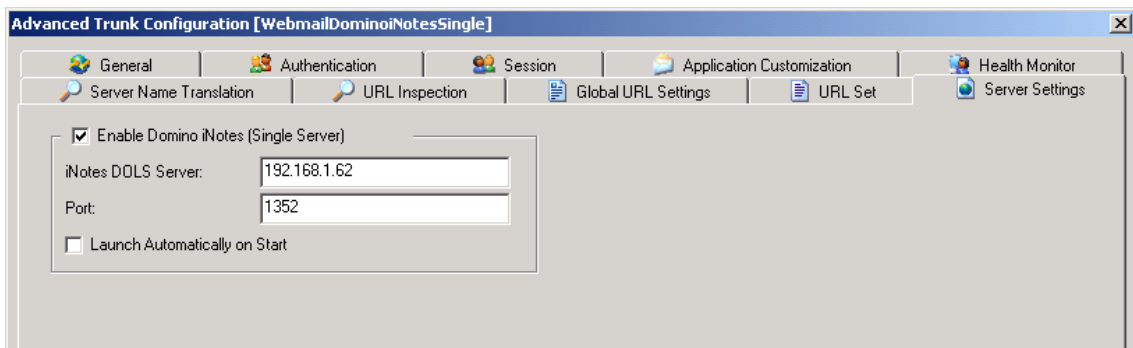


Table 6. Server Settings Parameters—Domino iNotes (Single Server)

Parameter	Description
Enable Domino iNotes (Single Server)	Enables offline access to Domino iNotes.
iNotes DOLS Server	Hostname or IP address of the DOLS server. We recommend that you use a hostname. <b>Note:</b> If you use a hostname to define the application, use the effective hostname as defined in the Domain Name System (DNS).
Port	Port number of the DOLS server.
Launch Automatically on Start	Automatically launches the SSL Wrapper to enable the operation of the Lotus® iNotes™ Sync Manager on the computer. For details, refer to Chapter 6: “SSL Wrapper”.

# Domino iNotes (Multiple Servers)

Figure 7. Server Settings Tab—Domino iNotes (Multiple Servers)

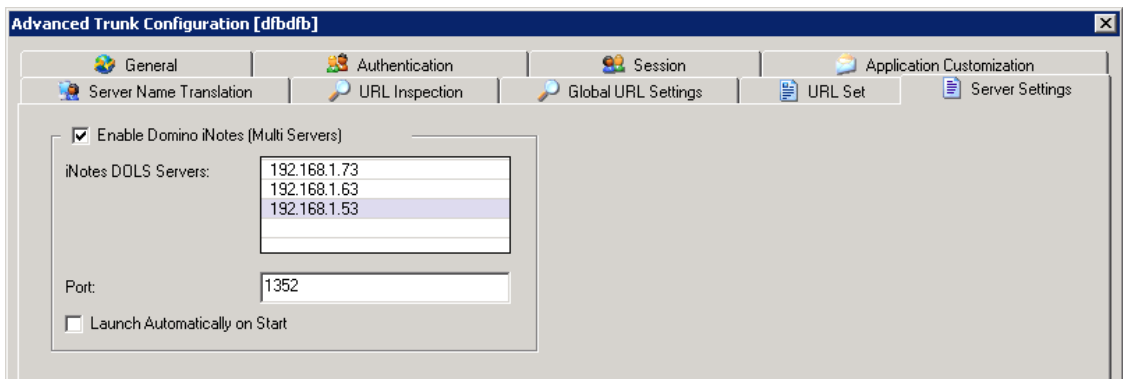


Table 7. Server Settings Parameters—Domino iNotes (Multiple Servers)

Parameter	Description
Enable Domino iNotes (Multi Servers)	Enables offline access to Domino iNotes.
iNotes DOLS Servers	Hostnames or IP addresses of the DOLS servers. We recommend that you use hostnames. <b>Note:</b> If you use a hostname to define an application, use the effective hostname as defined in the DNS.
Port	Port of the DOLS servers.
Launch Automatically on Start	Automatically launches the SSL Wrapper to enable the operation of the Lotus iNotes Sync Manager on the computer. For details, refer to Chapter 6: “SSL Wrapper”.

## Chapter 4

# Application Settings

The settings of an application depend on the following:

- Application type. The Application Aware approach of the Intelligent Application Gateway (IAG) provides application-specific out-of-the-box optimization for the supported applications, including features such as URL Inspection rulesets and character definitions, deleting application-specific folders and cookies, and more.
- Application properties. You select some of the application properties while configuring the application for access via the SSL VPN portal, or while creating a Webmail or Basic trunk, whereas others are automatically applied by the IAG. You can change application properties for each of your applications individually, via the Application Properties dialog box.

This chapter describes how you can later edit the application properties, as described in “Editing Application Properties” on page 67. It also describes how you can quickly create a new application based on an existing application, in “Duplicating an Application” on page 91.

## Editing Application Properties

This section describes how you can edit application properties in the Application Properties dialog box, including:

- “Accessing the Application Properties Dialog Box” on page 68
- “General Tab” on page 68
- “Web Servers Tab” on page 71
- “Web Settings Tab” on page 73
- “Web Server Security Tab” on page 78
- “Cookie Encryption Tab” on page 80
- “Download/Upload Tab” on page 82
- “Server Settings Tab” on page 85
- “Client Settings Tab” on page 86
- “Portal Link Tab” on page 87
- “Authorization Tab” on page 91



### Note

The tabs and parameters that are available in the dialog box vary, according to the application type.

## Accessing the Application Properties Dialog Box

This section describes how you access the Application Properties dialog box after you add an application to the portal or create a Webmail or Basic trunk.

### *To access the Application Properties dialog box:*

- In Portal trunks:  
In the main window of the Configuration program, in the “Applications” area, select and double-click the application whose properties you wish to edit;  
  
Or,  
Select the application and click **Edit...** below the Application list.  
*The Application Properties dialog box is displayed. It is described in the following sections.*
- In Webmail or Basic trunks:  
In the main window of the Configuration program, in the “Application Server” area, click **Configure...** next to “Application Properties”.  
*The Application Properties dialog box is displayed. It is described in the following sections.*

## General Tab

In the General tab you can:

- Change the application name.
- Copy the Application ID number.
- In portal trunks only: select prerequisite applications, that is, one or more applications that must be active in order for the application you are configuring here to run. **For example:** if the application you define here requires connection to an internal share, add a Local Drive Mapping application that will map the required drive, and define it to be a prerequisite application to the application you are configuring here.

Only applications of the type Client/Server and Legacy Applications can serve as prerequisite applications. All applications of this type that are defined in the portal’s Applications list are available for selection in the Prerequisite Applications list.



### Tip

the number of applications that are defined as prerequisites to the current application is indicated below the application list, in the “Number of Prerequisite Applications” field.

To define an application as a prerequisite, enable it in the Prerequisite Applications list. If an application that is defined as a prerequisite application is not launched when the user attempts to access the application you define here, the IAG automatically launches the prerequisite application prior to launching this application.

- Define the application’s inactivity period, in order to monitor the actual usage of the application. When a user does not use the application for the period of time defined here, an “Application Exited” message is sent to the Web Monitor. When the user resumes using the application, an “Application Accessed” message is sent to the Web Monitor. The user experience, however, is unaffected.

If the “Inactivity Period” field is set to zero, inactivity period is unlimited, that is, the application is only exited when the user’s session with the portal ends.

- Change the selection of the application Endpoint Policies, and access the Policy Editor. For details, refer to “Application Endpoint Policies” on page 99.




### Note

The “Endpoint Policies” area is disabled when the option “Disable Component Installation and Activation”, in the Session tab of the Advanced Trunk Configuration window, is activated, since endpoint computers’ compliance to the policies cannot be detected.

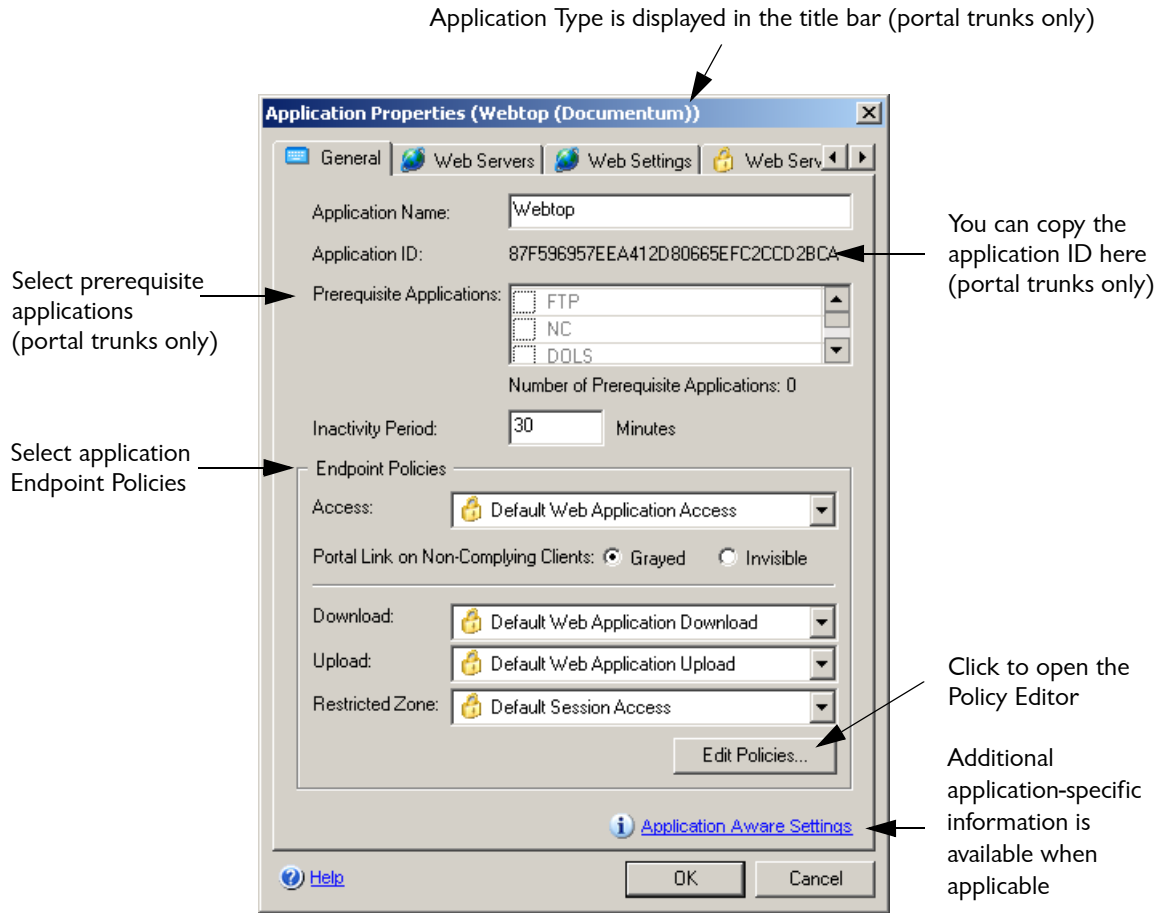
- Access additional application-specific settings or information.



### Note

The  [Application Aware Settings](#) link appears when there are application-specific settings or information for the selected application. For information about other relevant applications, see the *Intelligent Application Gateway Application Aware Settings* guide.

**Figure 8. Application Properties—Sample General Tab**



**Tip**

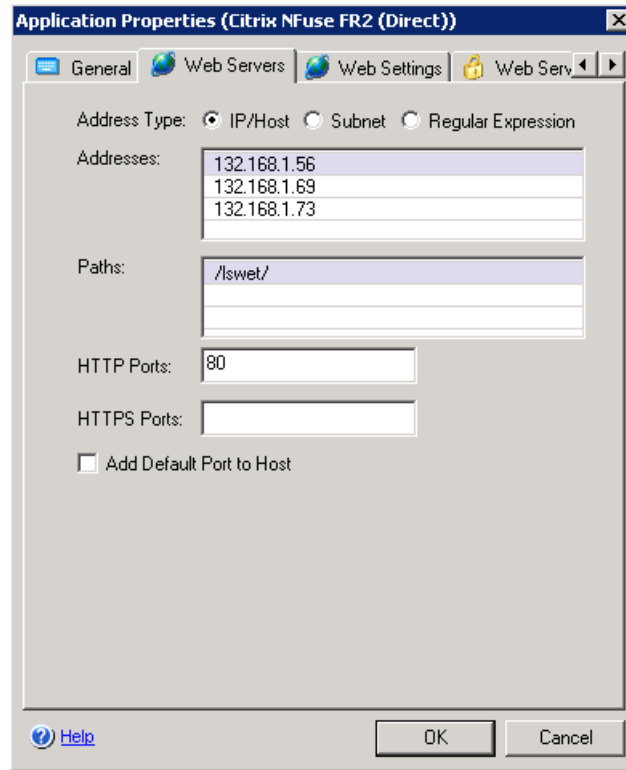
For Web and Browser-Embedded Applications:

- The method by which the IAG identifies URLs, in order to enforce the application's Upload and Download policies, is defined in the Download/Upload tab, described on page 82.
- The Restricted Zone option is activated in the Web Settings tab, described on page 73.

## Web Servers Tab

This tab is available in Portal trunks only, for Built-In Services, Web Applications, and Browser-Embedded Applications. It contains the configuration of the application's web server or servers. The parameters of this tab are described in Table 8 on page 71.

**Figure 9. Application Properties—Web Servers Tab**



**Table 8. Web Servers Tab Parameters**

Parameter	Description
Address Type	Select a method by which to define the address of the application server: IP/Host, Subnet, or Regular Expression.

**Table 8. Web Servers Tab Parameters (Cont'd)**

Parameter	Description
IP/Host	<p>Define an address or multiple addresses using IP addresses or hostnames, by double-clicking an empty line in the “Addresses” list and entering an IP address or hostname for each server.</p> <p><b>Note:</b> If you define an address using a hostname, use the effective hostname as defined in the DNS.</p>
Subnet	<p>Define multiple addresses using a subnet by entering subnet address and subnet mask in the respective fields.</p>
Regular Expression	<p>Define multiple addresses using the Regex++ regular expression syntax, by entering a regular expression that defines the address-range in the “Addresses” field.</p> <p><b>For example:</b> <code>[0-9A-Z-]+\.\whale\.</code></p>
Paths	<p>Define one or more paths on which the application resides by double-clicking an empty line and entering a path.</p> <p><b>Note:</b> A path must start with a slash.</p>
HTTP Ports HTTPS Ports	<p>HTTP and HTTPS port or ports.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Enter <code>Auto</code> to use the default port</li> <li>• Enter <code>All</code> to enable all ports</li> <li>• Leave the field empty to block all ports</li> <li>• Multiple port entries are comma-separated: <code>81,82,85,86</code></li> <li>• Define a range of ports with a dash: <code>81-86</code></li> </ul>
Add Default Port to Host	<p>Include the default port number (80 or 443) in the host header. Activate this option only if it is required by the server.</p>

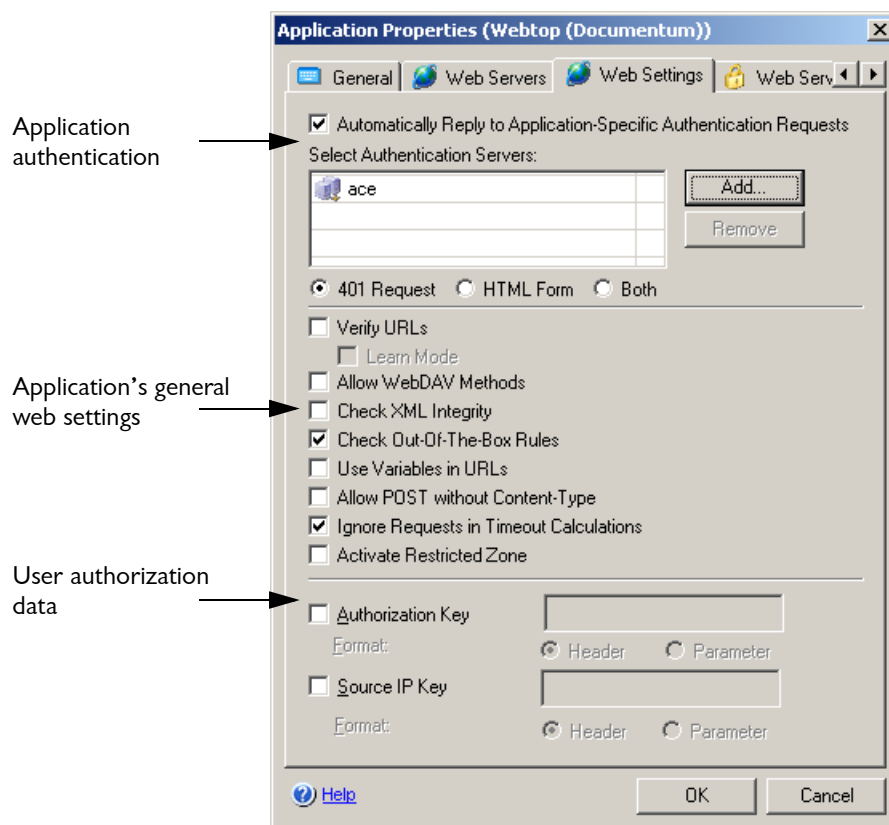


## Web Settings Tab

This tab is applicable in Portal trunks for Built-In Services, Web Applications, and Browser-Embedded Applications, and in Webmail and Basic trunks. It contains the application's web settings, as follows:

- Application authentication, described in “Application Authentication” on page 74.
- General web settings of the application are described in “General Web Settings” on page 75.
- User authorization data, described in “User Authorization Data” on page 77.

**Figure 10. Application Properties—Web Settings Tab**



## Application Authentication

This portion of the Web Settings tab is only relevant for applications that request users to authenticate. It defines how to authenticate against the application server, as described in Table 9 on page 74.

**Table 9. Web Settings Tab—Application Authentication**

Parameter	Description
Automatically Reply to Application-Specific Authentication Requests	Reply to the application authentication requests with user credentials.  When this option is activated, once users enter a set of credentials that is valid for the application, for example during the initial login, they do not have to authenticate again, against the application server. If the authentication data is not received by the application server, the session is deemed unauthenticated and access is denied.
Select Authentication Servers	Select a server or number of servers, that will be used for authentication against the application when users access the application.
401 Request	Select this option if the application requires users to authenticate using HTTP 401 requests.
HTML Form	Select this option if the application requires users to authenticate using an HTML form. *
Both	Select this option if the application might require users to authenticate using both HTTP 401 requests and HTML forms. *

\* The Form Authentication Engine handles HTML authentication forms. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to Appendix C: “Form Authentication Engine”.

### ***To add a server to the list of authentication servers:***

1. Double-click anywhere in the “Select Authentication Servers” list, or click **Add...**.  
*The Authentication and User/Group Servers dialog box is displayed.*
2. For instructions on how to use the Authentication and User/Group Servers dialog box, click **Help**.

## General Web Settings

General web settings of the application are described in Table 10 on page 75.

**Table 10. Web Settings Tab—General Web Settings**

Parameter	Description
Verify URLs	<p>When this option is activated, URL requests from the application are inspected against the URL Inspection rules of this application-type, as defined in the URL Set tab of the Advanced Trunk Configuration window.</p> <p>For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.</p> <p><b>Note:</b> Disabling this option disables URL inspection at the application level, and affects this application only. Also, requests from this application will still be checked against the general rules, such as the Internal Site rules. If you wish to disable URL inspection altogether, you need to set the IAG to Debug mode, in the General tab of the Advanced Trunk Configuration window.</p>
Learn Mode	<p>When this option is activated, URL requests from the application are inspected against the URL Inspection rules of this application-type, but the rules are not enforced. That is, if a request is not accepted by one of the application rules, the failure is logged in the Security log, and the request is allowed.</p>
Allow WebDAV Methods	<p>Allow browsers to send HTTP data to the application in requests that use WebDAV methods.</p>
Check XML Integrity	<p>Inspect XML integrity in HTTP data.</p>
Check Out-Of-The-Box Rules	<p>Check URLs against the application’s Out-Of-The-Box Rules, as defined in the URL Inspection tab of the Advanced Trunk Configuration window.</p> <p>For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to “Configuration in the URL Inspection Tab” on page 143.</p>

**Table 10. Web Settings Tab—General Web Settings (Cont'd)**

Parameter	Description
Use Variables in URLs	<p>Activate this option if any of the application's URLs use variables.</p> <p>For a description of how you use variables in URLs, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to "Using Variables in URLs" on page 173.</p>
Allow POST without Content-Type	<p>Indicates whether POST requests without a "Content-Type" header are handled or rejected.</p>
Ignore Requests in Timeout Calculations	<p>For each out-of-the-box application-type, the IAG automatically configures a list of Application Aware URLs that are ignored in the calculation of the Inactive Session Timeout, when this option is activated.</p> <p>You can access and edit the list via the Global URL Settings tab of the Advanced Trunk Configuration window. For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to "Ignoring URL Requests in Inactive Session Timeout Calculations" on page 162.</p>
Activate Restricted Zone	<p>Activate this option if you wish to restrict users' access to sensitive areas of the application, such as administrative areas, unless their computer meets the requirements of the Restricted Zone endpoint policy. Once you activate this option, make sure you also:</p> <ul style="list-style-type: none"><li>• Define the required Restricted Zone policy for the application. For details, refer to "Application Endpoint Policies" on page 99.</li><li>• Define the application's Restricted Zone URLs, in the Global URL Settings tab of the Advanced Trunk Configuration window. For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to "Global URL Settings Tab—URL Settings" on page 152.</li></ul>

## User Authorization Data

Use the “User Authorization Data” area of the Web Settings tab to configure the IAG to send data regarding the originator of the connection request to the application server. User Authorization Data parameters are described in Table 11 on page 77.

**Table 11. Web Settings Tab—User Authorization Data**

Parameter	Description
Authorization Key	Name of the header or parameter that the IAG uses to send the data to the application server. If you activate this option, you also have to configure the value of the Authorization Key header or parameter, which will be sent to the application server. For details, refer to “Configuring Authorization Key Value” on page 78.
Format	Select the format in which the IAG will send the Authorization Key to the application server: <ul style="list-style-type: none"><li>• Header: as an HTTP header</li><li>• Parameter: as part of the URL query string</li></ul>
Source IP Key	Name of the header or parameter that the IAG uses to send the IP address of the originator of the connection request to the application server.
Format	Select the format in which the IAG will send the Source IP Key to the application server: <ul style="list-style-type: none"><li>• Header: as an HTTP header</li><li>• Parameter: as part of the URL query string</li></ul>



### Tip

If a request contains a header or parameter with an identical name to a header or parameter you define here, it is blocked, since it is identified as a suspected attempt to sneak data to the application server. Therefore, make sure you assign the headers or parameters you define here unique names, that will not be used for any other purpose.

## Configuring Authorization Key Value

This section describes how you configure the value of the Authorization Key header or parameter, which will be sent to the application server, when you activate the option “Authorization Key” in the Web Settings tab.

### *To configure the value of Authorization Key:*

1. Access the following custom folder; if it does not exist, create it:  
...\\Whale-Com\\e-Gap\\von\\InternalSite\\inc\\CustomUpdate
2. Under the customUpdate folder, create an inc “hook” as follows:  
`<Trunk_Name><Secure(0=no/1=yes)>PostPostValidate.inc`

#### **For example:**

For an HTTPS trunk named “WhalePortal”, create the file:

WhalePortal1PostPostValidate.inc



#### **Tip**

If a file by this name already exists, you can use the existing file; you do not need to create a new file in this case.

3. In the file you defined in step 2, add the following lines:

```
<%  
SetSessionResourceParam g_cookie,  
"<Application_ID>","RWSAuthorization","<Value>"  
%>
```

Where:

- Application\_ID is the application’s ID number, as can be copied from the General tab of the Application Properties dialog box.
- Value is the value you wish to send to the application server

#### **For example**

To send a User\_group: unlimited header:

- In the Web Settings tab, name the Authorization Key User\_group and select the format “Header”
- In WhalePortal1PostPostValidate.inc, enter the value unlimited

## Web Server Security Tab

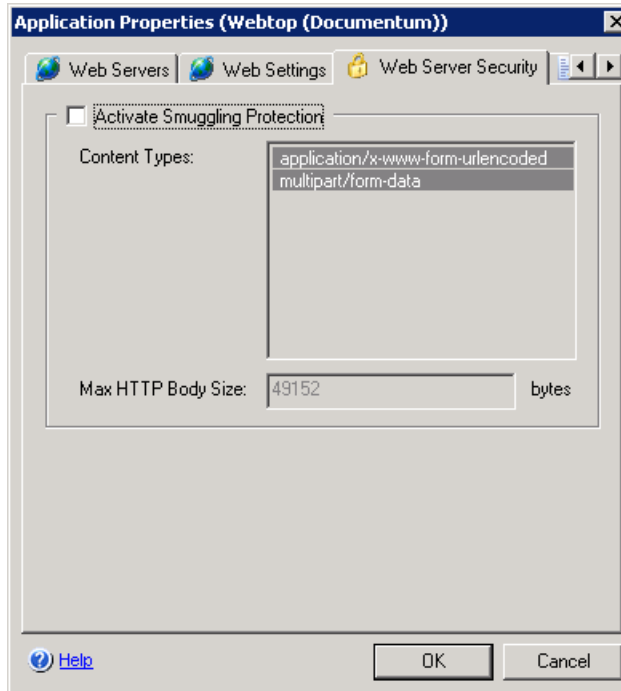


#### **Note**

This tab is not applicable for Client/Server and Legacy applications.

Use this tab to protect the application against HTTP Request Smuggling (HRS) attacks.

**Figure II. Application Properties–Web Server Security Tab**



**Table 12. Web Server Security Tab Parameters**

Parameter	Description
Activate Smuggling Protection	<p>Activating this option protects the application against HTTP Request Smuggling attacks by blocking requests where the following conditions prevail:</p> <ul style="list-style-type: none"> <li>• The method is POST.</li> <li>• The content-type is not listed in the content-type list</li> <li>• The length is larger than the size defined here, or both.</li> </ul> <p><b>Caution:</b> Activate this option only for servers that are vulnerable to HRS attacks, such as IIS 5.0 based servers. Activating this option unnecessarily or configuring it inaccurately might result in application malfunction.</p>
Content-Types	POST requests of a content-type other than the types listed here are blocked if they are larger than the size defined in “Max HTTP Body Size”.
Max HTTP Body Size	POST requests of a size larger than defined here are blocked if they are not listed in the “Content-Types” list.

## Cookie Encryption Tab

This tab is applicable in Portal trunks only, for Web Applications and Browser-Embedded Applications. You can use it to encrypt the application server's "Set-Cookie" headers, in order to hide cookie names and values, and protect them against unauthorized changes.



### Note

Once a cookie is encrypted, it cannot be manipulated by the application customizers' <HEADER\_CHANGE> element. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide:

- Application customizers are described in Chapter 7: "Application Customizers".
- The <HEADER\_CHANGE> element is described on page 234 of the guide.

Once you enable cookie encryption for an application, the IAG applies the encryption of "Set-Cookie" headers in one of two modes:

- **Exclude mode:** all "Set-Cookie" headers are encrypted, except for the cookies that are listed in the cookie lists, including both global and per-application lists.
- **Include mode:** only headers that are listed in the cookie list are encrypted. The list is applied per-application only.

Encrypted cookie names and values are decrypted by the IAG when they are returned by the browser in the "Cookie" header. If the cookie encryption process encounters problems when a remote user requests a page, the "Cookie" header in the request is blocked, and is not forwarded to the server. The request is processed, however, and the user experience is unaffected. In this case, a Warning message is reported in the Web Monitor, in the Event Viewer.



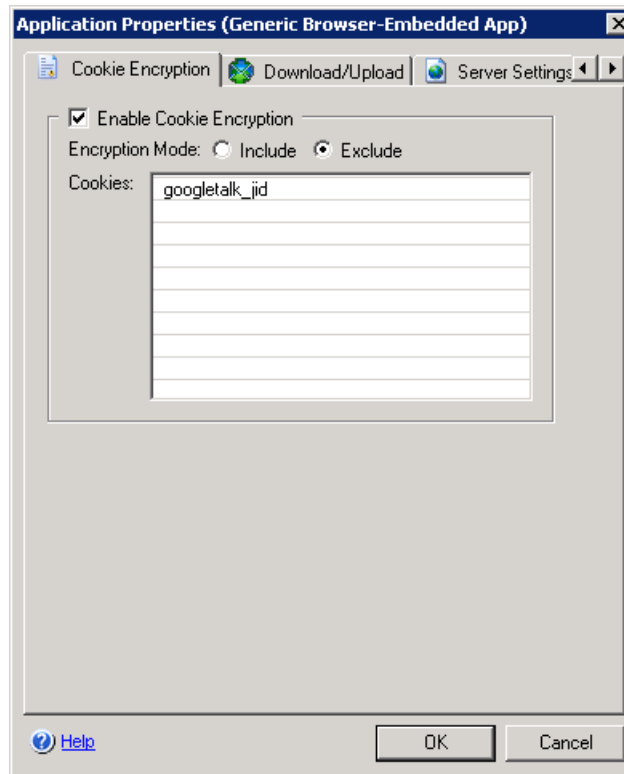
### Tip

Click the ID number of a message to view troubleshooting information. You can also access this information in Appendix A: "Troubleshooting Event Logging Messages", messages #94–101.

You enable cookie encryption, select the encryption mode, and configure the per-application cookie list in the Cookie Encryption tab, as described in Table 13 on page 81. For a description of the global exclude list, see "Global Exclude List" on page 82.



**Figure 12. Application Properties–Cookie Encryption Tab**



**Table 13. Cookie Encryption Tab Parameters**

Parameter	Description
Enable Cookie Encryption	Enables the Cookie Encryption option for the application.
Encryption Mode	<ul style="list-style-type: none"><li>• Exclude: all cookies are encrypted, except for those listed in the per-application cookie list and the global exclude list.</li><li>• Include: only cookies that are listed in the per-application cookie list are included in the encryption process.</li></ul>
Cookies	<p>Cookie list:</p> <ul style="list-style-type: none"><li>• In an “Exclude” encryption mode, per-application list of cookies that are excluded from the encryption process.</li><li>• In an “Include” encryption mode, per-application list of cookies that are included in the encryption process.</li></ul>

## Global Exclude List

The global list includes cookies that are excluded from the cookie encryption process of all the applications where the encryption mode is “Exclude”. You can add cookies to the list as required.



### Caution

Do not delete any of the cookies that are configured in the list by default.

### To edit the global exclude list:

1. Access the following file:  
`...\Whale-Com\e-Gap\Von\Conf\WhlExcludeCookie.xml`
2. Copy the file you accessed in step 1 into the following custom folder; if the folder does not exist, create it:  
`...\Whale-Com\e-Gap\Von\Conf\CustomUpdate`  
If such a file already exists, use the existing file.
3. In the file under the CustomUpdate folder, edit the cookie list under the tag `<EXCLUDE_COOKIE_LIST>`. Note that cookie names are defined using regular expressions; for details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to Appendix B: “Regex++, Regular Expression Syntax”.
4. In addition to the cookie list, the file `WhlExcludeCookie.xml` stores a security prefix that is used in the encryption of cookie names and cookie values, in the tag “SECURITY\_PREFIX”. By default, the value of the security prefix is “ce”. If required, you can change the value of the prefix in the file in the custom folder.

## Download/Upload Tab

This tab is applicable in Portal trunks for Built-In Services, Web Applications, and Browser-Embedded Applications, and in Basic trunks. It defines the method by which the IAG identifies URLs, in order to enforce the application’s Upload and Download policies.

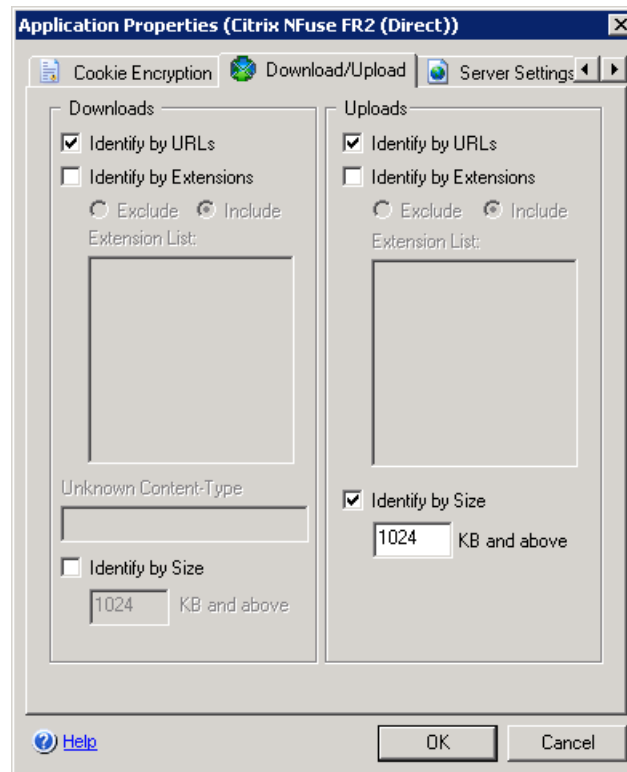


### Note

- If none of the options in the Download/Upload Tab are activated, no uploads or downloads to and from the application are blocked, regardless of the settings of the application’s Upload or Download policies.
- The application’s policies are defined in the General tab, described in “General Tab” on page 68.
- Configuration of the actual policies is described in “Application Endpoint Policies” on page 99.

The parameters of the Download/Upload tab are described in Table 14 on page 84.

**Figure 13. Application Properties—Download/Upload Tab**



**Tip**

By default, the IAG identifies responses without content-type as downloads. If you wish downloads without content-type to be considered regular responses, and not downloads, create the following registry key on the IAG:

- Location: ...\\WhaleCom\\e-Gap\\Von\\UrlFilter
- DWORD Value name: AllowResponseWithoutContentType
- DWORD Value data: 1

After you create the key, access the Configuration program, activate the configuration, and select the option “Apply changes made to external configuration settings”.

**Table 14. Download/Upload Tab Parameters**

Parameter	Description
Identify by URLs	<p>Identify URLs and methods by checking against the list of Download URLs or Upload URLs, respectively.</p> <p>You can access and edit the Download URLs and Upload URLs lists via the Global URL Settings tab of the Advanced Trunk Configuration window. For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to “Global URL Settings Tab—URL Settings” on page 152.</p>
Identify by Extensions	<p>Identify URLs by file extensions, which you define in “Extension List”.</p> <ul style="list-style-type: none"><li>• If the option “Exclude” is selected, when an endpoint policy is enforced, only files whose extensions are listed here are allowed</li><li>• If the option “Include” is selected, when an endpoint policy is enforced, files whose extensions are listed here are blocked</li></ul> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• Extensions in the Extension List should not include the preceding dot. For example: <code>exe</code> and not <code>.exe</code></li><li>• You can define that downloading or uploading of files without an extension is allowed or blocked by adding a <code>no_ext</code> entry in the relevant Extension List</li><li>• GET requests are treated as downloads; POST and PUT requests are treated as uploads</li><li>• In order to enable download blocking by extension, you need to also define the application’s unknown content-type, in the field “Unknown Content-Type”, below</li><li>• For the extensions in the list, verify that the association of extensions and content-types is identical between the IAG and the application server. At the IAG, the following file holds the definitions of file extensions and the associated content-types: <code>...\Whale-Com\e-Gap\von\conf\content-types.ini</code></li></ul>
Unknown Content-Type	<p>Applicable for downloads only, when the option “Identify by Extensions” is activated. The value you enter here should be identical to the application’s unknown content-type settings.</p>
Identify by Size	<p>Identify downloads or uploads based on the size of transfer data.</p> <p><b>Note:</b> GET requests are treated as downloads; POST and PUT requests are treated as uploads.</p>

## Server Settings Tab

This tab is applicable in Portal trunks only, for Client/Server and Legacy Applications and Browser-Embedded Applications. It contains the configuration of the application's non-web server or servers. The parameters available in this tab vary, according to the application you are editing.



### Tip

- In order to see a description of the parameters that are relevant to the current application, click [Help](#). For SSL Wrapper applications, the Help also provides a list of operating systems on which the application is supported.
- To edit server settings for Domino iNotes non-web servers in Webmail trunks, see “Editing Webmail Trunk Server Settings”.

**Figure 14. Application Properties—Sample Server Settings Tab**

Application Properties (Citrix NFuse FR2 (Direct))

Download/Upload Server Settings Client Settings

Citrix Farm Servers: 192.168.78

Citrix Farm Port: 1494

Help OK Cancel

# Client Settings Tab

This tab is applicable in Portal trunks only, for Client/Server and Legacy Applications and Browser-Embedded Applications. It determines the activation of the Socket Forwarding component on endpoint computers, for the application you are configuring.

Figure 15. Application Properties—Client Settings Tab

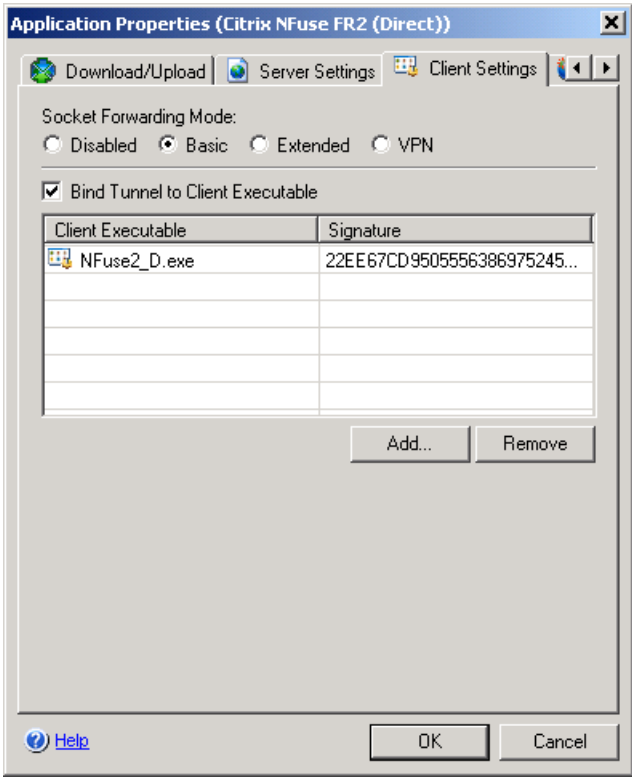


Table 15. Client Settings Tab Parameters

Parameter	Description
Socket Forwarding Mode	<p>Select whether to use the SSL Wrapper’s Socket Forwarding component with this application, and in which activation mode. For details on this component, including prerequisites for running it on endpoint computers, refer to Chapter 6: “SSL Wrapper”.</p> <ul style="list-style-type: none"><li>• Disabled: the Socket Forwarding component is not used with the application.</li><li>• Basic, Extended, and VPN activation modes are described in “Socket Forwarding Activation Modes” on page 174.</li></ul>

**Table 15. Client Settings Tab Parameters**

Parameter	Description
Bind Tunnel to Client Executable	<p>Applicable only when Socket Forwarding Mode is enabled for the application. Activating this option restricts access to the resources of this application (server IPs and ports) on endpoint computers to the process or processes you define here.</p> <p><b>For example:</b> when you configure a Telnet application, the SSL Wrapper tunnels all communications to and from the servers and port you define for this application, regardless of the process that initiates the communication. Using the “Bind Tunnel to Client Executable” option, you can restrict the tunneling to communications initiated by the Telnet process only, by defining the Telnet process as the client executable for this application.</p> <p>You can define multiple processes for an application. For each process, you can define the following:</p> <ul style="list-style-type: none"><li>• Client Executable: name of executable that runs the application on the endpoint computer. Use the “Add” button to add an executable, either by browsing and selecting a file or by manually entering the executable name in the “File name” field.</li><li>• Signature (optional): MD5 check sum of the executable. We recommend that you do not define a signature for applications whose check sum might change frequently, such as Internet Explorer and other Microsoft applications.</li></ul>

## Portal Link Tab

This tab is applicable in Portal trunks only, for all application types. You can use it to control the appearance of the link to the application from the portal homepage, as described in Table 16 on page 88.



### Note

The parameters you define in the Portal Link tab apply only if you use the Whale Portal, that is, the default portal homepage supplied with the IAG, or the Whale toolbar. In order to add the link on a custom homepage, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Using a Custom Portal Homepage” on page 61.

For the File Access application, you can also use this tab to hide the folder tree (left pane) in the remote user interface. This will prevent users from browsing to any folders other than the one defined as the application URL or its subfolders. For details, refer to “Hiding the Folder Tree in the End-User Interface” on page 234.

Figure 16. Application Properties—Portal Link Tab

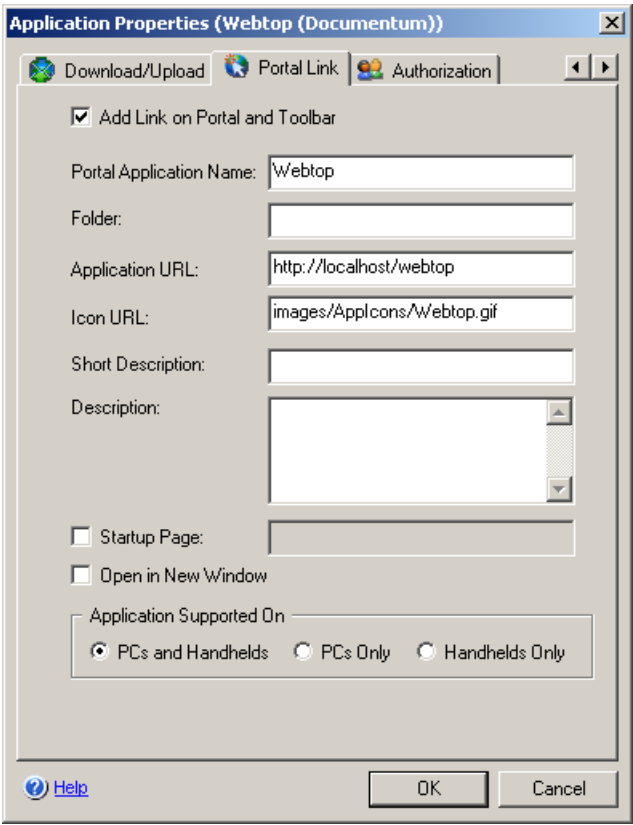


Table 16. Portal Link Tab Parameters

Parameter	Description
Add Link on Whale Portal and Toolbar	Adds a link to this application on the Whale Portal (default portal homepage supplied with the IAG) and Whale toolbar.
Portal Application Name	Name of the application on the portal homepage and in the Whale toolbar.



**Table 16. Portal Link Tab Parameters (Cont'd)**

Parameter	Description
Folder	<p>A folder or subfolder on the portal homepage via which users access the application. Enables you to group a number of applications on the portal homepage together under one link.</p> <p><b>For example:</b> you may want to create a folder called DriveMappings, and to place all Local Drive Mapping applications under it. Only the DriveMappings folder will be visible on the portal homepage.</p> <p>In order to place a number of applications under one folder, enter the same folder information for all the applications that will reside in the same folder.</p> <ul style="list-style-type: none"> <li>For a folder with no subfolders, enter only the folder name.</li> <li>For a subfolder, use this format: folder/subfolder A/subfolder B</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>The name of the “root” folder in the folder structure is the name of the Whale Portal application, as defined in the “Portal Application Name” field. By default “Whale Portal”.</li> <li>The folder structure is not retained in the Whale toolbar.</li> </ul>
Application URL	<p>Internal entry link URL, from the portal to the application.</p> <p><b>Note:</b> The URL must be an absolute URL, for example: <code>https://whale.com</code></p>
Icon URL	<p>URL of the icon representing the application (displayed in the portal to the left of the application name).</p>
Short Description	<p>Short description of the application (displayed in the portal directly under the application name).</p>
Description	<p>Additional description (displayed in the portal under the short description).</p>

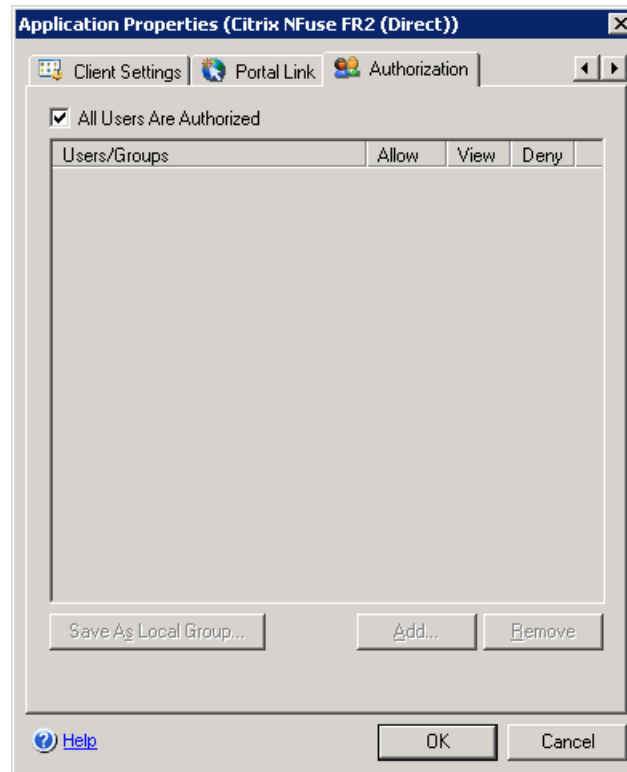
**Table 16. Portal Link Tab Parameters (Cont'd)**

Parameter	Description
Startup Page	<p>A page containing startup functionality you wish to assign to this application, in addition to the default functionality that is enabled by the IAG. When this option is activated, the page you define here is included by the default application startup page, and the operations you define in your page are implemented at the beginning of the application startup process.</p> <p>Default application startup for all applications is determined in the page <code>StartApp.asp</code>, located under:  <code>...\Whale-Com\e-Gap\von\InternalSite</code></p> <p>If you activate the Startup Page option, take the following steps:</p> <ul style="list-style-type: none"> <li>Place your own page in the following location:  <code>...\Whale-Com\e-Gap\von\InternalSite\inc\CustomUpdate</code>  <b>Note:</b> File extension must be <code>.inc</code></li> <li>Enter the name of the page, including its location under the <code>inc</code> folder, in the “Startup Page” text field.  <b>For example:</b></li> </ul> <div data-bbox="734 1058 1240 1106" data-label="Form"> </div> <p><b>Tip:</b> The page “notes” is automatically configured here for Domino iNotes and Domino Webmail applications. When you activate the Startup Page option, this page redirects the user to the appropriate server, according to the definitions of the repository against which the user authenticated when accessing the application. The “notes” page is located in the following location:  <code>...\Whale-Com\e-Gap\von\InternalSite\inc</code></p>
Open in New Window	Determines whether the application opens in a new window or not.
Application Supported On	Applicable for Web Applications only. Determines the type or types of computers on which the link is displayed: PCs, handheld devices, or both.

## Authorization Tab

This tab is applicable in Portal trunks only, for all application types. You can use it to configure portal homepage authorization and personalization; you can also use it to define local groups. For details, refer to “Users Setup” on page 32.

**Figure 17. Application Properties—Authorization Tab**



## Duplicating an Application

Duplicating an application enables you to quickly add a new application to the trunk, based on the definitions of an existing application. When you duplicate an application, most of the definitions of the new application are derived from the application from which it is copied, with the following exceptions:

- Application Name, which you assign when you create the new application.
- Application ID: a unique ID is assigned to the new application by the system.
- Portal Application Name is the name of the new application.

- Custom definitions of the application customizers and application access portal (SRA templates) are not applied to the new application.



#### Note

You cannot duplicate the following applications:

- Any of the applications in the Built-In Services group.
- SharePoint Portal 5.02, in the Web Applications group.

#### ***To duplicate an application:***

1. In the Configuration program, in the “Applications” area, select and right-click the application you wish to duplicate. From the drop-down menu, select **Duplicate...**

*The Application Duplicate Wizard is displayed.*

2. In the Wizard screen, assign a unique name to the application, then click **Finish**.

*The new application is added to the trunk, in the “Applications” area.*

3. Access the Application Properties dialog box of the new application, and change the application’s server definitions:
  - For Web Applications, in the Web Servers tab.
  - For Client/Server and Legacy Applications, in the Server Settings tab.
  - For Browser-Embedded Applications, in both the Web Servers and Server Settings tabs.

# Chapter 5

## Endpoint Security

The Intelligent Application Gateway (IAG) provides a number of features that help protect your internal network against access from non-secure endpoint computers.

This chapter describes the following:

- Endpoint security policies are used to create tiers of access by determining whether or not endpoint computers are allowed to access internal sites and applications, depending on their security settings. This feature is described in “Endpoint Policies” on page 93.
- Endpoint settings help you optimize endpoint computer settings that affect the functionality of some of the IAG features, as described in “Endpoint Settings” on page 108.
- The Attachment Wiper is a “virtual shredder” that wipes out sensitive information recorded by a web browser during an SSL VPN session, such as files, cookies, credentials, and more. For details, refer to “Attachment Wiper” on page 110.
- The Certified Endpoint option enables you to certify endpoint computers, using client certificates. This feature is described in “Certified Endpoints” on page 118.
- Whale Client Components are described in “Whale Client Components” on page 147.

### Endpoint Policies

SSL VPNs are accessed from clients of differing natures—company-owned laptops, home computers, public Internet kiosks, etc. The IAG is equipped with technology that identifies the security level of the endpoint computer, and can allow or deny access accordingly. You can use endpoint security policies to create tiers of access, by determining whether or not endpoint computers are allowed to access internal sites and applications, depending on their security settings.

#### **For example:**

You can set up your endpoint policies so that access to internal applications is allowed as follows:

- From corporate laptops: all applications are allowed.

- From home computers: all web applications are allowed.
- From an Internet kiosk: only Webmail applications are allowed.

When you define an endpoint policy, you determine which security components must be installed on the endpoint computer, in order for it to comply with the policy. Security components include options such as whether a compliant anti-virus program or a personal firewall are installed on the computer, whether the Attachment Wiper is launched on it, and more.

You use endpoint policies to control:

- Access to the site for both default and privileged sessions, at the trunk level.
- Access to each application that is accessible through the site, and, for web applications, upload and download to and from the application, and access to the application's restricted zone.

You can use the IAG's pre-defined policies, or define as many additional policies as you wish.



#### Note

Endpoint compliancy with all the policies, including application policies, is determined when the user first accesses the site. If some of the settings on the endpoint computer are changed after the login, in order for the changes to affect the computer's compliance with the endpoint policies, users need to log out of the site and log in again.

**For example:** if an anti-virus program is installed on the computer, but is not running when the user logs in, the computer does not comply with a policy that requires a "running anti-virus". If the user then runs the anti-virus program, without re-logging in to the site, the computer is still not considered as complying with this requirement, until the user logs out of the site and logs in again.

This section describes the following:

- "Endpoint Detection" on page 95
- "Session Endpoint Policies" on page 95
- "Application Endpoint Policies" on page 99
- "Default Policies" on page 101

Policy configuration options are described in:

- "Basic Policy Configuration" on page 103
- "Advanced Policy Configuration" on page 104

## Endpoint Detection

In order to be able to determine whether an endpoint complies with the endpoint policies, the IAG attempts to determine which security components are installed and running on the endpoint computer as soon as the user attempts to access the site. This is done by the Endpoint Detection ActiveX® component of the Whale Client Components, which is installed on the endpoint computer.



### Note

- For information on the Whale Client Components, refer to “Whale Client Components” on page 147.
- When the option “Disable Component Installation and Activation”, in the Session tab of the Advanced Trunk Configuration window, is activated, the Endpoint Detection component is not installed or activated on endpoint computers.

The Endpoint Detection component verifies the identity of the IAG site against the site’s server certificate, and checks whether the site is on the user’s Trusted Sites list; only if the site is trusted will the component run on the endpoint computer and collect the data that identifies which security components are installed and running on the computer.



### Tip

For information on how the IAG site can be added to the user’s Trusted Sites list refer to “IAG Trusted Sites” on page 160.

If the Endpoint Detection component is not running on the endpoint computer, compliance with policies is not detected. **For example:** on computers where the Whale Client Components are not enabled, or when using a browser other than Internet Explorer.

When detection is not functional on an endpoint computer, access may be denied even though it does comply with the requirements of the policy. **For example:** if an application’s policy requires a running anti-virus program, and such a program is running on the computer, access to the application is still denied, since the IAG can not detect that the program is running on this computer.

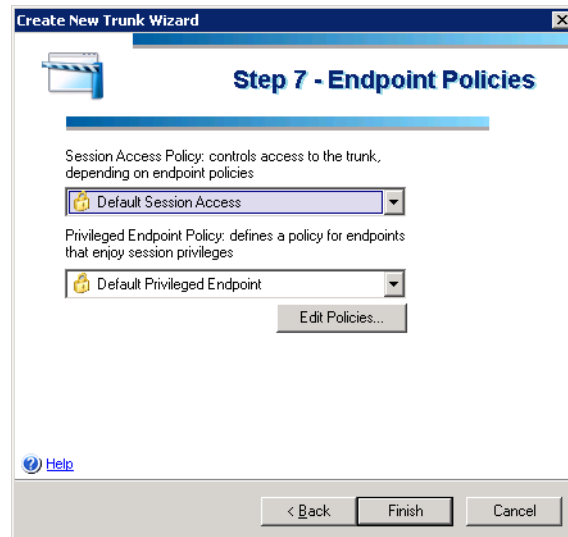
## Session Endpoint Policies

When you create a trunk, you assign it two session policies:

- **Session Access Policy** defines access permissions to the site. Only endpoints that comply with the selected policy are allowed access.

- **Privileged Endpoint Policy** defines the conditions that render an endpoint a “privileged” endpoint, which can enjoy session privileges. For information about privileged session settings refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Default and Privileged Session Settings” on page 137.

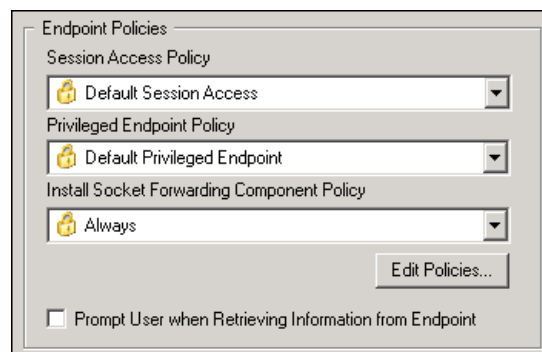
You select those policies in the “Endpoint Policies” step of the Create New Trunk Wizard:



### Note

The number of the step where you define endpoint policies for the session may vary, depending on the type of trunk you are configuring.

Once the trunk is created, you can change the selection of policies in the Session tab of the Advanced Trunk Configuration window, in the “Endpoint Policies” area:







### Note

The selection and editing of endpoint policies in both the Create New Trunk Wizard and in the Session tab of the Advanced Trunk Configuration window is disabled when the option “Disable Component Installation and Activation” in the “Session Configuration” area of the Session tab is activated.

In addition, you can use the “Endpoint Policies” area to do the following:

- Change the selected Install Socket Forwarding Component Policy. This policy is only relevant for Portal trunks; it defines the conditions under which the Socket Forwarding client component can be installed on the endpoint computer, in order to enable the use of the Socket Forwarding component for SSL Wrapper applications. For details, refer to Chapter 6: “SSL Wrapper”.



### Note

If you activate the option “Uninstall Socket Forwarding Component”, in the “Endpoint Settings” area of the Session tab, any Socket Forwarding Client Components that are installed on endpoint computers are removed when users next access the site. While this option is activated, the Socket Forwarding component is not installed on endpoint computers, regardless of a computer’s conformity to the Install Socket Forwarding Component Policy. For details, refer to “Endpoint Settings” on page 108.

- Notify users prior to retrieving information from their computer, and receive their consent for the retrieval of such information. For details, refer to “What Information is Collected from the End User’s Computer?” on page 97.

## What Information is Collected from the End User’s Computer?

While working with the IAG site, if endpoint detection is enabled on the end-user’s computer, the following information is collected by the Endpoint Detection component:

- Network domains: DNS and NetBIOS.
- User information: user name and user type.
- Certificates in “My certificate store”: certificate issuer and certificate subject. This includes all client certificates on the endpoint computer, not only the IAG certificate.

If required, for example, in order to comply with legal or corporate guidelines, you can configure the gateway so that users are notified before the information is retrieved from their computer, and are prompted to give their consent for the site to collect such information. On endpoints where users do not give their consent, detection is not performed, and the functionality of the Whale Client Components is disabled.



### Tip

For information on the Whale Client Components, refer to “Whale Client Components” on page 147.

### ***To notify and prompt users before the retrieval of information from their computers:***

1. At the IAG Configuration program, open the Advanced Trunk Configuration window and access the Session tab.
2. In the “Endpoint Policies” area, activate the option “Prompt User when Retrieving Information from Endpoint”.

*When users access the site, if endpoint detection is enabled on their computer, they are prompted with the following page:*

- *By selecting “Enable and continue with full functionality” users give their consent for the collection of information from their computers. They can then continue working with site, using all the functionality that is enabled by the Whale Client Components.*
- *For users who select “Continue with limited functionality”, information is not collected from their computers, and the Endpoint Detection component is not activated on their computer; this could result in limited functionality of the site.*

## Application Endpoint Policies

Application endpoint policies include the following:

- Access policy: controls access to the application.

For Web and Browser-Embedded applications:

- Download policy: helps prevent the spreading of sensitive data to undesired endpoints.
- Upload policy: helps prevent undesired endpoints from sending malicious data, such as viruses, malicious macros, and more, into the internal network.
- Restricted Zone policy: restrict users' access to sensitive areas of the application, such as administrative areas.



### Tip

- The method by which the IAG enforces the selected Download and Upload policies is defined in the Application Properties dialog box, in the Download/Upload tab. For details, refer to “Download/Upload Tab” on page 82.
- The Restricted Zone option is activated in the Application Properties dialog box, in the Web Settings tab. For details, refer to “Web Settings Tab” on page 73.

This section describes how:

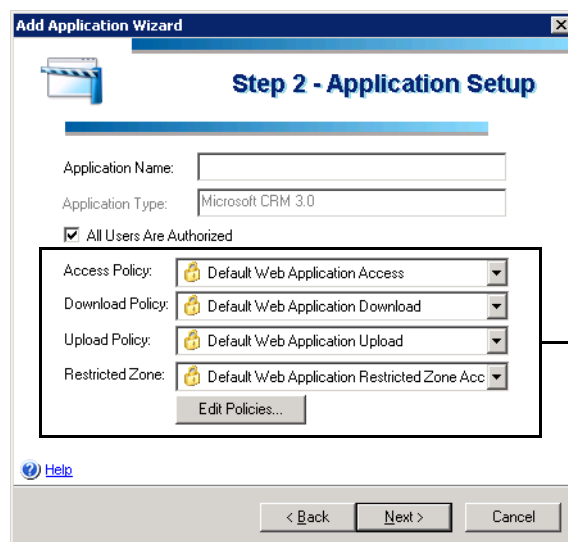
- Endpoint policies are defined for the trunk, as described in “Defining Application Endpoint Policies” on page 99.
- You edit existing application endpoint policies, as described in “Editing Application Policies” on page 100.

## Defining Application Endpoint Policies

When you add an application to a trunk, or define a Webmail or Basic trunk, the IAG automatically assigns the applicable default application endpoint policies, as follows:

- When defining Webmail and Basic trunks, and when adding an application from the Built-In Services group to a Portal trunk, the default application policies are selected automatically when you configure the trunk.

- When you add an application to a Portal trunk, the default application policies relevant for that application type are automatically selected in the “Application Setup” step of the Add Application Wizard. You can also select other application policies in this step, and edit the policies by clicking **Edit Policies** to access the Policies dialog box.



The selection and editing of endpoint policies is disabled when the option “Disable Component Installation and Activation”, in the Session tab of the Advanced Trunk Configuration window, is activated.

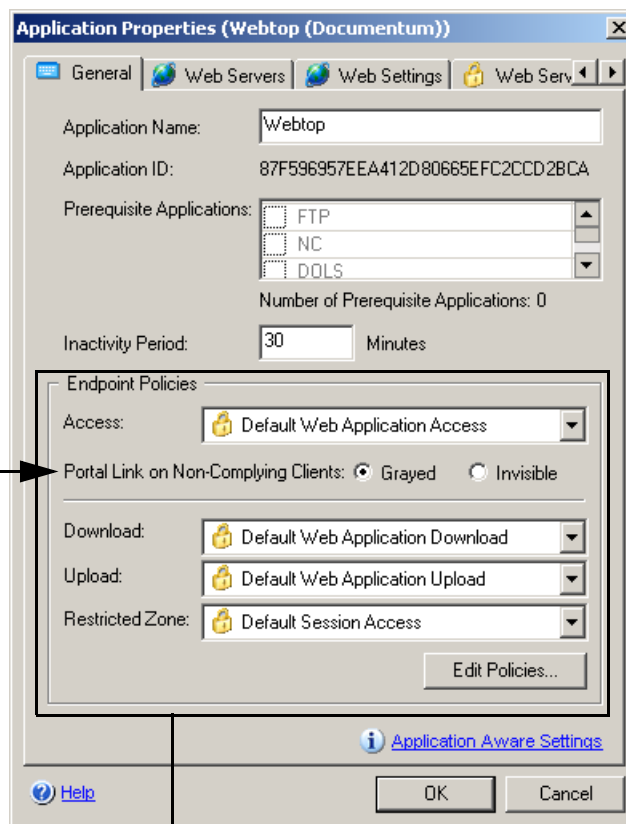
For all trunk and application types, you can later change and edit the policies as described in “Editing Application Policies” on page 100.

## Editing Application Policies

You edit Application Policies in the General tab of the Application Properties dialog box.

For Portal trunks, in sites that use the default portal homepage supplied with the IAG, you can also use the General tab to determine the display of the application’s link on the portal homepage when the endpoint does not comply with the application’s Access policy.


For sites that use the default portal homepage supplied with the IAG, this option determines the display of the application's link on the portal page when an endpoint does not comply with the application's Access policy.



The selection and editing of endpoint policies is disabled when the option “Disable Component Installation and Activation”, in the Session tab of the Advanced Trunk Configuration window, is activated.



### Tip

Click  for detailed information on the parameters in this tab.

## Default Policies

The IAG supplies you with pre-defined default policies for all the session and application policies. Those are optimized for a smooth running of the IAG, while still applying security restrictions.

**For example:** when you create a trunk, the following policies are selected by default:

- For Session Access Policy: Default Session Access. The default value of this policy is “True”, allowing all endpoints access.

- For Privileged Endpoint Policy: Default Privileged Endpoint. The default value of this policy is “False”, meaning that no endpoints will be considered “privileged” unless you edit this policy and set the criteria that will render an endpoint a privileged endpoint.



#### Note

The Install Socket Forwarding Component Policy is set to “Always” by default.

You can view the values of the default policies and edit their definitions, as well as create new policies, using one of the Policy Editors, as follows:

- The **Policy Editor** is an easy-to-use, basic editor you can use to create simple policies, without the need for defining variables and entering complex Boolean expressions. The basic editor can check the existence of the most commonly used endpoint security tools, such as anti-virus and personal firewall, as well as client configuration settings such as Whale Client Components, operating system, and user privilege level. For configuration instructions, refer to “Basic Policy Configuration” on page 103.
- Use the **Advanced Policy Editor** for more complex policies or attributes that are not presented in the basic editor. Once you edit a policy in the Advanced Policy Editor, you will only be able to open it for further editing in the Advanced Policy Editor; you will not be able to revert to editing in the basic Policy Editor. For detailed configuration instructions, refer to “Advanced Policy Configuration” on page 104.



#### Note

- When you edit a policy, the changes you make affect all the Whale Client Components that use this policy.

#### For example:

If the policy is used to control both session access and application access, changes you make to the policy will affect both session and application access.

In order to apply changes to a specific component only, create a dedicated policy and use it with the applicable component.

- All default policies can only be edited in the Advanced Policy Editor, since they contain complex expressions.

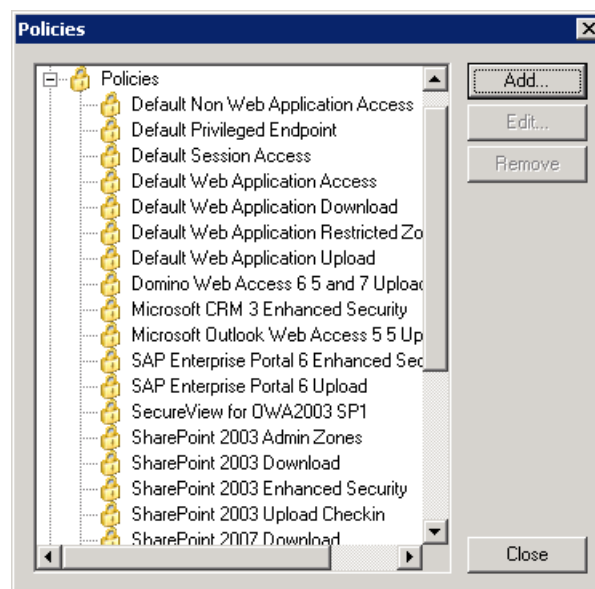
## Basic Policy Configuration

This section describes how you use the Policy Editor to edit and create policies and expressions, in Basic mode. For details on creating policies in Script mode, refer to “Configuration in the Advanced Policy Editor” on page 106.

### *To configure policies and expressions in Basic mode:*

1. In an area where you assign policies, click **Edit Policies...**.  
**For example:** in the Session tab of the Advanced Trunk Configuration window.  
*The Policies dialog box is displayed.*

**Figure 18. Policies Dialog Box**

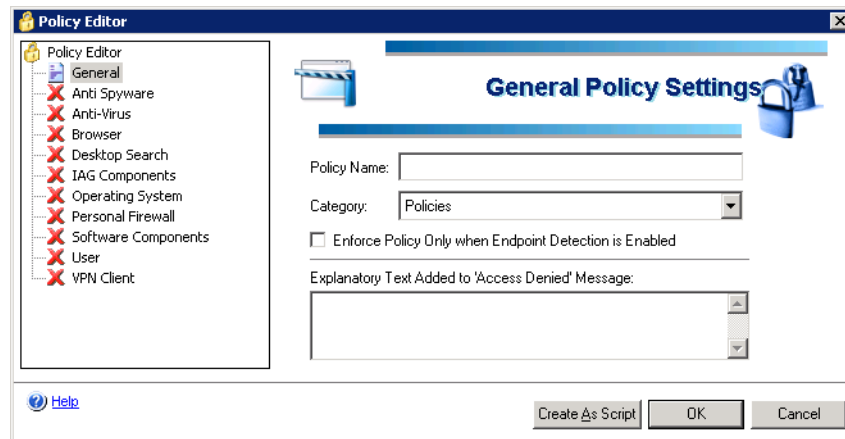


### **Tip**

For a description of where you can access the Policies dialog box, refer to “Session Endpoint Policies” on page 95 and “Application Endpoint Policies” on page 99.

2. Do one of the following:
  - To edit an existing policy that was previously created and edited in Basic mode, select the policy and click **Edit...**.
  - To edit an existing expression, click the **+** sign to expand the Expressions group, select the expression you wish to edit, then click **Edit...**.
  - To create a new policy or expression, click **Add...**.


*The basic Policy Editor is displayed.*



3. Enter general information about the policy or expression in the General Policy Settings screen. Once general information is defined, use the tree on the left to select and configure groups of pre-defined variables, which will compose the policy or expression. You can select as many groups and group-items as required in order to define the policy or expression.



#### Tip

Click  [Help](#) for detailed information on the parameters of each screen.

4. When you finish editing the policy, click **OK** to close the Policy Editor, then click **Close** to close the Policies dialog box.

## Advanced Policy Configuration

This section describes:

- The components of which policies are created, in “Advanced Configuration Overview” on page 105.
- Policy configuration in the Advanced Policy Editor, using Script mode, in “Configuration in the Advanced Policy Editor” on page 106.
- The format of variables that can be used to create policies and expressions using the Advanced Policy Editor, in “Variable Formats” on page 107.



## Advanced Configuration Overview

An endpoint policy is made of one or more components. A policy component can be:

- A variable. Variables are pre-defined basic endpoint detection parameters. You cannot edit variables.  
**For example:** the variable **Anti-Virus > Symantec > Norton > Running** checks whether the Norton® anti-virus is running on the endpoint computer.



### Tip

For a description of variable formats, refer to “Variable Formats” on page 107.

- An expression. Expressions are built from variables, free VBScript text, or a combination of both. You can use built-in expressions as is, edit them, or create your own expressions.  
**For example:** change the expression **Corporate Machine** from the default “False” to a condition that actually defines what a corporate machine is, such as:  
**Network > Domains > NetBIOS Domain = “OurDomain”.**



### Tip

Use expressions to define multiple conditions once, and apply them across several policies.

- VBScript text. Combine VBScript-syntax free text with expressions and variables to parse and manipulate them, in order to define a condition.  
**For example:** an expression that checks that the virus definitions of the Norton anti-virus were updated within the last seven days can be defined as follows:

```
DateDiff("d",Components_AV_Norton_LastUpdate,Now)<7
```



### Tip

To see a sample expression: in the Policies dialog box select the expression “Symantec Norton Anti-Virus Up-To-Date Sample” and click **Edit...**. For details, refer to “Configuration in the Advanced Policy Editor” on page 106.

## Configuration in the Advanced Policy Editor

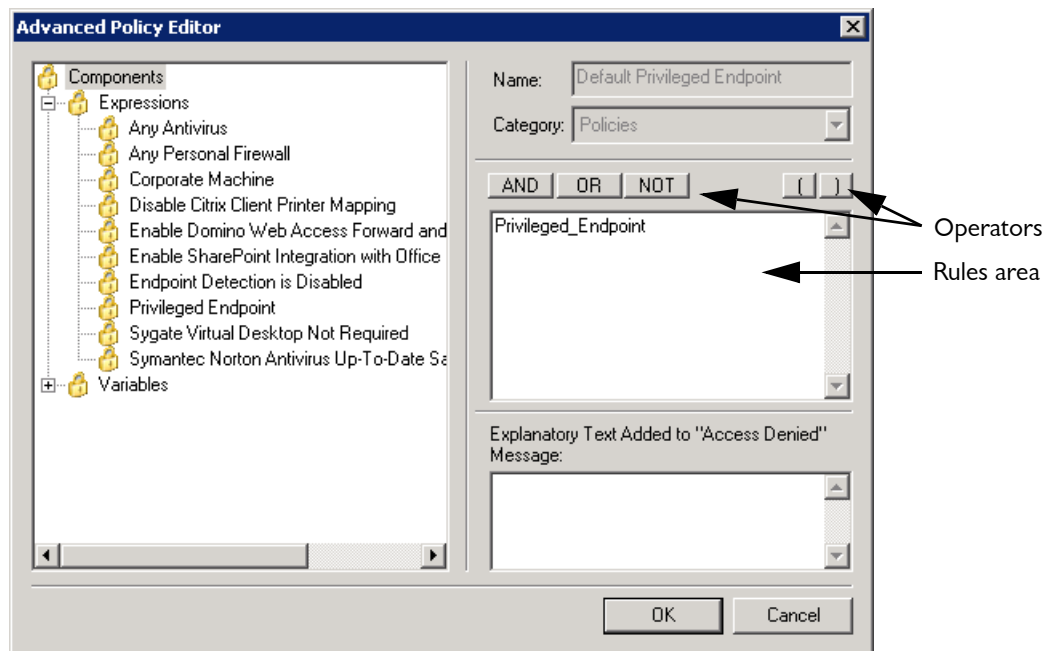
This section describes how you use the Advanced Policy Editor to edit and create policies and expressions, in Script mode. For details on creating policies in Basic mode, refer to “Basic Policy Configuration” on page 103.

### *To configure policies and expressions in Script mode:*

1. Access the Policies dialog box, as described in “Basic Policy Configuration” on page 103.
2. Do one of the following:
  - To edit an existing policy, select the policy and click **Edit...**.
  - To edit an existing expression, click the **+** sign to expand the Expressions group, select the expression you wish to edit, then click **Edit...**.
  - To create a new policy or expression, click **Add...**. In this case, the basic Policy Editor is displayed. To access the Advanced Policy Editor, click **Create As Script**.

*The Advanced Policy Editor is displayed.*

**Figure 19. Sample Policy Editor**



3. For new policies and expressions:
  - In the “Name” field, at the top right, assign a name.
  - In the “Category” field, select “Policies” or “Expressions”, accordingly.

You do not need to edit those fields for existing policies and expressions.

4. Define the rules of the policy or expression:
  - From the Components list, at the left of the Policy Editor, select a component to add it to the “Rules” area on the right.
  - Use the AND, OR, NOT, and parenthesis operators to create a combination of as many components as you require, or to combine VBScript-syntax free text with expressions and variables.
  - The “Rules” area is a free text area; you can edit and delete rules and rule-components in this area as required.
5. At the bottom right of the Advanced Policy Editor, you can enter text that will be displayed to users in the message they receive if their computer does not comply with the policy, and access is denied.



#### Note

Some of the default policies come with explanatory text, which is tailored for the functionality of the policy. If you change the policy, make sure you also change the explanatory text so that it reflects the new or revised functionality.

6. When you finish editing the policy, click **OK** to close the Advanced Policy Editor, then click **Close** to close the Policies dialog box.

## Variable Formats

This section describes the format of the variables you can use when creating policies and expressions.

**Table 17. Policy Variable Formats**

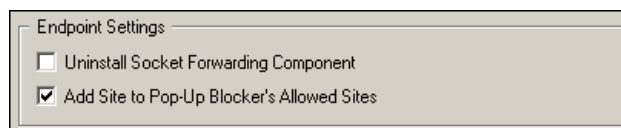
Variable	Data Type	Comments
APP/AS/AV/ PFW_*_Version_Product	String	Desktop Search/Anti Spyware/Anti-Virus/Personal Firewall product version.
APP/AS/AV/ PFW_*_Version_Engine	String	Desktop Search/Anti Spyware/Anti-Virus/Personal Firewall engine version.
APP/AS/AV/ PFW_*_Version_Dat	String	Desktop Search/Anti Spyware/Anti-Virus/Personal Firewall IDS definitions version.

**Table 17. Policy Variable Formats (Cont'd)**

Variable	Data Type	Comments
APP/AS/AV/ PFW_*_Version_Build	String	Desktop Search/Anti Spyware/Anti-Virus/Personal Firewall build number.
APP/AS/AV/PFW *_LastUpdate	Double	Date/time double. Use VBScript DateDiff("d",AS/ AV_*_LastUpdate,Now)<=7 ) ) to check last update.
Network_Domains_*	String	Name of domain.
System_Browser	String	Lower case, full string of user agent.
System_OS_ WinNTServicePackVersion	String	OS Service Pack Number. <b>For example:</b> 4.0
System_WindowsLogged OnUser_UserName	String	Name of Windows OS logged-on user name.
All other variables	Boolean	

## Endpoint Settings

This section describes how you can optimize endpoint computer settings, which might affect the experience of the remote user when working with the portal. Endpoint settings are defined in the Session tab of the Advanced Trunk Configuration window, in the “Endpoint Settings” area:



Endpoint settings that you can optimize include the following options:

- **Uninstall Socket Forwarding Component:** once this option is activated, the Socket Forwarding client component is uninstalled from each endpoint computer when the user next access the site. If more than one Socket Forwarding component is installed on a computer, activating this option deletes only the component of the

current IAG software version. For details on the Socket Forwarding component, which can be used with the SSL Wrapper, refer to Chapter 6: “SSL Wrapper”.

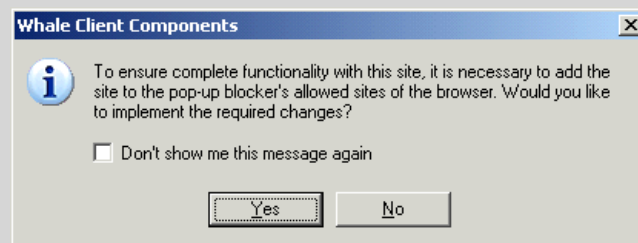
While this option is activated, the Socket Forwarding component is not installed on endpoint computers, regardless of a computer’s conformity to the Install Socket Forwarding Component Policy. For details on this policy, refer to “Session Endpoint Policies” on page 95.

- **Add Site to Pop-Up Blocker’s Allowed Sites:** this option is applicable for Internet Explorer browsers running on Windows, which feature a pop-up blocker, such as Internet Explorer on Windows XP SP2. It adds the site to the list of allowed sites in Internet Explorer’s pop-up blocker, so that pop-ups from the site are not blocked, and users can continue to receive messages and notifications, such as Inactive Session Timeout and Scheduled Logoff notifications. The site is removed from the pop-up blocker’s allowed sites when the Whale Client Components are uninstalled, as described in “Uninstalling the Whale Client Components” on page 167.



#### Tip

When the site is added to Internet Explorer’s pop-up blocker’s allowed sites, the user is notified by a message and is prompted to confirm the change:



If a user selects the option “Don’t show me this message again”, the notification will not be displayed again when users access this site. In order to receive the notification when applicable, instruct the user to restore the default settings of the Whale Component Manager, as described in “Restoring the Whale Client Components Defaults” on page 165.

## Attachment Wiper

The Attachment Wiper utility deletes persistent browser data that is downloaded to the browser from the sites protected by the IAG, or created by the browser, whenever the following occurs:

- The session ends, for example when the user closes the browser.
- When the user logs out using the site's Logoff mechanism.
- During a scheduled logoff or scheduled cleanup.

The Attachment Wiper utility deletes items that are saved in the browser's cache during the session, such as web pages, cookies, and files (including application-specific cached files).

The Attachment Wiper also deletes items that are saved in the browser's `offline` folder. These include files that were opened from within the browser, for editing by an external application, such as an Office application. For example: a document that was opened via the browser for editing in Microsoft Word. The `offline` folder is cleaned only when all the IAG sessions on the computer end. Only items that were written to the `offline` folder since the Attachment Wiper was first activated, during the initial login, are deleted.

Optionally, you can also configure the Attachment Wiper to delete items that are saved outside the cache, including the browser's History, Web Address AutoComplete, IntelliForms, Forms AutoComplete, and Cached Passwords. The Attachment Wiper deletes these items only when it quits, and not at the end of each session.



### Note

- All items are deleted according to the DOD 5220.22-M standard.
- If the user closes the browser without first logging out of the site, the Attachment Wiper does not quit immediately; in this case, it quits only on the next scheduled logoff or scheduled cleanup.

The Attachment Wiper utility includes a built-in crash recovery mechanism that ensures that all items are wiped even under extreme circumstances, such as a power shutdown. If, under those circumstances, the utility is terminated without deleting all the required items, when the computer is next started, the utility automatically runs and cleans up any remaining items.

The Attachment Wiper is an ActiveX component, and is part of the Whale Client Components, which users are prompted to download when they try to access a site, prior to the Login stage. It will only function if the required Whale Client Components are successfully installed on the endpoint computer. For details, refer to “Whale Client Components” on page 147.

**Tip**

You can set a policy whereby users can only access a site or an application if the Attachment Wiper is running on their computer. For details, refer to “Endpoint Policies” on page 93.

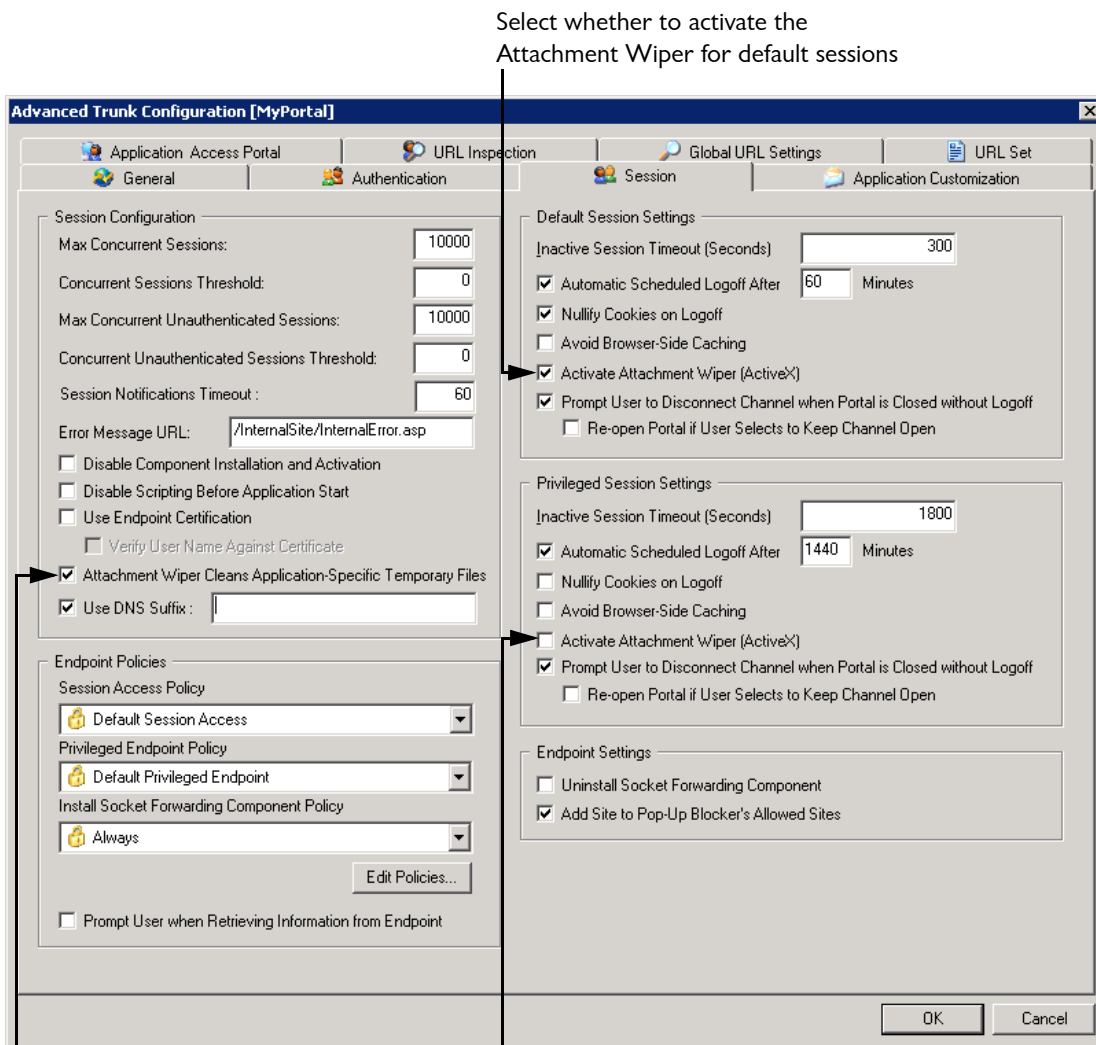
This section describes the following:

- How you configure the utility, in “Configuring the Attachment Wiper” on page 112.
- Cleanup of items that are saved outside the cache, described in “Cleanup of Items That Are Saved Outside the Cache” on page 113.
- Scheduled cleanup, which triggers a cleanup after a pre-configured timeout period, is described in “Configuring a Scheduled Cleanup” on page 115.
- The code that triggers the Attachment Wiper to initiate the cleanup of the browser’s cache on the client is embedded in the Logoff Message page that is supplied with the IAG. If, however, the trunk is configured to use a custom Logoff page, you need to add the code in the custom page. This option is described in “Enabling the Attachment Wiper on a Custom Logoff Message Page” on page 116.
- To cancel the disabling of the “Do not save encrypted pages to disk” setting on the endpoint computer running Internet Explorer, refer to “When Encrypted Pages Are Saved to a Location Other Than “Temp Files”” on page 117.

## Configuring the Attachment Wiper

You configure the Attachment Wiper in the Session tab of the Advanced Trunk Configuration window:

**Figure 20. Configuration of the Attachment Wiper**



Select whether to activate the Attachment Wiper for default sessions

Select whether to delete application-specific temporary files, for all sessions where the Attachment Wiper is activated

Select whether to activate the Attachment Wiper for privileged sessions

When you create a trunk, the Attachment Wiper is automatically configured as follows:



- The option “Activate Attachment Wiper” is activated for default sessions, and disabled for privileged sessions. To learn more about these types of sessions, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Default and Privileged Session Settings” on page 137.
- The option “Attachment Wiper Cleans Application-Specific Temporary Files” is activated. This option applies to all the sessions where the Attachment Wiper is activated. It determines whether or not the Attachment Wiper deletes application-specific temporary files for the relevant applications.

For a list of applications for which the Attachment Wiper deletes application-specific temporary files, as well as a description of the locations where the Attachment Wiper deletes files for each of these applications, and what types of files are deleted, refer to the *Intelligent Application Gateway Application Aware Settings* guide.

## Cleanup of Items That Are Saved Outside the Cache

This section describes how you configure the Attachment Wiper to:

- Clear the browser’s History pane and empty the History folder. History is cleared browser-wide.
- Clear the Web Address AutoComplete list, so that no addresses are displayed in the browser’s Address drop-down list, and clear the IntelliForms entries. These items are cleared browser-wide.
- Clear Cached Passwords in Forms AutoComplete and Wininet’s cached passwords (replies to application-specific authentication requests). These items are only cleared for the specific domains that were accessed via the IAG.
- Clear all additional fields that are saved by Forms AutoComplete. These items are cleared browser-wide.

***To configure cleanup of items that are saved outside the cache:***



### Tip

This procedure involves the customization of authentication pages. For a full description of the pages and the customization options available to you, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Authentication Pages” on page 96.

1. Access the following custom folder; if it does not exist, create it:  
...\\Whale-Com\\e-Gap\\von\\InternalSite\\inc\\customUpdate
2. Under the CustomUpdate folder, create an inc “hook”, which will be activated before the PostValidate.asp reaches the client side:

```
PrePostValidate.inc
```

Or,

```
PostPostValidate.inc
```

Name the file as follows:

```
<Trunk_Name><Secure (0=no/1=yes)><Hook_Name>
```

**For example:**

For an HTTPS trunk named “WhalePortal”, to create a “PrePostValidate” hook, create the file:

```
WhalePortal1PrePostValidate.inc
```

If such a file already exists, use the existing file.

3. In the file you defined in step 2, add the following lines:

```
<%  
    SetSessionParam g_cookie,ATTACHMENT_WIPER_CLEAR_HISTORY_PARAM, "<flag>"  
%>
```

Where flag may be any combination of the following:

Flag	Description
1	Clear History.
2	Clear Web Address AutoComplete and IntelliForms.
4	Clear Cached Passwords in Forms AutoComplete and Wininet's cached passwords (replies to application-specific authentication requests).
8	Clear all fields that are saved by Forms AutoComplete, except for Cached Passwords, which are cleared by flag 4.

**For example:**

In order to clear the browser's History, Web Address AutoComplete, and IntelliForms, without clearing any of the other items, add the lines:

```
<%  
    SetSessionParam g_cookie,ATTACHMENT_WIPER_CLEAR_HISTORY_PARAM, "3 "  
%>
```



**Note**

For the cleanup of the Forms AutoComplete data, it is recommended to use flags 4 and 8 together (12). It is not recommended to use flag 8 on its own.

## Configuring a Scheduled Cleanup

In addition to the automatic cleanup that is triggered at the end of a session or when a user is logged out, you can configure a “scheduled cleanup”, whereby the Attachment Wiper utility automatically triggers a cleanup after the timeout period you configure.

You can configure the scheduled cleanup to be triggered by any of the pages that users access while browsing the applications enabled through the trunk. If you configure a cleanup trigger in more than one page, the timeout defined in the page that was last accessed sets the trigger.

**For example:** if you configure a 900-second timeout in one of your pages, once a user receives the page, the timeout is set to 900 seconds. However, if you also configure a 300-second timeout in another page, once a user accesses it, the timeout is set to 300 seconds, regardless of the time that elapsed since the user accessed the previous page. In this example, 300 seconds after the user accesses the second page, the Attachment Wiper utility triggers the cleanup.



### Caution

Do not edit the pages that are supplied with the IAG. Configure the cleanup in your own pages, such as the application pages.

### *To configure a scheduled cleanup:*

1. In the page from where you wish to trigger the cleanup, add the following line:

- For Portal trunks:

```
<script language="JavaScript" src="http://localhost:6001/InternalSite/scripts/CacheClean.js"></script>
```

- For Webmail and Basic trunks:

```
<script language="JavaScript" src="/InternalSite/scripts/CacheClean.js"></script>
```

2. Still in the same page, add the following lines:

```
<script language="JavaScript">
var whaleCacheClean;
GetCacheCleanInstance();
SetTimeoutForCacheClean(Timeout);
</script>
```

Where (Timeout) is defined in seconds.

**For example:**

In order to trigger a cleanup 600 seconds after the user accessed the page, enter the line:

```
SetTimeoutForCacheClean(600)
```



**Note**

If you set the timeout to zero, the cleanup is triggered as soon as the user accesses the page.

## Enabling the Attachment Wiper on a Custom Logoff Message Page

This section describes the code you need to embed in the Logoff Message page used with the trunk, if you do not use the default page supplied with the IAG. The code triggers the Attachment Wiper to initiate the cleanup of the browser's cache.



**Tip**

You select the Logoff Message page used with the trunk in the Authentication tab of the Advanced Trunk Configuration window, in "Logoff Message". For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to "Configuration in the Authentication Tab" on page 82.

You can find sample code in the Logoff Message page supplied with the IAG:

```
...\Whale-Com\e-Gap\von\InternalSite\LogoffMsg.asp
```

***To configure a non-default Logoff Message page to trigger the Attachment Wiper:***

1. In your Logoff Message page, add the following line:

```
<script language="JavaScript" src="scripts/CacheClean.js"></script>
```

2. Still in the same page, add the following lines:

```
<script language="JavaScript">
var whaleCacheClean;
GetCacheCleanInstance();
ActivateCacheCleanDontSurf()
</script>
```

## When Encrypted Pages Are Saved to a Location Other Than “Temp Files”

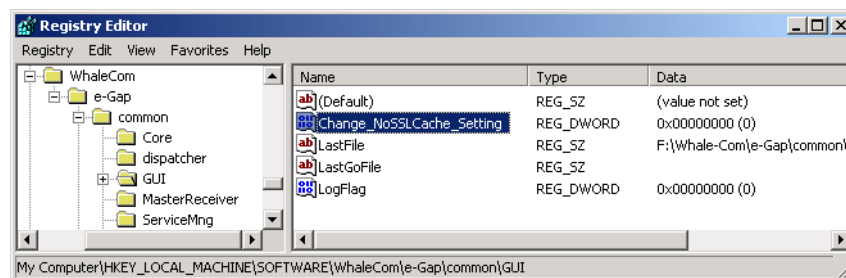
Normally, Internet Explorer browsers save encrypted (SSL) pages to the “temp files” folder. However, end-users can enable the “Do not save encrypted pages to disk” setting in Internet Explorer (Tools > Internet Options > Advanced tab), and prevent the browser from saving SSL pages to the default “temp files” folder. In this case, when users download an SSL page, they are prompted to provide an alternative location where it should be saved. In this setup, when a session ends, the Attachment Wiper clears the “temp files” folder, but cannot identify the location to which the encrypted pages are saved.


In order to prevent these pages from remaining on the endpoint computer, at the beginning of each session the Attachment Wiper automatically disables the “Do not save encrypted pages to disk” setting, if enabled, so that encrypted pages are saved to the “temp files” folder. At the end of the session, after the Attachment Wiper stops monitoring all open sessions, the “Do not save encrypted pages to disk” setting is reverted its original status.

You can cancel the disabling of the “Do not save encrypted pages to disk” setting, as described below.

### ***To cancel the disabling of the “Do not save encrypted pages to disk” setting on the endpoint computer:***

1. At the IAG, use the Registry Editor to access the following location:  
...\\WhaleCom\\e-Gap\\common\\GUI
2. Create a new DWORD value named Change\_NoSSLCache\_Setting, and set the value to 0.



3. Access the Configuration program. Click  to activate the configuration, select the option “Apply changes made to external configuration settings”, and click **Activate >**.

*Once the configuration is activated, the “Do not save encrypted pages to disk” setting is not changed on the endpoint computer.*

## Certified Endpoints

A Certified Endpoint is a computer that has been certified by the organization, using a client certificate.



### Tip

You can set a policy whereby users can only access a site or an application if their computer is a Certified Endpoint. For details, refer to “Endpoint Policies” on page 93.

The Certified Endpoint feature relies on PKI infrastructure (digital certificates and Certificate Authorities). In order to register a computer as a Certified Endpoint, end-users need to install a unique certificate, provided by the organization, on their computers.

To provide users with the required certificate, this feature may make use of any Certificate Authority (CA), installed on a remote computer (any computer other than the IAG). In addition, for Portal trunks, the IAG provides built-in support for Microsoft CA, installed locally, on the IAG.



### Note

- The Certified Endpoint feature is only supported on HTTPS trunks.
- Activating the option “Disable Component Installation and Activation” in the Session tab of the Advanced Trunk Configuration window disables the Certified Endpoints feature. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Session Configuration” on page 133.

## Certified Endpoint Configuration Overview

There are two ways of setting up the Certified Endpoint feature, depending on where the CA is installed:

- Using Microsoft CA installed on the IAG. This setup is only applicable for Portal trunks, and is described in “Enabling Certified Endpoint Using Microsoft CA Locally” on page 119.
- Using any CA installed on a remote computer. This setup can be used with any HTTPS trunk, and is described in “Enabling Certified Endpoints Using a Remote CA” on page 122.

## Enabling Certified Endpoint Using Microsoft CA Locally

To enable the Certified Endpoint feature using Microsoft CA installed locally on the IAG, perform the following steps:

- Install Microsoft CA on the IAG. For details, refer to “Installing a Microsoft Certificate Authority (Local CA Only)” on page 124.
- Optionally, define a policy for issuing the CA certificates. By default, a Manual policy is defined for the CA. You can change the policy to either Automatic or to Automatic with Delay. For details, refer to “Defining a Certification Authority Policy (Local CA Only)” on page 128.
- Optionally, edit some of the default configuration settings. Refer to “Editing the Default Configuration (Local CA Only)” on page 131.
- Before you activate the Certified Endpoint feature, make sure that end-users who are using Microsoft Internet Explorer prepare their endpoint computers, as described in “Preparing Endpoint Computers that Use Internet Explorer (Local CA Only)” on page 134.
- Enable the Certified Endpoint feature in the Configuration program: in the Session tab of the Advanced Trunk Configuration window, activate the option “Use Endpoint Certificate”. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Session Configuration” on page 133.
- Add the “Certified Endpoint Enrollment” application to the trunk. Refer to “Adding Certified Endpoint Enrollment to the Trunk (Local CA Only)” on page 135. Note the following:
  - If you use the default portal homepage supplied with the IAG, adding the Certified Endpoint Enrollment application to the trunk automatically adds the required links to the end-user’s portal. If you use a custom homepage, you can manually add this functionality to your page, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Adding Links to IAG Features on a Custom Homepage” on page 66.
  - The “Certified Endpoint Enrollment” application is not supported on Camino browsers on Mac OS X, since the underlying Microsoft application is not supported on those browsers.
- Update the Certificate Trust List (CTL) with the new CA. Refer to “Adding the CA to the Certificate Trust List (All CAs)” on page 136.
- Back up the certificate settings, as described in “Backing Up the Certificate Settings (All CAs)” on page 140.



### Note

After the initial backup, make sure to back up the certificate settings from time to time, especially before any IAG software upgrade or installation, or any other changes to system settings.

At this point, the Certified Endpoint feature is enabled. End-users can obtain a certificate and turn their computers into Certified Endpoints. For details, refer to “End-User Interaction (Local CA Only)” on page 140.

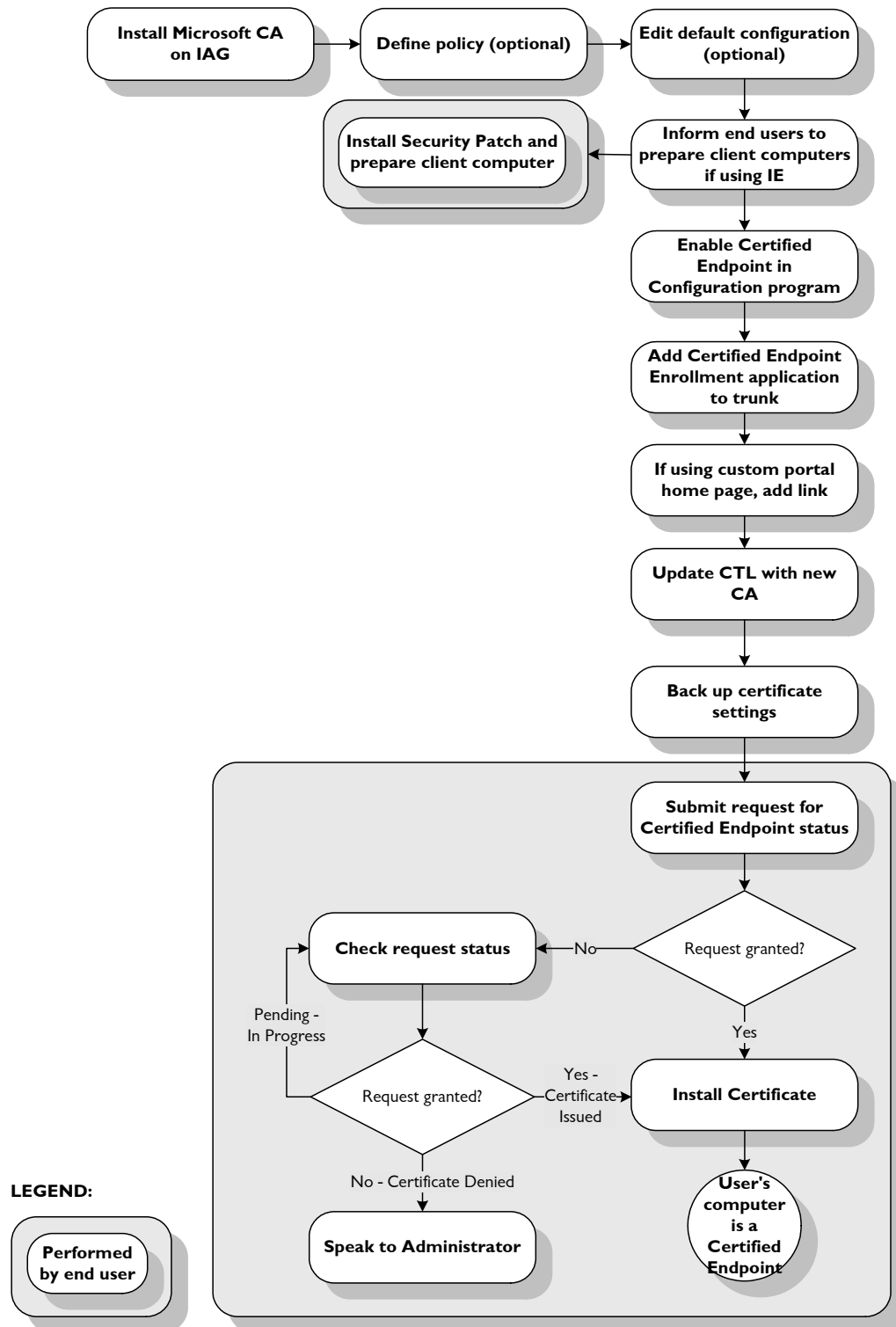
Once end-users request certificates, you can view and manage the requests using the Certification Authority. Refer to “Viewing and Processing Certificate Requests (Local CA Only)” on page 146.

Figure 21 on page 121 illustrates the following:

- Steps that the administrator has to perform to enable the Certified Endpoint feature when using a locally installed Microsoft CA.
- Steps that the end-user must perform in order to be recognized as a Certified Endpoint, depicted in the shaded areas.



**Figure 2I. Sample Flow for Enabling Certified Endpoint Using a Local CA**



## Enabling Certified Endpoints Using a Remote CA

A remote CA is any CA that is installed on a computer other than the IAG. You can use Microsoft CA or any other CA. When using a remote CA, you have to provide end-users with the necessary certificate to use the Certified Endpoint feature.



### Note

The Certified Endpoint feature is only supported on HTTPS trunks. The steps below describe how you enable Certified Endpoints for an existing trunk.

To enable the Certified Endpoint feature using a remote CA, perform the following steps:

- Install the certificates from the remote CA to the Trusted Root Certification Authorities/Certificate store on the IAG. If you require assistance with this installation, contact technical support.
- Enable the Certified Endpoint feature in the Configuration program, in the Session tab of the Advanced Trunk Configuration window. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Session Configuration” on page 133.
- Update the Certificate Trust List (CTL) with the new CA. Refer to “Adding the CA to the Certificate Trust List (All CAs)” on page 136.
- Back up the certificate settings, as described in “Backing Up the Certificate Settings (All CAs)” on page 140.



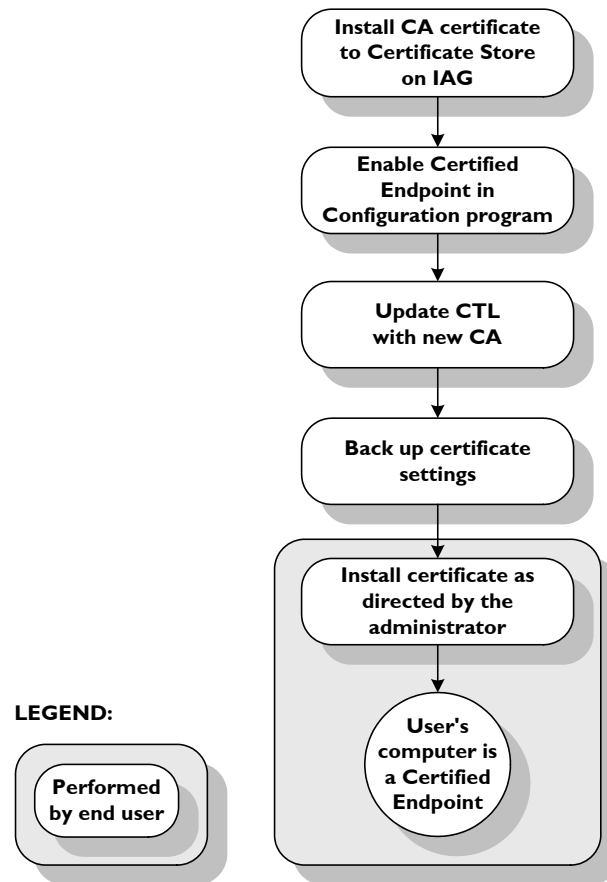
### Note

After the initial backup, make sure to back up the certificate settings from time to time, especially before any IAG software upgrade or installation, or any other changes to system settings.

Figure 22 on page 123 illustrates the following:

- Steps that the administrator has to perform to enable the Certified Endpoint feature when using a remote CA.
- Steps that the end-user must perform in order to be recognized as a Certified Endpoint, depicted in the shaded areas.

**Figure 22. Sample Flow for Enabling Certified Endpoint Using a Remote CA**



## Certified Endpoint Configuration Steps

Depending on the way you set up the Certified Endpoint feature (refer to “Certified Endpoint Configuration Overview” on page 118), the following procedures are available for configuring the Certified Endpoint feature:

- “Installing a Microsoft Certificate Authority (Local CA Only)” on page 124.
- “Defining a Certification Authority Policy (Local CA Only)” on page 128.
- “Editing the Default Configuration (Local CA Only)” on page 131.
- “Preparing Endpoint Computers that Use Internet Explorer (Local CA Only)” on page 134.
- “Adding Certified Endpoint Enrollment to the Trunk (Local CA Only)” on page 135.
- “Adding the CA to the Certificate Trust List (All CAs)” on page 136.
- “Backing Up the Certificate Settings (All CAs)” on page 140.

## Installing a Microsoft Certificate Authority (Local CA Only)

This section describes how you install the Microsoft Certificate Authority on the IAG, in order to provide users with the required certificates in a local CA setup. If you use a CA installed on a remote computer, you have to use other means in order to provide users with the certificates.

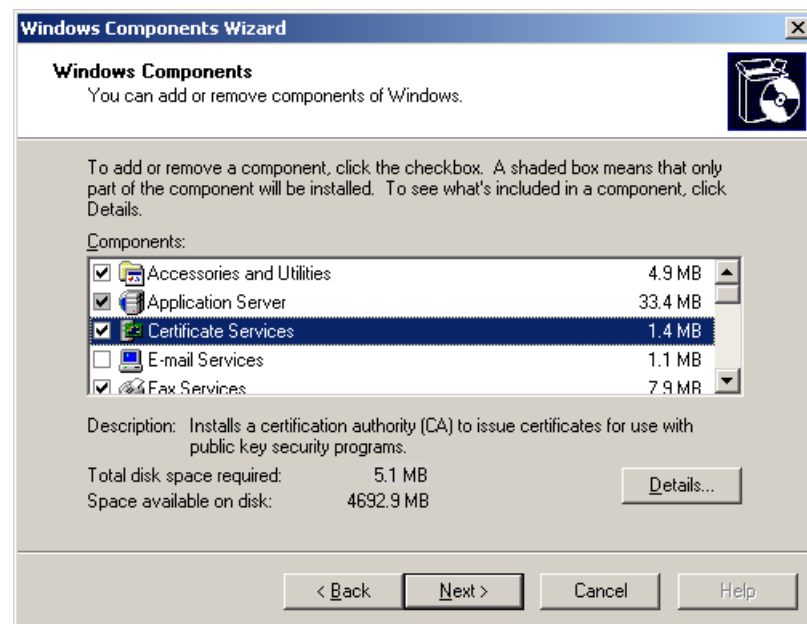
### *To install Microsoft Certificate Authority:*

1. In the Windows desktop, click **Start** and select **Settings > Control Panel > Add/Remove Programs**.

*The Add/Remove Programs Properties dialog box is displayed.*

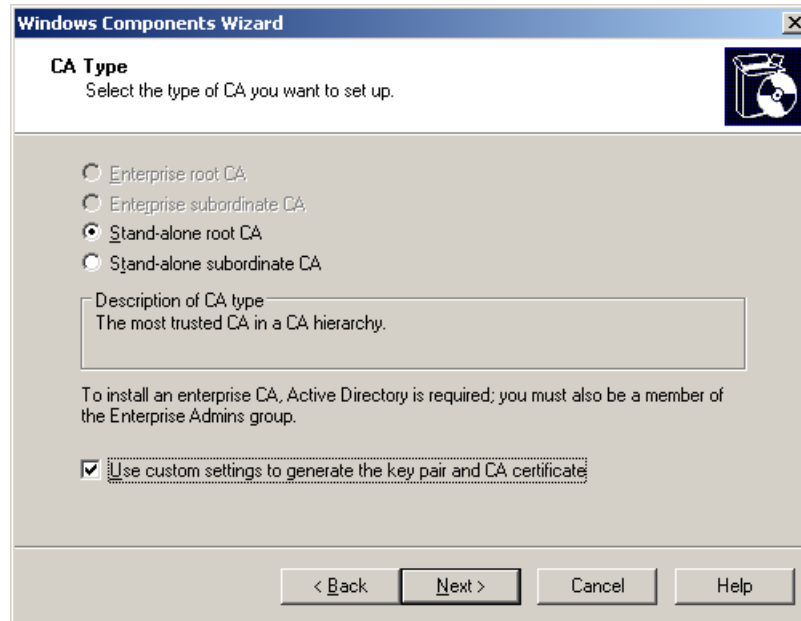
2. Click **Add/Remove Windows Component**.

*The Windows Components Wizard is displayed.*



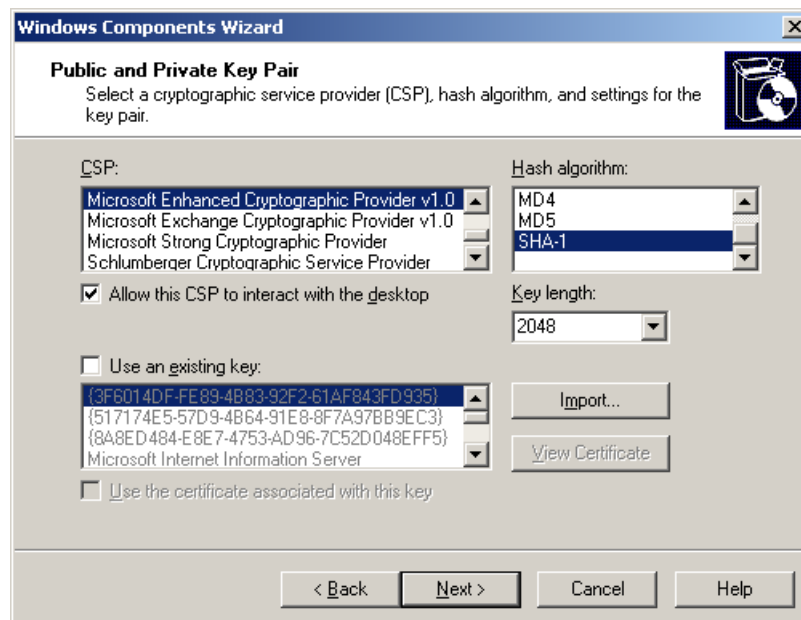
3. In the “Components” list, check **Certificate Services** and click **Next>**.

*The CA Type window of the Windows Components Wizard is displayed.*



4. Select **Stand-alone root CA**.
5. Check **Use custom settings to generate the key pair and CA certificate** and click **Next >**.

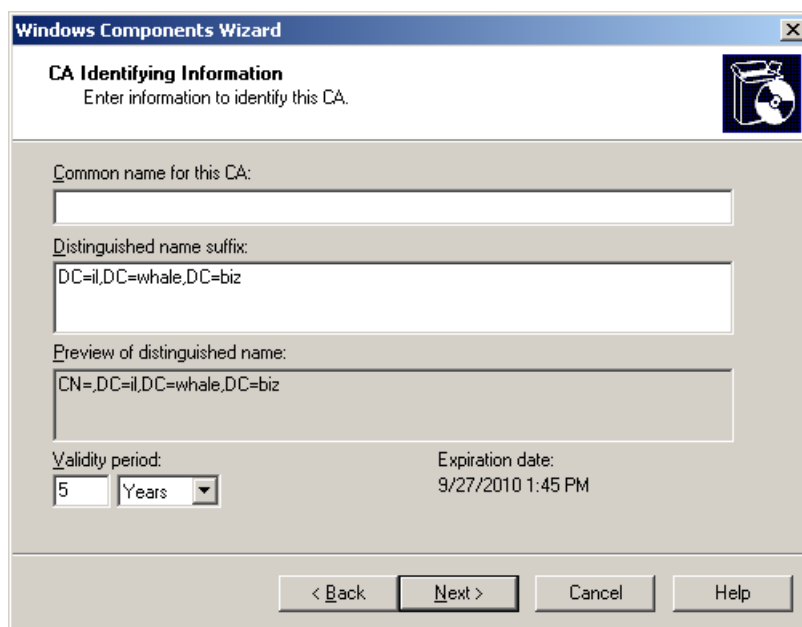
*The Public and Private Key Pair window of the Windows Components Wizard is displayed.*



6. Select the following:
  - In the “CSP” list, select **Microsoft Enhanced Cryptographic Provider v1.0**.
  - In the “Hash algorithm” list, select **SHA-1**.
  - In the “Key length” drop down list, select **2048**.

Click **Next >**.

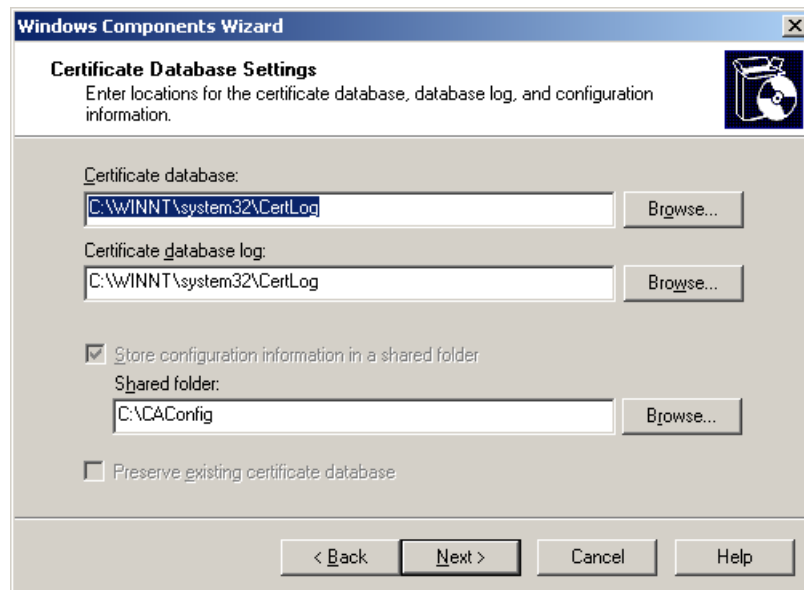
*The CA Identifying Information window of the Windows Components Wizard is displayed.*



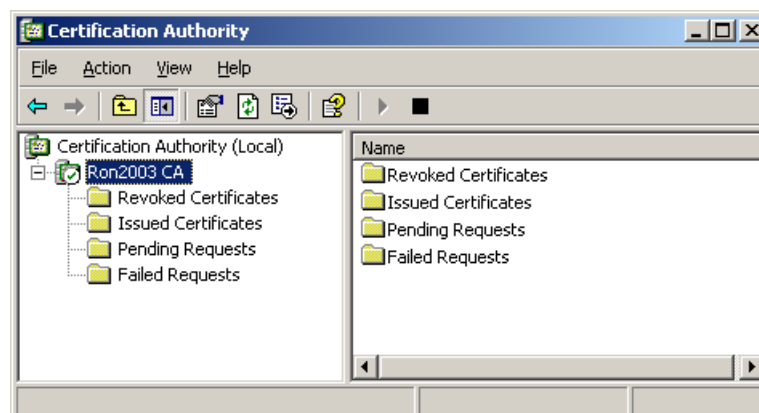
The screenshot shows the 'CA Identifying Information' window of the Windows Components Wizard. The window has a title bar 'Windows Components Wizard' and a subtitle 'CA Identifying Information'. Below the subtitle is the instruction 'Enter information to identify this CA.' and a CD icon. The main area contains four input fields: 'Common name for this CA:' (empty), 'Distinguished name suffix:' (containing 'DC=il,DC=whale,DC=biz'), 'Preview of distinguished name:' (containing 'CN=,DC=il,DC=whale,DC=biz'), and 'Validity period:' (set to '5' years). The 'Expiration date:' is '9/27/2010 1:45 PM'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

7. Enter the Common name for this Certificate Authority and click **Next >**.

*A cryptographic key is generated, and the Certificate Database Settings window of the Windows Component Wizard is displayed.*



8. Do not change the default values displayed in the Certificate Database Settings window. Click **Next >**.  
*If the IIS is running, you are prompted to stop the IIS.*
9. Click **Yes** to stop the IIS on your computer.  
*A progress bar appears and the Microsoft Certificate Authority is installed.*
10. Click **Finish** to exit the Windows Components Wizard.
11. To verify that the Certificate Authority is installed and working on your computer, in the Windows desktop, click **Start** and select **Programs > Administrative Tools > Authentication Authority**.  
*The Certification Authority window with the Certificate Authority you just installed is displayed.*



## Defining a Certification Authority Policy (Local CA Only)

The Microsoft CA provides two policies for issuing certificates:

- **Manual** - the user's request is defined as pending until the administrator manually issues the certificate.
- **Automatic** - the certificate is automatically issued after the request is received.

When the CA is installed, the default certification policy is Manual. You can change this policy at any time, as described in "Selecting Between Manual and Automatic Certification Policies" on page 128.

If you select the Automatic certification policy, by default, the certificate is issued immediately after the certification request is received. If you wish, you can change the policy to **Automatic with Delay**, whereby the certificate is issued only after the specified delay period. To configure this policy, refer to "Setting the Certification Policy to Automatic with Delay" on page 130.



### Note

When you change the certification policy, the change only affects new certification requests. Requests that were entered prior to the change will be treated according to the policy that prevails when the request was entered.

## Selecting Between Manual and Automatic Certification Policies

This procedure describes how you select between the Manual and Automatic certification policies.

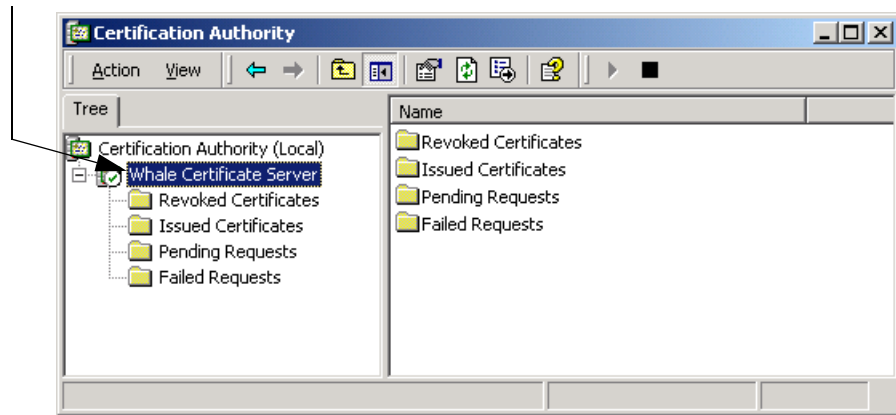
### *To select a certification policy:*

1. In the Windows desktop, click **Start** and select **Programs > Administrative Tools > Certification Authority**.

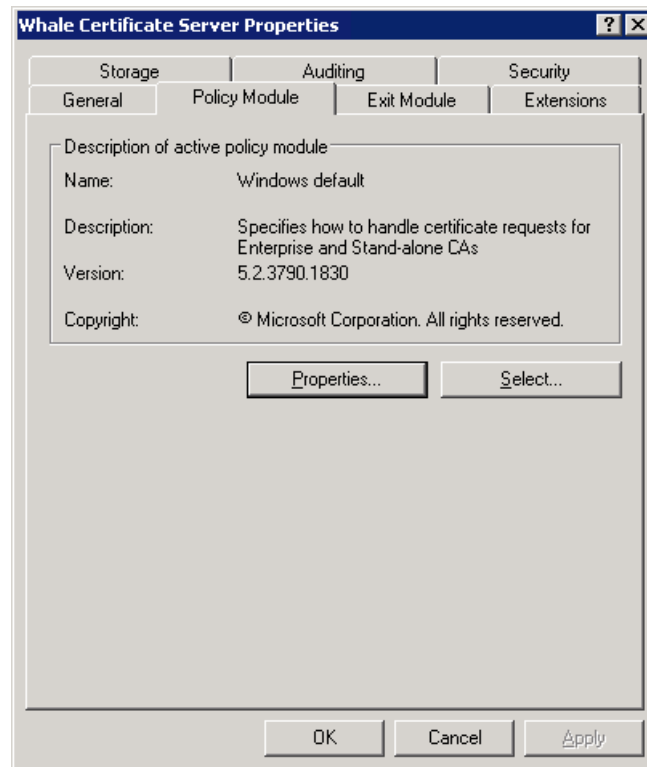
*The Certification Authority window is displayed.*



CA's home folder

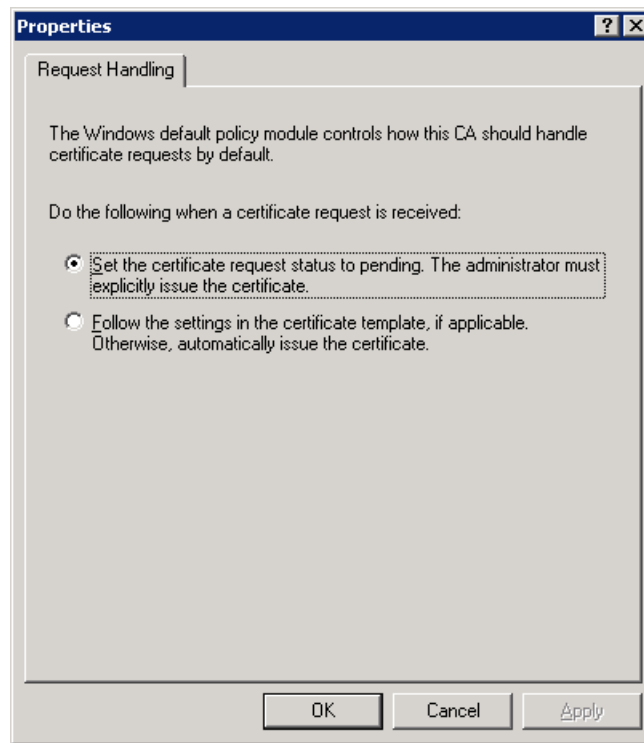


2. Right-click the home folder of the CA and select **Properties**.  
*The CA's Properties dialog box is displayed.*
3. Select the Policy Module tab.



4. Click **Properties...**.  
*The Properties dialog box is displayed.*
5. In the Request Handling tab, select one of the following actions:

- For manual mode, select the option:  
“Set the certificate request status to pending. The administrator must explicitly issue the certificate”.
- For automatic mode, select the option:  
“Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate”.



6. Click **OK**.

*The default action is set. It will be applied to all new requests. Existing requests are treated according to the policy that prevails when the request was entered.*

### Setting the Certification Policy to Automatic with Delay

In addition to the policies you can select via the Certification Authority interface, the IAG enables you to specify an Automatic with Delay policy. This policy automatically issues the certificate, but only after a defined delay interval.

#### *To define an Automatic with Delay policy:*

1. At the IAG, access the following file:  
...\\Whale-Com\\e-Gap\\Von\\WhaleSEP\\inc\\info.inc
2. Copy the file you accessed in step 1 to the following custom folder; if the folder does not exist, create it:

...\Whale-Com\e-Gap\Von\WhaleSEP\inc\CustomUpdate

If such a file already exists, use the existing file.

3. In the file under the CustomUpdate folder, locate the line:  
nAutoModeDelayInMinutes=0
4. Replace the value 0 with the required delay interval value.
5. Save the file.

*The default policy is set to Automatic with Delay.*



#### Note

If at a later time you change the policy to either Automatic or Manual, you need to manually reset the value of nAutoModeDelayInMinutes back to 0:

```
nAutoModeDelayInMinutes=0
```

## Editing the Default Configuration (Local CA Only)

The following Certified Endpoint configuration settings may be modified after installing the Microsoft CA:

- Pending timeout interval, for Manual certification policy. This setting defines the interval between the time users request a certificate, and the time they can receive it. After the specified interval, the end-user can no longer request the pending certificate, and must begin the certificate request process again. The default pending timeout interval is 10 days. To change this value, refer to “Setting Pending Timeout for Manual Certification Policy” on page 131.
- The fields that are displayed to users requesting certificates in the Certified Endpoint Certificate - User Information window, as described in “Customizing User Information Properties” on page 132.

## Setting Pending Timeout for Manual Certification Policy

This procedure describes how you change the pending timeout interval of the Manual certification policy.

### ***To set the pending timeout interval:***

1. At the IAG, open the following file:

...\Whale-Com\e-Gap\Von\WhaleSEP\inc\certdat.inc



#### Note

This file is only available on the IAG after you install the CA on the server, as described in “Installing a Microsoft Certificate Authority (Local CA Only)” on page 124.

2. Change the value of `nPendingTimeoutDays`. For example, `nPendingTimeoutDays=25`.
3. Save the file.

*The pending timeout interval is updated to the new value specified. It will be applied to all new requests. The pending timeout interval for existing requests is the interval that prevails when the request was entered.*

## Customizing User Information Properties

This section describes how you change the properties of the fields that are displayed to users requesting certificates in the Certified Endpoint Certificate - User Information window. The default properties are determined during the installation of the CA on the IAG, in the CA Identifying Information window.

**Figure 23. Properties That Can Be Edited in the User Information Window**

Certified Endpoint - Microsoft Internet Explorer

Whale Communications  
A Microsoft Subsidiary

**Certified Endpoint**

User Information

Please enter the following:

Name: Peter Reese

E-Mail:

Company: Whale Communications

Department: Engineering

City: Tel-Aviv

State: NA

Country/Region: IL

Submit >



### Tip

For information about customizing the look-and-feel of the Certified Endpoint Enrollment pages, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Customizing Certified Endpoint Enrollment Pages” on page 67.

***To edit the properties of the data fields in the User Information window:***

1. At the IAG, access the following file:  
`...\Whale-Com\e-Gap\Von\WhaleSEP\inc\info.inc`
2. Copy the file you accessed in step 1 to the following custom folder; if the folder does not exist, create it:  
`...\Whale-Com\e-Gap\Von\WhaleSEP\inc\CustomUpdate`  
If such a file already exists, use the existing file. The file contains the definitions of the User Information data fields.  
In the file under the CustomUpdate folder, change the properties of the data fields as required. For each field, you can assign a status, as follows:
  - **FIELD\_READONLY:** read-only. A read-only field is displayed in the User Information window, but users cannot edit its value.
  - **FIELD\_EDITABLE:** read-write. A read-write field is displayed in the User Information window with a text box, enabling users to enter a value.
  - **FIELD\_HIDDEN:** hides the field. A hidden field is not displayed in the User Information window.



**Note**

- The content of all fields except the `editEmail` field is automatically filled in, based on the certificate, therefore it is recommended that these fields retain their default **READONLY** status.
- A sample of how this code is implemented is provided in “Sample Code: info.inc” on page 134.
- For more information, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Customizing Certified Endpoint Enrollment Pages” on page 67.

3. Save the file.  
*When users next request a certificate, the data fields in the User Information window will display according to the properties you set here.*

### Sample Code: info.inc

```
<% ' CODEPAGE=65001 'UTF-8
' info.inc - global (DAT)a
if Session(INFO_INC) <> FILE_NOT_EXIST then
    include Session(INFO_INC)
else
    'Delay between certificate request and certificate issue in
    'automatic mode. Default value should be 0
    nAutoModeDelayInMinutes=0

    'default data fields edit status FIELD_READONLY, FIELD_EDITABLE,
    'FIELD_HIDDEN
    editCommonName=FIELD_READONLY
    editEmail=FIELD_EDITABLE
    editCompany=FIELD_READONLY
    editDepartment=FIELD_READONLY
    editLocalCity=FIELD_READONLY
    editState=FIELD_READONLY
    editCountry=FIELD_READONLY
end if%>
```

### Preparing Endpoint Computers that Use Internet Explorer (Local CA Only)



#### Note

This section is only relevant for endpoint computers using Microsoft Internet Explorer. No preparation is required for other browsers.

Before you activate the Certified Endpoint option, make sure that end-users who are using Microsoft Internet Explorer prepare their endpoint computers as follows:

- The browser needs to be configured to enable the download and launching of signed ActiveX objects.
- For Windows 2000 and Windows XP systems, power-user access level is required for the current user (like any other downloaded program on Windows 2000 and Windows XP).
- Users need to install the Microsoft Security Patch Q323172 on their computer. This patch resolves the “Flaw in Digital Certificate Enrollment Component Allows Certificate Deletion” security vulnerability.

The Q323172 security patch can be found at the following locations, depending on the operating system end-users are using. Instruct your end-users to follow the instructions on the web site to download and install the appropriate security patch.

- Microsoft Windows 2000:  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41568>
- Microsoft Windows XP:  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41598>
- Microsoft Windows XP 64-bit Edition:  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=41594>

### **Adding Certified Endpoint Enrollment to the Trunk (Local CA Only)**

This section describes how you add the Certified Endpoint Enrollment application to the list of applications that are enabled through the trunk. Once you add the application and activate the trunk, a “Make this computer certified” link is automatically added to the default portal homepage, enabling users to request a certificate and make their computer a Certified Endpoint.



#### **Note**

- The ability to add a Certified Endpoint is automatically available on the portal homepage only if you use the default portal homepage supplied with the IAG. If you use a custom homepage, you can add this functionality to your page, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Adding Links to IAG Features on a Custom Homepage” on page 66.
- The “Certified Endpoint Enrollment” application is not supported on Camino browsers on Mac OS X, since the underlying Microsoft application is not supported on those browsers.

#### ***To add the Certified Endpoint Enrollment application to the trunk:***

1. In the Configuration program, from the List pane, select the trunk for which you enabled the Certified Endpoint feature.
2. In the “Applications” area, under the Application List, click **Add...**, or double-click an empty line;

Or,

In the List pane, right-click the trunk and select **Add Application**.

*The Add Application Wizard is displayed.*

3. Select “Built-in Services” and, from the drop-down list, select **Certified Endpoint Enrollment**.
4. Click **Finish**.

**Note**

For more information about adding applications to a trunk, refer to “Creating an SSL VPN Portal” on page 28.

## Adding the CA to the Certificate Trust List (All CAs)

**Note**

If you are using a remote CA, import your server certificate into the local computer’s Trusted Root Certification Authorities/Certificate store before proceeding. For details, contact technical support.

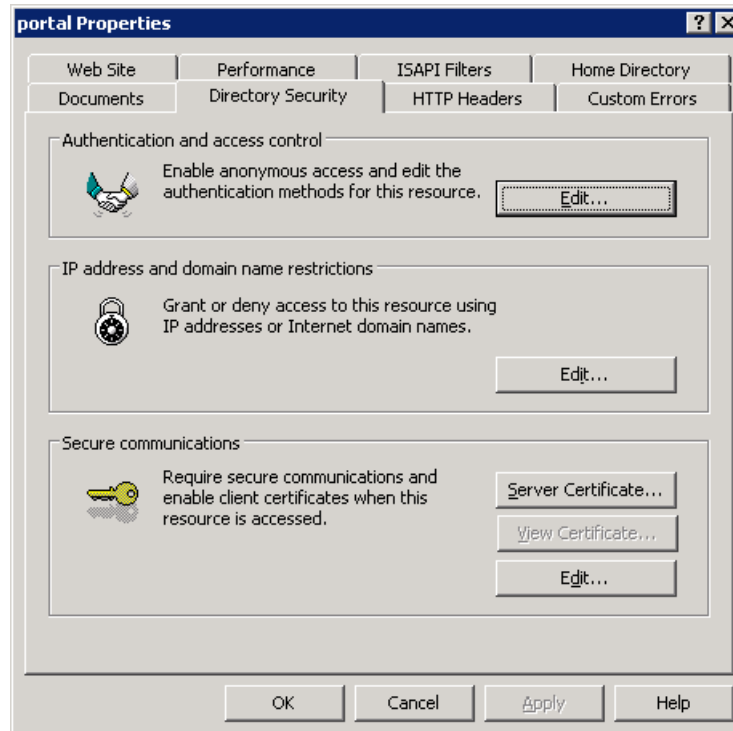
The Certificate Trust List (CTL) is a signed list of CA certificates that have been judged reputable by the administrator.

In order to use a CA, you have to notify the IAG that you trust the CA by adding it to the CTL for the portal.

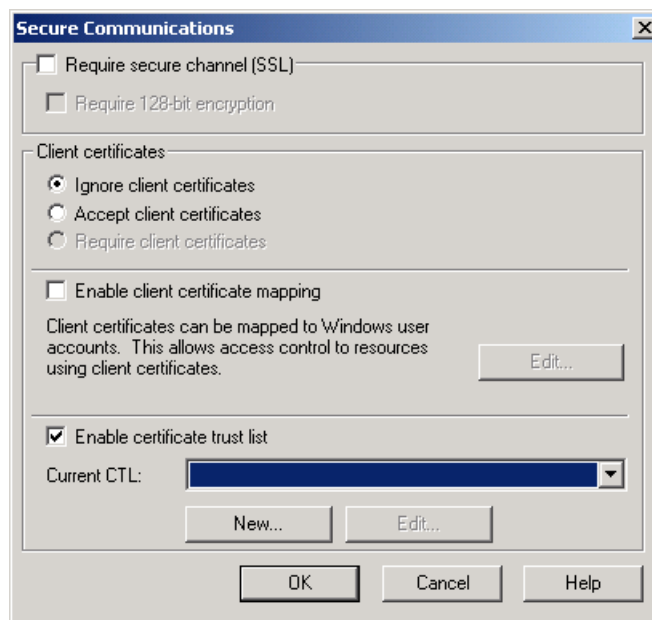
***To add a CA to the CTL:***

1. In the Windows desktop, click **Start** and select **Programs > Administrative Tools > Internet Information Services**.  
*The Internet Information Services (IIS) Manager window is displayed.*
2. Right-click on the portal and select **Properties**.  
*The portal Properties dialog box is displayed.*
3. Click the Directory Security tab.



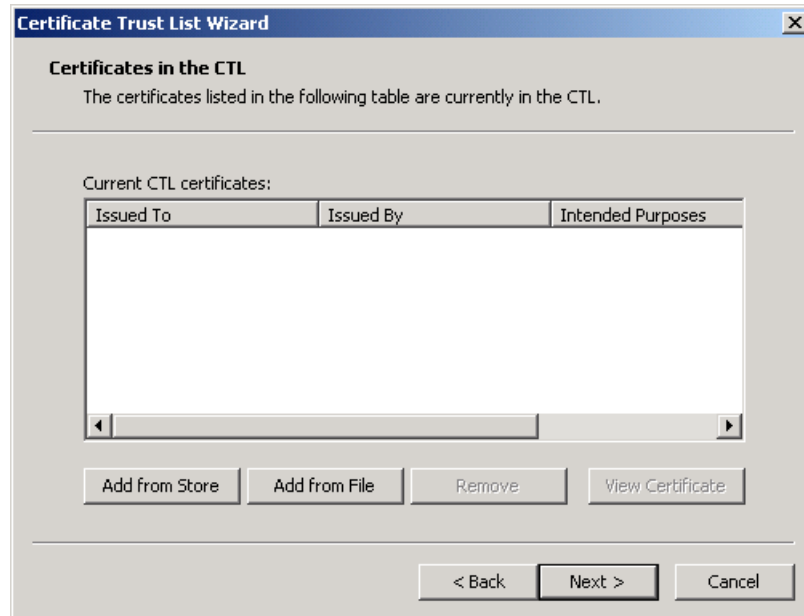


4. In the “Secure communications” area, click **Edit...**.  
*The Secure Communications dialog box is displayed.*



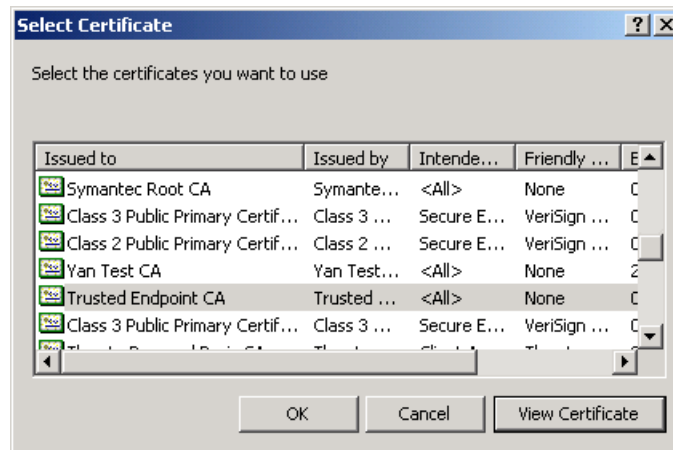
5. Check the option “Enable certificate trust list”, and click **New...**.  
*The Welcome to the Certificate Trust List Wizard screen is displayed.*
6. Click **Next >**.

*The Certificates in the CTL screen of the Certificate Trust List Wizard is displayed.*



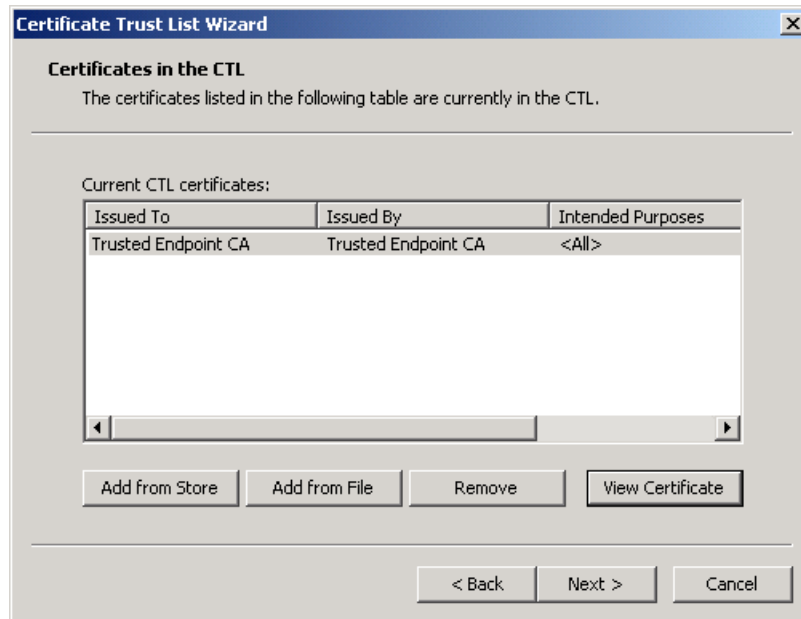
7. Click **Add from Store**.

*The Select Certificate dialog box is displayed.*



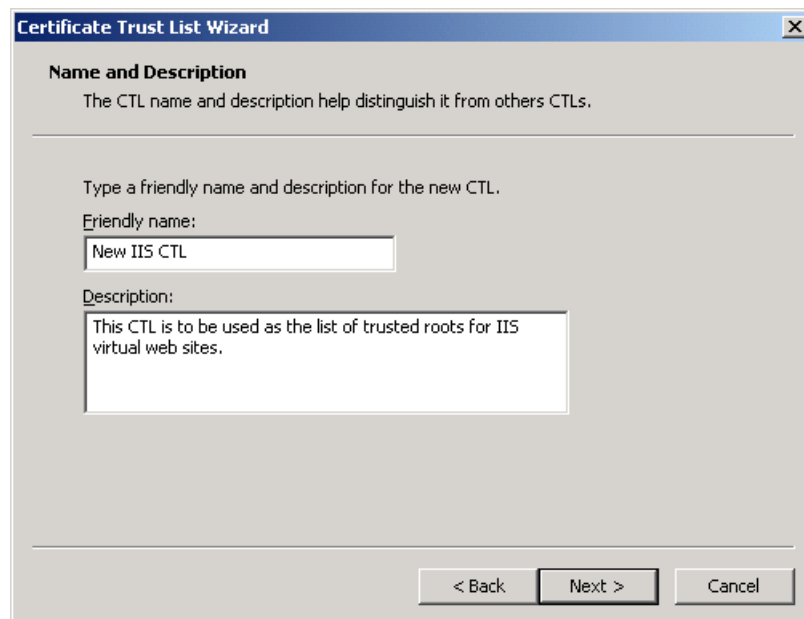
8. Select the certificate you wish to use and click **OK**.

*The Certificates in the CTL screen of the Certificate Trust List Wizard is displayed with the certificate you selected.*



9. Click **Next >**.

*The Name and Description screen of the Certificate Trust List Wizard is displayed.*



10. Enter a name and description for the new Certificate Trust List and click **Next >**.

*The Completing the Certificate Trust List Wizard screen of the Certificate Trust List Wizard with a summary of your settings is displayed.*

11. Click **Finish**.

*The Certificate Authority is added to the Certificate Trust List. The configuration process is complete. End-users can proceed to make their computers Certified Endpoints, in one of the following ways:*

- *Local CA installation: as described in “End-User Interaction (Local CA Only)” on page 140.*
- *Remote CA installation: end-users need to request a certificate by means determined by the administrator.*

## Backing Up the Certificate Settings (All CAs)

Make sure that you have a backup of the private key. If not, create backup files via the certificate store. After the initial backup, make sure to back up the certificate settings from time to time, especially before any IAG software upgrade or installation, or any other changes to system settings.



### Tip

For instructions on how to back up the certificate, see <http://www.thawte.com/ssl-digital-certificates/technical-support/ssl/iis6.html>




## End-User Interaction (Local CA Only)




### Note

This section is applicable only if the CA is installed locally, on the IAG.

Once the Certified Endpoint Enrollment application is added to the trunk, the appropriate tools need to be added to the end-user pages. The available tools depend on whether you are using the default portal homepage or your own custom page, as follows:

- If you use the default portal homepage, the following happens automatically:
  - The Certified Endpoint button  is added to the Whale toolbar.
  - A Certified Endpoint link  [Make this computer certified](#)  is added to the portal homepage.
- If you use a custom page, you must ensure that one or both of the following are added to the page so that users can request Certified Endpoint status:

- The Whale toolbar, where the Certified Endpoint button  is automatically added. For a description of how you can use the Whale toolbar with a custom homepage, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to the section “Using a Custom Portal Homepage”, to step 4 on page 62.
- A Certified Endpoint link, which can be added as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Adding Application Links on a Custom Portal Homepage” on page 63.

In order for an endpoint computer to be granted Certified Endpoint status, end-users have to take the following steps:

- Submit a request for a certificate to be issued, as described in “Requesting Certified Endpoint Status” on page 142.
- If so defined in the certification authority policy, check whether the request for Certified Endpoint status has been approved, as described in “Checking the Certified Endpoint Request Status” on page 144.
- Once the Certified Endpoint status has been approved, install the certificate, as described in “Installing the Certificate and Logging In as a Certified Endpoint User” on page 144.



#### Note

The Certified Endpoint button is not displayed on handheld devices. In order to grant Certified Endpoint status to a handheld device, do the following:

- Request Certified Endpoint status on a remote PC.  
Note that the certificate must be created with the option to export the private key.
- Once the request has been approved, install the certificate on the remote PC.
- Export the certificate to the handheld device. Make sure that you also export the private key.



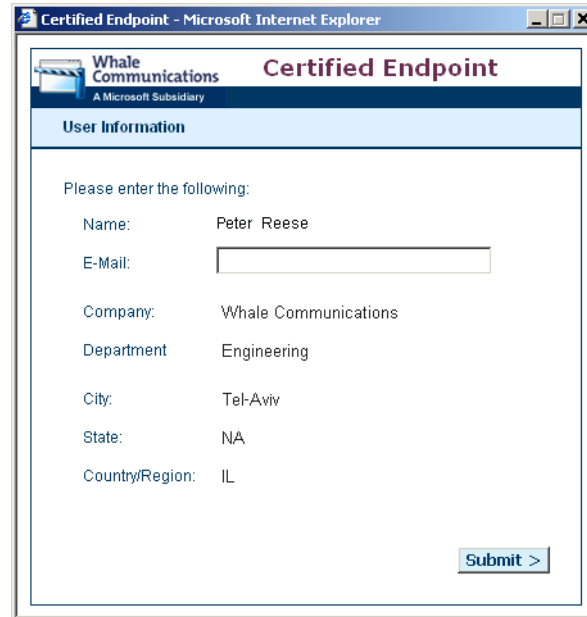
#### Tip

The endpoint enrollment pages shown in the procedures that follow are the default pages supplied with the IAG. For instructions on how you can customize the look-and-feel of the pages, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Customizing Certified Endpoint Enrollment Pages” on page 67.

## Requesting Certified Endpoint Status

*To submit a request to make a computer a Certified Endpoint:*

1. Access the portal and click the Certified Endpoint button or link.  
*The Certified Endpoint - User Information window is displayed.*



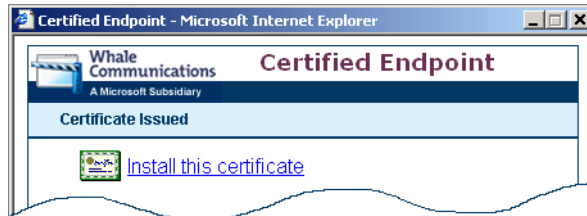
2. Enter the required user information in the text box or boxes.



### Note

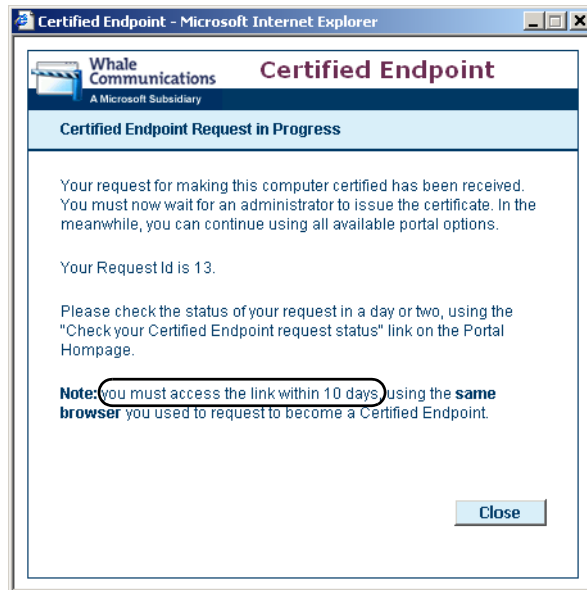
The fields available in this window may vary, according to the settings defined during the configuration of the Certified Endpoint feature, as described in “Customizing User Information Properties” on page 132.

3. At the bottom right corner of the screen, click **Submit >**.  
*A message is displayed, prompting you to confirm the request for a certificate.*
4. Click **Yes** to request a certificate.  
*Depending on your organization’s certification policy, one of the following is displayed:*
  - *If the certificate is issued immediately, you are notified in the Certified Endpoint window that the certificate has been issued, and are prompted to install the certificate on your computer.*



Refer to “Installing the Certificate and Logging In as a Certified Endpoint User” on page 144 for further details.

- If the certificate is not issued immediately, the Certified Endpoint window indicates that the Certified Endpoint request is in progress.



Close the Certified Endpoint window. Your computer is not yet certified. You can continue to use the available portal options as before.

Within the period of time specified on the Certified Endpoint window, you must use the same browser to check the status of your request, as described in “Checking the Certified Endpoint Request Status” on page 144.

## Checking the Certified Endpoint Request Status

The administrator needs to approve your request for Certified Endpoint status and issue a certificate accordingly. You must periodically check the status of the request and install the certificate, within the period of time specified in the Certified Endpoint window.



### Note

If you do not install the certificate within the specified time period, you must re-initiate the request process.

***To check whether the request for Certified Endpoint status has been approved:***

1. Access the portal and click the Certified Endpoint button or link.  
*One of the following is displayed in the Certified Endpoint window:*

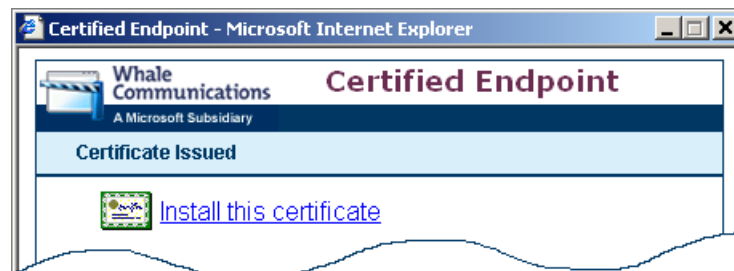
Message	Do This
Certificate Issued	Proceed to “Installing the Certificate and Logging In as a Certified Endpoint User” on page 144.
Certified Endpoint Request in Progress	Check again within the period of time specified on the Certified Endpoint window (described on page 144), using the same browser.
Certified Endpoint Request Denied	Speak to your administrator before requesting Certified Endpoint status again.

## Installing the Certificate and Logging In as a Certified Endpoint User

Once your Certified Endpoint status has been approved and a certificate issued, you must install the certificate on your computer in order to complete the Certified Endpoint process.

***To install the certificate and log in as a Certified Endpoint user:***

1. Access the portal and click the Certified Endpoint button or link.  
*The Certified Endpoint - Certificate Issued window is displayed.*



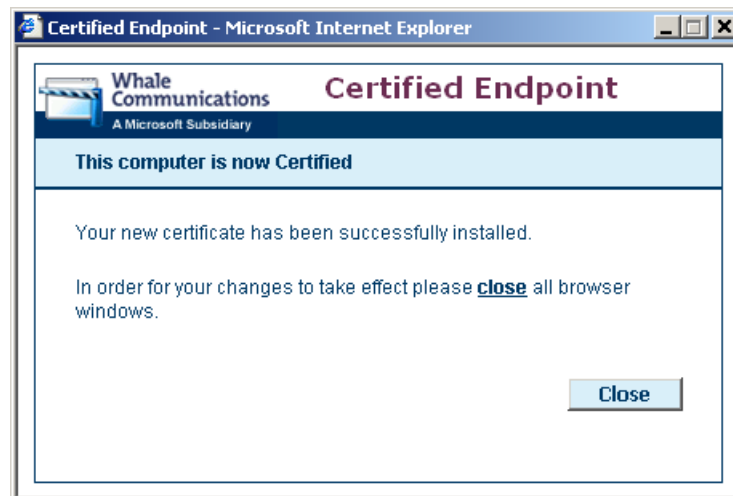


2. Click “Install this certificate” to add the certificate to your computer.
  - *If you are using Microsoft Internet Explorer, the certificate is installed on your computer. Proceed to step 4 of this procedure.*
  - *If you are using a different browser, a certificate download dialog box is displayed, in this example the Downloading Certificate dialog box, displayed by Netscape Navigator.*



3. Click **OK**.

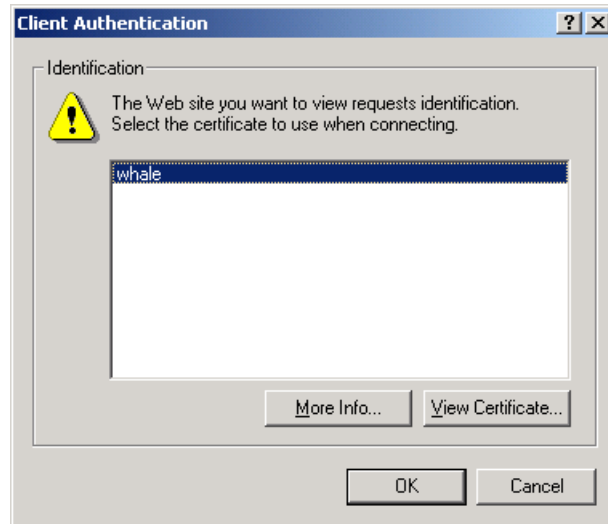
*The certificate is installed on the computer. Once the certificate is installed, the Certified Endpoint window indicates that this computer is now certified.*



4. Click **Close** to close the Certified Endpoint window.

*Your computer is now granted Certified Endpoint privileges, as set by the administrator.*
5. Close all open browser windows, then re-access the portal and log in.

*The Client Authentication dialog box is displayed.*




6. Select a certificate from the list and click **OK**.

*The login process is complete, and you are logged on as a Certified Endpoint. The Certified Endpoint button or link is no longer available.*



#### Tip

If your portal homepage includes the Whale toolbar, you can click  to access the System Information window, in order to verify your certified endpoint status. There should be a checkmark next to “Certified Endpoint”.

## Viewing and Processing Certificate Requests (Local CA Only)

After a certificate is requested, depending on your Certificate Authority Policy, you can perform one of the following actions for the certificate request:

- Issue a certificate for the pending request.
- Deny a certificate for the pending request.

You can view requests for Certificate Authorities in the Certification Authority window.

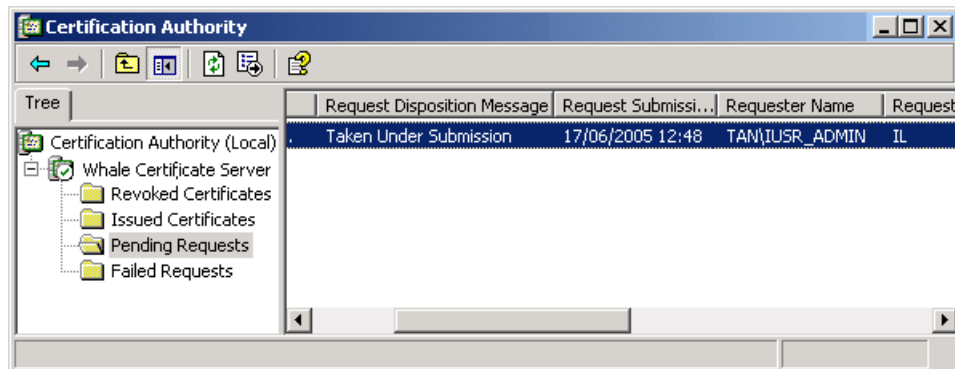
#### *To view certificate information:*

1. In the Windows desktop, click **Start** and select **Programs > Administrative Tools > Certification Authority**.  
*The Certification Authority window is displayed.*
2. Select the Certification Authority, and double-click one of the following folders:

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests

*The information in the selected folder is displayed in the right pane of the Certification Authority window.*

In the example below, the Pending Requests folder was selected and all pending requests are displayed.



#### ***To issue a certificate from a pending request:***

1. Right-click the pending request in the Certification Authority window and select **All Tasks > Issue**.

*The certificate is issued. The pending request is moved from the Pending Requests folder to the Issued Certificates folder.*

#### ***To deny a pending request for a certificate:***

1. Right-click the pending request in the Certification Authority window and select **All Tasks > Deny**.

*The pending request is denied and is placed in the Failed Requests folder. When the end-user checks the status of the Certified Endpoint request, a screen is displayed informing the end-user that the request was denied.*

## **Whale Client Components**

Whale Client Components are installed on the endpoint computer, in order to enable some of the IAG features. The components include the following:

- Whale Component Manager ActiveX object, which downloads, installs, manages, and removes all the Whale Client Components.
- Attachment Wiper ActiveX component; for details, refer to “Attachment Wiper” on page 110.

- Client Trace utility, used for support purposes.
- Endpoint Detection ActiveX component; for details, refer to “Endpoint Policies” on page 93.
- Non-web tunneling components, including:
  - SSL Wrapper ActiveX component; for details, refer to Chapter 6: “SSL Wrapper”.
  - Socket Forwarding component; for details, refer to “Technology Overview” on page 172.
  - Socket Forwarding Helper utility, used for support purposes.
  - Network Connector component; for details, refer to Chapter 7: “Network Connector”.

Since the Whale Client Components provide a wide range of options and features, when a user first accesses the site, the IAG detects whether it can install the components on the endpoint computer, according to the prerequisites described in “Prerequisites for Installing the Whale Client Components” on page 151.

- On endpoint computers that meet those prerequisites, the Whale Component Manager installs the Client Components, as required.
- On endpoint computers that do not meet these prerequisites, such as computers running non-Windows operating systems, or an Internet Explorer browser where the download and launching of signed ActiveX objects is disabled, the Client Components are not installed.

In cases where the SSL Wrapper ActiveX component is not installed on the computer, when the user attempts to access a non-web application, the SSL Wrapper Java™ applet runs on the endpoint computer, in order to enable access to the application. The Java applet provides only SSL Wrapper functionality, and does not enable any of the other features that are enabled by the Whale Client Components, such as endpoint policies or the Attachment Wiper.

The descriptions in this section do not apply to the SSL Wrapper Java applet. The applet, including the prerequisites for running it on the endpoint computer, is described in Chapter 6: “SSL Wrapper”.



### Note

You can disable component installation in the Session tab of the Advanced Trunk Configuration window, as follows:

- Activating the option “Disable Component Installation and Activation” disables the installation and activation of all the Whale Client Components on endpoint computers, including the SSL Wrapper Java applet, thus disabling all the features that are enabled by those components. It also disables the Certified Endpoints feature. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Session Configuration” on page 133.
- Activating the option “Uninstall Socket Forwarding Component” disables the installation of the Socket Forwarding component on endpoint computers and removes this component from all endpoint computers when users next access the site. For details, refer to “Endpoint Settings” on page 108.

This section describes:

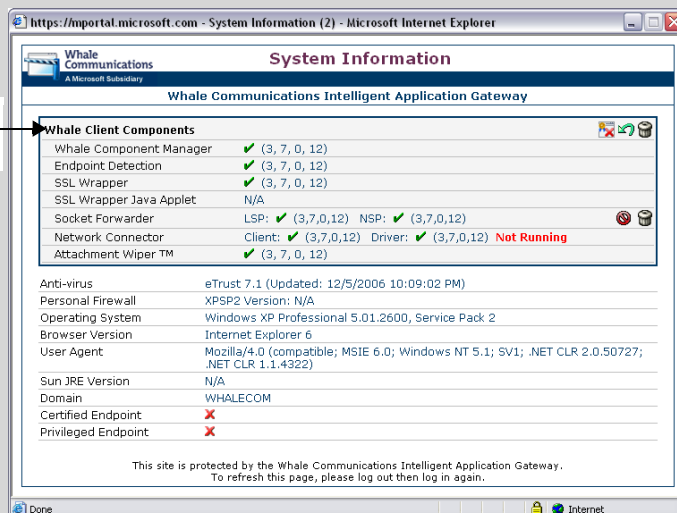
- The conditions under which the components are installed and run, and the available installation modes, in “Installing and Running the Components on Endpoint Computers” on page 150.
- How to configure users’ Trusted Sites lists, so that the Whale Client Components can verify that the site is trusted, in “IAG Trusted Sites” on page 160.
- How users can reset the Whale Component Manager settings on their computer to the default values, in “Restoring the Whale Client Components Defaults” on page 165.
- How users can remove the components from their computer, and how you can enforce the removal of the Socket Forwarding component from remote computers, in “Uninstalling the Whale Client Components” on page 167.



## Tip

Users can check whether the Whale Client Components are installed on their computer in the portal's System Information window:

Whale Client Components



## Installing and Running the Components on Endpoint Computers

This section describes how users can install and run the Whale Client Components on their computer, including:

- “Prerequisites for Installing the Whale Client Components” on page 151.
- The available installation modes, including:
  - “Online Whale Client Components Installation” on page 152.
  - “Whale Client Components Installer” on page 154.
  - “Offline Whale Client Components Installation” on page 157.
- “Prerequisites for Running the Whale Client Components” on page 159

Once the Client Components are installed on the endpoint computer, the Whale Component Manager updates installed components as updates become available.



## Note

- The installation and removal of the components may require a restart of the browser or of the computer. Users are notified accordingly.
- If removal of the components is not complete because a user selected not to restart the browser or computer, no updates will be installed.

## Prerequisites for Installing the Whale Client Components

Table 18 on page 151 lists the prerequisites on the endpoint computer for the installation of the Whale Client Components, including prerequisites for each of the available installation modes.

**Table 18. Prerequisites for Installing the Whale Client Components**

Prerequisite	Online Installation*	Component Installer	Offline Installation
Operating system: Windows 2000 or higher	✓	✓	✓
Browser: Internet Explorer 6.0 or higher	✓	✓**	✗
Browser enables download of signed ActiveX objects	✓	✗	✗
Browser enables running of signed ActiveX objects	✓	✗	✗
On Windows 2000, XP, and 2003, power-user privileges***	✓	✓	✓

\* For the Socket Forwarding component: the endpoint computer must meet the “Install Socket Forwarding Component Policy”, set in the Session tab, in the “Endpoint Policies” area. For details, refer to “Endpoint Policies” on page 93.

\*\* For the Network Connector component: any browser supported by the IAG. For a list of supported browsers, see “Supported Browsers” on page 19.

\*\*\* For the Socket Forwarding and Network Connector components: Administrator privileges.

## Online Whale Client Components Installation



### Note

The Whale Client Components are only installed on the endpoint computer in online installation mode if component installation is enabled for the trunk, that is, the option “Disable Component Installation and Activation” is **not** selected in the Session tab of the Advanced Trunk Configuration window.

This installation mode is suitable for end-users who have ActiveX download rights on an Internet Explorer browser, and are logged in with power-user or Administrator privileges.

In this mode, as soon as users try to access the site, prior to the Login stage, the IAG downloads the Whale Component Manager onto their computer. Once the Component Manager is installed on the endpoint computer, it determines the need for the installation of the rest of the components each time the user accesses the site, and installs them as follows:

- By default, the following components are installed automatically:
  - Attachment Wiper
  - Client Trace utility
  - Endpoint Detection

If required, you can configure other components that will be installed automatically, as described in “Configuring the List of Automatically Installed Components” on page 152.

- The rest of the components are installed as required. **For example:** when the user accesses a non-web application for the first time, the Component Manager installs the SSL Wrapper component.

### Configuring the List of Automatically Installed Components

This section describes how you can add components to the default list of components that the Component Manager installs automatically on the endpoint computer.

#### *To add components to the list of automatically installed components:*

1. At the IAG, access the following custom folder; if it does not exist, create it:  
`...\Whale-Com\e-Gap\von\InternalSite\inc\CustomUpdate`
2. Under the folder you accessed in step 1, create the following file:



- If you wish the changes you make to affect all trunks, create the file `InstallXml.inc`.
- If you wish the changes you make to be applied to a specific trunk, create the following file:

`<Trunk_Name><Secure(0=no/1=yes)>InstallXml.inc`

**For example:** for an HTTPS trunk named “MyTrunk”, create the file `mytrunk1InstallXml.inc`

If such a file already exists, use the existing file.

3. Copy the following lines into the file you created in step 2:

```
<%
Response.write "<Component Name=""SSL Wrapper"" ID=""1"" Install=""1"" />"
Response.write "<Component Name=""Network Connector"" ID=""17""
    Install=""1"" />"

if uninstall_1ln = "0" and remove_1ln = "0" then

    Response.write "<Component Name=""Socket Forwarding"" ID=""8""
        Install=""1"" />"
    Response.write "<Component Name=""Socket Forwarding activation: Basic""
        ID=""33"" Install=""1"" />"
    Response.write "<Component Name=""Socket Forwarding activation: Extended""
        ID=""65"" Install=""1"" />"
    Response.write "<Component Name=""Socket Forwarding activation: VPN""
        ID=""129"" Install=""1"" />"

end if
%>
```

4. Comment out the lines that are not applicable by adding ' at beginning of the line, where:
  - The following line adds the SSL Wrapper component to the list of automatically installed components:

```
Response.write "<Component Name=""SSL Wrapper"" ID=""1""
Install=""1"" />"
```

- The following line adds the Network Connector component to the list:

```
Response.write "<Component Name=""Network Connector""
ID=""17"" Install=""1"" />"
```

- The following line adds the Socket Forwarding component to the list:

```
Response.write "<Component Name=""Socket Forwarding""
ID=""8"" Install=""1"" />"
```

In addition, the following lines enable the Socket Forwarding activation mode:

**Basic mode:**

```
Response.write "<Component Name=""Socket Forwarding  
activation: Basic"" ID=""33"" Install=""1"" />"
```

**Extended mode:**

```
Response.write "<Component Name=""Socket Forwarding  
activation: Extended"" ID=""65"" Install=""1"" />"
```

**VPN mode:**

```
Response.write "<Component Name=""Socket Forwarding  
activation: VPN"" ID=""129"" Install=""1"" />"
```

Make sure the required Socket Forwarding Activation mode is enabled; if the component is used by multiple applications, in various Activation modes, make sure all the applicable modes are enabled.

*When users next access the site, the automatic component installation includes the additional components you defined here.*

## Whale Client Components Installer

This installation mode is suitable for end-users who do not have ActiveX download rights on an Internet Explorer browser, and are logged in with power-user or Administrator privileges. It can also be used on browsers other than Internet Explorer, by end-users who are logged in with Administrator privileges, to install the Network Connector component.

In this mode, users can download an auto-install file onto their computer, using either an “installer” toolbar button, or a link on the portal homepage. They can then log out of the site, and use this file to install the components in an offline mode.

In order to install the Whale Client Components in this mode, the following steps have to be taken:

- You need to configure the installer, as described in “Configuring the Whale Client Components Installer” on page 154.
- End-users need to install the components on their computer, as described in “Installing the Whale Client Components via the Installer” on page 156.

### Configuring the Whale Client Components Installer

In order for end-users to be able to use the Whale Client Components Installer, you need to add a link to the auto-install file on the portal homepage:

- If you use the Whale toolbar with the portal homepage, enable the “Whale Client Components Installer” button and define which installation file is used. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Content Changes in the Default Portal Homepage” on page 57.



#### Note

When using the Whale toolbar, the button is only visible on endpoint computers running a Windows operating system.

- If you use a custom homepage that does not include the Whale toolbar, add a link to the file on the custom page. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Adding Links to IAG Features on a Custom Homepage” on page 66.



#### Tip

For detailed information on the customization of the portal homepage and the Whale toolbar, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Portal Homepage Configuration” on page 54.

The following table lists the files that can be used for the installation of the Client Components, including which components are installed on the endpoint computer by each file.

**Table 19. Whale Client Components Installer—Installation Options**

File	Installs the following components:
WhlClientSetup-Basic.exe	Basic components: Attachment Wiper, Client Trace Utility, Endpoint Detection, SSL Wrapper ActiveX component.
WhlClientSetup-NetworkConnector.exe	Basic components + Network Connector component.
WhlClientSetup-SocketForwarder.exe	Basic components + Socket Forwarding component.
WhlClientSetup-All.exe	Basic components + Network Connector component + Socket Forwarding component.
WhlClientSetup-NetworkConnectorOnly.exe	Network Connector component only, without the basic components.




### Note

- If the installation detects that Whale Client Components are already installed on the computer, it upgrades any of the components that are of older versions, even if their installation is not enabled in the current installation configuration.
- When using the Whale toolbar, the “Network Connector component only” installer is always downloaded on browsers other than Internet Explorer, such as Netscape Navigator or Mozilla Firefox, so that the Network Connector client can run via the SSL Wrapper Java applet.


## Installing the Whale Client Components via the Installer

Once you configure the Whale Client Components Installer, as described in “Configuring the Whale Client Components Installer” on page 154, users can download the installer onto their computer using the installer button or link on the portal homepage.

### *To install the Whale Client Components via the Installer:*

1. At the portal homepage, click  on the Whale toolbar, or, if the Whale toolbar is not used, click the link to the installer.  
*The file that was defined during the configuration of the button or link is downloaded onto the computer. When prompted, select to save the file.*

2. Log out of the portal, using the site’s logout mechanism, and close all the browser windows that were opened through the portal.

**For example:** in sites that use the Whale toolbar, click  Logout to log out of the portal.

3. Run the file you downloaded in step 1.  
*The Whale Client Components Installation Wizard starts.*
4. Follow the instructions on the screen to complete the Wizard and install the components on the computer.

## Offline Whale Client Components Installation

This installation mode is suitable for end-users who don't have ActiveX download rights on an Internet Explorer browser, and are non-privileged (guest/user) users. In this setup, the administrator has to log in to the endpoint computer with power-user or Administrator privileges, and install the components before the user accesses the site.

In order to enable offline component installation, take the following steps:

- Configure the settings of the offline component installation, as described in “Configuring Offline Component Installation” on page 157.
- Deploy the component library to end-users, as described in “Deploying Offline Component Installation” on page 158.



### Note

- Inform users that during component installation, they should not access the portal homepage or any other location within the site.
- If the installation detects that Whale Client Components are already installed on the computer, it upgrades any of the components that are of older versions, even if their installation is not enabled in the current installation configuration.

## Configuring Offline Component Installation

You can configure the following aspects of the offline component installation:

- Determine which components users will be able to install. For example, you can select to enable the SSL Wrapper component, but not the Socket Forwarding component.
- Replace the graphic that appears the installation screens.
- Enable or disable Custom installation mode, where users can select which of the enabled components to install. If Custom mode is disabled, the installation will run in Typical mode, where all enabled components are installed.



### Note

Custom mode is only applicable when you deploy the components installation in Interactive mode, as described in “Deploying Offline Component Installation” on page 158.

### ***To configure offline component installation:***

1. Copy the file `ComponentsConfig.xml` from this location:  
...\\Whale-Com\\e-Gap\\utils\\OfflineClientSetup  
To:  
...\\Whale-Com\\e-Gap\\utils\\OfflineClientSetup\\CustomUpdate
2. In the file you copied in step 1, determine whether to enable the installation of each component or not, whereas:
  - `Install="1":` install
  - `Install="0":` don't install

#### **For example:**

The following line enables the installation of the Network Connector component:

```
<Component Name="Network Connector" ID="17" Install="1"/>
```

3. Still in the file you copied in step 1, determine whether to enable Custom installation mode, whereas:
  - `<CustomSetup Enable="1"/>`: enable Custom installation
  - `<CustomSetup Enable="0"/>`: disable Custom installation
4. In order to replace the graphic that appears in the installation screens, place your graphic in the following location:  
...\\Whale-Com\\e-Gap\\utils\\OfflineClientSetup\\CustomUpdate  
The replacement graphic must be:
  - A Bitmap (.bmp) format graphic
  - File name: `logo.bmp`
  - Size of the graphic must be the same size as the original graphic:  
Width 118 x Height 238 pixels

### **Deploying Offline Component Installation**

Once you configure the installation settings, as required, deploy the installation to end-users. You can deploy the installation in one of two modes:

- Silent mode, where no user intervention is required. Note that, when you use this deployment method, Custom installation is not applicable.
- Interactive mode, where an installation wizard guides the user through the installation.

Both deployment methods are described in this section.

### ***To deploy the offline component installation in Silent mode:***

1. Use the following command line to execute component installation in Silent mode:

```
...\Whale-Com\e-Gap\utils\OfflineClientSetup\Setup.exe -s
```

**For example:** use a batch file to run this command from the offline client setup location.

*Once this command is run on an endpoint computer, the Whale Client Components are installed on the computer with no user intervention.*

### ***To deploy the offline component installation in Interactive mode:***

1. Deploy the following folder, including all files and subfolders:

```
...\Whale-Com\e-Gap\utils\OfflineClientSetup
```

2. Advise users to double-click the file Setup.exe, located under this folder.

*The Whale Client Components Installation wizard starts. Users can follow the instructions on the screen to complete the wizard and install the components on their computer.*

## **Prerequisites for Running the Whale Client Components**

Table 20 on page 159 lists the prerequisites on the endpoint computer for running the Whale Client Components, once they are installed on the computer, including:

- Prerequisites for running the ActiveX components: Attachment Wiper, Endpoint Detection, and SSL Wrapper components.
- Prerequisites for running the Socket Forwarding component.
- Prerequisites for running the Network Connector component, both via the SSL Wrapper ActiveX component and via the SSL Wrapper Java applet.

There are no special prerequisites for running the Client Trace and Socket Forwarding Helper utilities.

**Table 20. Prerequisites for Running the Client Component**

<b>Prerequisite</b>	<b>ActiveX Components</b>	<b>Socket Forwarder</b>	<b>Network Connector via ActiveX SSL Wrapper</b>	<b>Network Connector via Java SSL Wrapper</b>
Operating system	Windows 2000 or higher	Windows 2000 or higher	Windows 2000 or higher	Windows 2000 or higher

**Table 20. Prerequisites for Running the Client Component (Cont'd)**

<b>Prerequisite</b>	<b>ActiveX Components</b>	<b>Socket Forwarder</b>	<b>Network Connector via ActiveX SSL Wrapper</b>	<b>Network Connector via Java SSL Wrapper</b>
Browser	Internet Explorer 6.0 or higher	Internet Explorer 6.0 or higher	Internet Explorer 6.0 or higher	Java SSL Wrapper supported browser *
Browser enables running of signed ActiveX objects	Required	Required	Required	NA
User privileges	Any	Any **	Administrator	Administrator
Windows DHCP Client service	NA	NA	Must be running	Must be running

\* The Java applet is supported on the browsers that are supported by the IAG, as listed in “Supported Browsers” on page 19.

\*\* Some applications might require Administrator privileges. For details, see “Technology Overview” on page 172.

## IAG Trusted Sites

This section describes how to configure the end-user’s Trusted Sites list. The list should contain each of the IAG sites the user needs to access, so that the Whale Client Components can verify it is trusted.



### Tip

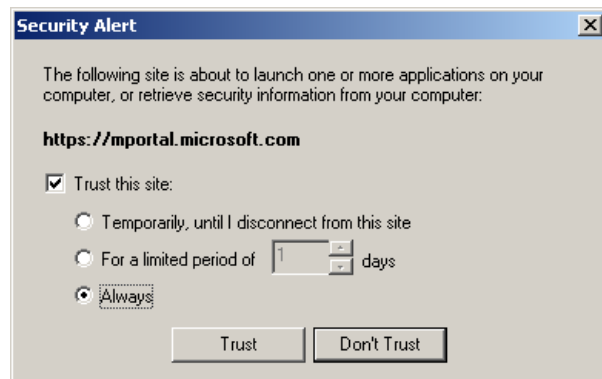
For a description of when the Whale Client Components verify that the IAG site is trusted, refer to:

- “Endpoint Detection” on page 95.
- “SSL Wrapper” on page 171.

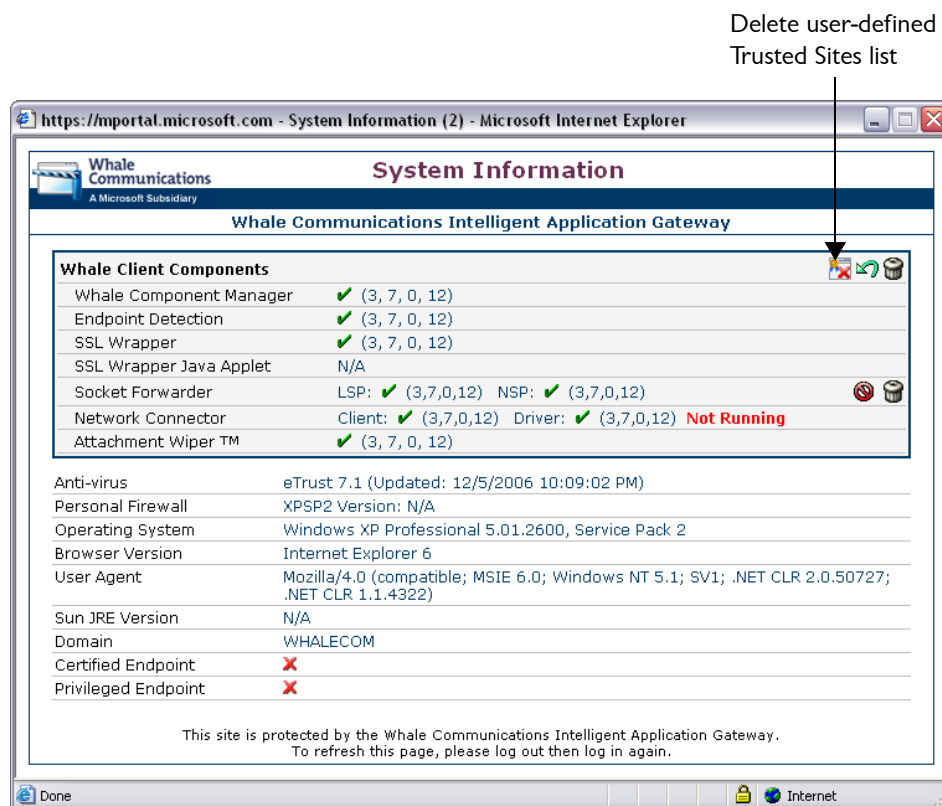
An IAG site can be added to the user’s Trusted Sites list on the endpoint in one of two ways:



- The domain administrator can remotely add the site or a number of sites to the user's Trusted Sites list with no user intervention. For details, refer to “Remote Configuration of Users’ Trusted Sites Lists” on page 162.
- Users can add the IAG site to their Trusted Sites list on demand, as shown in the sample prompt below:



Once users add a site or a number of sites to the list, they can remove them from the list via the System Information window, by clicking the button “Delete user-defined Trusted Sites list”; this removes all the user-defined sites from the list:



## Remote Configuration of Users' Trusted Sites Lists

This section describes how the domain administrator can remotely manage end-users' Trusted Sites list, so that users are not prompted when the Whale Client Components verify that the IAG site is trusted.

You control the configuration of the Trusted Sites list using a Registry key that you add to the user's endpoint, which you can deploy as you do any other managed configuration, for example via the Windows Logon Script, or as part of your Group Policy. You can also use this key to control which other sites users can add on demand to their IAG Trusted Sites list.

### *To configure the Trusted Sites list:*

1. At the IAG, access the following folder:  
`...\Whale-Com\e-Gap\von\InternalSite\samples`
2. From the `samples` folder, copy the following files to an external location; make sure they reside in the same folder:  
`CheckSite.bat`  
`CheckSite.reg`
3. At the location where you copied the files, edit the file `CheckSite.reg`, as described in Table 21 on page 163.

The file provides a sample configuration, which adds the following sites to users' Trusted Sites lists:

- `https://www.microsoft.com`
- `https://www.myPortal.com`

Note the following in the sample configuration:

- Users can add sites to the Trusted Sites list on demand; they cannot, however, add HTTP sites to the list.
  - Users will not be prompted if a trusted site's certificate is invalid. In this case, detection will not be performed.
  - Users will be prompted if an untrusted site's certificate is invalid, and will be able to add it to the Trusted Sites list on demand.
4. Deploy the `CheckSite.bat` file to the end-users whose Trusted Sites list you wish to configure.



#### **Note**

Make sure the file `CheckSite.reg` resides in the same folder as the file `CheckSite.bat`.

*At the endpoints where you deployed the configuration, the following Registry key is added or updated according to your definitions:*

`HKEY_CURRENT_USER\Software\WhaleCom\Client\CheckSite`

*The Trusted Sites configuration is applied on the endpoint, with the settings you defined here.*

**Table 21. Values of CheckSite.reg**

Value	Type	Description	Data
Managed	DWORD	Mandatory. Determines whether this configuration is applied, and whether the computer's Trusted Sites list is managed remotely or not.	<ul style="list-style-type: none"> <li>• 1: managed.</li> <li>• 0: unmanaged.</li> </ul> <p><b>Note:</b> Any number other than 1 is considered a zero.</p>
CanAddSites	DWORD	Optional. Determines whether the user can add other sites to the Trusted Sites list on demand.	<ul style="list-style-type: none"> <li>• 1: users can add sites to list.</li> <li>• 0: users cannot add sites to list.</li> </ul> <p>If this value is not defined, users cannot add sites to the list.</p>
CanAddHttpSites	DWORD	Optional. Determines whether the user can add HTTP sites to the list on demand. Applicable only when the value of "CanAddSites" is 1.	<ul style="list-style-type: none"> <li>• 1: users can add HTTP sites to Trusted Sites list.</li> <li>• 0: users cannot add HTTP sites to Trusted Sites list.</li> </ul> <p>If this value is not defined, users cannot add HTTP sites to the list.</p>
PromptInvalidCertTrusted	DWORD	Optional. Determines behavior when a trusted site's certificate is invalid.	<ul style="list-style-type: none"> <li>• 1: users are prompted and can select whether to add the site to the Trusted Sites list or not.</li> <li>• 0: users are not prompted; access to the site is denied.</li> </ul> <p>If this value is not defined, users are not prompted.</p>

**Table 2I. Values of CheckSite.reg (Cont'd)**

Value	Type	Description	Data
PromptInvalidCertUntrusted	DWORD	Optional. Determines whether users are prompted when an untrusted site's certificate is invalid.	<ul style="list-style-type: none"> <li>• 1: users are prompted and can select whether to add the site to the Trusted Sites list or not.</li> <li>• 0: users are not prompted; access to the site is denied.</li> </ul> <p>If this value is not defined, users are prompted.</p>
TrustedSite<#>	String	Mandatory. List of trusted sites.	<p>Define a site as follows: *</p> <ul style="list-style-type: none"> <li>• Schema: HTTPS or HTTP**</li> <li>• Host: FQDN or IP</li> <li>• Port number; optional for default ports (443 and 80).</li> </ul>
PilotExpirationTime	String	<p>Optional. End date of "pilot" mode. While in this mode, the identity of sites on the Trusted Sites list you defined here is not verified.</p> <p><b>Caution:</b> Use this option for a very limited time, and not during system up-time.</p>	<p>Date, using the following format:</p> <p>mm/dd/yyyy</p> <p>By default, no pilot period is configured.</p>

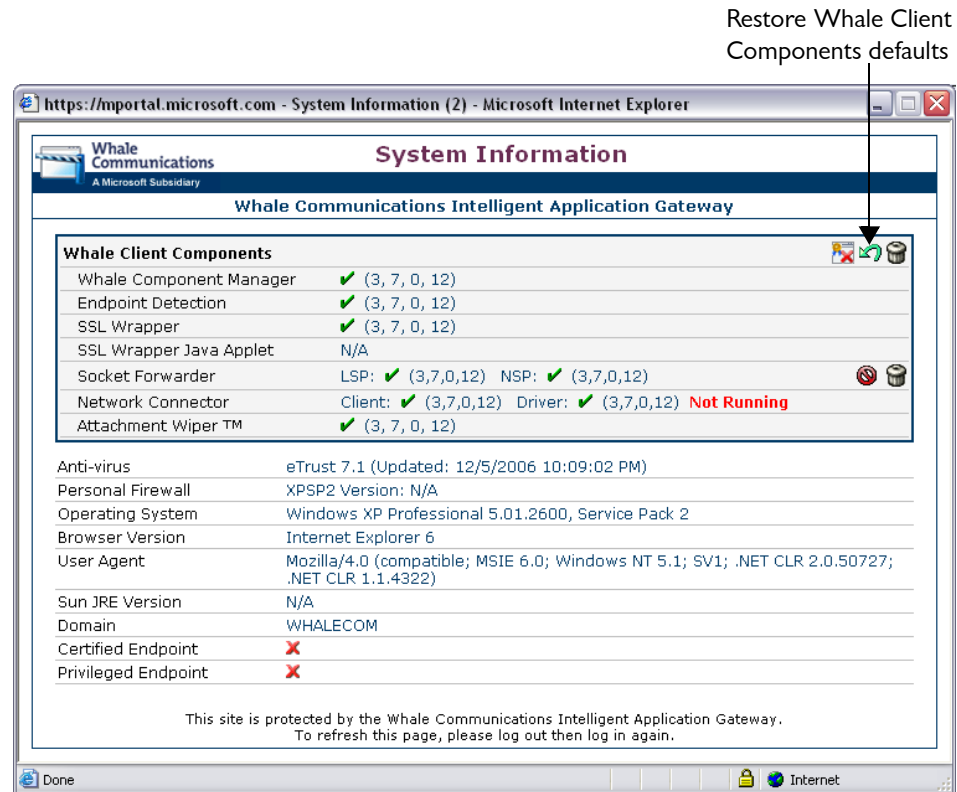
\* Values are case-insensitive.

\*\* The identity of trusted HTTP sites will not be verified, since they do not use a server certificate.

## Restoring the Whale Client Components Defaults

End-users can restore the Whale Client Components settings on their computer to the default values in one of two ways:

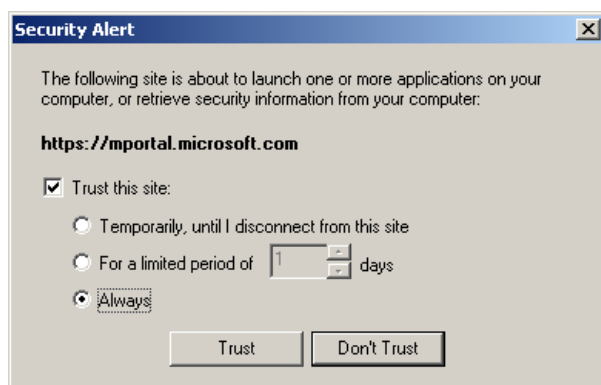
- In the System Information window, which they access from the portal homepage, by clicking the button “Restore Whale Client Components defaults”:



- By uninstalling the Whale Client Components from their computers, as described in “Uninstalling the Whale Client Components” on page 167.

Restoring the Whale Client Components defaults enables users to receive the following notifications, even in cases where the user previously selected the option “Don’t show me this message again” when the message was displayed. Once the defaults are restored, whenever applicable, the user receives notifications that are displayed when:

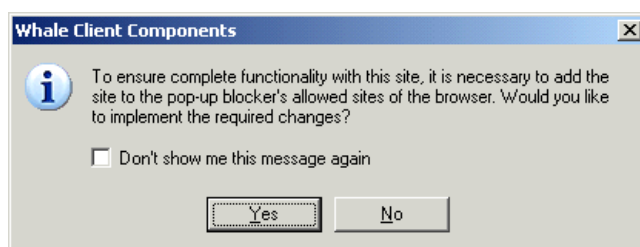
- It is necessary to add the site to the user's Trusted Sites list:



### Note

Restoring the defaults deletes only sites that the user added to the Trusted Sites list; it does not delete the administrator-configured sites from the list. For details on adding sites to the list, refer to “IAG Trusted Sites” on page 160.

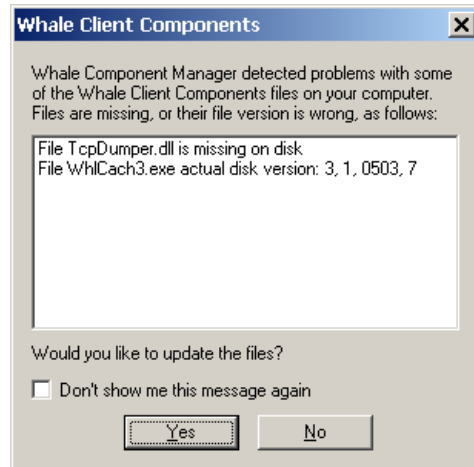
- It is necessary to add the site to the browser's pop-up blocker's allowed site:



### Tip

For details regarding this option, refer to “Endpoint Settings” on page 108.

- The Whale Component Manager detects problems with some of the Whale Client Components files on the computer:



- The browser has to be restarted after the installation of the Socket Forwarding component of the Whale Client Components:



### Tip

For details on the Socket Forwarding component, which can be used with the SSL Wrapper, refer to Chapter 6: “SSL Wrapper”.

## Uninstalling the Whale Client Components

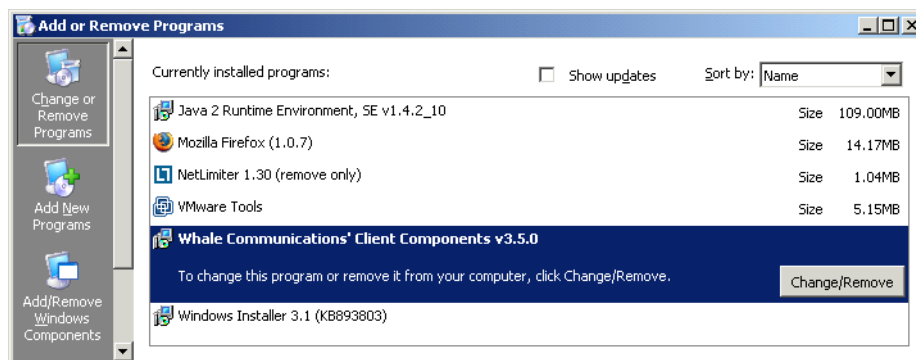


### Note

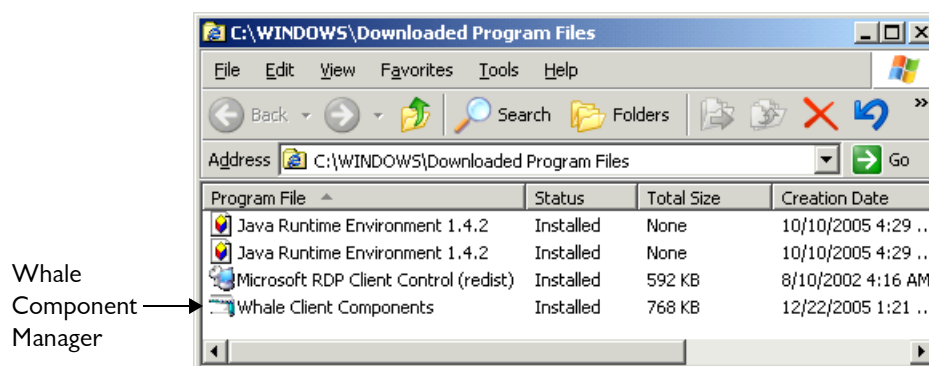
- Uninstalling the Client Components restores the Whale Component Manager settings on the endpoint computer to the default values, as described in “Restoring the Whale Client Components Defaults” on page 165.
- For Windows 2000, Windows XP, and Windows 2003 systems, power-user access level is required for the current user.


Once the Client Components are installed on the endpoint computer, they can be uninstalled as follows:

- In the Windows desktop, click **[Start]** and select **Settings > Control Panel > Add/Remove Programs** or **Add or Remove Programs**. Locate the version of the Whale Client Components you wish to remove, click **[Change/Remove]**, and follow the instructions on the screen to remove the components.



- Users can view the Whale Component Manager in the Downloaded Program Files folder. From this location, users are able to uninstall all versions of installed components as one unit.



- From the portal homepage, users can access the System Information window (by clicking ), where they can select to uninstall all the components, uninstall the Socket Forwarding component only, or enable and disable the Socket Forwarding component.



https://portal.microsoft.com - System Information (2) - Microsoft Internet Explorer

Whale Communications  
A Microsoft Subsidiary

### System Information

Whale Communications Intelligent Application Gateway

Whale Client Components	
Whale Component Manager	✓ (3, 7, 0, 12)
Endpoint Detection	✓ (3, 7, 0, 12)
SSL Wrapper	✓ (3, 7, 0, 12)
SSL Wrapper Java Applet	N/A
Socket Forwarder	LSP: ✓ (3,7,0,12) NSP: ✓ (3,7,0,12) <b>Not Running</b>
Network Connector	Client: ✓ (3,7,0,12) Driver: ✓ (3,7,0,12)
Attachment Wiper TM	✓ (3, 7, 0, 12)

Anti-virus eTrust 7.1 (Updated: 12/5/2006 10:09:02 PM)

Personal Firewall XPSP2 Version: N/A

Operating System Windows XP Professional 5.01.2600, Service Pack 2

Browser Version Internet Explorer 6

User Agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)

Sun JRE Version N/A

Domain WHALECOM

Certified Endpoint ✗

Privileged Endpoint ✗

This site is protected by the Whale Communications Intelligent Application Gateway.  
To refresh this page, please log out then log in again.

Done Internet

Uninstall all Whale Client Components

Uninstall Socket Forwarding component

Enable/disable Socket Forwarding component

- You can enforce the removal of the Socket Forwarding client component from all endpoint computers that access the site, by activating the option “Uninstall Socket Forwarding Component” in the Session tab of the Advanced Trunk Configuration window. For details, refer to “Endpoint Settings” on page 108.



# Chapter 6

## SSL Wrapper



### Note

- The SSL Wrapper components are part of the Whale Client Components. For details, refer to “Whale Client Components” on page 147.
- When working with SSL Wrapper applications via an HTTP trunk, tunneled traffic is not encrypted.

The SSL Wrapper provides secure SSL connectivity for non-web protocols, such as those used by client/server and legacy applications, from the Internet to the internal network, thus enabling users of the Intelligent Application Gateway (IAG) to safely access back-end applications. Via the portal homepage, remote users can access a range of applications, such as native messaging applications, standard email applications, collaboration tools, connectivity products, and more. The SSL Wrapper allows granular, per-user and per-server configurations and can be used in conjunction with the IAG endpoint security policies, providing for a secure SSL VPN experience. Multi-platform application support ensures that users can access their applications from computers running Windows, Mac OS X, and Linux operating systems, using a wide range of browsers.

In order for users to run SSL Wrapper applications, the IAG site has to be trusted. When a user launches an SSL Wrapper application, the SSL Wrapper Client Component verifies the identity of the IAG site against the site's server certificate, and checks whether the site is on the user's Trusted Sites list; only if the site is trusted will the application launch.



### Tip

For information on how the IAG site can be added to the user's Trusted Sites list refer to “IAG Trusted Sites” on page 160.

This chapter describes:

- The technology used by the SSL Wrapper, in “Technology Overview” on page 172.

- The conditions under which access to SSL Wrapper applications is enabled in endpoint computers, in “Enabling Access to SSL Wrapper Applications” on page 175.
- The types of applications supported by the SSL Wrapper, in “Supported Applications” on page 181.
- Steps you take in order to configure SSL Wrapper applications, in “Configuration Overview” on page 183.
- Remote users’ interaction with the SSL Wrapper, on page 183.



#### Tip

- Application-specific settings, required for some of the SSL Wrapper applications, are described in the *Intelligent Application Gateway Application Aware Settings* guide.
- If you are running XCompress™ on the IAG, you need to set the streaming optimization to “Low latency”. You can automate the process by copying the file `XCompress.js` from:

...\\Whale-Com\\e-Gap\\von\\samples\\CustomHooks

To:

...\\Whale-Com\\e-Gap\\common\\bin\\CustomHooks

Open the file you copied, and follow the instructions in the file to configure it for your system.

## Technology Overview

When supporting non-web applications over an SSL connection, the SSL Wrapper causes the application traffic at the endpoint to be tunneled through SSL to the SSL VPN gateway, that is, the e-Gap Internal Server. The SSL VPN gateway decrypts the traffic and sends the payload to the application server in the internal network. The Socket Forwarding component add-on, which is based on Microsoft’s Layered Service Provider (LSP) and Named Service Provider (NSP) technologies, can be used to support a wider variety of applications, such as supporting applications that jump ports, without needing to make on-the-fly changes to the operating system.

Application traffic can be tunneled through SSL using one of the following relay types:

- Simple relay: opens a port on the endpoint computer and tunnels the TCP traffic to and from a specific port on the application server. Using this type of relay, in order to communicate with the application server, the application on the endpoint computer needs to communicate

through the locally opened port. The SSL Wrapper makes changes, such as changes to the application settings, Registry, or `hosts` file, in order for the application to communicate through this tunnel.

- HTTP Proxy and SOCKS Proxy relays: opens a port on the endpoint computer. This port acts as either an HTTP or SOCKS proxy server, and tunnels the HTTP or SOCKS traffic to and from the application server. Using this type of relay, the application on the endpoint computer can communicate through the locally opened port with multiple servers and ports. The SSL Wrapper makes changes, such as changes to the application settings, Registry, or `hosts` file, in order for the application to communicate through this tunnel. This type of relay enables the SSL VPN proxy to request more than one server, thus enabling the support of dynamic ports.



#### Note

In browsers where the Java applet is used, when multiple portals are open concurrently, only applications that are launched from the portal that was accessed first can listen on HTTP/SOCKS proxy ports. Users cannot launch applications that use HTTP Proxy and SOCKS Proxy relays from additional portals. For a description of when the Java applet is used, refer to “Enabling Access to SSL Wrapper Applications” on page 175.

- Transparent relay: automatically creates a relay between the endpoint computer and the application server, for every application on the client that wants to communicate with the internal network. This type of relay is only supported by the Socket Forwarding component, and does not require any changes on the endpoint computer.
- Network Connector: supports full connectivity over a virtual transparent connection, and enables you to install, run, and manage remote connections, as if they were part of the corporate network. For details, refer to Chapter 7: “Network Connector”.



#### Tip

For a description of how the SSL Wrapper is used to handle unsigned HTTP requests generated by both web applications and non-web application components, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “HAT via Proxy” on page 338.

## Socket Forwarding Activation Modes

The Socket Forwarding component comprises two modules: Winsock2 Layered Service Provider (LSP) and Name Service Provider (NSP). When an application uses Winsock, Windows will load either the NSP module (when the application performs a name resolution) and/or the LSP module (when the application uses sockets to connect to a remote server).

The NSP and LSP modules intercept every networking activity performed by the application. Though this interception should not pose any problem, and is completely transparent to the application, there is a slight possibility that the application will not function correctly because of the NSP/LSP interception.

To minimize the risk of potential problems, certain applications are included in the LSP/NSP modules' block list. Based on this list, the NSP and LSP modules can completely disable themselves and stop intercepting network activities when they detect that the application within which they run is on their block list. When disabled in this manner, the LSP and NSP modules do not enable access from this application to the corporate network.



### Tip

When access to an application in the corporate network is blocked because it is included in the block list, users may still gain access to other application servers that reside on the local intranet or the Internet.

The LSP/NSP modules contain two inherent application lists:

- A block list, containing applications that are known to be problematic. Access to these applications from within the corporate network is always blocked, regardless of the selected Socket Forwarding activation mode.
- An allow list, containing applications for which the LSP/NSP will always be active, regardless of the selected Socket Forwarding activation mode.

Blocking of additional applications depends on the Socket Forwarding activation mode, defined during application configuration:

- **Basic:** in this mode, none of applications that load the LSP/NSP modules are enabled access to configured corporate resources, unless the SSL Wrapper is running and at least one tunnel is open. Windows services (non-interactive applications) are not allowed access to configured corporate resources in this mode, regardless of whether the SSL Wrapper is running or not.

- **Extended:** this mode is identical to the Basic mode, except that Windows services are enabled access to configured corporate resources.
- **VPN:** in this mode, the LSP/NSP modules are always active in all applications, that is, access is enabled to configured corporate resources, except for the applications listed in the block list.

Basic mode will enable most applications to work via the IAG, and is the recommended Socket Forwarding mode. For some applications, however, Extended mode or VPN mode is required.

You select the Socket Forwarding activation mode for an application when you configure the application, as described in “Configuration Overview” on page 183.

## Enabling Access to SSL Wrapper Applications

In order for users to be able to access SSL Wrapper applications, one of the following SSL Wrapper Client Components must run on their computer:

- **SSL Wrapper ActiveX component:** this is the recommended mode of operation. The component is part of the Whale Client Components; for a description of the installation and running of the components, see “Installing and Running the Components on Endpoint Computers” on page 150. In addition, some SSL Wrapper applications require users to be logged on with Administrator privileges in order to use the application, in cases where changes to the `hosts` file or the Registry have to be made. For details, refer to “Technology Overview” on page 172.

The SSL Wrapper ActiveX component is installed on the endpoint computer the first time a user attempts to access an SSL Wrapper application. If an application is configured to operate in Socket Forwarding Mode, and providing that the endpoint computer meets the Socket Forwarding component installation requirements, the Socket Forwarding component is installed, as well. For details, refer to “Socket Forwarding Component Installation” on page 178.

- **SSL Wrapper Java applet:** used as a fallback for endpoint computers where the SSL Wrapper ActiveX component cannot be installed or run, such as computers running Mac OS X or Linux operating systems, or an Internet Explorer browser on Windows where the download and launching of ActiveX components is disabled.
  - The Java applet is supported on the browsers that are supported by the IAG, as listed in “Supported Browsers” on page 19.

- In order for the Java applet to run on the endpoint computer, the computer must meet the requirements described in “SSL Wrapper Java Applet Prerequisites” on page 176.



#### Tip

If a personal firewall is installed on the endpoint computer, the following has to be added to the firewall’s trusted applications list:

- When working via the SSL Wrapper ActiveX component: the client executable `whlclnt3.exe`.
- When working via the SSL Wrapper Java applet: the browser’s executable. **For example:** when browsing with Firefox, add the executable `firefox.exe` to the list.

## SSL Wrapper Java Applet Prerequisites

The following is required in order for the SSL Wrapper Java applet to run on the endpoint computer, and for the applications to be accessed via the applet, when the SSL Wrapper ActiveX component cannot be installed or run on the computer:

- JRE™ version 1.4 and higher must be installed on the computer.
- Java trace level 5 (can be configured in the Java Console window) is not recommended and may cause the Java applet to go into an infinite loop. For details, see the following Sun™ Developer Network page:

[http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=5097873](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=5097873)

- The following browsers on Mac OS X require the installation of JEP (Java Embedding Plugin) for Mac OS X:
  - Mozilla
  - Mozilla Firefox
  - Mozilla Camino

For details, see <http://plugindoc.mozdev.org/OSX.html#Java>

- On Windows 2000 Professional operating systems, in Internet Explorer, the option “Script ActiveX controls marked safe for scripting” must be enabled in the Security Settings of the Internet Options.
- In order for an application to be accessed via the SSL Wrapper Java applet, in the Configuration program, the application’s Access policy should be configured with the option “Enforce Policy Only when Endpoint Detection is Enabled”:



- You activate this option in the Policy Editor, described in “Basic Policy Configuration” on page 103, in the General Policy Settings screen.



#### Tip

Click  [Help](#) for detailed information on the parameters of the screen.

- You select an application’s Access policy in the Add Application Wizard, in the Application Setup step. Once you add an application to the trunk, you can change the selected Access policy in the General tab of the Application Properties dialog box.
- In order to run an application where network aliases have to be created, users have to be logged on to the endpoint computer with **sudo** privileges for the `ifconfig` utility.
- In order to run an application where changes to the `hosts` file have to be made, users have to be logged on to the endpoint computer with **sudo** privileges for `hosts` file.
  - For a description of when changes to the `hosts` file might be required, refer to “Technology Overview” on page 172.
  - For information about **sudo** privileges, see <http://www.linuxhelp.ca/guides/sudo/>
- On Linux operating systems, console-based applications might require that the `xterm` application is installed on the endpoint computer. If `xterm` is not installed on the computer, users can manually run the application by opening a terminal and connecting to the relay that was opened for the application.



#### Tip

To display an application’s relay, select the application in the Portal Activity window, and click [Show Relay](#).

For details, refer to “Portal Activity Window” on page 184.

- On Mac OS X and Linux operating systems, when running a Telnet application that the operating system opened in a Terminal application (Mac OS X) or in `xterm` (Linux), the user needs to configure the Telnet application to work in Character mode, by entering `mode character` in the Telnet window. For more information, consult the Telnet manual pages.

## Uninstalling the SSL Wrapper Java Applet



### Note

Do not uninstall the Java applet while it is running on the computer.

Once the SSL Wrapper Java applet runs on the endpoint computer, users can remove it from their computer as follows:

1. Clean the following applet from the Java plug-in applets' cache:  
`sslvpnclient.jar`
2. Delete the following folder:
  - Windows operating systems: `%userprofile%\ .whalesslwrapper`
  - Mac OS X operating systems:  
`~/<username>/ .whalesslwrapper`  
Or,  
`/var/root/ .whalesslwrapper`
  - Linux operating systems:  
`~/<username>/ .whalesslwrapper`  
Or,  
`/root/ .whalesslwrapper`



### Note

If the folder `.whalesslwrapper` contains the file `backupdata.map`, this file might contain changes that were made to the system by the SSL Wrapper Java applet, and were not restored when the applet stopped running. **For example:** entries added to the `hosts` file.

In this case, don't delete the folder before backing it up. In order to restore the settings, contact technical support.

## Socket Forwarding Component Installation

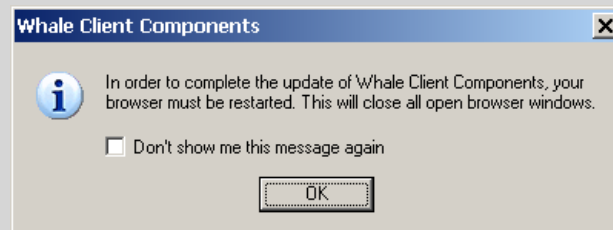
The conditions for the installation of the Socket Forwarding client component on the endpoint computer are described in "Prerequisites for Installing the Whale Client Components" on page 151.

After the initial installation of the Socket Forwarding client, users are required to restart their browser, and might be required to restart the computer. Once the client is installed, however, users do not require any privileges in order to use the application.



### Tip

When users are required to restart their browser, the following message is displayed:



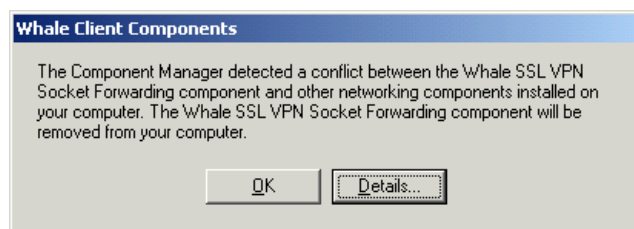
If a user selects the option “Don’t show me this message again”, this message will not be displayed again, even when a restart is required. In order to receive the message when applicable, instruct the user to restore the default settings of the Whale Component Manager, as described in “Restoring the Whale Client Components Defaults” on page 165.

During the installation of the Socket Forwarding component, the Whale Component Manager checks whether the Socket Forwarding LSP module conflicts with other LSP modules that are installed on the endpoint computer. For details, refer to “LSP Conflict Detection” on page 179.

If the Socket Forwarding component is not installed on the computer, but the SSL Wrapper component is, applications that are configured to work in Socket Forwarding Mode will still function. However, the additional capabilities enabled by the Socket Forwarding component, as described in “Technology Overview” on page 172, will not apply to the application in this setup.

## LSP Conflict Detection

If, during the installation of the Socket Forwarding component on the endpoint computer, the Whale Component Manager detects a conflict between the Socket Forwarding LSP module and other LSP modules installed on the computer, it removes the Socket Forwarding component. In this case, the user is notified as follows:





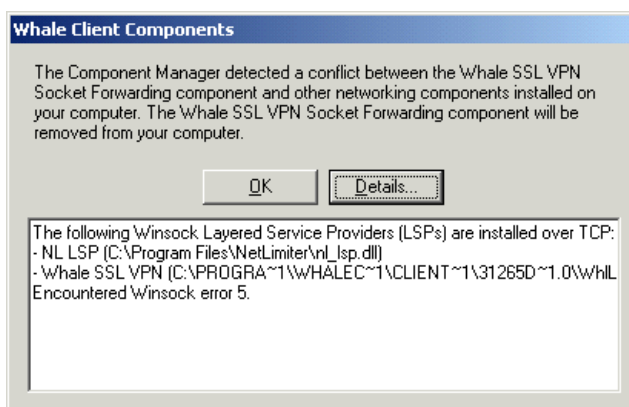
### Note

The removal of the component may require a restart of the browser or of the computer. Users are notified accordingly.

The following procedure describes how you can re-enable the installation of the Socket Forwarding component on the endpoint computer after a conflict is detected.

### *To re-enable the installation of the Socket Forwarding component:*

1. Determine which components conflict with the Socket Forwarding component:
  - In the message box that is displayed when the conflict is detected, click **Details...** to display the list of conflicting components:



Or,

- Access the following file: %temp%\SFConflictInfo.txt
2. In order to remove conflicting components, contact technical support.
  3. Once the conflicting components are removed, use the System Information window, which you access from the Whale toolbar on the portal homepage, to re-enable the installation of the Socket Forwarding component:

https://portal.microsoft.com - System Information (2) - Microsoft Internet Explorer

Whale Communications  
A Microsoft Subsidiary

System Information

Whale Communications Intelligent Application Gateway

Whale Client Components	
Whale Component Manager	✓ (3, 7, 0, 12)
Endpoint Detection	✓ (3, 7, 0, 12)
SSL Wrapper	✓ (3, 7, 0, 12)
SSL Wrapper Java Applet	N/A
Socket Forwarder	LSP: ✗ NSP: ✗ (Installation disabled)
Network Connector	Client: ✓ (3,7,0,12) Driver: ✓ (3,7,0,12) <b>Not Running</b>
Attachment Wiper™	✓ (3, 7, 0, 12)

Anti-virus eTrust 7.1 (Updated: 12/5/2006 10:09:02 PM)

Personal Firewall XPSP2 Version: N/A

Operating System Windows XP Professional 5.01.2600, Service Pack 2

Browser Version Internet Explorer 6

User Agent Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)

Sun JRE Version N/A

Domain WHALECOM

Certified Endpoint ✗

Privileged Endpoint ✗

This site is protected by the Whale Communications Intelligent Application Gateway.  
To refresh this page, please log out then log in again.

Done Internet

Enable Socket Forwarding Installation

- Access and run an application that requires the Socket Forwarding component, for example the application you tried to run when the conflict was detected.

*The Socket Forwarding component is installed on the computer.*



#### Note

The installation of the component may require a restart of the browser or of the computer. Users are notified accordingly.


## Supported Applications

The SSL Wrapper supports two types of applications:

- Client/server and legacy applications, also known as “native” applications. Those types of applications are initiated by the SSL Wrapper. The application’s configuration data is usually stored locally, on the endpoint computer. For example: Telnet; Citrix Program Neighborhood applications, Microsoft Windows XP and Windows 2000 Terminal Services Clients, and more.
- Browser-embedded applications are web initiated. The application’s configuration data is usually downloaded from the network at runtime. For example: Citrix NFuse FR2 and FR3 applications, IBM Host-On-Demand, Terminal Services Web Client, and more.



### Tip

- For a list of operating systems on which an application is supported, click  [Help](#) in the Server Settings tab of the Add Application Wizard or the Application Properties dialog box.
- The SSL Wrapper open architecture enables the addition of other applications, if required. For details, contact technical support.

## Generic Applications

This group includes the enhanced generic client applications and the generic Carbonized applications:

- Enhanced generic client applications are non-web applications that run in a console environment.
- Generic Mac OS X Carbon® Applications are non-web Mac OS X applications that run in a Carbon application framework.

For each of those application-types, you can select between the following options, depending on the requirements of the application you are configuring:

- **hosts required:** running the application requires the Java applet to make changes to the `hosts` file on the endpoint computer. If changes cannot be made to the file, for example due to insufficient user privileges, the application is not launched, and the relay that was opened for the application is closed.
- **hosts optional:** when the application attempts to launch, the Java applet attempts to make changes to the `hosts` file on the endpoint computer. If changes cannot be made to the file, the application is not launched. However, the relay that was opened for the application is left open. Users are presented with a message showing the open relay, so that they can manually run the application.
- **hosts disabled:** the Java applet does not have to make changes to the `hosts` file in order to run the application.

## Configuration Overview

You enable any of the SSL Wrapper applications to remote users via a Portal trunk. You can enable an unlimited number of applications via a single portal.

- For operating instructions on how to create a Portal trunk and add applications, refer to “Creating an SSL VPN Portal” on page 28.
- For out-of-the-box applications where the Socket Forwarding component is required, Socket Forwarding is enabled by default. In order to enable the Socket Forwarding component for other applications, once you add the application to the trunk, select the required Socket Forwarding Mode in the Application Properties dialog box, in the Client Settings tab.
  - For a description of the available activation modes, refer to “Socket Forwarding Activation Modes” on page 174.
  - For a description of the Client Settings tab, refer to “Client Settings Tab” on page 86.
- If you do not use the default portal homepage supplied with the IAG, you need to add links to the applications on your custom homepage, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Adding Application Links on a Custom Portal Homepage” on page 63.
- Some of the applications require additional setup. For details, refer to the *Intelligent Application Gateway Application Aware Settings* guide.

## Remote User Interaction with the SSL Wrapper






### Note

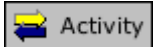
In the Session tab of the Advanced Trunk Configuration window, you determine the behavior of SSL Wrapper applications when the portal window closes without the user having logged off the site, such as when the browser crashes, or when the user accesses a non-portal page from within the portal. This is configured in the following options:

- “Prompt User to Disconnect Channel when Portal Closed without Logoff”
- “Re-open Portal if User Selects to Keep Channel Open”

You can configure different settings for default and privileged sessions. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Default and Privileged Session Settings” on page 137.

Remote users access SSL Wrapper applications via the portal homepage. You access the Portal Activity Window, described in “Portal Activity Window” on page 184, as follows:

- **Portal trunk:** when one or more SSL Wrapper applications run on a client, users can view the status and activities of the applications as follows:
  - On computers where the SSL Wrapper ActiveX component is used, a Portal Activity icon is added to the Windows System tray (to the right of the Windows taskbar): . Double-clicking this icon opens the Portal Activity window.
  - When the Network Connector is activated, the icon changes: . For details, refer to “Remote User Interaction with the Network Connector” on page 200.
  - On computers where the SSL Wrapper Java applet is used, the Portal Activity - SSL Wrapper Java Client window opens as soon as an SSL Wrapper application is launched on the computer.
- **Webmail trunk:** when an SSL Wrapper application runs on a client, a Portal Activity icon is added to the Windows System tray (to the right of the Windows taskbar): . Double-clicking this icon opens the Portal Activity window.

Clicking the Portal Activity icon, on the Whale toolbar, brings the Portal Activity window to the front of the screen: .



#### Note

If the endpoint browser or the client Java Plugin are set to connect to the web via a proxy, the SSL Wrapper Java applet will attempt to connect to the IAG site via the same proxy, using the applicable setting (except for Firefox browsers when the browser is set to connect to the web via proxy and the Java Plugin is set to use the browser settings).

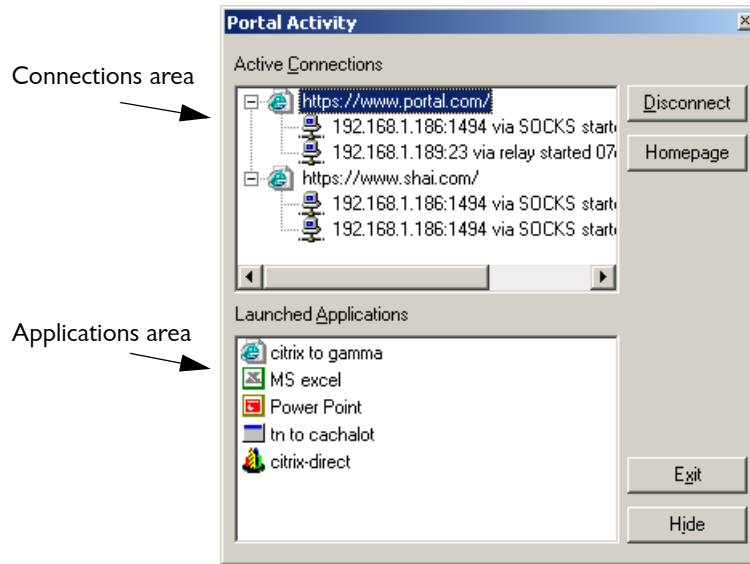
## Portal Activity Window

The Portal Activity window monitors the activity of the applications that are run by the SSL Wrapper client.

- When working via the SSL Wrapper ActiveX component, one Portal Activity window is used to monitor all the IAG sites that are accessed from the computer.
- When working via the SSL Wrapper Java applet, a separate Portal Activity window opens for each IAG site that is accessed from the computer.



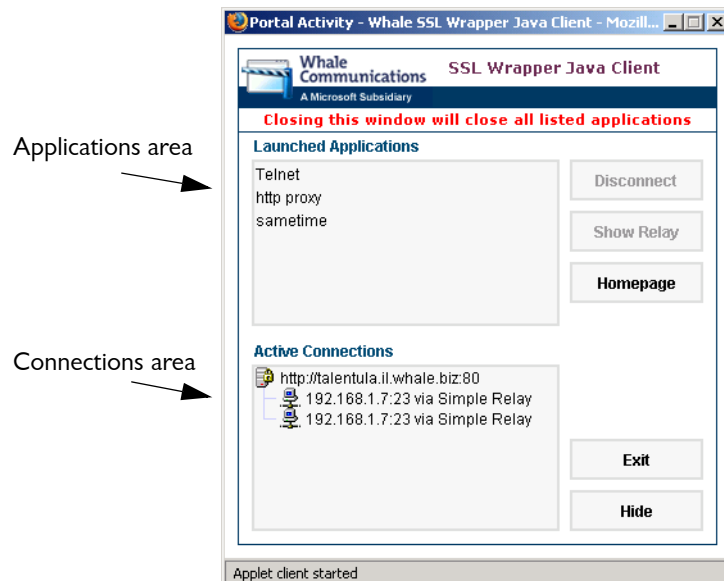
**Figure 24. Portal Activity Window–SSL Wrapper ActiveX Component**



**Tip**

For a description of the Portal Activity window when the Network Connector is running on the computer, refer to “Interaction on Computers Running the SSL Wrapper ActiveX Component” on page 201.

**Figure 25. Portal Activity Window–SSL Wrapper Java Applet**





### Note

Closing the window disconnects all the applications that are tunneled through the SSL Wrapper Java applet.

The Portal Activity window is divided into two main areas:

- Connections Area, described on page 186.
- Applications Area, described on page 187.

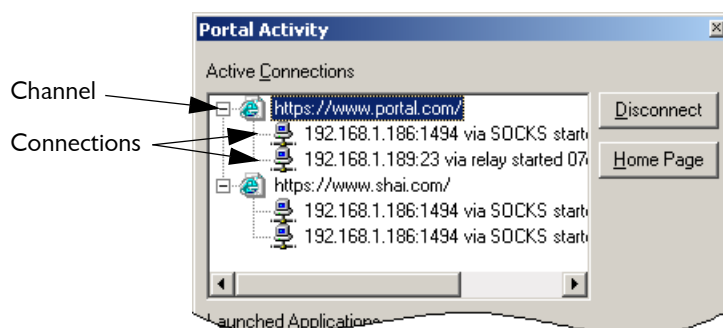
The Portal Activity window buttons are described on page 188.

## Connections Area

The Connections area of the Portal Activity window displays:

- Active channel or channels between the client and the trunk or trunks to which the client is connected (one channel per portal or trunk).
- Under each channel, the connection or connections that are currently open through the channel.

**Figure 26. Sample Portal Activity Window—Connections Area**

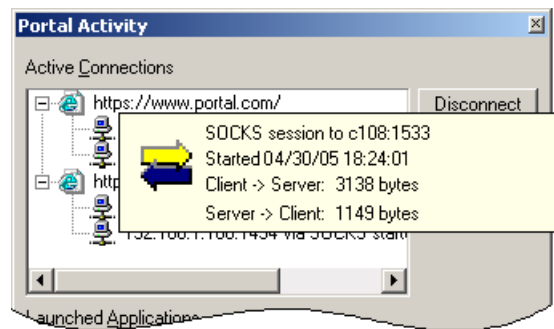


When you hover over a connection, you can see the following details regarding the connection:

- Address: IP address and port number
- Connection's connectivity option: SOCKS or Relay
- Date and time when the connection was established

When you double-click a connection, you can see the number of bytes sent:

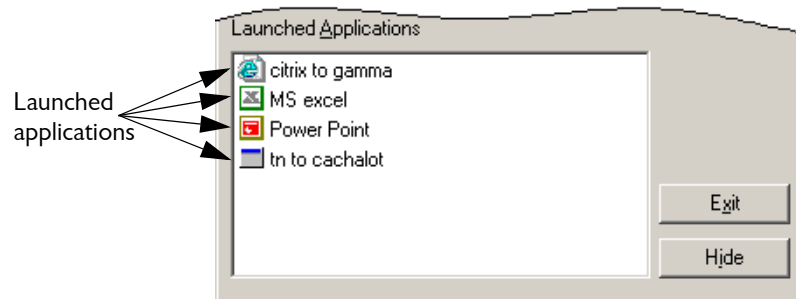
**Figure 27. Sample Portal Activity Window—Additional Connection Details**



## Applications Area

The Applications area of the Portal Activity window displays a list of the applications that were launched since the SSL Wrapper client was started.

**Figure 28. Sample Portal Activity Window—Applications Area**



When you double-click an application, you can see the following details regarding the application:

- Application name
- Date and time when the application was launched
- For client/server and legacy applications, the application command line.
- For browser-embedded applications, the text “Web Application” is displayed.

**Figure 29. Sample Portal Activity Window—Sample Application Details**



## Portal Activity Window Buttons

The following table describes the buttons of the Portal Activity window.

Button	Description
<b>Disconnect</b>	<p>Disconnects the item that is currently selected in the Connections area:</p> <ul style="list-style-type: none"> <li>If you select a channel, this button disconnects the channel, including all the connections that are open through the channel.</li> <li>If you select a single connection, this button disconnects it.</li> </ul> <p><b>Note:</b> Disconnecting a connection does not always completely disconnect the application. For applications that support reconnection, the tunnel listener remains open to allow reconnection if required.</p>
<b>Show Relay</b> (Java applet only)	Displays the open relay of the currently selected application.
<b>Homepage</b>	Takes you to the portal homepage of the selected channel or connection, without closing the Portal Activity window.
<b>Exit</b>	Closes all open channels and connections and exits the Portal Activity window. When using the ActiveX component, the Portal Activity icon is no longer displayed in the Windows System tray.
<b>Hide</b>	<p>Hides the Portal Activity window. To show the window again:</p> <ul style="list-style-type: none"> <li>When using the ActiveX component: either double-click the Portal Activity icon or right-click it and select <b>Show Status</b>. You can also click the Portal Activity icon on the portal homepage.</li> <li>When using the Java applet: click the Portal Activity icon on the portal homepage.</li> </ul>

# Network Connector

The Network Connector technology that is part of the Intelligent Application Gateway (IAG) enables you to install, run, and manage remote connections, as if they were part of the corporate network, supporting full connectivity over a virtual and secure transparent connection.

During a Network Connector session, remote endpoint computers are part of the corporate network. Depending on the Network Connector server configuration, they are able to:

- Communicate with all the computers in the network, that is, access and be accessed by all other network computers.
- Access corporate servers and complex systems such as mail, SMB, FTP, databases, and VoIP applications.
- Communicate with other remote Network Connector endpoint computers.

**For example:** the system administrator can connect to endpoint computers in order to install software updates, configure existing applications, or help users troubleshoot their systems.

This chapter describes the following:

- “Network Connector Technology Highlights” on page 189
- “Configuring the Network Connector” on page 190
- “Remote User Interaction with the Network Connector” on page 200
- “Network Connector Troubleshooting” on page 203

## Network Connector Technology Highlights

The Network Connector implements a client/server architecture, and is integrated into the IAG’s secure SSL tunnel. It supports all types of IP-based unicast traffic, in any direction: client to server, server to client, and client to client.

The Network Connector server provides the following features:

- Auto-detection and manual tuning of corporate networking parameters—DNS, WINS, gateway, and domain name—including support for multi-connection machines.
- Two IP provisioning methods.
- Internet access configuration, including split tunneling, non-split tunneling, and none.
- Protocol filters for IP-based protocols.
- Enabling access to additional networks.

## Configuring the Network Connector

In order to enable users to connect to the corporate network via the Network Connector, take the following steps:

- Configure the Network Connector server, as described in “Configuring the Network Connector Server” on page 190.



### Note

The Windows DHCP Client service must be running on the IAG server.

- In the Configuration program, use the Add Application Wizard to add the Network Connector application to the portal homepage. The application is an SSL Wrapper application, and is part of the Client/Server and Legacy Applications group in the Wizard.

Once you complete these steps, end-users can install the Network Connector client on their computer. The client is part of the Whale Client Components, described in “Whale Client Components” on page 147.



### Note

You cannot install the Network Connector client on the same computer where the Network Connector server is installed.

## Configuring the Network Connector Server

This section describes how you configure the Network Connector server.

### *To configure the Network Connector server:*

1. In the Configuration program, on the **Admin menu**, click **Network Connector Server...**

2. At the bottom left corner of the Network Connector Server window, check the option “Activate Network Connector”.


**Note**

Unchecking the option “Activate Network Connector” once the Network Connector is activated disables this feature.

3. Use the Network Connector Server window to configure the server. For details, refer to:
  - “Network Segment Tab” on page 192
  - “IP Provisioning Tab” on page 193
  - “Access Control Tab” on page 196
  - “Additional Networks Tab” on page 197
  - “Advanced Tab” on page 199


**Note**

Configuration in the IP Provisioning tab is mandatory. Configuration in the other tabs is optional, and depend on your network settings and your requirements.

4. Once you complete the configuration of the server, click **OK** in the Network Connector Server window in order to activate the Network Connector.
5. In the Configuration program, click  to save and activate the configuration, then click **Activate >** in the Activate Configuration screen.

*The configuration settings you have defined are applied to the Network Connector server. The Network Connector Windows service—Whale Network Connector Server—is started and is set to Automatic Startup mode.*

**Tip**

A dedicated network icon in the Windows System tray indicates that the Whale Network Connector Server service is started: 

## Network Segment Tab

Use this tab to:

- Select the relevant corporate connection that the server should use. This is normally the connection defined for the internal IP interface of the IAG. Once you select a connection, the fields in the Network Connection area are automatically populated with the connection information.
- Optionally, configure complementary networking data, as described in “Complementary Data” on page 192.

Figure 30. Sample Network Segment Tab

Network Connector Server

Network Segment | IP Provisioning | Access Control | Additional Networks | Advanced

Use the Following Connection:

Intel 21140-Based PCI Fast Ethernet Adapter (Generic)

Network Connection

IP Address: 192.168.2.220

Subnet Mask: 255.255.248.0

DNS (Primary): 192.168.1.11

DNS (Secondary): 192.168.1.37

DNS Suffix: il.whale.biz

WINS (Primary): 192.168.1.11

WINS (Secondary): 0.0.0.0

Gateway: 192.168.1.1

Complementary Data

Use the Following Data:

☒ Only if Network Configuration is Missing

☐ Always, Overriding Existing Network Configuration of This Server

DNS (Primary): . . .

DNS (Secondary): . . .

DNS Suffix: . . .

WINS (Primary): . . .

WINS (Secondary): . . .

Gateway: . . .

☒ Activate Network Connector

OK Cancel

## Complementary Data

In this section of the Network Segment tab, you can configure alternative network parameters, and select when they are used:

- **Only if Network Configuration is Missing:** data you enter in the “Complementary Data” area will be used only if no data is configured for the same item in the “Network Connection” area.
- **Always, Overriding Existing Network Configuration of This Server:** the data in the “Complementary Data” area will always be used, regardless of the configuration of the selected connection. Fields that are left empty are ignored.





### Note

If one or more of the fields are left empty in both the “Network Connection” and “Complementary Data” areas, it might result in limited client session.

**For example:** if no DNS is defined, no DNS services will be available for users connecting via the Network Connector.

## IP Provisioning Tab

Use this tab to define the IP pool from which clients are assigned IP addresses when connecting via the Network Connector.



### Note

- Make sure that your pool is sufficient for your needs, and consists of enough IP addresses for your remote clients. Note that IP addresses ending with zero or 255 are not used for IP assignment.  
**For example:** if you define the pool 192.168.0.0–192.168.0.9, the Network Connector server will be able to support up to 8 concurrent clients, since 192.168.0.0 will not be used, and 192.168.0.1 will be used by the server itself.
- You can use the Additional Networks option to define additional network destinations which will be available to clients when connecting via the Network Connector, as described in “Additional Networks Tab” on page 197.

The Network Connector server supports static IP provisioning, using either of the following types of IP pools:

- Corporate IP pool, consisting of corporate IP addresses, that is, IP addresses that belong to the corporate network, as defined in the Network Segment tab.
- Private IP pool, consisting of private IP addresses, that is, IP addresses that belong to a network segment that doesn’t overlap with the network segment, which is defined in the Network Segment tab.

**For example:** if the corporate segment is configured to 192.168.0.0/255.255.248.0, an example of a “corporate pool” would be 192.168.6.2–192.168.6.200, and an example of a “private pool” would be 10.16.16.2–10.16.16.200.



### Caution

- If the IP pool is a corporate pool, make sure to exclude the IP range you define here from your organization's DHCP server, to avoid IP conflict with Network Connector clients.
- IP conflicts between corporate computers and endpoint computers will result in idle sessions, in which remote clients launch the Network Connector application with no errors, but have no access to the Network Connector server, or to the resources that should be enabled to them via the server.
- If the IP pool is a private pool, and the Internet access level, defined in the Access Control tab, is "split" or "none", in order to enable access to the corporate network you must use the Additional Networks option to add the corporate network. In this setup, if you do not add the corporate network, remote clients are granted access to other clients only, and cannot access the corporate network. For details, refer to "Additional Networks Tab" on page 197.

### *To define the IP pool:*

1. In the "Pool Type" area, select the type of IP pool you wish to define. If you select "Private IP Addresses", additional configuration is required, as described in "Using a Private Pool: Additional Configuration" on page 195.
2. In the "Address Pool" area, define the range or ranges of IP addresses that can be assigned to remote clients. Note the following:
  - You can enter up to 10 ranges of IP addresses.
  - All the addresses you define here use the same subnet mask; you cannot define both corporate IPs and private IPs.
  - The subnet for the IP ranges you defined in displayed in "Pool Subnet".

**Figure 31. Sample IP Provisioning Tab**

Network Connector Server

Network Segment | IP Provisioning | Access Control | Additional Networks | Advanced

Pool Type

☒ Corporate IP Addresses  
☐ Private IP Addresses

Address Pool

From	To

Add...  
Edit...  
Remove

Pool Subnet: 192 . 168 . 0 . 0 / 255 . 255 . 248 . 0

☒ Activate Network Connector

OK Cancel

### Using a Private Pool: Additional Configuration

This section describes additional steps you should take if you select to use a private IP pool, that is, an IP provisioning pool that consists of private IP addresses.

In this setup, do the following:

- Configure your corporate gateway to route the private pool's subnet from the gateway's internal network card to the IP address of the Network Connector server.
- If your corporate firewall filters traffic on its internal interface, configure the firewall to allow bi-directional traffic between the private pool subnet and the corporate subnet, as defined in the Network Segment tab.
- In order to enable access to the WAN/Internet, configure the firewall to allow bi-directional traffic between the private pool subnet and the WAN, and define the private pool permissions.
- If you are using Network Address Translation (NAT), in order to enable access to the WAN/Internet, define the subnet of the private pool as an additional internal interface.

## Access Control Tab

Use this tab to:

- Define Internet access level for endpoint computers connecting via the Network Connector:
  - **Split Tunneling:** Internet traffic on the endpoint computer is routed through the computer's original Internet connection.
  - **Non-Split Tunneling:** Internet traffic on the endpoint computer is routed through the gateway of the corporate network. You can also select to disable local area access in this mode.



### Note

When using non-split tunneling, note the following:

- The Additional Networks option is not applicable in this access mode, since all network traffic passes through the Network Connector tunnel in this mode. For details, refer to “Additional Networks Tab” on page 197.
- If the Network Connector session on the endpoint computer is ended ungracefully, for example when the computer disconnects from the Internet, users are prompted to re-enable their Internet connection.

- **No Internet Access:** endpoint computers cannot access the Internet. You can also select to disable local area access in this mode.

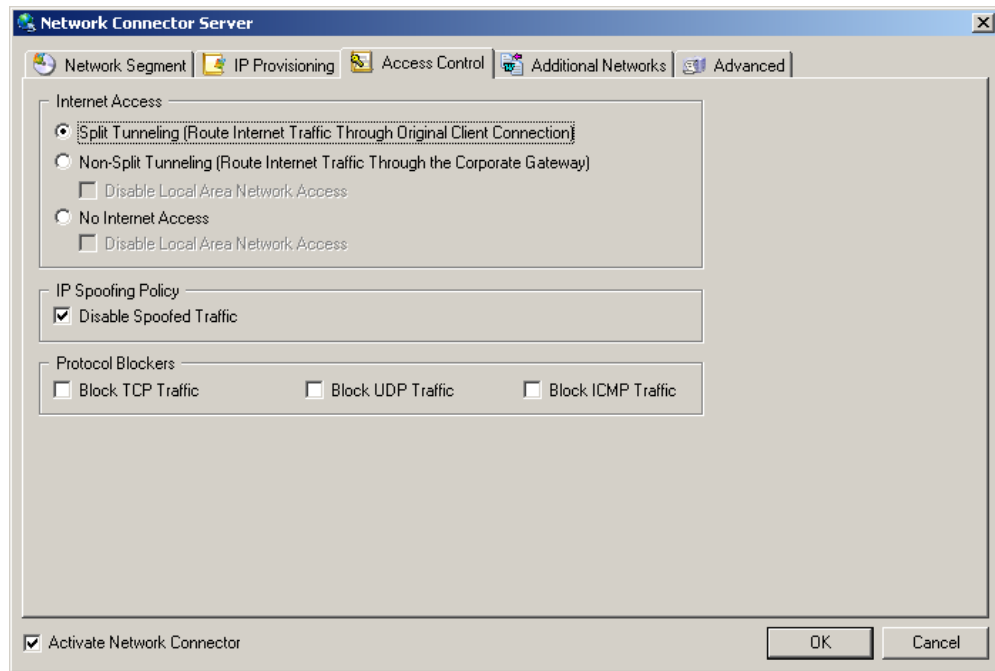


### Note

In this mode, endpoint computers can only access their local network, the network defined in the IP Provisioning tab, and any other networks defined in the Additional Network tab.

- Determine the IP Spoofing policy. By default, the option “Disable Spoofed Traffic” is selected; the Network Connector server checks and validates the source IP address of each packet, and tunnels only traffic from connected Network Connector clients. If you wish to enable the tunnelling of other traffic, uncheck this option.
- Apply filtering of any of the following IP-based protocols: TCP; UDP; ICMP.

**Figure 32. Sample Access Control Tab**



### **Additional Networks Tab**

In this tab, you can define network destinations that will be available to Network Connector clients in addition to the IP pool that you define in the IP Provisioning tab, as described in “IP Provisioning Tab” on page 193.

**For example:** if in the IP Provisioning tab you enable access to the corporate head office, use the Additional Networks tab to enable access to additional offices throughout the world, which are connected to the corporate head office via the corporate gateway.



### Note

- The Additional Networks option cannot be used if the Internet access level, defined in the Access Control tab, is “non-split”, since in this access mode all network traffic is tunneled over the virtual connection.
- Use the Additional Networks option if the IP pool that is defined in the IP Provisioning tab is a private pool, and the Internet access level, defined in the Access Control tab, is “split” or “none”. If you do not define the corporate network as an additional network in this setup, remote clients are granted access to other clients only, and cannot access the corporate network.

For each of the networks you define here, you select how to handle conflicts, in case the definitions you enter here conflict with the endpoint computer’s local network definitions:

- **Fail:** the connection attempt fails, and the computer is not connected via the Network Connector.
- **Prompt:** prompt user to select whether to fail the connection attempt, or to skip this network and connect to the other networks via the Network Connector.
- **Skip:** connection to this network is skipped. The computer is connected to all the other networks via the Network Connector.

### *To configure additional networks:*

1. In the Additional Networks tab, activate the option **Enable Access to the Following Additional Networks**.
2. Click **Add...**, and use the Add Network dialog box to define the network, including IP address, mask, and conflict handling.

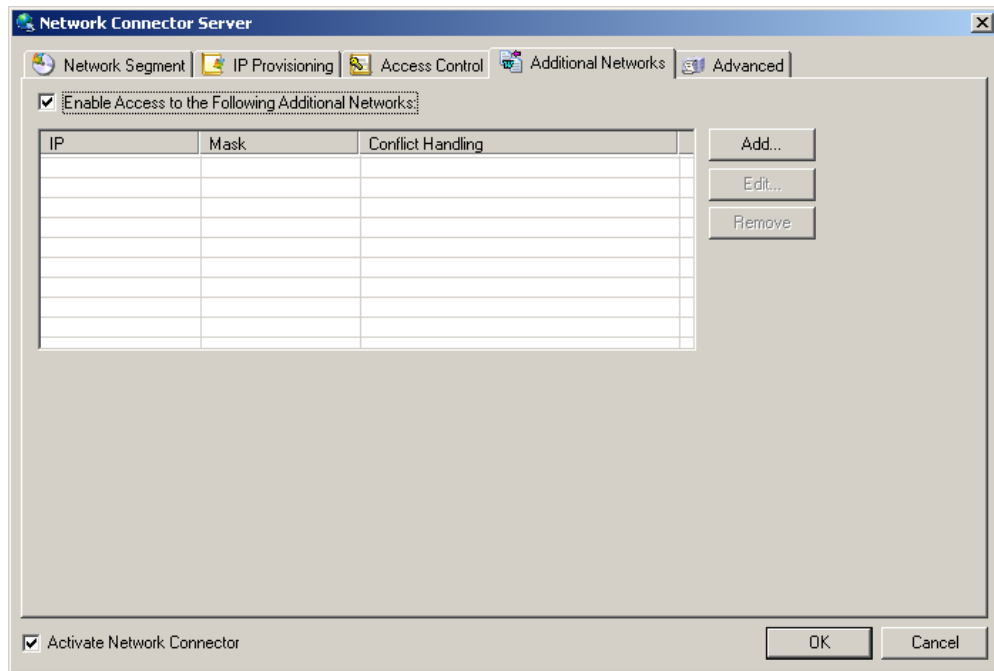


### Note

Make sure that the network’s IP address and mask are valid and do not overlap with the network that is defined in the IP Provisioning tab; invalid parameters may cause errors when remote users attempt to connect via the Network Connector.

3. Repeat step 2 to configure additional networks. You can add up to seven networks here.

**Figure 33. Sample Additional Networks Tab**



## Advanced Tab

Use this tab to configure advanced server settings:

- The “listener” area defines the listener of the Network Connector server.



### Note

The port you define here must be identical to the port number of the Network Connector application. If you change the default port defined here, 6003, take the following steps in the Configuration program:

- When you add the Network Connector application to the trunk, change the port number in the Add Application Wizard, in the Server Settings step, accordingly.

Or

- If the Network Connector application is already configured in the trunk, change the port number in the Application Properties dialog box, in the Server Settings tab.

- The “Log” and “Server Resources” areas are used for troubleshooting the Network Connector server. For details, refer to “Troubleshooting the Network Connector Server” on page 203.



### Note

Be sure to read the information provided in the server troubleshooting section before you change any of the settings in the “Log” and “Server Resources” areas.

**Figure 34. Sample Advanced Tab**

**Network Connector Server**

Network Segment | IP Provisioning | Access Control | Additional Networks | **Advanced**

**Listener**

Type: **TCP** Port: **6003**

**Log**

Log Level: **1**

Log Path: ☒ Server Executable Path  
☐ Alternative Path (Full Name): **c:\nnc.log**

**Server Resources**

Number of Threads: <b>1</b> per CPU	Device Timeout: <b>20000</b> Milliseconds
Tunnel Buffer Size: <b>64</b> KB	Service Timeout: <b>20000</b> Milliseconds
Device Buffer Size: <b>4</b> KB	<b>Restore Defaults</b>

☒ Activate Network Connector **OK** **Cancel**

## Remote User Interaction with the Network Connector

Remote users launch the Network Connector client via the Network Connector application link on the portal homepage.



### Note

- Only one Network Connector client can run on a computer at a time.
- It is recommended that while the Network Connector is active, you do not access other IAG portal sites.



Once the application is launched, users are connected to the internal network. They can access and be accessed by other network computers. They can run additional internal applications, without having to launch the application from the portal homepage.

Users' interaction with the Network Connector depends on the SSL Wrapper client component that is installed on their computer, as described in:

- “Interaction on Computers Running the SSL Wrapper ActiveX Component” on page 201.
- “Interaction on Computers Running the SSL Wrapper Java Applet” on page 202.



#### Tip

For a description of when a computer runs each of the SSL Wrapper clients, refer to “Whale Client Components” on page 147.

## Interaction on Computers Running the SSL Wrapper ActiveX Component

On computers that run the SSL Wrapper ActiveX client component, once the Network Connector client is running, the traffic of all non-web applications that are launched thereafter is tunneled through the Network Connector. This includes:

- SSL Wrapper applications that are launched via the portal homepage.
- Internal applications, that is, applications that are part of the corporate network, which are launched directly, and not via the portal homepage. **For example:** users can launch Microsoft Outlook on their computer directly, without a link on the portal homepage, and connect to the corporate Exchange server.

In addition, while end-users are connected via the Network Connector, they can launch any web application directly (not via the portal), including applications that are not defined as portal applications, and applications that are not supported by the IAG. Portal web applications can still be launched from the portal as usual.



#### Note

Disconnecting the Network Connector client disconnects all the applications that are tunneled through it. It does not, however, disconnect applications that are not tunneled through the Network Connector.

When the Network Connector client is running in this setup, a Network Connector icon replaces the SSL Wrapper icon in the Windows System tray (to the right of the Windows taskbar):

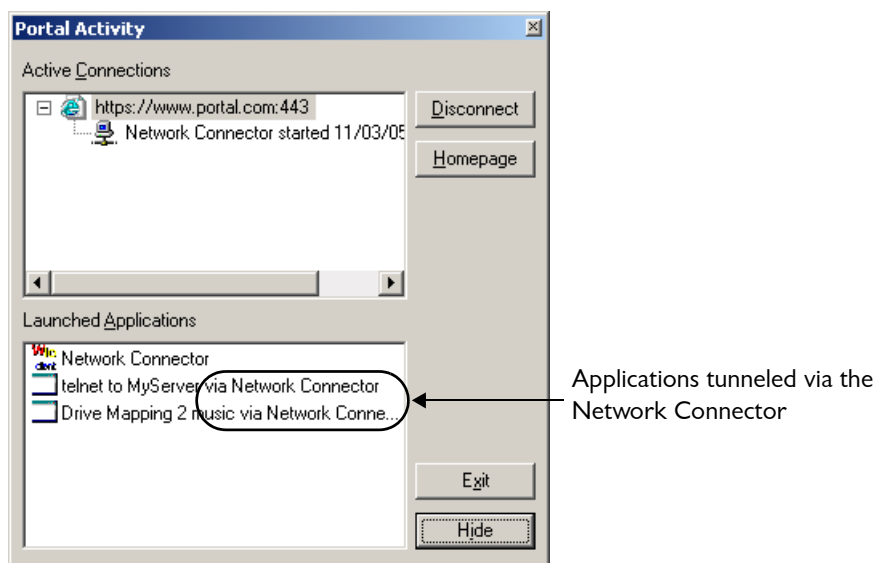
---

#### SSL Wrapper Icon    Network Connector Icon

---



- Hovering over the Network Connector icon displays the statistics of the traffic that is tunneled through the Network Connector.
- Right-clicking the icon enables you to disconnect the Network Connector.
- Double-clicking the icon opens the Portal Activity window. When an application is tunneled via the Network Connector, it is not listed in the “Active Connections” area. The connection of an SSL Wrapper application via the Network Connector is reported next to the application name, in the “Launched Applications” area:



#### Tip

For a detailed description of the Portal Activity window, refer to “Portal Activity Window” on page 184.

## Interaction on Computers Running the SSL Wrapper Java Applet

On computers that run the SSL Wrapper Java applet, the Network Connector application behaves like any other SSL Wrapper application.

Once the Network Connector client is running, some of the non-web application traffic is tunneled through the Network Connector, as follows:

- Internal applications, that is, applications that are part of the corporate network, which are launched directly, and not via the portal homepage, are tunneled through the Network Connector.
- SSL Wrapper applications that are launched via the portal homepage are **not** tunneled through the Network Connector client in this setup.

In addition, while end-users are connected via the Network Connector, they can launch any web application directly (not via the portal), including applications that are not defined as portal applications, and applications that are not supported by the IAG. Portal web applications can still be launched from the portal as usual.



#### Note

Disconnecting the Network Connector client disconnects all the applications that are tunneled through it. It does not, however, disconnect applications that were not tunneled through the Network Connector.

## Network Connector Troubleshooting

This section describes the Network Connector troubleshooting options, including:

- “Troubleshooting the Network Connector Server” on page 203
- “Troubleshooting the Network Connector Client” on page 206

### Troubleshooting the Network Connector Server

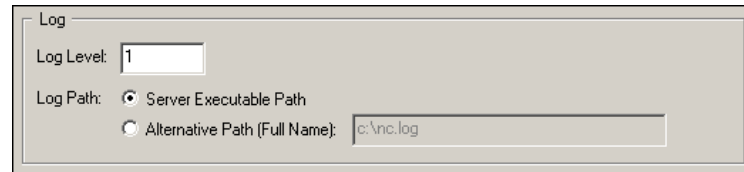
This section describes how you can troubleshoot the Network Connector Server, as follows:

- “Server Logs” on page 204
- “Server Resources” on page 205
- “Network Traffic Logs” on page 205

## Server Logs

The “Log” section of the Advanced tab of the Network Connector Server window defines the Network Connector server’s logging parameters.

**Figure 35. Advanced Tab—Log Area**



The screenshot shows a window titled "Log" with the following controls:

- Log Level:** A dropdown menu currently showing the value "1".
- Log Path:** Two radio button options:
  - ☒ **Server Executable Path**
  - ☐ **Alternative Path (Full Name):** A text input field containing the path "c:\nc.log".



### Tip

For a description of the Advanced tab, refer to “Advanced Tab” on page 199.

Logging parameters include:

- **Log Level:** can be 1–5, where 5 is the most detailed log level.



### Tip

Set the log level to 0 to disable logging when you finish troubleshooting the server.

- **Log Path:** defines the location where the log file is created:
  - **Server Executable Path:** the log file is created in the same location where the server executable resides, as follows:  
`...\Whale-Com\e-Gap\common\bin\whlios.log`
  - **Alternative Path:** the log file is created in the location you specify here. Make sure to enter the full file path.



### Tip

The log files can be written, read, and deleted while the Network Connector is in session.

## Server Resources

The “Server Resources” area of the Advanced tab of the Network Connector Server window defines the server’s resource usage. It is recommended you do not change the default settings; they are only used for advanced troubleshooting purposes. **For example:** perform server optimizations by fine tuning its threads and memory usage.

**Figure 36. Advanced Tab—Server Resources Area**

Server Resources			
Number of Threads:	1	per CPU	Device Timeout: 20000 Milliseconds
Tunnel Buffer Size:	16	KB	Service Timeout: 20000 Milliseconds
Device Buffer Size:	4	KB	<button>Restore Defaults</button>



### Tip

- For a description of the Advanced tab, refer to “Advanced Tab” on page 199.
- If you do change the default server resources settings, once you are through troubleshooting the server, in the “Server Resources” section of the Advanced tab, click **Restore Defaults**.

## Network Traffic Logs

This section describes how you enable the logging of network traffic on the Network Connector server.



### Caution

Use network traffic logs for advanced troubleshooting purposes only, since they create heavy, accumulative dump files. The files are not deleted automatically, and may reduce the server performance considerably.



### Tip

The dump files can be written, read, and deleted while the Network Connector is in session.

***To enable logging of network traffic on the Network Connector server:***

1. On the computer where the Network Connector server is installed, access the following Registry key:

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WhaleCom\e-Gap\RemoteAccess
```

2. Under the key you accessed in step 1, create a new Registry key: `NetworkConnector`.
3. Under the key you created in step 2, create a DWORD value named `log\sniff`, and set the value data to one of the following:
  - 1: enables logging of low level network traffic to and from remote clients.
  - 2: enables logging of tunneled network traffic to and from remote clients.
  - 3: enables logging of both low level and tunneled network traffic to and from remote clients.

The low level and tunneled traffic dumps consist of similar information, but are not necessarily the same, since not all low level traffic is tunneled, and vice versa.

*The dump files are created in the same location where the log files are created, as described in “Server Logs” on page 204, with the following file names:*

- *Low level network traffic:* `<log_file_name>.lowlevel.dmp`
- *Tunneled network traffic:* `<log_file_name>.tunnel.dmp`



#### Tip

- The `log\sniff` registry value is polled by the server executable while running, and may be updated while the Network Connector is in session.
- Set the `log\sniff` value to 0 to disable packet dumps when you finish troubleshooting the server.
- The dump files are written in TCPDUMP format.

## Troubleshooting the Network Connector Client

This section describes how you configure the Network Connector client to create logs and packet dumps, for troubleshooting purposes.



#### Tip

Both log and dump files can be written, read, and deleted while the Network Connector is in session.



#### Caution

It is recommended you **do not** enable dumps. They should be used for advanced troubleshooting purposes only, since they create heavy, accumulative dump files. The files are not deleted automatically, and may reduce the server performance considerably.

***To enable logs and packet dumps on the Network Connector client:***

1. On the endpoint computer, access the following Registry key:  
`My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WhaleCom\Client`
2. Under the key you accessed in step 1, create a new Registry key:  
`NetworkConnector`.
3. Under the key you created in step 2, create one or both of the following values:
  - In order to enable logging, create a DWORD value named `log`, and set the value data according to the required log level. Log level can be 1–4, where 4 is the most detailed log level.  
The log file is created in the same location where the client executable resides, as follows: `C:\Program Files\Whale Communications\Client Components\3.1.0\whlioc.log`



**Tip**

Set the `log` value to 0 to disable logging when you finish troubleshooting the client.

- In order to enable dumping of network packets, create a DWORD value named `log\sniff`, and set the value data to one of the following:
  - 1: enables logging of low level network traffic to and from the virtual network.
  - 2: enables logging of tunneled network traffic to and from the virtual network.
  - 3: enables logging of both low level and tunneled network traffic to and from the virtual network.

The low level and tunneled traffic dumps consist of similar information, but are not necessarily the same, since not all low level traffic is tunneled, and vice versa.

The dump files are created in the same location where the client executable resides, as follows: `C:\Program Files\Whale Communications\Client Components\3.1.0\whlioc.dmp`



**Tip**

- The `log\sniff` registry value is polled by the client executable while running, and may be updated while the Network Connector is in session.
- Set the `log\sniff` value to 0 to disable packet dumps when you finish troubleshooting the client.
- The dump files are written in TCPDUMP format.





# Providing Access to Internal File Systems

The Intelligent Application Gateway (IAG) provides two applications that enable remote users to access file systems on the internal network:

- The Local Drive Mapping application provides access to Windows shared network folders, as described in “Local Drive Mapping” on page 209.
- The File Access application provides access to Windows Network and Novell NetWare file servers, as described in “File Access” on page 211.

## Local Drive Mapping

The Local Drive Mapping application enables you to map internal Windows shared network folders (shares) to network drives on remote users’ local computers. Users can then connect to the shares directly from the remote computer, and, depending on policy configuration, download and upload files to and from those drives. Local Drive Mapping is supported on endpoint computers that run Windows XP, Windows 2003, and Windows 2000 operating systems.



### Note

We recommend that you enable this feature only for endpoints that comply with your corporate endpoint policy.

**For example:** only endpoints where the latest update of the corporate anti-virus program is running are allowed access to internal shares. For details on how you determine endpoint policies for an application refer to “Endpoint Policies” on page 93.

You can enable access to multiple shares, by adding multiple Local Drive Mapping applications to the trunk, one for each share. For each share, you can decide how it will be accessible to remote users:

- As soon as users log into the portal homepage, the share is automatically added to the Windows Explorer shares on the endpoint computer (default option).
- Via a link on the portal homepage.



#### Note

- Once the drive is mapped on the endpoint computer, it is displayed in Windows Explorer with the IP address of the local listener that is used as the relay to the application server.
- If you define a share as a prerequisite application to another application, the IAG automatically connects to the share prior to launching this application. For details regarding prerequisite applications, refer to “General Tab” on page 68.

## Mapping Shares

This section describes how you map one share; repeat the procedure to map multiple shares. In order to enable Local Drive Mapping on Windows XP/2003, additional configuration is required, as described in “Windows 2003/XP Support” on page 210.


### *To map a share to a local network drive:*

1. Using the Add Application Wizard, from the “Client/Server and Legacy Applications” drop-down list, add the applicable “Local Drive Mapping” application to the trunk.



#### Tip

For details, refer to “Creating an SSL VPN Portal” on page 28.

2. Define mapping parameters in the step “Server Settings”. For details, click  [Help](#).

*Once you add the application to the trunk and activate the configuration, the share is accessible to remote users as soon as they log into the portal homepage. The share is accessible either via Windows Explorer, or as a link on the portal homepage, depending on the configuration of the IAG.*

## Windows 2003/XP Support

Local Drive Mapping is supported on endpoint computers that run Windows XP, Windows 2003, and Windows 2000 operating systems. However, in order to enable Local Drive Mapping on Windows XP/2003, you must also add the application “Local Drive Mapping Setup (Windows XP/2003)” to the site, via the Add Application Wizard, and run it once from the endpoint computer prior to launching the “Local Drive Mapping” application.

This setup disables SMB over TCP/IP. In order to enable Local Drive Mapping on Windows XP/2003, users are required to run the setup application only once, at the end of which the application prompts them to restart the computer. In order to run this setup, users must be logged in with Administrator privileges, to enable changes to the Registry.



#### Note

This setup may decrease SMB performance (no direct hosting), and may impact applications that rely on SMB over TCP/IP.

We recommend that you set this application up as follows:

- In the Server Settings tab of the Add Application Wizard, **do not** enable the option “Launch Automatically on Start”, else users will be prompted to restart their computer each time they access the site.
- In the next step—Portal Link—activate the option “Add Link on Whale Portal and Toolbar” and define the link settings, so that the setup can be accessed via the portal homepage or the Whale toolbar. Use the “Description” field to add a note telling users of Windows XP/2003 they need only run this application once in order to enable access to mapped drives.
- Do not define this application as a prerequisite application to a Local Drive Mapping application, else users will be prompted to restart their computer each time they access the mapped drive.

## File Access

File Access is a web application that enables authorized remote users to access, view, and download files from the organization’s Windows Network and Novell NetWare file servers from any location, and to upload files to the servers, using a browser. Via the portal, File Access presents remote users with an Explorer-like view, from which all permitted file folders can be accessed.

This section describes:

- How File Access works, on page 212.
- How you enable remote access to the File Access application, on page 212.
- Configuration of the File Access option in the Configuration program, on page 220.

## How File Access Works

The File Access application enables you to define the domains, servers, and shares which will be accessible to authorized remote users over the Internet. The existing network resource definitions are used as the basis for the File Access definitions, including:

- Domains
- Servers
- Shares
- Individual user permissions

After you define the enabled File Access resources, remote users are able to view only the specific folders for which they already have access permissions within the organization. These will invariably be a subset of the cross-organization domains, servers, and shares, defined for File Access. However, if the remote user has permission to access a certain domain, server, or share, which was not defined as part of the File Access, these locations will not be accessible regardless of such permission.

## Enabling Remote Access to the File Access Application

This section describes how you set up the IAG to enable remote access to the File Access application:

- “Windows Domain Settings” on page 212 describes the steps you need to take in order to enable access to Windows file servers.
- “Novell NetWare Settings” on page 220 describes the steps you need to take in order to enable access to Novell NetWare Servers.



### Note

If you wish to enable access to both types of servers, follow the instructions provided in both sections.

## Windows Domain Settings



### Note

In order to configure the domain settings described here, you need to have a working knowledge of Windows networking.

This section describes the Windows domain setup required in order to share Windows Network resources through the File Access application, and the trust relationships between the domains in a multiple-domain environment.

You can set up the IAG Windows domain using one of two options:

- Define the IAG as a domain controller for a new Active Directory domain, as described in “Setting Up the IAG as a Domain Controller” on page 213.
- Join the IAG to an existing Windows domain; for this setup, refer to “Joining the IAG to an Existing Domain” on page 215.

## Setting Up the IAG as a Domain Controller

In this setup, you configure the IAG as the domain controller for a new Active Directory (Windows 2003) domain, in a new domain tree, in a new forest. Follow the guidelines provided below for this type of configuration:

- During the installation of the Active Directory on the IAG, make sure to select the following options:
  - Domain Controller for New Domain
  - New Domain Tree
  - New Forest
- At the IAG verify that, for the following Windows services, Startup Type is set to Automatic:
  - Computer Browser (optional, for performance enhancement)
  - Distributed Transaction Coordinator
  - Workstation
- Still at the IAG, on the Local Area Connection that is used to access File Access resources, verify that a Client for Microsoft Networks is installed and activated. For instructions, refer to “Installing a Client for Microsoft Networks” on page 217.
- Establish domain trust relationships between the IAG and every domain (one or more) that holds File Access users. Users can be part of a user domain or a resource domain. The File Access domain must trust the domain or domains that hold the users, whereas the trusted domains may not trust the File Access domain.
- Grant local logon permissions on the IAG to all File Access users, regardless of their privileges.



### Best Practice

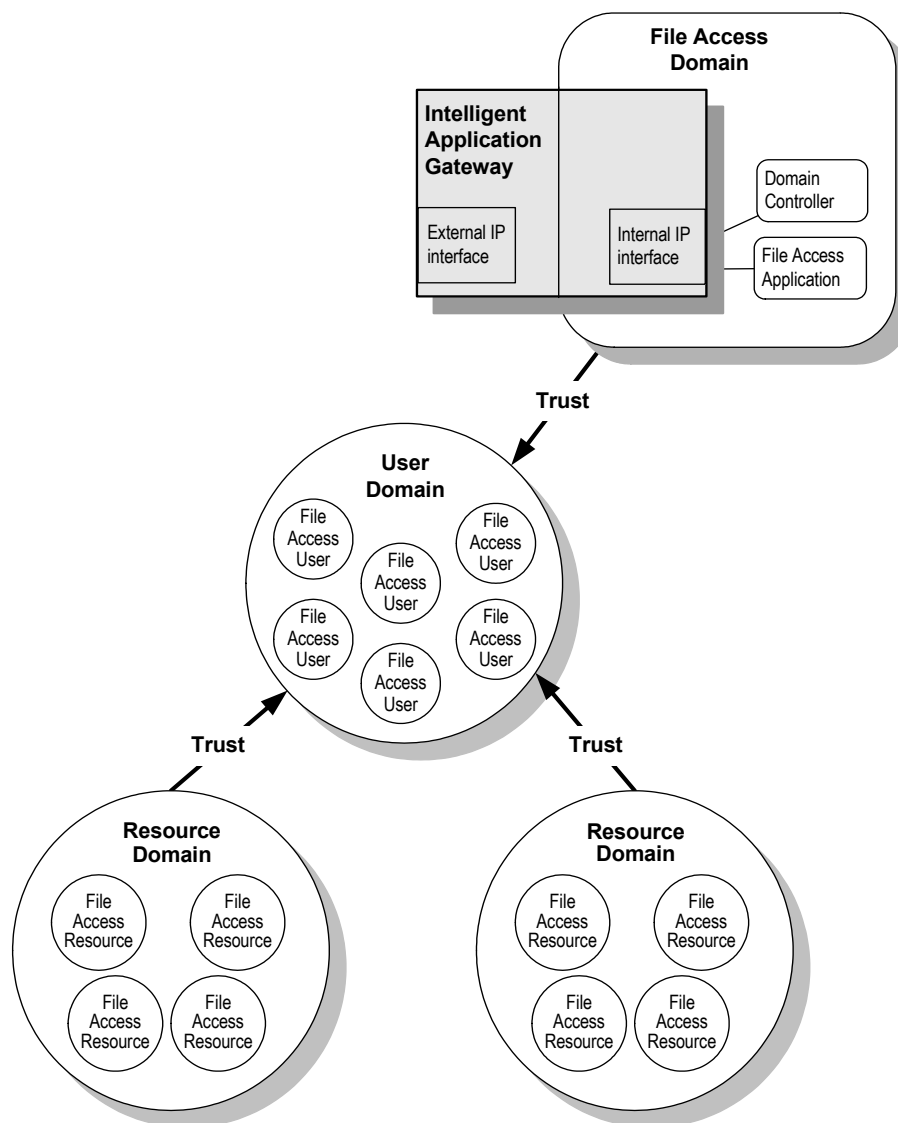
Create a group that will contain all File Access users from various domains.

Figure 37 on page 214 illustrates a sample File Access environment with three domain-types:

- File Access domain, consisting of the IAG.
- User domain, holding all File Access users. Although it is recommended that one domain holds all the File Access users, there can be multiple user domains in this setup. Users can also be part of a resource domain.
- Resource domains, holding the shared resources that are enabled via the File Access application.

Note the trust relationships between the domains in this setup.

**Figure 37. Sample Environment, with IAG as New Domain**



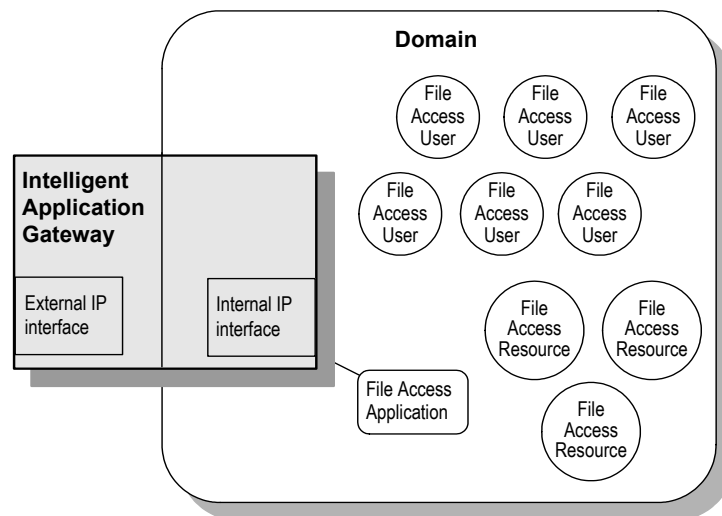
## Joining the IAG to an Existing Domain

In this setup, you join the IAG to an existing Windows domain, which holds all File Access users and resources. The following sections describe the steps you need to take in order to set up the IAG for this type of environment:

- If you are joining the IAG to a domain that is **not** a native Active Directory domain, that is, a Windows NT® 4.0 domain or an Active Directory Mixed Mode domain, you need to go through both sets of steps described below.
- If you are joining the IAG to a native Active Directory domain, that is, a Windows 2000 or Windows 2003 domain, skip the first set of steps and take the steps described in “Steps you need to take for all File Access installations when joining a domain:” on page 217.

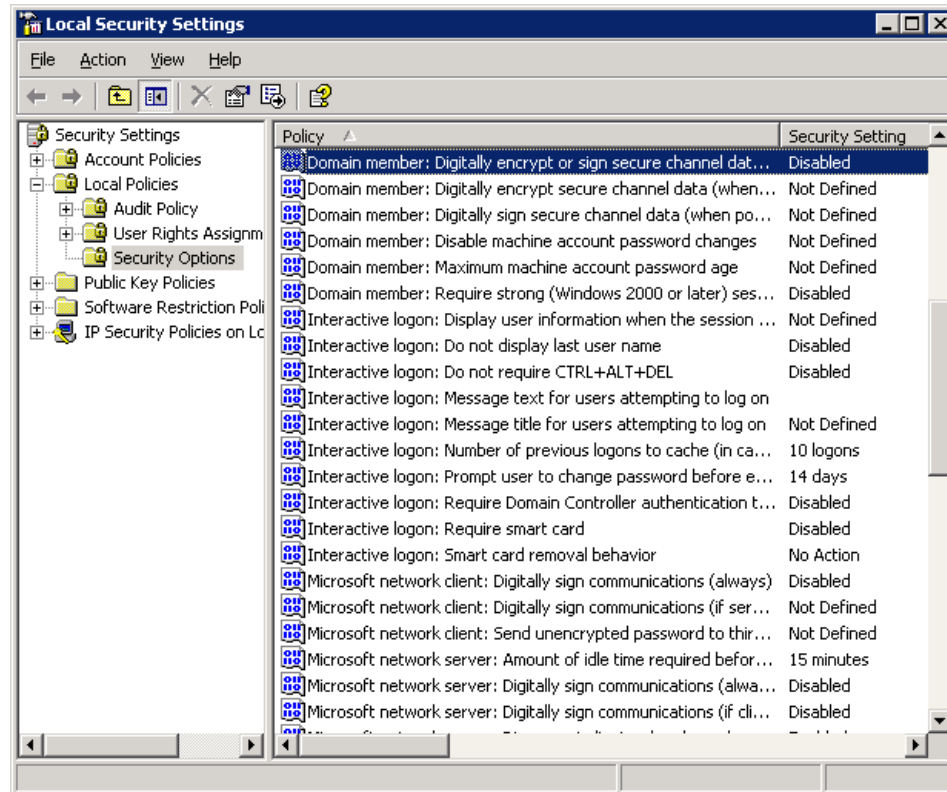
Figure 38 illustrates a sample File Access environment where the IAG joins an existing domain.

**Figure 38. Sample Environment, with IAG as Part of Domain**



***Steps you need to take if you are joining the IAG to a Windows NT 4.0 domain or an Active Directory mixed Mode domain:***

1. At the IAG, in the Windows desktop, click **Start**, then select **Programs > Administrative Tools > Local Security Policy**.  
*The Local Security Settings window is displayed.*
2. In the Tree pane, select **Local Policies > Security Options**.



3. In the right, Policy pane, set the Local Security Policy settings of the policies listed in Table 22.



#### Tip

To edit a policy, double-click it; in the Local Security Policy Setting dialog box, select the required setting and click **OK**.

**Table 22. Local Security Policy Settings**

Parameter	Description
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled
Domain member: Require strong (Windows 2000 or later) session key	Disabled
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Network Security: LAN Manager Authentication Level	Send LM & NTLM responses





#### Note

If you change any of the Local Security Policy settings, you need to restart the IAG in order for the change to go into effect.

#### *Steps you need to take for all File Access installations when joining a domain:*

1. At the IAG verify that, for the following Windows services, Startup Type is set to Automatic:
  - Computer Browser (optional, for performance enhancement)
  - Distributed Transaction Coordinator
  - Workstation
2. Still at the IAG, on the Local Area Connection that is used to access File Access resources, install a Client for Microsoft Networks. For detailed instructions, refer to “Installing a Client for Microsoft Networks” on page 217.
3. Join the IAG to the domain that holds the File Access users and shared resources.
4. Grant local logon permissions on the IAG to all File Access users, regardless of their privileges.



#### Best Practice

In the domain, create a group of all File Access users, and grant the group local logon permissions on the IAG, regardless of each user’s privileges.

### Installing a Client for Microsoft Networks

This section describes how you install a Client for Microsoft Networks on the IAG during the domain setup.

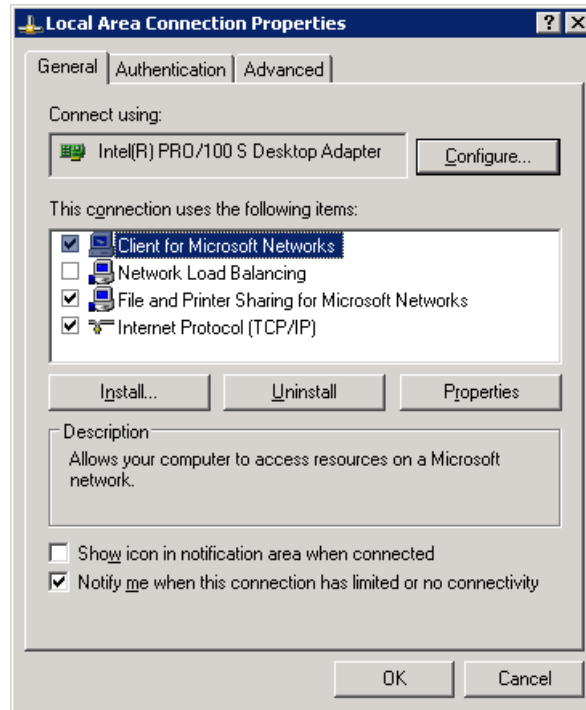


#### Note

You might be required to provide the Windows Server 2003 Installation CD during the course of this procedure.

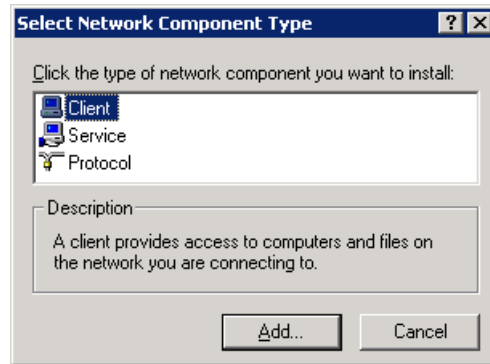
#### *To install a Client for Microsoft Networks:*

1. At the IAG, in the Windows desktop, click **[Start]**, then select **Settings > Network Connections**.
2. In the list of connections, select the Local Area Connection that is used to access the File Access resources.  
*The Local Area Connection Status dialog box is displayed.*
3. Click **[Properties]**.

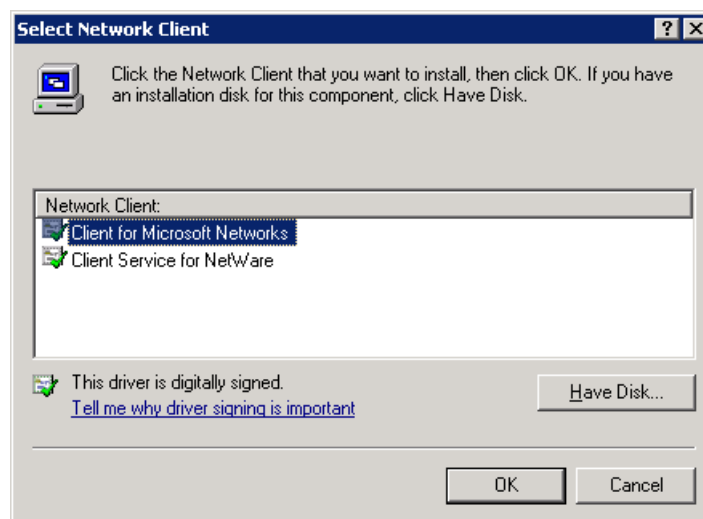


4. Under the component list (“This connection uses the following items”), check whether “Client for Microsoft Networks” is listed, and do one of the following:
  - If “Client for Microsoft Networks” **is listed**, and the box next to it is **checked**, you do not need to take any further steps. Click **OK** to close the dialog box.
  - If “Client for Microsoft Networks” **is listed**, and the box next to it is **unchecked**, check the box, then click **OK**. You do not need to take any further steps.
  - If “Client for Microsoft Networks” is **not listed** in the Local Area Connection Properties dialog box, continue with the following steps.
5. In the Local Area Connection Properties dialog box, under the component list, click **Install...**.

*The Select Network Component Type dialog box is displayed.*



6. Verify that “Client” is selected in the list, and click **Add...**.  
*The Select Network Client dialog box is displayed.*



7. Verify that “Client for Microsoft Networks” is selected in the list, and click **OK**. If prompted, insert the Windows Server 2003 Installation CD.  
*The Select Network Client dialog box closes. In the Local Area Connection Properties dialog box, “Client for Microsoft Networks” is listed.*
8. Make sure that the box next to “Client for Microsoft Networks” is **checked**, and click **OK** to close the dialog box.  
*The installation of the Client for Microsoft Networks is complete.*
9. Reset the IAG, as prompted.

## Novell NetWare Settings

In order to share Novell NetWare Server resources through the File Access application, you need to install a Novell® client on the IAG, as described in this section.



### Note

While remote users interact with Novell NetWare Servers through the File Access interface, temporary “virtual” users may be created on the IAG, with the following name format:

`whnwu_<hexadecimal_value>`

Those users are deleted as soon as the “real” user closes the File Access interface.

### *To set up the IAG to enable File Access to Novell NetWare Servers:*

1. Install a Novell client on the IAG, using a Typical installation mode.
2. When prompted, restart the IAG.

*Access to Novell NetWare Servers can be enabled on the IAG.*

## Configuring File Access in the Configuration Program: Overview

The following sections describe the configuration of the File Access option in the Configuration program.



### Note

The File Access application can only be configured and used via a Portal trunk.

In order to configure the option, you go through the following stages:

- You configure the File Access administration settings, including:
  - Remote users’ access to their Home folder and mapped drives, and share permissions
  - Settings that determine how you log on to Novell Directories in order to gain access to Novell NetWare Servers
  - Access permissions to Domains, Servers, Shares

Administration settings are described in “File Access Administration Settings” on page 221. These settings apply to all trunks where File Access is enabled.

- If the network includes Novell NetWare Services, and you wish to enable remote access to NetWare Servers, you need to set up authentication with the Novell Directory Service (NDS). For details, refer to “Configuring Authentication with the Novell Directory Service” on page 231.
- Add the File Access application to the trunk, as described in “Creating an SSL VPN Portal” on page 28.
  - If the trunk uses the default portal homepage supplied with the IAG, a link to the File Access application is automatically added to the page.
  - When using a custom homepage, you have to manually add the link to the page. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Using a Custom Portal Homepage” on page 61.
- Optionally, you can change the date format of files and folders, as will be viewed on remote users’ browsers, as described in “Changing the Date Format of Files and Folders” on page 234.
- You can also configure the File Access application so that users are not presented, in the end-user interface, with a folder tree on the left pane. This prevents users from browsing to any folders other than the one defined as the application URL or its subfolders. For details, refer to “Hiding the Folder Tree in the End-User Interface” on page 234.



#### Tip

You can customize the language definitions of the end-user pages, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Changing File Access Language Definitions” on page 71.

## File Access Administration Settings

You configure the File Access administration settings once, for all the trunks where the File Access option is activated. Administration settings include:

- Configuring remote users’ access to their Home folder and to mapped drives, and users’ view permissions to configured shares, described in “Configuring Home Directory, Mapped Drives, and Share Permissions” on page 223.
- The settings that determine how you log on to Novell Directories in order to gain access to Novell NetWare Servers, described in “Novell Logon Settings” on page 227.
- The domains, servers, and shares which are exposed to remote users using File Access, as described in “Configuring Access to Domains, Servers, and Shares” on page 229.

Once you configure the administration settings in the File Access window, the next time you open the window, the settings remain intact.



#### Note

In order to configure File Access administration settings, you must be a member of the Administrators group of the IAG.

## Accessing the File Access Window

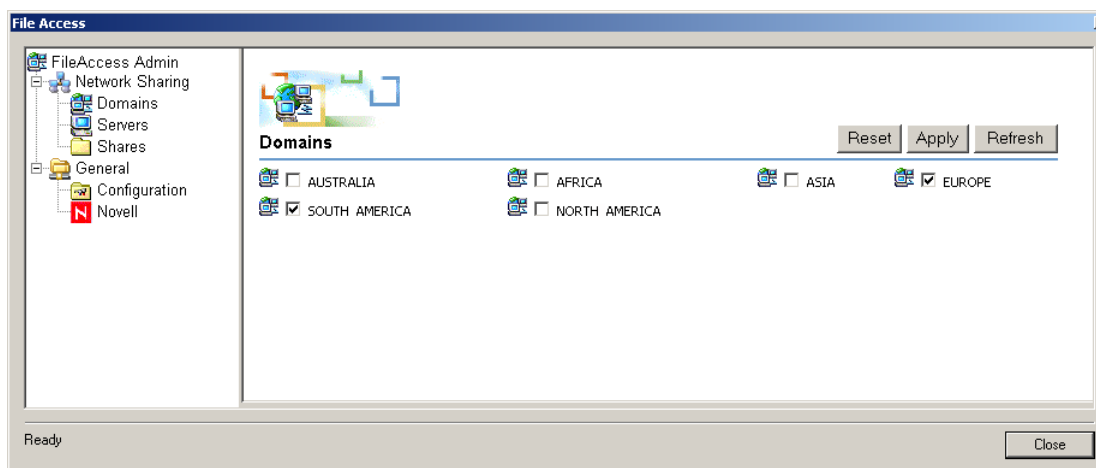
This section describes how you access the File Access window, in order to configure the global File Access administration settings.

### *To access the File Access window:*

1. In the Configuration program, on the **Admin** menu, click **File Access...**  
*The Windows' Enter Network Password dialog box is displayed.*
2. Enter User Name and Password, then click **OK**.

*The network is browsed, and the File Access window is displayed, showing all the domains in the network which are accessible from the File Access host. Depending on the complexity of the network, this may take a few seconds.*

**Figure 39. Sample File Access Administration Window**



## Configuring Home Directory, Mapped Drives, and Share Permissions

This section describes how you use the File Access Configuration window to configure the following access and view permissions for remote users, as they use the File Access interface:

- **Home Directory:** remote users' access to their Home Directory.
- **Mapped Drives:** remote users' access to their mapped drives. Mapped drives are defined by the users logon script, which is located in the organization's Domain Controller, in the `NETLOGON` directory.

File Access automatically supports batch files (`.bat`, `.exe`). For any other scripts, such as JavaScript™ (`.js`) or Visual Basic® (`.vbs`), you can do one of the following:

- “Wrap” each script within a separate batch file.
- During the configuration of users' access to mapped drives, specify the script engine that will be used to run the user's logon script, as detailed in the configuration procedure.



### Note

Before you configure the Mapped Drives option, see the following sections:

- “Limitations of Mapped Drives” on page 225.
- “Deleting User Profiles When Using Mapped Drives” on page 226.

- **Share Permissions:** users' permissions to view configured shares, that is, whether users will view all the shares that are configured for File Access, or only the shares for which they have access permissions.



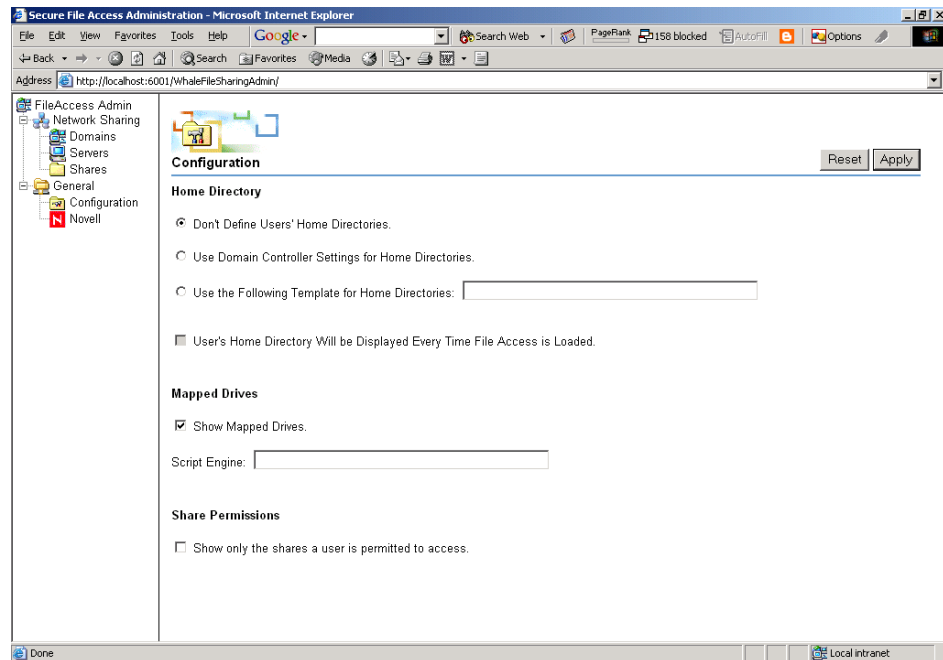
### Note

Share Permissions settings affect the Share level only; they do not affect the way users view folders in a share.

### *To configure Home Directory, mapped drives, and share permissions:*

1. Access the File Access window, as described in “Accessing the File Access Window” on page 222.
2. In the left pane of the File Access window, under **General**, click **Configuration**.

*The Configuration settings are displayed in the right pane.*



3. To configure access to the Home Directory, select one of the following options:

- **Don't Define User's Home Directories:** when this option is selected, the Home Directory is not accessible to remote users. The “My Home Directory” button and tree item are not displayed in the browser.
- **Use Domain Controller Settings for Home Directories:** the Home Directory is accessible to remote users, through a “My Home Directory” button and tree item. Home Directory path information is taken from the domain controller.
- **Use the Following Template for Home Directories:** the Home Directory is accessible to remote users, through a “My Home Directory” button and tree item. Home Directory path information is taken from the template you define in the text field. You can define the path to the template using one of two methods:
  - Valid UNC path.  
**For example:** \\server\share\dir1\dir2
  - Valid DFS path.  
**For example:** domain\server\share\dir1\dir2

In either of those path types, you can use one or both of the following variables: %domain% and %username%.

**For example:**

%domain%/users/%username%



4. Determine whether the browser will display the listing of the Home Directory each time a remote users accesses File Access. This is controlled by the option: **User's Home Directory Will be Displayed Every Time File Access is Loaded.**
5. To configure access to mapped drives, check the option **Show Mapped Drives**. If the users logon script is not a batch file (.bat, .exe), or not wrapped within a batch file, enter the full path of the script engine in the field **Script Engine**.



#### Note

- Before you configure the Mapped Drives option, see “Limitations of Mapped Drives” on page 225 and “Deleting User Profiles When Using Mapped Drives” on page 226.
- You can only specify one script engine type in the “Script Engine” field.

6. By default, users view all the shares that you configure for File Access. If you wish users to view only the configured shares for which they have access permissions, check the option: **Show only the shares a user is permitted to access.**
7. When you finish configuring users' access to the Home Directory and mapped drives, at the top right of the File Access window, click **Apply**.



#### Tip

In order to configure remote users' access to domains, servers, and shares, refer to “Configuring Access to Domains, Servers, and Shares” on page 229.

8. When you finish configuring administration settings, click **Close** at the bottom of the File Access window.

*Once you activate the configuration, remote users' ability to access their Home Directory and mapped drives, and to the shares configured for File Access, is determined according to the definitions you configured here.*

## Limitations of Mapped Drives

When defining mapped drives, please note the following:

- File Access supports the mapping of drives G and up.
- Due to a Windows API limitation, not all environment variables are supported by the File Access option. If you use unsupported environment variables in the users logon scripts, the remote user will not be able to access the mapped drives as expected.

In order to examine which environment variables are supported for a typical user, take the following steps at the IAG:

- Open a Command prompt, and impersonate the user by entering this command: `runas/user:<username> cmd.exe`  
Where <username> is the username as entered by the user during login
- In the secondary command window that opens, representing the user you defined, run the `set` command. The environment variables that are displayed are the variables that are supported by the IAG for this user.

### Deleting User Profiles When Using Mapped Drives

Each time a remote user accesses mapped drives via File Access, the File Access engine runs the user's logon script. For each new user, the operating system of the IAG creates and saves a user profile.

By default, user profiles are not deleted from the server, including old profiles that are no longer used. This consumes disk space unnecessarily. In addition, in environments where a large number of users access mapped drives, if a 10,000 profile limit is reached, new profiles cannot be created, and new users cannot access the drives.

This section describes how you can configure the IAG to delete user profiles from the IAG when required. Note the following:

- Only profiles of domain users are deleted; profiles of local users are not deleted.
- Least recently-used profiles are deleted first.
- Profiles of users who are currently connected to one or more mapped drives are not deleted.

#### ***To delete user profiles from the IAG:***

1. Access the following CustomUpdate folder; if it does not exist, create it:  
`...\Whale-Com\e-Gap\von\conf\CustomUpdate`
2. Copy the file `userProfiles.ini` from this folder:  
`...\Whale-Com\e-Gap\von\conf`  
Place it in the CustomUpdate folder you accessed in step 1. If such a file already exists in the custom folder, use the existing file.
3. Configure the parameters in the file in the custom folder:

**Table 23. Deleting User Profiles—Configuration Parameters**

Parameter	Description
EnableProfileDeletion	Determines whether user profiles are deleted from the IAG or not.
HighWaterMark	Number of profiles above which the deletion process starts. Must be equal to or greater than the LowWaterMark parameter.
LowWaterMark	Number of profiles that are kept on the IAG once the deletion process is complete. A minimum number of 50 profiles must remain undeleted.
SleepPeriod	After the number of minutes defined here, the process checks whether the HighWaterMark has been reached, and deletes excessive profiles as required.
DoNotRemoveProfile	<p>Defines a user profile that is not deleted.</p> <p><b>For example:</b></p> <p><code>DoNotRemoveProfile = MyDomain\Admin</code></p> <p>You can configure an unlimited number of profiles that will be left out of the deletion process, by configuring one <code>DoNotRemoveProfile</code> parameter for each profile.</p>

## Novell Logon Settings



### Note

- This section is only relevant if the network includes Novell NetWare Services, and you wish to enable remote access to NetWare Servers.
- The settings you configure here are not related to the Novell Directory server, which you can use for authentication and authorizing.

In the following procedure, you determine the logon credentials that are used during the configuration of users' access to the Novell NetWare Servers. Note that, during the configuration of the NetWare Servers, only the servers and shares that are enabled to the user with which you log on will be available in the File Access window.

**Tip**

The actual configuration of remote users' access to the NetWare Servers is described in "Configuring Access to Domains, Servers, and Shares" on page 229.

**To configure Novell logon settings:**

1. Access the File Access window, as described in "Accessing the File Access Window" on page 222.
2. In the left pane of the File Access window, under **General**, click **Novell**.  
*In the right pane, the Novell Logon settings are displayed.*

3. Select one of the following options:
  - **Using Windows User Name:** use the same credentials you used when you logged onto the File Access window, as described in "Accessing the File Access Window" on page 222.
  - **Using the Following User Name and Password:** enter credentials with which to log on.

**Tip**

Make sure the credentials you assign here enable you to view all the NetWare Servers to which you wish to configure access, such as the credentials of a Novell administrator.

4. Click **Save**, then click **Logon**.  
*The system logs you on to the Novell NetWare Services. When you configure Novell NetWare Servers, the servers and shares that are enabled to the user you define here are displayed in the File Access window.*

5. Go on to configure remote users' access to domains, servers, and shares, as described in the procedure that follows.



#### Note

- In order to log on to a different tree, enter the applicable credentials and click **Logon**.
- Only one set of credentials can be saved in the Novell Logon window.
- Any time after the initial configuration, in order to modify the configuration of remote users' access to the NetWare Servers, you need to log on to the Novell NetWare Services using the Novell Logon window.

## Configuring Access to Domains, Servers, and Shares

This section describes how you configure which domains, servers, and shares are enabled for remote access. If the network includes Novell NetWare Services, and you wish to enable remote access to NetWare Servers, refer to “Novell Logon Settings” on page 227 before you proceed.

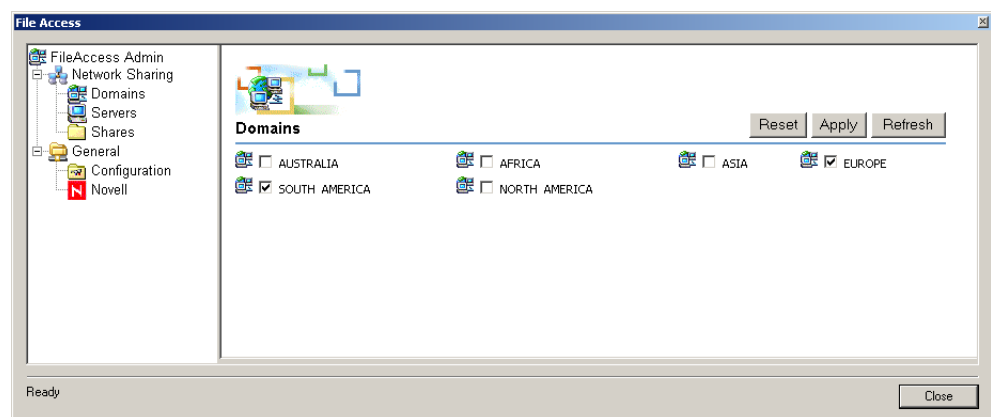


#### Tip

You can configure the File Access option so that users can only view the shares for which they have access permissions. For details, refer to “Configuring Home Directory, Mapped Drives, and Share Permissions” on page 223.

### *To configure access to domains, servers, and shares:*

1. Access the File Access window, as described in “Accessing the File Access Window” on page 222.





### Tip

If you need to refresh the display at any time, for instance if there have been changes in the domain structure since the last time you used the File Access window, click **Refresh**.

2. In the right pane of the File Access window, select the domains which will be accessible to remote users through File Access, and click **Apply**.



### Note

If the network includes Novell NetWare Services, the following services are available for selection in the Domains window:

- Novell® Directory Services®
- NetWare Servers

You can use the File Access window to enable access to NetWare Servers only; you cannot enable access to Novell Directory Services through the File Access option.

3. In the left pane of the File Access window, click **Servers**.  
*The network is browsed. In the File Access window, all the servers in the domains you selected are displayed, arranged under their respective domains.*
4. In the right pane of the File Access window, select the servers which will be accessible to remote users through File Access, and click **Apply**.
5. In the left pane of the File Access window, click **Shares**.  
*The network is browsed. In the File Access window, all the shares that are enabled on the selected servers are displayed, arranged under their respective servers.*



### Note

If you have previously configured shares in this screen to be accessible to remote users, and have since clicked **Apply** in either the Domains or the Servers screen, all the shares in this screen appear unselected, including shares that are accessible to remote users. In order to refresh the view, click **Reset**, then click **Refresh**.

6. In the right pane of the File Access window, select the shares which will be accessible to remote users through File Access, and click **Apply**.

**Tip**

If there are no shares in a selected server, the text “No shares on this server” appears under that server name.

7. When you finish configuring administration settings, click **Close** at the bottom of the File Access window.

*Once you activate the configuration, remote users are able to access the selected domains, servers, and shares through the File Access interface, depending on their access permissions within the organization.*

## Configuring Authentication with the Novell Directory Service

**Note**

This section is only relevant if the network includes Novell NetWare Services, and you wish to enable remote access to NetWare Servers.

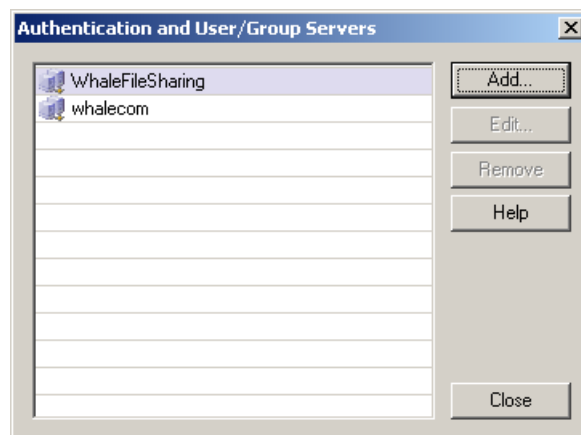
This section describes the steps you need to take in order to enable remote access to NetWare Servers, including:

- Configure a Novell Directory authentication server.
- Assign the Novell Directory authentication server as one of the trunk's session authentication servers.

***To enable remote access to NetWare Servers:***

1. In the Configuration program, on the **Admin** menu, click **Authentication and User/Group Servers...**

*The Authentication and User/Group Servers dialog box is displayed.*



2. In the Authentication and User/Group Servers dialog box, click **Add...**.  
*The Add Server dialog box is displayed.*

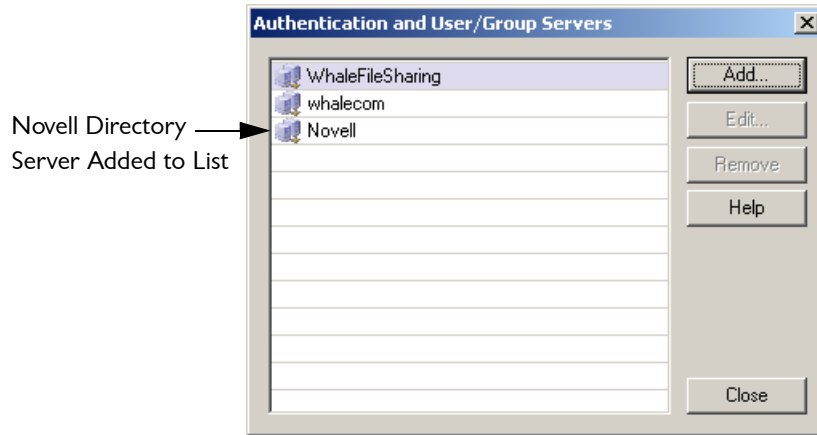
The screenshot shows a Windows-style dialog box titled "Add Server". It contains the following fields and controls:

- Type:** A dropdown menu currently showing "ACE".
- Name:** An empty text input field.
- IP/Host:** An empty text input field.
- Port:** A text input field containing "5500".
- Alternate IP/Host:** An empty text input field.
- Alternate Port:** A text input field containing "5500".
- Enable PIN Mode:** An unchecked checkbox.
- Use a Different Server for User/Group Authorization:** An unchecked checkbox.
- Select Server:** A dropdown menu currently showing "Built-In Users/Groups".
- Buttons:** "Help", "OK", and "Cancel" buttons at the bottom.

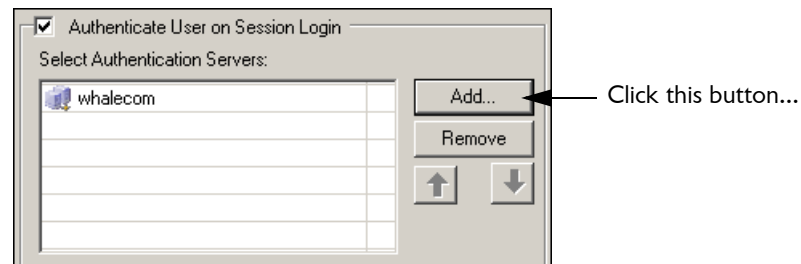
3. From the “Type” drop-down list select “Novell Directory”, and define the server. For details, click **Help**.
4. When you finish defining the sever, click **OK** to close the Add Server dialog box.

*In the Authentication and User/Group Servers dialog box, the Novell Directory server you defined is added to the list of authentication servers.*





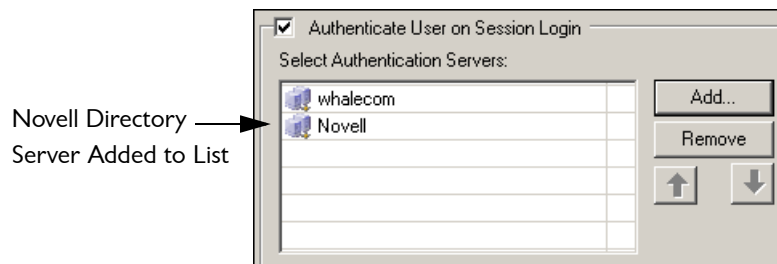
5. Close the Authentication and User/Group Servers dialog box.
6. In the main window of the Configuration program, next to “Advanced Trunk Configuration”, click **Configure...** to open the Advanced Trunk Configuration window. Select the Authentication tab.
7. In the Authentication tab, in the top left area, click **Add...** to the right of the “Select Authentication Servers” list.



*The Authentication and User/Group Servers dialog box is displayed.*

8. In the Authentication and User/Group Servers dialog box, select the server you defined in step 3, then click **Select**.

*The Authentication and User/Group Servers dialog box closes. In the Authentication tab, the Novell Directory server you defined is added to the list of servers in the Authentication tab:*



*Remote users access to Novell NetWare Servers is enabled.*

## Changing the Date Format of Files and Folders

The date format of files and folders that remote users view on their browsers is determined by the IAG where the File Access application is installed, not by the user's local computer.

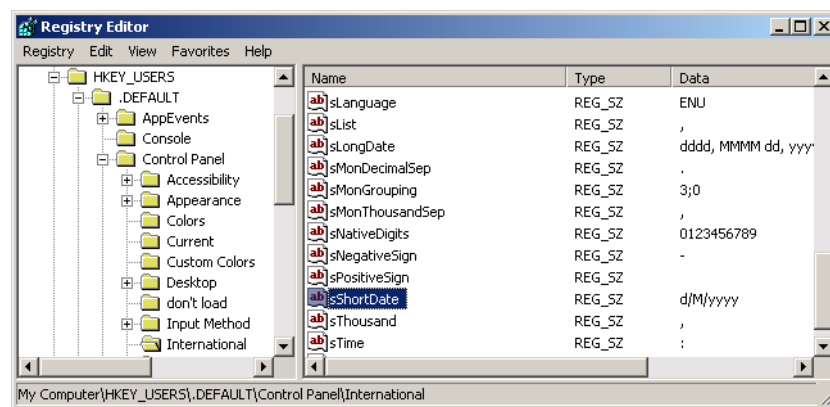
By default, the format is: M/d/yyyy. You can change the date format to d/M/yyyy, as described in this section.

### *To change the date format of files and folders:*

1. At the IAG where the File Access application is installed, use the Registry Editor to access the following location:

HKEY\_USERS\DEFAULT\Control Panel\International

2. Change the **Value data** of SShortDate to d/M/yyyy.



3. Restart the IAG.

*When remote users view files and folders, the date format is the one you set here.*

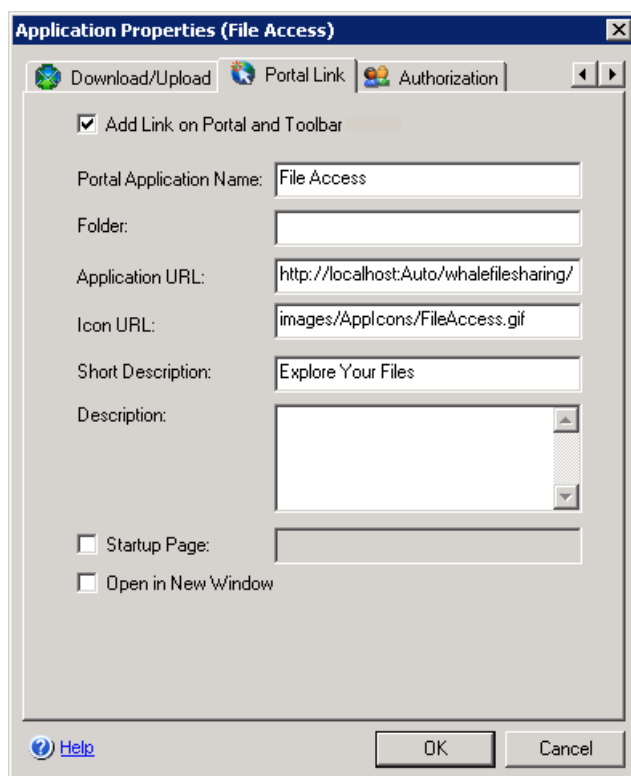
## Hiding the Folder Tree in the End-User Interface

By default, the end-users' File Access interface presents users with a folder tree in the left pane. The folder tree contains all the folders you enable in the File Access administration window, as described in "File Access Administration Settings" on page 221. If you wish to restrict users' access to a specific folder, you can define the path of the folder as the application URL, and disable the view of the folder tree. Users can then access only the path that is defined as the application URL, including all subfolders.

This procedure describes how you hide the folder tree if the trunk you are configuring uses the default portal homepage supplied with the IAG. If you use a custom homepage, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to "Adding Links to IAG Features on a Custom Homepage" on page 66.

***To hide the folder tree in the end-user interface:***

1. In the Configuration program's configuration pane, double-click the File Access application.  
*The Application Properties dialog box is displayed.*
2. Select the Portal Link tab.



3. In the "Application URL" field enter the following:  
`http://localhost:Auto/WhaleFileSharing/  
?Path=<path>&ShowFolders=False`  
Where path is the full path of the folder users will access.

**For example:**

`http://localhost:Auto/WhaleFileSharing/  
?Path=EUROPE/NORWAY/Bergen&ShowFolders=False`



**Note**

Parameter names and values are case sensitive.

4. Click **OK**.

*Once you activate the configuration, end-users will not be presented with a tree folder in the File Access interface. In this example, when users access the File Access application, they will be presented with the Bergen folder, and will be able to browse only this folder and its subfolders.*

**Tip**

The parameter `ShowFolders` can also be used with a Home Directory definition. That is, users will be directly presented with their Home Directory, and will be able to browse only the Home Directory and its subfolders.

## Chapter 9

# Monitoring and Control

This chapter describes the monitoring and control tools that are supplied and supported by the Intelligent Application Gateway (IAG):

- Event Logging is used to log IAG-related events. Events can be logged by several reporters, including both IAG tools and third-party network reporting solutions, as described in “Event Logging” on page 237.
- The Web Monitor enables anywhere, anytime snapshot viewing of IAG events, as well as event filtering and analyzing. Where an IAG High Availability Array is deployed, you can use the Web Monitor to monitor all the IAG servers that are part of the Array. For details, refer to “Web Monitor” on page 258.
- You can monitor SSL connection attempts in the Windows Event Viewer, as described in “SSL Event Monitoring” on page 301.

## Event Logging

This section describes the IAG Event Logging, as follows:

- The Event Logging mechanism is described in “Overview” on page 238.
- Although by default no configuration is required in order for the Event Logging to work, and IAG-related events are logged and reported with no user intervention, several configuration options are available to you if you wish to adapt message reporting to your needs. Those are listed in “Optional Event Logging Configuration Steps” on page 239, and are described in detail in the subsequent sections.
- For advanced troubleshooting purposes, you can temporarily disable the Event Logging mechanism altogether, as described in “Disabling Event Logging and Reporting” on page 258.



### Tip

You can troubleshoot warnings and errors that are reported by the Event Logging mechanism, according to the message that is displayed when the event occurs. Troubleshooting instructions are provided in Appendix A: “Troubleshooting Event Logging Messages”.

## Overview

The IAG Event Logging mechanism logs and records IAG-related events to a variety of tools and output formats. Using the event logs, you can gather information about system usage, monitor user activities, be alerted about security risks, troubleshoot the IAG, and assist remote users if they encounter problems while accessing the internal resources protected by the IAG.

## Event Categories

IAG-related events recorded by the Event Logging mechanism are categorized as follows:

- System events, including service startup and shutdown, and changes to the configuration.
- Security events, including login success or failure, security policy violation or change, and password change
- Session events, including the number of sessions that are open through a trunk, session start or stop, and other session-related items

## Event Logging Reporters

The events logged by the Event Logging mechanism can be used by various reporters:

- The built-in reporter enables you to log the events in a format that can be used by the Web Monitor. In the Web Monitor, you can use the Event Query window to query the events logged by the reporter and to filter events according to type, time, and more.



### Tip

For a description of the Event Query window of the Web Monitor, see “Event Query” on page 295.

- The RADIUS reporter reports events to a RADIUS Accounting server, either any external RADIUS Accounting server, or a Windows RADIUS Accounting server installed on the IAG.
- The Syslog reporter reports events to an external industry-standard Syslog server.
- The mail reporter sends email messages regarding specific events via an SMTP server.



### Note

The built-in reporter is activated and configured by default. In order to use any of the other reporters, you have to activate and configure them, as described in the corresponding sections.

## Event Logging Messages

Event logging messages are defined in a message definitions file. All the applicable IAG interfaces are configured to send the relevant message when required.

### For example:

- A message is sent each time the configuration is changed in the Configuration program.
- A message is sent whenever a user logs into the IAG site.



#### Tip

Use the messages to troubleshoot warnings and errors. For details, refer to Appendix A: “Troubleshooting Event Logging Messages”.

If required, you can edit the default messages, define additional messages, or send messages from your own interfaces, such as custom authentication pages.

## Optional Event Logging Configuration Steps

The following Event Logging configuration options are available to you, if required:

- General event logging parameters, which are related to the Web Monitor, are described in “Configuring General Settings” on page 240.
- Configuration of the built-in reporter is described in “Configuring the Built-In Reporter” on page 242.
- Configuration of the RADIUS reporter is described in “Configuring the RADIUS Reporter” on page 243.
- Configuration of the Syslog reporter is described in “Configuring the Syslog Reporter” on page 244.
- Configuration of the mail reporter is described in “Configuring the Mail Reporter” on page 245.



#### Note

The built-in reporter is activated and configured by default. In order to use any of the other reporters, you have to activate and configure them, as described in the corresponding sections.

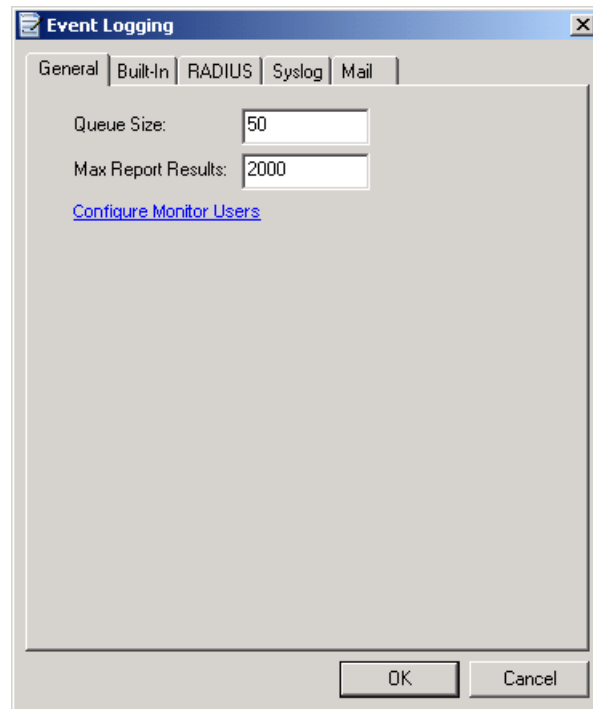
- Editing the default messages that are recorded by the Event Logging mechanism, defining additional messages, and sending messages from your own interfaces, such as custom authentication pages, are described in “Message Configuration” on page 249.

## Configuring General Settings

This section describes how you configure general Event Logging settings.

### *To configure general event logging settings:*

1. In the Configuration program, on the **Admin** menu, click **Event Logging...**  
*The Event Logging dialog box is displayed.*



2. Use the General tab to configure general settings, as described in Table 24, “General Tab Parameters”, on page 241.



**Table 24. General Tab Parameters**

Parameter	Description
Queue Size	<p>Number of events that are displayed in the Event Viewer window of the Web Monitor, as follows:</p> <ul style="list-style-type: none"><li>• Number of events that are displayed each time a user opens the Event Viewer window.</li><li>• Maximal number of events that are added to the message-list between refreshes.</li></ul> <p><b>For example:</b> if the queue size is 50, and the refresh rate is 15 seconds, after a refresh, no more than 50 events are added to the event list in the 15 seconds that elapse until the next refresh. If, in this setup, 60 events are received between refreshes, only the last 50 will be displayed in the event list.</p> <p>For a description of the Event Viewer window, refer to “Event Viewer” on page 293.</p>
Max Report Results	<p>Maximal number of events that can be fully displayed in the Web Monitor when you generate a query, as follows:</p> <ul style="list-style-type: none"><li>• Session Monitor - Statistics window: if the number of query results exceeds the number defined here, “Duration” is not displayed.</li><li>• Application Monitor - Statistics window: if the number of query results exceeds the number defined here, “Duration” and “Total Accesses” are not displayed.</li><li>• User Monitor - Statistics window: if the number of query results exceeds the number defined here, the results are not displayed. The user is notified accordingly.</li><li>• Event Report window: if the number of query results exceeds the number defined here, the number of results defined here is displayed.</li></ul> <p>For details, refer to “Web Monitor” on page 258.</p>
Configure Monitor Users	<p>Opens the computer’s Windows Local Users and Groups Manager and enables you to configure additional Web Monitor users. For details, refer to “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.</p>

## Configuring the Built-In Reporter

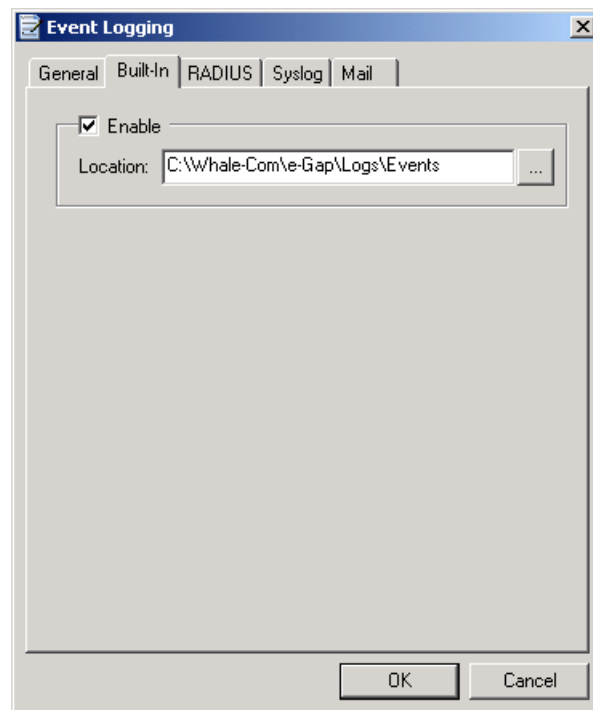
The built-in reporter enables you to save events into a log file. You can then use the Web Monitor to query the event log and to filter events according to type, time, and other parameters. For more information, see “Event Query” on page 295.

A new event log file is saved every day. Event log files are periodically deleted from the IAG, as part of the log file cleanup, described in “Log File Cleanup” on page 313.

By default, the built-in reporter is activated, and log files are saved to the `Logs\Events` folder under the IAG installation path. You can use in the Built-In tab of the Event Logging dialog box to change the default settings.

### *To configure the built-in reporter:*

1. In the Configuration program, on the **Admin** menu, click **Event Logging...**  
*The Event Logging dialog box is displayed.*



2. Use the Built-In tab to configure the settings of the built-in reporter.



#### **Note**

- If you disable the built-in reporter, you will not be able to query logs in the Web Monitor.
- It is recommended that the location where the log files are saved is on the IAG.

## Configuring the RADIUS Reporter

The RADIUS reporter logs event information to a RADIUS Accounting server. This information can then be exported in a format that any standard reporting utility can read, and visual statistics about the users and applications can be generated.



### Tip

You can install a Windows RADIUS Accounting server on the IAG, and log the information there.

### To configure the RADIUS reporter:

1. In the Configuration program, on the **Admin** menu, click **Event Logging...**  
*The Event Logging dialog box is displayed.*
2. Select the RADIUS tab, and check the “Enable” option.

The screenshot shows the 'Event Logging' dialog box with the 'RADIUS' tab selected. The 'Enable' checkbox is checked. The 'IP/Host' field is empty. The 'Port' field contains '1813'. The 'Alternate IP/Host' field is empty. The 'Alternate Port' field contains '1813'. The 'Secret Key' field is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

3. Define the RADIUS Accounting settings, as follows:

**Table 25. RADIUS Tab Parameters**

Parameter	Description
IP/Host	IP address or hostname of the RADIUS Accounting server
Port	Port number of the RADIUS Accounting server

**Table 25. RADIUS Tab Parameters (Cont'd)**

Parameter	Description
Alternate IP/Host	IP address or hostname of the alternate RADIUS Accounting server
Alternate Port	Port number of the alternate RADIUS Accounting server
Secret Key	Secret key that will be used to encrypt and decrypt the user password

4. Click **OK**.

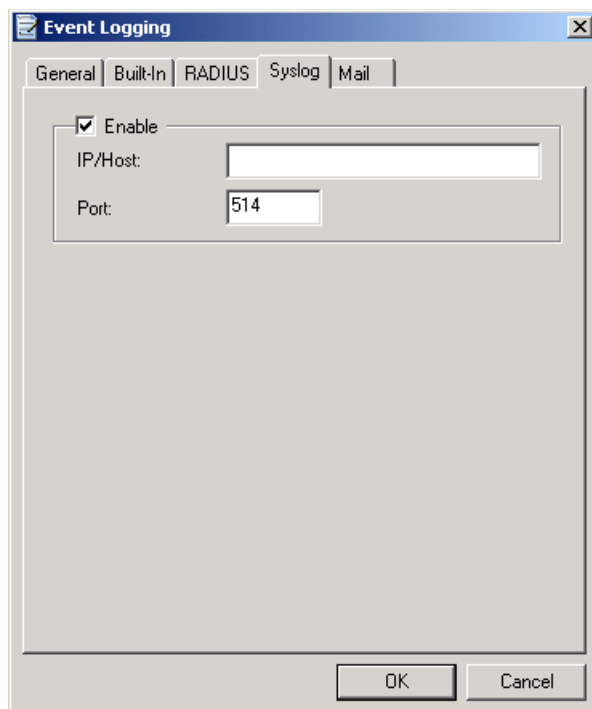
*IAG-related events are saved to the RADIUS Accounting server you defined here.*

## Configuring the Syslog Reporter

The Syslog reporter enables you to export system and security information from the IAG to an external industry-standard Syslog server, thus providing a greater level of network integration.

### *To configure the Syslog reporter:*

1. In the Configuration program, on the **Admin** menu, click **Event Logging...**  
*The Event Logging dialog box is displayed.*
2. Select the Syslog tab, and check the “Enable” option.



3. Define the Syslog settings, as follows:

**Table 26. Syslog Tab Parameters**

Parameter	Description
IP/Host	IP address or hostname of the Syslog server
Port	Port number of the Syslog server

4. Click **OK**.  
*IAG-related events are saved to the Syslog server you defined here.*

## Configuring the Mail Reporter

The mail reporter enables you to send email messages about selected event via an SMTP server. In order to configure the mail reporter, you have to take the following steps:

- Enable the reporter, and configure the following:
  - SMTP server information, including IP/Host, port, and, if required, user credentials
  - Mail details including the fields of the email messages issued by the mail reporter, and a list of recipients for the messages

The way in which you enable and configure the mail reporter is described in “Enabling the Mail Reporter to Send Messages” on page 246.

- By default, even when the mail reporter is activated, none of the messages that are handled by the Event Logging mechanism are sent to this reporter, since it should only be used to report specific—urgent or extremely important—IAG-related events. You therefore have to determine which of the messages should be sent by email, and manually configure them, as described in “Configuring which Messages are Sent by the Mail Reporter” on page 247.

## Enabling the Mail Reporter to Send Messages

This section describes how you enable the mail reporter to send event messages via the SMTP server.



### Note

Even when the mail reporter is enabled and configured, the SMTP server will not send event-related messages until you define which messages are sent to the mail reporter, as described in “Configuring which Messages are Sent by the Mail Reporter” on page 247.

### *To enable the mail reporter to send messages:*

1. In the Configuration program, on the **Admin** menu, click **Event Logging...**  
*The Event Logging dialog box is displayed.*
2. Select the Mail tab, and check the “Enable” option.

The screenshot shows the 'Event Logging' dialog box with the 'Mail' tab selected. The 'Enable' checkbox is checked. The 'IP/Host' field is empty. The 'Port' field contains '25'. The 'From' field is empty. The 'To' field is a multi-line text area, currently empty. The 'Subject' field contains 'Mail From IAG System'. The 'User' field is empty. The 'Password' field is empty. The 'Confirm Password' field is empty. At the bottom are 'OK' and 'Cancel' buttons.

3. Define the following settings:

**Table 27. Mail Tab Parameters**

Parameter	Description
IP/Host	IP address or hostname of the SMTP server
Port	Port number of the SMTP server
From	email address that appears in the email “From” field
To	email addresses to which you wish to send event logging email messages
Subject	Text that appears in the email “Subject” field
User	User name used to log into the SMTP server, if required
Password	Password used to log into the SMTP server, if required
Confirm Password	Confirmation of the password used to log into the SMTP server, if required

4. Click **OK**.
5. Go on to configure which of the IAG-related events will be sent to the recipients you configured here, as described in “Configuring which Messages are Sent by the Mail Reporter” on page 247.

### Configuring which Messages are Sent by the Mail Reporter

By default, the mail server does not send any messages to the email recipients, even if this option is enabled in the Event Logging dialog box, so that the recipients are not flooded with all of the event logging messages.

This procedure describes how you configure the messages that will be sent by mail to the recipients you configured in “Enabling the Mail Reporter to Send Messages” on page 246.



#### Note

Message configuration is implemented in an XML file. In order to edit it, you need to have a working knowledge of XML technology.

#### *To configure the messages that will be sent by mail:*

1. Create a custom message definitions file, as described in “Configuring Event Messages in the Message Definitions File” on page 249. If such a file already exists, use the existing file.

2. For each message that you wish to send to the SMTP server, under the <Reporters> element, add a new <Reporter> element with the value mail, as follows:


```
<Reporter>mail</Reporter>
```

For details regarding the reporting elements, refer to “<Reporters>” on page 256. For the full syntax of the message definitions file, refer to “Event Logging Message Definitions File” on page 250.

**For Example:**

To send an email message each time the number of concurrent authenticated sessions that can be opened through a trunk is exceeded, access the message “Number of Max Concurrent Sessions Exceeded”, and add the Mail reporter, as shown in the example that follows. Note that, for the clarity of the example, some of the event parameters were removed from the sample code.

```
<Message>
  <Id>15</Id>
  <Severity>Warning</Severity>
  <Type>Session</Type>
  <Name>AuthenticatedMaxExceeded</Name>
  <Desc>Number of Max Concurrent Sessions Exceeded</Desc>
  <DynamicDesc>VGhlIGlheGltYWwgbnVtYmVyIG9</DynamicDesc>
  <Params>
    <Param>
      <Name>MaxValue</Name>
    </Param>
  </Params>
  <Reporters>
    <Reporter>mail</Reporter>
    <Reporter>syslog</Reporter>
    <Reporter>builtin-log</Reporter>
  </Reporters>
</Message>
```

3. When you finish editing the file, still at the IAG, access the Configuration program. Click  to activate the configuration, select the option “Apply changes made to external configuration settings”, and click **Activate>**.

*Once the configuration is activated, the messages you configured here are reported to the SMTP server and sent to the recipients you configured in “Enabling the Mail Reporter to Send Messages” on page 246.*



## Message Configuration



### Note

Message configuration is implemented in an XML file. In order to edit it, you need to have a working knowledge of XML technology.

This section describes the following:

- How you edit the default message definitions file, in order to change the default event messages or to create additional, custom messages, in “Configuring Event Messages in the Message Definitions File” on page 249.
- The syntax of the definitions file, in “Event Logging Message Definitions File” on page 250.
- In order to send a custom event message, or in order to send event messages from custom interfaces, you need to configure the page from where you wish to send the message. For details, refer to “Event Messages Application Interface” on page 257.

### Configuring Event Messages in the Message Definitions File

This procedure describes how you configure the message definitions file, which holds the definitions of all event messages.


#### *To configure messages in the message definitions file:*

1. Access the following CustomUpdate folder; if it does not exist, create it:  
...\\Whale-Com\\e-Gap\\von\\conf\\CustomUpdate
2. Copy the file MessageDefinition.xml from this folder:  
...\\Whale-Com\\e-Gap\\von\\conf  
Place it in the CustomUpdate folder you accessed in step 1. If such a file already exists in the custom folder, use the existing file.
3. In the MessageDefinition.xml file, change the existing messages, or configure additional messages, as required. For a description of this file, refer to “Event Logging Message Definitions File” on page 250.



### Note

If you add new messages to the file, or if you wish to send messages from custom scripts, you also need to configure the functions that will send the messages, as described in “Event Messages Application Interface” on page 257.

4. When you finish editing the file, still at the IAG, access the Configuration program. Click  to activate the configuration, select the option “Apply changes made to external configuration settings”, and click **Activate >**.

*Once the configuration is activated, the messages you configured here are reported to the applicable reporter or reporters.*

## Event Logging Message Definitions File



### Note

This section describes the message definitions file. For instructions on the steps you need to take in order to edit the file, refer to “Configuring Event Messages in the Message Definitions File” on page 249. Do not make changes to the default file supplied with the IAG.

The message definitions file, `MessageDefinition.xml`, holds the definitions of all event messages under the root `<Messages>` element. Each message is defined in a dedicated `<Message>` sub-element. You can edit existing messages, or define new messages, according to the description and guidelines in “`<Message>`” on page 250.



### Caution

- Element names are case-sensitive.
- Be sure to follow the guidelines provided here. Message definitions that do not follow these guidelines may result in wrong or missing reports.
- In version 2 of the file, introduced in version 3.5, a new element was added under each `<Param>` element: `<Binary>`, described on page 255. If you are editing a version 2 file, and you copy into it custom elements which were originally created or edited in a version 1 file, be sure to add one `<Binary>` element under each `<Param>` element you copy into the new file.

## `<Message>`

### Description

Defines an Event Logging message.

### Usage

An unlimited number of `<Message>` elements can be nested under the root `<Messages>` element.

### Child Elements

<Message> must contain one each of the following elements:

- <Id>, described on page 251.
- <Severity>, described on page 252.
- <Type>, described on page 252.
- <Name>, described on page 253.
- <Desc>, described on page 253.
- <DynamicDesc>, described on page 253.

In addition, <Message> can contain one each of the following optional elements:

- <Params>, described on page 254.
- <Reporters>, described on page 256.



#### Note

If no reporters are defined for a message, the message is not sent to any of the Event Logging reporters. It is only sent to the Web Monitor, where it can be viewed in the Event Viewer, but cannot be queried in the Event Query window.

<Message> ➤ <Id>

### <Id>

#### Description

Unique message ID.

- For the default messages, do not change the message ID.
- For custom messages, use ID 10000 and up.

#### Usage

One and only one <Id> element must be nested under <Message>.

#### Child Elements

None.

**<Message>** ➤ **<Severity>**

## **<Severity>**

### **Description**

Message severity. Must be one of the following:

- Information: informative message denoting a normal event that might be of interest, such as user login or log out.
- Notice: normal but significant condition, such as users changing their password.
- Warning: events that might be problematic, but don't result in malfunction. For example: an unauthorized access attempt.
- Error: a significant problem, such as a failure to read the configuration.

### **Usage**

One and only one <Severity> element must be nested under <Message>.

### **Child Elements**

None.

**<Message>** ➤ **<Type>**

## **<Type>**

### **Description**

Message type. Must be one of the following:

- System: system events, such as service startup and shutdown and changes to the configuration.
- Security: security events, including login success or failure, security policy violation or change, and password change.
- Session: session events, including session start or stop, number of sessions, and other session-related events.



### **Tip**

In the IAG Event Manager, in the Event Viewer and the Event Report, this parameter is displayed in the “Category” column.

### **Usage**

One and only one <Type> element must be nested under <Message>.

### **Child Elements**

None.

**<Message>** ➤ **<Name>**

### **<Name>**

#### **Description**

Message name. Must contain only alphanumeric characters.

#### **Usage**

One and only one <Name> element must be nested under <Message>.

#### **Child Elements**

None.

**<Message>** ➤ **<Desc>**

### **<Desc>**

#### **Description**

Short description of the message. Must contain only alphanumeric characters and spaces.



#### **Tip**

In the IAG Event Manager, in the Event Viewer and the Event Report, the short description is displayed in the “Type” column.

#### **Usage**

One and only one <Desc> element must be nested under <Message>.

#### **Child Elements**

None.

**<Message>** ➤ **<DynamicDesc>**

### **<DynamicDesc>**

#### **Description**

Long description of the message. This description must be encoded using Base64 encoding, and must not contain the CR/LF (carriage return/line feed) character.



#### **Tip**

To view encoded text, or to encode text that you enter in this element, open the file in the Editor program. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Editor” on page 40.

You can include one or more parameters in the long description, as follows:

- Define a parameter using a <Param> element. For details, refer to “<Params>” on page 254.
- Include a parameter in the message using the following format:

[%<parameter\_name>%]

Where <parameter\_name> is the named assigned to the parameter in the <Name> sub-element of <Param>.

**For example:** to add a User Name parameter to the description of a successful login message, define a parameter named `UserName`, and include it in the message as follows:

User [%UserName%] logged in successfully.

### Usage

One and only one <DynamicDesc> element must be nested under <Message>.

### Child Elements

None.



## <Params>

### Description

Defines optional parameters that can be used as follows:

- As part of the long description of the message, in the <DynamicDesc> element. For details, see “<DynamicDesc>” on page 253.
- In the Web Monitor, in the Event Query window, to query events by trunk name and session ID. For information on querying events in the Web Monitor, refer to “Event Query” on page 295.



### Note

You cannot use custom parameters as query parameters in the Event Query.

### Usage

One and only one <Params> element can optionally be nested under <Message>.

### Child Elements

<Params> can contain an unlimited number of <Param> elements, described on page 255.

<Message> > <Params> > <Param>

### <Param>

#### Description

Child element of <Params>. Defines a single parameter. For a description of parameter usage, refer to “<Params>” on page 254.

#### Usage

An unlimited number of <Param> elements can be nested under <Params>.

### Child Elements

<Param> must contain one each of the following elements:

- <Name>, described on page 255.
- <Binary>, described on page 255.

<Message> > <Params> > <Param> > <Name>

### <Name>

#### Description

Child element of <Param>. Defines the parameter name.

#### Usage

One and only one <Name> element must be nested under <Param>.

### Child Elements

None.

<Message> > <Params> > <Param> > <Binary>

### <Binary>

#### Description

Child element of <Param>. Determines whether the parameter value is binary or not, where:

- 1: value is binary
- 0: value is non-binary

### Usage

One and only one <Binary> element must be nested under <Param>.

### Child Elements

None.

<Message> ➤ <Reporters>

## <Reporters>

### Description

Defines the reporter or reporters to which the message is sent. You can define any of the following reports:

- `builtin-log`: IAG's built-in reporter, described in “Configuring the Built-In Reporter” on page 242.
- `radius-accounting`: reporting to a RADIUS Accounting server, as described in “Configuring the RADIUS Reporter” on page 243.



### Note

Only the messages that are configured by default to report to the RADIUS reporter can be sent to the RADIUS Accounting server. No other messages can be sent to the RADIUS server, regardless of the configuration of this reporter.

- `syslog`: reporting to a Syslog server, as described in “Configuring the Syslog Reporter” on page 244.
- `mail`: sending an email message about the event, as described in “Configuring the Mail Reporter” on page 245.

### Usage

One and only one <Reporters> element can be nested under <Message>.

### Child Elements

<Reporters> can contain up to four <Reporter> elements, described on page 255, one for each reporter.

<Message> ➤ <Reporters> ➤ <Reporter>

## <Reporter>

### Description

Child element of <Reporters>. Defines a single reporter to which the message is sent. For a description of the reporters you can configure here, refer to “<Reporters>” on page 256.



## Usage

Up to four <Reporter> elements can be nested under <Reporters>, one for each reporter.

## Child Elements

None.

## Event Messages Application Interface

By default, all the applicable IAG interfaces are configured to send the relevant event message when required. If, however, you configure custom messages in the message definitions file, or if you wish to send messages from custom interfaces, such as a custom Login script, in order to send the message, you need to configure the page where you wish to send the message, as described in this section.

### *To configure message interface:*

1. In the page from where you wish to send the message, add the following function:

```
SetMessage <Message_ID>,<Optional_param_list>
```

Where:

- <Message\_ID> is the unique message ID defined in the message definitions file, in the <Id> element, described on page 251.
  - <Optional\_param\_list> holds the definition of message parameters, as follows:
    - If no parameters are defined in the message: null
    - If the message contains one or more parameters:  
Array(<message\_param>,<message\_param>...)  
Where <message\_param> is the parameter you define in the message definitions file, in the <Param> element, described on page 255.
2. If the message contains one or more parameters, for each parameter you need to create an object in the file, where the name of the parameter is identical to the name you use in the function you define in step 1.



### Tip

You can see a sample function call in the following page:

```
...\Whale-Com\e-Gap\von\InternalSite\samples\set_message.asp
```

3. If you are adding the function to your own page, such as your own login page, you need to include the following file in the page:

```
...\Whale-Com\e-Gap\von\InternalSite\inc\MonitorMgr.inc
```

## Disabling Event Logging and Reporting

This section describes how to disable and re-enable event logging and reporting.



### Note

Disable event logging and reporting for advanced troubleshooting purposes only, and be sure to re-enable it as soon as you finish troubleshooting the system.

### ***To disable event logging and reporting:***

- At the IAG, run the following command:

```
...\Whale-Com\e-Gap\utils\MonitorMgr\MonitorMgrUtil.exe -sms 0
```

*Events are no longer logged to the Event Logging mechanism, and event messages are not sent to any of the configured reporters.*

### ***To re-enable event logging and reporting:***

- At the IAG, run the following command:

```
...\Whale-Com\e-Gap\utils\MonitorMgr\MonitorMgrUtil.exe -sms 1
```

*Events are logged to the Event Logging mechanism, and event messages are sent to the configured reporters.*

## Web Monitor

The Web Monitor is a monitoring and reporting web application that enables you to view IAG-related events both from within the organization and from remote locations, using a web browser. Access from remote locations is fully secured by the IAG Application Aware security mechanisms, such as URL Inspection positive-logic rulesets, out-of-the-box character definitions, policy compliance, and session timeouts. In sites where an IAG High Availability Array is deployed, you can monitor each of the IAG servers within the array from a single Web Monitor.

A constantly updating snapshot of system, administrative, and remote user activities can be used to assist users online and troubleshoot any problems they may encounter while accessing the internal network via the IAG. You can zoom into a user's session in real-time, and pinpoint errors and situations that hinder usability. Remote access via the SSL VPN portal provides you with secure anytime, anywhere monitoring of system and user activities, and enables you to render users assistance while away from the office. Logs and queries are used to analyze usability variations and trends over time.

**For example:** a user notifies you that they cannot log into an application. When you zoom into the user's session you find that the application's Access policy requires that the Attachment Wiper is installed on the endpoint computer, but the user's computer does not comply with this policy. You can instruct the user to download and install the Whale Client Components when they next access the site. Thereafter, they are able to access the application smoothly.



#### Note

The Web Monitor application is protected by the Windows Local Users and Groups management tool. By default, access to the application is disabled, and you need to configure the user or users that are allowed to access it, as described in “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.


This section:

- Describes how you access the Web Monitor, including the configuration steps required in order to enable access from computers other than the IAG, and the list of supported browsers, in “Accessing the Web Monitor” on page 260.
- Describes the general Layout of the Web Monitor screen, in “Web Monitor Layout” on page 264.
- Provides you with helpful tips for using the Web Monitor, in “Tips for Using the Web Monitor” on page 265.
- Provides detailed explanations of the Web Monitor windows and views, and operations you can perform in the Web Monitor, as follows:
  - “Session Monitor - Current Status” on page 266
  - “Session Monitor - Active Sessions” on page 268
  - “Session Monitor - Statistics” on page 271
  - “Application Monitor - Current Status” on page 275
  - “Application Monitor - Active Sessions” on page 278
  - “Application Monitor - Statistics” on page 279
  - “User Monitor - Current Status” on page 285
  - “User Monitor - Active Sessions” on page 287
  - “User Monitor - Statistics” on page 288
  - “Event Viewer” on page 293
  - “Event Query” on page 295
- Support for sites running an IAG High Availability Array, in “Web Monitor High Availability Support” on page 298.

## Accessing the Web Monitor

You can access the Web Monitor from the web browsers listed in “Web Monitor Browser Support” on page 264, as follows:

- From the IAG:

In the Configuration program, click  on the toolbar, or, on the **Admin** menu, click **Web Monitor...**

Or,

In the Windows desktop, click **Start**, then point to **Programs > Whale Communications IAG > Additional Tools > Web Monitor**.

- From any computer that is on the same network as the IAG. The Web Monitor application can be accessed via port 50002 on the IAG.  
**For example:** if the IP address of the IAG is 192.168.1.45, enter the following URL at the browser’s Address bar: `http://192.168.1.45:50002`
- Remotely, via the IAG SSL VPN portal. To enable remote access via the portal, at the Configuration program, use the Add Application Wizard to add the Web Monitor application to the trunk (the application is part of the Built-In Services group). Once you add the application to the trunk, access the Authorization tab of the Application Properties dialog box and define the users that are authorized to access the application. **By default, no users are authorized to access the application.** For details, refer to “Defining Authorization for Portal Applications” on page 38.

In order to enable access to the Web Monitor from computers other than the IAG, you need to configure the user or users that are allowed to access it, as described in “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.

## Enabling Web Monitor Access from Computers Other Than the IAG



### Note

This section describes how you enable access to the Web Monitor application from computers other than the IAG; this configuration procedure is required for users who access this application both locally, from within the organization, and remotely, via the portal homepage. In addition, in order to enable remote access to the Web Monitor application via the portal homepage, you must also configure authorization for this application, as described in “Defining Authorization for Portal Applications” on page 38.

The Web Monitor application is protected by the Windows Local Users and Groups management tool. During the installation of the IAG, a dedicated group is created in the Windows Local Users and Groups Manager, on the IAG. This group is used for authentication against the Web Monitor application.

The group’s default settings are:

- Group name: Web Monitor Users
- One user is defined as a member of this group: IAG Administrator

By default, this user is disabled. In order to enable access by this user to the Web Monitor, you need to enable the user’s account and assign a password, as described in the procedure that follows. You can also use the Local Users and Groups Manager to add other users, from other groups and other domains, as members of the Web Monitor Users group, who are allowed to access the application.



### Note

In an IAG High Availability Array, you must assign the same users to the Web Monitor Users group on all the IAG servers that are part of the Array. For details, refer to “Web Monitor High Availability Support” on page 298.

### ***To grant the IAG Administrator user access to the Web Monitor:***

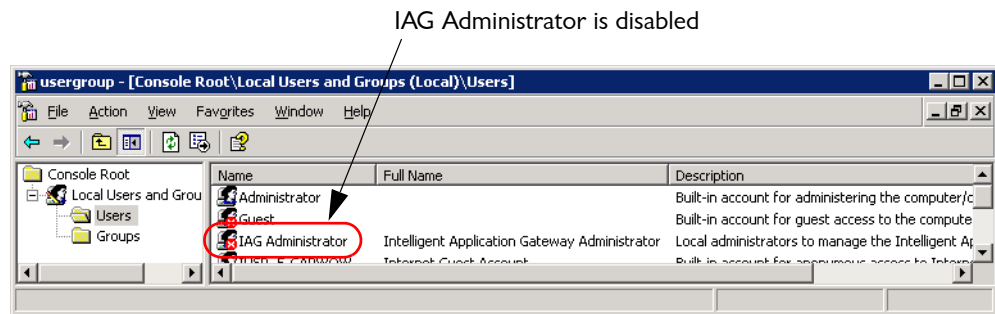
1. In the Configuration program, access the Local Users and Groups Manager.



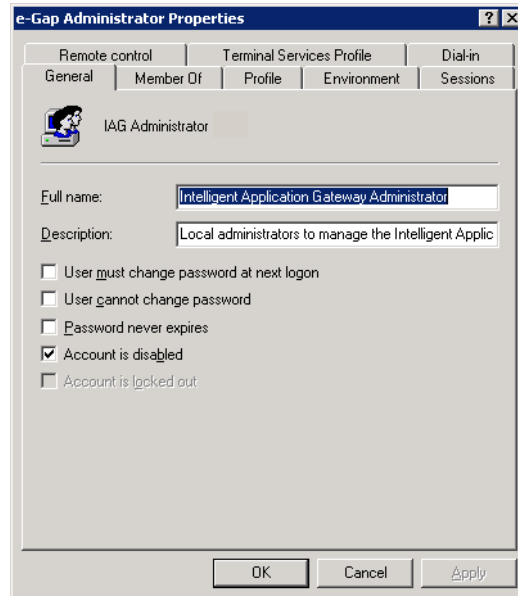
### Tip

You can quickly access the Local Users and Groups Manager via the Configuration program: select **Admin > Event Logging**, and in the Event Logging dialog box, in the General tab, click the link “Configure Monitor Users”.

2. In the Local Users and Groups Manager, from the tree in the left pane, under **Local Users and Groups**, select **Users**. Note that, in the right pane, the IAG Administrator user is disabled, as indicated by a red **X** next to the user’s name:

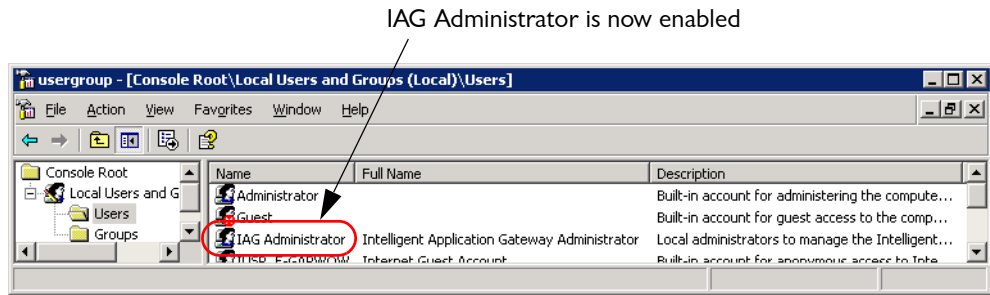


3. In the right pane of the Local Users and Groups Manager, right-click the IAG Administrator user and select **Properties**.  
*The IAG Administrator Properties dialog box is displayed.*



4. **Uncheck** the option “Account is disabled”, then click **OK** to close the dialog box.

*In the right pane of the Local Users and Groups Manager, the IAG Administrator user is now enabled:*



5. Assign a password for the IAG Administrator user: in the right pane of the Local Users and Groups Manager, right-click the IAG Administrator user and select **Set Password**.

*The Set Password dialog box is displayed.*

6. Use the Set Password dialog box to assign a password.

*The IAG Administrator user can now access the Web Monitor, using the password you assigned here.*



**Tip**

In order to enable access to the Web Monitor by additional users, access the Web Monitor Users group, under **Users**, and define as many users as required.

## Web Monitor Browser Support

You can access the Web Monitor using the following browsers:

Operating System	Supported Browsers
Windows 2000	<ul style="list-style-type: none"><li>• Internet Explorer 6.0</li><li>• Mozilla family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox 1.0.x and higher</li></ul>
Windows XP/2003	<ul style="list-style-type: none"><li>• Internet Explorer 6.0, 7.0</li><li>• Mozilla family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox 1.0.x and higher</li></ul>
Mac OS X *	Mozilla family: Netscape Navigator 7.1.x, 7.2.x; Mozilla 1.7.x; Firefox 1.0.x and higher; Camino 0.83 and higher

- \* On computers running Mac OS X, you cannot access the Web Monitor directly from the portal homepage. Access is possible from any computer that is on the same network as the IAG, via port 50002 on the IAG, as described in “Accessing the Web Monitor” on page 260.

## Web Monitor Layout

The Web Monitor is displayed in a web browser. The browser window is divided into two panes:

- In the menu, on the left, a list of links enables you to select the Web Monitor window that you wish to view. The links are grouped as follows:
  - Session Monitor, including Current Status, Active Sessions, and Statistics.
  - Application Monitor, including Current Status, Active Sessions, and Statistics.
  - User Monitor, including Current Status, Active Sessions, and Statistics.
  - Event Viewer.
  - Event Query.
  - High Availability Array, in sites that deploy an IAG High Availability Array.

The windows are described in detail in the sections that follow.



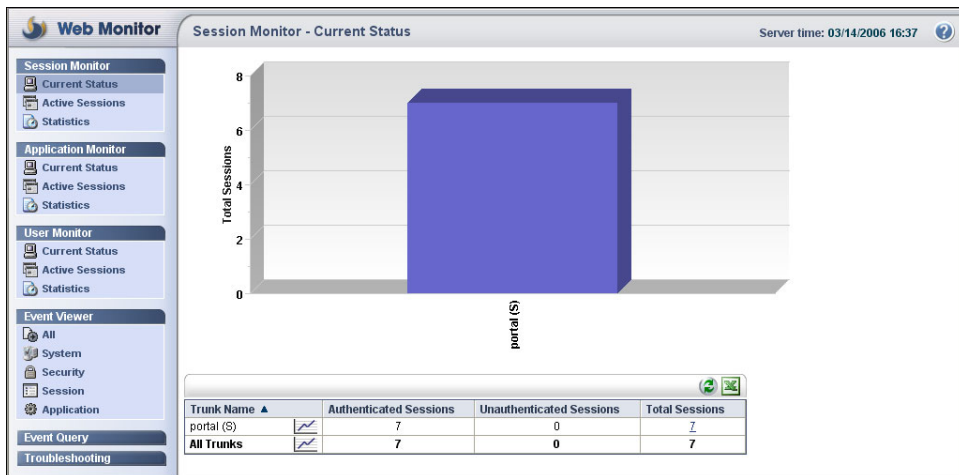


### Tip



- The selected view is highlighted.
- Click **Troubleshooting** for troubleshooting guidelines and instructions for Warning and Error messages.

- In the right pane, the Web Monitor window that you selected in the left pane is displayed.

**Figure 40. Sample Web Monitor Window**



## Tips for Using the Web Monitor


- Where times are displayed, such as in the Statistics windows, it is the time on the IAG, not the remote user's computer. The current time on the IAG is displayed at the top right corner of the screen. **For example:** Server time: 02/23/2006 17:40
- To generate reports in Microsoft Excel® format, click . You can then use Excel to manipulate the data according to your needs. **For example:** calculate the number of users that were concurrently logged onto a trunk at peak time, or create charts that will present comparisons, patterns, and trends of system usage.
- In the Current Status, Active Sessions, and Event Viewer windows, you can instantly refresh the data by clicking .
- A “lead user” is the user who accessed the site. **For example:** when a user logs in to the site using one set of credentials, and is then required to enter different credentials when accessing a specific

application, the lead user is the user who logged in to the site. In unauthenticated trunks, the lead user is the first user added during the session with the site.

- A user name is always displayed using the following syntax:  
`<domain_name>\<user_name>`
- In tables, you can specify a sort order by clicking the column heading by which you want to sort the data.
- In line charts, used in the Statistics and monitor over time windows, you can highlight a line in the chart by clicking it in the legend. **For example:** clicking a trunk name highlights the chart-line representing that trunk.
- Some of the Web Monitor defaults, such as refresh rates, the display of graphics, and the appearance of charts, are customizable. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Customizing the Web Monitor Windows” on page 72.

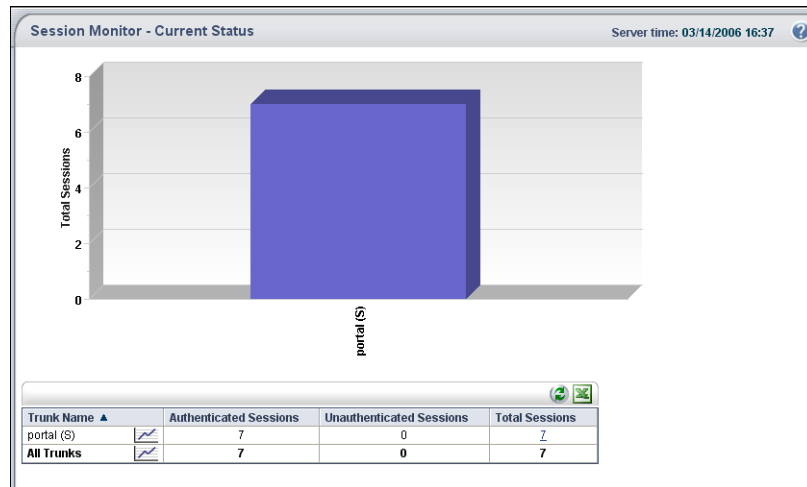
## Session Monitor - Current Status

This window provides online display of all the sessions that are currently open via all the trunks of the IAG you are monitoring:


- At the top part of the window, a column chart displays each trunk in a separate column, and shows the total number of sessions that are currently open through the trunk, that is, both authenticated and unauthenticated sessions.
- At the bottom part of the window, active trunks and open sessions are listed in a tabular format, including the number of authenticated and unauthenticated sessions. Clicking the number of total sessions opens the trunk’s Session Monitor - Active Sessions window, described in “Session Monitor - Active Sessions” on page 268.
- By default, the window refreshes the data every 15 seconds. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.
- You can also monitor session behavior over time, for a selected trunk or for all active trunks. In the table at the bottom of the window, click  next to the trunk you wish to monitor, or next to “All Trunks”, respectively. The Session Monitor Over Time window is displayed, as described on “Session Monitor Over Time” on page 267.

You can use the different displays to compare activity between trunks, and analyze trends and variations over time.


**Figure 4I. Sample Session Monitor - Current Status Window**



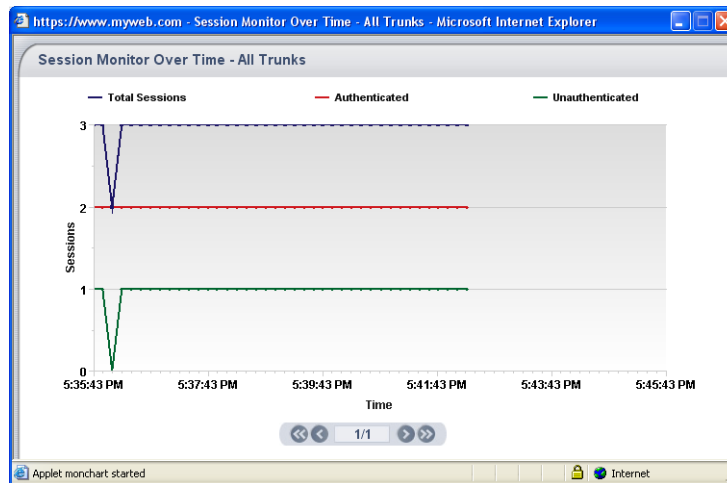
## Session Monitor Over Time

The Session Monitor Over Time window is displayed when you click  in the Session Monitor - Current Status window. Use it to monitor session behavior over time, for a selected trunk or for all active trunks.

Session behavior is displayed in a line chart, showing both authenticated and unauthenticated sessions, and the total number of sessions, at pre-defined intervals.

- By default, the window refreshes the data at 10-second intervals. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.
- Use the paging controls to scroll to the period of time you wish to monitor:  .

**Figure 42. Session Monitor Over Time**



## Session Monitor - Active Sessions

The Session Monitor - Active Sessions window provides a detailed snapshot of the currently-open sessions for each trunk. Use it for online user-access tracking and troubleshooting.

- You select which trunk to display at the top left corner of the window.
- The parameters that are provided for each session are listed in Table 28, “Parameters of the Session Monitor - Active Sessions”, on page 269.
- By default, the window refreshes the data every five minutes. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

**Figure 43. Sample Session Monitor - Active Sessions Window**



Current session is highlighted

Session Monitor - Active Sessions									
Server time: 03/14/2006 16:57									
Trunk: portal (S)									
#	Session ID	Lead User	Repository	Started At	Duration	Authenticated	Events	Terminate	
1	090983E1-98C0-4276-846B-922F0F3BB06D	whalecomruti	whalecom	03/14/2006 16:33:40	00:23:14	✓			
2	DC497D7F-A3AR-4R9A-AR50-9FA85B72A1CF	whalecomeddien	whalecom	03/14/2006 16:30:50	00:26:04	✓			
3	85C551A5-3200-43F2-ACDC-1B8BB6R0992S	whalecomiezy	whalecom	03/14/2006 16:30:06	00:26:48	✓			
4	7354EA22-39F3-4714-912C-20825443F56D	whalecomiezy	whalecom	03/14/2006 16:29:57	00:26:57	✓			
5	9F918386-R7F8-450A-B252-61E1D2RR7A5R	whalecomyarivm	whalecom	03/14/2006 16:29:41	00:27:13	✓			
6	BA3BB6D6-22BC-4E5C-95FD-01152E213946	whalecomamirm	whalecom	03/14/2006 16:29:35	00:27:19	✓			
7	78335EE9-3EBB-4DCB-B830-96600736452A	whalecomrachel	whalecom	03/14/2006 16:17:44	00:39:10	✓			

**Table 28. Parameters of the Session Monitor - Active Sessions**

Parameter	Description
Session ID	Unique session ID. Clicking the session ID opens the Session Details window, described in “Session Details” on page 270.
Lead User	User who initiated the session.
Repository	Authentication repository of the user who initiated the session.
Started At	Date and time when the session was started.
Duration	Duration of the session.
Authenticated	<p>Indicates whether the session is authenticated or unauthenticated.</p> <p>A session is unauthenticated when:</p> <ul style="list-style-type: none"><li>• The user’s identity is unknown, such as prior to the completion of the login process.</li><li>• The session is suspended before it is closed.</li></ul> <p>The following example describes a sample life cycle of a session, in a trunk where the Automatic Scheduled Logoff option is activated, and the Logoff Scheme is triggered every 60 minutes:</p> <ul style="list-style-type: none"><li>• As soon as a user accesses the site, an unauthenticated session is established.</li><li>• Once the user is authenticated, the session’s status changes to “authenticated”.</li><li>• 60 minutes later, the Scheduled Logoff is triggered, the session’s status changes to “unauthenticated”, and the user is prompted to re-authenticate.</li><li>• The user re-authenticates within the required timeframe, and the session is authenticated again.</li><li>• When the user finishes working with the site and logs off, the status of the session changes to “unauthenticated”. After a pre-defined period of time, the session closes. It is no longer displayed in the Session Monitor - Active Sessions window.</li></ul>

**Table 28. Parameters of the Session Monitor - Active Sessions (Cont'd)**

Parameter	Description
Events	Clicking  generates a report of events related to the session. The report is displayed in the Event Reports window, described in “Event Report” on page 297.
Terminate	<p>Clicking  terminates the session. A message prompts you to verify the termination; once you do, the status of the session changes to “unauthenticated”:</p> <div data-bbox="696 621 841 705" data-label="Image"> </div> <p><b>Note:</b> You cannot terminate the current session, or unauthenticated sessions.</p>

## Session Details

The Session Details window is displayed when you click a session’s ID in any of the Web Monitor’s Active Sessions windows. It provides in-depth session information, divided into the following tabs:

- The **General** tab provides general information about the session and about the users that are currently logged in to the session. Note the following:
  - For information about privileged sessions, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Default and Privileged Session Settings” on page 137.
  - The lead user is the user who initiated the session.
- The **Applications** tab lists all the applications for which the session users are authorized, and, for each application, whether users are allowed to access it or only view it, and whether it is launched or not.
- The **Endpoint Information** tab provides information about the endpoint computer from where the session was initiated, including:
  - Whale Client Components that are installed on the computer. For information about the Whale Client Components, refer to “Whale Client Components” on page 147.
  - Other software that is installed on the computer, which is related to the interaction of the computer with the IAG, such as anti-virus software or browser version.

- IP address and domain of the endpoint computer, and whether it is an IAG Certified Endpoint. For information about Certified Endpoints, refer to “Certified Endpoints” on page 118.

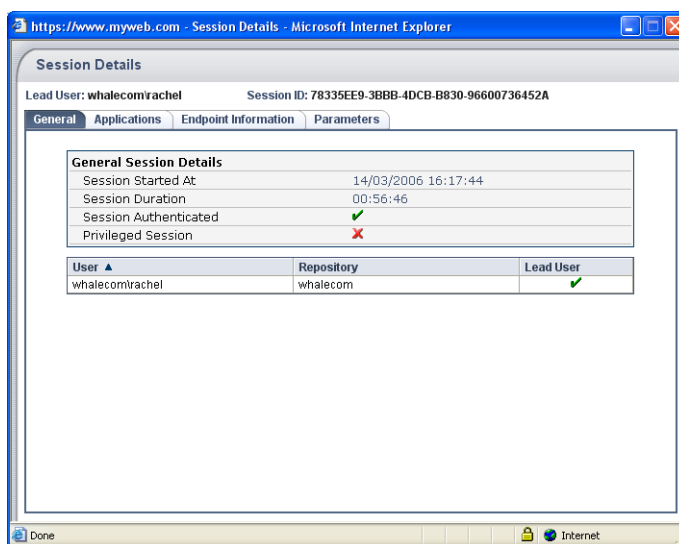


### Tip

The information provided in the Endpoint Information tab is similar to the information that is provided to the end-user, on the endpoint computer, in the System Information window.

- The **Parameters** tab lists all the session parameters, including the type and value of each parameter. You can view a list of all the session’s parameters, or only parameters of a selected type.

**Figure 44. Sample Session Details Window**



## Session Monitor - Statistics

This window enables you to view and analyze both the history and the current status of the IAG sessions, such as the number of concurrent sessions in a trunk, and compare them to the trunk’s limitations, as defined by the Concurrent Sessions settings.



- Use the query form to submit a query, as described in “Session Monitor - Statistics Window: Query Form” on page 272.
- The window then displays the query results, as described in “Session Monitor - Statistics Window: Query Results” on page 273.

## Session Monitor - Statistics Window: Query Form

When you first access the Session Monitor - Statistics window, the query form is displayed. Use this form to define the query:

- Select the trunk or trunks for which to generate the query.
- Define the period of time for which to generate the query:
  - Select a pre-defined period, such as “Today” or “Last Month”, at the top of the “Period” area.
  - Or,
  - Define start and end dates at the bottom of the “Period” area.
- Define the interval at which data is sampled, at the bottom right of the “Period” area. The intervals that are available for selection depend on the selected period. **For example:** if the selected period is a day, only an “Hour” interval can be defined; for a period of a week, you can select an interval of either an hour or a day.

By default, the maximal number of intervals that can be queried is 1,500. If required, you can change this value, as well as the number of intervals that are displayed on a single page in the default view, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72. Note, however, that a value of over 1,500 intervals is not recommended and may slow down the monitor’s performance considerably.

- Select the query type:
  -  **Sample Chart:** the number of concurrent sessions is sampled at the end of each interval.
  -  **Peak Chart:** the number of concurrent sessions reported is the highest number of sessions that were open during the interval period.

Once you submit the query, the results are displayed in the window, as described in “Session Monitor - Statistics Window: Query Results” on page 273.



**Figure 45. Session Monitor - Statistics Window: Query Form**



### Tip

After you submit a query, when you return to the query form from the “query results” view, you can click **Show last results** to display the results of the last query submitted, regardless of any changes you might have made in the query form.

## Session Monitor - Statistics Window: Query Results

Query results are displayed in the Session Monitor - Statistics window after you submit a query in the query form, as described in “Session Monitor - Statistics Window: Query Form” on page 272.

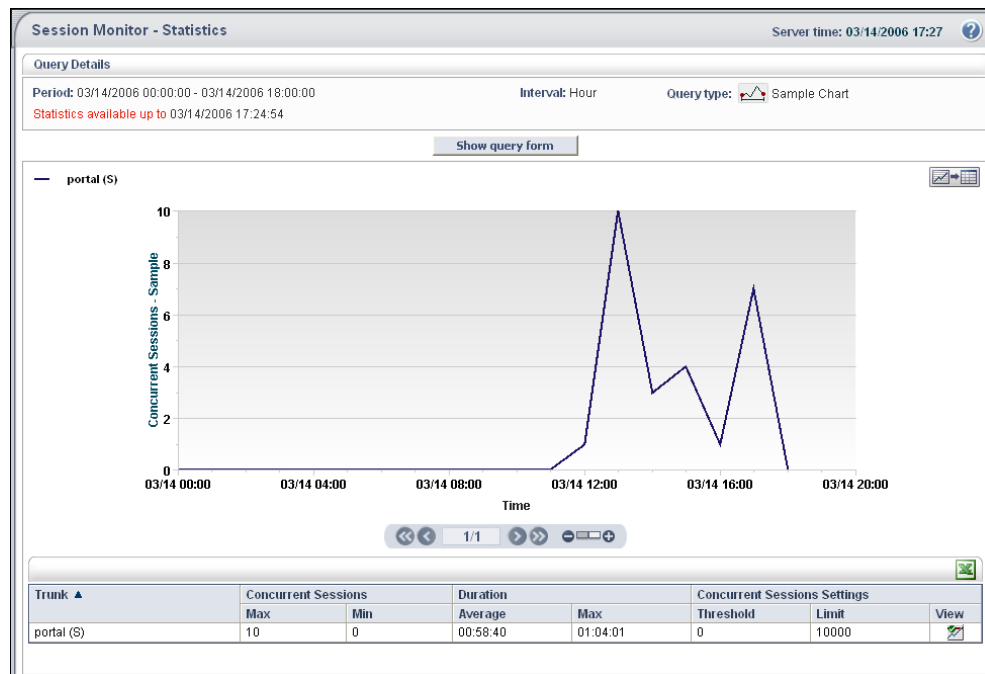
- At the top of the window, query details are displayed, including period, interval, and query type, as you defined in the query form. If query results are available only for a part of the defined period, this is also indicated, under the “Period” field.
- Query results are displayed in two views:
  - A line chart displays the number of concurrent sessions for each of the trunks in the query. The color that represents each trunk on the chart is indicated in the legend, to the left of the trunk name.
  - The table, at the bottom of the window, displays information on each of the trunks that were queried, as described in Table 29, “Session Monitor - Statistics Window: Query Results”, on page 274.
- You can view the data that is displayed in the chart in a tabular format by clicking .
- Use the paging and zooming controls to focus the view on the period of time you wish to monitor: .



## Tip

- When you zoom out to the smallest view, the window displays the entire period that is queried, up to the pre-defined interval limit.
- When you zoom in to the largest view, the window displays 10 intervals; to view additional intervals, use the paging controls.
- To return to the query form, click [Show query form](#).



**Figure 46. Session Monitor - Statistics Window: Query Results**



**Table 29. Session Monitor - Statistics Window: Query Results**



Parameter	Description
Trunk	Trunk name.
Concurrent Sessions	Minimal and maximal number of sessions that were concurrently open through the trunk during the query period.


**Table 29. Session Monitor - Statistics Window: Query Results (Cont'd)**

Parameter	Description
Duration	<p>The average and maximal duration of the sessions that were open through the trunk during the query period.</p> <p><b>Note:</b> If the number of results exceeds the number of “Max Report Results”, as defined in the Configuration program, in the General tab of the Event Logging dialog box (described in “Configuring General Settings” on page 240), “Duration” is not reported.</p>
Concurrent Sessions Settings	<p>Settings that are defined for the trunk in the Configuration program, in the Session tab of the Advanced Trunk Configuration window:</p> <ul style="list-style-type: none"> <li>• Threshold: the threshold above which each new session that opens generates a report, as defined in the “Concurrent Sessions Threshold” field of the Session tab.</li> <li>• Limit: maximal number of sessions that can be open through the trunk at the same time, as defined in the “Max Concurrent Sessions” field of the Session tab.</li> </ul> <p>For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to “Session Configuration” on page 133.</p>
View	<p>Clicking  adds the display of concurrent sessions threshold and limit to the chart; clicking  removes the display from the chart.</p>


## Application Monitor - Current Status

This window provides a view of all the applications that are enabled for access via the IAG, in all trunks.

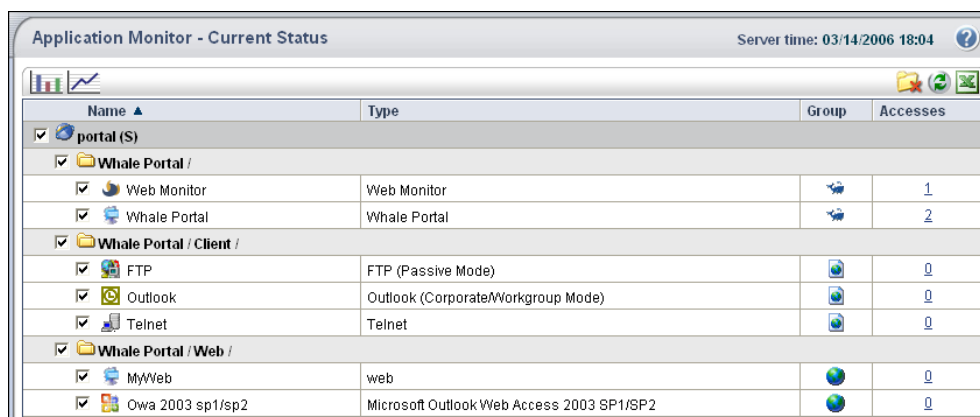
- The parameters that are provided for each application are described in Table 30, “Parameters of Application Monitor - Current Status Window”, on page 277.
- You can select whether to display applications in a folder view or not by clicking  or  at the top of the window, respectively. If no folders are defined, the button is disabled.

- By default, the window refreshes the data every 15 seconds. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.
- You can also use the Application Monitor to:
  - View the status of an application or any number of selected applications. Select the application or applications you wish to view, and click  on the toolbar at the top of the window. A column chart is displayed, showing the current status of the selected applications. By default, you can view the status of up to 15 applications. If required, you can change this value, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

The refresh rate of the window is synchronized with that of the Application Monitor window.

  - Monitor an application or any number of selected applications over time. Select the application or applications you wish to monitor, and click  on the toolbar at the top of the window. The Application Monitor Over Time window is displayed, as described in “Application Monitor Over Time” on page 277.


**Figure 47. Sample Application Monitor - Current Status Window**



**Table 30. Parameters of Application Monitor - Current Status Window**

Parameter	Description
Name	Application name, as defined in the Configuration program, in the General tab of the Application Properties dialog box, and the icon representing the application. <b>Note:</b> Applications are listed under the trunk where they are configured.
Type	Internal application type.
Group	The group to which the application belongs.
ID	This field is optional, and is not displayed by default. You can enable the display of this field in the file that controls the Web Monitor preferences, in the parameter “showAppID”. For details, refer to the <i>Intelligent Application Gateway Advanced Configuration</i> guide, to “Customizing the Web Monitor Windows” on page 72. Application ID, as displayed in the Configuration program, in the General tab of the Application Properties dialog box.
Accesses	Number of users currently accessing the application. Clicking the number of accesses displays the trunk’s Application Session Monitor - Active Sessions window, described in “Application Monitor - Active Sessions” on page 278.

## Application Monitor Over Time

The Application Monitor Over Time window is displayed when you click  in the Application Monitor - Current Status window. Use it to monitor application behavior over time, for any selected number of applications.

Application behavior is displayed in a line chart, showing the number of accesses for each selected application.

- By default, the window refreshes the data at 10-second intervals. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.


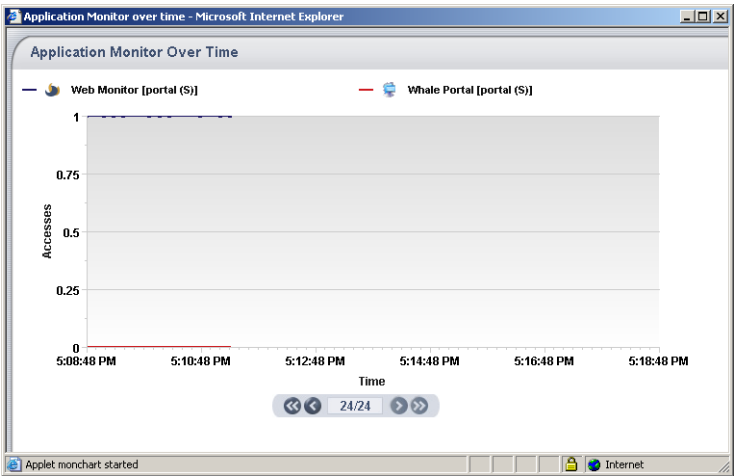
- Use the paging controls to scroll to the period of time you wish to monitor:  .

Figure 48. Application Monitor Over Time



### Application Monitor - Active Sessions

This window provides a detailed snapshot of the currently-open sessions for each application. Use it for online user-access tracking and troubleshooting.

- You select which trunk and application to display at the top part of the window.
- The parameters that are provided for each session are listed in Table 31, “Parameters of Application Monitor - Active Sessions Window”, on page 279.
- By default, the window refreshes the data every five minutes. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

Figure 49. Sample Application Monitor - Active Sessions Window


Application Monitor - Active Sessions

Server time: 03/21/2006 16:00

Trunk: portal (S) Application: Whale Portal

#	Session ID	Lead User	Repository	Application Started At	Application Duration	Events
1.	050D185C-70F5-4CD2-9B28-0BA8A9AF9CF5	whalecomlqa_admin	whalecom	03/21/2006 15:47:46	00:11:22	
2.	07D5860D-B846-40F8-992A-8CD45A813FC7	whalecomlrachel	whalecom	03/21/2006 15:41:42	00:17:26	
3.	237901D4-6404-4432-9C27-689B5F83A339	whalecomlqa_admin	whalecom	03/21/2006 15:37:15	00:21:53	
4.	3B6E1B23-628E-4C85-BC93-6583A609E7F9	whalecomlyarvm	whalecom	03/21/2006 15:36:57	00:22:11	
5.	4B53C8R8-69ED-4DB2-9218-KCC7037D2A58	whalecomlruti	whalecom	03/21/2006 15:32:38	00:26:30	

**Table 3I. Parameters of Application Monitor - Active Sessions Window**

Parameter	Description
Session ID	Unique session ID. Clicking the session ID opens the Session Details window, described in “Session Details” on page 270.
Lead User	User who initiated the session.
Repository	Authentication repository of the user who initiated the session.
Application Started At	Date and time when the application was launched.
Application Duration	Length of time during which the application was active.
Events	Clicking  generates a report of the session’s application-related events. The report is displayed in the Event Reports window, described in “Event Report” on page 297.

## Application Monitor - Statistics

This window enables you to view and analyze both the history and the current status of a selected application or any number of applications, such as the number of concurrent accesses to the application.

- Use the query form to submit a query, as described in “Application Monitor - Statistics Window: Query Form” on page 279.
- The window then displays the query results, as described in “Application Monitor - Statistics Window: Query Results View” on page 281.



### Application Monitor - Statistics Window: Query Form

When you first access the Application Monitor - Statistics window, the query form is displayed. Use this form to define the query:

- Define the period of time for which to generate the query:
  - Select a pre-defined period, such as “Today” or “Last Month”, at the top of the “Period” area.
- Or,
- Define start and end dates at the bottom of the “Period” area.

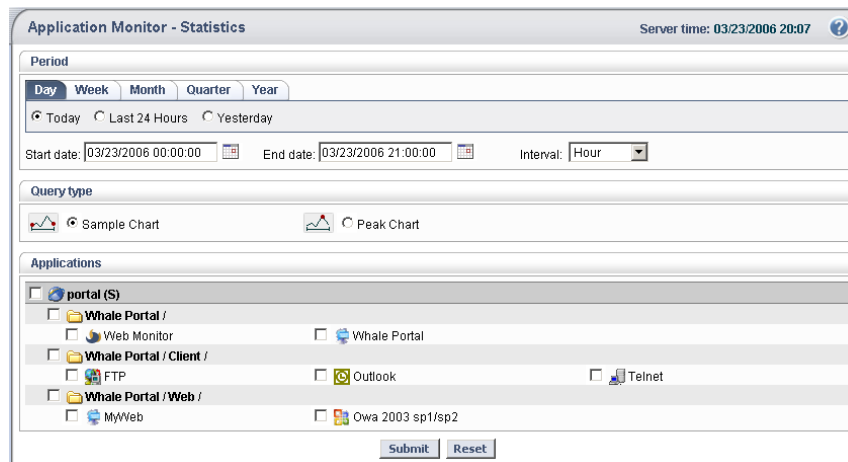
- Define the interval at which data is sampled, at the bottom right of the “Period” area. The intervals that are available for selection depend on the selected period. **For example:** if the selected period is a day, only an “Hour” interval can be defined; for a period of a week, you can select an interval of either an hour or a day.

By default, the maximal number of intervals that can be queried is 1,500. If required, you can change this value, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72. Note, however, that a value of over 1,500 intervals is not recommended and may slow down the monitor’s performance considerably.

- Select the query type:
  -  **Sample Chart:** the number of concurrent sessions is sampled at the end of each interval.
  -  **Peak Chart:** the number of concurrent sessions reported is the highest number of sessions that were open during the interval period.
- Select the application or applications for which to generate the query. By default, you can view query results for up to 15 applications. If required, you can change this value, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

Once you submit the query, the results are displayed in the window, as described in “Application Monitor - Statistics Window: Query Results View” on page 281.

**Figure 50. Application Monitor - Statistics Window: Query Form**



The screenshot shows the "Application Monitor - Statistics" window. At the top right, it says "Server time: 03/23/2006 20:07". The "Period" section has tabs for Day, Week, Month, Quarter, and Year. Below these are radio buttons for "Today", "Last 24 Hours", and "Yesterday". The "Start date" is 03/23/2006 00:00:00 and the "End date" is 03/23/2006 21:00:00. The "Interval" is set to "Hour". The "Query type" section has radio buttons for "Sample Chart" and "Peak Chart". The "Applications" section lists several applications with checkboxes: portal (S), Whale Portal / Web Monitor, Whale Portal / Client / FTP, Whale Portal / Web / MyWeb, Whale Portal, Outlook, Telnet, and Owa 2003 sp1/sp2. At the bottom are "Submit" and "Reset" buttons.







### Tip

After you submit a query, when you return to the query form from the “query results” view, you can click **Show last results** to display the results of the last query submitted, regardless of any changes you might have made in the query form.

## Application Monitor - Statistics Window: Query Results View

Query results are displayed in the Application Monitor - Statistics window after you submit a query in the query form, as described in “Application Monitor - Statistics Window: Query Form” on page 279.

- At the top of the window, query details are displayed, including period, interval, and query type, as you defined in the query form. If query results are available only for a part of the defined period, this is also indicated, under the “Period” field.
- Query results are displayed in two views:
  - A line chart displays the number of concurrent accesses to each of the applications in the query. The color that represents each application on the chart is indicated in the legend, to the left of the application name and icon.
  - The table, at the bottom of the window, displays information on each of the applications that were queried, as described in Table 32, “Application Monitor - Statistics Window: Query Results”, on page 282.
- You can view the data that is displayed in the chart in a tabular format by clicking .
- Use the paging and zooming controls to focus the view on the period of time you wish to monitor: .



### Tip

- When you zoom out to the smallest view, the window displays the entire period that is queried, up to the pre-defined interval limit.
- When you zoom in to the largest view, the window displays 10 intervals; to view additional intervals, use the paging controls.
- To return to the query form, click **Show query form**.

Figure 5I. Application Monitor - Statistics Window: Query Results View

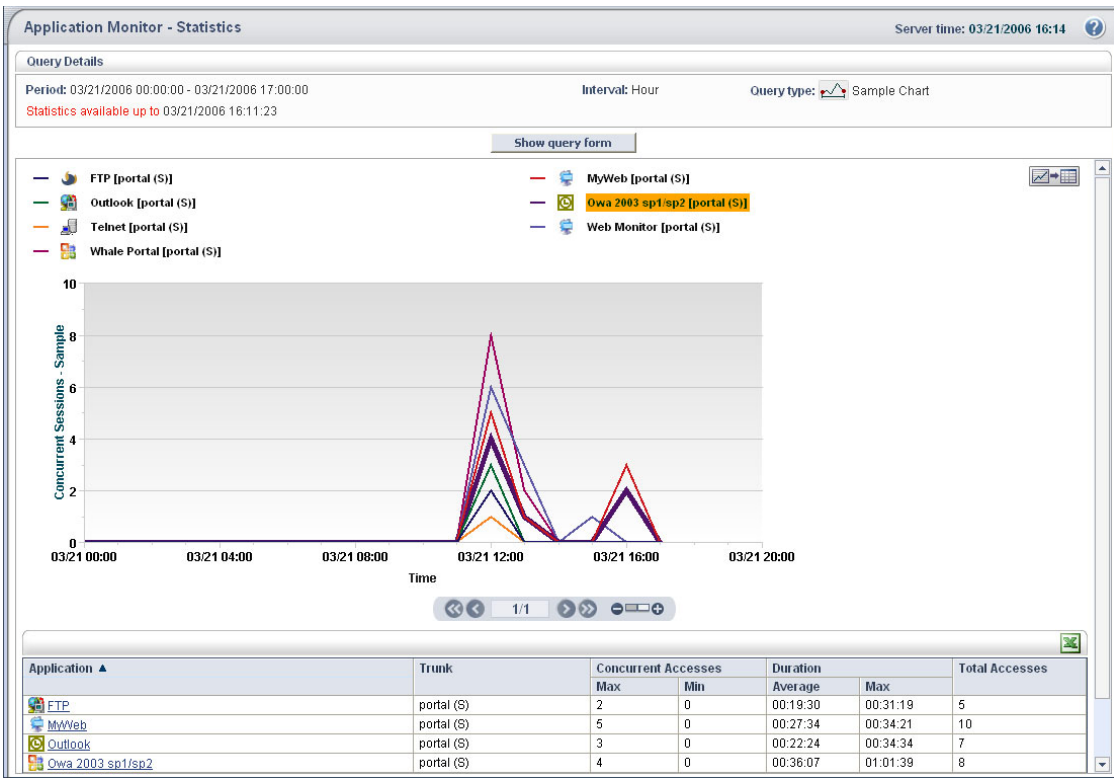


Table 32. Application Monitor - Statistics Window: Query Results

Parameter	Description
Application	Application name. Clicking the application name displays the Application Access Details window, described in “Application Access Details” on page 283.
Trunk	Trunk through which the application is enabled.
Concurrent Accesses	Minimal and maximal number of concurrent accesses to the application during the query period.

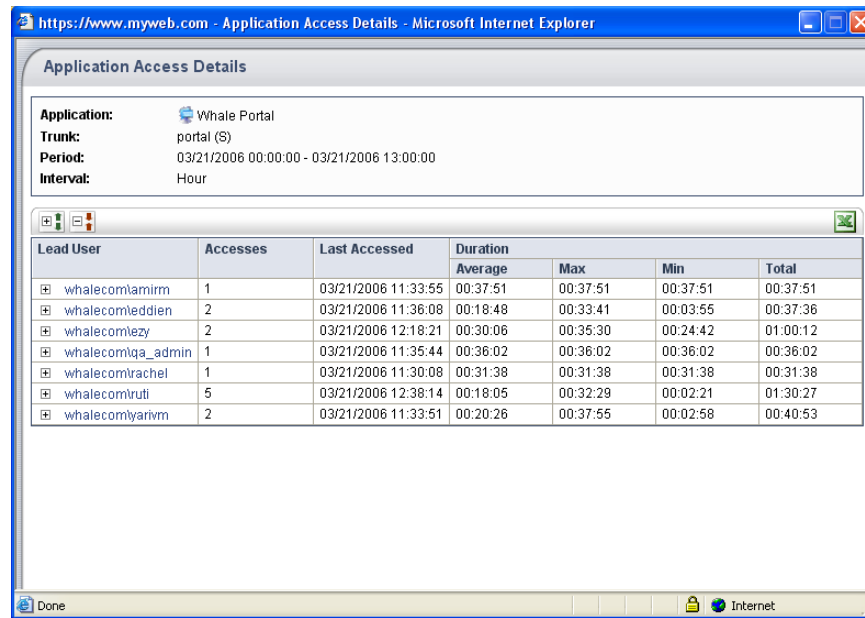
**Table 32. Application Monitor - Statistics Window: Query Results (Cont'd)**

Parameter	Description
Duration	<p>The average and maximal duration of accesses to the application during the query period.</p> <p><b>Note:</b> If the number of results exceeds the number of “Max Report Results”, as defined in the Configuration program, in the General tab of the Event Logging dialog box (described in “Configuring General Settings” on page 240), “Duration” is not reported.</p>
Total Accesses	<p>Total number of accesses to the application during the query period.</p> <p><b>Note:</b> If the number of results exceeds the number of “Max Report Results”, the number of total accesses is not reported.</p>



### Application Access Details

The Application Access Details window is displayed when you click an application name in the Application Monitor - Statistics window, in the Query Results view. It provides information on the application usage, as listed in Table 33, “Application Access Details—Parameters”, on page 284.

**Figure 52. Sample Application Access Details Window**



**Table 33. Application Access Details—Parameters**


Parameter	Description
Lead User	<p>User who initiated the session from where the application was accessed.</p> <p>Clicking the + sign next to the Lead User name, or clicking the name itself, expands the display and lists all of the user's accesses to the application during the query period, where the user name is the name used to access the application.</p> <p>Clicking  or  expands and collapses the display for all users, respectively.</p>
Accesses	Number of times the user accessed the application during the query period.
Last Accessed	Time when the application was last accessed by the user, during the query period.

**Table 33. Application Access Details—Parameters**

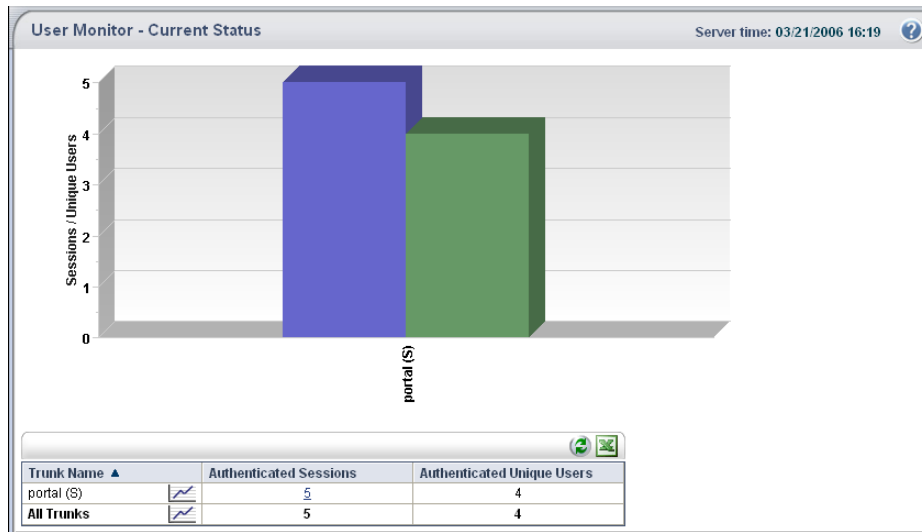
Parameter	Description
Duration	Duration of accesses to the application by the user, including average, maximal, and minimal duration, and the total access time.

## User Monitor - Current Status


The User Monitor - Current Status window provides online display of all the users that are currently connected to the IAG you are monitoring:

- At the top part of the window, a column chart is displayed. For each trunk, two columns represent the following:
  - Number of authenticated sessions that are currently open through the trunk.
  - Number of authenticated unique users currently using the trunk.  
**For example:** if a user opens two concurrent sessions with the trunk, two sessions are counted, but only one unique user.
- At the bottom part of the window, the information is presented in a tabular format. Clicking the number of authenticated sessions opens the trunk's User Monitor - Active Sessions window, described in "User Monitor - Active Sessions" on page 287.
- By default, the window refreshes the data every 15 seconds. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in "Customizing the Web Monitor Windows" on page 72.
- You can also monitor user behavior over time, for a selected trunk or for all active trunks. In the table at the bottom of the window, click  next to the trunk you wish to monitor, or next to "All Trunks", respectively. The User Monitor Over Time window is displayed, as described in "User Monitor Over Time" on page 286.


**Figure 53. Sample User Monitor - Current Status Window**



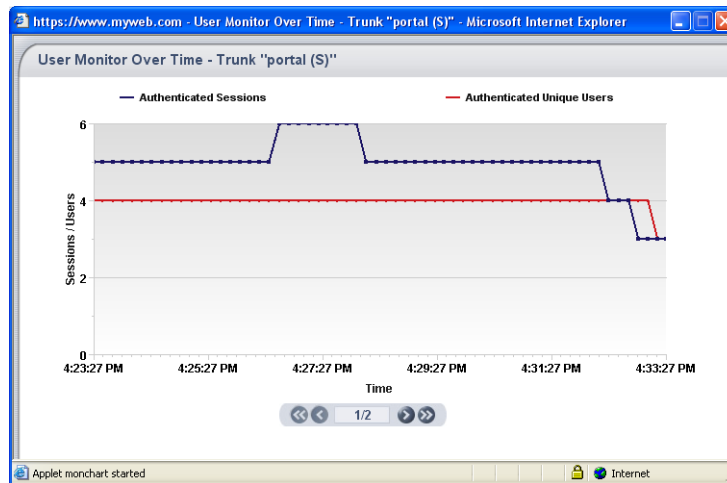
## User Monitor Over Time

The User Monitor Over Time window is displayed when you click  in the User Monitor - Current Status window. Use it to monitor user behavior over time, for a selected trunk or for all active trunks.

User behavior is displayed in a line chart, showing both authenticated sessions and authenticated unique users, at pre-defined intervals.

- By default, the window refreshes the data at 10-second intervals. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.
- Use the paging controls to scroll to the period of time you wish to monitor: .

**Figure 54. User Monitor Over Time**



## User Monitor - Active Sessions

This window provides a detailed snapshot of the currently-open sessions for each user. Use it for online user-access tracking and troubleshooting.

- You select which trunk to display at the top part of the window.
- The parameters that are provided for each session are listed in Table 34, “Parameters of the User Monitor - Active Sessions Window”, on page 287.
- By default, the window refreshes the data every five minutes. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

**Figure 55. Sample User Monitor - Active Sessions Window**




Current session is highlighted →

User Monitor - Active Sessions							
Server time: 03/21/2006 16:29							
Trunk: portal (S)							
#	Lead User	Session ID	Repository	Started At	Duration	Events	Terminate
1.	whalecomlrachel	2D828F4A-3F69-4903-BC58-D1004DFC1A77	whalecom	03/21/2006 16:26:19	00:00:59		
2.	whalecomlruti	→ E0113476-8557-4788-ABE2-F725545753A1	whalecom	03/21/2006 16:22:39	00:04:39		
3.	whalecomlqa_admin	050D185C-70F5-4CD2-8B28-0BA8A9AF9CF5	whalecom	03/21/2006 15:45:16	00:42:02		
4.	whalecomlrachel	07D5860D-B846-40F5-992A-5CD45A813CC7	whalecom	03/21/2006 15:41:04	00:46:14		
5.	whalecomlqa_admin	237901D4-5404-4432-9C27-689B5F83A339	whalecom	03/21/2006 15:36:54	00:50:24		
6.	whalecomlyarim	3B681B23-6288-4C85-BC93-65E3A60287F9	whalecom	03/21/2006 15:36:26	00:50:52		

**Table 34. Parameters of the User Monitor - Active Sessions Window**

Parameter	Description
Lead User	User who initiated the session.

**Table 34. Parameters of the User Monitor - Active Sessions Window (Cont'd)**

Parameter	Description
Session ID	Unique session ID. Clicking the session ID opens the Session Details window, described in “Session Details” on page 270.
Repository	Authentication repository of the user who initiated the session.
Started At	Date and time when the session was started.
Duration	Duration of the session.
Events	Clicking  generates a report of events related to the session. The report is displayed in the Event Reports window, described in “Event Report” on page 297.
Terminate	<p>Clicking  terminates the session; the session is no longer displayed in the User Session List.</p> <p><b>Tip:</b> Once you terminate a session, the status of the session in the Session Monitor - Active Sessions window changes to “unauthenticated”:</p> <div data-bbox="696 1121 841 1205"></div> <p>For details, refer to “Session Monitor - Active Sessions” on page 268.</p> <p><b>Note:</b> You cannot terminate the current session.</p>

## User Monitor - Statistics

This window enables you to view and analyze both the history and the current status of the users of the IAG, such as average session duration for each user, or the currently active sessions.

- Use the query form to submit a query, as described in “User Monitor - Statistics Window: Query Form” on page 289.
- The User Monitor - Statistics window then displays the query results, as described in “User Monitor - Statistics Window: Query Results View” on page 290.



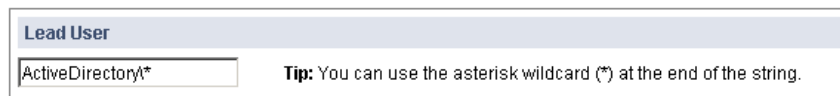
## User Monitor - Statistics Window: Query Form

When you first access the User Monitor - Statistics window, the query form is displayed. Use this form to define the query:

- Select the trunk for which to generate the query.
- Define the period of time for which to generate the query:
  - Select a pre-defined period, such as “Today” or “Last Month”, at the top of the “Period” area.

Or,

- Define start and end dates at the bottom of the “Period” area.
- Define the lead user or users for which to generate the query. Note the following:
  - Enter the user name using the following syntax:  
`<domain_name>\<user_name>`
  - You can use the asterisk wildcard (\*) at the end of the search string to define a group of users. **For example:** to enter a query for all users of a domain named “ActiveDirectory”, enter the following in the “Lead User” text box: ActiveDirectory\\*

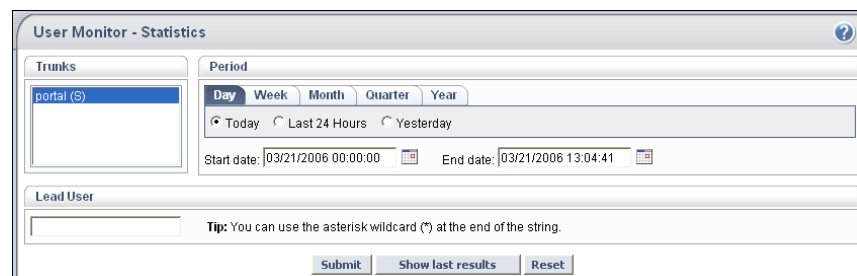


The screenshot shows a section of the query form titled "Lead User". It contains a text input field with the value "ActiveDirectory/\*". To the right of the field is a tip: "Tip: You can use the asterisk wildcard (\*) at the end of the string."

- The search is case-sensitive.

Once you submit the query, the results are displayed in the window, as described in “User Monitor - Statistics Window: Query Results View” on page 290.

**Figure 56. User Monitor - Statistics Window: Query Form**



The screenshot shows the "User Monitor - Statistics" window. It has a "Trunks" list on the left with "portal (S)" selected. The "Period" section has tabs for "Day", "Week", "Month", "Quarter", and "Year". Under "Day", there are radio buttons for "Today" (selected), "Last 24 Hours", and "Yesterday". Below these are "Start date" and "End date" fields with calendar icons. The "Lead User" field is empty. At the bottom are "Submit", "Show last results", and "Reset" buttons. A tip is present: "Tip: You can use the asterisk wildcard (\*) at the end of the string."



### Tip

After you submit a query, when you return to the query form from the “query results” view, you can click **Show last results** to display the results of the last query submitted, regardless of any changes you might have made in the query form.

## User Monitor - Statistics Window: Query Results View

Query results are displayed in the User Monitor - Statistics window after you submit a query in the query form, as described in “User Monitor - Statistics Window: Query Form” on page 289.

- At the top of the window, query details are displayed, including the query period, lead user or users, and trunk or trunks, as you defined in the query form. If query results are available only for a part of the defined period, this is also indicated, under the “Period” field.
- Query results are displayed in a table. The information that is provided for each user is described in Table 35, “User Monitor - Statistics Window: Query Results”, on page 291.

The number of results that can be displayed in the window is determined in the Configuration program, in the General tab of the Event Logging dialog box, in “Max Report Results” (described in “Configuring General Settings” on page 240). If the number of results exceeds the number of “Max Report Results”, no results are displayed.

**Figure 57. User Monitor - Statistics Window: Query Results View**

Lead User ▲	Average Session Duration	Total Session Duration	Accesses
whalecomlamirm	01:02:14	01:02:14	1
whalecomladdien	00:41:50	02:05:30	3
whalecomlezy	01:02:05	02:04:11	2
whalecomlqa_admin	00:55:17	02:45:53	3
whalecomlrachel	00:47:00	03:55:00	5

Application ▲	Number of Accesses	Last Access	Average Duration	Total Duration
MyWeb	3	03/21/2006 15:41:56	00:31:39	01:34:58
Owa 2003 sp1/sp2	3	03/21/2006 15:42:20	00:57:54	02:53:42
Web Monitor	1	03/21/2006 12:58:05	00:33:41	00:33:41

User	Access Date ▼	Duration
whalecomlrachel	03/21/2006 12:58:05	00:33:41



  

User	Access Date ▼	Duration
Whale Portal	03/21/2006 16:26:48	00:29:31
whalecomlruti	00:43:18	05:46:30
whalecomlyarivm	00:41:11	02:03:34

**Tip**

To return to the query form, click [Show query form](#).

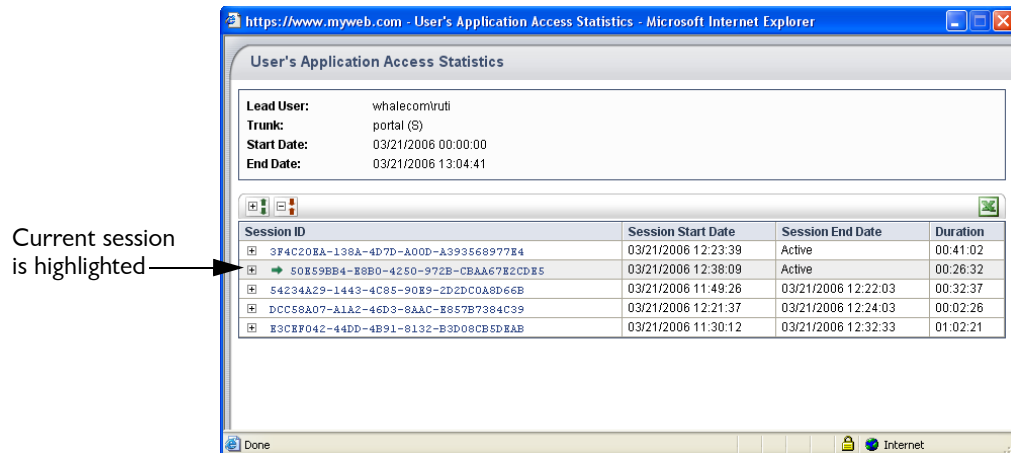
**Table 35. User Monitor - Statistics Window: Query Results**

Parameter	Description
Lead User	<p>User who initiated the session.</p> <p>Clicking the + sign next to the user name, or clicking the name itself, displays a list of all the applications that the user accessed during the query period. For each application, user access details are provided.</p> <p>Clicking  or  expands and collapses the display for all users, respectively.</p> <p>Once a user's view is expanded, clicking an application name, or clicking the + sign next to the application name, displays details regarding all of the user's accesses to the specific application.</p>
Average Session Duration	<p>Average duration of the user's sessions during the query period.</p>
Total Session Duration	<p>Total duration of the user's sessions during the query period.</p>
Accesses	<p>Number of times the user accessed the site during the query period.</p> <p>Clicking the number of accesses displays the User's Application Access Statistics window, described in "User's Application Access Statistics" on page 291.</p>



## User's Application Access Statistics

The User's Application Access Statistics window is displayed when you click a number of accesses in the "Accesses" column, in the User Monitor - Statistics Query Results window. It provides information on the application usage, as listed in Table 36, "User's Application Access Statistics—Parameters", on page 292.

**Figure 58. Sample User's Application Access Statistics Window**



**Table 36. User's Application Access Statistics—Parameters**

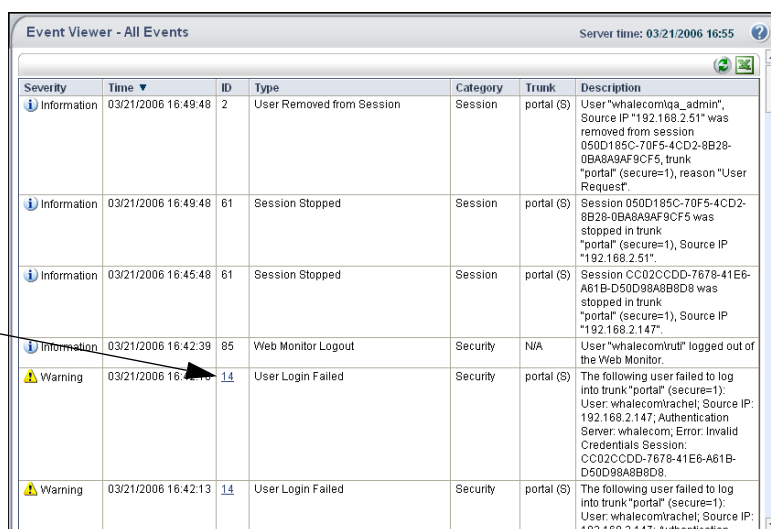
Parameter	Description
Session ID	<p>Unique session ID.</p> <p>Clicking the + sign next to the session ID, or clicking the ID itself, displays a list of all the applications the user accessed during the query period. For each application, user access details are displayed.</p> <p>Clicking  or  expands and collapses the display for all sessions, respectively.</p> <p>Once a session's view is expanded, clicking an application name, or clicking the + sign next to the application name, displays details regarding all of the user's accesses to the specific application during the session.</p>
Session Start Date	Date and time when the session was started.
Session End Date	<p>Date and time when the session was ended.</p> <p>For sessions that are currently active, "Active" is displayed.</p>
Duration	Duration of the session, from the time it was started until the time when the query was generated.

## Event Viewer

Using the event logs in the Event Viewer, you can view system, session, security, and application events and gather information about user and system activities. The Event Viewer window presents you with a constantly updating snapshot of recent events that occurred in the IAG you are monitoring.

**Figure 59. Sample Event Viewer**

Click the ID number to view troubleshooting information for this message. Applicable for Warning and Error messages.



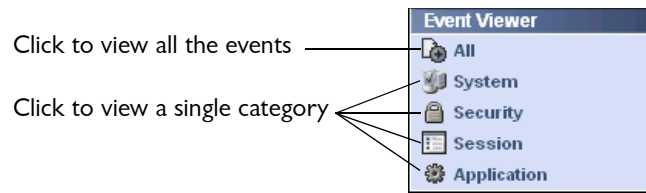
Severity	Time	ID	Type	Category	Trunk	Description
Information	03/21/2006 16:49:48	<a href="#">2</a>	User Removed from Session	Session	portal (S)	User "whalecom\ga_admin", Source IP "192.168.2.51" was removed from session 050D185C-70F5-4CD2-8B28-0BA8A9AF9CF5, trunk "portal" (secure=1), reason "User Request".
Information	03/21/2006 16:49:48	<a href="#">61</a>	Session Stopped	Session	portal (S)	Session 050D185C-70F5-4CD2-8B28-0BA8A9AF9CF5 was stopped in trunk "portal" (secure=1), Source IP "192.168.2.51".
Information	03/21/2006 16:45:48	<a href="#">61</a>	Session Stopped	Session	portal (S)	Session CC02CCDD-7678-41E6-A61B-D50D98A8B8D8 was stopped in trunk "portal" (secure=1), Source IP "192.168.2.147".
Information	03/21/2006 16:42:39	<a href="#">85</a>	Web Monitor Logout	Security	N/A	User "whalecom\trul" logged out of the Web Monitor.
Warning	03/21/2006 16:42:13	<a href="#">14</a>	User Login Failed	Security	portal (S)	The following user failed to log into trunk "portal" (secure=1): User: whalecom\trachel; Source IP: 192.168.2.147; Authentication Server: whalecom; Error: Invalid Credentials Session: CC02CCDD-7678-41E6-A61B-D50D98A8B8D8.
Warning	03/21/2006 16:42:13	<a href="#">14</a>	User Login Failed	Security	portal (S)	The following user failed to log into trunk "portal" (secure=1): User: whalecom\trachel; Source IP: 192.168.2.147; Authentication

By default, the window refreshes the data every 15 seconds. If required, you can customize the refresh rate, as described in the *Intelligent Application Gateway Advanced Configuration* guide, in “Customizing the Web Monitor Windows” on page 72.

The number of events that are displayed each time you open the Event Viewer window, and the maximal number of events that are added to the event list between refreshes, is determined in the Configuration program, in the General tab of the Event Logging dialog box, in “Queue Size”. For details, refer to “Configuring General Settings” on page 240.

- To view all events, in the left pane of the Web Monitor window, from the “Event Viewer” group, click **All**.
- To view only the events that are related to a single category—system, security, session, or application—click the corresponding link from the “Event Viewer” group. **For example:** to display only session-related events, click **Session**.

**Figure 60. Selecting Which Events to View**



**Table 37. Event Parameters**

Parameter	Description
Severity	Event severity can be one of the following: <ul style="list-style-type: none"><li>• Information: informative message denoting a normal event that might be of interest, such as user login or log out.</li><li>• Notice: normal but significant condition, such as users changing their password.</li><li>• Warning: events that might be problematic, but don't result in malfunction. For example: an unauthorized access attempt.</li><li>• Error: a significant problem, such as a failure to read the configuration.</li></ul>
Time	Time when the event occurred.
ID	Message ID. <b>Tip:</b> For Warning and Error messages, click the ID number to view troubleshooting information for the message.
Type	Short description of the event.
Category	Events are categorized as follows: <ul style="list-style-type: none"><li>• System events, such as service startup and shutdown and changes to the configuration.</li><li>• Security events, including login success or failure, security policy violation or change, and password change.</li><li>• Session events, including session start or stop, number of sessions, and other session-related events.</li><li>• Application events, such as access to the application.</li></ul>

**Table 37. Event Parameters**

Parameter	Description
Trunk	Name of the trunk where the event was generated.
Description	Long description of the event.

## Event Query

In the Event Query window, you can query events that are recorded by the built-in reporter of the Event Logging mechanism.

- For a description of the Event Logging mechanism, see “Event Logging” on page 237.
- For a description of the built-in reporter, including configuration instructions, see “Configuring the Built-In Reporter” on page 242.



### Note

If you disable the built-in reporter, you cannot generate Event Query reports.

Use this window to define and submit a query, as follows:

- Select the trunk or trunks for which to generate the query.
- Define the period of time for which to generate the query:
  - Select a pre-defined period, such as “Today” or “Last Month”, at the top of the “Period” area.
  - Or,
  - Define start and end dates at the bottom of the “Period” area.
- You can filter the query by one or more of the following event parameters: category, severity, and type. For a description of the parameters, refer to Table 37, “Event Parameters”, on page 294. When you narrow the query to a specific parameter, only the related items are listed for the other parameters. **For example:** if, in the “Category” list, you select “Security”, only security-related severities and message-types are displayed in the other lists.
- At the bottom part of the Event Query window, you can expand the “Advanced Options” area and use it to filter the query by the following:
  - **Session ID:** specific session.

- **Lead User:** according to user name. You can use the asterisk wildcard (\*) at the end of the search string to define a group of users. **For example:** to enter a query for all users of a domain named “ActiveDirectory”, enter the following in the “User” text box: ActiveDirectory\\*
- **Old Trunks:** define a query on old trunks, that is, trunks that are no longer defined in the Configuration program. Trunk names are comma-separated; HTTPS trunks are denoted by (S). For example: MyTrunk, MyTrunk (S).

You can select whether the query includes the trunks that are selected in the “Trunks” list by enabling or disabling the option **Include trunks selected in the “Trunks” list above**, respectively.



### Note

Generating Event Query reports uses system resources and might affect system performance. Depending on the size of the logs and on the query you define, report generation may take up to a few minutes. It is therefore important that you fine-tune the query as much as possible, especially the date range.

Once you submit the query, the results are displayed in the Event Report window, described in “Event Report” on page 297.


**Figure 61. Event Query**

The screenshot shows the 'Event Query' window. The title bar indicates the server time is 03/23/2006 19:58. The window is divided into several sections. The 'Trunks' section has a dropdown menu currently showing 'portal (S)'. The 'Period' section has tabs for 'Day', 'Week', 'Month', 'Quarter', and 'Year', and radio buttons for 'Today', 'Last 24 Hours', and 'Yesterday'. Below these are 'Start date' and 'End date' fields with calendar icons. The 'Message Filter' section has three columns: 'Category' (Application, Security, Session, System), 'Severity' (Error, Information, Notice, Warning), and 'Type' (Administrative Password Change, Application Access Policy Violation, Application Accessed, Application Authentication Failed). At the bottom, there is an 'Advanced Options' checkbox and 'Submit' and 'Reset' buttons.



## Event Report

The Event Report window is displayed when a report is generated by one of the following:

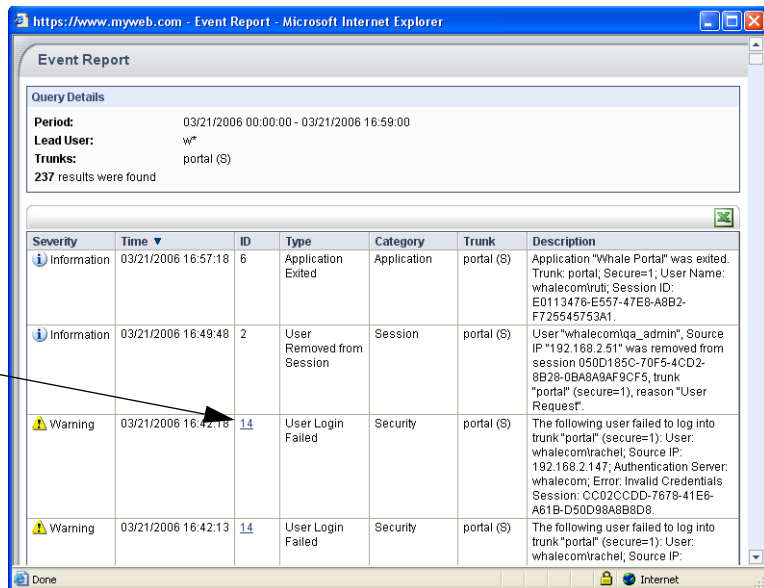
- When you generate a report in the Event Query window, as described in “Event Query” on page 295.
- When you click  in one of the Active Sessions windows.

The Event Report window is divided into two main areas:

- The top part of the window displays the following:
  - Period for which the query was generated.
  - Where applicable, filtering criteria such as “Categories”.
  - Trunk or trunks for which the query was generated.
  - Number of events that were found for the selected criteria. When the report is generated from within one of the Active Sessions windows, it is filtered by session ID.
  - Advanced options, when used.
- The main part of the window displays a list of reported events.
  - The parameters that are reported for each event are identical to the parameters of the Event Viewer, and are described in Table 37, “Event Parameters”, on page 294.
  - The maximal number of results that are displayed in the window is determined in the Configuration program, in the General tab of the Event Logging dialog box, in “Max Report Results”. For details, refer to “Configuring General Settings” on page 240.

**Figure 62. Sample Event Report**

Click the ID number to view troubleshooting information for this message. Applicable for Warning and Error messages.



Event Report

Query Details

Period: 03/21/2006 00:00:00 - 03/21/2006 16:59:00  
Lead User: w\*  
Trunks: portal (S)  
237 results were found

Severity	Time	ID	Type	Category	Trunk	Description
Information	03/21/2006 16:57:18	6	Application Exited	Application	portal (S)	Application "Whale Portal" was exited. Trunk: portal; Secure=1; User Name: whalecom\truti; Session ID: E0113476-E557-47E8-A8B2-F725545753A1.
Information	03/21/2006 16:49:48	2	User Removed from Session	Session	portal (S)	User "whalecom\lga_admin", Source IP "192.168.2.51" was removed from session 050D185C-70F5-4CD2-8B28-0BA8A9AF9CF5, trunk "portal" (secure=1), reason "User Request".
Warning	03/21/2006 16:42:18	<a href="#">14</a>	User Login Failed	Security	portal (S)	The following user failed to log into trunk "portal" (secure=1): User: whalecom\trachel; Source IP: 192.168.2.147; Authentication Server: whalecom; Error: Invalid Credentials Session: CC02CCDD-7678-41E6-A61B-D50D98A8B8D8.
Warning	03/21/2006 16:42:13	<a href="#">14</a>	User Login Failed	Security	portal (S)	The following user failed to log into trunk "portal" (secure=1): User: whalecom\trachel; Source IP:

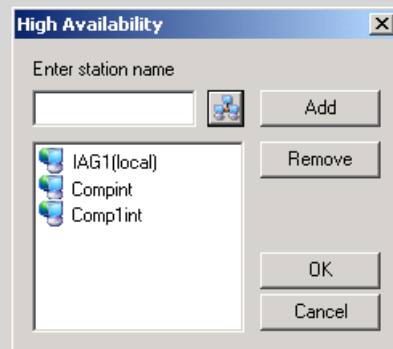
## Web Monitor High Availability Support

In sites where an IAG High Availability Array is deployed, you can monitor all the IAG servers that are part of the array from a single Web Monitor, whether you access the Monitor from within the organization or remotely. When you access the Web Monitor on one of the IAG servers that are part of the Array, the Monitor automatically maps itself to all the IAG servers in the Array.



### Tip

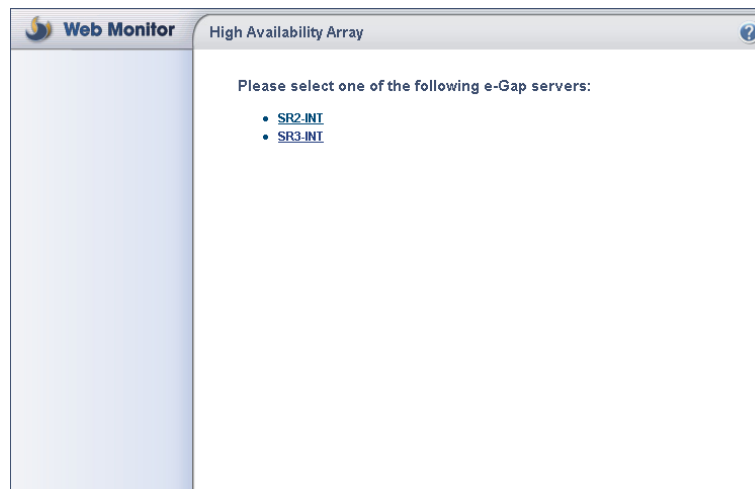
The list of IAG servers that are part of the Array is defined in the Configuration program, in the High Availability dialog box:



For a full description, refer to the *Intelligent Application Gateway High Availability Configuration* guide.

## Accessing IAG Servers in the Array

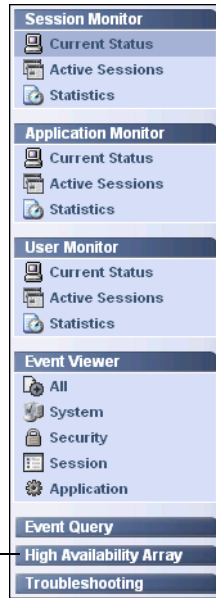
In sites that deploy a High Availability Array, when you first access the Web Monitor application, the High Availability Array window is displayed, listing the Intelligent Application Gateway servers:



Clicking the server you wish to monitor opens the main window of the Web Monitor.

Once the main window of the Web Monitor is displayed, access to the IAG servers that are part of the Array is enabled via a “High Availability Array” link on the menu of the Web Monitor browser window; clicking the link displays the High Availability Array window again.

“High Availability Array” link enables access to all IAG servers in the Array



If you cannot access an IAG server that is part of the Array via the applicable link, verify the following:

- The server is up and running.
- The server is accessible from the server where you are using the Web Monitor.
- You assigned the same users to the IAG Monitor Users group on all the IAG servers that are part of the Array. For details, refer to “Enabling Web Monitor Access from Computers Other Than the IAG” on page 261.



#### Tip

If access to the IAG fails while you are accessing the Web Monitor remotely, via the SSL VPN portal, and the failure is due to user authentication problems, the following message is displayed in the Event Viewer: “Login-On-The-Fly Failed”.

## Analyzing History Reports Once an IAG Server is Removed from the Array

Once you remove an IAG server from the High Availability Array, you are no longer able to query reports of events that were recorded on the server while it was still part of the Array. You can, however, copy the required logs onto one of the IAG servers which are part of the Array, and query the reports there, using the Event Query.

***To query reports of an IAG server that is removed from the Array:***

1. At the IAG server whose reports you wish to query, access the location where the logs of the Built-In reporter are saved:
  - The location is defined in the Built-In tab of the Event Logging dialog box, as described in “Configuring the Built-In Reporter” on page 242.

- By default, the logs are saved in the following location:

...\Whale-Com\e-Gap\logs\Events

Log files are saved under this folder in the following format:

<computer\_name>.BuiltinLog.default.<time\_stamp>

**For example:**

On a computer named “comp1”, a log file that was created on November 24, 2005 at 09:06:19 is named:

comp1.BuiltinLog.default.24.11.05-09-06-19.log

2. Copy the relevant file or files to one of the IAG servers that are part of the Array, placing them in the location where the logs of the Built-In reporter are saved on that computer, and rename the files so that <computer\_name> is the name of the computer where you are placing the file.

**For example:**

If you are placing the file described in step 1 on a computer named “comp2”, rename the file as follows:

comp2.BuiltinLog.default.24.11.05-09-06-19.log

If such a file already exists, change the time stamp as well.

*You can now query the events logged in the file or files you copied on the IAG server where you copied the files, in the Event Query.*

## SSL Event Monitoring

You can set the Registry settings of the IAG so that SSL connection attempts are reported in the Windows Event Viewer. You can select to view errors, warning, and informational and success events, or any combination of these event-types.

For details and instructions, see the following Microsoft article:

<http://support.microsoft.com/kb/260729/EN-US/>



**Note**

Make sure to restart the IAG after you make changes to the Registry.



# Chapter 10

## Troubleshooting

This chapter describes the following troubleshooting procedures:

- “Backup & Restore Utility” on page 303 provides instructions on how to back up and restore the configuration settings of the Intelligent Application Gateway (IAG).
- “Error Logging and Process Tracing” on page 307 describes how you run the IAG centralized logging and tracing mechanisms.
- “Log File Cleanup” on page 313, describing the log file cleanup for IAG and IIS log files, and the manner in which they are implemented. This section also provides instructions for configuring the log file cleanup process and for excluding IIS log files from the cleanup process.
- “Support Utilities” on page 319 describes how you run support utilities tests.
- “Restarting the Web Service in the IIS” on page 321 is required during some of the procedures relating to the IAG filter.

### Backup & Restore Utility

The Backup & Restore utility is comprised of the Backup utility, and the Restore utility. During backup, the IAG Backup & Restore utility uses the Windows `makecab.exe` utility to archive the necessary files and Registry values in a `.cab` file. It uses the Windows `extract.exe` utility to restore them.

We recommend that you create backups as follows:

- Run the Backup utility directly after the initial IAG configuration, to back up the IAG’s configuration settings.
- Following the initial backup, make sure to run the utility each time you modify the configuration settings, in order to ensure that the backup is updated at all times.
- Copy the backup file to a separate location whenever you make major changes to the configuration.

By default, the backup is created under the IAG installation path:

...\\whale-Com\\e-Gap\\Backup

**Tip**

If you do not see the backup file in this location, the default path may have been changed. Contact technical support for assistance in identifying the current path.

The name of the backup file that is created in the defined backup folder is:

`whlbackup.<host_name>.cab`

Where `host_name` is the name of the IAG.

Instructions for using the Backup & Restore utility are provided in:

- “Backing up the Configuration” on page 304
- “Restoring the Configuration” on page 305

**Tip**

Each time you run the Backup & Restore utility, a log is created in the this file: `...\Whale-Com\e-Gap\Logs\whlbackup.log`

## Backing up the Configuration

You can backup the configuration in one of the following methods:

- From within the Configuration interface, as described in “Backing up the Configuration in the Configuration Program” on page 304
- By running a Console application in a Command line, as described in “Running the Backup Utility as a Console Application” on page 305


**Note**

The BackUp utility can be run as-is, using the default settings, or can be configured. If you need to configure the utility, contact technical support for further details.

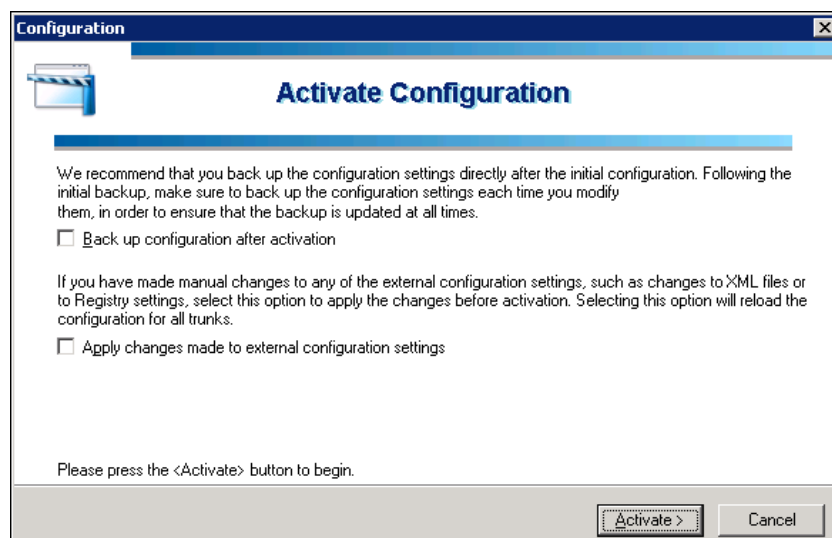
## Backing up the Configuration in the Configuration Program

You can select to back up the configuration settings each time you activate the configuration in the Configuration program.

***To back up the configuration in the Configuration program:***

1. In the Configuration program, when you click  to activate the configuration, the following is displayed:





2. Select the option “Back up configuration after activation”, then click **Activate >**.

*The IAG configuration is activated, and backed up.*

## Running the Backup Utility as a Console Application

You can run the Backup utility as a Console application, in a Command line.



### Note

If you back up the configuration in a Command line, you will only be able to restore it using a Command line, and not via the Configuration interface.

### *To run the Backup utility as a Console application:*

- At the IAG, open a Command line and type:

```
whlbackup.exe -b
```

*The IAG configuration is backed up.*

## Restoring the Configuration

Once you back up the IAG configuration using the Backup utility, you can use the Restore utility to restore the configuration settings into an installed IAG. You can restore the configuration using one of the following methods:

- From within the Configuration interface, as described in “Restoring the Configuration in the Configuration Program” on page 306
- By running a Console application in a Command line, as described in “Running the Restore Utility as a Console Application” on page 306



### Note


If you backed up the configuration in a Command line, you should restore it using a Command line; you can not restore it using the Configuration interface.

Before you restore the backup, make sure that the IAG that was backed up and the IAG to which you are restoring the configuration settings are compatible, as follows:

- Both IAG servers use the same passphrase.
- The same application shuttles are installed on both servers.

## Restoring the Configuration in the Configuration Program


*To restore the configuration in the Configuration program:*

1. In the Configuration program, on the **Admin** menu, click **Restore from Backup**.
2. Click  to activate the configuration  
*The IAG configuration settings are restored from the backup file, as defined in the file `whlbackup.ini`.*

## Running the Restore Utility as a Console Application

You can run the Restore utility as a Console application, in a Command line.

*To run the Restore utility as a Console application:*

1. At the IAG, open a Command line and type:  
`whlbackup.exe -r`
2. Still at the IAG, activate the configuration by clicking  in the Configuration program.  
*The IAG configuration settings are restored from the backup file, as defined in the file `whlbackup.ini`.*

## Error Logging and Process Tracing

The error logging and tracing mechanisms are used for error logging and for tracing of a variety of IAG processes. The error server, which controls the centralized logging and tracing mechanisms, serves two purposes:

- **Tracing:** the error server can trace the activities of each process that is defined to report to it, and create a trace log file, which can be used for debugging purposes. When required, and depending on the aspects of the IAG you need to examine, technical support will instruct you to run a trace, including details of the processes you need to include in it.
  - The manner in which you define traces is described in “Error Server and Trace Configuration File” on page 307.
  - The trace log file is described in “Error Server Trace and Log Files” on page 311.
- **Error logging:** the error server receives error reports from the processes that are connected to it, and logs them—as well as its own errors—in error logs. The log files are described in “Error Server Trace and Log Files” on page 311.

### Error Server and Trace Configuration File

The behavior of the trace mechanism, and of the error and trace log files, are controlled by the configuration file, `trace.ini`, located under:

...\Whale-Com\e-Gap\Common\Config

This file contains the following configurable parameters of the error server mechanism, which can be edited as required:

- Individual traces that the error server logs, as described in “Individual Trace Sections” on page 308.
- General trace and error log file parameters, as described in “General Trace Configuration Section” on page 310.



#### Warning

Edit only the individual and general trace sections of the configuration file. Do not make changes to any other sections of the file.

The manner in which the changes you make to the trace configuration file are activated is described in “Trace Activation” on page 311.

## Individual Trace Sections

In order to create a trace, you configure a `Trace` section in the `trace.ini` configuration file. Each individual trace section can hold one or more of the parameters described in the following table, depending on the trace level and individual trace parameters.

**Table 38. `trace.ini` file—Individual Trace Parameters**

Parameter	Description
<code>Trace</code>	Defines the elements that will be traced. Traces can be defined at different levels of granularity, including processes, instances, reporters, and classes. The parameters you need to define will be provided by technical support.
<code>trace-level</code>	Determines whether the trace is active, as well as the trace's log level: <ul style="list-style-type: none"><li>• The level <code>none</code> indicates that the trace is <b>not</b> active.</li><li>• Any level other than <code>none</code> indicates that the trace <b>is</b> active, and determines the log level. Available log levels are: <code>light</code>, <code>medium</code>, <code>heavy</code>, and <code>xheavy</code>.</li></ul>
<code>refresh*</code>	Refresh period of the trace, in seconds. After each refresh period, the process checks for changes in the configuration file: <ul style="list-style-type: none"><li>• If a new trace was added or an inactive trace activated for this process, the error server activates it.</li><li>• If any of the parameters in this trace were changed since the last refresh, the process applies the new parameters to the trace.</li></ul>
<code>max_size*</code>	Maximum size of the trace log file, in bytes.
<code>report_errors</code>	Select whether to report errors, which are reported in the error log, in the trace log as well.

\* This parameter can be defined in individual traces as well as in the general `[Trace]` section. If it is not defined here, the value in the general `[Trace]` section applies.

## Trace Templates

Following are sample templates you can use in order to create a trace, as defined in the `trace.ini` configuration file. These are samples only, and therefore appear in the file as comments, preceded by the number sign (`#`).

The last sample section, # [Trace], lists additional parameters that can either be applied to the individual trace section, or, if a parameter is not configured for the trace, be applied from the general [Trace] section of the file, as described in “General Trace Configuration Section” on page 310.

```
# [Trace\<process-name>\<instance-name>\<reporter-name>]
# *=<trace-level>
# <class-name>=<trace-level>
#
# [Trace\<process-name>\<reporter-name>]
# *=<trace-level>
# <class-name>=<trace-level>
#
# [Trace\<process-name>]
# *=<trace-level>
# <instance-name>=<trace-level>
# refresh=<refresh-time-in-seconds>
# max_size=<max-trace-file-size-in-bytes>
# report_errors=<yes/no>
#
# [Trace]
# refresh=<refresh-time-in-seconds>
# max_size=<max-trace-file-size-in-bytes>
# report_errors=<yes/no>
```

### Sample Individual Trace

The following example shows a trace that is configured for the Whale Manager Service process, with an extra-heavy trace level, and a refresh rate of two seconds. The maximum file size is 10 MB, and the trace is configured to log error reports in the error log.

```
[Trace\whlegapd]
*=xheavy
refresh=2
max_size=10000000
report_errors=yes
```

## General Trace Configuration Section

The general configuration section, [Trace], at the end of the `trace.ini` configuration file, holds general parameters that apply to all the configured individual traces, unless these trace parameters are configured in the individual trace sections. Some of the parameters also apply to the error log files. The general parameters are described in the following table.

**Table 39. trace.ini file—General Configuration Parameters**

Parameter	Description	Affected Files
refresh*	Refresh period, in seconds. After each refresh period, the process checks for changes in the configuration file: <ul style="list-style-type: none"><li>• If any new traces relevant to this process were added or activated since the file was last checked, the process starts tracing them.</li><li>• If any of the parameters in the existing traces were changed since the last refresh, the process applies the new parameters.</li></ul>	trace.ini
max_size*	Maximum file size, in bytes.	Error log files Trace log files
high_water low_water instances_kept	Log file cleanup parameters. <b>Note:</b> These parameters are defined in the Configuration program, and should not be changed in the configuration file. For instructions on configuring these parameters, see “Configuring Log File Cleanup Parameters” on page 317.	N/A
report_errors	Select whether to report errors, which are reported in the error log, in the trace log files as well.	Trace log files

\* If this parameter is configured in both the individual and the general [Trace] sections, the individual settings take precedence.

## Sample trace.ini General Configuration Section

```
[Trace]
refresh = 60
max_size = 1468006
high_water = 100
low_water = 50
instances_kept = 3
report_errors = yes
```



### Note

The `high_water`, `low_water`, and `instances_kept` parameters are derived from Configuration program definitions.

## Trace Activation

When the IAG processes are activated, each of the processes examines the trace configuration file. At this time, any changes in the file relevant to that process, such as new traces or changes to existing traces, are activated. In addition, the general parameters and the log file cleanup parameters (defined in the Configuration program) are implemented at this time.

Thereafter, the processes examine the configuration file and activate any relevant changes at the defined refresh intervals.

## Error Server Trace and Log Files

This section describes the trace and log files that are created by the Error Server, including:

- The file location and naming conventions, on page 311.
- The file size and the number of files retained on the server, on page 312.

## File Location and Naming



### Note

The file timestamps, as well as the timing of the events inside the files, are derived from the local computer's clock.

## Trace Files

For every active trace, the error server creates a trace log file under:

...\Whale-Com\e-Gap\Logs

In the following format:

<Server\_Name>.<Process\_Name>.<Instance\_Name>.<Time\_Stamp>.log

Where:

- <Server\_Name> represents the name of the server from which the log file originated.
- <Process\_Name> represents the name of the reporting process. Process names, as defined by the IAG.
- <Instance\_Name> represents the name of the reporting instance.
- <Timestamp> represents the log file creation time and date.

**For example:**

The name of a trace file created by the server “whlsrv”, by the “service” instance of the Whale Manager Service on October 1, 2005, at 12:47:46 is:

whlsrv.whlegapd.service.01.10.05-12-47-46.log

## Error Log Files

The error log files are created under:

...\Whale-Com\e-Gap\Logs\<Server\_Name>whlerrsrv.error.<Time\_Stamp>.log

Where <Timestamp> represents the time and date when the file is created. For example, the name of an error log file created on September 25, 2005, at 20:28:08, is:

whlerrsrv.error.25.09.05-20-28-08.log

## Size and Quantity of Files

### Trace Files

The error server writes the reported events into the trace log file, until the log file reaches the maximum file size allowed. The error server then creates a new trace log file, and logs events in the new file. The maximum file size can be defined as follows:

- The default maximum file size is set in the general [Trace] section of the trace configuration file, as described in “General Trace Configuration Section” on page 310.



- You can set a maximum file size for individual traces, which overrides the default maximum file size, as described in “Individual Trace Sections” on page 308.

If the maximum file size is configured in both the individual traces and the general [Trace] section, the individual settings take precedence.

In order to preserve disk space, the trace log files are periodically cleaned up, as described in “Log File Cleanup” on page 313.



#### Tip

The trace log of a process is **not** deleted when a process is stopped.

## Error Log Files

Entries are written into the error log file until the file reaches the maximum file size allowed. The error server then creates a new log file, and logs errors in the new file. The maximum file size is defined in the general [Trace] section of the trace configuration file, as described in “General Trace Configuration Section” on page 310.

In order to preserve disk space, the error log files are periodically cleaned up, as described in “Log File Cleanup” on page 313.

## Log File Cleanup

The cleanup of log files prevents a buildup of old log files, that can in time fill up the available disk space on the IAG. During cleanup, old log files of the following types are deleted:

- IAG log files, including:
  - Event logs
  - Error logs
  - Trace logs
- IIS log files.



#### Note

IIS log files can be excluded from the log file cleanup process, as described on page 318.

This section provides the following:

- A list of the configurable log file cleanup parameters, which control when a cleanup starts and stops, on page 314

- A description of how the log file cleanup process works, and of how the cleanup parameters are implemented, on page 314
- Instructions for configuring the cleanup parameters, on page 317
- Instructions for excluding IIS log files from the log file cleanup process, on page 318

## Log File Cleanup Parameters

The following log file cleanup parameters can be configured in the Configuration program:

**Table 40. Log File Cleanup Parameters**

Parameter	Description
Start Cleanup at ... MB	Total size, in megabytes, of IAG and IIS log files that can be kept on the disk, before the IAG starts a log file cleanup process.* <b>Tip:</b> Set this value according to the disk space you can allocate for this purpose.
Stop Cleanup at ... MB	Total size, in megabytes, of IAG and IIS log files that are kept on the disk after the log file cleanup process.*
Number of Undeleted Files	Optimal number of files retained after the log file cleanup process, as follows: <ul style="list-style-type: none"> <li>• Event, trace, and IIS log files—the number of files retained for each individual trace*</li> <li>• Error log files—the number of files retained is twice the number configured here</li> </ul> <b>Tip:</b> The ratio between undeleted error log files and other log files is hardcoded and cannot be changed.

- \* The deletion of IIS log files can be excluded from the log file cleanup process altogether, as described on page 29.

## How the Log File Cleanup Process Works

The log file cleanup process starts when one of the following occurs:

- The number of log files, including IAG event, error, and trace log files, and IIS log files, exceeds 2,048. This parameter is hard-coded and cannot be changed.

- The total size of all the IAG event, error, and trace log files, and IIS log files, exceeds the “Start Cleanup at ... MB” value.



#### Note

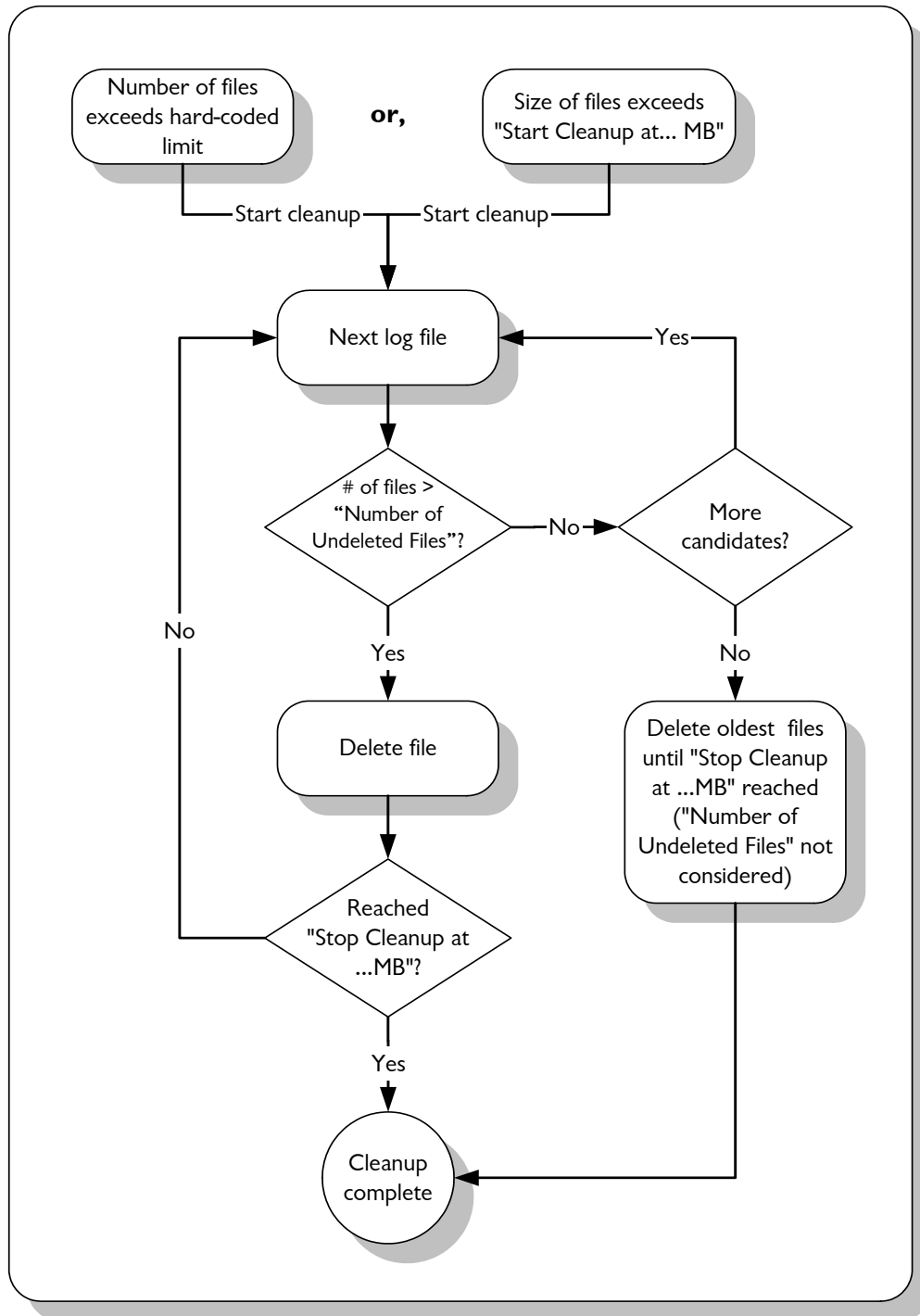
- The log file cleanup process is started **only** under one of the two conditions described above. Cleanup does not start when there is a disk overflow; if there is no more space on the disk, the error server stops writing error and trace logs onto the disk, without notification. It is therefore important to configure the “Start Cleanup at ... MB” parameter according to the disk’s capacity.
- IIS log files can be excluded from the log file cleanup process, as described on page 29.

Once the log file cleanup starts, the log files, are deleted, starting with the oldest files, according to the file modification time (not according to the file’s timestamp). Files are deleted until the total size of the files left on the disk reaches the value defined in “Stop Cleanup at ... MB”. For each type of file, the cleanup process leaves a number of files undeleted, as determined by the value defined in “Number of Undeleted Files”.

If, by deleting the files as described above, the total size of undeleted files is down to the value defined in “Stop Cleanup at ... MB”, the log file cleanup is complete. If, however, after leaving the number of files defined in “Number of Undeleted Files” the size still exceeds the “Stop Cleanup at ... MB” parameter, the cleanup process ignores the “Number of Undeleted Files” value and deletes more files, starting with the oldest file, until the total size of the log files in the IAG is reduced to the “Stop Cleanup at ... MB” value.

Figure 63 describes the flow of the log file cleanup mechanism:

**Figure 63. Log File Cleanup Mechanism**



## Configuring Log File Cleanup Parameters

You can change the default values of the log file cleanup parameters, including:

- The minimum and maximum amount of disk space allocated to the log files, including IAG event, error, and trace log files, and IIS log files.
- The number of files you wish to retain.



### Note

You can exclude IIS log files from the cleanup process, as described on page 318.

### *To configure log file cleanup parameters:*


1. In the Configuration program, on the **Admin** menu, click **Advanced Configuration...**

*The Advanced Configuration window is displayed.*

2. In the Log File Cleanup area, change one or more of the default values as required, as described in Table 40, “Log File Cleanup Parameters”, on page 314.

Click **OK**.

*The Advanced Trunk Configuration window closes.*

3. In the main window of the Configuration program, click  to save and activate the configuration.

*The log file cleanup process will start and stop at the defined total size of files values, and the error log server will retain the defined number of log files.*

## Excluding IIS Log Files from the Log File Cleanup Process

If you do not want the IIS logs to be calculated in the computation of the space allocated for log files, and do not want IIS log files to be deleted during the log file cleanup process, proceed as described below.

**To exclude the IIS log files from the log file cleanup process:**

1. At the IAG, use the Registry Editor to access the following Registry key:

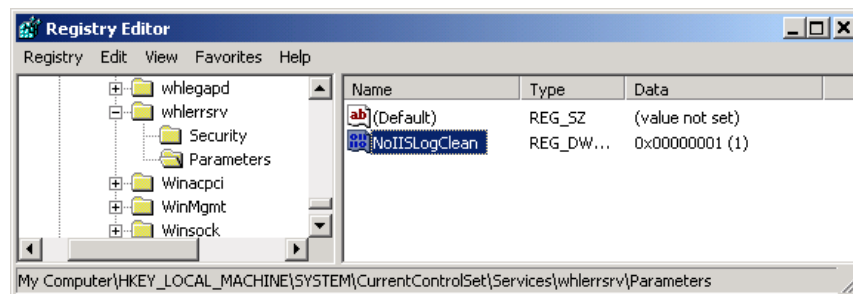
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\whlerrsrv\Parameters\



### Tip

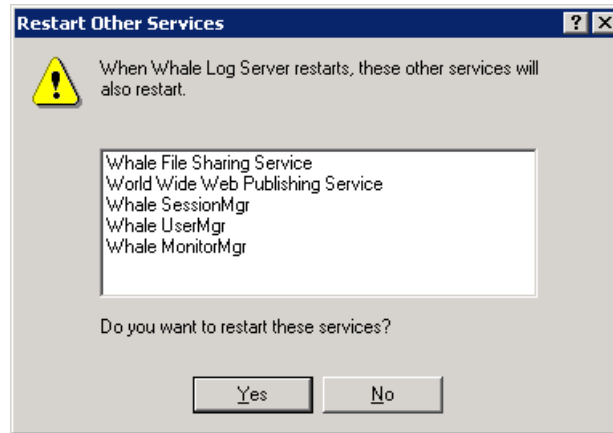
If the Parameters Registry key does not exist under ...\whlerrsrv\, you must create it.

2. Create a new DWORD value: NoIISLogClean.
3. Change the **Value data** of NoIISLogClean to 1, as shown in the example below:



4. Restart the Whale Log Server service, as follows:
  - In the Windows Control Panel double-click **Settings > Control Panel > Administrative Tools**, then double-click **Services**.
  - Right-click the Whale Log Server and select **Restart**.

*The Restart Other Services dialog box is displayed.*



### Tip

When you stop the Whale Log Server service, a number of other dependent services are also stopped. When you use the **Restart** command, the Whale Log Server service is automatically stopped and restarted, as are all the dependent services. For this reason, it is recommended that you use the **Restart** command and not the **Stop** command. If you do stop the service with the **Stop** command, make sure to manually start it and all the dependent services that were stopped.

5. Click **Yes** to restart all listed services.

*The Whale Log Server service and all other services in the list are stopped, and are then restarted automatically.*

*IIS log files will not be computed in the calculation of space defined in the trace.ini configuration file, and will not be deleted by the log file cleanup process on the IAG.*

## Support Utilities

The Support Utilities are a set of command line utilities designed for diagnostics purposes, which technical support may ask you to run in order to help to diagnose problems.



The utilities include:

- Pre-defined Support Utilities tests, which you can run to examine the system configuration, IAG functionality, and other data, in order to enhance diagnosing problems. For instructions on how to run these tests, see “Running Support Utilities Tests” on page 320.

- The Data Collection utility, which collects and packs files of different types to be sent to technical support for offline diagnostics purposes. For instructions on how to run the Data Collection Utility, see “Running the Data Collection Utility” on page 321.

## Running Support Utilities Tests

Before running the tests, note the following:

- For some of the tests, you may need to stop the Web service of the IIS, as described in “Restarting the Web Service in the IIS” on page 321.
- For information on the available tests and commands, you can use the following commands from the Command prompt:
  - Type `whltest --list` for a list of the available tests
  - Type `whltest -h` for a list of the command options
- If you used the `-N` or `-n` command options, alarms and warnings are displayed as pop-up messages during tests. In the message box:
  -  indicates an alarm. Alarms should be handled immediately, as they indicate serious IAG problems.
  -  indicates a warning. Warnings contain information you may need to take into consideration, but which does not necessarily have an immediate effect on the operation of the IAG.

After viewing the message box, click **OK** in the message box to continue running the tests.

### *To run a Support Utilities test:*

1. On the IAG, open a Command prompt and enter the command string, in this format:

```
whltest [<option><option>...][<name><name>...]
```

Where `<option>` indicates a required test option, and `<name>` contains the name of the test you wish to run.

For example: `whltest -n system`

where one test (`system`) is run with one option (`-n`).

2. Press `<Enter>`.

*The test is run, according to the parameters you entered in the command line. A log file is created whenever a test is run, containing any alarms or warnings, as well as general information gathered during the tests. The log file is named according to the IAG trace mechanism log file conventions, described in “File Location and Naming” on page 311.*





#### Note

For security reasons, it is recommended that you delete the Support Utilities log files after viewing them (including deletion from the Windows Recycle Bin), since they are not encrypted and contain the results of various sensitive tests.

## Running the Data Collection Utility

The Data Collection utility can be configured to collect any files required, as well as to automatically run any or all of the Support Utilities tests. If required, you will be instructed by technical support on how to do so.

#### ***To run the Data Collection utility:***

1. On the IAG, open a Command prompt and type:

```
whlcollect
```

2. Press <Enter>.

*The utility is run, and an archive file is created. This may take a few minutes.*

*The resulting file is named: <hostname> whlcollect.cab.*

*It is stored in: ...\\whale-Com\\e-Gap\\Backup.*

3. Encrypt the file created by the Data Collection utility, using an encryption utility such as PGP®.
4. Send the encrypted file to technical support.



#### Note

For security reasons, it is recommended that you delete the original and encrypted data collection files after viewing them (including deletion from the Windows Recycle Bin).

## Restarting the Web Service in the IIS

The following procedures describe how you stop the Internet Information Server (IIS) on the IAG, then restart the Web service, in order to reload the Web filters, filter extensions, and filter libraries, as required during some of the procedures described in this Guide.



#### Note

During this procedure, you stop the IIS, then re-start the Web service. If any other services on the IAG, such as FTP or SMTP, are using the IIS, you have to start them as well.

## Stopping the IIS

This procedure describes how you stop the IIS, as well as what steps to take in case the standard procedure does not stop it.

### *To stop the IIS:*

- On the IAG, open a Command prompt and type:

```
net stop iisadmin /y
```

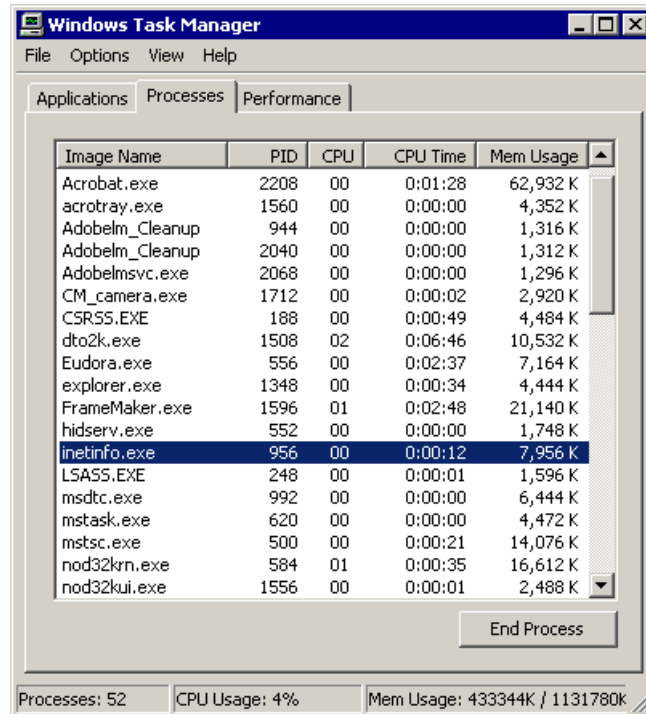
Press <Enter>.

*The following messages are displayed in the Command prompt:*

*The IIS is stopped. You now have to re-start the Web service, as described in “Starting the Web Service in the IIS” on page 323.*

### *If the IIS does not stop, take the following steps:*

1. Still on the IAG, open the Windows Task Manager and select the Processes tab.
2. Verify that the process `inetinfo.exe`, which runs the IIS, is listed in the Image Name column:



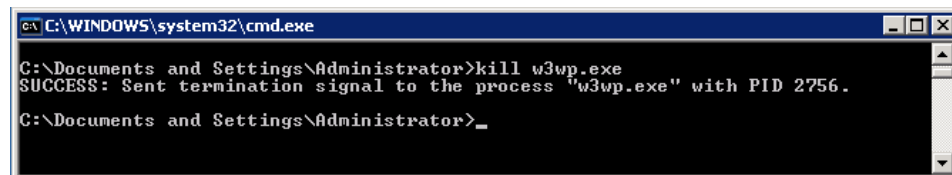
This is an indication that the IIS is still running.

3. Back in the Command prompt, type:

```
kill w3wp
```

Press <Enter>.

*The following message is displayed in the Command prompt:*



*The IIS is stopped. You now have to re-start it, as described in the following procedure.*

## Starting the Web Service in the IIS

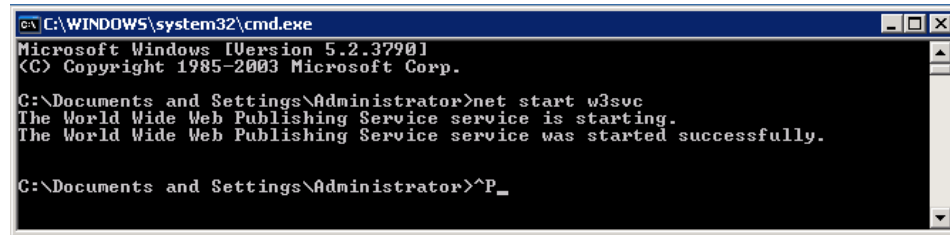
### To start the Web service in the IIS:

- In the Command prompt on the IAG, type:

```
net start w3svc
```

Press <Enter>.

*The following messages are displayed in the Command prompt:*



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>net start w3svc
The World Wide Web Publishing Service service is starting.
The World Wide Web Publishing Service service was started successfully.

C:\Documents and Settings\Administrator>^P_
```

*The Web service in the IIS is started and the filters are reloaded.*

## Appendix A

# Troubleshooting Event Logging Messages

This appendix describes how you troubleshoot events that are reported by the Intelligent Application Gateway (IAG) Event Logging mechanism, according to the message that is displayed when the event occurs. Troubleshooting instructions are provided for Error and Warning messages.

### Warning #4: Service Shutdown

#### Symptoms

A Windows service running on the IAG was stopped.

#### Cause

A Windows service that is required in order to run the IAG is not started.

#### Resolution

Start the relevant service on the IAG:

1. In the Windows Control Panel double-click **Administrative Tools**, then double-click **Services**.
2. Select and right-click the applicable service, then select **Start**.

### Warning #8: IAG Configuration Login Failed

#### Symptoms

When attempting to log in to the Configuration program, the login fails and the following message is displayed: "Incorrect Password".

#### Cause

Incorrect password used.

## Resolution

Log in using the correct password. If you forgot the password, you can assign a new password for the Configuration program as follows:

1. At the IAG, access the Service Policy Manager.
2. In the Service Policy Manager, on the **Admin** menu, click **Change Passwords...**
3. In the Change Password dialog box, activate the option “Use same password for all applications”, then enter the passphrase and the new password, and click **Change...**



### Note

- The password must contain at least six digits.
- Changing the password in this manner is global, and affects the Service Policy Manager, as well.

## Warning #11: Concurrent Sessions Threshold Reached

### Symptoms

None.

### Cause

This is a warning that the threshold of the number of sessions that can be open through the site at the same time was reached. When the threshold is reached, this message is logged whenever a new session is established, until the number goes below the threshold again. Once the maximal number of sessions that can be open through the site at the same time is reached, new sessions can no longer be established.

## Resolution

If this event occurs on a regular basis, do one of the following:

- Verify that the defined threshold is not too low.
- Increase the number of sessions that can be open through the site, and raise the threshold accordingly.

You define those settings at the IAG, in the Configuration program, as follows:

1. Open the Advanced Trunk Configuration window of the relevant trunk, and access the Session tab.
2. Modify the required settings in the “Concurrent Sessions Threshold” and “Max Concurrent Sessions” fields, respectively.

## **Warning #I2: Concurrent Unauthenticated Sessions Threshold Reached**

### **Symptoms**

None.

### **Cause**

This is a warning that the threshold of the number of unauthenticated sessions that can be open through the site at the same time was reached. When the threshold is reached, this message is logged whenever a new unauthenticated session is established, until the number goes below the threshold again. Once the maximal number of unauthenticated sessions that can be open through the site at the same time is reached, additional unauthenticated sessions can not be established.

### **Resolution**

If this event occurs on a regular basis, do one of the following:

- Verify that the defined threshold is not too low.
- Increase the number of unauthenticated sessions that can be open through the site, and raise the threshold accordingly.

You define those settings at the IAG, in the Configuration program, as follows:

1. Open the Advanced Trunk Configuration window of the relevant trunk, and access the Session tab.
2. Modify the required settings in the “Concurrent Unauthenticated Sessions Threshold” and “Max Concurrent Unauthenticated Sessions” fields, respectively.

## **Warning #I4: User Login Failed**

### **Symptoms**

A remote user attempts to access the site. Access is denied, and the following message is displayed in the browser window: “Failed to authenticate”.

## Cause

The failure can be caused by:

- Wrong credentials entered by the remote user, such as wrong user name or password, the user selecting the wrong Directory (authentication server) in the login page, and more.
- Authentication server is not configured correctly in the Configuration program. For example:
  - Invalid IP/host value or invalid port.
  - Server access credentials are not strong enough.
  - Groups/users search in the authentication server is defined inaccurately, thus the IAG cannot find a unique instance of the user name.
- Authentication server is not running.
- Authentication server is not reachable from the IAG.

The cause of the login failure is reported in the message, in the “Error” field.

## Resolution

Depending on the type of error, do one or more of the following:

- At the IAG, verify the configuration of the authentication server:
  1. In the Configuration program, on the **Admin** menu, click **Authentication and User/Groups Servers**.
  2. In the Authentication and User/Group Servers dialog box, select the relevant server, and click **Edit...**. For details on each of the parameters in the Edit Server dialog box, click **Help**.
- Verify that the authentication server is running.
- Verify that the authentication server is reachable from the IAG. If not, check the following:
  - Network connections
  - Verify the configuration of the ISA firewall rule that enables the connection from the IAG to the application server. For details, examine the ISA logs and alerts, and if necessary consult ISA troubleshooting.



## **Warning #15: Number of Max Concurrent Sessions Exceeded**

### **Symptoms**

A remote user attempts to log in to the site. Access is denied, and the following message is displayed in the browser window: “There are too many users on the web site at the moment. Please try to access the site again in a few minutes.”

### **Cause**

The maximal number of authenticated sessions that can be open through the site at the same time was reached.

### **Resolution**

If this event occurs on a regular basis, increase the number of sessions that can be open through the site:

1. In the Configuration program, open the Advanced Trunk Configuration window of the relevant trunk, and access the Session tab.
2. In the “Max Concurrent Sessions” field, increase the number of sessions that can be open through the site simultaneously.

## **Warning #16: Number of Max Concurrent Unauthenticated Sessions Exceeded**

### **Symptoms**

A remote user attempts to access the site. Access is denied, and the following message is displayed in the browser window: “There are too many users on the web site at the moment. Please try to access the site again in a few minutes.”

### **Cause**

The maximal number of unauthenticated sessions that can be open through the site at the same time was reached.

### **Resolution**

If this event occurs on a regular basis, increase the number of unauthenticated sessions that can be open through the site:

1. In the Configuration program, open the Advanced Trunk Configuration window of the relevant trunk, and access the Session tab.
2. In the “Max Concurrent Unauthenticated Sessions” field, increase the number of unauthenticated sessions that can be open through the site simultaneously.

## Warning #17: Request Too Long

### Symptoms

A remote user requests a page. The request is denied, and a message is displayed in the browser window, informing the user what part of the request is too long: URL, method, HTTP version, or Header section.

### Cause

The request is invalid since part of it is too long, as indicated in the message. The allowed length is:

- URL: 2,083 bytes
- Method: 32 bytes
- HTTP version: 16 bytes
- Header section: 2,048 bytes

### Resolution

Check the browser that was used to request the page.

## Warning #18: Invalid Request Version

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “Invalid HTTP request version”.

### Cause

The browser on the remote computer sent the request using an invalid HTTP protocol version.

### Resolution

Verify that the browser that was used to request the page is configured to use HTTP version 1.1 or 1.0. For example, in Internet Explorer 6.0, take the following steps:

1. On the **Tools** menu, click **Internet Options...**
2. In the Internet Options dialog box, select the Advanced tab. Under “HTTP 1.1. Settings”, verify that the option “Use HTTP 1.1” is selected.

## **Warning #19: Attempt to Sneak Source IP Data**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “An attempt to sneak source IP was detected”.

### **Cause**

The request contains a header or parameter that is identical to the header or parameter that is configured as the “Source IP key” header or parameter for this application. This could be an attempt to sneak data to the application server, using this header or parameter.

### **Resolution**

In order to avoid a situation where the header or parameter is used in “legal” requests, make sure you assign it a unique name, that will not be used for any other purpose. If the header or parameter name is unique, when it is used in a request, it is an indication that this is a malicious request, that should be blocked.

To define the “Source IP key” header or parameter for this application, take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application and access the Web Settings tab.
2. Under the option “Source IP key”, assign a unique header or parameter name.

For details, refer to “Web Settings Tab” on page 73.

## **Warning #20: Attempt to Sneak Negotiate Header**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “An attempt to sneak authorization info was detected”.

### **Cause**

The request contains a “negotiate” authorization header.

## Resolution

If you wish to cancel the blocking of “negotiate” authorization headers, take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window of the relevant trunk, and access the URL Inspection tab.
2. Uncheck the option “Block “Negotiate” Authorization Header”.



### Note

A “negotiate” authorization header sent by clients may contain malformed code, which could cause denial of service and browser crashes. This vulnerability was announced in Microsoft’s Security Bulletin MS04-011, as ASN.1 “Double Free” Vulnerability - CAN-2004-0123.

## Warning #22: Login On-The-Fly Failed

### Symptoms

A remote user attempts to add authentication credentials on-the-fly, for example, in order to access an application that requires different credentials than those used to access the site. The attempt fails, and the following message is displayed in the browser window: “Failed to authenticate”.

### Cause

The failure can be caused by:

- Wrong credentials entered by the remote user, such as wrong user name or password, the user selecting the wrong Directory (authentication server) in the login page, and more.
- Authentication server is not configured correctly in the Configuration program. For example:
  - Invalid IP/host value or invalid port.
  - Server access credentials are not strong enough.
  - Groups/users search in the authentication server is defined inaccurately, thus the IAG cannot find a unique instance of the user name.
- Authentication server is not running.
- Authentication server is not reachable from the IAG.

The cause of the login failure is reported in the message, in the “Error” field.

## Resolution

Depending on the type of error, do one or more of the following:

- Verify configuration of the authentication server on the IAG:
  1. Access the Configuration program, and on the **Admin** menu, click **Authentication and User/Groups Servers**.
  2. In the Authentication and User/Group Servers dialog box, select the relevant server, and click **Edit...**. For details on each of the parameters in the Edit Server dialog box, click **Help**.
- Verify that the authentication server is running.
- Verify that the authentication server is reachable from the IAG. If not, check the following:
  - Network connections
  - Verify the configuration of the ISA firewall rule that enables the connection from the IAG to the application server. For details, examine the ISA logs and alerts, and if necessary consult ISA troubleshooting.

## Warning #23: Application Form Authentication Failed

### Symptoms

A remote user attempts to access an application. The attempt fails.

### Cause

Despite the fact that, in the Configuration program, the application is configured to automatically reply to the application server's authentication request (HTML form), the login attempt failed. This can be caused by one of the following:

- The credentials that were used for the authentication were not accepted by the application. This can be due to one of the following reasons:
  - The authentication server used for the login does not contain the user credentials that are required by the application.
  - Incorrect configuration of the Form Authentication Engine for this application.
- The browser used by the remote user is not supported by the IAG; for a list of supported browsers refer to "Supported Browsers" on page 19.

## Resolution

Take the following steps:

- Verify that the correct authentication server is used to reply to the login request:
  1. In the Configuration program, access the application and open the Application Properties dialog box.
  2. Access the Web Settings tab. Verify that the authentication server that is selected for the option “Automatically Reply to Application-Specific Authentication Requests” contains the user credentials required by the application.

For details, refer to “Application Authentication” on page 74.

- Verify the configuration of the Form Authentication Engine for this application. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to Appendix C: “Form Authentication Engine”.

## Warning #24: Application Authentication Failed

### Symptoms

A remote user attempts to access an application. The attempt fails, and the following message is displayed: “You do not have permissions to view this Directory or page using the credentials you supplied.”

### Cause

The application is configured to automatically reply to the application’s authentication request (HTTP 401 request). The credentials supplied by the authentication server are not accepted by the application.

## Resolution

In the Configuration program, verify the configuration of the authentication server for this application:

1. Open the Application Properties dialog box and access the Web Settings tab.
2. Under the option “Automatically Reply to Application-Specific Authentication Requests”, verify that the selected authentication server is valid for this application.

For details, refer to “Web Settings Tab” on page 73.

## Warning #25: Failed to Send Message

### Symptoms

The IAG's Event Logging mechanism failed to send a message to a reporter, even though, in the Message Definitions file, the message is configured to be sent to this reporter, and the reporter is activated in the Configuration program.



#### Tip

For a description of the Message Definitions file, refer to “Event Logging Message Definitions File” on page 250.

### Cause

- Reporter is not configured correctly in the Configuration program.
- Reporter's server is not running.
- Reporter's server is not reachable from the IAG.

### Resolution

- Verify configuration of the reporter: in the Configuration program: on the **Admin** menu, click **Event Logging**, and, in the relevant tab, check the values of the reporter's parameters, such as the server's address or user credentials. For details, refer to “Optional Event Logging Configuration Steps” on page 239.
- Verify that the reporter's server is running.
- Verify that the reporter's server is reachable from the IAG. If not, check the following:
  - Network connections.
  - Verify the configuration of the ISA firewall rule that enables the connection from the IAG to the application server. For details, examine the ISA logs and alerts, and if necessary consult ISA troubleshooting.

## Warning #26: URL Changed

### Symptoms

During URL verification, the IAG filter changes the URL. The remote user's experience is not affected.

### Cause

The requested URL contains an illegal sequence of characters. For example: multiple slashes.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window of the relevant trunk and access the URL Inspection tab.
2. In the “Out-Of-The-Box Security Configuration” area, edit the application’s Legal Characters list to include the character that caused the error, as reported in the message, in the “Reason” field.  
For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “URL Inspection Tab—Out-Of-The-Box Security Configuration” on page 147.

## Error #29: Failed to Read Configuration

### Symptoms

The message is logged after you activate the Configuration program. The IAG is not functioning as expected, or is not functioning at all. Remote users might experience problems while working with the site, or might not be able to access the site at all.

### Cause

Problem with the configuration files of the module that failed. This might be caused by one or more of the following:

- Files were not modified through `CustomUpdate` folders.
- Files were modified through `CustomUpdate` folders, but the configuration settings are wrong.
- File incompatibility during system upgrade.

### Resolution

Verify that all modifications to the module’s default settings are performed according to the instructions provided in the IAG’s documentation-set.



## Warning #31: Global Out-Of-The-Box Rules

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL is blocked by the application’s Out-Of-The-Box Security Rules.”

### Cause

The requested URL contains an illegal character, according to the definition of the trunk’s global out-of-the-box security configuration.

### Resolution

If you wish to cancel the enforcement of global out-of-the-box security rules for this trunk, in the Configuration program, take the following steps:

1. Open the Advanced Trunk Configuration window of the relevant trunk and access the URL Inspection tab.
2. In the “Out-Of-The-Box Security Configuration” area, uncheck the option “Check Global Out-Of-The-Box Rules”.



#### Note

This option is global, and affects all the applications in the trunk.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “URL Inspection Tab—Out-Of-The-Box Security Configuration” on page 147.

## Warning #33: Invalid Request

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The page cannot be displayed”.

### Cause

The request is invalid, possibly since it contains too many headers. This could be caused by an IIS bug on the requesting client.

### Resolution

Check the browser used to request the page.

## Warning #34: Download Policy Size Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

### Cause

The response failed since the size of the transfer data renders it a download, and the application’s Download policy forbids downloads to the requesting endpoint.

### Resolution

In the Configuration program, do one of the following:

- If, for this application, you wish responses of this size to be considered regular responses, and not downloads, increase the size of data above which a response is considered a download, as follows:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Downloads” area, increase the size defined in “Identify by Size”.For details, refer to “Download/Upload Tab” on page 82.
- If you wish to cancel the identification of downloads by size for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Downloads” area, uncheck the option “Identify by Size”.



#### Note

If none of the options in the “Downloads” area are activated, no downloads from the application are blocked, regardless of the settings of the application’s Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application’s Download policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #35: Download Policy File Extension Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

### Cause

The response failed since its extension renders it a download, and the application’s Download policy forbids downloads to the requesting endpoint.

### Resolution

In the Configuration program, do one of the following:

- If, for this application, you wish responses with this extension to be considered regular responses, and not downloads, edit the application’s downloads Extension List, as follows:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Downloads” area, edit the Extension List accordingly.  
For details, refer to “Download/Upload Tab” on page 82.
- If you wish to cancel the identification of downloads by extensions for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Downloads” area, uncheck the option “Identify by Extensions”.



#### Note

If none of the options in the “Downloads” area are activated, no downloads from the application are blocked, regardless of the settings of the application’s Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application’s Download policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #36: Download Policy Violation - No Content-Type

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

### Cause

The response header does not contain a content-type. Responses without content-type are rendered a download, and the application’s Download policy forbids downloads to the requesting endpoint.

### Resolution

At the IAG, do one of the following:

- If you wish downloads without content-type to be considered regular responses, and not downloads, create the following Registry key:
  - **Location:** ...\\Whale-Com\\e-Gap\\Von\\UrlFilter
  - **DWORD Value name:** AllowResponseWithoutContentType
  - **DWORD Value data:** 1

After you create the key, access the Configuration program, activate the configuration, and select the option “Apply changes made to external configuration settings”.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application’s Download policy in the Configuration program.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #37: Download Policy Content-Type and Extension Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

## Cause

The response failed since its content-type and extension render it a download, and the application's Download policy forbids downloads to the requesting endpoint.

## Resolution

At the IAG, do one of the following:

- If you wish responses with this content-type to be considered regular responses, and not downloads, take the following steps:
  1. Access the file that holds the definitions of file extensions and the associated content-types:  
`...\Whale-Com\e-Gap\von\conf\content-types.ini`  
In this file, identify the extension associated with this content-type. If the file does not contain this content-type, add the appropriate extension/content-type pair to the file.
  2. In the Configuration program, edit the application's downloads Extension List so that the extension associated with this content-type is not considered a download. The list is defined in the Application Properties dialog box, in the Download/Upload tab, in the "Downloads" area. For details, refer to "Download/Upload Tab" on page 82.
- If you wish responses with this extension to be considered regular responses for this application, and not downloads, edit the application's downloads Extension List accordingly, as described in step 2, above.
- If you wish to cancel the identification of downloads by extensions for this application, uncheck the option "Identify by Extensions" in the "Downloads" area of the Download/Upload tab.



### Note

If none of the options in the "Downloads" area are activated, no downloads from the application are blocked, regardless of the settings of the application's Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application's Download policy in the Configuration program.
  - The application's policies are selected in the Application Properties dialog box, in the General tab. For details, refer to "General Tab" on page 68.

- Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #38: Download Policy Content-Type Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

### Cause

The response failed since its content-type renders it a download, and the application’s Download policy forbids downloads to the requesting endpoint.

### Resolution

At the IAG, do one of the following:

- If you wish responses with this content-type to be considered regular responses, and not downloads, take the following steps:
  1. Access the file that holds the definitions of file extensions and the associated content-types:  
`...\\Whale-Com\\e-Gap\\von\\conf\\content-types.ini`  
 In this file, identify the extension associated with this content-type. If the file does not contain this content-type, add the appropriate extension/content-type pair to the file.
  2. In the Configuration program, edit the application’s downloads Extension List so that the extension associated with this content-type is not considered a download. The list is defined in the Application Properties dialog box, in the Download/Upload tab, in the “Downloads” area. For details, refer to “Download/Upload Tab” on page 82.
- If you wish to cancel the identification of downloads by extensions for this application, uncheck the option “Identify by Extensions” in the “Downloads” area of the Download/Upload tab.



#### Note

If none of the options in the “Downloads” area are activated, no downloads from the application are blocked, regardless of the settings of the application’s Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application's Download policy in the Configuration program.
  - The application's policies are selected in the Application Properties dialog box, in the General tab. For details, refer to "General Tab" on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to "Application Endpoint Policies" on page 99.

## **Warning #39: Download Policy Violation - File Extension Unmatched**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: "According to your organization's Download policy, the requested download is not allowed."

### **Cause**

The response failed since its content-type does not match the file extension. This was discovered while checking whether the response is a download according to its file extension, since the application's Download policy forbids downloads to the requesting endpoint.

### **Resolution**

Do one of the following:

- If you wish this extension/content-type pair to be considered a match, take the following steps:
  1. At the IAG, access the file that holds the definitions of file extensions and the associated content-types:  
`...\Whale-Com\e-Gap\von\conf\content-types.ini`
  2. At the application server, access the file that holds the extension/content-type definitions.
  3. Verify that the association of extensions and content-types is consistent for both files. If you find discrepancies between the files, edit the file on the IAG to match the application server's file.
  4. At the IAG, in the Configuration program, verify that the application's downloads Extension List is configured so that the extension used here is not considered a download. The list is

defined in the Application Properties dialog box, in the Download/Upload tab, in the “Downloads” area. For details, refer to “Download/Upload Tab” on page 82.

- If you wish to cancel the identification of downloads by extensions for this application, uncheck the option “Identify by Extensions” in the “Downloads” area of the Download/Upload tab.



#### Note

If none of the options in the “Downloads” area are activated, no downloads from the application are blocked, regardless of the settings of the application’s Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application’s Download policy in the Configuration program.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #40: Download Policy URL Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Download policy, the requested download is not allowed.”

### Cause

The response failed since this URL is defined as a download URL for this application-type, and the application’s Download policy forbids downloads to the requesting endpoint.

### Resolution

In the Configuration program, do one of the following:

- In order for this request not to be considered a download for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.



2. In the “URL Settings” area, click **Configure** next to “Download URLs”.
3. In the Download URLs Settings dialog box, remove the corresponding rule.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Download URLs” on page 153.

- If you wish to cancel the identification of downloads by URLs for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Downloads” area, uncheck the option “Identify by URLs”.



#### Note

If none of the options in the “Downloads” area are activated, no downloads from the application are blocked, regardless of the settings of the application’s Download policy.

- If you wish to enable downloads from the application to the requesting endpoint, edit the application’s Download policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #41: Upload Policy URL Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Upload policy, the requested upload is not allowed.”

### Cause

The request failed since this URL is defined as an upload URL for this application-type, and the application’s Upload policy forbids uploads from the submitting endpoint.



#### Tip

The portion of the URL that caused the failure is indicated in the message, in the “URL” parameter.

## Resolution

In the Configuration program, do one of the following:

- In order for this request not to be considered an upload for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.
  2. In the “Upload URLs” list, access the corresponding rule, and do one of the following:
    - If required, click **Edit...**, and use the Edit Upload URLs dialog box to change the URL or the method, as applicable.
    - If you wish this URL to be considered an upload only if it contains attachments, in the Edit Upload URLs dialog box, activate the option “Check for Attachments in Content”.
    - If the URL failed on parameters, in the Edit Upload URLs dialog box, either configure the rule so that parameters are not checked, or change the method that is used to check parameters, as applicable.
    - If you wish the URL to always be considered a regular request, and not an upload, remove it from the “Upload URLs” list.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Upload URLs” on page 155.

- If you wish to cancel the identification of uploads by URLs for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Uploads” area, uncheck the option “Identify by URLs”.



### Note

If none of the options in the “Uploads” area are activated, no uploads to the application are blocked, regardless of the settings of the application’s Upload policy.

- If you wish to enable uploads from the submitting endpoint to the application, edit the application’s Upload policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #42: Upload Policy Size Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Upload policy, the requested upload is not allowed.”

### Cause

The request failed since the size of the transfer data render it an upload, and the application’s Upload policy forbids uploads from the submitting endpoint.

### Resolution

In the Configuration program, do one of the following:

- If you wish requests of this size to be considered regular requests, and not uploads, increase the size of data above which a request from this application is considered an upload:
  1. Open the Application Properties dialog box, and access the Download/Upload tab.
  2. In the “Uploads” area, increase the size defined in “Identify by Size”.

For details, refer to “Download/Upload Tab” on page 82.

- If you wish to cancel the identification of uploads by size for this application, uncheck the option “Identify by Size” in the “Uploads” area of the Download/Upload tab.



#### Note

If none of the options in the “Uploads” area are activated, no uploads to the application are blocked, regardless of the settings of the application’s Upload policy.

- If you wish to enable uploads from the requesting endpoint, edit the application’s Upload policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #43: Upload Policy File Extension Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Upload policy, the requested upload is not allowed.”

### Cause

The request failed since its extension renders it an upload, and the application’s Upload policy forbids uploads from the submitting endpoint.

### Resolution

In the Configuration program, do one of the following:

- If, for this application, you wish requests with this extension to be considered regular requests, and not uploads, edit the application’s uploads Extension List, as follows:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Uploads” area, edit the Extension List accordingly. For details, refer to “Download/Upload Tab” on page 82.
- If you wish to cancel the identification of uploads by extensions for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Uploads” area, uncheck the option “Identify by Extensions”.



#### Note

If none of the options in the “Uploads” area are activated, no uploads to the application are blocked, regardless of the settings of the application’s Upload policy.

- If you wish to enable uploads from the submitting endpoint to the application, edit the application’s Upload policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #44: Failed to Create Parameter List

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL you are trying to access contains an illegal parameter.”

### Cause

The URL query string or the POST data parameters of the requested URL are illegal, due to one of the following reasons:

- They contain an illegal character, according to the definition of the application’s Out-Of-The-Box Security Configuration.
- The IAG filter failed to construct a legal parameter list from the URL query string or from POST data parameters. For example: a parameter that contains only a value, with no name.

### Resolution

Use the Configuration program to determine whether the failure was caused by an illegal character or by an illegal parameter list:

1. Open the Application Properties dialog box, and access the Web Settings tab.
2. Uncheck the option “Check Out-Of-The-Box Rules”. For details, refer to “Web Settings Tab” on page 73.
3. Request the URL again, and observe whether the request is accepted or not:
  - If the request does not fail this time, it is an indication that the failure was caused by an illegal character.
  - If the request fails again, it is an indication that the failure is caused by the filter failing to construct a legal parameter list from the URL query string or from POST data parameters.

According to the reason of the failure, take the steps listed below to resolve the problem. Before you do so, in the Web Settings tab, **check** the option “Check Out-Of-The-Box Rules”, so that it is activated again.

***If the failure was caused by an illegal character, take the following steps:***

1. On the IAG, activate a trace that will record the IAG filter activities:
  - a) Access the following file:  
...\\Whale-Com\\e-Gap\\common\\conf\\trace.ini

- b) Add the following section to the file:
 

```
[Trace\WhlFilter\WHLFILTRULESET]
*=xheavy
```

 Save the file.
2. Use a browser to request the URL again.
3. Locate the log file of the trace you activated, in the following location:
 

```
...\Whale-Com\e-Gap\logs
```

 The log file is named as follows:
 

```
WhlFilter.default.<Time_Stamp>.log
```
4. In the trace log file, find the following warning message:
 

```
WARN: CanonicalizeEscapeChar(): Check allowed characters
after escape list in Param. String=<FailedString> failed
```

 Where <FailedString> is a parameter that contains one or more illegal characters, which caused the failure.



#### Tip

For more information on the tracing process, see “Error Logging and Process Tracing” on page 307.

5. At the Configuration program, open the Advanced Trunk Configuration window and access the URL Inspection tab.
6. In the “Out-Of-The-Box Security Configuration” area, edit the application’s rule so that the list of Legal Characters includes all the characters found in the parameter that caused the error. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “URL Inspection Tab—Out-Of-The-Box Security Configuration” on page 147.
7. When you are finished with the tracing, de-activate the trace you activated in step 1, by deleting or commenting-out the trace definition.

***If the failure was caused by an illegal parameter list, take the following steps:***

1. At the Web Monitor, look at the description of the Warning message. In the “Parameter List” field, check whether all parameters are “legal”, that is, each parameter consists of a parameter name/parameter value pair.
2. If one or more of the parameters are “illegal”, check the requesting browser.

## Warning #45: Bad Parameter in URL

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL you are trying to access contains an illegal parameter.”

### Cause

The requested URL was rejected by a URL Inspection rule since one of its parameters renders the request invalid.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and select the URL Set tab.
2. In the URL List, select the rule that caused the failure, according to the details provided in the message.
3. In the Parameter List, edit the rule of the parameter that caused the error.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## Warning #46: Mandatory Parameter Missing from URL

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL you are trying to access contains an illegal parameter.”

### Cause

The requested URL was rejected by a URL Inspection rule since a mandatory parameter is missing from the URL.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and select the URL Set tab.

2. In the URL List, select the rule that caused the failure, according to the details provided in the message.
3. In the Parameter List, select the rule of the parameter that caused the error. In the “Existence” column select “Optional”, so that the missing parameter is optional, not mandatory.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## **Warning #47: POST without Content-Type not Allowed**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The upload is blocked since the request does not contain a Content-Type header.”

### **Cause**

The request does not contains a Content-Type header, and the method used in the request is POST. According to the configuration of the IAG, POST without a Content-Type header is not allowed.

### **Resolution**

In order to allow POST requests without a Content-Type header for this application, take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application, and select the Web Settings tab.
2. Check the option “Allow POST without Content-Type”.

For details, refer to “Web Settings Tab” on page 73.

## **Warning #48: Application Out-Of-The-Box Rule**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL is blocked by the application’s Out-Of-The-Box Security Rules.”

### **Cause**

The requested URL contains an illegal character, according to the definition of the application’s out-of-the-box security configuration.



## Resolution

In the Configuration program, do one of the following:

- If you wish the character that caused the error to be considered a legal character for this application, take the following steps:
  1. Open the Advanced Trunk Configuration window of the relevant trunk and access the URL Inspection tab.
  2. In the “Out-Of-The-Box Security Configuration” area, edit the application’s Legal Characters list to include the character that caused the error, as reported in the message, in the “Reason” field.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “URL Inspection Tab—Out-Of-The-Box Security Configuration” on page 147.

- If you wish to cancel out-of-the-box security checks for this application, take the following steps:
  1. Open the Application Properties dialog box, and access the Web Settings tab.
  2. Uncheck the option “Check Out-Of-The-Box Rules”.

For details, refer to “Web Settings Tab” on page 73.

## Warning #49: Unknown Application

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You are not authorized to access this application. For assistance, please contact your system administrator.”

### Cause

Wrong configuration of the application in the Configuration program.

## Resolution

Take the following steps in the Configuration program:

1. Use the Application Properties dialog box to locate the application, according to the server configuration in the Web Servers tab.
2. Verify the configuration of the server’s addresses, paths, and ports for this application.

For details, refer to “Web Servers Tab” on page 71.

## Warning #50: Method not Defined

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The page cannot be displayed. Ruleset configuration invalid.”

### Cause

The URL Inspection rule defined for this URL does not specify a method.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and access the URL Set tab.
2. In the URL List, access the rule that caused the request to fail, and, in the “Methods” column, assign a method or methods for this URL.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## Warning #51: Invalid Method

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. You are trying to access the URL using an illegal method.”

### Cause

According to the configuration of the application’s URL Inspection ruleset, the method used to send the request is not valid for requested URL.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and access the URL Set tab.
2. In the URL List, access the rule that caused the request to fail, and, in the “Methods” column, assign the appropriate method for this URL.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## **Warning #52: Data not Allowed with Method**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. WebDAV methods are not allowed.”

### **Cause**

The request uses a WebDAV method, while attempting to send data to the application. According to the configuration of the application, such requests are not allowed.

### **Resolution**

Take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application, and select the Web Settings tab.
2. Activate the option “Allow WebDAV Methods”.

For details, refer to “Web Settings Tab” on page 73.

## **Warning #53: File Upload Forbidden**

### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Upload policy, the requested upload is not allowed.”

### **Cause**

The request failed since when it contains attachments it is considered an upload URL, and the application’s Upload policy forbids uploads from the submitting endpoint.

### **Resolution**

In the Configuration program, do one of the following:

- In order for this request not to be considered an upload for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.
  2. In the “URL Settings” area, click **Configure...** next to “Upload URLs”.
  3. In the Upload URLs Settings dialog box, remove the corresponding rule.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Upload URLs” on page 155.

- If you wish to cancel the identification of uploads by URLs for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Download/Upload tab.
  2. In the “Uploads” area, uncheck the option “Identify by URLs”.



#### Note

If none of the options in the “Uploads” area are activated, no uploads to the application are blocked, regardless of the settings of the application’s Upload policy.

- If you wish to enable uploads from the submitting endpoint to the application, edit the application’s Upload policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #54: Failed XML Integrity Verification

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The page cannot be displayed. The request failed the XML Integrity verification.”

### Cause

The request failed the inspection of XML integrity in HTTP data.

### Resolution

If you wish to cancel the inspection of XML integrity in HTTP data for this application, take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application, and select the Web Settings tab.
2. Uncheck the option “Check XML Integrity”.

For details, refer to “Web Settings Tab” on page 73.

## Warning #55: Parameters not Allowed with URL

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL you are trying to access contains an illegal parameter.”

### Cause

According to the configuration of the application’s ruleset, the requested URL is not allowed to contain parameters.

### Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and select the URL Set tab.
2. In the URL List, access the rule that caused the failure, according to the details provided in the message. In the “Parameters” column select either “Handle” or “Ignore”, so that parameters are not rejected. Note that, if you set the value of “Parameters” to “Handle”, you also have to define the parameters for this URL.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## Warning #57: Unrecognized Application

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You are not authorized to access this application. For assistance, please contact your system administrator.”

### Cause

Wrong configuration of the application in the Configuration program.

### Resolution

Take the following steps in the Configuration program:

1. Use the Application Properties dialog box to locate the application, according to the server configuration in the Web Servers tab.

2. Verify the configuration of the server's addresses, paths, and ports for this application.

For details, refer to “Web Servers Tab” on page 71.

### **Warning #58: Unresolved Request**

#### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The requested URL is not associated with any configured application.”

#### **Cause**

The requested URL contains a signature that cannot be resolved to identify the requested application server.

#### **Resolution**

Contact technical support.

### **Warning #59: Invalid Reroute Destination**

#### **Symptoms**

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “The requested URL is not associated with any configured application.”

#### **Cause**

The URL that the user requested was rerouted according to a “Manual URL Replacement” rule, and the destination server is not recognized by the IAG filter.

#### **Resolution**

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and select the Application Access Portal tab.
2. In the “Manual URL Replacement” area, edit the applicable rule.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Manual URL Replacement” on page 272.

## Warning #62: Unauthorized Access Attempt

### Symptoms

A remote user attempts to access an application from the portal homepage. The request is denied, and the following message is displayed in the browser window: “You are not authorized to access the application.”

### Cause

The user is not authorized to view or access the requested application.

### Resolution

- Change the authorization settings for this application.
- If you are using the default portal homepage that is supplied with the IAG, you can personalize the application so that the link to the application is not displayed on the homepage of users that are not authorized to access the application.

Authorization and personalization of an application are defined in the Configuration program, in the Authorization tab of the Application Properties dialog box. For details, refer to “Users Setup” on page 32.

## Warning #64: Application Access Policy Violation

### Symptoms

A remote user attempts to access an application from the portal homepage. The request is denied, and the following message is displayed in the browser window: “Your computer does not meet the security policy requirements of this application.”

### Cause

The requesting endpoint does not comply with the requirements of the application’s Access policy.

### Resolution

Instruct the user what steps have to be taken in order for the endpoint to comply with the policy. You can view the definitions of the policy in the Configuration program, in the Policy Editors.

To access the Policy Editors, take the following steps in the Configuration program:

1. Open the Application Properties dialog box, and select the General tab.
2. In the “Endpoint Policies” area click **Edit Policies...**
3. In the Policies dialog box, select the applicable policy and click **Edit...**

For more details, refer to “Endpoint Policies” on page 93.

## Warning #65: Session Access Policy Violation

### Symptoms

A remote user attempts to access the portal homepage or site. The request is denied, and the following message is displayed in the browser window: “Your computer does not meet the security policy requirements of this site.”

### Cause

The requesting endpoint does not comply with the requirements of the trunk’s Session Access Policy.

### Resolution

Instruct the user what steps have to be taken in order for the endpoint to comply with the policy. You can view the definitions of the policy in the Configuration program, in the Policy Editors.

To access the Policy Editors, take the following steps in the Configuration program:

1. Open the Application Properties dialog box, and select the General tab.
  2. In the “Endpoint Policies” area click **Edit Policies...**
  3. In the Policies dialog box, select the applicable policy and click **Edit...**
- For more details, refer to “Endpoint Policies” on page 93.

## Warning #66: Attempt to Sneak Authorization Data

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “An attempt to sneak authorization info was detected.”

### Cause

The request contains a header or parameter that is identical to the header or parameter that is configured as the “Authorization key” header or parameter for this application. This could be an attempt to sneak data to the application server, using this header or parameter.



## Resolution

In order to avoid a situation where the header or parameter is used in “legal” requests, make sure you assign it a unique name, that will not be used for any other purpose. If the header or parameter name is unique, when it is used in a request, it is an indication that this is a malicious request, that should be blocked.

To define the “Authorization key” header or parameter for this application, take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application and access the Web Settings tab.
2. Under the option “Authorization key”, assign a unique header or parameter name.

For details, refer to “Web Settings Tab” on page 73.

## Warning #67: URL Path not Allowed

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “You have attempted to access a restricted URL. The URL you are trying to access contains an illegal path.”

### Cause

The path of the requested URL was rejected by the URL Inspection engine.

## Resolution

Take the following steps in the Configuration program:

1. Open the Advanced Trunk Configuration window, and select the URL Set tab.
2. Do one of the following, depending on the rule that caused the failure, as specified in the “Description” field of the message:
  - If the rule that caused the failure is “Default rule”, use the URL List to add a new rule, or edit one of the existing rules, so that the requested URL is allowed.
  - If the failure was caused by an existing rule, and the name of the rule is specified in the message’s “Description” field, access the rule in the URL List. In the “URL” column, edit the path of the URL.

For details about the configuration of rulesets, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Configuring a Ruleset in the URL Set Tab” on page 164.

## Error #73: Connection to Non-Web Application Failed

### Symptoms

A remote user attempts to launch an SSL Wrapper application, either via the portal homepage, or by logging into a site that automatically launches the application. The application is launched, but fails to connect to the server.

### Cause

The IAG can not establish a connection with the application server. The failure can be caused by one of the following:

- Application server is not configured correctly in the Configuration program. For example: an invalid IP address, port, or path.
- Application server is not running.
- Application server is not reachable from the IAG.

The cause of the login failure is reported in the message, in the “Error” field.

### Resolution

- Verify the configuration of the application server in the Configuration program, in the Application Properties dialog box, in the Server Settings tab. For details, refer to “Server Settings Tab” on page 85.
- Verify that the application server is running.
- Verify that the application server is reachable from the IAG. If not, check the following:
  - Network connections
  - Verify the configuration of the ISA firewall rule that enables the connection from the IAG to the application server. For details, examine the ISA logs and alerts, and if necessary consult ISA troubleshooting.

## Warning #76: Failed to Start Application

### Symptoms

A remote user attempts to launch an SSL Wrapper application, either via the portal homepage, or by logging into a site that automatically launches the application. The request is denied, and a message is displayed, informing the user that the server failed to execute the application.

### Cause

The IAG failed to load and initialize the application profile from the Configuration program. The cause for the error is reported in the message, in the “Error” field. It can be due to incorrect configuration of the application server in the Configuration program. For example: an invalid IP address, port, or path.

### Resolution

Verify the configuration of the application server in the Configuration program, in the Application Properties dialog box, in the Server Settings tab. For details, refer to “Server Settings Tab” on page 85.

## Warning #77: Unauthorized Access Attempt

### Symptoms

A remote user attempts to launch an SSL Wrapper application, either via the portal homepage, or by logging into a site that automatically launches the application. The request is denied, and the following message is displayed: “Access to the requested resource denied”.

### Cause

The requested server is not defined as an application in the Configuration program, or the client executable is not authorized to access the server.

### Resolution

The resolution depends on the error that is displayed in the long description of the message, in the “Error” field:

- The message “Access denied (unknown server)” indicates that the user requested a server that is not defined as an application server in the Configuration program. In this case, do one of the following:
  - In the Configuration program, verify the configuration of the application servers in the Application Properties dialog box, in the Server Settings tab. For details, refer to “Server Settings Tab” on page 85:
    - For Portal trunks: in the Application Properties dialog box, in the Server Settings tab.
    - For Webmail trunks: in the Advanced Trunk Configuration window, in the Server Settings tab.
  - If the user attempted to connect to the application by manually entering the server address, verify that the user tried to connect to the correct server.
  - On the endpoint computer, verify the configuration of the server settings in the client application.

- The message “Invalid application process...” is applicable for Portal trunks only. It indicates that the executable that runs the application on the client, and attempted to access the application server, is not authorized to access this application. In this case, in the Configuration program, in the Application Properties dialog box, in the Client Settings tab, verify the configuration of the option “Bind Tunnel to Client Executable” (Client Executable and Signature). For details, refer to “Client Settings Tab” on page 86.

## **Error #79: Connection to Web Application Failed**

### **Symptoms**

A remote user attempts to access an application from the portal homepage. The request is denied, and the following message is displayed in the browser window: “The page cannot be displayed”.

### **Cause**

The IAG can not establish a connection with the application server. The failure can be caused by one of the following:

- Application server is not configured correctly in the Configuration program. For example: an invalid IP address, port, or path.
- Application server is not running.
- Application server is not reachable from the IAG.

The cause of the login failure is reported in the message, in the “Error” field.

### **Resolution**

- Verify the configuration of the application server in the Configuration program as follows:
  - For Portal trunks: in the Application Properties dialog box, in the Web Servers tab. For details, refer to “Web Servers Tab” on page 71.
  - For Webmail or Basic trunks: in the “Application Server” area of the Configuration pane.
- Verify that the application server is running.
- Verify that the application server is reachable from the IAG. If not, check the following:
  - Network connections
  - Verify the configuration of the ISA firewall rule that enables the connection from the IAG to the application server. For details, examine the ISA logs and alerts, and if necessary consult ISA troubleshooting.

## Warning #81: User Failed to Change Password

### Symptoms

A remote user attempts to change the password. The attempt fails, and one of the following messages is displayed in the browser window:

“Failed to change password.”

Or,

“The new password you entered cannot be used, since it does not comply with the password policy set by your administrator.”

### Cause

- The message “Failed to change password” indicates one of the following:
  - User entered the wrong password in the “Old password” field.
  - Settings of the Configuration program or the authentication server, which are required in order to enable users to change their passwords, are not configured correctly.
- The message “The new password you entered cannot be used, since it does not comply with the password policy set by your administrator” indicates that the user attempted to use a password that does not comply with the authentication server’s password policy, such as password length, complexity, or history.

### Resolution

Depending on the message the user receives, and the error indicated in the message, do one of the following:

- Take the steps required in order to enable users to change their passwords, as detailed in the *Intelligent Application Gateway Advanced Configuration* guide, in “Change Password Requirements” on page 93.
- Advise the user of the relevant password policy.

## Warning #82: Unauthorized Access Attempt

### Symptoms

A remote user attempts to launch an SSL Wrapper application, either via the portal homepage, or by logging into a site that automatically launches the application. The request is denied, and the following message is displayed: “Access to the requested resource denied”.

### Cause

Internal error.

### Resolution

If this event occurs on a regular basis, contact technical support.

## Warning #83: Form Login Response Failed

### Symptoms

A remote user attempts to access an application. The attempt might fail.

### Cause

The application is configured so that the Form Authentication Engine automatically replies to the application's authentication requests. The evaluation of the login attempt result failed.

### Resolution

Verify the configuration of the Form Authentication evaluator for this application.

- For a description of the Form Authentication Engine, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to Appendix C: "Form Authentication Engine".
- The evaluator is defined in the <LOGIN\_EVALUATOR> element. The failure is most likely caused by the <HEADER> sub-element.

## Warning #87: Service Policy Manager Login Failed

### Symptoms

When attempting to log in to the Service Policy Manager program, the login fails and the following message is displayed: "Incorrect Password".

### Cause

Incorrect password used.

### Resolution

Log in using the correct password. If you forgot the password, you can assign a new password for the Service Policy Manager program as follows:

- At the IAG, delete the following file:  
`...\Whale-Com\e-Gap\common\conf\auth.sec`

*When you next access the Service Policy Manager, you are prompted to assign a new password.*



#### **Note**

- The password must contain at least six digits.
- Changing the password in this manner is global, and affects the Configuration program, as well.

## **Warning #91: Passphrase Entry Failed**

### **Symptoms**

The IAG administrator is prompted to enter a passphrase while working with the IAG, for example, when activating the configuration. After submitting the passphrase, a message informs the administrator that the passphrase is incorrect.

### **Cause**

Incorrect passphrase used.

### **Resolution**

Enter the correct passphrase.

## **Warning #93: HTTP Request Smuggling (HRS) Attempt**

### **Symptoms**

A remote user attempts to access an application from the portal homepage. The request is denied, and the following message is displayed in the browser window: “HTTP Request Smuggling (HRS) attempt detected”.

### **Cause**

The request is suspected as being an HRS attack, as indicated by its method, content-type, and length.

### **Resolution**

To define this request as “legal” for this application, take the following steps in Configuration program:

1. Open the Application Properties dialog box for this application and access the Web Server Security tab.
2. If the option “Activate Smuggling Protection” is not already activated, activate it.

**Caution**

Activate this option only for servers that are vulnerable to HRS attacks, such as IIS 5.0 based servers. Activating this option unnecessarily or configuring it inaccurately might result in application malfunction.

3. Configure the option to enable the request by doing one or both of the following:
  - Add the request's content-type to the "Content-Types" list.
  - Define the "Max HTTP Body Size" option to be equal to or larger than the size of the request.

For details, refer to "Web Server Security Tab" on page 78.

**Warning #94: Unencrypted Cookie Name****Symptoms**

A remote user requests a page. The request is processed and the user experience is unaffected. However, a "Cookie" header in the request is blocked, and is not forwarded to the server.

**Cause**

A cookie encryption violation was detected. The cookie name is not encrypted, and is not listed in the cookie encryption exclude lists.

**Resolution**

In order to enable the browser to send this cookie in an unencrypted from, you need to add it to the list of cookies that are excluded from the cookie encryption process. Take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application and access the Cookie Encryption tab.
2. Add the cookie that was blocked to the "Cookies" list. The name of the cookie is provided in the "Description" field of the event in the Web Monitor's Event Viewer.

For details, refer to "Cookie Encryption Tab" on page 80.

**Warning #95: Cookie Name Cannot be Decrypted****Symptoms**

A remote user requests a page. The request is processed and the user experience is unaffected. However, a "Cookie" header in the request is blocked, and is not forwarded to the server.



### Cause

A cookie encryption violation was detected. An encrypted cookie name could not be decrypted since it contains an invalid security digest.

### Resolution

In the browser that was used to request the page, delete the cookie that was blocked. The name of the cookie is provided in the “Description” field of the event in the Event Viewer.

## Warning #96: Name of “Excluded” Cookie is Encrypted

### Symptoms

A remote user requests a page. The request is processed and the user experience is unaffected.

### Cause

A cookie encryption violation was detected. The cookie name is encrypted, although it is listed in one or more of the cookie encryption exclude lists.

### Resolution

In order to enable the browser to send this cookie in an encrypted form, you need to remove it from the list of cookies that are excluded from the cookie encryption process, as follows:

1. Use the IAG’s trace mechanism to resolve the original name of the encrypted cookie:
  - a) At the IAG, access the trace configuration file:  
`...\Whale-Com\e-Gap\Common\Config\trace.ini`
  - b) Add the following lines to the file:  
`[Trace\WhlFilter\WHLFLTSECUREREMOTE]`  
`*=xheavy`  
Save the file.
  - c) Use a browser to request the URL that caused the Warning message, as detailed in the “Description” field of the event in the Web Monitor’s Event Viewer.
  - d) At the IAG, access the trace log file in the following location:  
`...\Whale-Com\e-Gap\logs`  
The file is named:  
`<Server_Name>.WhlFilter.default.<Time_Stamp>.log`

Resolve the original name of the cookie that was blocked using the “EncryptedName” and “OrigName” parameters in the log file; the encrypted cookie name is indicated in the “Description” field of the event in the Event Viewer.

2. In order to exclude the cookie from the cookie encryption process, remove it from the exclude list where it is defined. Two lists define the exclusion of cookies from the process; both are configured at the IAG:
  - Per-application list. The cookies that are listed here are excluded from the process for this application only. To edit this list, in the Configuration program, open the Application Properties dialog box for this application, access the Cookie Encryption tab, and remove the cookie from the “Cookies” list.  
For details, refer to “Cookie Encryption Tab” on page 80.
  - Global list. The cookies that are listed here are excluded from the process for all applications. To edit this list, access the following file:  
...\\Whale-Com\\e-Gap\\Von\\Conf\\WhlExcludeCookie.xml  
Copy the file into a CustomUpdate subfolder, and remove the cookie from the list under the tag <EXCLUDE\_COOKIE\_LIST>. Note that cookie names are defined using regular expressions.  
For details, refer to “Global Exclude List” on page 82.

## **Warning #97: Cookie Encryption Mismatch**

### **Symptoms**

A remote user requests a page. The request is processed and the user experience is unaffected. However, a “Cookie” header in the request is blocked, and is not forwarded to the server.

### **Cause**

A cookie encryption violation was detected. The cookie name is encrypted, while the cookie value is unencrypted.

### **Resolution**

In the browser that was used to request the page, delete the cookie that was blocked. The name of the cookie is provided in the “Description” field of the event in the Web Monitor’s Event Viewer.

## **Warning #98: Cookie Value Cannot be Decrypted**

### **Symptoms**

A remote user requests a page. The request is processed and the user experience is unaffected. However, a “Cookie” header in the request is blocked, and is not forwarded to the server.

### **Cause**

A cookie encryption violation was detected. An encrypted cookie value could not be decrypted since it contains an invalid security digest.

### **Resolution**

In the browser that was used to request the page, delete the cookie that was blocked. The name of the cookie is provided in the “Description” field of the event in the Web Monitor’s Event Viewer.

## **Warning #99: Name of “Included” Cookie not Encrypted**

### **Symptoms**

A remote user requests a page. The request is processed and the user experience is unaffected. However, a “Cookie” header in the request is blocked, and is not forwarded to the server.

### **Cause**

A cookie encryption violation was detected. The cookie name is not encrypted, although it is listed in the cookie encryption include list.

### **Resolution**

In order to enable the browser to send this cookie in an unencrypted form, you need to remove it from the list of cookies that are included in the cookie encryption process. Take the following steps in the Configuration program:

1. Open the Application Properties dialog box for this application and access the Cookie Encryption tab.
2. Remove the cookie that was blocked from the “Cookies” list. The name of the cookie is provided in the “Description” field of the event in the Web Monitor’s Event Viewer.

For details, refer to “Cookie Encryption Tab” on page 80.

## Warning #100: Encrypted Cookie Name

### Symptoms

A remote user requests a page. The request is processed and the user experience is unaffected.

### Cause

A cookie encryption violation was detected. The cookie name is encrypted, but is not listed in the cookie encryption include list.

### Resolution

In order to enable the browser to send this cookie in an encrypted form, you need to add it to the list of cookies that are included in the cookie encryption process, as follows:

1. Use the IAG's trace mechanism to resolve the original name of the encrypted cookie:
    - a) At the IAG, access the trace configuration file:  
`...\Whale-Com\e-Gap\Common\Conf\trace.ini`
    - b) Add the following lines to the file:  
`[Trace\WhlFilter\WHLFILTSECUREREMOTE]`  
`*=xheavy`  
Save the file.
    - c) Use a browser to request the URL that caused the Warning message, as detailed in the "Description" field of the event in the Event Viewer.
    - d) At the IAG, access the trace log file in the following location:  
`...\Whale-Com\e-Gap\logs`  
The file is named:  
`<Server_Name>.WhlFilter.default.<Time_Stamp>.log`  
Resolve the original name of the cookie that was blocked using the "EncryptedName" and "OrigName" parameters in the log file; the encrypted name is indicated in the "Description" field of the event in the Web Monitor's Event Viewer.
  2. Still at the IAG, in the Configuration program, open the Application Properties dialog box for this application and access the Cookie Encryption tab.
  3. Add the cookie that was blocked to the "Cookies" list.
- For details, refer to "Cookie Encryption Tab" on page 80.

## Warning #101: Cookie Size Too Big

### Symptoms

None.

### Cause

A cookie encryption violation was detected. The size of the encrypted “Set-Cookie” header exceeds the 4 KB limit.

### Resolution

In order to exclude this cookie from the cookie encryption process, take the following steps:

1. Use the IAG’s trace mechanism to resolve the original name of the encrypted cookie:
  - a) At the IAG, access the trace configuration file:  
`...\Whale-Com\e-Gap\Common\Conf\trace.ini`
  - b) Add the following lines to the file:  
`[Trace\WhlFilter\WHLFILTSECUREREMOTE]`  
`*=xheavy`  
Save the file.
  - c) Use a browser to request the URL that caused the Warning message, as detailed in the “Description” field of the event in the Web Monitor’s Event Viewer.
  - d) At the IAG, access the trace log file in the following location:  
`...\Whale-Com\e-Gap\logs`  
The file is named:  
`<Server_Name>.WhlFilter.default.<Time_Stamp>.log`  
Resolve the original cookie name using the “EncryptedName” and “OrigName” parameters in the log file; the encrypted name is indicated in the “Description” field of the event in the Event Viewer.
2. Still at the IAG, in the Configuration program, open the Application Properties dialog box for this application and access the Cookie Encryption tab.
3. In order to exclude the cookie from the cookie encryption process, do one of the following:
  - If the encryption mode is “Include”, remove the cookie that was blocked from the “Cookies” list.
  - If the encryption mode is “Exclude”, add the cookie that was blocked to the “Cookies” list.

For details, refer to “Cookie Encryption Tab” on page 80.

## Warning #105: Restricted Zone Policy URL Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Restricted Zone policy, the requested URL is not allowed.”

### Cause

The request failed since this URL is defined as a restricted zone URL for this application-type, and the application’s Restricted Zone policy forbids access to the zone from this endpoint.

### Resolution

In the Configuration program, do one of the following:

- In order for this URL not to be part of the restricted zone for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.
  2. In the “Restricted Zone URLs” list, select the corresponding rule, and do one of the following:
    - Click **Edit...**, and use the Edit Restricted Zone URLs dialog box to change the URL or the method, as applicable.
    - If you wish the URL not to be part of the restricted zone, remove it from the “Restricted Zone URLs” list.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Restricted Zone URLs” on page 158.

- If you wish to disable the Restricted Zone feature for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Web Settings tab.
  2. Uncheck the option “Activate Restricted Zone”.
- If you wish to enable access to the restricted zone from the submitting endpoint, edit the application’s Restricted Zone policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #106: Restricted Zone Policy Parameters Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Restricted Zone policy, the requested URL is not allowed.”

### Cause

The request failed since this URL is defined as a restricted zone URL for this application-type, and the application’s Restricted Zone policy forbids access to the zone from this endpoint.

### Resolution

In the Configuration program, do one of the following:

- In order for this URL not to be part of the restricted zone for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.
  2. In the “Restricted Zone URLs” list, select the corresponding rule, and do one of the following:
    - Click **Edit...**, and, in the Edit Restricted Zone URLs dialog box, either configure the rule so that parameters are not checked, or change the method that is used to check parameters, as applicable.
    - If you wish the URL not to be part of the restricted zone, remove it from the “Restricted Zone URLs” list.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Restricted Zone URLs” on page 158.

- If you wish to disable the Restricted Zone feature for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Web Settings tab.
  2. Uncheck the option “Activate Restricted Zone”.
- If you wish to enable access to the restricted zone from the submitting endpoint, edit the application’s Restricted Zone policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.

## Warning #107: Restricted Zone Policy Upload File Violation

### Symptoms

A remote user requests a page. The request is denied, and the following message is displayed in the browser window: “According to your organization’s Restricted Zone policy, the requested URL is not allowed.”

### Cause

The request failed since this URL is defined as a restricted zone URL for this application-type, and the application’s Restricted Zone policy forbids access to the zone from this endpoint.

### Resolution

In the Configuration program, do one of the following:

- In order for this URL not to be part of the restricted zone for this application-type, take the following steps:
  1. Open the Advanced Trunk Configuration window and access the Global URL Settings tab.
  2. In the “Restricted Zone URLs” list, select the corresponding rule, and do one of the following:
    - If you wish this URL to be considered a restricted zone only if it contains attachments, click **Edit...**, and, in the Edit Forbidden URLs dialog box, activate the option “Check for Attachments in Content”.
    - If you wish the URL not to be part of the restricted zone, remove it from the “Restricted Zone URLs” list.

For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to “Restricted Zone URLs” on page 158.

- If you wish to disable the Restricted Zone feature for this application, take the following steps:
  1. Open the Application Properties dialog box and access the Web Settings tab.
  2. Uncheck the option “Activate Restricted Zone”.
- If you wish to enable access to the restricted zone from the submitting endpoint, edit the application’s Restricted Zone policy.
  - The application’s policies are selected in the Application Properties dialog box, in the General tab. For details, refer to “General Tab” on page 68.
  - Configuration of the endpoint policies is via the Policy Editors, which you can access via the General tab of the Application Properties dialog box. For details, refer to “Application Endpoint Policies” on page 99.



## **Warning #108: Unable to Retrieve Information from LDAP Server**

### **Symptoms**

A remote user logs in to the site. The login process is slower than usual.

### **Cause**

The site-to-site VPN is not configured in the ISA Server on the IAG, thus the ISA Server blocks traffic from the remote LDAP server.

### **Resolution**

At the IAG, do the following:

1. Add all remote sites to the ISA Server Internal Networks. For details, refer to the ISA Server help system.
2. Add routing entries to the Route Table, to route all traffic that is sent to the remote sites to the appropriate gateway.

